Synology®

Synology MailPlus Server Administrator's Guide

Based on MailPlus Server 2.0

Table of Contents

Chapter 1: Introduction

Chapter 2: Getting Started with MailPlus Server

Chapter 3: Mail Migration

Chapter 4: User Licenses

Chapter 5: Account Settings

Chapter 6: Protocol Settings

Chapter 7: SMTP Settings

Chapter 8: Domain Settings

Chapter 9: Security Settings

Chapter 10: Monitor Settings

Chapter 11: Disaster Recovery

Introduction

The Synology MailPlus suite is an advanced, secured email service with high usability. This suite includes two packages: **MailPlus Server** and **MailPlus**. MailPlus Server provides many management details and settings, while MailPlus provides client management and email services.

This administrator's guide will guide you through setting up MailPlus Server and provide more detailed configuration instructions including DNS settings, mail service migration, and other security adjustments. MailPlus High-availability will help you achieve continuous email services, the mail queue feature provides management options for deferred messages, and the status monitoring feature provides you an overview of MailPlus health status.

Chapter

2

Getting Started with MailPlus Server

With the Synology **MailPus Server** package, your Synology NAS can become a mail system that supports SMTP, POP3, and IMAP. User accounts and email messages can be centrally managed and archived on your Synology NAS. In addition, the **MailPlus** package provides DSM users with an easy-to-use, browser-based email client for viewing, managing, and sending messages.

The following chapter will help you get started with **MailPlus Server** and **MailPlus** on your Synology NAS.

Connect Synology NAS to the Internet

There are three ways to connect your Synology NAS to the Internet: direct connection, PPPoE connection, or connection through a router. For details on accessing your Synology NAS via the Internet, refer to **here**.

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 your 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) will provide free static IP addresses, however users must connect via PPPoE to retrieve this static IP address.
    1. Log in to **DSM**.
    2. Go **Control Panel** > **Network**.
    3. In the **Network Interface** tab, select **PPPoE**, and then click on 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 this IP address in Synology NAS.
    1. Log in to **DSM**.
    2. Go to **Control Panel** > **Network**.
    3. In the **Network Interface** tab, select a network port and click on the **Edit** button.
    4. Enter your static IP address.

Set up DNS

A valid, registered domain name is required to allow clients to deliver emails to MailPlus Server over the Internet. In addition, you'll need to set up the MX record and A record of your DNS server.

MX record, or Mail Exchanger record, is a type of resource record in the Domain Name System (DNS). It specifies how Internet email should be routed using Simple Mail Transfer Protocol (SMTP). Each MX record contains a hostname and a preference. A hostname guides emails to arrive at the right destination. A preference points out the relative priority of various servers.

For example: to make sure an email address like *alex@example.com* works properly, you have to set up the MX record of the domain *example.com*. To do so, you need to point the MX record to the IP address or domain name of your Synology NAS. If you already have registered a domain name, you'll be able to modify these settings in the management console for that domain name.

- **A record**: example.com > 111.222.112.223
- **MX record**: example.com > nas.example.com with priority 0.

For example: to make sure *alex@example.com* receives emails properly, you are required to set up the MX record for *example.com*, pointing the MX record of this domain to your Synology MailPlus Server. If the domain *example.com* is only used on Synology MailPlus Server, then when setting the MX record, the **Host** and **Points to** settings can be the same. The lower the number set in the priority setting, the higher the priority.

Reverse DNS setup

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

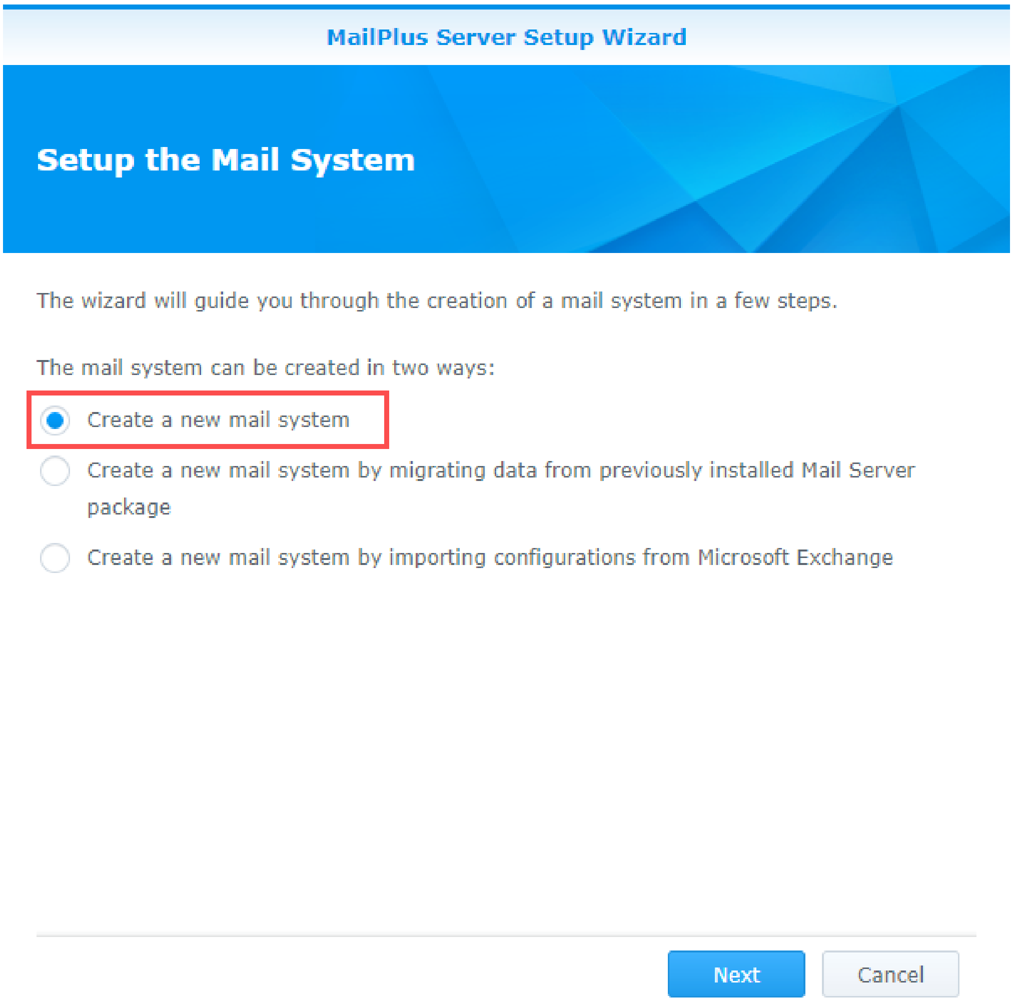
- **What is reverse DNS?** Reverse DNS refers to translating the numeric addresses of a website (i.e. the IP address) to the domain/hostname, as opposed to the forward DNS process which translates the domain/hostname to the IP address. Reverse DNS refers also to locating which domain name/host belongs 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 also be accessed by just using the IP address.
- **What does reverse DNS do?** Why would you need a reverse DNS set up for your mail server? Reverse DNS is one of the basic requirements for running a mail system. It is often used as a spam filter to determine whether the IP address of the 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 services. If you cannot set up reverse DNS by yourself and keep on experiencing email delivery problems, please add another SMTP server for normal email delivery. We recommend that you use a more well-known SMTP server to avoid being taken as spammer when sending an email.
- **How to set up Reverse DNS?** Set up Reverse DNS on your own host -- Some ISPs may delegate a portion of the zone to you so that you can host your 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 assigned to you. It may be either your host or yourself, if the host has delegated the Reverse DNS for your IP space (containing one or multiple IP addresses) to you. A PTR record usually represents the IP entered backwards, 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 the 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 see how to enable SMTP (Simple Mail Transfer Protocol). Please remember that the screenshots below are for reference only, and your settings may differ.

1 Go to **Package Center** to find and install **MailPlus Server**.

2 Launch **MailPlus Server**, and choose **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 choose to **Create a mail system by migrating the data from a previously installed Mail Server Package**. Check the tutorial on how to migrate Mail Server to MailPlus Server **here**.



MailPlus Server Setup Wizard

Setup the Mail System

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

The mail system can be created in two ways:

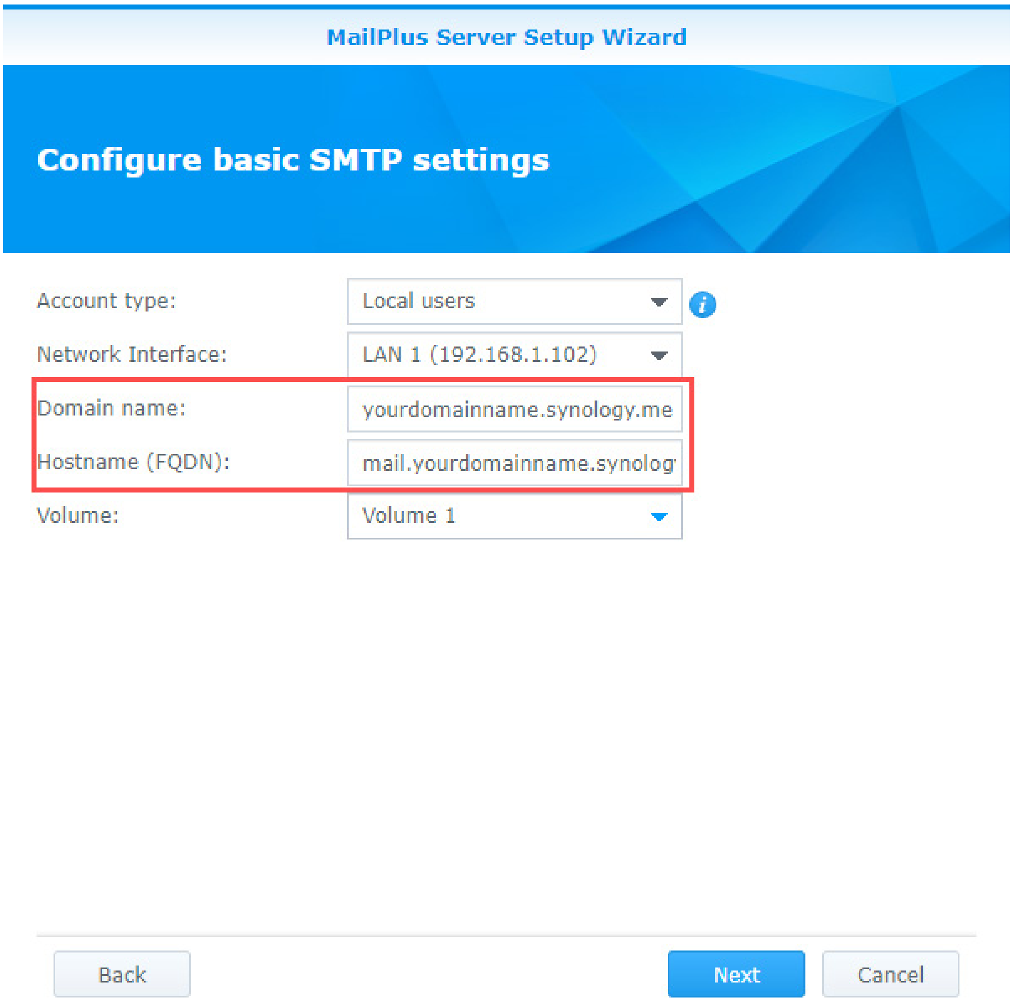
● Create a new mail system

○ Create a new mail system by migrating data from previously installed Mail Server package

○ Create a new mail system by importing configurations from Microsoft Exchange

3 Enter your domain name and hostname (FQDN).

- **Domain name**: Domain name is the location or address where email messages are received. Please check if your domain name matches the MX records from your DNS settings.
- **Hostname (FQDN)**: The hostname is the address of your MailPlus Server. Please check if the hostname matches the A records from your DNS settings.



MailPlus Server Setup Wizard

Configure basic SMTP settings

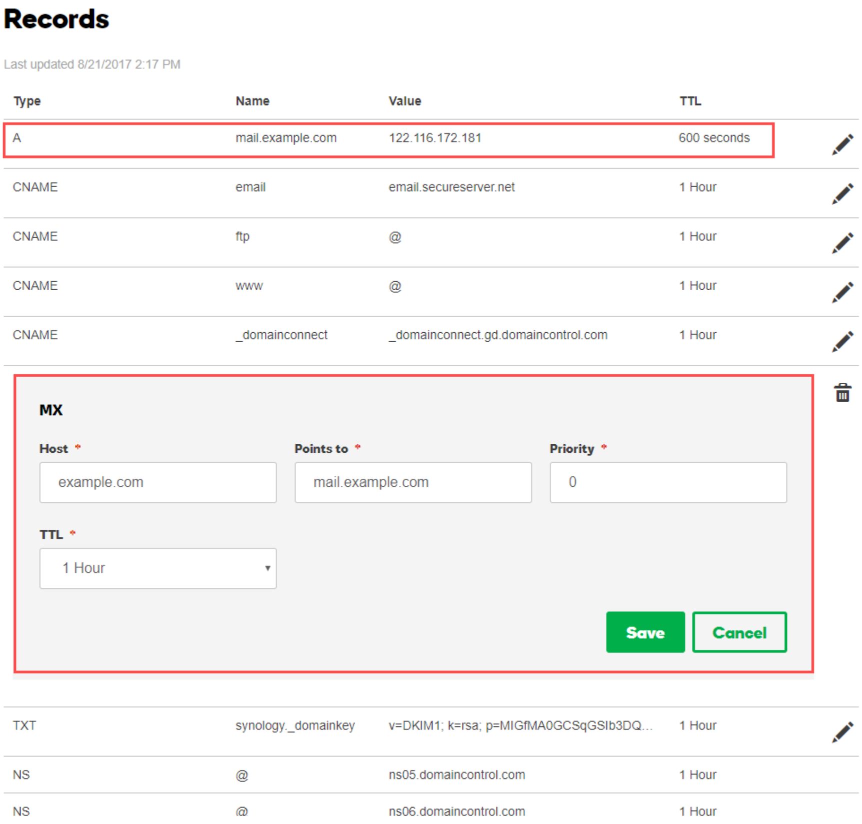
Account type:	Local users
Network Interface:	LAN 1 (192.168.1.102)
Domain name:	yourdomainname.synology.me
Hostname (FQDN):	mail.yourdomainname.synolog
Volume:	Volume 1

- For example: if your domain name is *example.com*, then your MailPlus Server address will be set up under *mail.example.com*, you can refer to the following instructions to complete this setup.

1 When setting up the A record, point “mail.example.com” to the static IP address of MailPlus Server.

2 When setting up the MX record, enter “example.com” in the **Host** field, “mail.example.com” in the **Points to** field, and “0” in the **Priority** field.

3 In MailPlus Server, set the domain name as “example.com”, and the hostname (FQDN) as “mail.example.com”.



Records

Last updated 8/21/2017 2:17 PM

Type	Name	Value	TTL
A	mail.example.com	122.116.172.181	600 seconds
CNAME	email	email.secureserver.net	1 Hour
CNAME	ftp	@	1 Hour
CNAME	www	@	1 Hour
CNAME	_domainconnect	_domainconnect.gd.domaincontrol.com	1 Hour

MX

Host *: example.com

Points to *: mail.example.com

Priority *: 0

TTL *: 1 Hour

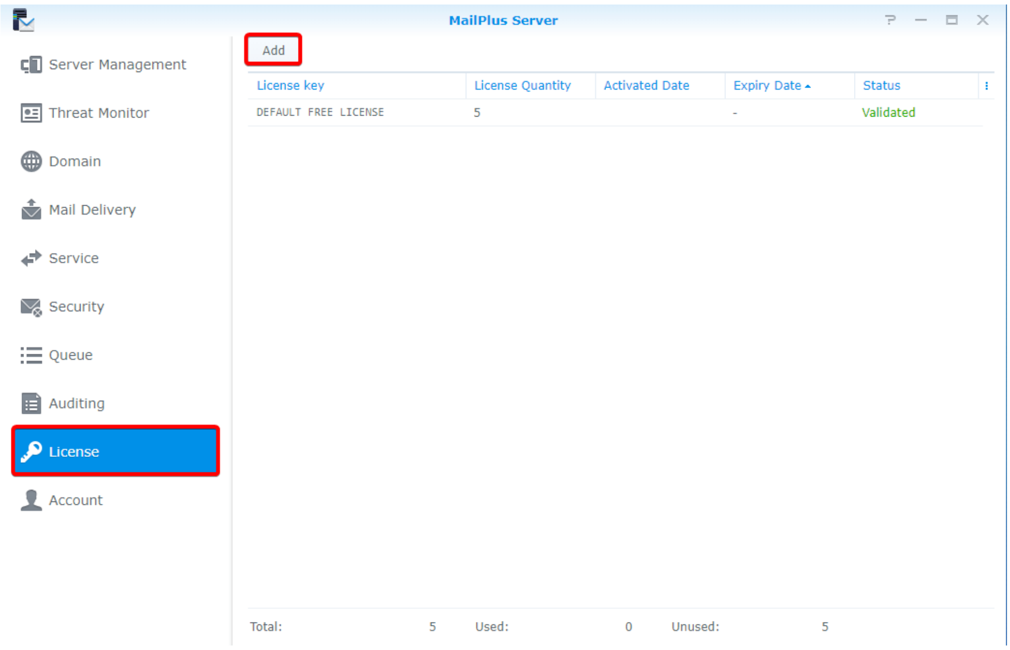
Type	Name	Value	TTL
TXT	synology._domainkey	v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQ...	1 Hour
NS	@	ns05.domaincontrol.com	1 Hour
NS	@	ns06.domaincontrol.com	1 Hour

4 You can modify the following additional 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 to be used for MailPlus Server.
- **Volume**: Select a volume in which MailPlus Server and its data will be stored.

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

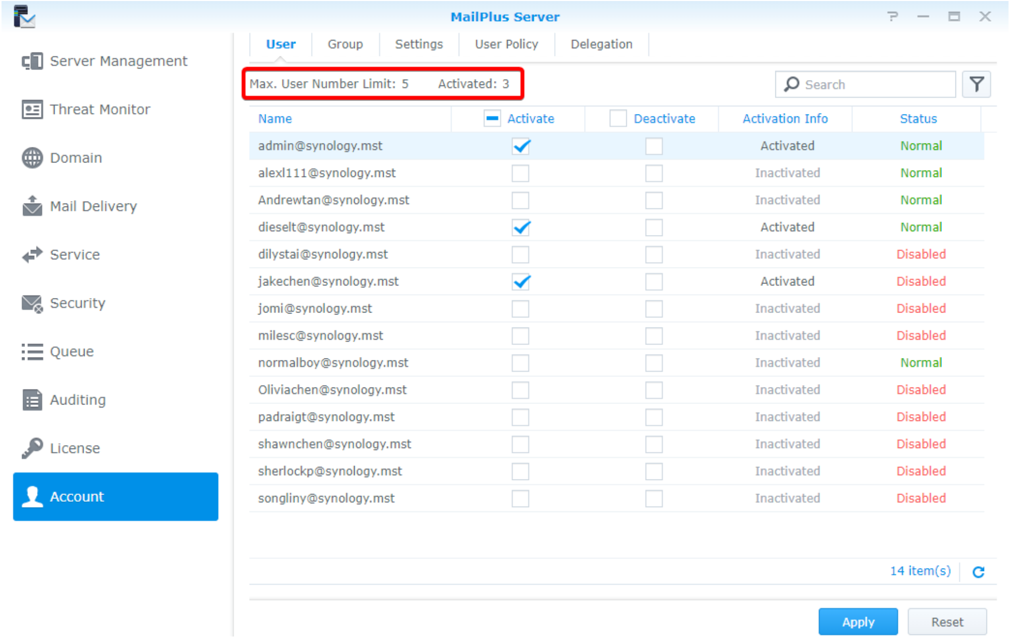
6 MailPlus Server is installed with 5 free email accounts by default, and you can add more licenses in the **License** page if you need to activate more email accounts. For more information on the MailPlus license mechanism, please refer to **here**.



License key	License Quantity	Activated Date	Expiry Date	Status
DEFAULT FREE LICENSE	5		-	Validated

Total: 5 Used: 0 Unused: 5

7 Please go to the **Account** page to activate email accounts. You can choose to activate users or groups, and on the upper left corner you can view the total number of users that can be activated. For more information, please refer to the **Activate accounts** section.



Max. User Number Limit: 5 Activated: 3

Name	Activate	Deactivate	Activation Info	Status
admin@synology.mst	☑	□	Activated	Normal
alexl111@synology.mst	□	□	Inactivated	Normal
Andrewtan@synology.mst	□	□	Inactivated	Normal
dieselt@synology.mst	☑	□	Activated	Normal
dilystai@synology.mst	□	□	Inactivated	Disabled
jakechen@synology.mst	☑	□	Activated	Disabled
jomi@synology.mst	□	□	Inactivated	Disabled
milesc@synology.mst	□	□	Inactivated	Disabled
normalboy@synology.mst	□	□	Inactivated	Normal
Oliviachen@synology.mst	□	□	Inactivated	Disabled
padraigt@synology.mst	□	□	Inactivated	Disabled
shawnchen@synology.mst	□	□	Inactivated	Disabled
sherlockp@synology.mst	□	□	Inactivated	Disabled
songliny@synology.mst	□	□	Inactivated	Disabled

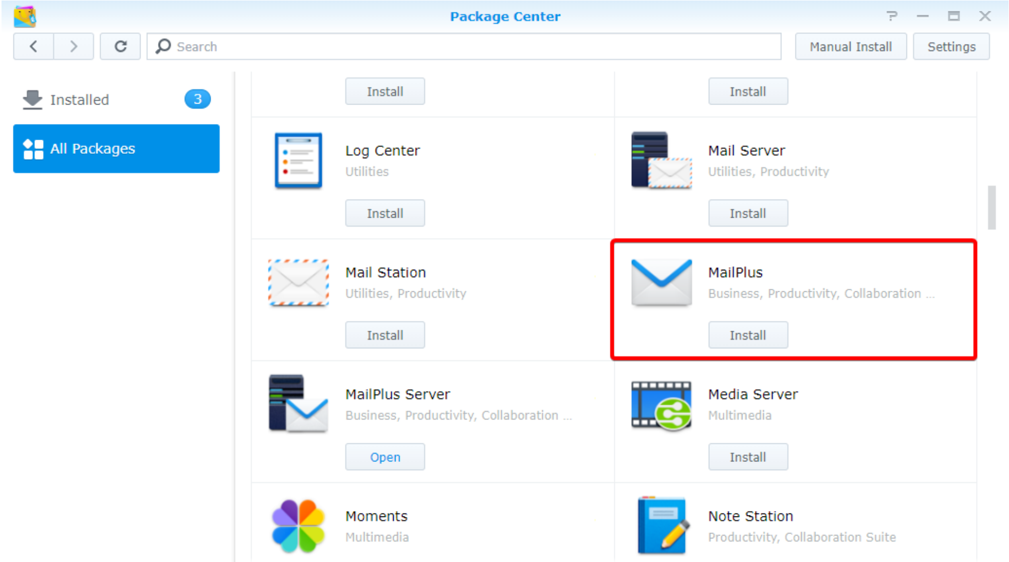
Set up MailPlus Email Client

Access emails on Synology NAS with MailPlus

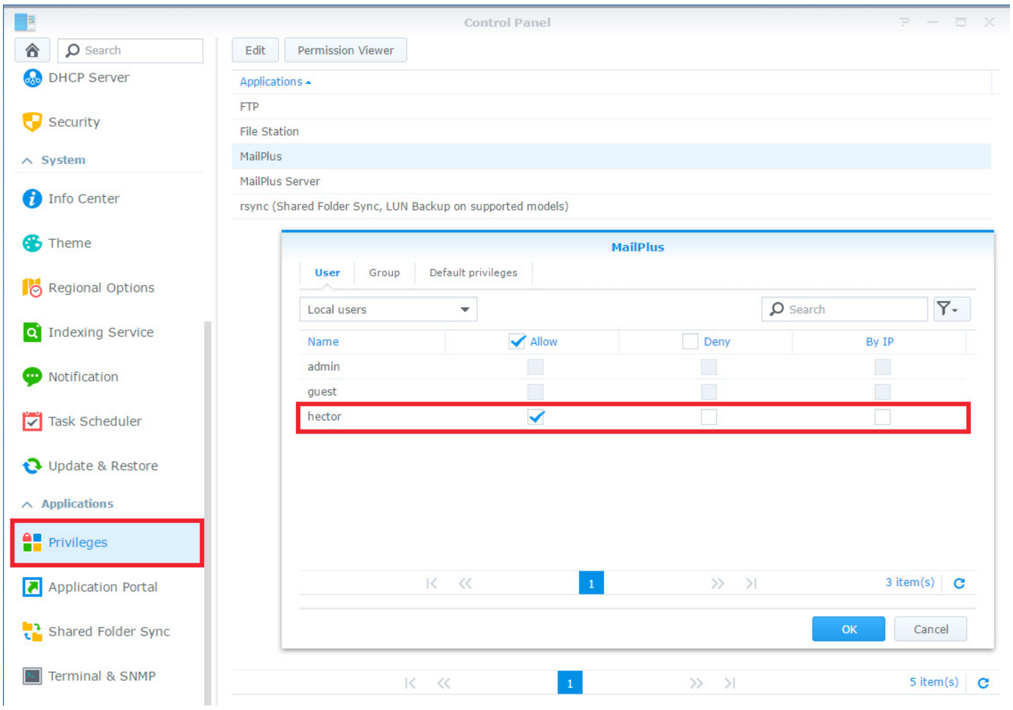
MailPlus is an add-on package that provides a web-based interface for users to access and manage emails hosted on the Synology NAS. In addition, multiple POP3 accounts can be created in MailPlus, allowing users to receive and store messages with other email services (e.g., Gmail, Office 365).

Install MailPlus

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



2 Go to **Control Panel** > **Privileges**, and allow your accounts to access **MailPlus**.

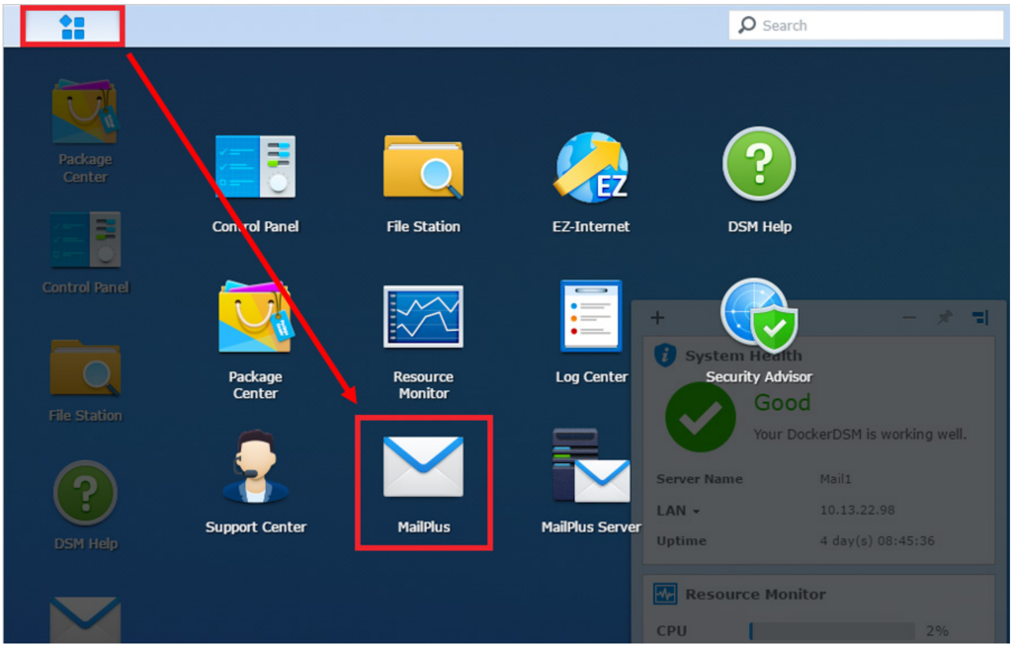


Name	☑ Allow	□ Deny	By IP
admin	□	□	□
guest	□	□	□
hector	☑	□	□

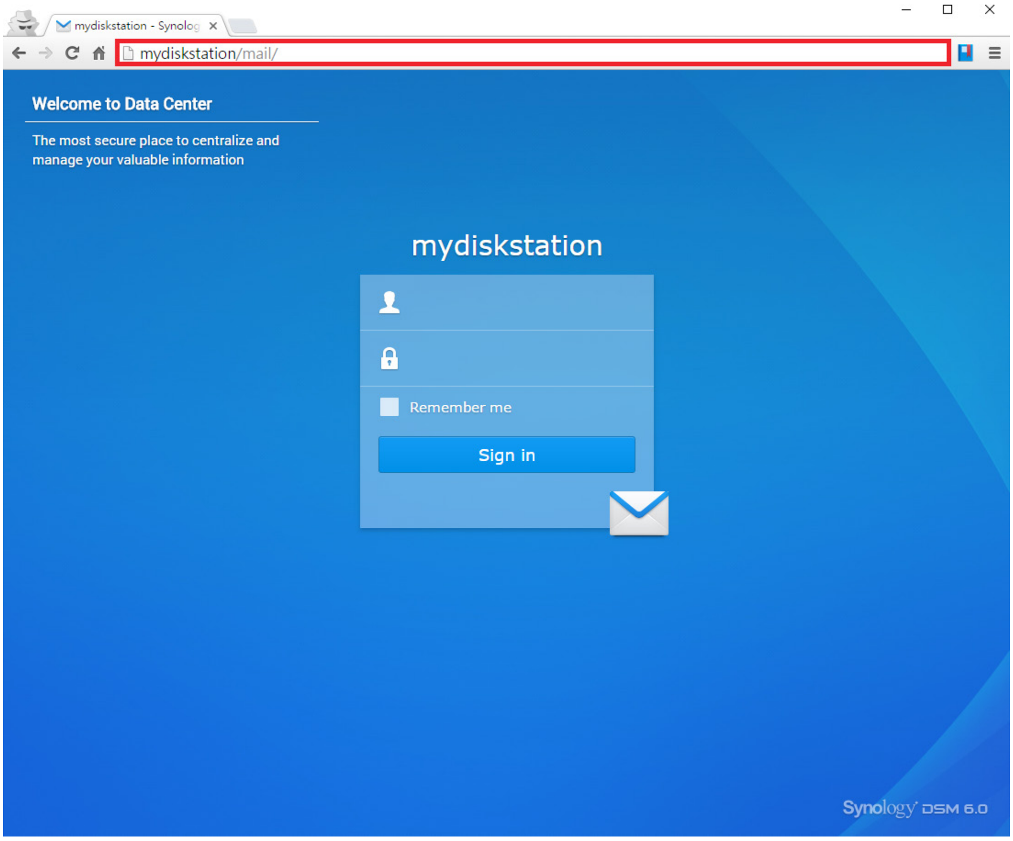
Run MailPlus

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

- Go to Main Menu > MailPlus.



- Access MailPlus directly via Application Portal. Enter the name of your Synology NAS followed by "/mail" in the address bar of your web browser. For example, if your Synology NAS is called *mydiskstation*, enter *mydiskstation/mail*. Please find how to enable Application Portal here.



Welcome to Data Center

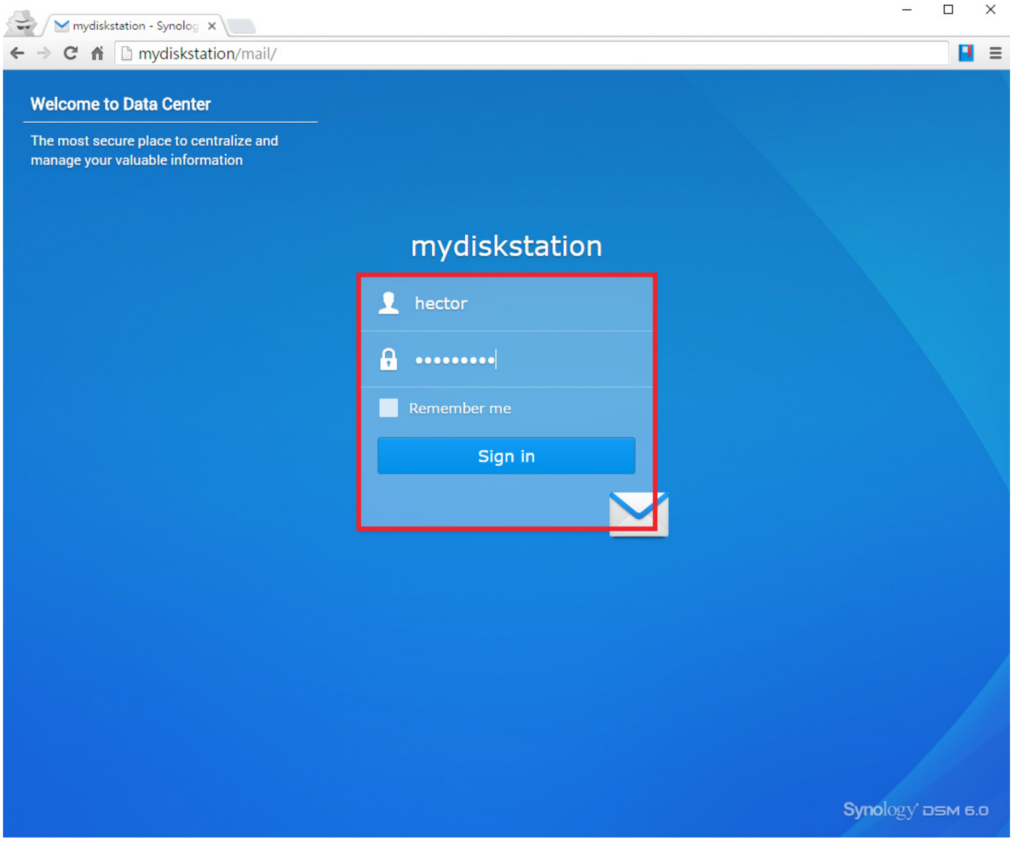
The most secure place to centralize and manage your valuable information

mydiskstation

□ Remember me

Sign in

2 Enter your DSM username and password to log in.



Welcome to Data Center

The most secure place to centralize and manage your valuable information

mydiskstation

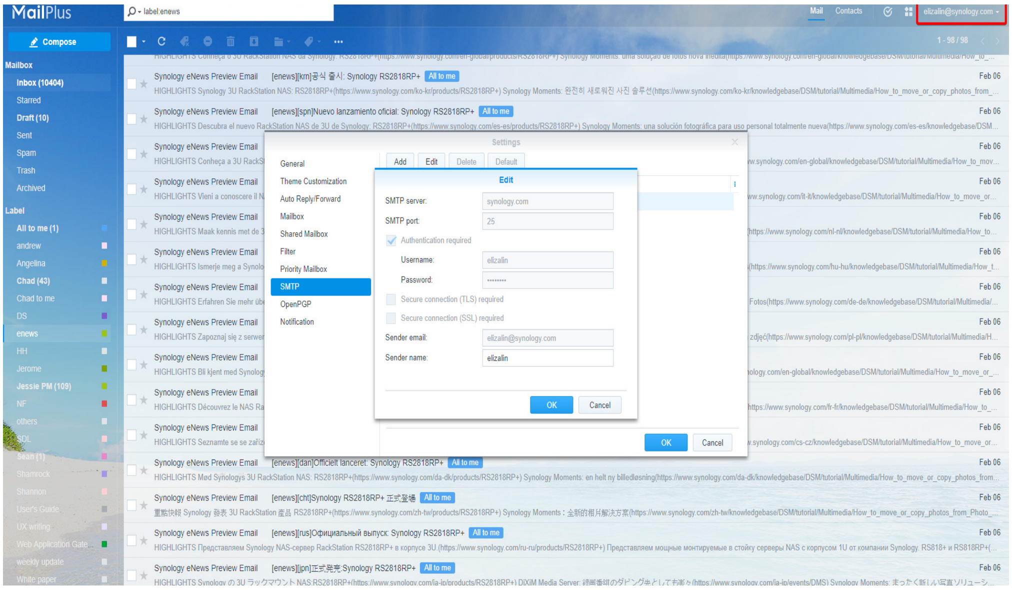
hector

•••••••••

□ Remember me

Sign in

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



Edit

SMTP server: synology.com

SMTP port: 25

☑ Authentication required

Username: elizalin

Password: ••••••••

□ Secure connection (TLS) required

□ Secure connection (SSL) required

Sender email: elizalin@synology.com

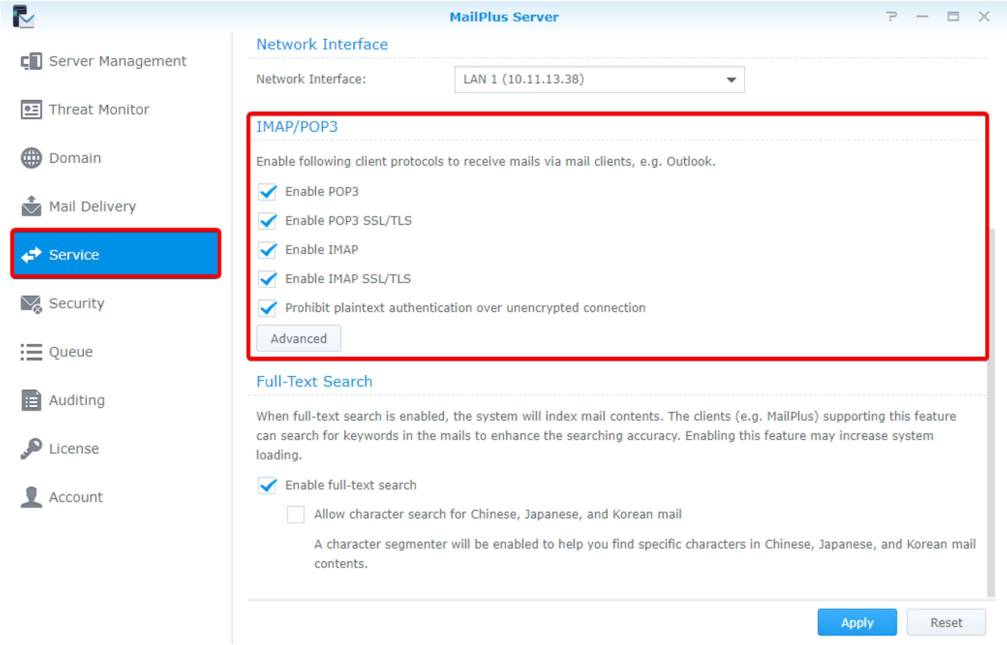
Sender name: elizalin

Third Party Email Clients

Access emails on Synology NAS with other email clients

Email accounts on the 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 the Synology NAS.

1 Launch **MailPlus Server**, and go to the **Service** page to enable IMAP or POP3 depending on the client.



Network Interface

Network Interface: LAN 1 (10.11.13.38)

IMAP/POP3

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

☑ Enable POP3

☑ Enable POP3 SSL/TLS

☑ Enable IMAP

☑ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Advanced

Full-Text Search

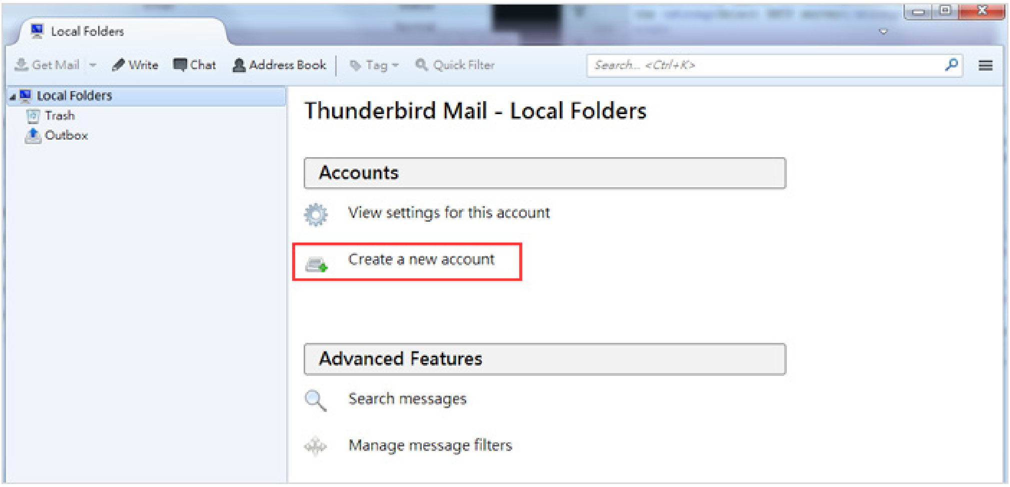
When full-text search is enabled, the system will index mail contents. The clients (e.g. MailPlus) supporting this feature can search for keywords in the mails to enhance the searching accuracy. Enabling this feature may increase system loading.

☑ Enable full-text search

□ Allow character search for Chinese, Japanese, and Korean mail

A character segmenter will be enabled to help you find specific characters in Chinese, Japanese, and Korean mail contents.

2 Launch Thunderbird on your computer, and click **Create a new account**.



Thunderbird Mail - Local Folders

Accounts

View settings for this account

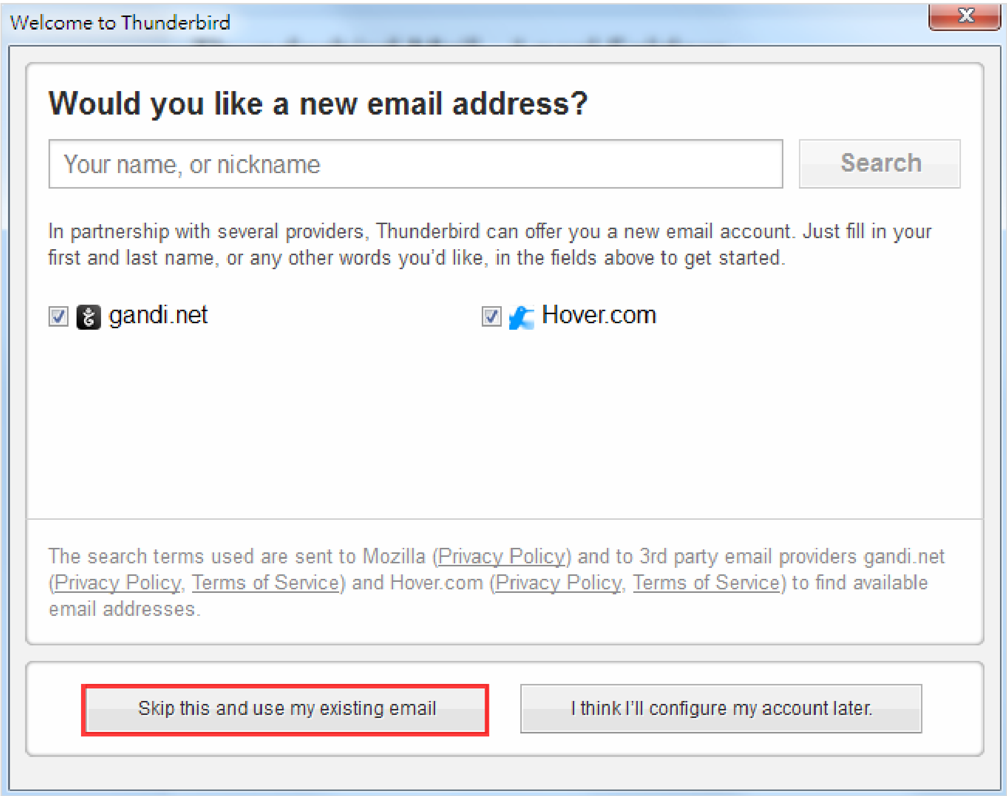
Create a new account

Advanced Features

Search messages

Manage message filters

3 Click **Skip this and use my existing email**.


Welcome to Thunderbird

Would you like a new email address?

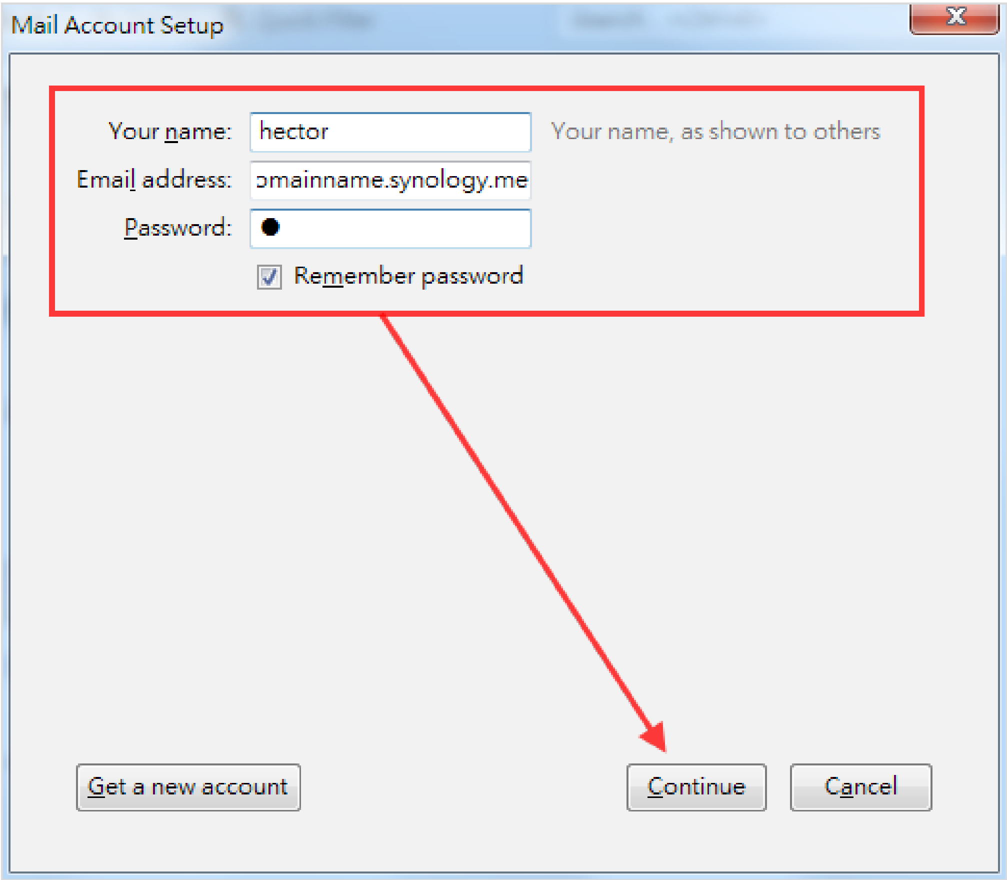
In partnership with several providers, Thunderbird can offer you a new email account. Just fill in your first and last name, or any other words you'd like, in the fields above to get started.

☑ gandi.net ☑ Hover.com

The search terms used are sent to Mozilla (Privacy Policy) and to 3rd party email providers gandi.net (Privacy Policy, Terms of Service) and Hover.com (Privacy Policy, Terms of Service) to find available email addresses.

Skip this and use my existing email
I think I'll configure my account later.

4 Enter the name, email address, and password for your DSM user account. (For example, *hector@mydomainname.synology.me*.) Click **Continue**.



Mail Account Setup

Your name: hector

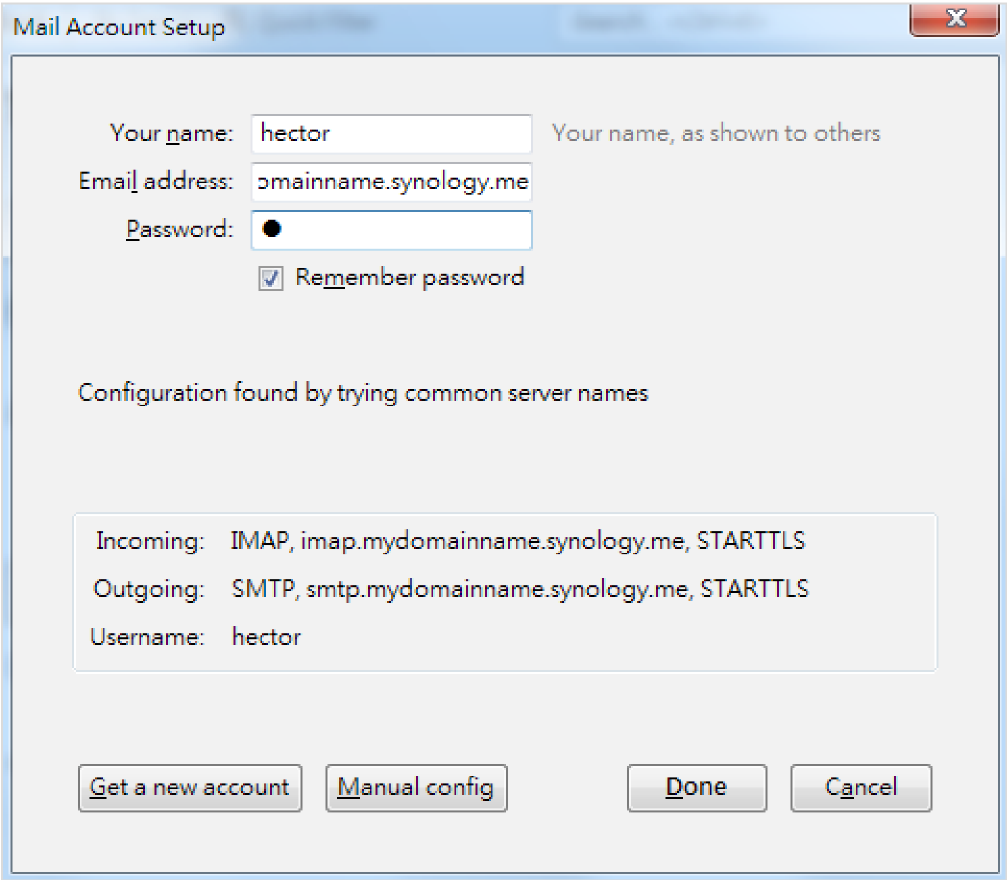
Your name, as shown to others

Email address: ɔmainname.synology.me

Password: ●

☑ Remember password

5 Thunderbird searches for your address. If your settings are correct, you'll see the screen below.



Mail Account Setup

Your name: hector

Your name, as shown to others

Email address: ɔmainname.synology.me

Password: ●

☑ Remember password

Configuration found by trying common server names

Incoming: IMAP, imap.mydomainname.synology.me, STARTTLS

Outgoing: SMTP, smtp.mydomainname.synology.me, STARTTLS

Username: hector

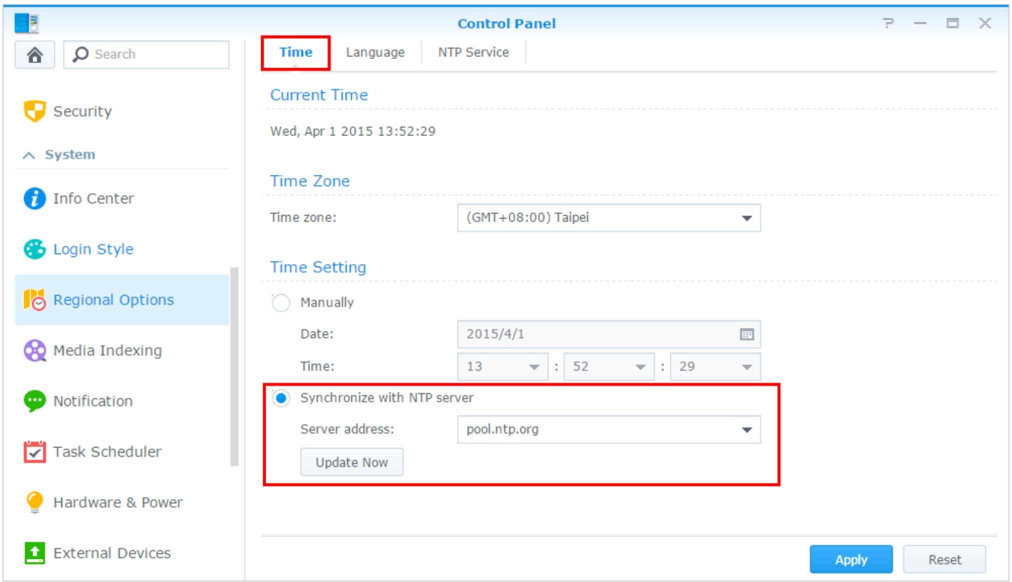
6 Now the email of the selected account will be displayed in Thunderbird!

Troubleshoot

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

1 Check if the settings on your MailPlus such as SMTP, DNS, and MX are correct.

2 Check if the Internet settings of your Synology NAS are correct. Go to **Control Panel** > **Regional Options**. Under the **Time** tab, tick **Synchronize with a 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.



Current Time

Wed, Apr 1 2015 13:52:29

Time Zone

Time zone: (GMT+08:00) Taipei

Time Setting

○ Manually

Date: 2015/4/1

Time: 13 : 52 : 29

● Synchronize with NTP server

Server address: pool.ntp.org

Update Now

Apply Reset

3 Check if the port number on your router is correct.

4 Please visit this **website** to check if your IP is listed as spammer. If so, remove your IP from the block list on the same website.

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

1 Check if you have enabled protocols for IMAP and POP3.

2 Check if your username and password are correct.

3 Check if the settings on your MailPlus such as SMTP, DNS, and MX are correct.

4 Check if the Internet settings of your Synology NAS are correct. Go to **Control Panel** > **Regional Options**. Under the **Time** tab, tick **Synchronize with a NTP server** and click on **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 Check if your IP is listed as spammer. Go to **http://www.spamhaus.org/sbl/** to check out. If so, remove your IP from the block list on the same website.

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

1 Make sure the DNS is correctly configured. You will need to point the MX and A records to Synology NAS, so that other email servers can find the Synology NAS.

2 Make sure 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 **http://canyouseeme.org/** and inputting the port 25.

4 Check the message in the returned mail if any. So you can find the detailed reason of the 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 the sender. If your reverse DNS lookup doesn't correspond to the sending domain name, you emails will be rejected. Please check with your ISP. Another possibility is that your IP address is listed in the SPAM block list. You can check this by visiting this **website**.

Mail Migration

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

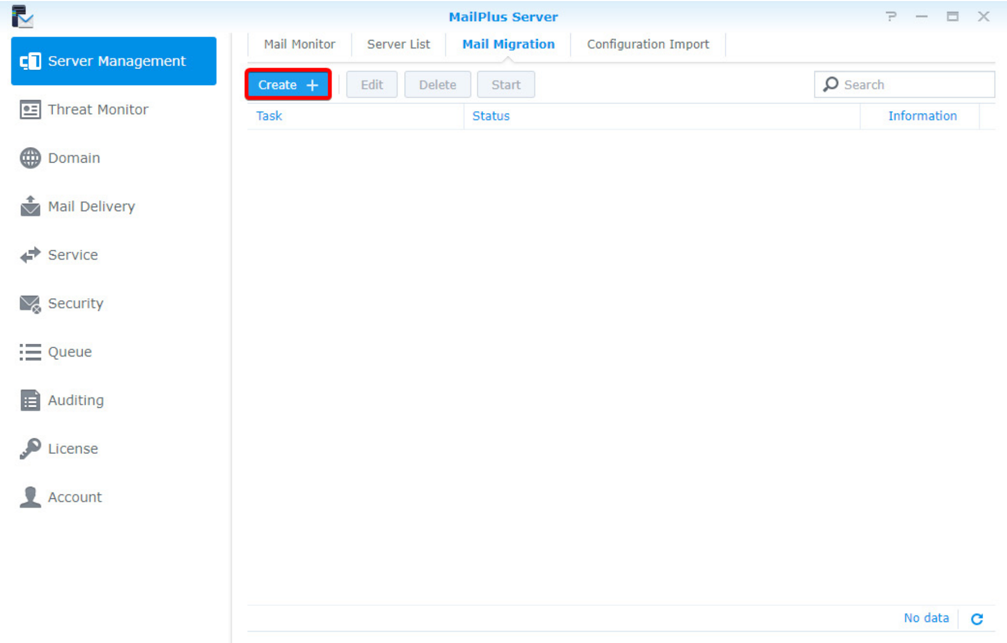
- Make sure your Synology NAS is running DSM 6.0 or later, and supports MailPlus Server (See the applied models here).
- Set up MailPlus Server on your Synology NAS to be the destination mail server.
- Collect the usernames and passwords of the source accounts and those of the matching MailPlus Server accounts.

Create a mail migration task on MailPlus Server

Log in to MailPlus Server and go to **Server Management** > **Mail Migration**, and click the **Create** button to create a mail migration task. Then, specify the task settings on the following tabs as instructed. In this chapter, Microsoft Exchange will be used as an example for demonstration purposes.

Configure general task settings

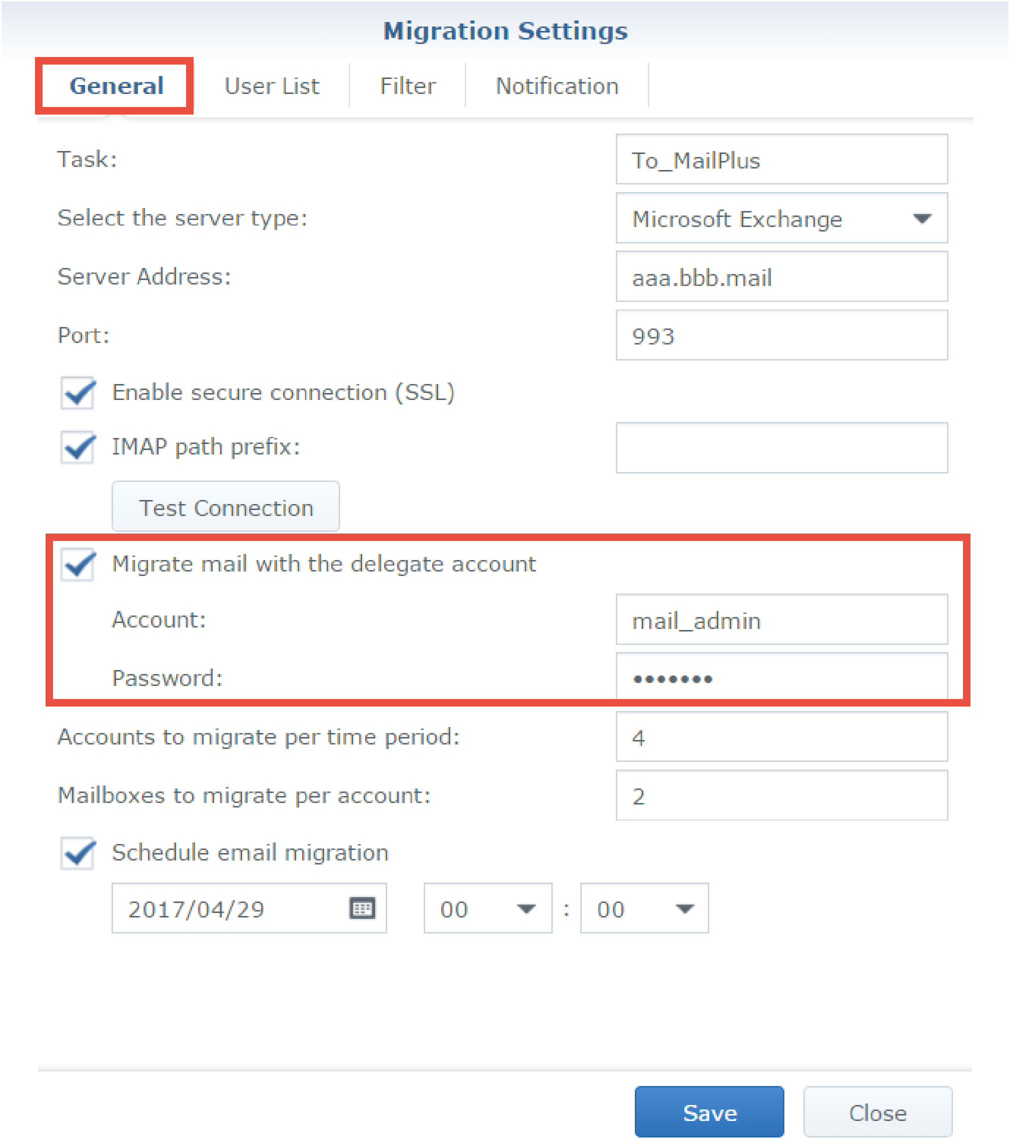
1 Go to **Server Management** > **Mail Migration**, and click the **Create** button.



2 Go to the **General** tab in the **Migration Settings** window, set **Select the server type** to **Microsoft Exchange** and fill in required information of the source Microsoft Exchange server.

3 To know the **IMAP path prefix**, check the settings of the source Microsoft Exchange server.

4 If you have a delegate account on the source server that has full access permissions of all the other source accounts, select **Migrate mail with the delegate account** and fill in its account credentials. This account allows you to migrate emails without acquiring access permissions of each source account.



Migration Settings

Task: To_MailPlus

Select the server type: Microsoft Exchange

Server Address: aaa.bbb.mail

Port: 993

☑ Enable secure connection (SSL)

☑ IMAP path prefix:

☑ Migrate mail with the delegate account

Account: mail_admin

Password: •••••••

Accounts to migrate per time period: 4

Mailboxes to migrate per account: 2

☑ Schedule email migration

2017/04/29 00 : 00

5 Specify the settings for **Accounts to migrate per time period** and **Mailboxes to migrate per account** according to the source server's capability. For example, Microsoft Exchange Server 2013 allows at most 16 mailboxes to migrate per account.

Note: To know how to migrate emails from other sources (e.g. Gmail or Yahoo Mail), please see this **help article**.

Import a user list

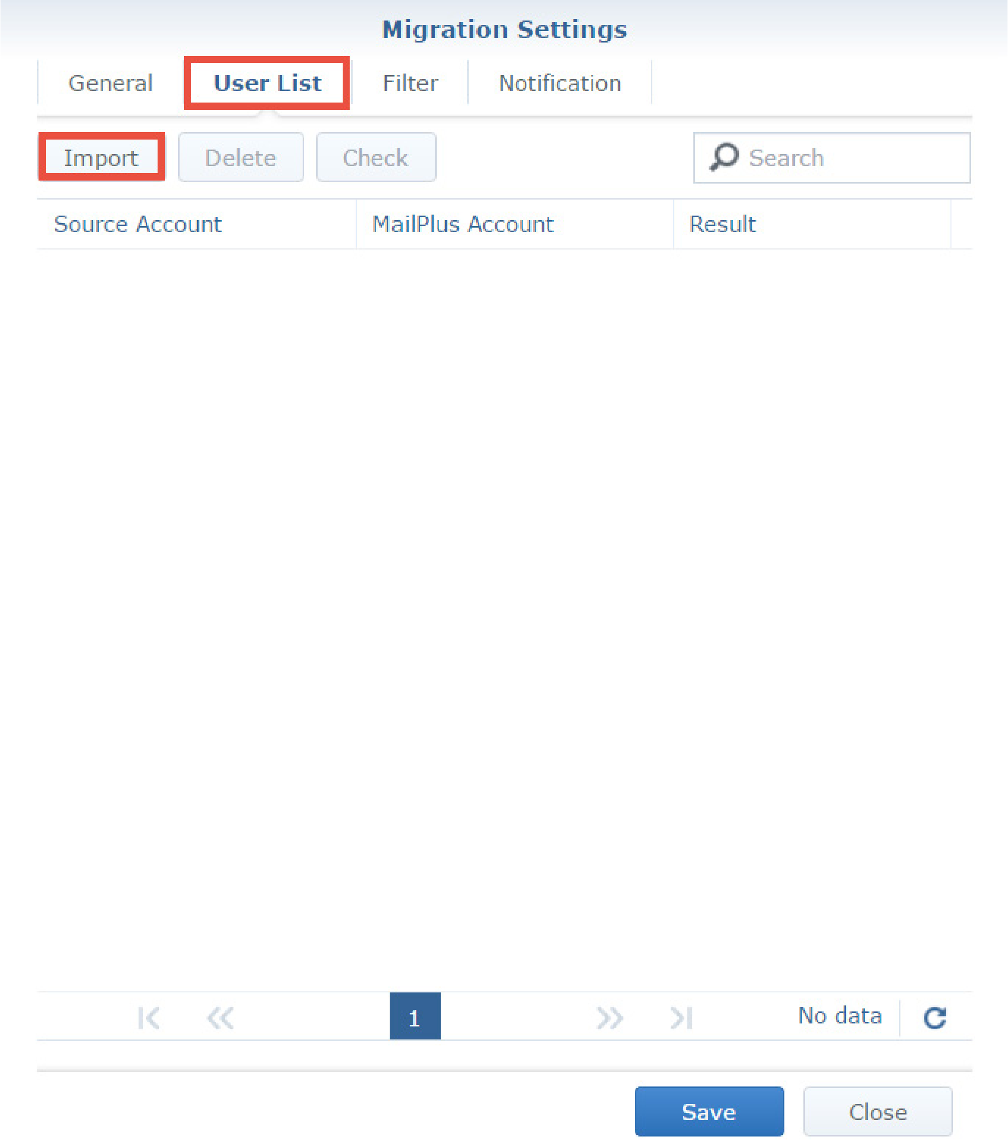
1 Prepare a user list following the requirements below:

- The user list should be a CSV file. It can be generated with Microsoft Excel or Google spreadsheets.
- List one user account information in one row.
- List each user's following types of 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 passwords (e.g. source_account_X,,MailPlus_Server_account_X).

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

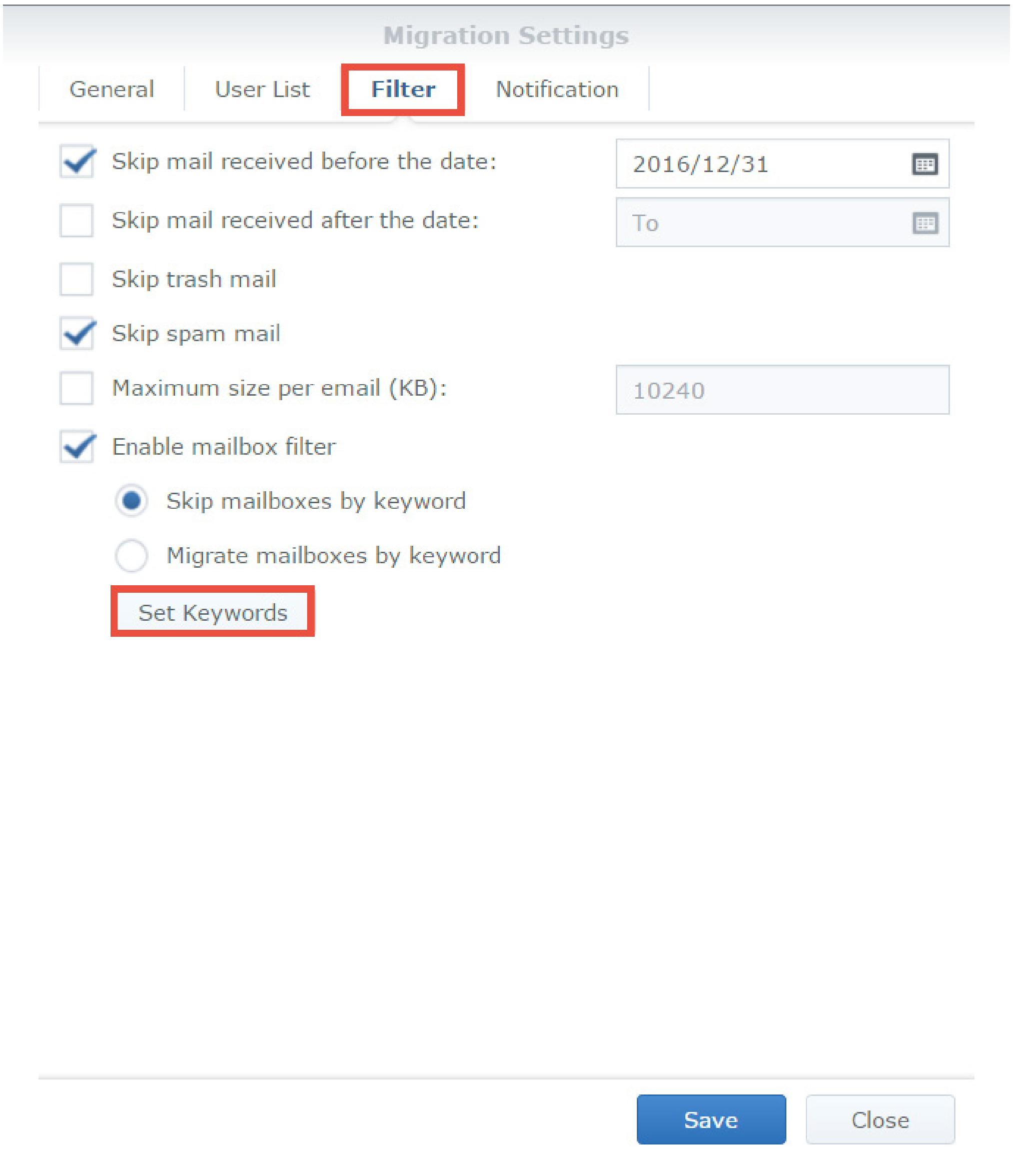
source_account_1,source_account_1_password,MailPlus_Server_account_1
source_account_2,source_account_2_password,MailPlus_Server_account_2
source_account_3,source_account_3_password,MailPlus_Server_account_3
...
source_account_N,source_account_N_password,MailPlus_Server_account_N

3 Go to **User List**. There you can import the list and check if all the account data are correct.



Set up email and mailbox filters

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



☑ Skip mail received before the date: 2016/12/31

□ Skip 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

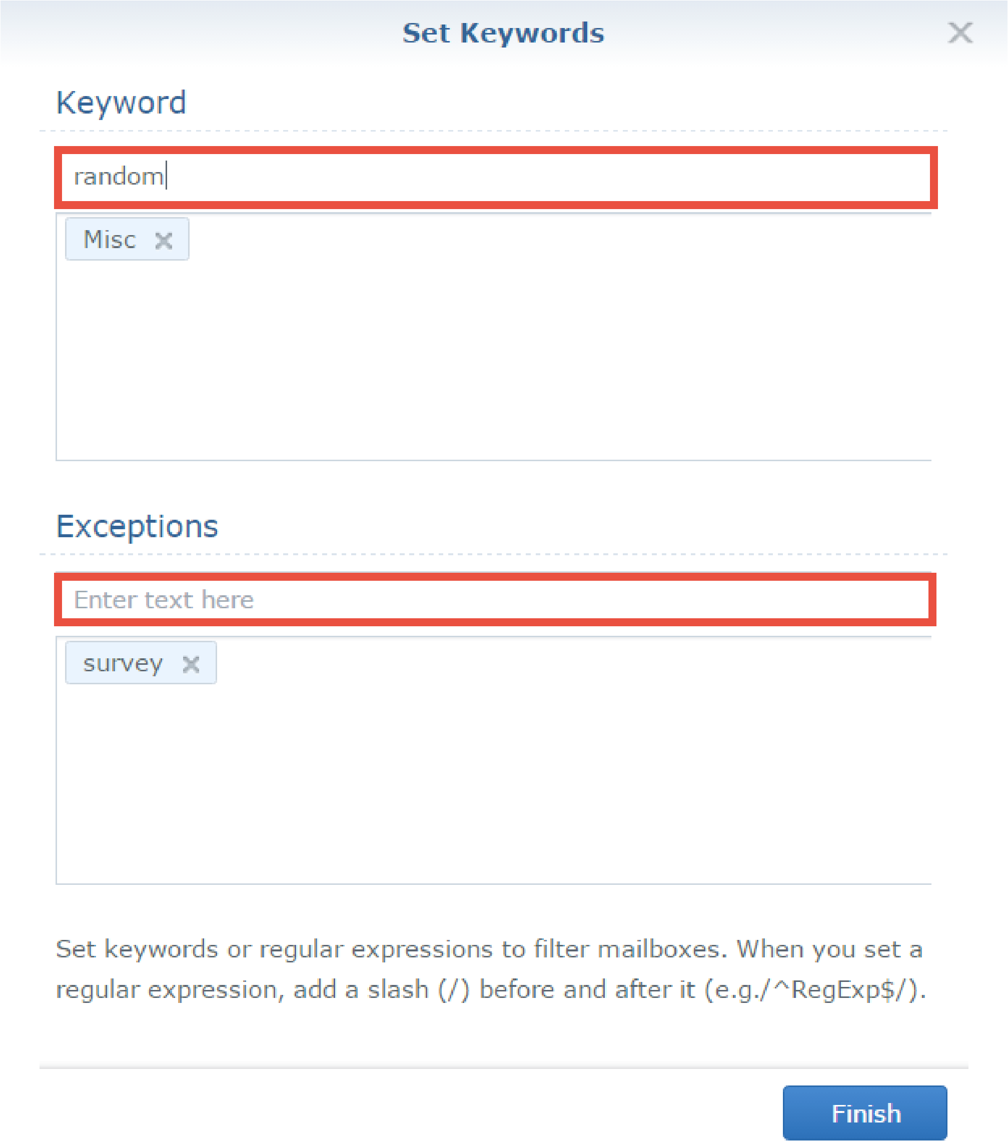
Set Keywords

2 To filter mailboxes with keywords, select **Enable mailbox filter** and the 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 matched mailboxes according to the filter policy.
- **Exceptions**: Enter text so that matched mailboxes will not be processed according to the filter policy.

4 You can enter regular expressions in the two areas when they are surrounded by a slash on each side (e.g. /REGULAR_EXPRESSION/).

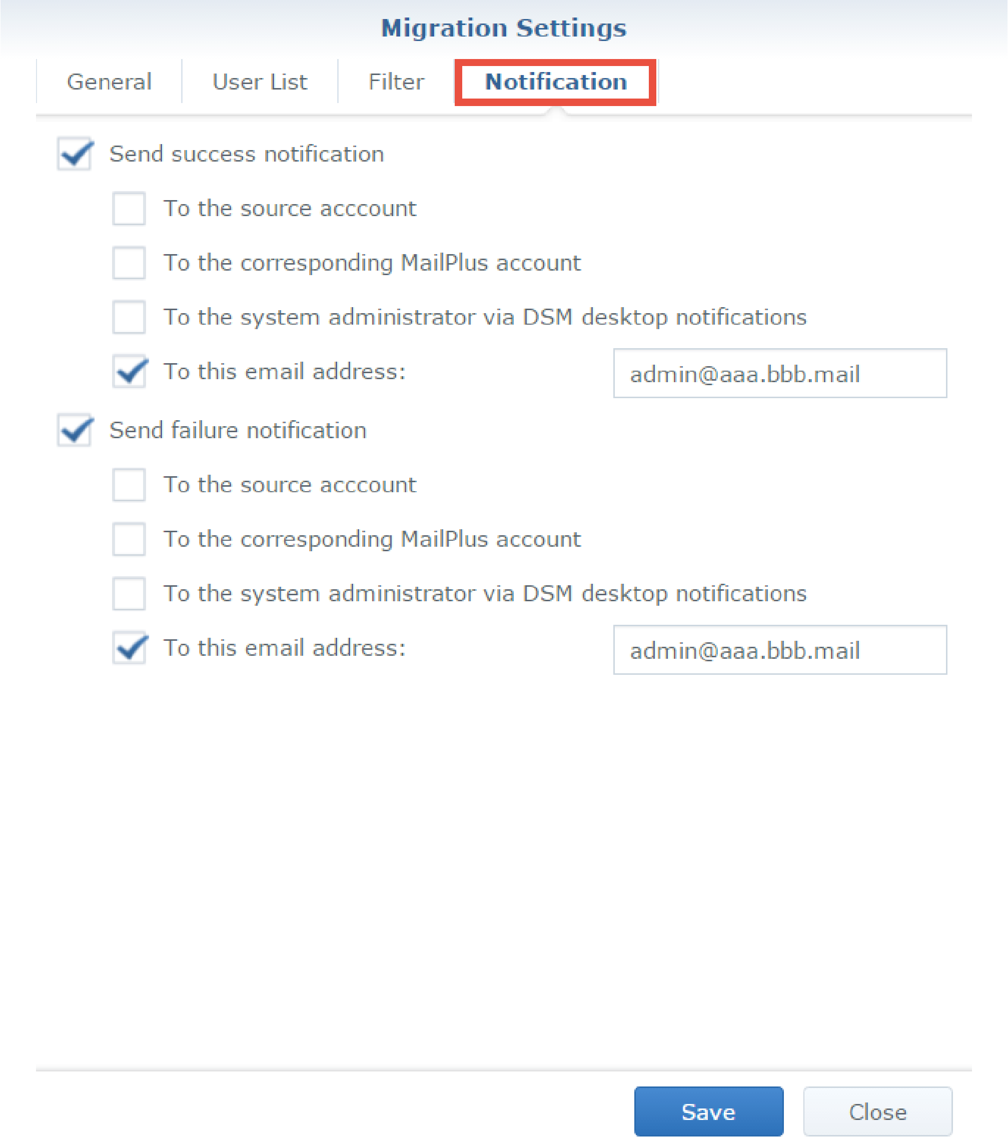


Set keywords or regular expressions to filter mailboxes. When you set a regular expression, add a slash (/) before and after it (e.g./^RegExp$/).

Set up migration notifications

1 Make sure **Enable SMTP** (at **Protocol** > **SMTP**) is selected on MailPlus Server to allow notification delivery.

2 On the **Notification** tab, determine whether MailPlus Server should send notifications of each account's migration result and where the administrator should receive them.



Migration Settings

☑ Send success notification

□ To the source acccount

□ 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 acccount

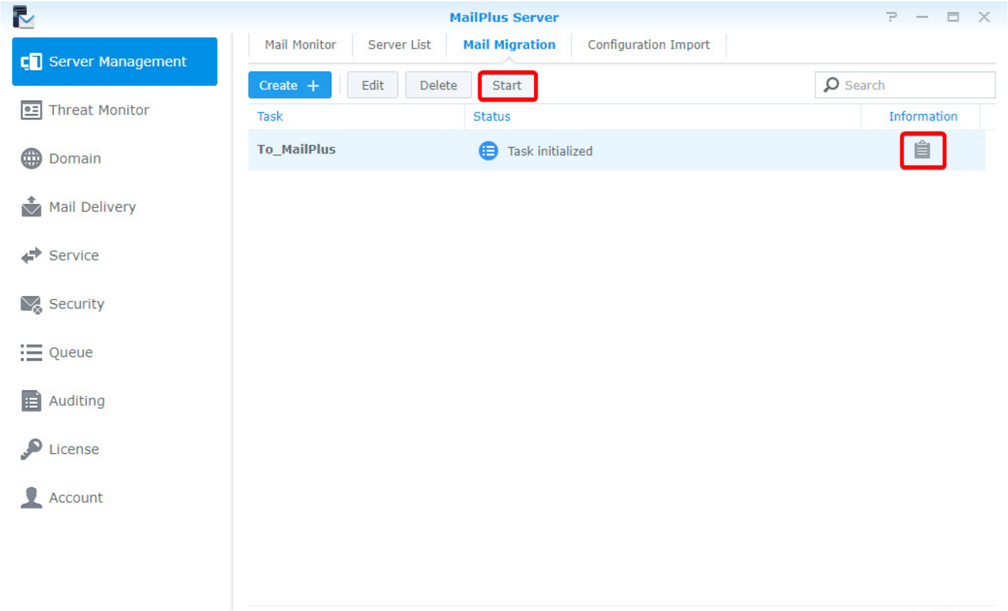
□ To the corresponding MailPlus account

□ To the system administrator via DSM desktop notifications

☑ To this email address: admin@aaa.bbb.mail

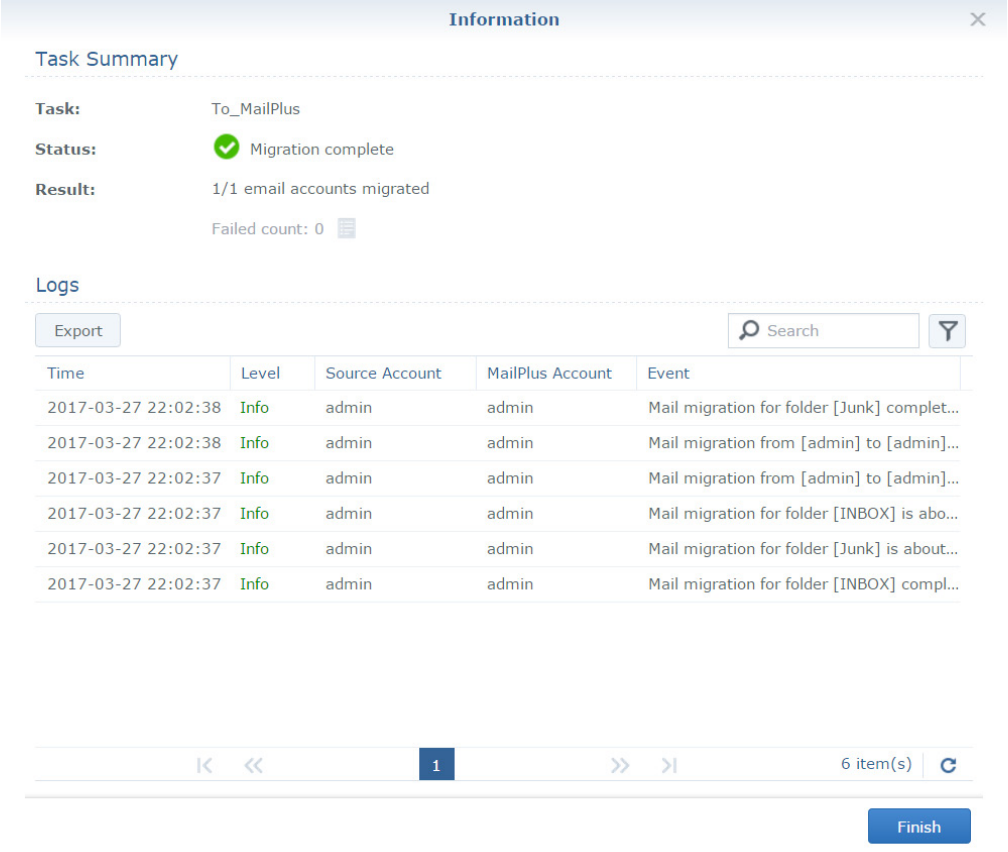
Run a mail migration task

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



Task	Status	Information
To_MailPlus	Task initialized	

2 To see migration statistics and logs, click **Information** (the document icon).



Information

Task Summary

Task: To_MailPlus

Status: Migration complete

Result: 1/1 email accounts migrated

Failed count: 0

Logs

Time	Level	Source Account	MailPlus Account	Event
2017-03-27 22:02:38	Info	admin	admin	Mail migration for folder [Junk] complet...
2017-03-27 22:02:38	Info	admin	admin	Mail migration from [admin] to [admin]...
2017-03-27 22:02:37	Info	admin	admin	Mail migration from [admin] to [admin]...
2017-03-27 22:02:37	Info	admin	admin	Mail migration for folder [INBOX] is abo...
2017-03-27 22:02:37	Info	admin	admin	Mail migration for folder [Junk] is about...
2017-03-27 22:02:37	Info	admin	admin	Mail migration for folder [INBOX] compl...

How to 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.

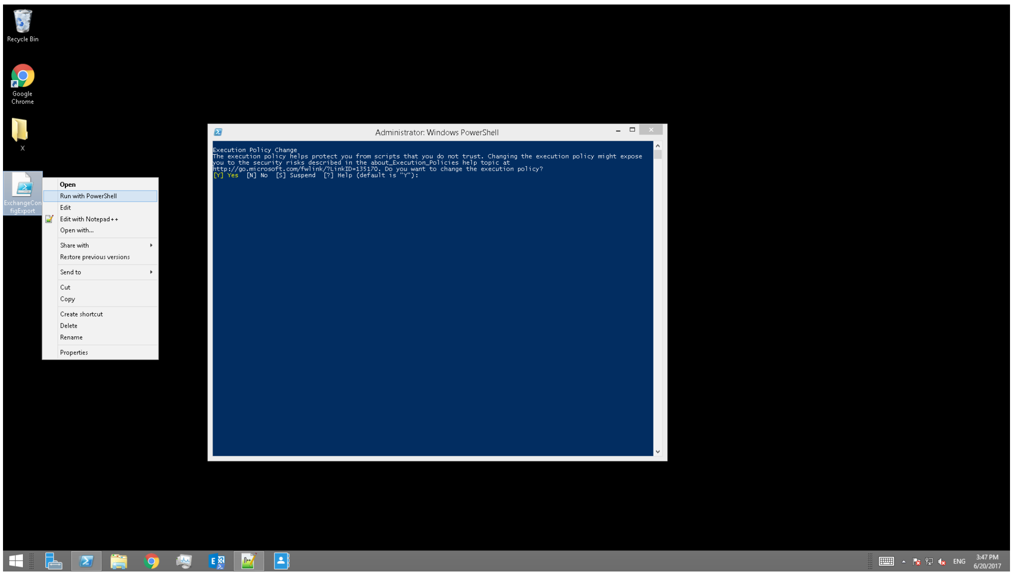
Export system configurations and aliases from Microsoft Exchange

1 Download the script file (**ExchangeConfigExport.ps1**) from here.

2 Log in as the system administrator to the Windows computer running the Microsoft Exchange server.

3 Move the script file to the Windows computer.

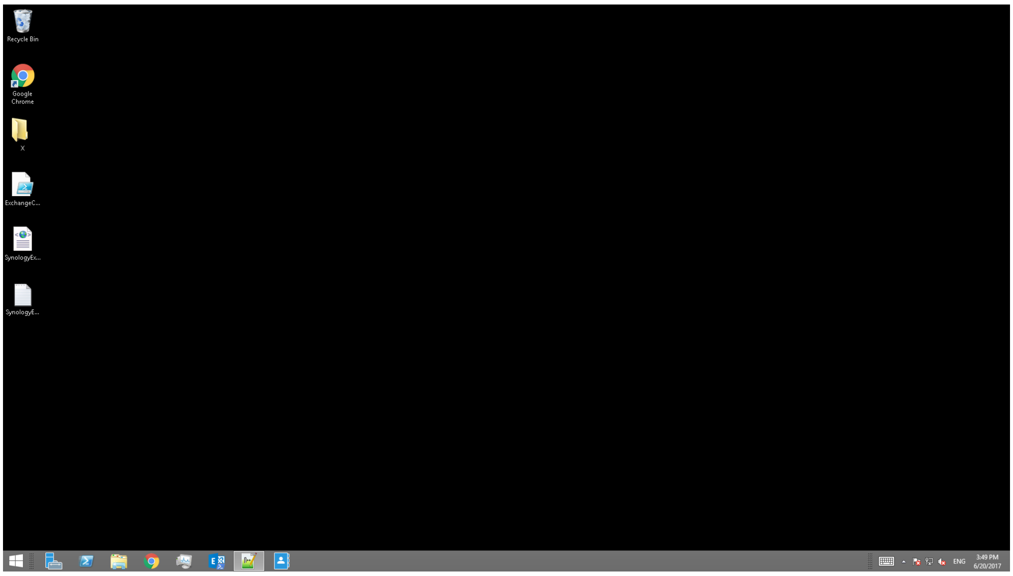
4 Execute the script file on the Microsoft Exchange server using Windows PowerShell.



```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"):
```

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.



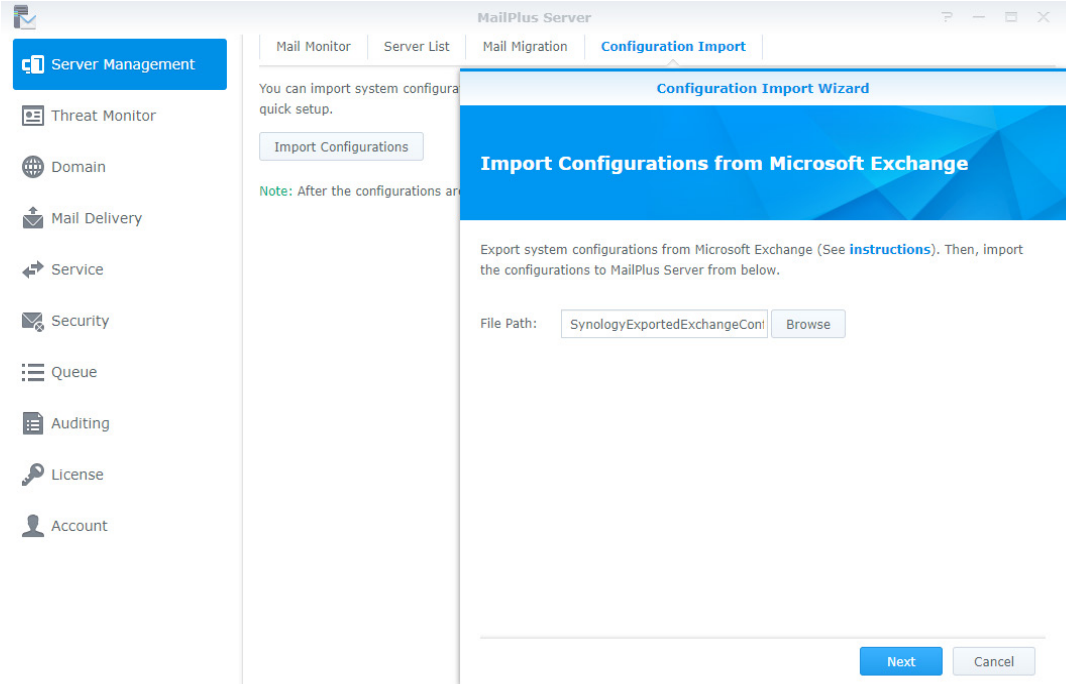
7 Move the generated .xml file and .txt file to your local computer.

Import system configurations to MailPlus Server

1 Begin the import process in either way:

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

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



You can import system configura quick setup.

Note: After the configurations ar

Export system configurations from Microsoft Exchange (See instructions). Then, import the configurations to MailPlus Server from below.

File Path: SynologyExportedExchangeConf

3 Click **Next** to check configuration details at **General Settings** (e.g. SMTP and security settings) and **Criteria** (e.g. black and white lists). Click **Import** to finish the import.

Chapter

4

User Licenses

Sufficient licenses are required to properly run MailPlus Server. The number of licenses required is determined by the number of accounts that are to be activated. By default, MailPlus comes with 5 free email accounts and allows you to add more accounts with additional purchased licenses. To purchase licenses, please refer to **Purchase licenses**. The number of enabled accounts will not be determined by the following factors:

- Deactivated accounts
- Email alias
- Number of domains (including other domains)
- DSM users that are not specified account types (when choosing LDAP users as the account type, local users will not be counted as license users)

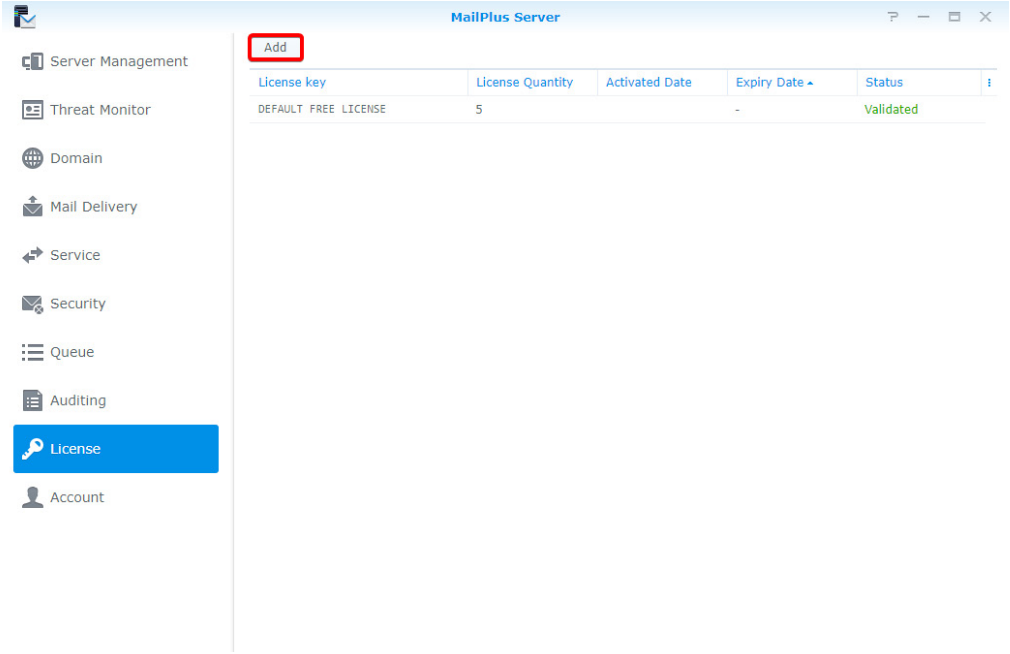
Purchase licenses

MailPlus license packs include 5 or 20 units of email accounts and can be purchased through Synology authorized **resellers**. For more details on MailPlus license packs, please refer to **MailPlus License Pack**.

Install licenses

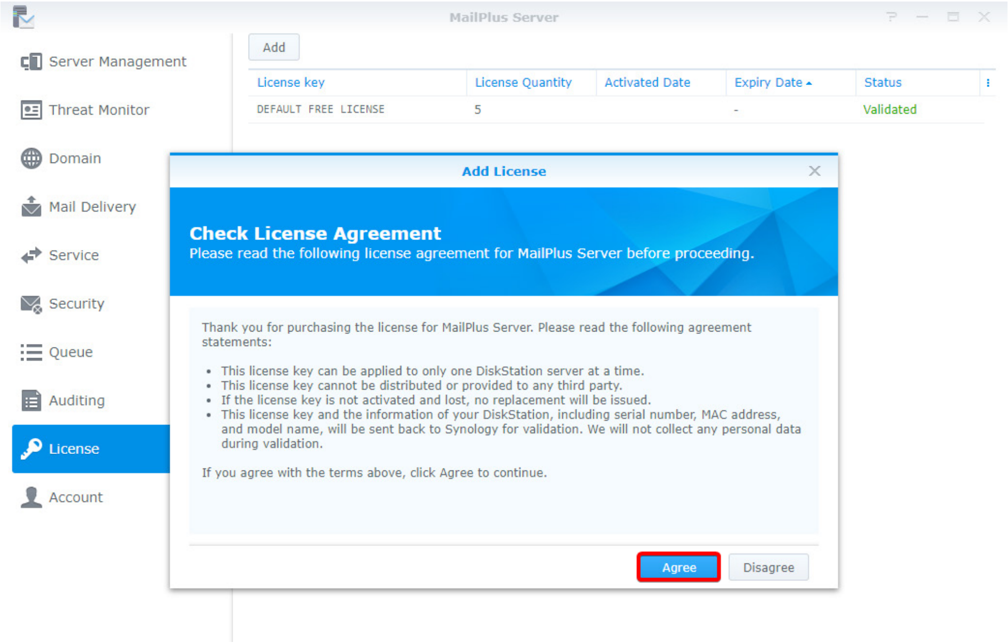
Purchased licenses must be installed to activate email accounts. Please refer to the following steps:

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



License key	License Quantity	Activated Date	Expiry Date ▴	Status
DEFAULT FREE LICENSE	5		-	Validated

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



License key	License Quantity	Activated Date	Expiry Date	Status
DEFAULT FREE LICENSE	5		-	Validated

Add License

Check License Agreement

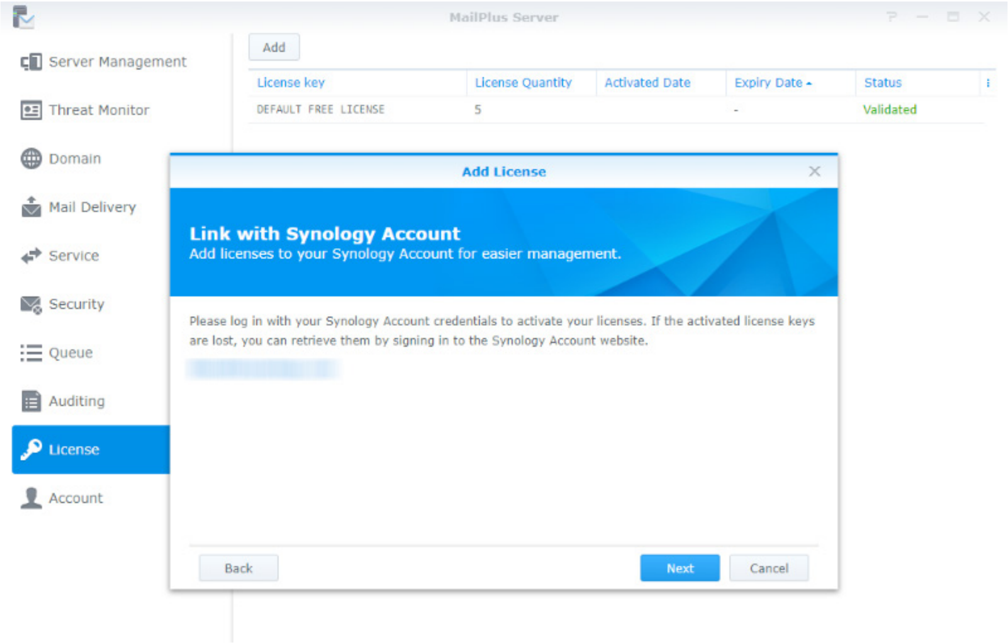
Please read the following license agreement for MailPlus Server before proceeding.

Thank you for purchasing the license for MailPlus Server. Please read the following agreement statements:

- This license key can be applied to only one DiskStation server at a time.
- This license key cannot be distributed or provided to any third party.
- If the license key is not activated and lost, no replacement will be issued.
- This license key and the information of your DiskStation, including serial number, MAC address, and model name, will be sent back to Synology for validation. We will not collect any personal data during validation.

If you agree with the terms above, click Agree to continue.

3 Please log in to **Synology Account** to allow licenses to be registered under the selected Synology account. Should there be situations where licenses are unable to be retrieved after being activated, log in to the Synology Account web page to check all the licenses that are registered under the account. After logging in to Synology Account, please click **Next**.



License key	License Quantity	Activated Date	Expiry Date	Status
DEFAULT FREE LICENSE	5		-	Validated

Add License

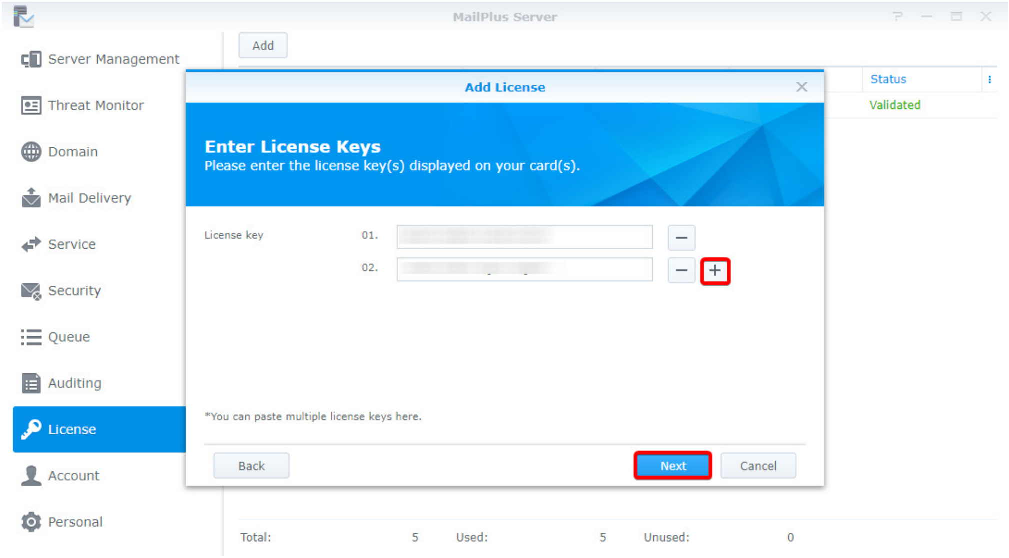
Link with Synology Account

Add licenses to your Synology Account for easier management.

Please log in with your Synology Account credentials to activate your licenses. If the activated license keys are lost, you can retrieve them by signing in to the Synology Account website.

[redacted]

4 Enter the license number in the license number field as shown in the image below. If you need to add more than one license, click on the **+** button to add more license number fields.



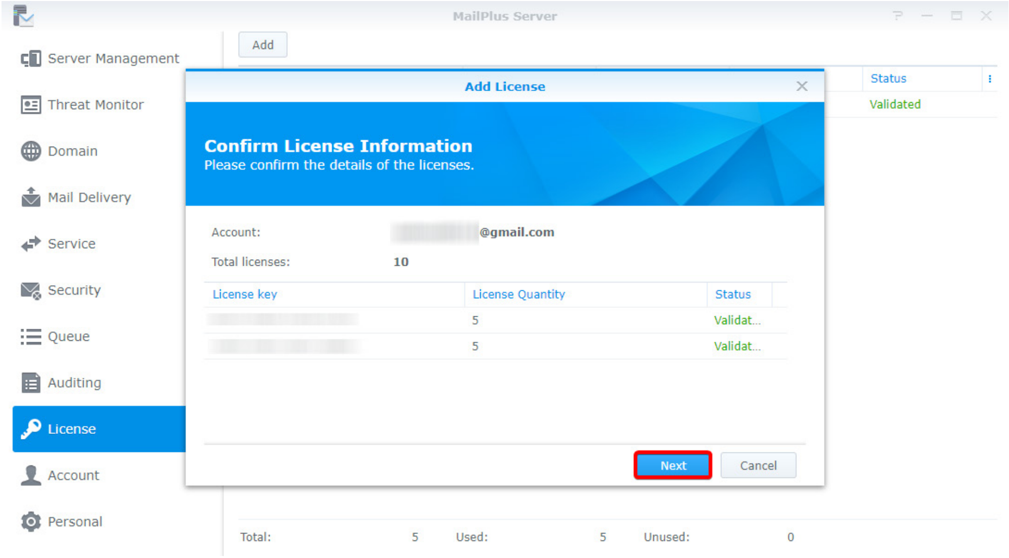
Enter License Keys
Please enter the license key(s) displayed on your card(s).

License key 01. [redacted]
02. [redacted]

*You can paste multiple license keys here.

Total: 5 Used: 5 Unused: 0

5 Check and confirm if the number of licenses to be installed and their respective license numbers are correct, once the licenses are activated, you may not migrate them to another MailPlus Server. After confirming the information is correct, please click **Next** to complete adding licenses.



Confirm License Information
Please confirm the details of the licenses.

Account: [redacted]@gmail.com
Total licenses: 10

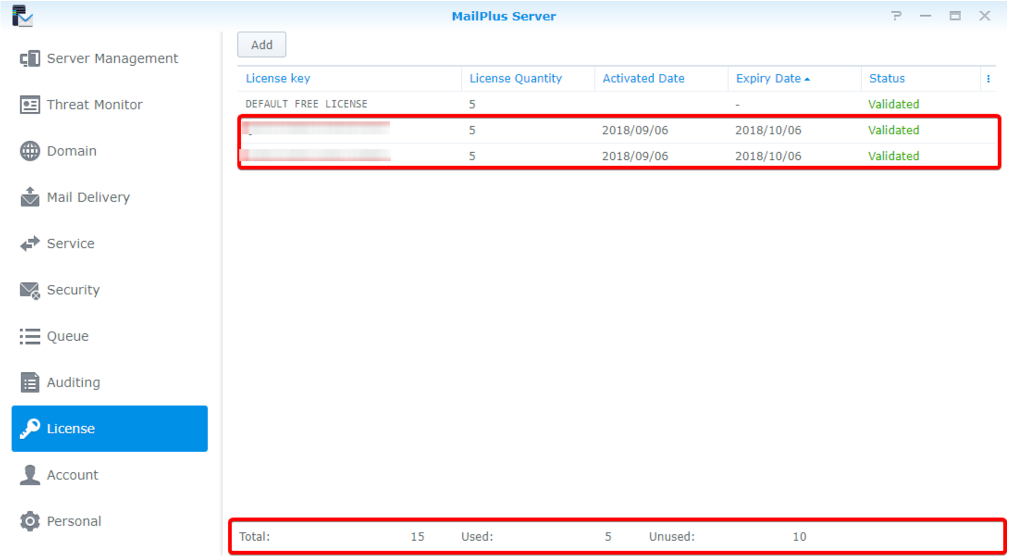
License key	License Quantity	Status
[redacted]	5	Validat...
[redacted]	5	Validat...

Total: 5 Used: 5 Unused: 0

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

- License key
- The quantity of email accounts provided by the 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.



License key	License Quantity	Activated Date	Expiry Date ▲	Status
DEFAULT FREE LICENSE	5		-	Validated
[redacted]	5	2018/09/06	2018/10/06	Validated
[redacted]	5	2018/09/06	2018/10/06	Validated

Total: 15 Used: 5 Unused: 10

How to use licenses

After adding the licenses, you can go **Account** > **User** to choose which accounts to activate. For more details, refer to **Activate accounts**.

Chapter

5

Account Settings

Account system

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

In addition to activating user accounts from existing local users on DSM, you can also 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 also cannot simultaneously synchronize more than one directory services and accounts.

Note: MailPlus Server can only choose one of the following account sources: Local, LDAP, or Domain.

Modify Account type

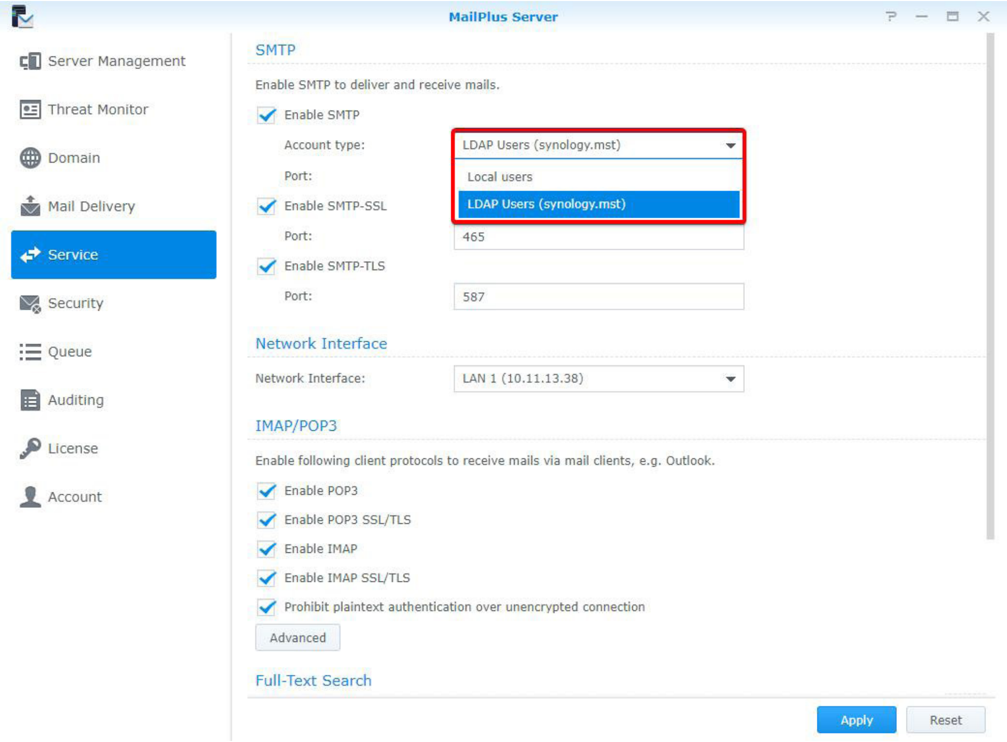
Please refer to the following steps to modify account type:

1 Log 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).



SMTP

Enable SMTP to deliver and receive mails.

☑ Enable SMTP

Account type: LDAP Users (synology.mst)

Local users

LDAP Users (synology.mst)

Port:

☑ Enable SMTP-SSL

Port: 465

☑ Enable SMTP-TLS

Port: 587

Network Interface

Network Interface: LAN 1 (10.11.13.38)

IMAP/POP3

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

☑ Enable POP3

☑ Enable POP3 SSL/TLS

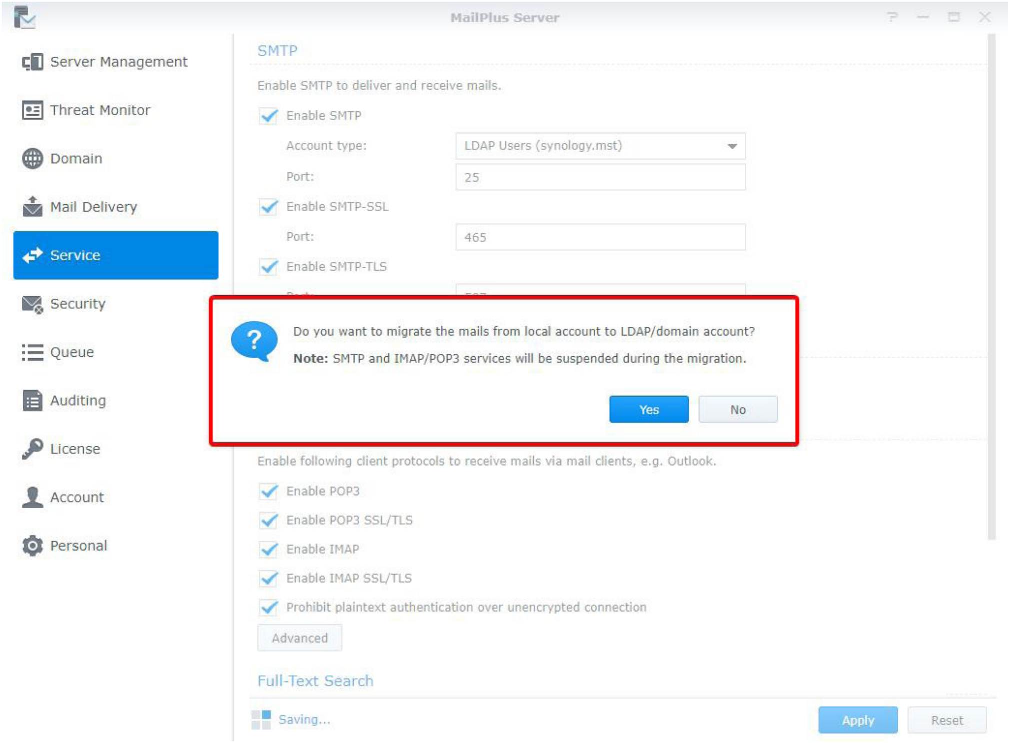
☑ Enable IMAP

☑ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Full-Text Search

5 Click on **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 then click **Apply**, an alert window will appear.



SMTP

Enable SMTP to deliver and receive mails.

☑ Enable SMTP

Account type: LDAP Users (synology.mst)

Port: 25

☑ Enable SMTP-SSL

Port: 465

☑ Enable SMTP-TLS

Do you want to migrate the mails from local account to LDAP/domain account?

Note: SMTP and IMAP/POP3 services will be suspended during the migration.

Yes No

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

☑ Enable POP3

☑ Enable POP3 SSL/TLS

☑ Enable IMAP

☑ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Note: Different account types will have different email addresses, thereby user emails under each account type 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 from directory service accounts with the same username as local users. Different usernames will be automatically ignored.

Activate accounts

You must activate user accounts in MailPlus Server to start using email services, including sending and receiving emails.

Before starting MailPlus Server, you must activate the accounts that will be using your email service. Sufficient licenses are required to activate accounts, for more information please refer to the **User Licenses** section.

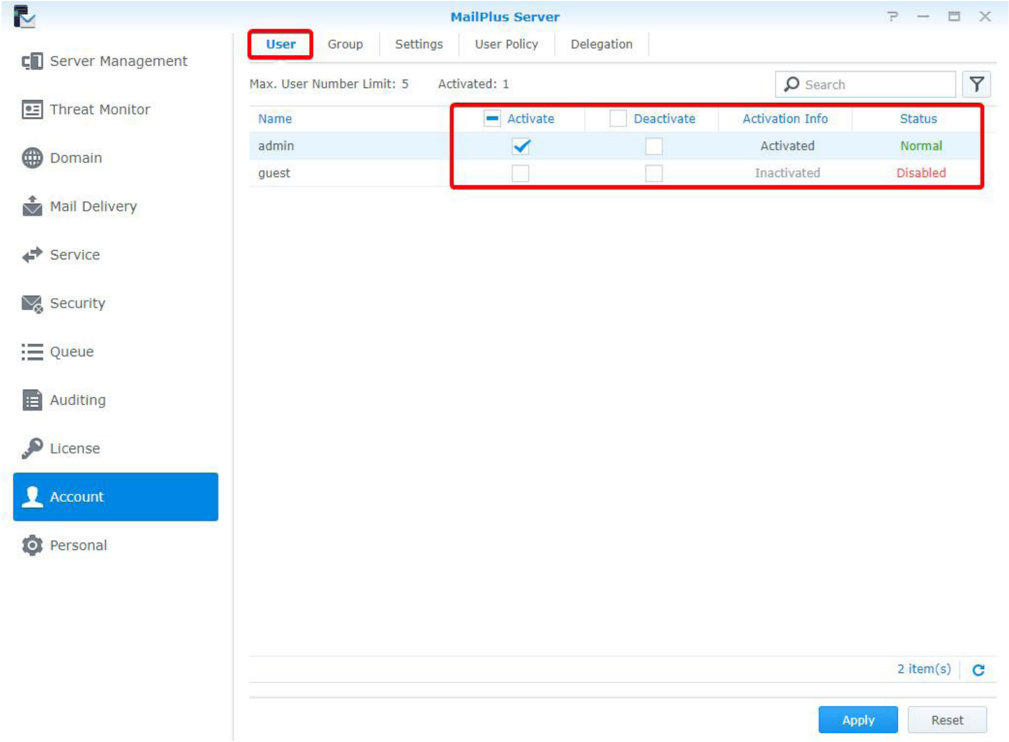
If you have already activated a number of user accounts, and these users cannot log in to DSM or launch MailPlus/MailPlus Server, please check if you have disabled any user accounts, or if the user accounts have privileges to the MailPlus or MailPlus Server applications. For more information please refer to DSM **Help**.

Activate user accounts

Activating user accounts require a sufficient amount of licenses, for more instructions please refer to **User Licenses**. If you need to activate a larger amount of users, please refer to **Activate groups** and **Default status**. Please refer to the following steps:

1 Go to **Account** > **User**.

2 Select the users for which you want to activate. If the checkboxes under the **Activate** and **Deactivate** columns are not ticked for a certain user, then the status of this user will be set as the default status. Please refer to **Default status**. Ticking the **Activate** checkbox will reduce the amount of licenses available.



Max. User Number Limit: 5 Activated: 1

Name	Activate	Deactivate	Activation Info	Status
admin	☑	□	Activated	Normal
guest	□	□	Inactivated	Disabled

3 The Activation Info column displays if the license has been applied to the user.

4 The Status column includes Normal, Deactivated, Username not supported.

> ***Note:*** Users can use email services properly only when the accounted is Activated under Activation Info, and Normal under Status.

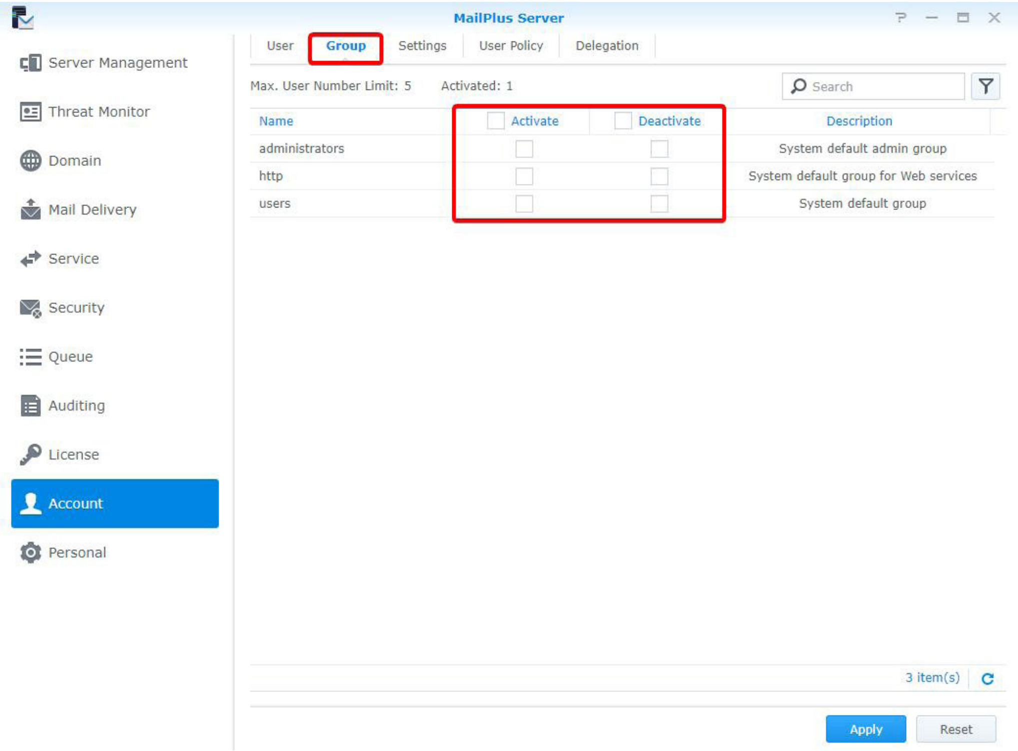
5 Click Apply to activate users.

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



Max. User Number Limit: 5 Activated: 1

Name	□ Activate	□ Deactivate	Description
administrators	□	□	System default admin group
http	□	□	System default group for Web services
users	□	□	System default group

3 item(s)

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

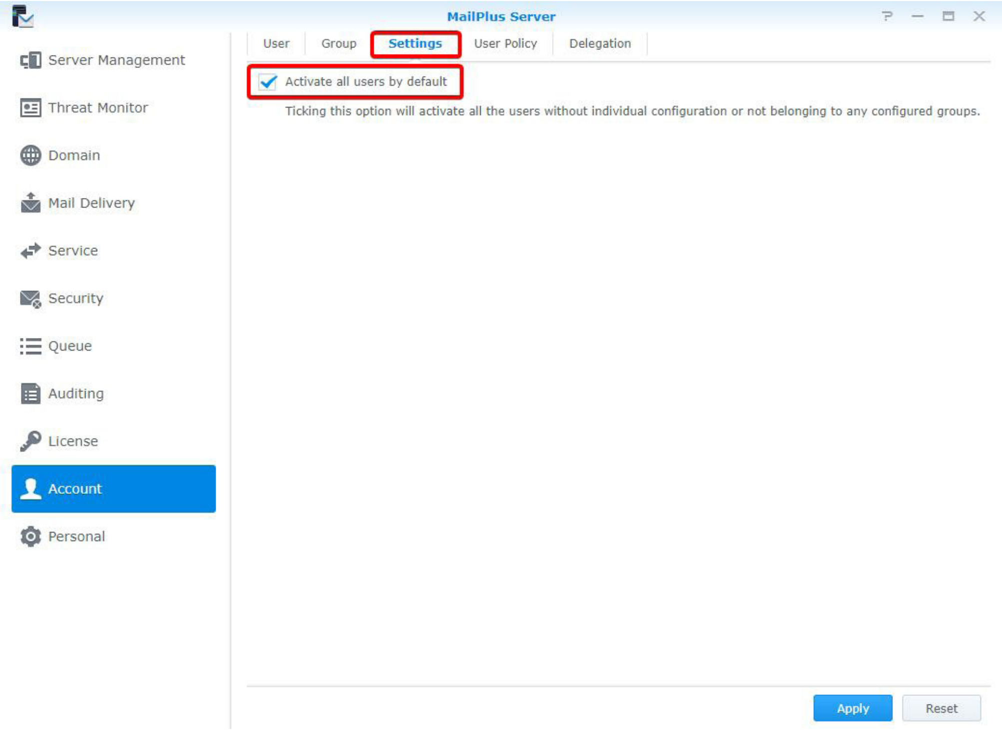
Default status

You can view your default status under the **Settings** tab in the **Account** page.

The default status settings will be applied to user accounts with **Normal** statuses that have not been activated or deactivated. Please refer to the following steps:

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

> ***Note:*** Activating by default will use the relative amount of licenses. Please make sure you have sufficient licenses available.



☑ Activate all users by default

Ticking this option will activate all the users without individual configuration or not belonging to any configured groups.

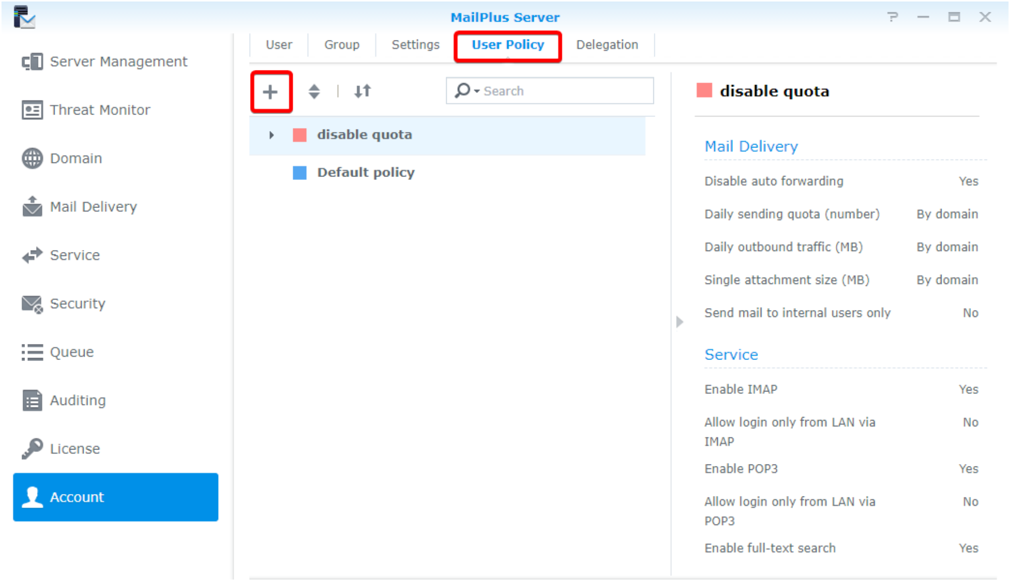
2 Click **Apply** to apply settings.

Create user policies

You can create dedicated user policies for email services on MailPlus for certain users or groups. Please refer to the following steps to create user policies:

1 Go to **Account** > **User Policy**.

2 Click the plus button to create a new policy.



disable quota

Mail Delivery

Disable auto forwarding	Yes
Daily sending quota (number)	By domain
Daily outbound traffic (MB)	By domain
Single attachment size (MB)	By domain
Send mail to internal users only	No

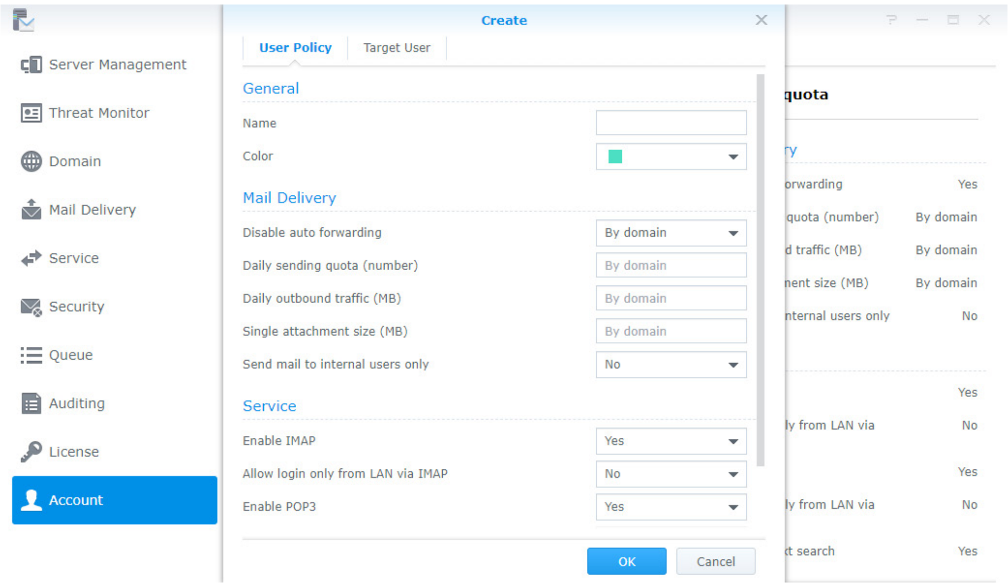
Service

Enable IMAP	Yes
Allow login only from LAN via IMAP	No
Enable POP3	Yes
Allow login only from LAN via POP3	No
Enable full-text search	Yes

3 Enter a policy name in the **Name** field in the **User Policy** tab in the **Create** window.

4 Select a color for the policy from the **Color** drop-down menu to allow for easy management in the future.

Note: For more information on policy functions, please refer to **Policy information and restrictions**.



General

Name	
Color	🟩

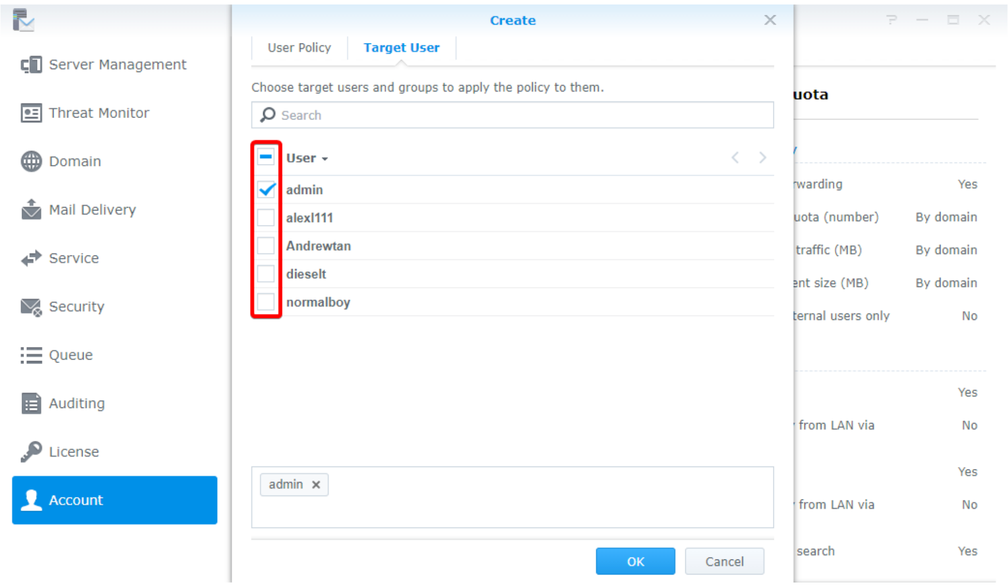
Mail Delivery

Disable auto forwarding	By domain
Daily sending quota (number)	By domain
Daily outbound traffic (MB)	By domain
Single attachment size (MB)	By domain
Send mail to internal users only	No

Service

Enable IMAP	Yes
Allow login only from LAN via IMAP	No
Enable POP3	Yes

5 Switch to the **Target User** tab and select a user to apply the policy to. You can also search for users in the search field at the top of the page.



Choose target users and groups to apply the policy to them.

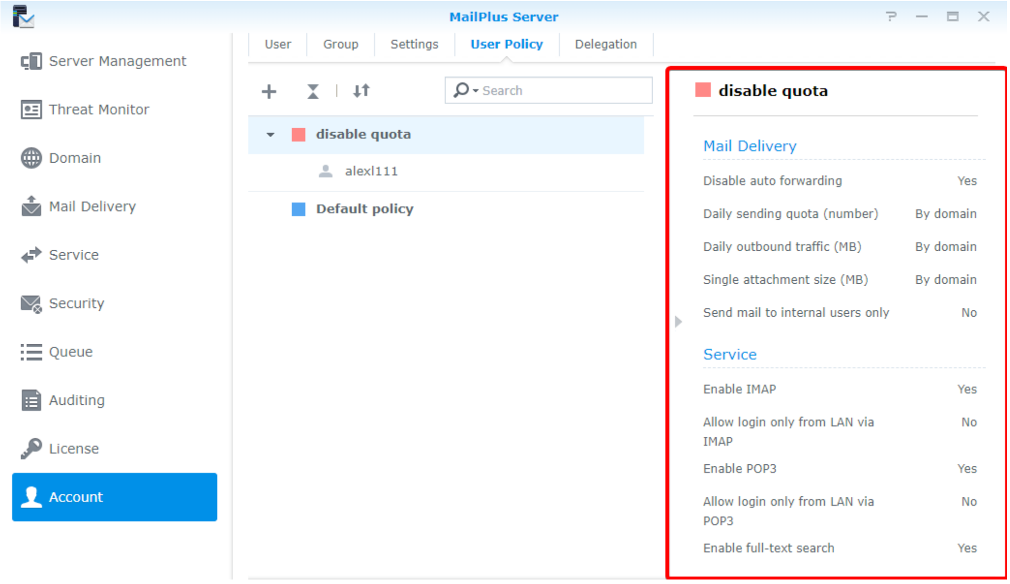
	User
☑	admin
□	alexl111
□	Andrewtan
□	dieselt
□	normalboy

admin ×

warding	Yes
uota (number)	By domain
traffic (MB)	By domain
ent size (MB)	By domain
ternal users only	No
	Yes
from LAN via	No
	Yes
from LAN via	No
search	Yes

6 Click **OK** to finish.

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



- 🟥 disable quota
  - alexl111
- 🟦 Default policy

🟥 disable quota

Mail Delivery

Disable auto forwarding	Yes
Daily sending quota (number)	By domain
Daily outbound traffic (MB)	By domain
Single attachment size (MB)	By domain
Send mail to internal users only	No

Service

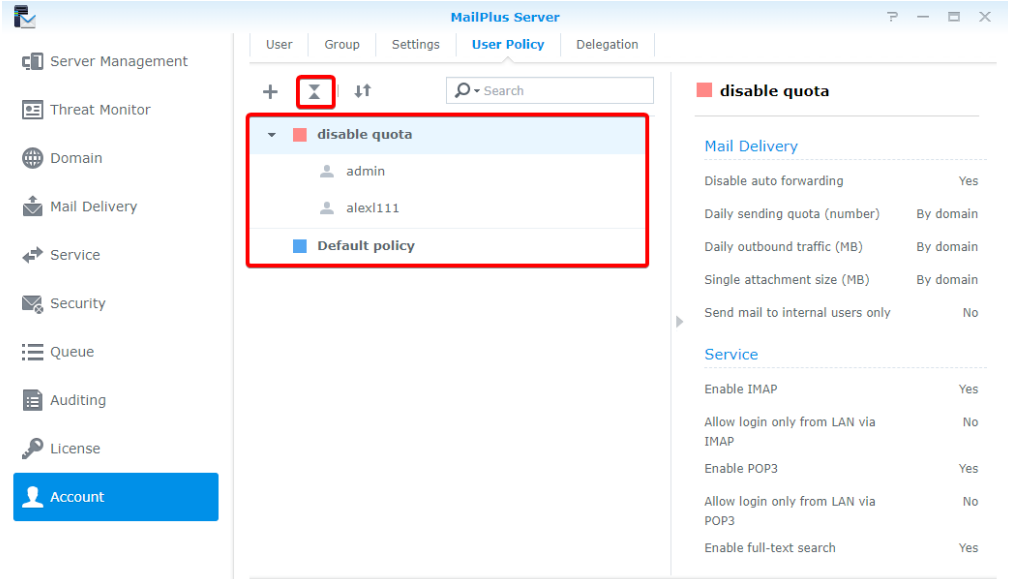
Enable IMAP	Yes
Allow login only from LAN via IMAP	No
Enable POP3	Yes
Allow login only from LAN via POP3	No
Enable full-text search	Yes

Change user policy priority

Multiple user policies may be applied to one user, however only one policy will take effect, therefore the policy that will take effect will be based on the priority settings of the 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 The highest policy has higher priority over the lower policies. (For example, based on the image below, the priority in descending order will be as follows: *Old policy*, *New policy*, *Default policy*. Therefore *Old policy* will be applied to *admin* instead of *New policy*.)



disable quota

Mail Delivery

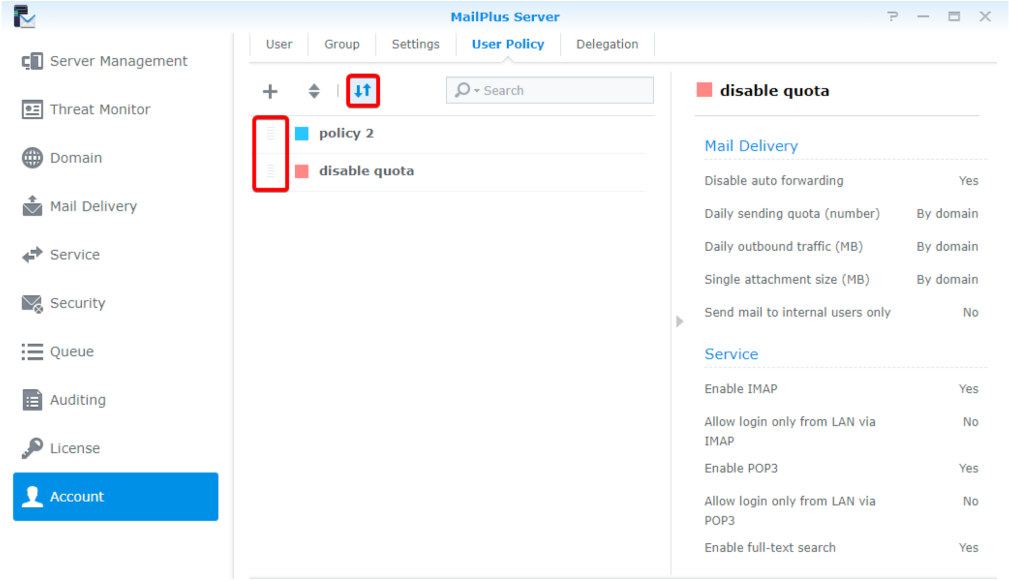
Disable auto forwarding	Yes
Daily sending quota (number)	By domain
Daily outbound traffic (MB)	By domain
Single attachment size (MB)	By domain
Send mail to internal users only	No

Service

Enable IMAP	Yes
Allow login only from LAN via IMAP	No
Enable POP3	Yes
Allow login only from LAN via POP3	No
Enable full-text search	Yes

3 Click the change priority button (the two-way arrow icon) to change 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.



disable quota

Mail Delivery

Disable auto forwarding	Yes
Daily sending quota (number)	By domain
Daily outbound traffic (MB)	By domain
Single attachment size (MB)	By domain
Send mail to internal users only	No

Service

Enable IMAP	Yes
Allow login only from LAN via IMAP	No
Enable POP3	Yes
Allow login only from LAN via POP3	No
Enable full-text search	Yes

4 Hover to the left of the policy and drag and drop the policy to a suitable position based on the desired priority order.

5 Click the change priority button (the two-way arrow icon) to close the drag and drop function and allow for the new priority order to take effect.

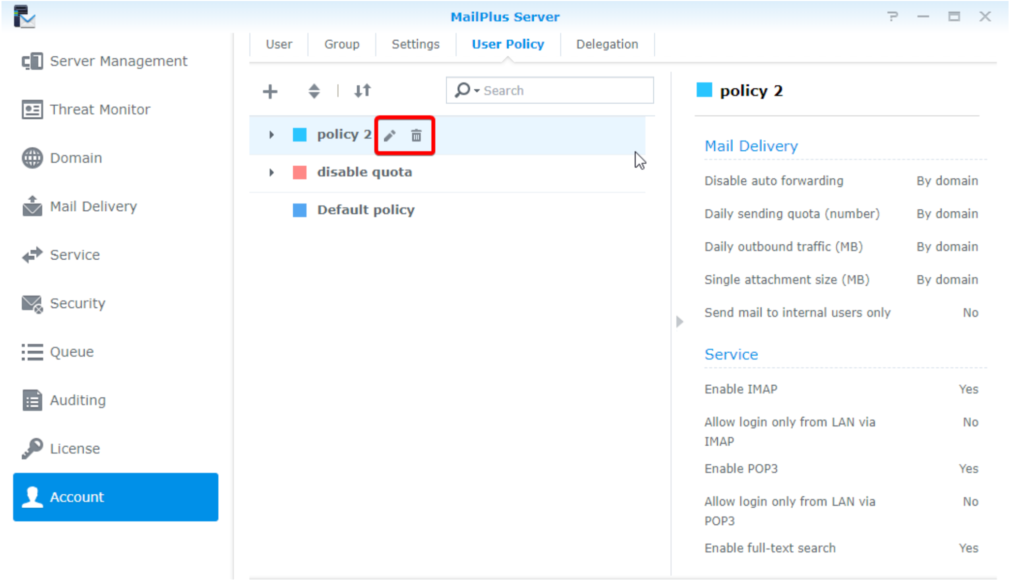
> ***Note:*** **Default policy** will always have the lowest priority. For more information, please refer to **Default policies**.

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 buttons will appear. Click the pencil icon for policy editing, or click the trash-can icon to delete policy.



policy 2

disable quota

Default policy

policy 2

Mail Delivery

Disable auto forwarding By domain

Daily sending quota (number) By domain

Daily outbound traffic (MB) By domain

Single attachment size (MB) By domain

Send mail to internal users only No

Service

Enable IMAP Yes

Allow login only from LAN via IMAP No

Enable POP3 Yes

Allow login only from LAN via POP3 No

Enable full-text search Yes

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 following setting details of default policy:

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

Since the default policy is one of the policies that will apply to all users, it may not meet your expectations due to certain restrictions. If you do not want specific restrictions to take effect, you will need to disable these restrictions. For more information, please refer to Policy information and 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 the settings of the domain.

Note:

1. 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 the settings of the domain.

Note:

1. If an email message has been rejected before being delivered, then it will not be counted against the quota.
2. If an email message has been returned after being deliver, then it will be counted against the quota.
3. The value set for the default policy is equal to the **Daily quota** value in the **Daily Quota** section of the **Usage Limit** tab on the **Domain** page.
4. When the value is 0, users will not have any restrictions.
5. 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 the settings of the domain.

Note:

1. If an email message has been rejected before being delivered, then it will not be counted against the quota.
2. If an email message has been returned after being deliver, then it will be counted against the quota.
3. The value set for the default policy is equal to the **Daily traffic limit (MB)** value in the **Daily Quota** section of the **Usage LImit** tab on the **Domain** page.
4. When the value is 0, users will not have any restrictions.
5. 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 the attachment size.	Users will not be restricted by the attachment size.	Policies will follow the settings of the domain.

Note:

1. The value set for the default policy is equal to the **Maximum size per mail (MB)** value in the **General** tab on the **Mail Delivery** page.
2. 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 are restricted to sending emails to internal users only.	Users are not restricted to sending emails to internal users only.

Note: Currently there are no available settings that restricts all users to send emails to internal users only.

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

Note: If the **Enable IMAP** checkbox under the **IMAP/POP3** section on the **Service** page is not ticked, then IMAP services will not be available and the user policy will not take effect. Users will not be able to log in 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 are restricted to only logging in from a subdomain via IMAP.	Users have no restrictions when logging to MailPlus.

Note:

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

No.	Policy	Results of Enabling Policy	Results of Disabling Policy
08	Enable POP3	Allows users 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, then POP3 services will not be available and the user policy will not take effect. Users will not be able to log in 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 are restricted to only logging in from a subdomain via POP3.	Users have no restrictions when logging to MailPlus.

Note:

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

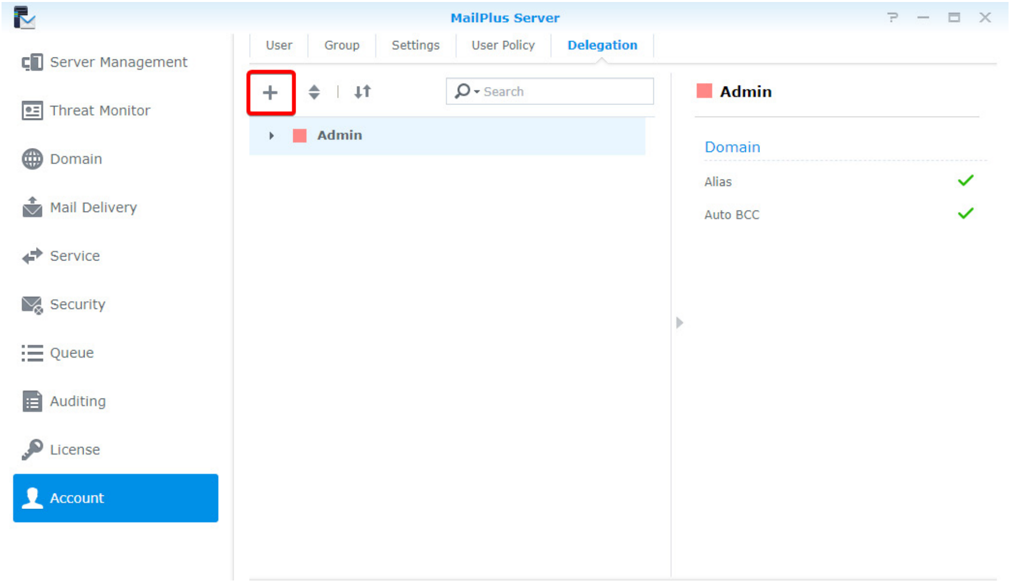
No.	Policy	Results of Enabling Policy	Results of Disabling Policy
010	Enable full-text search	Server will index email content of the users.	Server will not index the email content of the users.

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

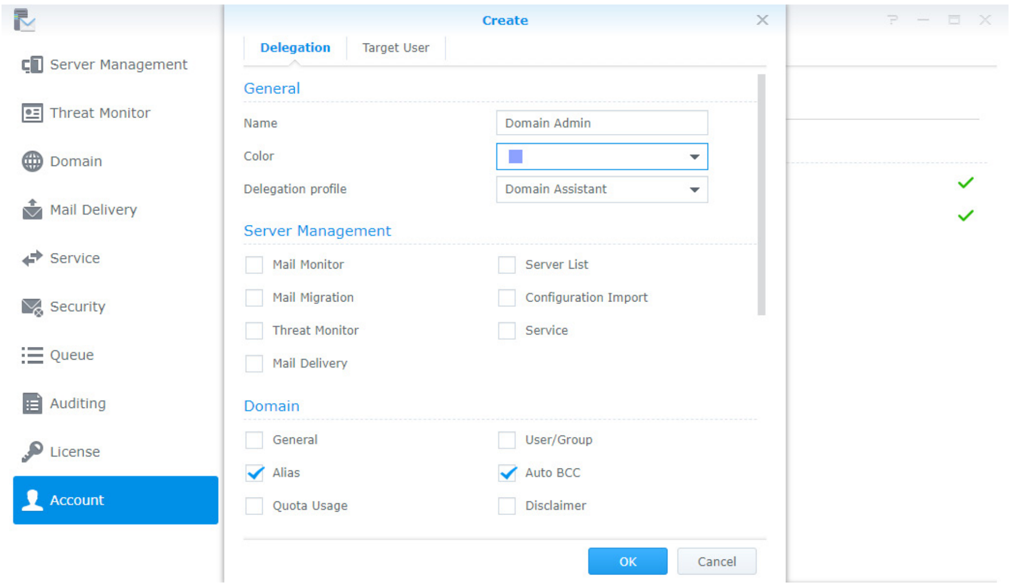
Create delegation policies

In 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 On the pop-up, go to the **Delegation** tab and enter the required information. The system will automatically tick the options below for you based on the delegation profile you select. It will switch to **Custom** when you tick or untick any options below. Please refer to **this article** to know more about the corresponding delegated permissions.



General

Name: Domain Admin

Color:

Delegation profile: Domain Assistant

Server Management

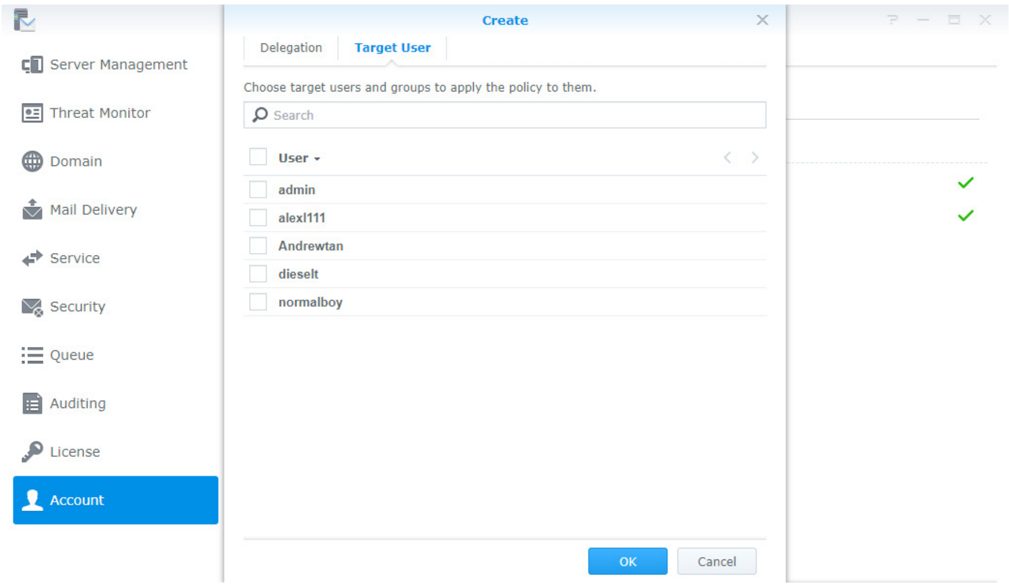
□ Mail Monitor	□ Server List
□ Mail Migration	□ Configuration Import
□ Threat Monitor	□ Service
□ Mail Delivery	

Domain

□ General	□ User/Group
☑ Alias	☑ Auto BCC
□ Quota Usage	□ Disclaimer

For example, if you select **Domain Manager** for Domain Admin, users regulated by this delegation policy can manage all settings of the 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 those domains.

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



Choose target users and groups to apply the policy to them.

- □ User
- □ admin
- □ alexl111
- □ Andrewtan
- □ dieselt
- □ normalboy

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

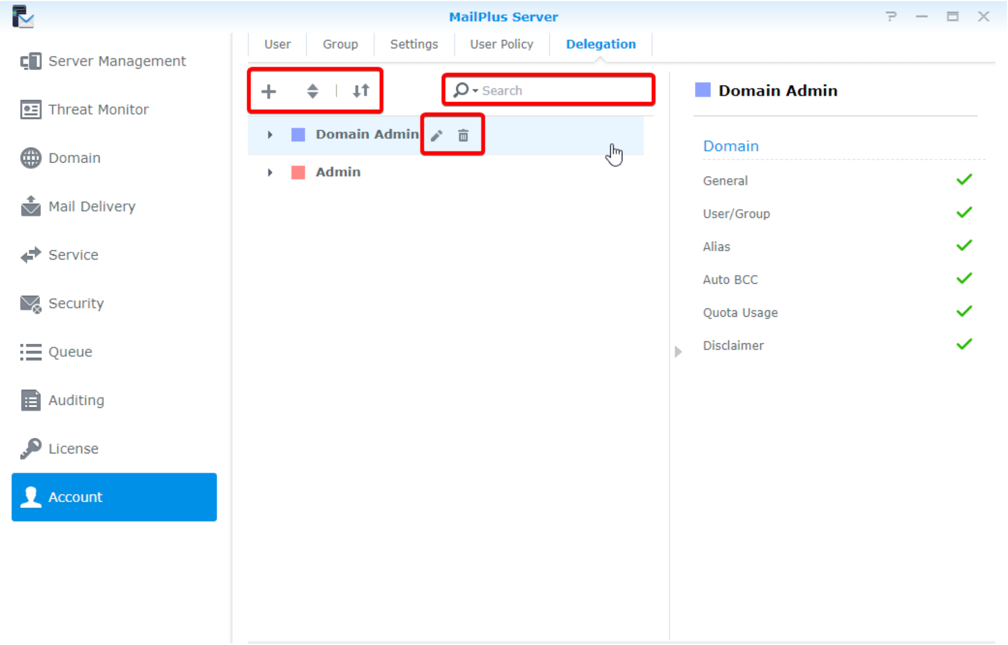
Manage delegation policies

1 Go to **Account** > **Delegation**.

2 Select Domain Admin, then you can view, edit and delete the 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**:
  1 Click the two-way arrow icon to set the priority.
  2 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 in 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 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 that of DSM. In other words, users who are from the administration group on DSM will also be able access all MailPlus Server settings. General users will only see the **Personal** page.

Chapter 6

Protocol Settings

In addition to email service protocol related server settings, you can also open and close ports for certain protocols, or rebind network interfaces of servers here. Since the protocol settings affect external operations of the entire server, please make sure your settings are set according to your needs.

SMTP

The SMTP protocol 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 Protocol** 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 not specifying **STARTTLS**. Currently our SMTP is not encrypted, if you need to configure this, 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. SMTPS must send encrypted packets out after handshake. If you need to relay using this protocol, please refer to **here** for more information.

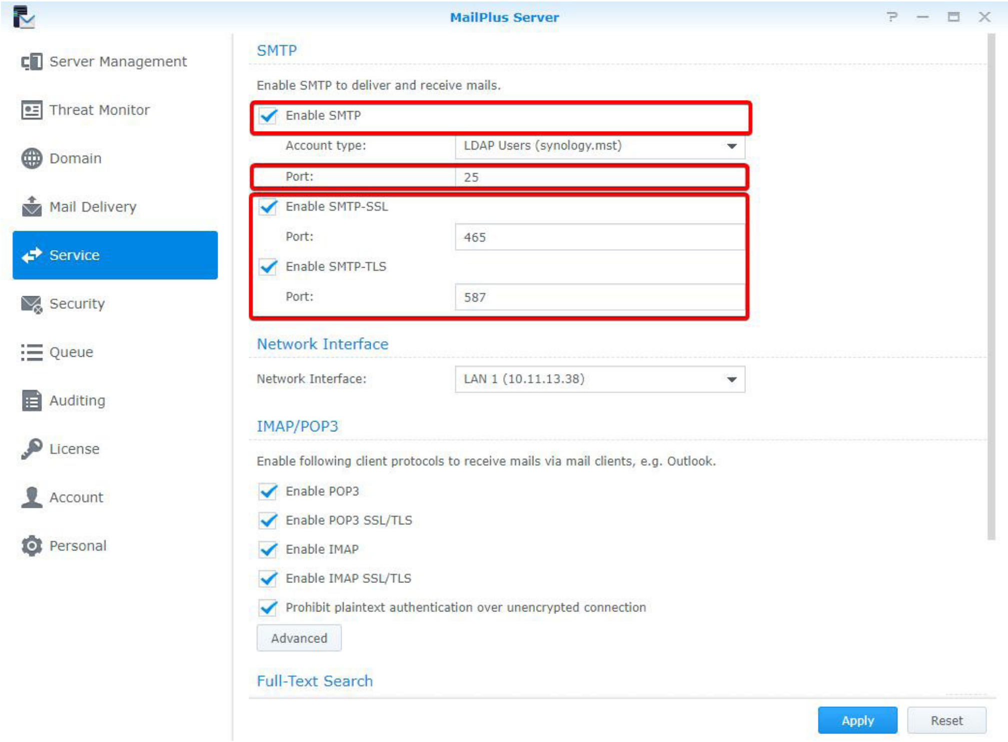
- **SMTP-TLS**: SMTP is a supported protocol for SMTP-TILS, and performs encryption through START-TILS. During this time, SMTP-TILS requires authentication, therefore it is often used for the internal protocol between client and **MSA**.

Set up SMTP

Please refer to configure SMTP and respective ports:

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

Note: This is the main protocol for the mail server.



SMTP

Enable SMTP to deliver and receive mails.

☑ Enable SMTP

Account type: LDAP Users (synology.mst)

Port: 25

☑ Enable SMTP-SSL

Port: 465

☑ Enable SMTP-TLS

Port: 587

Network Interface

Network Interface: LAN 1 (10.11.13.38)

IMAP/POP3

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

☑ Enable POP3

☑ Enable POP3 SSL/TLS

☑ Enable IMAP

☑ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Full-Text Search

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

Note: Unless there are special conditions, we recommend using the default port 25.

3 You can adjust the following settings:

- **Enable SMTP-SSL**: Use 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 settings.

IMAP/POP3

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

> ***Note:*** Both protocols encrypt through START-TILS, since DSM no longer supports SSL encrypted connection, please do not set up SSL for encrypted connection.

- **IMAP**: **IMAP protocol** is a standard protocol that allows users to access stored information on email servers. Compared to POP3, IMAP provides more supported options for email services.
- **POP3**: **POP3 protocol** is also a standard protocol that allows users to access stored information on email servers.

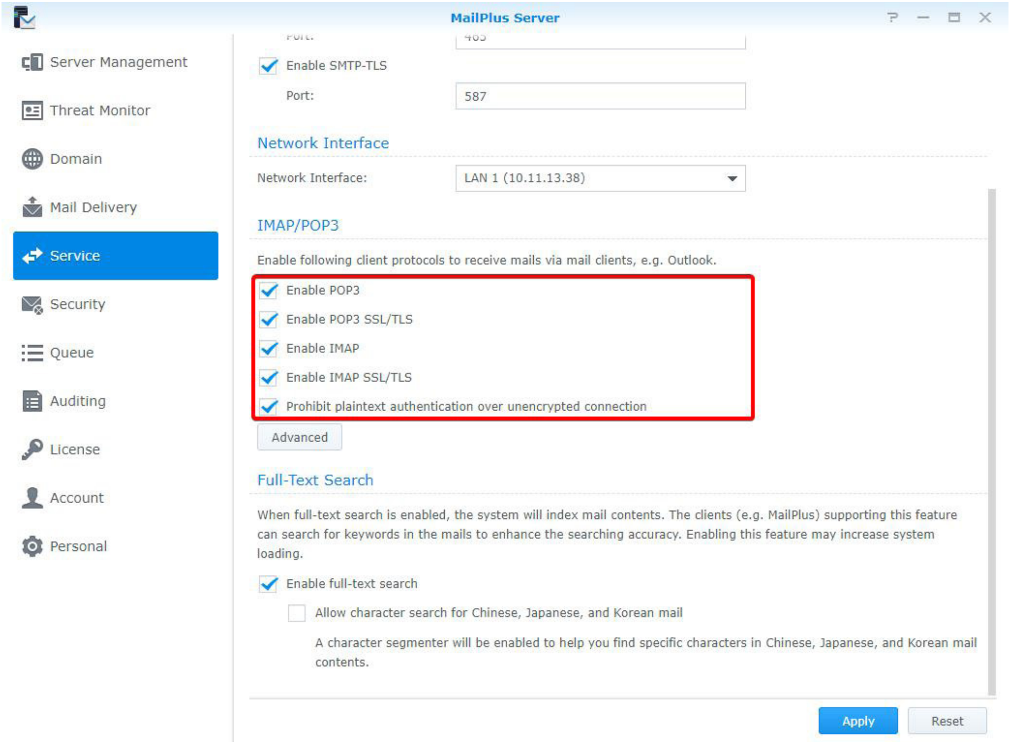
Set up IMAP/POP3

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**: Email client software will receive messages using POP3.
- **Enable POP3 SSL/TLS**: Encryption for POP3 connection.
- **Enable IMAP**: Email client software will receive messages using IMAP.
- **Enable IMAP SSL/TLS**: Encryption for IMAP connection.



☑ Enable SMTP-TLS

Port: 587

Network Interface

Network Interface: LAN 1 (10.11.13.38)

IMAP/POP3

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

☑ Enable POP3

☑ Enable POP3 SSL/TLS

☑ Enable IMAP

☑ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Advanced

Full-Text Search

When full-text search is enabled, the system will index mail contents. The clients (e.g. MailPlus) supporting this feature can search for keywords in the mails to enhance the searching accuracy. Enabling this feature may increase system loading.

☑ Enable full-text search

□ Allow character search for Chinese, Japanese, and Korean mail

A character segmenter will be enabled to help you find specific characters in Chinese, Japanese, and Korean mail contents.

Apply Reset

3 Click **Apply** to save settings.

Network Interface

After setting up MailPlus Server, a set of protocols will be set by default. After you install MailPlus Server or configure high-availability, MailPlus Server will bind with a network interface to allow MailPlus Server to support **High-availability cluster**. Your email service 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 a local network, PPPoE, and a bonded network interface. When your MailPlus Server is running under a high-availability architecture, you can bind MailPlus Server with a local network and a bonded network interface. You can use **manual configuration** to retrieve the IP address of the network interface.

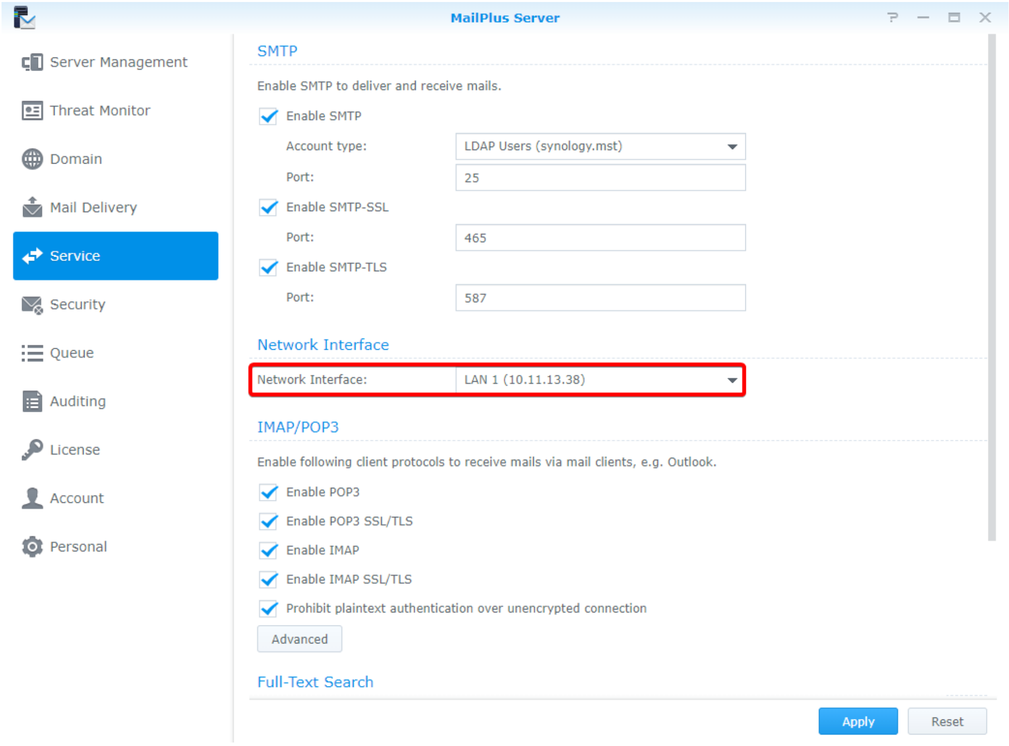
> ***Note:*** When your MailPlus Server binds with a bonded network interface, you cannot unbind the bonded network interface. If you want to unbind the bonded network interface, you must first modify the network interface or uninstall MailPlus Server.

Modify Network Interface

1 Log in to **DSM**.

2 Launch **MailPlus Server**.

3 Go to **Service** > **Network Interface**, and switch network interfaces from the **Network Interface** drop-down menu.



SMTP

Enable SMTP to deliver and receive mails.

☑ Enable SMTP

Account type: LDAP Users (synology.mst)

Port: 25

☑ Enable SMTP-SSL

Port: 465

☑ Enable SMTP-TLS

Port: 587

Network Interface

Network Interface: LAN 1 (10.11.13.38)

IMAP/POP3

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

☑ Enable POP3

☑ Enable POP3 SSL/TLS

☑ Enable IMAP

☑ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Full-Text Search

4 Click **Apply** to save settings.

Chapter

7

SMTP Settings

Once you have completed the basic configuration for MailPlus Server during the installation stage, you may still need to adjust or modify email services and more detailed settings including secured connection for the SMTP protocol. These modifications can be done here.

Service Settings

You can go to the **Mail Delivery** page to set up **MailPlus Server** rules for sending and receiving emails such as specifying the maximum size per email and maximum recipients per message.

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

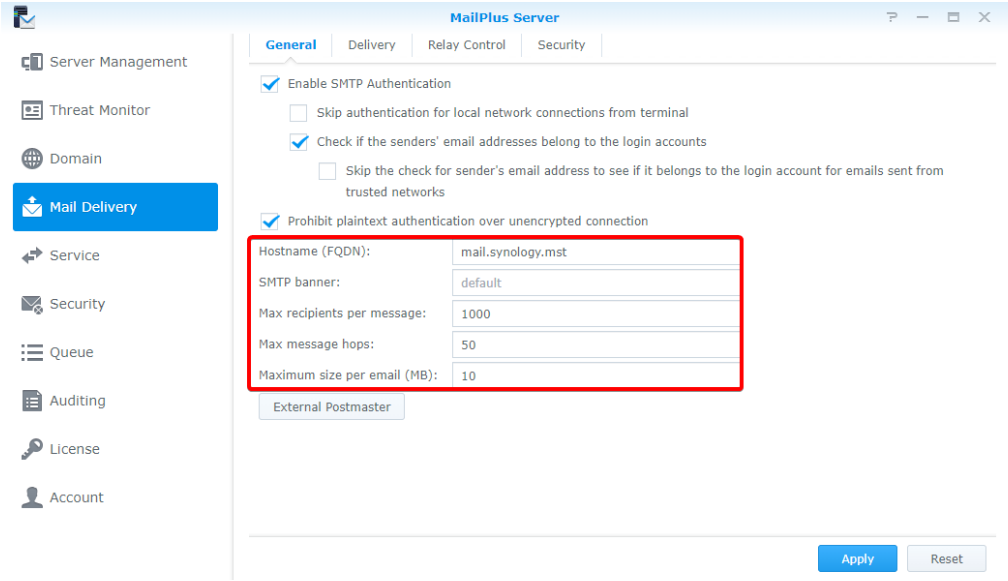
- **SMTP profile**: You can specify a hostname for **MailPlus Server** and an SMTP banner on a client's Telnet terminal, and also setup up rules for sending and receiving emails such as specifying the maximum size per email and maximum recipients per message to avoid using excessive resources.
- **Full-text search**: The full-text search feature allows **MailPlus** web client to index emails to improve the performance of searching mails. This feature supports indexing e-mails with Chinese, Japanese, and Korean characters. Since full-text search indexes all email content, it may require additional computing resources. You can decide whether or not to enable the full-text search feature, or 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** send 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 the DNS server.
- **SMTP banner**: Specify the texts 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.



☑ Enable SMTP Authentication

☐ Skip authentication for local network connections from terminal

☑ Check if the senders' email addresses belong to the login accounts

☐ Skip the check for sender's email address to see if it belongs to the login account for emails sent from trusted networks

☑ Prohibit plaintext authentication over unencrypted connection

Hostname (FQDN): mail.synology.mst

SMTP banner: default

Max recipients per message: 1000

Max message hops: 50

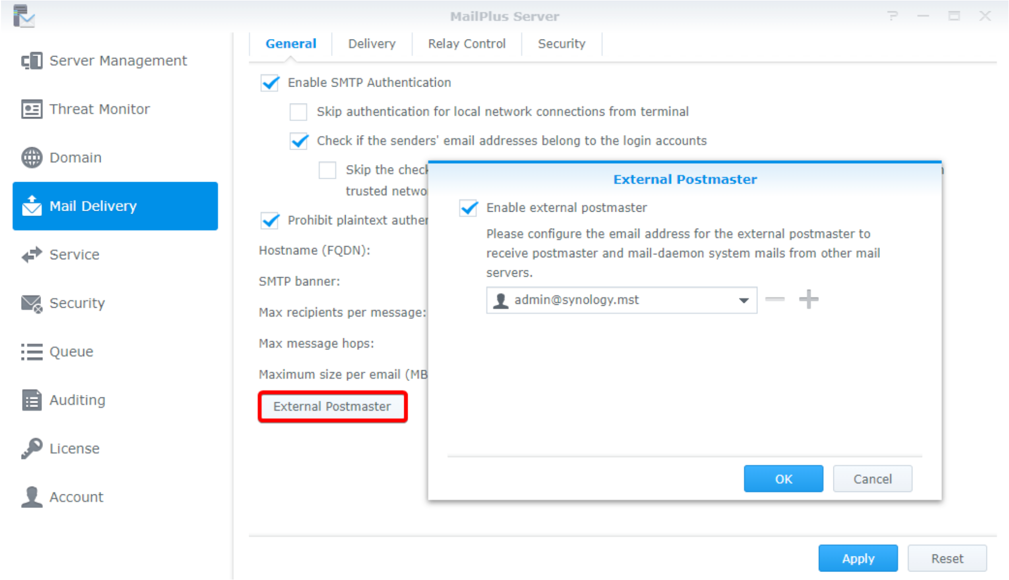
Maximum size per email (MB): 10

2 Click **Apply** to save settings.

External Postmaster

External postmaster is set to receive system mails 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 to add email addresses for external postmasters.



☑ Enable SMTP Authentication

□ Skip authentication for local network connections from terminal

☑ Check if the senders' email addresses belong to the login accounts

□ Skip the check ... trusted netwo...

☑ Prohibit plaintext authen...

Hostname (FQDN):

SMTP banner:

Max recipients per message:

Max message hops:

Maximum size per email (MB

External Postmaster

☑ Enable external postmaster

Please configure the email address for the external postmaster to receive postmaster and mail-daemon system mails from other mail servers.

admin@synology.mst

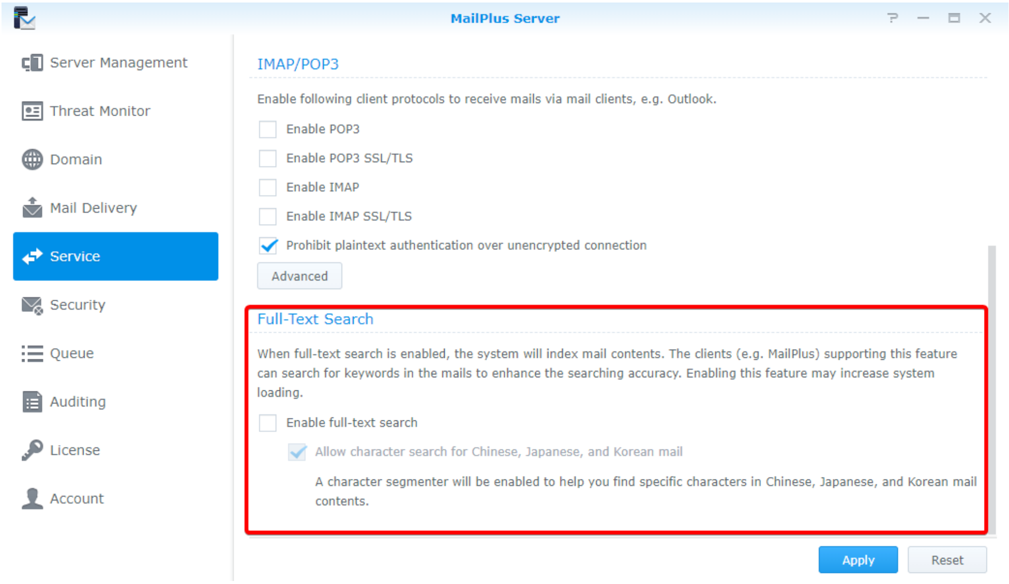
5. Click **OK** to save the settings.

Full-Text Search

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

> ***Note:*** Enabling this feature may increase system loading when there is a larger amount 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 to disable full-text search for specific users and reduce server loading.
   - **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 mail contents.



IMAP/POP3

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

□ Enable POP3

□ Enable POP3 SSL/TLS

□ Enable IMAP

□ Enable IMAP SSL/TLS

☑ Prohibit plaintext authentication over unencrypted connection

Full-Text Search

When full-text search is enabled, the system will index mail contents. The clients (e.g. MailPlus) supporting this feature can search for keywords in the mails to enhance the searching accuracy. Enabling this feature may increase system loading.

□ Enable full-text search

☑ Allow character search for Chinese, Japanese, and Korean mail

A character segmenter will be enabled to help you find specific characters in Chinese, Japanese, and Korean mail contents.

3 Click **Apply** to save settings.

SMTP secure connection

Enhance your mail server security and stability through analyzing user connection, login info, and email content. You can use this setting option to set up the criteria for providing services to users using your mail server. This will not only safeguard your service quality but also prevent MailPlus Server from becoming an open relay for spammers and being blacklisted as a result.

- **SMTP authentication**: When enabling SMTP authentication, users need to enter their DSM user account and password for authentication to relay 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**.

- **Black and white list**: When your server continues to receive spam emails, you can set up specific rules in the blacklist to reject services. In addition, when your server has enabled **Antivirus scan**, **Authentication**, and other scanning features, you may accidentally reject emails you wish to keep, in this case you can use the whitelist to skip security scanning to ensure important emails can be received.
- **Sender policy**: Scans the sender address. You can set up the criteria to reject unqualified formats or unauthenticated addresses.
- **Connection Policy**: Limits the number of client IP while running scans during the connection phase to prevent situations where one IP address consumes too much resources or conducts massive attacks.
- **Advanced settings**: During the connection phase, requires accurate commands and other advanced settings. Refer to **Advanced settings** for more information.

Enable SMTP Authentication

Authentication prevents malicious users from relaying spam through your email 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.

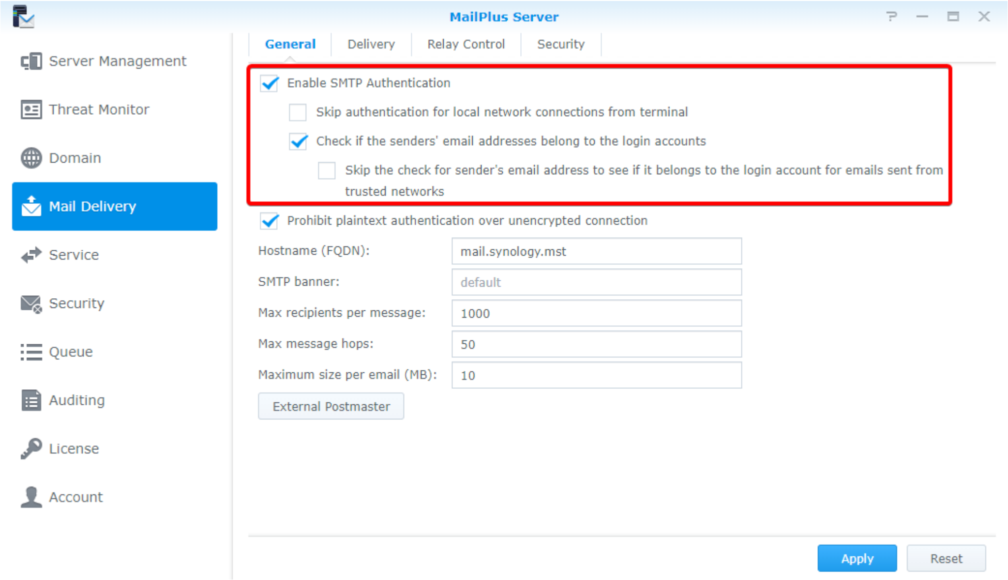
1 Go to **Mail Delivery** > **General** and choose to tick the **Enable SMTP Authentication** checkbox.

2 When you ticked the **Enable SMTP Authentication** checkbox, you can adjust the following settings:

- **Skip authentication for local network connections from terminal**: Users accessing email services using local network do not require authentication.

- **Check if the sender's email addresses belong to the login accounts**: When sending emails, the logged-in user has to use an email address that belongs to the login account.

> ***Note:*** If you tick the **Check if the senders' email addresses belong to the login accounts** checkbox in the **General** tab, mails from **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 in the **General** section, mails from local networks will not be blocked by **MailPlus Server**.



☑ Enable SMTP Authentication

□ Skip authentication for local network connections from terminal

☑ Check if the senders' email addresses belong to the login accounts

□ Skip the check for sender's email address to see if it belongs to the login account for emails sent from trusted networks

☑ Prohibit plaintext authentication over unencrypted connection

Hostname (FQDN): mail.synology.mst

SMTP banner: default

Max recipients per message: 1000

Max message hops: 50

Maximum size per email (MB): 10

3 Click **Apply** to save settings.

Create Black & White List

The system will take specific actions on certain messages based on various criteria specified in **Black and White List**. You can refer to the following steps to create rules for black and white lists:

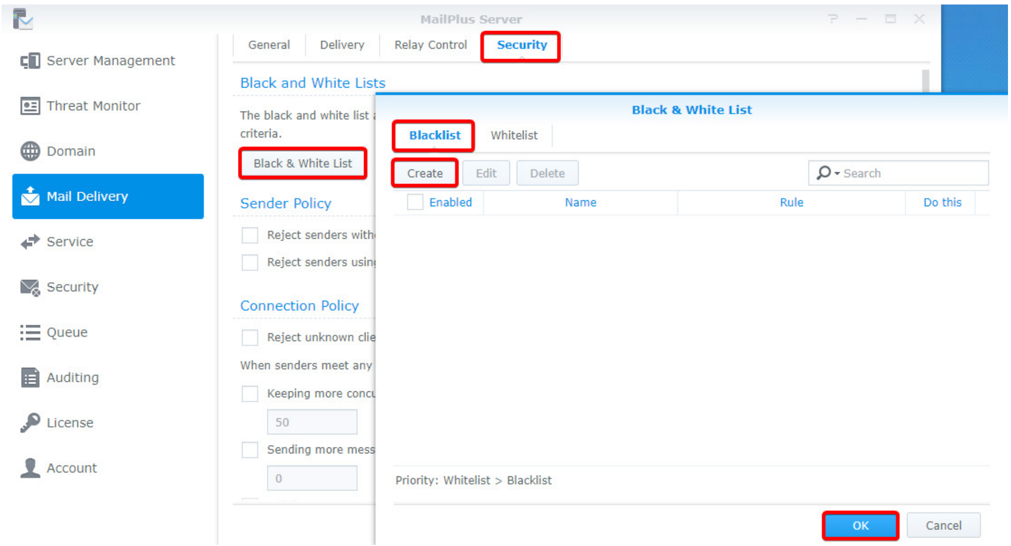
> ***Note:*** If an email message matches the criteria set in both the blacklist and whitelist, then this email will be received since the whitelist takes priority over the blacklist. Please refer to the **Whitelist information and restrictions** section.

1 Go to **Mail Delivery** > **Security** and click on the **Black & White List** button.

2 In the **Black & White List** window you can manage **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 through matching email messages.

3 In the **Blacklist** tab, please click **Create**.



Priority: Whitelist > Blacklist

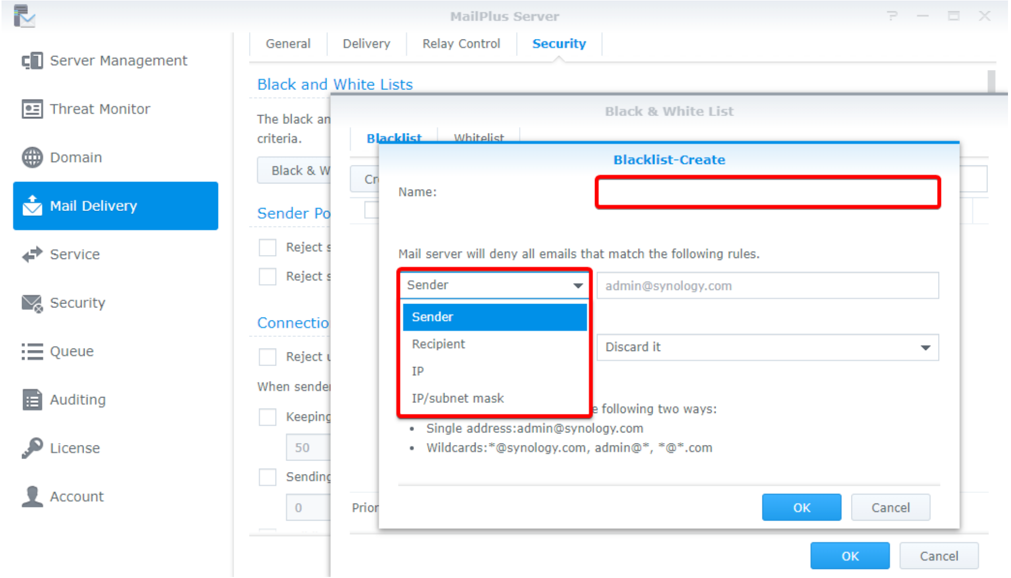
4 Name the blacklist (whitelist) rule in the **Name** field.

5 Choose a type of rule:

- **IP**: System takes specific actions when the sender IP address matches specified criteria.
- **IP/subnet mask**: System takes specific actions when sender IP address and its subnet mask matches specified criteria.
- **Sender:** System takes specific actions when sender address matches specified criteria.
- **Recipient**: System takes specific actions when recipient address matches specified criteria.
- **Domain**: An available option for **Whitelist**. System takes specific actions when the sender domain matches specified criteria.

Note:

1. The sender address in **Sender** is determined by the information retrieved from **MAIL FROM**.
2. The recipient address in **Recipient** is determined by the information retrieved from **RCPT TO**.



Mail server will deny all emails that match the following rules.

e following two ways:

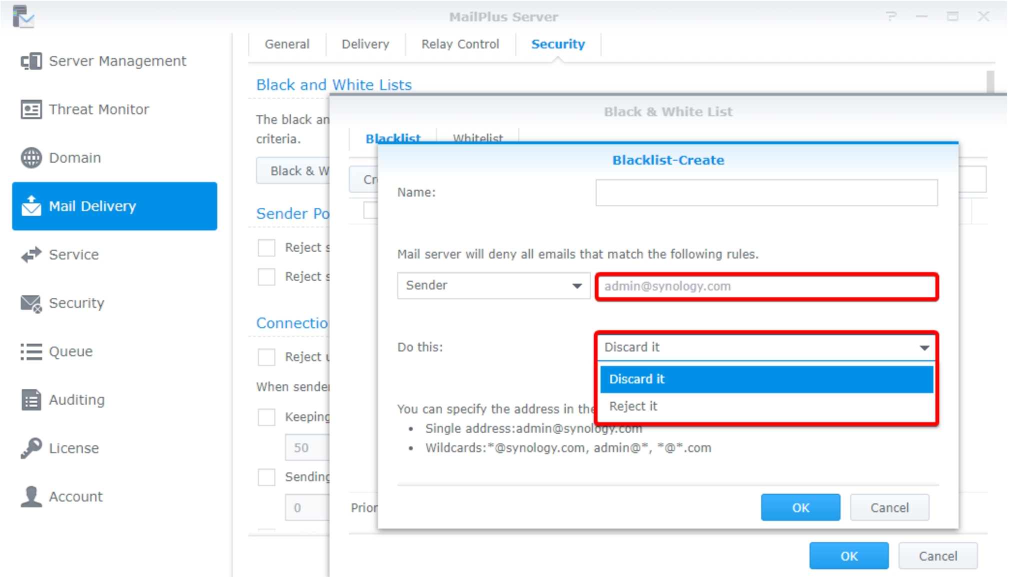
- Single address:admin@synology.com
- Wildcards:*@synology.com, admin@*, *@*.com

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 is 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**: When selecting this option, the sender will be notified when their emails are rejected.
- **Discard it**: When selecting this option, the sender will not be notified when their emails are discarded.



Name:

Mail server will deny all emails that match the following rules.

Sender: admin@synology.com

Do this: Discard it

Discard it
Reject it

You can specify the address in the
- Single address:admin@synology.com
- Wildcards:*@synology.com, admin@*, *@*.com

8 Click **OK** to complete settings.

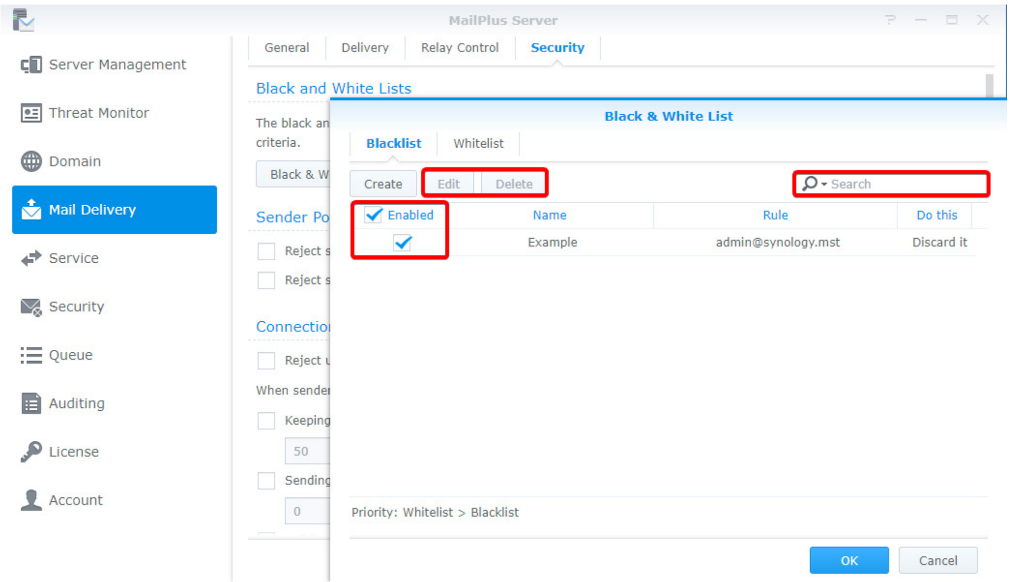
Edit and delete Black & White List

1 You can enter keywords in the search field at 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 rules from the blacklist or whitelist).

3 When you need to edit or delete a specific rule, first, select the rule, then click the **Edit** or **Delete** buttons.

4 Click **OK** to save settings.



Enabled	Name	Rule	Do this
✓	Example	admin@synology.mst	Discard it

Priority: Whitelist > Blacklist

Whitelist information and restrictions

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

	DNSBL	SPF	Antivirus Scans	DKIM	DMARC	smtpd_*_ restrictions
IP	v	v	v	v	v	v
IP/subnet mask	v	v		v	v	v
Sender		v	v			v
Recipient		v	v			v
Domain		v	v	v	v	v

Note:

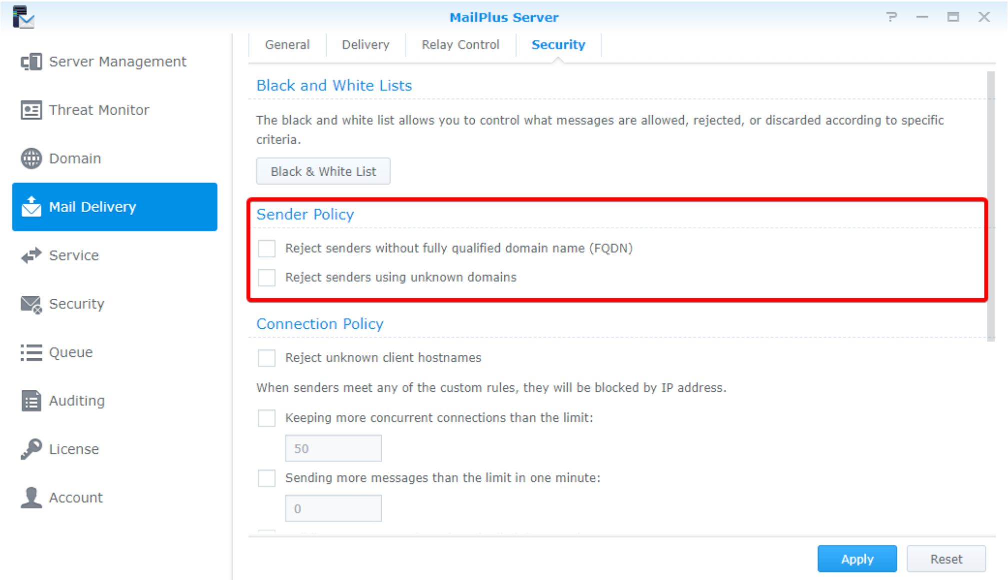
1. There are certain tests the whitelist will not skip, emails that do not pass these tests will fail to deliver. For example, when adding the *sender admin@example.com* onto the whitelist, since the sender rule does not support DNSBL, DKIM and DMARC, it must pass DNSBL, DKIM, or DMARC tests to avoid delivery failure.
2. If you wish to skip all the tests listed in the table, it is recommended to 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 the 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 the sender domain from **MAIL FROM** does not match any DNS A record, MX record, or when MX record is incorrect, emails will be rejected.



Black and White Lists

The black and white list allows you to control what messages are allowed, rejected, or discarded according to specific criteria.

Sender Policy

□ Reject senders without fully qualified domain name (FQDN)

□ Reject senders using unknown domains

Connection Policy

□ Reject unknown client hostnames

When senders meet any of the custom rules, they will be blocked by IP address.

□ Keeping more concurrent connections than the limit: 50

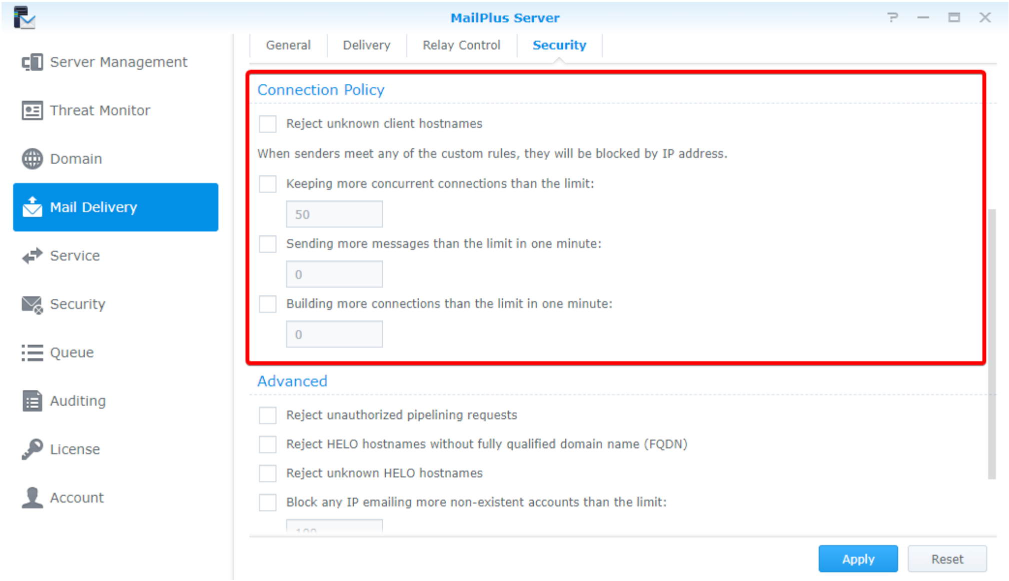
□ Sending more messages than the limit in one minute: 0

Connection Policy

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

2 Under the **Connection Policy** section, set up the criteria to reject client connections or block IP addresses due to certain issues with MailPlus Server clients. The policies include the following:

- **Reject unknown client hostnames**: When the IP address or the client hostname is incorrect or does not exist, then 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, then 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 within one minute with the same IP address exceeds this this number, connections will be blocked until the next minute starts.



Connection Policy

□ Reject unknown client hostnames

When senders meet any of the custom rules, they will be blocked by IP address.

□ Keeping more concurrent connections than the limit:

50

□ Sending more messages than the limit in one minute:

0

□ Building more connections than the limit in one minute:

0

Advanced

□ Reject unauthorized pipelining requests

□ Reject HELO hostnames without fully qualified domain name (FQDN)

□ Reject unknown HELO hostnames

□ Block any IP emailing more non-existent accounts than the limit:

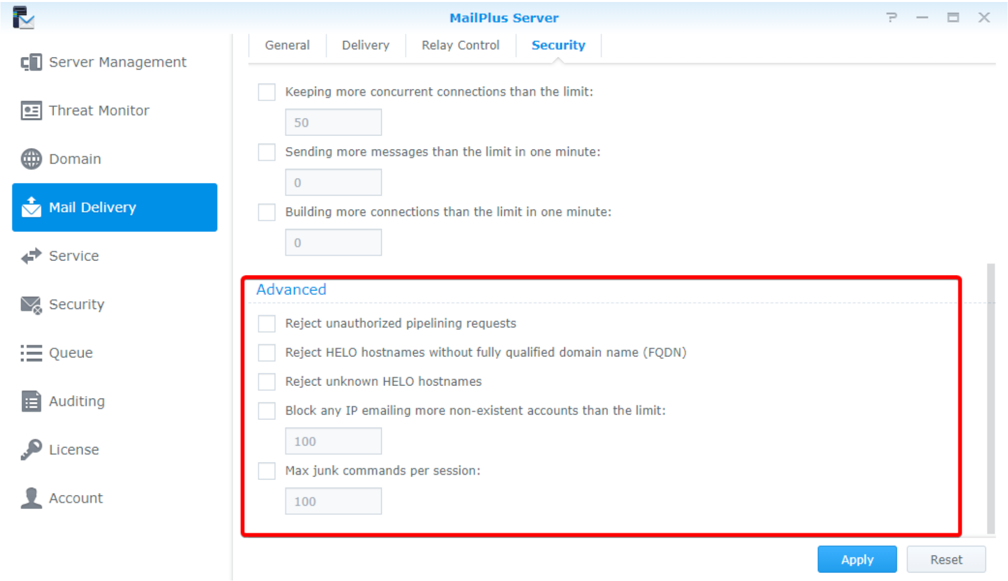
100

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 HELP hostnames without 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 the 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 on MailPlus Server.
- **Max junk commands per session**: When the number of connected clients exceeds specified number of junk commands (noop, vrfy, etrn, rset) within the same session, then every 10 junk commands will cause a one-second delay on mail delivery.



□ Keeping more concurrent connections than the limit:
50

□ Sending more messages than the limit in one minute:
0

□ Building more connections than the limit in one minute:
0

Advanced

□ Reject unauthorized pipelining requests

□ Reject HELO hostnames without fully qualified domain name (FQDN)

□ Reject unknown HELO hostnames

□ Block any IP emailing more non-existent accounts than the limit:
100

□ Max junk commands per session:
100

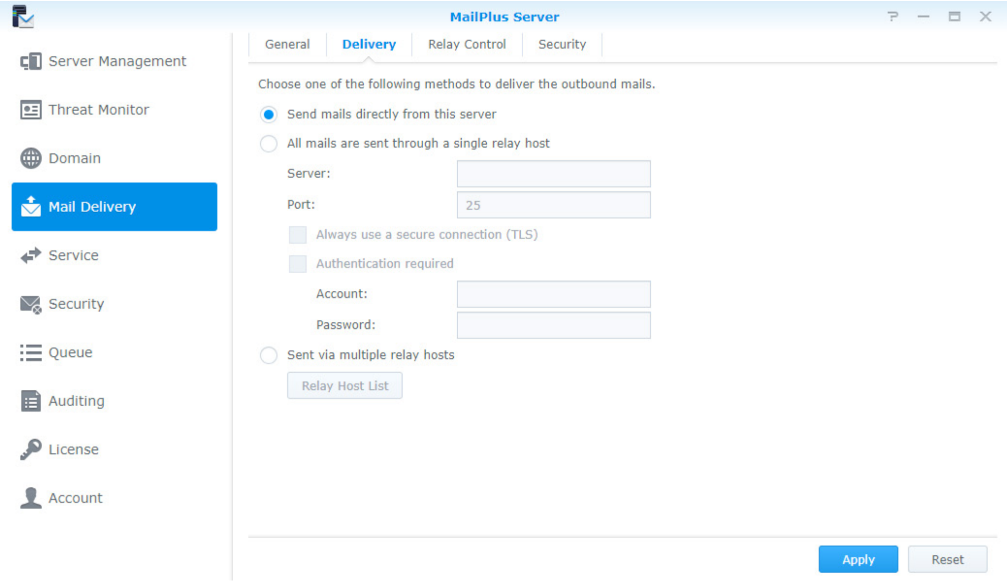
Mail Relay

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 security features are also provided.

Set up delivery control

In 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**.
2. Select a rule type:
   - **Send mails directly from this server**: All mails will be sent by MailPlus Server directly.
   - **All mails are sent through a single relay host**: Tick this checkbox to find more settings below. Enter the IP address or hostname of the relay server in the **Server** field, and enter the port number of the relay server 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 connection, if MailPlus Server is the relay server, please refer to this **article**. 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 for the relay server to use the server for mail relay.



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: 25

□ Always use a secure connection (TLS)

□ Authentication required

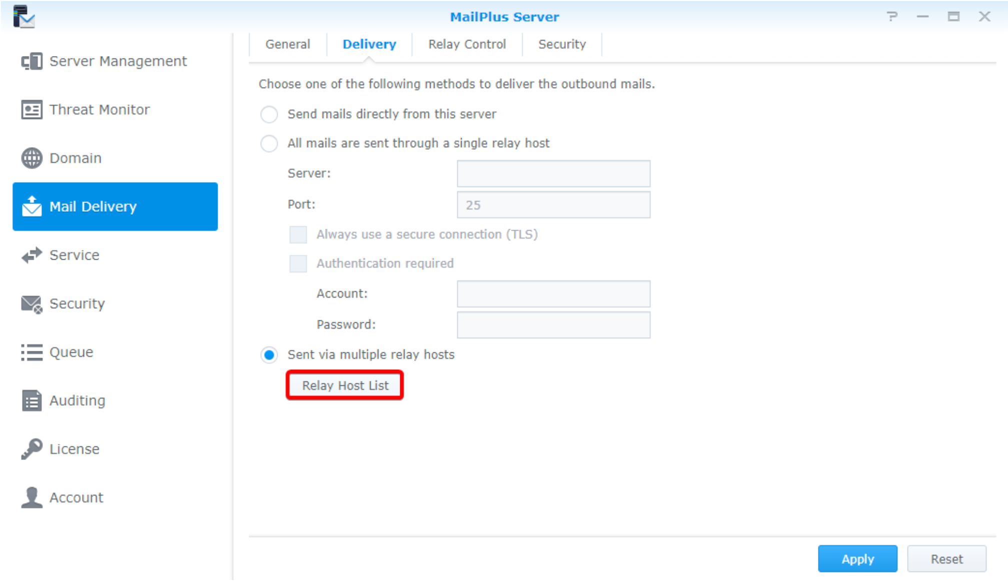
Account:

Password:

○ Sent via multiple relay hosts

> ***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 settings.

- **Sent via multiple relay hosts**: Mails fit a certain rule will be sent through a designated relay server. After ticking this option, you can adjust recipient and sender rule by clicking the **Relay Host List** button.



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: 25

□ Always use a secure connection (TLS)

□ Authentication required

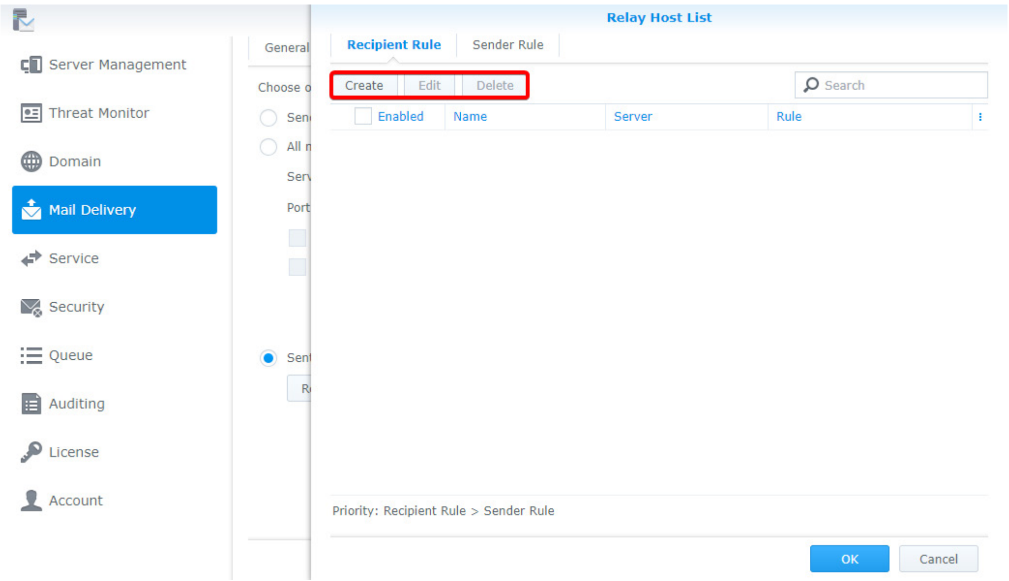
Account:

Password:

● Sent via multiple relay hosts

- **Recipient Rule**: Mails sent to designated mail 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**: Mails sent from designated addresses or domains will be sent through a designated relay server.

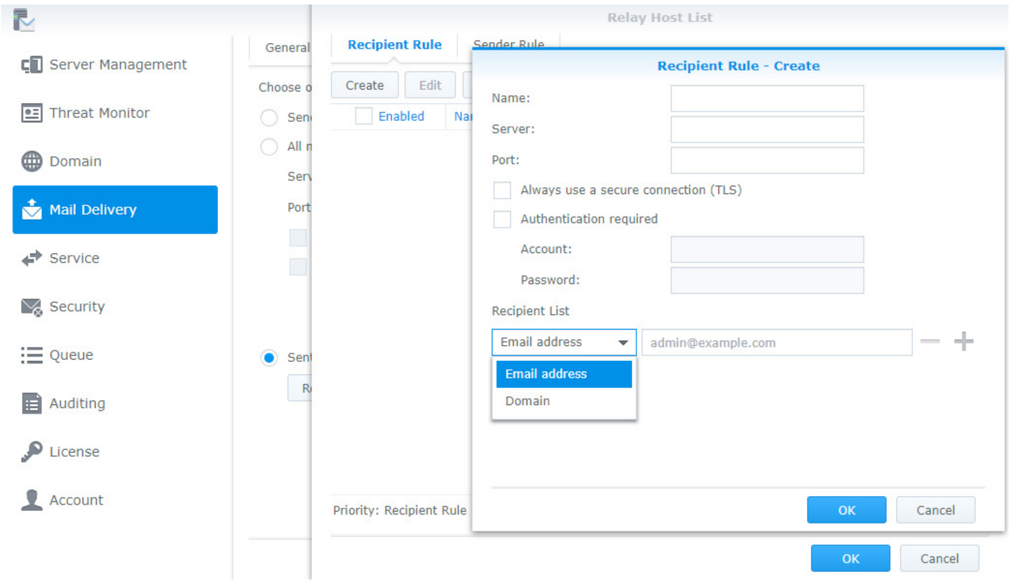
1 Click the **Create**, **Edit** or **Delete** button to manage recipient and sender rules.



2 Enter the name of the rule, specify a relay server and port.

3 Edit the **Recipient List** by selecting email address or domain so emails relayed to the server will be received by the specified email addresses or domains.

4 Click **OK** to save settings.



5 Click **Apply** to save settings.

Set up Relay Control

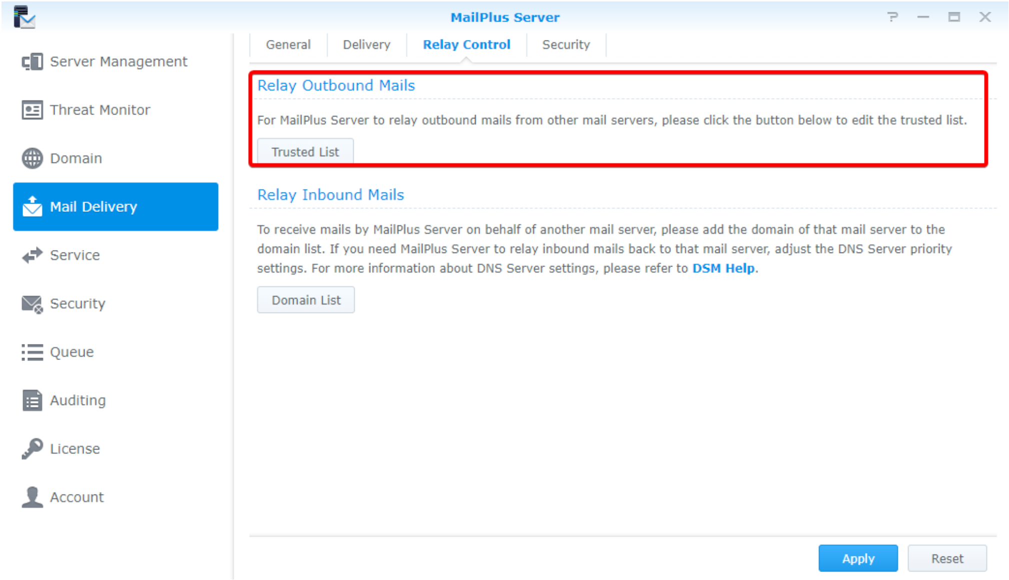
In the **Relay Control** tab, you can adjust settings of MailPlus Server so it can send or receive mails for multiple mail servers.

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

  1 Go to **Mail Delivery** > **Relay Control**.

  2 Click the **Trusted List** button in the **Relay Outbound Mails** section.

  3 Click **Create** and enter rule name, and specify the IP address or subnet mask of other mail servers.



Relay Outbound Mails

For MailPlus Server to relay outbound mails from other mail servers, please click the button below to edit the trusted list.

Relay Inbound Mails

To receive mails by MailPlus Server on behalf of another mail server, please add the domain of that mail server to the domain list. If you need MailPlus Server to relay inbound mails back to that mail server, adjust the DNS Server priority settings. For more information about DNS Server settings, please refer to **DSM Help**.

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

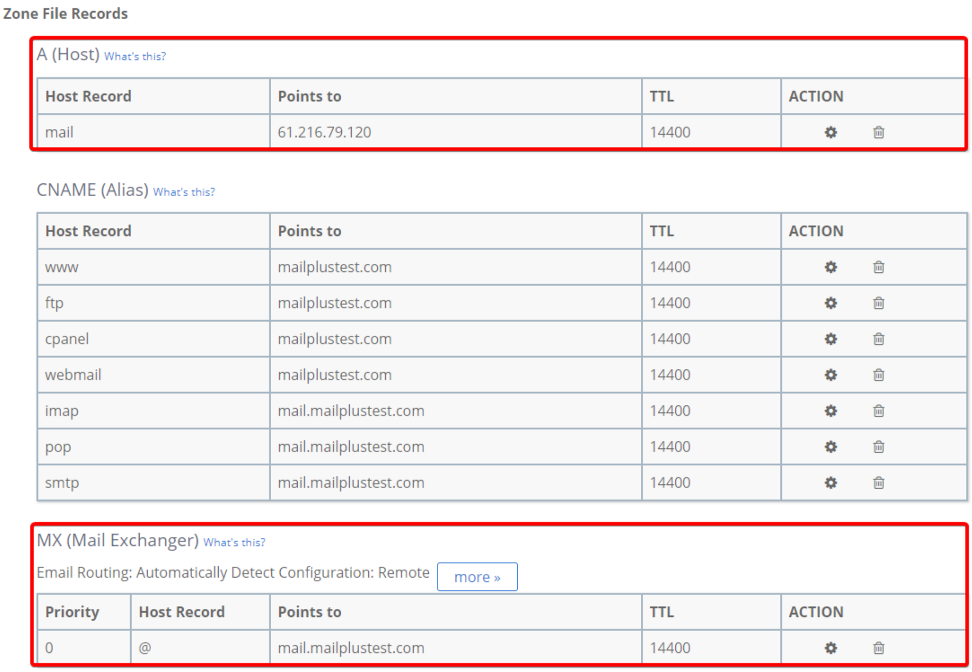
Note:
If you tick the **Check if the senders' email addresses belong to the login accounts** checkbox in the **General** tab, mails from **Trusted List** might be rejected by **MailPlus Server**. You can go to the **General** tab, and tick the **Skip the check for sender's email address to see if it 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 in the **General** section, mails from local networks will not be blocked by **MailPlus Server**.

Relay inbound mails for other mail servers

To relay inbound mails for other mail servers, please set up a DNS record first. You may refer to the following steps and then go to **Domain List** to add the 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 will use bluehost as the example.

2 After logging into bluehost, adjust the following settings accordingly. 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 mails 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	⚙ 🗑

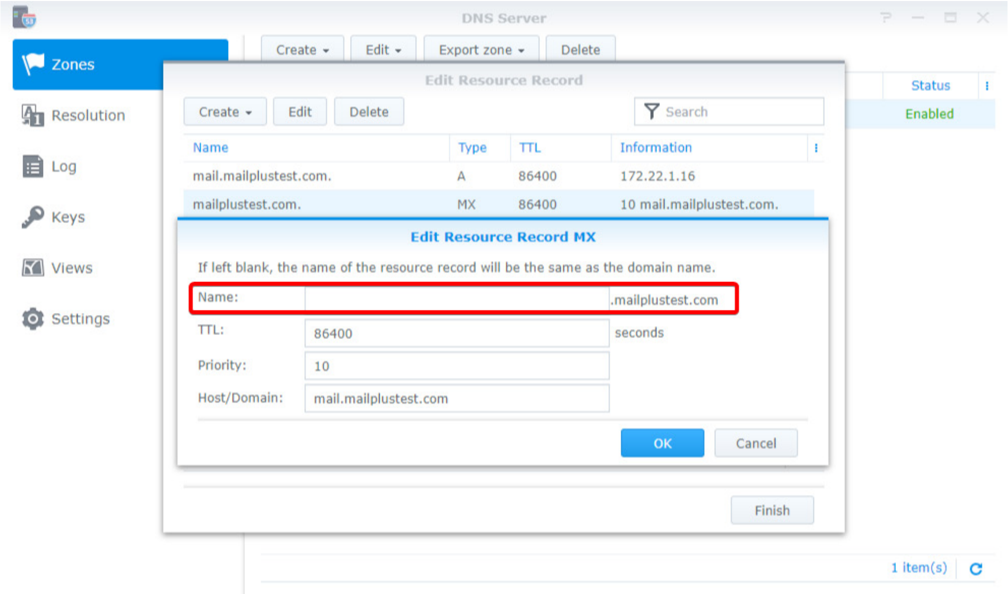
MX (Mail Exchanger) What's this?

Email Routing: Automatically Detect Configuration: Remote

Priority	Host Record	Points to	TTL	ACTION
0	@	mail.mailplustest.com	14400	⚙ 🗑

3 Set up a Synology internal DNS server for MailPlus Server to find your main mail server.

4 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.



Edit Resource Record

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

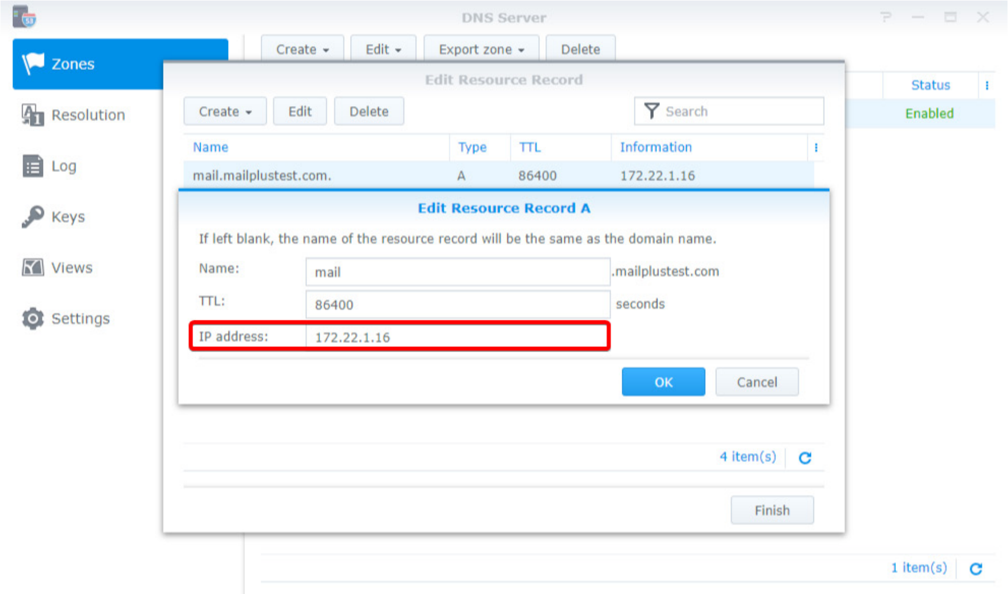
If left blank, the name of the resource record will be the same as the domain name.

Name: .mailplustest.com

TTL: 86400 seconds

Priority: 10

Host/Domain: mail.mailplustest.com



Edit Resource Record

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

Edit Resource Record A

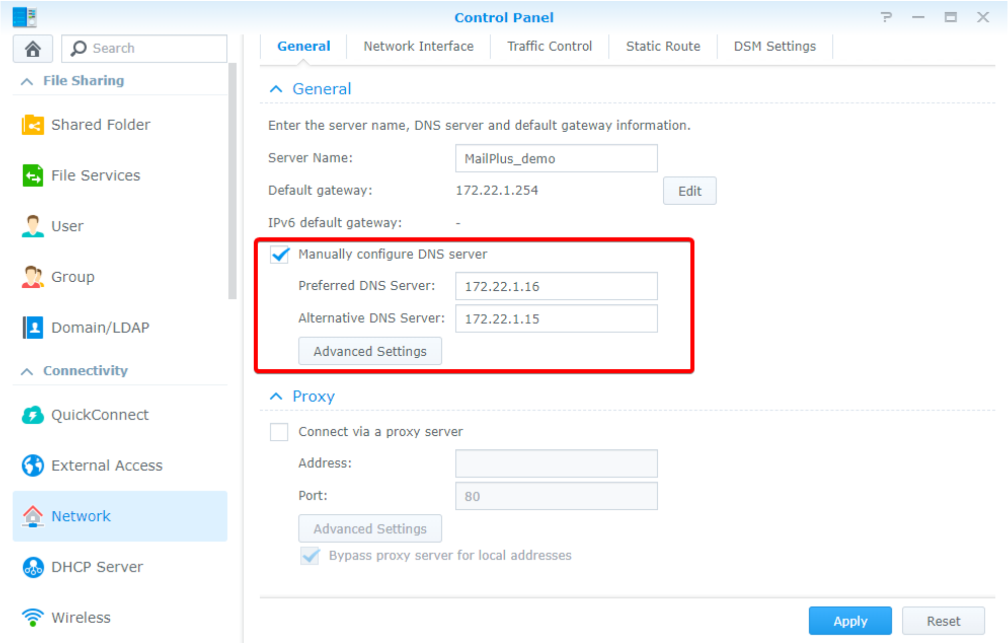
If left blank, the name of the resource record will be the same as the domain name.

Name: mail .mailplustest.com

TTL: 86400 seconds

IP address: 172.22.1.16

5 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 enter 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 mails, it will check the MX records of the two DNS servers, and send the mails to the mail server with the higher priority.



Enter the server name, DNS server and default gateway information.

Server Name: MailPlus_demo

Default gateway: 172.22.1.254

IPv6 default gateway: -

☑ Manually configure DNS server

Preferred DNS Server: 172.22.1.16

Alternative DNS Server: 172.22.1.15

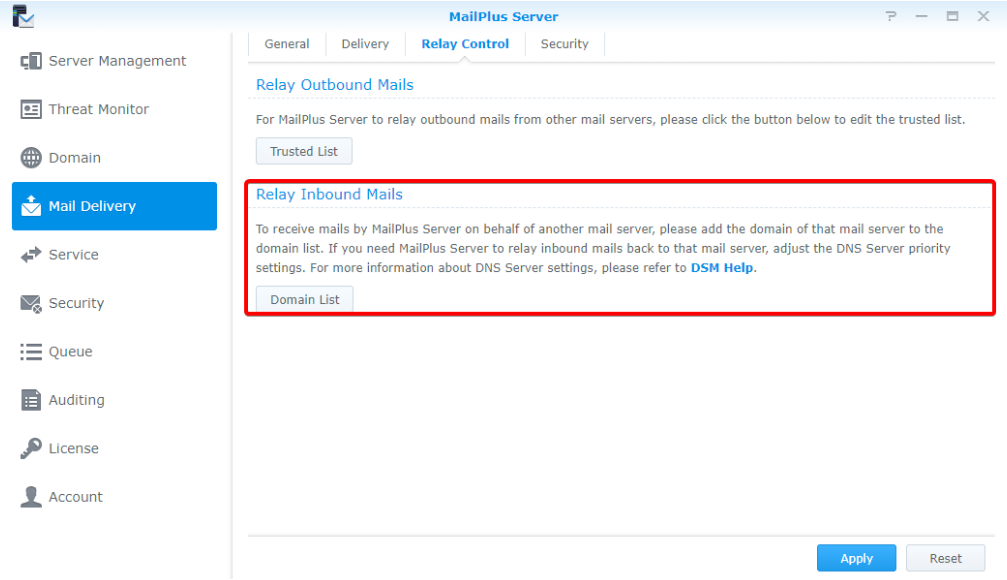
□ Connect via a proxy server

Address:

Port: 80

☑ Bypass proxy server for local addresses

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



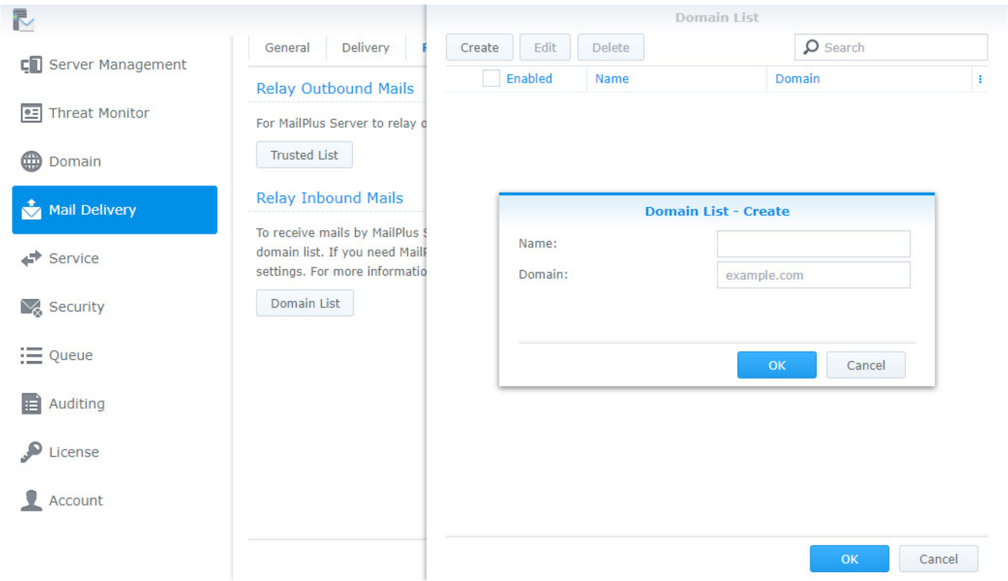
Relay Outbound Mails

For MailPlus Server to relay outbound mails from other mail servers, please click the button below to edit the trusted list.

Relay Inbound Mails

To receive mails by MailPlus Server on behalf of another mail server, please add the domain of that mail server to the domain list. If you need MailPlus Server to relay inbound mails back to that mail server, adjust the DNS Server priority settings. For more information about DNS Server settings, please refer to **DSM Help**.

7 Click the **Create** button.



8 Enter rule name and domain.

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

Note:

1. Although mails are sent internally, you should configure the security settings in the **Spam** and **Antivirus** tab of **Security** to avoid malicious mails.

2. Since the security settings are turned on, you can add mails to the whitelist in **Mail Delivery** > **Security** to avoid blocking.

3. Network segment of all servers should be the same.

Domain Settings

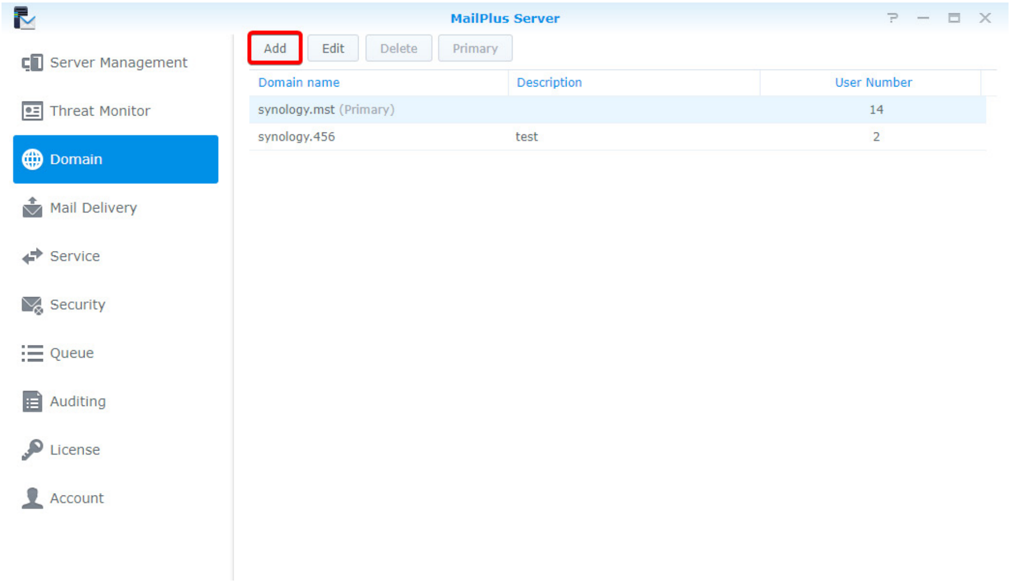
Domain

After setting up multiple domain settings, you can host various email domains in a single MailPlus Server to centralize mails sent to your domains. You can also customize the alias, auto BCC, usage limit and disclaimer for every domain.

Create a domain on MailPlus Server

Log in to MailPlus Server and go to **Domain** to create a new domain. Then, specify the task settings on the following tabs as instructed. In this chapter, synology.456 will be used as an example for demonstration purposes.

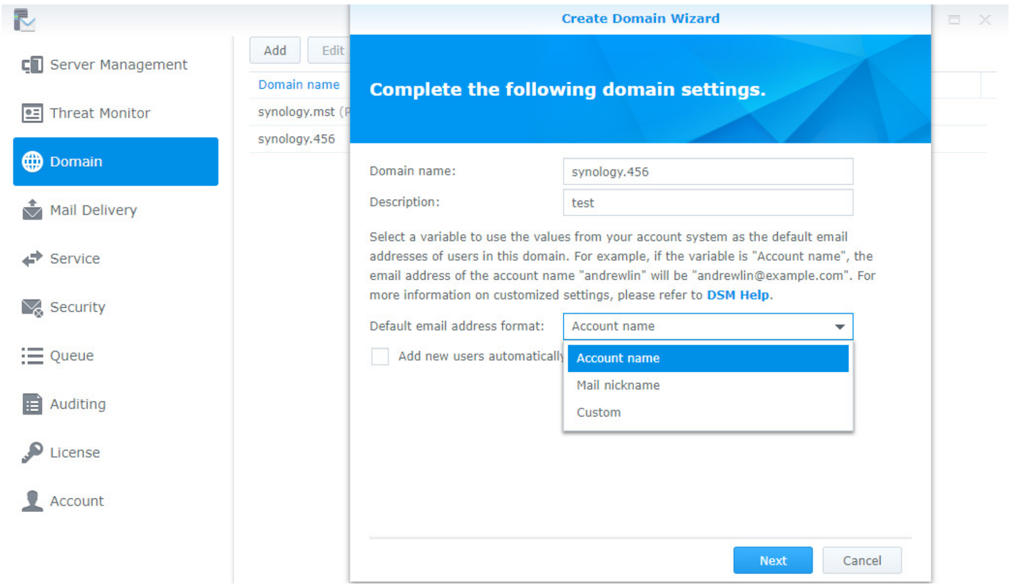
1 Go to **Domain**, and click the **Add** button.



Domain name	Description	User Number
synology.mst (Primary)		14
synology.456	test	2

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 can choose **Account name**, **Mail nickname**, **Display name** or **Custom** based on the account type you chose in **Service** > **SMTP** > **Account type**.



Complete the following domain settings.

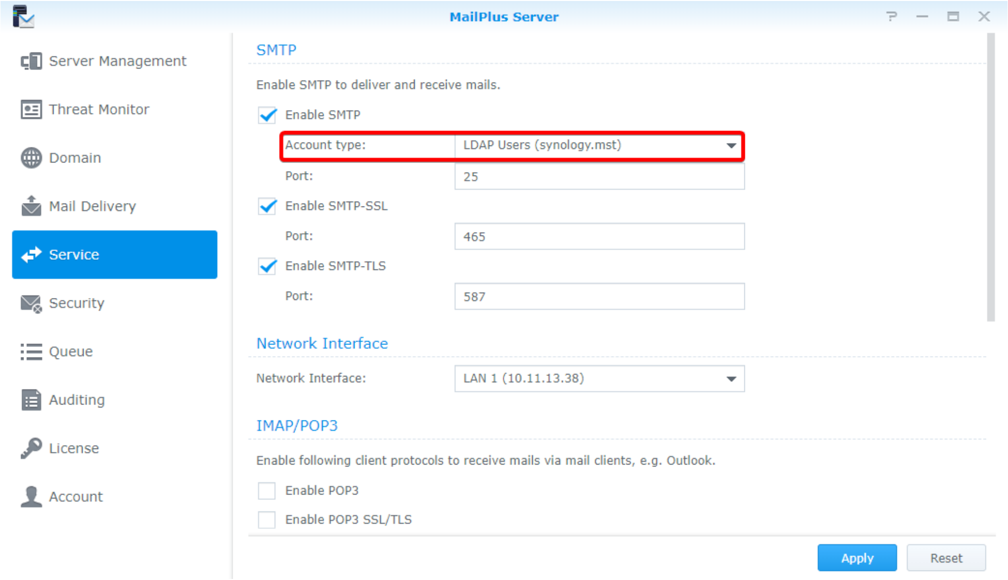
Domain name: synology.456

Description: test

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: Account name

□ Add new users automatically



SMTP

Enable SMTP to deliver and receive mails.

☑ Enable SMTP

Account type: LDAP Users (synology.mst)

Port: 25

☑ Enable SMTP-SSL

Port: 465

☑ Enable SMTP-TLS

Port: 587

Network Interface

Network Interface: LAN 1 (10.11.13.38)

IMAP/POP3

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

□ Enable POP3

□ Enable POP3 SSL/TLS

The following table shows the default settings MailPlus Server provides for different users.

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

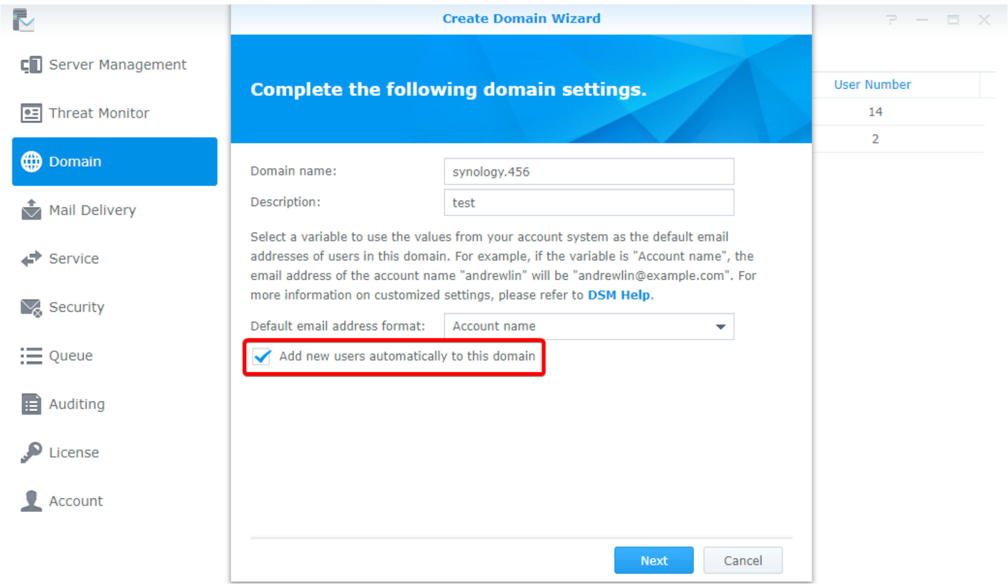
4 In addition to the above options, you can select **Custom** to enter variables in the **Custom variables** field as the default email address formats. The following table shows the variables that MailPlus Server supports:

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 the 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 the surname. For example, if x = 2, the first two letters of the surname will be used.
<xg>	Uses the first x letters of the 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. For more information, please refer to the manual of your account system.

Variables supported by MailPlus Server vary according to different account systems 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 **Add new users automatically to this domain** checkbox to add new users automatically to the domain. MailPlus Server will use the information fetched by the default email address format as users' email addresses.



Complete the following domain settings.

Domain name: synology.456

Description: test

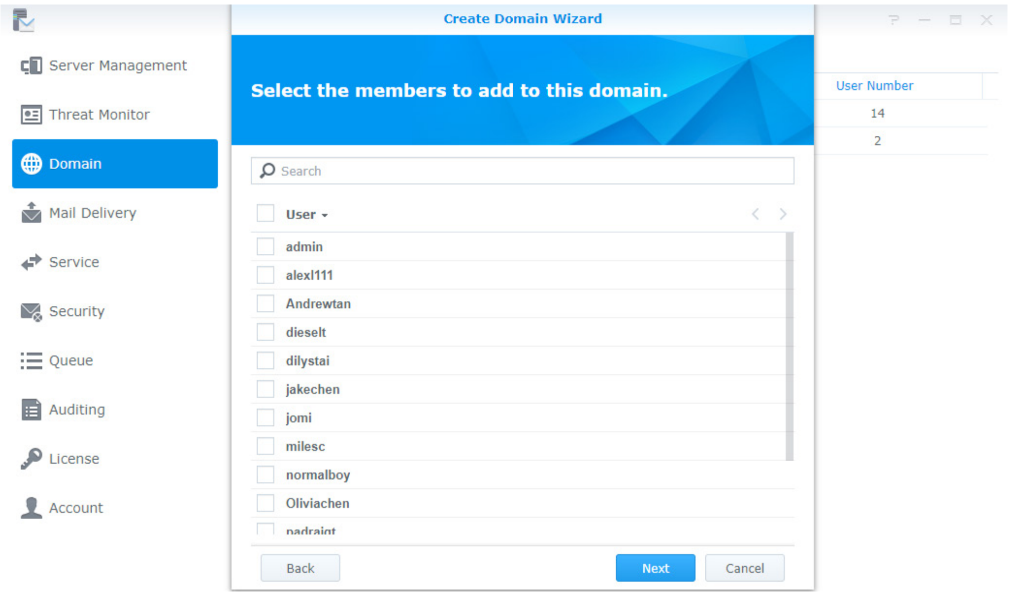
Select a variable to use the values from your account system as the default email addresses of users in this domain. For example, if the variable is "Account name", the email address of the account name "andrewlin" will be "andrewlin@example.com". For more information on customized settings, please refer to DSM Help.

Default email address format: Account name

☑ Add new users automatically to this domain

6 After setting up, click **Next**.

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



Select the members to add to this domain.

□ User
□ admin
□ alexl111
□ Andrewtan
□ dieselt
□ dilystai
□ jakechen
□ jomi
□ milesc
□ normalboy
□ Oliviachen
□ padraigt

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

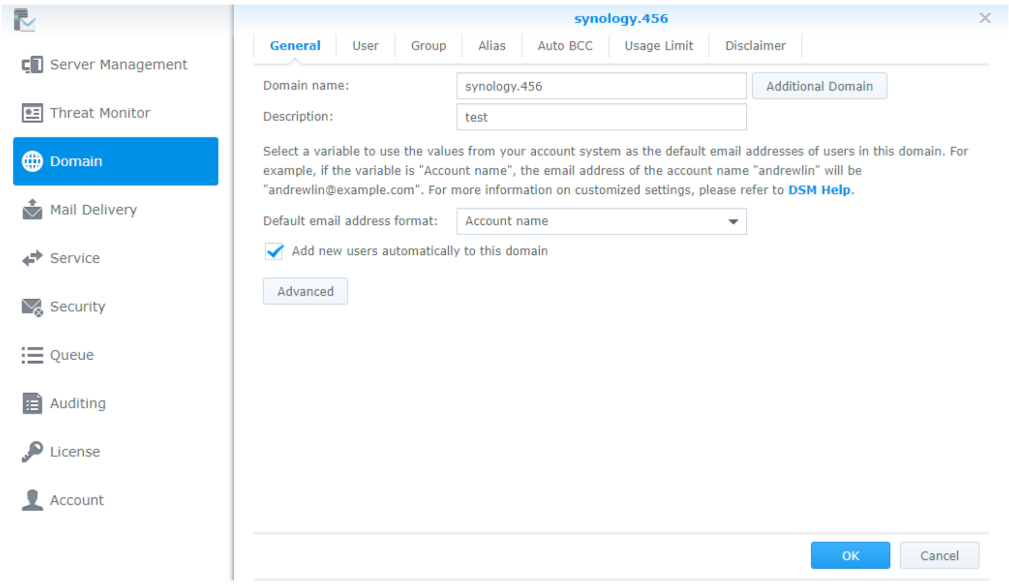
Domain management

MailPlus Server provides management settings for administrators and users in every 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 mails sent to non-exist email addresses or email addresses not activated in a specified 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**: Alias is one of the most common service settings. You can create an alias for one or many recipients. When an email is sent to this alias, the server will automatically deliver mails to all users in the alias. External email addresses can be included in the alias.
- **Auto BCC**: 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.
- **Sending Limit and Daily Quota**: Monitor user outbound messages and traffic.
- **Disclaimer**: Automatically appends a disclaimer to outbound messages at the end of the email content. You can configure settings to apply disclaimers based on specific conditions, and customize disclaimer content to meet different requirements.

Edit general settings for a domain

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



Domain name: synology.456

Description: test

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: Account name

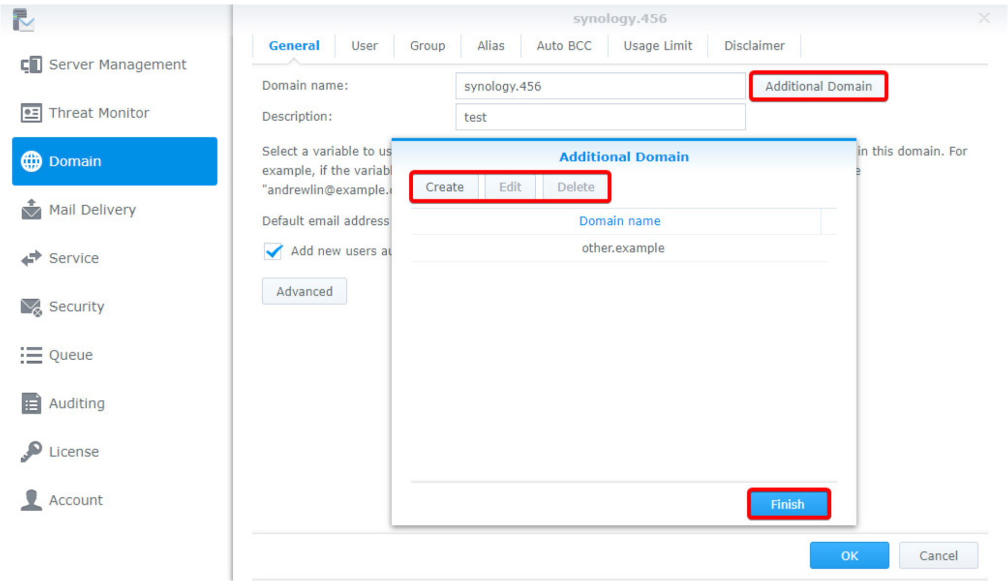
☑ Add new users automatically to this domain

Create and edit additional domains

In Additional Domain, you can create additional domain names for the host to receive emails. The settings of additional domains will be the same as that 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 name and click corresponding buttons to proceed with the actions.
3. In the Additional Domain page, you can view all additional domain names you have created. Using the example above, in addition to receiving emails from domain synology.456, you can also receive emails of an additional domain if it is included as a recipient.

4 Click **Finish** to save settings.



Domain name: synology.456

Description: test

Additional Domain

Domain name
other.example

Note: MX records on DNS Server may require relevant adjustments.

Adjust advanced settings

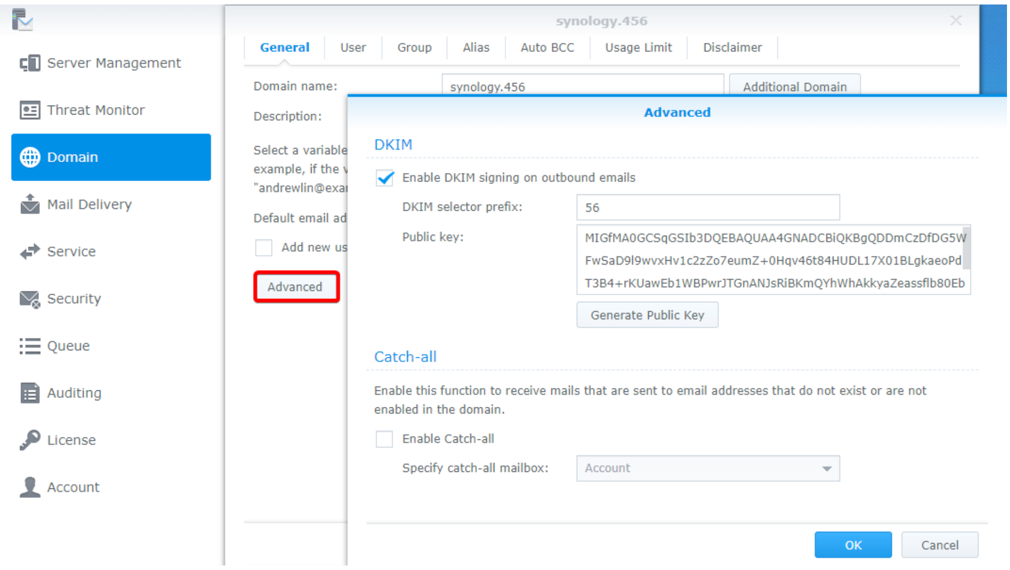
1 Go to **Domain** > synology.456 > **Edit** > **General** and click the **Advanced** button.

2 In the pop-up window of **Advanced**, you can adjust settings of **DKIM** and **Catch-all** for synology.456.

- **DKIM**: You can enable DKIM signing to prevent messages from being modified and identity theft.
    1 Under the **DKIM** section, tick the **Enable DKIM signing on outbound emails** checkbox if you want recipients to trust your delivered messages and to prevent identity theft. You can adjust the DKIM signature below:
    - **DKIM selector prefix**: Add prefix to the DKIM signature. You can enter a DKIM selector prefix of your own choice.
    - **Public key**: Displays the content of the public key used by the system. If the system does not have a public key and private key when enabling DKIM signing, then the system will generate the keys automatically.

    2 Click the **Generate Public Key** button to generate a new set of public key and private key. Currently the system generates keys with key lengths of 1024 bits.

    Note: Existing keys will be deleted after clicking the **Generate Public Key** button.



Domain name: synology.456

Advanced

DKIM

☑ Enable DKIM signing on outbound emails

DKIM selector prefix: 56

Public key: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDmCzDfDG5W FwSaD9l9wvxHv1c2zZo7eumZ+0Hqv46t84HUDL17X01BLgkaeoPd T3B4+rKUawEb1WBPwrJTGnANJsRiBKmQYhWhAkkyaZeassflb80Eb

Catch-all

Enable this function to receive mails that are sent to email addresses that do not exist or are not enabled in the domain.

□ Enable Catch-all

Specify catch-all mailbox: Account

3 Click **OK** to save settings. In addition, to ensure DSKIM signatures can be authenticated by other receiving servers, you need to create a DNS TXT record to allow DKIM authentication to operate properly:

- **TXT record value**: v=DKIM1; k=rsa; p=[DKIM public key] For example, if the domain of MailPlus Server is example.com, and the **DKIM selector prefix** is abc, the public key generated by the system is MIGfMA0GCSqGSIb3DQE, then 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 set a user account to serve as the Catch-all mailbox to receive mails 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.

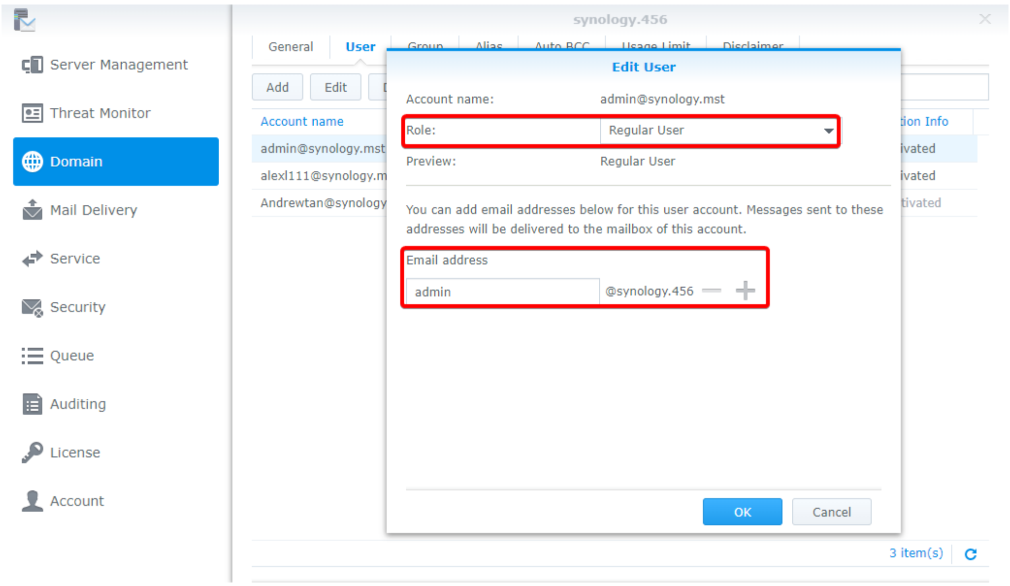
Edit and remove user accounts

1 Go to **Domain**, select synology.456, and click **Edit**.

2 Go to 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**: You can set Regular User for users that do not have the privilege to manage domains.
  - **Follow group settings**: Follow 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.



Account name	ion Info
admin@synology.mst	ivated
alexl111@synology.m	ivated
Andrewtan@synology	tivated

Edit User

Account name: admin@synology.mst

Role: Regular User

Preview: Regular User

You can add email addresses below for this user account. Messages sent to these addresses will be delivered to the mailbox of this account.

Email address

admin @synology.456

4 If you want to remove user accounts, select target user accounts 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**.

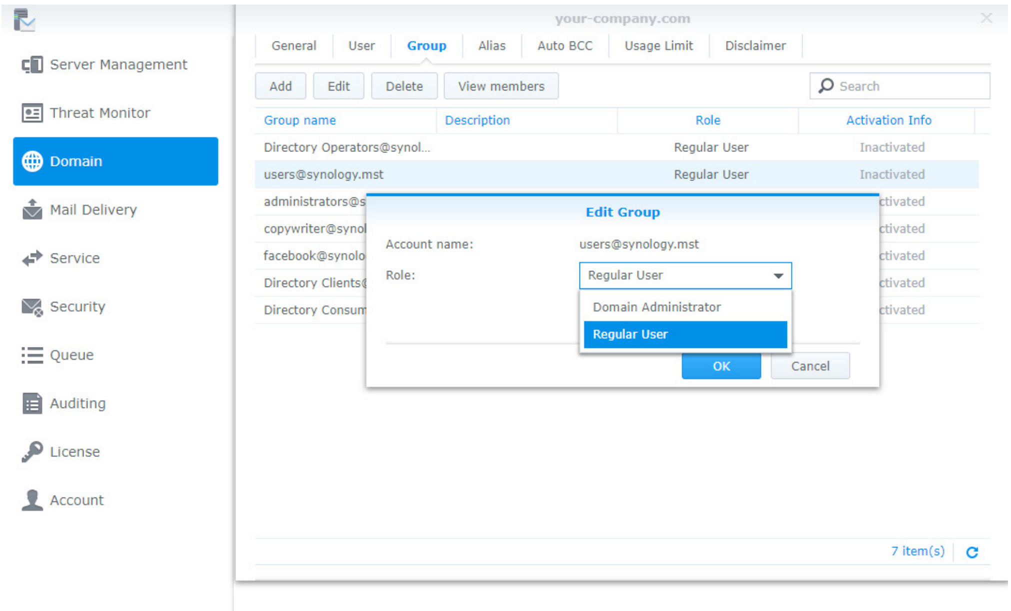
4 Confirm the email addresses of the members, and click **Apply**.

Edit and remove groups

1 Go to **Domain**, select synology.456, and click **Edit**.

2 Go to the **Group** tab, select a user group you want to edit, and click **Edit**.

3 In the **Edit Group** window, you can select **Domain Administrator** in the **Role** drop-down menu so all the users in **Group** will have the permissions as a **Domain Administrator**.



Group name	Description	Role	Activation Info
Directory Operators@synol...		Regular User	Inactivated
users@synology.mst		Regular User	Inactivated
administrators@s			ctivated
copywriter@synol			ctivated
facebook@synolo			ctivated
Directory Clients(			ctivated
Directory Consum			ctivated

Edit Group

Account name: users@synology.mst

Role: Regular User

4 You can select user groups 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

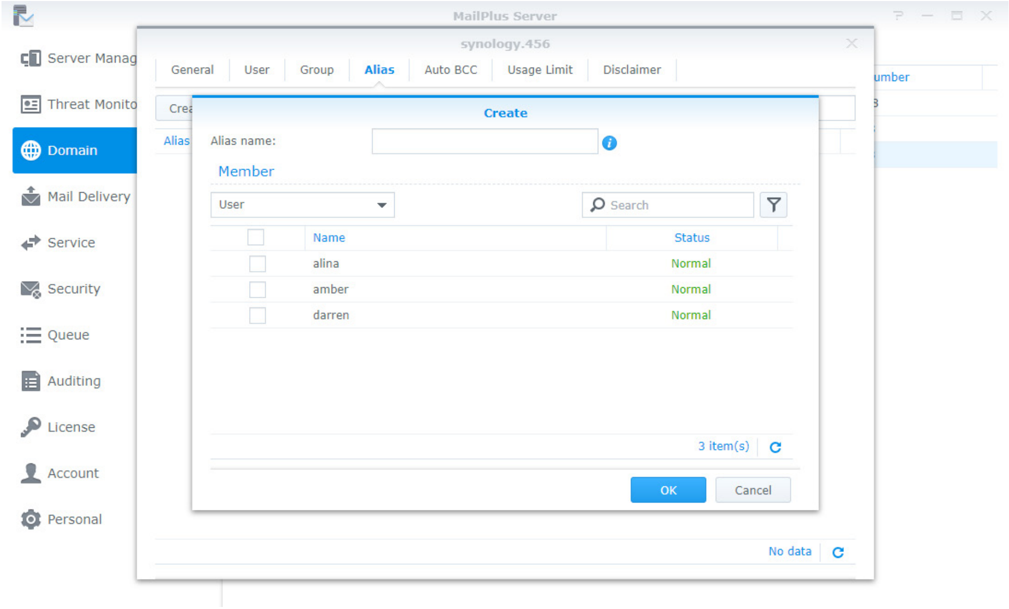
You can create aliases to allow users to send emails to multiple recipients using one alias.

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 Click the drop-down menu below to view aliases, users, groups, or external mailboxes, and add the desired ones to the alias.



	Name	Status
□	alina	Normal
□	amber	Normal
□	darren	Normal

5 Add users to the alias by ticking the check boxes.

6 You can choose users from more than one source, including user accounts, group accounts, and even other aliases.

7 Click **OK** to save settings.

Edit and delete aliases

Please refer to the following the 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 field at the upper-right corner of the page).

3 Click the **Edit** or **Delete** button.

Import/Export aliases

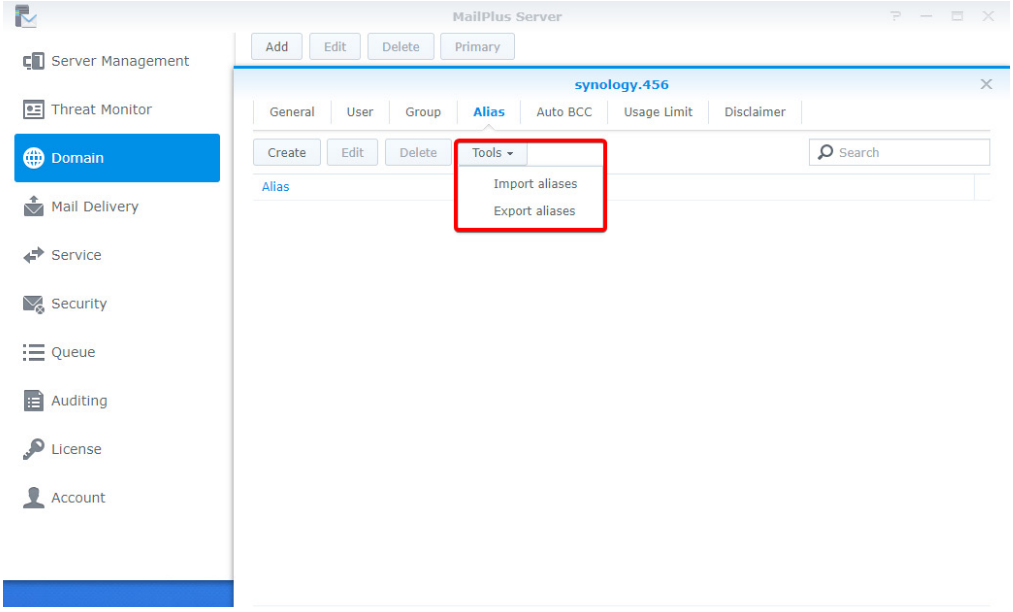
If you want to import or export existing alias lists or alias lists you have previously created, please refer to the following steps:

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 the imported alias name already exists, then this alias will not be imported or updated.
- **Export aliases**: Export and download alias file in 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**.

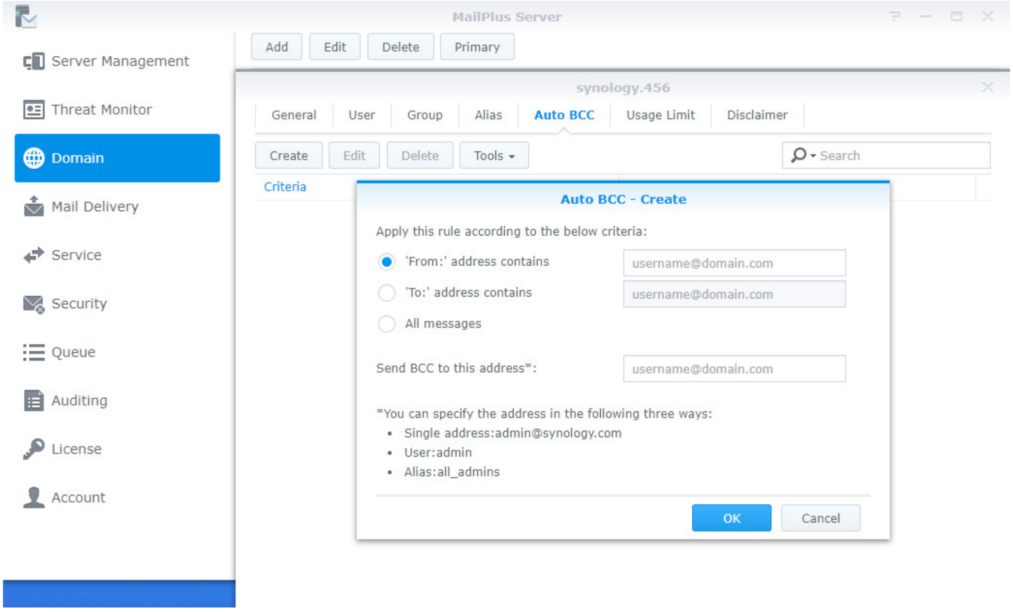
2 Go to **Auto BCC**, and click the **Create** button.

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**: In addition to the notification mail sent from the internal system, for other mails a BCC will be automatically sent to the specified address.

4 Enter the destination address for the BCC to be automatically sent to in the **Send BCC to this address*** field.

5 You can enter email addresses, user accounts, or aliases.



Auto BCC - Create

Apply this rule according to the below criteria:

● 'From:' address contains username@domain.com

○ 'To:' address contains username@domain.com

○ All messages

Send BCC to this address*: username@domain.com

*You can specify the address in the following three ways:

- Single address:admin@synology.com
- User:admin
- Alias:all_admins

6 Click **OK** to save 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.

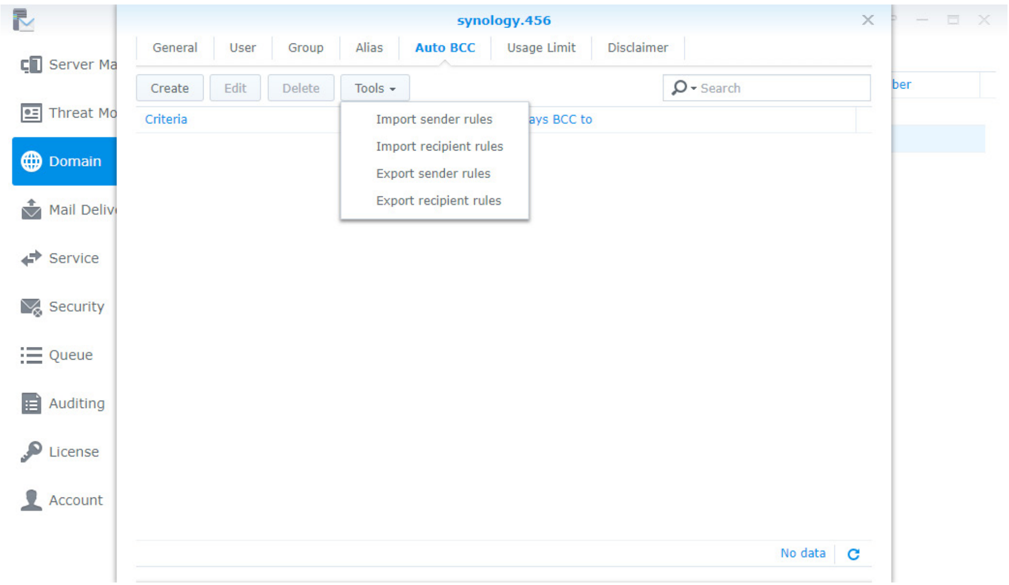
Import/Export Auto BCC rules

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**. Additionally, please make sure the imported file is a postfix format.

Set up Sending Limit and Daily Quota

1 Go to **Domain**, select synology.456, and click **Edit**.

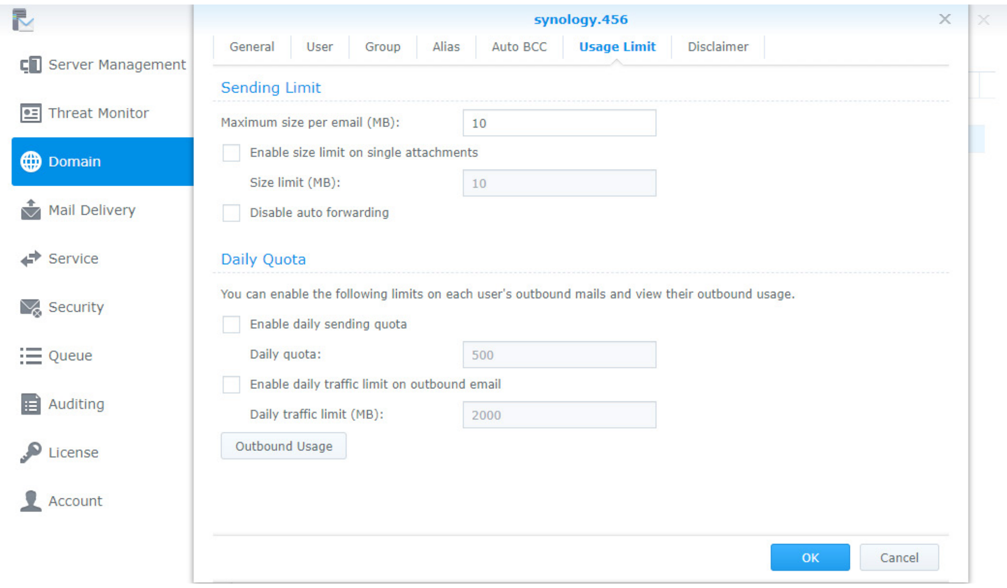
2 Go to the **Usage Limit** tab.

3 Under the **Sending Limit** section, adjust the following settings:

- **Maximum size per email (MB)**: Specify the total size of outbound messages each user can send out every day.
- **Enable size limit on single attachments**: Tick this option to specify the size limit for single attachments, then enter a value in the **Size limit (MB)** field below.
- **Disable auto forwarding**: Tick this option to disable auto forwarding.

4 Under the **Daily Quota** section, adjust the following settings:

- **Enable daily sending quota**: Tick this option to limit the number of outbound messages a user can send daily.
- **Enable daily traffic limit on outbound email**: Tick this option to limit the total size of outbound messages a user can send daily.
- **Outbound Usage**: Click this button to view the outbound email usage of an individual user.



Sending Limit

Maximum size per email (MB): 10

□ Enable size limit on single attachments

Size limit (MB): 10

□ Disable auto forwarding

Daily Quota

You can enable the following limits on each user's outbound mails and view their outbound usage.

□ Enable daily sending quota

Daily quota: 500

□ Enable daily traffic limit on outbound email

Daily traffic limit (MB): 2000

Outbound Usage

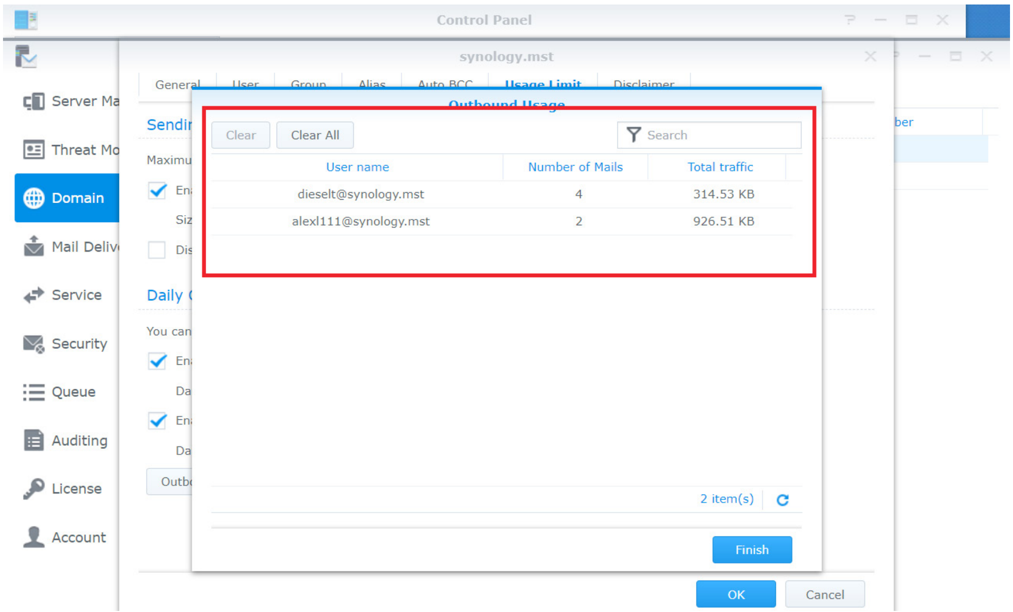
You can view the total number of recorded outbound messages here. If a user has reached the daily quota, you can clear records to allow the user to continue sending emails.

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 at 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 for all users on the list.



User name	Number of Mails	Total traffic
dieselt@synology.mst	4	314.53 KB
alexl111@synology.mst	2	926.51 KB

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

Create disclaimers

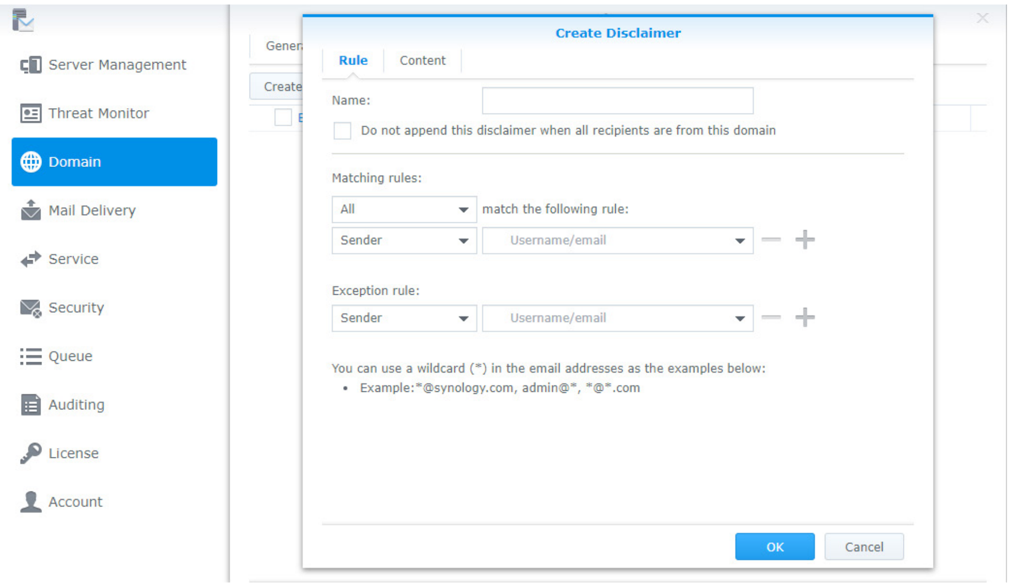
This Disclaimer function allows users to automatically include custom messages in outbound emails, shown at the bottom or end of the emails. Please refer to the following steps to create disclaimers:

> ***Note:*** You can have multiple disclaimers and rules, however only one disclaimer can be applied to one email. Please refer to **Edit** and **Delete** Disclaimers.

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.



Name:

□ Do not append this disclaimer when all recipients are from this domain

Matching rules:

All match the following rule:

Sender Username/email — +

Exception rule:

Sender Username/email — +

You can use a wildcard (*) in the email addresses as the examples below:

- Example:*@synology.com, admin@*, *@*.com

4 Enter the disclaimer name in the **Name** field.

5 Choose to tick the **Do not append this disclaimer when all recipients are from this domain** checkbox:

- When detected as an internal email (emails sent to other internal users) by the server, the disclaimer will not be appended.

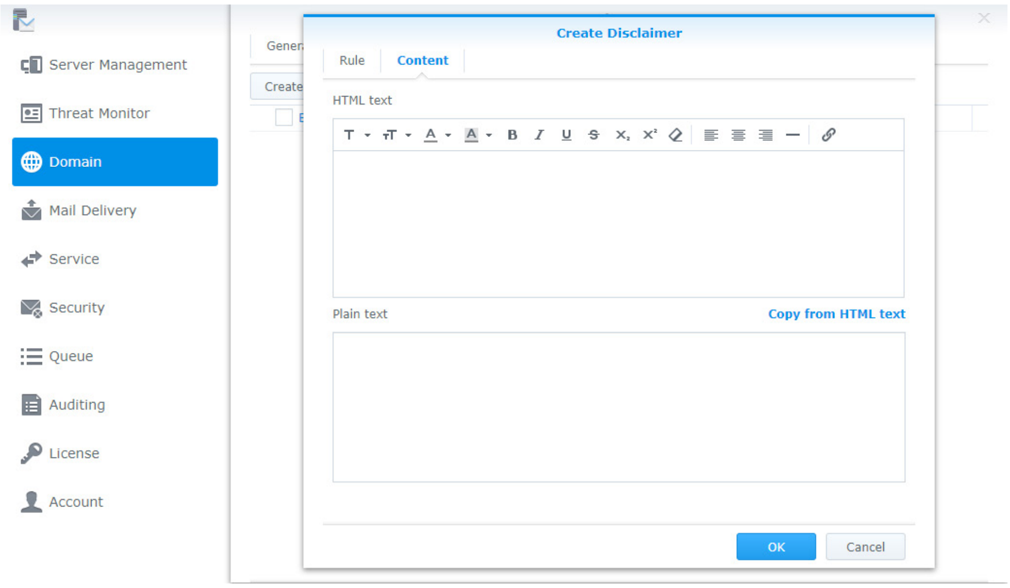
> ***Note:*** If one of the recipients is not an internal user, the disclaimer will still be appended.

6 Set the criteria using the following options:

- **Matching rules**: Includes two options, **All** and **any**. When selecting **All**, the disclaimer will be appended only if all matching rules are met. When selecting **any**, the disclaimer will be appended if at least one matching 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 matching the criteria for **Matching rules**.

7 Click the **+** button to create more than one **Matching rule** or **Exception rule**, and click the **-** button to remove a rule.

8 After setting up the rules, go to the **Content** tab to edit your **HTML text** and **Plain text** content to make sure the content displays correctly on the client end. For more information, please refer to **this article**.



9 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, removing all HTML tags. Click **OK** to finish.

Edit and delete disclaimers

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

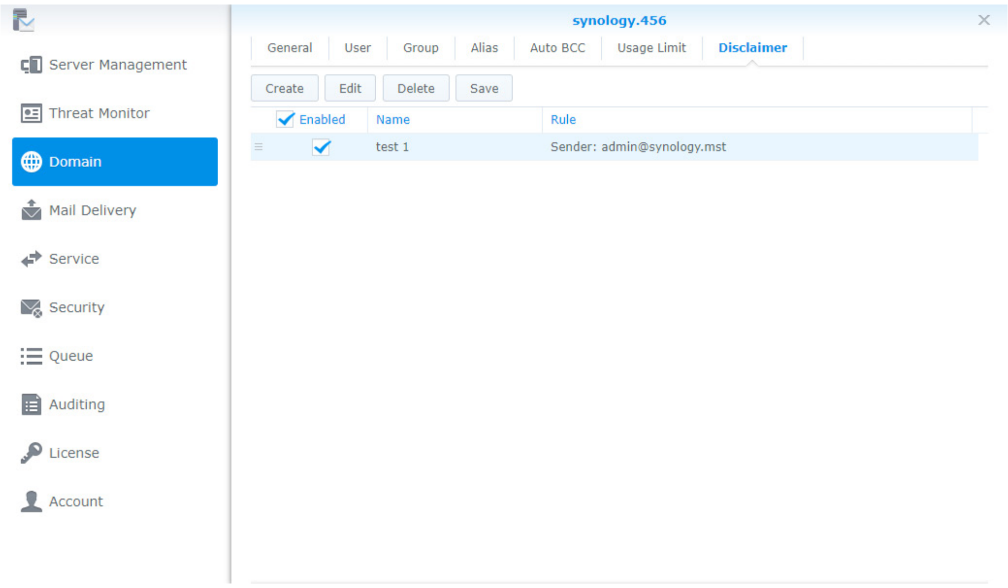
> ***Note:*** Disclaimer will be checked from top to bottom to determine if the criteria have been met. When a criterion has been met, the disclaimer will be applied, thereby ending the disclaimer check.

1 Go to **Domain**, select synology.456, and click **Edit**.

2 Go to the **Disclaimer** tab. Higher disclaimers have more priority than lower ones. To change their priority, select a desired one and drag and drop it to a suitable position.

3 Choose to enable the disclaimer rule.

4 Select a disclaimer rule you want to modify, and click the **Edit** or **Delete** button.



☑ Enabled	Name	Rule
✓	test 1	Sender: admin@synology.mst

5 Click **Save** to apply 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 provides spam detection standards based the delivery nature of spam messages to prevent spam.

- **Anti-Spam**: Uses SpamAssasin as the engine to provide users flexible detection rules. Through auto learning and a spam reporting mechanism, MailPlus Server blocks spam messages according to your environment, achieving the best results.
- **Postscreen**: Reduces the probability of receiving spam from rejecting services for spam servers based on open blacklists and the characteristics of senders from spam servers.
- **Greylist:** Runs actions based on the characteristics of senders from spam servers. Since greylists will affect the delivery speed of messages, please fully understand the greylist mechanism before enabling this feature.

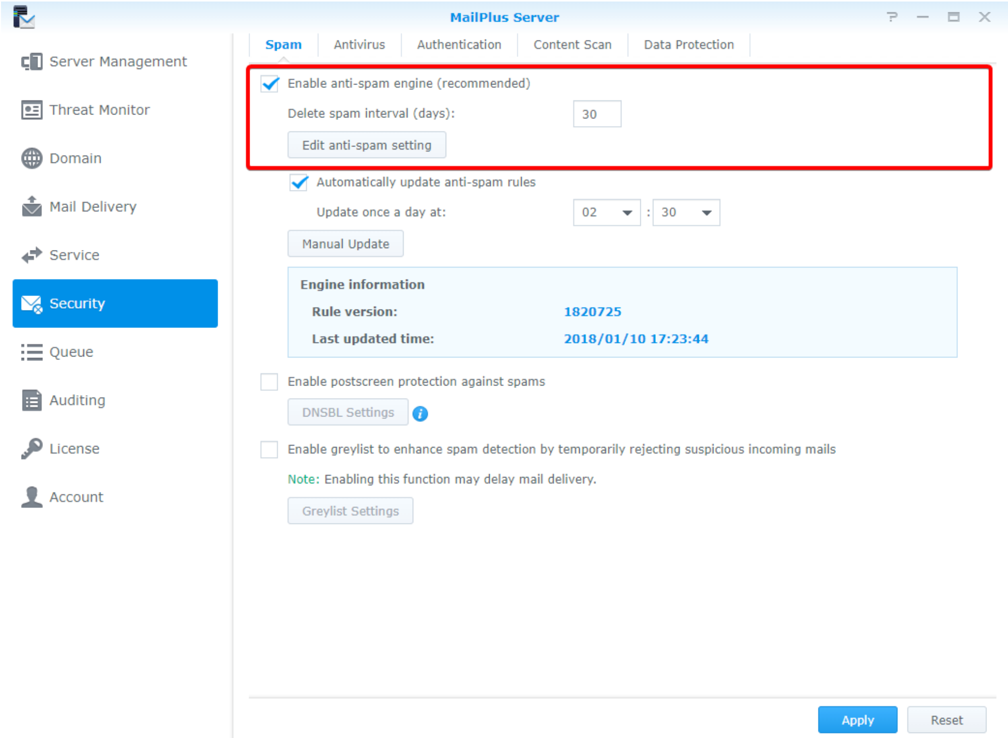
Enable Anti-Spam

MailPlus Server uses the SpamAssasin Anti-Spam engine. The SpamAssassin built-in spam detection filters out spam based on the spam score threshold. When an email matches your pre-set detection rule, a point will be added to the score. Messages exceeding the threshold will be marked as spam. You can enable anti-spam directly using the default rules in SpamAssassin. Please refer to the following steps to enable Anti-Spam:

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

- **Enable anti-spam engine**: Tick this option to enable anti-spam. For more information, 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 days, therefore spam messages received over a period of time will be automatically deleted. You can set up the interval here, the default interval is 30 days.

Note: If anti-spam is not enabled, spam will still be regularly deleted.



☑ Enable anti-spam engine (recommended)

Delete spam interval (days): 30

☑ Automatically update anti-spam rules

Update once a day at: 02 : 30

Engine information

Rule version: 1820725

Last updated time: 2018/01/10 17:23:44

☐ Enable postscreen protection against spams

☐ Enable greylist to enhance spam detection by temporarily rejecting suspicious incoming mails

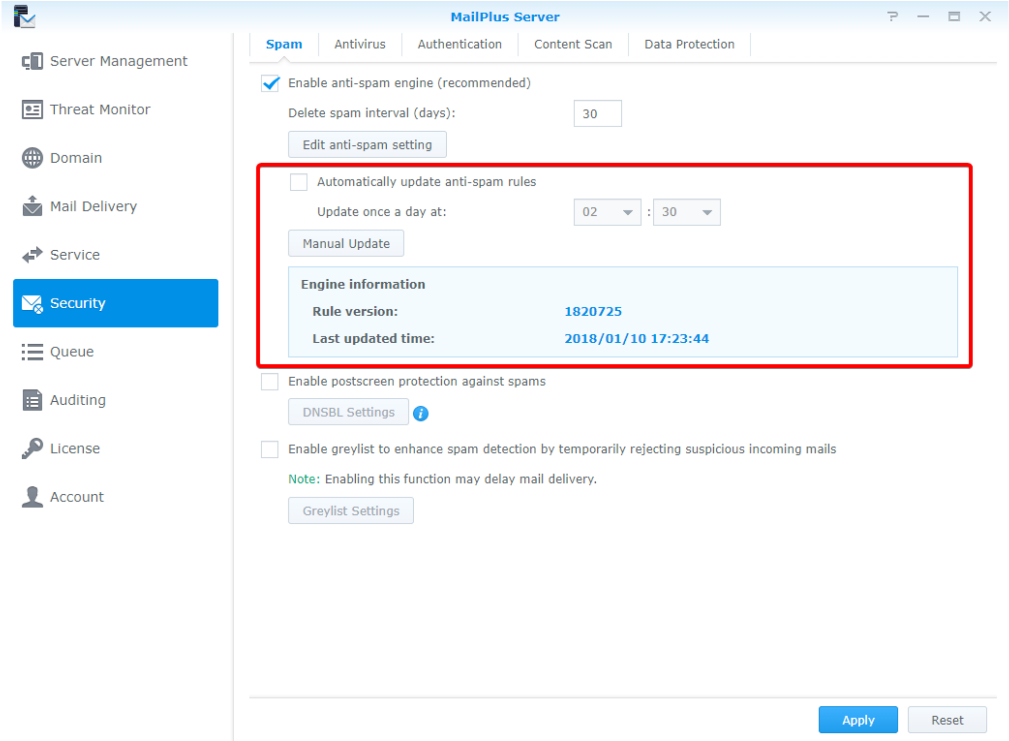
Note: Enabling this function may delay mail delivery.

Update Anti-Spam rules

Anti-Spam spam detection rules are from the database of SpamAssassin. You should regularly update rules to ensure the mail protection features are up-to-date. Please refer to the following steps to update Anti-Spam rules:

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

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



☑ Enable anti-spam engine (recommended)

Delete spam interval (days): 30

□ Automatically update anti-spam rules

Update once a day at: 02 : 30

Engine information

Rule version: 1820725

Last updated time: 2018/01/10 17:23:44

□ Enable postscreen protection against spams

□ Enable greylist to enhance spam detection by temporarily rejecting suspicious incoming mails

Note: Enabling this function may delay mail delivery.

Anti-Spam general settings

The **Anti-Spam** feature provides various customizable settings. You can adjust your Anti-Spam engine according to your environment. Please refer to the following steps to edit the general settings of **Anti-Spam**:

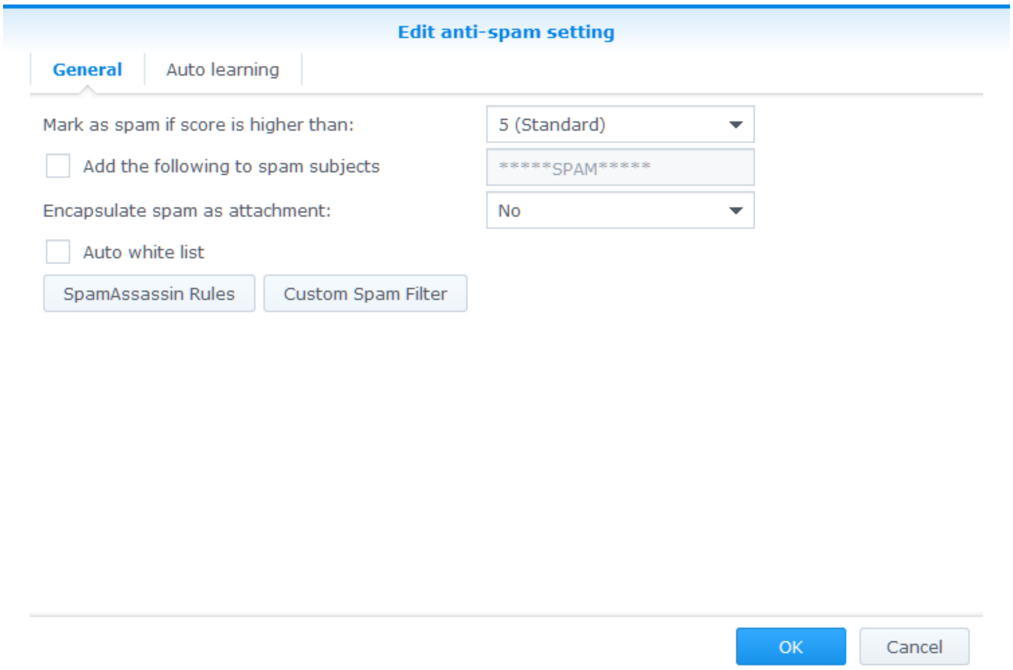
1 Go to **Security** > **Spam** and click the **Edit anti-spam setting** button.

2 Go to the **General** tab in the **Edit anti-spam setting** window, you can adjust the following settings:

- **Mark as spam if score is higher than**: Select a spam score threshold. A message that exceeds the threshold 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 choose to add specific content to the subject of the 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	Report spam without taking other actions.
Yes	Report spam as an attachment encapsulated in a new message.
Yes, as plain text only	Report spam as plain text to avoid web bugs and malicious scripts, then encapsulate as an attachment and send to the recipient. .

- **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.



Edit anti-spam setting

Mark as spam if score is higher than: 5 (Standard)

□ Add the following to spam subjects: *****SPAM*****

Encapsulate spam as attachment: No

□ Auto white list

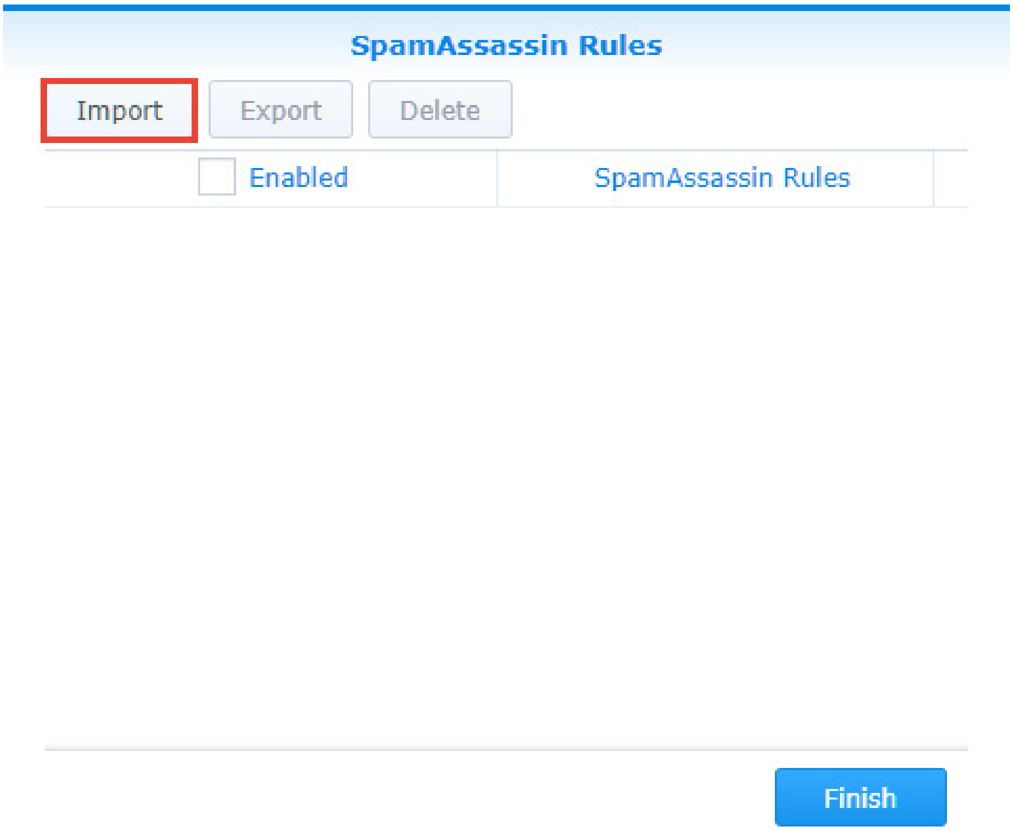
SpamAssassin Rules

1 Go to **Security** > **Spam**, and click the **Edit anti-spam setting** button.

2 Go to the **General** tab in the **Edit anti-spam setting** 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 after imported. You can refer to the **rules** provided by SpamAssassin, or add rules based on the **rules guideline**.



SpamAssassin Rules

4 Select the rule you want to edit, and choose to take the corresponding actions such as **Enable**, **Export**, and **Delete**.

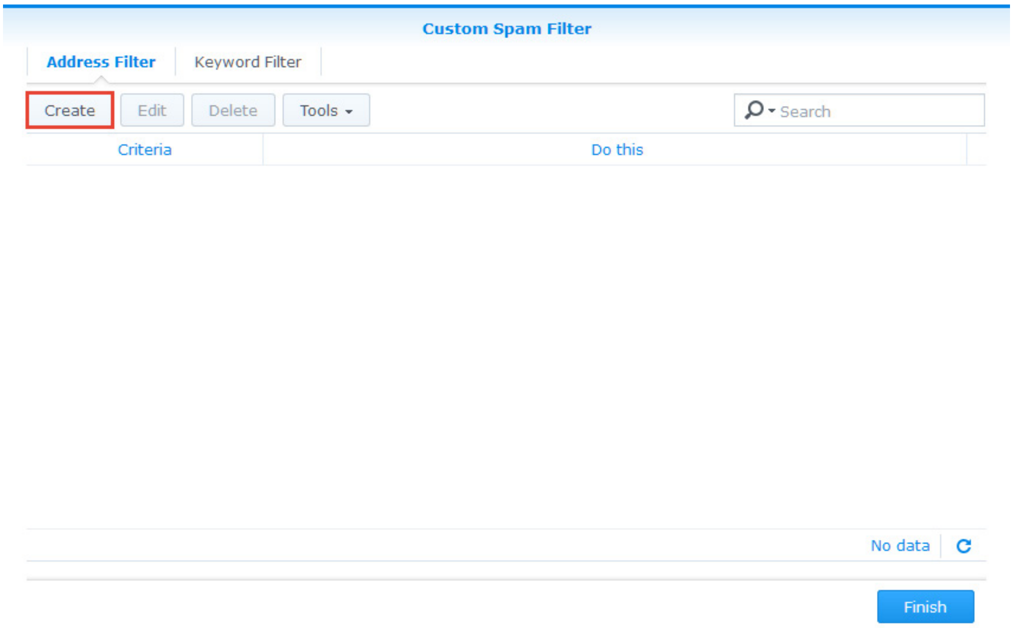
5 Click **Finish** to complete the settings.

Custom Spam Filter

1 Go to **Security** > **Spam**, and click the **Edit anti-spam setting** button.

2 Go to the **General** tab in the **Edit anti-spam setting** window, and click the **Custom Spam Filter** button.

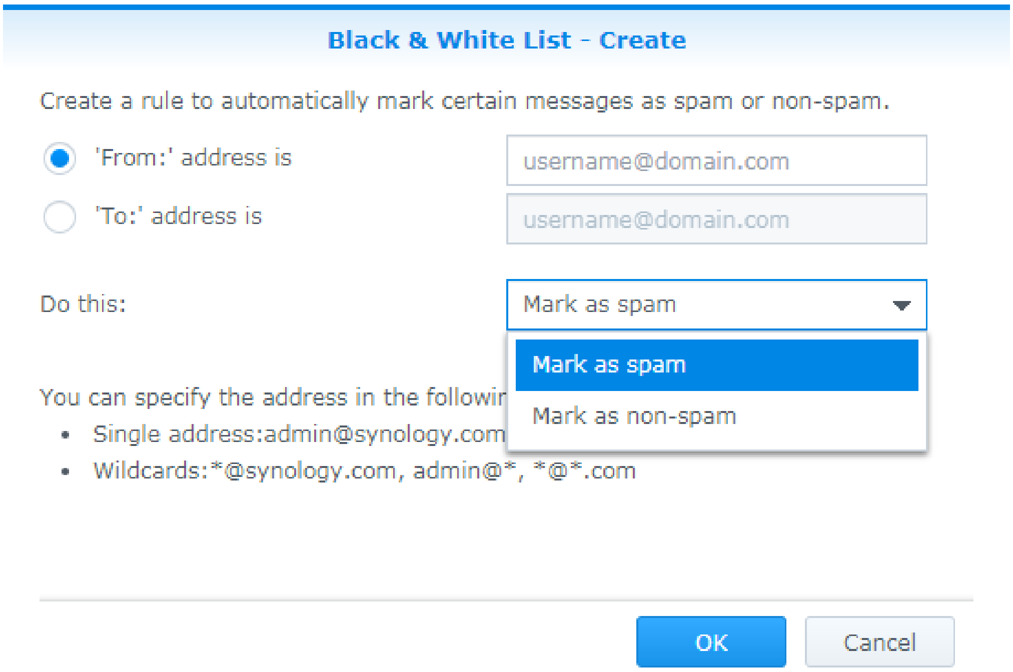
3 Go to the **Address Filter** tab in the **Edit anti-spam** window, and click the **Create** button.



4 Messages will be marked as spam or non-spam based on the sender and recipient criteria. Wildcard characters (*) can be used in the addresses entered.

5 From the **Do this** drop-down menu, select **Mark as spam** or **Mark as non-spam**.

Note: The spam score will be ignored when selecting these actions.



Create a rule to automatically mark certain messages as spam or non-spam.

● 'From:' address is: username@domain.com

○ 'To:' address is: username@domain.com

Do this: Mark as spam

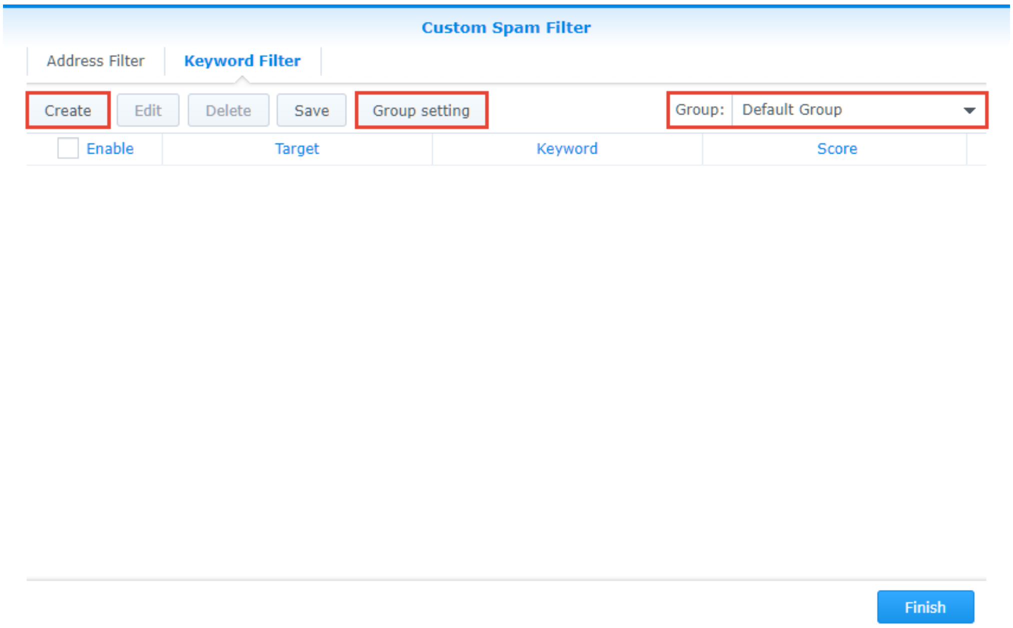
- Mark as spam
- Mark as non-spam

You can specify the address in the followir

- Single address:admin@synology.com
- Wildcards:*@synology.com, admin@*, *@*.com

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

7 Go to the **Keyword Filter** tab in the **Custom Spam Filter** window. You can also manage your keywords by groups. Click on the **Group setting** button to create your group. You can select a group you want to edit from the **Group** drop-down menu on the right.



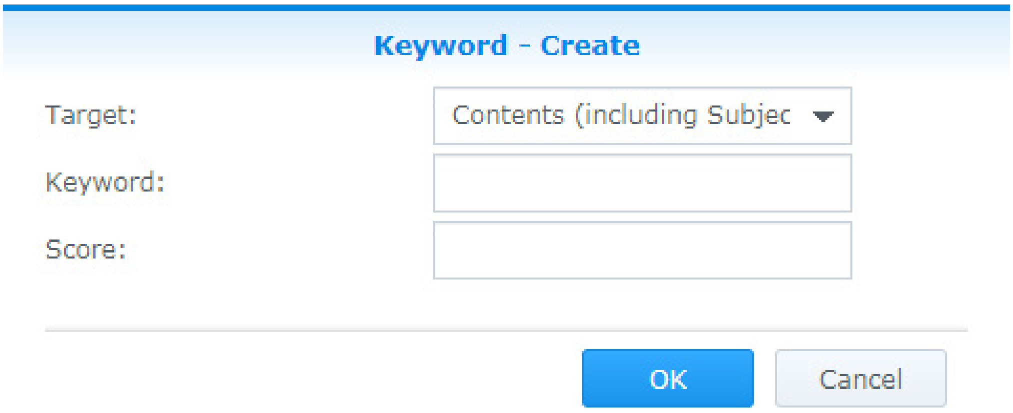
8 Click the **Create** button to customize your rules:

- **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. Regular expression can be used. For more information on regular expression, please refer to **here**.
- **Score**: Specify the number of points that will be added to the total spam score of the email when detecting the keyword.

Note: The email will be marked as spam if the total spam score exceeds the spam score threshold.



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

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

Auto learning and spam reporting settings

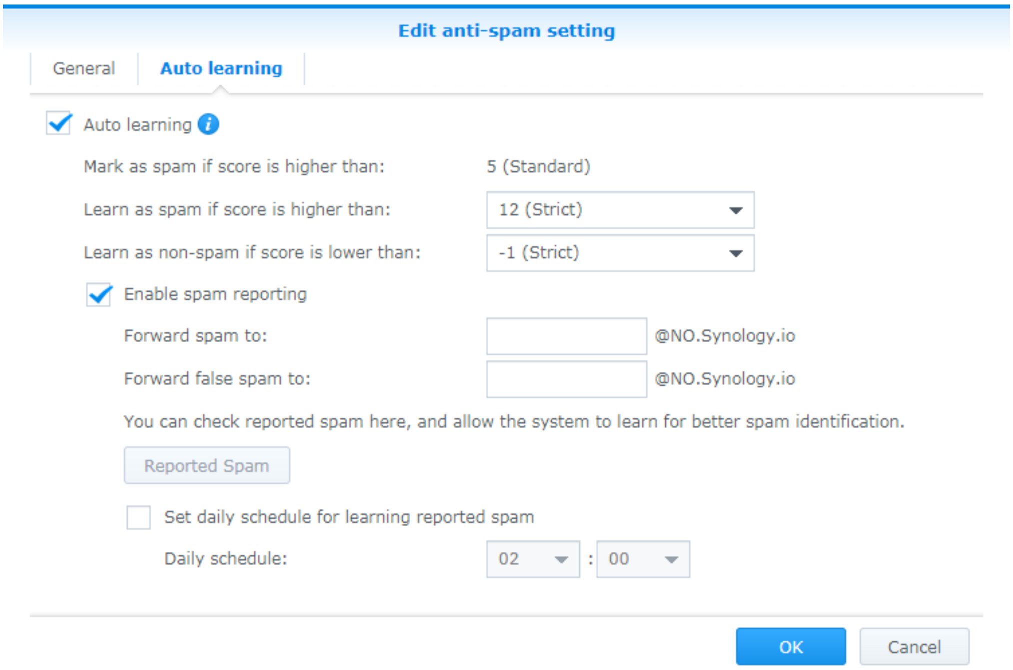
After the anti-spam engine starts running, you can train MailPlus Server to better detect spam with specialized algorithms. Auto learning and spam reporting improves anti-spam detection results to meet different MailPlus Server usage:

- **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 in order for the email to be further analyzed.
- **Spam reporting**: Users can report spam when the Anti-Spam engine is unable to detect spam, or when a message is mistreated as spam. Reporting incorrect categorization to the Anti-Spam engine allows the engine to relearn and improve.

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

1 Go to **Security** > **Spam**, and click the **Edit anti-spam setting** button.

2 Go to the **Auto learning** tab in the **Edit anti-spam setting** window.



Edit anti-spam setting

General | Auto learning

☑ Auto learning

Mark as spam if score is higher than: 5 (Standard)

Learn as spam if score is higher than: 12 (Strict)

Learn as non-spam if score is lower than: -1 (Strict)

☑ Enable spam reporting

Forward spam to: @NO.Synology.io

Forward false spam to: @NO.Synology.io

You can check reported spam here, and allow the system to learn for better spam identification.

Reported Spam

□ Set daily schedule for learning reported spam

Daily schedule: 02 : 00

OK | Cancel

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

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

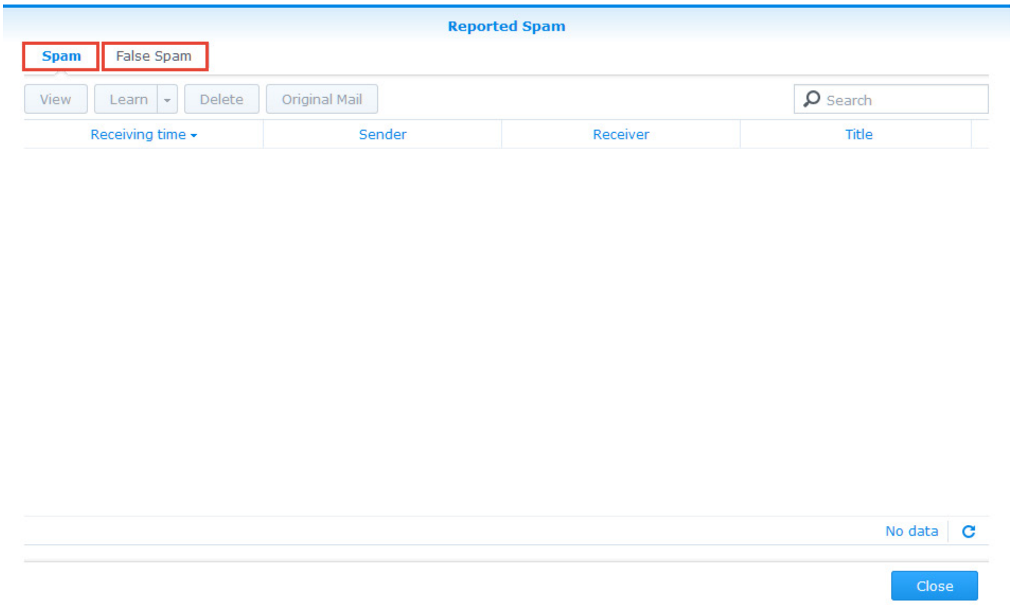
4 Tick the **Enable spam reporting** checkbox to adjust the following settings:

> ***Note:*** The reporting process involves collecting spam to a specific mailbox to undergo learning. Therefore after enabling spam reporting, users can report spam and non-spam based on the following two methods:
>
> 1. If users receive messages using MailPlus, the forwarding mailbox has already been configured for these users. Users just need to mark messages as spam on MailPlus, or go to the spam mailbox on MailPlus to mark messages as non-spam.
> 2. If users receive messages using third party email clients, then they must use the forward as attachment feature from the email clients in order 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 false 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. In 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 the emails in the spam and non-spam mailboxes. Please refer to the following to manage reported spam:

Function	Description
View	View the message content.
Learn	Allow the anti-spam engine to quickly learn from the selected email. After the email has been learned, it will be removed from the list.
Learn All	**Learn All** can be found from the drop-down menu next to the **Learn** button. Click **Learn All** to learn from all the email messages.
Delete	Remove selected messages to prevent them from being learned by the anti-spam engine.
Original Mail	Open a new browser tab to view the original mail.
Search	Search for senders, recipients, subjects in the search field at the upper-right corner to search for email messages.



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

Note:

1. 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 license user, and will only be used to receive email samples.
2. 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 two main functions:

- Checks if the sender follows smtp standards and sends commands after the smtp server greeting. If the sender sends a command before the smtp server greeting, then this sender will be blocked.

- Checks other DNSBL servers based on the sender's IP address. If the IP address is blacklisted by other servers, then this sender will be blocked.

DNSBL Settings

Postscreen allows for setting up multiple DNSBL servers, however relies on one DNSBL server to make the decision. Matching a criteria during server check results in spam points. Spam points generated from testing different servers will be accumulated. When this the total accumulated score exceeds the value specified in **DNSBL Score Threshold**, services will be rejected. Please refer to the following steps to adjust DNSBL settings:

1 Go to **Security** > **Spam**, and click the **Enable postscreen protection against spams** checkbox.

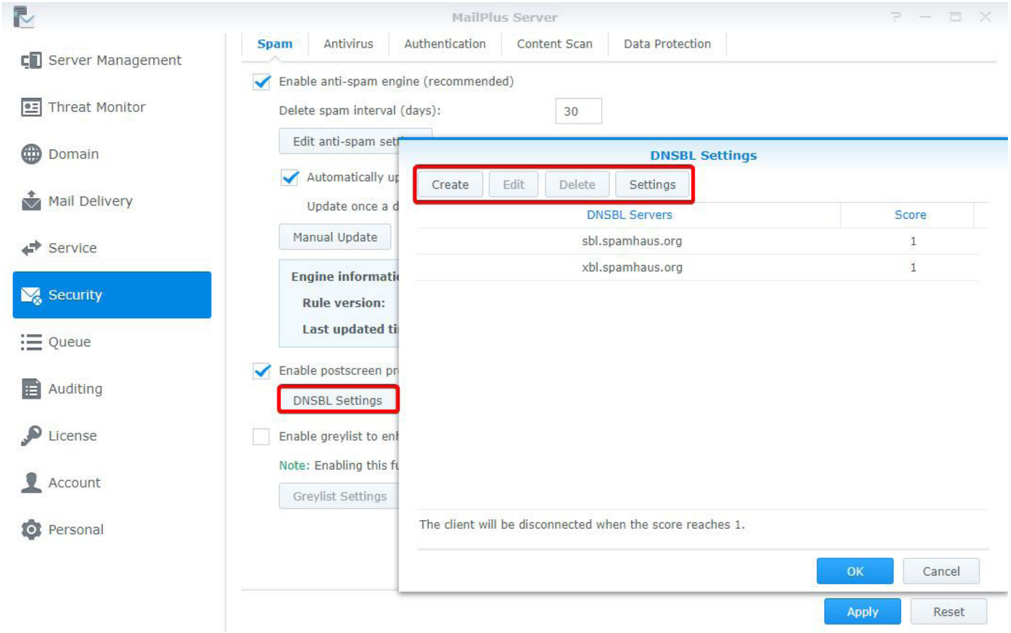
2 Click the **DNSBL Settings** button to edit the servers that are to be checked.

3 Click the **Settings** button to specify **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 field.

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



☑ Enable anti-spam engine (recommended)

Delete spam interval (days): 30

☑ Automatically up

Update once a d

Engine informati

Rule version:

Last updated ti

☑ Enable postscreen pr

DNSBL Settings

☐ Enable greylist to en

Note: Enabling this fu

DNSBL Settings

DNSBL Servers	Score
sbl.spamhaus.org	1
xbl.spamhaus.org	1

The client will be disconnected when the score reaches 1.

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

Enable Greylist

When there are new inbound messages, the system will check if there are past IP address, sender, and recipient records of these inbound messages. If there are no records found, the message will be treated as a suspicious message, and an error message will be sent back to the sender, requesting for the sender to try sending the message again later. According to smtp protocol standards, senders receiving the error messages will try to send the message again at a later time, however most spam senders will give up sending the message. When regular senders send the message again after a period of time, the system will receive the message. The Greylist mechanism uses this method to reject spam.

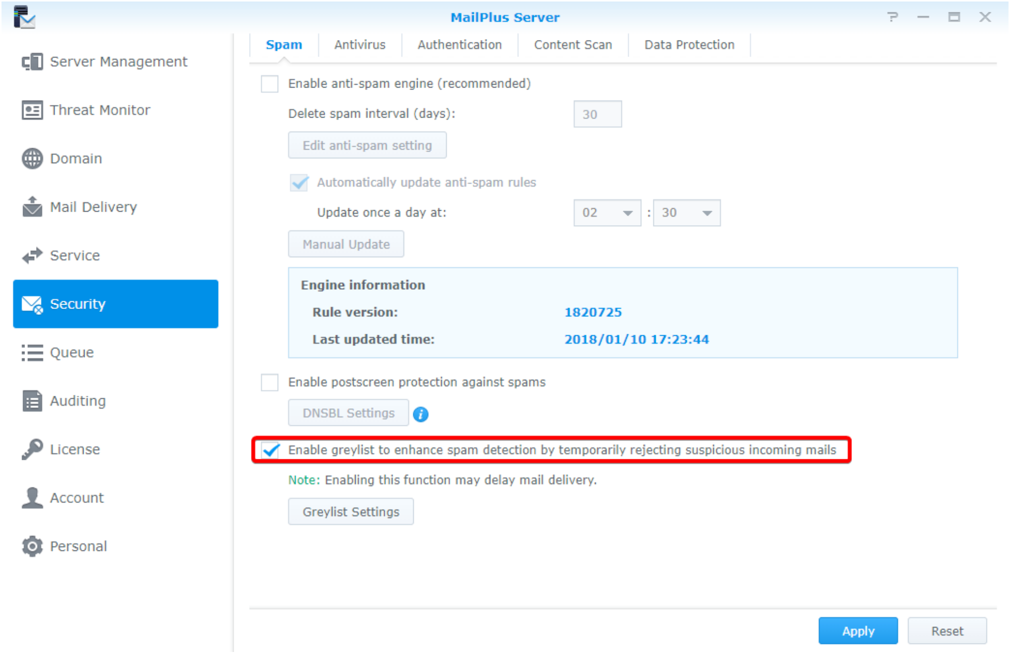
When enabling greylist, the greylist will run default actions for all the sources, these actions include the following:

- **Whitelist**: Passes the test directly, and temporary error messages will not be sent back.
- **Greylist**: When records of the inbound messages cannot be found, the greylist mechanism allows temporary error messages to be sent back to the sender
- **Blacklist**: Rejects the messages directly.

Note: The greylist mechanism may delay the delivery of regular messages. When enabling this feature, please make sure you fully understand the effects of the greylist mechanism.

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.



□ Enable anti-spam engine (recommended)

Delete spam interval (days): 30

☑ Automatically update anti-spam rules

Update once a day at: 02 : 30

Engine information

Rule version: 1820725

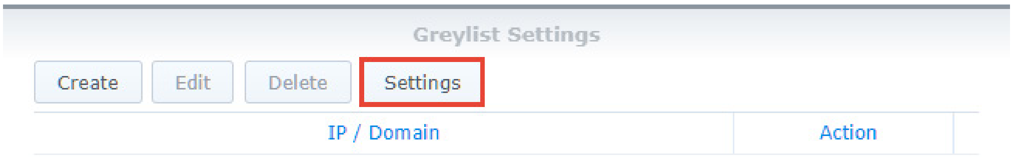
Last updated time: 2018/01/10 17:23:44

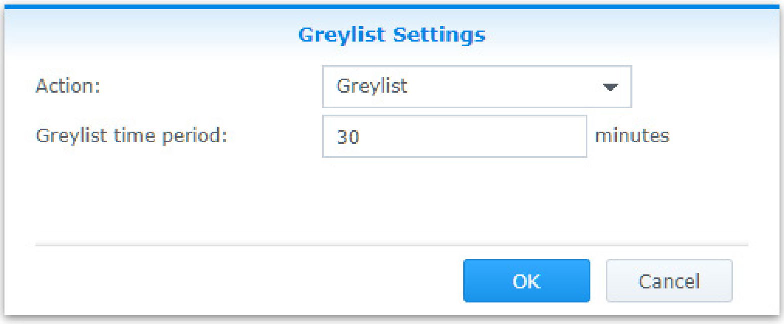
□ Enable postscreen protection against spams

☑ Enable greylist to enhance spam detection by temporarily rejecting suspicious incoming mails

Note: Enabling this function may delay mail delivery.

2 Click the **Greylist Settings** button to set up default actions, or set up actions for specific IP addresses or domain names.



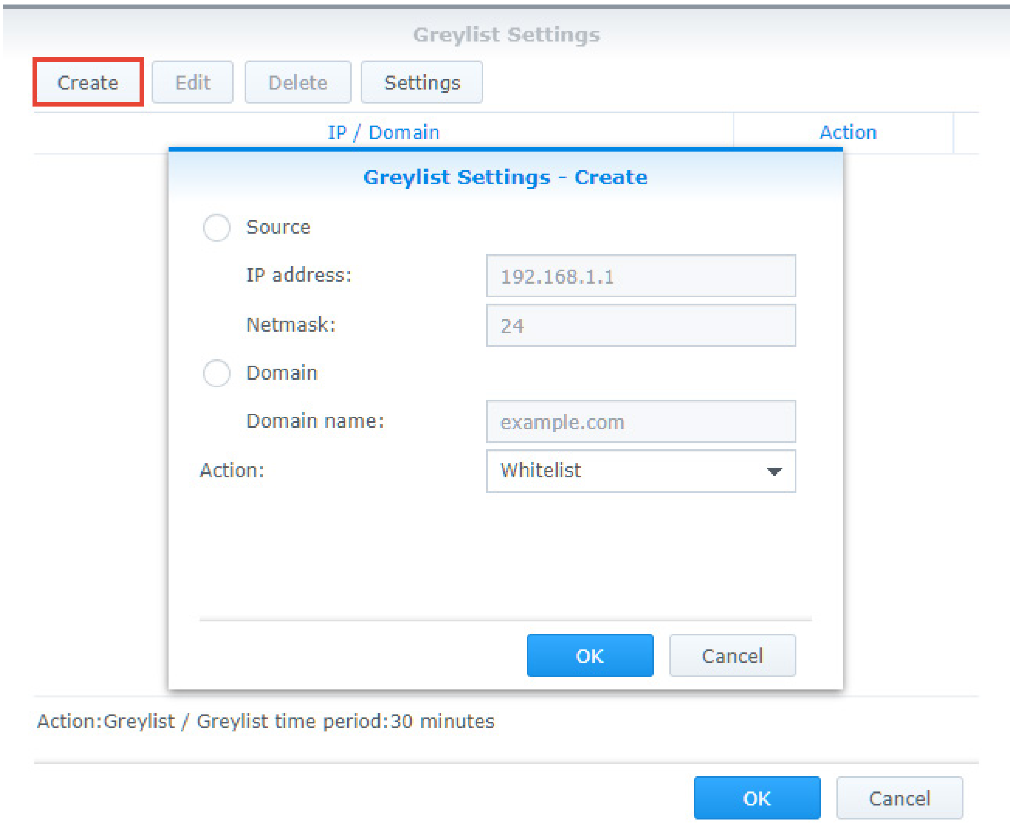


Action: Greylist

Greylist time period: 30 minutes

3 In the **Greylist Settings** window, click the **Settings** button to set up a default action for all sources.

4 From the **Action** drop-down menu, select a default action. In the **Greylist time period** field enter a greylist delay time, this will be applied to all greylist actions.



○ Source

IP address: 192.168.1.1

Netmask: 24

○ Domain

Domain name: example.com

Action: Whitelist

Action:Greylist / Greylist time period:30 minutes

5 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.

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

Note: The domain source here is taken from searching the IP address via DNS, not from **MAIL FROM** of the message.

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

Antivirus scan

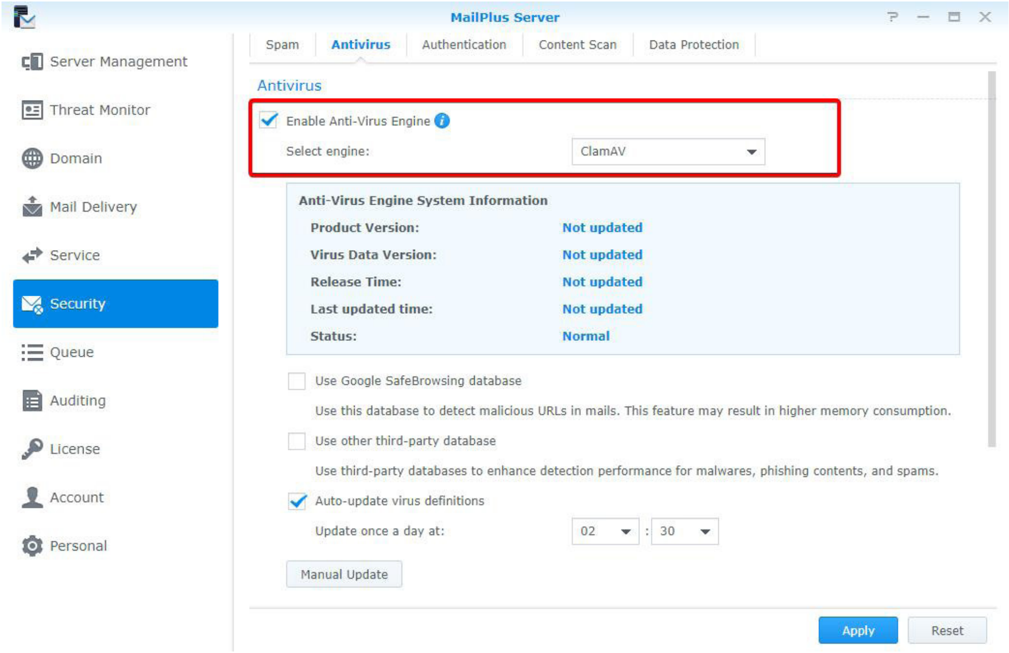
MailPlus Server provides ClamAV, a free anti-virus engine, and McAfee, a paid, subscription based anti-virus engine to protect against malware threats. You can also set up actions to take upon detecting viruses.

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

- **ClamAV**: ClamAV is the default antivirus system in MailPlus Server, it provides complete protection for your server free of cost.
- **McAfee**: MailPlus Server integrates with a paid DSM Package Center antivirus package. Subscribe to the **Antivirus by McAfee** package, and select **McAfee** as your antivirus engine for convenient management, antivirus scheduling, log, and more advanced settings.

Enable Anti-Virus Engine

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



Antivirus

☑ Enable Anti-Virus Engine

Select engine: ClamAV

Anti-Virus Engine System Information

Product Version:	Not updated
Virus Data Version:	Not updated
Release Time:	Not updated
Last updated time:	Not updated
Status:	Normal

☐ Use Google SafeBrowsing database

Use this database to detect malicious URLs in mails. This feature may result in higher memory consumption.

☐ Use other third-party database

Use third-party databases to enhance detection performance for malwares, phishing contents, and spams.

☑ Auto-update virus definitions

Update once a day at: 02 : 30

2 Select the following engines from the **Select engine** drop-down menu:

- **ClamAV**: ClamAV is a free antivirus engine provided 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 your antivirus engine, please refer to the following steps to configure settings:

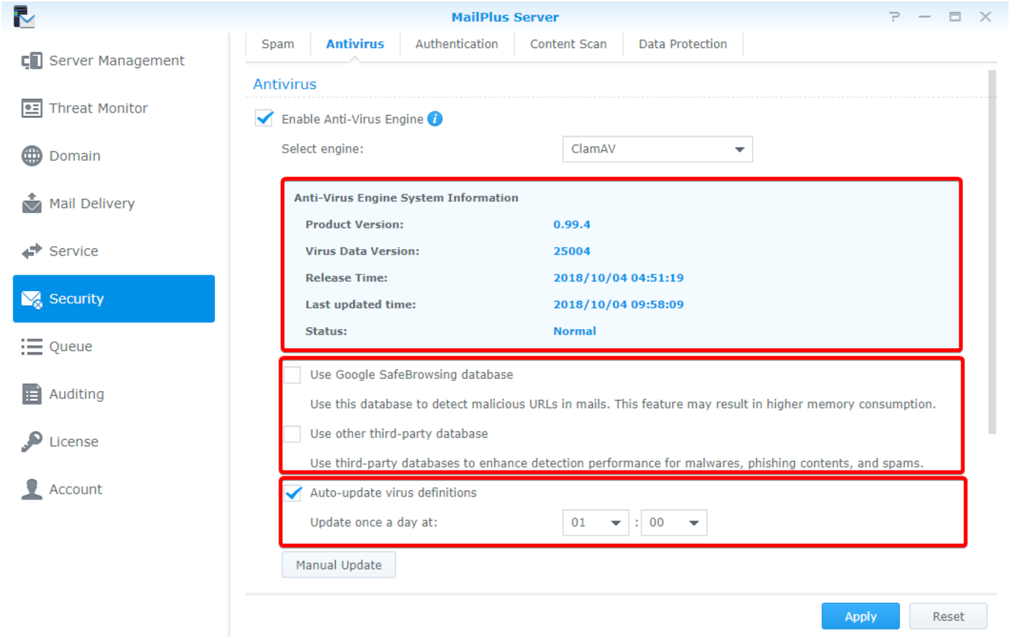
1 Under **Anti-Virus Engine System Information** you can view antivirus engine information. Please update your anti-virus engine regularly.

2 ClamAV uses external databases to enhance selected functions:

- **Use Google SafeBrowsing database**: Use the integrated Google SafeBrowsing database to detect if a message includes malicious links.
- **Use other third-party database**: Use 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 and enhance virus detection.
- **Manual Update**: Click the **Manual Update** button to immediately update virus definitions.



Antivirus

☑ Enable Anti-Virus Engine

Select engine: ClamAV

Anti-Virus Engine System Information

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

☐ Use Google SafeBrowsing database

Use this database to detect malicious URLs in mails. This feature may result in higher memory consumption.

☐ Use other third-party database

Use third-party databases to enhance detection performance for malwares, phishing contents, and spams.

☑ Auto-update virus definitions

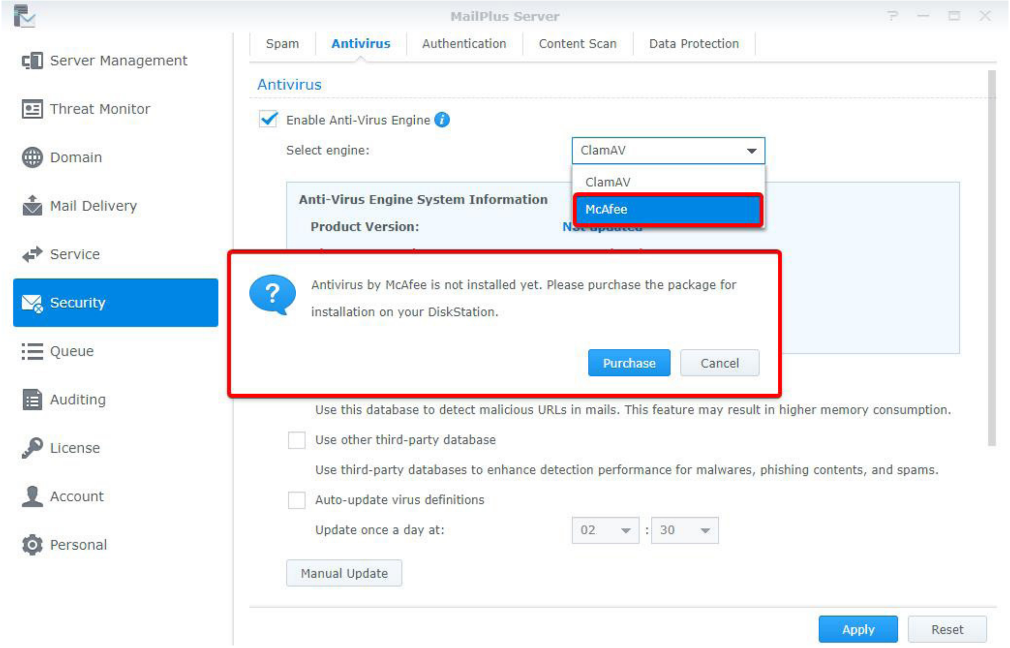
Update once a day at: 01 : 00

4 Click **Apply** to save settings.

McAfee

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

1 If your McAfee is not installed 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**.



Antivirus

☑ Enable Anti-Virus Engine

Select engine: ClamAV

Anti-Virus Engine System Information

Product Version: Not updated

Antivirus by McAfee is not installed yet. Please purchase the package for installation on your DiskStation.

Use this database to detect malicious URLs in mails. This feature may result in higher memory consumption.

☐ Use other third-party database

Use third-party databases to enhance detection performance for malwares, phishing contents, and spams.

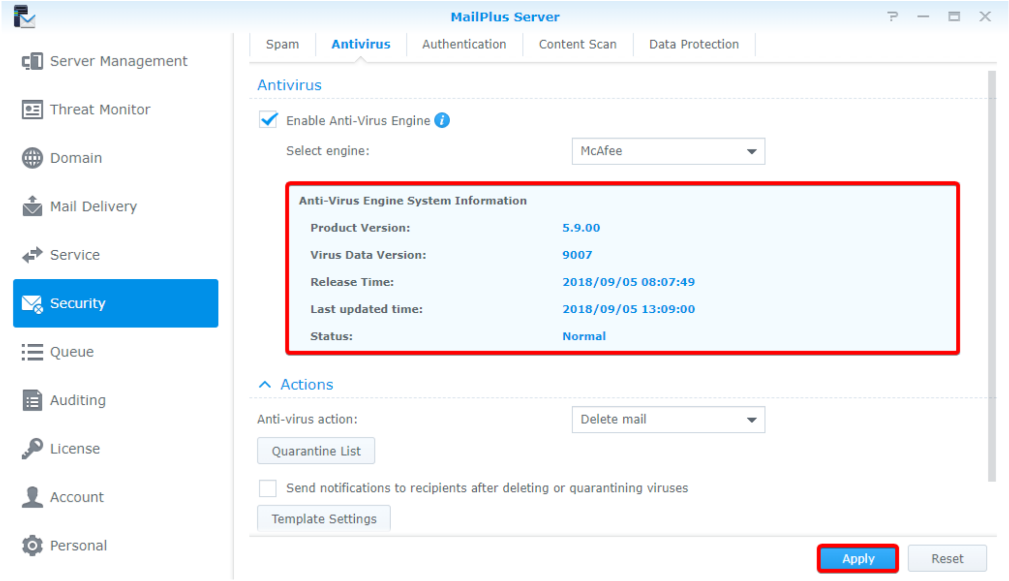
☐ Auto-update virus definitions

Update once a day at: 02 : 30

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

Note:

1. McAfee settings must be configured in the **Antivirus by McAfee** package.
2. If the status is abnormal (possibly due to license issues or corrupt virus definition files, et cetera), then **Antivirus by McAfee** will not scan the 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.



Antivirus

☑ Enable Anti-Virus Engine

Select engine: McAfee

Anti-Virus Engine System Information

Product Version:	5.9.00
Virus Data Version:	9007
Release Time:	2018/09/05 08:07:49
Last updated time:	2018/09/05 13:09:00
Status:	Normal

Actions

Anti-virus action: Delete mail

□ Send notifications to recipients after deleting or quarantining viruses

3 Click Apply to save settings.

Anti-Virus action settings

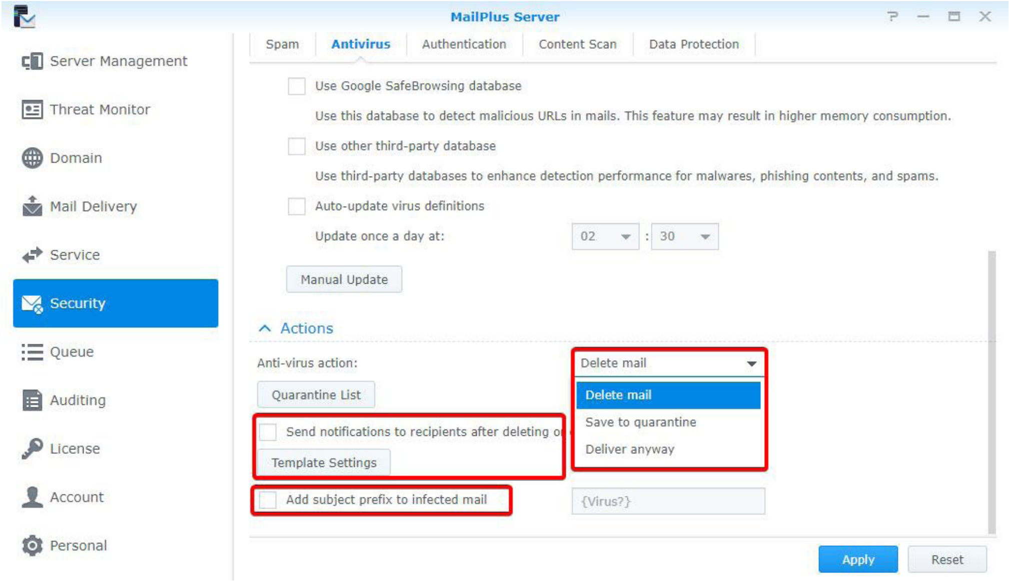
1 Go to Security > Antivirus.

2 Select an action to take when detecting email messages including viruses from the Anti-virus action drop-down menu:

- Delete mail: Delete the email message.
- Save to quarantine: Block the email message and save to the quarantine section. You can adjust settings for the quarantined messages.
- Deliver anyway: Deliver the email message.

3 If you have selected Delete mail or Save to quarantine, you can choose to tick the Send notifications to recipients after deleting or quarantining viruses checkbox to further understand the situation. After running the above action, a notification message will be sent to the recipient of the original email message. You can click on the Template Settings button below to adjust the notification message template. Different messages can be set up in Template Settings according to quarantined or deleted messages.

4 If you select Deliver anyway, you can tick the Add subject prefix to infected mail checkbox to label suspicious email messages.



□ Use Google SafeBrowsing database

Use this database to detect malicious URLs in mails. This feature may result in higher memory consumption.

□ Use other third-party database

Use third-party databases to enhance detection performance for malwares, phishing contents, and spams.

□ Auto-update virus definitions

Update once a day at: 02 : 30

Actions

Anti-virus action: Delete mail

□ Send notifications to recipients after deleting o

□ Add subject prefix to infected mail {Virus?}

5 Click Apply to save settings.

Quarantine List

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

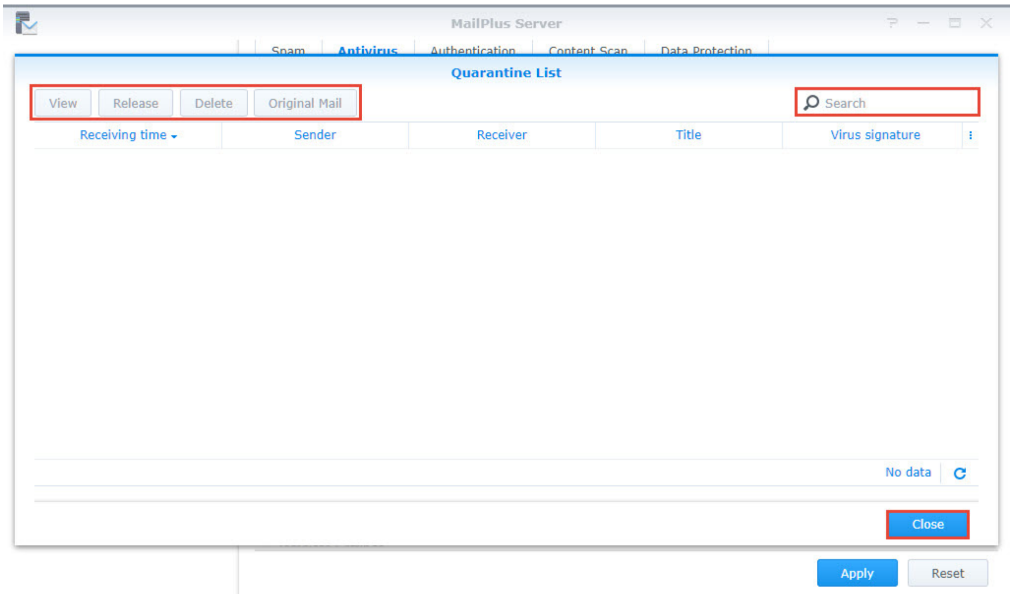
1 Go to **Security** > **Antivirus**, and click the **Quarantine List** button.

2 You can search for senders, recipients, title, virus definitions in the search field at the upper-right corner of the **Quarantine List** window.

3 Select a quarantined message, and click the **View** or **Original Mail** button to confirm the content.

4 Choose the following actions based on the message content:

- **Release**: Release the message to the recipient.
- **Delete**: Delete message.



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

Authentication

The purpose of authentication is to verify the sender's identity in order to prevent receiving fraudulent messages and protect against identity theft.

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

SPF

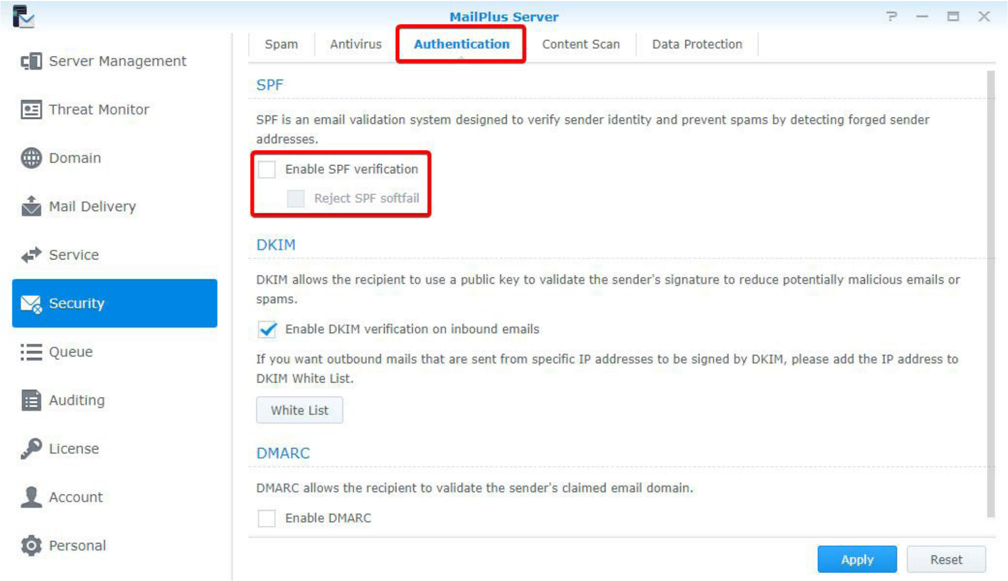
Enabling SPF verification allows the system to check the SPF records of the sender’s domain in DNS and prevent email fraud. When SPF verification fails, the result will be identified as fail or softfail. Please refer to the following steps to adjust SPF verification settings.

> ***Note:*** If your MailPlus Server is set up to receive messages forwarded from other mail servers, then the SPF mechanism may block relayed messages since the relay server location is not included in the 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 choose to tick the **Reject SPF softfail** checkbox to reject **softfail** messages, otherwise all messages with the verification result as **softfail** will be received.



SPF

SPF is an email validation system designed to verify sender identity and prevent spams by detecting forged sender addresses.

☐ Enable SPF verification

☐ Reject SPF softfail

DKIM

DKIM allows the recipient to use a public key to validate the sender's signature to reduce potentially malicious emails or spams.

☑ Enable DKIM verification on inbound emails

If you want outbound mails that are sent from specific IP addresses to be signed by DKIM, please add the IP address to DKIM White List.

White List

DMARC

DMARC allows the recipient to validate the sender's claimed email domain.

☐ Enable DMARC

3 Click **Apply** to save settings.

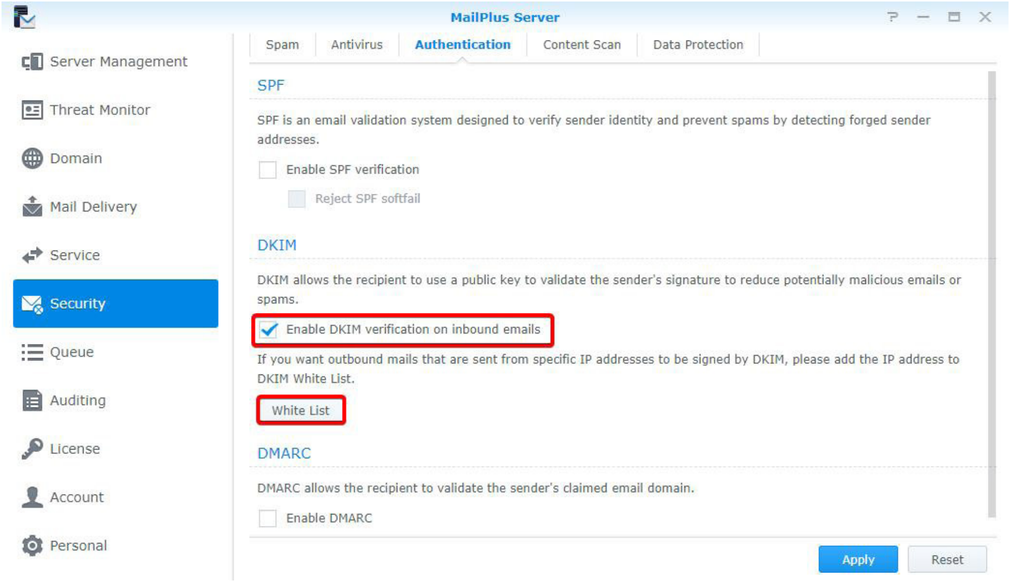
DKIM

You can enable DKIM verification to prevent messages from being modified and 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 the sender’s identity for inbound messages and reduce messages from unknown sources.

3 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 the host within the range connects to MailPlus Server to send outbound messages, the system will attach DKIM signatures to the messages.



SPF

SPF is an email validation system designed to verify sender identity and prevent spams by detecting forged sender addresses.

□ Enable SPF verification

□ Reject SPF softfail

DKIM

DKIM allows the recipient to use a public key to validate the sender's signature to reduce potentially malicious emails or spams.

☑ Enable DKIM verification on inbound emails

If you want outbound mails that are sent from specific IP addresses to be signed by DKIM, please add the IP address to DKIM White List.

White List

DMARC

DMARC allows the recipient to validate the sender's claimed email domain.

□ Enable DMARC

4 Click Apply to save settings.

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. Please refer to the following steps to enable DMARC verification:

1 Go to Security > Authentication.

2 Tick the Enable DMARC checkbox to enable DMARC.

Content protection

The content protection feature filters suspicious messages based on your settings.

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

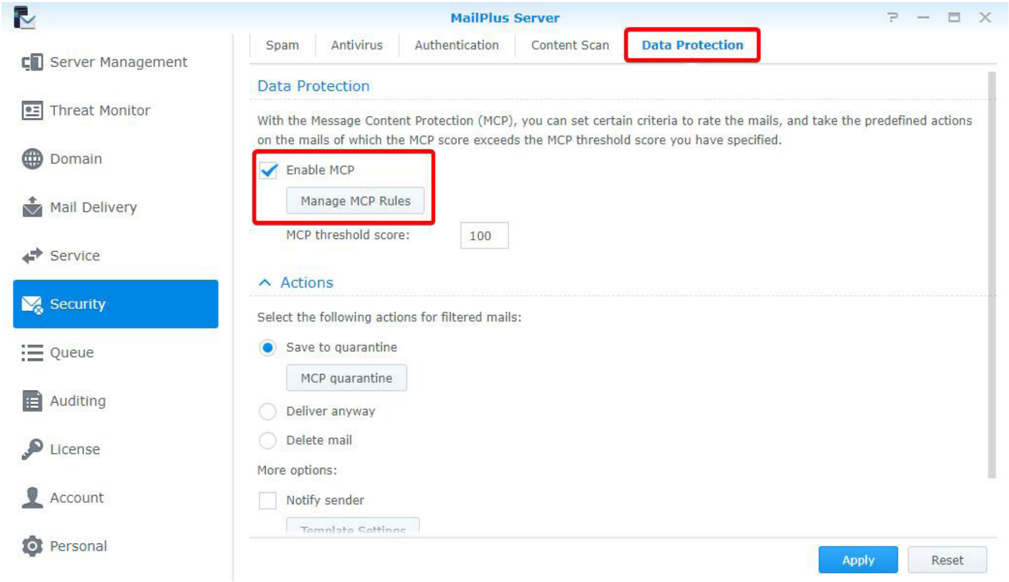
MCP rules

Set up MCP (Message Content Protection) rules and specify a MCP threshold score. When a mail matches the rule's criteria, the rule score will be summed to the total MCP score, and if the total score exceeds the MCP threshold score, the system will filter or block the mail. 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.



Data Protection

With the Message Content Protection (MCP), you can set certain criteria to rate the mails, and take the predefined actions on the mails of which the MCP score exceeds the MCP threshold score you have specified.

☑ Enable MCP

Manage MCP Rules

MCP threshold score: 100

Actions

Select the following actions for filtered mails:

● Save to quarantine

MCP quarantine

○ Deliver anyway

○ Delete mail

More options:

□ Notify sender

Template Settings

4 In the **Manage MCP Rules** window, click the **Create** button.

5 The **Add MCP Rules** window includes the following items:

- **Name**: Enter a name to identify the rule.
- **Target**: Choose a section of the email from the **Target** drop-down menu as a target to be matched:

Section	Description
Title	View the message content.
Contents (including Subject)	Email message content and subject.
Sender	The sender of the email message.
Recipient	The recipient of the email message.
Custom header	The specific header of the original email message.

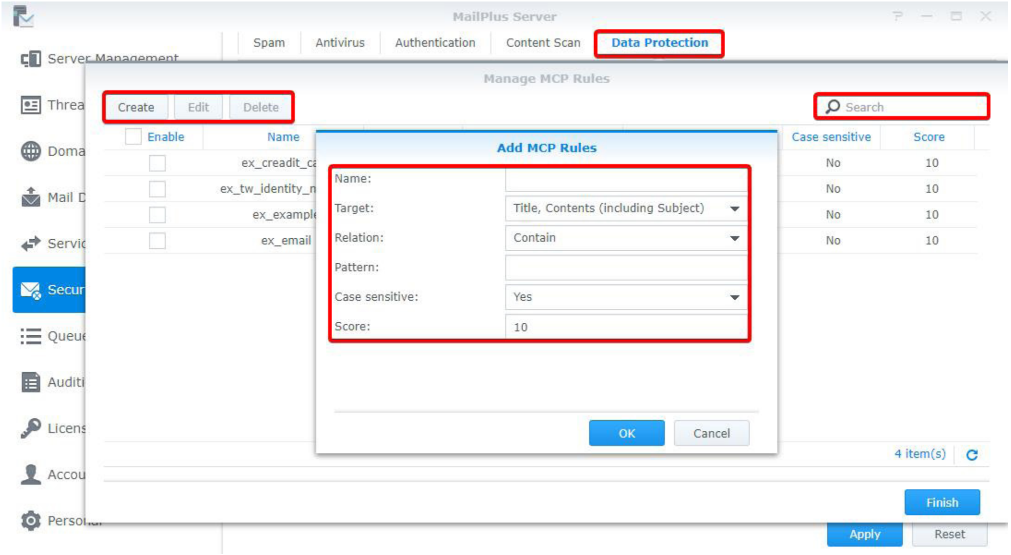
- **Custom header**: When selecting **Custom header** from the **Target** drop-down menu, the **Custom header** field will appear. Enter a specific header here.
- **Relation**: Choose a matching criteria from the **Relation** drop-down menu:

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

- **Pattern**: Matching content for the rule.
- **Case sensitive**: Choose **Yes** or **No** to determine if the matching content is case sensitive.
- **Score**: The number of points to be generated when matching the criteria of this rule.

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

7 In the **Manage MCP Rules** window, you can select a rule to **Enable**, **Edit**, or **Delete**. You can also search for rules in the search field at the upper-right corner.



Enable	Name	Case sensitive	Score
□	ex_creadit_ca	No	10
□	ex_tw_identity_n	No	10
□	ex_exampl	No	10
□	ex_email	No	10

Name:	
Target:	Title, Contents (including Subject)
Relation:	Contain
Pattern:	
Case sensitive:	Yes
Score:	10

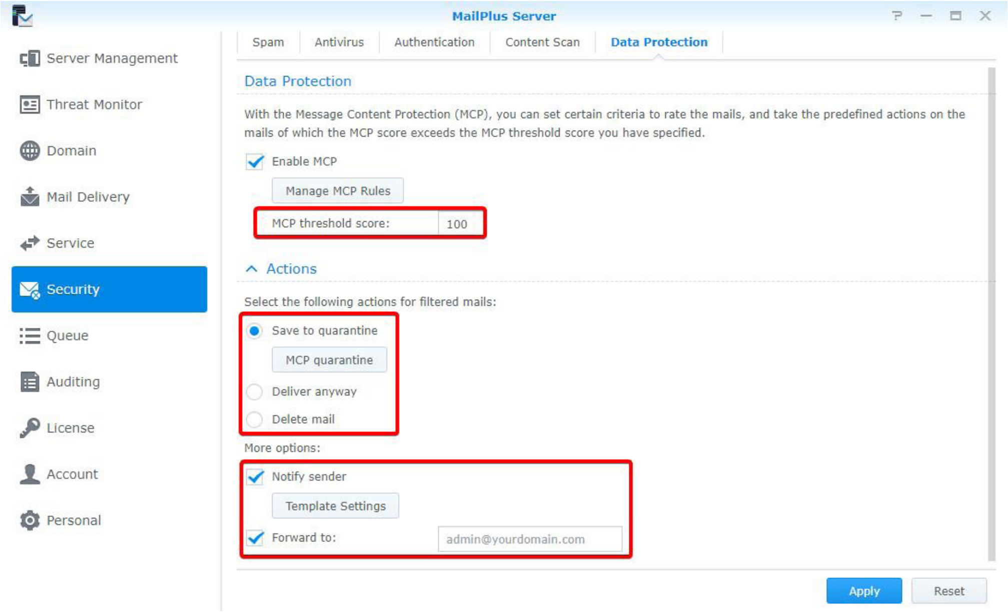
8 Click **Finish** to complete the settings.

Actions

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

1. Go to **Security** > **Data Protection**, and enter an MCP threshold score 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**: Block the email message and save to the quarantine section. You can click the **MCP quarantine** button to view the contents of the quarantine messages. Please refer to **Quarantine List** for more information on managing quarantined messages.
   - **Deliver anyway**: Deliver the email message.
   - **Delete mail**: Delete the email message.
   - **More options**: In addition, when a message exceeds the threshold score, you can choose to notify specific users.

Function	Description
Notify sender	Send a notification message to notify sender that the message has been blocked. You can click the **Template Settings** button to set up the notification content.
Forward to	Forward the original message to a specific mailbox.


MailPlus Server

Server Management
Threat Monitor
Domain
Mail Delivery
Service
Security
Queue
Auditing
License
Account
Personal

Spam | Antivirus | Authentication | Content Scan | Data Protection

Data Protection

With the Message Content Protection (MCP), you can set certain criteria to rate the mails, and take the predefined actions on the mails of which the MCP score exceeds the MCP threshold score you have specified.

☑ Enable MCP

Manage MCP Rules

MCP threshold score: 100

Actions

Select the following actions for filtered mails:

● Save to quarantine

MCP quarantine

○ Deliver anyway

○ Delete mail

More options:

☑ Notify sender

Template Settings

☑ Forward to: admin@yourdomain.com

Apply | Reset

3 Click Apply to save settings.

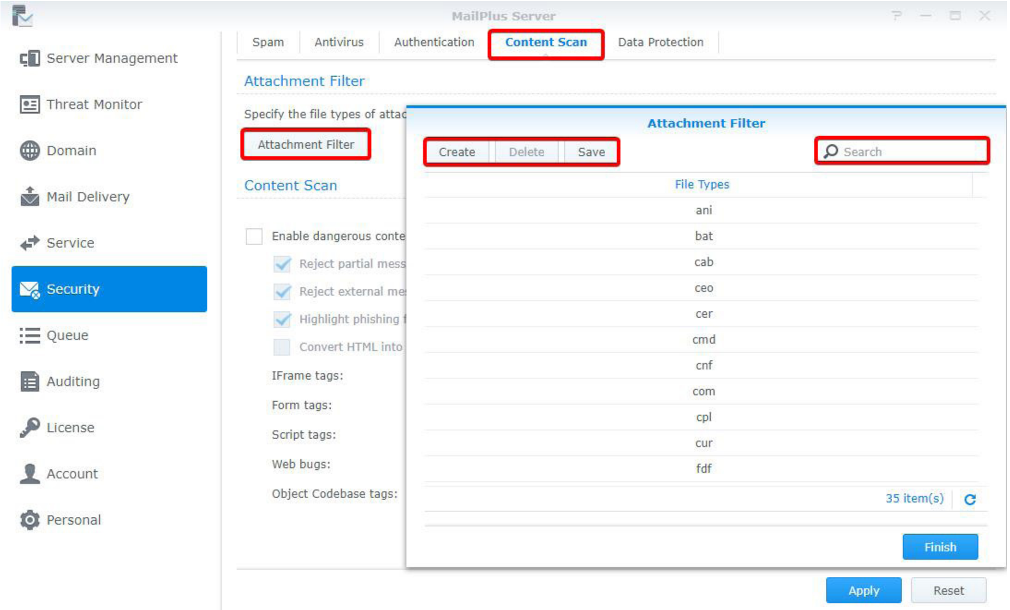
Attachment Filter

This Attachment Filter feature blocks messages based on the file types of the attachment contents. Please refer to the following steps to set up Attachment Filter:

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 file types at the upper-right corner.


MailPlus Server

Server Management
Threat Monitor
Domain
Mail Delivery
Service
Security
Queue
Auditing
License
Account
Personal

Spam | Antivirus | Authentication | Content Scan | Data Protection

Attachment Filter

Specify the file types of attac

Attachment Filter

Content Scan

□ Enable dangerous conte

☑ Reject partial mess

☑ Reject external me

☑ Highlight phishing

□ Convert HTML into

IFrame tags:

Form tags:

Script tags:

Web bugs:

Object Codebase tags:

Attachment Filter

Create | Delete | Save | Search

File Types
ani
bat
cab
ceo
cer
cmd
cnf
com
cpl
cur
fdf

35 item(s)

Finish

Apply | Reset

4 Click Save.

5 Click Finish to complete settings.

Content Scan

The Content Scan feature blocks messages or modifies message content based on the suspicious contents of the messages. Please refer to the following steps to adjust Content Scan settings:

Note: Modified content may not meet expectations. Please make sure you enable the 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**: Reject email messages that are split across multiple incomplete messages (specifically email messages with Content-Type value of header message/partial).
   - **Reject external message bodies**: Reject email messages that point to external resources. (Specifically email messages with Content-Type value of message/external-body).
   - **Highlight phishing fraud**: When the system detects phishing links in the email messages, the links in the messages will be highlighted to alert recipients and prevent them from clicking unwanted links.
   - **Convert HTML into plain text**: Messages with HTML formats will be converted to plain text. You can set up different tags to perform different actions.

Function	Description
Allow	Deliver the message.
Reject	Reject the message.
Make tags ineffective	Deliver the message after making the tag ineffective.

Note: Please specify the settings for each tag.

Chapter

10

Monitor Settings

Monitor server status

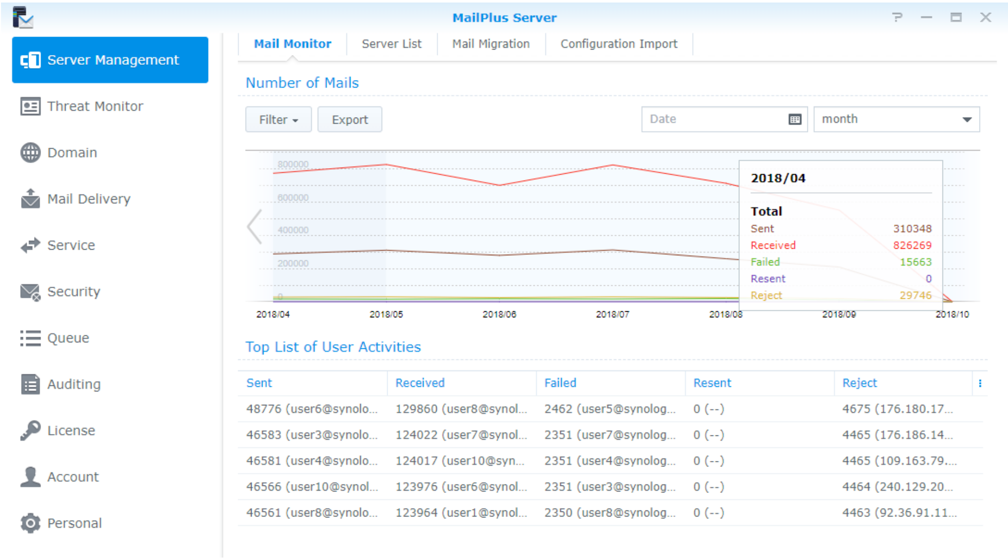
Quickly oversee server operation status with a graphical interface:

- **Mail Traffic Monitor**: Monitor the server’s mail traffic by specific time intervals.
- **Threat Monitor**: You can view the amount of email threats have been blocked by each security setting of your server. You can quickly identify all the threat sources and conveniently adjust security settings accordingly.
- **Server List**: View a list of server clusters and their operation status.

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 Activity** section displays 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 **High-availability cluster**, please view the log from the primary server.



2018/04

Total

Sent	310348
Received	826269
Failed	15663
Resent	0
Reject	29746

Sent	Received	Failed	Resent	Reject
48776 (user6@synolo...	129860 (user8@synol...	2462 (user5@synolog...	0 (--)	4675 (176.180.17...
46583 (user3@synolo...	124022 (user7@synol...	2351 (user7@synolog...	0 (--)	4465 (176.186.14...
46581 (user4@synolo...	124017 (user10@syn...	2351 (user4@synolog...	0 (--)	4465 (109.163.79....
46566 (user10@synol...	123976 (user6@synol...	2351 (user3@synolog...	0 (--)	4464 (240.129.20...
46561 (user8@synolo...	123964 (user1@synol...	2350 (user8@synolog...	0 (--)	4463 (92.36.91.11...

Monitor traffic by different time interval lengths

Monitor email traffic on 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 point of time. Please refer to the steps below to adjust 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 at 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 interval:

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

> ***Note:*** MailPlus Sever reserves different mail number data for different lengths of time intervals. You can only switch to the intervals with available data.

Fix display of detailed data from a specific time

Data displayed in the detailed information panel on the chart changes as you hover over different time points on the chart. To view detailed information of a selected time point, 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.

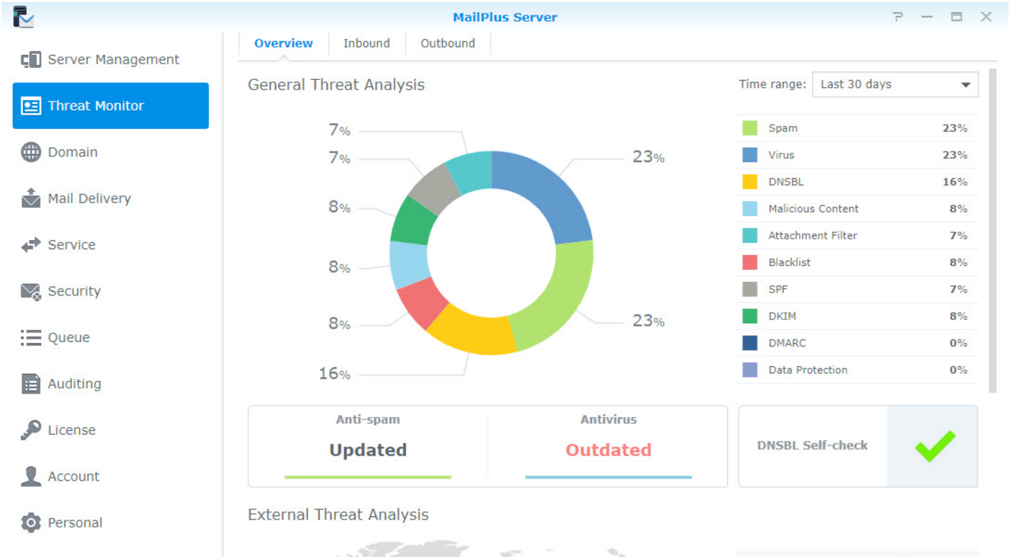
Export data from a specific time interval

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 as an html file from the specified time interval.

Threat Monitor

Detailed information on email threats and their sources are displayed in **Threat Monitor**. You can adjust settings according to the data to achieve email security.

> ***Note:*** If you have already set up **High-availability cluster**, please view the log from the primary server.



Time range: Last 30 days

Spam	23%
Virus	23%
DNSBL	16%
Malicious Content	8%
Attachment Filter	7%
Blacklist	8%
SPF	7%
DKIM	8%
DMARC	0%
Data Protection	0%

Anti-spam: Updated

Antivirus: Outdated

View General Threat Analysis

General Threat Analysis displays threat data and statistics for outbound and inbound email messages 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 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 the count statistics, hover the mouse to a specific type.
   - **Threat doughnut chart**: See the percentage statistics of each threat type. Select or deselect threat types in 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 in the DNSBL blacklist. Click to see more details.

View External Threat Analysis

The external threat analysis displays sources of blocked inbound email 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 email comes from the area. To see the count statistics, hover the mouse to the circle.
   - **Threat Source**: This list shows the top six sources of blocked email with their corresponding counts.

View Blocked Inbound and Outbound Mail

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

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

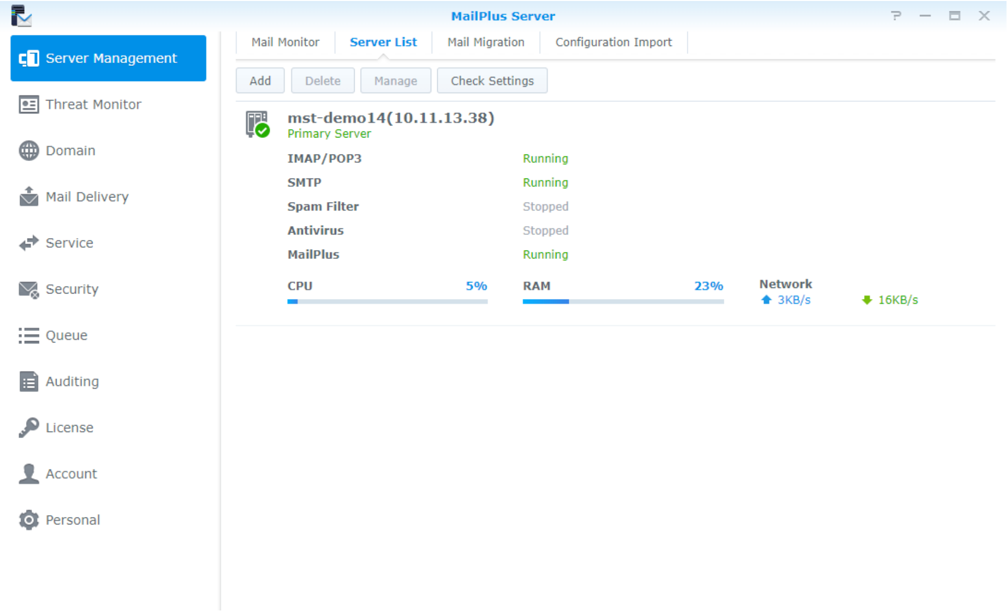
> ***Note:***
> 1. To change threat types in display, select or deselect the legends under the chart.
> 2. To see count statistics of each threat type, hover the mouse to the chart.

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

Server List

Get a quick overview of the server information of MailPlus Server in the **Server List** tab on **Server Management**, including information on CPU, RAM, network usage, et cetera. 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 the MailPlus package.
- **Getting ready**: This status means you have just enabled or disabled this function, and it is getting ready to switch statuses.
- **Syncing mails**: When you are setting up or removing MailPlus Server high-availability clusters, the system will sync mails. This status means the system is currently syncing mails.



mst-demo14(10.11.13.38)
Primary Server

IMAP/POP3	Running
SMTP	Running
Spam Filter	Stopped
Antivirus	Stopped
MailPlus	Running

CPU 5% RAM 23% Network 3KB/s 16KB/s

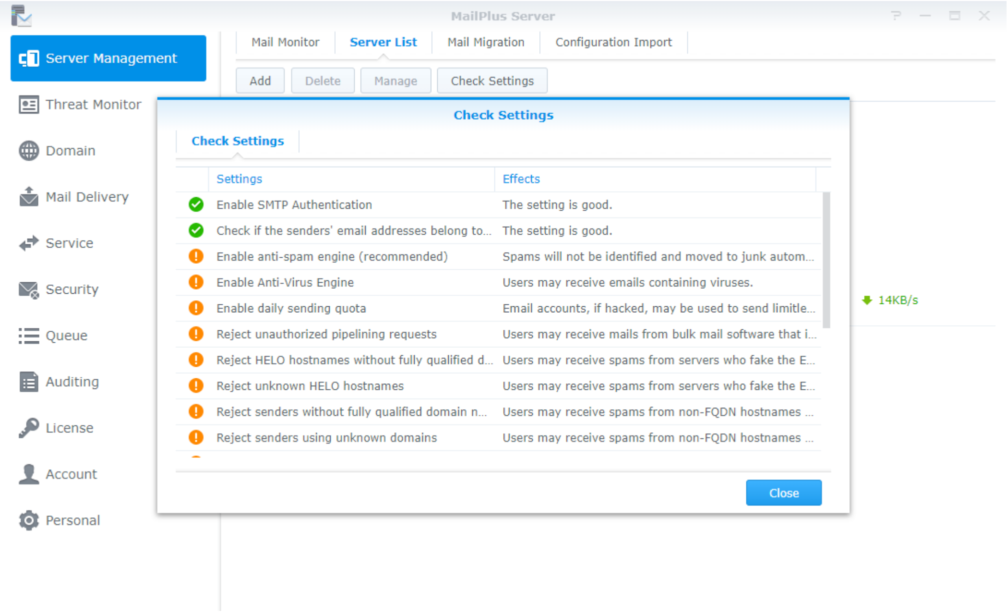
Note: If Antivirus or MCP are enabled, Spam Filter will also be enabled even if Anti-Spam was not enabled, however it spam scanning will not be conducted.

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.



	Settings	Effects
✓	Enable SMTP Authentication	The setting is good.
✓	Check if the senders' email addresses belong to...	The setting is good.
!	Enable anti-spam engine (recommended)	Spams will not be identified and moved to junk autom...
!	Enable Anti-Virus Engine	Users may receive emails containing viruses.
!	Enable daily sending quota	Email accounts, if hacked, may be used to send limite...
!	Reject unauthorized pipelining requests	Users may receive mails from bulk mail software that i...
!	Reject HELO hostnames without fully qualified d...	Users may receive spams from servers who fake the E...
!	Reject unknown HELO hostnames	Users may receive spams from servers who fake the E...
!	Reject senders without fully qualified domain n...	Users may receive spams from non-FQDN hostnames ...
!	Reject senders using unknown domains	Users may receive spams from non-FQDN hostnames ...

Monitor Mail Queue

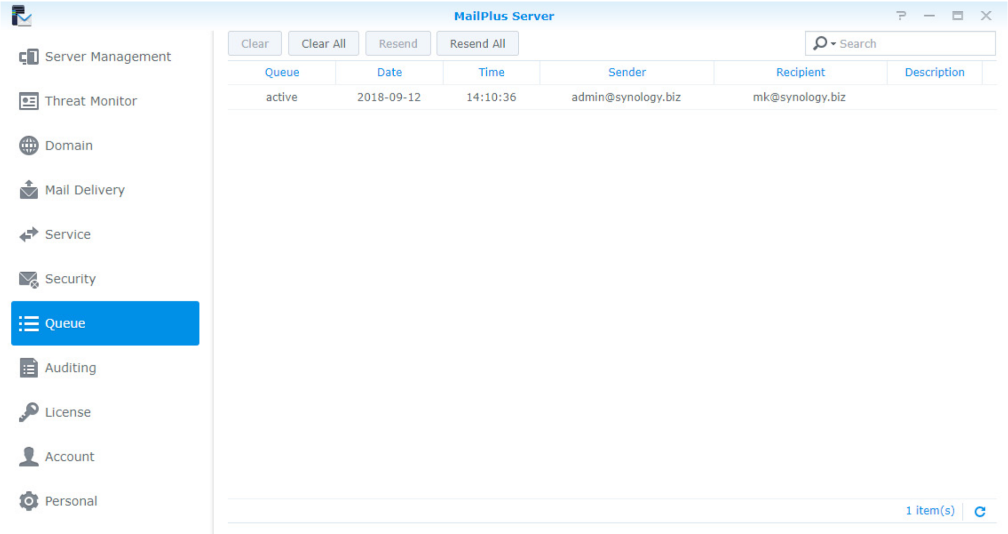
View pending emails and determine what actions to take.

Monitor messages in mail queue

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

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

- The date and time when the message entered the queue.
- The message sender and recipient.
- Why the message is waiting in the mail queue. (The **Description** column shows why the messages fail to deliver.)



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

Mail queue status are categorized into the three types shown as follows:

- **Hold**: The message is to be processed.
- **Active**: The message is now being processed.
- **Deferred**: The system fails to deliver the message and will resend it later.

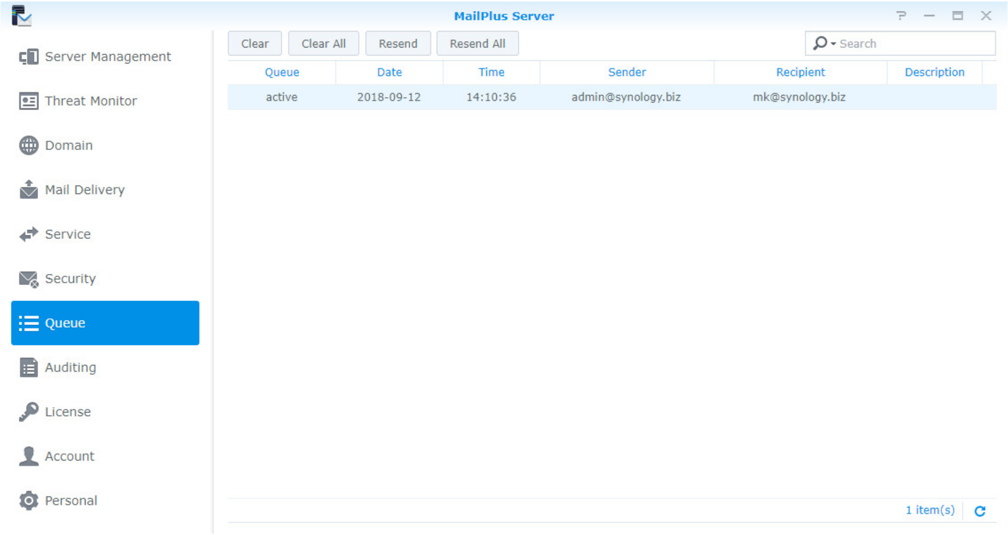
Note: Deferred messages will be returned to the sender if all redelivery attempts fail during the following 5 days.

Manage messages in mail queue

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

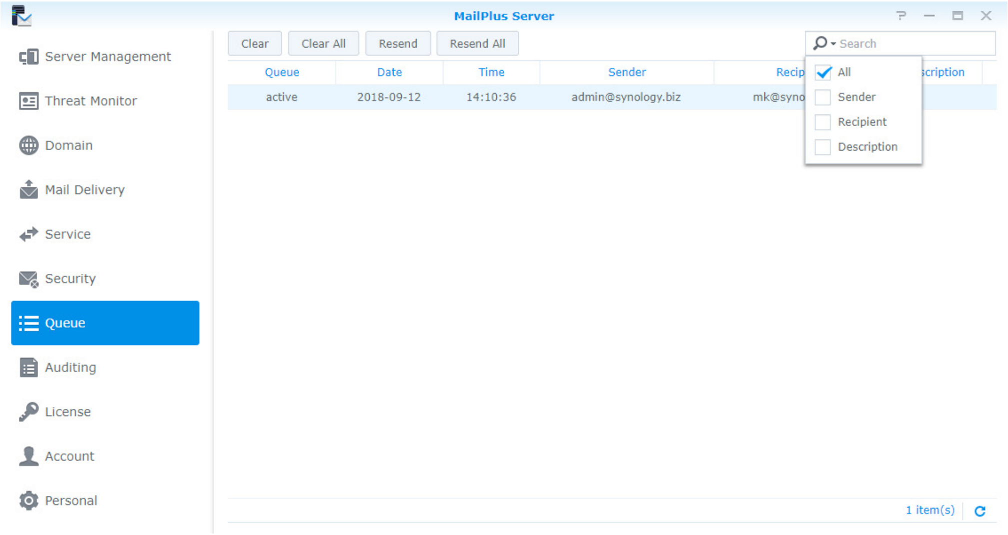
1 Go to **Queue**, and do the following:

- To redeliver messages, select the message in mail queue, and click the **Resend** button. The status of the message will switch from **Hold** to **Active**.
- To remove messages, select the messages in 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.



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

2 You can also search for messages in the search field at the upper-right corner of the page to find out about the statuses of the messages.



Queue	Date	Time	Sender	Recip	cription
active	2018-09-12	14:10:36	admin@synology.biz	mk@syno	

☑ All
□ Sender
□ Recipient
□ Description

Monitor Mail Log

Mail log records all activities of the server. View the log content to understand root problems and find solutions accordingly. Log generates large files. Detailed monitoring settings can be configured in the **Auditing** page.

- **View Logs**: View, search, and analyze your logs. You can quickly find messages recorded in logs.
- **Archive and Manage Logs**: Flexible management ways that allow you to set up archive intervals, backup, rotation rules, and send logs to secondary servers, et cetera.
- **Log Report**: Regularly send logs through email messages, allowing you to quickly view log content.

View Mail Logs

Please refer to the following steps to view Mail Log:

1 Go to **Auditing** > **Log**.

2 From the drop-down menus at the top, select **Mail Log** and **Internal database**.

3 Mail Log displays the message ID, the date and time generated, sender, recipient, title, size, and status of each message. The statuses are categorized as follows:
   - **Received**: This status means a user on MailPlus Server has received a message. If a user on MailPlus Server has sent a message to another user on MailPlus Server, then the status on the log records will be shown as **Received**. If multiple users on MailPlus Server receive the same message, multiple log records will be generated, however if the message is sent to an alias email address on MailPlus Server, only one log record for the alias email address will be generated 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** statuses will be generated whether the **Keep mail copy in the Inbox** checkbox is ticked or not.
   - **Sent**: When sending messages to email addresses from other servers, multiple log records will be generated if the recipient includes multiple email address 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 have failed to deliver.

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

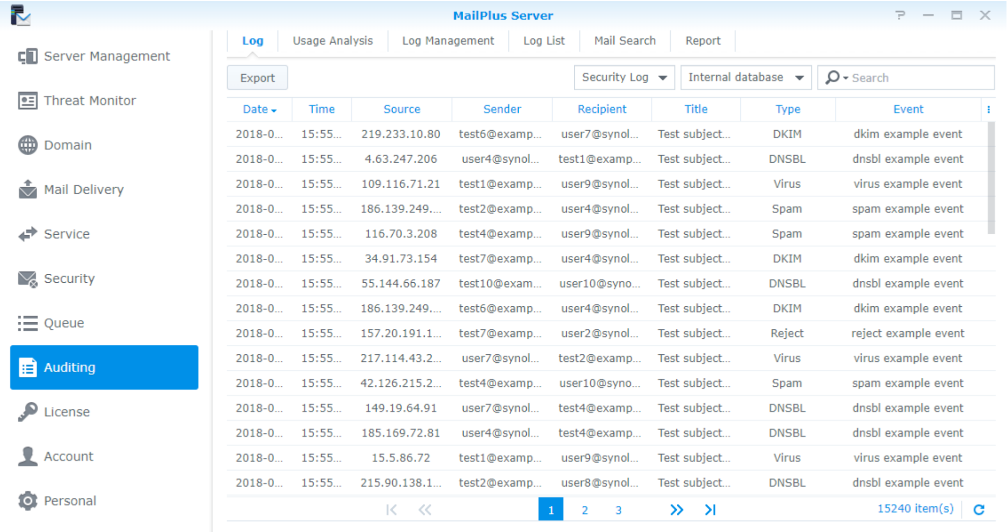
View Security Logs

Security log displays the time and date an event is generated, along with the source, sender, recipient, title, type, and event description of an event. Security log types are categorized as follows: Reject, Spam, Virus, DNSBL, Malicious Content, Attachment Filter, Blacklist, SPF, DKIM, DMARC, and Data Protection, all of which are related to the security setting features. The **Reject** type means that MailPlus Server has rejected the message after running full analysis. You can refer to the following steps to view Security Log:

Note: If you have set up **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**.



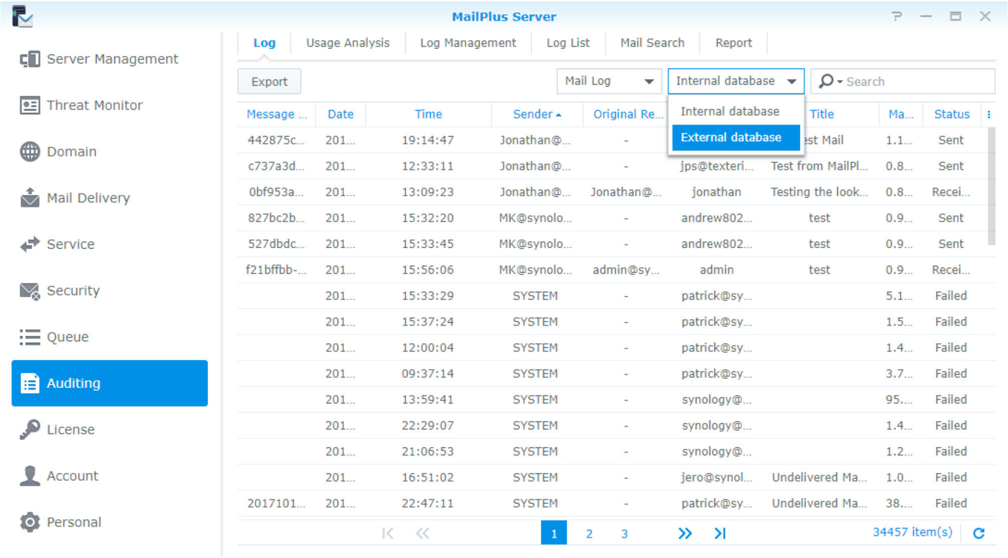
Date	Time	Source	Sender	Recipient	Title	Type	Event
2018-0...	15:55...	219.233.10.80	test6@examp...	user7@synol...	Test subject...	DKIM	dkim example event
2018-0...	15:55...	4.63.247.206	user4@synol...	test1@examp...	Test subject...	DNSBL	dnsbl example event
2018-0...	15:55...	109.116.71.21	test1@examp...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

View External database

If you have archived logs, generated a log database, or downloaded log files, you can view log content in the database by viewing External database. Please refer to the following steps to view external database:

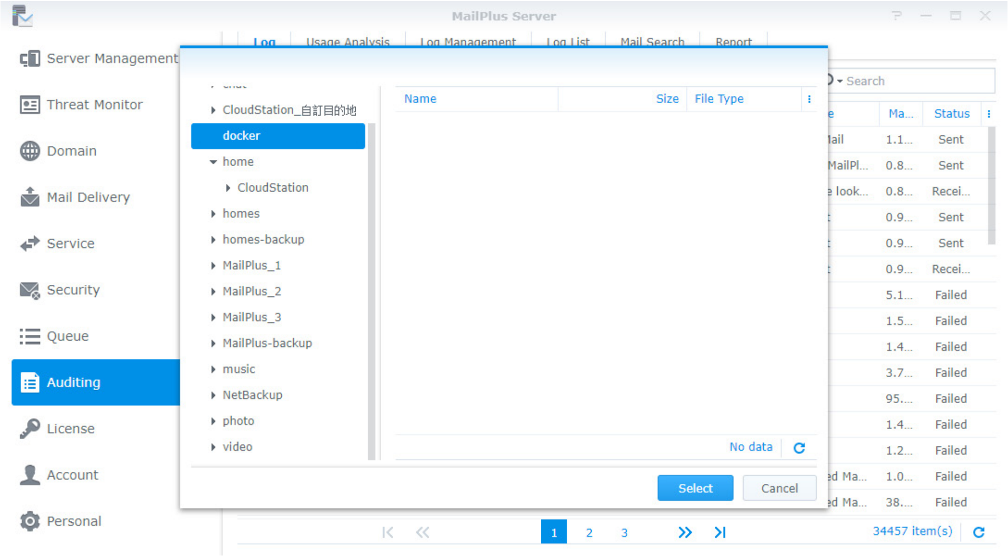
1 Go to **Auditing** > **Log**.

2 From the drop-down menus at the top, select **Mail Log** or **Security Log**, and select **External database**.



Message ...	Date	Time	Sender	Original Re...		Title	Ma...	Status
442875c...	201...	19:14:47	Jonathan@...	-		st 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
f21bffbb-...	201...	15:56:06	MK@synolo...	admin@sy...	admin	test	0.9...	Recei...
	201...	15:33:29	SYSTEM	-	patrick@sy...		5.1...	Failed
	201...	15:37:24	SYSTEM	-	patrick@sy...		1.5...	Failed
	201...	12:00:04	SYSTEM	-	patrick@sy...		1.4...	Failed
	201...	09:37:14	SYSTEM	-	patrick@sy...		3.7...	Failed
	201...	13:59:41	SYSTEM	-	synology@...		95....	Failed
	201...	22:29:07	SYSTEM	-	synology@...		1.4...	Failed
	201...	21:06:53	SYSTEM	-	synology@...		1.2...	Failed
	201...	16:51:02	SYSTEM	-	jero@synol...	Undelivered Ma...	1.0...	Failed
2017101...	201...	22:47:11	SYSTEM	-	patrick@sy...	Undelivered Ma...	38....	Failed

3 Find the location of your external database on Synology NAS.

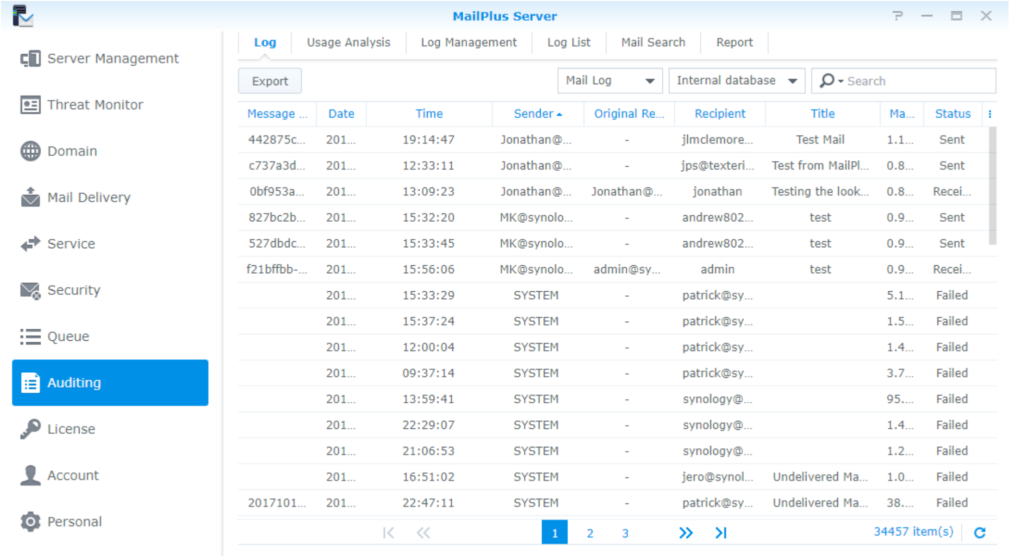


4 Click the **Select** button.

Search Logs

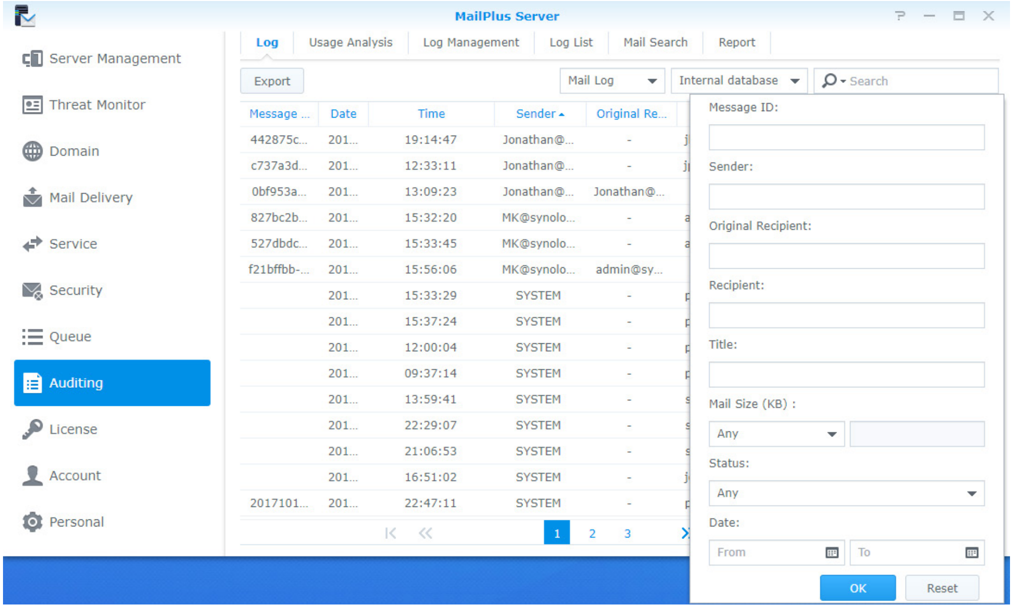
In **Auditing** > **Log**, you can search logs of interest according to criteria using simple search or advanced search methods.

- **Simple search**: You can enter keywords in the search field at the upper-right corner of the page. When viewing Mail Log, the keywords entered are used to search for content from the Message ID, Sender, Recipient, Title columns. When viewing Security Log, the keywords entered are used to search for content from the Source, Sender, Recipient, Title, and Event columns.



Message ...	Date	Time	Sender ▴	Original Re...	Recipient	Title	Ma...	Status
442875c...	201...	19:14:47	Jonathan@...	-	jlmclemore...	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
f21bffbb-...	201...	15:56:06	MK@synolo...	admin@sy...	admin	test	0.9...	Recei...
	201...	15:33:29	SYSTEM	-	patrick@sy...		5.1...	Failed
	201...	15:37:24	SYSTEM	-	patrick@sy...		1.5...	Failed
	201...	12:00:04	SYSTEM	-	patrick@sy...		1.4...	Failed
	201...	09:37:14	SYSTEM	-	patrick@sy...		3.7...	Failed
	201...	13:59:41	SYSTEM	-	synology@...		95....	Failed
	201...	22:29:07	SYSTEM	-	synology@...		1.4...	Failed
	201...	21:06:53	SYSTEM	-	synology@...		1.2...	Failed
	201...	16:51:02	SYSTEM	-	jero@synol...	Undelivered Ma...	1.0...	Failed
2017101...	201...	22:47:11	SYSTEM	-	patrick@sy...	Undelivered Ma...	38....	Failed

- **Advanced search**: You can click the magnifying glass icon in the search field at the upper-right corner of the page. Set up the search criteria for each item in order to conduct advanced search, click **OK** after you are done. In the **Status** drop-down menu, you can select **Within domain** to search for messages that are sent from a user on MailPlus Server to other internal users.



Message ...	Date	Time	Sender ▴	Original Re...
442875c...	201...	19:14:47	Jonathan@...	-
c737a3d...	201...	12:33:11	Jonathan@...	-
0bf953a...	201...	13:09:23	Jonathan@...	Jonathan@...
827bc2b...	201...	15:32:20	MK@synolo...	-
527dbdc...	201...	15:33:45	MK@synolo...	-
f21bffbb-...	201...	15:56:06	MK@synolo...	admin@sy...
	201...	15:33:29	SYSTEM	-
	201...	15:37:24	SYSTEM	-
	201...	12:00:04	SYSTEM	-
	201...	09:37:14	SYSTEM	-
	201...	13:59:41	SYSTEM	-
	201...	22:29:07	SYSTEM	-
	201...	21:06:53	SYSTEM	-
	201...	16:51:02	SYSTEM	-
2017101...	201...	22:47:11	SYSTEM	-

Message ID:

Sender:

Original Recipient:

Recipient:

Title:

Mail Size (KB) : Any

Status: Any

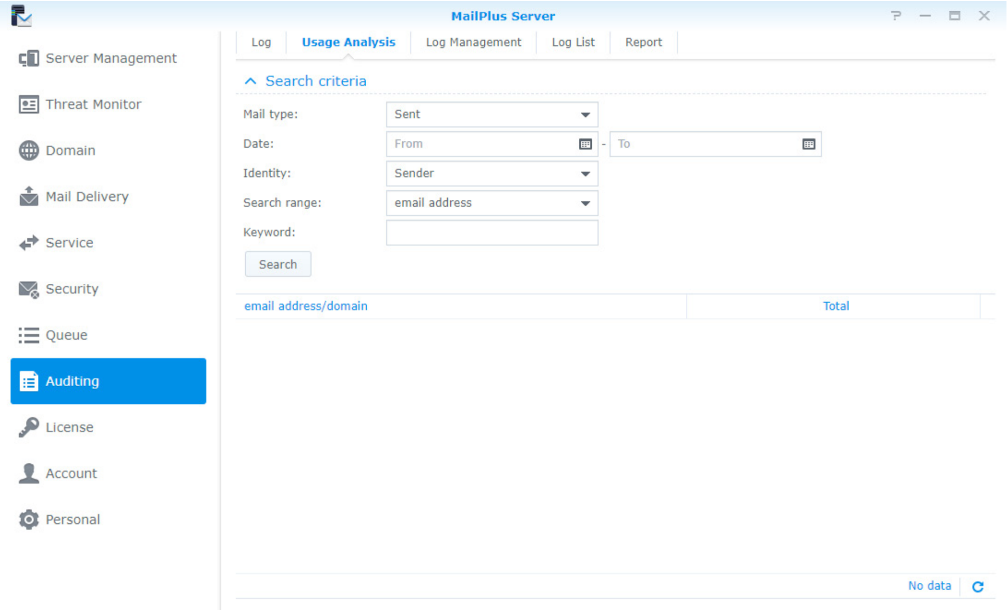
Date: From To

Export log content

You can export logs as html files in **Auditing** > **Log**. If you click the **Export** button after log search your search results will be exported. Please refer to **Search Logs**.

Usage Analysis

You can conduct usage analysis in **Auditing** > **Usage Analysis**, and analyze inbound and outbound messages sent by the email address or domain.



Mail type: Sent

Date: From - To

Identity: Sender

Search range: email address

Keyword:

Archive logs

You can configure log archiving settings. MailPlus Server will archive mail logs, security logs, and postfix logs according to the specified time. When you cannot access your shared folder, the archive feature will automatically disable. Please refer to the following steps to archive log:

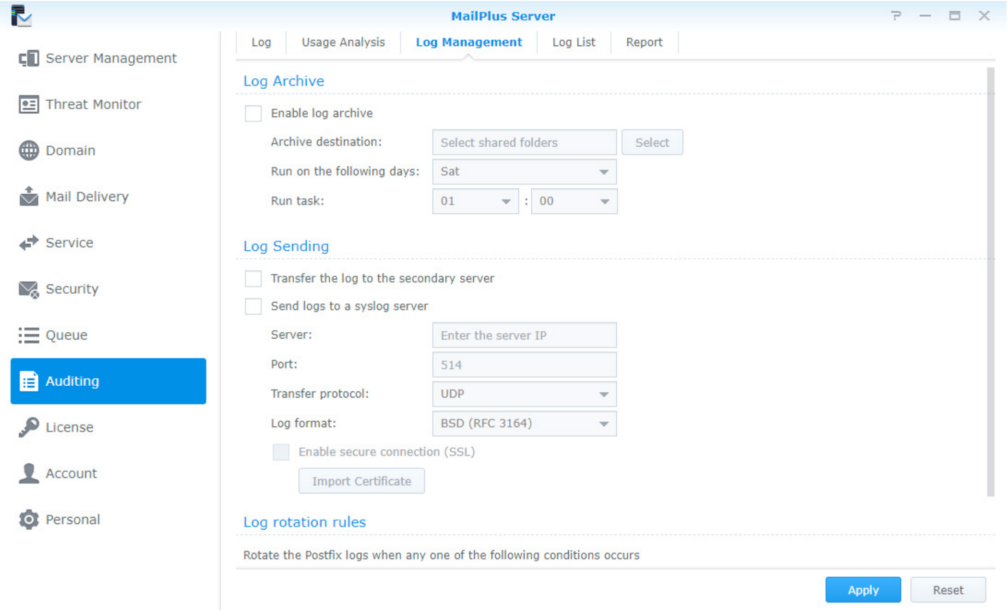
1 Go to **Auditing** > **Log Management**.

2 Under the **Log Archive** section, tick the **Enable log archive** 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 archive tasks.

5 Click **Apply** to save settings.



□ Enable log archive

Archive destination: Select shared folders

Run on the following days: Sat

Run task: 01 : 00

□ Transfer the log to the secondary server

□ Send logs to a syslog server

Server: Enter the server IP

Port: 514

Transfer protocol: UDP

Log format: BSD (RFC 3164)

□ Enable secure connection (SSL)

Rotate the Postfix logs when any one of the following conditions occurs

Send logs to the secondary server

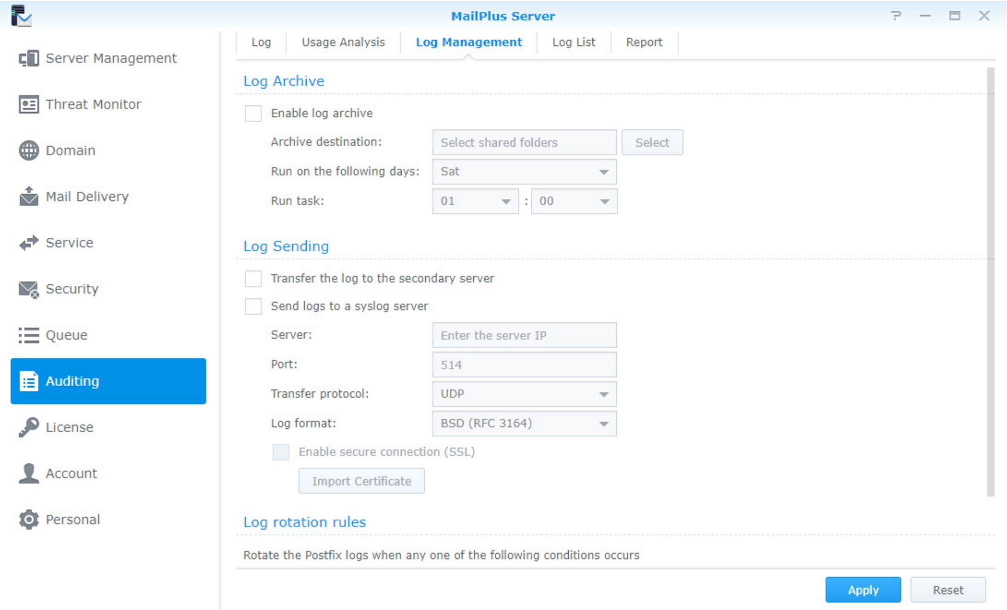
After setting up **High-availability cluster**, logs will be collected to the primary server. You can also choose to send a copy to the secondary server. Sending logs to the secondary server requires generating the log database (please refer to **Generate log database**), you can check afterwards by viewing external database in **Auditing** > **Log**. Please refer to the following steps to send log to the secondary server:

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

Send Postfix logs to other syslog servers

Please refer to the following steps to send postfix log to other syslog servers:

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



Log Archive

□ Enable log archive

Archive destination: Select shared folders

Run on the following days: Sat

Run task: 01 : 00

Log Sending

□ Transfer the log to the secondary server

□ Send logs to a syslog server

Server: Enter the server IP

Port: 514

Transfer protocol: UDP

Log format: BSD (RFC 3164)

□ Enable secure connection (SSL)

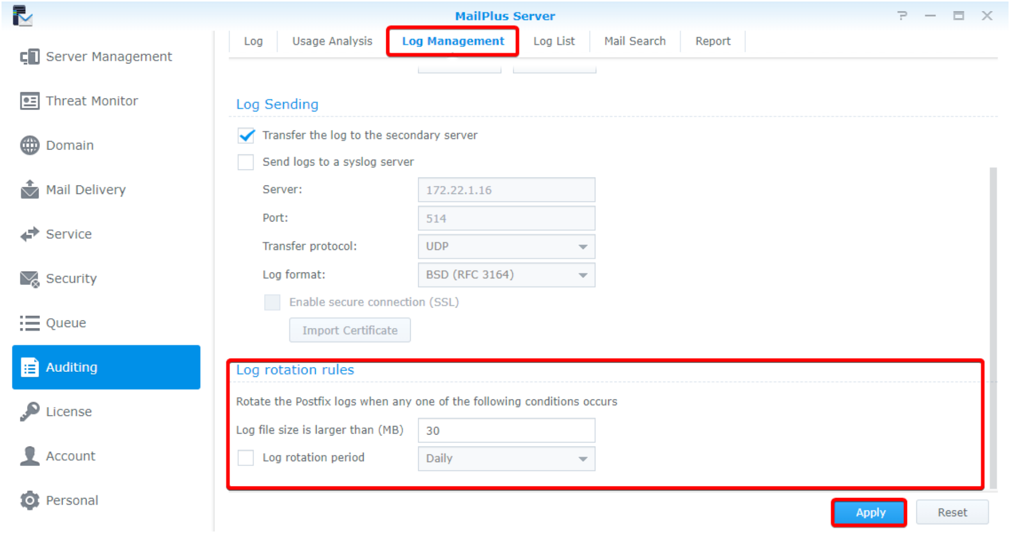
Log rotation rules

Rotate the Postfix logs when any one of the following conditions occurs

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 option from the drop-down menu.
4 Click **Apply** to save settings.



Log Sending

☑ Transfer the log to the secondary server

□ Send logs to a syslog server

Server: 172.22.1.16

Port: 514

Transfer protocol: UDP

Log format: BSD (RFC 3164)

□ Enable secure connection (SSL)

Log rotation rules

Rotate the Postfix logs when any one of the following conditions occurs

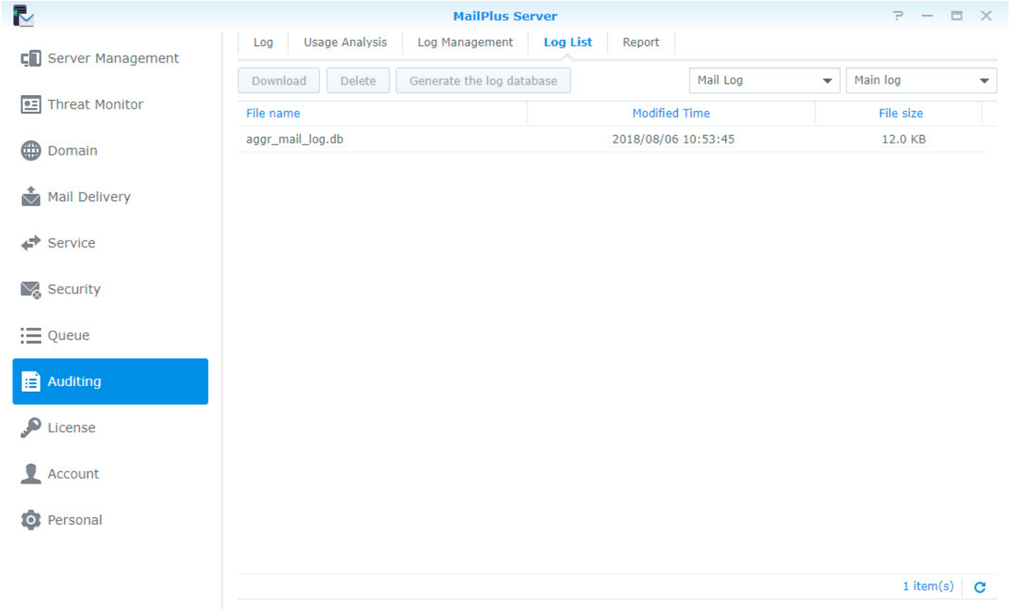
Log file size is larger than (MB) 30

□ Log rotation period Daily

Download and delete log files

You can save mail log database, security log database, or postfix logs on MailPlus Server, and **View External database** in **Auditing** > **Log**. Please refer to the following steps to download and delete log files:

1. Go to **Auditing** > **Log List**.
2. Select **Mail Log**, **Security Log**, or **Postfix Logs** from the drop-down menu at the top.
3. If you have set up MailPlus Server high-availability and enabled **Transfer the log to the secondary server** (please refer to **Send logs to the secondary server**), on secondary servers you can select **Received logs** from the drop-down menu at the top, 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.

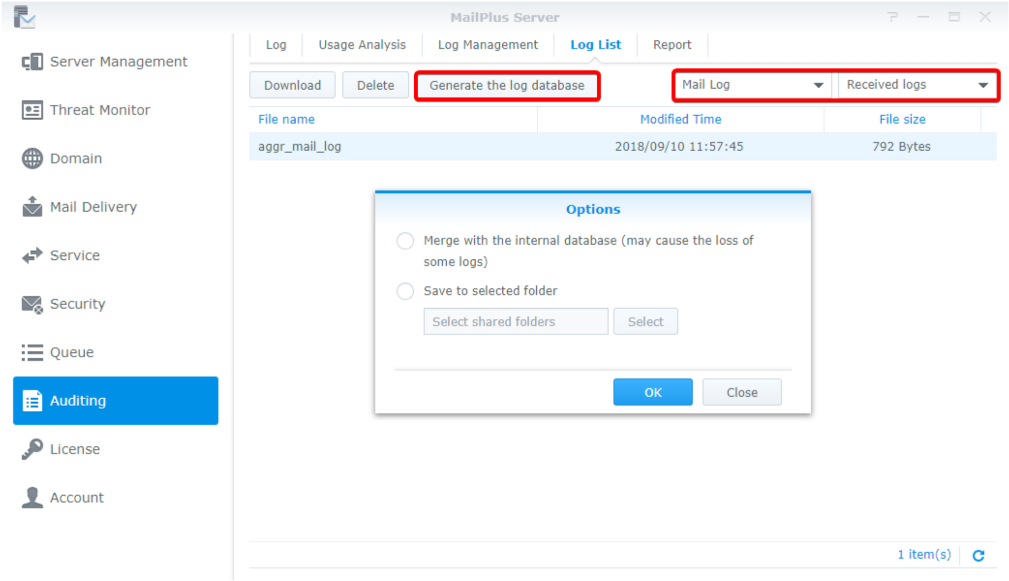


File name	Modified Time	File size
aggr_mail_log.db	2018/08/06 10:53:45	12.0 KB

Generate log database

If you have enabled **Transfer the log to the secondary server** (please refer to **Send logs to the secondary server**), you can convert received log content back to database files using the **Generate the log database** feature. You can **View External database** in **Auditing** > **Log**, to view generated log database files.

1 Go to **Auditing** > **Log List**.
2 Select **Mail Log**, **Security Log** or **Postfix logs** from the drop-down menu at the top.
3 Select **Received logs** from the drop-down menu at the top.
4 Select a log file, and click the **Generate the 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 select a destination folder.
6 Click **OK** to finish.



Mail Log | Received logs

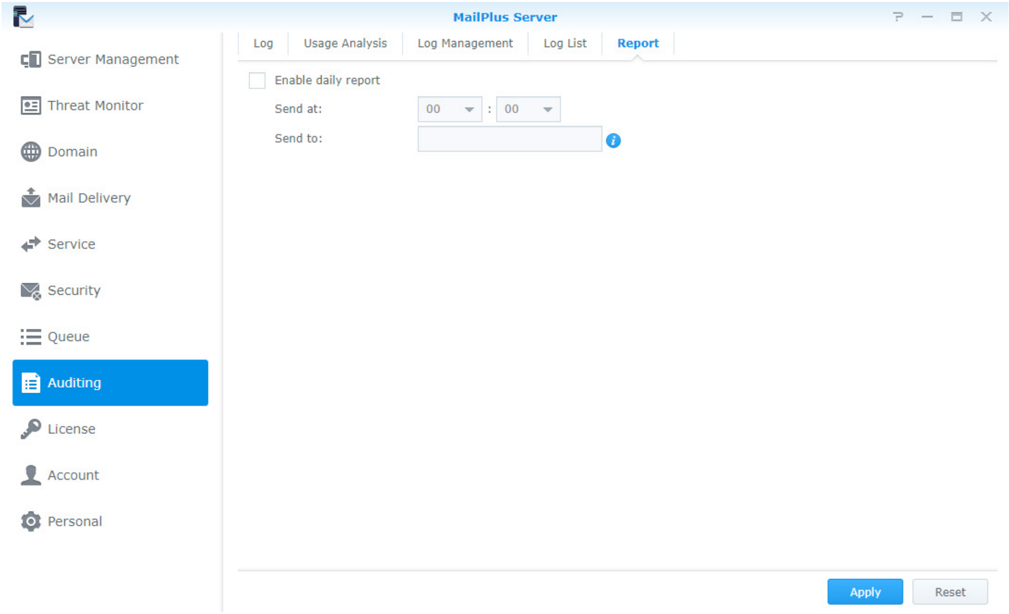
File name	Modified Time	File size
aggr_mail_log	2018/09/10 11:57:45	792 Bytes

○ Merge with the internal database (may cause the loss of some logs)
○ Save to selected folder

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 the daily reports. You can specify up to two email addresses, please separate by semicolon (;).



□ Enable daily report
Send at: 00 : 00
Send to:

Chapter

11

Disaster Recovery

High-availability cluster

Synology MailPlus Server provides two solutions: **single node** configuration and **high-availability** configuration. Single node configuration requires one Synology NAS server to run email services. For high-availability configuration, the high-availability (HA) cluster is composed of two Synology NAS servers to ensure uninterrupted mail services during unexpected events.

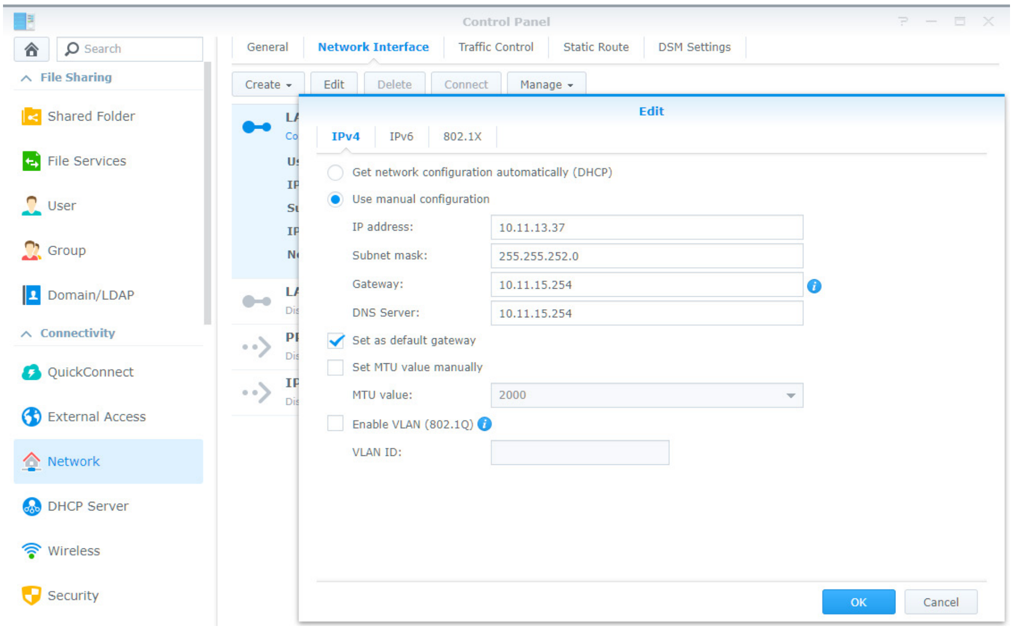
High-availability (HA) configuration introduction

The high-availability (HA) cluster is composed of two Synology NAS servers, one assuming the role of the "primary server" while the other acts as the "secondary server". Users and other mail servers connect to the main IP address of the MailPlus Server HA cluster. The primary server runs on the main IP address of the MailPlus Server HA cluster and receives all mail service requests. These requests will then be assigned to either the primary or secondary server to be processed, and a **two-way synchronization** will be performed for mail data to be transferred from the primary server to the secondary server or vice versa. The primary and secondary server may process different service requests, however data will remain consistent and synchronized across both servers. You can add or edit new settings in MailPlus Server, and the new settings will be applied to both the primary and secondary server. 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 synced back to the primary server. When the secondary server malfunctions, the primary server will assume all workload, and data modifications processed during that 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 thereby cannot run on Synology NAS simultaneously. If service continuity is required, it is recommended that you use the MailPlus high-availability cluster architecture designed for mail services. After the high-availability cluster recovers, data remains consistent across both servers, preventing the loss of updated data on the secondary server during the split-brain error.

Before configuring High-availability (HA)

- **Prepare two Synology NAS servers**: Install the MailPlus Server package on both Synology NAS servers. Initialize MailPlus Server on one of the servers, this server will be use as the "primary server", for more information on how to set up MailPlus Server, please refer to **Set up MailPlus Server**. MailPlus Server on the other Synology NAS server should remain uninitialized, and this Synology NAS server will be used as the "secondary server".
- **Assign two sets of static IP addresses for the primary and secondary servers**: The IP addresses for both Synology NAS Servers must be under the **same LAN**, and the IP address must not be retrieved via PPPoE or DHCP. The network card with the IP address should be set up to perform **manual network configuration**.



○ Get network configuration automatically (DHCP)
● Use manual configuration

IP address: 10.11.13.37
Subnet mask: 255.255.252.0
Gateway: 10.11.15.254
DNS Server: 10.11.15.254

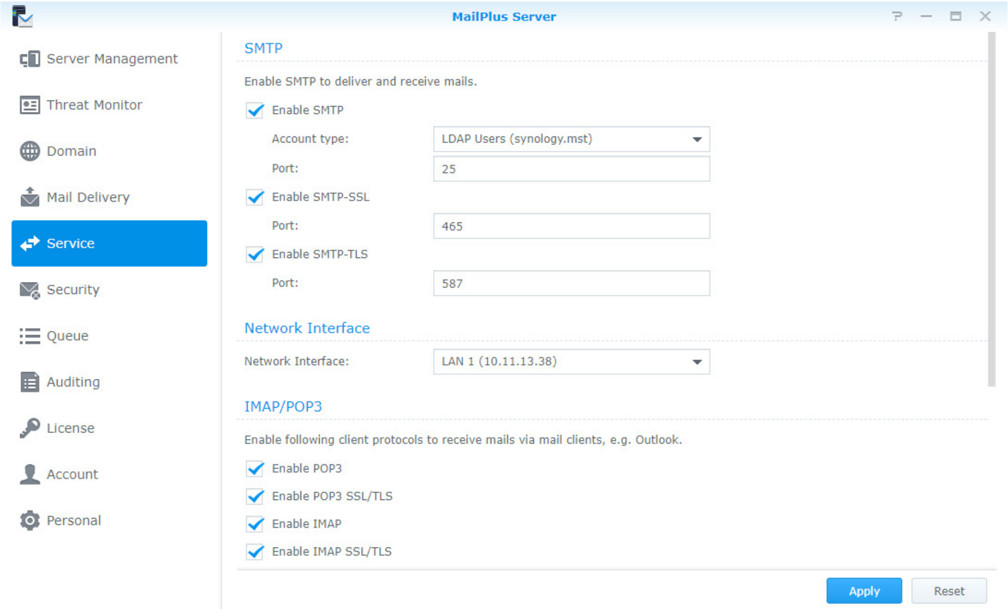
☑ Set as default gateway
□ Set MTU value manually
MTU value: 2000
□ Enable VLAN (802.1Q)
VLAN ID:

- The **2-step verification** feature must be disabled on the secondary server.
- **Both servers must join the same domain**: Both your Synology NAS servers must join Windows Active Directory or LDAP server. For information on how to join Windows Active Directory, please refer to this **tutorial article**. For more information on how to join LDAP, 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 **Active Directory Server** or **Directory Server** and set up your own Windows Active Directory or LDAP server to manage accounts.
- **Prepare another external IP address that is under the same LAN**: You should prepare a set of external IP address under the same LAN for both the primary and secondary Synology NAS servers to be used as the external IP address for MailPlus Server HA. Users can access services using this IP address even when manual switch or failover to another server occurs.

Configure High-availability (HA)

1 Launch **MailPlus Server** after it has been set up.

2 Go to **Service**, and check if **Domain Users** or **LDAP Users** has been selected from the **Account type** drop-down menu under the **SMTP** section.



Enable SMTP to deliver and receive mails.

☑ Enable SMTP
Account type: LDAP Users (synology.mst)
Port: 25
☑ Enable SMTP-SSL
Port: 465
☑ Enable SMTP-TLS
Port: 587

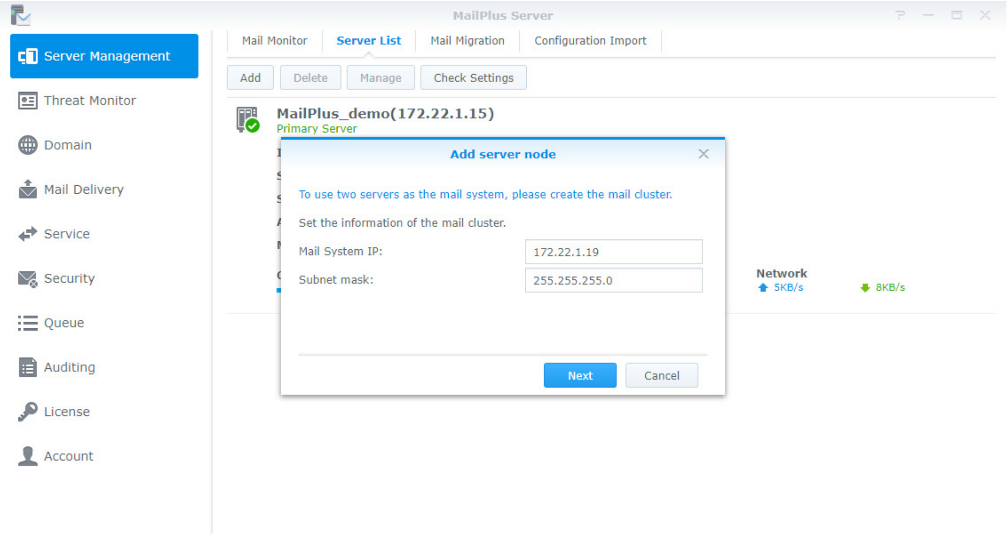
Network Interface: LAN 1 (10.11.13.38)

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

☑ Enable POP3
☑ Enable POP3 SSL/TLS
☑ Enable IMAP
☑ Enable IMAP SSL/TLS

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

4 Enter the main external IP address for the HA cluster, and click **Next** when done.



Add server node

To use two servers as the mail system, please create the mail cluster.

Set the information of the mail cluster.

Mail System IP: 172.22.1.19

Subnet mask: 255.255.255.0

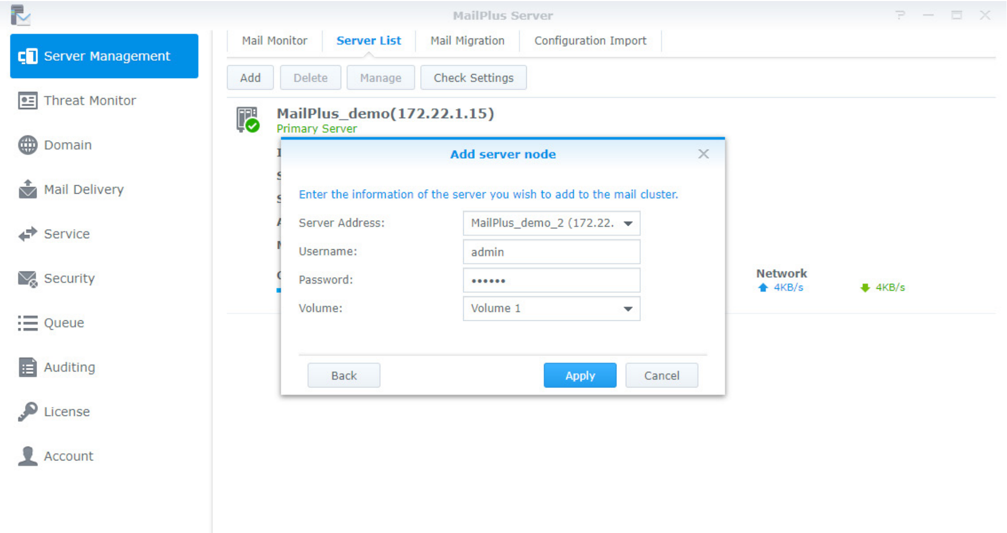
5 Enter an IP address in the **Server Address** field or select a Synology NAS server to use as the secondary server for the HA cluster from the **Server Address** drop-down menu, Synology NAS servers under the same LAN will be searched and included in this drop-down menu.

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 the admin account or other accounts from an administrator group for the secondary server in the **Username** and **Password** fields.

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

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



Add server node

Enter the information of the server you wish to add to the mail cluster.

Server Address: MailPlus_demo_2 (172.22.

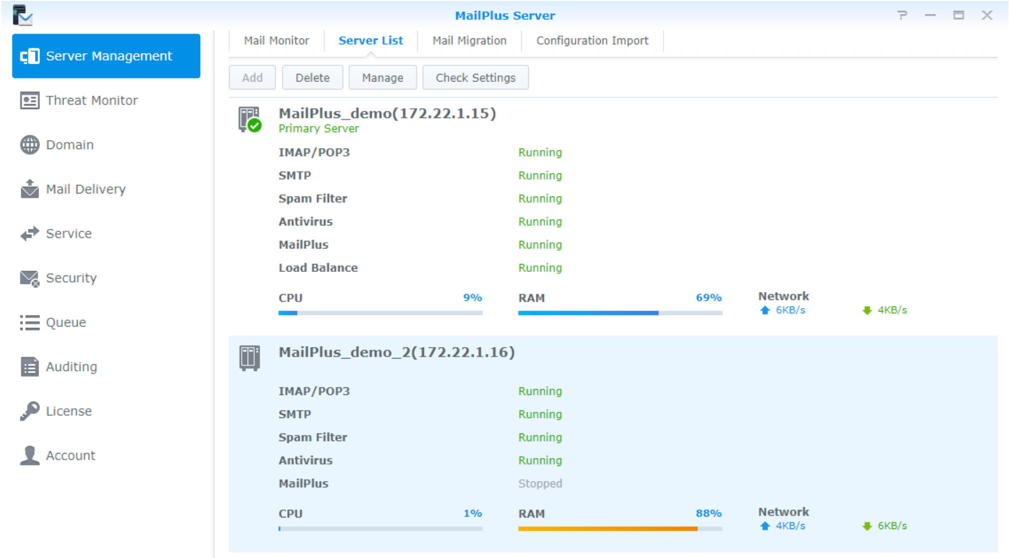
Username: admin

Password: ••••••

Volume: Volume 1

9 After completing the settings, email messages will be synchronized to the secondary server. **The time required for synchronization depends on the amount of email messages on the primary server**. During

synchronization, you will still be able to send and receive messages, and all services will be processed by the primary server before synchronization is complete. After synchronization has been completed, the primary and secondary server will share the workload.



MailPlus_demo(172.22.1.15)
Primary Server

IMAP/POP3	Running
SMTP	Running
Spam Filter	Running
Antivirus	Running
MailPlus	Running
Load Balance	Running

CPU 9% RAM 69% Network 6KB/s 4KB/s

MailPlus_demo_2(172.22.1.16)

IMAP/POP3	Running
SMTP	Running
Spam Filter	Running
Antivirus	Running
MailPlus	Stopped

CPU 1% RAM 88% Network 4KB/s 6KB/s

Modify High-availability (HA) cluster configuration

1 Launch **MailPlus Server** after it has been set up.

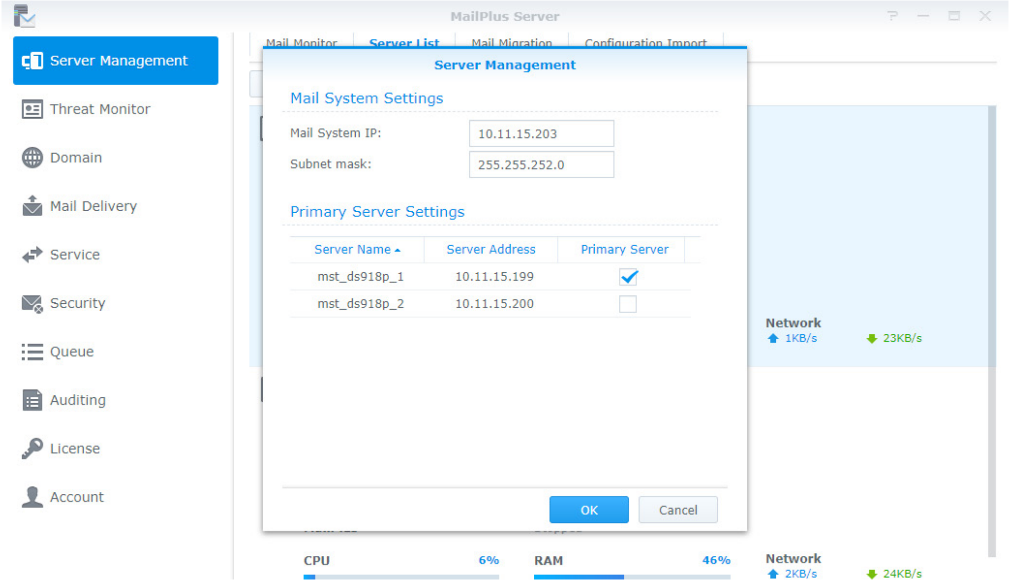
2 Go to **Server Management** > **Server List**.

3 Click the **Manage** button.

4 Under the **Mail System Settings** section, you can modify the IP address and subnet mask settings of your MailPlus system (HA cluster).

Note: The modified the IP address and subnet mask, along with the IP address of the primary and secondary servers must be under the same subnet.

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



Server Management

Mail System Settings

Mail System IP: 10.11.15.203

Subnet mask: 255.255.252.0

Primary Server Settings

Server Name	Server Address	Primary Server
mst_ds918p_1	10.11.15.199	☑
mst_ds918p_2	10.11.15.200	□

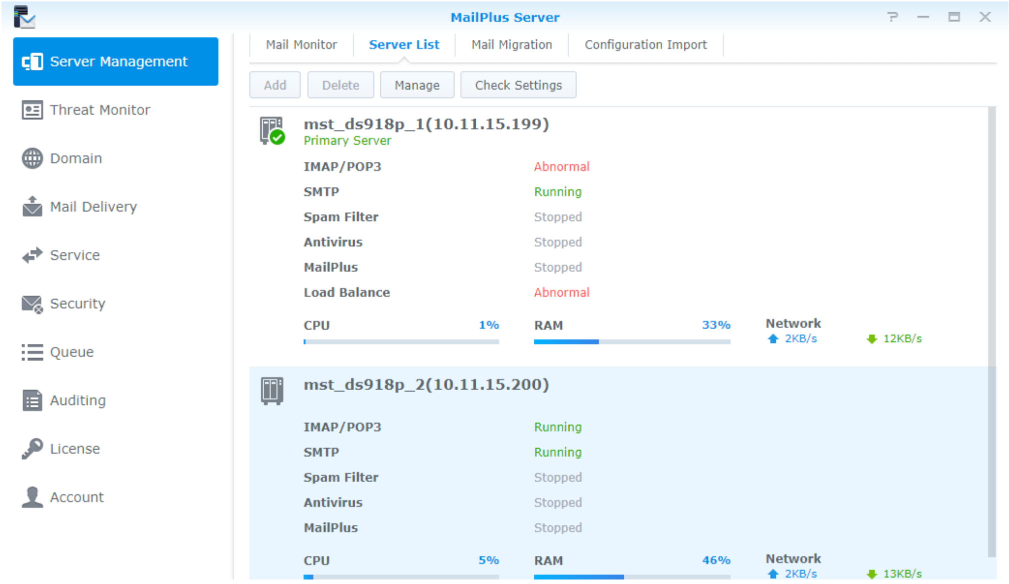
Network 1KB/s 23KB/s

CPU 6% RAM 46% Network 2KB/s 24KB/s

Remove High-availability (HA) configuration

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

1 Log in to **DSM** of the Synology NAS server you would like to keep, and launch **MailPlus Server**.
2 Go to **Server Management** > **Server List**.
3 Select the Synology NAS server you want to remove.



mst_ds918p_1(10.11.15.199)
Primary Server

IMAP/POP3	Abnormal
SMTP	Running
Spam Filter	Stopped
Antivirus	Stopped
MailPlus	Stopped
Load Balance	Abnormal

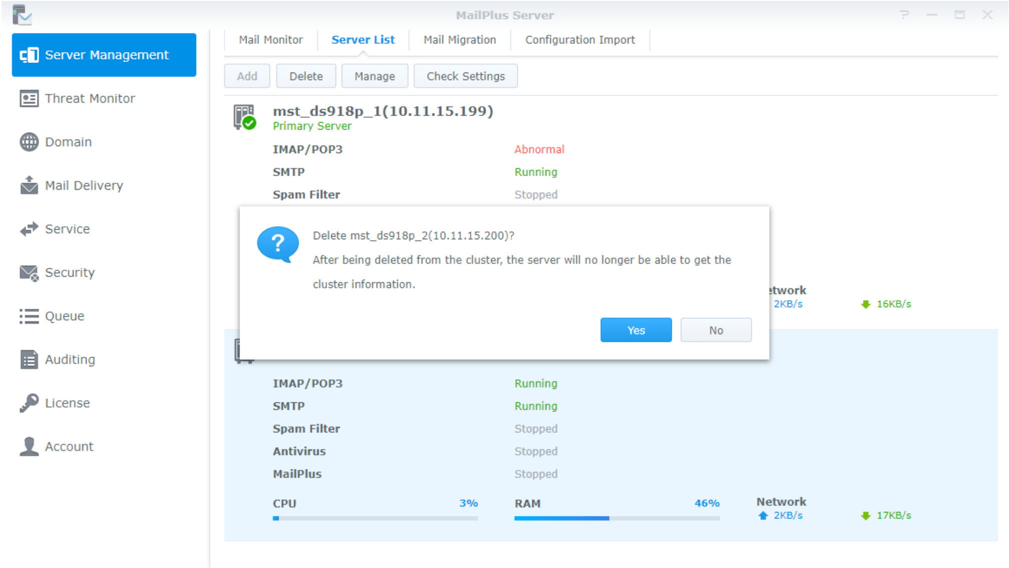
CPU 1% RAM 33% Network 2KB/s 12KB/s

mst_ds918p_2(10.11.15.200)

IMAP/POP3	Running
SMTP	Running
Spam Filter	Stopped
Antivirus	Stopped
MailPlus	Stopped

CPU 5% RAM 46% Network 2KB/s 13KB/s

4 Click the **Delete** button.
5 Click **Yes** in the popup confirmation window.



mst_ds918p_1(10.11.15.199)
Primary Server

IMAP/POP3	Abnormal
SMTP	Running
Spam Filter	Stopped

Delete mst_ds918p_2(10.11.15.200)?

After being deleted from the cluster, the server will no longer be able to get the cluster information.

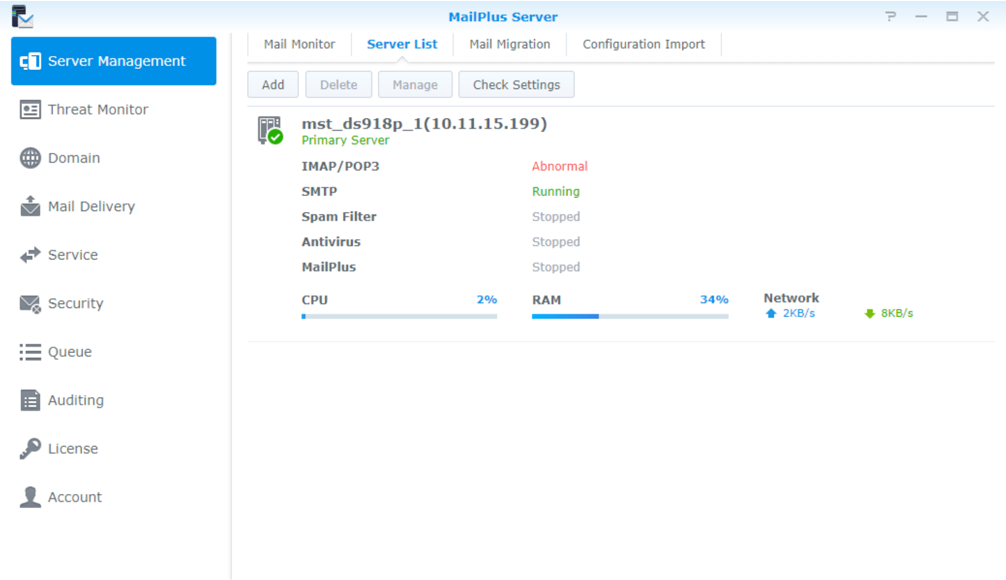
twork 2KB/s 16KB/s

IMAP/POP3	Running
SMTP	Running
Spam Filter	Stopped
Antivirus	Stopped
MailPlus	Stopped

CPU 3% RAM 46% Network 2KB/s 17KB/s

6 After the email messages have been synchronized, HA configuration removal will be complete. The server you would like to keep will still continue to receive and process email 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.



mst_ds918p_1(10.11.15.199)
Primary Server

IMAP/POP3 Abnormal
SMTP Running
Spam Filter Stopped
Antivirus Stopped
MailPlus Stopped

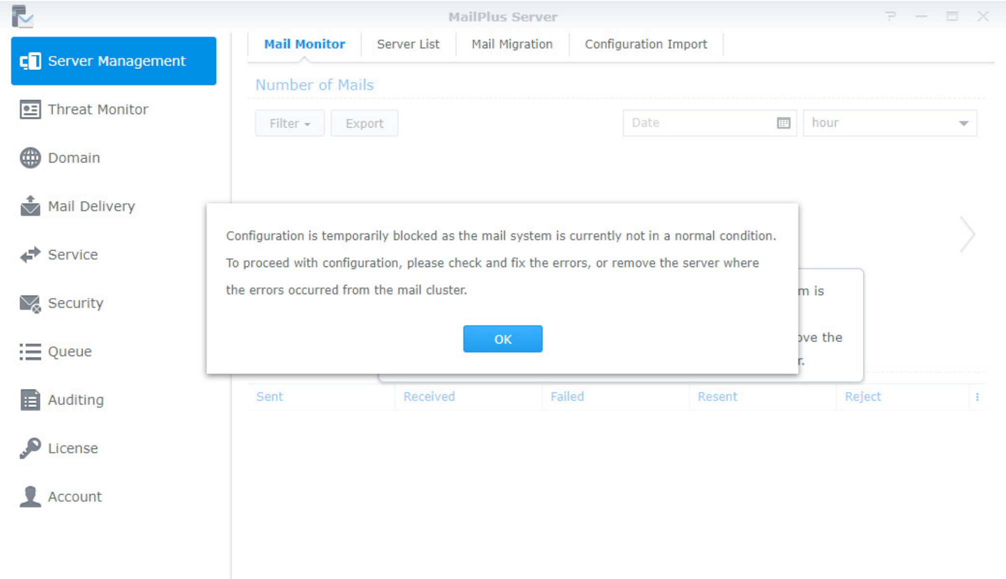
CPU 2%
RAM 34%
Network 2KB/s 8KB/s

Server malfunction

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

Primary server malfunction

When the original primary server malfunctions, the original secondary server will take over the external IP address of the HA cluster and receive and process email service requests independently. 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 the settings on MailPlus Server during the time, therefore your primary server needs to be recovered at the earliest opportunity. If your original primary server cannot be recovered, please refer to **Remove High-availability (HA) configuration** to remove the original primary server. After removal, MailPlus Server will go back to running on a **single-node** configuration.



Configuration is temporarily blocked as the mail system is currently not in a normal condition. To proceed with configuration, please check and fix the errors, or remove the server where the errors occurred from the mail cluster.

Secondary server malfunction

When the original secondary server malfunctions, the original primary server will take over the external IP address of the HA cluster and receive and process all email service requests independently. Please recover your original secondary server at the earliest opportunity. If your original secondary server cannot be recovered, please refer to **Remove High-availability (HA) configuration** to remove the original secondary server. After removal, MailPlus Server will go back to running on a **single-node** configuration.

Backup and restore Mail

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

- MailPlus Server **system configuration** backup
- MailPlus Server **mailbox** and **email** backup

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

System configuration backup

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

1 Launch **Hyper Backup** on the source Synology NAS server.

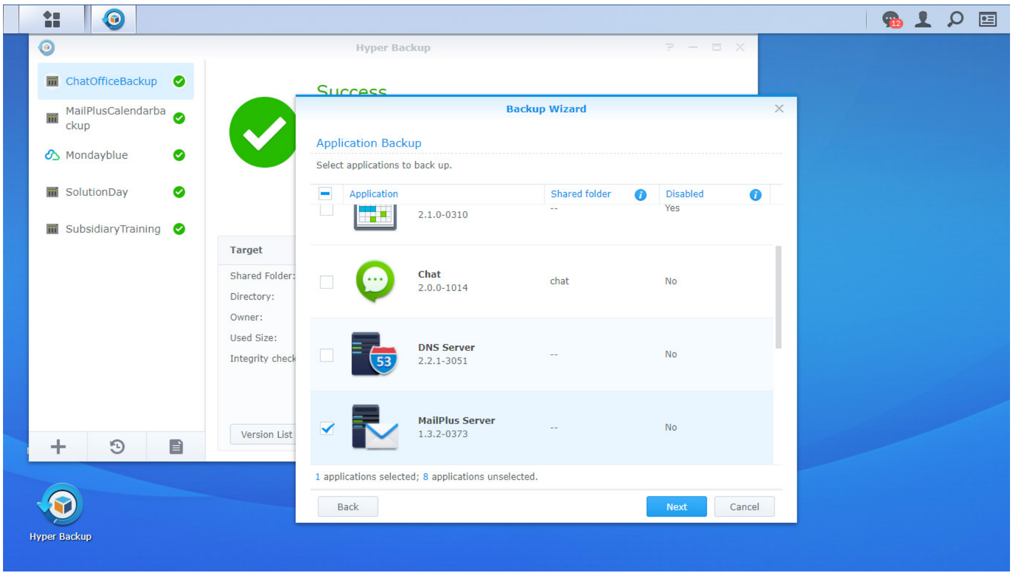
2 Click **+** in the lower-left corner to create a new data backup task.

3 Select a backup destination type:

- **Local Shared Folder & External Storage**: Selecting this option will back up data to a local Synology NAS or an external USB/SD storage device.
- **Remote Synology NAS**: The **Hyper Backup Vault** package needs to be installed and running on the remote destination.

4 Specify tasks settings to complete settings. For more information on how to create backup tasks, please refer to this **Help article**.

5 When the system asks you to select an application to back up, please select **MailPlus Sever**.



Backup Wizard

Application Backup

Select applications to back up.

☐	Application	Shared folder	Disabled
☐	2.1.0-0310	--	Yes
☐	Chat 2.0.0-1014	chat	No
☐	DNS Server 2.2.1-3051	--	No
☑	MailPlus Server 1.3.2-0373	--	No

1 applications selected; 8 applications unselected.

Back | Next | Cancel

6 After completing backup task settings, the system will be ready to back up the following MailPlus Server settings (found on the left menu of the MailPlus Server interface):

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

Mailbox and email backup

Back up all mailbox and email messages to a MailPlus compatible Synology NAS server. For more information, please refer to the following sections.

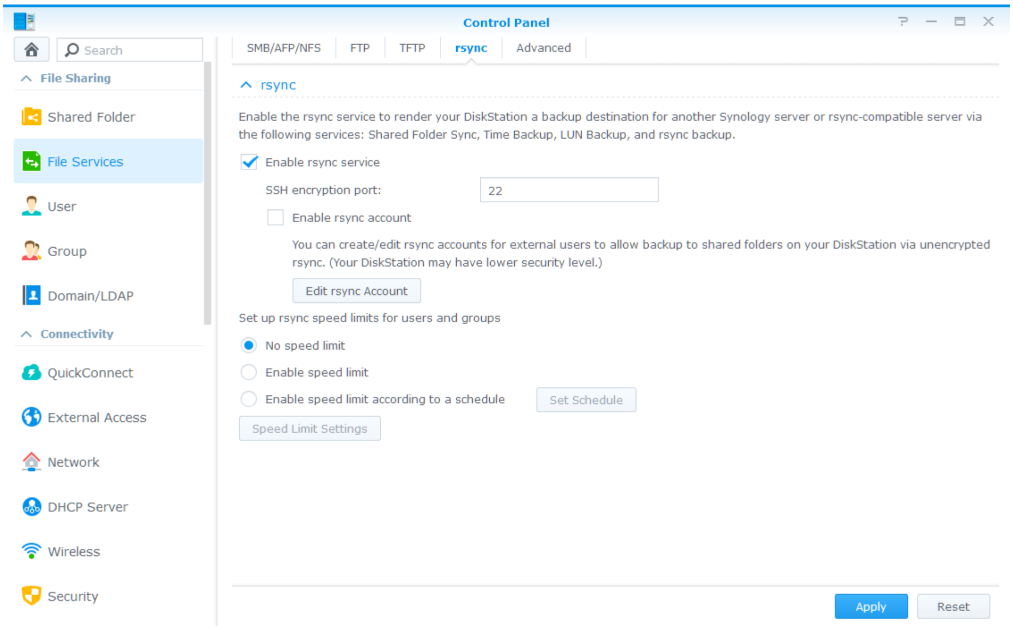
Enable Shared Folder Sync

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

1 Log in to **DSM**.

2 Go to **Control Panel** > **File Services** > **rsync**.

3 Tick the **Enable rsync service** checkbox to enable **Shared Folder Sync**.



rsync

Enable the rsync service to render your DiskStation a backup destination for another Synology server or rsync-compatible server via the following services: Shared Folder Sync, Time Backup, LUN Backup, and rsync backup.

☑ Enable rsync service

SSH encryption port: 22

□ Enable rsync account

You can create/edit rsync accounts for external users to allow backup to shared folders on your DiskStation via unencrypted rsync. (Your DiskStation may have lower security level.)

Set up rsync speed limits for users and groups

● No speed limit

○ Enable speed limit

○ Enable speed limit according to a schedule

4 Click **Apply**.

Create sync tasks

Log in to the source Synology NAS server, and refer to the following steps to create sync tasks:

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 destination shared folder to sync to.

5 Specify destination Synology NAS details and the following sync settings:

- **Customize SSH encryption port for encrypted shared folder sync**: Specify a desired encryption port for SSH transfer encryption.
- **Enable SSH transfer encryption**: Encrypts data during transfer. This option provides better security, while non-encrypted transfer offers better performance. You can choose according to your needs.
- **Enable transfer compression**: Compresses data during transfer. This option reduces bandwidth usage, however it increases CPU workload.

- **Enable block-level synchronization**: Syncs only the modified portions instead of the whole file. This option reduces bandwidth usage, however increases CPU workload.

6 When prompted, select any of the following options to decide when to sync from the source to the destination:
   - **Run sync on modification**: Runs sync immediately once any change occurs at the source shared folder.
   - **Run sync manually**: Runs sync tasks manually from the source shared folder.
   - **Advanced schedule**: Click the **Schedule Plan** button and specify when to run sync tasks.

7 Click **Apply**. Now you can see the sync task on the task list. The system will run tasks according to the specified schedule.

Manage sync tasks

Log in to the source Synology NAS server, 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 the sync tasks is not in progress, please click the **Sync Now** button to perform the task right away.
   - If the 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 completed, only the modified parts will be synced. Clicking this button allows you to manually sync all data again.

Note:

1. 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 the content of any shared folder(s) monitored by the sync task, **Shared Folder Sync** would resume the task.
2. Please do not use the Cloud Station Server package and Cloud Sync to run backup since its two-way synchronization feature may corrupt the data.
3. If a **MailPlus** shared folder already exists in the destination, the folder will be renamed as **MailPlus_1** after the backup is complete.
4. If you would like to use data from **MailPlus_1**, please manually move the data to the **MailPlus** shared folder.
5. 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

Go to the destination Synology NAS server. The system configuration, mailbox, and email are stored in the local shared folder. Please refer to the following steps to restore system configuration, mailbox, and email:

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 restoring, the current MailPlus Server configuration will be overwritten.

4 The backed up mailbox and email do not require restoring and can be used immediately.

5 Contact **Synology Technical Support** to migrate MailPlus Server Licenses from the source Synology NAS to the destination Synology NAS.

6 After migrating the licenses, you can run mail services on the destination.

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