Synology

Synology Administrator-Handbuch für

Synology MailPlus Server

Basierend auf
Synology MailPlus Server 2.2

Inhaltsverzeichnis

Einleitung

Die Synology MailPlus Suite bietet einen fortschrittlichen und sicheren E-Mail-Dienst mit hoher Benutzerfreundlichkeit. Diese Suite besteht aus zwei Paketen: MailPlus Server und MailPlus. MailPlus Server ist eine Verwaltungskonsole mit verschiedenen Einstellungen, während MailPlus eine E-Mail-Plattform für Client-Benutzer darstellt.

Dieses Administrator-Handbuch führt Sie durch die Einrichtung von MailPlus Server und bietet Ihnen detaillierte Konfigurationsanweisungen, einschließlich DNS-Einstellungen, Migration von E-Mail-Diensten sowie weitere Sicherheitseinstellungen. Darüber hinaus sind die nachfolgenden Hauptmerkmale in diesem Handbuch enthalten, um bewährte Methoden und Prozesse zu gewährleisten: MailPlus High-Availability für einen stabilen und kontinuierlich verfügbaren E-Mail-Dienst, die E-Mail-Warteschlange für die Verwaltung zurückgestellter Nachrichten, sowie die Verwaltungskonsole mit einer Übersicht über den Zustand von MailPlus.

Kapitel 1: Implementierungsrichtlinien

Dieses Kapitel bietet eine Anleitung zu bewährten Methoden, die bei der Implementierung von MailPlus zu beachten sind, um die Stabilität und Leistungsfähigkeit von E-Mail-Diensten zu gewährleisten. Nachstehend werden folgende Themen behandelt: wie man ein Synology NAS für MailPlus auswählt, wie man Arbeitsspeicher und Speicheranforderungen berechnet, welche Faktoren bei der Nutzung des SSD-Cache zu berücksichtigen sind, sowie Empfehlungen über die Ausführung I/O-intensiver Pakete neben MailPlus auf einem NAS.

Ein Synology NAS auswählen

Synology bietet eine Vielzahl von NAS-Geräten mit unterschiedlichen Formfaktoren, Funktionen und Möglichkeiten. Nicht alle davon sind für MailPlus Server geeignet. Folgendes kann Ihnen bei der Auswahl des passenden Synology NAS behilflich sein:

1. Auf der **MailPlus-Lizenzseite** finden Sie eine Liste der unterstützten Geräte, die nach der maximalen Anzahl gleichzeitiger Benutzer und maximalen Serverleistung sortiert ist.
   - **Die maximale Anzahl gleichzeitiger Benutzer** betrifft die empfohlene maximale Anzahl von MailPlus-Benutzern.
   - **Die maximale Serverleistung** betrifft die maximale Anzahl an E-Mails, die MailPlus Server pro Tag verarbeiten kann.
2. Besuchen Sie die **Synology-Produktseite**, um eine Liste aller Modelle anzuzeigen, die MailPlus unterstützen. Durch Klicken auf das gewünschte Modell erhalten Sie weitere Informationen über seine technischen Daten.

Anmerkung:

- Die Kennzahlen basieren auf Labortests, die intern von Synology durchgeführt wurden. Die Testumgebung ist nachstehend angeführt:
  - Beim Test mit der maximalen Anzahl an gleichzeitigen Benutzern blieben CPU- und RAM-Auslastung jeweils unter 80 %.
  - Bei getesteten Modellen mit erweiterbarem Speicher wurde der maximale Arbeitsspeicher installiert.
  - In Modellen mit 2 Einschüben und zwei Steckplätzen für M.2-Laufwerke wurden zwei SSDs für SSD-Cache installiert.
  - In Modellen mit mehr als 4 Einschüben wurden zwei SSDs für SSD-Cache installiert.
  - In Modellen der FS-Serie wurden 12 SSDs in einer RAID F1-Konfiguration installiert.
  - Wegen der Datensynchronisierung zwischen beiden Servern ist die Leistung des E-Mail-Systems im High-Availability-Modus etwas geringer.
  - Funktionen, die bei allen oben genannten Tests aktiviert waren: Anti-Spam, Virenschutz, DNSBL, Graue Liste, Inhalt scannen, Volltextsuche (nur in englischer Sprache).
- Die tatsächlichen Grenzwerte können je nach Systemkonfiguration variieren. Um dieselbe Leistung zu erzielen, sollten Sie SSDs installieren und den Arbeitsspeicher erweitern.

Arbeitsspeicher und Speicheranforderungen berechnen

Unter Berücksichtigung der Faktoren, die sich auf die Speichernutzung eines NAS auswirken, lauten die empfohlenen Speichergrößen auf der Grundlage der Benutzeranzahl wie folgt:

- für < 250 Benutzer: mindestens 8 GB RAM
- für 250 - 500 Benutzer: mindestens 16 GB RAM
- für 500 - 1000 Benutzer: mindestens 32 GB RAM
- für > 1.000 Benutzer: mindestens 64 GB RAM

Berechnung der RAM-Auslastung

Die Größe der Speicherauslastung ist in erster Linie von der Anzahl der Benutzer des E-Mail-Dienstes abhängig. Beachten Sie jedoch, dass die nachfolgenden Dienste ebenfalls große Speicherkapazitäten beanspruchen können:

- **Anti-Spam**: Das standardmäßige Anti-Spam-Modul von MailPlus, Rspamd, benötigt häufig viel Speicher.
- **Antivirenprogramm**: Virenschutzdienste wie ClamAV und McAfee können speicherintensiv sein, insbesondere bei der Aktualisierung ihrer Offline-Virus-Datenbanken auf die neueste Version.
- **MailPlus-Web-Client**: MailPlus Server kann gleichzeitig mehrere Anforderungen von Web-Clients erhalten, wenn diese E-Mails abrufen und E-Mail-Entwürfe speichern. Wenn die Anzahl der Benutzer die **maximale Anzahl der gleichzeitigen Benutzer** überschreitet, wie in den Spezifikationen des Synology NAS-Modells angeführt, können plötzliche Auslastungsspitzen der Speichernutzung auftreten, da MailPlus Server versucht, alle Client-Anforderungen zu verarbeiten.

Berechnung der Anforderungen für die Volume-Größe

Verwenden Sie die nachfolgende Formel, um die erforderliche Speichergröße für MailPlus zu berechnen:

- Geschätzte Speichergröße = [(die durchschnittliche Anzahl der ein- und ausgehenden E-Mails pro Tag)*(die durchschnittliche Größe von E-Mails)*(die Anzahl der Benutzer)*(Tage)]

Die durchschnittliche Größe einer E-Mail beträgt 300 KB, die durchschnittliche Anzahl der E-Mails, die von einer Einzelperson gesendet und empfangen werden, beträgt 100 pro Tag, und ein E-Mail-Dienst wird gewöhnlich zwischen drei bis fünf Jahren verwendet.

Wenn Ihr MailPlus beispielsweise 200 Benutzer unterstützt, beträgt die erforderliche Speichergröße:

100 (die durchschnittliche Anzahl der ein- und ausgehenden E-Mails pro Tag)*300 KB (die durchschnittliche Größe einer E-Mail)*200 (die Anzahl der Benutzer)*1095 (die Anzahl der Tage in drei Jahren) = 6,12 TB

Falls Sie Probleme bei der Berechnung der erforderlichen Speichergröße haben, **kontaktieren**

Sie uns, um individuelle Empfehlungen zu erhalten.

SSD-Cache nutzen

Der SSD-Cache ist eine Methode zur Verbesserung der Systemleistung durch vorübergehende Speicherung häufig abgerufener Daten (auch als „heiße Daten" bekannt) auf einem Teil oder auf der gesamten SSD.

Da die Nachrichten bei MailPlus regelmäßig abgerufen und geschrieben werden, ist es erforderlich, dass kleine Dateien direkt gelesen und auf das Laufwerk geschrieben werden. Da die durchschnittliche E-Mail-Größe relativ klein ist, kann die Zunahme der Lese-/Schreibgeschwindigkeit beträchtlich sein, wenn die Daten (auch teilweise) auf einem SSD-Cache gespeichert werden. Durch die Installation einer zusätzlichen SSD und Nutzung des SSD-Cache von Synology wird die Gesamtleistung des E-Mail-Dienstes verbessert.

Anmerkung:

- Größere Firmenkunden sollten für optimale Leistung jedenfalls SSD-Cache verwenden.
- Für optimale Leistung wird dringend empfohlen, ein NAS der FS-Serie zu verwenden und das Volume ausschließlich mit SSDs zu erstellen.

Empfohlene Größe des SSD-Cache

SSDs werden für verschiedene Zwecke entwickelt. Bei der Wahl der passenden SSD für Ihr System sollten Sie die Faktoren Haltbarkeit, konstante Leistung und Schutz vor Stromausfällen berücksichtigen.

Synology SSDs sind SSDs der Enterprise-Klasse, die speziell für rund um die Uhr betriebene NAS-Umgebungen entwickelt wurden und deren Kompatibilität mit Synology-Systemen in strengen Tests sichergestellt wurde. Intensive Tests wie I/O-Belastungstests, Stromausfalltests und Temperaturtests stellen sicher, dass Synology SSDs über die hohe Zuverlässigkeit und konstante Leistung verfügen, die in Firmenumgebungen nötig sind – besonders für so zentrale Anwendungen wie Ihren E-Mail-Server.

Neben Synology SSDs hat Synology auch **SSDs von Drittanbietern** getestet und verifiziert. Die Leistung einer SSD kann je nach Hersteller deutlich variieren.

Mehr zur Auswahl der passenden SSD für Ihren SSD-Cache erfahren Sie in **diesem Artikel**.

Empfohlene Größe des SSD-Cache

Die tatsächliche Größe des SSD-Cache hängt vom Umfang der häufig verwendeten Daten auf dem Volume ab. Es werden mindestens zwei SSDs benötigt, um ein redundantes RAID 1/5/6/10-Laufwerk für die Nutzung eines Lese/Schreib-Cache zu erstellen. Beispiel: Wenn Sie einen Lese/Schreib-Cache mit 480 GB erstellen möchten, werden mindestens zwei identische SSDs mit je 480 GB benötigt.

Häufig verwendete Daten werden auf der SSD zwischengespeichert; bei MailPlus Server sind häufig verwendete Daten hauptsächlich die kürzlich abgerufenen E-Mails, auf die mit hoher Wahrscheinlichkeit häufig zugegriffen wird. Häufig verwendete Daten machen etwa drei bis

sechs Prozent des gesamten Speicherplatzes aus, der für E-Mail-Dienste verwendet wird.

- Beispiel: Die Größe der häufig verwendeten Daten auf einem E-Mail-Speicherplatz mit 1 TB beträgt wahrscheinlich: 1.024 GB*6 % = 61,4 GB

Der SSD-Cache sollte jedoch eine größere Kapazität als die tatsächliche Größe der häufig verwendeten Daten aufweisen, um die Leistung sicherzustellen. Wir empfehlen, dass die tatsächliche Größe des SSD-Cache etwa doppelt so groß wie die geschätzte Größe der häufig verwendeten Daten ist.

- Ausgehend von dem obigen Beispiel beträgt die ideale Cache-Größe: 61,4 GB*2 = 122,8 GB.

In diesem Fall wird ein SSD-Cache mit 480 GB den Mindestanforderungen mehr als gerecht.

Die nachfolgende Anleitung bietet eine schnelle Berechnung der SSD-Cache-Größe anhand der Anzahl der Benutzer:

- Für < 500 Benutzer: 480 GB*2
- Für 500 - 1.000 Benutzer: 1 TB*2
- Für > 1.000 Benutzer: 2 TB*2

Wenn Sie bereits ein Synology NAS haben, kann die Größe der häufig verwendeten Daten und die entsprechende Cache-Größe mit dem **SSD-Cache-Ratgeber** im **Speicher-Manager** bestimmt werden.

Anmerkung:

- Weitere Informationen zum SSD-Cache finden Sie in den nachfolgenden Artikeln und Dokumenten:
  - **Hilfe-Artikel zum SSD-Cache**
  - **Häufig gestellte Fragen zur Nutzung von Synology SSD-Cache**
  - **White Paper: Verwendung der SSD-Technologie von Synology zur Verbesserung der Systemleistung**
- SSD-Cache wird als Möglichkeit empfohlen, die Verarbeitung von E-Mails zu beschleunigen, auch wenn die Anzahl der MailPlus-Benutzer nicht die **maximale Anzahl der gleichzeitigen Benutzer** erreicht, wie in den Spezifikationen des Modells angeführt.

Ausführung mehrerer I/O-intensiver Pakete auf demselben NAS

Um die Leistung und Datensicherheit als bewährtes Verfahren zu gewährleisten, sollten I/O-intensive Pakete, wie MailPlus Server, Synology Drive Server und Synology Chat Server nicht auf demselben Synology NAS installiert werden. Da alle obigen Pakete hohe I/O-Ressourcen verbrauchen, kann es aufgrund von konkurrierenden Ressourcen zwischen den unterschiedlichen Diensten leicht zu Systemfehlern kommen. Wenn es sich bei den Paketen jedoch nicht ausschließlich um I/O-intensive Dienste handelt, ist ein Synology NAS in der Lage, mehrere Dienste gleichzeitig auszuführen. Beispiel: MailPlus Server und Synology Drive sollten nicht auf demselben NAS installiert werden, Synology Calendar kann jedoch gemeinsam mit MailPlus ausgeführt werden, da es sich dabei um keinen I/O-intensiven Dienst handelt.

Kapitel 2: Erste Schritte mit MailPlus Server

Mit MailPlus Server kann ein Synology NAS als E-Mail-System fungieren, das SMTP, POP3 und IMAP unterstützt. Benutzerkonten und E-Mails können auf einem Synology NAS zentral verwaltet und archiviert werden. MailPlus als Client-Paket bietet Benutzern von E-Mail-Diensten eine benutzerfreundliche und browserbasierte E-Mail-Plattform für das Anzeigen, Verwalten und Senden von Nachrichten.

Dieses Kapitel unterstützt Sie bei Ihren ersten Schritten mit MailPlus Server und MailPlus.

Synology NAS mit dem Internet verbinden

Es gibt drei Möglichkeiten, um ein Synology NAS mit dem Internet zu verbinden: direkte Verbindung, PPPoE-Verbindung oder Verbindung über einen Router. Detaillierte Anweisungen dazu, wie Sie über das Internet auf ein Synology NAS zugreifen, finden Sie in **dieser Anleitung**.

Eine externe statische IP-Adresse ist für ein E-Mail-System unbedingt erforderlich. Obwohl ein E-Mail-System auch mit einer dynamischen IP-Adresse betrieben werden kann, ist es mit einer statischen IP-Adresse zuverlässiger. Wir empfehlen Ihnen, eine externe statische IP-Adresse für Ihr E-Mail-System zu registrieren. Weitere Informationen erhalten Sie von Ihrem Internet-Serviceanbieter (ISP).

Konfiguration von statischem IP/PPPoE

Es gibt zwei Möglichkeiten, um externe statische IP-Adressen auf dem Synology NAS einzurichten:

- **PPPoE**: Einige Internetanbieter (ISP) stellen kostenlose statische IP-Adressen bereit; die Benutzer müssen sich jedoch über PPPoE verbinden, um eine statische IP-Adresse abzurufen.
  1. Melden Sie sich bei DSM an.
  2. Gehen Sie zu **Systemsteuerung** > **Netzwerk**.
  3. Wählen Sie auf der Registerkarte **Netzwerkschnittstelle** die Option **PPPoE** aus und klicken Sie auf die Schaltfläche **Bearbeiten**.
  4. Richten Sie das Modem und den Netzwerkport ein.
  5. Geben Sie den Benutzernamen und das Kennwort ein, den bzw. das Sie von Ihrem Internetanbieter erhalten haben.
- **Statische IP-Adresse**: Wenn Sie bereits eine statische IP-Adresse haben, können Sie diese

im Synology NAS eingeben.

1. Melden Sie sich bei DSM an.
2. Gehen Sie zu **Systemsteuerung** > **Netzwerk**.
3. Wählen Sie auf der Registerkarte **Netzwerkschnittstelle** einen Netzwerkport aus und klicken Sie auf die Schaltfläche **Bearbeiten**.
4. Geben Sie Ihre statische IP-Adresse ein.

DNS einrichten

Ein gültiger und registrierter Domainname ist Voraussetzung dafür, dass ein Client E-Mails über das Internet an MailPlus Server zustellen kann. Eine E-Mail-Adresse besteht aus zwei Teilen. Der Teil vor @ ist der Benutzername und der Teil nach @ ist der Domainname. Beispiel: Die E-Mail-Adresse von Alex lautet „alex@beispiel.com“. Sein Domainname lautet „beispiel.com“. Um sicherzustellen, dass eine E-Mail-Adresse wie „alex@beispiel.com“ korrekt funktioniert, müssen Sie den MX-Eintrag und A-Eintrag einrichten, damit die E-Mails MailPlus Server erreichen können. Sie können diese Einträge auf dem DNS-Server Ihres Domain-Anbieters konfigurieren.

MX-Eintrag

Der MX-Eintrag oder Mail Exchange-Datensatz gibt an, wie das Internet Ihre E-Mails mit SMTP (Simple Mail Transfer Protocol) befördern soll. Jeder MX-Eintrag enthält einen Hostnamen und eine Präferenz. Ein Hostname leitet E-Mails zum richtigen E-Mail-Server. Eine Präferenz bestimmt die Priorität mehrerer Server. Je geringer die hier eingetragene Nummer, desto höher die Priorität.

Sie können mehrere MX-Einträge für eine Domain mit mehreren E-Mail-Servern einrichten, und jedem Eintrag eine Präferenznummer zuweisen. Der primäre Server sollte die niedrigste Nummer aufweisen, z. B. Null, um sicherzustellen, dass dieser E-Mail-Server zuerst auf Anforderungen antwortet. Wenn keine Antwort vom primären Server erfolgt, probiert das Internet die anderen als Failover verwendeten E-Mail-Server der Reihe nach entsprechend ihren Präferenznummern aus, bis einer von ihnen eine Antwort sendet.

Beispiel: Wenn die E-Mail-Adresse ***alex@beispiel.com*** lautet, müssen Sie den MX-Eintrag einrichten, der auf den Mailserver verweist, der E-Mails für die Domain ***beispiel.com*** in Empfang nehmen soll. Daher sollten Sie die zu bearbeitende Domain in das Feld **Host** und den Hostnamen von Ihrem MailPlus Server in das Feld **Verweist auf** eingeben. Der Präferenzeintrag, den Sie dem primären Server zuweisen, sollte Null oder in der Nähe von Null sein.

Host	Verweist auf	Voreinstellung
beispiel.com	mail.beispiel.com	0

In diesem Fall würde der MX-Lookup für ***beispiel.com*** den Eintrag ***mail.beispiel.com*** zurückgeben.

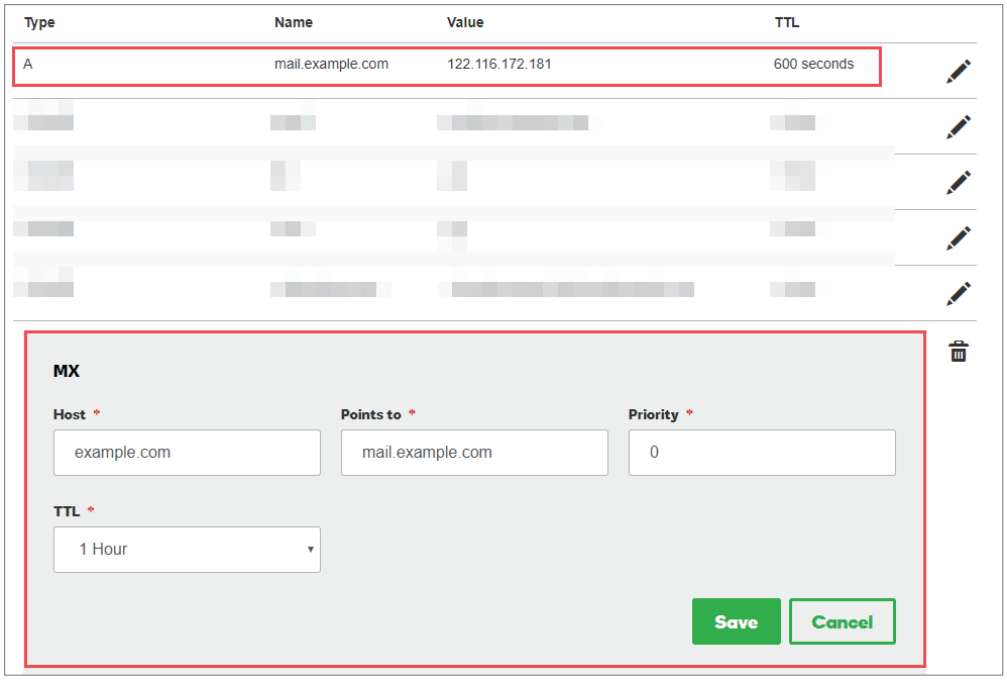
Nachdem der MX-Lookup den Mailserver gefunden hat, benötigt das Internet seine IP-Adresse, um das Ziel für die Zustellung des E-Mails zu ermitteln. Aus diesem Grunde müssen Sie einen A-Eintrag für Ihren Mailserver einrichten.

A-Eintrag

Der A-Eintrag oder Adresseintrag verweist eine Domain oder Subdomain zur IP-Adresse des Host-Servers. Damit kann das Internet IP-Adressen identifizieren, wenn Personen leicht zu merkende Domainnamen verwenden.

Im Falle von ***alex@beispiel.com*** ist ***mail.beispiel.com*** die Subdomain von ***beispiel.com*** und der Host-Server ist das Synology NAS, auf dem MailPlus Server ausgeführt wird.

Von Hostname	Zu IP-Adresse
mail.beispiel.com	111.116.172.181



Die Beispiele und Abbildung dienen nur zur Veranschaulichung. Die Benutzeroberfläche des DNS-Eintrags des jeweiligen Anbieters kann sich unterscheiden. Wenn Sie Probleme bei der Konfiguration von DNS-Einträgen haben, wenden Sie sich bitte an Ihren Domainanbieter.

Reverse DNS einrichten

Die Zuweisung spezifischer DNS-Einträge zu einem Domainnamen wird auch als **Forward DNS (DNS-Weiterleitung)** bezeichnet. Sie führt einen Domainnamen zum richtigen Server. Es gibt auch den umgekehrten Vorgang, der **Reverse DNS** genannt wird.

Was ist Reverse DNS?

Als Reverse DNS wird die Übersetzung der numerischen Adressen von Websites (d. h. die IP-Adresse) in den Domain-/Hostnamen bezeichnet, im Gegensatz zur DNS-Weiterleitung, bei der ein Domain-/Hostname in eine IP-Adresse übersetzt wird. Reverse DNS bezeichnet auch die Ermittlung, welcher Domainname/-Host zu einer bestimmten IP-Adresse gehört; aus diesem Grund wird der Vorgang auch häufig als **Reverse DNS Lookup** bezeichnet. Domainnamen mit gültiger Reverse DNS können über eine IP-Adresse erreicht werden.

Was macht Reverse DNS?

Reverse DNS ist eine der grundlegenden Anforderungen für ein E-Mail-System. Außerdem wird es häufig als Spamfilter eingesetzt, um festzustellen, ob die IP-Adresse einer eingehenden Nachricht mit einem authentifizierten Domainnamen übereinstimmt, und um die Nachricht zu blockieren, falls dies nicht der Fall ist. Wenn Sie kein Reverse DNS für Ihren Mailserver einrichten, werden die von Ihrem Mailserver gesendeten Nachrichten von den meisten großen E-Mail-Anbietern blockiert. Wenn Sie Reverse DNS nicht selbst einrichten können und regelmäßig Probleme bei der Zustellung Ihrer E-Mails haben, müssen Sie einen zweiten SMTP-Server für die Mailübermittlung hinzufügen. Wir empfehlen Ihnen die Verwendung eines bekannten SMTP-Servers, damit Ihre E-Mails nicht als Spam abgewiesen werden.

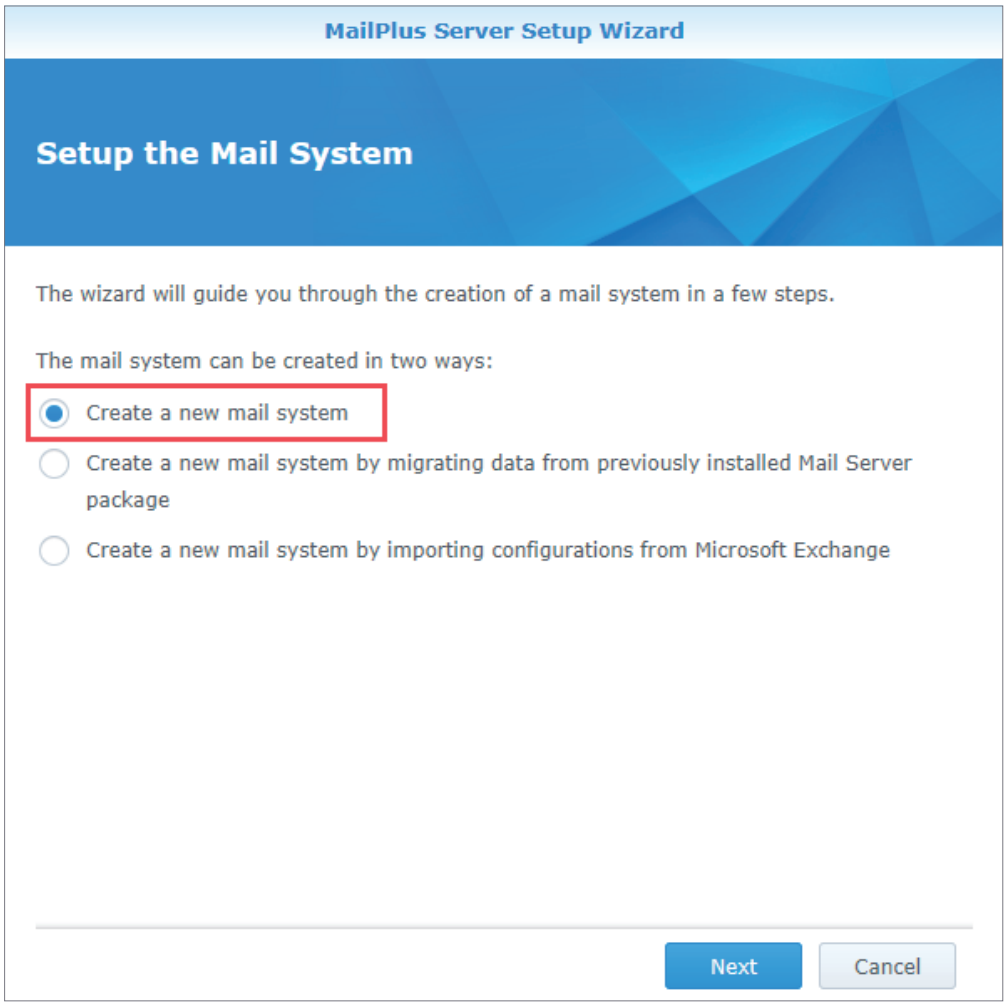
So richten Sie Reverse DNS ein

- **Einrichten von Reverse DNS auf Ihrem eigenen Host**: Bei manchen ISPs wird ein Teil der Zone an Benutzer delegiert, sodass Benutzer ihr eigenes Reverse DNS hosten können. Sie können Reverse DNS konfigurieren, indem Sie PTR-Einträge in einem DNS-Server bestimmen. PTR-Einträge werden von der Stelle verwaltet, welche die IP-Adresse festlegt. Dies kann entweder Ihr Host sein oder Sie selbst, wenn der Host das Reverse DNS für den IP-Raum (der eine oder mehrere IP-Adressen enthält) an Sie delegiert hat. Ein PTR-Eintrag ist normalerweise die rückwärts eingegebene IP, gefolgt von einem in-addr.arpa-Eintrag.
- **Einrichten von Reverse DNS mit Ihrem Internetanbieter (ISP)**: Nur der ISP bzw. der Besitzer Ihrer IP-Adresse können entsprechende PTR-Einträge hinzufügen. Möglicherweise müssen Sie sich wegen der Konfiguration von Reverse DNS an den ISP bzw. das Unternehmen wenden.

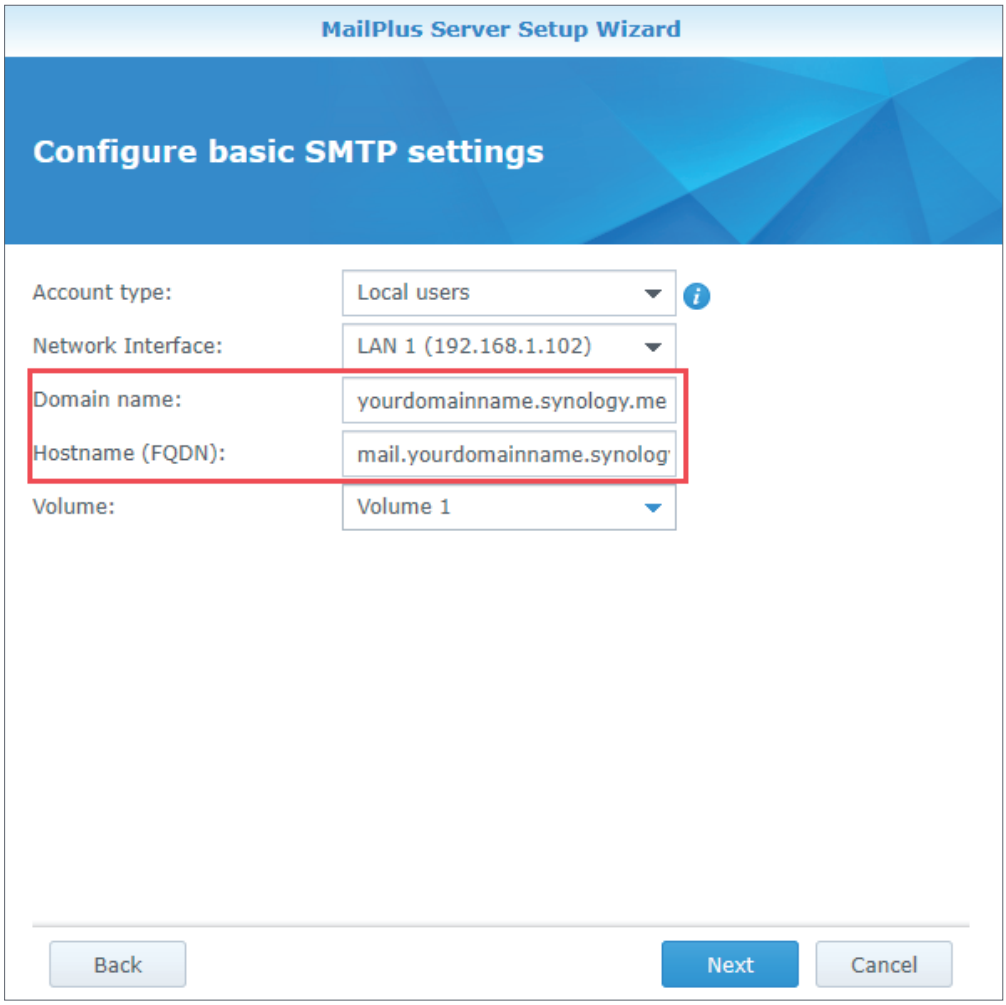
MailPlus Server einrichten

Nach Abschluss der Installation können Sie mit der Einrichtung von MailPlus Server beginnen. Der folgende Abschnitt erklärt die Konfiguration der grundlegenden Einstellungen für SMTP (Simple Mail Transfer Protocol). Beachten Sie, dass die nachfolgenden Screenshots nur als Referenz dienen. Ihre Einstellungen können davon abweichen.

1. Gehen Sie zum **Paketzentrum**, um **MailPlus Server** zu installieren.
2. Starten Sie **MailPlus Server** und wählen Sie **Neues E-Mail-System erstellen**, um ein völlig neues E-Mail-System einzurichten. Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren. Alternativ können Sie auch die Option **Neues E-Mail-System durch Migrieren der Daten vom zuvor installierten Mail Server erstellen** auswählen. In **dieser Anleitung** finden Sie Informationen zur Migration von Mail Server auf MailPlus Server.



3. Geben Sie Ihren Domainnamen und Hostnamen (FQDN) ein:
   - **Domainname**: Der Domainname ist der Ort bzw. die Adresse, wo E-Mail-Nachrichten empfangen werden. Überprüfen Sie bitte, ob der Domainname mit dem MX-Eintrag in den DNS-Einstellungen übereinstimmt.
   - **Hostname (FQDN)**: Der Hostname ist die Adresse Ihres MailPlus Server. Überprüfen Sie bitte, ob der Hostname mit dem A-Eintrag in den DNS-Einstellungen übereinstimmt.



4. Ändern Sie die folgenden Einstellungen je nach Bedarf:

   - **Kontotyp**: Wählen Sie einen Benutzerkontotyp (lokal, LDAP oder Domainbenutzer) aus, der für die Verwendung der MailPlus-Dienste zulässig ist.
   - **Netzwerkschnittstelle**: Wählen Sie einen LAN-Port aus, der für MailPlus Server verwendet wird.
   - **Volume**: Wählen Sie ein Volume aus, auf dem MailPlus Server und die zugehörigen Daten gespeichert werden.

5. Klicken Sie auf **Weiter**, um die Zusammenfassung der Einstellungen zu überprüfen, und auf **Übernehmen**, um die Konfiguration abzuschließen.

6. Nach der Einrichtung von MailPlus Server können Sie **Konten aktivieren**, damit bestimmte Benutzer die E-Mail-Dienste nutzen können. Beachten Sie bitte, dass zur Aktivierung von mehr als fünf Benutzerkonten zusätzliche Lizenzen erworben werden müssen. Weitere Informationen zu MailPlus-Lizenzen finden Sie auf der **Lizenzseite von MailPlus** .

Anmerkung:

- Alle Benutzer erhalten standardmäßig die Anwendungsberechtigungen von MailPlus Server. Das Ändern der Berechtigungseinstellungen in der **Systemsteuerung** kann die Funktionalität von MailPlus Server beeinträchtigen und sollte daher vermieden werden. Weitere Informationen dazu finden Sie unter **Konten aktivieren**.
- Nach der Einrichtung von MailPlus Server wird dem Synology NAS automatisch ein freigegebener Ordner **MailPlus** hinzugefügt. Um sicherzustellen, dass Client-Benutzer auf MailPlus zugreifen können, sollten die Standardberechtigungseinstellungen des freigegebenen Ordners beibehalten werden. Wir raten davon ab, die Berechtigungen selbstständig zu ändern.

MailPlus Client einrichten

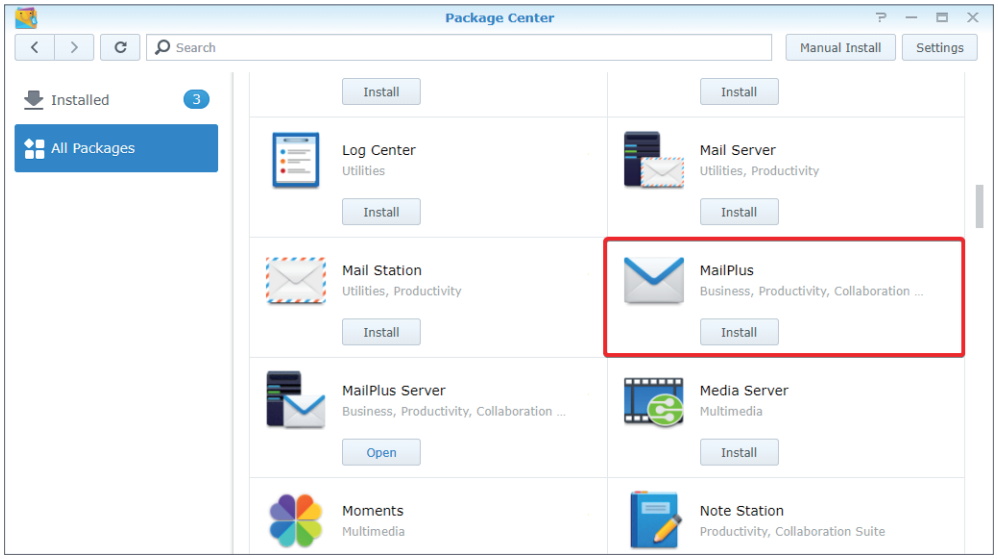
Mit MailPlus auf E-Mails auf dem Synology NAS zugreifen

MailPlus ist ein Zusatzpaket mit einer webbasierten Oberfläche für Client-Benutzer, um auf E-Mails, die auf einem Synology NAS gehostet werden, zuzugreifen und diese zu verwalten.

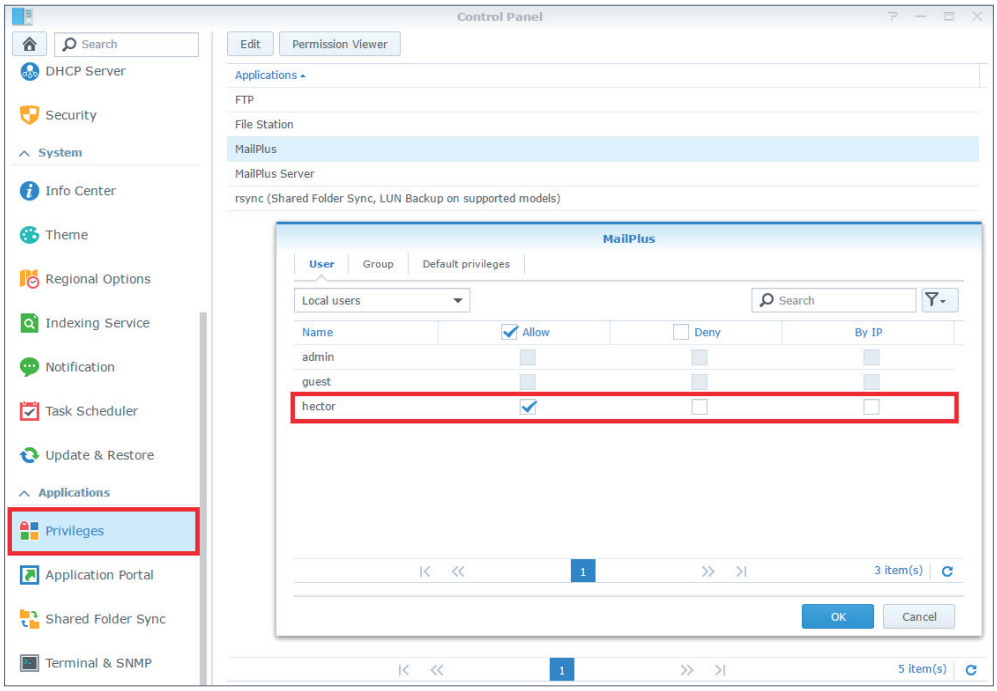
In MailPlus können mehrere POP3-Konten erstellt werden, sodass Benutzer Nachrichten über andere E-Mail-Dienste (z. B. Mozilla® Thunderbird®, Gmail und Office 365) abrufen können.

MailPlus installieren

1. Gehen Sie zum **Paketzentrum**, um **MailPlus** zu installieren.



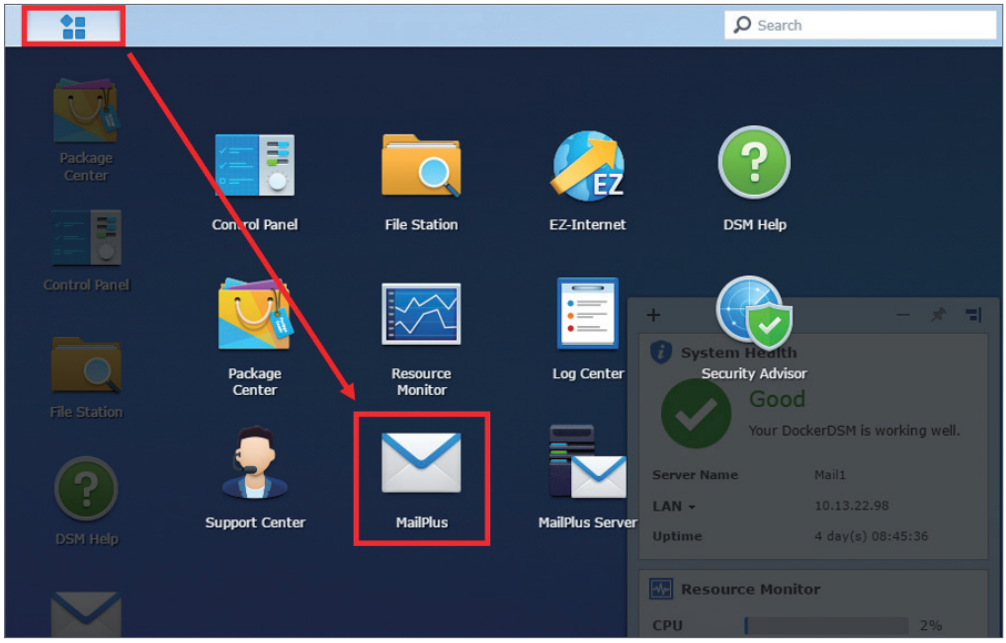
2. Gehen Sie zu **Systemsteuerung** > **Berechtigungen**, um bestimmten Benutzern oder Konten den Zugriff auf **MailPlus** zu erlauben.



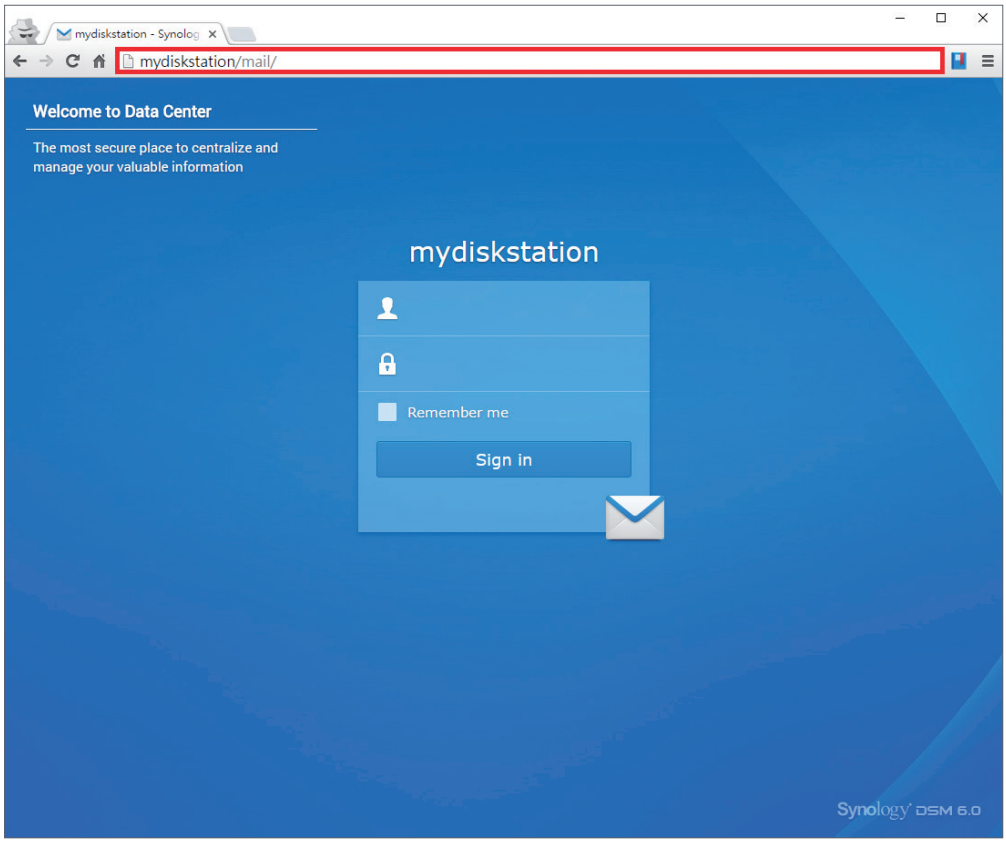
MailPlus ausführen

1. Es gibt zwei Methoden, um die Anmeldeseite von MailPlus zu öffnen:

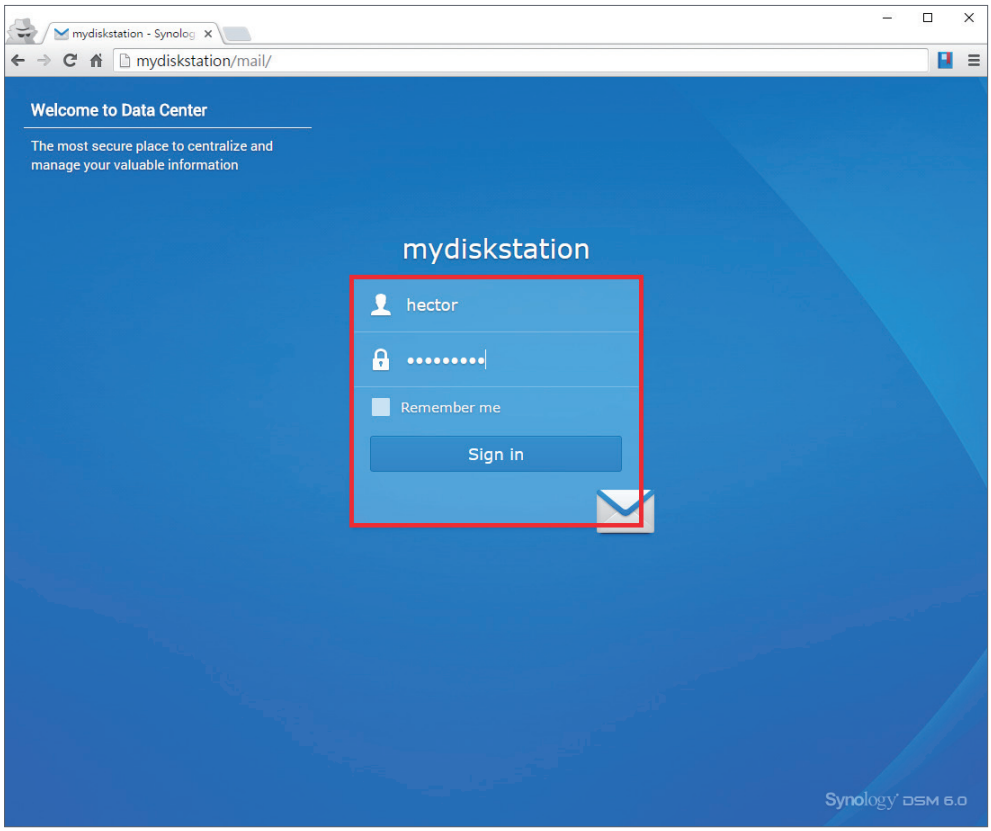
   - Gehen Sie zu **Hauptmenü** > **MailPlus**.



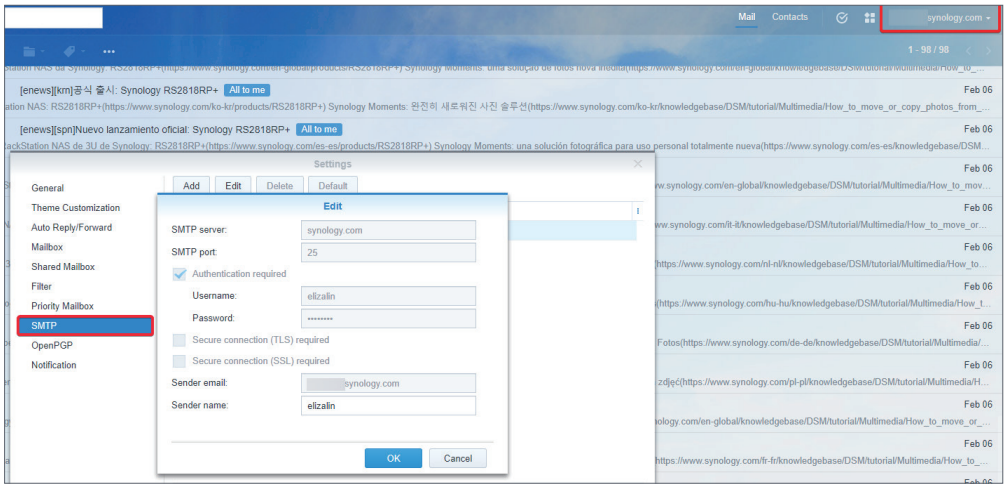
   - Greifen Sie auf MailPlus über das **Anwendungsportal** zu. Geben Sie den Namen des Synology NAS, gefolgt von „/mail“ in die Adresszeile Ihres Webbrowsers ein. Wenn das Synology NAS beispielsweise den Namen *mydiskstation* hat, geben Sie *mydiskstation/mail* ein. In **diesem Hilfe-Artikel** erfahren Sie, wie Sie das **Anwendungsportal** aktivieren.



2. Geben Sie Ihren DSM-Benutzernamen und Ihr Kennwort ein, um sich anzumelden.



3. Wenn die Einstellungen von MailPlus Server vor der Installation von MailPlus konfiguriert wurden, werden die SMTP-Einstellungen von MailPlus Server unter **Einstellungen** > **SMTP** automatisch angezeigt.

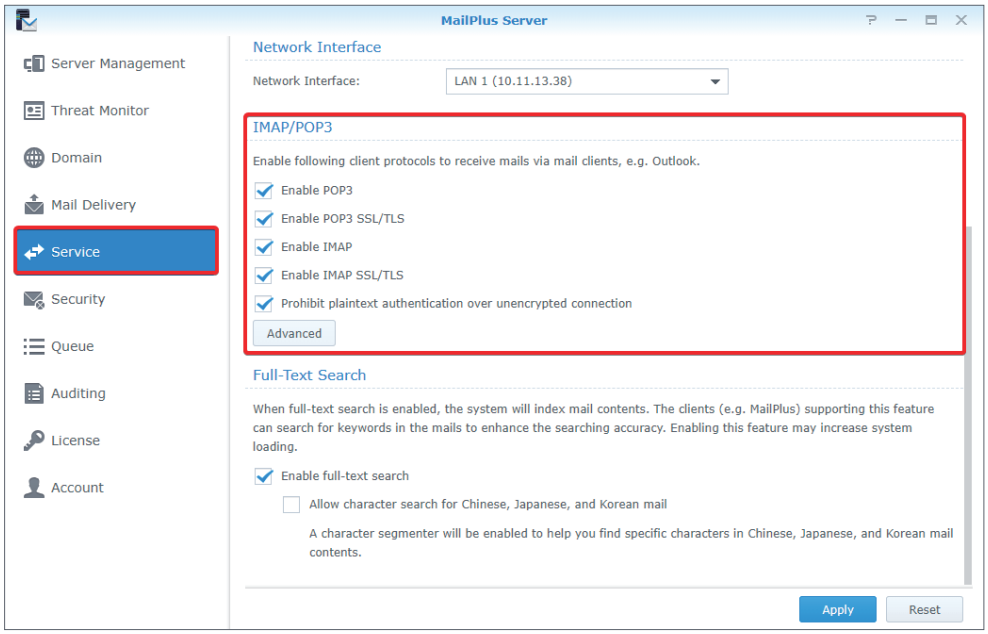


E-Mail-Clients von Drittanbietern

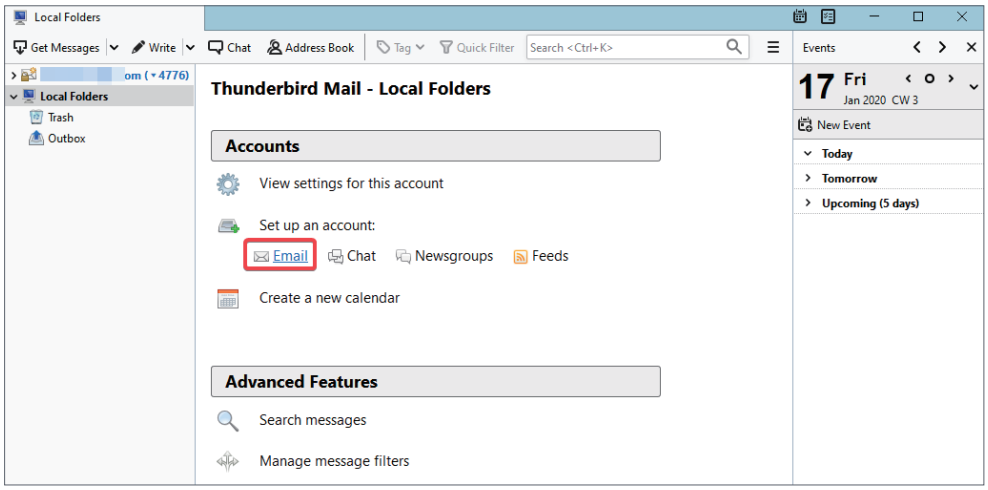
Mit anderen E-Mail-Clients auf E-Mails auf dem Synology NAS zugreifen

E-Mail-Konten auf dem Synology NAS können mit verschiedenen E-Mail-Clients, wie z. B. Microsoft® Outlook® oder Mozilla® Thunderbird® verknüpft werden. Im folgenden Beispiel werden wir mit Thunderbird® auf ein E-Mail-Konto zugreifen, das auf einem Synology NAS gehostet wird.

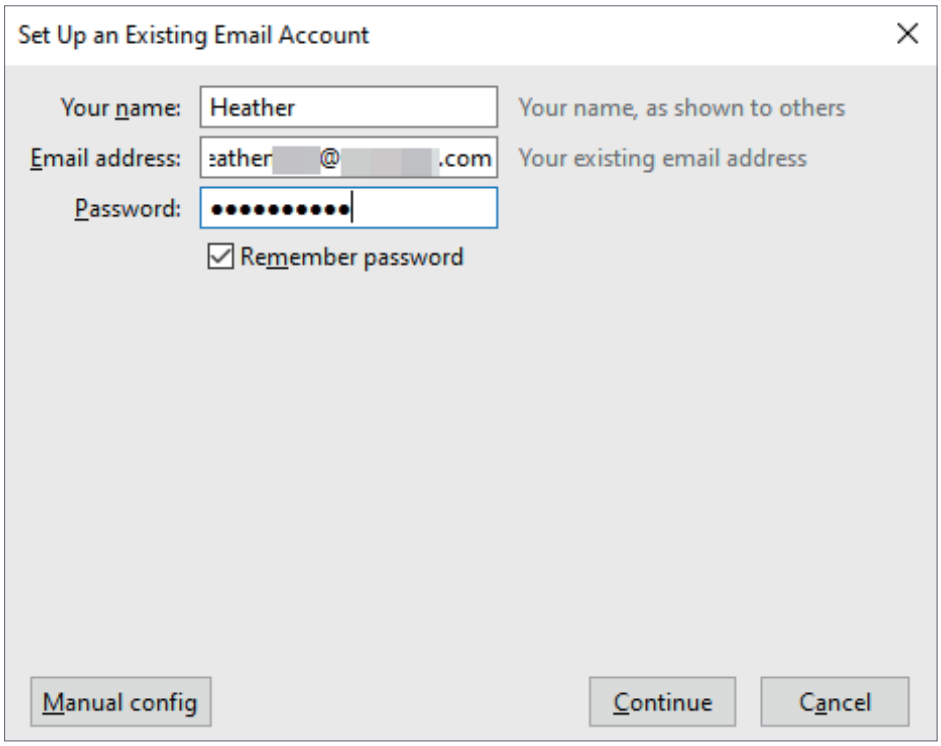
1. Starten Sie **MailPlus Server** und gehen Sie zur Seite **Dienst**, um IMAP und POP3 zu aktivieren.



2. Starten Sie Thunderbird® auf Ihrem Computer und klicken Sie auf **E-Mail**, um das Fenster **Bestehendes E-Mail-Konto einrichten** zu öffnen.

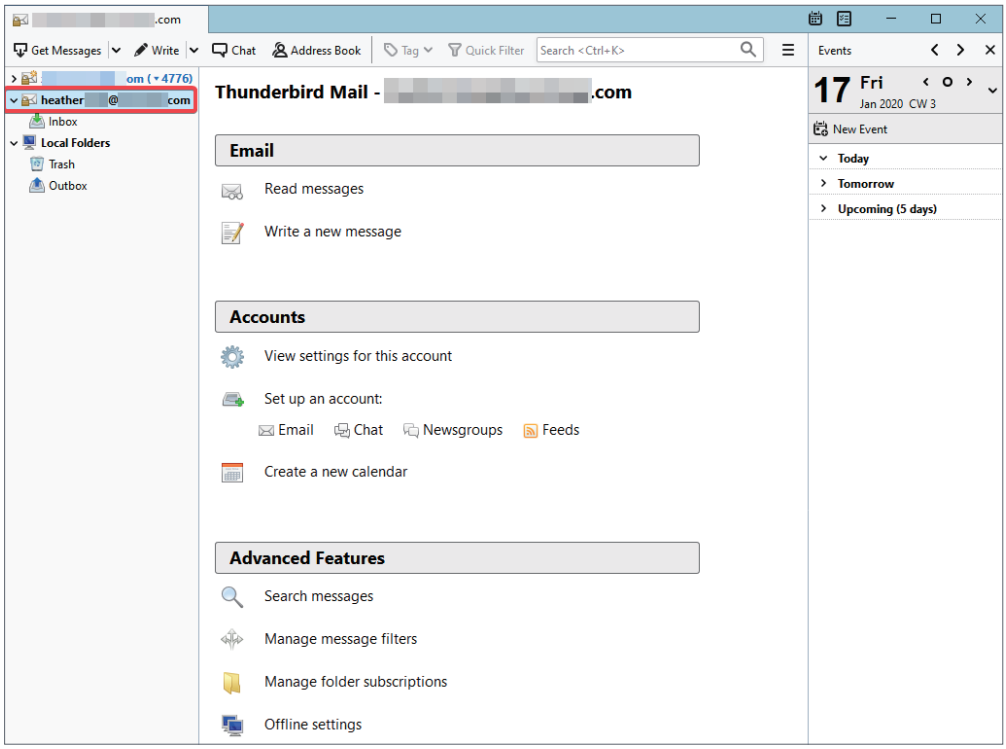


3. Geben Sie den Namen, die MailPlus-Adresse und das Kennwort für Ihr DSM-Benutzerkonto ein. Klicken Sie auf **Fortsetzen**.



4. Thunderbird® sucht nach Ihrem MailPlus-Konto. Wenn die Einstellungen korrekt sind, klicken Sie auf **Fertig**, um die Einstellungen abzuschließen.

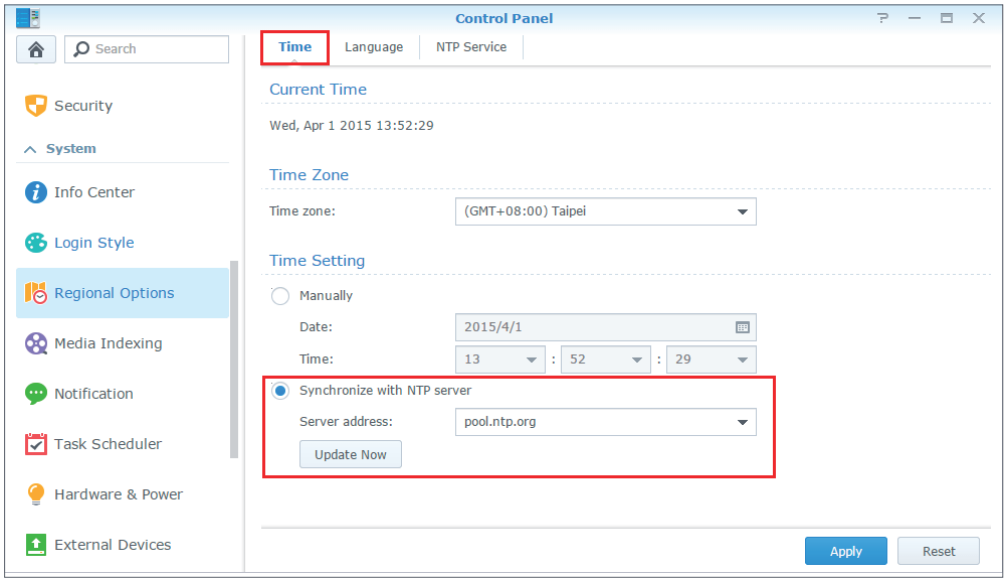
5. Nachdem die Einrichtung abgeschlossen ist, wird Ihr MailPlus-Konto im linken Bereich angezeigt. Durch Doppelklick auf das Konto können Sie alle Postfächer ausklappen.



Fehlerbehebung

Warum kann ich keine E-Mails per Webmail von MailPlus senden oder empfangen?

1. Überprüfen Sie, ob die Einstellungen von MailPlus, z. B. SMTP, DNS und MX, korrekt sind.
2. Überprüfen Sie, ob die Interneteinstellungen des Synology NAS korrekt sind. Gehen Sie zu **Systemsteuerung** > **Regionale Optionen**. Setzen Sie auf der Registerkarte **Uhrzeit** ein Häkchen bei **Mit einem NTP-Server synchronisieren** und klicken Sie auf **Jetzt aktualisieren**, um zu überprüfen, ob die Interneteinstellungen korrekt sind. Wenn das Ergebnis korrekt zurückgegeben wird, stimmen die Einstellungen.



3. Überprüfen Sie, ob die Portnummer an Ihrem Router korrekt ist.
4. Besuchen Sie **Spamhaus**, um zu überprüfen, ob Ihre IP als Spammer gelistet ist. Wenn ja, entfernen Sie Ihre IP von der Blockierungsliste auf derselben Website.

Warum kann ich keine E-Mails über E-Mail-Clients senden oder empfangen?

1. Überprüfen Sie, ob Sie IMAP und POP3 aktiviert haben.
2. Überprüfen Sie, ob Ihr Benutzername und das Kennwort korrekt eingegeben sind.
3. Überprüfen Sie, ob die Einstellungen von MailPlus, z. B. SMTP, DNS und MX, korrekt sind.
4. Überprüfen Sie, ob die Interneteinstellungen des Synology NAS korrekt sind. Gehen Sie zu **Systemsteuerung** > **Regionale Optionen**. Setzen Sie auf der Registerkarte **Uhrzeit** ein Häkchen bei **Mit einem NTP-Server synchronisieren** und klicken Sie auf **Jetzt aktualisieren**, um zu überprüfen, ob die Interneteinstellungen korrekt sind. Wenn das Ergebnis korrekt zurückgegeben wird, stimmen die Einstellungen.
5. Überprüfen Sie, ob die Portnummer an Ihrem Router korrekt ist.
6. Besuchen Sie **Spamhaus**, um zu überprüfen, ob Ihre IP als Spammer gelistet ist. Wenn ja, entfernen Sie Ihre IP von der Blockierungsliste auf derselben Website.

Warum kann ich keine E-Mails empfangen, die von anderen Mailservern gesendet werden (z. B. Gmail)?

1. Vergewissern Sie sich, dass die DNS-Einstellungen korrekt konfiguriert sind. Sie müssen die MX- und A-Einträge auf das Synology NAS verweisen lassen, damit andere Mailserver das Synology NAS finden können.
2. Vergewissern Sie sich, dass das Synology NAS über eine statische IP-Adresse verfügt und mit dem Internet verbunden ist, oder dass Ihr Domainname korrekt auf Ihre dynamische IP-Adresse verweist.
3. Wenn das Synology NAS hinter einer NAT-Firewall oder einem Router liegt, müssen Sie überprüfen, ob die Portweiterleitung korrekt funktioniert. Die Funktion der Portweiterleitung können Sie auf der Website **CanYouSeeMe** überprüfen. Geben Sie Port 25 ein.
4. Falls eine E-Mail zurückgegeben wird, lesen Sie diese bitte, um detaillierte Ursachen für den Fehler zu erfahren.

Warum werden E-Mails an bestimmte Webmail-Konten wie z. B. Gmail oder Hotmail abgewiesen?

Viele kostenlose E-Mail-Anbieter überprüfen mittels Reverse DNS Lookup die Authentizität des Absenders. Wenn Ihr Reverse DNS Lookup nicht mit dem Domainnamen der sendenden Domain übereinstimmt, werden Ihre E-Mails abgewiesen. Wenden Sie sich hierzu an Ihren Internet-Serviceanbieter. Eine weitere Möglichkeit ist, dass Ihre IP-Adresse auf der Spam-Blockierungsliste steht. Dies können Sie unter **Spamhaus** nachprüfen.

Kapitel 3: E-Mail-Migration

Mit seinem integrierten Tool zur E-Mail-Migration unterstützt Sie MailPlus Server bei der unkomplizierten Migration von E-Mails von anderen Mailservern (z. B. Microsoft Exchange- und IMAP-Mailserver) und von externen Diensten (z. B. Gmail und Yahoo Mail).

In diesem Artikel erfahren Sie, wie Sie E-Mails von Microsoft Exchange auf MailPlus Server migrieren. Bitte achten Sie vor dem Beginn darauf, dass Sie bereits Folgendes ausgeführt haben:

- Überprüfen Sie, ob auf dem Synology NAS DSM 6.0 oder höher ausgeführt wird und MailPlus Server unterstützt wird (kompatible Modelle finden Sie **hier**).
- Richten Sie MailPlus Server auf dem Synology NAS ein, der als Ziel-Mailserver fungieren soll.
- Sammeln Sie die Benutzernamen und Kennwörter der Quellkonten und die entsprechenden MailPlus-Kontonamen.

Eine E-Mail-Migrationsaufgabe in MailPlus Server erstellen

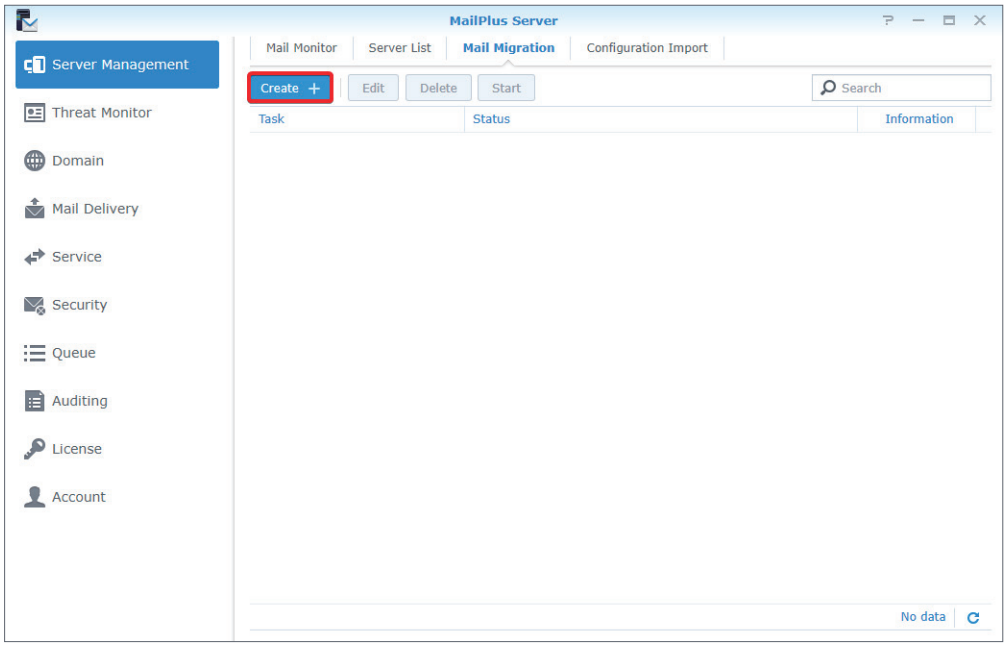
Melden Sie sich bei MailPlus Server an, gehen Sie zu **Server-Management** > **E-Mail-Migration** und klicken Sie auf die Schaltfläche **Erstellen**, um eine E-Mail-Migrationsaufgabe zu erstellen. In diesem Abschnitt dient Microsoft Exchange als Beispiel zur Veranschaulichung.

Anmerkung:

- Informationen zur Migration von E-Mails von anderen Quellen (z. B. Gmail oder Yahoo Mail) finden Sie in **diesem Hilfe-Artikel**.

Allgemeine Aufgabeneinstellungen konfigurieren

1. Gehen Sie zu **Server-Management** > **E-Mail-Migration** und klicken Sie auf die Schaltfläche **Erstellen**.

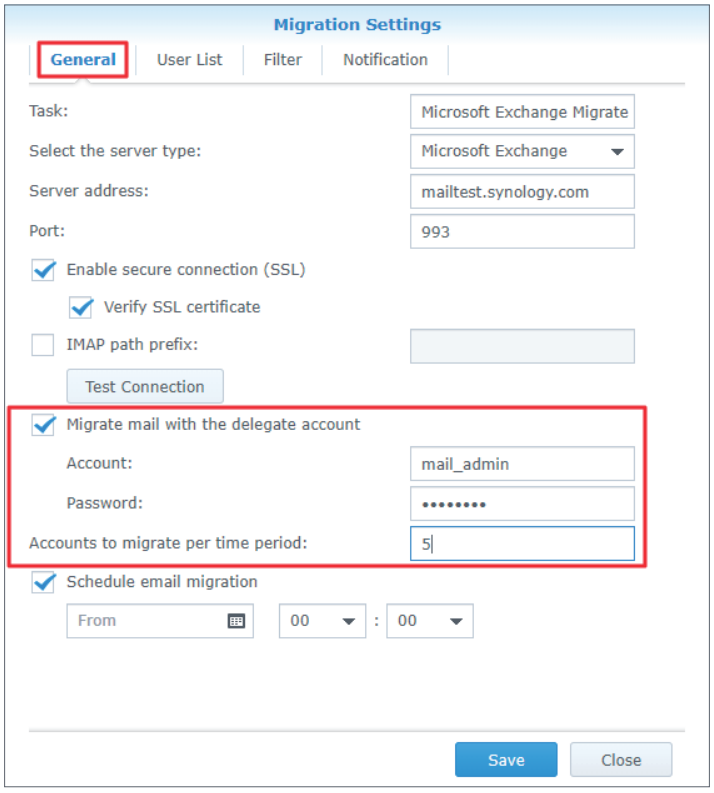


2. Gehen Sie im Fenster **Migrationseinstellungen** zur Registerkarte **Allgemein**, ändern Sie die Option **Servertyp auswählen** auf **Microsoft Exchange** und tragen Sie die erforderlichen Daten des Microsoft Exchange-Servers ein.

3. Das **IMAP-Pfad-Präfix** finden Sie in den Einstellungen des Microsoft Exchange-Servers.

4. Wenn Sie auf dem Quellserver über ein Stellvertreterkonto mit voller Zugriffsberechtigung auf alle anderen Quellkonten verfügen, wählen Sie **Mail mit dem Stellvertreterkonto migrieren** und tragen Sie die Anmeldeinformationen des Kontos ein. Mit diesem Konto können Sie E-Mails migrieren, ohne die Zugriffsberechtigungen für jedes Quellkonto einzuholen.

5. **Pro Zeitraum zu migrierende Konten** kann je nach Kapazität des Servers festgelegt werden.

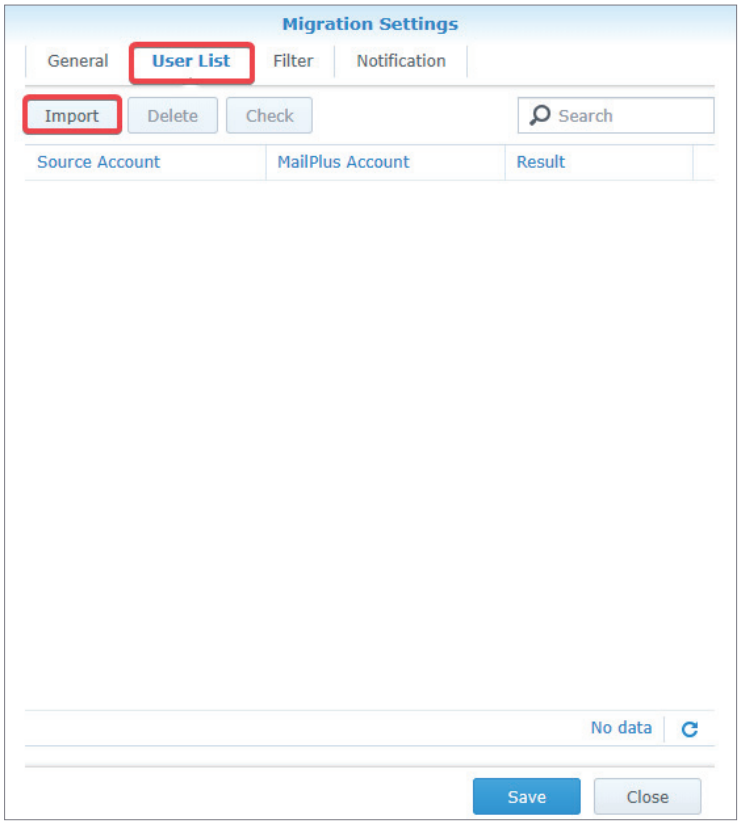


Eine Benutzerliste importieren

1. Erstellen Sie eine Benutzerliste, welche die folgenden Anforderungen erfüllt:
   - Erstellen Sie die Benutzerliste im CSV-Format mit Microsoft Excel, Google Sheets, usw.
   - In einer Zeile sollten jeweils die Informationen eines Benutzerkontos aufgeführt sein.
   - Listen Sie die folgenden Informationen für jeden Benutzer von links nach rechts auf: Quellkonto, Quellkonto-Kennwort und entsprechendes MailPlus Server-Konto.
   - Jede Art von Information sollte mit einem Komma (,) getrennt sein.
   - Wenn **Microsoft Exchange** als Quellserver-Typ gewählt wurde und **Mail mit dem Stellvertreterkonto migrieren** aktiviert ist, können Sie das Kennwort des Quellkontos weglassen (z. B. Quellkonto_X,,MailPlus_Server_Konto_X).
2. Eine gültige Benutzerliste sollte wie folgt aussehen:

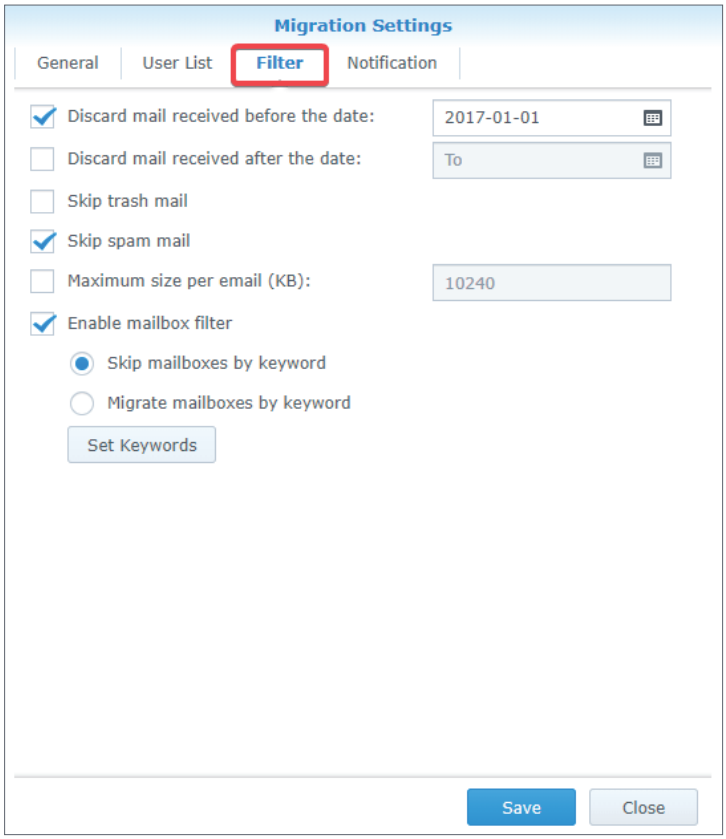
Quellkonto_1,Quellkonto_1_Kennwort,MailPlus_Server_Konto_1
Quellkonto_2,Quellkonto_2_Kennwort,MailPlus_Server_Konto_2
Quellkonto_3,Quellkonto_3_Kennwort,MailPlus_Server_Konto_3
...
Quellkonto_N,Quellkonto_N_Kennwort,MailPlus_Server_Konto_N

3. Gehen Sie zu **Benutzerliste**, wo Sie die Liste importieren können. Überprüfen Sie, ob alle Kontodaten korrekt sind.



E-Mail- und Postfachfilter einrichten

1. Auf der Registerkarte **Filter** können Sie Kriterien angeben, nach denen E-Mails oder Postfächer migriert oder übersprungen werden sollen.

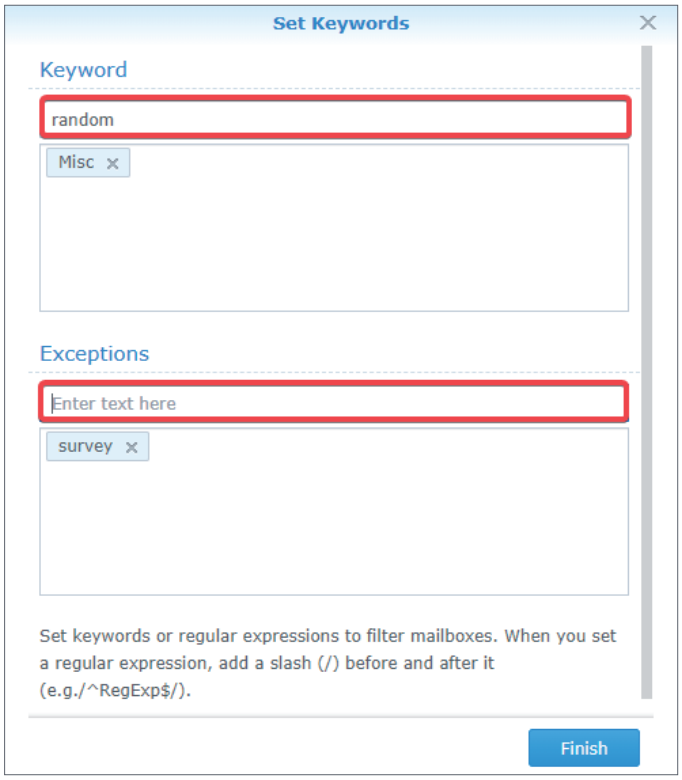


2. Um Postfächer nach Schlüsselwörtern zu filtern, aktivieren Sie das Kontrollkästchen **Postfachfilter aktivieren** und wählen Sie eine Filter-Richtlinie (**Postfächer nach Schlüsselwort überspringen** oder **Postfächer nach Schlüsselwort migrieren**).

3. Klicken Sie auf **Schlüsselwort festlegen** und geben Sie einen Text in die folgenden Bereiche ein:

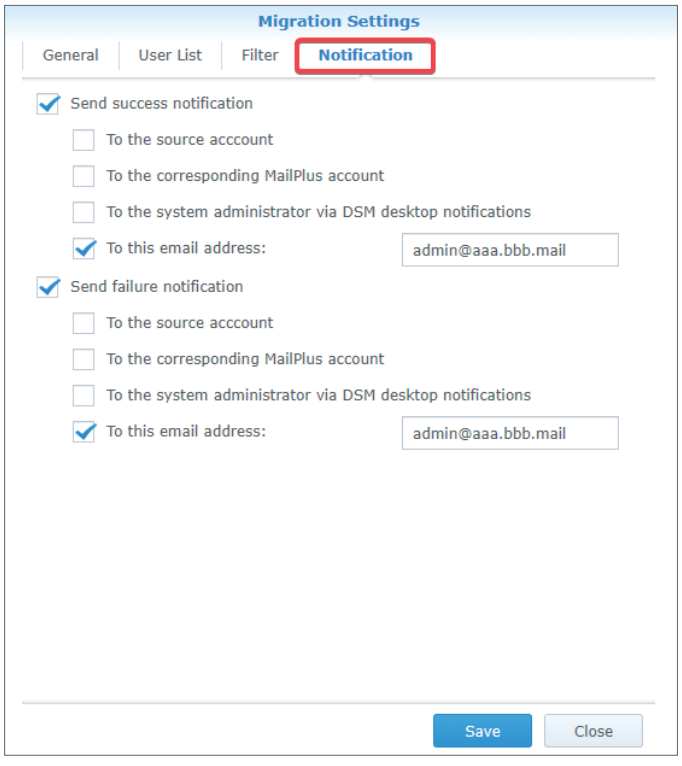
   - **Schlüsselwort**: Geben Sie hier Text ein, damit übereinstimmende Postfächer gemäß der gewählten Filter-Richtlinie verarbeitet werden.
   - **Ausnahmen**: Geben Sie hier Text ein, damit übereinstimmende Postfächer nicht verarbeitet werden.

4. Sie können reguläre Ausdrücke in beide Bereiche, innerhalb von Schrägstrichen (/), eingeben (z. B. /REGULÄRER_AUSDRUCK/).



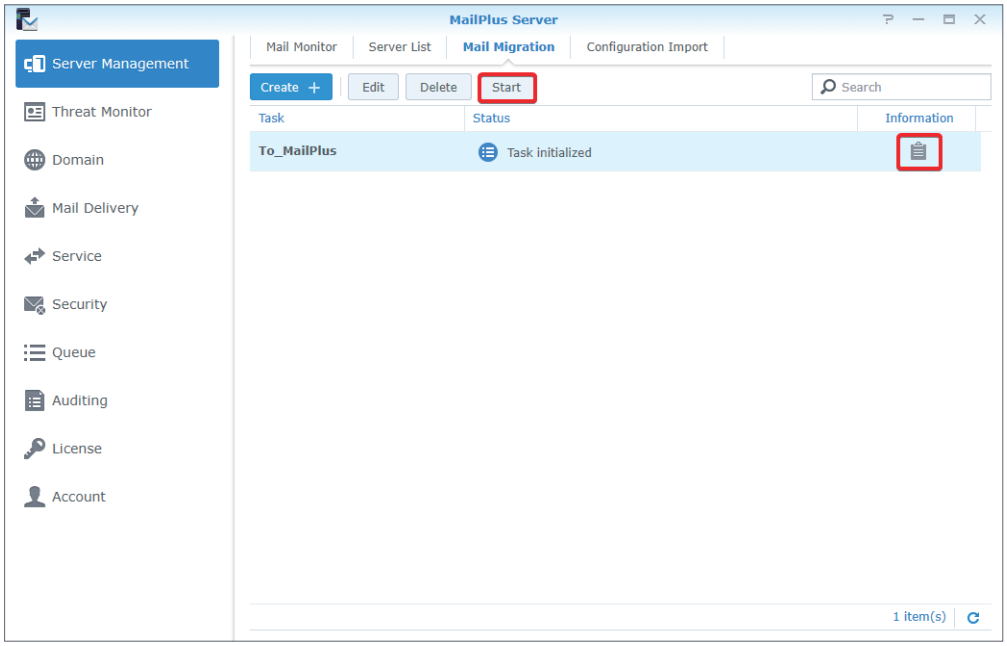
Migrationsbenachrichtigungen einrichten

1. Damit Benachrichtigungen übermittelt werden können, stellen Sie sicher, dass **SMTP aktivieren** (unter **Dienst**) in MailPlus Server aktiviert ist.
2. Auf der Registerkarte **Benachrichtigung** können Sie angeben, ob MailPlus Server Benachrichtigungen über die Ergebnisse jeder Kontomigration schicken soll und wo der Administrator sie erhalten soll.

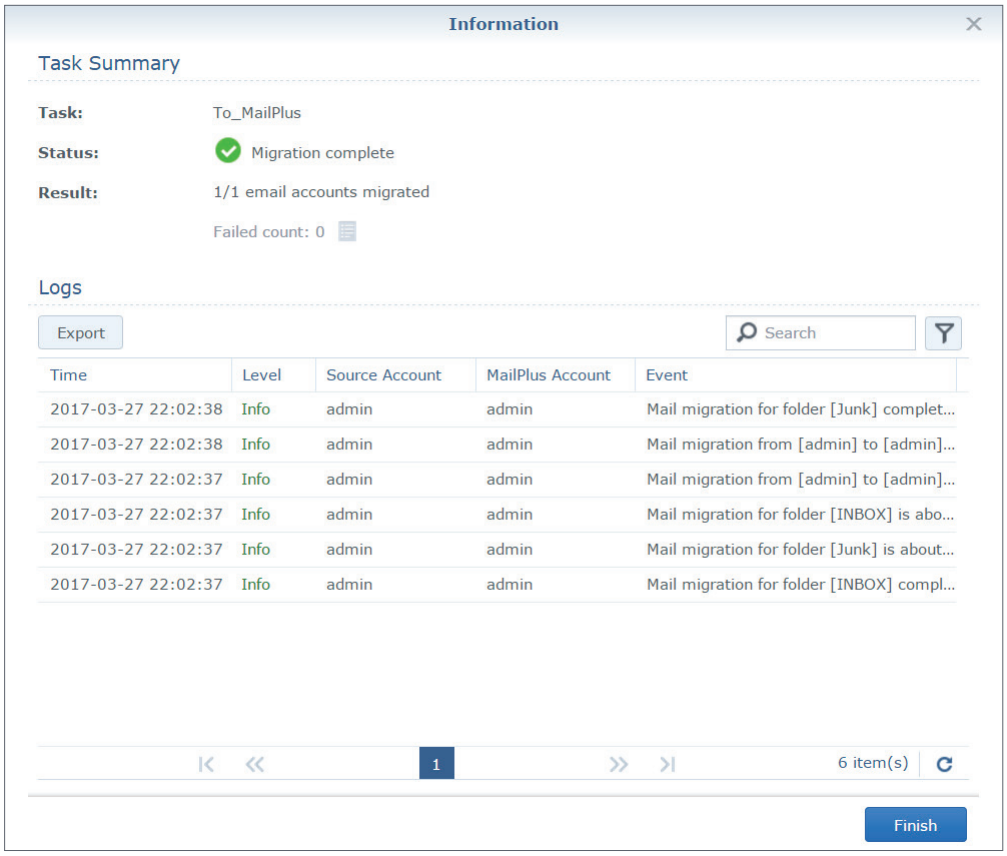


Eine E-Mail-Migrationsaufgabe ausführen

1. Unter **Server-Management** > **E-Mail-Migration** können Sie eine Migrationsaufgabe auswählen und auf **Start** klicken, um diese auszuführen. Um Migrationsfehler zu vermeiden, sollten Sie weder die IMAP/POP3-Einstellungen in MailPlus Server ändern noch E-Mails auf dem Quell-Mailserver verschieben oder löschen.



2. Klicken Sie auf **Informationen** (das Dokumentsymbol), um Migrationsstatistiken und -protokolle anzuzeigen.

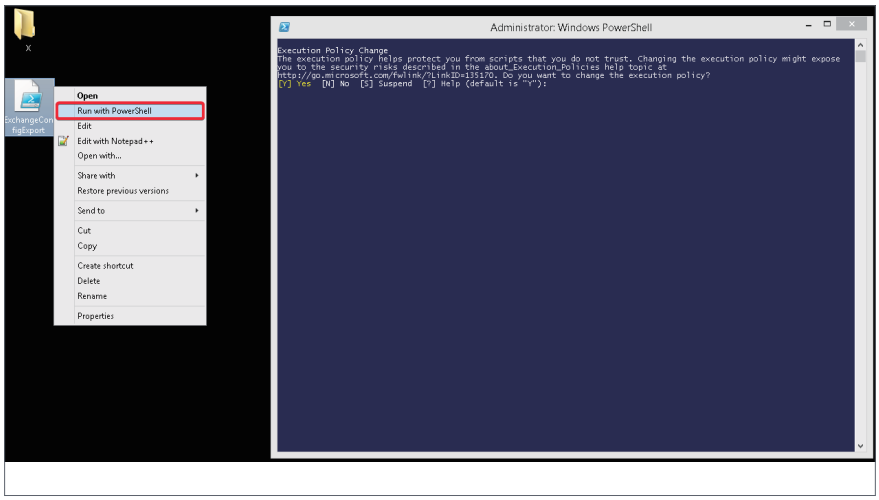


Importieren von Systemkonfigurationen von Microsoft Exchange in MailPlus Server

Sie können Systemkonfigurationen und Aliasnamen von einem Microsoft Exchange-Server exportieren und anschließend zu MailPlus Server importieren, um diese weiterhin zu verwenden.

Systemkonfigurationen und Aliasnamen von Microsoft Exchange exportieren

1. Laden Sie die Skriptdatei (**ExchangeConfigExport.ps1**) **hier** herunter.
2. Melden Sie sich als Systemadministrator auf einem Windows-Computer an, auf dem der Microsoft Exchange-Server ausgeführt wird.
3. Verschieben Sie die Skriptdatei auf den Windows-Computer.
4. Führen Sie über die Windows PowerShell die Skriptdatei auf dem Microsoft Exchange-Server aus.

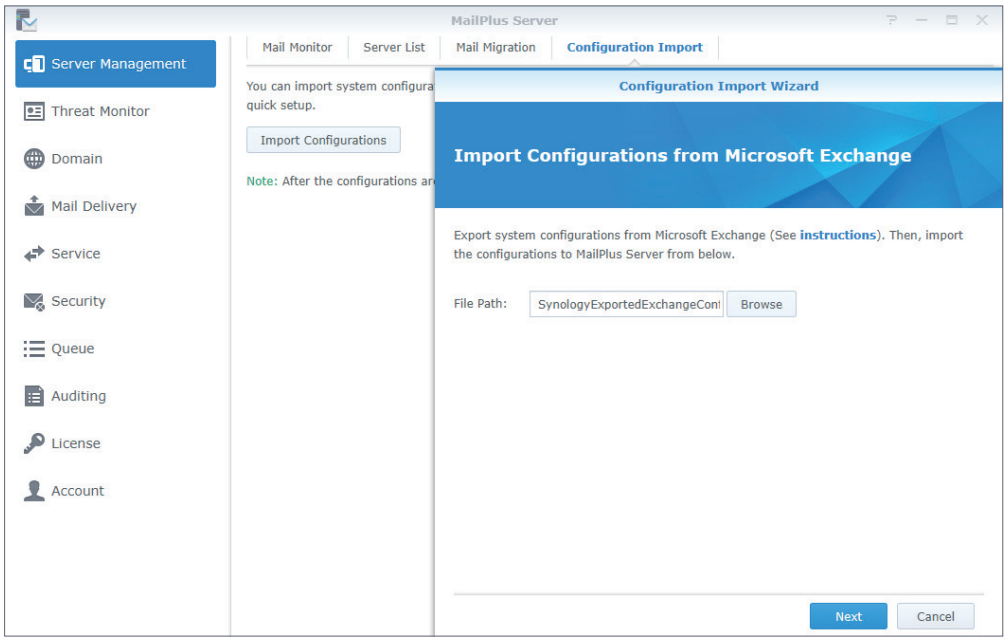


5. Wenn Sie bezüglich der Änderung der Ausführungsrichtlinie gefragt werden, wählen Sie **Ja**, um die Ausführung des Skripts zuzulassen.
6. Bei Abschluss der Ausführung exportiert der Microsoft Exchange-Server die Systemkonfigurationen in eine Datei namens **SynologyExportedExchangeConf.xml** und die Aliasnamen in eine Datei namens **SynologyExportedAlias.txt**.

7. Verschieben Sie die erstellte .xml-Datei und .txt-Datei auf Ihren lokalen Computer.

Systemkonfigurationen in MailPlus Server importieren

1. Starten Sie den Importvorgang wie folgt:
   - Wenn MailPlus Server erst initialisiert wird: Starten Sie MailPlus Server und wählen Sie **Neues E-Mail-System durch Importieren der Konfigurationen von Microsoft Exchange erstellen**.
   - Wenn MailPlus Server bereits initialisiert wurde: Starten Sie MailPlus Server und gehen Sie zu **Server-Management** > **Konfigurations-Import** > **Konfigurationen importieren**.
2. Klicken Sie auf **Durchsuchen**, um die Datei **SynologyExportedExchangeConf.xml** von Ihrem lokalen Computer zu importieren.



3. Klicken Sie auf Weiter, um die Konfigurationsdaten unter **Allgemeine Einstellungen** (z. B. SMTP- und Sicherheitseinstellungen) und **Kriterien** (z. B. Blacklist und Whitelist) zu überprüfen. Klicken Sie auf **Importieren**.

Kapitel 4: Benutzerlizenzen

Für die Ausführung von MailPlus Server sind genügend Lizenzen erforderlich. Die Anzahl der erforderlichen Lizenzen wird von der Anzahl der zu aktivierenden Konten bestimmt. MailPlus Server beinhaltet standardmäßig fünf kostenlose E-Mail-Konten. Sie können je nach Bedarf weitere Konten hinzufügen, indem Sie zusätzliche Lizenzen erwerben.

Die Anzahl der Lizenzbenutzer ist von den nachstehenden Punkten nicht betroffen:

- **Deaktivierte Konten**: Beispiel: Die Lizenz eines ehemaligen Mitarbeiters kann auf einen neuen Mitarbeiter übertragen werden.
- **E-Mail-Alias**: Jeder Benutzer kann ohne Zusatzkosten Aliasnamen hinzufügen, da Alias-E-Mail-Adressen mit bestehenden Benutzerkonten verbunden sind.
- **Mehrere Domains (einschließlich weiterer Domains)**: Da MailPlus Server mehrere Domains verarbeiten kann, erfordert die Verwendung mehrerer Domains keine zusätzlichen Lizenzen.
- **DSM-Benutzer, die nicht zum angegebenen Kontotyp gehören**: Beispiel: Wenn der Kontotyp auf LDAP-Benutzer eingestellt ist, gelten lokale Benutzer nicht als Lizenzbenutzer.

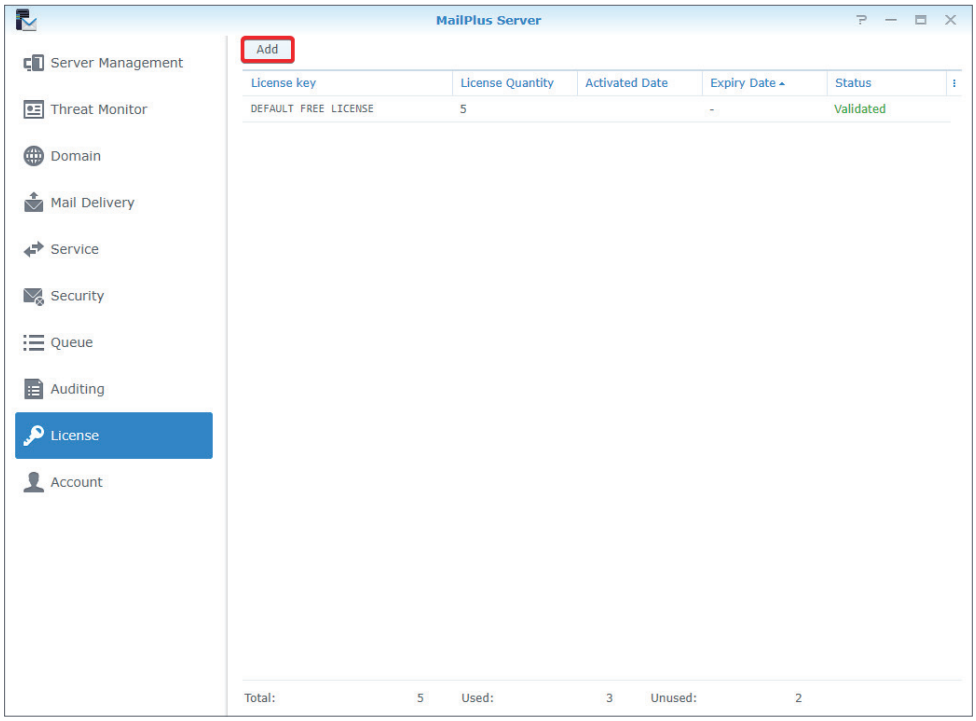
Lizenzen kaufen

Lizenzpakete für MailPlus enthalten fünf oder 20 Einheiten von E-Mail-Konten und können bei **Vertragshändlern von Synology** erworben werden. Weitere Informationen über Lizenzpakete für MailPlus finden Sie auf der **Lizenzseite von MailPlus**.

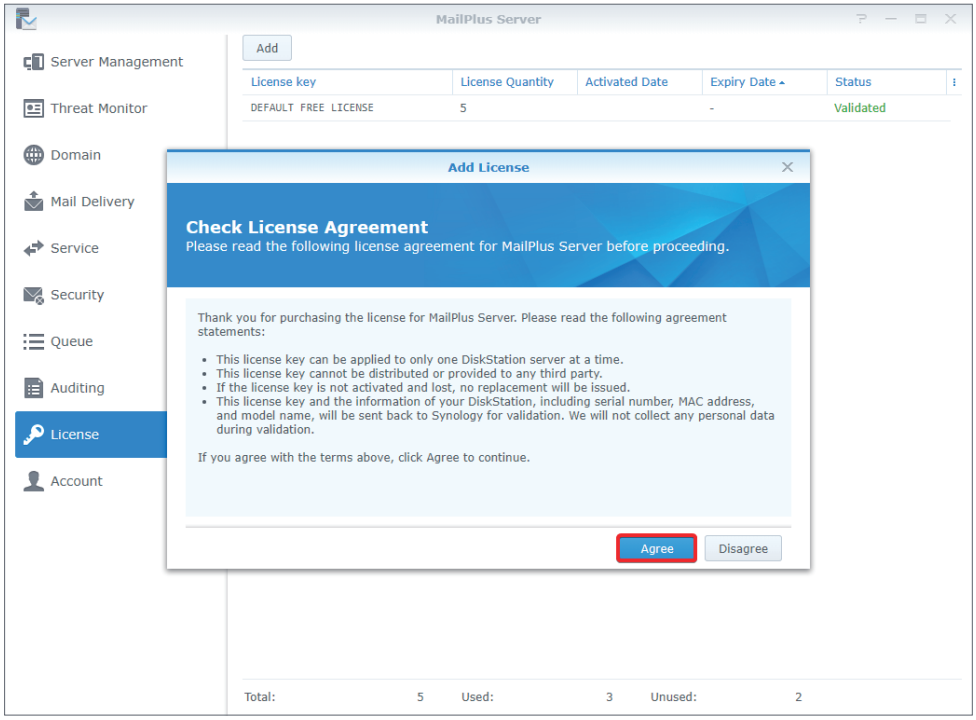
Lizenzen installieren

Gekaufte Lizenzen müssen installiert werden, um E-Mail-Konten zu aktivieren. Gehen Sie hierzu wie folgt vor:

1. Gehen Sie zu **Lizenz** und klicken Sie auf die Schaltfläche **Hinzufügen**, um Lizenzen hinzuzufügen.



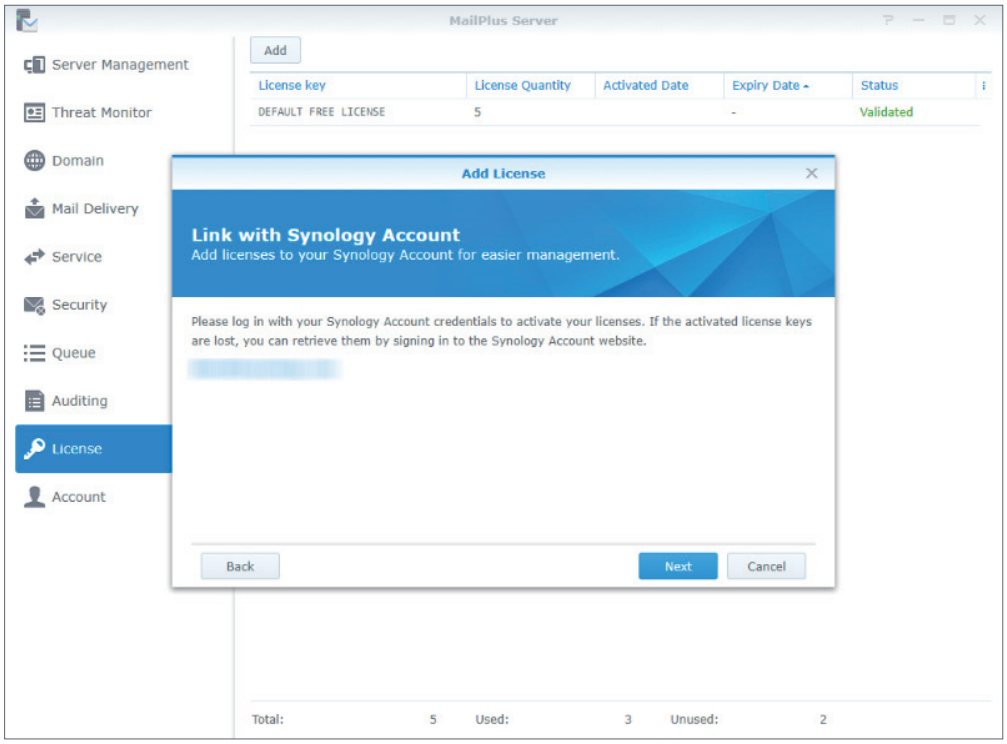
2. Lesen Sie im Fenster **Lizenz hinzufügen** die Lizenzvereinbarung für MailPlus Server aufmerksam durch. Nach Überprüfung und Bestätigung des Inhalts klicken Sie auf **Zustimmen**.



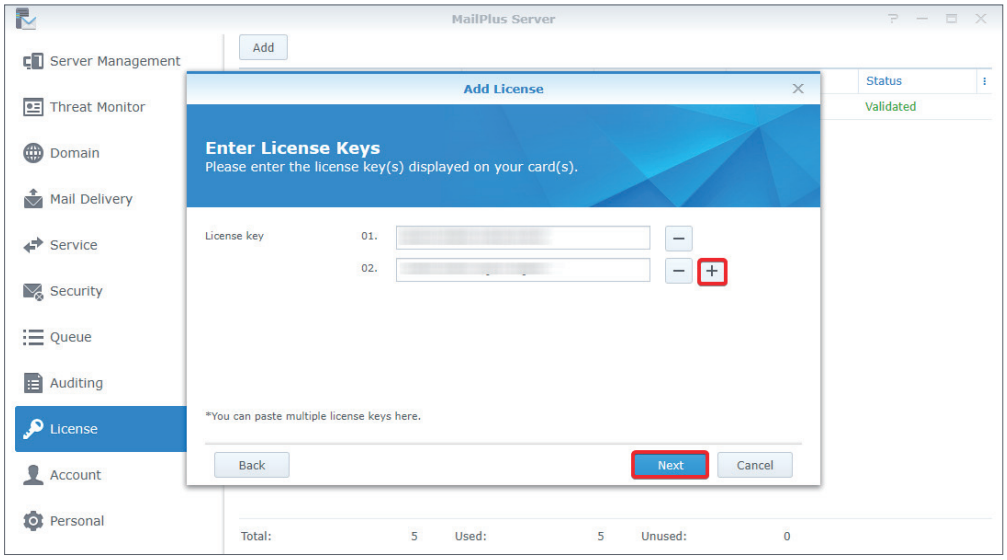
3. Melden Sie sich beim Synology-Konto an und klicken Sie auf **Weiter**.

Anmerkung:

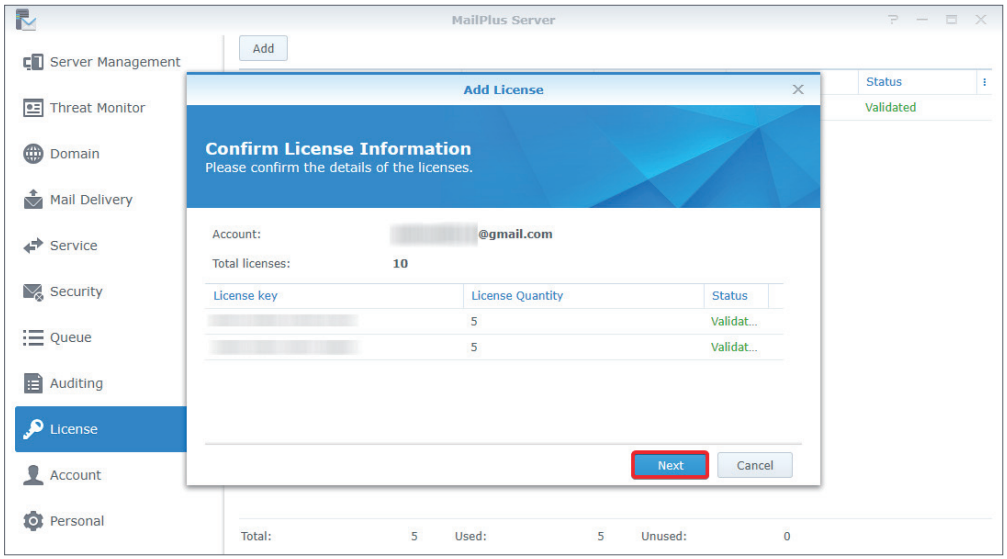
- Sollten Lizenzen nach der Aktivierung nicht abgerufen werden können, melden Sie sich beim **Synology-Konto** an, um eine technische Support-Anfrage zu übermitteln.



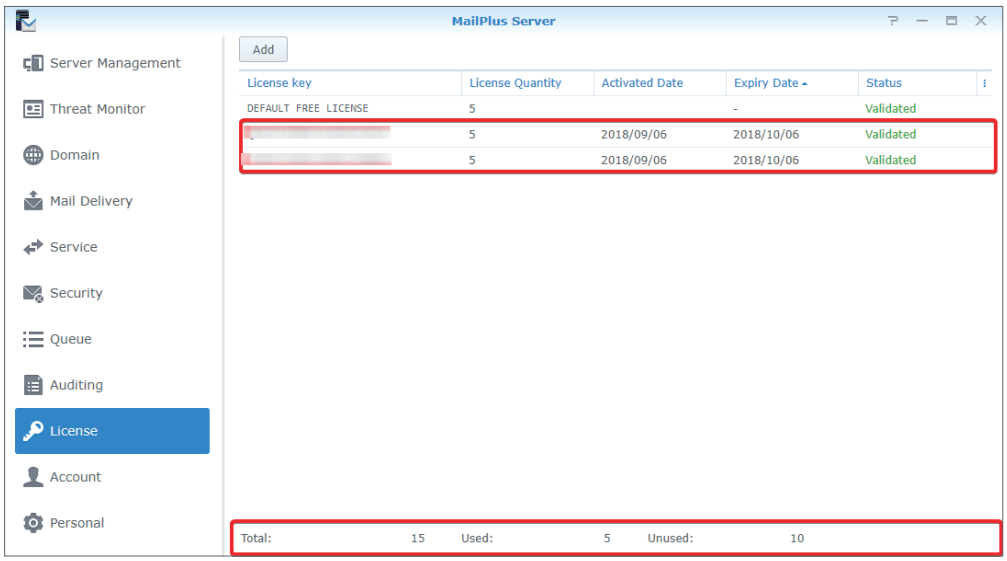
4. Geben Sie die Lizenznummer in das Feld **Lizenzschlüssel** ein, wie unten abgebildet. Wenn Sie mehr als eine Lizenz hinzufügen müssen, klicken Sie auf das Plus-Symbol (+), um weitere Felder hinzuzufügen.



5. Überprüfen und bestätigen Sie, ob die Anzahl der zu installierenden Lizenzen und ihre jeweiligen Lizenzschlüssel korrekt sind. Nachdem Sie die Korrektheit der Informationen bestätigt haben, klicken Sie auf **Weiter**, um das Hinzufügen von Lizenzen abzuschließen.



6. Nachdem Sie Lizenzen hinzugefügt haben, können Sie zur Seite **Lizenz** wechseln, um die Details und den Status jeder Lizenz zu überprüfen:
   - Lizenzschlüssel
   - Anzahl der von jeder Lizenz bereitgestellten E-Mail-Konten
   - Aktivierungsdatum der Lizenz
   - Ablaufdatum der Lizenz
   - Status der Lizenzgültigkeit
7. Zudem können Sie unten auf der Seite **Lizenz** die gesamte Anzahl der Lizenzen anzeigen, die auf MailPlus Server installiert sind, sowie die Anzahl der benutzten und nicht benutzten Lizenzen.



Lizenzen nutzen

Nach dem Hinzufügen der Lizenzen können Sie zu **Konto** > **Benutzer** wechseln, um auszuwählen, welche Konten aktiviert werden sollen. Ausführliche Anweisungen finden Sie unter **Konten aktivieren**.

Kapitel 5: Kontoeinstellungen

Kontosystem

MailPlus Server verwendet dasselbe Kontosystem wie DSM, daher können Sie Benutzerkonten in MailPlus Server von bestehenden Benutzerkonten in DSM aktivieren.

Zusätzlich zur Aktivierung von Benutzerkonten lokaler Benutzer können Sie Benutzerkonten von LDAP-/Domain-Benutzern aktivieren (gehen Sie zu **DSM** > **Systemsteuerung** > **Domain/LDAP**, um LDAP- und Domain-Konten anzubinden). DSM kann jedoch nicht mehr als einen Verzeichnisdienst gleichzeitig synchronisieren; daher kann MailPlus Server ebenfalls nicht mehr als einen Verzeichnisdienst und ein Kontosystem gleichzeitig synchronisieren.

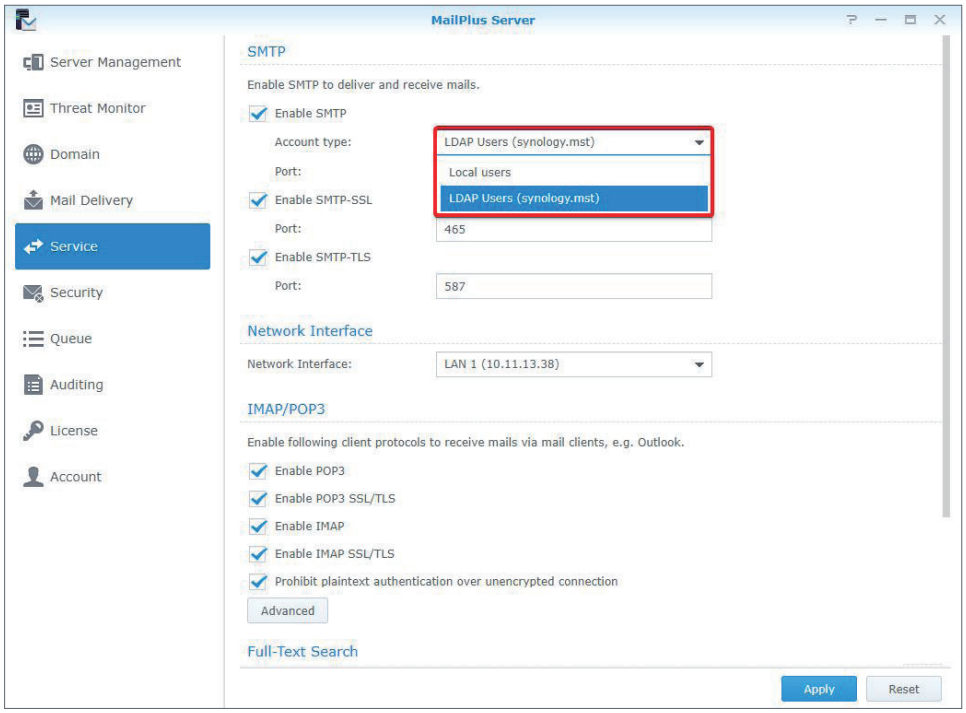
Anmerkung:

- MailPlus Server kann jeweils nur einen der folgenden Kontotypen verwenden: **Lokal**, **LDAP** oder **Domain**.

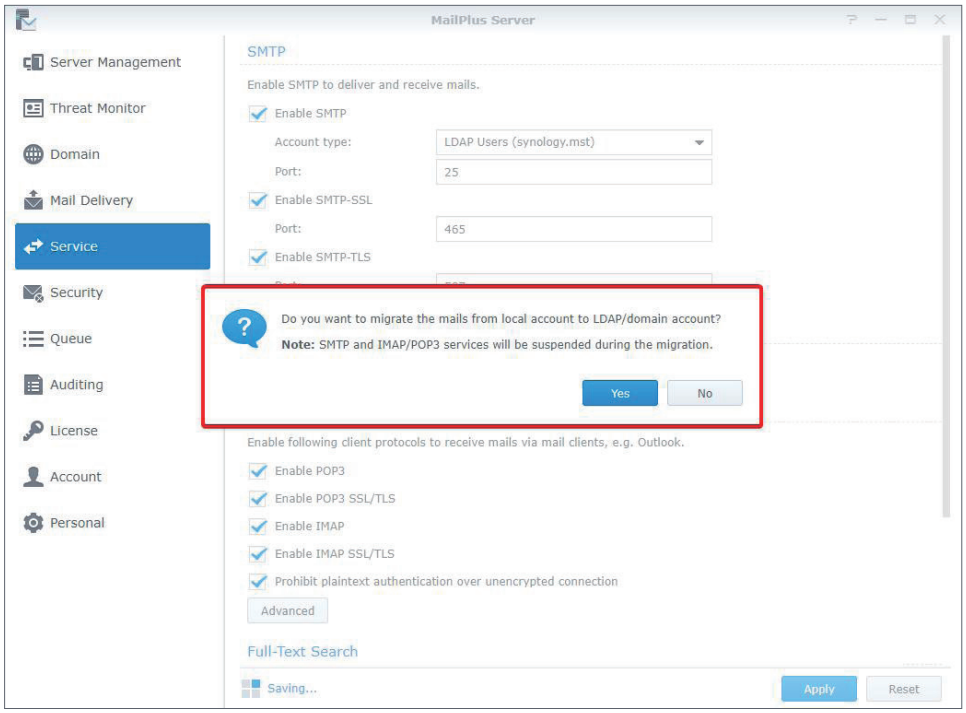
Kontotyp ändern

Gehen Sie wie folgt vor, um den Kontotyp zu ändern:

1. Melden Sie sich bei Ihrem DSM an.
2. Gehen Sie zu **Systemsteuerung** > **Domain/LDAP**, um sich an einen bestimmten Verzeichnisdienst anzubinden. Wenn Sie **Lokale Benutzer** als Kontotyp verwenden, können Sie diesen Schritt überspringen.
3. Starten Sie **MailPlus Server**.
4. Gehen Sie zu **Dienst**, um einen Kontotyp aus dem Dropdown-Menü **Kontotyp** auszuwählen. (in diesem Bereich wird nur der auf DSM konfigurierte Verzeichnisdienst angezeigt.)



5. Klicken Sie auf **Übernehmen**, um Benutzerkonten vom Verzeichnisdienst zu importieren. Wie nachstehend abgebildet, wird ein Warnhinweis eingeblendet, wenn Sie von **Lokale Benutzer** zu **LDAP-Benutzer** oder **Domainbenutzer** wechseln und auf **Übernehmen** klicken.



Anmerkung:

- Da unterschiedliche Kontotypen unterschiedliche E-Mail-Adressen aufweisen, können E-Mails von verschiedenen Kontotypen nicht gemeinsam genutzt werden. Wenn Sie E-Mails von **Lokale Benutzer** zu **LDAP-Benutzer** oder **Domainbenutzer** migrieren möchten, klicken Sie auf **Ja**. Das System migriert nur E-Mails zu Verzeichnisdienst-Konten, die dieselben Benutzernamen wie lokale Benutzer aufweisen. Konten mit unterschiedlichen Benutzernamen werden automatisch ignoriert.

Konten aktivieren

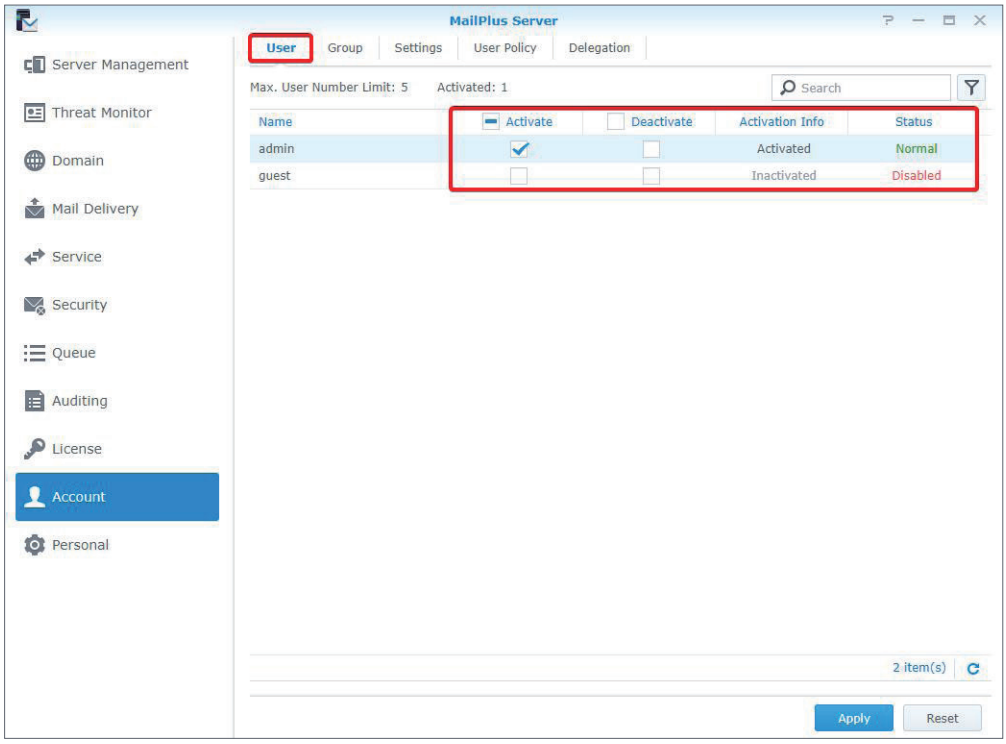
Sie müssen Benutzerkonten in MailPlus Server aktivieren, um E-Mail-Dienste verwenden zu können, wie beim Senden und Empfangen von E-Mails. Sie benötigen daher genügend Lizenzen, um die Konten zu aktivieren, die E-Mail-Dienste nutzen. Weitere Informationen finden Sie im Abschnitt **Benutzerlizenzen**.

Wenn Sie bereits einige Benutzerkonten aktiviert haben, und diese Benutzer sich nicht bei DSM anmelden oder MailPlus / MailPlus Server nicht starten können, überprüfen Sie bitte, ob Sie einzelne Benutzerkonten deaktiviert haben und ob diese Benutzerkonten über Berechtigungen für MailPlus oder MailPlus Server verfügen. Weitere Informationen über Client-Anmeldeprobleme finden Sie in **diesem Artikel**.

Benutzerkonten aktivieren

Die Aktivierung von Benutzerkonten erfordert eine ausreichende Anzahl an Lizenzen. Weitere Anweisungen finden Sie im Abschnitt **Benutzerlizenzen**. Gehen Sie wie folgt vor, um Benutzerkonten zu aktivieren:

1. Gehen Sie zu **Konto** > **Benutzer**.
2. Wählen Sie die Benutzer aus, die Sie aktivieren möchten. Wenn die Kontrollkästchen unter den Spalten **Aktivieren** und **Deaktivieren** für einen bestimmten Benutzer nicht aktiviert sind, wird der Status dieses Benutzers als Standardstatus festgelegt. Weitere Details finden Sie unter **Standardstatus**. Nach Markierung des Kontrollkästchens **Aktivieren** wird die Anzahl der verfügbaren Lizenzen verringert.



3. In der Spalte **Aktivierungs-Info** wird angezeigt, ob eine Lizenz für den Benutzer übernommen wurde.

4. In der Spalte **Status** wird der Status von DSM-Benutzern wie folgt angezeigt: **Normal**, **Deaktiviert** und **Benutzername nicht unterstützt**.

Anmerkung:

- Benutzer können E-Mail-Dienste nur ordnungsgemäß verwenden, wenn ein Konto unter **Aktivierungs-Info** mit **Aktiviert** und unter **Status** mit **Normal** bezeichnet ist. Die Kontoeinstellung kann als einziger Eintrag in der MailPlus-Berechtigung stehen, ohne die Einstellungen in der **Systemsteuerung** zu ändern.

5. Klicken Sie auf **Übernehmen**, um Benutzer zu aktivieren.

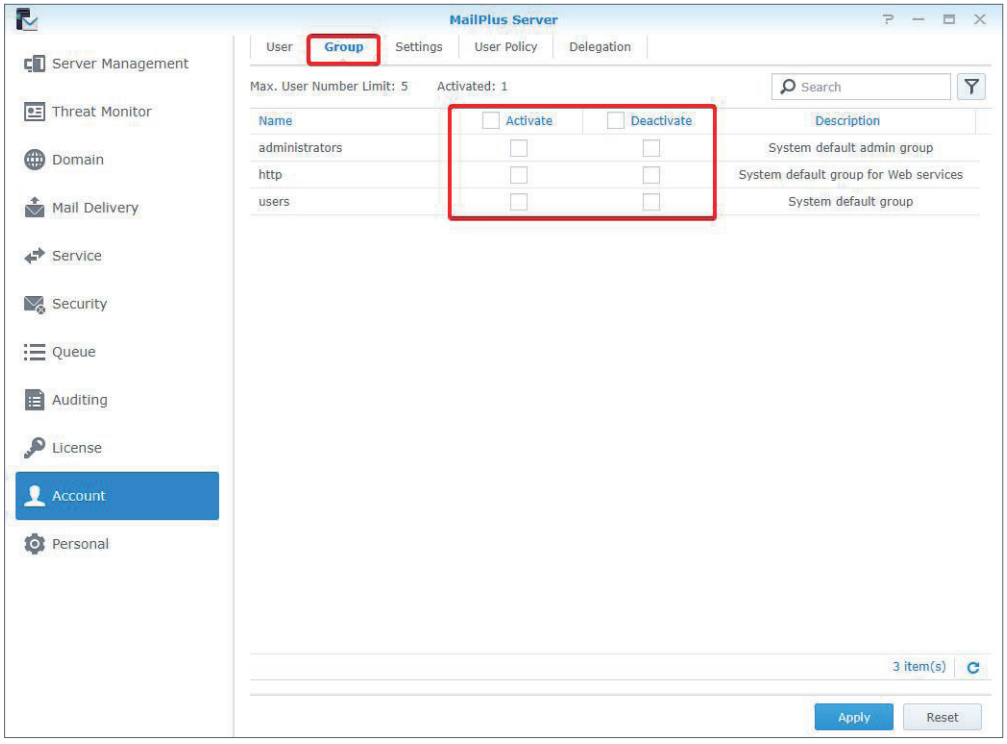
Gruppen aktivieren

Hier können Sie Benutzergruppen auf einfache Weise aktivieren und deaktivieren. Die Einstellungen werden für alle Mitglieder innerhalb derselben Gruppe übernommen. Gehen Sie hierzu wie folgt vor:

1. Gehen Sie zu **Konto** > **Gruppe**, um eine Gruppe zu aktivieren oder zu deaktivieren.

Anmerkung:

- Die absteigende Reihenfolge der Priorität für die Bestimmung des zuletzt aktivierten Benutzerkontos lautet wie folgt: Einstellungen für **Benutzer**, Einstellungen für **Gruppe** und Einstellungen für **Standard**.



2. Klicken Sie auf **Übernehmen**, um Benutzer innerhalb der Gruppe zu aktivieren.

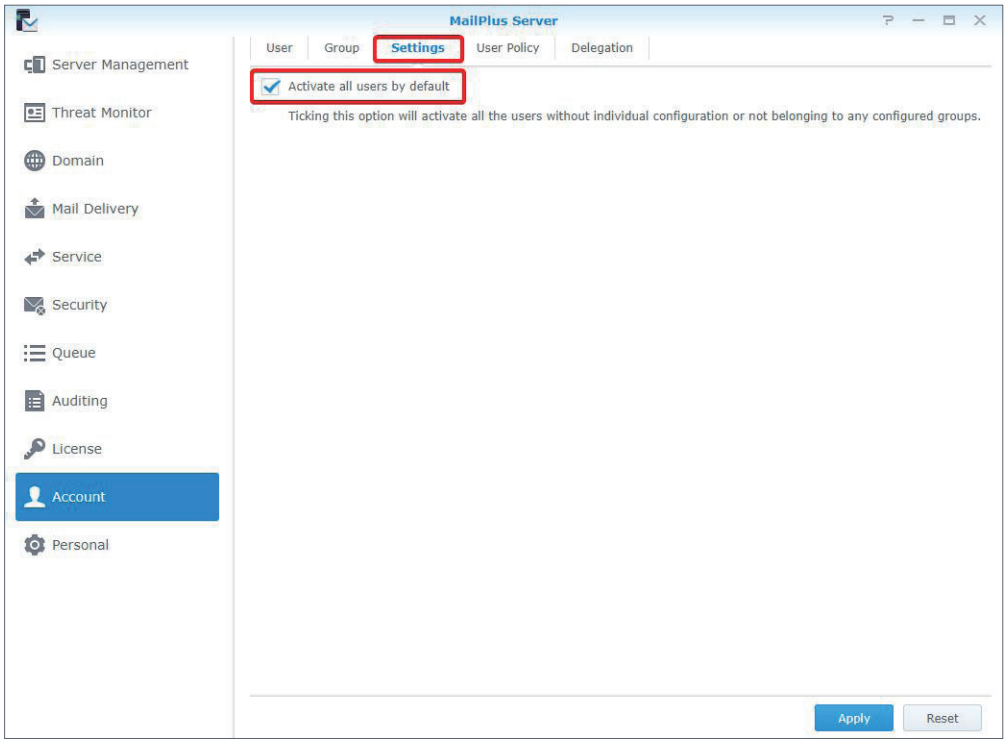
Standardstatus

Sie können den Standardstatus auf der Registerkarte **Einstellungen** auf der Seite **Konto** anpassen. Die Einstellungen des Standardstatus werden für Benutzerkonten mit dem Status **Normal** übernommen, die nicht aktiviert oder deaktiviert wurden. Gehen Sie hierzu wie folgt vor:

1. Gehen Sie zu **Konto** > **Einstellungen** und wählen Sie aus, ob das Kontrollkästchen **Standardmäßig alle Benutzer aktivieren** markiert werden soll.

Anmerkung:

- Die standardmäßige Aktivierung kann eine große Anzahl von Lizenzen verwenden. Bitte vergewissern Sie sich, ob Sie über genügend Lizenzen verfügen.

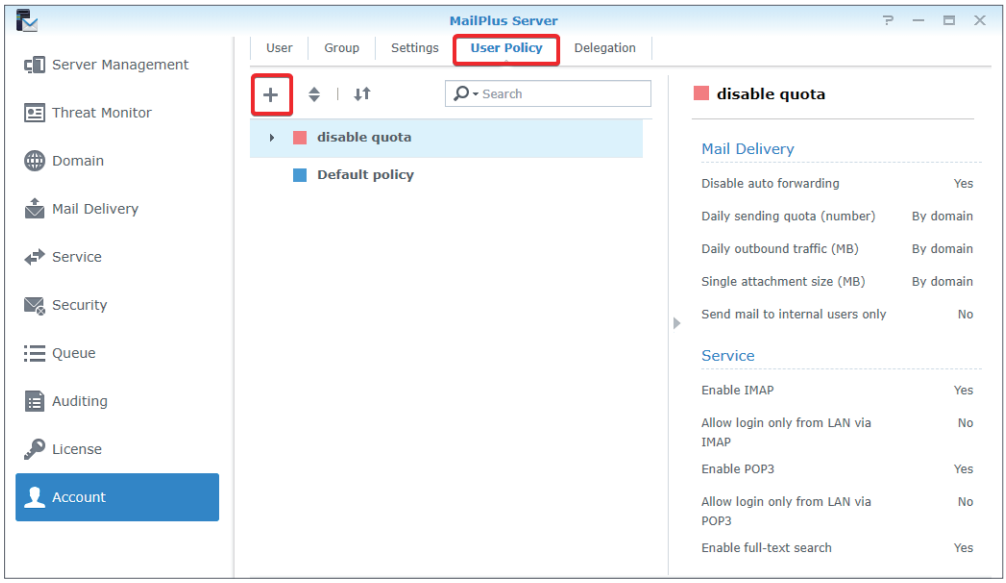


2. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Benutzerrichtlinien erstellen

Nach der Aktivierung von Benutzern oder Gruppen können Sie je nach Bedarf dedizierte E-Mail-Dienst-Richtlinien für bestimmte Benutzer oder Gruppen erstellen. Gehen Sie wie folgt vor, um Benutzerrichtlinien zu erstellen:

1. Gehen Sie zu **Konto** > **Benutzerrichtlinie**.
2. Klicken Sie auf das Plus-Symbol (+), um eine neue Richtlinie zu erstellen.

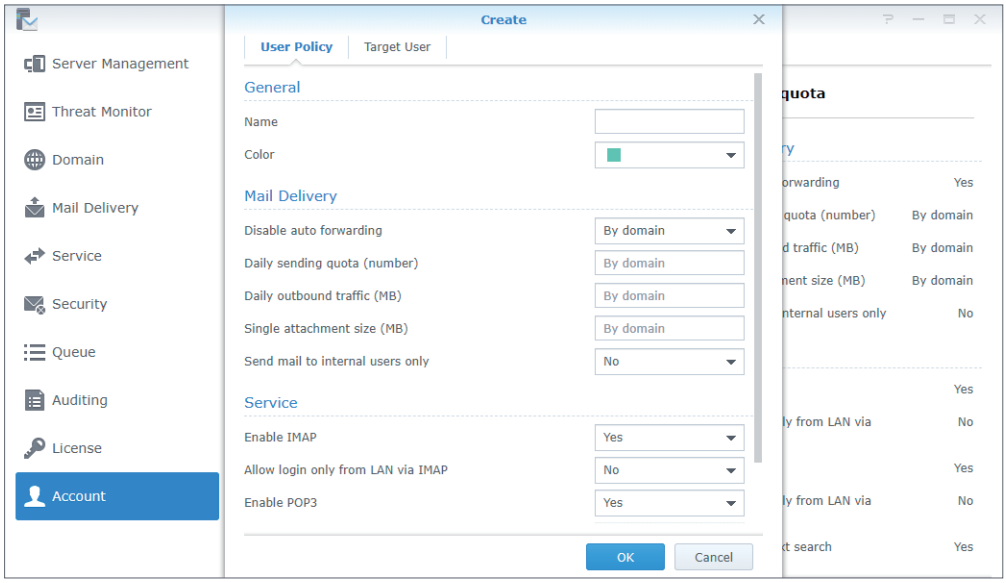


3. Gehen Sie im Fenster **Erstellen** zu **Benutzerrichtlinie**, und geben Sie in das Feld **Name** eine Bezeichnung für die Richtlinie ein.

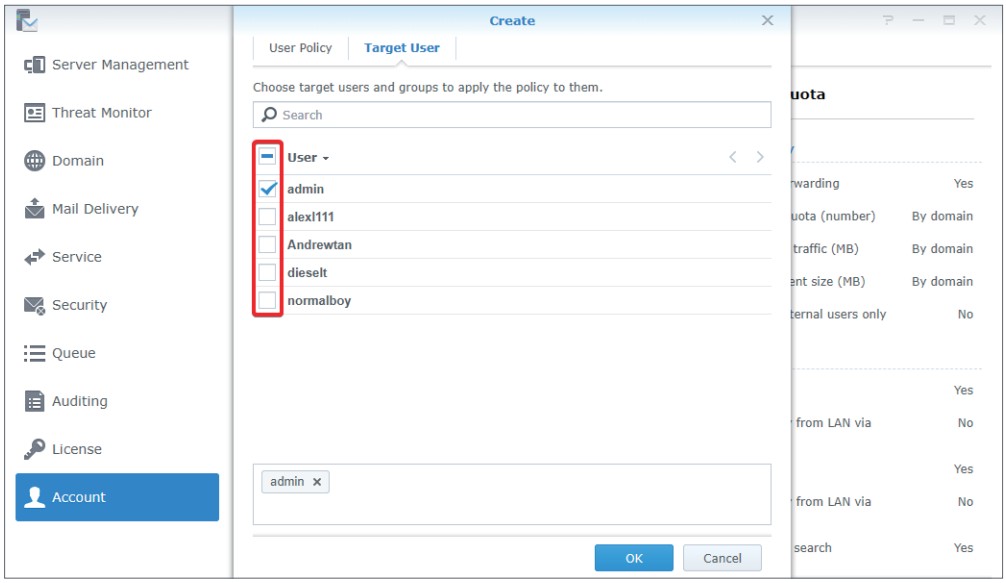
4. Wählen Sie im Dropdown-Menü **Farbe** eine Farbe für die Richtlinie aus, um diese besser zu erkennen.

Anmerkung:

- Details über Richtlinieninformationen finden Sie unter **Richtlinieninformationen und Beschränkungen**.

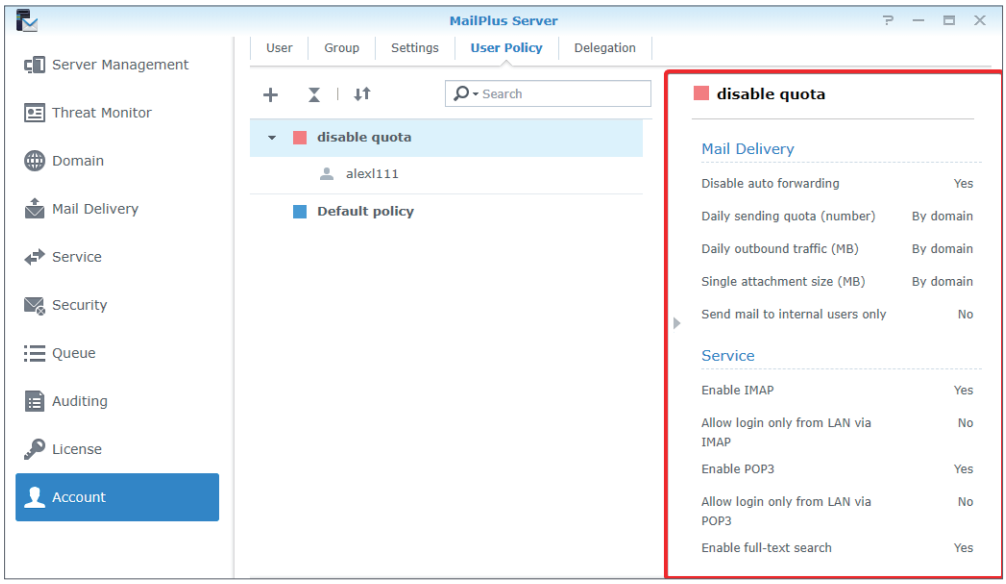


5. Wechseln Sie zur Registerkarte **Zielbenutzer** und wählen Sie einen Benutzer oder eine Gruppe aus, für den bzw. die die Richtlinie gelten soll. Sie können die gewünschten Benutzer oder Gruppen auch mit der Suchleiste oben im Fenster finden.



6. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

7. Nachdem eine Richtlinie erstellt wurde, wird sie auf der Seite **Benutzerrichtlinie** aufgeführt. Wählen Sie eine Richtlinie aus, um Details und Einstellungen der Richtlinie im rechten Bereich der Seite anzuzeigen.



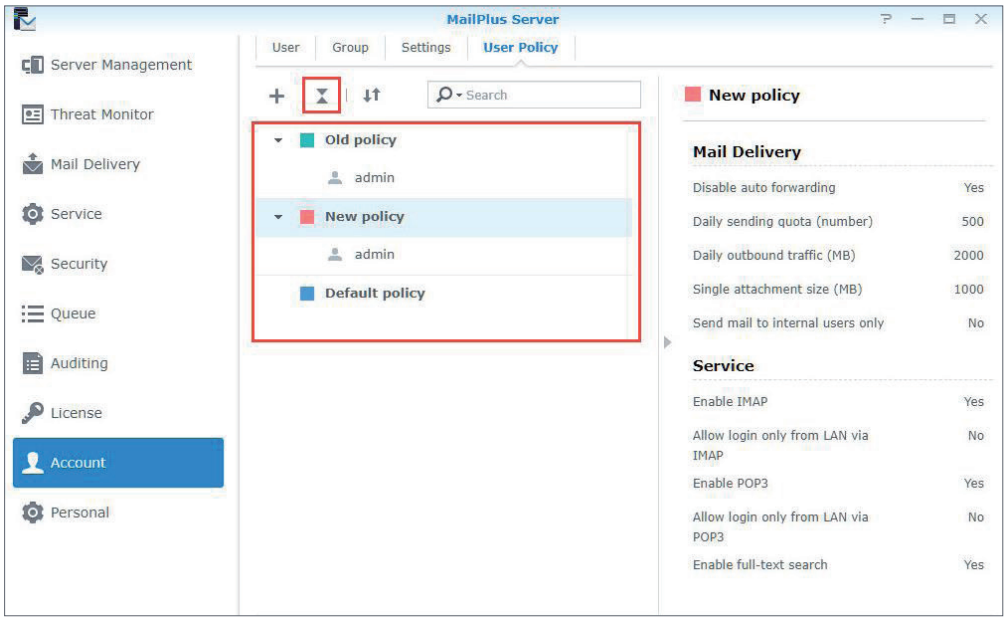
Priorität von Benutzerrichtlinien ändern

Es können mehrere Benutzerrichtlinien auf einen Benutzer angewendet werden; es ist jedoch nur eine Richtlinie wirksam. Welche Richtlinie wirksam ist, hängt von den Prioritätseinstellungen der Benutzerrichtlinien ab. Gehen Sie wie folgt vor, um die Priorität einer Benutzerrichtlinie zu ändern:

1. Gehen Sie zu **Konto** > **Benutzerrichtlinie** und klicken Sie auf das doppelte Dreiecksymbol, um Zielbenutzer/-gruppen anzuzeigen oder auszublenden.

2. Höher platzierte Richtlinien haben eine größere Priorität als niedriger platzierte Richtlinien. (in der nachstehenden Abbildung lautet die Priorität in absteigender Reihenfolge

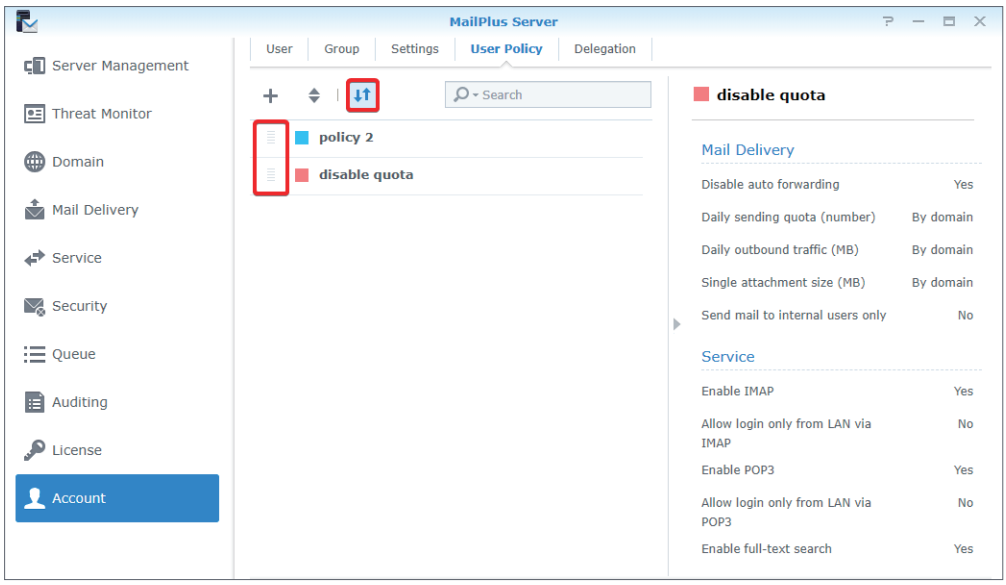
beispielsweise wie folgt: ***Alte Richtlinie***, ***Neue Richtlinie***, ***Standardrichtlinie***. Daher wird ***Alte Richtlinie*** anstatt ***Neue Richtlinie*** auf den Administrator angewendet.)



3. Klicken Sie auf das Symbol mit den beiden Pfeilen, um die Priorität der Richtlinie zu ändern.

Anmerkung:

- Wenn Sie eine bestimmte Richtlinie auf einen Benutzer anwenden möchten, achten Sie darauf, dass diese Richtlinie eine höhere Priorität als andere Richtlinien hat.



4. Bewegen Sie den Mauszeiger zur linken Seite der Richtlinie und ziehen Sie sie entsprechend Ihrer gewünschten Reihenfolge an die richtige Position.

5. Klicken Sie auf das Symbol mit den beiden Pfeilen, um die Drag & Drop-Funktion zu schließen, damit die neue Reihenfolge der Priorität wirksam wird.

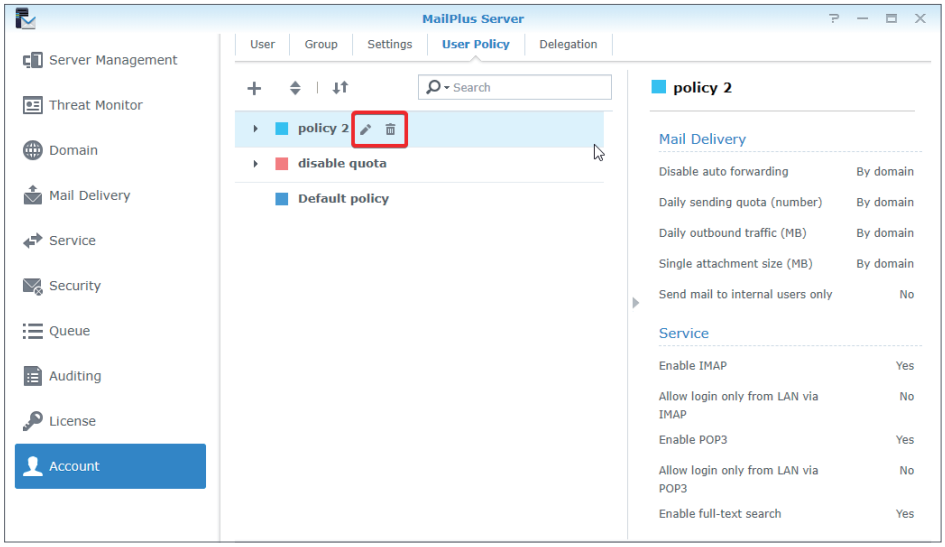
Anmerkung:

- **Die Standardrichtlinie** hat immer die niedrigste Priorität. Weitere Informationen finden Sie unter **Standardrichtlinien**.

Benutzerrichtlinien bearbeiten und löschen

Sie können die Einstellungen der Richtlinie bearbeiten, Benutzer zu einer Richtlinie hinzufügen/aus dieser löschen oder die Farbe der Richtlinie ändern. Gehen Sie wie folgt vor, um eine Benutzerrichtlinie zu bearbeiten oder zu löschen:

1. Gehen Sie zu **Konto** > **Benutzerrichtlinie**.
2. Bewegen Sie den Mauszeiger zur Richtlinie, die Sie bearbeiten möchten. Es werden zwei Symbole eingeblendet. Klicken Sie auf das Bleistiftsymbol, um die Richtlinie zu bearbeiten, oder auf das Papierkorbsymbol, um die Richtlinie zu löschen.



Standardrichtlinien

Die Standardrichtlinie des Systems gilt für Benutzer, für die keine spezielle Richtlinie vorgeschrieben ist. Die Standardrichtlinie ist eine bereits vorhandene Richtlinie, die nicht bearbeitet, gelöscht oder neu priorisiert werden kann. Beachten Sie bitte die nachstehenden Einstellungsdetails der Standardrichtlinie:

Automatische Weiterleitung deaktivieren	Die Standardeinstellung ist **Nach Domain**.
Tagessendequote (Anzahl)	Die Standardeinstellung ist **Nach Domain**.
Max. ausgehender Traffic (MB)	Die Standardeinstellung ist **Nach Domain**.
Größe einzelner Anhang (MB)	Die Standardeinstellung ist **Nach Domain**.
Mails nur an interne Benutzer senden	Die Standardeinstellung ist **Nein**.
IMAP aktivieren	Die Standardeinstellung ist **Ja**.
Anmeldung nur von LAN via IMAP erlauben	Die Standardeinstellung ist **Nein**.
POP3 aktivieren	Die Standardeinstellung ist **Ja**.
Anmeldung nur von LAN via POP3 erlauben	Die Standardeinstellung ist **Nein**.
Volltextsuche aktivieren	Die Standardeinstellung ist **Ja**.

Da die Standardrichtlinie für alle Benutzer gilt, erfüllt sie in Bezug auf bestimmte

Beschränkungen möglicherweise nicht Ihre Erwartungen. Wenn Sie nicht möchten, dass bestimmte Beschränkungen wirksam werden, müssen Sie diese Beschränkungen deaktivieren.

Richtlinieninformationen und Beschränkungen

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie	Nach Domain
01	Automatische Weiterleitung deaktivieren	Benutzer dürfen E-Mails nicht automatisch weiterleiten.	Benutzer dürfen E-Mails automatisch weiterleiten.	Richtlinien folgen den Domaineinstellungen.

Anmerkung:

- Diese Richtlinie hat keine Auswirkung auf die manuelle Weiterleitung.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie	Nach Domain
02	Tagessendequote (Anzahl)	Benutzer werden durch eine Quote beschränkt.	Benutzer werden nicht durch eine Quote beschränkt.	Richtlinien folgen den Domaineinstellungen.

Anmerkung:

- Wenn eine E-Mail vor der Zustellung zurückgewiesen wurde, wird sie bei der Quote nicht berücksichtigt.
- Wenn eine E-Mail nach der Zustellung retourniert wurde, wird sie bei der Quote berücksichtigt.
- Der für die Standardrichtlinie eingestellte Wert entspricht dem Wert der **Tagesquote** im Abschnitt **Tagesquote** auf der Registerkarte **Nutzungslimit** der Seite **Domain**.
- Wenn der Wert **0** beträgt, gelten keine Beschränkungen für Benutzer.
- Sie müssen zu **Mailübermittlung** > **Allgemein** wechseln und das Kontrollkästchen **SMTP-Authentifizierung** aktivieren.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie	Nach Domain
03	Max. ausgehender Traffic (MB)	Benutzer werden durch den ausgehenden Traffic beschränkt.	Benutzer werden nicht durch den ausgehenden Traffic beschränkt.	Richtlinien folgen den Domaineinstellungen.

Anmerkung:

- Wenn eine E-Mail vor der Zustellung zurückgewiesen wurde, wird sie bei der Quote nicht berücksichtigt.
- Wenn eine E-Mail nach der Zustellung retourniert wurde, wird sie bei der Quote berücksichtigt.
- Der für die Standardrichtlinie eingestellte Wert entspricht dem Wert **Tägliches Traffic-Limit (MB)** im Abschnitt **Tagesquote** auf der Registerkarte **Nutzungslimit** der Seite **Domain**.
- Wenn der Wert **0** beträgt, gelten keine Beschränkungen für Benutzer.
- Sie müssen zu **Mailübermittlung** > **Allgemein** wechseln und das Kontrollkästchen **SMTP-Authentifizierung** aktivieren.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie	Nach Domain
04	Größe einzelner Anhang (MB)	Benutzer werden durch Anhanggrößen eingeschränkt.	Benutzer werden nicht durch Anhanggrößen eingeschränkt.	Richtlinien folgen den Domaineinstellungen.

Anmerkung:

- Der für die Standardrichtlinie eingestellte Wert entspricht dem Wert **Maximale Größe für E-Mail (MB)** auf der Registerkarte **Allgemein** der Seite **Mailübermittlung** page.
- Der für die Standardrichtlinie eingestellte Wert gilt für externe E-Mails.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie
05	Mails nur an interne Benutzer senden	Benutzer werden darauf beschränkt, Mails nur an interne Benutzer zu senden.	Benutzer werden nicht darauf beschränkt, Mails nur an interne Benutzer zu senden.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie
06	IMAP aktivieren	Benutzern wird erlaubt, IMAP zu verwenden.	Benutzern wird nicht erlaubt, IMAP zu verwenden.

Anmerkung:

- Wenn das Kontrollkästchen **IMAP aktivieren** im Abschnitt **IMAP/POP3** auf der Seite **Dienst** nicht markiert ist, sind IMAP-Dienste nicht verfügbar und die Benutzerrichtlinie ist nicht wirksam. Benutzer können IMAP nicht nutzen, auch wenn IMAP in der Benutzerrichtlinie aktiviert ist.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie
07	Anmeldung nur von LAN via IMAP erlauben	Benutzer werden darauf beschränkt, sich über IMAP nur von einer Subdomain anzumelden.	Benutzer werden bei der Anmeldung bei MailPlus nicht beschränkt.

Anmerkung:

- Wenn das Kontrollkästchen **IMAP aktivieren** im Abschnitt **IMAP/POP3** auf der Seite **Dienst** nicht markiert ist, sind IMAP-Dienste nicht verfügbar und die Benutzerrichtlinie ist nicht wirksam. Benutzer können sich nicht via IMAP anmelden, auch wenn **Anmeldung nur von LAN via IMAP erlauben** in der Benutzerrichtlinie aktiviert ist.
- MailPlus-Web-Clients werden durch diese Einstellung nicht beschränkt.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie
08	POP3 aktivieren	Benutzern wird erlaubt, POP3 zu verwenden.	Benutzern wird nicht erlaubt, POP3 zu verwenden.

Anmerkung:

- Wenn das Kontrollkästchen **POP3 aktivieren** im Abschnitt **IMAP/POP3** auf der Seite **Dienst** nicht markiert ist, sind POP3-Dienste nicht verfügbar und die Benutzerrichtlinie ist nicht wirksam. Benutzer können POP3 nicht nutzen, auch wenn POP3 in der Benutzerrichtlinie aktiviert ist.

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie
09	Anmeldung nur von LAN via POP3 erlauben	Benutzer werden darauf beschränkt, sich über POP3 nur von einer Subdomain anzumelden.	Benutzer werden bei der Anmeldung bei MailPlus nicht beschränkt.

Anmerkung:

- Wenn das Kontrollkästchen **POP3 aktivieren** im Abschnitt **IMAP/POP3** auf der Seite **Dienst** nicht markiert ist, sind POP3-Dienste nicht verfügbar und die Benutzerrichtlinie ist nicht wirksam. Benutzer können sich nicht via POP3 anmelden, auch wenn **Anmeldung nur von LAN via POP3 erlauben** in der Benutzerrichtlinie aktiviert ist.
- Sie können sich mit einem externen Netzwerk weiterhin bei MailPlus anmelden. (MailPlus verbindet sich mit dem Mailserver über das interne Netzwerk.)

Nr.	Richtlinie	Ergebnisse der Aktivierung der Richtlinie	Ergebnisse der Deaktivierung der Richtlinie
010	Volltextsuche aktivieren	Der Server indiziert E-Mail-Inhalte von Benutzern.	Der Server indiziert keine E-Mail-Inhalte von Benutzern.

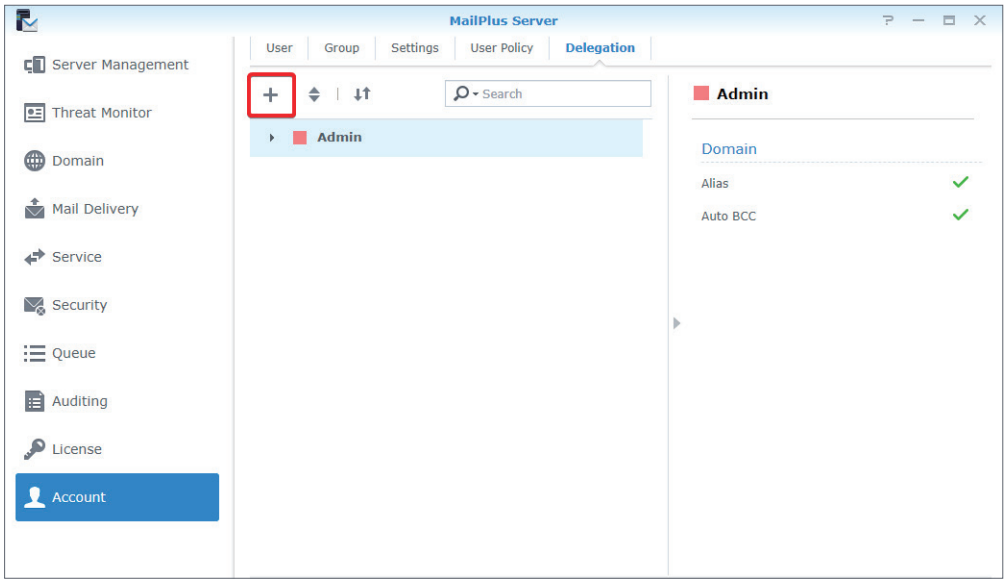
Anmerkung:

- Wenn bei **Volltextsuche aktivieren** im Abschnitt **Volltextsuche** auf der Seite **Dienst** kein Häkchen gesetzt ist, ist die Benutzerrichtlinie nicht wirksam und die E-Mail-Inhalte der Benutzer werden nicht indiziert.

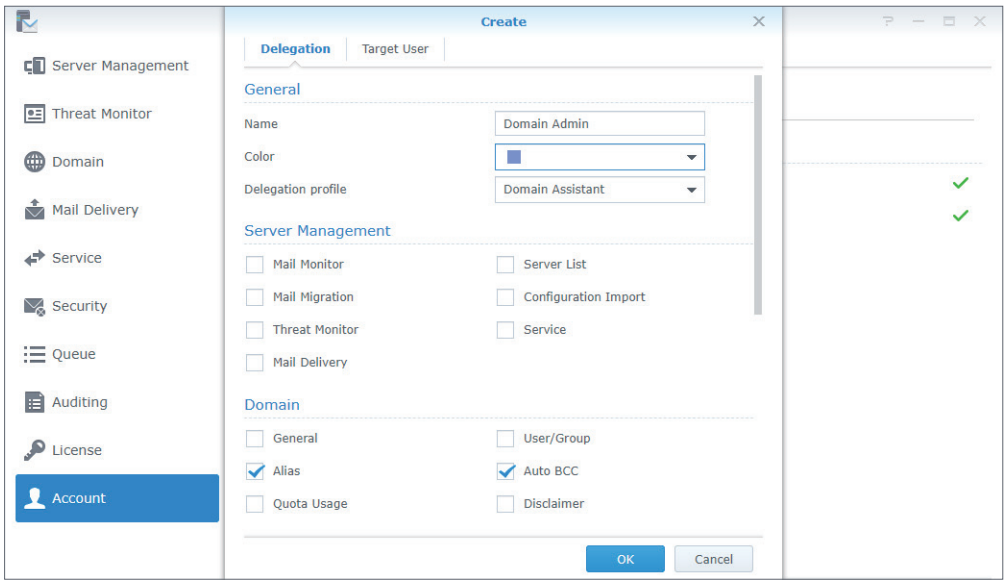
Delegationsrichtlinien erstellen

Auf der Registerkarte **Delegation** können Sie die Verwaltung von Einstellungen hinsichtlich Serverwaltung, Domain, Sicherheit, Überprüfung und Konto (ausgenommen Lizenz) von MailPlus Server entsprechend dem von Ihnen zugewiesenen Delegationsprofil an andere Benutzer delegieren. In diesem Abschnitt wird der ***Domain-Admin*** als Beispiel zur Veranschaulichung verwendet.

1. Gehen Sie zu **Konto** > **Delegation** und klicken Sie in der oberen Leiste auf das Plus-Symbol.

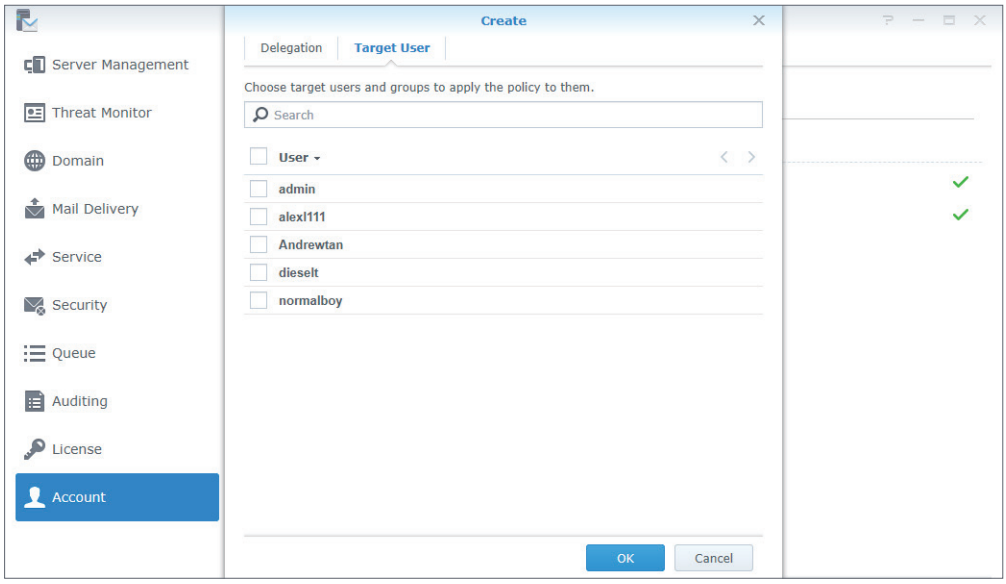


2. Gehen Sie im eingeblendeten Fenster zur Registerkarte **Delegation** und geben Sie die erforderlichen Informationen ein. Das System markiert automatisch die untenstehenden Optionen entsprechend des gewählten Delegationsprofils. Das Profil wechselt zu **Benutzerdefiniert**, wenn Sie unten Optionen markieren oder die Markierung aufheben. In **diesem Artikel** finden Sie weitere Informationen über delegierte Berechtigungen.



Wenn Sie beispielsweise **Domänenmanager** für *Domain-Admin* wählen, können Benutzer, für die diese Delegationsrichtlinie gilt, alle Einstellungen vorhandener Domains verwalten. Wenn Sie jedoch **Domain-Assistent** für *Domain-Admin* wählen, können Benutzer, für die diese Delegationsrichtlinie gilt, nur den Alias und die autom. BCC-Weiterleitung von Domains verwalten.

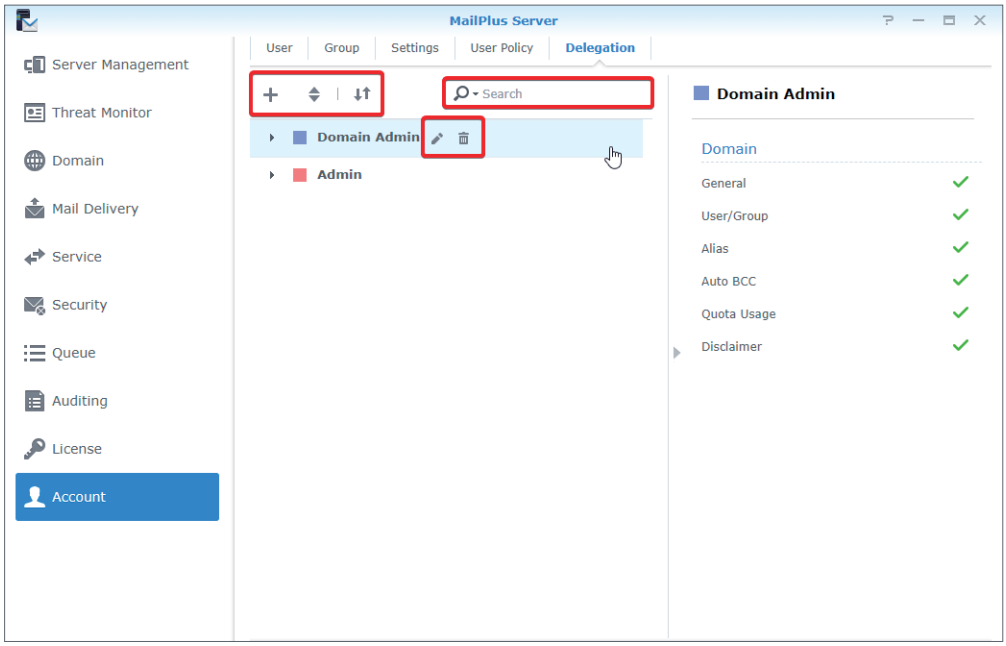
3. Gehen Sie dann zur Registerkarte **Zielbenutzer**, um die Benutzer/Gruppen auszuwählen, für welche die definierte Delegationsrichtlinie gelten soll.



4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

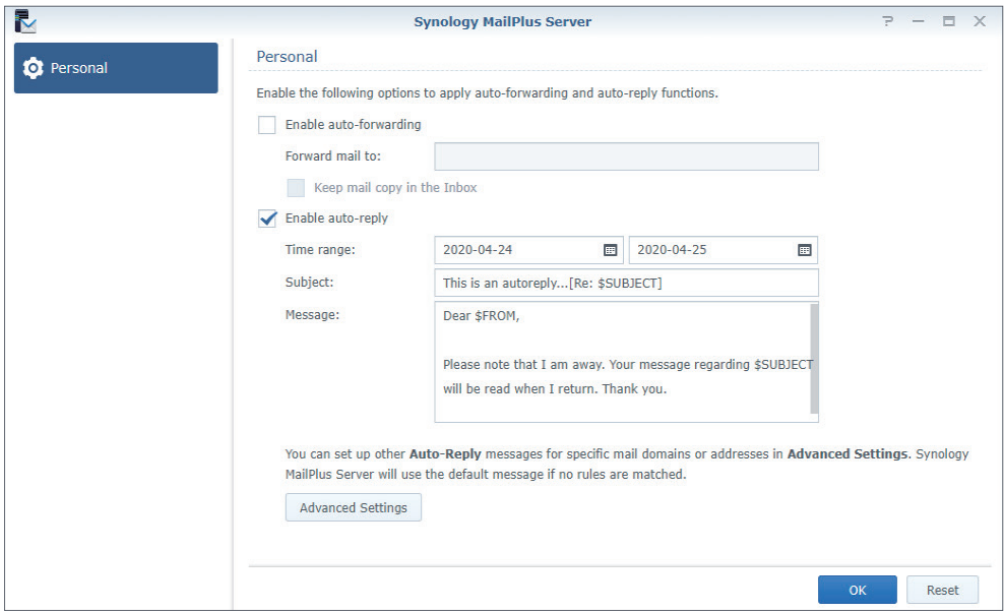
Delegationsrichtlinien verwalten

1. Gehen Sie zu **Konto** > **Delegation**.
2. Wählen Sie ***Domain-Admin*** aus, um eine Richtlinie anzuzeigen, zu bearbeiten und zu löschen.
3. Mit den Schaltflächen in der oberen Symbolleiste und dem Vorschaufenster auf der rechten Seite können Sie Delegationsrichtlinien verwalten:
   - **Richtlinienpriorität einstellen**:
     - Klicken Sie auf das Symbol mit den beiden Pfeilen, um die Priorität festzulegen.
     - Klicken Sie auf ***Domain-Admin*** und verschieben Sie die Richtlinie per Drag-and-Drop an eine geeignete Position. Wenn ein Benutzer/eine Gruppe von mehr als einer Delegationsrichtlinie gesteuert wird, verwendet das System die höchste Richtlinie auf der Liste für den Benutzer/die Gruppe.
   - **Eine Delegationsrichtlinie ausklappen/einklappen**: Klicken Sie auf das doppelte Dreiecksymbol, um die Zielbenutzer/Gruppen aus- oder einzuklappen.
   - **Eine Delegationsrichtlinie suchen**: Geben Sie den Richtliniennamen oder seine Benutzer in die Suchleiste oben ein.
   - **Vorschau einer Delegationsrichtlinie anzeigen**: Zeigen Sie den Namen, das Profil und weitere Details der Delegationsrichtlinie in der Vorschau an.
   - **Eine Delegationsrichtlinie bearbeiten**: Klicken Sie zum Bearbeiten der Richtlinie auf das Bleistiftsymbol.
   - **Eine Delegationsrichtlinie löschen**: Klicken Sie auf das Papierkorbsymbol, um die Richtlinie zu löschen.



Berechtigungen verwalten

Berechtigungseinstellungen für MailPlus Server werden mit den DSM-Einstellungen synchronisiert. Benutzer aus der Administrationsgruppe in DSM können auf alle Einstellungen von MailPlus Server zugreifen, während allgemeine Benutzer nur die Seite **Persönlich** anzeigen können (wie in der Abbildung unten).



Anmerkung:

- Die Standardberechtigungseinstellungen von MailPlus Server in der **Systemsteuerung** sollten beibehalten werden. Alle Benutzer sollten Rechte für MailPlus Server haben, ansonsten ist die Funktionalität des Pakets eingeschränkt.

Kapitel 6: Protokolleinstellungen

MailPlus Server bietet eine zentrale Oberfläche zur Konfiguration von E-Mail-Protokollen. Sie können Ports für bestimmte Protokolle öffnen/schließen oder die Netzwerkschnittstelle Ihres Servers neu binden. Da sich Protokolleinstellungen auf die externen Vorgänge des gesamten Servers auswirken, stellen Sie bitte sicher, dass die Einstellungen Ihren Anforderungen entsprechen.

SMTP

SMTP benutzt drei Ports. In MailPlus Server werden sie als SMTP (Portnummer: 25), SMTP-SSL (Portnummer: 465) sowie SMTP-TLS (Portnummer: 587) angezeigt. Die drei Protokolle und ihre jeweiligen Funktionen sind nachstehend angeführt:

- **SMTP**: **SMTP** ist ein Standardprotokoll für den Empfang externer E-Mails und die Zustellung interner E-Mails. MailPlus Server verwendet Postfix und stellt E-Mails mit Hilfe des Hamming-Codes zu, wenn **STARTTLS** nicht angegeben wurde. Derzeit ist unser SMTP nicht verschlüsselt. Wenn Sie eine Verschlüsselung benötigen, finden Sie **hier** weitere Informationen.
- **SMTP-SSL**: SMTPS ist ein unterstütztes Protokoll für SMTP-SSL. Da DSM die SSL-Verschlüsselung nicht mehr unterstützt, kann MailPlus Server nur über TLS eine Verbindung zu SMTP-SSL herstellen.

Anmerkung:

- Dies unterscheidet sich von der Verschüsselung von SMTP über STARTTLS. SMTP muss verschlüsselte Pakete nach einem Handshake versenden. Wenn die Übermittlung mit diesem Protokoll erfolgen soll, finden Sie **hier** weitere Informationen.

- **SMTP-TLS**: SMTPS ist ein unterstütztes Protokoll für SMTP-TLS und nimmt die Verschlüsselung über STARTTLS vor. SMTP-TLS erfordert eine Authentifizierung; daher wird es häufig für das interne Protokoll zwischen Client und **MSA** verwendet.

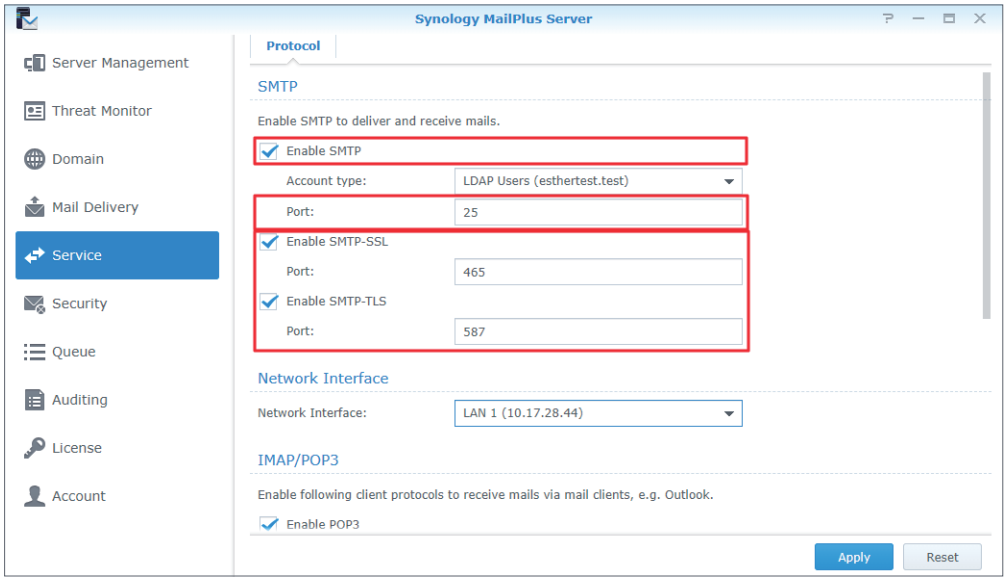
SMTP einrichten

Beachten Sie bitte die nachfolgenden Anweisungen zur Konfiguration von SMTP und der jeweiligen Ports:

1. Gehen Sie zu **Dienst** > **Protokoll** > **SMTP** und setzen Sie ein Häkchen bei **SMTP aktivieren**.

Anmerkung:

- SMTP ist das Hauptprotokoll in einem Mailserver.



2. Sie können die Portnummer im Feld **Port** ändern.

Anmerkung:

- Wir empfehlen wir Ihnen die Verwendung des Standardports 25, sofern keine besonderen Umstände vorliegen.

3. Sie können die folgenden Einstellungen anpassen:
   - **SMTP-SSL aktivieren**: Verwendet SMTPS als Protokoll. Sie können die Portnummer von SMTP-SSL im Feld **Port** ändern.
   - **SMTP-TLS aktivieren**: Ermöglicht die Authentifizierung und STARTTLS-Verschlüsselung bei einer erzwungenen Verbindung. Sie können die Portnummer von SMTP-TLS im Feld **Port** ändern.
4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

IMAP/POP3

IMAP/POP3 bietet verschlüsselte und unverschlüsselte Optionen; dabei verwendet es vier Ports. In MailPlus Server sind diese Ports IMAP (Portnummer: 143), IMAPS (Portnummer: 993), POP3 (Portnummer: 110) und POP3S (Portnummer: 995). Über diese Protokolle können Sie E-Mail-Daten von MailPlus Server mit unterschiedlichen E-Mail-Clients abrufen.

Anmerkung:

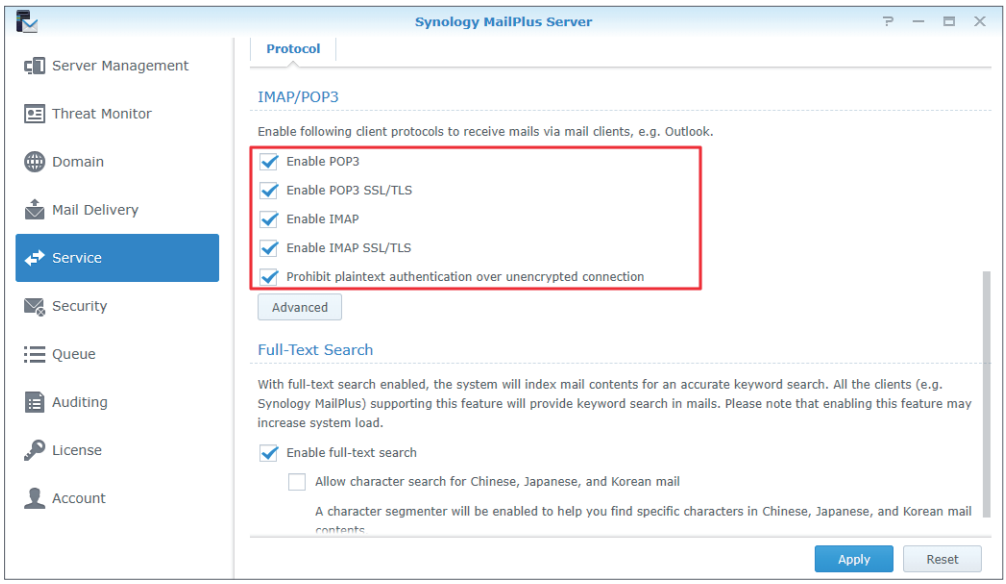
- Beide Protokolle verschlüsseln über STARTTLS. Da DSM eine über SSL verschlüsselte Verbindung nicht mehr unterstützt, richten Sie bitte kein SSL für eine verschlüsselte Verbindung ein.

- **IMAP**: **IMAP** ist ein Standardprotokoll, mit dem Benutzer auf die auf einem Mailserver gespeicherten Daten zugreifen können. IMAP-Clients bearbeiten E-Mails direkt auf dem Mailserver, der auf allen IMAP-Client-Postfächern gespiegelt wird; daher werden alle an E-Mails vorgenommene Änderungen geräteübergreifend synchronisiert.
- **POP3**: **POP3** ist ein Standardprotokoll, mit dem Benutzer auf die auf einem Mailserver gespeicherten Daten zugreifen können. POP3-Clients laden E-Mails vom Server herunter und speichern sie lokal. Daher werden die an einer E-Mail vorgenommenen Änderungen nicht zurück zum Mailserver synchronisiert.

IMAP/POP3 einrichten

Gehen Sie bitte wie folgt vor, um IMAP, POP3 und ihre jeweiligen Protokolle zu konfigurieren:

1. Gehen Sie zu **Dienst** > **IMAP/POP3**.
2. Sie können die folgenden Einstellungen im Bereich **IMAP/POP3** anpassen:
   - **POP3 aktivieren**: Setzen Sie ein Häkchen, damit die E-Mail-Client-Software Nachrichten mittels POP3 empfangen kann.
   - **POP3 SSL/TLS aktivieren**: Setzen Sie ein Häkchen, damit die POP3-Client-Verbindung mit SSL/TLS geschützt werden kann.
   - **IMAP aktivieren**: Setzen Sie ein Häkchen, damit die E-Mail-Client-Software Nachrichten mittels IMAP empfangen kann.
   - **IMAP SSL/TLS aktivieren**: Setzen Sie ein Häkchen, damit die IMAP-Client-Verbindung mit SSL/TLS geschützt werden kann.



3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Netzwerkschnittstelle

Nachdem Sie MailPlus Server installieren oder High-Availability konfigurieren, wird MailPlus Server an eine Netzwerkschnittstelle gebunden, um den **High-Availability-Cluster** zu unterstützen. Der auf dem Server gehostete E-Mail-Dienst wird auf dieser Netzwerkschnittstelle ausgeführt.

Netzwerkschnittstelle anbinden

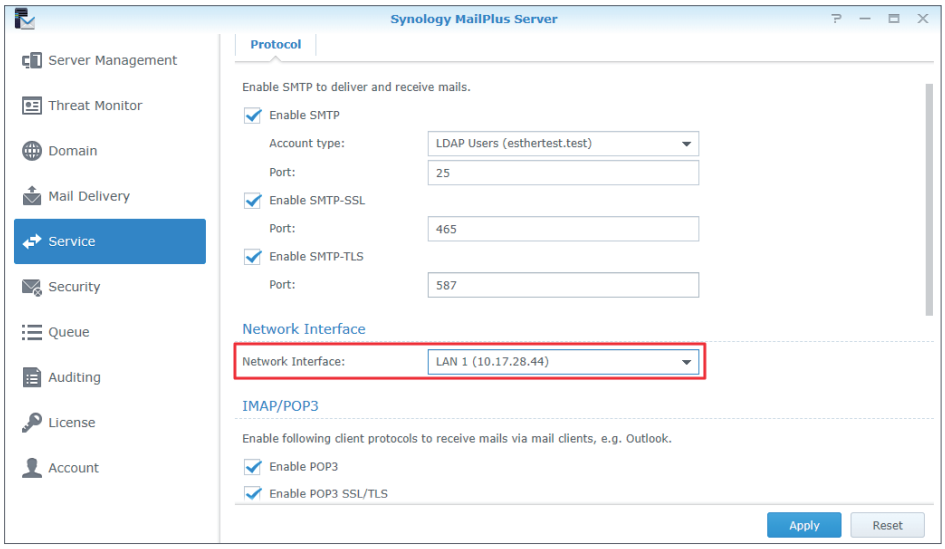
Wenn Ihr MailPlus Server auf einem einzigen Server ausgeführt wird, können Sie MailPlus Server an LAN, PPPoE oder eine verbundene Netzwerkschnittstelle anbinden. Wenn Ihr MailPlus Server in einer High-Availability-Architektur ausgeführt wird, können Sie MailPlus Server an LAN oder eine verbundene Netzwerkschnittstelle anbinden. Sie können die **manuelle Konfiguration** nutzen, um die IP-Adresse der Netzwerkschnittstelle abzurufen.

Anmerkung:

- Wenn Ihr MailPlus Server an eine verbundene Netzwerkschnittstelle angebunden wird, können Sie die verbundene Netzwerkschnittstelle nicht entfernen. Wenn Sie die verbundene Netzwerkschnittstelle entfernen möchten, müssen Sie zuerst die Netzwerkschnittstelle ändern oder MailPlus Server deinstallieren.

Netzwerkschnittstelle ändern

1. Melden Sie sich bei DSM an.
2. Starten Sie **MailPlus Server**.
3. Gehen Sie zu **Dienst** > **Netzwerkschnittstelle** und wechseln Sie im Dropdown-Menü **Netzwerkschnittstelle** zwischen den Netzwerkschnittstellen.



4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Nach der grundlegenden Konfiguration von MailPlus Server im Zuge der Installation müssen Sie möglicherweise SMTP-bezogene Limits für Benutzeranmeldungen oder Übermittlung eingehender/ausgehender E-Mails einrichten.

Kapitel 7: SMTP-Einstellungen

Diensteinstellungen

Sie können auf die Seite **Mailübermittlung** wechseln, um Regeln für das Senden und Empfangen von E-Mails einzurichten.

MailPlus Server bietet schnelle und unkomplizierte Optionen für die Diensteinstellung, wie nachstehend angeführt:

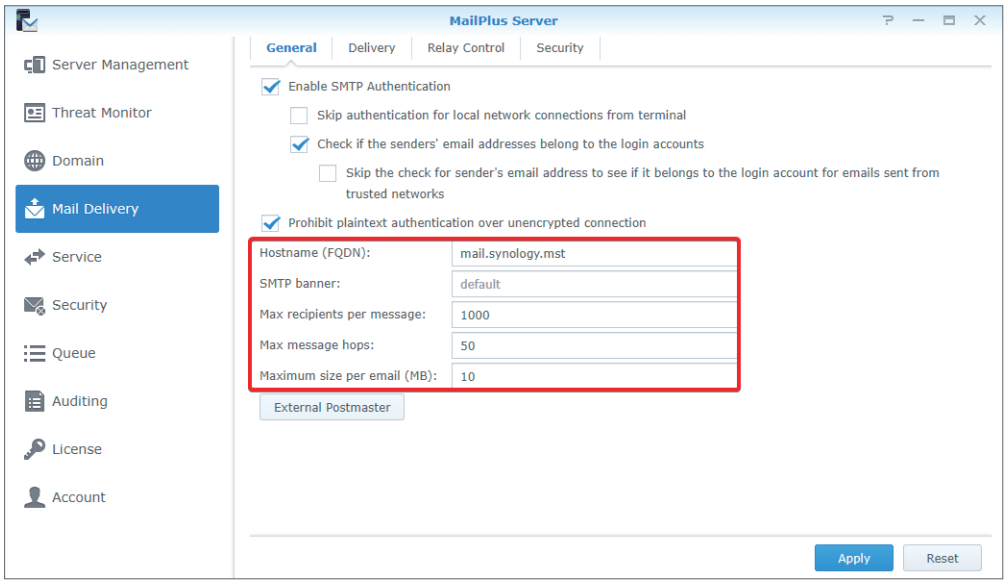
- **SMTP-Profil**: Sie können einen Hostnamen für MailPlus Server und ein SMTP-Banner auf dem Telnet-Terminal eines Clients angeben. Außerdem können Sie Regeln für das Senden und Empfangen von E-Mails einrichten, wie z. B. die Festlegung der maximalen Größe pro E-Mail sowie der maximalen Empfänger pro Nachricht, um den Verbrauch übermäßiger Ressourcen zu vermeiden.
- **Volltextsuche**: Sie können die Volltextsuche aktivieren, um die Leistung der E-Mail-Suche zu verbessern. Mit dieser Funktion können MailPlus-Web-Clients E-Mails indizieren, auch solche mit chinesischen, japanischen und koreanischen Schriftzeichen. Da die Volltextsuche den gesamten Inhalt der E-Mails indiziert, werden möglicherweise zusätzliche Rechenressourcen benötigt. Sie können die Volltextsuche wahlweise aktivieren und sie zudem für bestimmte Benutzer deaktivieren. Weitere Informationen finden Sie unter **Benutzerrichtlinien erstellen**.

SMTP-Profil einrichten

Ein SMTP-Profil enthält Regeln darüber, wie MailPlus Server E-Mails an andere Mailserver sendet.

1. Gehen Sie zu **Mailübermittlung** > **Allgemein**.
   - **Hostname (FQDN)**: Geben Sie den Hostnamen von MailPlus Server im FQDN-Format an. Stellen Sie sicher, dass der Hostname mit der IP-Adresse auf einem DNS-Server übereinstimmt.
   - **SMTP-Banner**: Geben Sie den Text an, der im Telnet-Terminal des SMTP-Clients angezeigt wird.
   - **Max. Empfänger pro Nachricht**: Legen Sie die maximale Anzahl von Empfängern für eingehende bzw. ausgehende Nachrichten fest. Nachrichten, die dieses Limit überschreiten, werden abgelehnt.
   - **Max. Nachrichtensprünge**: Legen Sie die maximale Anzahl an Sprüngen (d. h. Mailweiterleitungen) für eingehende bzw. ausgehende Nachrichten fest. Nachrichten, die dieses Limit überschreiten, werden abgelehnt.

- **Maximale Größe für E-Mail (MB)**: Legen Sie die maximale Größe für eingehende bzw. ausgehende Nachrichten fest. Nachrichten, die dieses Limit überschreiten, werden abgelehnt.

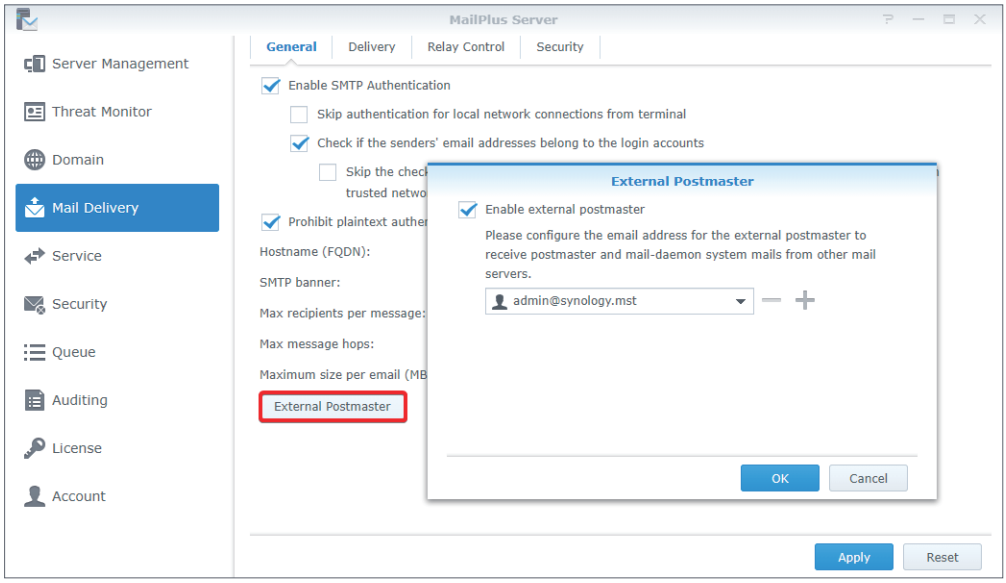


2. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Externer Postmaster

Der externe Postmaster ist eingerichtet, um von anderen Mailservern an Mailer-daemon- und Postmaster-Aliasnamen gesendete System-E-Mails zu empfangen.

1. Gehen Sie zu **Mailübermittlung** > **Allgemein**.
2. Klicken Sie auf die Schaltfläche **Externer Postmaster**.
3. Markieren Sie das Kontrollkästchen **Externen Postmaster aktivieren**.
4. Klicken Sie auf das Plus-Symbol/die Schaltfläche **Hinzufügen**, um E-Mail-Adressen für externe Postmaster hinzuzufügen.



5. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

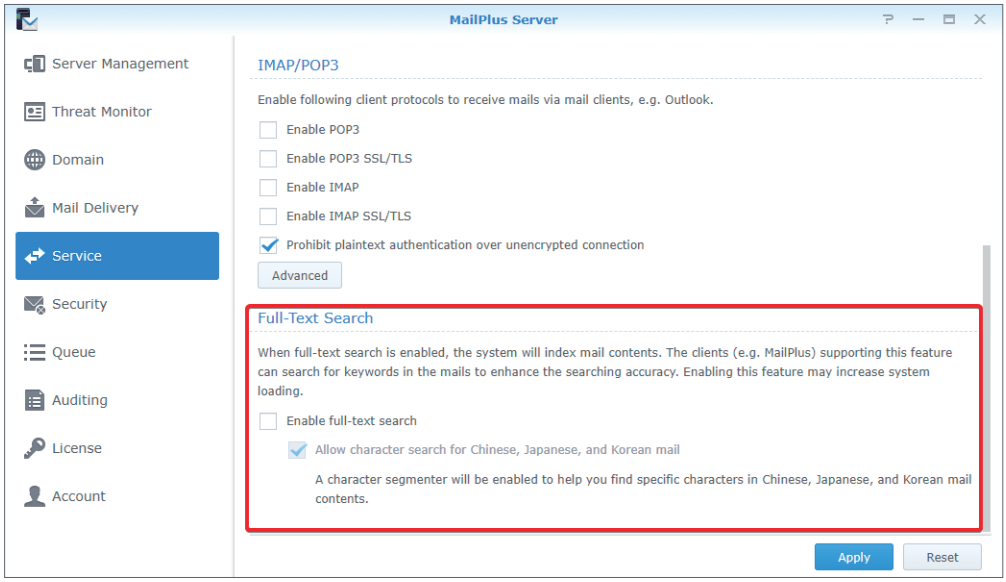
Volltextsuche

Bei aktivierter Volltextsuche indiziert der Server Betreffzeilen, Absender, Empfänger und Nachrichteninhalt von E-Mails, und ermöglicht Ihnen, bequem nach Schlüsselwörtern auf Clients zu suchen, die diese Funktion unterstützen (z. B. MailPlus).

Anmerkung:

- Die Aktivierung dieser Funktion kann die Systemauslastung erhöhen, wenn eine große Anzahl ausgehender und eingehender Nachrichten vorhanden ist.

1. Gehen Sie zu **Dienst**.
2. Im Bereich **Volltextsuche** können Sie folgende Einstellungen anpassen:
   - **Volltextsuche aktivieren**: Wenn Sie diese Option markieren, finden Sie unter **Benutzerrichtlinien erstellen** detaillierte Informationen. Sie können die Volltextsuche für bestimmte Benutzer deaktivieren, um eine hohe Serverauslastung zu vermeiden.
   - **Zeichensuche für chinesische, japanische und koreanische E-Mails zulassen**: Wenn Sie diese Option markieren, wird eine Zeichen-Segmentierung aktiviert, damit Sie spezifische Zeichen in chinesischen, japanischen und koreanischen E-Mail-Inhalten finden.



3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Gesicherte SMTP-Verbindung

MailPlus Server kann die Sicherheit und Stabilität durch Analyse der Benutzerverbindung, der Anmeldeinfos und der E-Mail-Inhalte verbessern. Somit wird nicht nur Ihre Dienstqualität geschützt, sondern auch verhindert, dass MailPlus Server zu einem Open Relay für Spammer

wird und folglich auf eine Blacklist gesetzt wird.

- **SMTP-Authentifizierung**: Bei aktivierter SMTP-Authentifizierung müssen Benutzer ihre DSM-Benutzerkonten und Kennwörter zur Authentifizierung eingeben, wenn sie E-Mails über den Server übermitteln.

Anmerkung:

- Die Authentifizierung ist nur für die Weiterleitung von E-Mails erforderlich. Damit wird verhindert, dass ein Open Relay für Spammer entsteht. Weitere Informationen finden Sie in **diesem Artikel**.

- **Blacklist und Whitelist**: Wenn Ihr Server weiterhin Spam-E-Mails empfängt, können Sie Blacklist-Regeln einrichten, um E-Mails aus bestimmten Quellen abzulehnen. Allerdings kann MailPlus Server versehentlich legitime E-Mails ablehnen, wenn **Virenscan**, **Authentifizierung** oder andere Funktionen zum Überprüfen von E-Mails aktiviert sind. In diesem Fall können Sie die Whitelist verwenden, um die Sicherheitsuntersuchung zu überspringen, damit wichtige E-Mails empfangen werden können.
- **Absenderrichtlinie**: Sie können Kriterien einrichten, um unzulässige Formate oder nicht authentifizierte Absenderadressen abzulehnen.
- **Verbindungsrichtlinie**: Sie können Verbindungen von Client-IP-Adressen beschränken, die nicht identifiziert werden können oder MailPlus Server überlasten könnten.
- **Erweiterte Einstellungen**: Bei der Verbindungsphase sind korrekte Befehle und andere erweiterte Einstellungen erforderlich. Weitere Informationen finden Sie unter **Erweiterte Einstellungen**.

SMTP-Authentifizierung aktivieren

Mit der Authentifizierung wird verhindert, dass böswillige Benutzer Ihren Mailserver für die Weiterleitung von Spam-E-Mails benutzen. Wir empfehlen daher die Funktion der Benutzerauthentifizierung zu aktivieren. Benutzer, die diese Authentifizierung nicht bestehen, können ihre E-Mails nicht weiterleiten. So können Sie verhindern, dass Ihr Server auf Blacklists gesetzt wird.

Anmerkung:

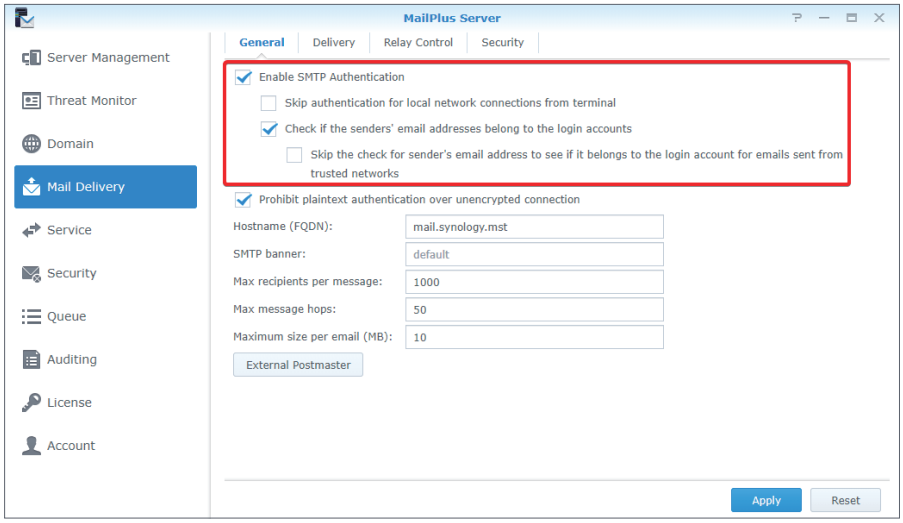
- Einige Funktionen in MailPlus Server, wie z. B. die **Tagesquote**, erfordern eine Authentifizierung.

1. Gehen Sie zu **Mailübermittlung** > **Allgemein** und wählen Sie aus, ob Sie das Kontrollkästchen **SMTP-Authentifizierung aktivieren** markieren.
2. Bei markiertem Kontrollkästchen **SMTP-Authentifizierung aktivieren** können Sie die folgenden Einstellungen anpassen:
   - **Authentifizierung für lokale Netzwerkverbindungen von Terminal überspringen**: Benutzer, die das lokale Netzwerk für den Zugriff auf E-Mail-Dienste nutzen, benötigen keine Authentifizierung.
   - **Überprüfen, ob die E-Mail-Adressen des Absenders zu den Anmeldekonten gehören**: Benutzer müssen die E-Mail-Adressen ihrer Anmeldekonten verwenden, um E-Mails zu

senden.

Anmerkung:

- Wenn Sie bei **Überprüfen, ob die E-Mail-Adressen des Absenders zu den Anmeldekonten gehören** auf der Registerkarte **Allgemein** ein Häkchen setzen, können E-Mails auf der **Liste vertrauenswürdiger IPs** von MailPlus Server abgelehnt werden. Sie können zur Registerkarte **Allgemein** wechseln und bei **Die Prüfung, ob die Absender-E-Mail-Adresse zum Anmeldekonto gehört, für von vertrauenswürdigen Netzwerken gesendete E-Mails überspringen** ein Häkchen setzen, um diese Prüfung zu überspringen. Wenn Sie auf der Registerkarte **Allgemein** bei **Authentifizierung für lokale Netzwerkverbindungen von Terminal überspringen** ein Häkchen setzen, werden E-Mails von lokalen Netzwerken nicht von MailPlus Server blockiert.



3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

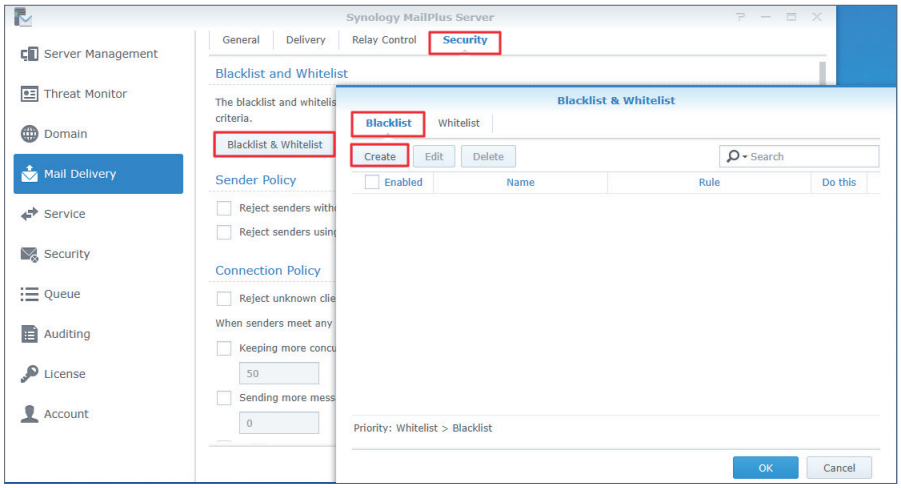
Blacklist und Whitelist erstellen

Das System führt bestimmte Aktionen bei Nachrichten aus, die auf verschiedenen unter **Blacklist & Whitelist** angegebenen Kriterien basieren. Sie können hierzu wie folgt vorgehen, um Regeln für die Blacklist und Whitelist zu erstellen:

Anmerkung:

- Wenn eine E-Mail-Nachricht Kriterien von Blacklist und Whitelist erfüllt, wird diese E-Mail empfangen, da die Whitelist eine höhere Priorität hat als die Blacklist. Beachten Sie den Abschnitt **Informationen und Beschränkungen zur Whitelist**.

1. Gehen Sie zu **Mailübermittlung** > **Sicherheit** und klicken Sie auf **Blacklist & Whitelist**.
2. Im Fenster **Blacklist & Whitelist** können Sie Ihre Blacklist und Whitelist verwalten. In diesem Abschnitt verwenden wir die **Blacklist** zur Veranschaulichung:
   - **Blacklist**: Legen Sie Regeln fest, nach denen E-Mail-Nachrichten abgelehnt/verworfen werden.
   - **Whitelist**: Legen Sie Regeln fest, nach denen übereinstimmende E-Mail-Nachrichten durchgelassen werden.
3. Klicken Sie in der Registerkarte **Blacklist** auf **Erstellen**.



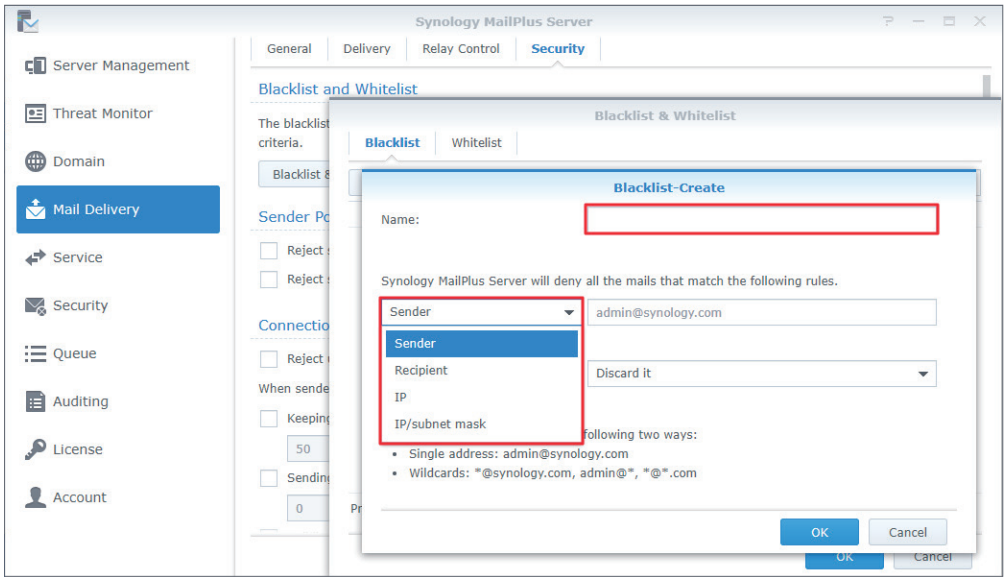
4. Benennen Sie die Regel für die Blacklist (Whitelist) im Feld **Name**.

5. Wählen Sie einen Regeltyp:

   - **Absender**: Führt bestimmte Aktionen aus, wenn eine Absenderadresse den angegebenen Kriterien entspricht.
   - **Empfänger**: Führt bestimmte Aktionen aus, wenn eine Empfängeradresse den angegebenen Kriterien entspricht.
   - **IP**: Führt bestimmt Aktionen aus, wenn die IP-Adresse eines Absenders den angegebenen Kriterien entspricht.
   - **IP/Subnetzmaske**: Führt bestimmte Aktionen aus, wenn die IP-Adresse eines Absenders und die Subnetzmaske den angegebenen Kriterien entspricht.
   - **Domain**: Führt bestimmte Aktionen aus, wenn eine Absenderdomain den angegebenen Kriterien entspricht. Diese Option ist nur für die **Whitelist** verfügbar.

Anmerkung:

- Die Adresse unter **Absender** wird von den Informationen bestimmt, die von **MAIL FROM** abgerufen werden.
- Die Adresse unter **Empfänger** wird von den Informationen bestimmt, die von **RCPT TO** abgerufen werden.

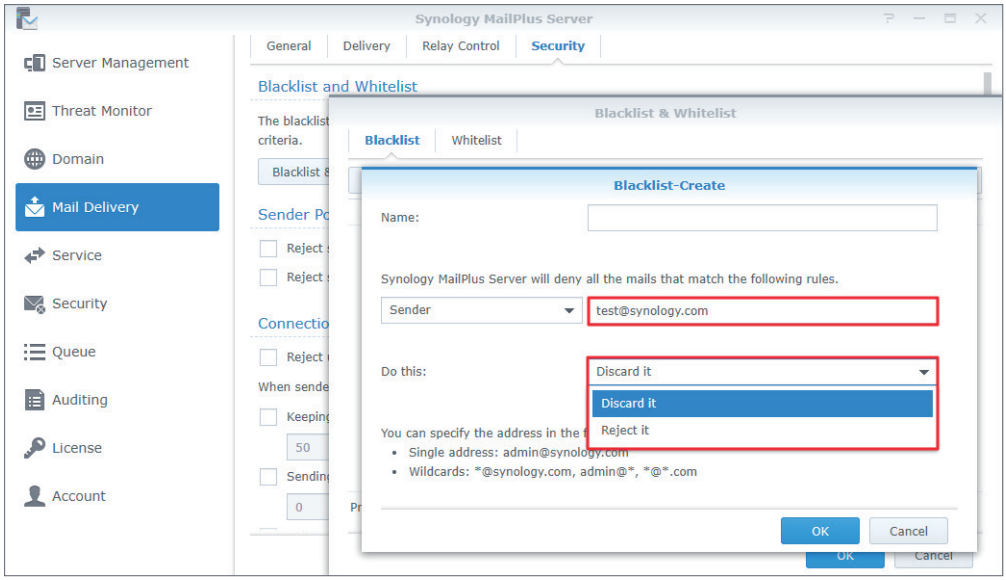


6. Legen Sie die Kriterien für den gewählten Regeltyp fest. Beachten Sie den grauen Text im Eingabefeld, um das korrekte Format zu verwenden. Sie können auch Sternchen (*) verwenden, wenn Sie die Kriterien für den Absender oder Empfänger angeben.

7. Wählen Sie eine Aktion, die bei übereinstimmenden Kriterien ausgeführt werden soll, im Dropdown-Menü **Vorgang ausführen** aus.

Anmerkung:
- **Whitelist** beinhaltet diese Option nicht, da sie den Empfang von E-Mails mit übereinstimmenden Kriterien immer zulässt.

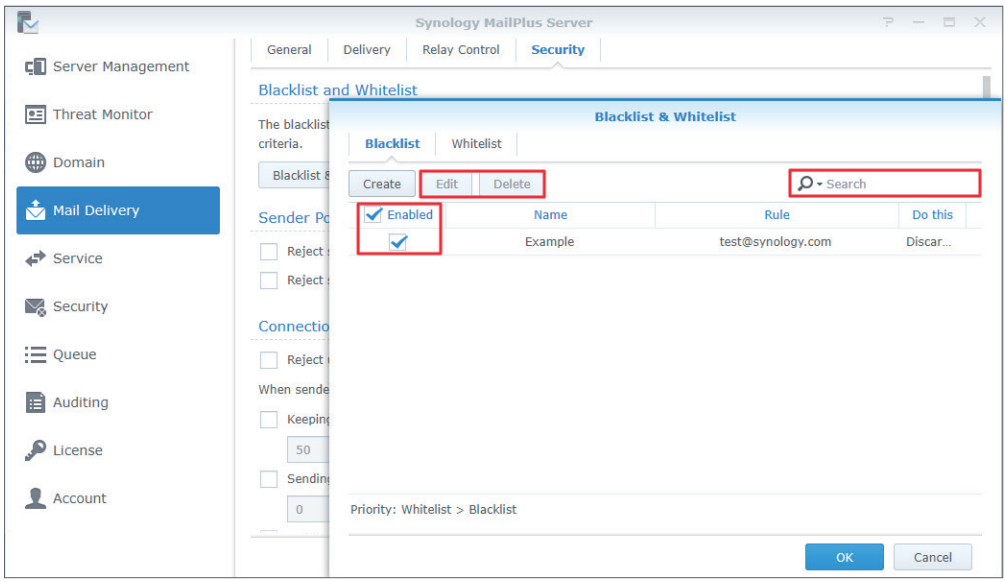
- **Ablehnen**: Absender werden benachrichtigt, wenn ihre E-Mails abgelehnt wurden.
- **Verwerfen**: Absender werden nicht benachrichtigt, wenn ihre E-Mails verworfen wurden.



8. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

Blacklist und Whitelist bearbeiten und löschen

1. Sie können Schlüsselwörter in das Suchfeld im Fenster **Blacklist & Whitelist** oben rechts eingeben, um nach der Blacklist/Whitelist zu suchen, die Sie ändern möchten.
2. Sie können das Kontrollkästchen **Aktiviert** markieren, um eine Regel zu aktivieren oder zu deaktivieren. (Sie müssen die Regel aus der Blacklist oder Whitelist nicht löschen.)
3. Wenn Sie eine bestimmte Regel bearbeiten oder löschen müssen, wählen Sie zuerst die Regel aus und klicken Sie auf **Bearbeiten** oder **Löschen**.
4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.



Informationen und Einschränkungen zur Whitelist

Whitelist-Einstellungen können die Tests überspringen, die für Blacklists erforderlich sind. Je nach Typ der Einstellungen können sie darüber hinaus die Tests DNSBL, SPF, Virenscans, DKIM und DMARC überspringen. In der folgenden Tabelle sehen Sie, welche Tests je nach Whitelist-Einstellungen übersprungen werden:

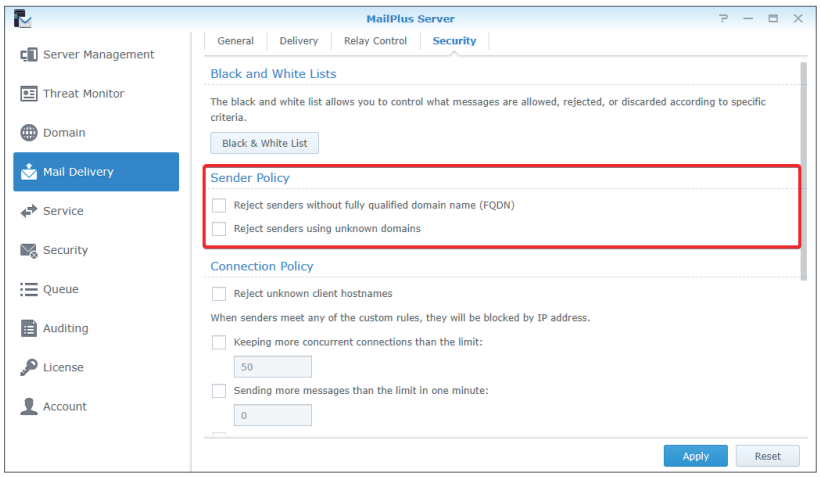
	DNSBL	SPF	Virenscans	DKIM	DMARC	smtpd_*_restrictions
IP	V	V	V	V	V	V
IP/ Subnetzmaske	V	V		V	V	V
Absender		V	V			V
Empfänger		V	V			V
Domain		V	V	V	V	V

Anmerkung:

- Es gibt bestimmte Tests, die eine Whitelist nicht überspringt; E-Mails, die diese Tests nichts bestehen, werden daher nicht zugestellt. Beispiel: Wenn der Absender ***admin@beispiel.com*** sich auf der Whitelist befindet und die Absenderregel DNSBL, DKIM und DMARC nicht unterstützt, muss er DNSBL-, DKIM- oder DMARC-Tests bestehen, um einen Zustellungsfehler zu vermeiden.
- Wenn alle in der Tabelle aufgeführten Tests übersprungen werden sollen, empfehlen wir Ihnen, dass Sie Whitelist-Regeln auf Grundlage der IP-Adresse einrichten.

Absenderrichtlinie

1. Gehen Sie zu **Mailübermittlung** > **Sicherheit**.
2. Richten Sie im Bereich **Absenderrichtlinie** bestimmte Kriterien ein, um E-Mails abzulehnen. Die Richtlinien enthalten die folgenden Optionen:
   - **Absender ohne voll qualifizierten Domainnamen (FQDN) zurückweisen**: Wenn der Domainname eines Absenders unter **MAIL FROM** mit dem FQDN-Format nach RFC-Standard nicht übereinstimmt, werden die E-Mails abgelehnt.
   - **Absender mit unbekannten Domains zurückweisen**: Wenn MailPlus Server nicht das endgültige Empfangsterminal ist und eine Absenderdomain unter **MAIL FROM** mit keinem DNS A- und MX-Eintrag übereinstimmt oder wenn der MX-Eintrag nicht korrekt ist, werden die E-Mails abgelehnt.

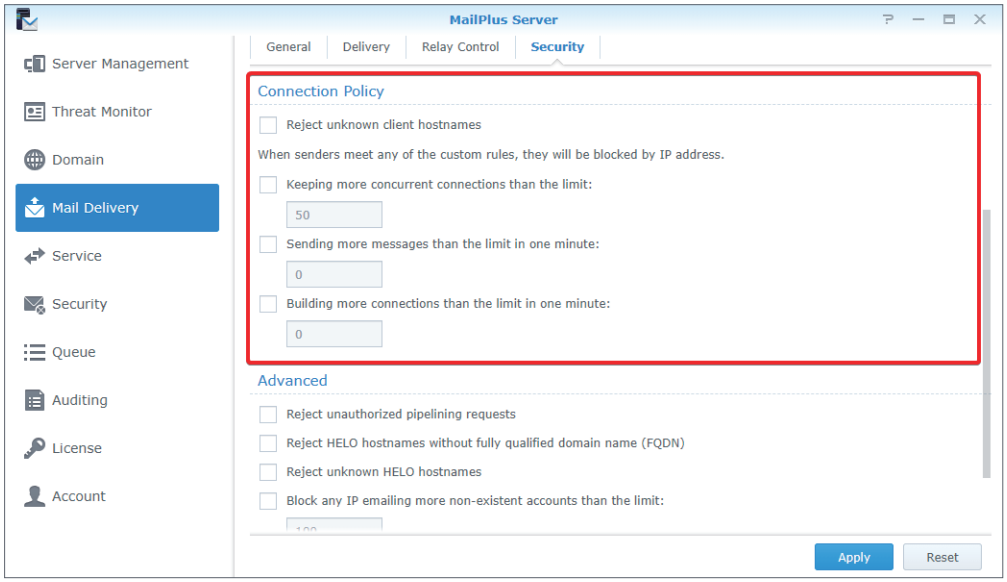


Verbindungsrichtlinie

1. Gehen Sie zu **Mailübermittlung** > **Sicherheit**.
2. Richten Sie im Bereich **Verbindungsrichtlinie** die Kriterien ein, um Client-Verbindungen zu beschränken oder verdächtige IP-Adressen zu blockieren. Die Richtlinien enthalten die folgenden Optionen:
   - **Unbekannte Client-Hostnamen ablehnen**: Wenn IP-Adresse oder Client-Hostname nicht korrekt oder nicht vorhanden sind, wird die Client-Verbindung zu MailPlus Server abgelehnt.
   - **Es werden mehr gleichzeitige Verbindungen erhalten als der Grenzwert**: Sie können die maximalen gleichzeitigen Verbindungen für den Server festlegen. Wenn die Anzahl

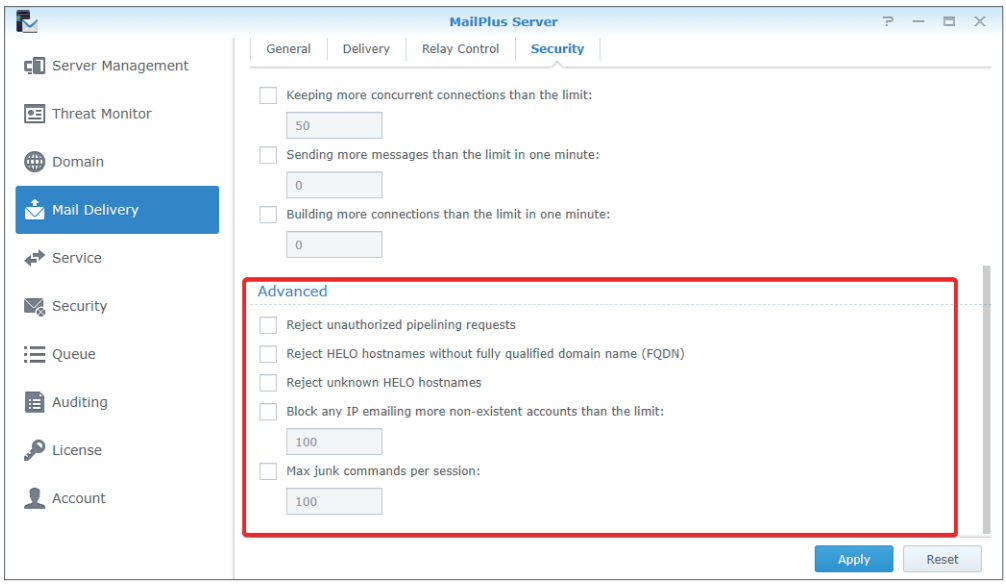
der gleichzeitigen Verbindungen mit derselben IP-Adresse diese Zahl überschreitet, werden Verbindungen blockiert, bis die Gesamtzahl niedriger als der Grenzwert ist.

- **Es werden in einer Minute mehr als die festgelegten Nachrichten gesendet**: Sie können die maximale Anzahl von E-Mail-Nachrichten festlegen, die innerhalb einer Minute gesendet werden können. Wenn die Anzahl der innerhalb einer Minute gesendeten E-Mails von derselben IP-Adresse diese Zahl überschreitet, werden E-Mails von dieser IP-Adresse blockiert, bis die nächste Minute beginnt.
- **Es werden in einer Minute mehr als die festgelegten Verbindungen aufgebaut**: Sie können die maximale Anzahl an Verbindungen innerhalb einer Minute festlegen. Wenn die Anzahl der Verbindungen mit derselben IP-Adresse diese Zahl innerhalb einer Minute überschreitet, werden Verbindungen blockiert, bis die nächste Minute beginnt.



Erweiterte Einstellungen

1. Gehen Sie zu **Mailübermittlung** > **Sicherheit**.
2. Im Bereich **Erweitert** können Sie Sicherheitseinstellungen für die Mailübermittlung anpassen:
   - **Unbefugte Pipelining-Anforderungen zurückweisen**: Lehnt Verbindungen ab, die fortlaufend SMTP-Anfragen senden.
   - **HELO-Hostnamen ohne voll qualifizierten Domainnamen (FQDN) zurückweisen**: Lehnt Verbindungen ab, wenn Hostnamen bei HELO oder EHLO unvollständige Domainnamen aufweisen.
   - **Unbekannte HELO-Hostnamen ablehnen**: Lehnt Verbindungen ab, wenn Hostnamen bei HELO oder EHLO über keinen DNS A- oder MX-Eintrag verfügen.
   - **Alle IPs blockieren, die mehr als den Grenzwert für nicht existierende Konten mailen**: Blockiert die IP-Adresse eines Benutzers bis zum nächsten Tag, wenn der Benutzer mit derselben IP-Adresse an einem Tag mehr als den Grenzwert an E-Mails an nicht existierende Konten in MailPlus Server sendet.
   - **Max. Junk-Befehle pro Sitzung**: Wenn die Anzahl der verbundenen Clients die angegebene Anzahl an Junk-Befehlen (NOOP, VRFY, ETRN und RSET) innerhalb derselben



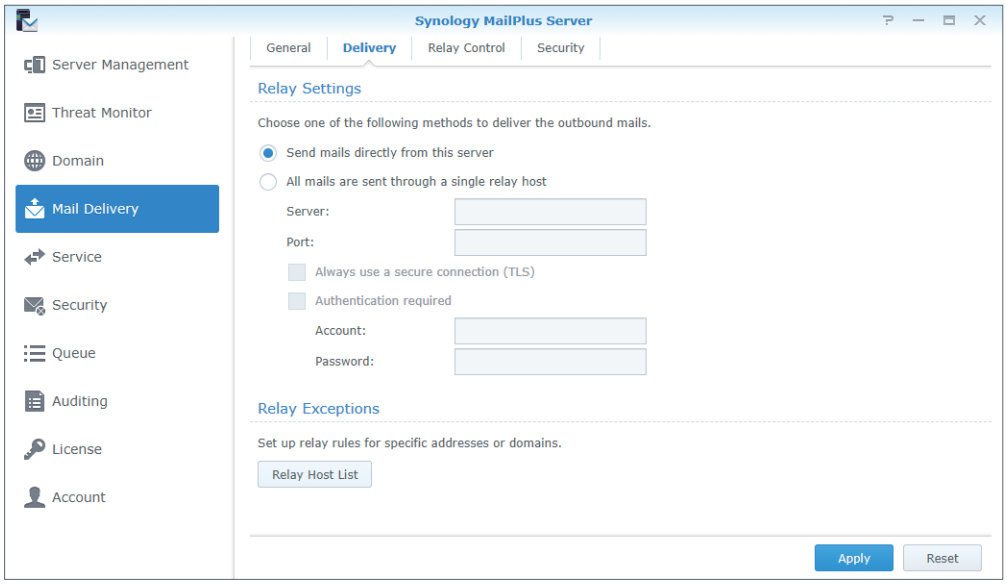
Mail-Relay

Wenn Sie E-Mails über andere Server versenden oder E-Mails für andere Server versenden/empfangen möchten, können Sie Mail-Relay, SMTP-Authentifizierung, Verschlüsselung und andere bereitgestellte Sicherheitsfunktionen konfigurieren.

Übermittlungssteuerung einrichten

Auf der Registerkarte **Übermittlung** können Sie Einstellungen von MailPlus Server konfigurieren, um E-Mails über bestimmte Server weiterzuleiten, damit alle ausgehenden E-Mails über den angegebenen Server versendet werden.

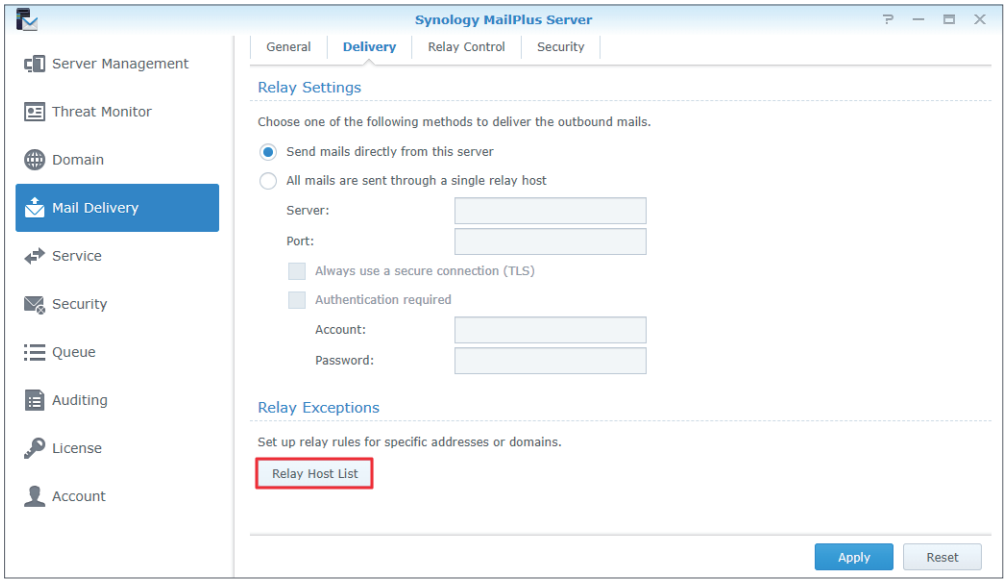
1. Gehen Sie zu **Mailübermittlung** > **Übermittlung** > **Relay-Einstellungen**.
2. Wählen Sie einen Regeltyp:
   - **E-Mails direkt von diesem Server senden**: Alle E-Mails werden direkt von MailPlus Server versendet.
   - **Alle E-Mails werden durch einen einzigen Relay-Host gesendet**: Alle E-Mails werden vom unten angegebenen Relay-Server gesendet. Geben Sie die IP-Adresse oder den Hostnamen des Relay-Servers in das Feld **Server** und seine Portnummer in das Feld **Port** ein. Nach Aktivierung dieser Option können Sie die nachfolgenden Sicherheitseinstellungen anpassen:
     - **Immer eine sichere Verbindung verwenden (TLS)**: MailPlus Server sendet STARTTLS, um verschlüsselte Verbindungen zu ermöglichen. Wenn MailPlus Server der Relay-Server ist, finden Sie **hier** weitere Informationen. In MailPlus Server lautet die standardmäßige TLS-Sicherheitsstufe **may**.
     - **Authentifizierung erforderlich**: Wenn Ihr Relay-Server die Authentifizierung aktiviert hat, geben Sie das Konto und Kennwort des Relay-Servers ein, um ihn für Mail-Relay zu verwenden.



Anmerkung:

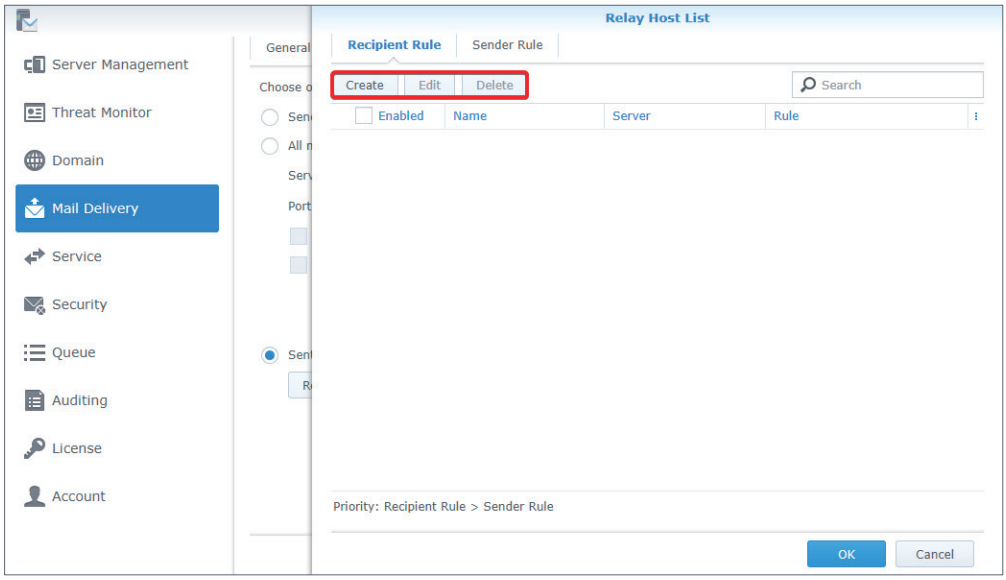
- STARTTLS und SMTPS unterscheiden sich. Wenn Sie SMTPS verwenden möchten, verfügt MailPlus Server über keine entsprechende Konfigurationsoberfläche. Informationen zur Konfiguration der Einstellungen finden Sie unter **wrappermode**.

E-Mails, die einer bestimmten Regel für E-Mail-Adressen oder Domains entsprechen, können über einen designierten Relay-Server versendet werden. Klicken Sie unter **Relay-Ausnahmen** auf **Relay-Hostliste**, um Regeln für Sender und Empfänger anzupassen.



- **Empfängerregel**: An festgelegte E-Mail-Adressen oder Domains gesendete E-Mails werden über einen designierten Relay-Server versendet. Die Priorität der Empfängerregeln ist höher als die der Absenderregeln.
- **Absenderregel**: Von festgelegten Adressen oder Domains gesendete E-Mails werden über einen designierten Relay-Server versendet.

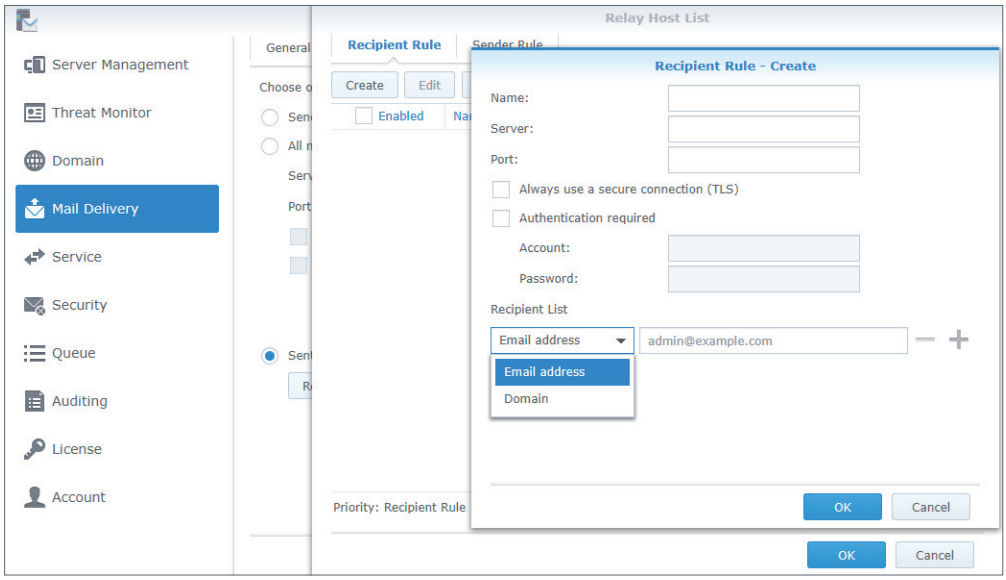
  a. Klicken Sie auf die Schaltfläche **Erstellen**, **Bearbeiten** oder **Löschen**, um Empfänger- und Absenderregeln zu verwalten.



b. Geben Sie einen Regelnamen ein und legen Sie einen Relay-Server und Port fest.

c. Bearbeiten Sie die **Empfängerliste** durch Auswahl einer E-Mail-Adresse oder Domain, damit die an den Server weitergeleiteten E-Mails unter den angegegebenen E-Mail-Adressen oder Domains empfangen werden.

d. Klicken Sie auf **OK**, um die Einstellungen zu speichern.



e. Klicken Sie auf **Übernehmen**, um die Einstellungen abzuschließen.

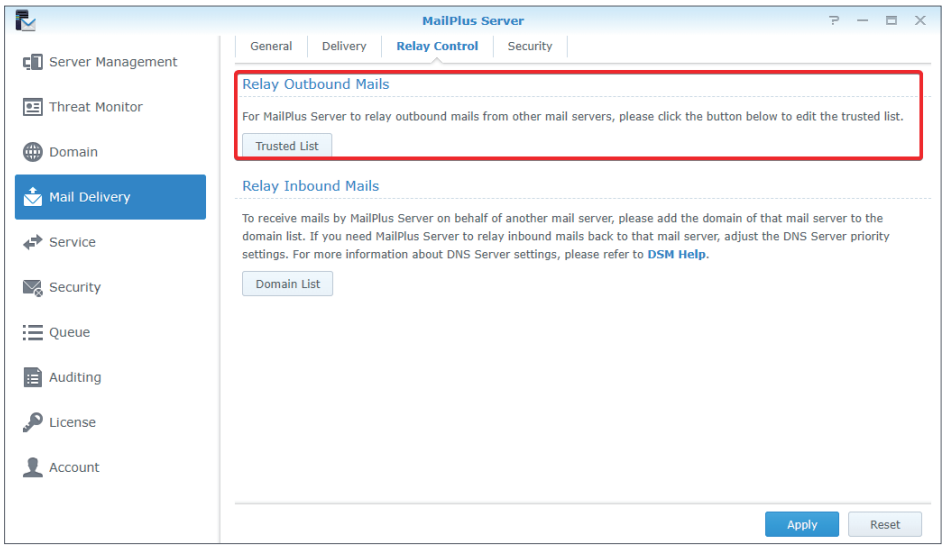
Relay-Steuerung einrichten

Auf der Registerkarte **Relay-Steuerung** können Sie die Einstellungen von MailPlus Server anpassen, damit es E-Mails für mehrere Mailserver senden oder empfangen kann.

- **Ausgehende E-Mails für andere Mailserver übermitteln**:

1. Gehen Sie zu **Mailübermittlung** > **Relay-Steuerung**.
2. Klicken Sie auf die Schaltfläche **Liste vertrauenswürdiger IPs** im Bereich **Ausgehende**

E-Mails übermitteln.



3. Klicken Sie auf **Erstellen** und geben Sie einen Regelnamen ein. Geben Sie IP-Adresse oder Subnetzmaske anderer Mailserver an.
4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

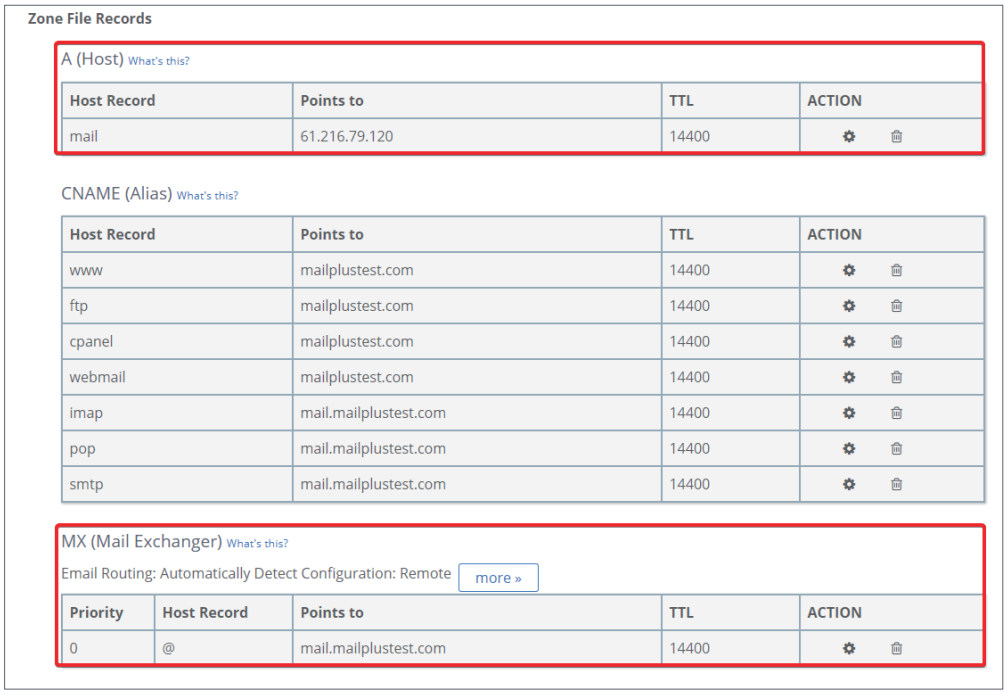
Anmerkung:

- Wenn Sie bei **Überprüfen, ob die E-Mail-Adressen des Absenders zu den Anmeldekonten gehören** auf der Registerkarte **Allgemein** ein Häkchen setzen, können E-Mails auf der **Liste vertrauenswürdiger IPs** von MailPlus Server abgelehnt werden. Sie können zur Registerkarte **Allgemein** wechseln und bei **Die Prüfung, ob die Absender-E-Mail-Adresse zum Anmeldekonto gehört, für von vertrauenswürdigen Netzwerken gesendete E-Mails überspringen** ein Häkchen setzen, um diese Prüfung zu überspringen. Wenn Sie auf der Registerkarte **Allgemein** bei **Authentifizierung für lokale Netzwerkverbindungen von Terminal überspringen** ein Häkchen setzen, werden E-Mails von lokalen Netzwerken nicht von MailPlus Server blockiert.

Eingehende E-Mails für andere Mailserver übermitteln

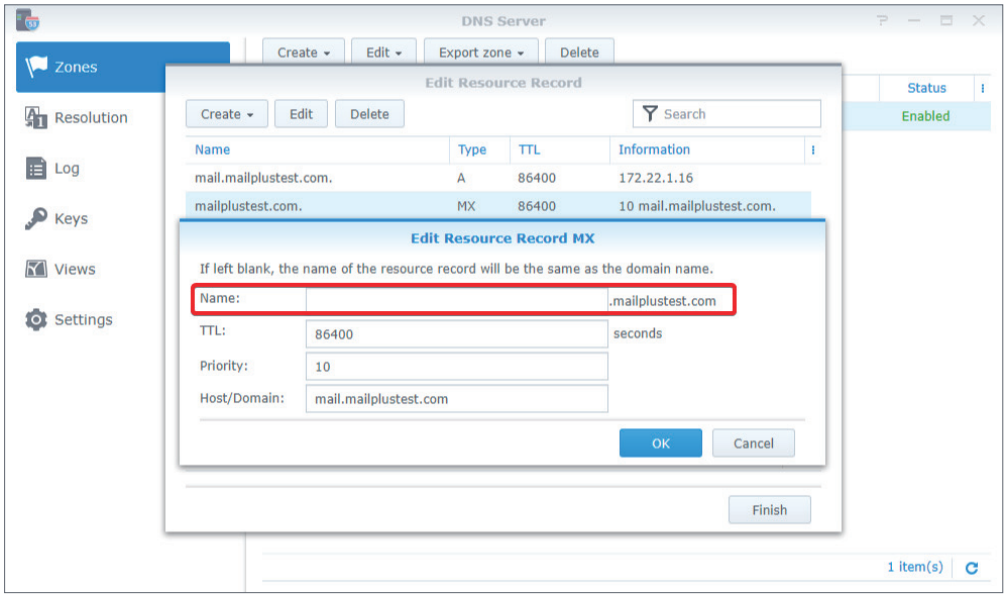
Um eingehende E-Mails für andere Mailserver zu übermitteln, richten Sie zuerst einen DNS-Eintrag ein. Sie können hierfür die folgenden Schritte beachten und zu **Domainliste** wechseln, um einen Mailserver hinzuzufügen. Wir verwenden hier einen externen Server und einen internen Server als Beispiel.

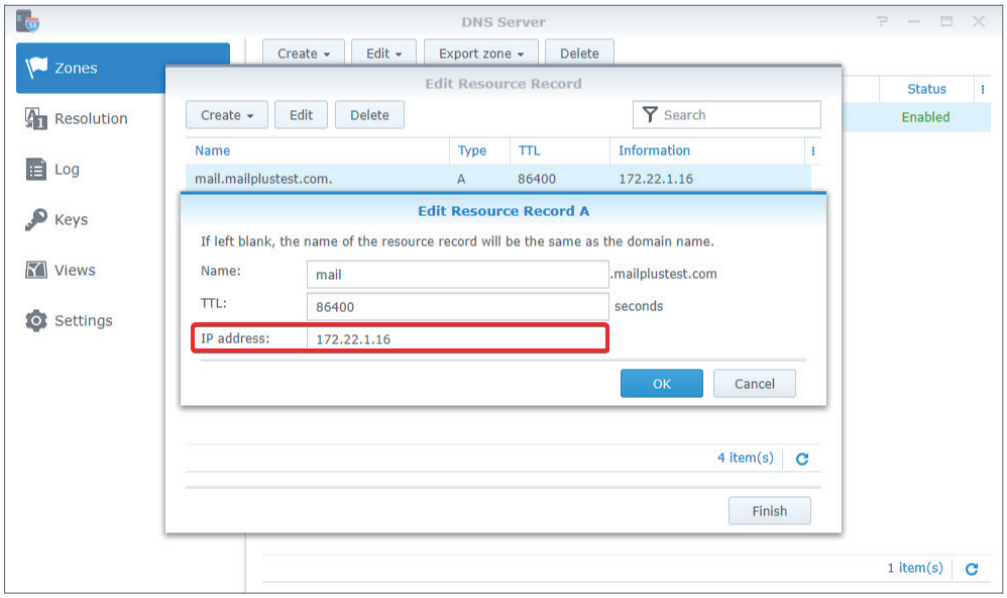
1. Richten Sie einen externen DNS-Server für MailPlus Server ein. Wir verwenden hier Bluehost® als Beispiel.
2. Passen Sie nach der Anmeldung bei Bluehost® die folgenden Einstellungen an. Tragen Sie Ihren Domainnamen im MX-Eintrag auf dem externen DNS-Server und die IP-Adresse von MailPlus Server im A-Eintrag ein. So können andere Mailserver basierend auf diesen DNS-Einträgen E-Mails an MailPlus Server senden.



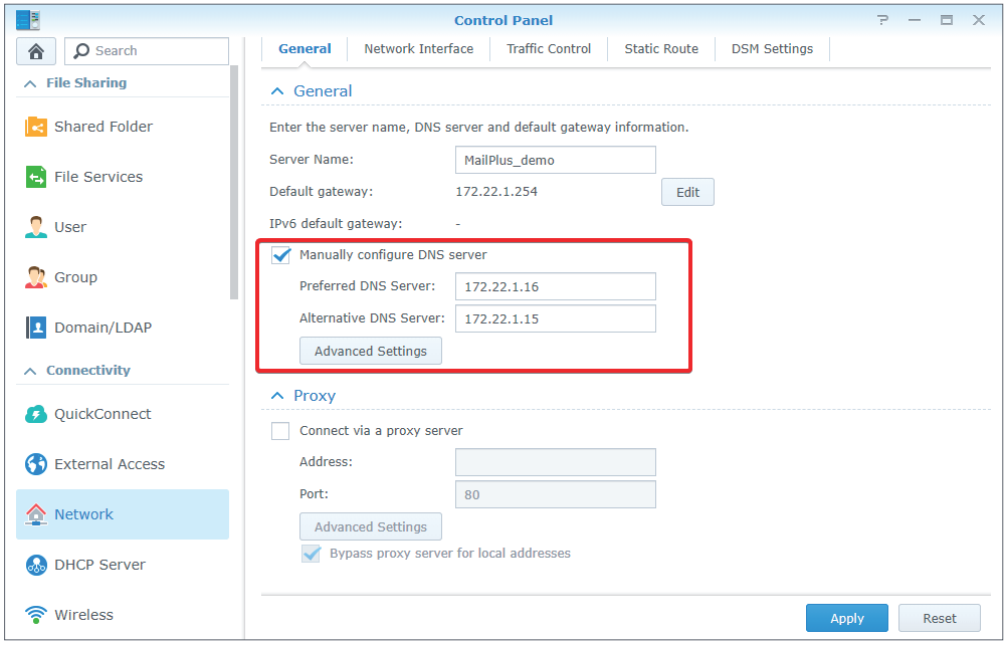
3. Richten Sie einen internen Synology DNS-Server ein, damit MailPlus Server Ihren primären Mailserver finden kann.

4. Tragen Sie Ihren Domainnamen im MX-Eintrag auf dem internen DNS-Server und die IP-Adresse der Domain im A-Eintrag ein. Die Priorität der DNS-Einträge auf dem internen DNS-Server muss höher sein als jene auf dem externen DNS-Server.

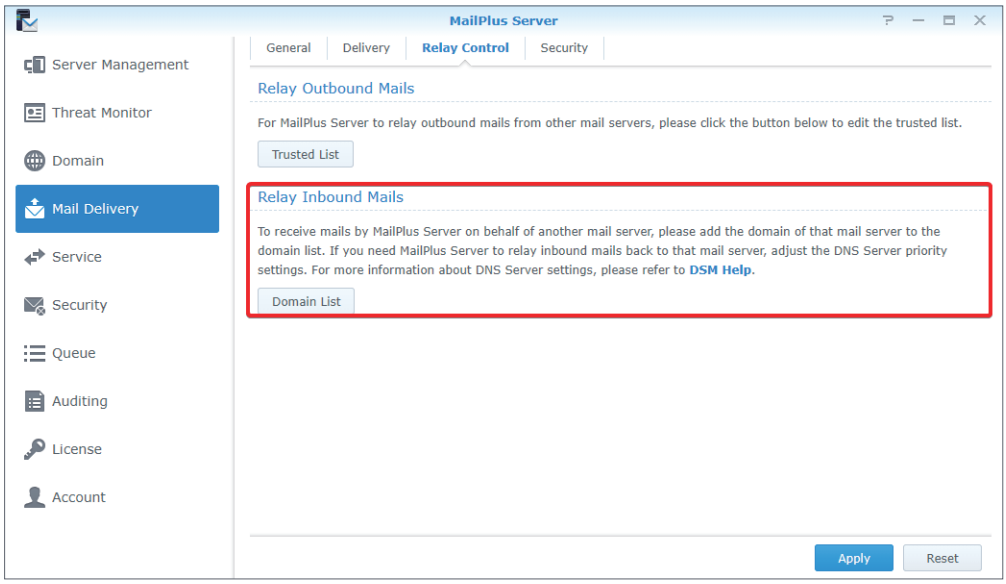




5. Gehen Sie zu **DSM** > **Systemsteuerung** > **Netzwerk** > **Allgemein** und markieren Sie das Kontrollkästchen **DNS-Server manuell konfigurieren**. Geben Sie die IP-Adresse des internen DNS-Servers in das Feld **Bevorzugter DNS-Server**, und die IP-Adresse des externen DNS-Servers in das Feld **Alternativer DNS-Server** ein, um sicherzustellen, dass die internen und externen Verbindungen von MailPlus Server ordnungsgemäß funktionieren können. Wenn MailPlus Server E-Mails empfängt, überprüft es die MX-Einträge der beiden DNS-Server und sendet E-Mails an den Mailserver mit höherer Priorität.

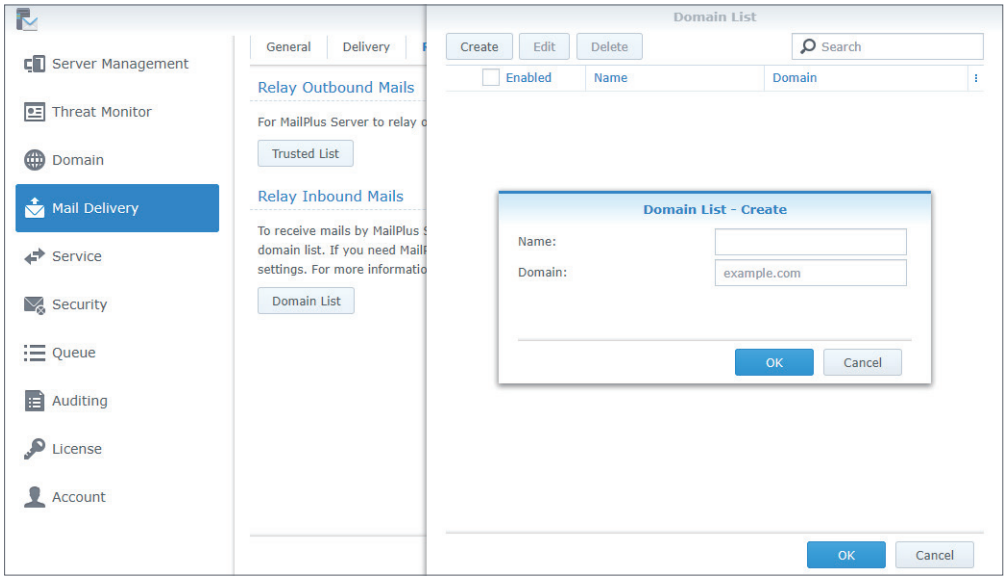


6. Starten Sie MailPlus Server und gehen Sie zu **Mailübermittlung** > **Relay-Steuerung**.
   Klicken Sie im Bereich **Eingehende E-Mails übermitteln** auf die Schaltfläche **Domainliste**.



7. Klicken Sie auf die Schaltfläche **Erstellen**.

8. Geben Sie den Namen der Regel und die Domain ein.



9. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Anmerkung:

- Auch wenn E-Mails intern gesendet werden, sollten Sie die Sicherheitseinstellungen auf den Registerkarten **Spam** und **Antivirenprogramm** der Seite **Sicherheit** konfigurieren, um böswillige E-Mails zu vermeiden.
- Da Sicherheitseinstellungen aktiviert sind, können Sie E-Mails unter **Mailübermittlung** > **Sicherheit** zur Whitelist hinzufügen, um eine Blockierung zu vermeiden.
- Das Netzwerksegment aller Server sollte identisch sein.

Kapitel 8: Domäneneinstellungen

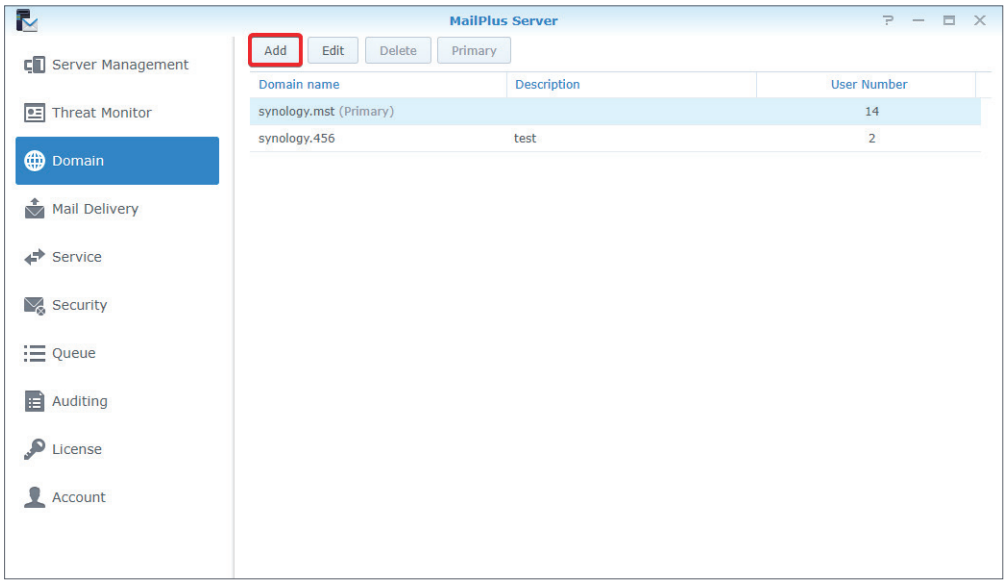
Domain

Sie können mehrere E -Mail-Domains in einem einzigen MailPlus Server hosten, um E-Mails zu zentralisieren, die an Ihre Domains gesendet werden. Sie können auch Aliasnamen, autom. BCC-Weiterleitung, Nutzungslimits und Fußzeilen für jede Domain anpassen.

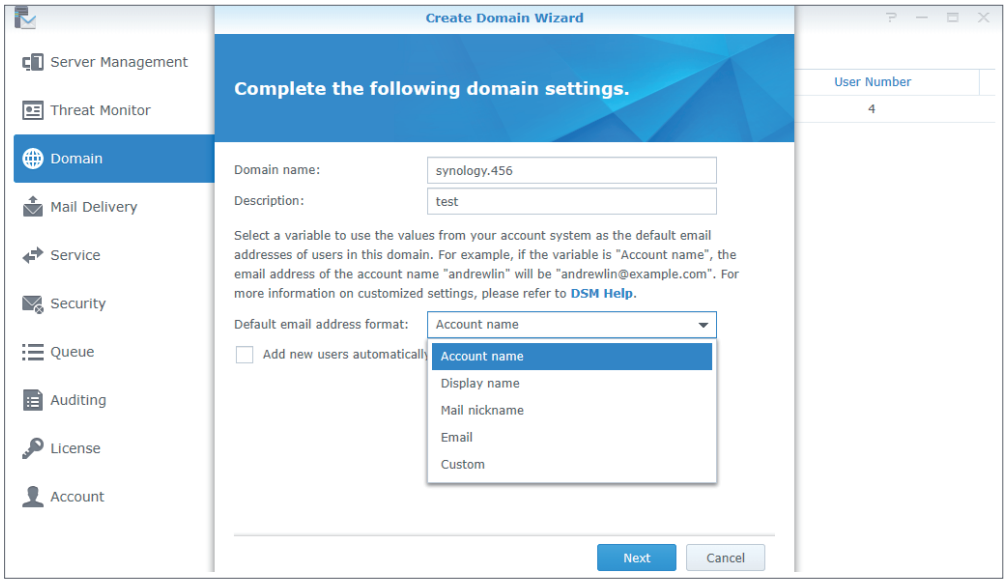
Eine Domain in MailPlus Server erstellen

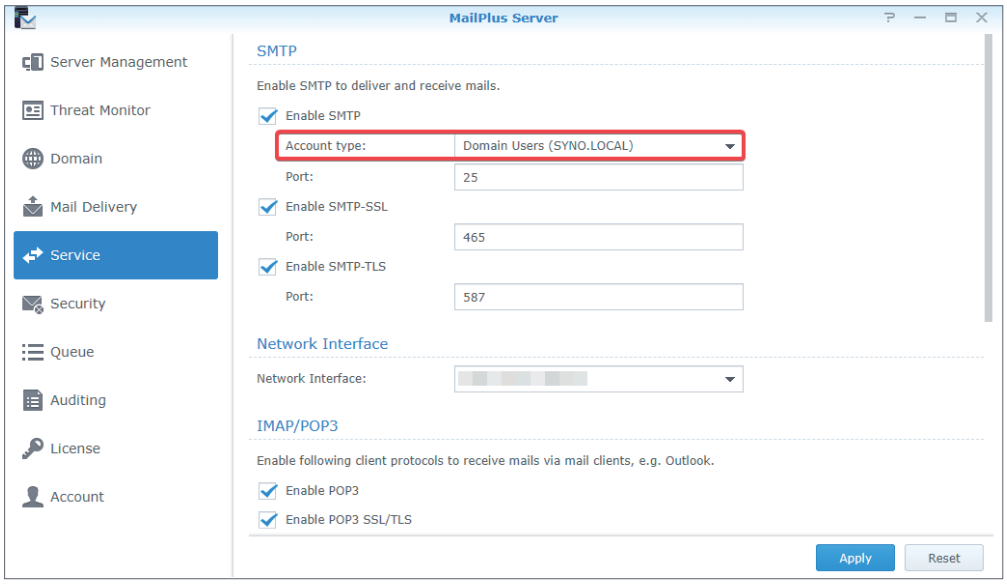
Melden Sie sich bei MailPlus Server an und gehen Sie zu **Domain**, um eine neue Domain zu erstellen. In diesem Abschnitt wird ***synology.456*** zur Veranschaulichung verwendet.

1. Gehen Sie zu **Domain** und klicken Sie auf die Schaltfläche **Hinzufügen**.



2. Tragen Sie den Domainnamen ***synology.456*** und ihre Beschreibung ein.
3. Wenn Sie Mitglieder zu der Domain hinzufügen, ruft MailPlus Server Informationen vom Kontosystem basierend auf den Einstellungen von **Standard-Adressformat für E-Mails** ab. Sie können **Kontoname**, **Angezeigter Name**, **E-Mail-Spitzname**, **E-Mail**, oder **Benutzerdefiniert** entsprechend dem Kontotyp auswählen, den Sie unter **Dienst** > **SMTP** > **Kontotyp** eingestellt haben.





Die folgende Tabelle zeigt die Standardeinstellungen an, die MailPlus Server für jeden Kontotyp bereitstellt.

Kontotyp	Standardeinstellungen
Lokale Benutzer	Kontoname E-Mail-Spitzname
LDAP-Benutzer	Kontoname E-Mail-Spitzname
Domainbenutzer	Kontoname Angezeigter Name E-Mail-Spitzname E-Mail

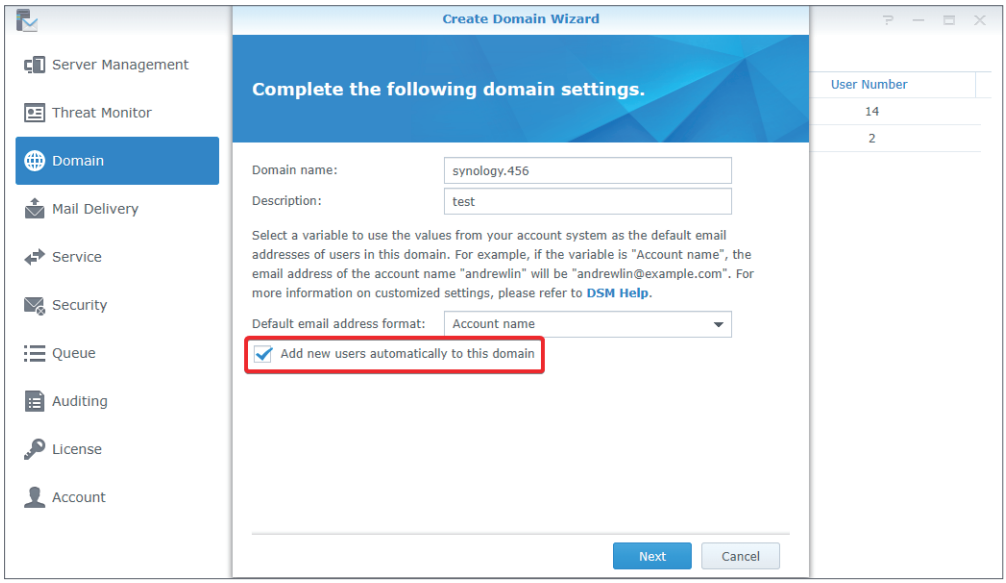
4. Neben den oben angeführten Optionen können Sie auch **Benutzerdefiniert** auswählen, um Variablen in das Feld **Benutzerdefinierte Variablen** als Standard-Adressformat für E-Mails einzugeben. Die folgende Tabelle zeigt die von MailPlus Server unterstützten Variablen:

Variable	Wert
<a>	Kontoname
<g>	Vorname
<i>	Anfangsbuchstabe zweiter Vorname
<s>	Nachname
<d>	Angezeigter Name
<m>	E-Mail-Spitzname
<xa>	Verwendet die ersten x Buchstaben eines Kontonamens. Bei x = 2 werden beispielsweise die ersten beiden Buchstaben des Kontonamens verwendet.
<xs>	Verwendet die ersten x Buchstaben eines Nachnamens. Bei x = 2 werden beispielsweise die ersten beiden Buchstaben des Nachnamens verwendet.
<xg>	Verwendet die ersten x Buchstaben eines Vornamens. Bei x = 2 werden beispielsweise die ersten beiden Buchstaben des Vornamens verwendet.
<benutzerdefiniertes Attribut>	Sie können auch eine von Ihrem Kontosystem unterstützte Variable eingeben, um den entsprechenden Wert abzurufen.

Die von MailPlus Server unterstützten Variablen variieren je nach dem unter **Dienst** > **SMTP** gewählten Kontosystem. Weitere Details entnehmen Sie bitte der folgenden Tabelle:

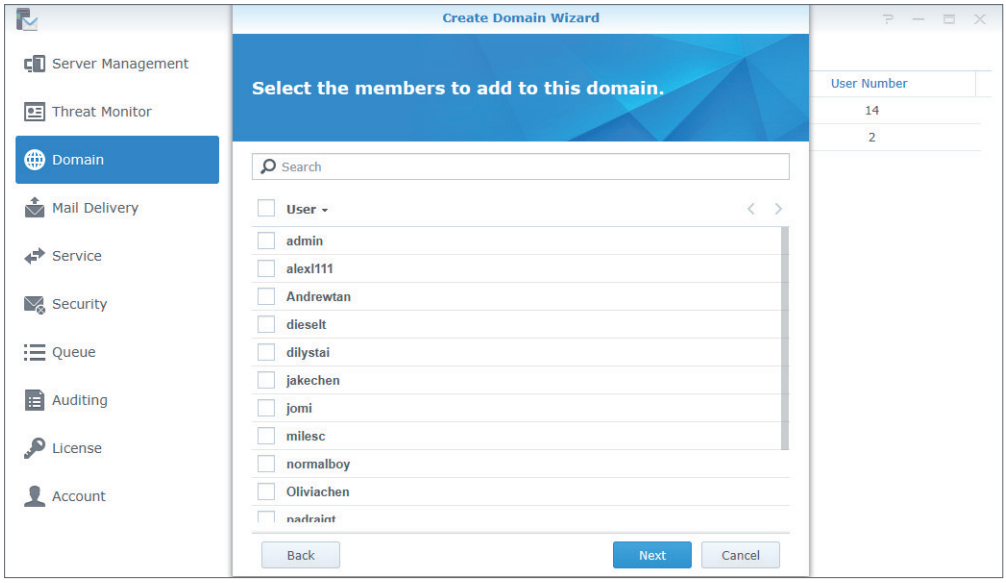
Variable	Lokale Benutzer	LDAP-Benutzer	Domainbenutzer
<a>	O	O	O
<g>	X	X	O
<i>	X	X	O
<s>	X	X	O
<d>	X	X	O
<m>	O	O	O
<xa>	O	O	O
<xs>	X	X	O
<xg>	X	X	O
<benutzerdefiniertes Attribut>	X	O	O

5. Benutzer können das Kontrollkästchen **Neue Benutzer automatisch zu dieser Domäne hinzufügen** markieren, um neue Benutzer automatisch zur Domain hinzuzufügen. MailPlus Server ruft die Informationen ab, um Benutzer-E-Mail-Adressen auf der Grundlage des Standard-Adressformats für E-Mails zu verfassen.



6. Klicken Sie nach der Einrichtung auf **Weiter**.

7. Fügen Sie Benutzer zu dieser Domain hinzu und klicken Sie auf **Weiter**, um die Mitglieder von ***synology.456*** zu überprüfen.



8. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

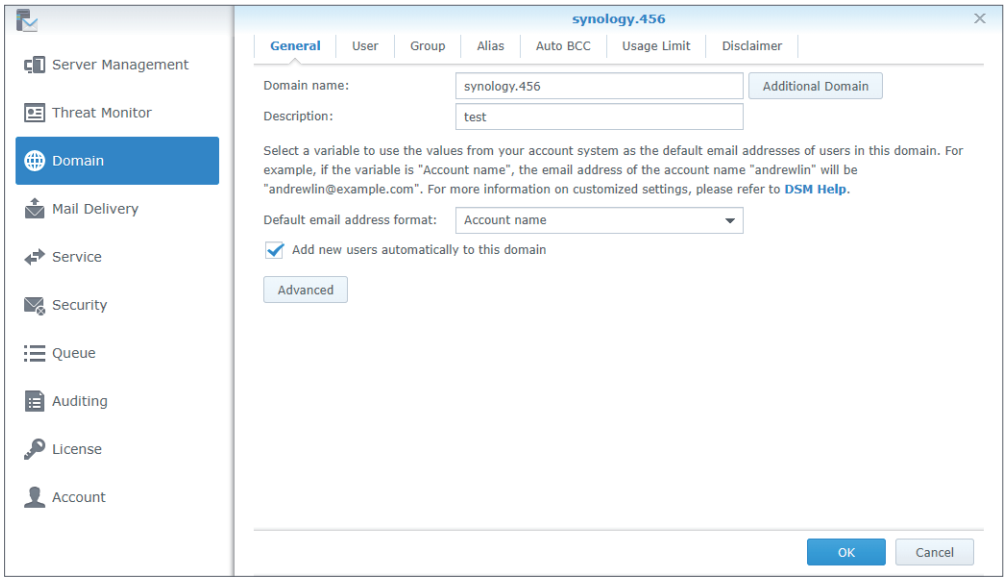
Domainverwaltung

MailPlus Server bietet Verwaltungseinstellungen für Administratoren und Benutzer in jeder Domain.

- **Allgemein**: Sie können Domainnamen und Domainbeschreibung bearbeiten, das Standard-Adressformat für E-Mails ändern, eine zusätzliche Domain erstellen, DKIM-Signierung bei ausgehenden E-Mails aktivieren sowie Catch-All aktivieren, um E-Mails zu erhalten, die an nicht vorhandene oder in einer bestimmten Domain nicht aktivierte E-Mail-Adressen gesendet wurden.
- **Benutzerkonten**: Sie können neue Mitglieder zu einer Domain hinzufügen und Rollen, wie z. B. **Domänenadmininstrator** und **Gewöhnlicher Benutzer** für Benutzer unter dieser Domain auswählen.
- **Gruppenkonten**: Sie können Mitglieder als Gruppe zu einer Domain hinzufügen, damit die Benutzer in der Gruppe über dieselben Rolleneinstellungen verfügen können.
- **Alias**: Sie können einen Alias für einen oder mehrere Empfänger erstellen. Wenn eine E-Mail an einen Alias gesendet wird, stellt der Server sie automatisch an alle Benutzer im Alias zu. Ein Alias kann auch externe E-Mail-Adressen enthalten.
- **Automatische BCC**: Sie können das System basierend auf bestimmten Kriterien für Absender, Empfänger oder alle Nachrichten automatisch eine Blindkopie (BCC = Blind Carbon Copy) an eine bestimmte Adresse senden lassen.
- **Grenzwert für Senden und Tagesquote**: Sie können die Anzahl der ausgehenden Nachrichten beschränken und Limits für den Datenverkehr festlegen.
- **Fußzeile**: Sie können Bedingungen konfigurieren, um Fußzeilen (Disclaimer) anzuhängen und deren Inhalt je nach Bedarf anzupassen. Basierend auf Ihren Einstellungen werden Disclaimer automatisch am Ende ausgehender E-Mails angehängt.

Allgemeine Einstellungen für eine Domain bearbeiten

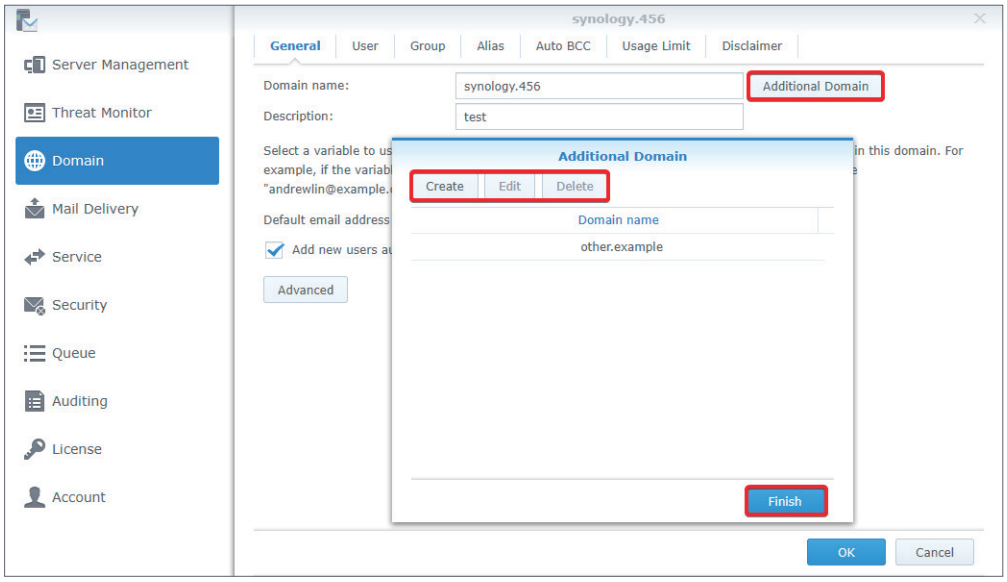
Auf der Registerkarte **Allgemein** können Sie Domain-Informationen bearbeiten, das Standard-Adressformat für E-Mails anpassen und neue Benutzer automatisch zu ***synology.456*** hinzufügen.



Zusätzliche Domains erstellen und bearbeiten

Im Fenster **Zusätzliche Domain** können Sie zusätzliche Domainnamen für den Host erstellen, um E-Mails zu empfangen. Die Einstellungen von zusätzlichen Domains folgen den Einstellungen von ***synology.456***.

1. Gehen Sie zu **Domain** > ***synology.456*** > **Allgemein** und klicken Sie auf die Schaltfläche **Zusätzliche Domain**.
2. Klicken Sie auf die Schaltfläche **Erstellen**, um eine zusätzliche Domain zu erstellen. Wenn Sie bearbeiten oder löschen möchten, wählen Sie Ihre Zieldomain aus und klicken Sie auf die entsprechenden Aktionsschaltflächen.
3. Auf der Seite **Zusätzliche Domain** können Sie alle zusätzlichen Domains anzeigen, die Sie erstellt haben. Entsprechend des obigen Beispiels können Sie zusätzlich zum Empfang von E-Mails von der Domain ***synology.456*** auch E-Mails von einer weiteren Domain empfangen, wenn sie als Empfänger enthalten ist.
4. Klicken Sie auf **Fertig stellen**, um die Einstellungen zu speichern.



Anmerkung:

- MX-Einträge auf DNS Server erfordern möglicherweise entsprechende Anpassungen.

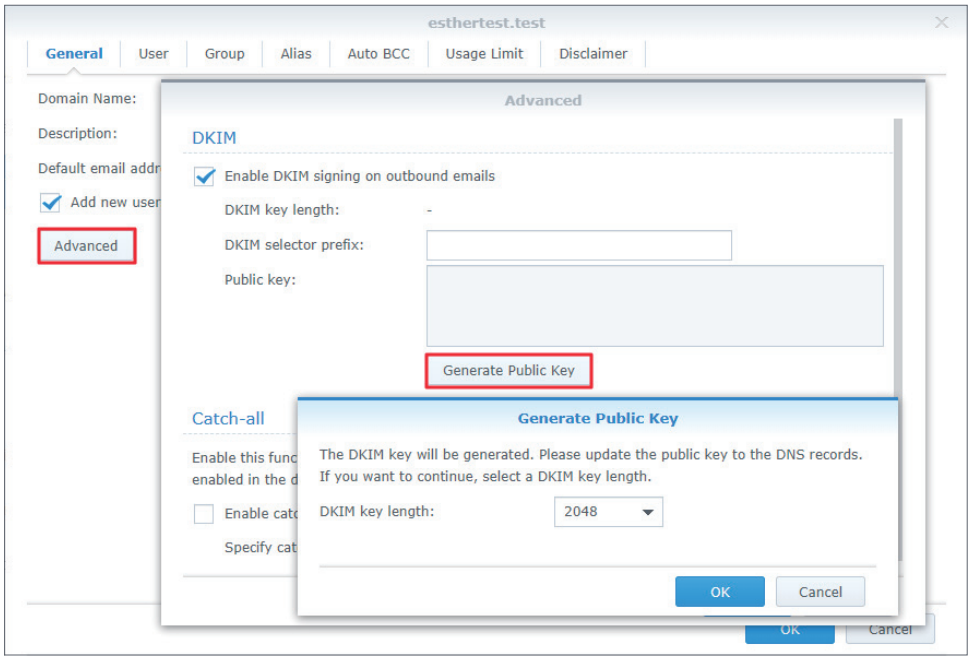
Erweiterte Einstellungen anpassen

1. Gehen Sie zu **Domain** > ***synology.456*** > **Bearbeiten** > **Allgemein** und klicken Sie auf die Schaltfläche **Erweitert**.
2. Im eingeblendeten Fenster **Erweitert** können Sie die Einstellungen von **DKIM** und **Catch-All** für ***synology.456*** anpassen.
   - **DKIM**: Sie können die DKIM-Signierung aktivieren, um Identitätsdiebstahl zu vermeiden und zu verhindern, dass Nachrichten geändert werden.
     a. Markieren Sie im Bereich **DKIM** das Kontrollkästchen **DKIM-Signierung bei ausgehenden E-Mails aktivieren**, wenn Sie Identitätsdiebstahl verhindern und die Vertrauenswürdigkeit Ihrer gesendeten Nachrichten für Empfänger gewährleisten möchten. Sie können die DKIM-Signatur wie folgt anpassen:
        - **DKIM-Auswahlpräfix**: Das zu einer DKIM-Signatur hinzugefügte Präfix. Sie können ein DKIM-Auswahlpräfix nach Wahl eingeben.
        - **Öffentlicher Schlüssel**: Der Inhalt eines öffentlichen Schlüssels. Wenn das System bei Aktivierung der DKIM-Signierung über keinen öffentlichen und privaten Schlüssel verfügt, werden Schlüssel automatisch generiert.

     b. Klicken Sie auf die Schaltfläche **Öffentlichen Schlüssel generieren**, um eine neue Gruppe des öffentlichen und privaten Schlüssels zu erstellen. Das System erstellt standardmäßig 2048-Bit-Schlüssel. (Wenn der DKIM-Schlüssel abgelehnt wird, ändern Sie die Schlüssellänge bitte auf 1024 oder 512 Bit.)

Anmerkung:

- Vorhandene Schlüssel werden gelöscht, wenn Sie auf die Schaltfläche **Öffentlichen Schlüssel generieren** klicken.



c. Klicken Sie auf **OK**, um die Einstellungen zu speichern. Um sicherzustellen, dass DKIM-Signaturen von anderen empfangenden Servern authentifiziert werden können, müssen Sie außerdem einen DNS TXT-Datensatz erstellen, um die DKIM-Authentifizierung zu ermöglichen:

   Das Format eines TXT-Datensatzwertes: **v=DKIM1; k=rsa; p=DKIM public key**

   Beispiel: Wenn die Domain von MailPlus Server ***beispiel.com*** lautet, ist das DKIM-Auswahlpräfix ***abc*** und der vom System erstellte öffentliche Schlüssel lautet *MIGfMA0GCSqGSIb3DQE*. Ihr TXT-Datensatz sollte wie folgt lauten:

   - **TXT-Datensatzname**: *abc._domainkey.beispiel.com*
   - **TXT-Datensatzwert**: *v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQE*

- **Catch-All**: Aktivieren Sie **Catch-All**, um ein Benutzerkonto als Catch-All-Postfach für den Empfang von E-Mails einzurichten, die an nicht vorhandene oder in der Domain nicht aktivierte E-Mail-Adressen gesendet werden.

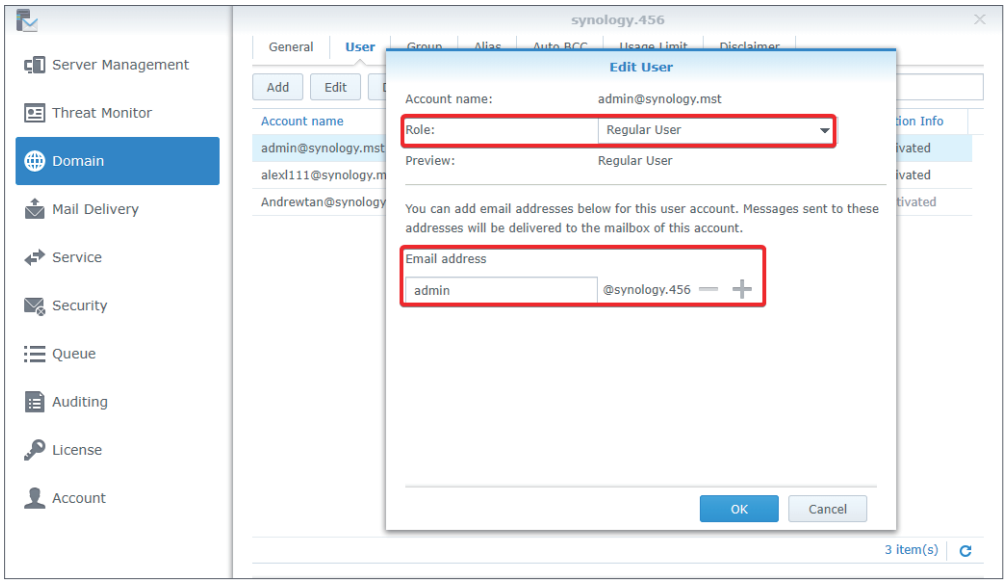
Benutzerkonten zu einer Domain hinzufügen

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zur Registerkarte **Benutzer** und klicken Sie auf **Hinzufügen**.
3. Wählen Sie Benutzerkonten aus.
4. Bestätigen Sie die E-Mail-Adressen der ausgewählten Benutzer.

Benutzerkonten bearbeiten und entfernen

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Wählen Sie auf der Registerkarte **Benutzer** ein Konto aus, und klicken Sie auf **Bearbeiten**.

3. Passen Sie im Fenster **Benutzer bearbeiten** die folgenden Einstellungen an:
   - **Rolle**: Wählen Sie eine Rolle aus dem Dropdown-Menü aus:
     - **Domänenadministrator**: Administratoren können alle Domaineinstellungen verwalten, außer dem Erstellen und Löschen von Domains.
     - **Gewöhnlicher Benutzer**: Gewöhnliche Benutzer sind nicht berechtigt, Domains zu verwalten.
     - **Gruppeneinstellungen folgen**: Die Berechtigungen werden von den Gruppeneinstellungen des Benutzers in der Domain bestimmt.
   - **E-Mail-Adresse**: Sie können mehrere E-Mail-Adressen eingeben. An diese Adressen gesendete Nachrichten werden an das Postfach dieses Kontos übermittelt.



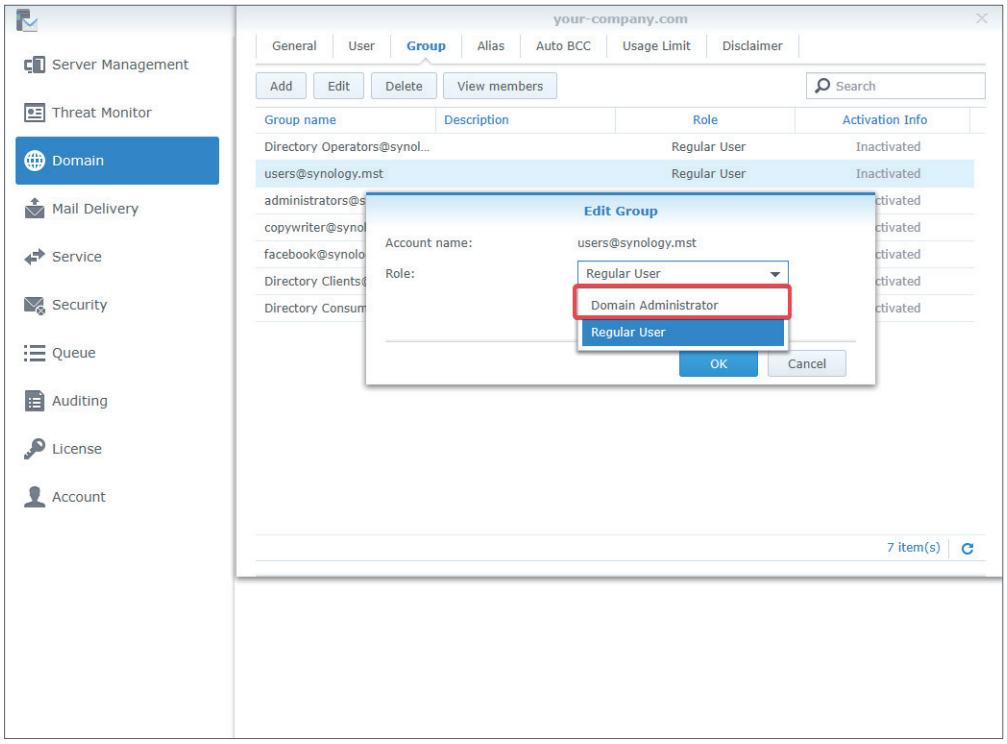
4. Wenn Sie ein Benutzerkonto entfernen möchten, wählen das Konto des Zielbenutzers aus und klicken Sie auf **Löschen**.

Gruppen zu einer Domain hinzufügen

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zur Registerkarte **Gruppe** und klicken Sie auf **Hinzufügen**.
3. Wählen Sie Benutzergruppen aus und klicken Sie auf **Weiter**.
4. Bestätigen Sie die E-Mail-Adressen der Mitglieder. Klicken Sie auf **Übernehmen**.

Gruppen bearbeiten und entfernen

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Wählen Sie in der Registerkarte **Gruppe** eine zu bearbeitende Gruppe aus, und klicken Sie auf **Bearbeiten**.
3. Im Fenster **Gruppe bearbeiten** können Sie **Domänenadministrator** im Dropdown-Menü **Rolle** auswählen, damit alle Benutzer in der Gruppe über die Rechte als **Domänenadministrator** verfügen.

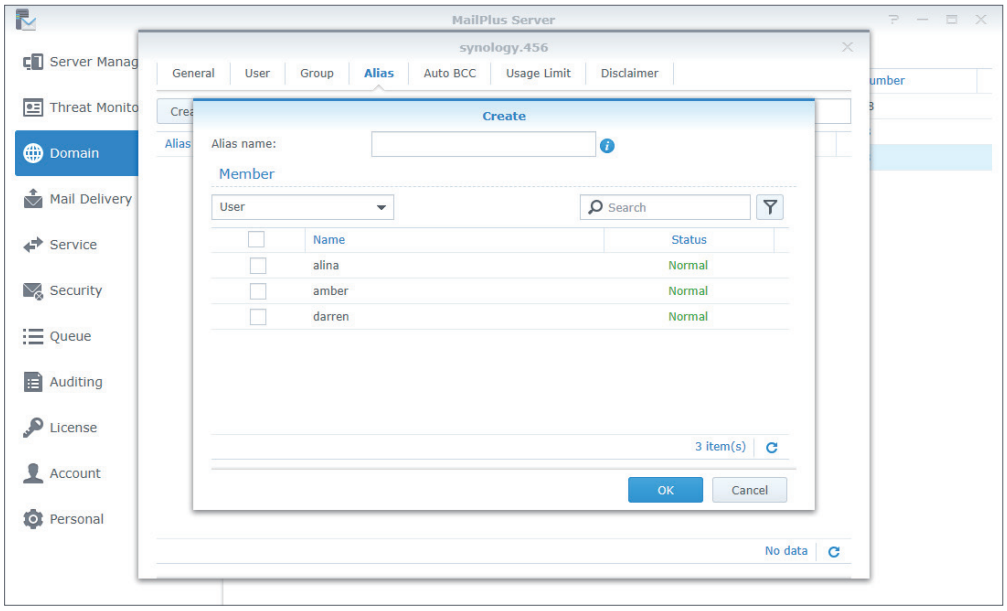


4. Wählen Sie die Gruppe aus, die Sie entfernen möchten, und klicken Sie auf die Schaltfläche **Löschen**.
5. Sie können auf die Schaltfläche **Mitglieder anzeigen** klicken, um zu überprüfen, ob sich bestimmte Benutzer der Gruppe nicht in dieser Domain befinden.

Aliasnamen erstellen

Sie können Aliasnamen erstellen, damit Benutzer E-Mails an mehrere Empfänger mit einem Alias senden können.

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zu **Alias** und klicken Sie auf die Schaltfläche **Erstellen**.
3. Geben Sie im Feld **Aliasname** den Namen des Alias ein.
4. Treffen Sie eine Auswahl aus dem Dropdown-Menü, um Aliasnamen, Benutzer, Gruppen oder externe Postfächer anzuzeigen.



5. Fügen Sie Benutzer zum Alias hinzu, indem Sie die Kontrollkästchen markieren.
6. Sie können Benutzer aus mehr als einer Quelle auswählen, einschließlich Benutzerkonten, Gruppenkonten und andere Aliasnamen.
7. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Aliasnamen bearbeiten und löschen

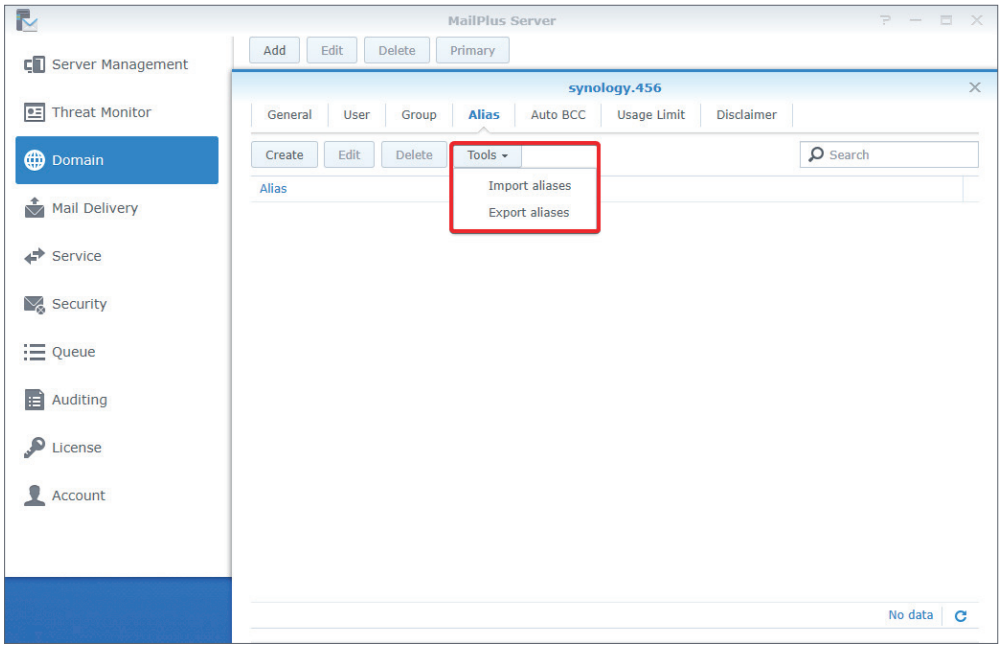
Gehen Sie wie folgt vor, um einen Alias zu bearbeiten oder zu löschen:

1. Gehen Sie zu **Domain**, wählen Sie ***synology.456*** und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zu **Alias** und wählen Sie den Alias aus, den Sie ändern möchten. (Sie können auch in der Suchleiste oben rechts auf der Seite nach Aliasnamen suchen.)
3. Klicken Sie auf die Schaltfläche **Bearbeiten** oder **Löschen**.

Aliasnamen importieren/exportieren

Wenn Sie vorhandene oder zuvor erstellte Aliaslisten importieren möchten, gehen Sie hierzu wie folgt vor:

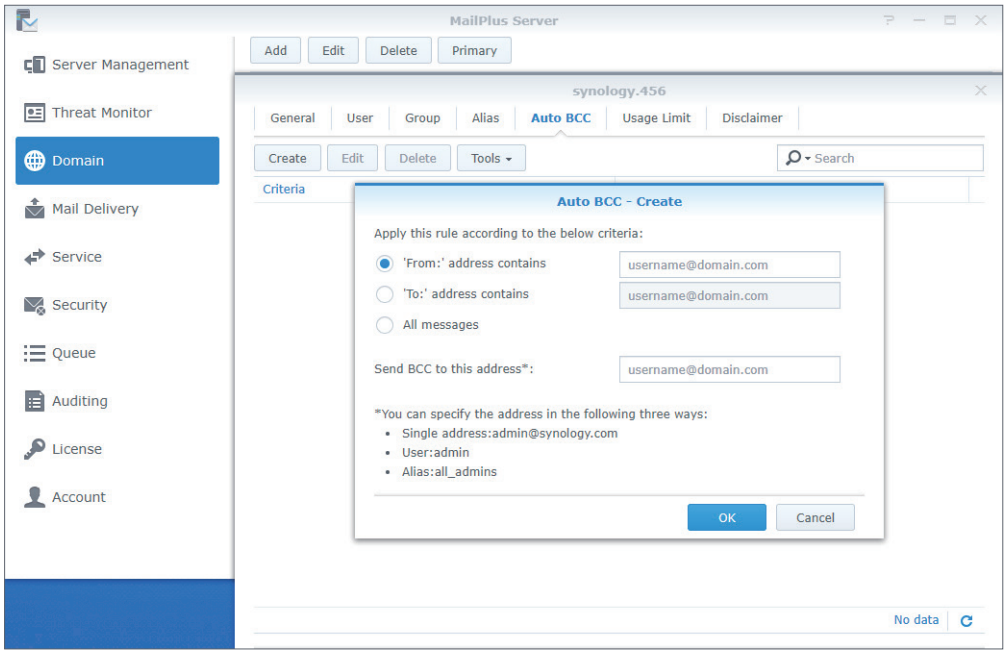
1. Gehen Sie zu **Domain**, wählen Sie ***synology.456*** und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zu **Alias** und klicken Sie auf die Schaltfläche **Extras**.
3. Wählen Sie aus, ob Aliasnamen importiert oder exportiert werden sollen:
   - **Aliasnamen importieren**: Wenn ein importierter Aliasname bereits vorhanden ist, wird er nicht importiert oder aktualisiert.
   - **Aliasnamen exportieren**: Aliasdateien werden exportiert und im Postfix-Format heruntergeladen.



Automatische BCC-Regeln erstellen

Mit den Einstellungen der autom. BCC-Weiterleitung können Sie eine Blindkopie (BCC = Blind Carbon Copy) an eine bestimmte Adresse senden, die auf bestimmten Kriterien für Absender, Empfänger oder alle Nachrichten basiert. Bitte gehen Sie wie folgt vor, um eine automatische BCC-Regel zu erstellen:

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zu **Automatische BCC** und klicken Sie auf die Schaltfläche **Erstellen**.
3. Geben Sie die Kriterien der automatischen BCC an:
   - **„Von:"-Adresse enthält**: Eine Blindkopie (BCC) wird automatisch gesendet, wenn die Information **MAIL FROM** im originalen Inhalt der E-Mail mit den hier eingegebenen Informationen übereinstimmt.
   - **„An:"-Adresse enthält**: Eine Blindkopie (BCC) wird automatisch gesendet, wenn die Information **RCPT TO** im originalen Inhalt der E-Mail mit den hier eingegebenen Informationen übereinstimmt.
   - **Alle Nachrichten**: Eine Blindkopie (BCC) wird automatisch für alle E-Mails gesendet, ausgenommen Benachrichtigungs-E-Mails des internen Systems.
4. Geben Sie die Adresse, an welche die Blindkopie automatisch gesendet wird, in das Feld **Als BCC an diese Adresse senden*** ein.
5. Sie können E-Mail-Adressen, Benutzerkonten oder Aliasnamen eingeben.



6. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Automatische BCC-Regeln bearbeiten und löschen

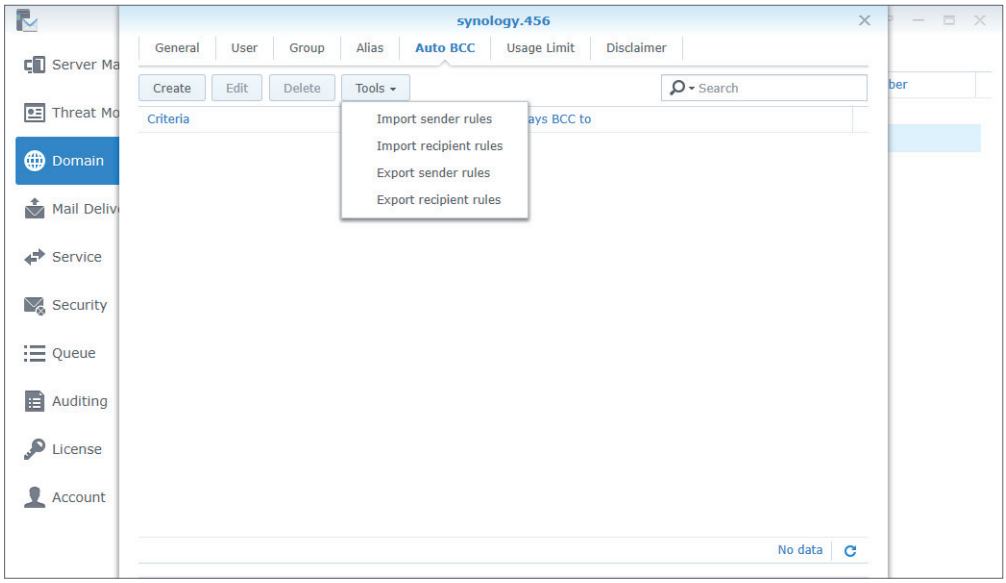
Gehen Sie wie folgt vor, um automatische BCC-Regeln zu bearbeiten oder zu löschen:

1. Gehen Sie zu **Domain**, wählen Sie ***synology.456*** und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zu **Automatische BCC** und wählen Sie die automatische BCC-Regel aus, die Sie ändern möchten.
3. Klicken Sie auf die Schaltfläche **Bearbeiten** oder **Löschen**.

Automatische BCC-Regeln importieren/exportieren

Gehen Sie wie folgt vor, um automatische BCC-Regeln zu importieren oder zu exportieren:

1. Gehen Sie zu **Domain**, wählen Sie ***synology.456*** und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zu **Automatische BCC** und klicken Sie auf die Schaltfläche **Extras**.
3. Wählen Sie aus, ob Absender- oder Empfängerregeln importiert oder exportiert werden sollen.

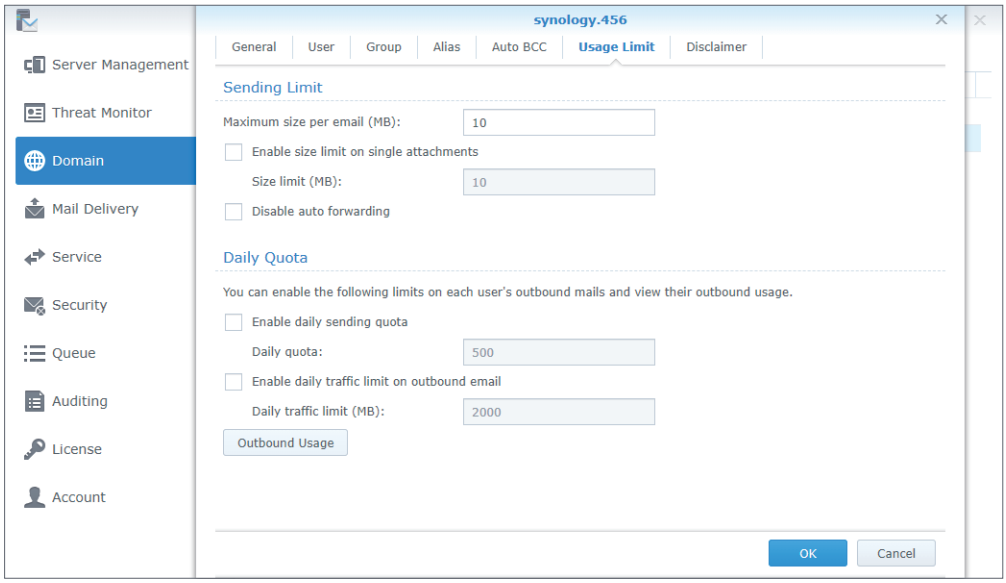


Anmerkung:

- **Das Importieren und Exportieren aller Nachrichtenregeln** ist hier nicht verfügbar, da diese Funktion bereits in der **grundlegenden Konfigurationsdokumentation** von Postfix enthalten ist. Informationen hierzu finden Sie unter **Immer als BCC**.
- Stellen Sie sicher, dass die importierten Dateien das Postfix-Format haben.

Grenzwert für Senden und Tagesquote einrichten

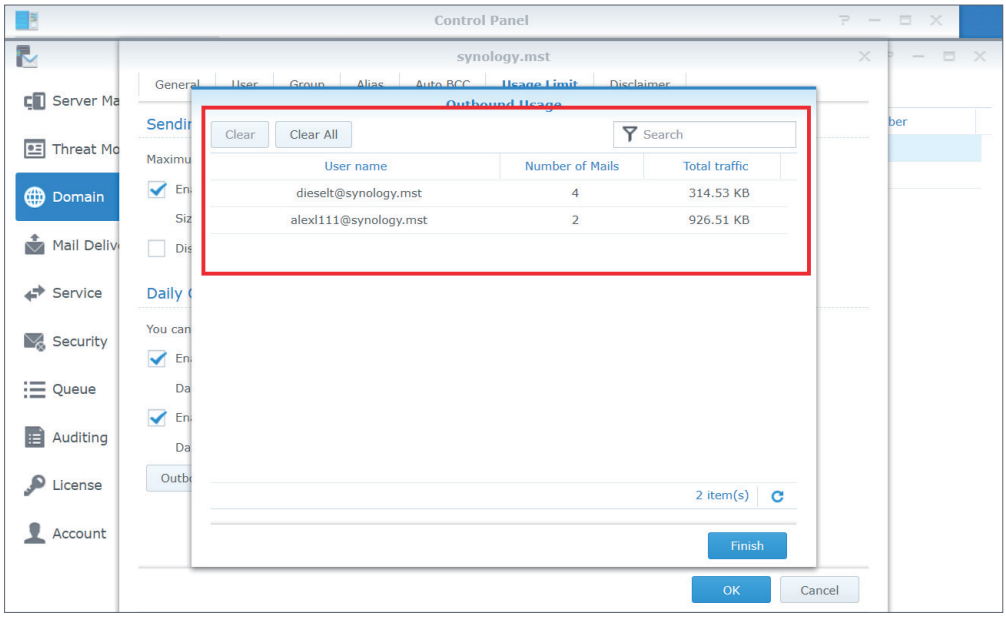
1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zur Registerkarte **Nutzungslimit**.
3. Passen Sie im Bereich **Grenzwert für Senden** die folgenden Einstellungen an:
   - **Maximale Größe für E-Mail (MB)**: Geben Sie die Größenbeschränkung für ausgehende E-Mails an.
   - **Größenbeschränkung auf einzelne Anhänge anwenden**: Geben Sie die Größenbeschränkung für einzelne Anhänge an. Geben Sie einen Wert im untenstehenden Feld **Größenbeschränkung (MB)** ein.
   - **Automatische Weiterleitung deaktivieren**
4. Passen Sie im Bereich **Tagesquote** die folgenden Einstellungen an:
   - **Tägliche Sendequote aktivieren**: Begrenzen Sie die Anzahl ausgehender Nachrichten, die ein Benutzer täglich versenden kann.
   - **Tägliches Traffic-Limit auf ausgehende E-Mails anwenden**: Beschränken Sie die Gesamtgröße der ausgehenden Nachrichten, die ein Benutzer täglich versenden kann.
   - **Ausgehende Mails**: Zeigen Sie Statistiken zu ausgehenden E-Mails für einzelne Benutzer an.



Ausgehende Mails

Sie können die gesamte Anzahl der hier verzeichneten ausgehenden Nachrichten anzeigen. Wenn ein Benutzer die Tagesquote erreicht hat, können Sie Einträge löschen, damit der Benutzer weiterhin E-Mails versenden kann.

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zur Registerkarte **Nutzungslimit** und klicken Sie auf die Schaltfläche **Ausgehende Mails**.
3. Wählen Sie einen bestimmten Benutzer aus der Liste aus. Sie können auch in der Suchleiste oben rechts nach Benutzern suchen.
4. Klicken Sie auf **Löschen**, um die Einträge der ausgehenden Mails des Benutzers zu löschen und Maileinträge zurückzusetzen. Klicken Sie auf die Schaltfläche **Alle löschen**, um die Maileinträge aller Benutzer auf der Liste zu löschen.



5. Klicken Sie auf **Fertig stellen**, um die Einstellungen abzuschließen.

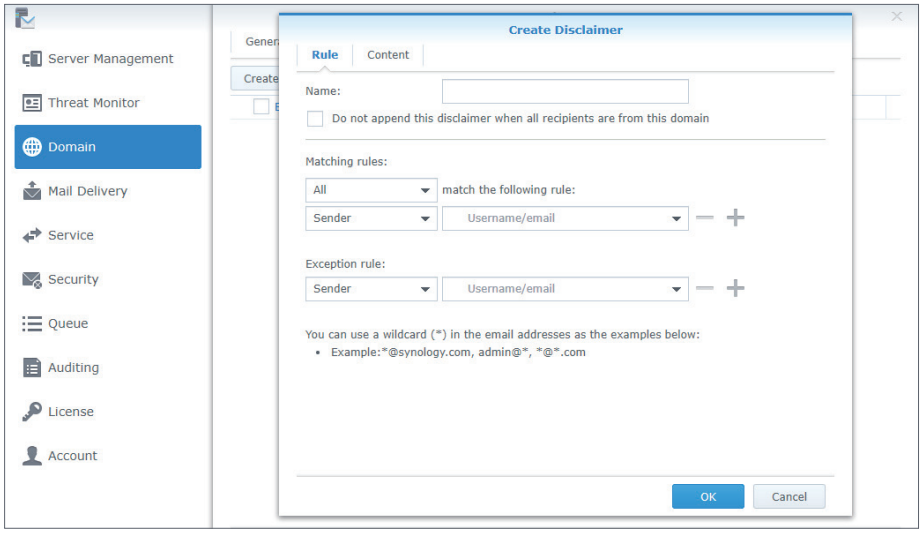
Fußzeilen erstellen

Mit der Fußzeilen-Funktion können Benutzer automatisch einen benutzerdefinierten Text auf der Unterseite oder am Ende von ausgehenden E-Mails hinzufügen. Gehen Sie wie folgt vor, um Fußzeilen zu erstellen:

Anmerkung:

- Sie können mehrere Fußzeilen und Regeln haben; es kann jedoch nur eine Fußzeile an eine E-Mail angehängt werden.

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zur Registerkarte **Fußzeile** und klicken Sie auf die Schaltfläche **Erstellen**.
3. Gehen Sie zur Registerkarte **Regeln** im Fenster **Fußzeile erstellen**.



4. Geben Sie den Namen der Fußzeile in das Feld **Name** ein.
5. Wählen Sie aus, ob das Kontrollkästchen **Diese Fußzeile nicht anhängen, wenn Nachricht nur an Empfänger in dieser Domain verschickt wird** markiert werden soll:

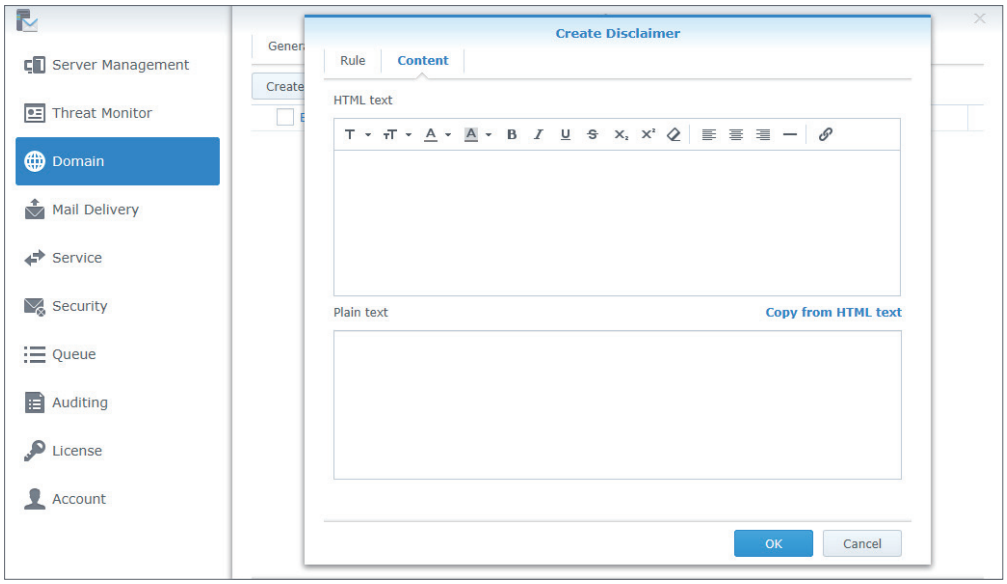
Anmerkung:

- Wenn eine E-Mail vom Server als interne E-Mail (E-Mails an interne Benutzer) erkannt wird, wird die Fußzeile nicht angehängt.
- Wenn einer der Empfänger kein interner Benutzer ist, wird die Fußzeile angehängt.

6. Legen Sie die Kriterien anhand der folgenden Optionen fest:
   - **Übereinstimmende Regel**: Wählen Sie die Definition für die Übereinstimmung: **Alle** oder **eine**. Wenn Sie **Alle** auswählen, wird die Fußzeile nur angehängt, wenn alle Regeln erfüllt sind. Wenn Sie **Eine** auswählen, wird die Fußzeile angehängt, wenn mindestens eine Regel erfüllt ist.

- **Der folgenden Regel entsprechen**: Wählen Sie aus, ob die Fußzeile basierend auf den **Empfänger** oder **Absender** angehängt werden soll. Die Einstellungen unterstützen Platzhalter (*).
- **Die Ausnahmeregel** hat eine höhere Priorität als **Übereinstimmende Regeln**. Wenn eine **Ausnahmeregel** erstellt wird, werden Fußzeilen nicht angehängt, selbst wenn die Kriterien für **Übereinstimmende Regeln** erfüllt sind.

7. Klicken Sie auf das Plus-Symbol (+), um mehr als eine **Übereinstimmende Regel** oder **Ausnahmeregel** zu erstellen, und auf das Minus-Symbol (-), um eine Regel zu entfernen.
8. Nach der Einrichtung der Regeln gehen Sie zur Registerkarte **Inhalt**, um den Inhalt im Feld **HTML-Text** und **Klartext** zu bearbeiten und sicherzustellen, dass der Inhalt beim Client korrekt angezeigt wird.



9. Wenn Ihr Inhalt im Feld **Klartext** dem Inhalt im Feld **HTML-Text** entsprechen soll, klicken Sie auf **Von HTML-Text kopieren**, um den Inhalt vom **HTML- Text**-Editor in den **Klartext**-Editor zu kopieren und alle HTML-Tags zu entfernen.
10. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

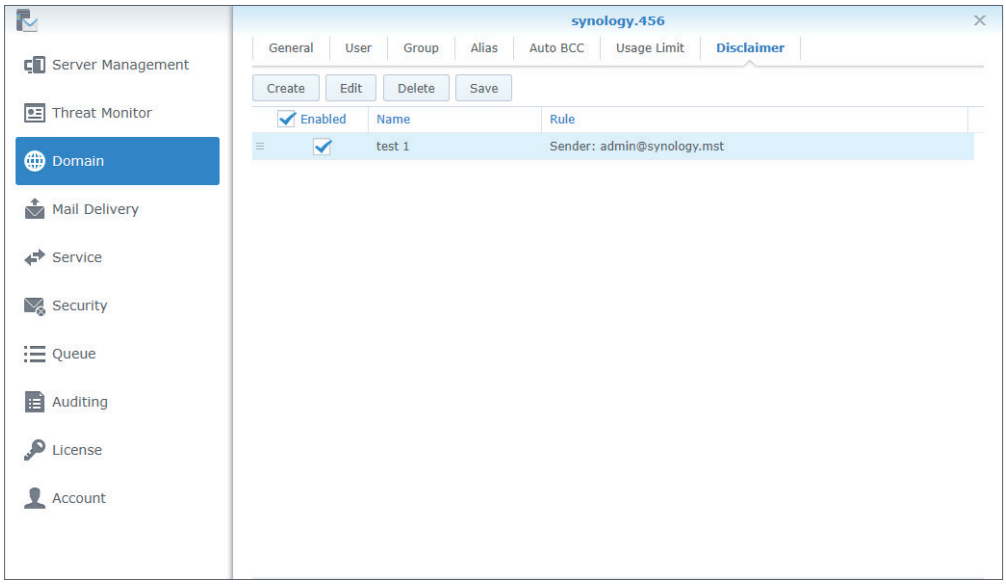
Fußzeilen bearbeiten und löschen

Da Fußzeilen anhand ihrer Priorität verwendet werden, können Sie diese nicht nur bearbeiten und löschen, sondern hier auch Prioritätseinstellungen anpassen. Gehen Sie wie folgt vor, um Fußzeilen zu verwalten:

Anmerkung:

- Das System überprüft, welche Fußzeile von oben nach unten angehängt werden soll. Wenn die Kriterien für eine Fußzeile erfüllt sind, wird die Fußzeile angehängt und die Überprüfung beendet.

1. Gehen Sie zu **Domain**, wählen Sie *synology.456* und klicken Sie auf **Bearbeiten**.
2. Gehen Sie zur Registerkarte **Fußzeile**. In der Liste weiter oben stehende Fußzeilen haben höhere Priorität als jene weiter unten. Um die Priorität zu ändern, wählen Sie eine Fußzeile aus und verschieben Sie sie an die gewünschte Position.
3. Wählen Sie die Fußzeilen-Regel aus, die aktiviert werden soll.
4. Wählen Sie eine zu ändernde Fußzeilen-Regel aus und klicken Sie auf die Schaltfläche **Bearbeiten** oder **Löschen**.



5. Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

Kapitel 9: Sicherheitseinstellungen

Die Sicherheitsfunktionen von MailPlus Server umfassen die folgenden vier Bereiche: **Spam**, **Virenscans**, **Authentifizierung** und **Inhaltsschutz**. Sie können Einstellungen anpassen, um den Schutz für einen bestimmten Bereich zu erhöhen.

Spam

MailPlus Server bietet Standards der Spam-Erkennung, die auf der Zustellungsart von Spam-Nachrichten basieren. In MailPlus Server sind folgende Anti-Spam-Technologien verfügbar:

- **Anti-Spam**: Verwendet Rspamd und SpamAssassin als Anti-Spam-Module. Zudem kann MailPlus Server Spam-Nachrichten mit den Mechanismen des automatischen Lernens und der Spam-Meldungen nach Ihren Bedürfnissen blockieren.
- **Postscreen**: Verringert die Wahrscheinlichkeit für den Erhalt von Spam-Nachrichten durch Zurückweisung von Diensten für Spam-Server gemäß offener Blacklists und den Merkmalen der Absender von Spam-Servern.
- **Graue Liste**: Führt Aktionen anhand von Merkmalen der Absender von Spam-Servern aus. Da graue Listen sich auf die Zustellungsgeschwindigkeit von Nachrichten auswirken, stellen Sie bitte sicher, dass Sie den Mechanismus von grauen Listen vollständig verstanden haben, bevor Sie diese Funktion aktivieren.

Anti-Spam aktivieren

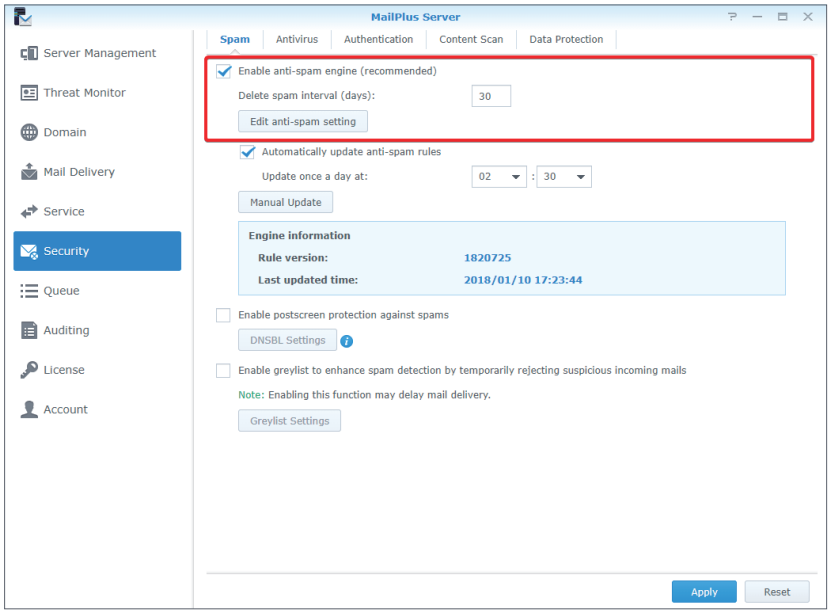
MailPlus Server verwendet das Anti-Spam-Modul Rspamd gemeinsam mit Regeln aus der SpamAssassin-Datenbank, um Spam zu erkennen und anhand des Grenzwertes für die Spam-Punktzahl herauszufiltern. Wenn eine E-Mail mit einer voreingestellten Erkennungsregel übereinstimmt, wird der Punktzahl ein weiterer Punkt hinzugefügt. E-Mails, die diesen Grenzwert überschreiten, werden als Spam markiert. Gehen Sie wie folgt vor, um Anti-Spam zu aktivieren:

1. Gehen Sie zu **Sicherheit** > **Spam**, um die folgenden Einstellungen anzupassen:
   - **Anti-Spam-Modul aktivieren**: Weitere Informationen zur Anti-Spam-Funktion finden Sie unter **Allgemeine Anti-Spam-Einstellungen**, **Anti-Spam-Regeln aktualisieren**, **Benutzerspezifischer Spam-Filter** und **Einstellungen für automatisches Lernen und Spam-Meldungen**.
   - **Spam-Intervall (Tage) löschen**: Als Spam markierte Nachrichten werden an das Spam-Postfach gesendet. Spam-Nachrichten werden nach der angegebenen Anzahl von Tagen

automatisch gelöscht. Sie können den Intervall für das automatische Löschen von Spam (standardmäßig 30 Tage) anpassen.

Anmerkung:

- Auch wenn das Anti-Spam-Modul nicht aktiviert ist, wird Spam regelmäßig gelöscht.

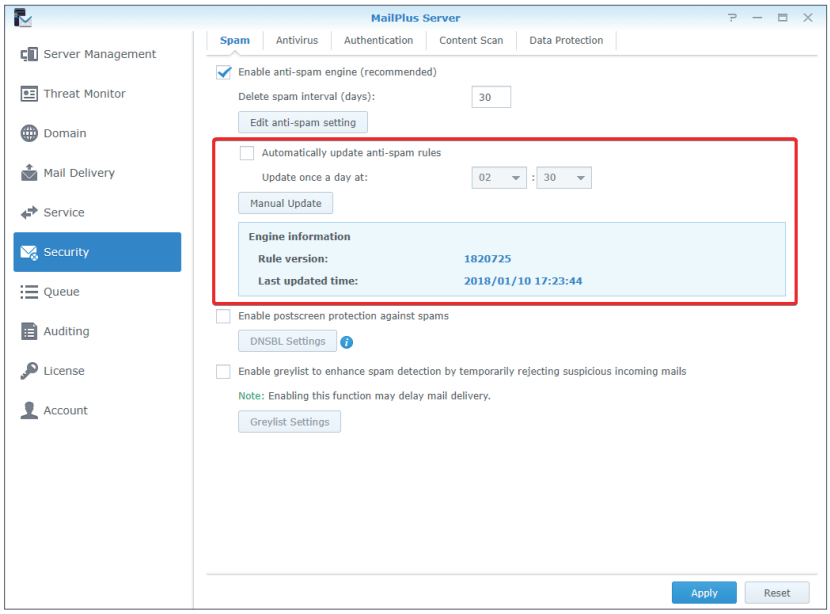


Anti-Spam-Regeln aktualisieren

Eine regelmäßige Aktualisierung der Anti-Spam-Regeln ist erforderlich, um sicherzustellen, dass die E-Mail-Schutzfunktionen auf dem neuesten Stand sind. Gehen Sie hierzu wie folgt vor:

1. Gehen Sie zu **Sicherheit** > **Spam**, um die folgenden Einstellungen anzupassen:

   - **Anti-Spam-Regeln automatisch aktualisieren**: Setzen Sie hier ein Häkchen, um einen Aktualisierungsplan einzurichten. Das System lädt dann nach Zeitplan die neuesten Anti-Spam-Regeln von der offiziellen SpamAssassin-Website herunter.
   - **Aktualisieren einmal pro Tag um**: Richten Sie einen täglichen Zeitplan ein, um die Regeln herunterzuladen.
   - **Manuelle Aktualisierung**: Klicken Sie hierauf, um die Anti-Spam-Regeln sofort zu aktualisieren. Im Bereich **Modul-Informationen** unter der Schaltfläche wird die letzte Aktualisierungszeit und die Version der Spam-Erkennungsregeln angezeigt.



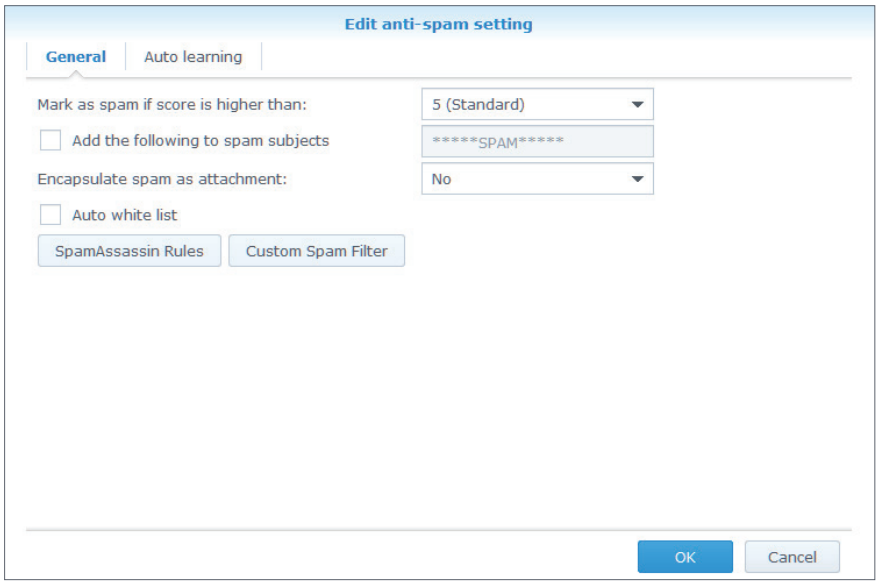
Allgemeine Anti-Spam-Einstellungen

Die Anti-Spam-Funktion stellt verschiedene anpassbare Einstellungen bereit. Sie können das Anti-Spam-Modul nach Bedarf anpassen. Gehen Sie wie folgt vor, um allgemeine Anti-Spam-Einstellungen zu bearbeiten:

1. Gehen Sie zu **Sicherheit** > **Spam**, und klicken Sie auf die Schaltfläche **Anti-Spam-Einstellungen bearbeiten**.
2. Gehen Sie zur Registerkarte **Allgemein** im Fenster **Anti-Spam-Einstellungen bearbeiten**. Hier können Sie die folgenden Einstellungen anpassen:
   - **Als Spam markieren, wenn Punktzahl höher ist als**: Eine Nachricht, die den von Ihnen festgelegten Grenzwert überschreitet, wird als Spam markiert.
   - **Folgendes zum Spam-Betreff hinzufügen**: Wenn eine Nachricht den Grenzwert für die Spam-Punktzahl überschreitet und als Spam markiert wird, können Sie einen Text zum Betreff hinzufügen, um Benutzer über Spam zu informieren. Markieren Sie das Kontrollkästchen**Folgendes zum Spam-Betreff hinzufügen** und bearbeiten Sie den Standardinhalt.
   - **Spam als Anhang verkapseln**: Als Spam markierte E-Mails werden als Anhang gemeldet, der in einer neuen Nachricht verkapselt ist. Zu den Optionen des Dropdown-Menüs zählen:

Optionen	Beschreibung
Nein	Meldet Spam ohne weitere Aktionen.
Ja	Meldet Spam als Anhang einer neuen Nachricht.
Ja, Nur-Text	Meldet Spam als Nur-Text, um Webfehler und bösartige Skripte zu umgehen; anschließend verkapselt es ihn als Anhang und sendet ihn an Empfänger.

- **Automatische Whitelist**: Mit dieser Funktion kann das System eingehende und ausgehende E-Mail-Nachrichten analysieren, um festzustellen, ob auf eine externe E-Mail-Adresse in der Vergangenheit eine Antwort von einem Benutzer erfolgt ist. Auf diese Weise wird vermieden, dass E-Mails fälschlicherweise als Spam behandelt werden.

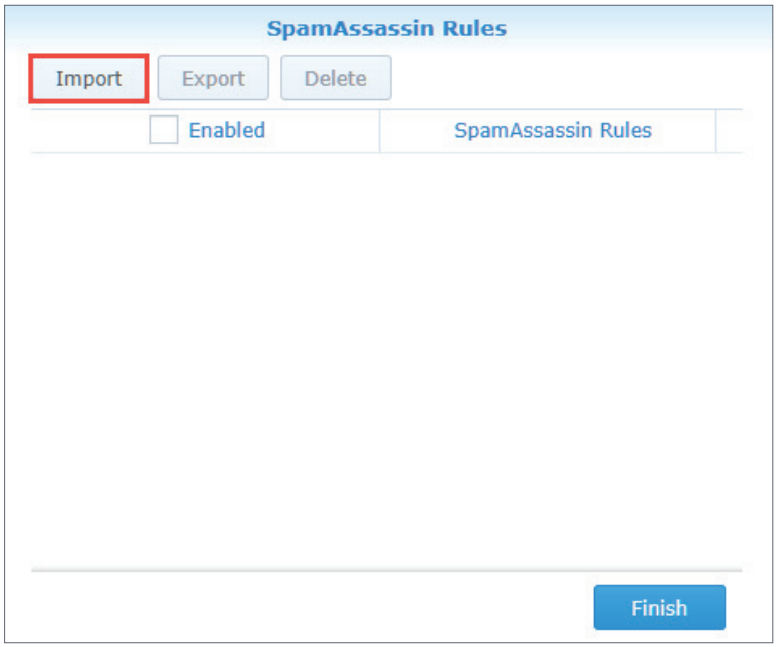


SpamAssassin-Regeln

1. Gehen Sie zu **Sicherheit** > **Spam**, und klicken Sie auf die Schaltfläche **Anti-Spam-Einstellungen bearbeiten**.
2. Gehen Sie zur Registerkarte **Allgemein** im Fenster **Anti-Spam-Einstellungen bearbeiten**, und klicken Sie auf die Schaltfläche **SpamAssassin-Regeln**.
3. Klicken Sie auf die Schaltfläche **Importieren**, um SpamAssassin-Regeln hinzuzufügen.

Anmerkung:

- Importierte Dateien müssen die Dateierweiterung „.cf“ aufweisen. Die Regeln werden aktiviert, sobald sie importiert wurden. Weitere Informationen finden sie in **den Regeln**, die von SpamAssassin bereitgestellt wurden; oder fügen Sie Regeln anhand **der Richtlinie für Regeln** hinzu.

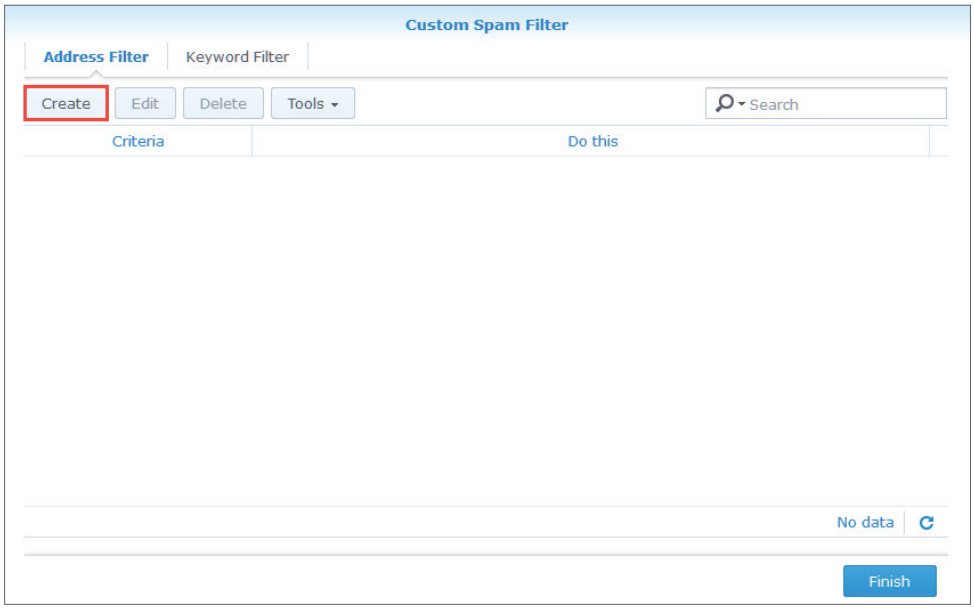


4. Wählen Sie die Regel, die Sie bearbeiten möchten, sowie eine entsprechende Aktion, wie z. B. **Aktivieren**, **Exportieren** und **Löschen**.
5. Klicken Sie auf **Fertig stellen**, um die Einstellungen abzuschließen.

Benutzerspezifischer Spam-Filter

Es gibt zwei Arten von Spam-Filtern, die Sie einrichten können, um verdächtige E-Mails herauszufiltern: **Addressfilter** und **Schlüsselwortfilter**. Sie können die Filter je nach Bedarf anpassen. Bitte gehen Sie wie folgt vor, um einen Spam-Filter zu erstellen:

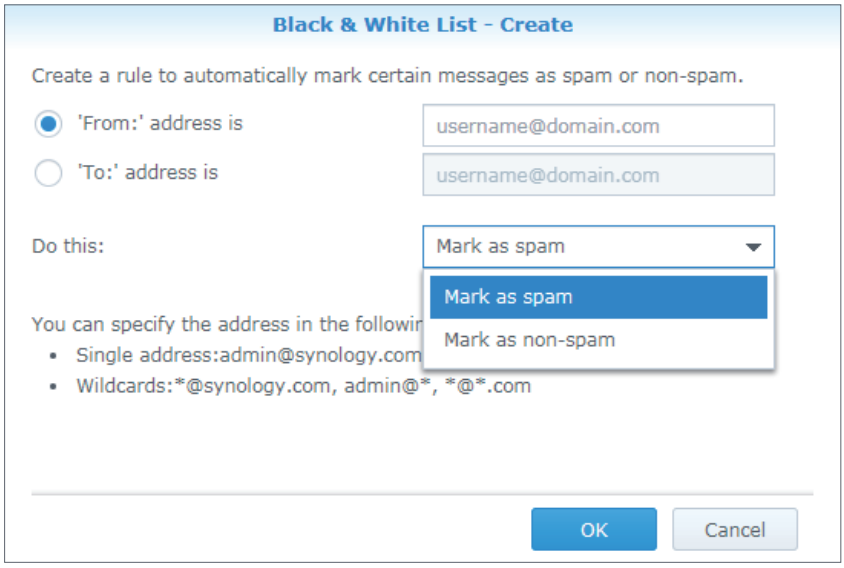
1. Gehen Sie zu **Sicherheit** > **Spam**, und klicken Sie auf die Schaltfläche **Anti-Spam-Einstellungen bearbeiten**.
2. Gehen Sie zur Registerkarte **Allgemein** im Fenster **Anti-Spam-Einstellungen bearbeiten**, und klicken Sie auf die Schaltfläche **Benutzerspezifischer Spam-Filter**.
3. Gehen Sie zur Registerkarte **Adressfilter** im Fenster **Benutzerspezifischer Spam-Filter**, und klicken Sie auf die Schaltfläche **Erstellen**.



4. Nachrichten werden anhand der Absender- und Empfängerkriterien als Spam oder Nicht-Spam markiert. Bei den eingegebenen Adressen können Platzhalter (*) verwendet werden.
5. Wählen Sie aus dem Dropdown-Menü **Vorgang ausführen** die Option **Als Spam markieren** oder **Als Nicht-Spam markieren**.

Anmerkung:

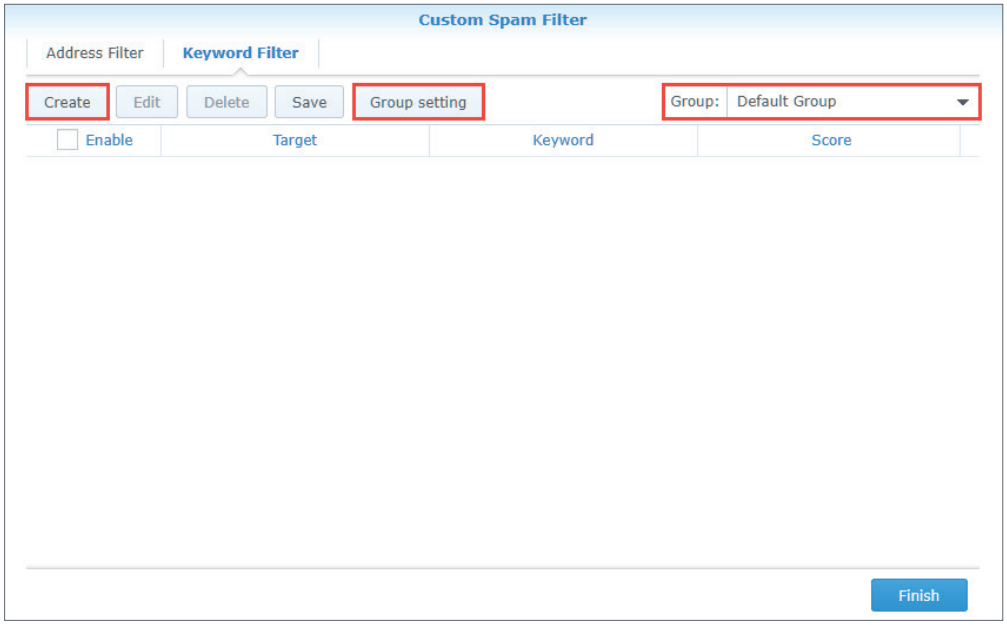
- Die Spam-Punktzahl wird bei der Konfiguration dieser Aktionen ignoriert.



6. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.
7. Gehen Sie zur Registerkarte **Schlüsselwortfilter** im Fenster **Benutzerspezifischer Spam-Filter**.
8. Klicken Sie auf die Schaltfläche **Gruppeneinstellung**, um eine Gruppe zu erstellen. Sie können mehrere Gruppen einrichten, um Schlüsselwortfilter zu kategorisieren und die Filter anschließend nach Gruppe zu verwalten:

- Markieren Sie das Kontrollkästchen im Feld **Aktivieren**, um eine gesamte Gruppe zu aktivieren oder zu deaktivieren.
- Um eine Gruppe zu erstellen, zu bearbeiten oder zu löschen, wählen Sie diese aus und klicken Sie auf die Aktionsschaltflächen in der oberen Symbolleiste.

9. Bevor Sie einen Schlüsselwortfilter erstellen, müssen Sie im Dropdown-Menü die Gruppe auswählen, der er angehört.



10. Klicken Sie auf die Schaltfläche **Erstellen**, um die Regel anzupassen:

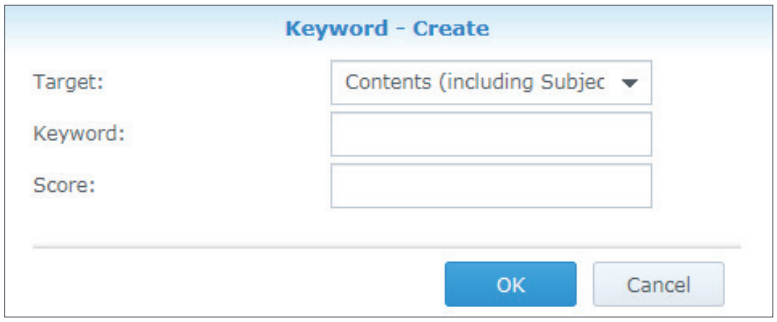
- **Ziel**: Im Dropdown-Menü **Ziel** können Sie die folgenden zu filternden Optionen auswählen:

Optionen	Beschreibung
Titel	E-Mail-Titel
Inhalt (einschließlich Betreff)	E-Mail-Inhalt und -Titel

- **Schlüsselwort**: Geben Sie die zu filternden Schlüsselwörter ein. Hier kann ein regulärer Ausdruck verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie in **Wikipedia**.
- **Punktzahl**: Geben Sie die Anzahl der Punkte an, die zur gesamten Spam-Punktzahl einer E-Mail hinzugefügt werden, wenn das Schlüsselwort erkannt wurde.

Anmerkung:

- Eine E-Mail wird als Spam markiert, wenn die gesamte Spam-Punktzahl den Grenzwert für Spam überschreitet.



Anmerkung:

- Bei Durchführung dieser Änderungen können Sie auf Wunsch auch den Grenzwert für die Spam-Punktzahl neu anpassen. Gehen Sie zur Registerkarte **Allgemein** im Fenster **Anti-Spam-Einstellungen bearbeiten**, um den Grenzwert für die Spam-Punktzahl anzupassen. Je höher der Grenzwert für die Spam-Punktzahl ist, desto lockerer sind die Kriterien für Spam, d. h. E-Mails werden mit geringerer Wahrscheinlichkeit als Spam markiert. Je niedriger der Grenzwert für die Spam-Punktzahl ist, desto strenger sind die Kriterien für Spam, d. h. E-Mails werden mit größerer Wahrscheinlichkeit als Spam markiert.

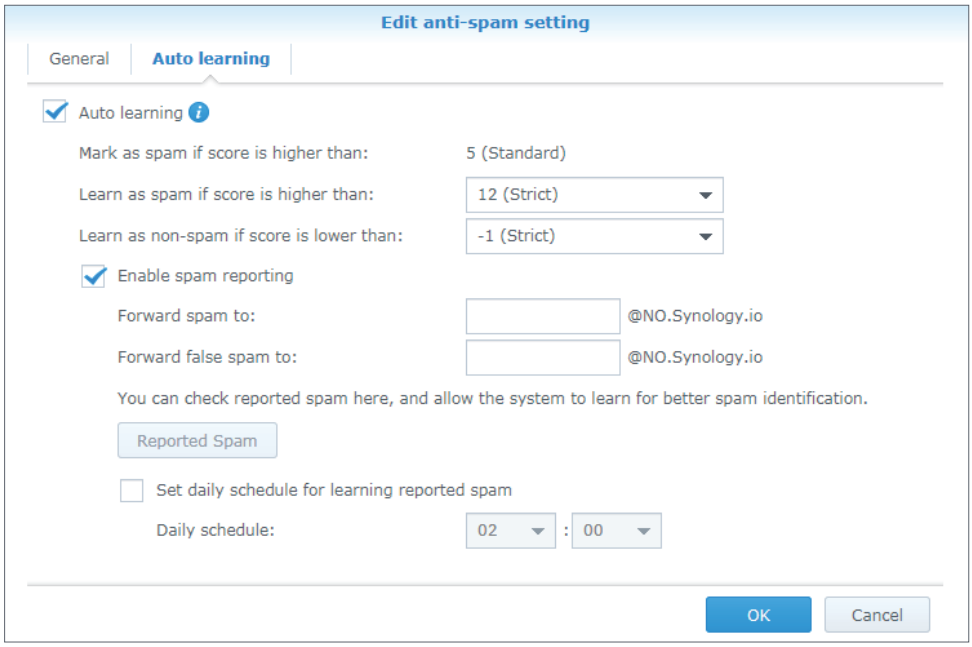
Einstellungen für automatisches Lernen und Spam-Meldungen

Nachdem das Anti-Spam-Modul gestartet wurde, können Sie MailPlus Server lernen lassen, um Spam mit speziellen Algorithmen besser zu erkennen. Automatisches Lernen und Spam-Meldungen tragen dazu bei, die Genauigkeit der Spam-Erkennung zu verbessern, um individuellen Bedürfnissen gerecht zu werden.

- **Automatisches Lernen**: Bei der Spam-Erkennung durch das Anti-Spam-Modul wählt das System automatisch eine E-Mail aus, die mit auf der Punktzahl basierenden Kriterien übereinstimmt, damit die E-Mail weiter analysiert werden kann.
- **Spam-Meldungen**: Benutzer können Spam melden, wenn die Spam-Erkennung durch das Anti-Spam-Modul fehlgeschlagen ist, oder wenn eine Nachricht fälschlicherweise als Spam erkannt wurde. Wenn eine falsche Kategorisierung an das Anti-Spam-Modul gemeldet wird, kann das Modul neu lernen, um die Genauigkeit zu verbessern.

Gehen Sie bitte wie folgt vor, um automatisches Lernen und Spam-Meldungen einzurichten:

1. Gehen Sie zu **Sicherheit** > **Spam**, und klicken Sie auf die Schaltfläche **Anti-Spam-Einstellungen bearbeiten**.
2. Gehen Sie zur Registerkarte **Automatisches Lernen** im Fenster **Anti-Spam-Einstellungen bearbeiten**.



3. Markieren Sie das Kontrollkästchen **Automatisches Lernen**, um die folgenden Einstellungen anzupassen:

   - **Als Spam markieren, wenn Punktzahl höher ist als**: Sie sehen den Grenzwert für Spam, der unter **Allgemein** eingerichtet wurde.
   - **Als Spam lernen, wenn Punktzahl höher ist als**: Wenn die Spam-Punktzahl bei der Spam-Erkennung höher ist als dieser Wert, wertet das Anti-Spam-Modul die Schlüsselwörter im Nachrichteninhalt weiter aus, um die Datenbank des Anti-Spam-Moduls zu erweitern und seine Lernfähigkeit zu verbessern. Wenn in Zukunft dieselben Schlüsselwörter erkannt werden, können Nachrichten eher als Spam identifiziert werden.
   - **Als Nicht-Spam lernen, wenn Punktzahl niedriger ist als**: Wenn die Spam-Punktzahl bei der Spam-Erkennung niedriger ist als dieser Wert, wertet das Anti-Spam-Modul die Schlüsselwörter im Nachrichteninhalt weiter aus, um die Datenbank des Anti-Spam-Moduls zu erweitern und seine Lernfähigkeit zu verbessern. Wenn in Zukunft dieselben Schlüsselwörter erkannt werden, können Nachrichten eher als Nicht-Spam identifiziert werden.

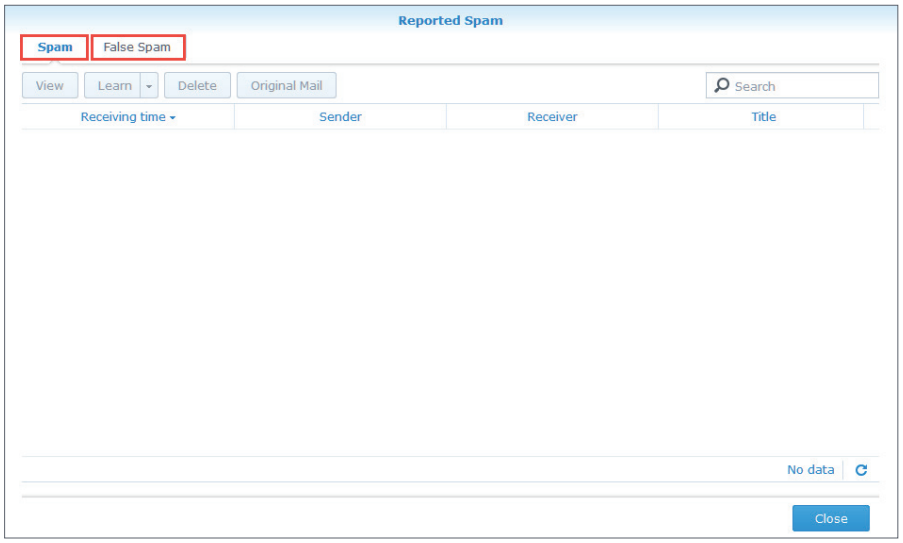
4. Markieren Sie das Kontrollkästchen **Spam-Meldungen aktivieren**, um die folgenden Einstellungen anzupassen:

Anmerkung:

- Beim Meldevorgang wird Spam in einem bestimmten Postfach gesammelt, um den Lernprozess zu durchlaufen. Nach Aktivierung der Spam-Meldungen können Benutzer Spam und Nicht-Spam daher anhand der folgenden zwei Methoden melden:
  - Wenn Benutzer Nachrichten über MailPlus empfangen, wurde die weiterleitende Mailbox für diese Benutzer bereits konfiguriert. Benutzer müssen in MailPlus lediglich Nachrichten als Spam markieren oder das Spam-Postfach von MailPlus öffnen, um Nachrichten als Nicht-Spam zu markieren.
  - Wenn Benutzer Nachrichten mit E-Mail-Clients von Drittanbietern empfangen, müssen sie die Funktion **Als Anhang weiterleiten** der E-Mail-Clients nutzen, um E-Mails als Anhänge an das meldende Postfach weiterzuleiten.

- **Spam weiterleiten an**: Geben Sie eine E-Mail-Adresse ein, an die gemeldeter Spam weitergeleitet wird, wenn Benutzer E-Mail-Clients von Drittanbietern verwenden, um E-Mails zu empfangen und zu melden. Die ursprüngliche E-Mail wird als Anhang an diese E-Mail-Adresse weitergeleitet.
- **Falsch erkannten Spam weiterleiten an**: Geben Sie eine E-Mail-Adresse ein, an die gemeldeter Nicht-Spam weitergeleitet wird, wenn Benutzer E-Mail-Clients von Drittanbietern verwenden, um E-Mails zu empfangen und zu melden. Die ursprüngliche E-Mail wird als Anhang an diese E-Mail-Adresse weitergeleitet.
- **Als Spam gemeldet**: Klicken Sie auf **Als Spam gemeldet**, um den gesamten gemeldeten Spam sowie falsch erkannten Spam anzuzeigen. Wählen Sie auf der E-Mail-Liste eine E-Mail aus und klicken Sie auf die Schaltfläche **Lernen**, um dem Anti-Spam-Modul zu ermöglichen, die Spam-Erkennung für den gewählten E-Mail-Typ zu verbessern. E-Mails, die den Lernprozess durchlaufen haben, werden entfernt. Sie können dem System ermöglichen, von E-Mails in den Spam- und Nicht-Spam-Postfächern zu lernen. Beachten Sie hierzu die nachstehende Spam-Verwaltung:

Funktion	Beschreibung
Anzeigen	Nachrichteninhalt anzeigen.
Lernen	Dem Anti-Spam-Modul ermöglichen, schnell aus der ausgewählten E-Mail zu lernen. Nachdem ein E-Mail den Lernprozess durchlaufen hat, wird es aus der Liste entfernt.
Alle lernen	Dem Anti-Spam-Modul ermöglichen, aus allen E-Mail-Nachrichten zu lernen. Die Option **Alle lernen** finden Sie im Dropdown-Menü neben der Schaltfläche **Lernen**.
Löschen	Ausgewählte E-Mails entfernen, um zu verhindern, dass das Anti-Spam-Modul aus ihnen lernt.
Original-E-Mail	Die Original-E-Mail in einer neuen Browser-Registerkarte öffnen.
Suchen	Schlüsselwörter (Absender, Empfänger und Betreff) im Suchfeld oben rechts eingeben, um nach bestimmten E-Mail-Nachrichten zu suchen.



- **Täglichen Zeitplan für das Erlernen von gemeldetem Spam festlegen**: Markieren Sie diese Option, um den Zeitraum festzulegen, in dem das System automatisch aus allen gemeldeten Spam- und Nicht-Spam-Nachrichten lernt.

Anmerkung:

- Die unter **Spam weiterleiten an** eingegebene E-Mail-Adresse darf nicht den Benutzernamen von bereits vorhandenen Benutzern verwenden. Die E-Mail-Adresse wird nicht als lizenzierter Benutzer berücksichtigt und nur verwendet, um E-Mail-Beispiele zu empfangen.
- Die unter **Falsch erkannten Spam weiterleiten an** eingegebene E-Mail-Adresse darf nicht den Benutzernamen von bereits vorhandenen Benutzern verwenden.

5. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

Postscreen

Postscreen überprüft die Verbindungsquelle während der Verbindungsphase und bestimmt, ob Dienste fortgesetzt werden. Postscreen beinhaltet die folgenden zwei Hauptfunktionen:

- Es wird überprüft, ob ein Absender SMTP-Standards einhält und Befehle nach der Begrüßung des SMTP-Servers sendet. Wenn ein Absender einen Befehl vor der Begrüßung des SMTP-Servers sendet, wird dieser Absender blockiert.
- Es werden weitere DNSBL-Server auf der Grundlage der IP-Adresse des Absenders überprüft. Wenn die IP-Adresse eines Absenders von anderen Servern auf eine Blacklist gesetzt wurde, wird dieser Absender blockiert.

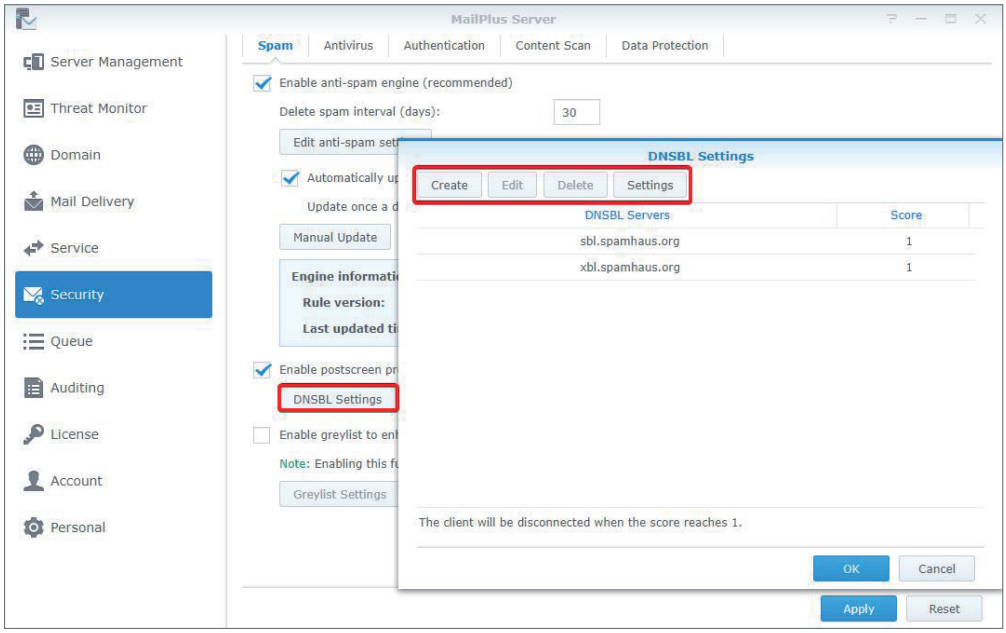
DNSBL-Einstellungen

Postscreen ermöglicht die Einrichtung mehrerer DNSBL-Server. Die Übereinstimmung mit Kriterien bei der Serverprüfung ergibt Spam-Punkte und von unterschiedlichen Servern generierten Spam-Punkte werden zusammengezählt. Wenn die gesamte Punktzahl den unter **Grenzwert für die DNSBL-Punktzahl** angegebenen Wert überschreitet, werden Dienste zurückgewiesen. Gehen Sie wie folgt vor, um DNSBL-Einstellungen anzupassen:

1. Gehen Sie zu **Sicherheit** > **Spam**, und markieren Sie das Kontrollkästchen **Postscreen-Spamschutz aktivieren**.
2. Klicken Sie auf die Schaltfläche **DNSBL-Einstellungen**, um die Server zu bearbeiten, die überprüft werden sollten.
3. Klicken Sie auf die Schaltfläche **Einstellungen**, um den **Grenzwert für die DNSBL-Punktzahl** für die Zurückweisung von Diensten anzugeben.
4. Klicken Sie auf **Erstellen**, um die zu überprüfenden Server hinzuzufügen.

> **Anmerkung:**
>
> - Hier können Sie DNSWL-Server (DNS-basierte Whitelist) hinzufügen und negative Zahlen in den entsprechenden **Punktzahl**-Feldern eingeben.

5. Sie können einen ausgewählten DNSBL-Server **Bearbeiten** oder **Löschen**.



6. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

Graue Liste aktivieren

Bei einer neuen eingehenden Nachricht überprüft das System, ob Einträge der IP-Adresse, des Absenders oder des Empfängers vorliegen, die den Einträgen in der eingehenden Nachricht entsprechen. Wenn keine Einträge gefunden werden, wird die Nachricht als verdächtig eingestuft. Eine Fehlermeldung wird an den Absender mit der Aufforderung zurückgesendet, die Nachricht später erneut zu senden. Gemäß den SMTP-Standards versuchen Absender, die Fehlermeldungen erhalten, Nachrichten zu einem späteren Zeitpunkt erneut zu senden. Die meisten Absender von Spam verzichten jedoch darauf, Nachrichten erneut zu senden. Wenn normale Absender Nachrichten später erneut senden, empfängt das System diese. Die graue Liste nutzt diese Methode, um Spam zu blockieren.

Wenn die graue Liste aktiviert ist, werden die folgenden Standardaktionen für E-Mails aus allen Quellen ausgeführt:

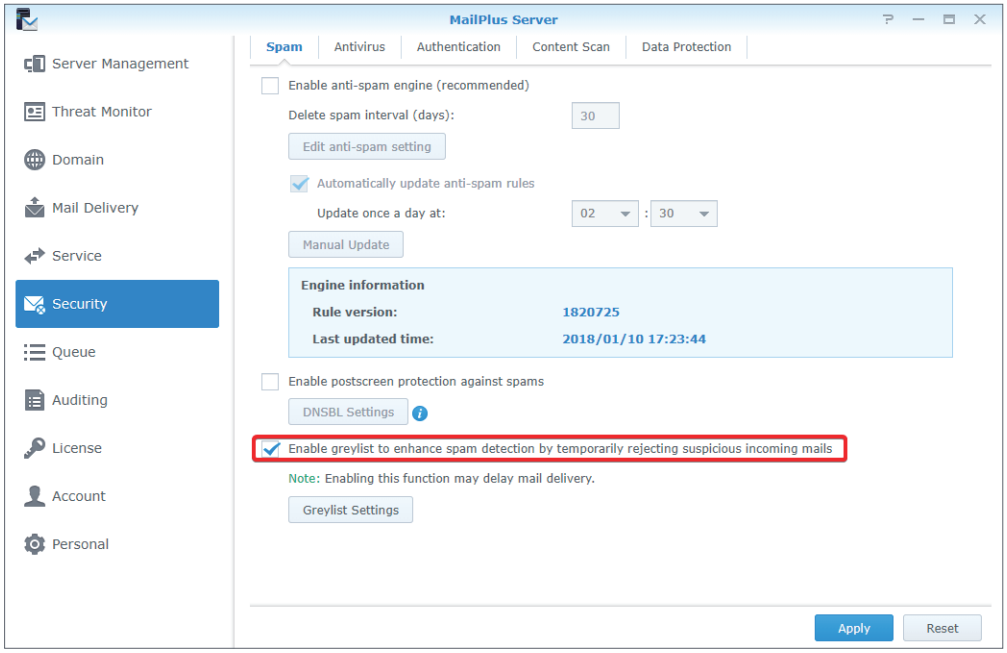
- **Whitelist**: Besteht die Prüfung direkt, und es werden keine temporären Fehlermeldungen zurückgesendet.
- **Graue Liste**: Sendet Fehlermeldungen an Absender, mit denen noch nicht kommuniziert wurde.
- **Blacklist**: Weist Nachrichten direkt zurück.

Anmerkung:

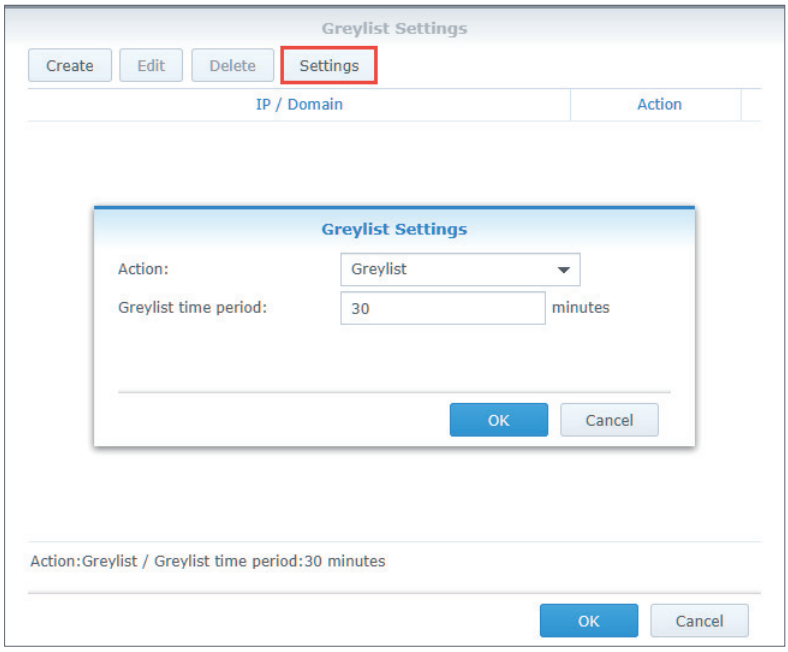
- Der Mechanismus der grauen Liste kann die Zustellung seriöser Nachrichten eventuell verzögern. Stellen Sie bitte sicher, dass Sie diesen Mechanismus vollständig verstanden haben, bevor Sie die graue Liste aktivieren.

Gehen Sie wie folgt vor, um die graue Liste zu aktivieren:

1. Gehen Sie zu **Sicherheit** > **Spam** und markieren Sie das Kontrollkästchen **Graue Liste aktivieren, um die Spam-Erkennung durch vorübergehendes Zurückweisen verdächtiger eingehender E-Mails zu verbessern**.

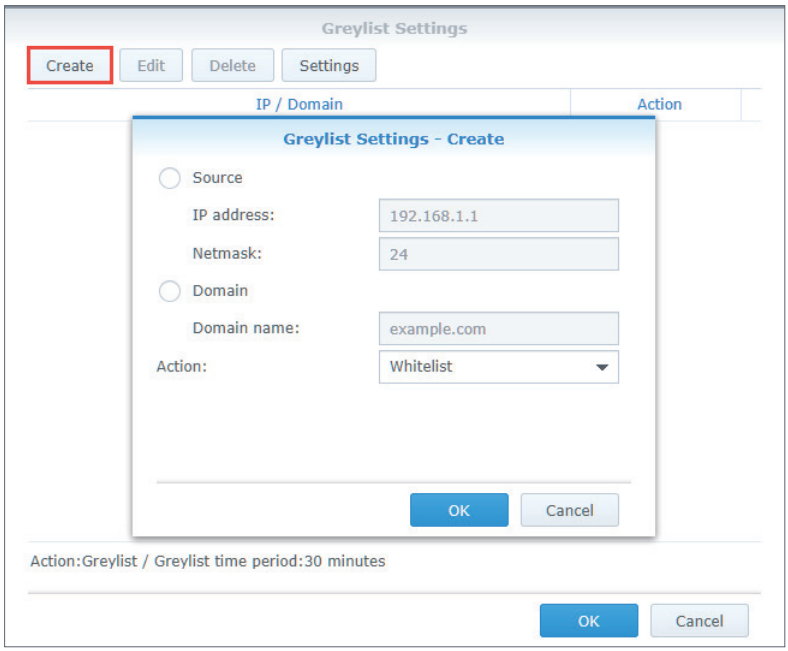


2. Klicken Sie auf die Schaltfläche **Einstellungen Graue Liste**, um Standardaktionen für alle Quellen oder Aktionen für eine(n) bestimmte(n) IP-Adresse oder Domainnamen einzurichten.
3. Klicken Sie im Fenster **Einstellungen Graue Liste** auf die Schaltfläche **Einstellungen**, um eine Standardaktion für alle Quellen einzurichten.



4. Wählen Sie im Dropdown-Menü **Aktion** eine Standardaktion aus. Geben Sie in das Feld **Zeitraum graue Liste** eine Verzögerungszeit für die graue Liste ein, die auf alle Aktionen der grauen Liste angewendet wird.

5. Klicken Sie auf **Erstellen**, um unterschiedliche Aktionen für bestimmte Absenderquellen einzurichten. Sie können verschiedene Befehle für graue Listen einrichten, ausgenommen der Standardaktion für bestimmte Benutzer.



6. Wählen Sie im eingeblendeten Fenster eine Absenderquelle und eine Aktion aus dem Dropdown-Menü **Aktion** aus.

Anmerkung:

- Die hier angeführte Domainquelle wird von der per DNS gesuchten IP-Adresse abgerufen und nicht aus dem Feld **MAIL FROM** in einer Nachricht.

7. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

Virenscan

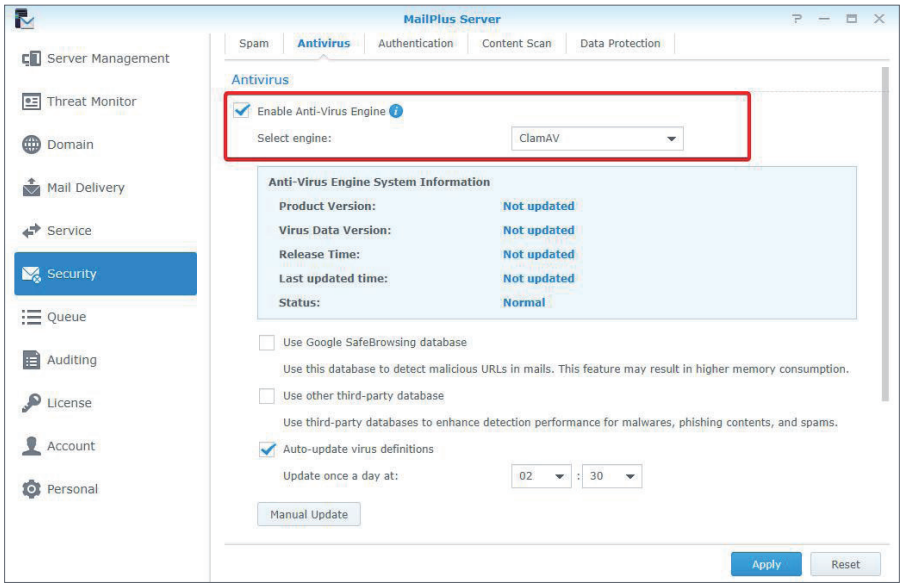
MailPlus Server bietet ClamAV, ein kostenloses Antivirenmodul, sowie McAfee, ein bezahlbares Antivirenprogramm auf Abonnementbasis, um vor Bedrohungen durch Schadprogramme zu schützen. Sie können Aktionen einrichten, die bei der Erkennung von Viren ausgeführt werden.

Mit der Virenerkennung können Sie überprüfen, ob Ihre E-Mails schädliche Software oder Malware enthalten.

- **ClamAV**: ClamAV ist das standardmäßige Antivirensystem in MailPlus Server, das ohne zusätzliche Kosten einen vollständigen Schutz für Ihren Server bereitstellt.
- **McAfee**: MailPlus Server integriert das bezahlbare Antivirenpaket**Antivirus by McAfee**. Abonnieren Sie **Antivirus by McAfee** und wählen Sie **McAfee** als Ihr Antivirenmodul, um von komfortabler Verwaltung, Antivirenplanung, Protokollen und zusätzlichen erweiterten Einstellungen zu profitieren. Beachten Sie bitte, dass MailPlus Server keine E-Mails scannt, die größer als 20 MB sind, um übermäßig lange Scanzeiten zu vermeiden.

Antivirenmodul aktivieren

1. Gehen Sie zu **Sicherheit** > **Antivirus** und setzen Sie ein Häkchen bei **Antivirenmodul aktivieren**.

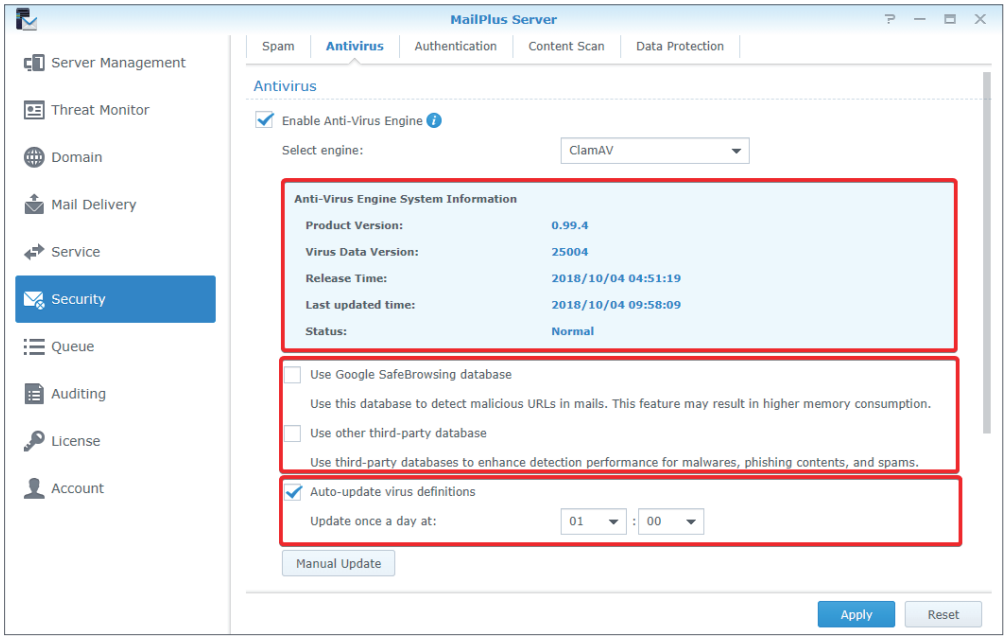


2. Wählen Sie eine der folgenden Optionen im Dropdown-Menü **Modul auswählen**:
   - **ClamAV**: ClamAV ist ein kostenloses Antivirenmodul, das von MailPlus Server unterstützt wird.
   - **McAfee**: McAfee ist ein Antivirenmodul auf Abonnementbasis, das eine zusätzliche Installation erfordert. (Gehen Sie zum **Paketzentrum**, um **Antivirus by McAfee** zu installieren.)
3. Beachten Sie die nachstehenden Abschnitte, um die Einstellungen abzuschließen.

ClamAV

Wenn Sie ClamAV als Antivirenmodul wählen, gehen Sie bitte wie folgt vor, um die Einstellungen zu konfigurieren:

1. Unter **Systeminformationen für Antivirenmodul** können Sie die Informationen des Antivirenmoduls anzeigen. Bitte sorgen Sie für eine regelmäßige Aktualisierung des Antivirenmoduls.
2. ClamAV nutzt die folgenden externen Datenbanken, um die Genauigkeit der Erkennung zu verbessern:
   - **Datenbank von Google Safe Browsing verwenden**: Nutzt die integrierte Datenbank von Google Safe Browsing, um festzustellen, ob eine Nachricht schädliche Links enthält.
   - **Andere Drittanbieter-Datenbank verwenden**: Nutzt Sanesecurity und andere **Drittanbieter-Datenbanken**, um die Virenerkennung zu verbessern.
3. Sie können Virendefinitionen wahlweise automatisch oder manuell aktualisieren:
   - **Virendefinitionen automatisch aktualisieren**: Aktivieren Sie die automatische Aktualisierung, damit das System die neuesten Virendefinitionen nach täglichem Zeitplan herunterladen kann.
   - **Manuelle Aktualisierung**: Klicken Sie hierauf, um die Virendefinitionen sofort zu aktualisieren.



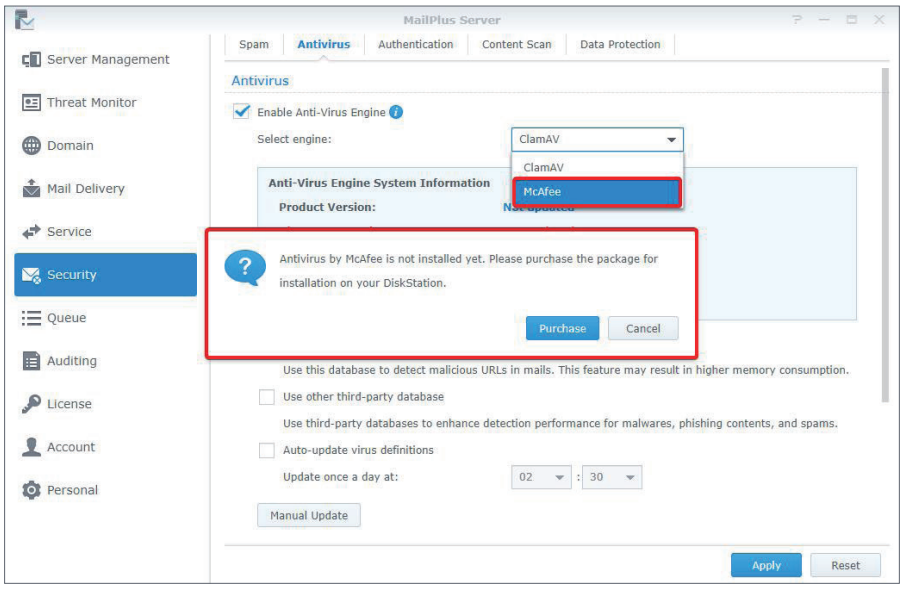
4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

McAfee

Wenn Sie McAfee als Ihr Antivirenmodul auswählen, müssen Sie zum **Paketzentrum** wechseln, um das Paket zu erwerben.

1. Wenn Sie McAfee nicht installiert haben oder die Lizenz abgelaufen ist, wird ein Warnhinweis eingeblendet, der Sie darauf hinweist, zum **Paketzentrum** zu wechseln, um

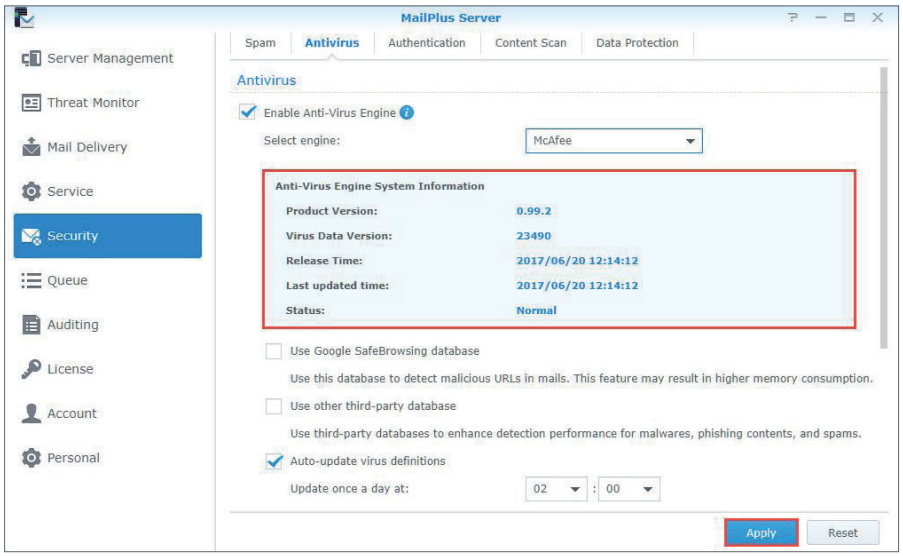
Antivirus by McAfee zu installieren und die Lizenz über das **Synology-Konto** zu erwerben.



2. Unter **Systeminformationen für Antivirenmodul** können Sie die Informationen von McAfee anzeigen.

Anmerkung:

- Die Einstellungen von McAfee müssen im Paket **Antivirus by McAfee** konfiguriert werden.
- Wenn der Status nicht normal ist (möglicherweise durch Lizenzprobleme, beschädigte Virendefinitionsdateien, usw.), kann **Antivirus by McAfee** Nachrichten nicht scannen. Bitte beheben Sie das Problem oder wechseln Sie zurück zu ClamAV. Wenn ein Benutzer **Antivirus by McAfee** manuell deaktiviert, wechselt MailPlus Server automatisch zu ClamAV.

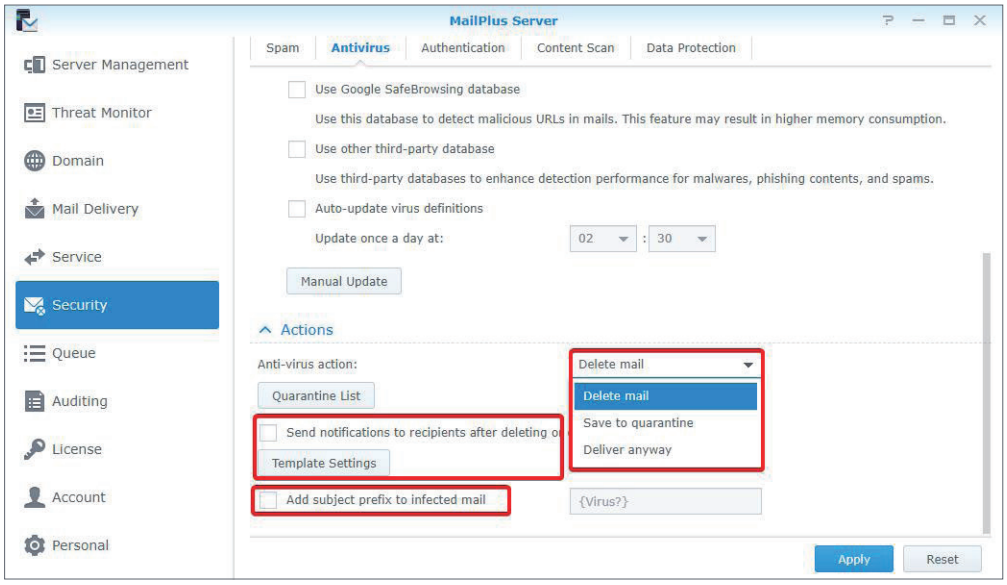


3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Einstellungen für Antivirenaktion

1. Gehen Sie zu **Sicherheit** > **Antivirenprogramm**.

2. Wählen Sie im Dropdown-Menü **Antivirenaktion** eine Aktion aus, die bei E-Mails ausgeführt werden soll, die Viren enthalten:
   - **E-Mail löschen**: Löscht E-Mails.
   - **In Quarantäne speichern**: Blockiert E-Mails und speichert sie im Bereich Quarantäne.
   - **Trotzdem zustellen**: Stellt E-Mails zu.
3. Wenn Sie **E-Mail löschen** oder **In Quarantäne speichern** ausgewählt haben, können Sie bei **Nach dem Löschen oder Speichern von E-Mails in der Quarantäne Benachrichtigungen an den Empfänger senden** ein Häkchen setzen, um darüber zu informieren. Eine Benachrichtigungsmeldung wird an den Empfänger der Original-E-Mail gesendet. Sie können auf die Schaltfläche **Vorlageneinstellungen** unten klicken, um die Vorlagen für Benachrichtigungsmeldungen für jeweils unter Quarantäne gestellte und gelöschte E-Mails anzupassen.
4. Wenn Sie **Trotzdem zustellen** ausgewählt haben, können Sie das Kontrollkästchen **Betreff-Präfix zu infizierter Mail hinzufügen** markieren, um verdächtige E-Mails kennzuzeichnen.



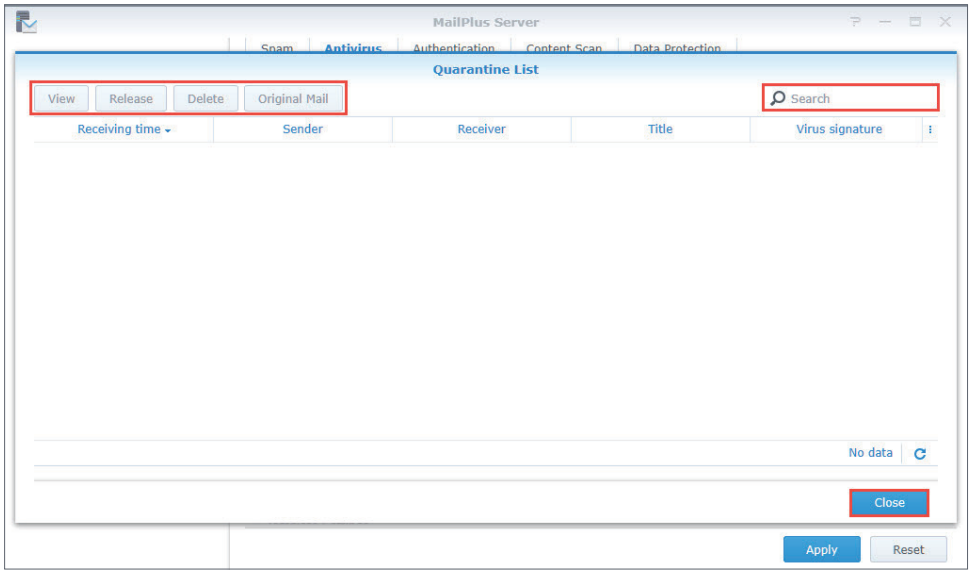
5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Quarantäneliste

Wenn Sie E-Mails im Bereich Quarantäne gespeichert haben, können Sie die unter Quarantäne gestellten E-Mails anzeigen und verwalten. Gehen Sie wie folgt vor, um die Einstellungen der Quarantäneliste anzupassen:

1. Gehen Sie zu **Sicherheit** > **Antivirenprogramm** und klicken Sie auf die Schaltfläche **Quarantäneliste**.
2. Sie können in der Suchleiste oben rechts im Fenster **Quarantäneliste** nach Absendern, Empfängern, Titeln und Virendefinitionen suchen.
3. Wählen Sie eine unter Quarantäne gestellte E-Mail aus und klicken Sie auf die Schaltfläche **Anzeigen** oder **Original-E-Mail**, um den Inhalt zu überprüfen.
4. Wählen Sie eine der folgenden Aktionen anhand des E-Mail-Inhalts aus:

- **Freigeben**: Gibt die E-Mail an den Empfänger frei.
- **Löschen**: Löscht die E-Mail.



5. Klicken Sie auf **Schließen**, um die Einstellungen abzuschließen.

Authentifizierung

Die Authentifizierung dient dazu, die Identität eines Absenders zu verifizieren, um betrügerische Nachrichten zu blockieren und vor Identitätsdiebstahl zu schützen.

- **SPF (Sender Policy Framework)**: Der SPF-Mechanismus verifiziert die Legitimität des Hosts eines Absenders. SPF-Einträge werden für zahlreiche Domains aktuell im DNS veröffentlicht und informieren über den Standort der Hosts, die autorisiert sind, E-Mails über eine Domain zu versenden. Wenn daher ein Host eines Netzwerks Nachrichten an MailPlus Server zustellt, verifiziert das System die SPF-Einträge der Domain des Absenders im DNS und stellt fest, ob der Host autorisiert ist, E-Mails über diese Domain zu versenden. Wenn die SPF-Authentifizierung fehlschlägt, wird sie je nach SPF-Eintrag als **fehlgeschlagen** oder **Softfail** klassifiziert, und das System behandelt die zwei Ergebnisse auf unterschiedliche Weise.
- **DKIM (DomainKeys Identified Mail)**: Der DKIM-Mechanismus verifiziert die Identität eines Absenders mit Verschlüsselungsmethoden, um zu überprüfen, ob der E-Mail-Inhalt geändert wurde. Mit dem DKIM-Mechanismus generiert der Host eines Absenders eine Gruppe von öffentlichen und privaten Schlüsseln und veröffentlicht den öffentlichen Schlüssel im DNS; der private Schlüssel wird zur Erstellung einer digitalen Signatur verwendet, die an E-Mails angefügt wird. Wenn der empfangende Host eine Nachricht empfängt, überprüft er den öffentlichen Schlüssel für die Domain des Absenders im DNS und verwendet den öffentlichen Schlüssel, um die Signatur sowie die Identität des Absenders zu verifizieren und zu überprüfen, ob die Nachricht geändert wurde.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)**: Der DMARC-Mechanismus basiert auf den Verifizierungsmethoden von SPF und DKIM. Wenn das System Nachrichten empfängt, prüft es, ob der Absender die SPF- und DKIM-Verifizierung besteht und damit, ob der Absender betrügerisch ist oder nicht.

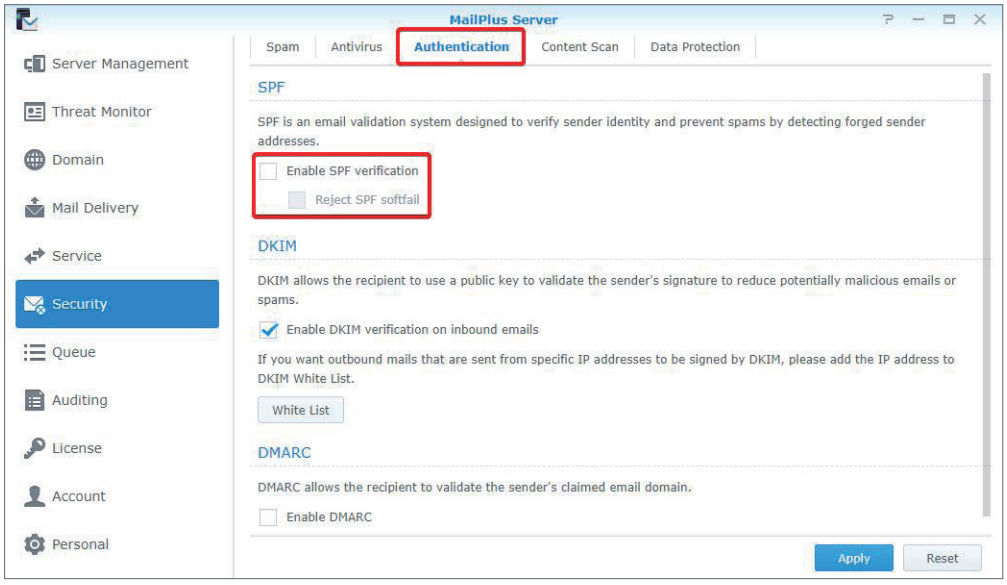
SPF

Bei aktivierter SPF-Verifizierung kann das System die SPF-Einträge der Domain eines Absenders im DNS überprüfen, um E-Mail-Betrug zu verhindern. Wenn die SPF-Verifizierung fehlschlägt, werden die Ergebnisse als **fehlgeschlagen** oder **Softfail** identifiziert. Gehen Sie wie folgt vor, um die Einstellungen der SPF-Verifizierung anzupassen:

Anmerkung:

- Wenn Ihr MailPlus Server dafür eingerichtet wurde, weitergeleitete Nachrichten von anderen Mailservern zu empfangen, blockiert der SPF-Mechanismus möglicherweise übermittelte Nachrichten, da der Standort eines Relay-Servers nicht in den SPF-Einträgen eines Absenders enthalten ist. (Weitere Informationen finden Sie in **diesem Artikel**.) Fügen Sie bitte den Relay-Server zur Whitelist hinzu oder deaktivieren Sie die SPF-Verifizierung.

1. Gehen Sie zu **Sicherheit** > **Authentifizierung**.
2. Markieren Sie im Bereich **SPF** das Kontrollkästchen **SPF-Verifizierung aktivieren**.
   - Wenn das Verifzierungsergebnis **fehlgeschlagen** lautet, wird die Nachricht zurückgewiesen.
   - Wenn das Verifizierungsergebnis **Softfail** lautet, können Sie bei **SPF-Softfail zurückweisen** ein Häkchen setzen, um **Softfail**-Nachrichten zurückzuweisen; ansonsten werden alle Nachrichten mit dem Ergebnis **Softfail** empfangen.



3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

DKIM

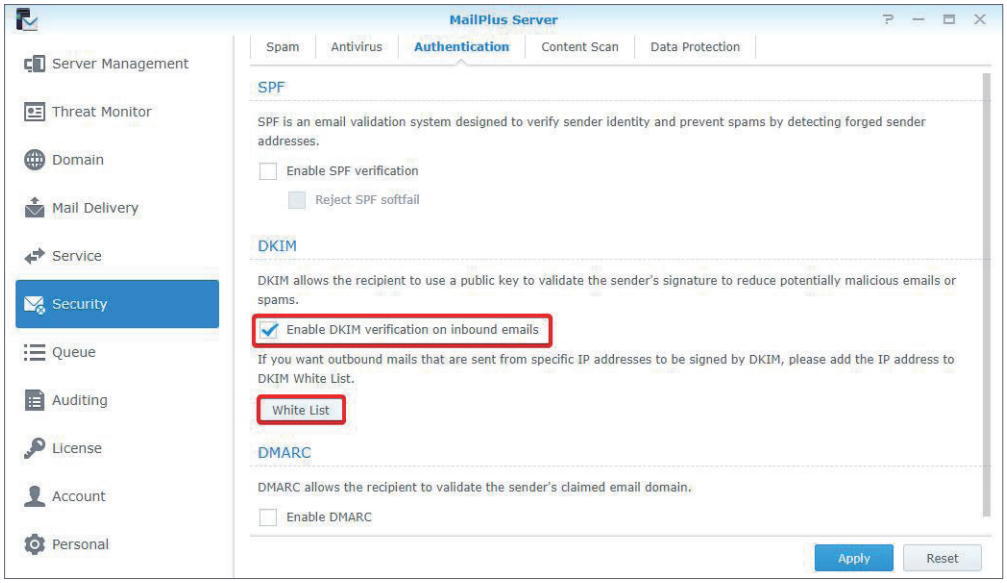
Sie können die DKIM-Verifizierung aktivieren, um Identitätsdiebstahl zu vermeiden und zu verhindern, dass Nachrichten geändert werden. Gehen Sie wie folgt vor, um die Einstellungen der DKIM-Verifizierung anzupassen:

1. Gehen Sie zu **Sicherheit** > **Authentifizierung**.

2. Setzen Sie unter **DKIM** ein Häkchen bei **DKIM-Verifizierung bei eingehenden E-Mails aktivieren**, wenn Sie die Identität eines Absenders für eingehende Nachrichten verifizieren und Nachrichten von unbekannten Quellen reduzieren möchten.

3. Wählen Sie einen Wert für **Mindestschlüssellänge für DKIM-Verifizierung** aus. DKIM weist eine E-Mail zurück, wenn die Schlüssellänge für die DKIM-Signierung kürzer ist als der gewählte Wert. Eine Vergrößerung der Mindestschlüssellänge kann verhindern, dass E-Mails von weniger sicheren Domains die DKIM-Verifizierung bestehen könnten.

4. Klicken Sie auf **Whitelist**, um bestimmte IP-Adressbereiche zur Whitelist hinzuzufügen, damit bestimmte Absender die Authentifizierung bestehen können, und um DKIM-Signaturen an Nachrichten anzuhängen. Wenn ein Host innerhalb des Bereichs eine Verbindung zu MailPlus Server herstellt, um ausgehende Nachrichten zu versenden, hängt das System DKIM-Signaturen an die Nachrichten an.



5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Anmerkung:

- Von DKIM zurückgewiesene E-Mails werden in MailPlus 2.1 und höheren Versionen in das Postfach **Spam** verschoben. Eine Warnung wird eingeblendet, wenn diese E-Mails auf MailPlus-Clients angezeigt werden.

DMARC

Da DMARC auf SPF- und DKIM-Verifizierung basiert, richten Sie bitte SPF für Ihre Domain ein und generieren Sie einen öffentlichen Schlüssel, um die DKIM-Signierung bei ausgehenden E-Mails zu aktivieren, bevor Sie mit den DMARC-Einstellungen fortfahren. Gehen Sie wie folgt vor, um die DMARC-Verifizierung zu aktivieren:

1. Gehen Sie zu **Sicherheit** > **Authentifizierung**.

2. Setzen Sie ein Häkchen bei **DMARC aktivieren**, um DMARC zu aktivieren.

Anmerkung:

- Von DMARC unter Quarantäne gestellte E-Mails werden in MailPlus 2.1 und höheren Versionen in das Postfach **Spam** verschoben. Eine Warnung wird eingeblendet, wenn diese E-Mails auf MailPlus-Clients angezeigt werden.

Inhaltsschutz

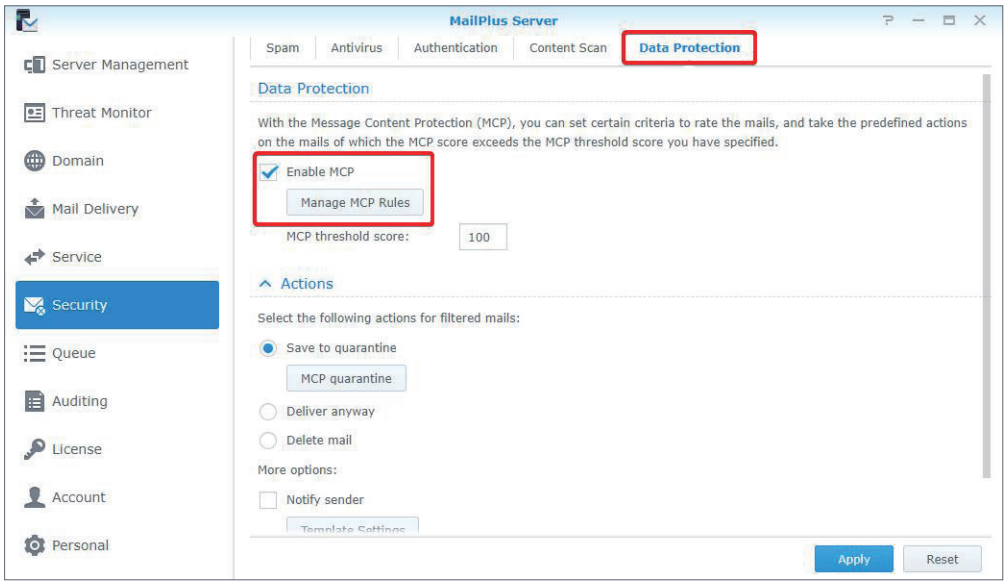
Mit der Funktion des Inhaltsschutzes können verdächtige E-Mails anhand Ihrer Einstellungen herausgefiltert werden.

- **MCP-Regeln**: Stellt Suchanfragen auf der Grundlage des Inhalts der Original-E-Mail. Wenn zuviele verdächtige Inhalte identifiziert wurden, wird die E-Mail in den Bereich Quarantäne gestellt, oder andere festgelegte Aktionen werden ausgeführt.
- **Anhangsfilter**: Filtert E-Mail-Nachrichten nach der Art des Anhangs.
- **Inhalt scannen**: Verbessert das Scannen von E-Mail-Inhalten. Verweigert oder modifiziert E-Mails, die Phishing-Links oder HTML-Tags enthalten, um die Sicherheit zu erhöhen.

MCP-Regeln

Richten Sie Regeln für MCP (Message Content Protection) ein und geben Sie einen MCP-Schwellwert an. Wenn eine E-Mail mit den Kriterien einer Regel übereinstimmt, wird die Regelwertung zur MCP-Gesamtwertung hinzugezählt. Überschreitet die Gesamtwertung den MCP-Schwellwert, filtert das System die E-Mail heraus oder blockiert sie. Gehen Sie wie folgt vor, um MCP zu aktivieren und zu verwalten.

1. Gehen Sie zu **Sicherheit** > **Datenschutz** und markieren Sie das Kontrollkästchen **MCP aktivieren** im Bereich **Datenschutz**.
2. Geben Sie einen Wert in das Feld **MCP-Schwellwert** ein.
3. Klicken Sie auf die Schaltfläche **MCP-Regeln verwalten**, um neue Regeln hinzuzufügen.



4. Klicken Sie im Fenster **MCP-Regeln verwalten** auf die Schaltfläche **Erstellen**.

5. Das Fenster **MCP-Regeln hinzufügen** enthält die folgenden Elemente:

   - **Name**: Geben Sie einen Regelnamen ein.
   - **Ziel**: Wählen Sie aus dem Dropdown-Menü **Ziel** einen Bereich von E-Mails als abzugleichendes Ziel aus:

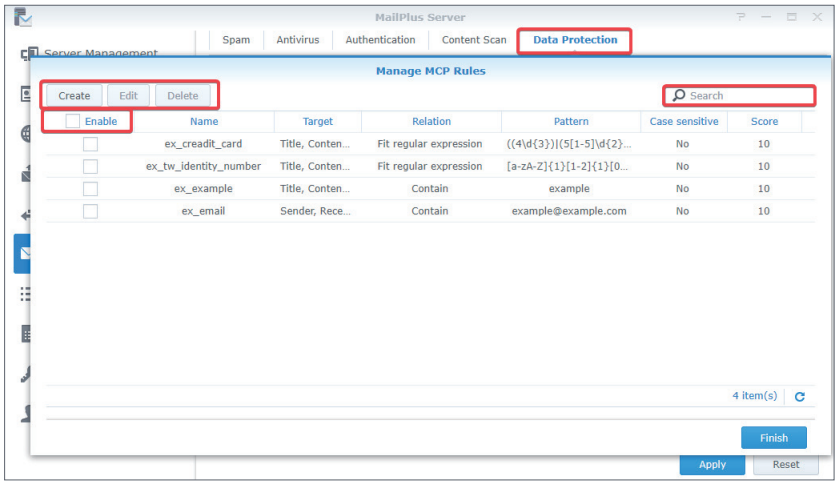
Bereich	Beschreibung
Titel	Titel der E-Mail-Nachricht
Inhalt (einschließlich Betreff)	Inhalt und Betreff der E-Mail-Nachricht
Absender	Der Absender einer E-Mail-Nachricht
Empfänger	Der Empfänger einer E-Mail-Nachricht
Benutzerdefinierte Kopfzeile	Die spezifische Kopfzeile einer ursprünglichen E-Mail-Nachricht

   - **Benutzerdefinierte Kopfzeile**: Wenn **Benutzerdefinierte Kopfzeile** im Dropdown-Menü **Ziel** ausgewählt ist, wird das Feld **Benutzerdefinierte Kopfzeile** angezeigt. Geben Sie hier eine spezifische Kopfzeile ein.
   - **Beziehung**: Wählen Sie ein Übereinstimmungskriterium aus dem Dropdown-Menü **Beziehung** aus:

Kriterien	Beschreibung
Enthalten	Wenn der Zielbereich einer E-Mail den übereinstimmenden Inhalt enthält, entspricht die E-Mail der Regel.
Entspricht	Wenn der Zielbereich einer E-Mail mit dem übereinstimmenden Inhalt identisch ist, entspricht die E-Mail der Regel.
Stimmt mit regulärem Ausdruck überein	Wenn der Zielbereich einer E-Mail den übereinstimmenden Inhalt enthält, entspricht die E-Mail der Regel. Ein regulärer Ausdruck kann für den übereinstimmenden Inhalt verwendet werden.

   - **Muster**: Geben Sie den übereinstimmenden Inhalt für die Regel ein.
   - **Unterscheidet zwischen Groß- oder Kleinschreibung**: Wählen Sie **Ja** oder **Nein**, um zu bestimmen, ob bei der Übereinstimmung zwischen Groß- und Kleinschreibung unterschieden wird.
   - **Punktzahl**: Geben Sie die Anzahl der Punkte an, die generiert werden, wenn die Kriterien dieser Regel übereinstimmen.

6. Klicken Sie auf **OK**, um die Erstellung der Regeln abzuschließen.
7. Im Fenster **MCP-Regeln verwalten** können Sie eine Regel erstellen, aktivieren, bearbeiten oder löschen. Sie können auch in der Suchleiste oben rechts nach einer Regel suchen.



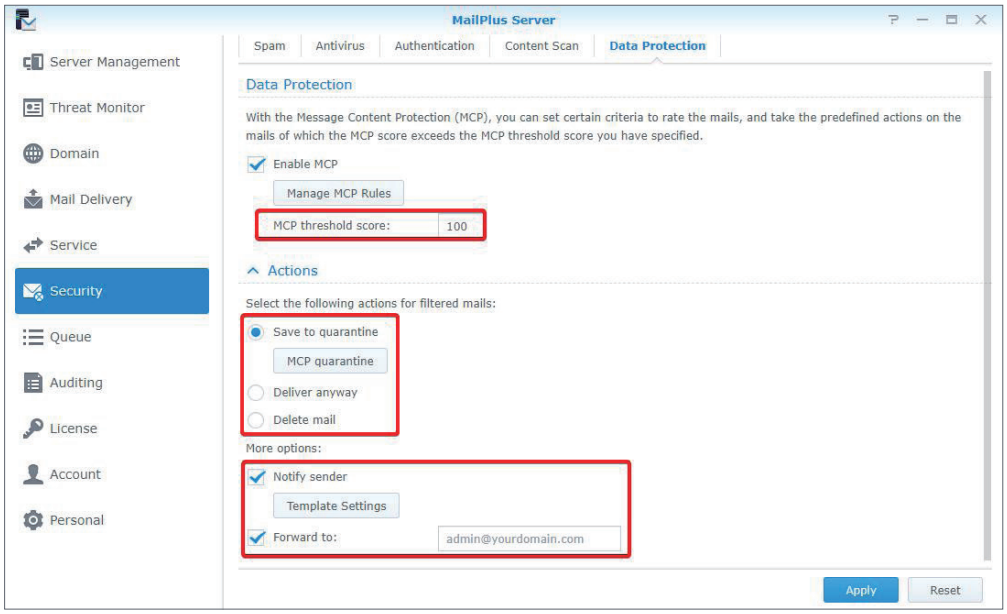
8. Klicken Sie auf **Fertig stellen**, um die Einstellungen abzuschließen.

Aktionen

Wenn die Gesamtwertung der übereinstimmenden Regeln den **MCP-Schwellwert** überschreitet, werden bestimmte Aktionen ausgeführt. Siehe die folgenden Schritte zur Einrichtung von Aktionen:

1. Gehen Sie zu **Sicherheit** > **Datenschutz** und geben Sie einen Wert in das Feld **MCP-Schwellwert** im Bereich **Datenschutz** ein.
2. Im Bereich **Aktionen** können Sie Aktionen einrichten, die ausgeführt werden, wenn der **MCP-Schwellwert** überschritten wurde:
   - **In Quarantäne speichern**: Blockiert E-Mail-Nachrichten und speichert sie im Bereich Quarantäne. Sie können auf **MCP-Quarantäne** klicken, um den Inhalt von Quarantänenachrichten anzuzeigen. Weitere Informationen über die Verwaltung von unter Quarantäne gestellten Nachrichten finden Sie unter **Quarantäneliste**.
   - **Trotzdem zustellen**: Stellt E-Mail-Nachrichten zu.
   - **E-Mail löschen**: Löscht E-Mail-Nachrichten.
   - **Weitere Optionen**: Benachrichtigt Absender oder leitet E-Mail-Nachrichten an ein bestimmtes Postfach weiter.

Funktion	Beschreibung
Absender benachrichtigen	Sendet eine E-Mail-Benachrichtigung, um Absender über die Blockierung ihrer E-Mails zu verständigen. Sie können auf die Schaltfläche **Vorlageneinstellungen** klicken, um den Inhalt der Benachrichtigung einzurichten.
Weiterleiten an	Leitet die ursprünglichen E-Mails an ein bestimmtes Postfach weiter.

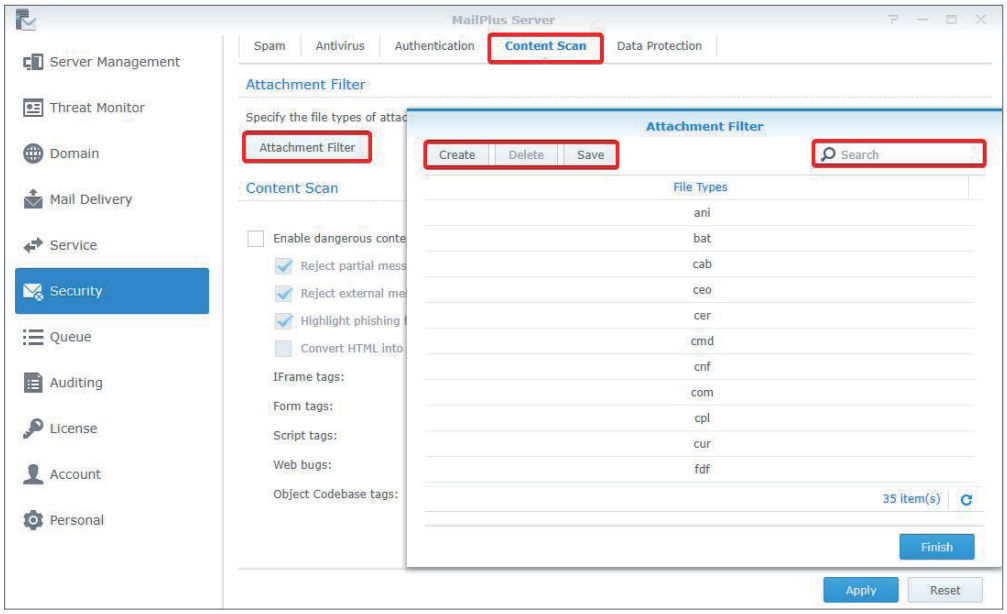


3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Anhangsfilter

Mit dem Anhangsfilter können Nachrichten anhand der Dateitypen im Anhang blockiert werden. Siehe die folgenden Schritte zur Einrichtung von Anhangsfiltern:

1. Gehen Sie zu **Sicherheit** > **Inhalt Scannen**.
2. Klicken Sie im Bereich **Anhangsfilter** auf die Schaltfläche **Anhangsfilter**.
3. Klicken Sie im Fenster **Anhangsfilter** auf die Schaltfläche **Erstellen**, um neue Dateitypen hinzuzufügen. Sie können einen Dateityp wahlweise **Löschen** oder oben rechts nach bestimmten Dateitypen suchen.



4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Fertig stellen**, um die Einstellungen abzuschließen.

Inhalt scannen

Die Funktion Inhalt scannen blockiert verdächtige Nachrichten oder ändert ihren Inhalt. Gehen Sie wie folgt vor, um die Einstellungen von **Inhalt scannen** anzupassen:

Anmerkung:

- Der geänderte Inhalt entspricht u.U. nicht den Erwartungen. Stellen Sie bitte sicher, dass Sie Funktionen nach Bedarf aktivieren.

1. Gehen Sie zu **Sicherheit** > **Inhalt scannen**.
2. Markieren Sie im Bereich **Inhalt scannen** das Kontrollkästchen **Scan auf gefährliche Inhalte aktivieren**, und passen Sie die folgenden Einstellungen an:
   - **Teilnachrichten ablehnen**: Lehnt E-Mails ab, die auf mehrere unvollständige Nachrichten aufgeteilt sind (inbesondere E-Mail-Nachrichten mit Content-Type-Wert „header message/partial“).
   - **Externe Nachrichtentexte ablehnen**: Lehnt E-Mails ab, die auf externe Ressourcen verweisen (insbesondere E-Mail-Nachrichten mit Content-Type-Wert „message/external-body“).
   - **Phishing-Betrug hervorheben**: Hebt erkannte Phishing-Links in einer E-Mail hervor, um Empfänger zu warnen.
   - **HTML in Klartext konvertieren**: Konvertiert Nachrichten im HTML-Format in Klartext.
   - Sie können für jedes Tag eine der folgenden Aktionen einrichten:

Aktion	Beschreibung
Zulassen	Stellt Nachrichten zu.
Verwerfen	Weist Nachrichten zurück.
Tags unwirksam machen	Stellt Nachrichten zu, nachdem Tags unwirksam gemacht wurden.

Anmerkung:

- Geben Sie bitte die Einstellungen für jedes Tag an.

Kapitel 10: Überwachungseinstellungen

Überwachen des Serverstatus

Sie können den Betriebsstatus des Servers über eine grafische Benutzeroberfläche schnell überblicken:

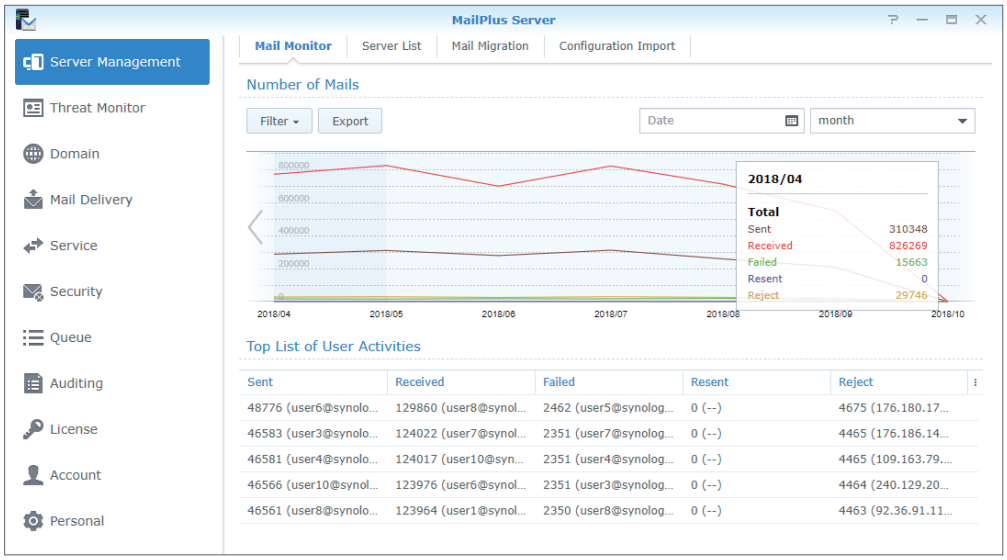
- **Überwachung des E-Mail-Datenverkehrs**: Überwacht den Datenverkehr des Servers nach bestimmten Zeitintervallen.
- **Bedrohungsmonitor**: Zeigt die Anzahl der E-Mail-Bedrohungen an, die von der jeweiligen Sicherheitseinstellung Ihres Servers blockiert wurden. Sie können alle Bedrohungsquellen schnell ermitteln und die Sicherheitseinstellungen entsprechend anpassen.
- **Serverliste**: Zeigt eine Liste der Server-Cluster und ihren Betriebsstatus an.

Überwachung des E-Mail-Datenverkehrs

Auf der Registerkarte **Mail Monitor** unter **Server-Management** wird die Statistik der E-Mail-Aktivität eines vergangenen Zeitraums angezeigt. Der Bereich **Top-Liste der Benutzeraktivitäten** enthält eine Liste der aktivsten E-Mail-Adressen jedes Datenverkehrstyps. Weitere Informationen über E-Mail-Datenverkehrstypen finden Sie unter **E-Mail-Protokolle anzeigen**.

Anmerkung:

- Wenn Sie bereits einen **High-Availability-Cluster** eingerichtet haben, überprüfen Sie die Protokolle auf dem primären Server.



Datenverkehr nach unterschiedlich langen Zeitintervallen überwachen

Sie können den E-Mail-Datenverkehr in MailPlus Server nach **Stunde**, **Tag**, **Woche** oder **Monat** überwachen. Jeder Datenpunkt im Diagramm **Anzahl E-Mails** gibt die Gesamtanzahl der E-Mails (eines bestimmten E-Mail-Datenverkehrstyps) während des Zeitintervalls an. Gehen Sie wie folgt vor, um den Zeitintervall anzupassen:

1. Gehen Sie zu **Server-Management** > **Mail Monitor**.
2. Sie können die Datums- und Zeitintervalle aus dem Feld **Datum** sowie aus dem Dropdown-Menü oben rechts im Bereich **Anzahl E-Mails** auswählen.

Datenverkehr eines bestimmten Zeitintervalls überwachen

Sie können bestimmte Zeitpunkte mit den folgenden zwei Methoden überwachen:

1. Bewegen Sie den Mauszeiger zum linken oder rechten Ende des Diagramms und klicken Sie auf die Pfeilsymbole, um sich zu einem bestimmten Zeitpunkt vor oder zurück zu bewegen.
2. Wählen Sie ein gewünschtes Datum aus dem Feld **Datum** oben rechts im Bereich **Anzahl E-Mails** aus.

Anmerkung:

- MailPlus Server reserviert eine unterschiedliche Anzahl von E-Mail-Daten für unterschiedlich lange Zeiträume. Sie können nur zu Zeitintervallen wechseln, die verfügbare Daten enthalten.

Anzeige der Detaildaten eines bestimmten Zeitraums fixieren

Die im Bereich der Detailinformationen auf dem Diagramm angezeigten Daten verändern sich, wenn Sie den Mauszeiger über bestimmte Zeitpunkte bewegen. Um Detailinformationen eines gewählten Zeitintervalls anzuzeigen, bewegen Sie den Cursor zum gewünschten Zeitintervall und drücken Sie die linke Maustaste, um den Bereich der Detailinformationen zu fixieren.

Daten von bestimmten Datenverkehrstypen anzeigen oder ausblenden

1. Gehen Sie zu **Server-Management** > **Mail Monitor**.
2. Klicken Sie auf die Schaltfläche **Filter** im Bereich **Anzahl E-Mails**, und markieren Sie die Kontrollkästchen, um die Daten von bestimmten Datenverkehrstypen anzuzeigen oder auszublenden.

Daten eines bestimmten Zeitintervalls exportieren

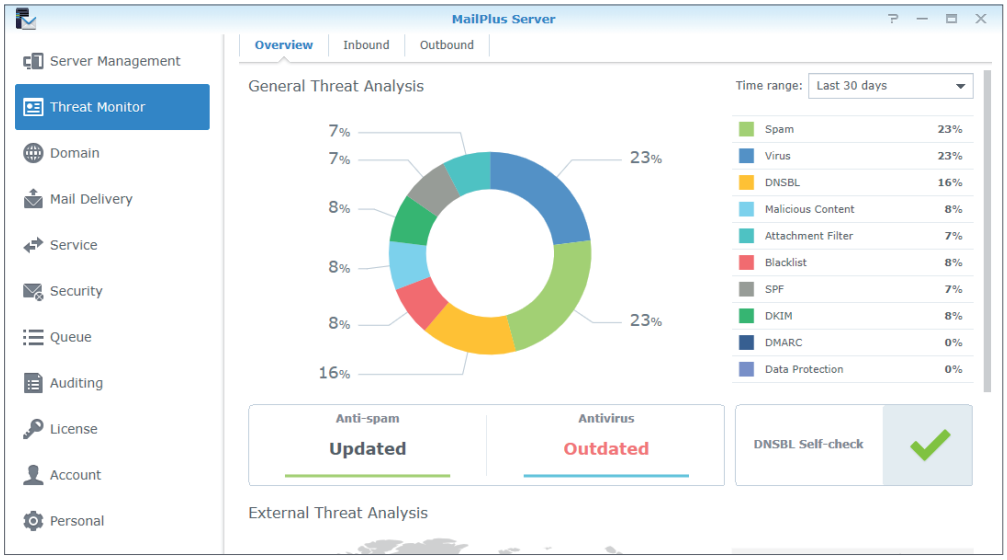
1. Gehen Sie zu **Server-Management** > **Mail Monitor**.
2. Klicken Sie im Bereich **Anzahl E-Mails** auf den Zeitintervall, den Sie auf dem Diagramm näher untersuchen möchten.
3. Klicken Sie oben auf die Schaltfläche **Exportieren**.
4. MailPlus Server exportiert die Daten sodann in eine .html-Datei.

Bedrohungsmonitor

Detailinformationen über E-Mail-Bedrohungen und ihre Quellen werden unter **Bedrohungsmonitor** angezeigt. Sie können die Einstellungen entsprechend der Bedrohungsanalyse anpassen, um MailPlus Server zu schützen.

Anmerkung:

- Wenn Sie bereits einen **High-Availability-Cluster** eingerichtet haben, überprüfen Sie die Protokolle auf dem primären Server.



Allgemeine Bedrohungsanalyse anzeigen

Die allgemeine Bedrohungsanalyse zeigt die Daten und Statistiken von aus- und eingehenden E-Mails auf einer grafischen Darstellung an. Gehen Sie wie folgt vor, um die Einstellungen von **Allgemeine Bedrohungsanalyse** anzupassen.

1. Gehen Sie zu **Bedrohungsmonitor** > **Überblick**.
2. Bedrohungsdaten und Statistiken werden gemeinsam mit den entsprechenden Einstellungen im Bereich **Allgemeine Bedrohungsanalyse** angezeigt:
   - **Zeitbereich**: Hier können Sie Statistiken zu Bedrohungen für einen bestimmten Zeitbereich anzeigen.
   - **Bedrohungsliste**: Zeigt prozentuale Aufteilung nach Bedrohungstyp. Um absolute Zahlen zu sehen, bewegen Sie den Mauszeiger über einen bestimmten Typ.
   - **Bedrohungs-Kreisdiagramm**: Zeigt prozentuale Aufteilung nach Bedrohungstyp. Sie können in der Liste rechts nach Bedarf Bedrohungstypen auswählen oder abwählen.
   - **Anti-Spam-Funktion**: Zeigt den Status des Anti-Spam-Moduls an. Durch Anklicken gelangen Sie zu der Seite, auf der Sie entsprechende Einstellungen vornehmen können.
   - **Antivirenfunktion**: Zeigt den Status des Antivirenmoduls an. Durch Anklicken gelangen Sie zu der Seite, auf der Sie entsprechende Einstellungen vornehmen können.
   - **DNSBL-Selbsttest**: Zeigt an, ob das Synology NAS sich auf einer DNSBL-Blacklist befindet.

Klicken, um weitere Details anzuzeigen.

Externe Bedrohungsanalyse anzeigen

Die externe Bedrohungsanalyse zeigt Quellen blockierter eingehender E-Mails und die entsprechenden Statistiken an.

1. Gehen Sie zu **Bedrohungsmonitor** > **Überblick**.
2. Im Bereich **Externe Bedrohungsanalyse** finden Sie eine Karte der Bedrohungen und die Anzahl für jede Quelle:
   - **Bedrohungskarte**: Jeder Kreis stellt eine Bedrohungsquelle dar. Je größer der Kreis, desto mehr blockierte E-Mails kommen aus diesem Gebiet. Um absolute Zahlen zu sehen, bewegen Sie den Mauszeiger über einen Kreis.
   - **Bedrohungsquelle**: Die Liste zeigt die sechs wichtigsten Quellen blockierter Mails und die entsprechenden Zahlen an.

Blockierte eingehende und ausgehende E-Mails anzeigen

Unter **Eingehend** und **Ausgehend** finden Sie Statistiken zu blockierten eingehenden bzw. ausgehenden E-Mails sowie die Top-Absender/Empfänger solcher E-Mails.

1. Gehen Sie zu **Bedrohungsmonitor**.
2. Klicken Sie auf die Registerkarte **Eingehend** oder **Ausgehend**.
   - **Zeitbereich**: Wählen Sie den Zeitbereich aus, um Statistiken zu blockierten eingehenden bzw. ausgehenden E-Mails über einen bestimmten Zeitraum anzuzeigen.
   - **Statistiken der blockierten Mails**: Das Diagramm zeigt die Trends für jeden Bedrohungstyp eingehender E-Mails (unter **Eingehend**) oder ausgehender E-Mails (unter **Ausgehend**) für den gewünschten Zeitbereich an.

Anmerkung:

- Um die angezeigten Bedrohungstypen zu ändern, wählen Sie die entsprechenden Legenden unter dem Diagramm aus oder heben Sie die Auswahl auf.
- Um die Anzahl für jeden Bedrohungstyp zu sehen, bewegen Sie den Mauszeiger über das Diagramm.

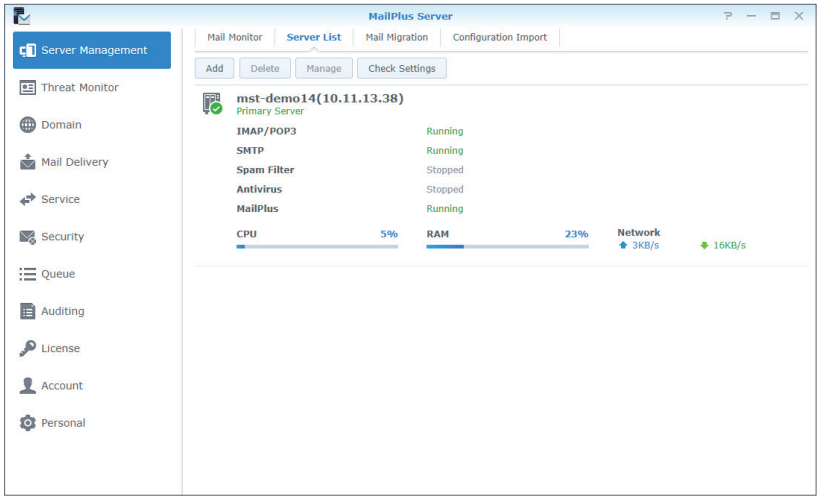
   - **Top-Absender blockierter Mails**: Die Tabelle zeigt die Top 10-Absender blockierter eingehender E-Mails (unter **Eingehend**) oder ausgehender E-Mails (unter **Ausgehend**) mit der Anzahl an. Um die vollständige Liste anzuzeigen, klicken Sie auf **Alle anzeigen**.
   - **Top-Empfänger blockierter Mails**: Die Tabelle zeigt die Top 10-Empfänger blockierter eingehender E-Mails (unter **Eingehend**) oder ausgehender E-Mails (unter **Ausgehend**) mit der Anzahl an. Um die vollständige Liste anzuzeigen, klicken Sie auf **Alle anzeigen**.

Serverliste

In der Registerkarte **Serverliste** auf der Seite **Server-Management** erhalten Sie einen Überblick über MailPlus Server mit Informationen zu CPU-, RAM- und Netzwerkauslastung. In der folgenden Liste finden Sie die möglichen Statusoptionen der Funktionen von MailPlus

Server:

- **Wird ausgeführt**: Die Funktion wird ordnungsgemäß ausgeführt.
- **Gestoppt**: Die Funktion wurde nicht aktiviert.
- **Abnormal**: Die Funktion ist nicht normal.
- **Nicht installiert**: Gilt nur für MailPlus. Dieser Status bedeutet, dass Sie MailPlus nicht installiert haben.
- **Wird vorbereitet**: Dieser Status bedeutet, dass Sie diese Funktion gerade aktiviert oder deaktiviert haben, und sie bereit für den Wechsel des Status ist.
- **E-Mails werden synchronisiert**: Wenn Sie einen MailPlus High-Availability-Cluster einrichten oder entfernen, synchronisiert das System die E-Mails. Dieser Status bedeutet, dass das System E-Mails synchronisiert.



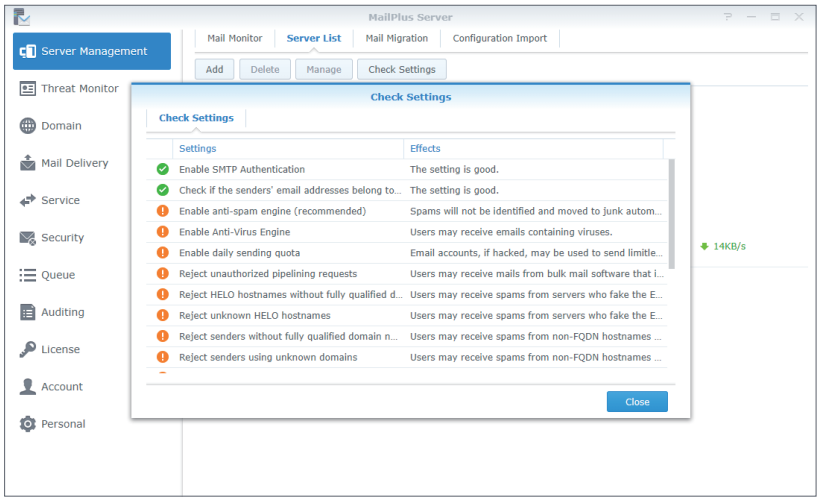
Anmerkung:

- Wenn **Antivirenprogramm** oder **MCP** aktiviert sind, wird der **Spam-Filter** ebenfalls aktiviert, auch wenn **Anti-Spam** nicht aktiviert ist; die Spam-Erkennung wird jedoch nicht ausgeführt.

Einstellungen überprüfen

Sie können unter **Einstellungen überprüfen** überprüfen, ob die Einstellungen auf Ihrem MailPlus Server den empfohlenen Einstellungen von Synology entsprechen. Sie können hier auch die Auswirkungen von verschiedenen Einstellungen sehen. Gehen Sie hierzu wie folgt vor:

1. Gehen Sie zu **Server-Management** > **Serverliste**.
2. Klicken Sie auf die Schaltfläche **Einstellungen überprüfen**.



Mail-Warteschlange überwachen

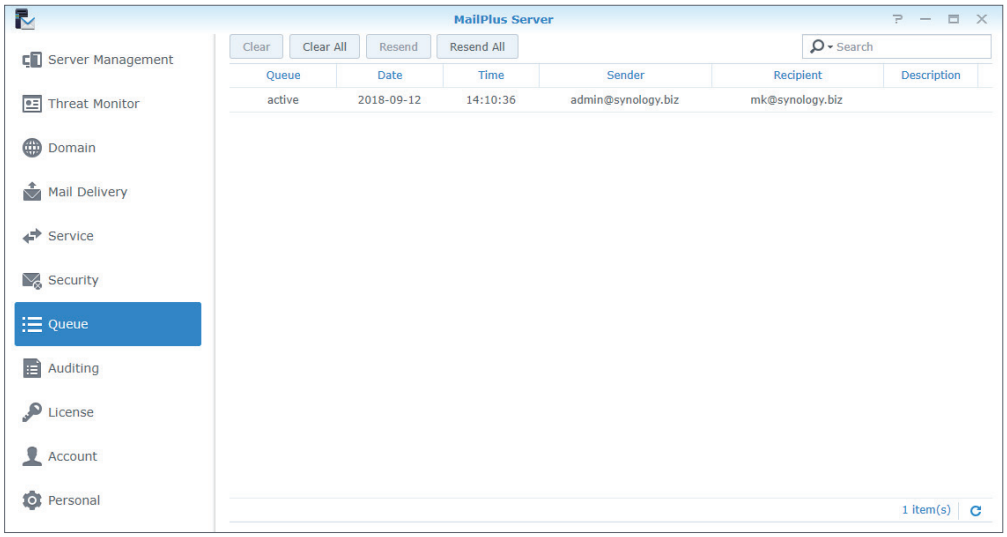
Sie können ausstehende E-Mails in der Mail-Warteschlange anzeigen und bestimmen, welche Aktion ausgeführt werden soll.

Nachrichten in der Mail-Warteschlange überwachen

Auf der Seite **Warteschlange** können Sie alle ausstehenden E-Mails überprüfen, die an andere Server gesendet werden sollen bzw. erneut an andere Server gesendet werden sollen, nachdem sie zurückgewiesen wurden.

Die Informationen zu den E-Mails in der Warteschlange werden wie folgt angezeigt:

- Datum und Uhrzeit des Einfügens der E-Mail in die Warteschlange
- Absender und Empfänger der E-Mail
- Warum sich eine Nachricht in der Mail-Warteschlange befindet (die Spalte **Beschreibung** gibt an, warum eine E-Mail nicht zugestellt werden konnte.)



Der Status der Mail-Warteschlange wird nach den folgenden drei Typen kategorisiert:

- **Halten**: Nachrichten warten auf Verarbeitung.
- **Aktiv**: Nachrichten werden gerade verarbeitet.
- **Zurückgestellt**: Nachrichten konnten nicht zugestellt werden und werden später erneut gesendet.

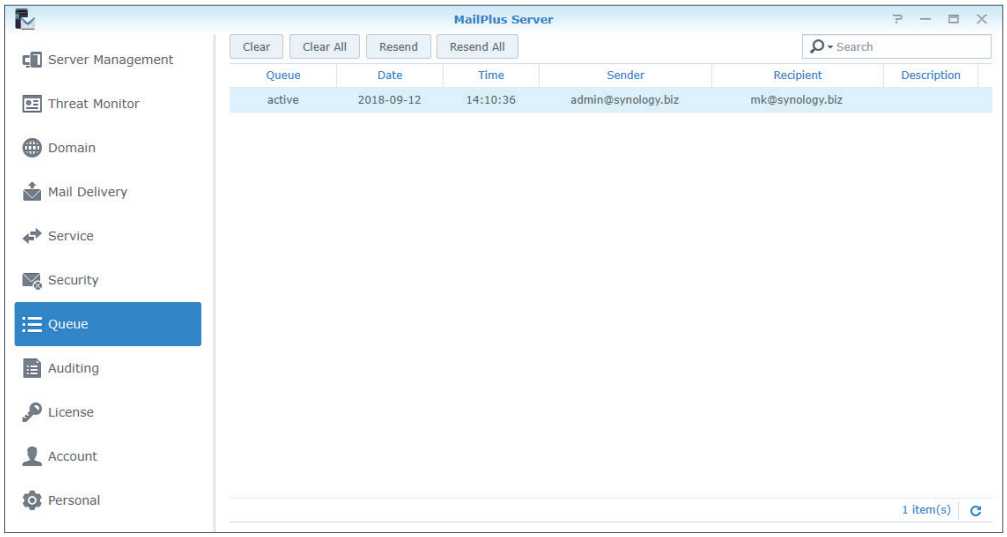
Anmerkung:

- Zurückgestellte E-Mails werden an Absender zurückgeschickt, wenn alle Versuche der Neuzustellung in den nächsten fünf Tagen fehlschlagen.

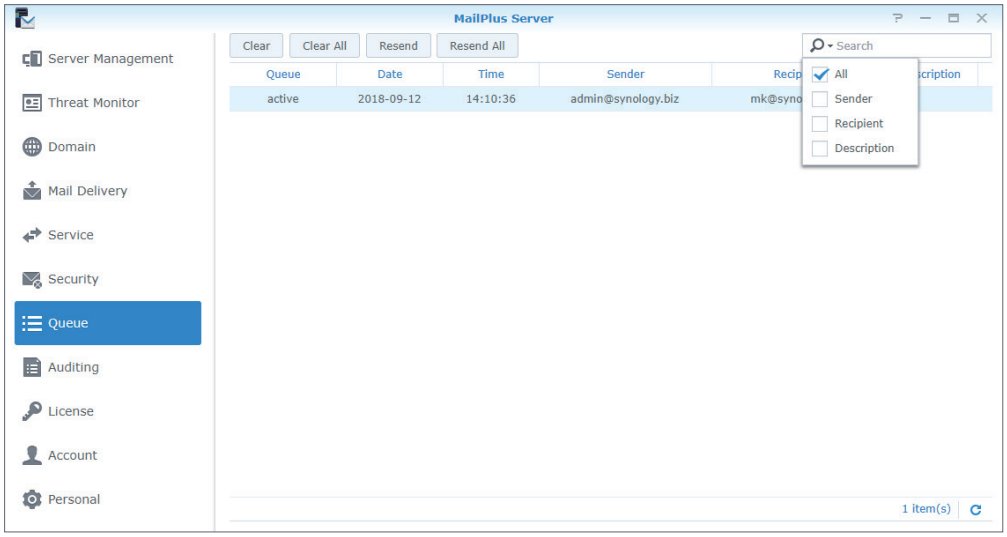
Nachrichten in der Mail-Warteschlange verwalten

Sie können wahlweise eine sofortige Neuzustellung versuchen oder die Zustellung von Nachrichten in der Warteschlange abbrechen. Gehen Sie wie folgt vor, um Nachrichten in der Mail-Warteschlange zu verwalten:

1. Gehen Sie zu **Warteschlange**, um Folgendes zu tun:
   - Um eine Nachricht erneut zuzustellen, wählen Sie diese in der Mail-Warteschlange aus und klicken Sie auf **Erneut senden**. Der Status der Nachricht ändert sich von **Bitte warten** zu **Aktiv**.
   - Um eine Nachricht zu entfernen, wählen Sie diese in der Mail-Warteschlange aus und klicken Sie auf **Löschen**. Die Nachricht wird aus der Warteschlange entfernt.
   - Um alle Nachrichten erneut zu senden, klicken Sie auf die Schaltfläche **Alle erneut senden**.
   - Um alle Nachrichten zu entfernen, klicken Sie auf die Schaltfläche **Alle löschen**.



2. Sie können auch in der Suchleiste oben rechts auf der Seite nach Nachrichten suchen, um den Status der jeweiligen Nachricht anzuzeigen.



E-Mail-Protokoll überwachen

E-Mail-Protokolle verzeichnen alle Aktivitäten des Servers. Sie können den Inhalt der Protokolle anzeigen, um nach Ursachen für Probleme und deren Lösung zu suchen. Beachten Sie bitte, dass Protokolldateien eine große Kapazität des Speicherplatzes beanspruchen können.

Die folgenden Protokolleinstellungen können auf der Seite **Überprüfung** konfiguriert werden.

- **Protokolle anzeigen**: Die in Protokollen verzeichneten Nachrichten anzeigen, suchen und analysieren.
- **Protokolle archivieren und verwalten**: Verschiedene Verwaltungseinstellungen konfigurieren, wie Archivierungsintervalle, Sicherung, Rotationsregeln sowie das Senden von Protokollen an sekundäre Server.
- **Protokollbericht**: Ermöglicht ein regelmäßiges Versenden von Protokollen per E-Mail-Benachrichtigungen.

E-Mail-Protokolle anzeigen

Gehen Sie wie folgt vor, um E-Mail-Protokolle anzuzeigen:

1. Gehen Sie zu **Überprüfung** > **Protokoll**.
2. Wählen Sie aus den Dropdown-Menüs im oberen Bereich die Optionen **E-Mail-Protokoll** und **Interne Datenbank** aus.
3. E-Mail-Protokolle zeigen die Nachrichten-ID, das generierte Datum und die Uhrzeit, den Absender, Empfänger, Titel, die Größe sowie den Status jeder Nachricht an. Der jeweilige Status wird wie folgt kategorisiert:
   - **Empfangen**: Dieser Status bedeutet, dass ein Benutzer von MailPlus eine Nachricht empfangen hat. Wenn ein MailPlus-Benutzer eine Nachricht an einen anderen MailPlus-Benutzer gesendet hat, wird der Status auf den Protokolleinträgen als **Empfangen** angezeigt. Wenn mehrere MailPlus-Benutzer dieselbe Nachricht empfangen, werden mehrere Protokolleinträge generiert. Wenn die Nachricht jedoch an eine Alias-E-Mail-Adresse in MailPlus Server gesendet wurde, wird der Protokolleintrag für die Alias-E-Mail-Adresse auch dann generiert, wenn der Alias mehrere Empfängeradressen enthält, und wenn einige der Benutzer im Alias von anderen Servern stammen. Wenn die autom. Weiterleitung aktiviert ist, werden Protokolleinträge mit dem Status **Empfangen** unabhängig davon generiert, ob das Kontrollkästchen **E-Mail-Kopie im Posteingang behalten** aktiviert ist.
   - **Gesendet**: Wenn Nachrichten an E-Mail-Adressen von anderen Servern gesendet wurden, werden mehrere Protokolleinträge generiert, sofern der Empfänger mehrere E-Mail-Adressen von anderen Servern enthält.
   - **Erneut senden**: Dieser Status bedeutet, dass mehrere Versuche zum erneuten Senden von Nachrichten an E-Mail-Adressen von anderen Servern unternommen wurden. Dieser Status wird bei MailPlus Server 1.3.0-0370 und höher nicht mehr verwendet.
   - **Fehlgeschlagen**: Dieser Status bedeutet, dass an andere Server gesendete Nachrichten nicht zugestellt werden konnten.

Anmerkung:

- Wenn Sie die Regeln von **Automatische BCC**, die **Automatische Weiterleitung** oder die **Automatische Antwort** eingerichtet haben, können zusätzliche Protokollinhalte generiert werden.
- Wenn Sie einen **High-Availability-Cluster** eingerichtet haben, überprüfen Sie die Protokolle auf dem primären Server.

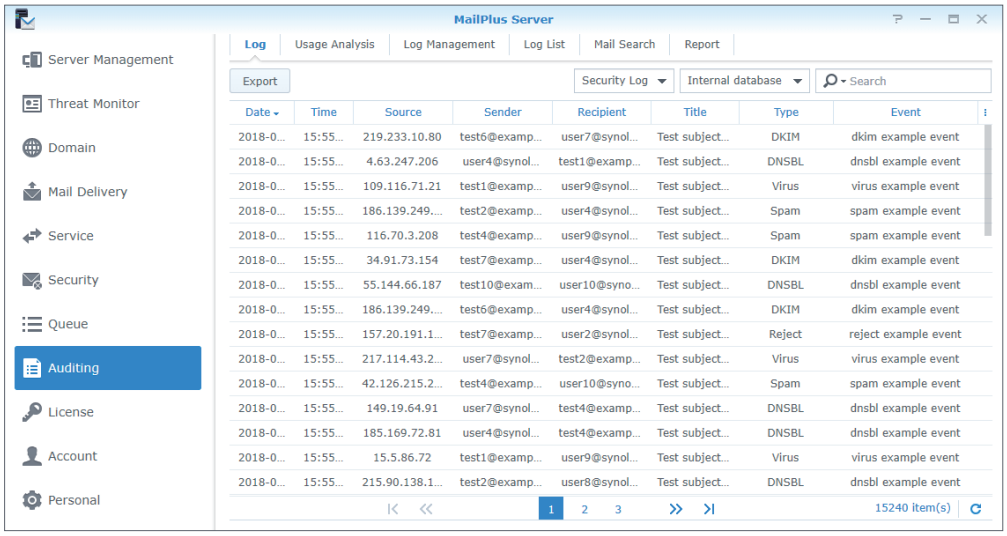
Sicherheitsprotokolle anzeigen

Sicherheitsprotokolle zeigen die Uhrzeit und das Datum eines Ereignisses sowie Quelle, den Absender, den Empfänger, den Titel, den Typ und die Ereignisbeschreibung an. Sicherheitsprotokolle werden wie folgt kategorisiert: **Abgelehnt**, **Spam**, **Virus**, **DNSBL**, **bösartige Inhalte**, **Anhangsfilter**, **Blacklist**, **SPF**, **DKIM**, **DMARC** und **Datenschutz**. Diese beziehen sich alle auf Sicherheitseinstellungen in MailPlus Server. Der Typ **Abgelehnt** bedeutet, dass MailPlus Server eine Nachricht nach Ausführung einer vollständigen Analyse zurückgewiesen hat. Gehen Sie wie folgt vor, um Sicherheitsprotokolle anzuzeigen:

Anmerkung:

- Wenn Sie bereits einen **High-Availability-Cluster** eingerichtet haben, überprüfen Sie die Protokolle auf dem primären Server.

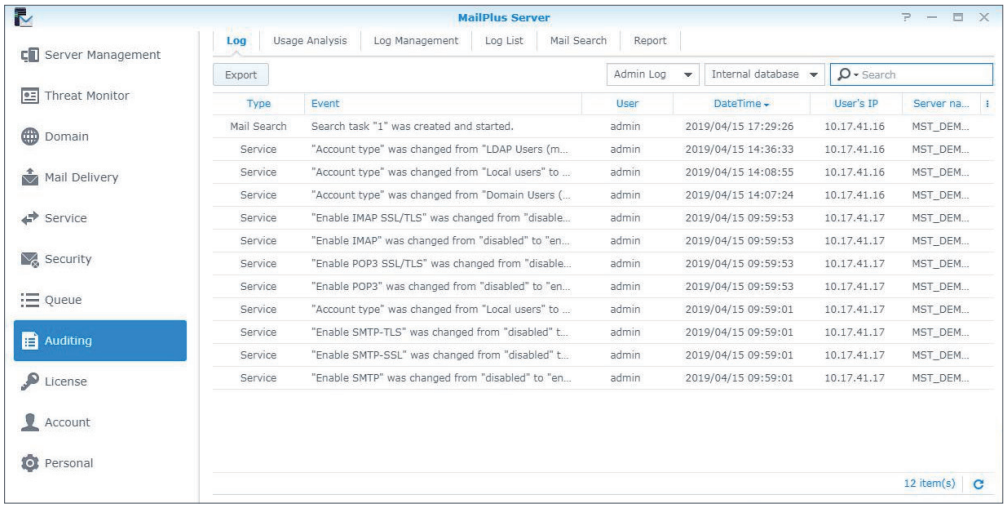
1. Gehen Sie zu **Überprüfung** > **Protokoll**.
2. Wählen Sie aus den Dropdown-Menüs im oberen Bereich die Optionen **Sicherheitsprotokoll** und **Interne Datenbank** aus.



Administrationsprotokolle anzeigen

Administrationsprotokolle verzeichnen vorgenommene Änderungen an den Einstellungen von MailPlus Server. Jedes Protokoll zeigt eine kurze Beschreibung des Ereignisses sowie den Typ, den Benutzer, die Uhrzeit und das Datum, die IP-Adresse des Benutzers und den Servernamen an. Gehen Sie wie folgt vor, um Administrationsprotokolle anzuzeigen:

1. Gehen Sie zu **Überprüfung** > **Protokoll**.
2. Wählen Sie aus den Dropdown-Menüs im oberen Bereich die Optionen **Admin-Protokoll** und **Interne Datenbank** aus.

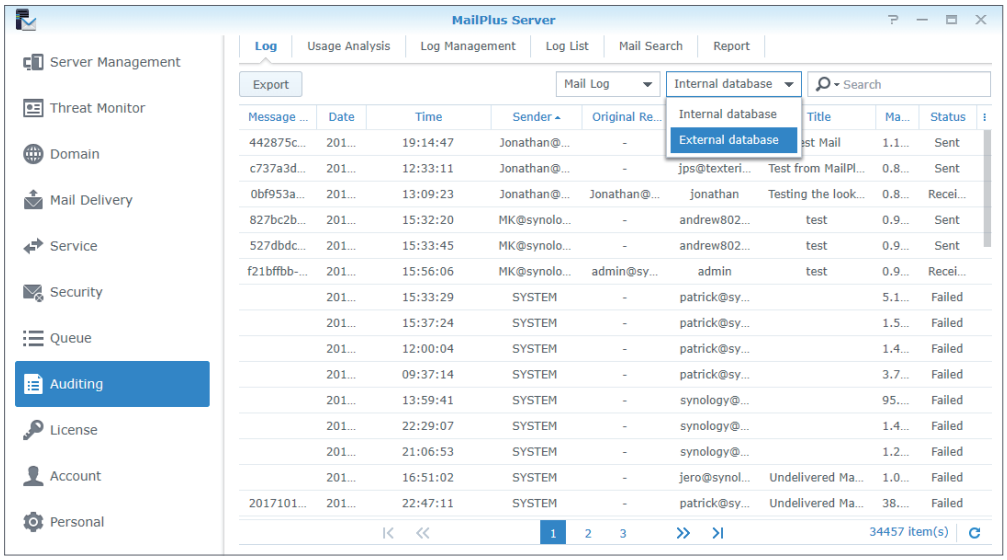


Externe Datenbank anzeigen

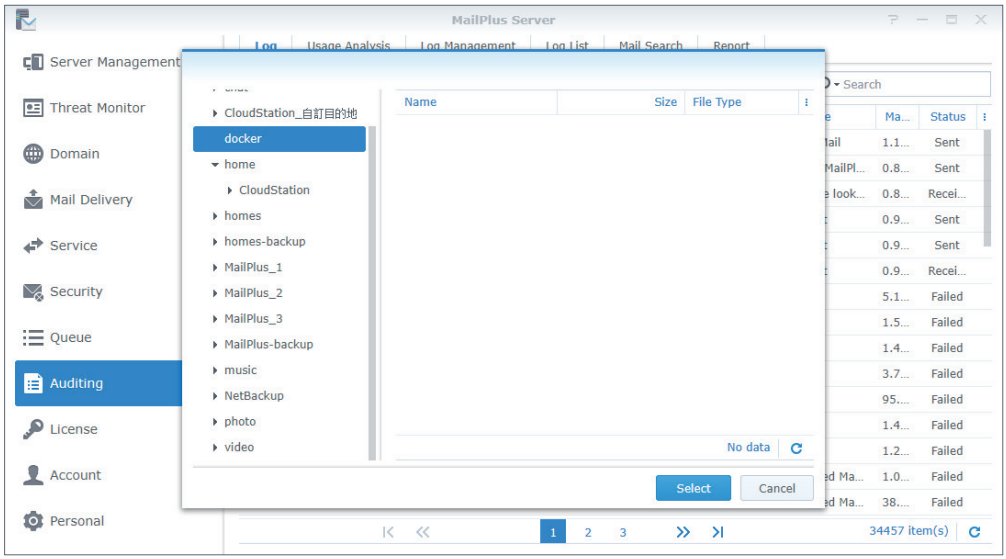
Wenn Sie Protokolle archiviert, eine Protokolldatenbank generiert oder Protokolldateien heruntergeladen haben, können Sie die unter **Externe Datenbank** gespeicherten Protokollinhalte anzeigen.

Gehen Sie wie folgt vor, um die externe Datenbank anzuzeigen:

1. Gehen Sie zu **Überprüfung** > **Protokoll**.
2. Wählen Sie aus den Dropdown-Menüs im oberen Bereich die Optionen **E-Mail-Protokoll**, **Sicherheitsprotokoll** oder **Admin-Protokoll** aus und wählen Sie anschließend **Externe Datenbank**.



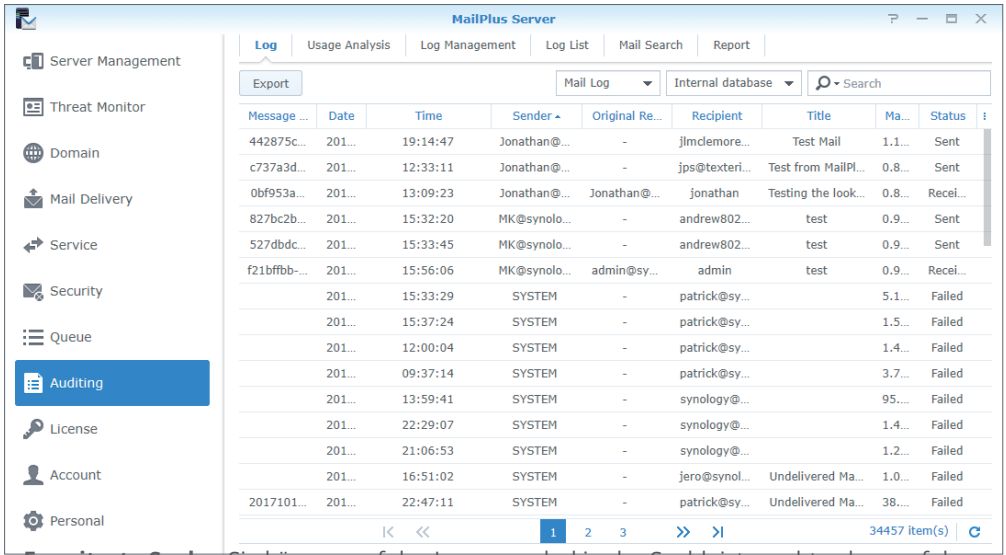
3. Suchen Sie den Speicherort Ihrer externen Datenbank auf dem Synology NAS.
4. Klicken Sie auf die Schaltfläche **Auswählen**.



Protokolle suchen

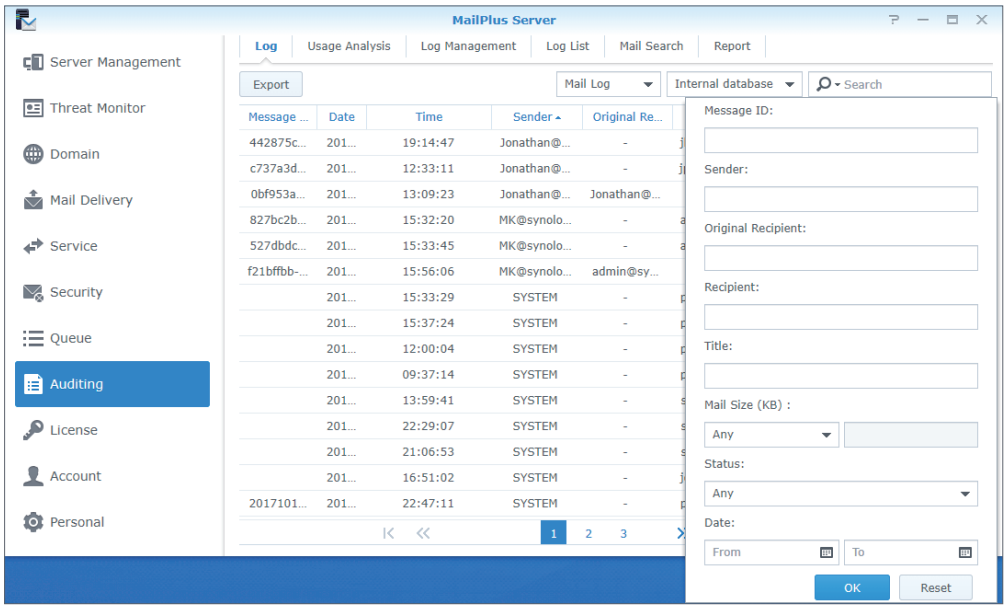
Unter **Überprüfung** > **Protokoll** können Sie mit der einfachen oder der erweiterten Suche nach Protokollen suchen.

- **Einfache Suche**: Sie können Schlüsselwörter in das Suchfeld oben rechts auf der Seite eingeben:
  - Beim **E-Mail-Protokoll** werden die eingegebenen Schlüsselwörter für die Suche nach Inhalten in den Spalten **Nachrichten-ID**, **Absender**, **Empfänger** und **Titel** verwendet.
  - Beim **Sicherheitsprotokoll** werden die eingegebenen Schlüsselwörter für die Suche nach Inhalten in den Spalten **Quelle**, **Absender**, **Empfänger**, **Titel** und **Ereignis** verwendet.
  - Beim **Admin-Protokoll** werden die eingegebenen Schlüsselwörter für die Suche nach Inhalten in den Spalten **Typ**, **Ereignis**, **Benutzer**, **IP des Benutzers** und **Servername** verwendet.



- **Erweiterte Suche**: Sie können auf das Lupensymbol in der Suchleiste rechts oben auf der Seite klicken. Legen Sie Suchkriterien für jedes Element fest, um eine präzise erweiterte Suche durchzuführen. Klicken Sie auf **OK**, nachdem Sie die Einstellungen abgeschlossen

habe. Im Dropdown-Menü **Status** können Sie **Innerhalb der Domain** auswählen, um Nachrichten zu suchen, die unter internen Benutzern gesendet wurden.

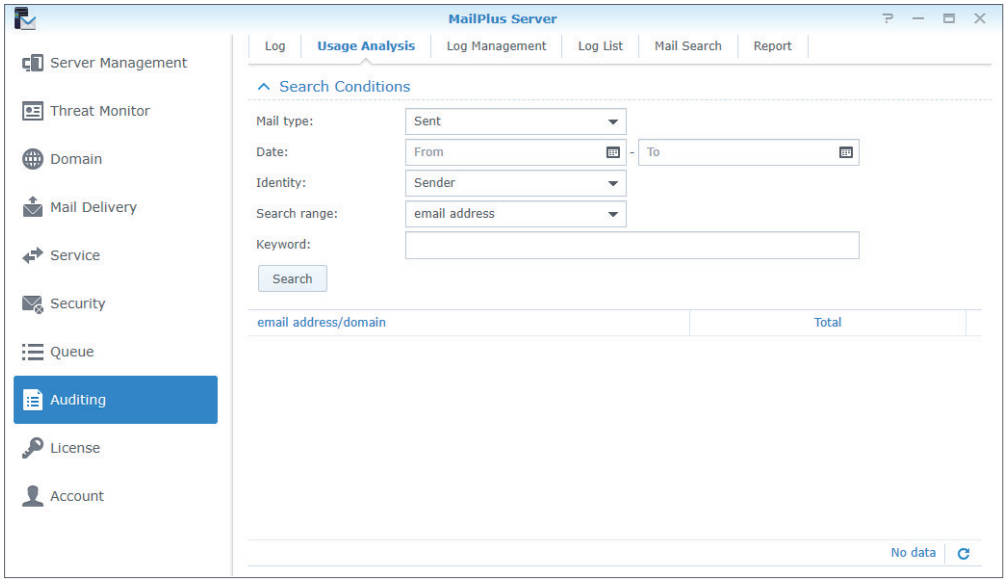


Protokollinhalte exportieren

Sie können Protokolle als .html-Datei unter **Überprüfung** > **Protokoll** exportieren. Wenn Sie nach der Protokollsuche auf die Schaltfläche **Exportieren** klicken, werden die Suchergebnisse exportiert. Beachten Sie hierzu **Protokolle suchen**.

Nutzungsanalyse

Sie können eine Nutzungsanalyse unter **Überprüfung** > **Nutzungsanalyse** durchführen, um eingehende und ausgehende Nachrichten zu analysieren, die von jeder E-Mail-Adresse oder Domain gesendet wurden.

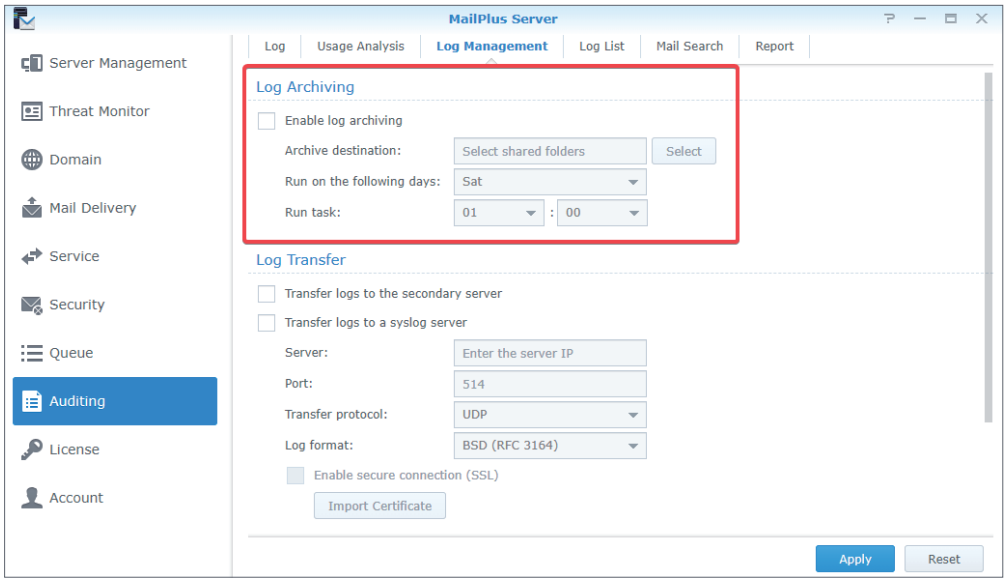


Protokolle archivieren

Sie können die Einstellungen zur Protokollarchivierung konfigurieren. MailPlus Server archiviert E-Mail-Protokolle, Sicherheitsprotokolle und Postfix-Protokolle nach einem benutzerdefinierten Zeitplan. Beachten Sie bitte, dass die Archivierungsfunktion automatisch deaktiviert wird, wenn Sie auf den freigegebenen Ordner nicht zugreifen können.

Gehen Sie wie folgt vor, um Protokolle zu archivieren:

1. Gehen Sie zu **Überprüfung** > **Protokollverwaltung**.
2. Markieren Sie im Bereich **Protokollarchivierung** das Kontrollkästchen **Protokollarchivierung aktivieren**.
3. Klicken Sie auf die Schaltfläche **Auswählen** neben dem Feld **Archivziel**, und wählen Sie das Ziel für die Archivdateien aus.
4. Wählen Sie die Zeit für die Ausführung von Archivierungsaufgaben aus.
5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.



Protokolle an den sekundären Server übertragen

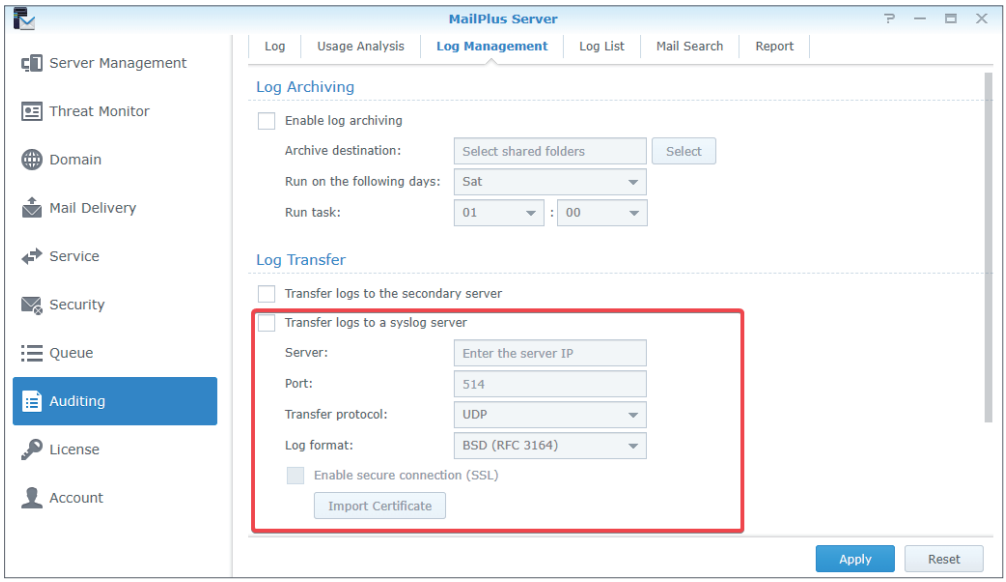
Nachdem ein **High-Availability-Cluster** eingerichtet wurde, werden Protokolle auf dem primären Server gesammelt. Sie können eine Kopie an den sekundären Server senden. Für das Senden von Protokollen an den sekundären Server muss eine Protokolldatenbank generiert werden (beachten Sie hierzu bitte **Protokolldatenbank erstellen**). Gehen Sie wie folgt vor, um Protokolle an den sekundären Server zu senden:

1. Gehen Sie zu **Überprüfung** > **Protokollverwaltung**.
2. Markieren Sie im Bereich **Protokollübertragung** das Kontrollkästchen **Protokolle an den sekundären Server übertragen**.
3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Postfix-Protokolle an andere Syslog-Server übertragen

Gehen Sie wie folgt vor, um Postfix-Protokolle an andere Syslog-Server zu senden:

1. Gehen Sie zu **Überprüfung** > **Protokollverwaltung**.
2. Markieren Sie im Bereich **Protokollübertragung** das Kontrollkästchen **Protokolle an einen Syslog-Server übertragen**.
3. Geben Sie die Daten des Syslog-Servers ein.
4. Wenn Sie das Kontrollkästchen **Sichere Verbindung (SSL) aktivieren** markieren, müssen Sie eventuell auf die Schaltfläche **Zertifikat importieren** klicken, um das Zertifikat des Syslog-Servers vor dem Senden von Protokollen zu importieren.
5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

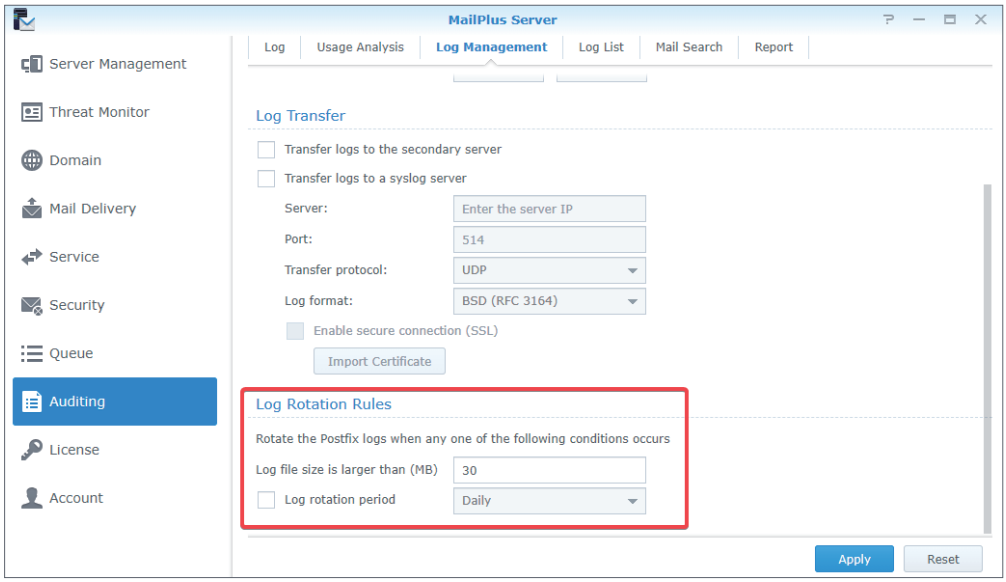


Protokoll-Rotationsregeln einrichten

Sie können die Rotationszeit und die Dateigröße für Postfix-Protokolle einrichten. Die aktuellsten 400 Millionen Einträge der E-Mail-Protokolldatenbank und Sicherheitsprotokoll-Datenbank werden beibehalten.

Gehen Sie wie folgt vor, um Protokoll-Rotationsregeln einzurichten:

1. Gehen Sie zu **Überprüfung** > **Protokollverwaltung**.
2. Geben Sie im Bereich **Protokoll-Rotationsregeln** einen Wert in das Feld **Protokolldatei ist größer als (MB)** ein.
3. Markieren Sie im Bereich **Protokoll-Rotationsregeln** das Kontrollkästchen **Protokoll-Rotationszeit** und wählen Sie aus dem Dropdown-Menü eine Rotationszeit aus.
4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

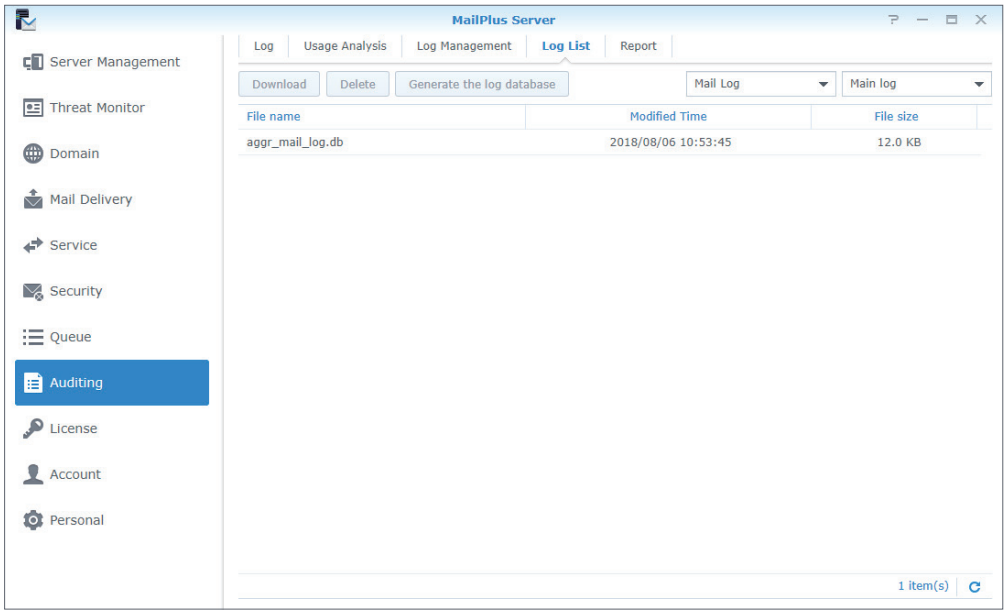


Protokolldateien herunterladen und löschen

Sie können E-Mail-Protokolle, Sicherheitsprotokolle, Admin-Protokolle oder Postfix-Protokolle unter **Überprüfung** > **Protokollliste** speichern oder entfernen.

Gehen Sie wie folgt vor, um Protokolldateien herunterzuladen oder zu löschen:

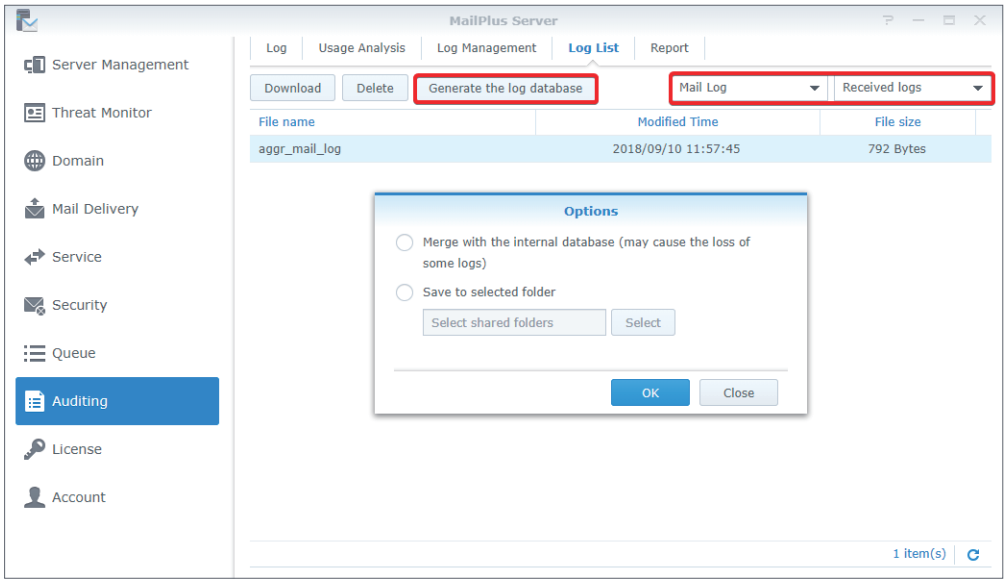
1. Gehen Sie zu **Überprüfung** > **Protokollliste**.
2. Wählen Sie **E-Mail-Protokoll**, **Sicherheitsprotokoll**, **Admin-Protokoll** oder **Postfix-Protokolle** aus dem Dropdown-Menü im oberen Bereich aus.
3. Wenn Sie einen MailPlus High-Availability-Cluster eingerichtet und die Option **Protokolle an den sekundären Server übertragen** aktiviert haben, können Sie **Empfangene Protokolle** aus dem Dropdown-Menü auf dem sekundären Server auswählen; wählen Sie andernfalls **Hauptprotokoll**.
4. Nach dem Auswählen einer Protokolldatei können Sie auf die Schaltfläche **Herunterladen** klicken, um die Datei herunterzuladen, oder auf **Löschen**, um die Datei vom Server zu löschen.



Protokolldatenbank generieren

Wenn Sie die Option **Protokolle an den sekundären Server übertragen** aktiviert haben, können Sie mit der Funktion **Protokolldatenbank generieren** empfangene Protokollinhalte zurück zu Datenbankdateien konvertieren. Mit der Option **Externe Datenbank anzeigen** unter **Überprüfung** > **Protokoll** können Sie Dateien in der Protokolldatenbank anzeigen.

1. Gehen Sie zu **Überprüfung** > **Protokollliste**.
2. Wählen Sie **E-Mail-Protokoll**, **Sicherheitsprotokoll** oder **Postfix-Protokoll** aus dem Dropdown-Menü aus.
3. Wählen Sie **Empfangenes Protokoll** aus dem Dropdown-Menü aus.
4. Wählen Sie eine Protokolldatei aus und klicken Sie auf die Schaltfläche **Protokolldatenbank generieren**.
5. Wählen Sie die Option **Mit interner Datenbank zusammenlegen (einige Protokolle können verloren gehen)** oder **In ausgewähltem Ordner speichern** und anschließend einen Zielordner aus.
6. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.



Anmerkung:

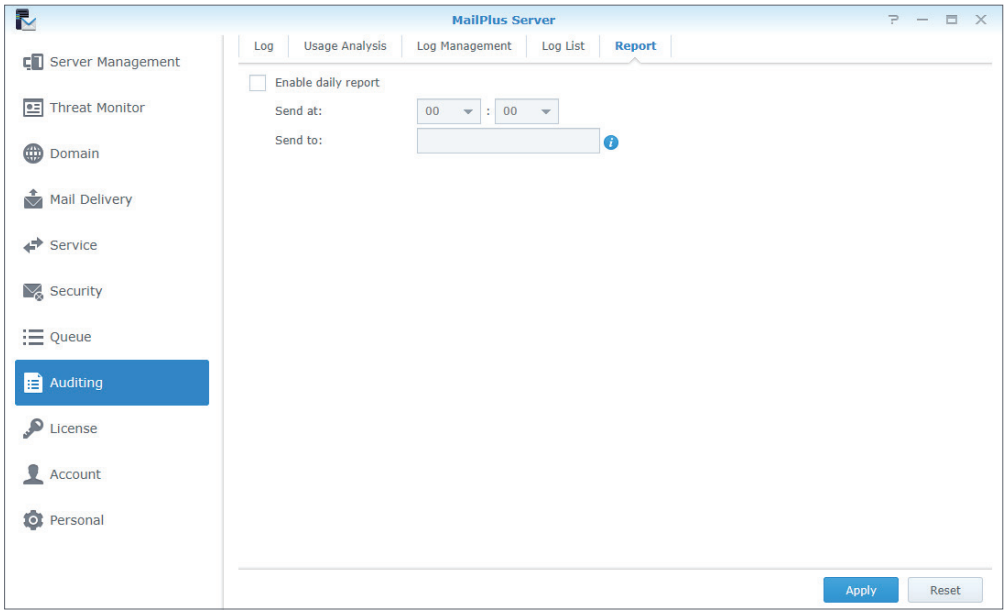
- Sie müssen keine Protokolldatenbank für das **Admin-Protokoll** generieren. Sie können es auf beiden Servern anzeigen, nachdem Sie die Option **Protokolle an den sekundären Server übertragen** aktiviert haben.
- Es werden nur Protokolle, die nach Aktivierung der Option **Protokolle an den sekundären Server übertragen** generiert wurden, mit dem anderen Server synchronisiert.

Tagesberichte einrichten

Sie können die Funktion der Tagesberichte aktivieren, damit Postfix-Protokolle des vorhergehenden Tages an eine bestimmte E-Mail-Adresse gesendet werden.

Gehen Sie wie folgt vor, um Tagesberichte einzurichten.

1. Gehen Sie zu **Überprüfung** > **Bericht**.
2. Markieren Sie das Kontrollkästchen **Tagesbericht aktivieren**.
3. Wählen Sie eine Zustellungszeit aus.
4. Geben Sie in das Feld **Senden an** die Zieladresse für Tagesberichte ein. Sie können bis zu zwei E-Mail-Adressen festlegen, die durch einen Strichpunkt (;) getrennt werden müssen.



E-Mail-Suche einrichten

Sie finden alle indizierten E-Mails in MailPlus Server, sowie Funktionen zum Anzeigen, Löschen und Exportieren der Suchergebnisse.

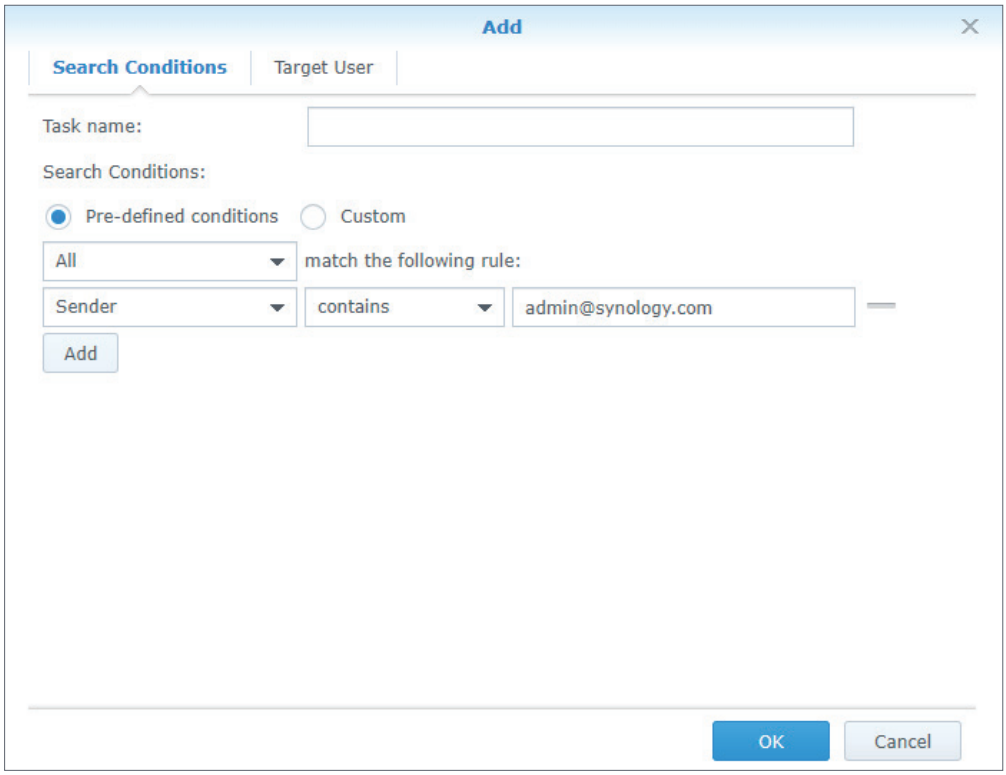
Bitte gehen Sie wie folgt vor, um eine E-Mail-Suchaufgabe zu erstellen:

1. Gehen Sie zu **Überprüfung** > **E-Mail-Suche**.
2. Klicken Sie auf das Plus-Symbol (+), um eine neue Aufgabe zu erstellen.
3. Geben Sie **Aufgabenname** ein.
4. Legen Sie die **Suchbedingungen** fest:
   - **Vordefinierte Bedingungen**: Sie können mehrere Suchbedingungen zu einer Suchaufgabe hinzufügen. Treffen Sie eine Auswahl aus dem Dropdown-Menü, um E-Mails zu suchen, die mit **allen** oder **einer der** Bedingungen übereinstimmen, und definieren Sie die Bedingungen nach **Absender**, **Empfänger**, **Betreff**, **Schlüsselwort**, **E-Mail-Größe (MB)** oder **Datum**, welche die eingegebenen Schlüsselwörter **enthalten** oder **nicht enthalten**.
   - **Benutzerdefiniert**: Sie können die Suchbedingungen auch mit Suchoperatoren und Schlüsselwörtern anpassen. Beispiel: Um nach einer E-Mail über ***GDPR*** zu suchen, die nach dem ***25. Mai 2018*** von der Adresse ***admin@synology.com*** gesendet wurde, können Sie ***after:2018/05/25 AND from:admin@synology.com AND GDPR*** als Suchbedingung eingeben.

Suchoperator	Nutzung	Beispiel
from:	Nachrichten vom angegebenen Absender	from:amy
to:	Nachrichten an den angegebenen Empfänger	to:david

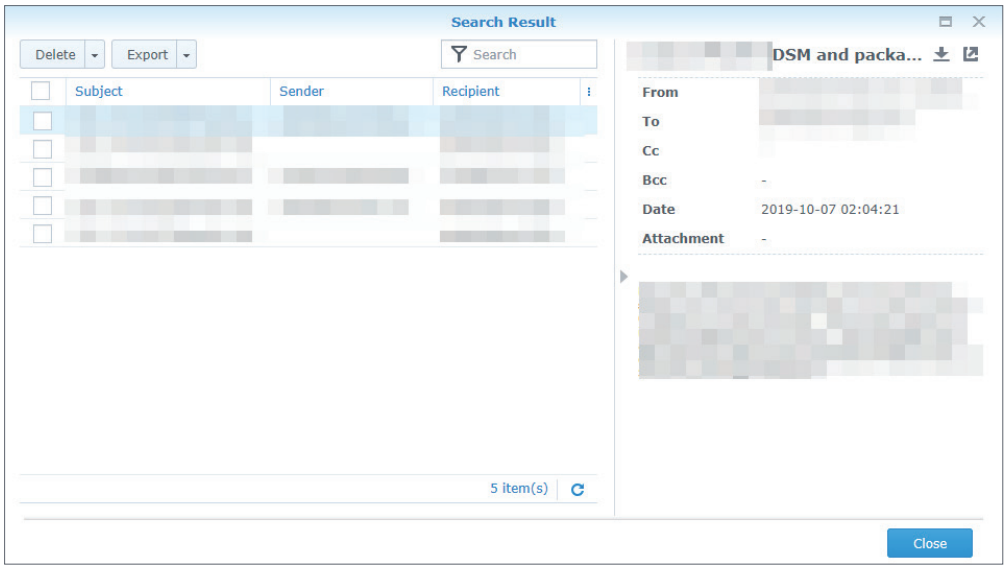
Suchoperator	Nutzung	Beispiel
subject:	Nachrichten mit bestimmten Begriffen im Betreff	subject:Abendessen
OR	Nachrichten, die mehrere angegebene Begriffe enthalten	from:amy OR from:david
- oder NOT	Nachrichten, die aus den Suchergebnissen entfernt werden sollen	Abendessen - Film
( )	Nachrichten, die die angegebenen Begriffe zusammen enthalten	subject:(Abendessen Film)
in:	Nachrichten im angegebenen Postfach	in: "Vorgeschlagene Funktion"
label:	Nachrichten mit einer bestimmten Kennzeichnung	label:freunde
before: oder after:	Nachrichten, die in einem bestimmten Zeitraum gesendet wurden	after:2004/04/16
larger: oder smaller:	Nachrichten größer oder kleiner als eine bestimmte Größe in MB	larger:10M
filename:	Anhänge mit einem bestimmten Namen oder Dateityp	filename:pdf
has:attachment	Nachrichten mit Anhängen	has:attachment
is:starred	Nachrichten mit Sternchen	is:starred
is:unread	Ungelesene Nachrichten	is:unread

5. Wählen Sie **Zielbenutzer**. Wenn keine Zielbenutzer angegeben werden, sucht die Aufgabe standardmäßig nach allen Benutzern.
6. Klicken Sie auf **OK**, und die Suchaufgabe wird sofort gestartet.
7. Sie können eine laufende Aufgabe stoppen, indem Sie sie auswählen und rechts auf **Aufgaben beenden** klicken. Klicken Sie auf **Suche**, wenn Sie eine Aufgabe erneut starten möchten.
8. Sie können eine Aufgabe **Bearbeiten**, **Kopieren** oder **Löschen**, indem Sie sie auswählen und auf das entsprechende Symbol klicken.



E-Mail-Suchergebnisse anzeigen

1. Gehen Sie zu **Überprüfung** > **E-Mail-Suche** und wählen Sie eine abgeschlossene Suchaufgabe aus.
2. Rechts können Sie **Aufgabenberichte herunterladen** oder auf **Ergebnis anzeigen** klicken, um weitere Details und Aktionen angezeigt zu bekommen. Aufgabenberichte zeigen Ihnen Details zu einer Aufgabe an, darunter die Anzahl der durchsuchten E-Mails sowie die gelöschten E-Mails.
3. Im Fenster **Ergebnis anzeigen** können Sie jede E-Mail anzeigen, löschen oder exportieren. Details zu jeder E-Mail werden rechts angezeigt, wenn Sie sie auswählen. Sie können auch die ursprüngliche E-Mail oder ihre Anhänge herunterladen oder die E-Mail in einer neuen Registerkarte öffnen.



E-Mail-Suchergebnisse exportieren

Wir empfehlen, wichtige E-Mail-Suchergebnisse stets zu exportieren und Sicherungskopien auf Ihrem lokalen Gerät zu speichern, falls Sie sie später noch einmal benötigen sollten.

1. Gehen Sie zu **Überprüfung** > **E-Mail-Suche** und wählen Sie eine abgeschlossene Suchaufgabe aus.
2. Wählen Sie eine Aufgabe aus und klicken Sie rechts auf **Ergebnis anzeigen**.
3. Wählen Sie die Suchergebnisse aus, die Sie exportieren möchten, und klicken Sie auf **Exportieren**.
4. Sie können auf das Pfeilsymbol neben **Exportieren** klicken, um zu bestimmen, ob sowohl E-Mail-Liste wie auch ursprüngliche E-Mails oder nur die E-Mail-Liste exportiert werden soll.
5. Sie finden die exportierte E-Mail-Liste als Datei namens **export_list.csv**, die mit einem Programm, das .csv-Dateien unterstützt, bearbeitet werden kann. Wenn Sie eine Überprüfungsaufgabe verteilen möchten, können Sie den Datensatz auf mehrere Dateien aufteilen. Exportierte Original-E-Mails finden Sie als .eml-Dateien im Ordner **eml**.

E-Mail-Suchergebnisse importieren

Wenn Sie E-Mail-Suchergebnisse exportiert und auf Ihrem lokalen Gerät gespeichert haben, können Sie die E-Mail-Liste zur Überprüfung der E-Mails jederzeit importieren.

1. Gehen Sie zu **Überprüfung** > **E-Mail-Suche**.
2. Klicken Sie neben dem Papierkorbsymbol auf das Symbol **Aufgaben importieren**.
3. Laden Sie eine E-Mail-Liste im CSV-Format hoch und geben Sie einen Aufgabennamen ein.
4. Klicken Sie auf **Importieren**.
5. Nachdem der Import abgeschlossen wurde, wird die Aufgabe oben in der Aufgabenliste angezeigt.

Kapitel 11: Disaster Recovery

High-Availability-Cluster

MailPlus Server bietet zwei Lösungen: **Einzelknoten**-Konfiguration und **High-Availability**-Konfiguration. Die Einzelknoten-Konfiguration erfordert ein Synology NAS, um E-Mail-Dienste auszuführen, während die High-Availability-Konfiguration zwei Synology NAS benötigt, um einen High-Availability-Cluster (HA) zu bilden, der unterbrechungsfreie E-Mail-Dienste bei unvorhergesehenen Ereignissen gewährleistet.

Einführung in die High-Availability-(HA)-Konfiguration

Der High-Availability-(HA)-Cluster besteht aus zwei Synology NAS-Geräten, von denen einem die Rolle des „primären Servers“ zukommt und der andere als „sekundärer Server“ fungiert. Benutzer und andere Mailserver stellen eine Verbindung zur Haupt-IP-Adresse des MailPlus HA-Clusters her. Der primäre Server wird auf der Haupt-IP-Adresse des MailPlus HA-Clusters ausgeführt und empfängt alle Dienstanforderungen. Diese Anforderungen werden anschließend dem primären oder dem sekundären Server zur Verarbeitung zugewiesen.

Eine Zwei-Wege-Synchronisierung wird durchgeführt, um sicherzustellen, dass E-Mail-Daten und Servereinstellungen konsistent bleiben und über primäre und sekundäre Server synchronisiert werden. Wenn beide Server unterschiedliche Dienstanforderungen verarbeiten oder wenn Sie die Einstellungen von MailPlus Server auf einem der beiden Server bearbeiten, kann die Zwei-Wege-Synchronisierung die Wahrscheinlichkeit einer Dateninkonsistenz verringern.

Im Gegensatz zu E-Mail-Daten und Servereinstellungen werden Protokolle in der HA-Konfiguration auf dem primären Server gesammelt. Sie können Protokolle auf dem primären Server anzeigen oder **Protokolle an den sekundären Server übertragen** wählen, um eine Kopie zu versenden.

Die HA-Konfiguration minimiert Dienstunterbrechungen bei Fehlfunktionen des Servers. Wenn der primäre Server eine Fehlfunktion hat, übernimmt der sekundäre Server vorübergehend alle E-Mail-Dienstanforderungen. Nach der Wiederherstellung des primären Servers werden Datenänderungen, die in der Failover-Phase verarbeitet wurden, wieder mit dem primären Server synchronisiert. Wenn der sekundäre Server ausfällt, übernimmt der primäre Server die gesamte Arbeitslast, und die in dieser Zeit ausgeführten Datenänderungen werden ebenfalls mit dem sekundären Server synchronisiert, nachdem dieser wiederhergestellt ist.

Anmerkung:

- MailPlus High-Availability-Cluster und Synology High Availability (SHA) sind zwei verschiedene Cluster-Systeme und können nicht gleichzeitig auf demselben Synology NAS ausgeführt werden.
- Synology High Availability wird für MailPlus 2.2 und höher unterstützt.
- Wenn eine kontinuierliche Dienstbereitstellung erforderlich ist, sollten Sie den für E-Mail-Dienste konzipierten MailPlus High-Availability-Cluster in Erwägung ziehen. Nachdem ein High-Availability-Cluster wiederhergestellt wurde, bleiben die Daten auf beiden Servern konsistent. Somit wird der Verlust von Daten verhindert, die während des Split-Brain-Fehlers aktualisiert wurden.
- In SHA werden zwei MailPlus-Server als ein einziger betrachtet und teilen sich die 5 kostenlosen Lizenzen. In MailPlus HA sind dagegen 10 kostenlose Lizenzen verfügbar.

Vor der Konfiguration von High Availability (HA)

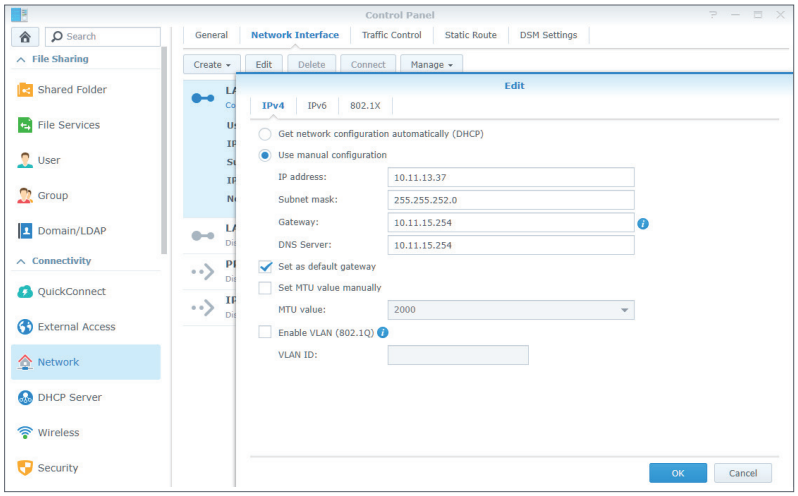
1. **Bereiten Sie zwei Synology NAS-Geräte vor**:

   - Melden Sie sich beim selben Synology-Konto unter **Systemsteuerung** > **Info-Center** > **Synology-Konto** auf den beiden Synology NAS-Geräten an.
   - Synchronisieren Sie die Systemzeit zwischen den beiden Synology NAS-Geräten unter **Systemsteuerung**> **Regionale Optionen** > **Uhrzeit**.
   - Gehen Sie zum **Paketzentrum** , um **MailPlus Server** und **MailPlus** auf beiden Synology NAS-Geräten zu installieren und zu initialisieren. Weitere Informationen zur Einrichtung von MailPlus Server finden Sie im Abschnitt **MailPlus Server einrichten**.
   - Nach der Einrichtung von MailPlus Server wird dem Synology NAS automatisch ein freigegebener Ordner **MailPlus** hinzugefügt. Um sicherzustellen, dass Client-Benutzer auf MailPlus zugreifen können, empfehlen wir Ihnen, Berechtigungen nicht selbst zu bearbeiten. Legen Sie die Berechtigungseinstellungen für den freigegebenen Ordner **MailPlus** als Standard fest.
   - Legen Sie die Berechtigungen der Zielbenutzer oder der Zielgruppen für MailPlus Server und MailPlus unter **Systemsteuerung** > **Berechtigungen** fest. Die Einstellungen sollten bei beiden Synology NAS-Geräten identisch sein.

Anmerkung:

- Die Größe der Volumes, auf denen sich MailPlus Server befindet, sollte gleich groß sein. Da außerdem alle eingehenden und ausgehenden E-Mails vollständig mit beiden Volumes synchronisiert werden, stellen Sie bitte sicher, dass die Volume-Größe die Anforderungen an den E-Mail-Speicherplatz erfüllt.
- Wenn Sie einen SSD-Cache auf beiden Volumes bereitgestellt haben, beachten Sie bitte Folgendes:
  - Es sollte sich um Lese/Schreib-Caches in einer RAID 1-Konfiguration handeln.
  - Die Cache-Größe sollte identisch sein.
- Die Funktion der 2-Stufen-Verifizierung muss bei der Erstellung des HA-Clusters auf dem sekundären Server vorübergehend deaktiviert werden.

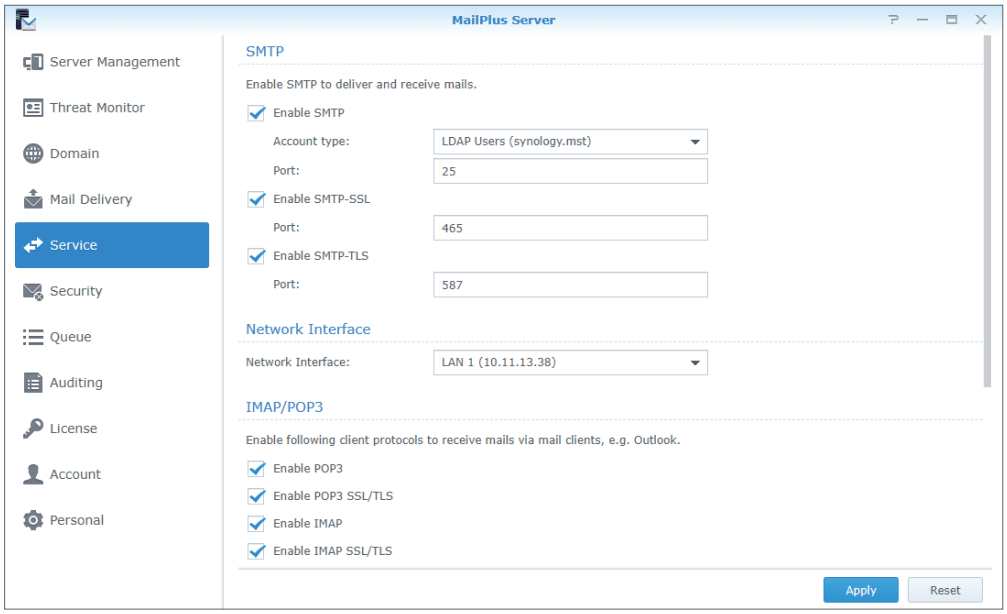
2. **Weisen Sie den primären und sekundären Servern zwei Gruppen von statischen IP-Adressen zu**:
   - Die IP-Adressen für beide Synology NAS-Geräte müssen sich im selben LAN befinden.
   - Die IP-Adressen dürfen nicht über PPPoE oder DHCP abgerufen werden.
   - Die Netzwerkkarte der IP-Adresse sollte für eine manuelle Netzwerkkonfiguration eingerichtet sein.



3. **Beide Synology NAS-Geräte müssen an dieselbe Domain angebunden werden**:
   - Beide Synology NAS-Geräte müssen einem Windows Active Directory- oder LDAP-Server beitreten. Weitere Informationen zur Anbindung von Windows Active Directory finden Sie in **dieser Anleitung**. Weitere Informationen zur Anbindung von LDAP-Server finden Sie in **diesem Artikel**.
   - Wenn Sie in Ihrer Umgebung über keinen Windows Active Directory- oder LDAP-Server verfügen, können Sie zum **Paketzentrum** wechseln und **Synology Directory Server** oder **LDAP Server** installieren, um eine Domain oder einen LDAP-Server für die Kontoverwaltung einzurichten. Beachten Sie bitte, dass bei selbstgehosteten LDAP- oder Domain-Diensten das Risiko für eine Unterbrechung des E-Mail-Dienstes besteht, wenn das Synology NAS, das das Verzeichnis hostet, abnormal ist oder nicht reagiert.
4. **Bereiten Sie eine interne und externe IP-Adresse für den HA-Cluster vor**:
   - Reservieren Sie eine nicht verwendete interne statische IP-Adresse, die sich im selben LAN wie die IP-Adressen der beiden Synology NAS befinden sollte, sowie eine nicht verwendete externe IP-Adresse für den HA-Cluster.
   - Konfigurieren Sie Portweiterleitungsregeln auf dem Router, um den Datenverkehr zwischen internen und externen Cluster-IP-Adressen weiterzuleiten.
   - Registrieren Sie die externe Cluster-IP-Adresse auf einem öffentlichen DNS-Server (Domain Name System).

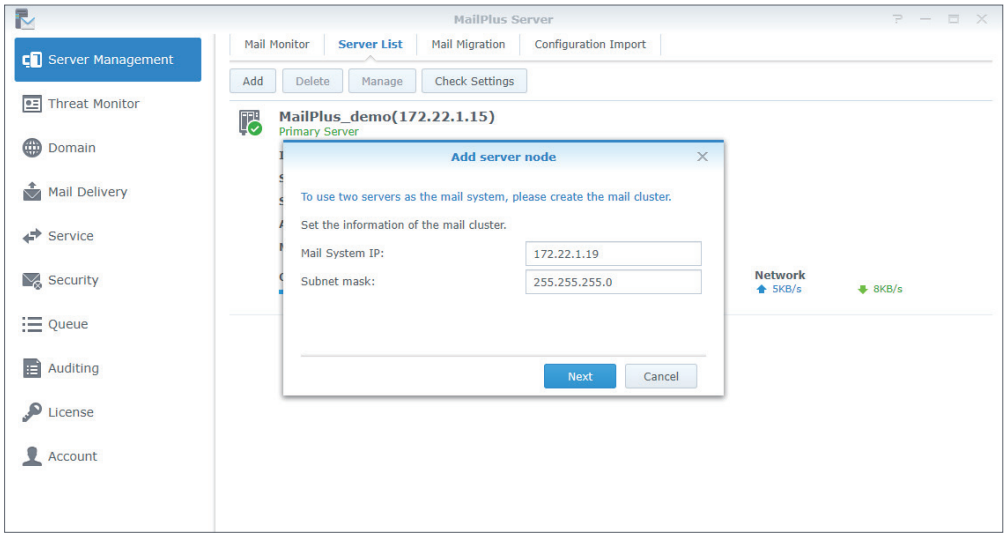
High Availability (HA) konfigurieren

1. Starten Sie MailPlus Server nach der Einrichtung.
2. Gehen Sie zu **Dienst** und überprüfen Sie, ob Sie **Domainbenutzer** oder **LDAP-Benutzer** aus dem Dropdown-Menü **Kontotyp** im Bereich **SMTP** ausgewählt haben.



3. Gehen Sie zu **Server-Management** > **Serverliste** und klicken Sie auf die Schaltfläche **Hinzufügen**.

4. Geben Sie die interne Haupt-IP-Adresse für den HA-Cluster ein und klicken Sie auf **Weiter**.



5. Geben Sie die IP-Adresse des sekundären Servers in das Feld **Serveradresse** ein oder wählen Sie ein Synology NAS zur Verwendung als sekundärer Server aus dem Dropdown-Menü **Serveradresse** aus. Das Synology NAS im selben LAN wird gesucht und in dieses Dropdown-Menü aufgenommen.

Anmerkung:

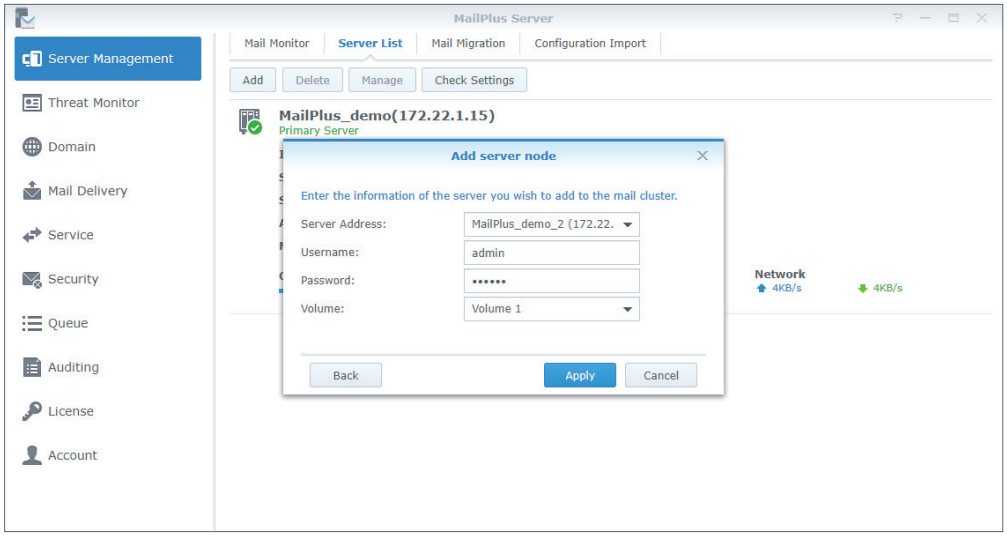
- Sekundäre Server müssen sich mit einer **Netzwerkschnittstelle** verbinden. Sie müssen die IP-Adresse der angebundenen Netzwerkschnittstelle eingeben.

6. Geben Sie die Anmeldedaten eines Kontos der Administratorgruppe auf dem sekundären Server in das Feld **Benutzername** und **Kennwort** ein. Beachten Sie bitte, dass die 2-Stufen-Verifizierung bei der Erstellung des HA-Clusters auf dem sekundären Server vorübergehend deaktiviert werden muss.

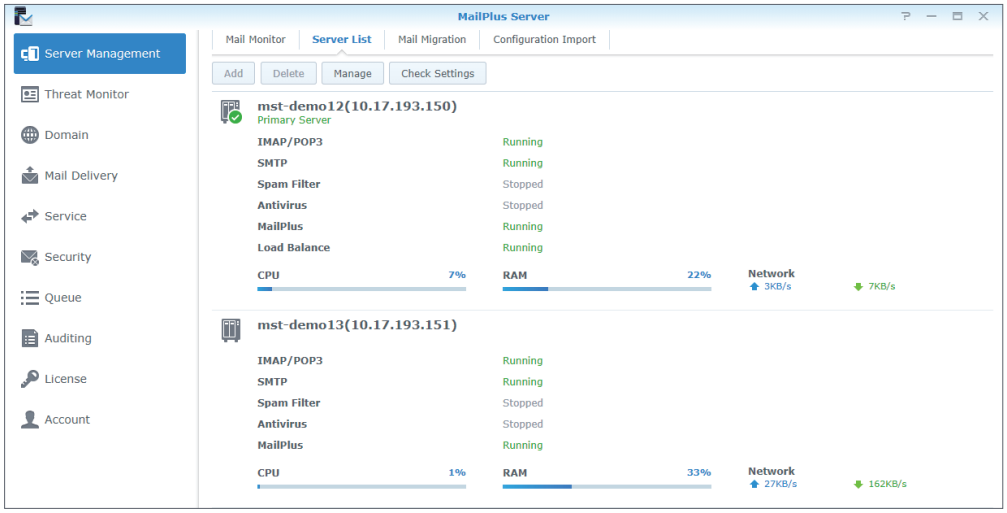
7. Im Dropdown-Menü **Volume** sehen Sie eine Liste der Volumes, die auf dem sekundären Server erstellt wurden. Wählen Sie das Volume aus, dass für die Speicherung der E-Mail-

Daten und der auf MailPlus bezogenen Daten auf dem sekundären Server verwendet wird.

8. Klicken Sie nach Bestätigung der richtigen Einstellungen auf **Übernehmen**.



9. Nachdem Sie die Einstellungen abgeschlossen haben, werden die E-Mails mit dem sekundären Server synchronisiert. Die erforderliche Zeit für die Synchronisierung hängt von der Anzahl der E-Mails ab, die auf dem primären Server gespeichert sind. Während der Synchronisierung können Sie weiterhin E-Mails senden und empfangen. Alle Dienste werden vom primären Server verarbeitet, bis die Synchronisierung abgeschlossen ist. Nachdem die Synchronisierung abgeschlossen ist, teilen sich der primäre und der sekundäre Server die Arbeitslast.



Anmerkung:

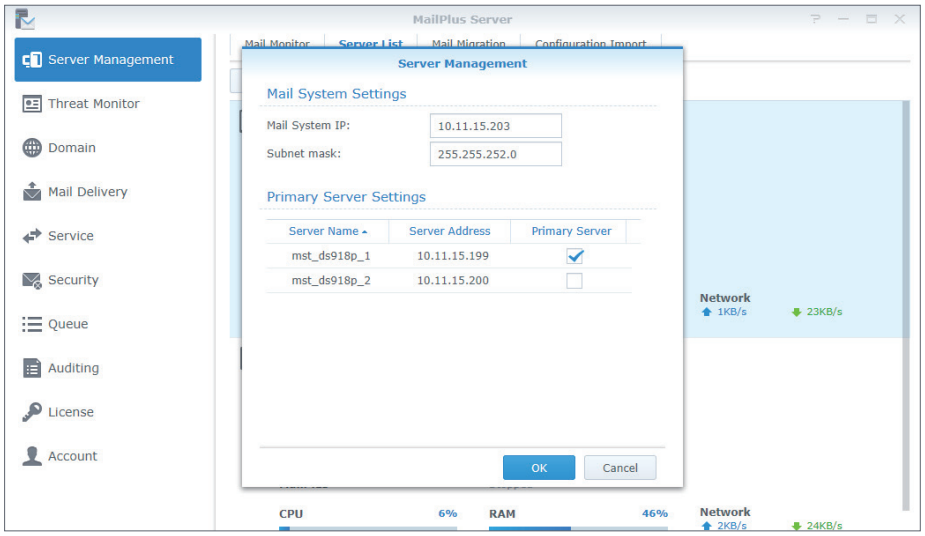
- Während der ersten Synchronisierung sind MailPlus-Dienste zwar verfügbar, aufgrund der hohen Serverauslastung jedoch relativ langsam. Wenn Sie daher MailPlus Server bereits längere Zeit verwendet haben und eine große Anzahl von E-Mails vorhanden ist, wird empfohlen, dass Sie die meisten E-Mails vorab mit **Hyper Backup** auf den sekundären Server kopieren, um die Ladezeit zu verringern und die Synchronisierung zu beschleunigen. Detaillierte Anweisungen über die Verwendung von **Hyper Backup** zur Sicherung von E-Mails finden Sie unter **E-Mails sichern und wiederherstellen**.

Eine High-Availability-(HA)-Cluster-Konfiguration ändern

1. Starten Sie MailPlus Server nach der Einrichtung.
2. Gehen Sie zu **Server-Management** > **Serverliste**.
3. Klicken Sie auf die Schaltfläche **Verwalten**.
4. Im Bereich **E-Mail-Systemeinstellungen** können Sie die Einstellungen der IP-Adresse und Subnetzmaske des HA-Clusters ändern.

> **Anmerkung:**
>
> - Die geänderte IP-Adresse und Subnetzmaske muss sich im selben LAN wie die IP-Adresse des primären und sekundären Servers befinden.

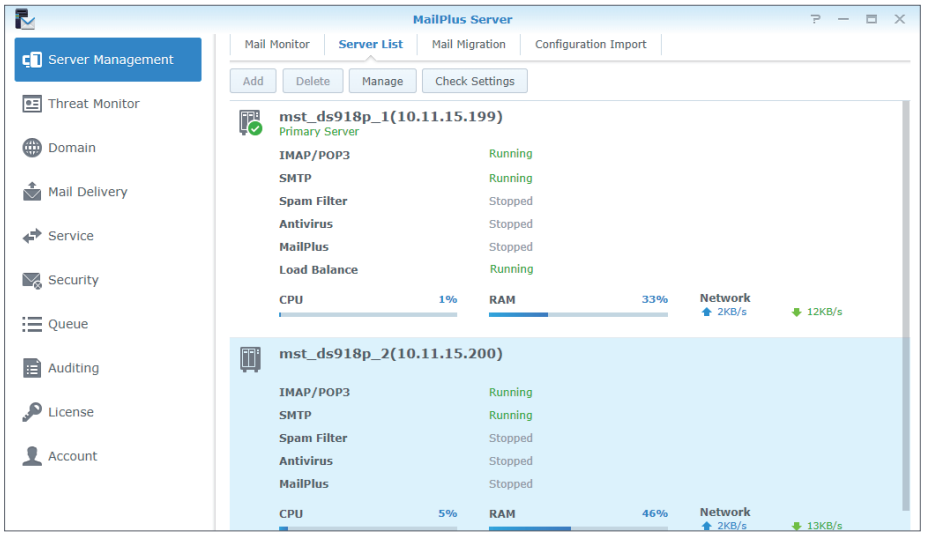
5. Im Bereich **Einstellungen für primären Server** können Sie ein Synology NAS auswählen, der als primärer Server des HA-Clusters fungieren soll. Der primäre Server wird auf der internen IP-Adresse des HA-Clusters ausgeführt und empfängt alle E-Mail-Dienstanforderungen. Diese Anforderungen werden anschließend dem primären oder dem sekundären Server zugewiesen.



Eine High-Availability-(HA)-Cluster-Konfiguration entfernen

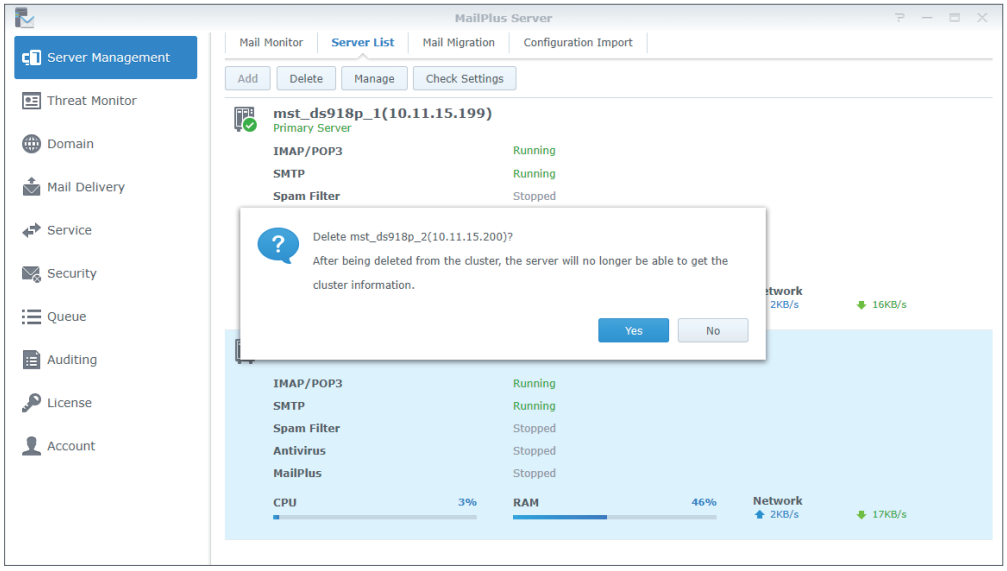
Wenn Sie eine HA-Konfiguration entfernen, werden die E-Mail-Daten mit beiden Synology NAS-Geräten synchronisiert, um die Datenkonsistenz zu gewährleisten. Nach Entfernung der Konfiguration wird die interne IP-Adresse des HA-Clusters von keinem Synology NAS mehr verwendet. Sie müssen eventuell die Portweiterleitungs- und DMZ-Einstellungen („Demilitarized Zone“) Ihrer Firewall anpassen oder die relevanten DNS-Einträge ändern. Gehen Sie bitte wie folgt vor, um eines der Synology NAS aus dem HA-Cluster zu entfernen:

1. Melden Sie sich beim DSM des Synology NAS an, das Sie beibehalten möchten, und starten Sie MailPlus Server.
2. Gehen Sie zu **Server-Management** > **Serverliste**.
3. Wählen Sie das Synology NAS aus, das Sie entfernen möchten.

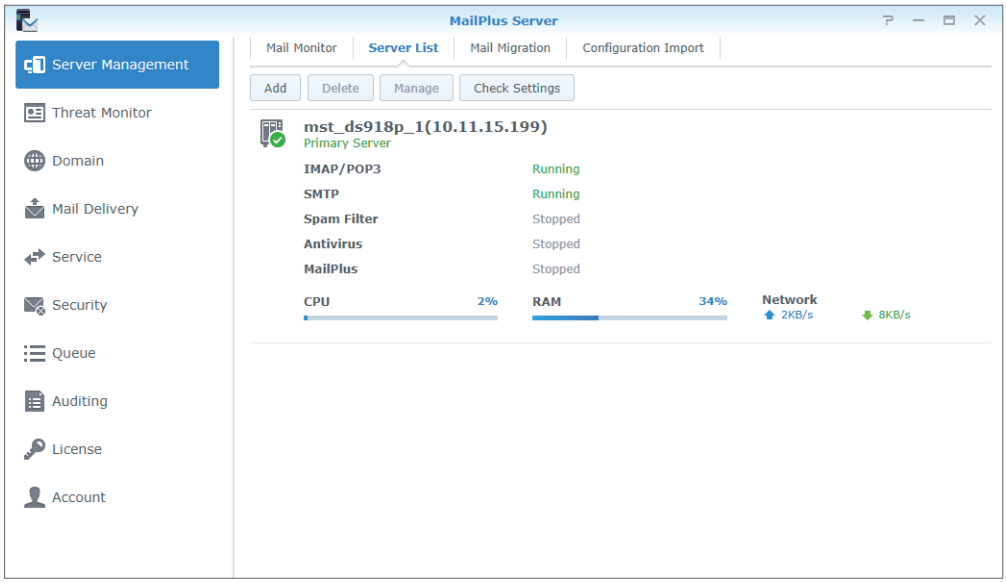


4. Klicken Sie auf die Schaltfläche **Löschen**.

5. Klicken Sie im eingeblendeten Bestätigungsfeld auf **Ja**.



6. Nachdem alle E-Mail synchronisiert wurden, wird der HA-Cluster aufgelöst. Der Server, den Sie beibehalten möchten, empfängt und verarbeitet weiterhin E-Mail-Dienstanforderungen. Überprüfen Sie bitte, ob Sie Portweiterleitungs- oder DMZ-Einstellungen („Demilitarized Zone“) Ihrer Firewall anpassen oder relevante DNS-Einträge ändern müssen.



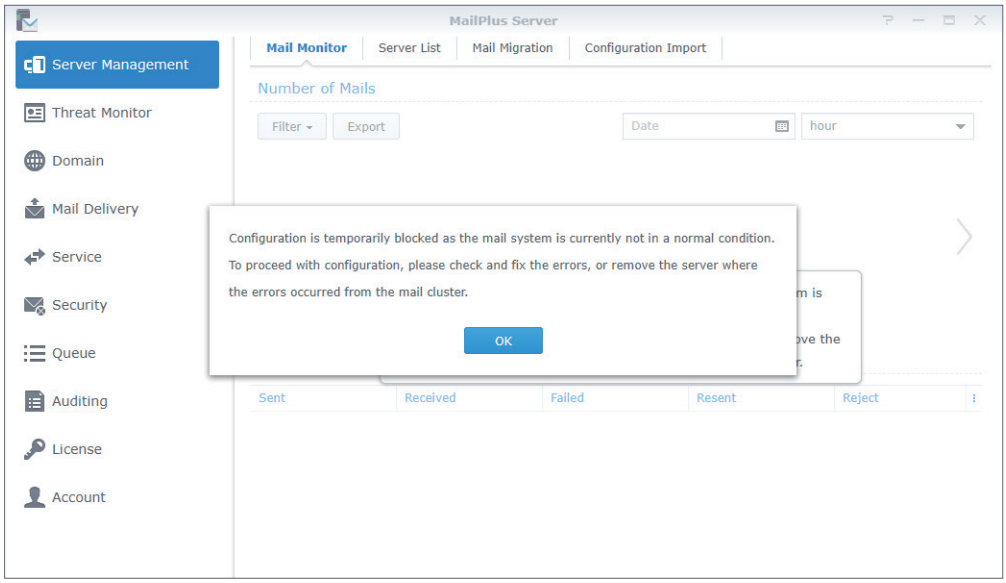
Server-Fehlfunktion

Wenn eines der Synology NAS im HA-Cluster ausfällt, stellt das andere weiterhin E-Mail-Dienste bereit. Die in den nachfolgenden Abschnitten erwähnten primären und sekundären Server beziehen sich auf die ursprünglichen Rollen der Server in der HA-Konfiguration, und nicht auf die Rollen nach einer Übergabe.

Fehlfunktion des primären Servers

Wenn der ursprüngliche primäre Server ausfällt, übernimmt der ursprüngliche sekundäre Server die interne IP-Adresse des HA-Clusters. Er beginnt damit, Dienstanforderungen unabhängig zu empfangen und zu verarbeiten. Wenn Sie MailPlus Server auf dem ursprünglichen sekundären Server starten, wird ein Warnhinweis des E-Mail-Systems eingeblendet und Sie können die Einstellungen von MailPlus Server während der Übergabe nicht anpassen.

Der primäre Server muss zum frühestmöglichen Zeitpunkt wiederhergestellt werden. Wenn der ursprüngliche primäre Server nicht wiederhergestellt werden kann, beachten Sie bitte **Eine High-Availability-(HA)-Konfiguration entfernen**, um ihn zu entfernen. Nach der Entfernung wird MailPlus Server auf einer Einzelknoten-Konfiguration ausgeführt.



Fehlfunktion des sekundären Servers

Wenn der ursprüngliche sekundäre Server ausfällt, übernimmt der ursprüngliche primäre Server die interne IP-Adresse des HA-Clusters und verarbeitet unabhängig alle Dienstanforderungen. Stellen Sie bitte den ursprünglichen sekundären Server zum frühestmöglichen Zeitpunkt wieder her. Wenn der ursprüngliche sekundäre Server nicht wiederhergestellt werden kann, beachten Sie bitte **Eine High-Availability-(HA)-Konfiguration entfernen**, um ihn zu entfernen. Nach der Entfernung wird MailPlus Server auf einer Einzelknoten-Konfiguration ausgeführt.

E-Mails sichern und wiederherstellen

Sie können folgende Datensicherungsfunktionen in DSM nutzen, um MailPlus Server zu sichern. Die Sicherungsfunktion von MailPlus Server beinhaltet Folgendes:

- **Sicherung der Systemkonfiguration**
- **Sicherung von Postfach und E-Mails**

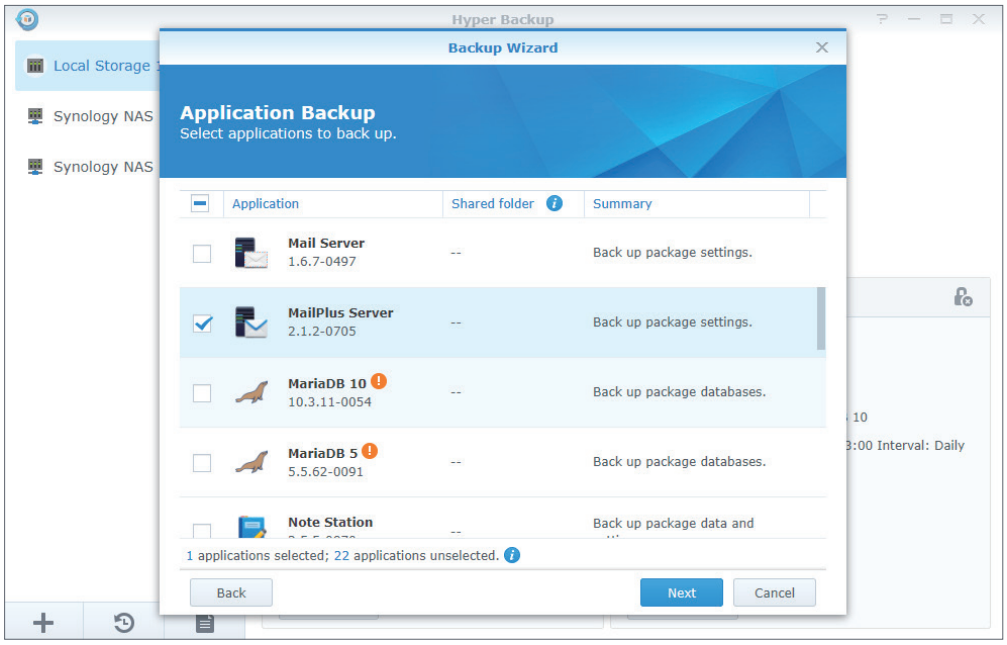
In den Systemeinstellungen von MailPlus Server kommen Änderungen seltener vor; daher können Sie **Hyper Backup** zur Ausführung von geplanten Sicherungsaufgaben verwenden. Postfächer und E-Mail-Nachrichten ändern sich im E-Mail-System jedoch laufend und erfordern daher eine Sicherung in Echtzeit. Es wird daher empfohlen, dass Sie die **Synchronisierung freigegebener Ordner** zur Sicherung von Postfächern und E-Mail-Nachrichten nutzen, um Datenverluste zu vermeiden, wenn lediglich die geplante Datensicherung ausgeführt wird.

Sicherung der Systemkonfiguration

Sichern Sie die E-Mail-Systemkonfiguration mit Hyper Backup auf einem mit MailPlus kompatiblen Synology NAS.

1. Starten Sie **Hyper Backup** auf dem Quell-Synology NAS.

2. Klicken Sie auf das Plus-Symbol (+) unten links, um eine neue Datensicherungsaufgabe zu erstellen.
3. Wählen Sie einen Typ des Datensicherungsziels aus:
   - **Lokaler Ordner und USB**: Mit dieser Option werden Daten auf einem lokalen Synology NAS oder auf einem externen USB/SD-Speichergerät gesichert.
   - **Remote-NAS-Gerät**: Hyper Backup Vault muss vorher auf dem Remote-Ziel installiert und gestartet sein.
4. Legen Sie die Aufgabeneinstellungen fest. Weitere Informationen zur Erstellung von Sicherungsaufgaben finden Sie in **diesem Hilfe-Artikel**.
5. Wählen Sie **MailPlus Server** aus, wenn das System Sie auffordert, eine zu sichernde Anwendung auszuwählen.



6. Nachdem die Einstellungen der Sicherungsaufgabe abgeschlossen sind, ist das System bereit, die folgenden Einstellungen von MailPlus Server (auf der linken Seite der Benutzeroberfläche von MailPlus Server) zu sichern:
   - **Domain**
   - **Mailübermittlung**
   - **Dienst**
   - **Sicherheit**
   - **Überprüfung**
   - **Lizenz**
   - **Konto**

Sicherung von Postfach und E-Mails

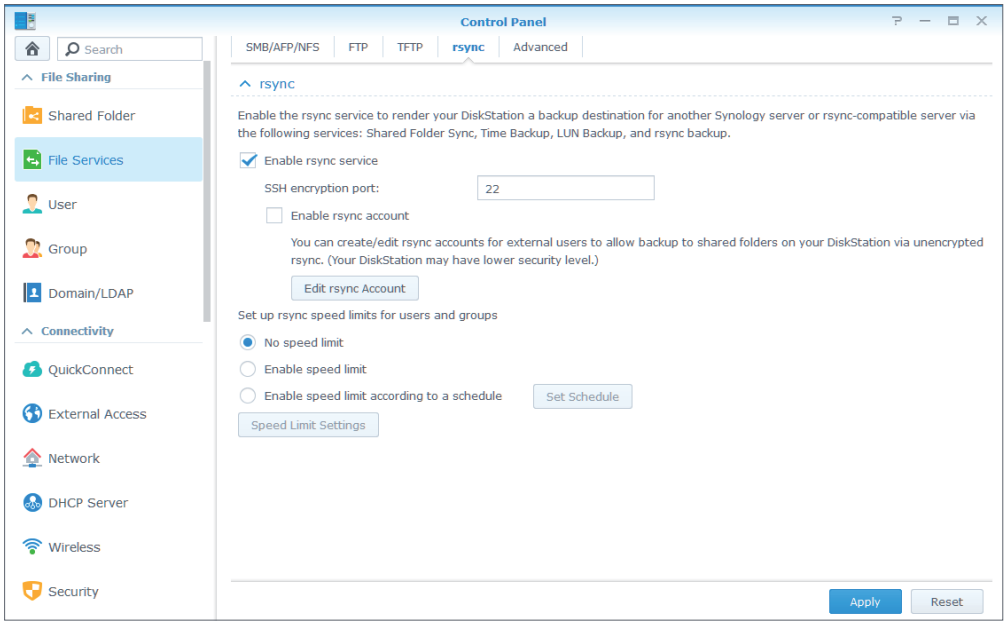
Beachten Sie bitte die folgenden Abschnitte, um das gesamte Postfach sowie E-Mail-Nachrichten mit Synchronisierungsaufgaben auf einem mit MailPlus kompatiblen Synology

NAS zu sichern:

Synchronisierung freigegebener Ordner aktivieren

Sie müssen die **Synchronisierung freigegebener Ordner** auf dem Ziel-Synology NAS aktivieren.

1. Melden Sie sich bei DSM an.
2. Gehen Sie zu **Systemsteuerung** > **Dateidienste** > **rsync**.
3. Markieren Sie das Kontrollkästchen **rsync-Dienst aktivieren**, um die **Synchronisierung freigegebener Ordner** zu aktivieren.



4. Klicken Sie auf **Übernehmen**.

Synchronisierungsaufgabe erstellen

Melden Sie sich beim Synology NAS an und gehen Sie wie folgt vor, um eine Synchronisierungsaufgabe zu erstellen:

1. Gehen Sie zu **Systemsteuerung** > **Synchronisierung freigegebener Ordner** und klicken Sie auf die Schaltfläche **Aufgabenliste**.
2. Klicken Sie im Fenster **Aufgabenliste** auf die Schaltfläche **Erstellen**.
3. Geben Sie einen Aufgabennamen in das Feld **Aufgabenname** ein.
4. Wählen Sie einen freigegebenen Ordner zur Synchronisierung aus.
5. Geben Sie die Details des Ziel-Synology NAS und die folgenden Synchronisierungseinstellungen ein:
   - **SSH-Verschlüsselungsport für verschlüsselte Synchronisierung freigegebener Ordner anpassen**: Verwendet Ihren gewünschten Verschlüsselungsport für die Verschlüsselung der SSH-Übertragung.
   - **SSH-Übertragungsverschlüsselung aktivieren**: Verschlüsselt die Daten während

der Übertragung. Diese Option bietet mehr Sicherheit, während die unverschlüsselte Übertragung leistungsfähiger ist.

- **Übertragungskomprimierung aktivieren**: Komprimiert die Daten während der Übertragung. Diese Option verringert die Bandbreitennutzung, führt jedoch zu einer höheren CPU-Auslastung.
- **Synchronisierung in Blöcken aktivieren**: Synchronisiert lediglich geänderte Segmente anstatt einer gesamten Datei. Diese Option verringert die Bandbreitennutzung, führt jedoch zu einer höheren CPU-Auslastung.

6. Wenn Sie dazu aufgefordert werden, können Sie eine der nachstehenden Optionen auswählen, um festzulegen, wann von der Quelle zum Ziel synchronisiert wird:
   - **Synchronisierung der Änderung ausführen**: Synchronisiert sofort nach vorgenommenen Änderungen am freigegebenen Quellordner.
   - **Synchronisierung manuell ausführen**: Synchronisiert nur dann vom freigegebenen Quellordner, wenn Sie auf die Schaltfläche klicken.
   - **Erweiterter Zeitplan**: Synchronisiert basierend auf Ihrem festgelegten Zeitplan. Klicken Sie auf **Zeitplan planen**, um anzugeben, wann die Synchronisierungsaufgabe durchzuführen ist.
7. Klicken Sie auf **Übernehmen**. Sie sehen jetzt die Synchronisierungsaufgabe in der Aufgabenliste. Das System führt Aufgaben automatisch nach dem angegebenen Zeitplan aus.

Synchronisierungsaufgaben verwalten

Melden Sie sich beim Quell-Synology NAS an und gehen Sie wie folgt vor, um Synchronisierungsaufgaben zu verwalten:

1. Gehen Sie zu **Systemsteuerung** > **Synchronisierung freigegebener Ordner** und klicken Sie auf die Schaltfläche **Aufgabenliste**.
2. Wählen Sie eine Aufgabe im Fenster **Aufgabenliste** aus, um wie folgt vorzugehen:
   - Klicken Sie auf **Bearbeiten**, um Aufgaben zu bearbeiten.
   - Klicken Sie auf **Löschen**, um Aufgaben zu löschen.
   - Wenn eine Synchronisierungsaufgabe nicht gerade läuft, klicken Sie auf die Schaltfläche **Jetzt synchronisieren**, um die Aufgabe umgehend durchzuführen.
   - Wenn eine Synchronisierungsaufgabe läuft, klicken Sie auf die Schaltfläche **Abbrechen**, um die laufende Aufgabe zu stoppen.
   - Wenn Sie Synchronisierungsaufgaben erstmalig ausführen, führt die **Synchronisierung freigegebener Ordner** eine **Vollständige Synchronisierung** aus. Nach Abschluss der ersten Synchronisierungsaufgabe werden nur geänderte Elemente synchronisiert. Sie

können auf **Vollständige Synchronisierung** klicken, um alle Daten erneut manuell zu synchronisieren.

Anmerkung:

- Wenn der Zeitplan einer Synchronisierungsaufgabe auf **Synchronisierung der Änderung ausführen** gesetzt ist, kann die laufende Synchronisierungsaufgabe durch Klicken auf **Abbrechen** gestoppt werden. Wenn dagegen Änderungen an einem oder mehreren in der Synchronisierungsaufgabe enthaltenen, freigegebenen Ordnern vorgenommen werden, wird die Aufgabe von der Funktion „Synchronisierung freigegebener Ordner" fortgesetzt.
- Sie sollten Synology Drive, Cloud Station Server und Cloud Sync nicht zur Ausführung der Datensicherung nutzen, da ihre Zwei-Wege-Synchronisierung Daten beschädigten könnte.
- Wenn der freigegebene Ordner **MailPlus** bereits im Ziel vorhanden ist, wird der Ordner auf **MailPlus_1** umbenannt, nachdem die Sicherung abgeschlossen ist.
- Wenn Sie Daten von **MailPlus_1** nutzen möchten, verschieben Sie diese bitte manuell zum freigegebenen Ordner **MailPlus**.
- Um Kontofehler zu vermeiden, verbinden Sie das Ziel mit demselben Verzeichnisserver wie der Server, der für die Quelle (z. B. LDAP-Server oder Windows Active Directory-Domain) verwendet wird.

Systemkonfiguration, Postfach und E-Mails wiederherstellen

Die Systemkonfiguration, Postfächer und E-Mails werden im lokalen freigegebenen Ordner auf dem Ziel-Synology NAS gespeichert. Gehen Sie bitte wie folgt vor, um Systemkonfiguration, Postfächer und E-Mails wiederherzustellen:

1. Starten Sie **Hyper Backup**.
2. Stellen Sie die gesicherte Konfiguration aus dem lokalen freigegebenen Ordner wieder her. Weitere Informationen finden Sie in **diesem Hilfe-Artikel**.
3. Nach der Wiederherstellung wird die aktuelle Konfiguration von MailPlus Server überschrieben.
4. Die gesicherten Postfächer und E-Mails müssen nicht wiederhergestellt werden. Sie können sofort verwendet werden.

Anmerkung:

- Die Funktion „Datensicherung und Wiederherstellung" ist derzeit mit MailPlus Server 1.0-164 (und höher) kompatibel, der auf DSM 6.0 (und höher) ausgeführt wird.

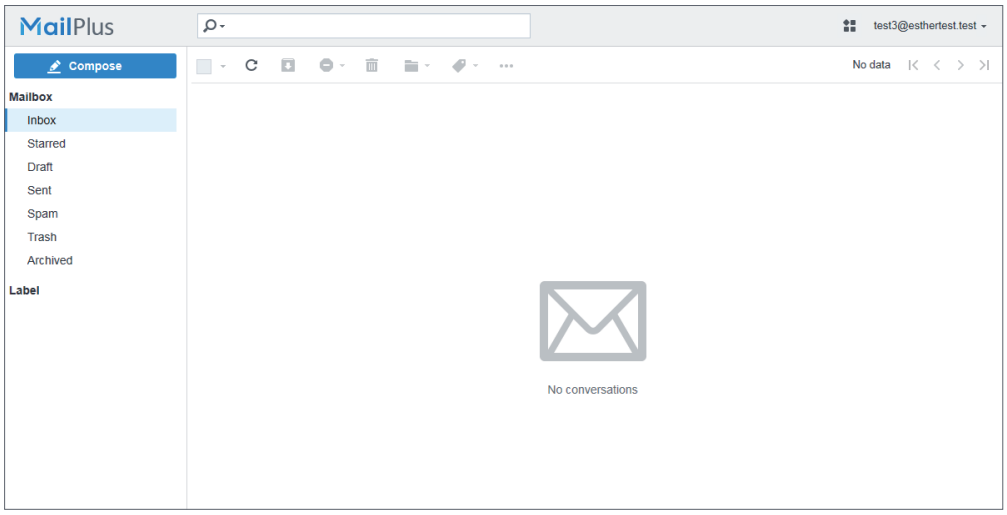
MailPlus bietet Client-Benutzern einen benutzerfreundlichen Webmail-Dienst für das Anzeigen, Verwalten und Senden von E-Mails. Detailinformationen zur Einrichtung von MailPlus finden Sie im Abschnitt **MailPlus Client einrichten**.

Dieser Abschnitt führt Sie durch die Konfiguration und Bedienerführung von MailPlus. Detaillierte Anweisungen finden Sie in **den Hilfe-Artikeln**.

Kapitel 12: MailPlus-Bedienerführung

Grundlegende Bedienung

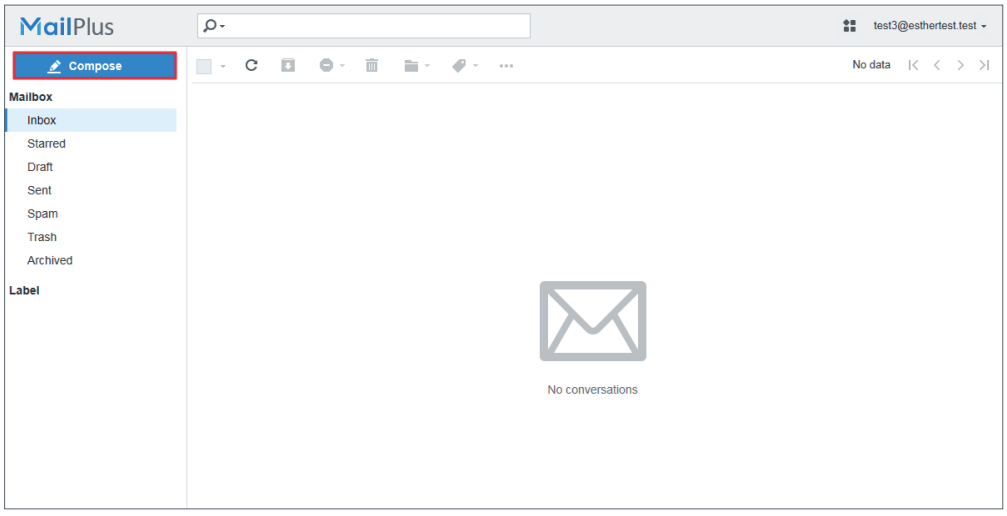
Standardmäßig wird nach der Anmeldung Ihr **Postfach** angezeigt.



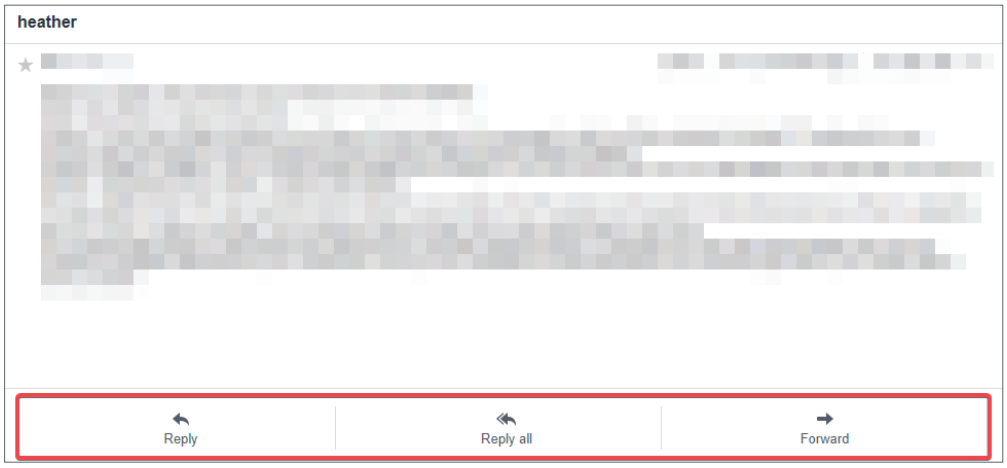
E-Mails öffnen und verwalten

Im **Postfach** können Sie Folgendes tun:

- **E-Mail verfassen**: Klicken Sie oben links auf die Schaltfläche **Verfassen**, um mit dem Entwurf einer E-Mail zu beginnen. MailPlus speichert E-Mail-Entwürfe automatisch. Sie können das Fenster **Verfassen** jederzeit schließen und über das Feld **Entwurf** erneut öffnen, um fortzusetzen.



- **Auf E-Mail antworten**: Es gibt drei Möglichkeiten, eine E-Mail in MailPlus zu beantworten:
  - **Antworten**: Klicken Sie auf **Antworten**, um dem Absender zu antworten.
  - **Allen antworten**: Klicken Sie auf **Allen antworten**, um allen Empfängern (einschließlich CC-Empfängern) gleichzeitig zu antworten.
  - **Weiterleiten**: Klicken Sie auf **Weiterleiten**, wenn Sie eine E-Mail an jemand anderen als die ursprünglichen Empfänger senden möchten.



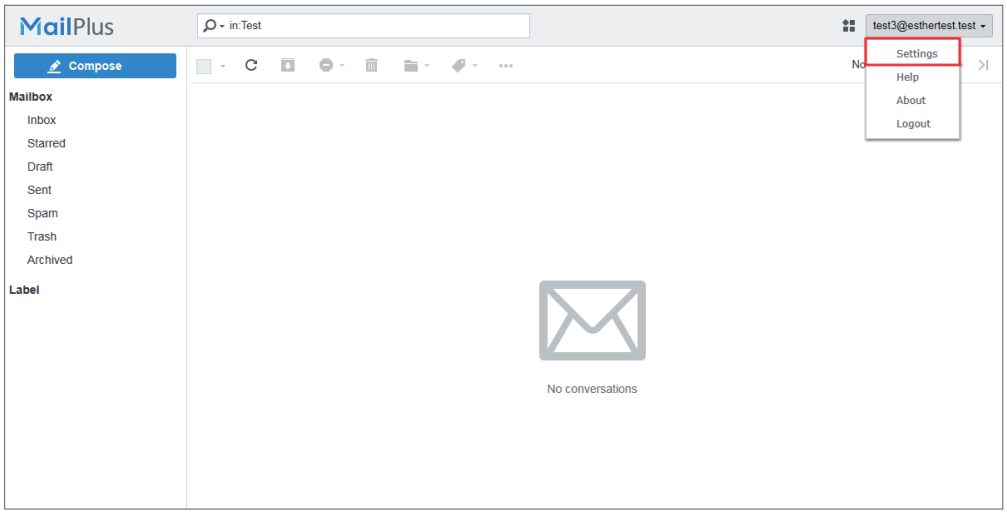
- **E-Mails nach Postfach organisieren**: Sie können je nach Bedarf mehrere Postfächer erstellen. Bewegen Sie den Cursor oben links über **Postfach**, und Sie sehen gleich daneben ein Plussymbol (+). Klicken Sie auf das Plus-Symbol (+), um ein neues Postfach hinzuzufügen.
- **E-Mails nach Kennzeichnung verwalten**: Sie können Kennzeichnungen individuell anpassen, um Ihre E-Mails zu kategorisieren. Bewegen Sie den Cursor im linken Bereich über **Kennzeichnung**, und Sie sehen gleich daneben ein Plussymbol (+). Klicken Sie auf das Plus-Symbol (+), um eine neue Kennzeichnung hinzuzufügen. Geben Sie einen Namen ein und wählen Sie eine Kennzeichnungsfarbe zur leichteren Erkennung aus.

Erweiterte Einstellungen

Mit MailPlus können Client-Benutzer ihr Webmail-Layout anpassen, Nachrichten automatisch beantworten/weiterleiten, Postfach-Einstellungen vornehmen und sogar Protokolle (z. B. SMTP und OpenPGP) für die Mailübermittlung anpassen. MailPlus-Administratoren können in Synology MailPlus Server allgemeine Einstellungen für alle Benutzer verwalten. **Kontakte** und zugehörige Einstellungen finden Sie im App Launcher.

In diesem Kapitel erläutern wir die Konfiguration von **SMTP**, **OpenPGP** und **Blacklist/ Whitelist**. Wenn Sie detaillierte Anweisungen zu anderen Einstellungen benötigen, beachten Sie bitte **diesen Hilfe-Artikel**.

Klicken Sie oben rechts auf Ihren Kontonamen und anschließend im Dropdown-Menü auf **Einstellungen**, um mit der Konfiguration von MailPlus zu beginnen.



Zusätzliche SMTP-Server hinzufügen

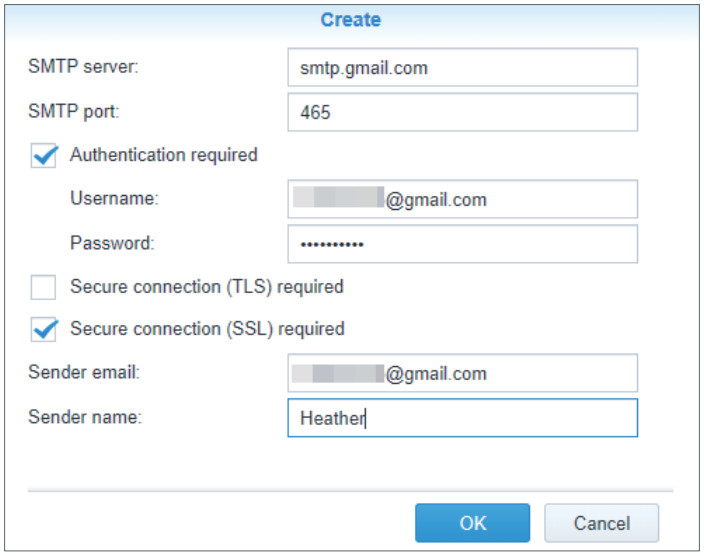
MailPlus unterstützt mehrere SMTP-Server für die Mailübermittlung. Wenn keine zusätzlichen SMTP-Server hinzugefügt werden, wird MailPlus Server automatisch als standardmäßiger SMTP-Server für die Zustellung aller E-Mails eingerichtet. Es können nur Einstellungen für **Absendername** bearbeitet werden.

Es können auch weitere SMTP-Server hinzugefügt werden, an die E-Mails von MailPlus gesendet werden können. Beispiel: Sie können den SMTP-Server von Google hinzufügen, um E-Mails über Ihr Google-Konto in MailPlus zu versenden. Gehen Sie zum Hinzufügen eines SMTP-Servers wie folgt vor:

1. Gehen Sie zu **Einstellungen** > **SMTP**.
2. Geben Sie die folgenden Daten ein:
   - **SMTP-Server**: Suchen Sie den SMTP-Server in den Hilfe-Artikeln oder Anleitungen Ihres E-Mail-Anbieters.
   - **SMTP-Port**: Die Portnummer wird automatisch auf den für SMTP-Verbindungen über SSL/TLS benötigten Wert aktualisiert. Standardmäßig wird Port 465 für SMTP-Verbindungen über SSL verwendet und Port 587 für SMTP-Verbindungen über TLS. Wenn Sie bei SSL und TLS keine Häkchen setzen, wird Port 25 als Standardport für SMTP-Verbindungen verwendet.
   - **Authentifizierung erforderlich**: Setzen Sie ein Häkchen, wenn der SMTP-Server eine Authentifizierung erfordert.
     - **Benutzername**: Geben Sie Ihre E-Mail-Adresse ein.
     - **Kennwort**: Geben Sie Ihr E-Mail-Kennwort ein.
   - **Sichere Verbindung (TLS) erforderlich**: Setzen Sie ein Häkchen, um Verbindungen mit TLS-Zertifikaten zu sichern.
   - **Sichere Verbindung (SSL) erforderlich.**: Setzen Sie ein Häkchen, um Verbindungen mit SSL-Zertifikaten zu sichern.
   - **E-Mail-Absender**: Geben Sie Ihre E-Mail-Adresse ein. Beachten Sie bitte: Wenn diese

Adresse nicht mit der unter **Benutzername** eingegebenen E-Mail-Adresse übereinstimmt, können Ihre E-Mails als Spam markiert werden.

- **Absendername**: Geben Sie einen Absendernamen (auch als Bezeichnung „von“ bekannt) ein , anhand dessen die Empfänger Sie erkennen können.



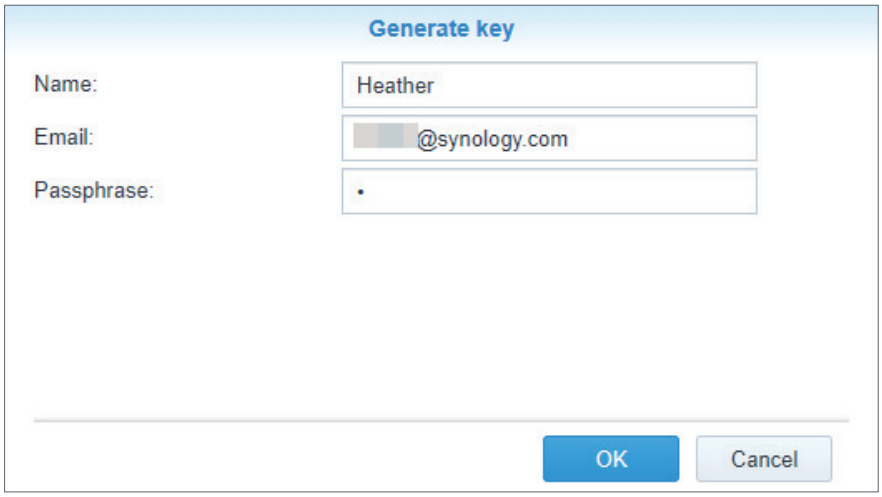
3. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
4. Nun sollten Sie das neu hinzugefügte SMTP-Serverkonto auf der Liste sehen.
   - Sie können auf die Schaltflächen in der oberen Symbolleiste klicken, um den Server zu bearbeiten, zu löschen oder als standardmäßigen SMTP-Server festzulegen.
   - Beim Verfassen einer E-Mail können Sie zwischen SMTP-Servern im Feld **Von:** wechseln.

E-Mails per OpenPGP verschlüsseln

OpenPGP (Pretty Good Privacy) ist eine schlüsselbasierte Verschlüsselungstechnologie für E-Mails. OpenPGP verschlüsselt E-Mails, sodass nur vorgesehene Empfänger auf deren Inhalt zugreifen können. Auf diese Weise können sensible E-Mail-Nachrichten und übertragene Daten wirksam vor Angriffen auf die Privatsphäre geschützt werden.

OpenPGP-Schlüssel erstellen

1. Setzen Sie ein Häkchen bei **OpenPGP aktivieren** und klicken Sie auf **Schlüsselverwaltung**.
2. Klicken Sie auf **Erstellen**, um ein neues OpenPGP-Schlüsselpaar zu erstellen.
   - **Name**: Geben Sie den gewünschten Namen ein.
   - **E-Mail**: Geben Sie Ihr MailPlus-Konto ein.
   - **Passphrase**: Geben Sie eine Passphrase ein, die zum Verschlüsseln und Entschlüsseln Ihres privaten Schlüssels verwendet wird.



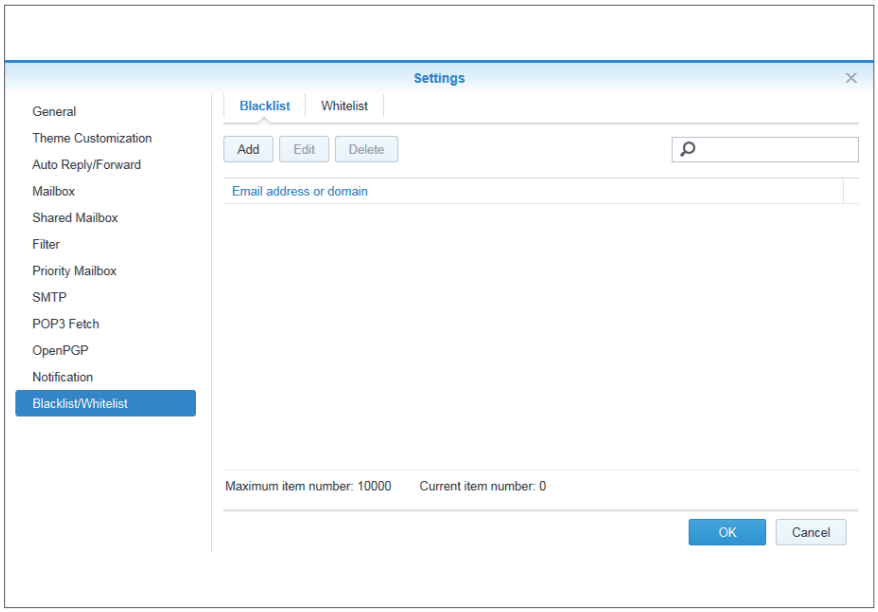
3. Klicken Sie auf **OK**, um ein Paar aus öffentlichem und privatem Schlüssel zu erstellen.

OpenPGP-Schlüssel verwalten

- **Öffentlicher Schlüssel**: Klicken Sie auf **Exportieren**, um den öffentlichen Schlüssel zu exportieren und Absendern zu übergeben, die E-Mails an Sie verschlüsseln sollen.
- **Privater Schlüssel**: Geben Sie den privaten Schlüssel nicht weiter, denn er dient dazu, an Sie gesendete Nachrichten zu entschlüsseln.
- Wenn Sie verschlüsselte E-Mails an andere senden müssen, klicken Sie bitte auf **Importieren**, um deren öffentlichen Schlüssel aus einer Datei oder Texteingabe zu importieren.

Blacklist/Whitelist verwalten

Auf der Seite **Blacklist/Whitelist** können Sie eine eigene Blacklist und Whitelist erstellen, um bestimmte E-Mail-Adressen oder Domains zu blockieren oder zuzulassen. Sie können E-Mail-Adressen oder Domains, die Spam versenden, zur **Blacklist** hinzufügen und so blockieren. Wenn Sie umgekehrt feststellen, dass legitime E-Mails blockiert werden, können Sie die E-Mail-Adressen oder Domainnamen der Absender zur **Whitelist** hinzufügen und zulassen.



E-Mail-Adresse oder Domainnamen hinzufügen

1. Klicken Sie für einen neuen Eintrag in der Blacklist/Whitelist auf **Hinzufügen**.
2. Geben Sie die E-Mail-Adresse oder Domain an und klicken Sie auf **OK**, um die Einstellungen zu speichern.
3. Die neu hinzugefügte E-Mail-Adresse oder Domain sollte nun in der Liste aufscheinen.

E-Mail-Adresse oder Domainnamen löschen

1. Klicken Sie auf die gewünschte E-Mail-Adresse oder Domain und auf **Löschen**.
2. Klicken Sie zur Bestätigung auf **Ja** oder auf **Nein**, um die Änderungen zu verwerfen.

Vorhandene E-Mail-Adressen oder Domainnamen bearbeiten

1. Klicken Sie auf die gewünschte E-Mail-Adresse oder Domain und auf **Bearbeiten**.
2. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.
3. Die E-Mail-Adresse oder Domain wurde aus Ihrer Liste entfernt.

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

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

SYNOLOGY UK LTD.
Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL
Vereinigtes Königreich
Tel.: +44 (0)1908048029

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

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

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

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

Synology®

synology.com