Synology®

# 관리자 가이드

# Synology MailPlus Server

사용 제품

**Synology MailPlus Server 2.2**

# 목차

# 소개

Synology MailPlus 제품군은 가용성이 우수한 고급 보안 메일 서비스입니다 . 이 제품군은 MailPlus Server 및 MailPlus 등 두 가지 패키지로 구성되어 있습니다 . MailPlus Server 는 다양한 설정을 제공하는 관리 콘솔이며 MailPlus 는 클라이언트 사용자의 이메일 플랫폼입니다 .

이 관리자 가이드는 MailPlus Server 설정 과정을 설명하고 DNS 설정 , 메일 서비스 마이그레이션 및 기타 보안 조정 등 상세한 구성 지침을 제공합니다 . 또한 이 가이드에서는 유용하게 사용할 수 있도록 안정적이고 지속적인 메일 서비스에 필요한 MailPlus high-availability, 지연된 메시지 관리에 사용되는 메일 대기열 및 MailPlus 상태 개요를 표시하는 모니터링 콘솔과 같은 주요 기능도 설명합니다 .

# 1 장 : 배포 지침

이 장은 메일 서비스의 안정성과 성능을 보장하기 위해 MailPlus 를 배포할 때 준수해야 하는 모범 사례에 대한 안내입니다 . MailPlus 에 적합한 Synology NAS 선택 방법 , RAM 및 저장소 요구 사항 예측 방법 , SSD 캐시를 사용할 때 고려해야 할 사항 , 동일한 NAS 에서 MailPlus 와 함께 여러 I/O 집약적 패키지를 실행하는 방법을 설명합니다 .

## Synology NAS 선택

Synology 는 폼 팩터 , 기능 및 용량이 다양한 NAS 를 제공합니다 . 일부 제품은 MailPlus Server 에 적합하지 않습니다 . 사용자 요구 사항을 충족하는 Synology NAS 를 선택하는 데 도움을 받으려면 아래를 참조하십시오 .

1. 최대 동시 사용자 수와 최대 서버 성능을 기준으로 정렬된 **MailPlus 라이센스 페이지**에서 지원되는 장치 목록을 확인합니다 .
   - **최대 동시 사용자 수**는 권장 최대 MailPlus 사용자 수를 나타냅니다 .
   - **최대 서버 성능**은 MailPlus Server 가 하루에 처리할 수 있는 최대 이메일 수를 나타냅니다 .
2. **Synology 제품 페이지**를 참조하여 MailPlus 를 지원하는 모든 모델의 목록을 확인하십시오 . 원하는 모델을 클릭하면 자세한 사양을 확인할 수 있습니다 .

**참고 :**

- 수치는 Synology 내부에서 진행한 실험실 테스트를 기준으로 합니다 . 테스트 환경은 다음과 같습니다 .
  - 최대 동시 사용자 수 테스트 시 CPU 사용량과 RAM 사용량 모두 80% 이하였습니다 .
  - 확장 가능한 메모리로 테스트한 모델에는 RAM 을 최대 용량으로 설치했습니다 .
  - 베이 2 개와 이중 M.2 드라이브 슬롯이 장착된 모델에는 SSD 캐시용 SSD 가 2 개 설치되었습니다 .
  - 베이가 5 개 이상 장착된 모델에는 SSD 캐시용 SSD 가 2 개 설치되었습니다 .
  - FS 시리즈에는 SSD 12 개가 RAID F1 구성으로 설치되었습니다 .
  - 두 서버 간 데이터 동기화로 인해 high-availability 모드에서 메일 시스템 성능이 약간 감소합니다 .
  - 위 모든 테스트에서 활성화된 기능에는 스팸 방지 , 안티 바이러스 , DNSBL, 그레이리스트 , 콘텐츠 검사 , 전체 텍스트 검색 ( 영어만 ) 등이 있습니다 .
- 실제 제한 사항은 시스템 구성에 따라 다를 수 있습니다 . 동일한 성능을 얻으려면 SSD 를 설치하고 RAM 을 확장하는 것이 좋습니다 .

# RAM 및 저장소 요구 사항 예측

NAS 의 메모리 사용량에 영향을 미치는 여러 가지 요인을 기준으로 사용자 수에 따른 권장 메모리 크기는 다음과 같습니다 .

- 사용자 250 명 미만 : 최소 8GB RAM
- 사용자 250~500 명 : 최소 16GB RAM
- 사용자 500~1000 명 : 최소 32 GB RAM
- 사용자 1,000 명 초과 : 최소 64GB RAM

## RAM 사용량 예측

사용되는 메모리 양은 주로 메일 서비스 사용자 수에 따라 다릅니다 . 그러나 다음 서비스도 메모리를 많이 사용할 수 있다는 점에 유의하십시오 .

- **스팸 방지** : 기본 MailPlus 스팸 방지 엔진인 Rspamd 는 메모리를 많이 사용할 수 있습니다 .
- **안티 바이러스** : ClamAV 및 McAfee 와 같은 안티 바이러스 서비스는 특히 오프라인 바이러스 데이터베이스를 최신 버전으로 업데이트할 때 메모리를 많이 사용할 수 있습니다 .
- **MailPlus 웹 클라이언트** : MailPlus Server 는 이메일을 읽고 이메일 초안을 저장할 때 웹 클라이언트로부터 여러 요청을 동시에 수신할 수 있습니다 . 사용자 수가 Synology NAS 모델 사양에서 지정된 **최대 동시 사용자 수**를 초과할 경우 MailPlus Server 가 모든 클라이언트 요청을 처리하려고 할 때 메모리 사용량이 갑자기 급증할 수 있습니다 .

## 볼륨 크기 요구 사항 예측

다음 공식을 사용하여 MailPlus 의 저장소 크기 요구 사항을 예측합니다 .

- 예상 저장소 크기 = [( 일일 평균 수신 및 발신 이메일 수 )*( 평균 이메일 크기 )*( 사용자 수 )*( 일 수 )]

평균 이메일 크기는 300KB 이고 , 한 사람이 보내고 받는 평균 이메일 수는 하루에 100 개이며 , 메일 서비스는 보통 3~5 년 간 지속됩니다 .

예를 들어 MailPlus 에서 사용자 200 명을 지원하는 경우 필요한 저장소 크기는 다음과 같습니다 .

100( 일일 평균 수신 및 발신 이메일 수 )*300KB( 평균 이메일 크기 )*200( 사용자 수 )*1095(3 년 내 일 수 ) = 6.12TB

필요한 저장소 크기를 예측하는 데 문제가 있으면 **당사에 연락**하여 고객 지원을 요청하십시오 .

## SSD 캐시 활용

SSD 캐시는 자주 액세스하는 데이터 ( 핫 데이터라고도 함 ) 를 SSD 의 일부 또는 전체에 임시로 저장하여 시스템 성능을 향상시키는 방법입니다 .

MailPlus 는 종종 메시지를 읽고 쓰는 데 관여하며 , 이 경우 저용량 파일을 임의로 읽고 드라이브에 기록해야 합니다 . 평균 이메일 크기는 상대적으로 작으므로 이메일 ( 또는 일부 ) 이 SSD 캐시에 저장되면 읽기 / 쓰기 속도가 증가할 수 있습니다 . SSD 를 추가로 설치하고 Synology SSD 캐시를 활용하면 전반적인 메일 서비스 성능이 향상됩니다 .

**참고 :**

- 기업 사용자는 최고의 성능을 얻으려면 SSD 캐시를 활용해야 합니다 .
- 최적의 성능을 위해 FS 시리즈 NAS 를 사용하고 모든 SSD 로 볼륨을 만드는 것이 좋습니다 .

### 권장 SSD 캐시 크기

SSD 는 다양한 용도로 설계되며 시스템에서 사용하는 데 적합한 SSD 를 선택할 경우 내구성 , 일관된 성능 및 정전 보호 기능 등을 고려해야 합니다 .

Synology SSD 는 무중단 NAS 환경을 위해 제작되었으며 엄격한 유효성 검사를 통해 Synology 시스템과 상호 운용할 수 있는지가 검증된 엔터프라이즈급 SSD 입니다 . I/O 스트레스 , 전원 사이클 및 온도 시험이 포함된 집중 테스트는 Synology SSD 가 기업 환경에 적합한 안정성과 일관된 성능을 모두 제공할 수 있는지 , 특히 메일 서버와 같은 중요한 작업에 적합한지를 보장합니다 .

Synology 는 Synology SSD 외에도 다른 여러 **타사 SSD** 를 테스트하고 검증했습니다 . 제조업체에 따라 SSD 성능이 크게 달라질 수 있습니다 .

SSD 캐시에 적합한 SSD 를 선택하는 방법에 대한 자세한 내용은 **이 문서**를 참조하십시오 .

### 권장 SSD 캐시 크기

실제 SSD 캐시 크기는 볼륨의 핫 데이터 양에 따라 다릅니다 . 읽기 - 쓰기 캐시를 사용할 수 있도록 RAID 1/5/6/10 중복 드라이브를 형성하는 데 SSD 가 최소 두 개 이상 필요합니다 . 예를 들어 480GB 읽기 - 쓰기 캐시를 만들려면 480GB SSD 가 최소 두 개 이상 필요합니다 .

핫 데이터는 SSD 내에서 캐시됩니다 . MailPlus Server 의 경우 핫 데이터는 주로 자주 액세스할 가능성이 높은 최근에 액세스한 이메일로 구성됩니다 . 핫 데이터는 일반적으로 메일 서비스에 사용되는 총 저장소 공간의 3~6% 를 차지합니다 .

- 예를 들어 1TB 메일 저장소 공간의 핫 데이터 크기는 다음과 같습니다 . 1,024GB*6% = 61.4GB

그러나 성능을 보장하기 위해 SSD 캐시 용량은 실제 핫 데이터 크기보다 더 커야 합니다 . 실제 SSD 캐시 크기를 예상 핫 데이터 크기의 두 배로 설정하는 것이 좋습니다 .

- 위 예의 경우 적합한 캐시 크기는 다음과 같습니다 . 61.4GB*2 = 122.8GB.

이 경우 480GB SSD 캐시는 최소 요구 사항 이상을 충족합니다 .

다음 안내를 통해 사용자 수에 따라 SSD 캐시 크기를 빠르게 예측할 수 있습니다 .

- 사용자 500 명 미만 : 480GB*2
- 사용자 500~1,000 명 : 1 TB*2
- 사용자 1,000 명 초과 : 2 TB*2

Synology NAS 가 이미 있으면 **저장소 관리자**에서 **SSD 캐시 어드바이저**를 사용하여 핫 데이터 크기와 적절한 캐시 크기를 결정할 수 있습니다 .

**참고 :**

- SSD 캐시에 대한 자세한 내용은 다음 문서를 참조하십시오 .
  - **SSD 캐시 도움말 문서**
  - **Synology SSD 캐시 사용에 대한 질문과 대답**
  - **백서 : Synology SSD 기술을 사용하여 시스템 성능 향상**
- MailPlus 사용자 수가 모델 사양에서 지정된 **최대 동시 사용자 수**에 도달하지 않더라도 SSD 캐시를 이메일 처리 속도를 향상시키는 방법으로 사용하는 것이 좋습니다 .

## 같은 NAS 에서 여러 I/O 집약적 패키지 실행

성능 및 데이터 보안을 강화하기 위해 MailPlus Server, Synology Drive Server 및 Synology Chat Server 와 같은 I/O 집약적 패키지를 같은 Synology NAS 에 설치하지 않는 것이 좋습니다 . 위 모든 패키지가 I/O 리소스를 많이 사용합니다 . 즉 , 여러 가지 서비스가 리소스를 경쟁적으로 사용하므로 시스템 오류가 쉽게 발생할 수 있습니다 . 그러나 패키지가 모든 I/O 집약적 서비스가 아니면 Synology NAS 는 여러 서비스를 동시에 실행할 수 있습니다 . 예를 들어 MailPlus Server 와 Synology Drive 를 같은 NAS 에 설치해서는 안 되지만 Synology Calendar 는 I/O 집약적인 서비스가 아니므로 MailPlus 와 함께 실행할 수 있습니다 .

# 2 장 : MailPlus Server 시작하기

MailPlus Server 를 사용하면 Synology NAS 에서 SMTP, POP3 및 IMAP 를 지원하는 메일 시스템 역할을 수행할 수 있습니다 . 사용자 계정과 이메일 메시지를 중앙에서 관리하고 Synology NAS 에 보관할 수 있습니다 . 클라이언트 패키지인 MailPlus 는 메시지를 보고 , 관리하고 , 전송할 수 있도록 사용이 간편한 브라우저 기반 이메일 플랫폼을 메일 서비스 사용자에게 제공합니다 .

이 장은 MailPlus Server 와 MailPlus 를 시작하는 데 유용한 내용을 설명합니다 .

## Synology NAS 를 인터넷에 연결

Synology NAS 를 인터넷에 연결하는 방법에는 직접 연결 , PPPoE 연결 또는 라우터를 통한 연결 등 세 가지 방법이 있습니다 . 인터넷을 통해 Synology NAS 에 액세스하는 방법에 대한 자세한 내용은 **이 자습서**를 참조하십시오 .

외부 고정 IP 주소를 보유하는 것은 메일 시스템에 있어 중요합니다 . 동적 IP 주소를 사용하여 메일 시스템을 실행할 수 있지만 고정 IP 주소를 사용하는 것이 더욱 안정적입니다 . 메일 시스템용 외부 고정 IP 주소를 등록하는 것이 좋습니다 . 자세한 내용은 해당 인터넷 서비스 공급자 (ISP) 에게 문의하십시오 .

### 고정 IP/PPPoE 구성

Synology NAS 에서 외부 고정 IP 주소를 설정하는 방법에는 두 가지가 있습니다 .

- **PPPoE**: 일부 인터넷 서비스 공급자 (ISP) 는 무료로 고정 IP 주소를 제공하지만 사용자는 고정 IP 주소를 검색하려면 PPPoE 를 통해 연결해야 합니다 .
    1. DSM 에 로그인합니다 .
    2. **제어판** > **네트워크**로 이동합니다 .
    3. **네트워크 인터페이스** 탭에서 **PPPoE** 를 선택하고 **편집** 버튼을 클릭합니다 .
    4. 모뎀 및 네트워크 포트를 설정합니다 .
    5. 인터넷 서비스 공급자 (ISP) 에서 제공한 사용자 이름과 패스워드를 입력합니다 .
- **고정 IP 주소** : 고정 IP 주소가 이미 있으면 Synology NAS 에 입력하면 됩니다 .
    1. DSM 에 로그인합니다 .
    2. **제어판** > **네트워크**로 이동합니다 .
    3. **네트워크 인터페이스** 탭에서 네트워크 포트를 선택하고 **편집** 버튼을 클릭합니다 .
    4. 고정 IP 주소를 입력합니다 .

# DNS 설정

클라이언트가 인터넷을 통해 이메일을 MailPlus Server 에 배달하도록 하려면 등록된 유효한 도메인 이름이 필요합니다 . 이메일 주소는 두 부분으로 구성됩니다 . @ 의 앞부분은 사용자 이름이고 @ 의 뒷부분은 도메인 이름을 나타냅니다 . 예를 들어 Alex 의 이메일 주소는 "alex@example.com" 입니다 . 도메인 이름은 "example.com" 입니다 . "alex@example.com" 과 같은 이메일 주소가 작동하는지 확인하려면 이메일이 MailPlus Server 에 도달할 수 있도록 MX 레코드와 A 레코드를 설정해야 합니다 . 도메인 공급자의 DNS 서버에서 이러한 레코드를 구성할 수 있습니다 .

## MX 레코드

MX 레코드 (Mail Exchanger 레코드 ) 는 인터넷에서 SMTP(Simple Mail Transfer Protocol) 를 사용하여 이메일을 라우팅하는 방법을 지정합니다 . 각 MX 레코드에는 호스트 이름과 기본 설정이 포함되어 있습니다 . 호스트 이름은 이메일이 올바른 메일 서버에 도착하도록 안내합니다 . 기본 설정은 여러 서버의 우선순위를 나타냅니다 . 기본 설정 번호가 낮을수록 우선 순위가 높습니다 .

메일 서버가 여러 개 있는 도메인 하나에 MX 레코드를 여러 개 설정하고 각 레코드에 기본 설정 번호를 할당할 수 있습니다 . 이 메일 서버가 처음 요청에 응답하게 하려면 기본 서버의 숫자가 가장 낮아야 합니다 ( 예 : 0). 기본 서버에서 응답이 없으면 인터넷은 다른 메일 서버 중 하나에서 응답할 때까지 기본 설정 번호에 따라 순차적으로 다른 메일 서버를 대체 작동에 사용하려고 합니다 .

예를 들어 이메일 주소가 **alex@example.com** 이면 메일 서버를 가리키는 MX 레코드를 설정해야 합니다 . 그러면 메일 서버가 도메인 **example.com** 대신 이메일을 수신합니다 . 따라서 **호스트** 필드에 편집 중인 도메인을 , **대상** 필드에 MailPlus Server 의 호스트 이름을 입력해야 합니다 . 기본 서버에 할당한 기본 설정 레코드는 0 이거나 0 과 가까워야 합니다 .

| 호스트 | 대상 | 기본 설정 |
|---|---|---|
| example.com | mail.example.com | 0 |

이렇게 하면 **example.com** 의 MX 조회에서 **mail.example.com** 을 반환합니다 .

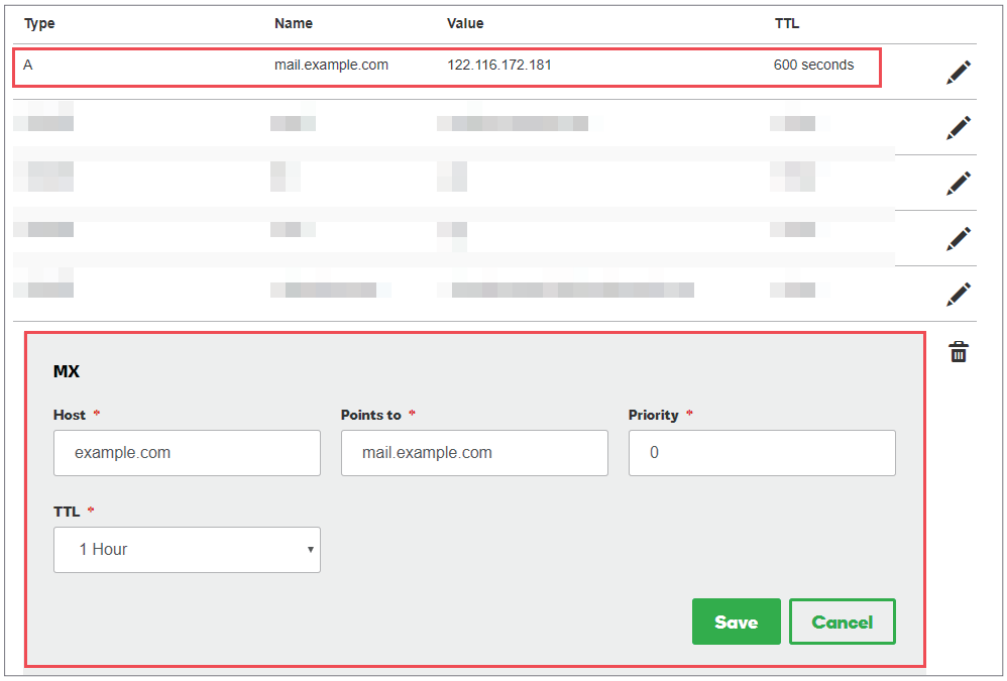
MX 조회에서 메일 서버를 찾으면 인터넷에는 메일 배달 대상을 찾는 데 IP 주소가 필요합니다 . 따라서 메일 서버의 A 레코드를 설정해야 합니다 .

## A 레코드

A 레코드 (Address 레코드 ) 는 도메인 또는 하위 도메인을 호스트 서버의 IP 주소로 가리킵니다 . 이 레코드를 통해 인터넷은 사람들이 기억하기 쉬운 도메인 이름을 사용할 경우 IP 주소를 식별할 수 있습니다 .

**alex@example.com** 의 경우 **mail.example.com** 은 **example.com** 의 하위 도메인이고 호스트 서버는 MailPlus Server 가 실행 중인 Synology NAS 입니다 .

| 호스트 이름에서 | IP 주소로 |
|---|---|
| mail.example.com | 111.116.172.181 |




예와 이미지는 설명용입니다 . 각 공급자가 제공하는 DNS 레코드 인터페이스는 다를 수 있습니다 . DNS 레코드를 구성하는 데 문제가 있으면 도메인 공급자에 문의하십시오 .

## 역방향 DNS 설정

특정 DNS 레코드를 도메인 이름에 할당하는 프로세스를 **정방향 DNS** 라고 하며 도메인 이름을 정확한 서버로 연결합니다 . **역방향 DNS** 라고 하는 역방향 프로세스도 있습니다 .

### 역방향 DNS 란 ?

역방향 DNS 는 웹사이트의 숫자 주소 ( 즉 , IP 주소 ) 를 도메인 / 호스트 이름으로 변환하는 것을 말하며 도메인이나 호스트 이름을 IP 주소로 변환하는 정방향 DNS 프로세스와 반대 개념입니다 . 또한 역방향 DNS 는 지정한 IP 주소에 속하는 도메인 이름 / 호스트를 찾는 것을 의미합니다 . 이러한 점으로 인해 이 프로세스를 종종 **역방향 DNS 조회**라고 합니다 . 도메인 이름에 유효한 역방향 DNS 가 있으면 IP 주소를 통해 액세스할 수 있습니다 .

### 역방향 DNS 역할

역방향 DNS 는 메일 시스템의 기본 요구 사항 중 하나입니다 . 역방향 DNS 는 주로 수신되는 메시지의 IP 주소가 인증된 도메인 이름과 일치하는지 여부를 확인하고 그렇지 않으면 메시지를 차단하는 스팸 필터로 사용됩니다 . 메일 서버에 역방향 DNS 를 설정하지 않으면 메일 서버에서 보낸 메시지는 대부분의 주요 이메일 메일 공급자에 의해 차단됩니다 . 역방향 DNS 를 직접 설정할 수 없고 계속해서 메일 배달 문제가 발생하면 메일 배달에 다른 SMTP 서버를 추가하십시오 . 이메일을 보낼 때 이메일이 스패머로 처리되지 않도록 하려면 잘 알려진 SMTP 서버를 사용하는 것이 좋습니다 .

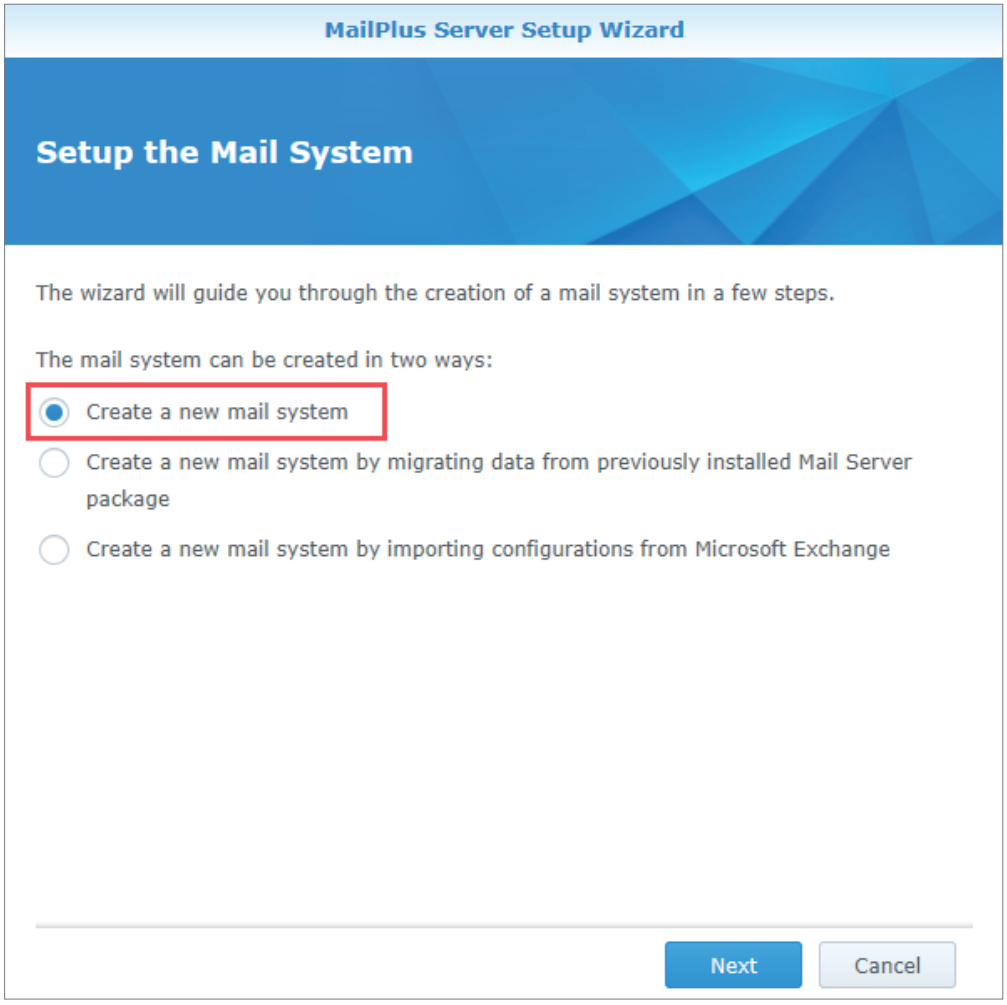
**역방향 DNS 설정 방법**

- **자체 호스트에 역방향 DNS 설정** : 일부 ISP 는 사용자가 자체 역방향 DNS 를 호스팅할 수 있도록 사용자에게 영역 일부를 위임할 수 있습니다 . DNS 서버에서 PTR 레코드를 확인하여 역방향 DNS 를 구성할 수 있습니다 . PTR 레코드는 IP 주소를 제어하는 엔터티에서 관리됩니다 . 호스트가 IP 주소 한 개 또는 여러 개가 포함된 IP 공간에 대한 역방향 DNS 를 사용자에게 위임한 경우 엔터티는 사용자 호스트 또는 사용자 자체일 수 있습니다 . 일반적으로 PTR 레코드는 뒤에서 입력된 in-addr.arpa 항목 앞의 IP 를 나타냅니다 .
- **ISP 를 통해 역방향 DNS 설정** : ISP 또는 IP 주소를 소유하고 있는 엔터티만 적절한 PTR 레코드를 추가할 수 있습니다 . 역방향 DNS 를 구성하려면 ISP 나 엔터티에 문의해야 할 수도 있습니다 .

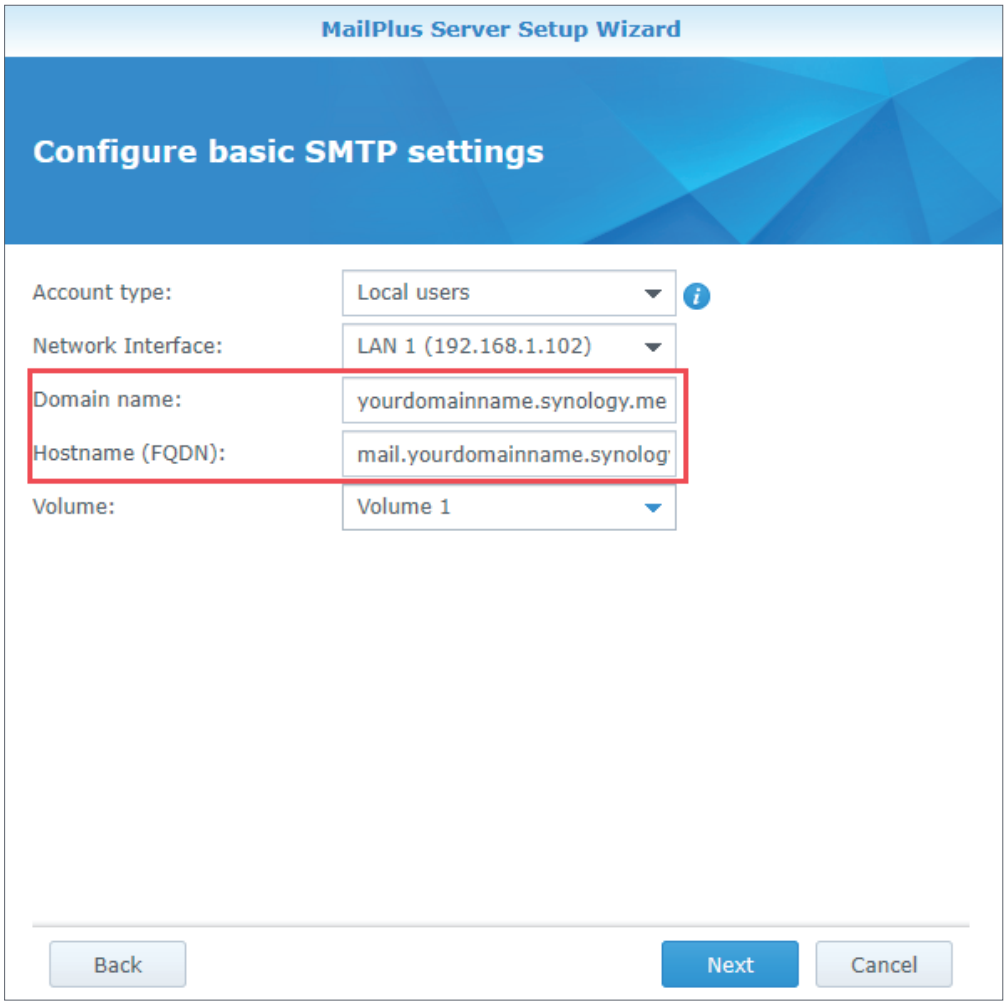
# MailPlus Server 설정

설치가 완료되면 MailPlus Server 설정을 시작할 수 있습니다 . 다음 섹션에서는 기본 SMTP(Simple Mail Transfer Protocol) 설정을 구성하는 방법을 설명합니다 . 다음 스크린샷은 참고용입니다 . 설정은 다를 수 있습니다 .

1. **패키지 센터**로 이동하여 **MailPlus Server** 를 설치합니다 .
2. **MailPlus Server** 를 실행하고 완전히 새로운 메일 시스템을 설정하려면 **새 메일 시스템 생성**을 선택한 후 **다음**을 클릭하여 계속 설정합니다 . 그렇지 않으면 **이전에 설치한 Mail Server 에서 데이터를 마이그레이션하여 새 메일 시스템을 생성합니다**를 선택하면 됩니다 . Mail Server 를 MailPlus Server 로 마이그레이션하는 방법은 **이 자습서**를 참조하십시오 .




3. 도메인 이름과 호스트 이름 (FQDN) 을 입력합니다 .
   - **도메인 이름** : 도메인 이름은 이메일 메시지를 수신하는 위치나 주소입니다 . 도메인 이름이 DNS 설정의 MX 레코드와 일치하는지 확인하십시오 .
   - **호스트 이름 (FQDN)**: 호스트 이름은 MailPlus Server 주소입니다 . 호스트 이름이 DNS 설정의 A 레코드와 일치하는지 확인하십시오 .




4. 필요에 맞게 다음 설정을 수정합니다 .
   - **계정 유형** : MailPlus 서비스를 사용할 수 있는 사용자 계정 유형 ( 로컬 , LDAP 또는 도메인 사용자 ) 을 선택합니다 .
   - **네트워크 인터페이스** : MailPlus Server 에 사용할 LAN 포트를 선택합니다 .
   - **볼륨** : MailPlus Server 와 데이터를 저장할 볼륨을 선택합니다 .
5. **다음**을 클릭하여 설정 요약을 확인하고 **적용**을 클릭하여 설정을 마칩니다 .
6. MailPlus Server 를 설정한 후 **계정을 활성화**하면 특정 사용자가 메일 서비스를 사용할 수 있습니다 . 사용자 계정을 6 개 이상 활성화하려면 라이센스를 추가로 구매해야 합니다 . MailPlus 라이센스 메커니즘에 대한 자세한 내용은 **MailPlus 라이센스 페이지**를 참조하십시오 .

**참고 :**

- 기본적으로 MailPlus Server 의 응용 프로그램 권한은 모든 사용자에게 부여됩니다 . **제어판**에서 권한 설정을 편집하면 MailPlus Server 기능이 영향을 받을 수 있으므로 편집하면 안 됩니다 . 자세한 내용은 **계정 활성화**를 참조하십시오 .
- MailPlus Server 를 설정하면 **MailPlus** 공유 폴더가 자동으로 Synology NAS 에 추가됩니다 . 클라이언트 사용자가 MailPlus 에 액세스할 수 있게 하려면 공유 폴더의 권한 설정을 기본값으로 유지해야 합니다 . 권한을 직접 편집하지 않는 것이 좋습니다 .

# MailPlus 클라이언트 설정

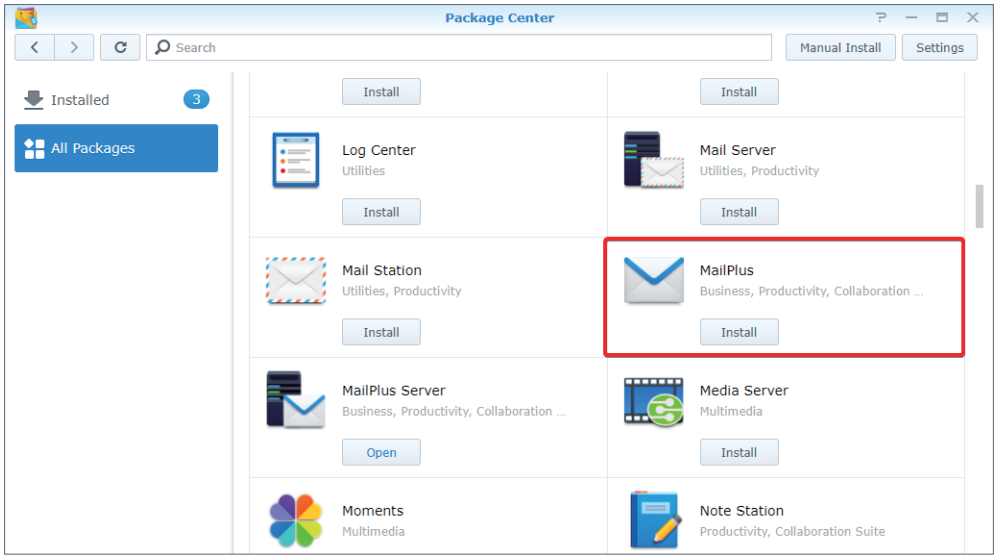
## MailPlus 를 사용하여 Synology NAS 에서 이메일 액세스

MailPlus 는 Synology NAS 에서 호스팅되는 이메일을 액세스 및 관리하는 클라이언트 사용자에게 웹 기반 인터페이스를 제공하는 애드온 패키지입니다 .

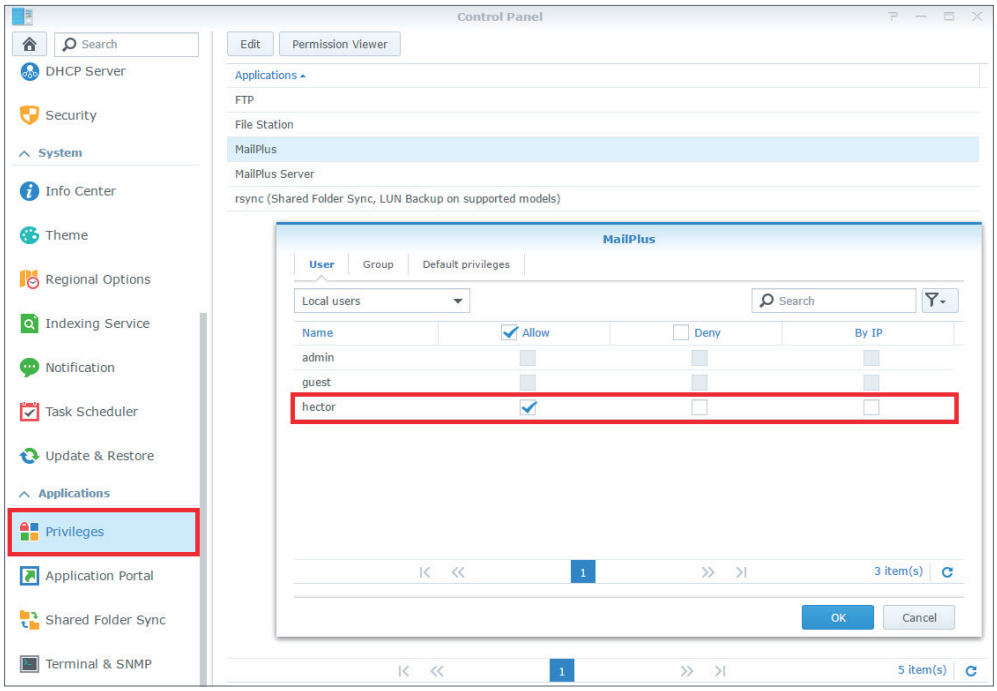
MailPlus 에서 POP3 계정 여러 개를 만들면 사용자가 다른 이메일 서비스 공급자 ( 예 : Mozilla® Thunderbird®, Gmail 및 Office 365) 를 통해 메시지를 가져올 수 있습니다 .

## MailPlus 설치

1. **패키지 센터**로 이동하여 **MailPlus** 를 설치합니다 .



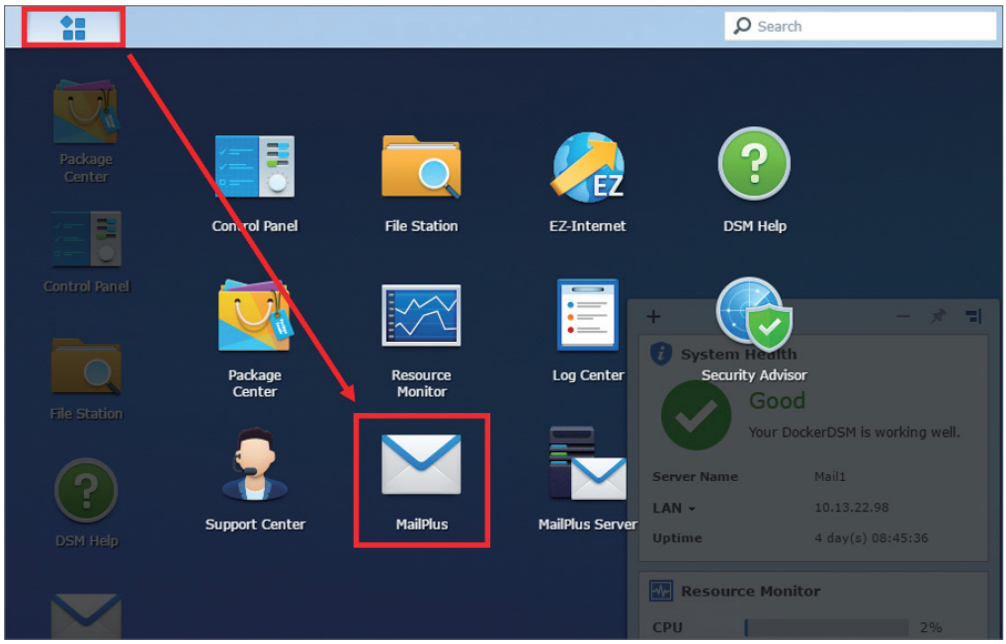

2. **제어판** > **권한**으로 이동하여 대상 사용자나 그룹이 **MailPlus** 에 액세스하도록 허용합니다 .



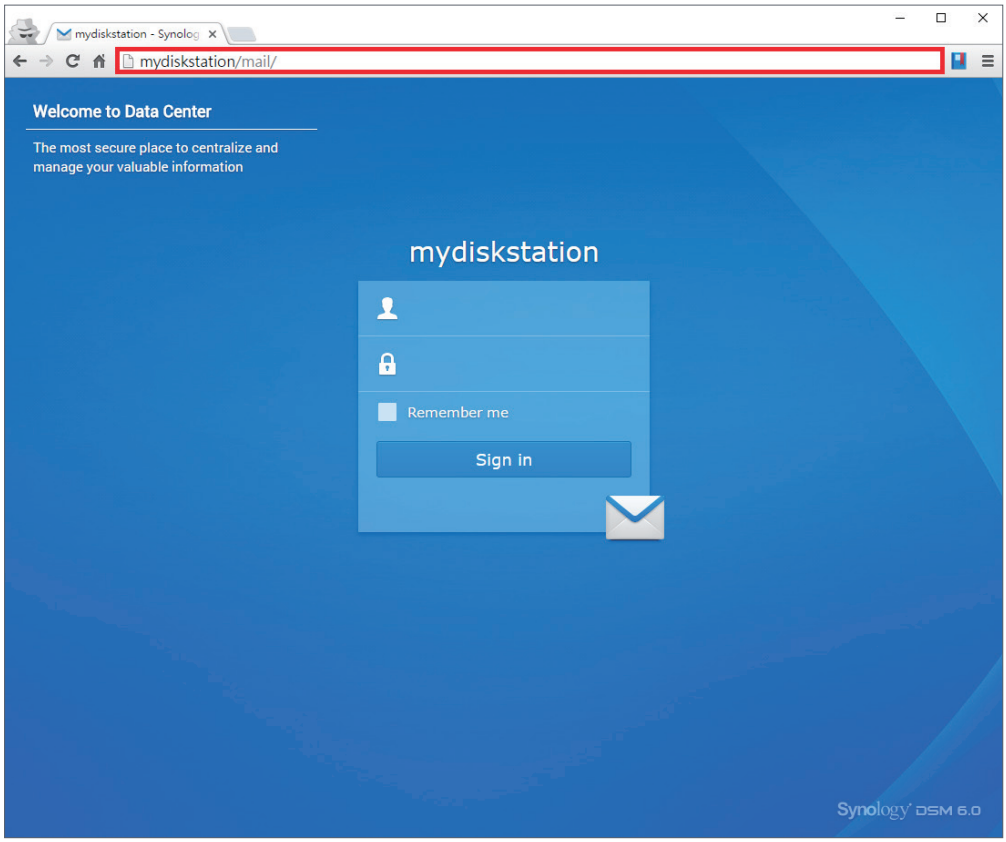
# MailPlus 실행

1. MailPlus 로그인 페이지를 실행하는 방법에는 두 가지가 있습니다 .

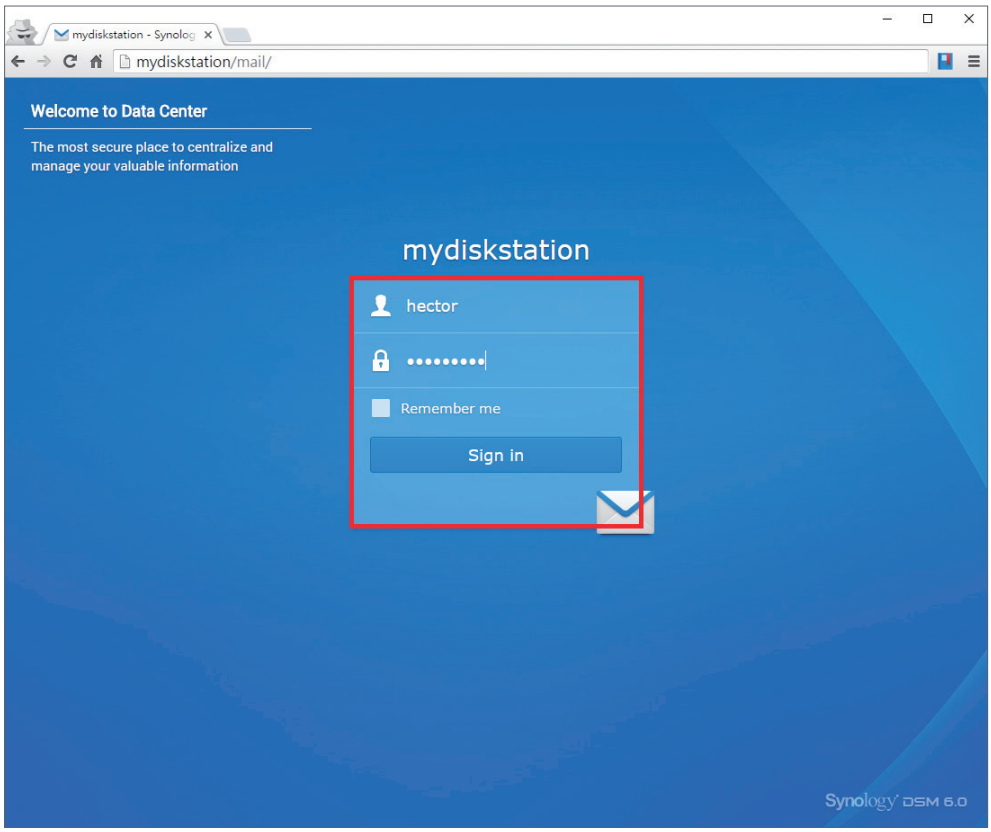
   - **메인 메뉴** > **MailPlus** 로 이동합니다 .



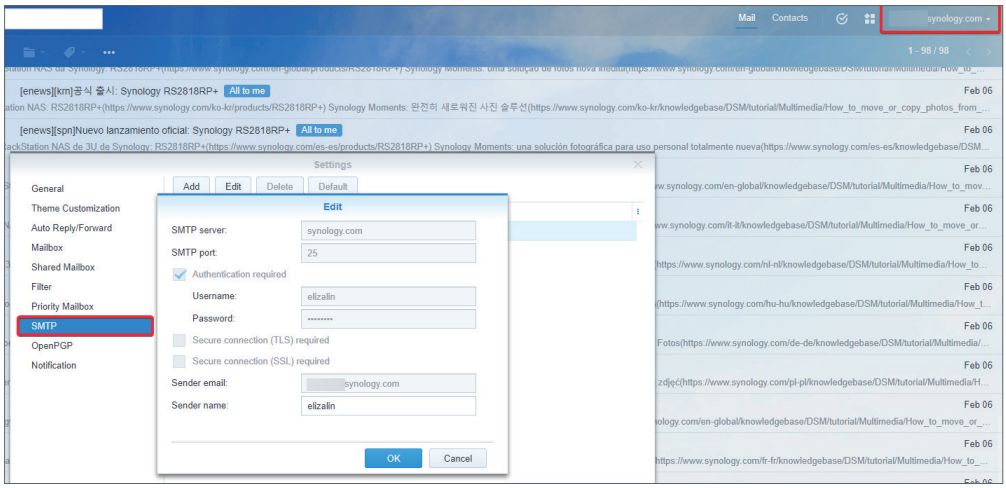

   - **응용 프로그램 포털**을 통해 MailPlus 에 액세스합니다 . 웹 브라우저의 주소 표시줄에 Synology NAS 이름을 입력한 후 "/mail" 을 입력합니다 . 예를 들어 Synology NAS 가 **mydiskstation** 이면 **mydiskstation/mail** 을 입력합니다 . **응용 프로그램 포털**을 활성화하는 방법은 **이 도움말 문서**를 참조하십시오 .



2. DSM 사용자 이름과 패스워드를 입력하여 로그인합니다 .




3. MailPlus 를 설치하기 전에 MailPlus Server 설정이 구성되면 MailPlus Server 의 SMTP 설정이 자동으로 **설정** > **SMTP** 에 표시됩니다 .

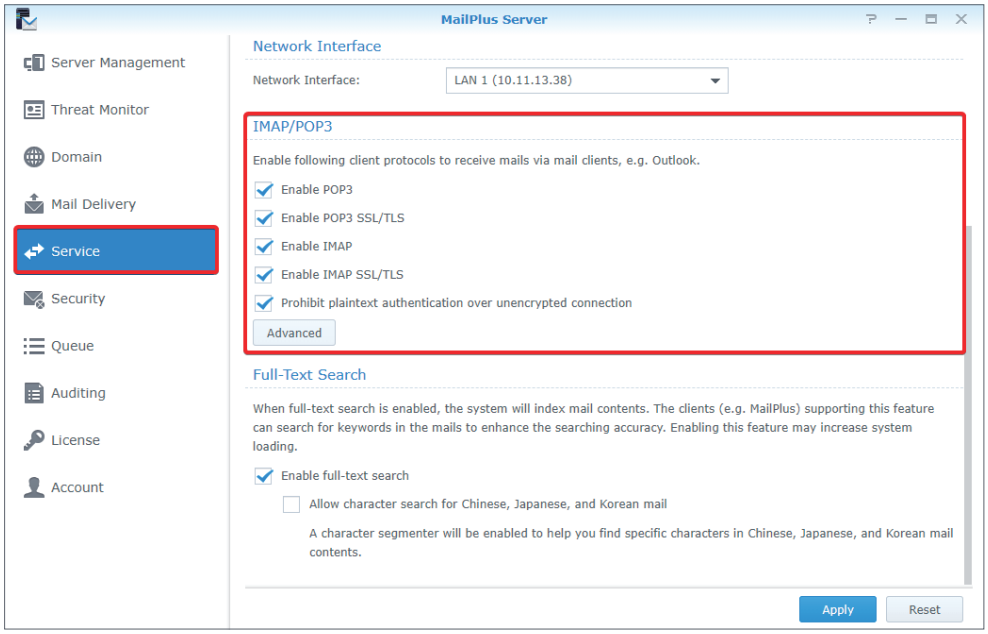


# 타사 이메일 클라이언트

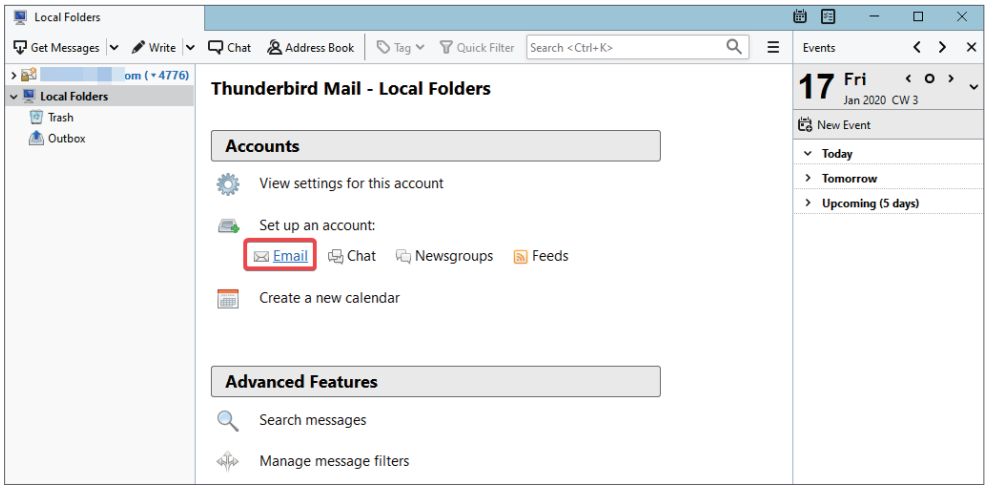
## 다른 이메일 클라이언트를 사용하여 Synology NAS 에서 이메일 액세스

Synology NAS 의 이메일 계정을 Microsoft® Outlook® 또는 Mozilla® Thunderbird® 와 같은 다양한 메일 클라이언트에 연결할 수 있습니다 . 아래 예에서는 Thunderbird® 를 사용하여 Synology NAS 에 호스팅된 이메일 계정에 액세스하는 방법을 보여줍니다 .

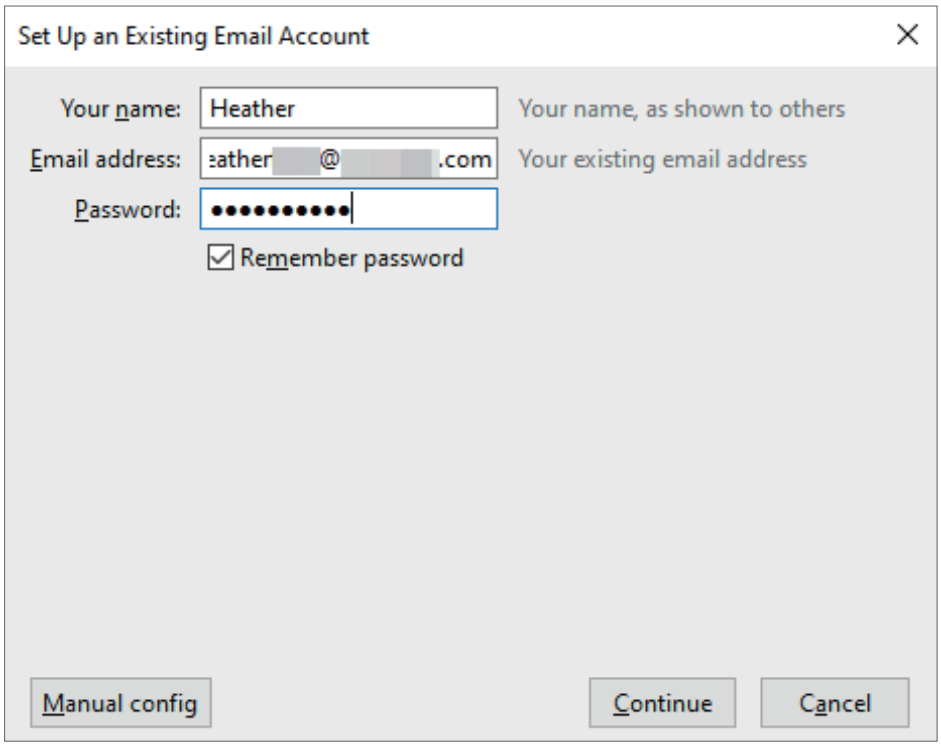
1. **MailPlus Server** 를 시작하고 **서비스** 페이지로 이동하여 IMAP 및 POP3 를 활성화합니다 .




2. 컴퓨터에서 Thunderbird® 를 시작하고 **이메일**을 클릭하여 **기존 이메일 계정 설정** 창을 시작합니다 .

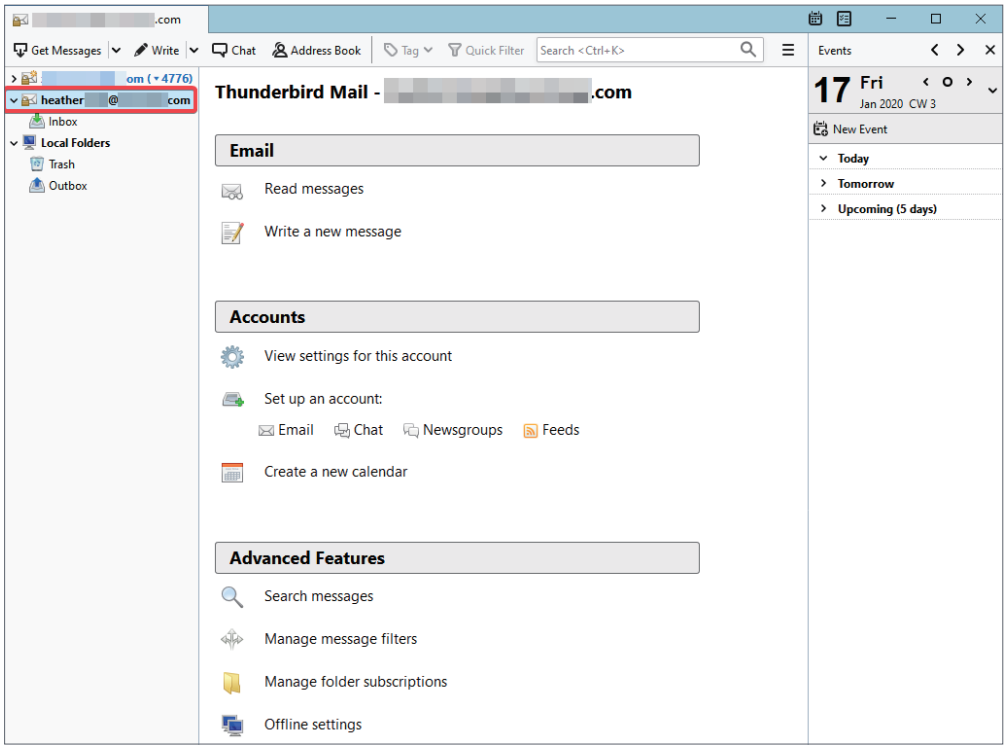


3. DSM 사용자 계정의 이름 , MailPlus 주소 및 패스워드를 입력합니다 . **계속**을 클릭합니다 .




4. Thunderbird® 가 MailPlus 계정을 검색합니다 . 설정이 올바르면 **완료**를 클릭하여 설정을 마칩니다 .

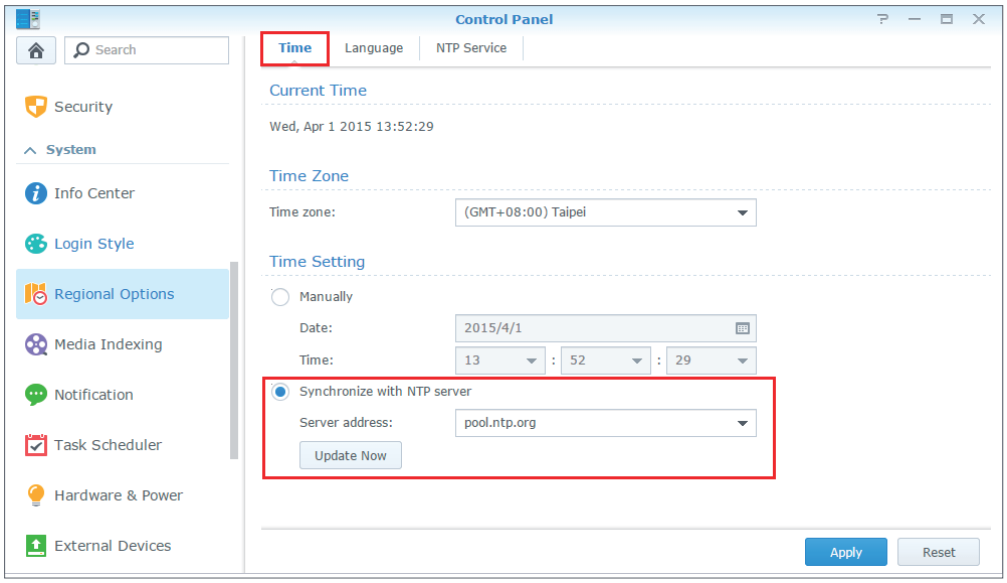
5. 설정이 완료되면 MailPlus 계정이 왼쪽 패널에 나타납니다 . 계정을 더블 클릭하면 모든 사서함을 확장할 수 있습니다 .



# 문제 해결

## MailPlus 에서 웹메일을 통해 이메일을 보내거나 받을 수 없는 이유는 무엇입니까 ?

1. SMTP, DNS 및 MX 와 같은 MailPlus 설정이 올바른지 확인합니다 .
2. Synology NAS 의 인터넷 설정이 올바른지 확인합니다 . **제어판** > **지역 옵션**으로 이동합니다 . **시간** 탭에서 **NTP 서버와 동기화**를 선택하고 **지금 업데이트** 버튼을 클릭하여 인터넷 설정이 올바른지 검사합니다 . 결과가 성공적으로 반환되면 설정이 올바른 것입니다 .




3. 라우터의 포트 번호가 올바른지 확인합니다 .
4. 사용 중인 IP 가 스패머로 등록되었는지 확인하려면 **Spamhaus** 에 방문하십시오 . 그럴 경우 같은 웹사이트의 차단 목록에서 사용자 IP 를 제거합니다 .

## 이메일 클라이언트를 통해 이메일을 보내거나 받을 수 없는 이유는 무엇입니까 ?

1. IMAP 및 POP3 가 활성화되었는지 확인합니다 .
2. 사용자 이름과 패스워드가 올바른지 확인합니다 .
3. SMTP, DNS 및 MX 와 같은 MailPlus 설정이 올바른지 확인합니다 .
4. Synology NAS 의 인터넷 설정이 올바른지 확인합니다 . **제어판** > **지역 옵션**으로 이동합니다 . **시간** 탭에서 **NTP 서버와 동기화**를 선택하고 **지금 업데이트** 버튼을 클릭하여 인터넷 설정이 올바른지 검사합니다 . 결과가 성공적으로 반환되면 설정이 올바른 것입니다 .
5. 라우터의 포트 번호가 올바른지 확인합니다 .
6. 사용 중인 IP 가 스패머로 등록되었는지 확인하려면 **Spamhaus** 에 방문하십시오 . 그럴 경우 같은 웹사이트의 차단 목록에서 사용자 IP 를 제거합니다 .

### 다른 메일 서버 ( 예 : Gmail) 에서 보낸 이메일을 받을 수 없는 이유는 무엇입니까 ?

1. DNS 설정이 올바르게 구성되었는지 확인합니다 . 다른 메일 서버에서 Synology NAS 를 찾을 수 있도록 MX 레코드와 A 레코드가 Synology NAS 를 가리켜야 합니다 .
2. Synology NAS 가 고정 IP 주소를 가지고 있고 인터넷에 연결되어 있는지 또는 도메인 이름이 동적 IP 를 올바르게 가리키고 있는지 확인합니다 .
3. Synology NAS 가 NAT 방화벽 / 라우터를 통과하도록 설정되어 있으면 포트 전달이 제대로 작동하는지 확인하십시오 . **CanYouSeeMe 웹사이트**로 이동하고 포트 25 를 입력하면 포트 전달이 작동하는지 여부를 확인할 수 있습니다 .
4. 오류가 있으면 반환된 메일의 메시지를 검토하여 오류 발생 상세 원인을 확인합니다 .

### Gmail 또는 Hotmail 과 같은 특정 웹메일 계정으로 이메일을 보낼 때 거부당하는 이유는 무엇입니까 ?

다수의 무료 이메일 공급자는 역방향 DNS 를 조회하여 보낸 사람의 유효성을 검사합니다 . 역방향 DNS 조회가 보낸 도메인 이름과 일치하지 않으면 이메일이 거부됩니다 . ISP 에 문의하십시오 . 사용자 IP 주소가 스팸 차단 목록에 추가되어 있을 수도 있습니다 . **Spamhaus** 에 방문하여 이를 확인할 수 있습니다 .

# 3 장 : 메일 마이그레이션

기본 제공 메일 마이그레이션 도구를 사용하면 복잡한 설정 없이 MailPlus Server 가 MailPlus 가 아닌 메일 서버 ( 예 : Microsoft Exchange 및 IMAP 메일 서버 ) 와 타사 서비스 ( 예 : Gmail 및 Yahoo Mail) 의 이메일을 마이그레이션할 수 있습니다 .

이 장에서는 이메일을 Microsoft Exchange 에서 MailPlus Server 로 마이그레이션하는 방법을 설명합니다 . 시작하기 전에 다음 작업을 완료했는지 확인하십시오 .

- Synology NAS 에서 DSM 6.0 이상이 실행되고 MailPlus Server 를 지원하는지 확인합니다 ( 호환 모델은 **여기** 참조 ).
- Synology NAS 에서 MailPlus Server 가 대상 메일 서버가 되도록 설정합니다 .
- 원본 계정의 사용자 이름과 패스워드 , 해당 MailPlus 계정 이름을 수집합니다 .

## MailPlus Server 에서 메일 마이그레이션 작업 만들기

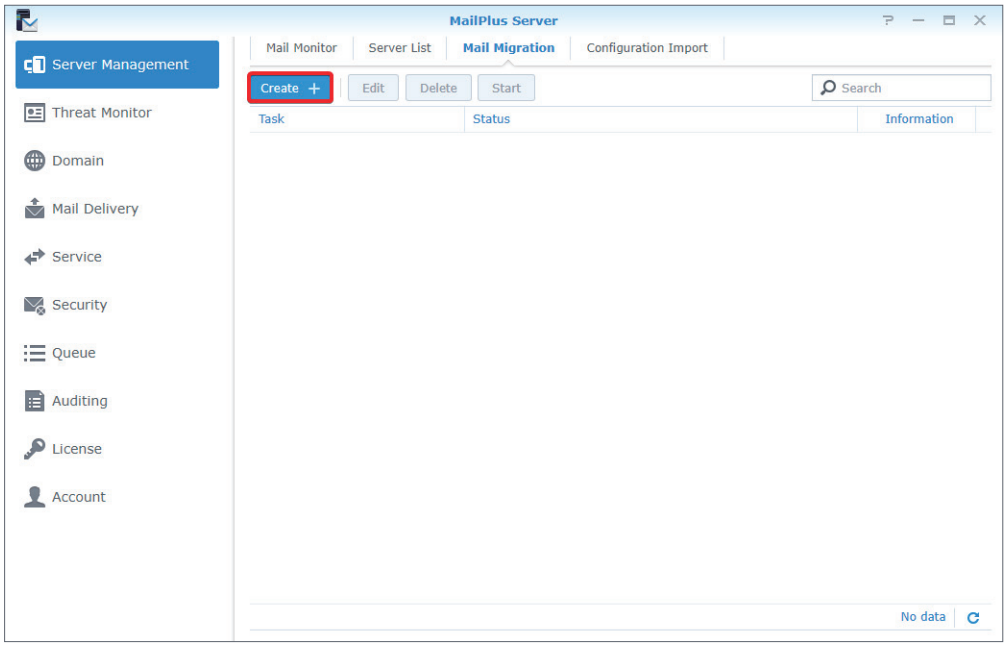
MailPlus Server 서버에 로그인하고 **서버 관리** > **메일 마이그레이션**으로 이동한 후 **생성** 버튼을 클릭하여 메일 마이그레이션 작업을 만듭니다 . 이 섹션에서는 Microsoft Exchange 를 예로 사용하여 설명합니다 .

**참고 :**

- 다른 원본 ( 예 : Gmail 또는 Yahoo Mail) 에서 이메일을 마이그레이션하는 방법을 확인하려면 **이 도움말 문서**를 참조하십시오 .

### 일반 작업 설정 구성

1. **서버 관리** > **메일 마이그레이션**으로 이동하고 **생성** 버튼을 클릭합니다 .

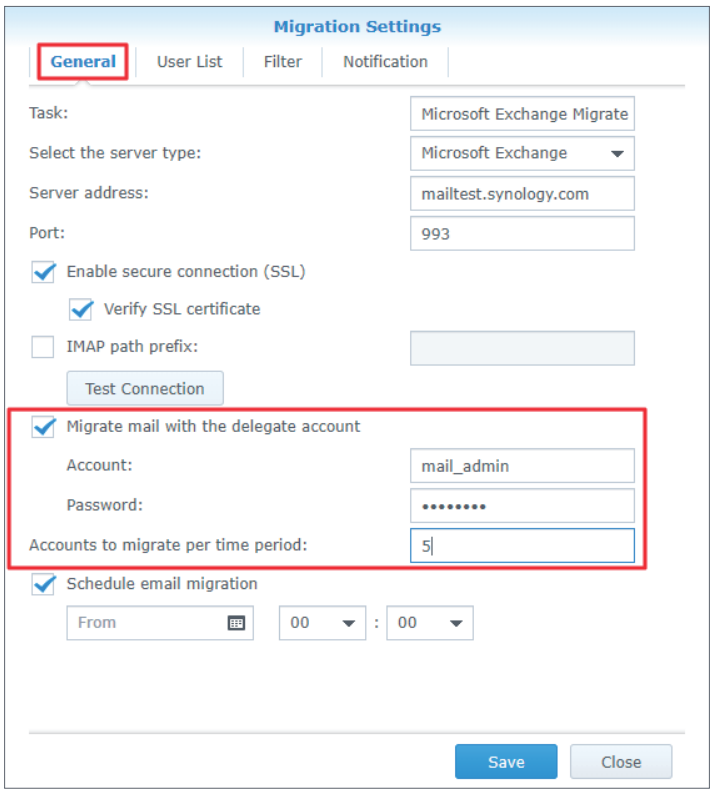



2. **마이그레이션 설정** 창의 **일반** 탭으로 이동하고 **서버 유형 선택**을 **Microsoft Exchange** 로 설정한 후 Microsoft Exchange 서버의 필수 정보를 입력합니다 .

3. Microsoft Exchange Server 설정에서 **IMAP 경로 접두사**를 찾을 수 있습니다 .

4. 다른 모든 원본 계정에 대한 전체 액세스 권한이 있는 위임 계정이 원본 서버에 있으면 **위임 계정을 사용하여 메일 마이그레이션**을 선택하고 계정 자격 증명을 입력합니다 . 이 계정을 사용하면 각 원본 계정에 대한 액세스 권한을 요청하지 않고도 이메일을 마이그레이션할 수 있습니다 .

5. 원본 서버 기능에 따라 **기간별로 마이그레이션할 계정**을 지정할 수 있습니다 .

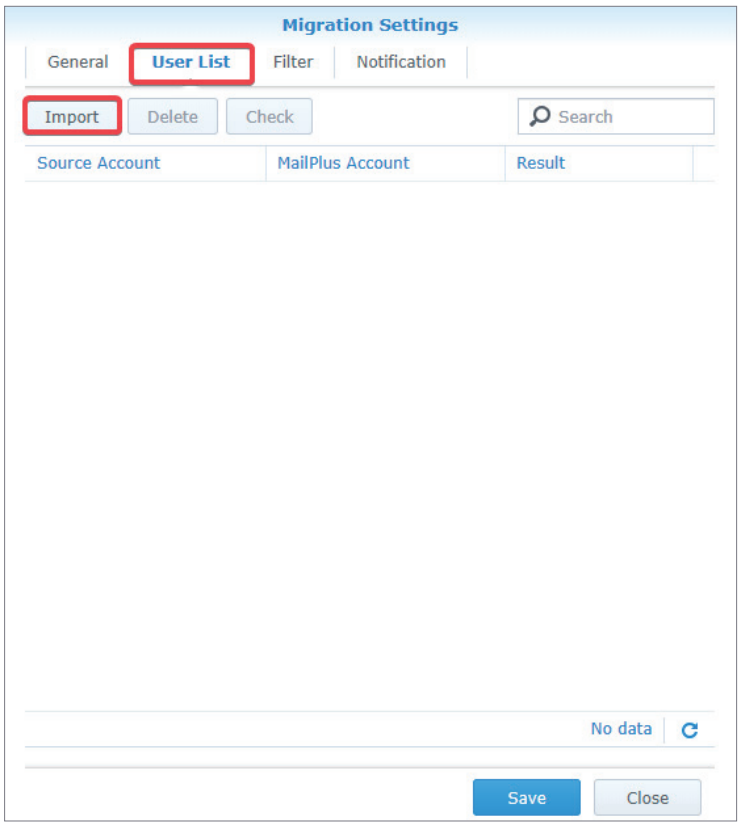


## 사용자 목록 가져오기

1. 먼저 , 아래 요구 사항을 충족하는 사용자 목록을 준비합니다 .
   - Microsoft Excel, Google 스프레드시트 등을 사용하여 사용자 목록을 CSV 형식으로 생성합니다 .
   - 한 행에 하나씩 사용자 계정 정보를 나열합니다 .
   - 왼쪽에서 오른쪽 방향으로 원본 계정 , 원본 계정 패스워드 및 해당 MailPlus Server 계정 등 각 사용자 정보를 나열합니다 .
   - 각 정보 유형은 쉼표 (,) 로 구분됩니다 .
   - 원본 서버 유형이 **Microsoft Exchange** 로 설정되어 있고 **위임 계정을 사용하여 메일 마이그레이션**이 활성화되어 있으면 원본 계정 패스워드를 생략할 수 있습니다 ( 예 : source_account_X,,MailPlus_Server_account_X).
2. 유효한 사용자 목록은 다음과 같은 형식이어야 합니다 .

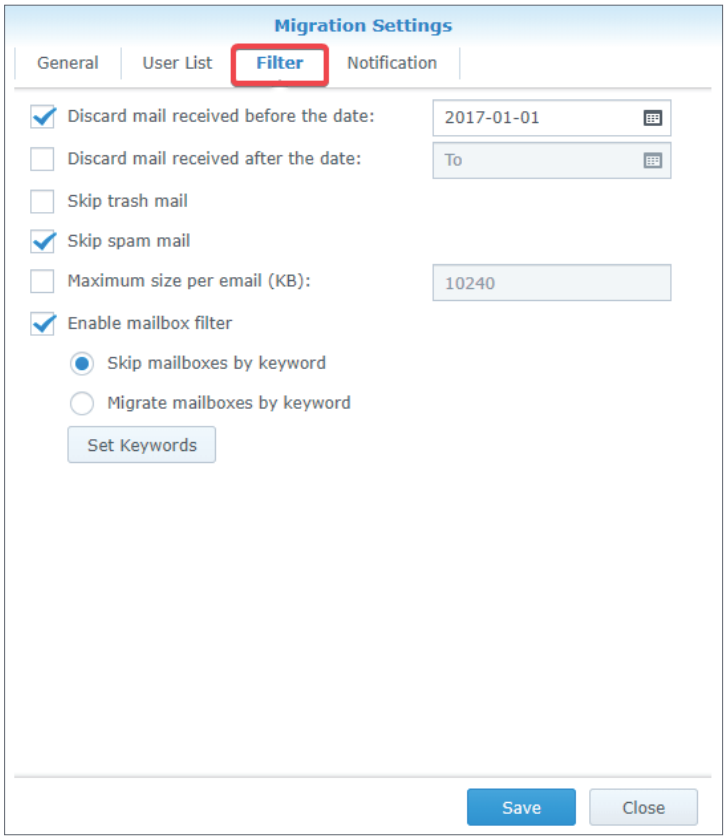
| |
|---|
| source_account_1,source_account_1_password,MailPlus_Server_account_1 |
| source_account_2,source_account_2_password,MailPlus_Server_account_2 |
| source_account_3,source_account_3_password,MailPlus_Server_account_3 |
| ... |
| source_account_N,source_account_N_password,MailPlus_Server_account_N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

3. **사용자 목록**으로 이동합니다 . 여기서 목록을 가져올 수 있습니다 . 모든 계정 데이터가 올바른지 확인합니다 .



## 이메일 및 사서함 필터 설정

1. **필터** 탭에서 마이그레이션 기준을 지정하거나 특정 이메일과 사서함을 건너뜁니다 .

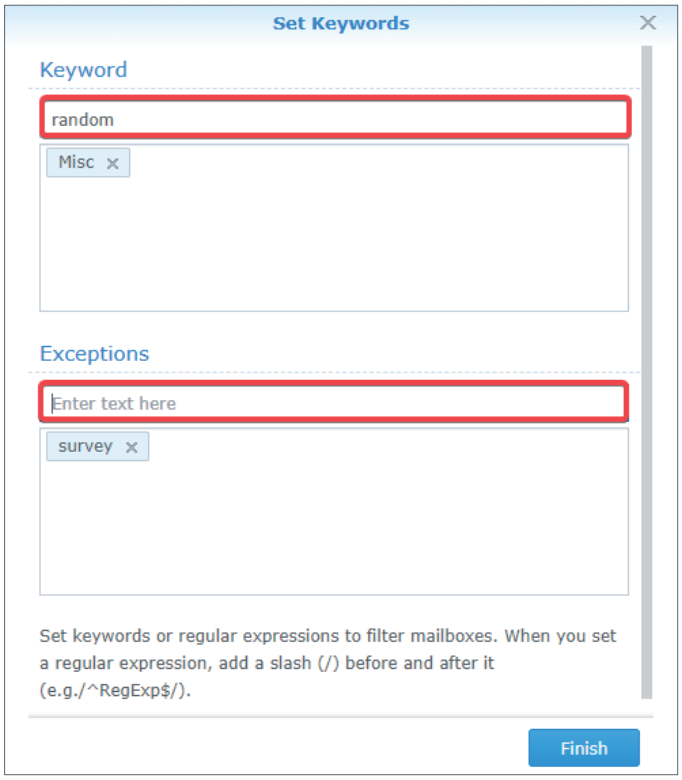



2. 키워드로 사서함을 필터링하려면 **사서함 필터 활성화** 확인란을 선택하고 필터 정책 ( **키워드로 사서함 건너뛰기** 또는 **키워드로 사서함 마이그레이션** ) 을 선택합니다 .

3. **키워드 설정**을 클릭하고 두 영역에 텍스트를 입력합니다 .

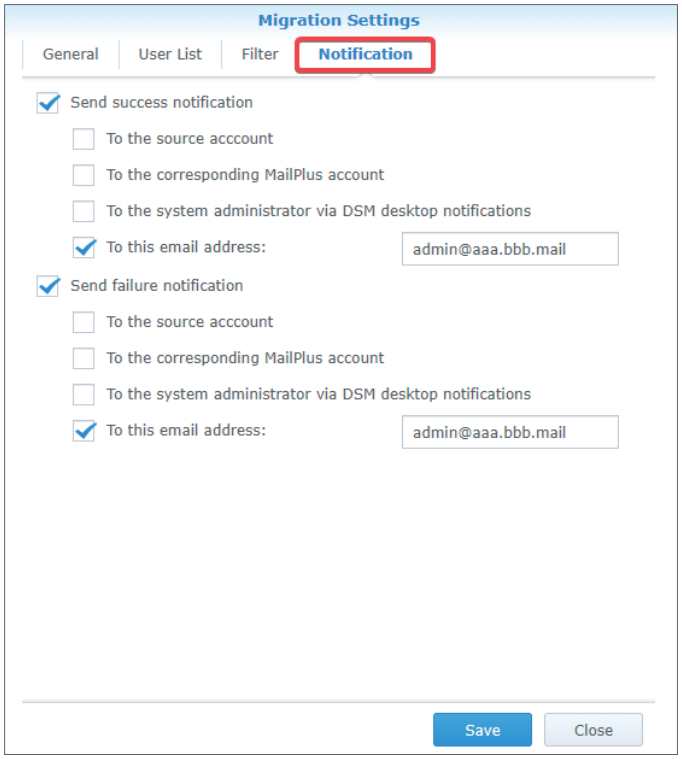
   - **키워드** : 선택한 필터 정책에 따라 일치하는 사서함을 처리하도록 텍스트를 입력합니다 .
   - **예외** : 일치하는 사서함이 처리되지 않도록 텍스트를 입력합니다 .

4. 두 영역에 정규식을 입력할 수 있습니다 . 그러면 정규식 양쪽 끝에 슬래시가 있어야 합니다 ( 예 : /REGULAR_EXPRESSION/).



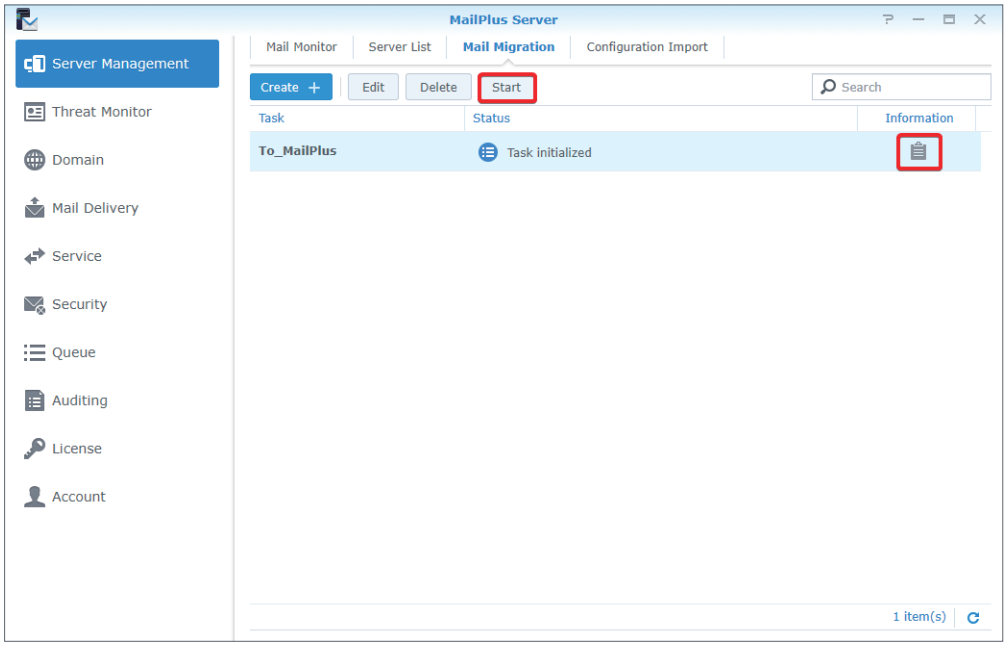

## 마이그레이션 알림 설정

1. 알림 전달을 허용하려면 MailPlus Server 의 **서비스**에서 **SMTP 활성화**를 선택해야 합니다 .
2. **알림** 탭에서 MailPlus Server 가 각 계정의 마이그레이션 결과 알림을 전송해야 하는지 여부와 관리자가 알림을 수신하는 위치를 결정합니다 .

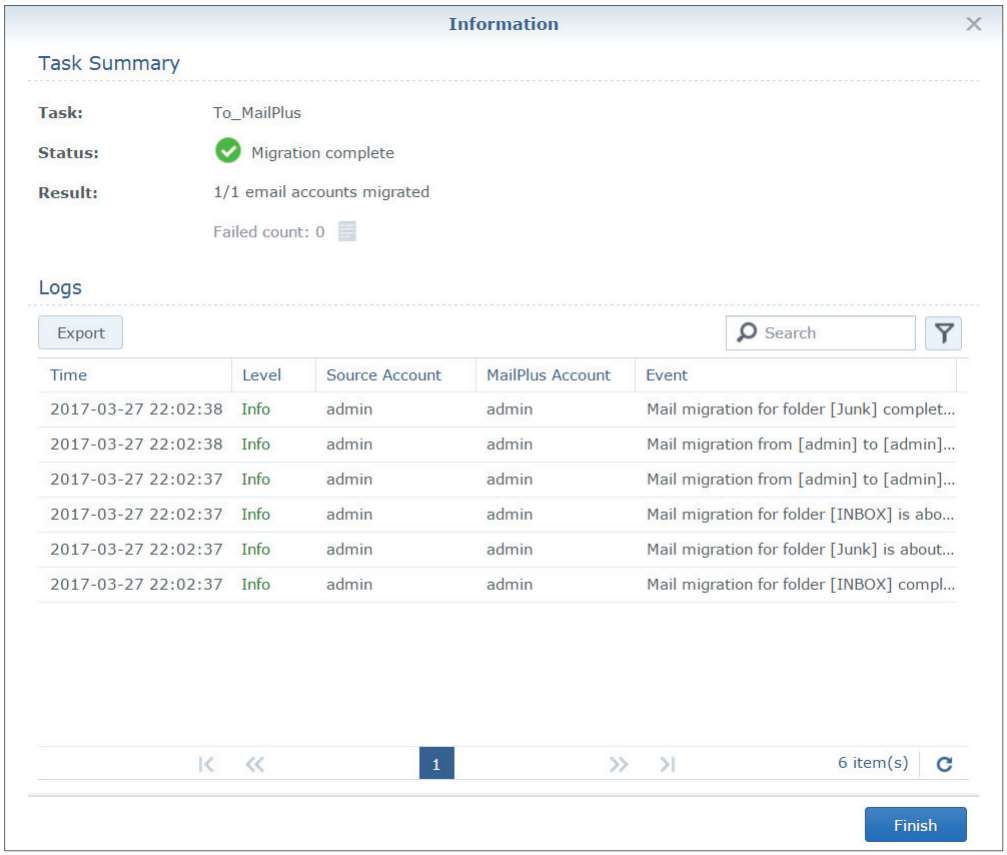


## 메일 마이그레이션 작업 실행하기

1. **서버 관리** > **메일 마이그레이션**에서 마이그레이션 작업을 선택하고 **시작**을 클릭하여 실행합니다 . 마이그레이션 오류를 방지하려면 MailPlus Server 에서 IMAP/POP3 설정을 변경하지 않거나 원본 메일 서버에서 이메일을 이동 / 삭제하지 마십시오 .




2. **정보** ( 문서 아이콘 ) 를 클릭하여 마이그레이션 통계와 로그를 확인합니다 .

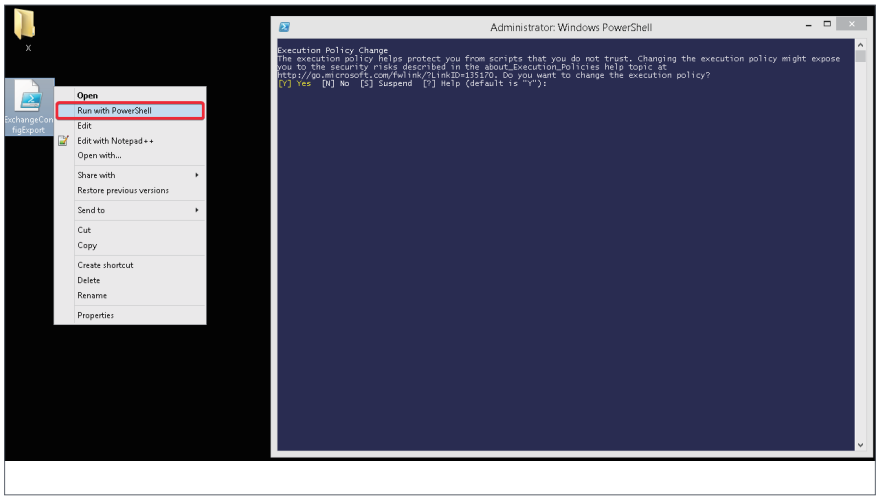


# 시스템 구성을 Microsoft Exchange 에서 MailPlus Server 로 가져오기

지속적으로 사용할 수 있도록 Microsoft Exchange 서버의 시스템 구성과 별칭을 내보내고 MailPlus Server 로 가져올 수 있습니다 .

## Microsoft Exchange 에서 시스템 구성 및 별칭 내보내기

1. 여기에서 스크립트 파일 (**ExchangeConfigExport.ps1**) 을 다운로드합니다 .
2. Microsoft Exchange Server 가 실행 중인 Windows 컴퓨터에 시스템 관리자로 로그인합니다 .
3. 스크립트 파일을 Windows 컴퓨터로 이동합니다 .
4. Windows PowerShell 을 사용하는 Microsoft Exchange 서버에서 스크립트 파일을 실행합니다 .




5. 실행 정책 변경 여부를 묻는 창이 나타나면 **예**를 선택하여 스크립트 실행을 허용합니다 .
6. 실행이 완료되면 Microsoft Exchange 서버에서 시스템 구성을 **SynologyExportedExchangeConf.xml** 파일로 , 별칭을 **SynologyExportedAlias.txt** 파일로 내보냅니다 .

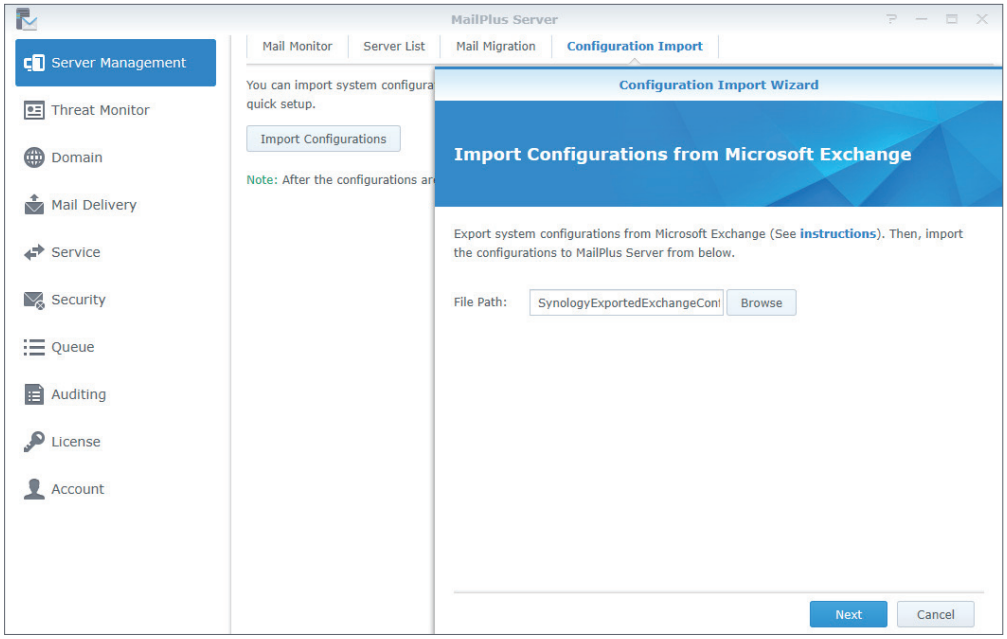

7. 생성된 .xml 파일과 .txt 파일을 로컬 컴퓨터로 옮깁니다 .

## 시스템 구성을 MailPlus Server 로 가져오기

1. 다음 방식 중 하나로 가져오기 프로세스를 시작합니다 .

   - MailPlus Server 를 초기화하려는 경우 : MailPlus Server 를 시작하고 **Microsoft Exchange 에서 구성을 가져와 새로운 메일 시스템 생성**을 선택합니다 .
   - MailPlus Server 가 이미 초기화된 경우 : MailPlus Server 를 시작하고 **서버 관리** > **구성 가져오기** > **구성 가져오기**로 이동합니다 .

2. **탐색**을 클릭하여 로컬 컴퓨터에서 **SynologyExportedExchangeConf.xml** 파일을 가져옵니다 .




3. **다음**을 클릭하여 **일반 설정** ( 예 : SMTP 및 보안 설정 ) 과 **기준** ( 예 : 블랙리스트 및 화이트리스트 ) 에서 구성 세부 사항을 확인합니다 . **가져오기**를 클릭합니다 .

# 4 장 : 사용자 라이센스

MailPlus Server 를 실행하려면 라이센스가 충분하게 있어야 합니다 . 필요한 라이센스 수는 활성화할 계정 수에 따라 결정됩니다 . 기본적으로 MailPlus Server 는 무료 이메일 계정을 5 개 제공합니다 . 라이센스를 추가로 구매하면 계정을 추가할 수 있습니다 .

라이센스 사용자 수는 다음에 의한 영향을 받지 않습니다 .

- **비활성화된 계정** : 예를 들어 전 직원의 라이센스를 신입 사원에게 적용할 수 있습니다 .
- **이메일 별칭** : 별칭 이메일 주소가 기존 사용자 계정에 바인딩되므로 각 사용자는 추가 비용 없이 별칭을 추가할 수 있습니다 .
- **여러 도메인 ( 기타 도메인 포함 )**: MailPlus Server 는 여러 도메인을 처리할 수 있으므로 여러 도메인을 사용할 경우 추가 라이센스가 필요 없습니다 .
- **지정된 계정 유형에 속하지 않는 DSM 사용자** : 예를 들어 계정 유형이 LDAP 사용자로 설정된 경우 로컬 사용자는 라이센스 사용자로 계산되지 않습니다 .

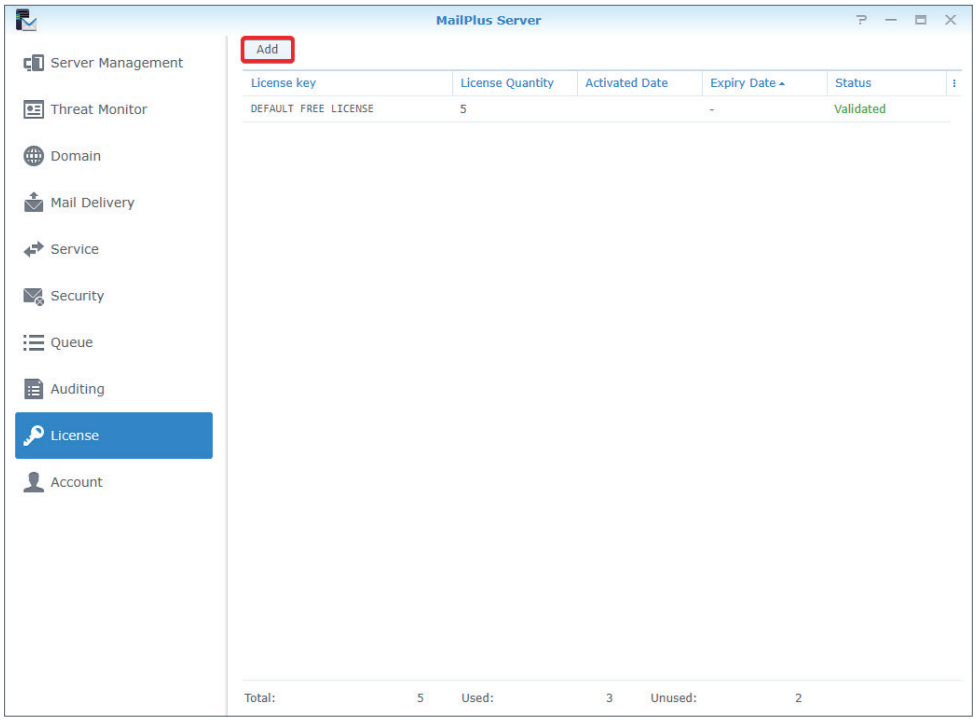
## 라이센스 구매

MailPlus 라이센스 팩에는 이메일 계정이 5 개 또는 20 개 포함되어 있으며 **Synology 공인 대리점**을 통해 라이센스 팩을 구매할 수 있습니다 . MailPlus 라이센스 팩에 대한 자세한 내용은 **MailPlus 라이센스 페이지**를 참조하십시오 .

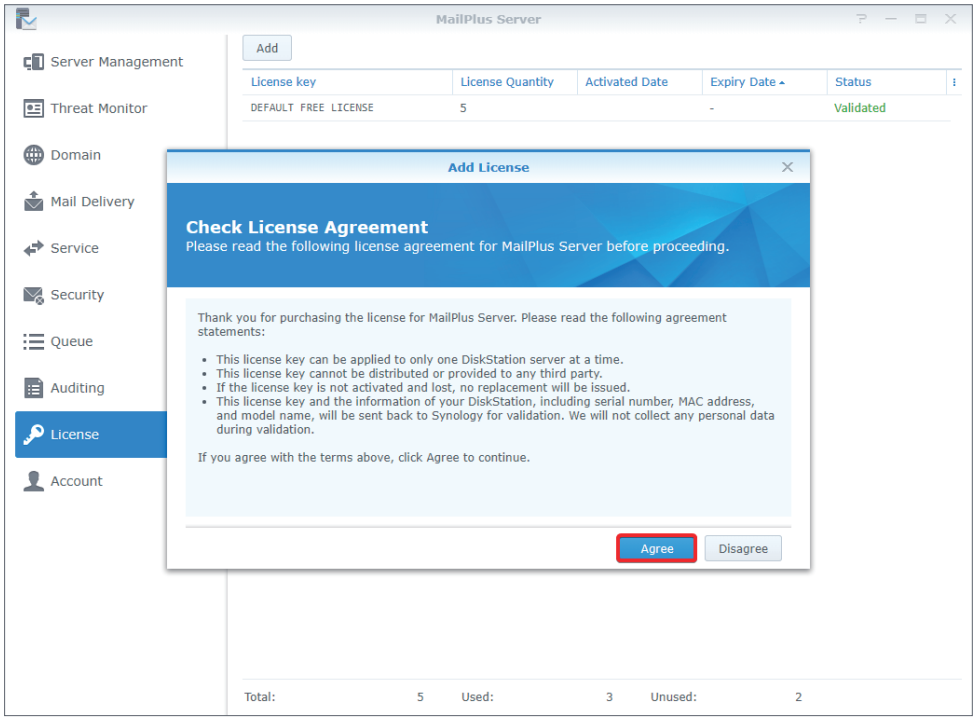
## 라이센스 설치

이메일 계정을 활성화하려면 구매한 라이센스를 설치해야 합니다 . 다음 단계를 참조하십시오 .

1. **라이센스**로 이동하고 **추가** 버튼을 클릭하여 라이센스를 추가합니다 .



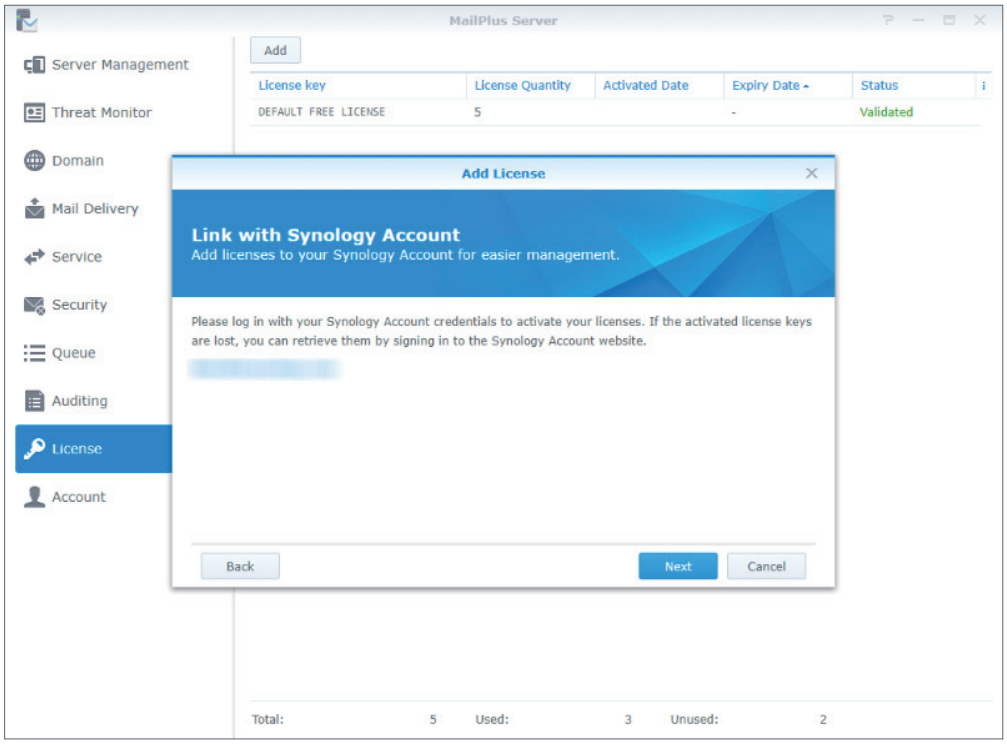

2. **라이센스 추가** 창에서 MailPlus Server 의 라이센스 계약을 주의 깊게 읽으십시오 . 내용을 확인한 후 **동의**를 클릭합니다 .



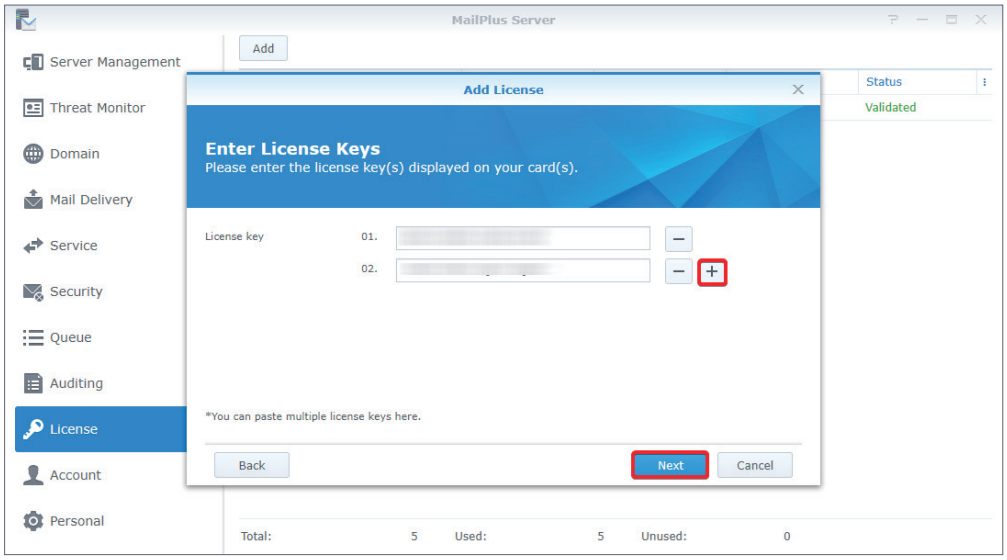

3. Synology 계정에 로그인하고 **다음**을 클릭합니다 .

**참고 :**

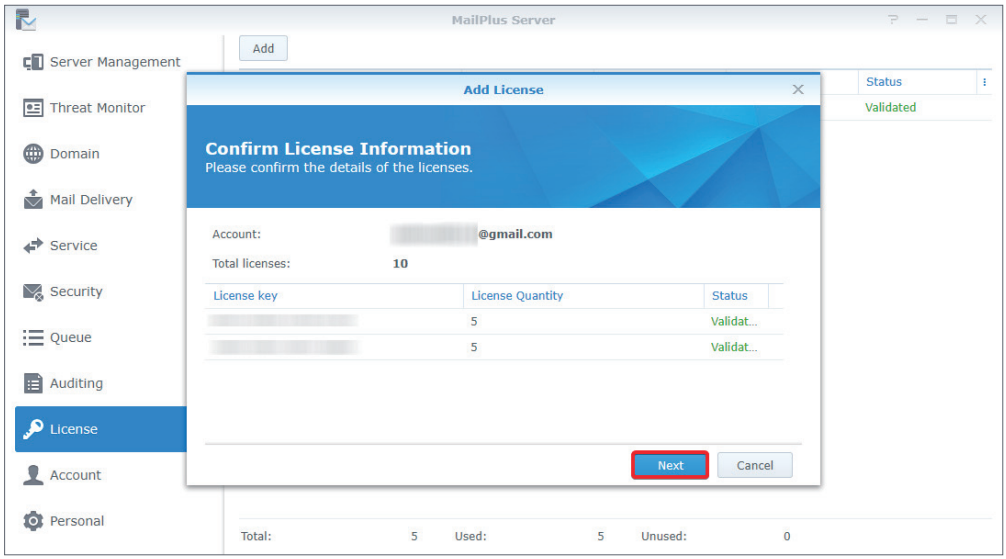
- 활성화 후 라이센스를 검색할 수 없으면 **Synology 계정**에 로그인하여 기술 지원 티켓을 제출하십시오 .



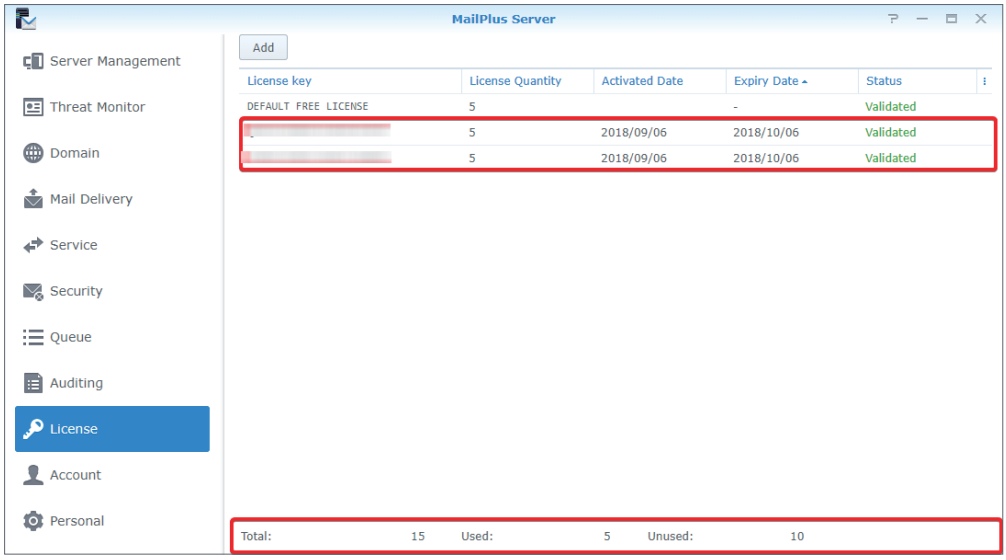

4. 다음 이미지와 같이 **라이센스 키** 필드에 라이센스 번호를 입력합니다 . 라이센스를 두 개 이상 추가해야 하는 경우 더하기 아이콘 (+) 을 클릭하여 필드를 추가합니다 .




5. 설치할 라이센스 수와 해당 라이센스 키가 올바른지 확인합니다 . 정보가 올바른지 확인한 후 **다음**을 클릭하여 라이센스 추가를 마칩니다 .




6. 라이센스가 추가되면 **라이센스** 페이지로 이동하여 각 라이센스의 세부 정보와 상태를 확인할 수 있습니다 .
   - 라이센스 키
   - 각 라이센스에서 제공하는 이메일 계정 수
   - 라이센스 활성일
   - 라이센스 만료일
   - 라이센스 유효 상태
7. 또한 **라이센스** 페이지 하단에서 MailPlus Server 에 설치된 총 라이센스 수와 사용한 라이센스와 사용하지 않은 라이센스 수를 확인할 수 있습니다 .




## 라이센스 사용

라이센스를 추가한 후 **계정** > **사용자**로 이동하여 활성화할 계정을 선택할 수 있습니다 . 자세한 내용은 **계정 활성화**를 참조하십시오 .

# 5 장 : 계정 설정

## 계정 시스템

MailPlus Server 는 DSM 과 동일한 계정 시스템을 사용합니다 . 따라서 DSM 의 기존 사용자 계정에서 MailPlus Server 의 사용자 계정을 활성화할 수 있습니다 .

로컬 사용자의 사용자 계정 활성화 외에도 **DSM** > **제어판** > **도메인 /LDAP** 로 이동하고 LDAP 와 도메인 계정을 바인딩하여 LDAP/ 도메인 사용자의 사용자 계정을 활성화할 수 있습니다 . 하지만 DSM 은 한 번에 디렉토리 서비스 두 개 이상을 동기화할 수 없으므로 , MailPlus Server 는 디렉토리 서비스와 계정 시스템 두 개 이상을 동시에 동기화할 수 없습니다 .

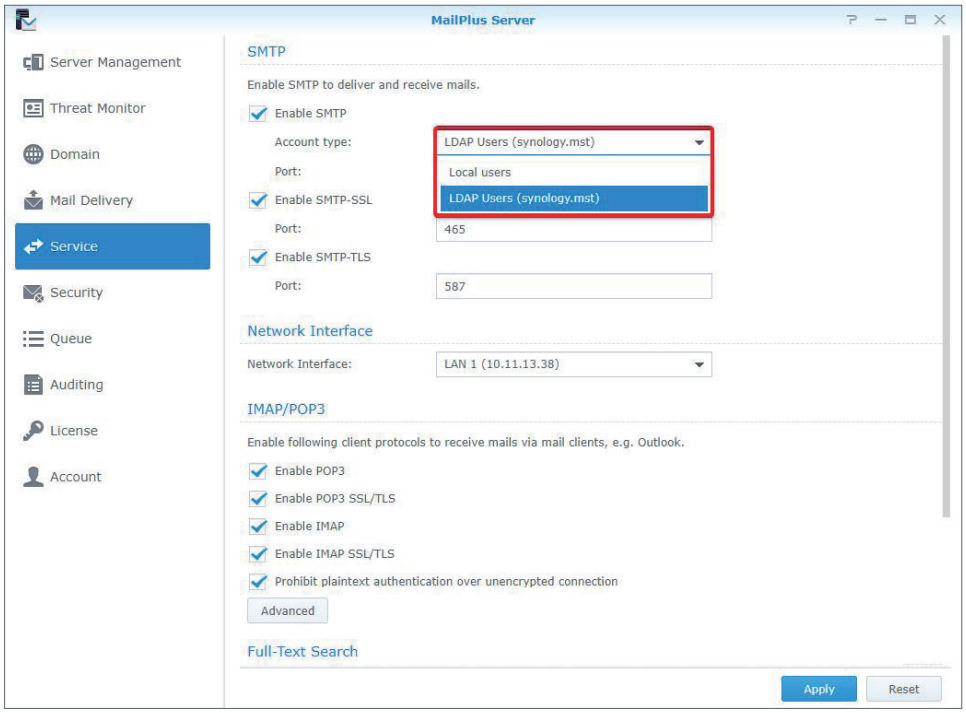
**참고 :**

- MailPlus Server 는 한 번에 **로컬** , **LDAP** 또는 **도메인** 계정 유형 중 하나만 사용할 수 있습니다 .

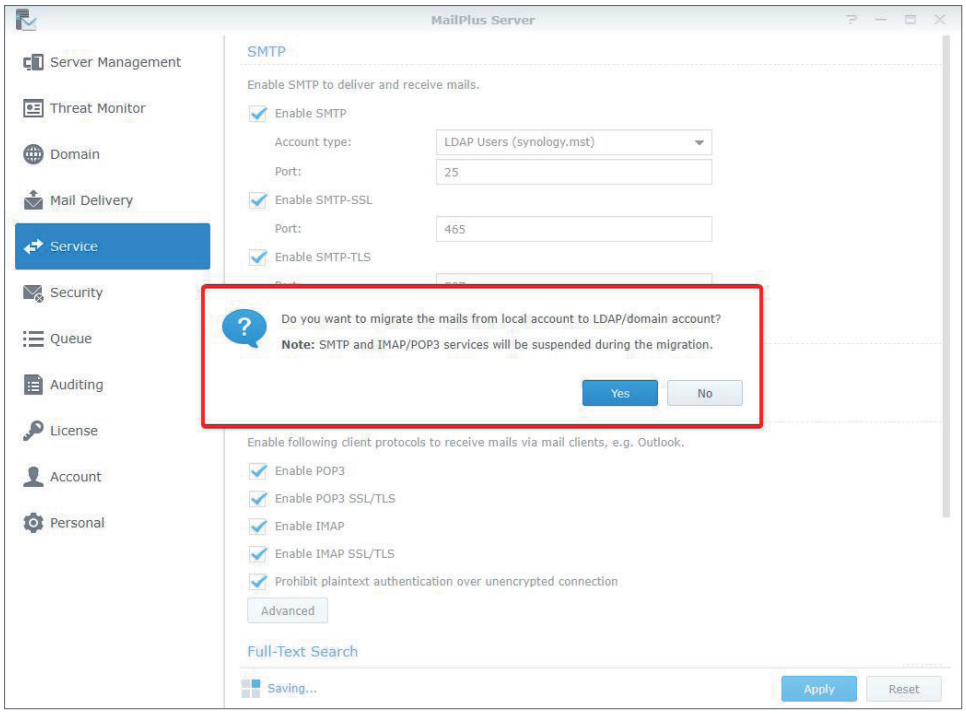
### 계정 유형 수정

사용자 계정을 수정하려면 다음 단계를 수행하십시오 .

1. DSM 에 로그인합니다 .
2. **제어판** > **도메인 /LDAP** 로 이동하여 특정 디렉토리 서비스를 바인딩합니다 . **로컬 사용자**를 계정 유형으로 사용할 경우 이 단계를 건너뛰십시오 .
3. **MailPlus Server** 를 시작합니다 .
4. **서비스**로 이동하고 **계정 유형** 드롭다운 메뉴에서 계정 유형을 선택합니다 . DSM 에 구성된 디렉토리 서비스만 여기에 표시됩니다 .




5. **적용**을 클릭하여 디렉토리 서비스에서 사용자 계정을 가져옵니다 . 다음 이미지와 같이 **로컬 사용자**를 **LDAP 사용자** 또는 **도메인 사용자**로 전환하고 **적용**을 클릭하면 경고 창이 표시됩니다 .




**참고 :**

- 계정 유형에 따라 이메일 주소가 다르므로 , 다른 계정 유형의 이메일을 공유할 수 없습니다 . **로컬 사용자**의 이메일을 **LDAP 사용자** 또는 **도메인 사용자**로 마이그레이션하려면 **예**를 클릭하십시오 . 시스템은 로컬 사용자와 동일한 사용자 이름이 있는 디렉토리 서비스 계정으로만 이메일을 마이그레이션합니다 . 사용자 이름이 다른 계정은 자동으로 무시됩니다 .

# 계정 활성화

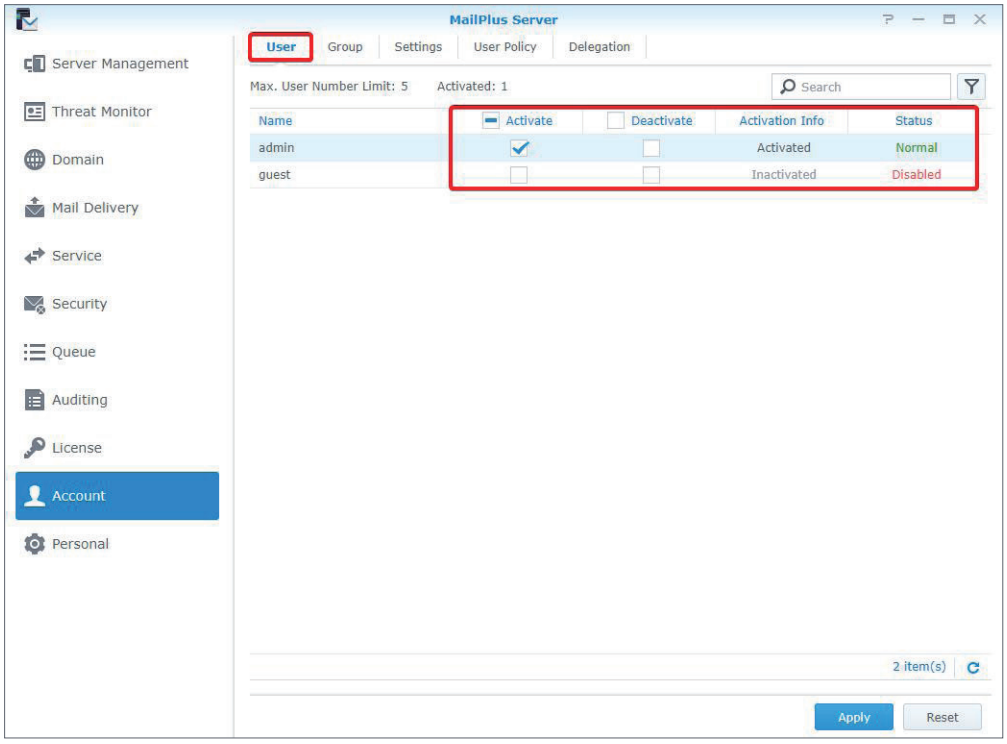
이메일 전송 및 수신과 같은 메일 서비스를 사용하려면 MailPlus Server 에서 사용자 계정을 활성화해야 합니다 . 따라서 메일 서비스를 사용할 계정을 활성화하려면 라이센스가 충분하게 있어야 합니다 . 자세한 내용은 **사용자 라이센스** 섹션을 참조하십시오 .

이미 일부 사용자 계정을 활성화했고 이러한 사용자가 DSM 에 로그인하거나 MailPlus/MailPlus Server 를 시작할 수 없으면 사용자 계정을 비활성화했는지와 이러한 사용자 계정에 MailPlus 또는 MailPlus Server 에 대한 권한이 있는지 확인하십시오 . 클라이언트 로그인 문제에 대한 자세한 내용은 **이 문서**를 참조하십시오 .

## 사용자 계정 활성화

사용자 계정을 활성화하려면 라이센스가 충분하게 있어야 합니다 . 자세한 내용은 **사용자 라이센스** 섹션을 참조하십시오 . 사용자 계정을 활성화하려면 다음 단계를 수행하십시오 .

1. **계정** > **사용자**로 이동합니다 .
2. 활성화할 사용자를 선택합니다 . **활성화** 및 **비활성화** 열 아래에서 특정 사용자의 확인란을 선택하지 않으면 이 사용자 상태는 기본 상태로 설정됩니다 . 자세한 내용은 **기본 상태**를 참조하십시오 . **활성화** 확인란을 선택하면 사용 가능한 라이센스 수가 줄어듭니다 .




3. **활성화 정보** 열에 라이센스가 사용자에게 적용되었는지 여부가 표시됩니다 .
4. **상태** 열에는 **일반** , **비활성화됨** 및 **사용자 이름이 지원되지 않음**과 같은 DSM 사용자 상태가 표시됩니다 .

**참고 :**

- 사용자는 계정이 **활성화 정보**에서 **활성화됨**이고 **상태**에서 **정상**인 경우에만 메일 서비스를 올바르게 사용할 수 있습니다 . **제어판**에서 설정을 수정하지 않고 계정 설정을 MailPlus 권한에서 유일한 항목으로 남겨둘 수 있습니다 .

5. **적용**을 클릭하여 사용자를 활성화합니다 .

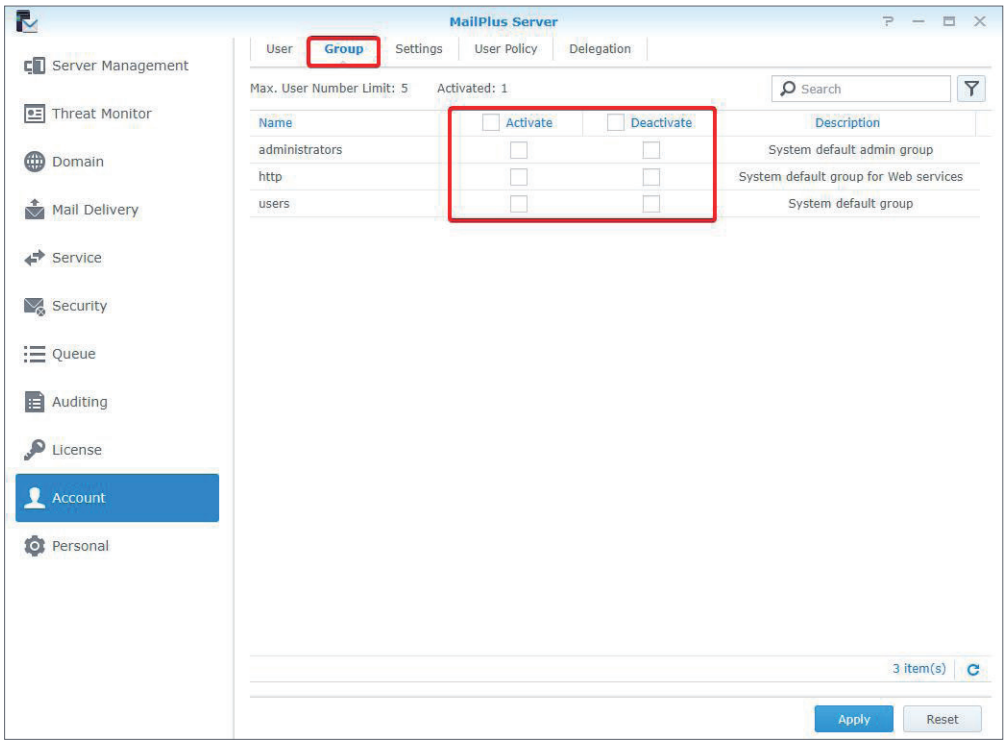
## 그룹 활성화

여기에서 사용자 그룹을 간편하게 활성화 및 비활성화할 수 있습니다 . 설정은 같은 그룹 내 모든 구성원에게 적용됩니다 . 다음 단계를 참조하십시오 .

1. **계정** > **그룹**으로 이동하여 그룹을 활성화하거나 비활성화합니다 .

**참고 :**

- 마지막으로 활성화된 사용자 계정을 확인하는 우선 순위의 내림차순 순서는 **사용자** 설정 , **그룹** 설정 및 **기본** 설정입니다 .




2. **적용**을 클릭하여 그룹 내 사용자를 활성화합니다 .

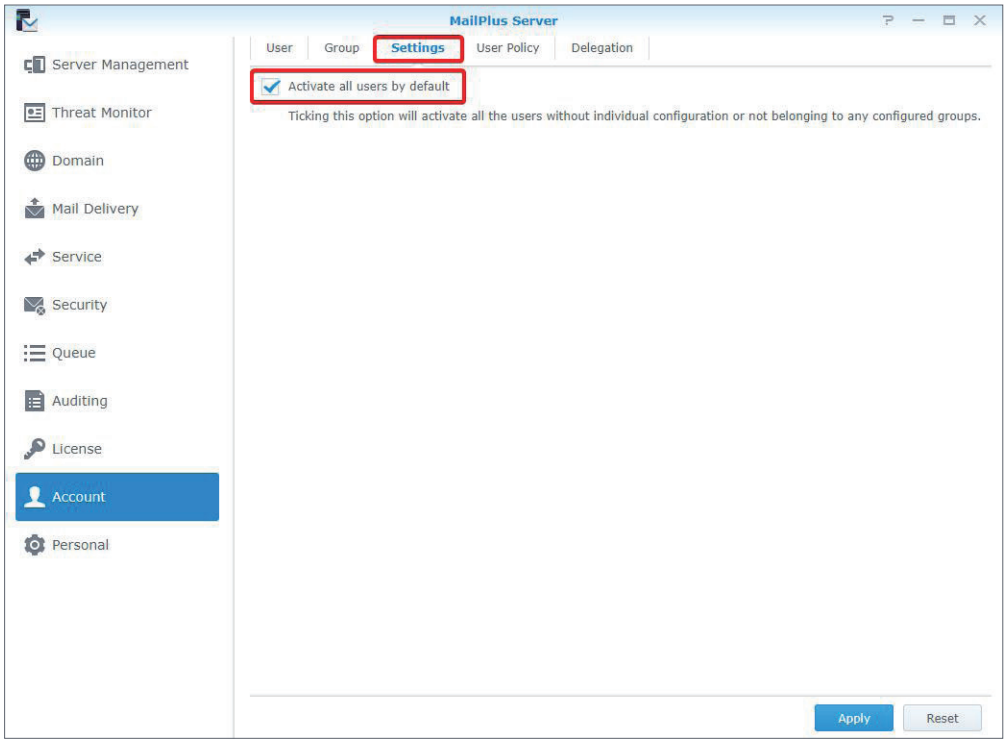
## 기본 상태

**계정** 페이지의 **설정** 탭에서 기본 상태를 조정할 수 있습니다 . 기본 상태 설정은 활성화 또는 비활성화되지 않은 **정상** 상태의 사용자 계정에 적용됩니다 . 다음 단계를 참조하십시오 .

1. **계정** > **설정**으로 이동하고 **기본적으로 모든 사용자 활성화** 확인란을 선택할지 여부를 선택합니다 .

**참고 :**

- 기본적으로 활성화에서는 라이센스를 여러 개 사용할 수 있습니다 . 라이센스가 충분하게 있는지 확인하십시오 .



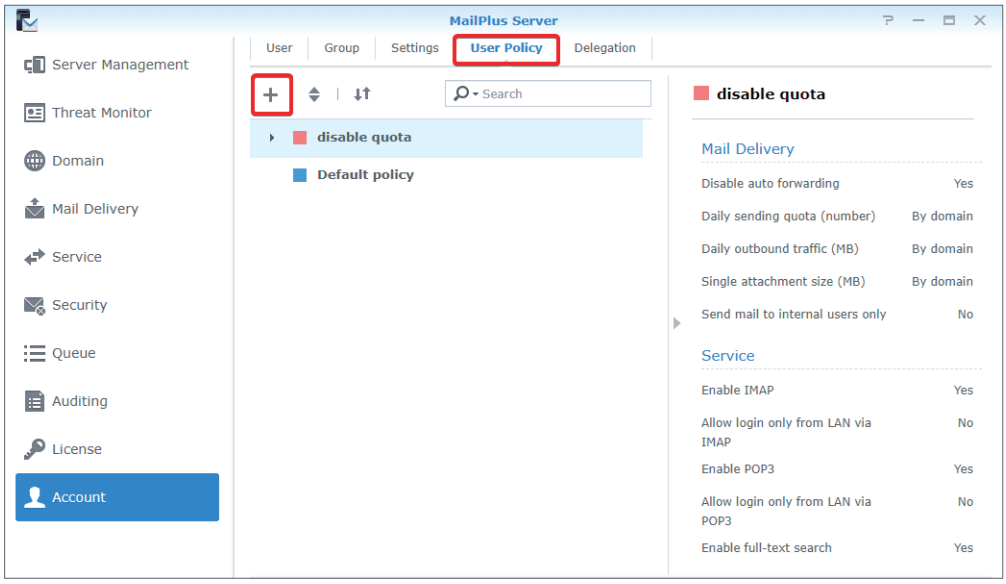

2. **적용**을 클릭하여 설정을 저장합니다 .

## 사용자 정책 만들기

사용자나 그룹을 활성화한 후 조직의 요구 사항을 충족하는 특정 사용자나 그룹의 전용 메일 서비스 정책을 만들 수 있습니다 . 다음 단계를 참조하여 사용자 정책을 만드십시오 .

1. **계정** > **사용자 정책**으로 이동합니다 .

2. 더하기 아이콘 (+) 을 클릭하여 새 정책을 만듭니다 .

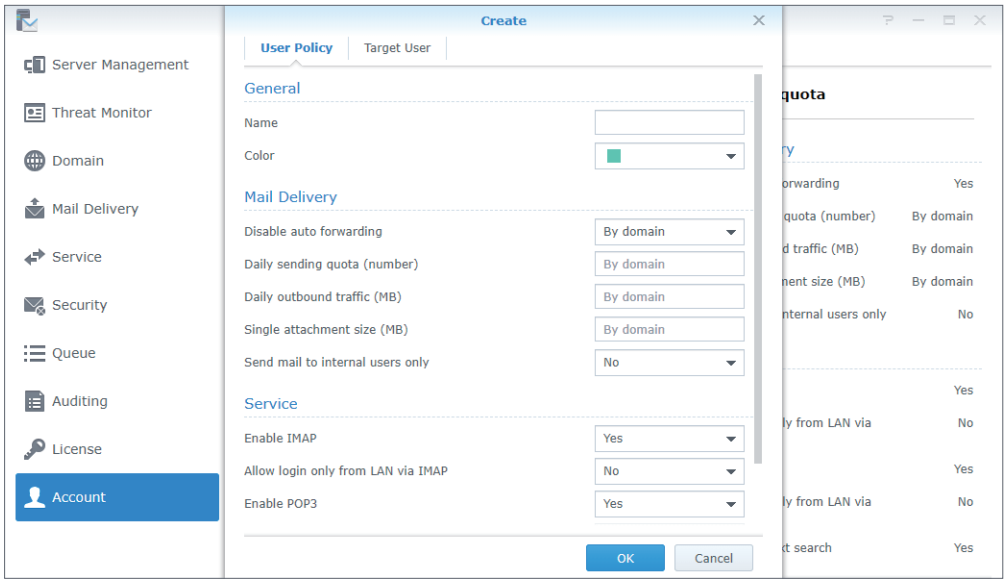



3. **만들기** 창에서 **사용자 정책**으로 이동하고 **이름** 필드에 정책 이름을 입력합니다 .

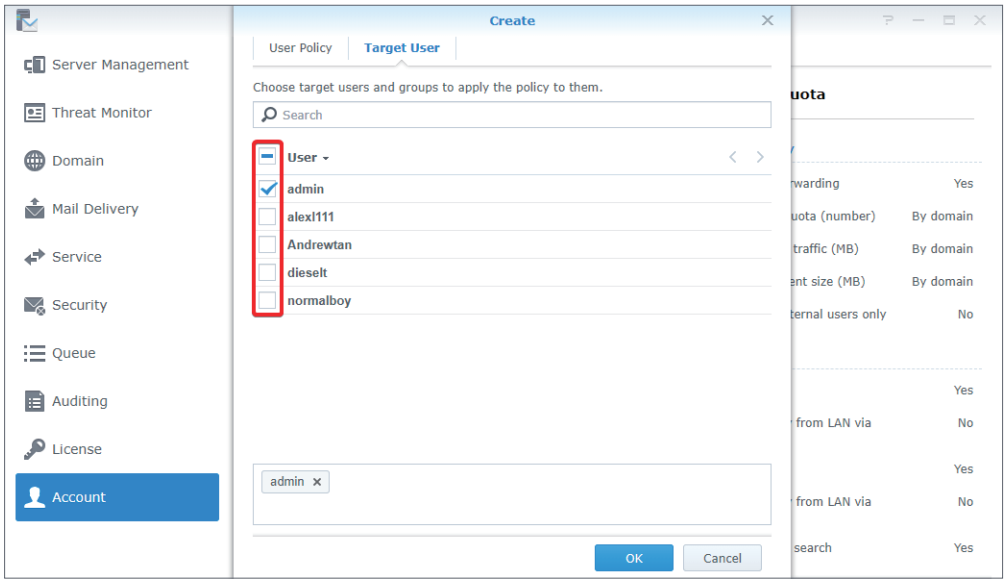
4. 쉽게 식별할 수 있도록 **색상** 드롭다운 메뉴에서 정책 색상을 선택합니다 .

**참고 :**

- 정책 정보에 대한 자세한 내용은 **정책 정보 및 제한 사항**을 참조하십시오 .

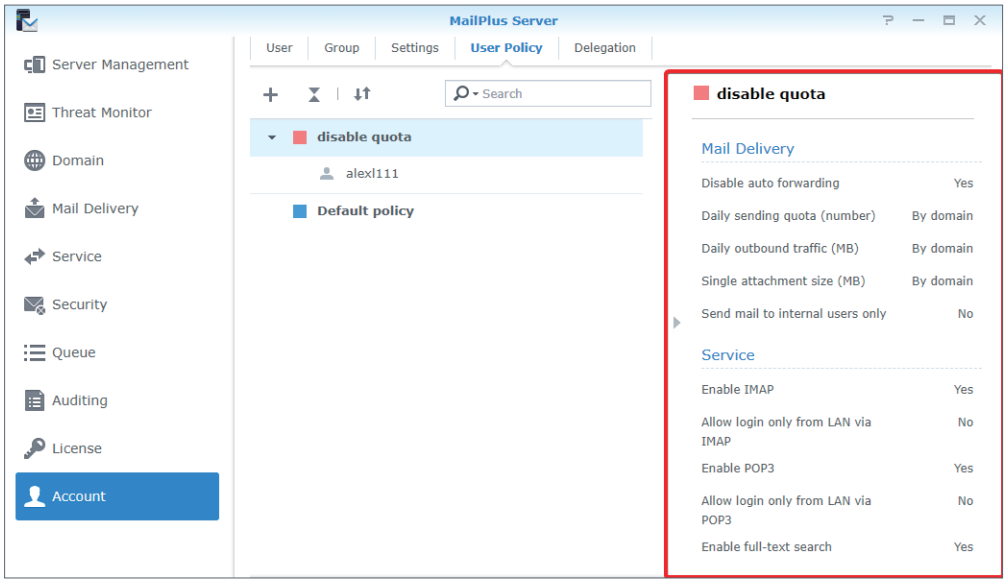



5. **대상 사용자** 탭으로 전환하고 정책을 적용할 사용자나 그룹을 선택합니다 . 창 상단에 있는 검색 창을 사용하여 대상을 찾을 수도 있습니다 .




6. **확인**을 클릭하여 설정을 완료합니다 .

7. 정책이 생성되면 **사용자 정책** 페이지에 나열됩니다 . 페이지 오른쪽 패널에서 정책 세부 정보와 설정을 미리 볼 정책을 선택합니다 .

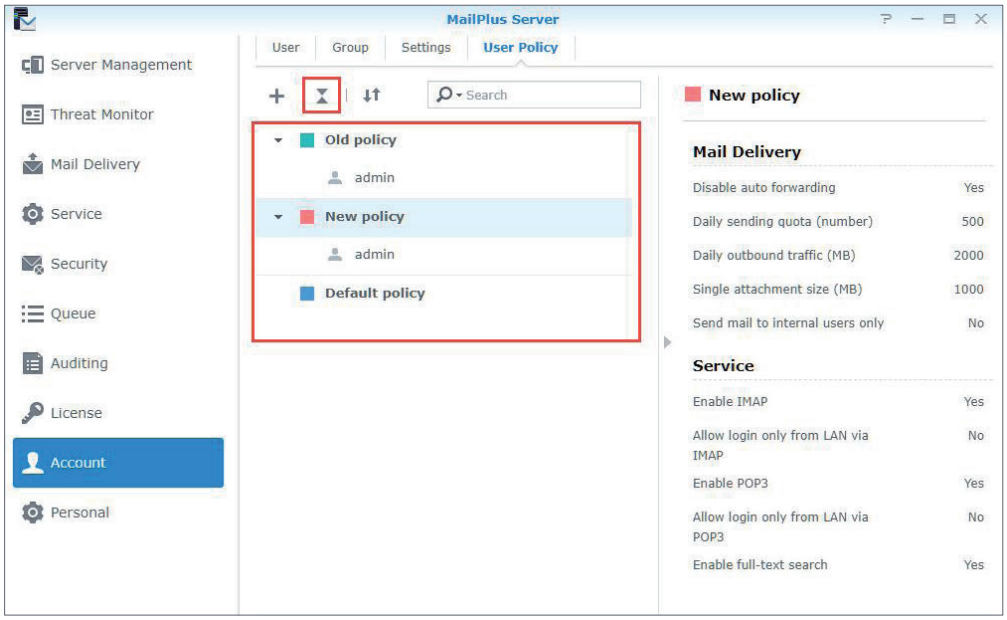



## 사용자 정책 우선 순위 변경

사용자 한 명에게 사용자 정책을 여러 개 적용할 수 있지만 정책 하나만 유효합니다 . 유효한 정책은 사용자 정책의 우선 순위 설정에 따라 다릅니다 . 다음 단계를 참조하여 사용자 정책 우선 순위를 변경하십시오 .

1. **계정** > **사용자 정책**으로 이동하고 이중 삼각형 아이콘을 클릭하여 대상 사용자 / 그룹을 표시하거나 숨깁니다 .

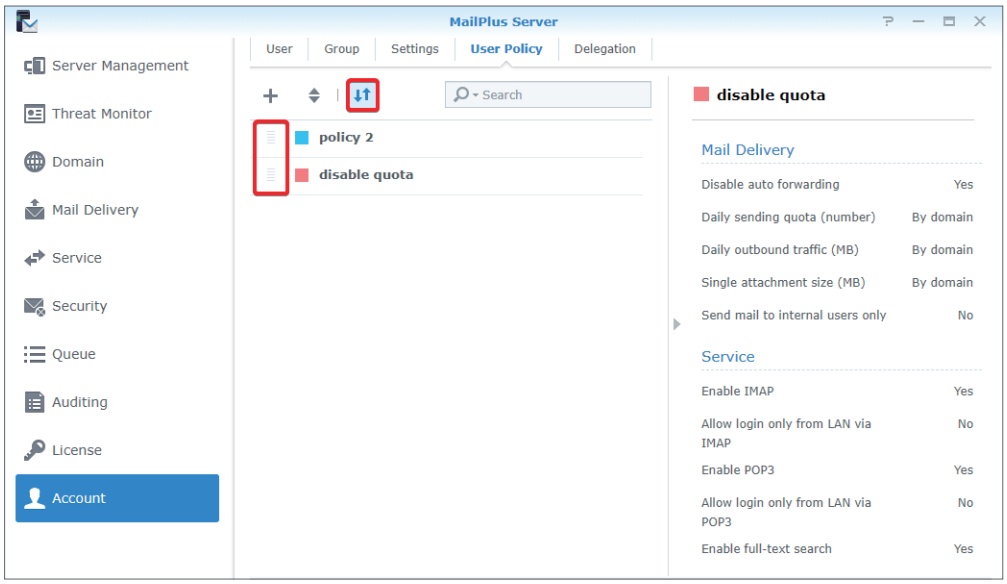
2. 정책이 높을수록 낮은 정책보다 우선 순위가 높습니다 . 예를 들어 아래 이미지에서 내림차순 우선 순위는 **이전 정책** , **새 정책** , **기본 정책**입니다 . 따라서 **새 정책** 대신 **이전 정책**이 관리자에게 적용됩니다 .




3. 양방향 화살표 아이콘을 클릭하여 정책 우선 순위를 변경합니다 .

**참고 :**

- 사용자 한 명에게 특정 정책을 적용하려면 이 정책의 우선 순위가 다른 정책보다 높은지 확인하십시오 .




4. 정책 왼쪽에 마우스 커서를 올려놓고 끌어 정책을 원하는 순서에 맞게 적절한 위치에 놓습니다 .

5. 양방향 화살표 아이콘을 클릭하여 끌어서 놓기 기능을 닫고 새 우선 순위 순서를 적용합니다 .

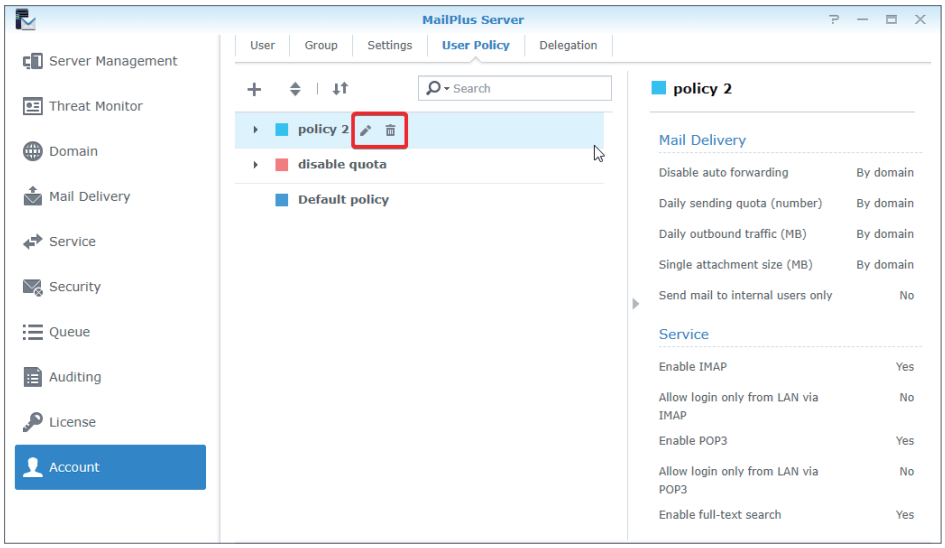
**참고 :**

- 우선 순위가 가장 낮은 정책은 항상 **기본 정책**입니다 . 자세한 내용은 **기본 정책**을 참조하십시오 .

## 사용자 정책 편집 및 삭제

정책 설정을 편집하거나 , 정책에 사용자를 추가 또는 삭제하거나 , 정책 색상을 변경할 수 있습니다 . 다음 단계를 참조하여 사용자 정책을 편집 또는 삭제하십시오 .

1. **계정** > **사용자 정책**으로 이동합니다 .
2. 편집할 정책에 마우스 커서를 올려놓습니다 . 그러면 아이콘 두 개가 나타납니다 . 연필 아이콘을 클릭하여 정책을 편집하거나 휴지통 아이콘을 클릭하여 삭제합니다 .




## 기본 정책

시스템 기본 정책은 사용자 지정 정책에 의해 규제되지 않은 사용자에게 적용됩니다 . 기본 정책은 이미 있는 정책으로 , 편집 또는 삭제하거나 우선 순위를 재지정할 수 없습니다 . 다음 기본 정책의 설정 세부 정보를 참조하십시오 .

| | |
|---|---|
| 자동 전달 비활성화 | 기본값은 **도메인별**입니다 . |
| 일일 발송 할당량 ( 숫자 ) | 기본값은 **도메인별**입니다 . |
| 일일 아웃바운드 트래픽 (MB) | 기본값은 **도메인별**입니다 . |
| 단일 첨부 파일 크기 (MB) | 기본값은 **도메인별**입니다 . |
| 내부 사용자에게만 메일 발송 | 기본값은 **아니요**입니다 . |
| IMAP 활성화 | 기본값은 **예**입니다 . |
| IMAP 를 통해 LAN 에서 로그인만 허용 | 기본값은 **아니요**입니다 . |
| POP3 활성화 | 기본값은 **예**입니다 . |
| POP3 를 통해 LAN 에서 로그인만 허용 | 기본값은 **아니요**입니다 . |
| 전체 텍스트 검색 활성화 | 기본값은 **예**입니다 . |

기본 정책은 모든 사용자에게 적용되므로 특정 제한 사항에 대한 기대치를 충족하지 못할 수 있습니다 . 특정 제한 사항이 적용되지 않도록 하려면 이러한 제한 사항을 비활성화해야 합니다 .

## 정책 정보 및 제한 사항

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 | 도메인별 |
|---|---|---|---|---|
| 01 | 자동 전달 비활성화 | 사용자는 이메일을 자동 전달할 수 없습니다 . | 사용자는 이메일을 자동 전달할 수 있습니다 . | 정책은 도메인 설정을 따릅니다 . |

**참고 :**

- 이 정책은 수동 전달에 영향을 주지 않습니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 | 도메인별 |
|---|---|---|---|---|
| 02 | 일일 발송 할당량 ( 숫자 ) | 사용자는 할당량에 의해 제한됩니다 . | 사용자는 할당량에 의해 제한되지 않습니다 . | 정책은 도메인 설정을 따릅니다 . |

**참고 :**

- 이메일 메시지가 배달되기 전에 거부되면 할당량에 계산되지 않습니다 .
- 이메일 메시지가 배달된 후 반환되면 할당량에 계산됩니다 .
- 기본 정책에 설정된 값은 **도메인** 페이지의 **사용량 제한** 탭에 있는 **일일 할당량** 섹션의 **일일 할당량** 값과 동일합니다 .
- 값이 **0** 이면 사용자에게 제한 사항이 적용되지 않습니다 .
- **메일 배달** > **일반**으로 이동하고 **SMTP 인증 활성화** 확인란을 선택해야 합니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 | 도메인별 |
|---|---|---|---|---|
| 03 | 일일 아웃바운드 트래픽 (MB) | 사용자는 아웃바운드 트래픽에 의해 제한됩니다 . | 사용자는 아웃바운드 트래픽에 의해 제한되지 않습니다 . | 정책은 도메인 설정을 따릅니다 . |

**참고 :**

- 이메일 메시지가 배달되기 전에 거부되면 할당량에 계산되지 않습니다 .
- 이메일 메시지가 배달된 후 반환되면 할당량에 계산됩니다 .
- 기본 정책에 설정된 값은 **도메인** 페이지의 **사용량 제한** 탭에 있는 **일일 할당량** 섹션의 **일일 트래픽 제한 (MB)** 값과 동일합니다 .
- 값이 **0** 이면 사용자에게 제한 사항이 적용되지 않습니다 .
- **메일 배달** > **일반**으로 이동하고 **SMTP 인증 활성화** 확인란을 선택해야 합니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 | 도메인별 |
|---|---|---|---|---|
| 04 | 단일 첨부 파일 크기 (MB) | 사용자는 첨부 파일 크기에 의해 제한됩니다 . | 사용자는 첨부 파일 크기에 의해 제한되지 않습니다 . | 정책은 도메인 설정을 따릅니다 . |

**참고 :**

- 기본 정책에 설정된 값은 **메일 배달** 페이지의 **일반** 탭에 있는 **메일당 최대 크기 (MB)** 값과 동일합니다 .
- 기본 정책에 설정된 값은 외부 이메일에 적용됩니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 |
|---|---|---|---|
| 05 | 내부 사용자에게만 메일 발송 | 사용자는 내부 사용자에게만 이메일을 보낼 수 있습니다 . | 사용자는 외부 사용자에게도 이메일을 보낼 수 있습니다 . |

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 |
|---|---|---|---|
| 06 | IMAP 활성화 | 사용자는 IMAP 를 사용할 수 있습니다 . | 사용자는 IMAP 를 사용할 수 없습니다 . |

**참고 :**

- **서비스** 페이지의 **IMAP/POP3** 섹션에서 **IMAP 활성화** 확인란을 선택하지 않으면 IMAP 서비스를 사용할 수 없으며 사용자 정책이 적용되지 않습니다 . 사용자는 사용자 정책에서 IMAP 가 활성화되더라도 IMAP 를 사용할 수 없습니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 |
|---|---|---|---|
| 07 | IMAP 를 통해 LAN 에서 로그인만 허용 | 사용자는 IMAP 를 통해 하위 도메인에서 로그인만 할 수 있습니다 . | 사용자는 MailPlus 에 로그인할 수 있습니다 . |

**참고 :**

- **서비스** 페이지의 **IMAP/POP3** 섹션에서 **IMAP 활성화** 확인란을 선택하지 않으면 IMAP 서비스를 사용할 수 없으며 사용자 정책이 적용되지 않습니다 . 사용자는 사용자 정책에서 **IMAP 를 통해 LAN 에서 로그인만 허용**이 활성화되더라도 IMAP 를 통해 로그인할 수 없습니다 .
- MailPlus 웹 클라이언트는 이 설정에 의해 제한되지 않습니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 |
|---|---|---|---|
| 08 | POP3 활성화 | 사용자는 POP3 를 사용할 수 있습니다 . | 사용자는 POP3 를 사용할 수 없습니다 . |

**참고 :**

- **서비스** 페이지의 **IMAP/POP3** 섹션에서 **POP3 활성화** 확인란을 선택하지 않으면 POP3 서비스를 사용할 수 없으며 사용자 정책이 적용되지 않습니다 . 사용자는 사용자 정책에서 POP3 가 활성화되더라도 POP3 를 사용할 수 없습니다 .

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 |
|---|---|---|---|
| 09 | POP3 를 통해 LAN 에서 로그인만 허용 | 사용자는 POP3 를 통해 하위 도메인에서 로그인만 할 수 있습니다 . | 사용자는 MailPlus 에 로그인할 수 있습니다 . |

**참고 :**

- **서비스** 페이지의 **IMAP/POP3** 섹션에서 **POP3 활성화** 확인란을 선택하지 않으면 POP3 서비스를 사용할 수 없으며 사용자 정책이 적용되지 않습니다 . 사용자는 사용자 정책에서 **POP3 를 통해 LAN 에서 로그인만 허용**이 활성화되더라도 POP3 를 통해 로그인할 수 없습니다 .
- 계속 외부 네트워크를 사용하여 MailPlus 에 로그인할 수 있습니다 . (MailPlus 는 내부 네트워크를 사용하여 메일 서버에 연결합니다 .)

| 번호 | 정책 | 정책 활성화 결과 | 정책 비활성화 결과 |
|---|---|---|---|
| 010 | 전체 텍스트 검색 활성화 | 서버에서 사용자의 이메일 콘텐츠를 인덱싱합니다 . | 서버에서 사용자의 이메일 콘텐츠를 인덱싱하지 않습니다 . |

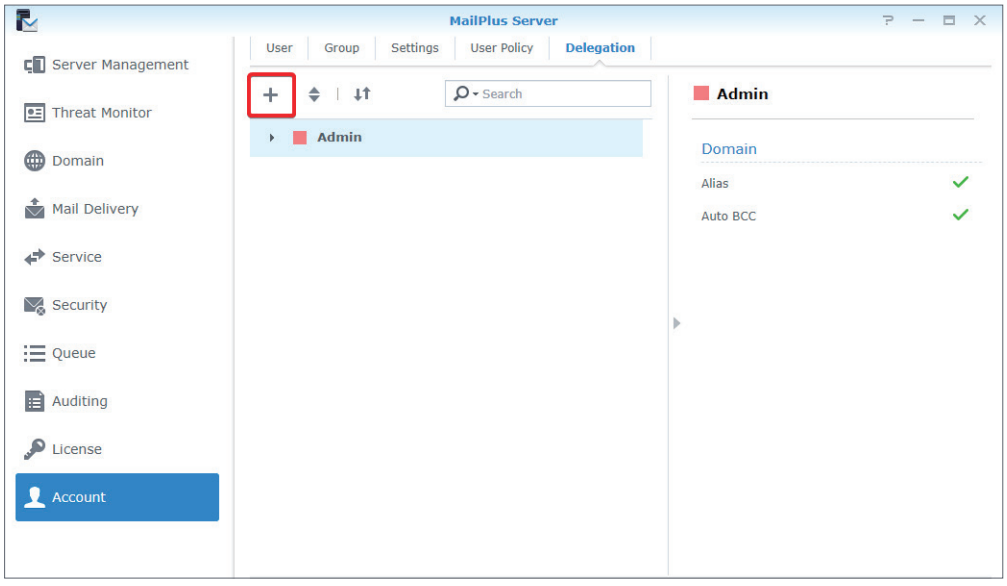
**참고 :**

- **서비스** 페이지의 **전체 텍스트 검색** 섹션에서 **전체 텍스트 검색 활성화** 확인란을 선택하지 않으면 사용자 정책이 적용되지 않으며 사용자의 이메일 콘텐츠도 인덱싱되지 않습니다 .

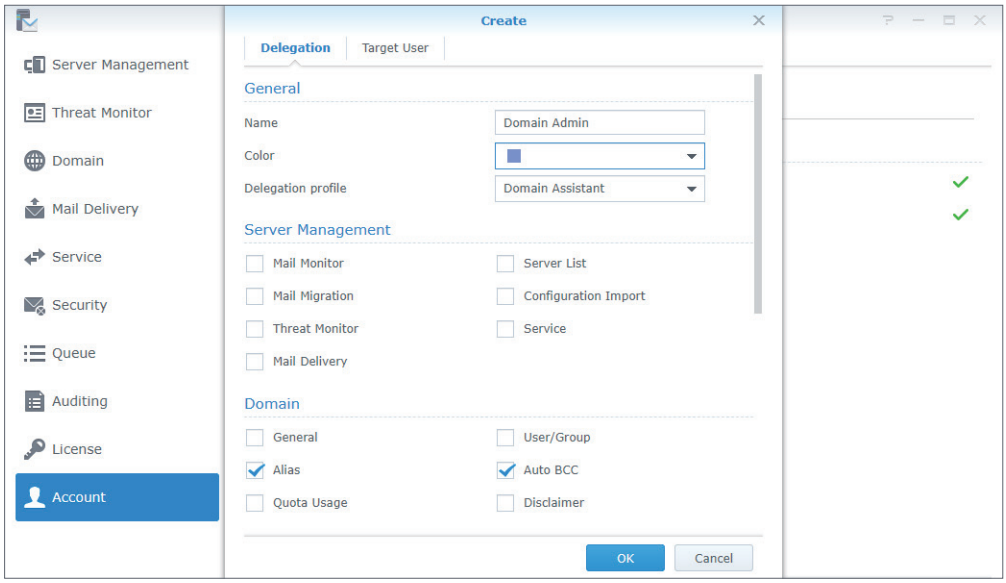
## 위임 정책 만들기

**위임** 탭에서 사용자가 할당한 위임 프로필에 따라 다른 사용자가 서버 관리 , 도메인 , 보안 , 감사 및 MailPlus Server 계정 ( 라이센스 제외 ) 과 관련된 설정을 관리하도록 위임할 수 있습니다 . 이 장에서는 설명을 위해 **도메인 관리자**를 예로 사용합니다 .

1. **계정** > **위임**으로 이동하고 상단 표시줄에 있는 더하기 아이콘을 클릭합니다 .

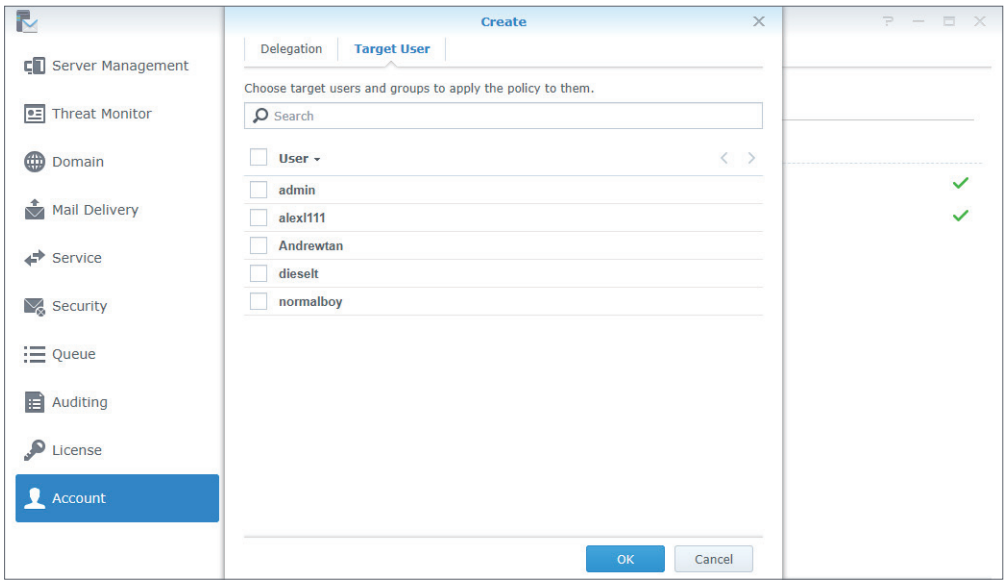



2. 팝업 창에서 **위임** 탭으로 이동하고 필요한 정보를 입력합니다 . 시스템은 선택한 위임 프로필에 따라 아래 옵션을 자동으로 선택합니다 . 아래 모든 옵션을 선택하거나 선택 취소하면 프로필은 **사용자 지정**으로 전환됩니다 . 위임된 권한에 대한 자세한 내용은 **이 문서**를 참조하십시오 .




예를 들어 도메인 관리자에 **도메인 관리자**를 선택하면 이 위임 정책에서 규제된 사용자는 기존 도메인의 모든 설정을 관리할 수 있습니다 . 그러나 도메인 관리자에 **도메인 도우미**를 선택하면 이 위임 정책이 적용되는 사용자는 도메인의 별칭과 자동 BCC 만 관리할 수 있습니다 .

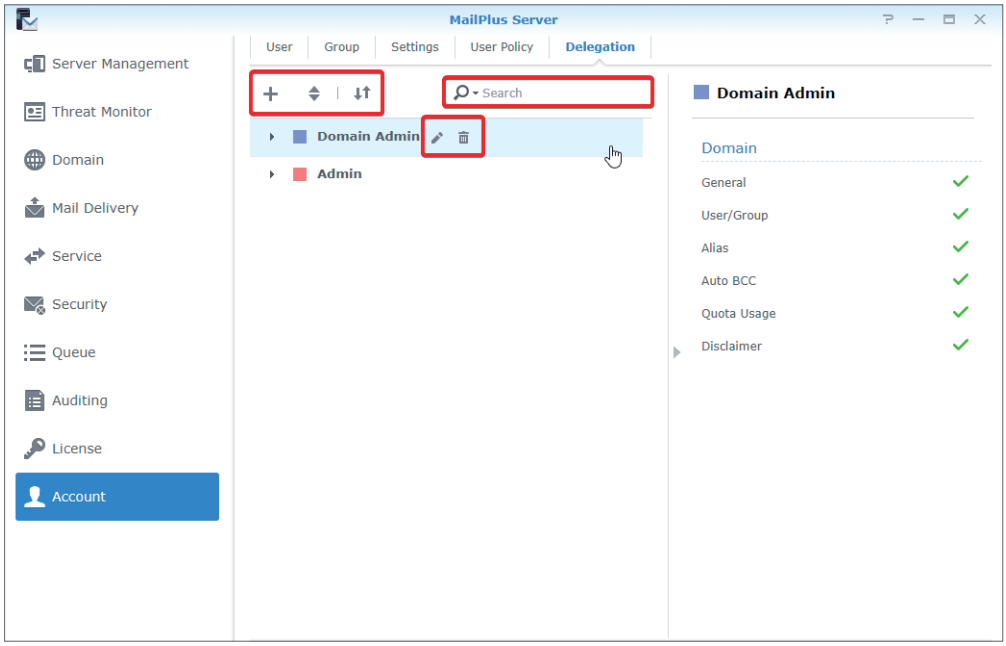
3. **대상 사용자** 탭으로 이동하여 지정된 위임 정책에 따라 규제할 사용자 / 그룹을 선택합니다 .




4. **확인**을 클릭하여 설정을 저장합니다 .

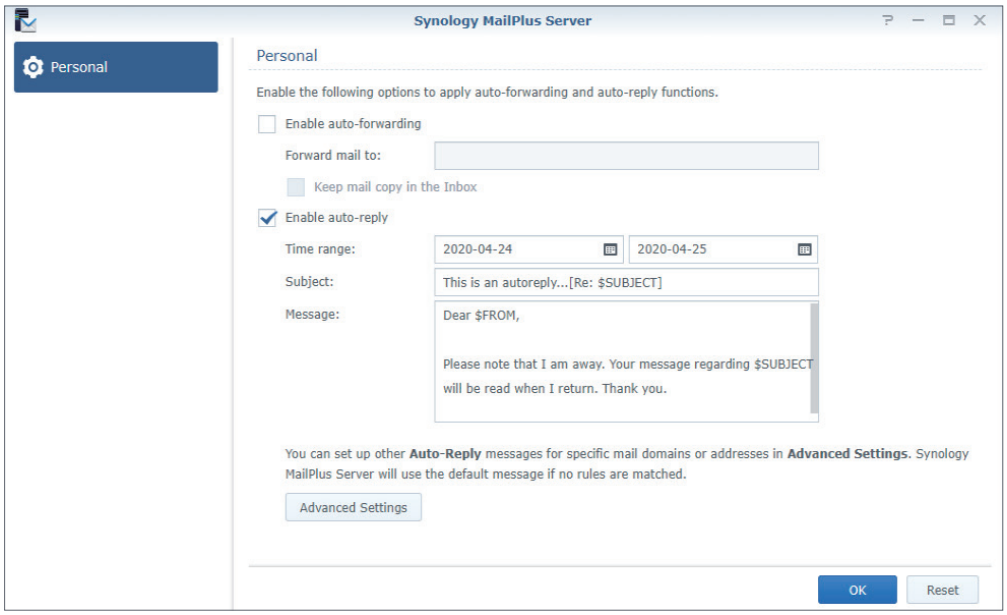
## 위임 정책 관리

1. **계정** > **위임**으로 이동합니다 .
2. 도메인 관리자를 선택하여 정책을 보고 , 편집하고 , 삭제합니다 .
3. 상단 도구 모음의 버튼과 오른쪽에 있는 미리 보기 패널을 사용하여 위임 정책을 관리할 수 있습니다 .
   - **정책 우선 순위 설정** :
     - 양방향 화살표 아이콘을 클릭하여 우선 순위를 설정합니다 .
     - 도메인 관리자를 클릭하고 정책을 끌어 적합한 위치에 놓습니다 . 사용자 / 그룹이 위임 정책 두 개 이상의 규제를 받는 경우 시스템은 목록에서 우선 순위가 가장 높은 정책을 사용자 / 그룹에 적용합니다 .
   - **위임 정책 확대 / 축소** : 이중 삼각형 아이콘을 클릭하여 대상 사용자 / 그룹을 확대하거나 축소합니다 .
   - **위임 정책 검색** : 상단 검색 창에 정책 이름이나 사용자를 입력합니다 .
   - **위임 정책 미리 보기** : 위임 정책의 이름 , 프로필 및 기타 세부 정보를 미리 봅니다 .
   - **위임 정책 편집** : 펜 아이콘을 클릭하여 정책을 편집합니다 .
   - **위임 정책 삭제** : 휴지통 아이콘을 클릭하여 정책을 삭제합니다 .



# 권한 관리

MailPlus Server 권한 설정이 DSM 설정과 동기화됩니다 . DSM 의 관리 그룹에 속하는 사용자는 모든 MailPlus Server 설정에 액세스할 수 있지만 일반 사용자는 다음 이미지와 같은 **개인** 페이지만 볼 수 있습니다 .




**참고 :**

- **제어판**에서 MailPlus Server 의 권한 설정을 기본값으로 유지해야 합니다 . MailPlus Server 에 대한 권한이 모든 사용자에게 있어야 합니다 . 그렇지 않으면 패키지 기능이 제한됩니다 .

# 6 장 : 프로토콜 설정

MailPlus Server 는 메일 서비스 프로토콜의 중앙 집중식 구성 인터페이스를 제공합니다 . 특정 프로토콜의 포트를 열거나 닫거나 서버의 네트워크 인터페이스를 다시 바인딩할 수 있습니다 . 프로토콜 설정이 전체 서버의 외부 작업에 영향을 미치므로 필요에 맞게 설정이 구성되었는지 확인하십시오 .

## SMTP

SMTP 는 포트 세 개를 사용합니다 . MailPlus Server 에서 이러한 포트는 SMTP( 포트 번호 : 25), SMTP-SSL( 포트 번호 : 465) 및 SMTP-TLS( 포트 번호 : 587) 로 표시됩니다 . 프로토콜 세 개와 해당 역할은 다음과 같습니다 .

- **SMTP**: **SMTP** 는 외부 이메일을 수신하고 내부 이메일을 배달하는 데 사용되는 표준 프로토콜입니다 . MailPlus Server 는 접미사를 사용하며 **STARTTLS** 가 지정되지 않은 경우 해밍 (hamming) 코드를 사용하여 이메일 메시지를 배달합니다 . 현재 Synology SMTP 는 암호화되어 있지 않습니다 . 암호화가 필요하면 **여기**를 참조하십시오 .
- **SMTP-SSL**: SMTPS 는 SMTP-SSL 에 지원되는 프로토콜입니다 . DSM 이 더 이상 SSL 암호화를 지원하지 않으므로 MailPlus Server 는 TLS 를 통해서만 SMTP-SSL 에 연결할 수 있습니다 .

**참고 :**

- 이는 STARTTLS 를 통해 SMTP 를 암호화하는 것과 다릅니다 . SMTP 는 핸드셰이크 후에 암호화된 패킷을 전송해야 합니다 . 이 프로토콜을 사용하여 릴레이해야 하는 경우 자세한 내용은 **여기**를 참조하십시오 .

- **SMTP-TLS**: SMTPS 는 SMTP-TLS 에 지원되는 프로토콜이며 STARTTLS 를 통해 암호화를 수행합니다 . SMTP-TLS 에는 인증이 필요하므로 주로 클라이언트와 **MSA** 간의 내부 프로토콜에 사용됩니다 .

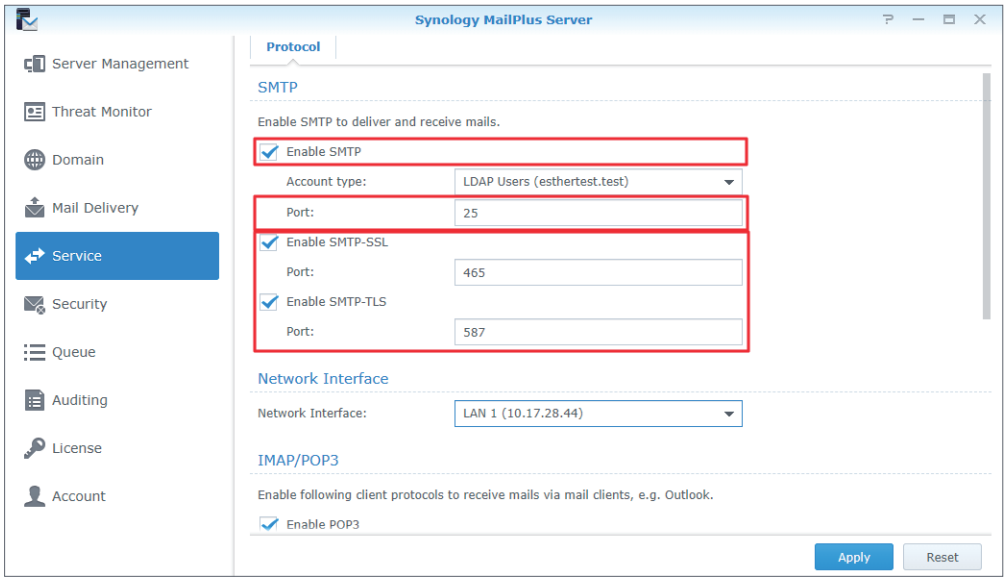
### SMTP 설정

SMTP 및 해당 포트의 구성은 다음 지침을 참조하십시오 .

1. **서비스** > **프로토콜** > **SMTP** 로 이동하고 **SMTP 활성화** 확인란을 선택합니다 .

**참고 :**

- SMTP 는 메일 서버의 기본 프로토콜입니다 .




2. **포트** 필드에서 포트 번호를 변경할 수 있습니다 .

**참고 :**

- 특별한 경우가 아니라면 기본 포트 25 를 사용하는 것이 좋습니다 .

3. 다음 설정을 조정할 수 있습니다 .
   - **SMTP-SSL 활성화** : SMTPS 를 프로토콜로 사용합니다 . **포트** 필드에서 SMTP-SSL 포트 번호를 변경할 수 있습니다 .
   - **SMTP-TLS 활성화** : 강제 연결 중에 인증 및 STARTTLS 암호화를 허용합니다 . **포트** 필드에서 SMTP-TLS 포트 번호를 변경할 수 있습니다 .
4. **적용**을 클릭하여 설정을 저장합니다 .

## IMAP/POP3

IMAP/POP3 는 암호화된 옵션과 암호화되지 않은 옵션을 모두 제공하므로 포트 4 개를 사용합니다 . MailPlus Server 에서 이러한 포트는 IMAP( 포트 번호 : 143), IMAPS( 포트 번호 : 993), POP3( 포트 번호 : 110) 및 POP3S( 포트 번호 : 995) 입니다 . 이러한 프로토콜을 통해 여러 가지 이메일 클라이언트를 사용하여 MailPlus Server 에서 이메일 정보를 검색할 수 있습니다 .

**참고 :**

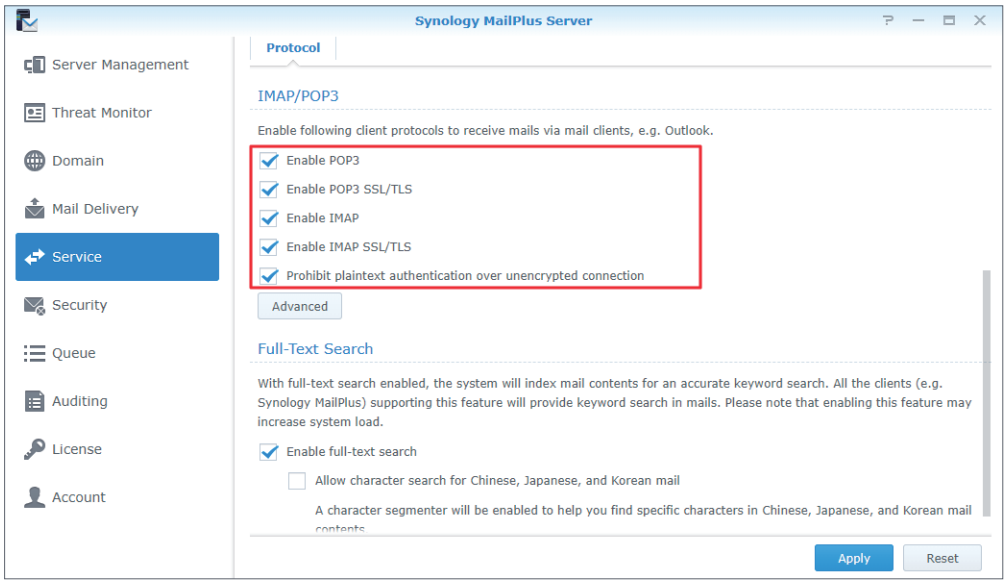
- 두 프로토콜 모두 STARTTLS 를 통해 암호화합니다 . DSM 에서는 더 이상 SSL 암호화 연결을 지원하지 않으므로 암호화 연결에 SSL 을 설정하지 마십시오 .

- **IMAP**: **IMAP** 는 사용자가 메일 서버에 저장된 데이터에 액세스할 수 있게 해주는 표준 프로토콜입니다 . IMAP 클라이언트는 메일 서버에서 이메일을 수정합니다 . 수정된 이메일은 모든 IMAP 클라이언트 사서함에 미러링되므로 이메일의 모든 변경 사항이 여러 장치에서 동기화됩니다 .
- **POP3**: **POP3** 는 사용자가 메일 서버에 저장된 데이터에 액세스할 수 있게 해주는 표준 프로토콜입니다 . POP3 클라이언트는 서버에서 이메일을 다운로드하여 로컬에 저장하므로 이메일 변경 사항이 메일 서버로 다시 동기화되지 않습니다 .

## IMAP/POP3 설정

다음 단계를 참조하여 IMAP, POP3 및 해당 포트를 구성할 수 있습니다 .

1. **서비스** > **IMAP/POP3** 로 이동합니다 .
2. **IMAP/POP3** 섹션에서 다음 설정을 조정할 수 있습니다 .
   - **POP3 활성화** : 이메일 클라이언트 소프트웨어에서 POP3 를 사용하여 메시지를 수신하도록 허용하려면 선택합니다 .
   - **POP3 SSL/TLS 활성화** : SSL/TLS 를 통해 POP3 클라이언트 연결을 보호하려면 선택합니다 .
   - **IMAP 활성화** : 이메일 클라이언트 소프트웨어에서 IMAP 를 사용하여 메시지를 수신하도록 허용하려면 선택합니다 .
   - **IMAP SSL/TLS 활성화** : SSL/TLS 로 IMAP 클라이언트 연결을 보호하려면 선택합니다 .




3. **적용**을 클릭하여 설정을 저장합니다 .

# 네트워크 인터페이스

MailPlus Server 를 설치하거나 high-availability 를 구성하면 MailPlus Server 는 **High-availability 클러스터**를 지원하도록 네트워크 인터페이스와 바인딩됩니다 . 서버에서 호스팅되는 메일 서비스는 이 네트워크 인터페이스에서 실행됩니다 .

## 네트워크 인터페이스 바인딩

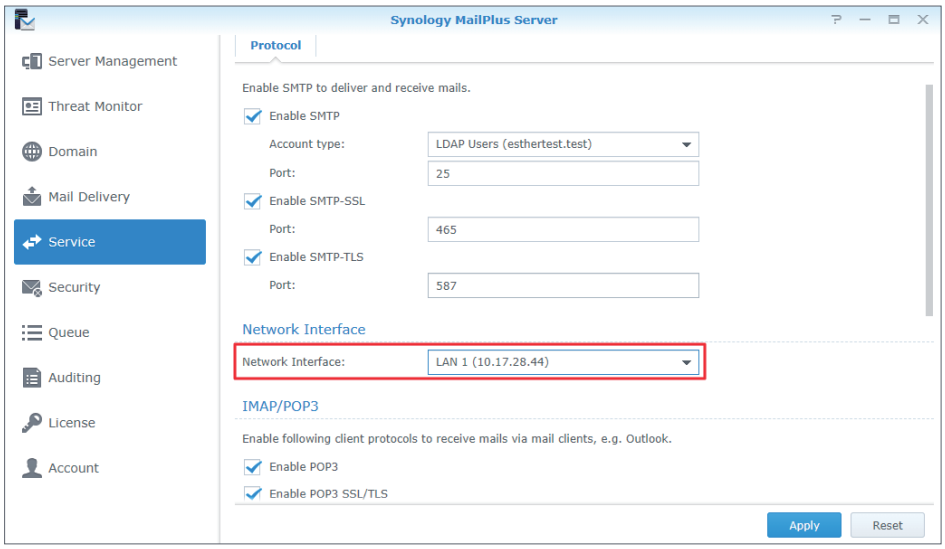
MailPlus Server 가 단일 서버에서 실행 중이면 MailPlus Server 를 LAN, PPPoE 및 연결된 네트워크 인터페이스와 바인딩할 수 있습니다 . MailPlus Server 가 고가용성 아키텍처에서 실행 중이면 MailPlus Server 를 LAN 이나 연결된 네트워크 인터페이스와 바인딩할 수 있습니다 . **수동 구성**을 사용하여 네트워크 인터페이스의 IP 주소를 검색할 수 있습니다 .

**참고 :**

- MailPlus Server 가 연결된 네트워크 인터페이스와 바인딩되면 연결된 네트워크 인터페이스를 바인딩 해제할 수 없습니다 . 연결된 네트워크 인터페이스를 바인딩 해제하려면 먼저 네트워크 인터페이스를 수정하거나 MailPlus Server 를 제거해야 합니다 .

## 네트워크 인터페이스 수정

1. DSM 에 로그인합니다 .
2. **MailPlus Server** 를 시작합니다 .
3. **서비스** > **네트워크 인터페이스**로 이동하고 **네트워크 인터페이스** 드롭다운 메뉴에서 네트워크 인터페이스를 전환합니다 .




4. **적용**을 클릭하여 설정을 저장합니다 .

설치 단계에서 기본 MailPlus Server 구성을 완료한 후에 사용자 로그인이나 인바운드 / 아웃바운드 메일 배달에 대한 SMTP 관련 제한을 설정해야 할 수 있습니다 .

# 7 장 : SMTP 설정

## 서비스 설정

**메일 배달** 페이지로 이동하여 이메일 전송 및 수신 규칙을 설정할 수 있습니다 .

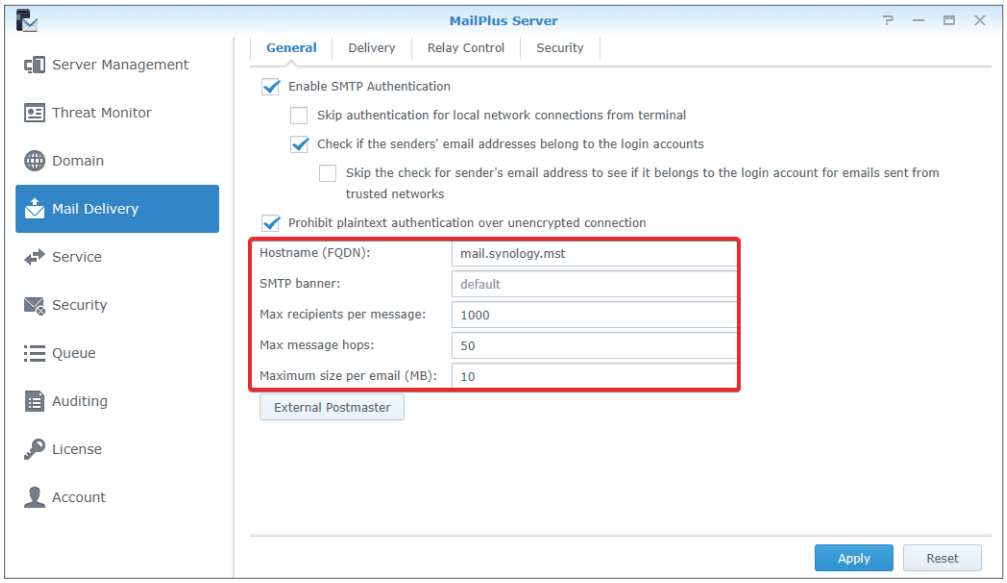
MailPlus Server 는 다음을 포함한 빠르고 편리한 서비스 설정 옵션을 제공합니다 .

- **SMTP 프로필** : 클라이언트의 Telnet 터미널에서 MailPlus Server 의 호스트 이름과 SMTP 배너를 지정할 수 있습니다 . 또한 리소스를 초과 사용하지 않도록 이메일당 최대 크기와 메시지당 최대 받는 사람 수를 지정하는 등 이메일 전송 및 수신 규칙을 설정할 수 있습니다 .
- **전체 텍스트 검색** : 전체 텍스트 검색 기능을 활성화하면 메일 검색 성능을 향상시킬 수 있습니다 . 이 기능을 사용하면 MailPlus 웹 클라이언트가 중국어 , 일본어 및 한국어 문자가 포함된 이메일을 인덱싱할 수 있습니다 . 전체 텍스트 검색 기능은 모든 이메일 콘텐츠를 인덱싱하므로 추가 컴퓨팅 리소스가 필요할 수 있습니다 . 전체 텍스트 검색 기능 활성화 여부를 결정하고 추가로 특정 사용자의 전체 텍스트 검색 기능을 비활성화할 수 있습니다 . 자세한 내용은 **사용자 정책 만들기**를 참조하십시오 .

### SMTP 프로필 설정

SMTP 프로필에는 MailPlus Server 가 다른 메일 서버로 이메일을 보내는 방법에 대한 규칙이 포함되어 있습니다 .

1. **메일 배달** > **일반**으로 이동합니다 .
   - **호스트 이름 (FQDN)**: MailPlus Server 의 호스트 이름을 FQDN 형식으로 지정합니다 . 호스트 이름은 DNS 서버의 IP 주소와 일치해야 합니다 .
   - **SMTP 배너** : SMTP 클라이언트의 Telnet 터미널에 표시될 텍스트를 지정합니다 .
   - **메시지당 최대 받는 사람 수** : 인바운드 / 아웃바운드 메시지의 최대 받는 사람 수를 설정합니다 . 제한을 초과하는 메시지는 거부됩니다 .
   - **최대 메시지 홉 수** : 인바운드 / 아웃바운드 메시지로 생성되는 최대 홉 ( 즉 , 메일 릴레이 ) 수를 설정합니다 . 제한을 초과하는 메시지는 거부됩니다 .
   - **이메일당 최대 크기 (MB)**: 인바운드 / 아웃바운드 메시지 최대 크기를 설정합니다 . 제한을 초과하는 메시지는 거부됩니다 .

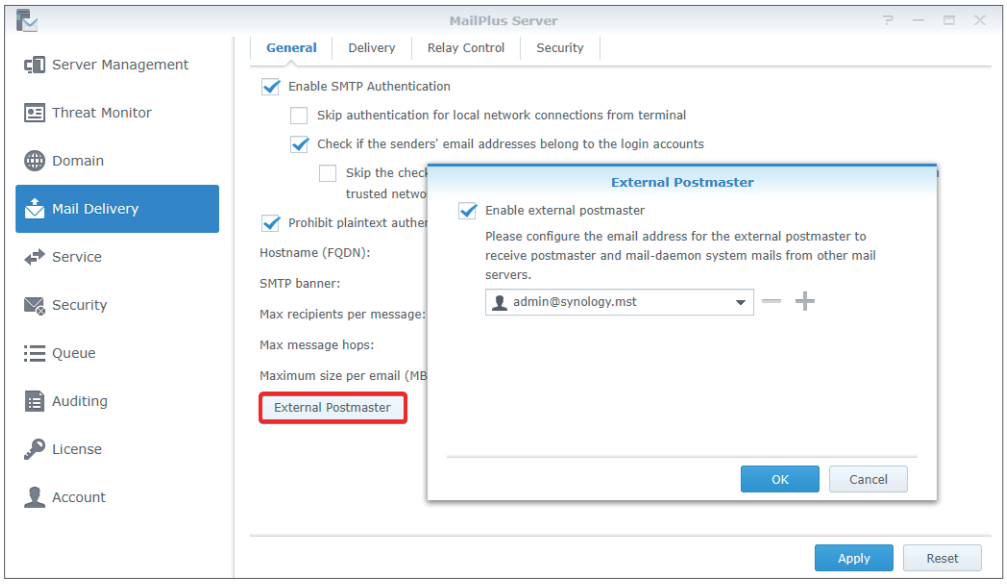



2. **적용**을 클릭하여 설정을 저장합니다 .

## 외부 전자 메일 관리자

외부 전자 메일 관리자는 Mailer-daemon 과 다른 메일 서버의 전자 메일 관리자 별칭으로 발송된 시스템 이메일을 수신할 수 있습니다 .

1. **메일 배달** > **일반**으로 이동합니다 .
2. **외부 전자 메일 관리자** 버튼을 클릭합니다 .
3. **외부 전자 메일 관리자 활성화** 확인란을 선택합니다 .
4. 더하기 아이콘 / **추가** 버튼을 클릭하여 외부 전자 메일 관리자의 이메일 주소를 추가합니다 .



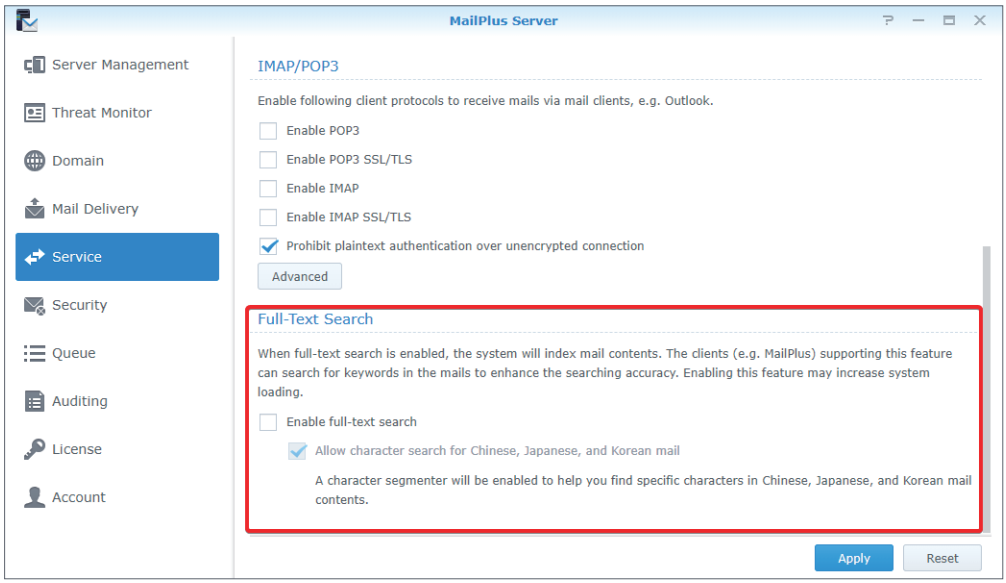

5. **확인**을 클릭하여 설정을 저장합니다 .

### 전체 텍스트 검색

전체 텍스트 검색 기능이 활성화되면 서버는 이메일 제목 줄 , 보낸 사람 , 받는 사람 및 메시지 콘텐츠를 인덱싱합니다 . 이를 통해 사용자와 클라이언트 사용자는 이 기능을 지원하는 클라이언트 ( 예 : MailPlus) 에서 키워드를 편리하게 검색할 수 있습니다 .

> **참고 :**
>
> - 이 기능을 활성화할 때 아웃바운드 및 인바운드 메시지가 많이 있으면 시스템 로드가 증가할 수 있습니다 .

1. **서비스**로 이동합니다 .
2. **전체 텍스트 검색** 섹션에서 다음 설정을 조정할 수 있습니다 .
   - **전체 텍스트 검색 활성화** : 이 옵션을 선택한 경우 자세한 내용은 **사용자 정책 만들기**를 참조하십시오 . 서버 로드를 방지하기 위해 특정 사용자의 전체 텍스트 검색 기능을 비활성화할 수 있습니다 .
   - **중국어 , 일본어 및 한국어 메일에 문자 검색 허용** : 이 옵션을 선택하면 중국어 , 일본어 및 한국어 메일 콘텐츠에서 특정 문자를 찾을 수 있도록 문자 세그멘터가 활성화됩니다 .




3. **적용**을 클릭하여 설정을 저장합니다 .

## SMTP 보안 연결

MailPlus Server 는 사용자 연결 , 로그인 정보 및 이메일 콘텐츠를 분석하여 보안과 안정성을 강화할 수 있습니다 . 이렇게 하면 서비스 품질을 보호할 뿐만 아니라 MailPlus Server 가 스패머용 오픈 릴레이가 되어 블랙리스트에 포함되는 것을 방지할 수 있습니다 .

- **SMTP 인증** : SMTP 인증을 활성화한 경우 사용자가 서버를 통해 이메일을 릴레이하면 인증에 필요한 DSM 사용자 계정과 패스워드를 입력해야 합니다 .

**참고 :**

- 인증은 이메일 릴레이에만 필요합니다 . 이는 스패머용 오픈 릴레이가 되지 않도록 하기 위함입니다 . 자세한 내용은 **이 문서**를 참조하십시오 .

- **블랙리스트 및 화이트리스트** : 서버에서 스팸 이메일을 계속 수신하는 경우 블랙리스트 규칙을 설정하여 특정 소스 이메일에 대한 서비스를 거부할 수 있습니다 . 반면 **안티 바이러스 검사** , **인증** 또는 기타 검사 기능이 활성화된 경우 MailPlus Server 에서우발적으로 합법적인 이메일을 거부할 수 있습니다 . 이 경우 중요한 이메일을 수신할 수 있도록 화이트리스트를 사용하여 보안 검사를 건너뛸 수 있습니다 .
- **발신자 정책** : 정규화되지 않은 형식이나 인증되지 않은 보낸 사람 주소를 거부하도록 기준을 설정할 수 있습니다 .
- **연결 정책** : 식별할 수 없거나 MailPlus Server 에 과부하를 일으킬 수 있는 클라이언트 IP 의 연결을 제한할 수 있습니다 .
- **고급 설정** : 연결 단계 중에는 정확한 명령과 기타 고급 설정이 필요합니다 . 자세한 내용은 **고급 설정**을 참조하십시오 .

## SMTP 인증 활성화

인증은 악의적인 사용자가 메일 서버를 통해 스팸을 릴레이하는 것을 방지합니다 . 사용자 인증 기능을 활성화하는 것이 좋습니다 . 인증을 통과하지 못한 사용자는 이메일을 전달할 수 없습니다 . 이렇게 하면 서버가 블랙리스트에 나열되지 않습니다 .

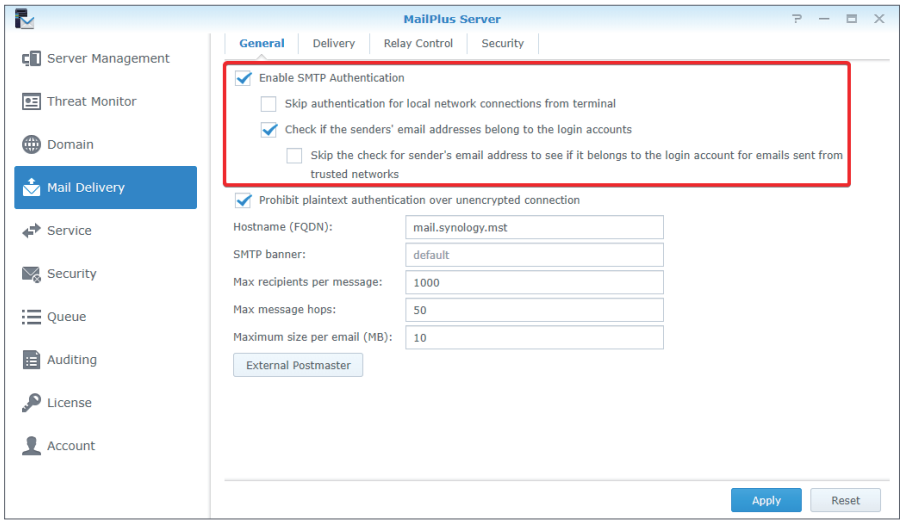
**참고 :**

- **일일 할당량**과 같은 MailPlus Server 의 일부 기능에는 인증이 필요합니다 .

1. **메일 배달** > **일반**으로 이동하고 **SMTP 인증 활성화** 확인란을 선택할지 여부를 선택합니다 .
2. **SMTP 인증 활성화** 확인란을 선택하면 다음 설정을 조정할 수 있습니다 .
   - **터미널에서 로컬 네트워크 연결을 위한 인증 건너뛰기** : 로컬 네트워크를 사용하여 메일 서비스에 액세스하는 사용자에게는 인증이 필요하지 않습니다 .
   - **보낸 사람 이메일 주소가 로그인 계정에 속하는지 확인** : 사용자는 이메일을 보내려면 로그인 계정에 속한 이메일 주소를 사용해야 합니다 .

**참고 :**

- **일반** 탭에서 **보낸 사람 이메일 주소가 로그인 계정에 속하는지 확인** 확인란을 선택하면 **신뢰할 수 있는 목록**에 있는 이메일이 MailPlus Server 에서 거부될 수 있습니다 . **일반** 탭으로 이동하고 **신뢰할 수 있는 네트워크에서 발송된 이메일의 로그인 계정에 속하는지 확인하기 위해 보낸 사람 이메일 주소 확인 건너뛰기** 확인란을 선택하면 확인을 건너뛸 수 있습니다 . **일반** 탭에서 **터미널에서 로컬 네트워크 연결 인증 건너뛰기** 확인란을 선택하면 로컬 네트워크에서 발송된 이메일은 MailPlus Server 에서 차단되지 않습니다 .




3. **적용**을 클릭하여 설정을 저장합니다 .

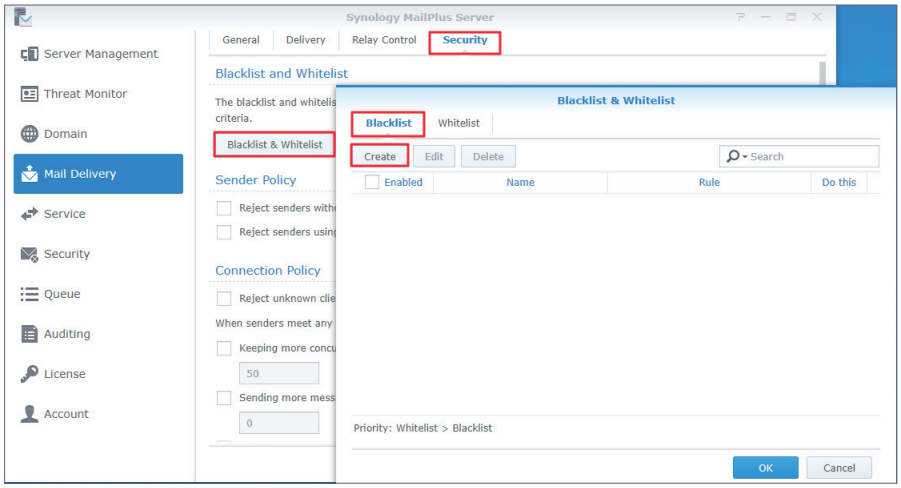
## 블랙리스트 및 화이트리스트 만들기

시스템은 **블랙리스트 및 화이트리스트**에서 지정된 다양한 기준에 따라 특정 메시지에 특정 작업을 수행합니다 . 다음 단계를 참조하여 블랙리스트와 화이트리스트의 규칙을 만들 수 있습니다 .

**참고 :**

- 이메일 메시지가 블랙리스트와 화이트리스트에 설정된 모든 기준과 일치하면 화이트리스트가 블랙리스트보다 우선시되므로 이 이메일이 수신됩니다 . **화이트리스트 정보 및 제한 사항** 섹션을 참조하십시오 .

1. **메일 배달** > **보안**으로 이동하고 **블랙리스트 및 화이트리스트**를 클릭합니다 .
2. **블랙리스트 및 화이트리스트** 창에서 블랙리스트와 화이트리스트를 관리할 수 있습니다 . 이 섹션에서는 **블랙리스트**를 사용하여 설명합니다 .
   - **블랙 리스트** : 일치하는 이메일 메시지를 거부 / 폐기하는 규칙을 설정합니다 .
   - **화이트 리스트** : 일치하는 이메일 메시지를 전달할 수 있도록 규칙을 설정합니다 .
3. **블랙리스트** 탭에서 **생성**을 클릭합니다 .



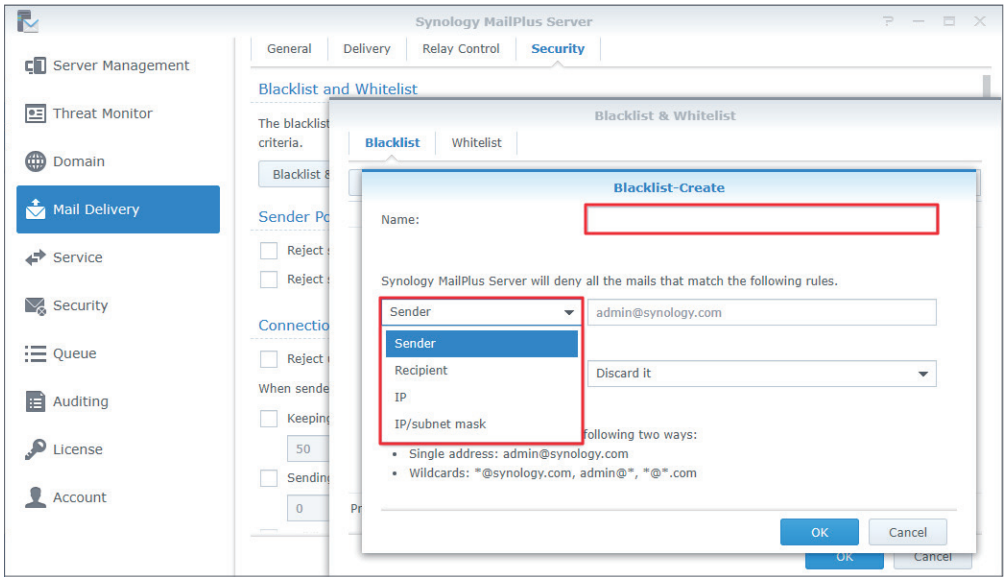

4. **이름** 필드에 블랙리스트 ( 화이트리스트 ) 규칙 이름을 지정합니다 .

5. 규칙 유형을 선택합니다 .

- **보낸 사람** : 보낸 사람 주소가 지정된 기준과 일치하면 특정 작업을 수행합니다 .
- **받는 사람** : 받는 사람 주소가 지정된 기준과 일치하면 특정 작업을 수행합니다 .
- **IP**: 보낸 사람 IP 주소가 지정된 기준과 일치하면 특정 작업을 수행합니다 .
- **IP/ 서브넷 마스크** : 보낸 사람 IP 주소와 서브넷 마스크가 지정된 기준과 일치하면 특정 작업을 수행합니다 .
- **도메인** : 보낸 사람 도메인이 지정된 기준과 일치하면 특정 작업을 수행합니다 . **화이트리스트**에서만 이 옵션을 사용할 수 있습니다 .

**참고 :**

- **보낸 사람** 주소는 **MAIL FROM** 에서 검색된 정보로 확인됩니다 .
- **받는 사람** 주소는 **RCPT TO** 에서 검색된 정보로 확인됩니다 .



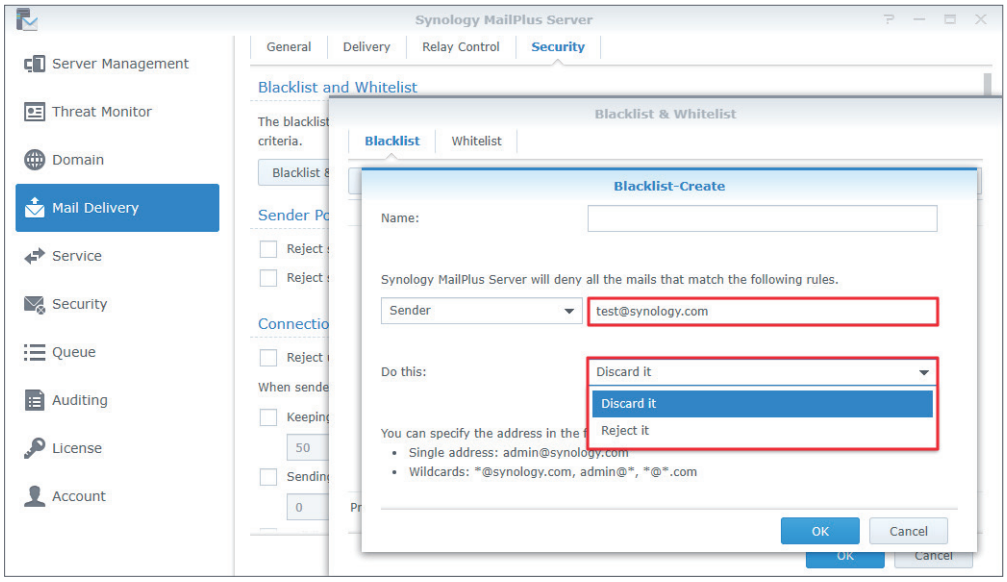

6. 선택한 규칙 유형의 조건을 지정합니다 . 올바른 형식은 입력 필드의 회색 텍스트를 참조하십시오 . 보낸 사람 또는 받는 사람 조건을 지정할 때 별표 (*) 를 입력할 수 있습니다 .

7. **수행** 드롭다운 메뉴에서 조건이 일치할 때 수행할 작업을 선택합니다 .

**참고 :**

- **화이트리스트**에는 이 옵션이 포함되어 있지 않습니다 . 항상 기준과 일치하는 이메일을 수신할 수 있기 때문입니다 .

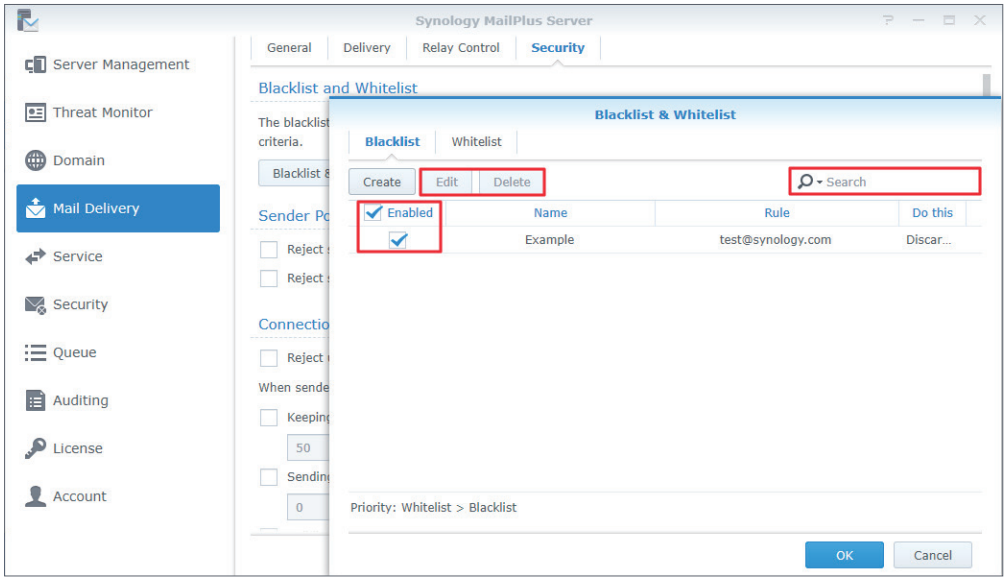
- **거부** : 이메일이 거부되면 보낸 사람에게 알림이 발송됩니다 .
- **폐기** : 이메일이 삭제되면 보낸 사람에게 알림이 발송되지 않습니다 .




8. **확인**을 클릭하여 설정을 완료합니다 .

## 블랙리스트와 화이트리스트 편집 및 삭제

1. **블랙 및 화이트 리스트** 창 오른쪽 위 구석에 있는 검색 필드에 키워드를 입력하여 수정하려는 블랙리스트 또는 화이트리스트를 검색할 수 있습니다 .
2. **활성화** 확인란을 선택하여 규칙을 활성화하거나 비활성화할 수 있습니다 . 블랙리스트 또는 화이트리스트에서 규칙을 삭제할 필요는 없습니다 .
3. 특정 규칙을 편집 또는 삭제해야 하는 경우 먼저 규칙을 선택하고 **편집** 또는 **삭제**를 클릭합니다 .
4. **확인**을 클릭하여 설정을 저장합니다 .



## 화이트리스트 정보 및 제한 사항

화이트리스트 설정에서는 블랙리스트에 필요한 테스트를 건너뛸 수 있습니다 . 또한 설정 유형에 따라 DNSBL, SPF, 안티 바이러스 검사 , DKIM 및 DMARC 테스트도 건너뛸 수 있습니다 . 다음 표에서는 여러 가지 화이트 리스트 설정을 기준으로 건너뛸 테스트를 보여줍니다 .

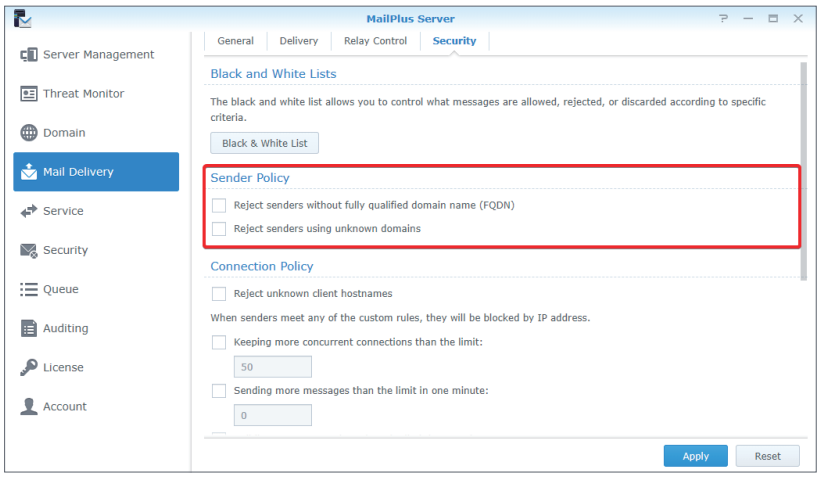
| | DNSBL | SPF | 안티 바이러스 검사 | DKIM | DMARC | smtpd_*_restrictions |
|---|---|---|---|---|---|---|
| **IP** | v | v | v | v | v | v |
| **IP/ 서브넷 마스크** | v | v | | v | v | v |
| **보낸 사람** | | v | v | | | v |
| **받는 사람** | | v | v | | | v |
| **도메인** | | v | v | v | v | v |

**참고 :**

- 화이트리스트에는 건너뛰지 않는 특정 테스트가 있으며 이러한 테스트를 통과하지 못한 이메일은 배달되지 않습니다 . 예를 들어 보낸 사람 **admin@example.com** 이 화이트리스트에 있으면 배달 실패를 방지하기 위해 DNSBL, DKIM 또는 DMARC 테스트를 통과해야 합니다 . 보낸 사람 규칙은 DNSBL, DKIM 및 DMARC 를 지원하지 않기 때문입니다 .
- 표에 나열된 모든 테스트를 건너뛰려면 IP 주소를 기준으로 화이트리스트 규칙을 설정하는 것이 좋습니다 .

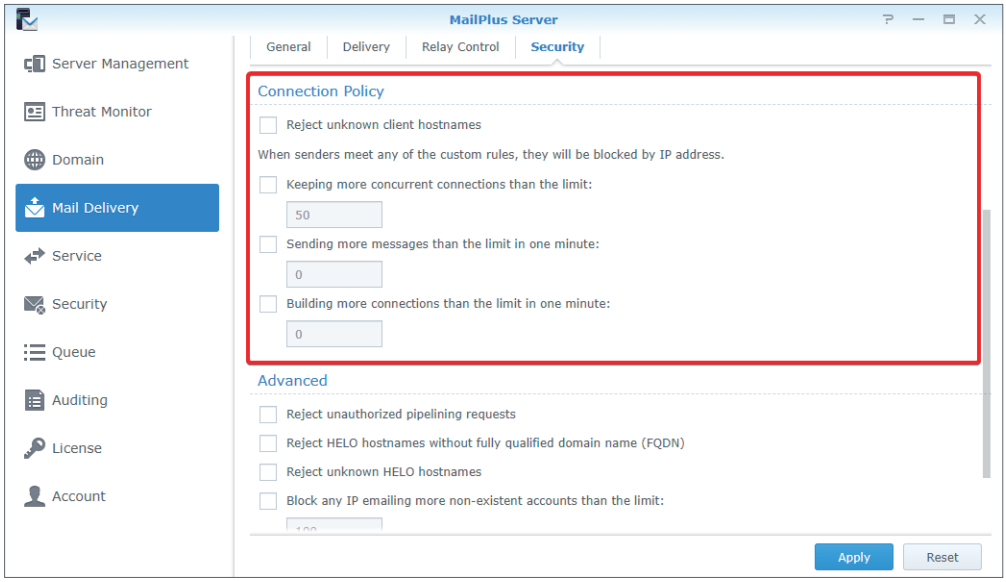
## 발신자 정책

1. **메일 배달** > **보안**으로 이동합니다 .
2. **발신자 정책** 섹션에서 이메일을 거부할 특정 기준을 설정합니다 . 정책에는 다음이 포함됩니다 .
   - **FQDN( 정규화된 도메인 이름 ) 이 없는 보낸 사람 거부** : **MAIL FROM** 의 보낸 사람 도메인 이름이 RFC 표준 FQDN 형식과 일치하지 않으면 이메일이 거부됩니다 .
   - **알 수 없는 도메인을 사용하여 보낸 사람 거부** : MailPlus Server 가 최종 수신 터미널이 아니며 **MAIL FROM** 의 보낸 사람 도메인이 DNS A 레코드와 MX 레코드와 일치하지 않거나 MX 레코드가 잘못되면 이메일이 거부됩니다 .



## 연결 정책

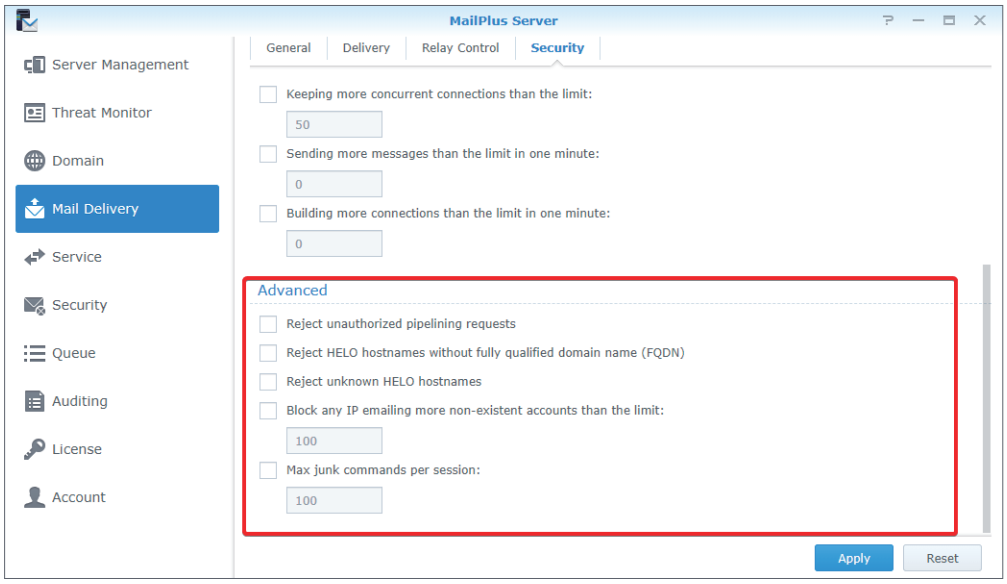
1. **메일 배달** > **보안**으로 이동합니다 .
2. **연결 정책** 섹션에서 클라이언트 연결을 제한하거나 의심스러운 IP 주소를 차단하도록 기준을 설정합니다 . 정책에는 다음이 포함됩니다 .
   - **알 수 없는 클라이언트 호스트 이름 거부** : IP 주소나 클라이언트 호스트 이름이 잘못되었거나 없으면 MailPlus Server 에 대한 클라이언트 연결이 거부됩니다 .
   - **제한보다 많은 동시 연결 유지** : 서버의 최대 동시 연결을 설정할 수 있습니다 . 동일한 IP 주소를 사용하는 동시 연결 수가 이 수를 초과하면 총 수가 제한보다 낮아질 때까지 연결이 차단됩니다 .
   - **1 분 내에 제한보다 많은 메시지 발송** : 1 분 이내에 보낼 수 있는 최대 이메일 메시지 수를 설정할 수 있습니다 . 동일한 IP 주소에서 1 분 이내에 보낸 이메일 수가 이 수를 초과하면 다음 분이 시작될 때까지 이 IP 주소의 이메일이 차단됩니다 .
   - **1 분 내에 제한보다 많은 연결 구축** : 1 분 내 최대 연결 수를 설정할 수 있습니다 . 동일한 IP 주소를 사용하는 연결 수가 1 분 이내에 이 수를 초과하면 다음 분이 시작될 때까지 연결이 차단됩니다 .




## 고급 설정

1. **메일 배달** > **보안**으로 이동합니다 .
2. **고급** 섹션에서 메일 배달 보안 설정을 조정할 수 있습니다 .
   - **미승인 파이프라이닝 요청 거부** : SMTP 요청을 계속 보내는 연결을 거부합니다 .
   - **FQDN( 정규화된 도메인 이름 ) 이 없는 HELO 호스트 이름 거부** : HELO 또는 EHLO 중에 호스트 이름에 불완전한 도메인 이름이 있으면 연결을 거부합니다 .
   - **알 수 없는 HELO 호스트 이름 거부** : HELO 또는 EHLO 중에 호스트 이름에 DNS A 레코드 또는 MX 레코드가 없으면 연결을 거부합니다 .

- **제한보다 많은 존재하지 않은 계정 IP 이메일 보내기 차단** : 같은 날 동일한 IP 주소를 사용하는 사용자가 지정된 제한을 초과하여 존재하지 않는 MailPlus Server 계정으로 이메일을 보내면 다음 날까지 사용자의 IP 주소가 차단됩니다 .
- **세션당 최대 정크 명령 수** : 연결된 클라이언트 수가 동일한 세션 내에서 지정된 정크 명령 ( 즉 , NOOP, VRFY, ETRN 및 RSET) 수를 초과하면 정크 명령 10 개마다 메일 배달이 1 초씩 지연됩니다 .



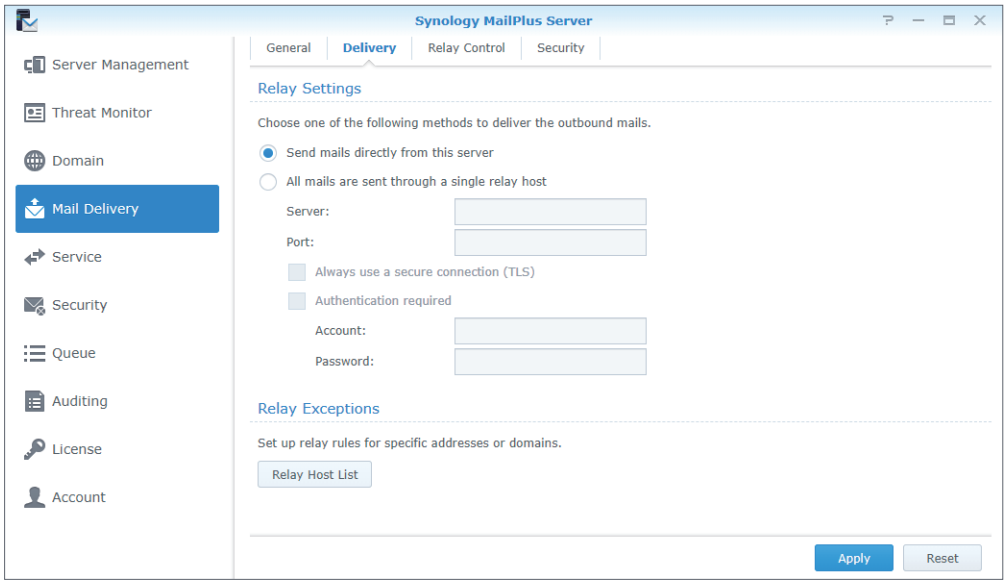

# 메일 릴레이

다른 서버를 통해 이메일을 보내거나 다른 서버의 이메일을 전송 / 수신하려면 메일 릴레이 , SMTP 인증 , 암호화 및 기타 제공된 보안 기능을 구성하면 됩니다 .

## 배달 제어 설정

**배달** 탭에서 MailPlus Server 설정을 구성하여 특정 서버를 통해 이메일을 릴레이할 수 있으므로 , 지정된 서버를 통해 모든 발신 이메일을 보낼 수 있습니다 .

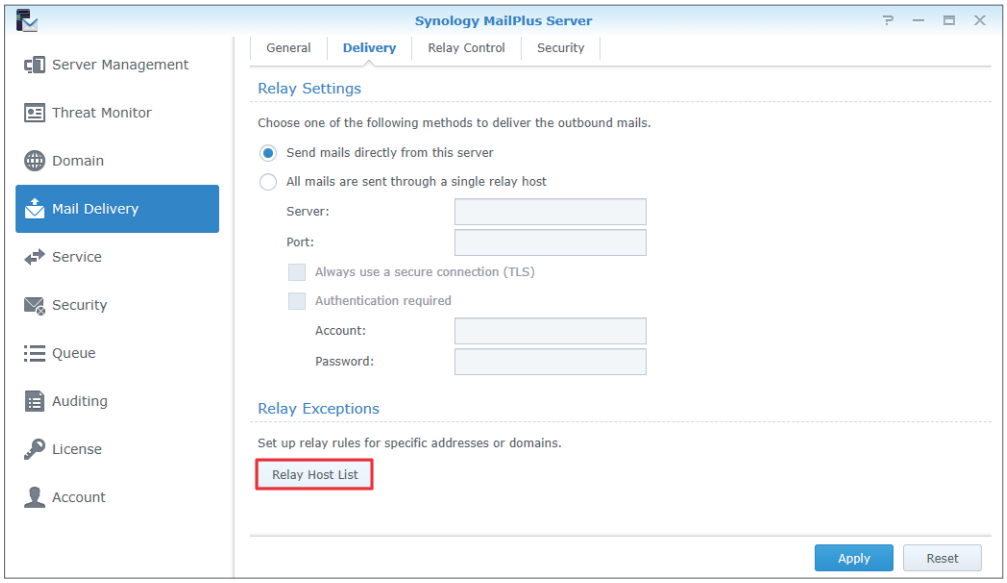
1. **메일 배달** > **배달** > **릴레이 설정**으로 이동합니다 .
2. 규칙 유형을 선택합니다 .
   - **이 서버에서 직접 메일 보내기** : 모든 이메일은 MailPlus Server 에서 직접 발송됩니다 .
   - **모든 메일은 단일 릴레이 규칙을 통해 발송됨** : 모든 이메일은 아래에 지정한 릴레이 서버에서 전송됩니다 . **서버** 필드에 릴레이 서버의 IP 주소나 호스트 이름을 , **포트** 필드에 포트 번호를 입력합니다 . 이 옵션을 선택하면 다음 보안 설정을 조정할 수 있습니다 .
     - **항상 보안 연결 사용 (TLS)**: MailPlus Server 는 STARTTLS 를 전송하여 암호화된 연결을 활성화합니다 . MailPlus Server 가 릴레이 서버이면 **여기**를 참조하십시오 . MailPlus Server 에서 기본 TLS 보안 수준은 **일 수 있음**입니다 .
     - **인증 필요** : 릴레이 서버에 활성화된 인증이 있으면 메일 릴레이에 사용할 릴레이 서버의 계정과 패스워드를 입력하십시오 .




**참고 :**

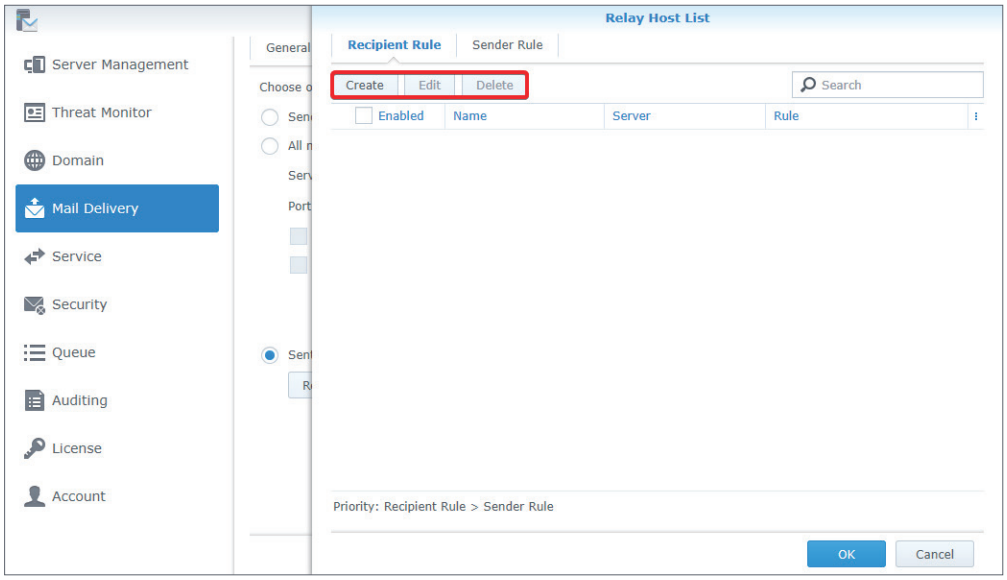
- STARTTLS 와 SMTPS 는 다릅니다 . SMTPS 를 사용하려는 경우 MailPlus Server 는 이를 구성하기 위한 인터페이스를 제공하지 않습니다 . **wrappermode** 를 참조하여 설정을 구성하십시오 .

특정 규칙과 일치하는 이메일 , 특정 이메일 주소 또는 도메인을 지정된 릴레이 서버를 통해 전송할 수 있습니다 . **릴레이 예외**에서 **릴레이 호스트 목록** 버튼을 클릭하면 받는 사람 규칙과 보낸 사람 규칙을 조정할 수 있습니다 .




- **받는 사람 규칙** : 지정된 이메일 주소 또는 도메인으로 발송된 이메일은 지정된 릴레이 서버를 통해 발송됩니다 . 받는 사람 규칙이 보낸 사람 규칙 보다 우선 적용됩니다 .
- **보낸 사람 규칙** : 지정된 주소 또는 도메인에서 발송된 이메일은 지정된 릴레이 서버를 통해 발송됩니다 .

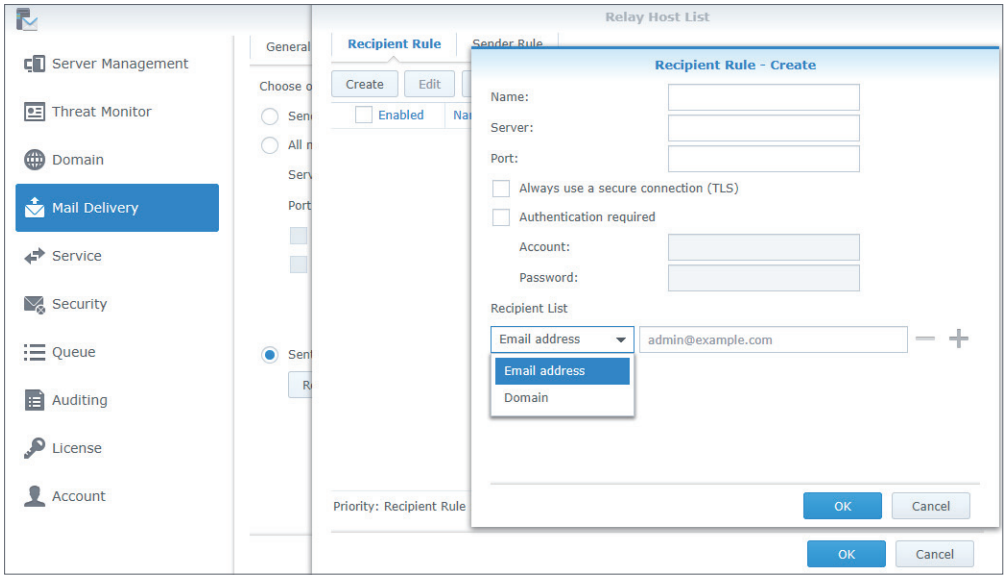
  a. **생성** , **편집** 또는 **삭제** 버튼을 클릭하여 받는 사람과 보낸 사람 규칙을 관리합니다 .




b. 규칙 이름을 입력하고 릴레이 서버와 포트를 지정합니다 .

c. 서버에 릴레이된 이메일이 지정된 이메일 주소 또는 도메인에서 수신되도록 이메일 주소 또는 도메인을 선택하여 **받는 사람 목록**을 편집합니다 .

d. **확인**을 클릭하여 설정을 저장합니다 .



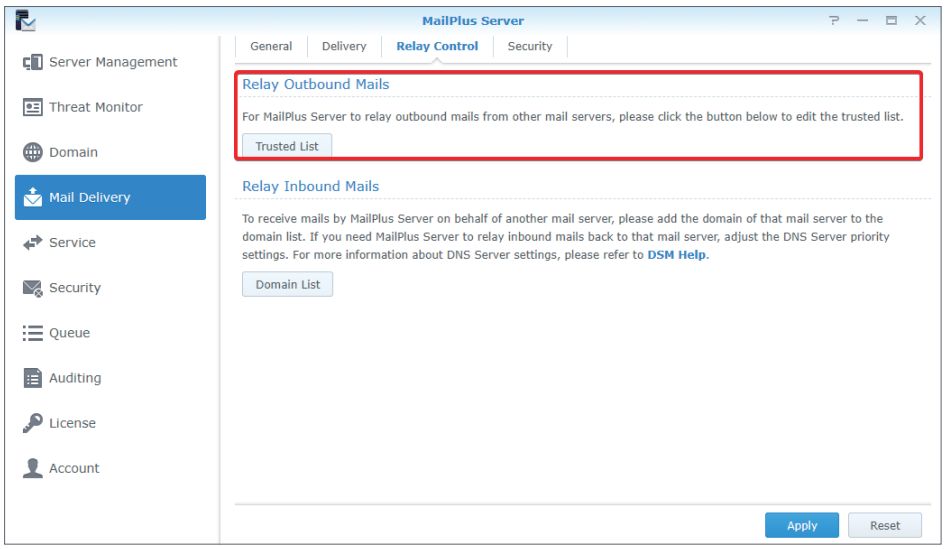

e. **적용**을 클릭하여 설정을 마칩니다 .

## 릴레이 제어 설정

**릴레이 제어** 탭에서 MailPlus Server 설정을 조정하면 메일 서버 여러 개의 이메일을 보내거나 받을 수 있습니다 .

- **다른 메일 서버의 아웃바운드 메일 릴레이** :

  1. **메일 배달** > **릴레이 제어**로 이동합니다 .
  2. **릴레이 아웃바운드 메일** 섹션에서 **신뢰할 수 있는 목록** 버튼을 클릭합니다 .




  3. **생성**을 클릭하고 규칙 이름을 입력합니다 . 다른 메일 서버의 IP 주소 또는 서브넷 마스크를 지정합니다 .
  4. **확인**을 클릭하여 설정을 저장합니다 .

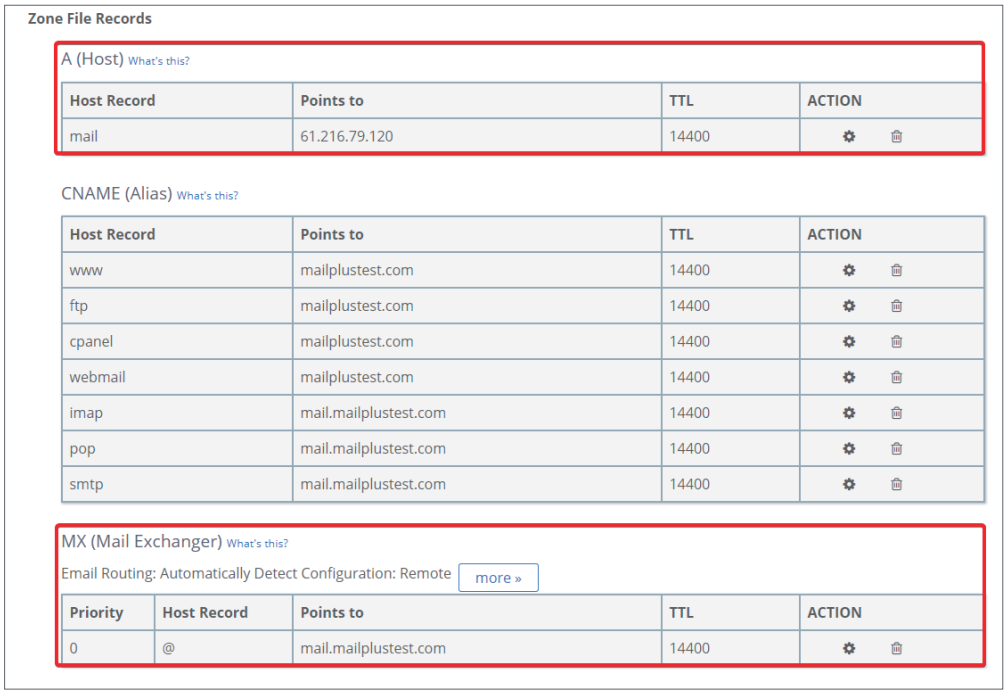
**참고 :**

- **일반** 탭에서 **보낸 사람 이메일 주소가 로그인 계정에 속하는지 확인** 확인란을 선택하면 **신뢰할 수 있는 목록**에 있는 이메일이 MailPlus Server 에서 거부될 수 있습니다 . **일반** 탭으로 이동하고 **신뢰할 수 있는 네트워크에서 발송된 이메일의 로그인 계정에 속하는지 확인하기 위해 보낸 사람 이메일 주소 확인 건너뛰기** 확인란을 선택하면 확인을 건너뛸 수 있습니다 . **일반** 탭에서 **터미널에서 로컬 네트워크 연결 인증 건너뛰기** 확인란을 선택하면 로컬 네트워크에서 발송된 이메일은 MailPlus Server 에서 차단되지 않습니다 .

## 다른 메일 서버의 인바운드 메일 릴레이

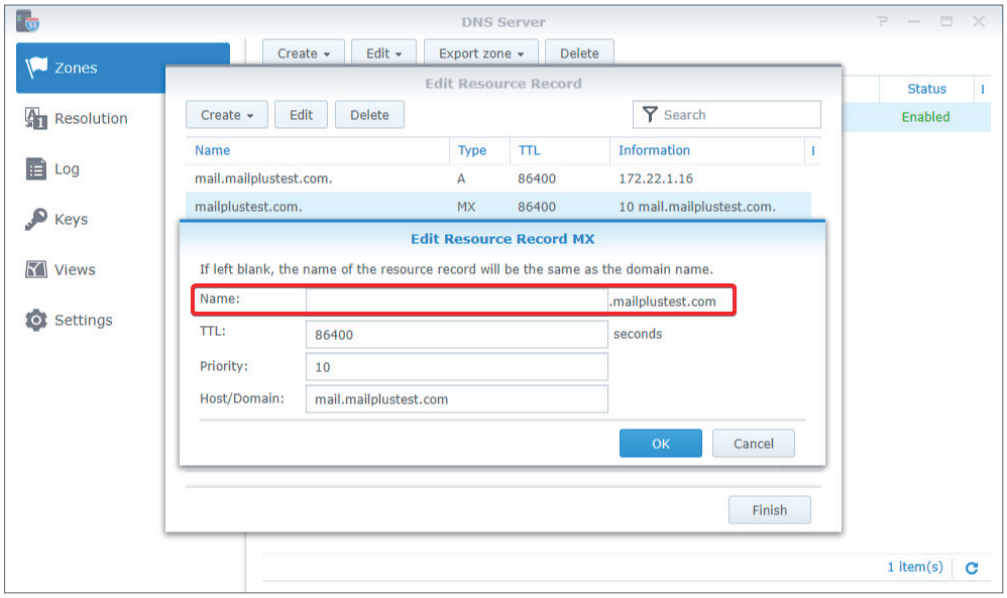
다른 메일 서버의 인바운드 이메일을 릴레이하려면 먼저 DNS 레코드를 설정하십시오 . 다음 단계를 참조하고 **도메인 목록**으로 이동하여 메일 서버를 추가할 수 있습니다 . 여기서는 외부 서버와 내부 서버 각각 한 개를 예로 사용합니다 .

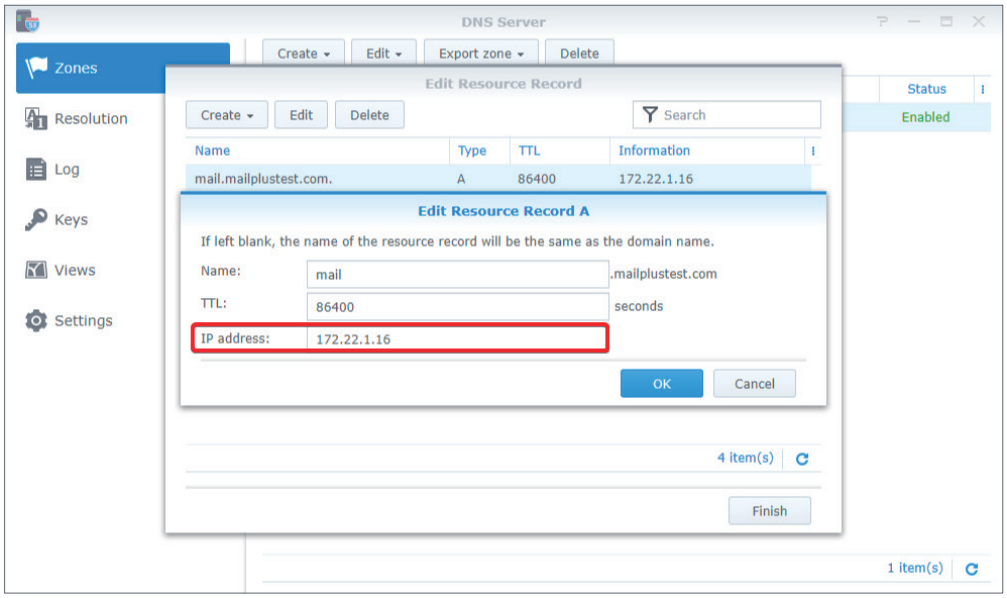
1. MailPlus Server 용 외부 DNS 서버를 설정합니다 . 여기서는 예로 Bluehost® 를 사용합니다 .
2. Bluehost® 에 로그인한 후 다음 설정을 조정합니다 . 외부 DNS 서버의 MX 레코드에 도메인 이름을 입력하고 A 레코드에 MailPlus Server 의 IP 주소를 입력합니다 . 이러한 방식으로 다른 메일 서버가 해당 DNS 레코드를 기준으로 MailPlus Server 로 이메일을 보낼 수 있습니다 .



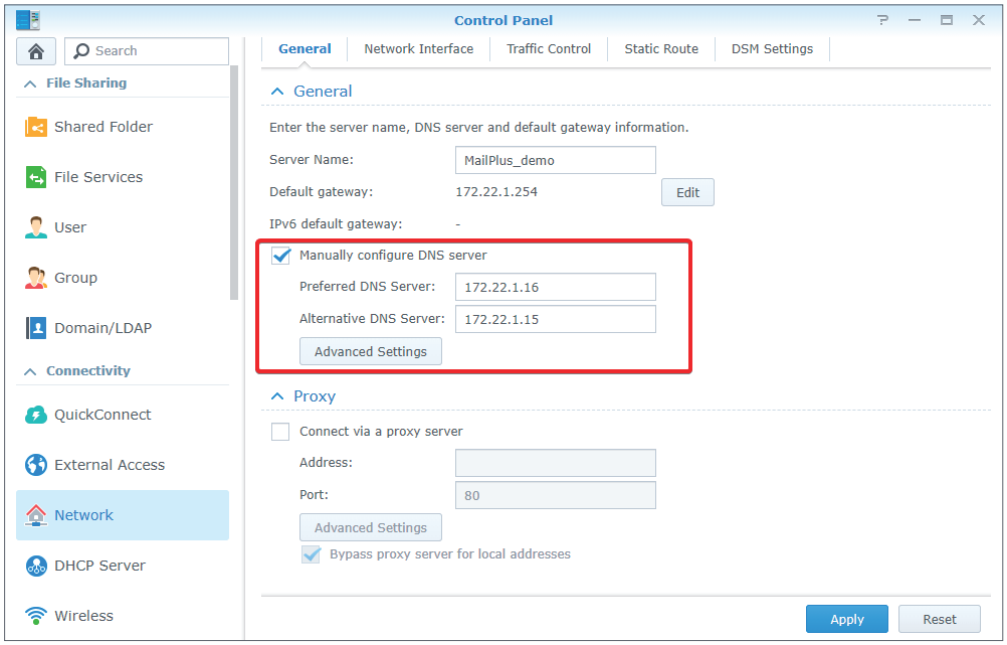

3. MailPlus Server 용 내부 Synology DNS Server 를 설정하여 기본 메일 서버를 찾습니다 .

4. 내부 DNS 서버의 MX 레코드에 도메인 이름을 입력하고 A 레코드에 도메인의 IP 주소를 입력합니다 . 내부 DNS 서버의 DNS 레코드 우선 순위는 외부 DNS 서버의 DNS 레코드보다 높아야 합니다 .

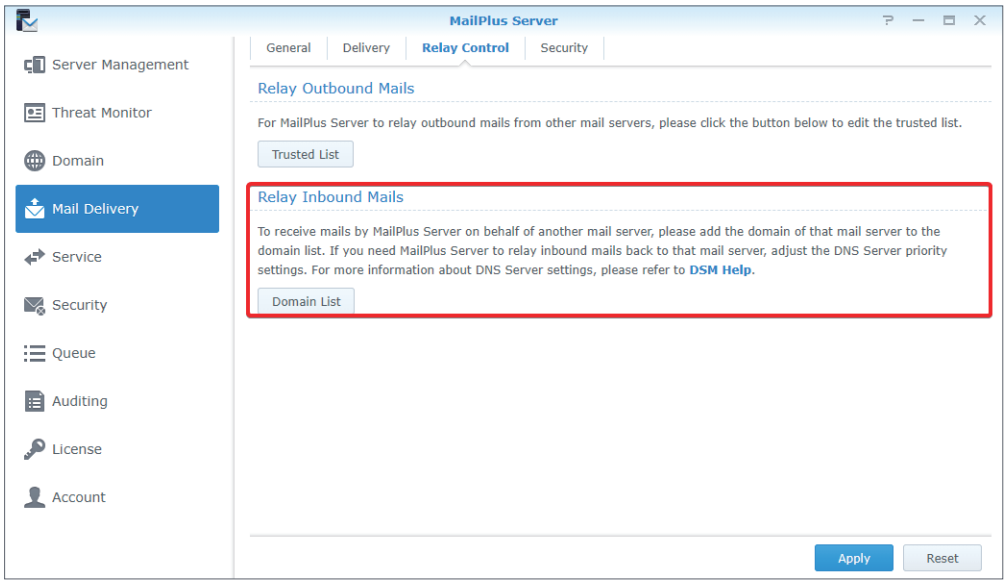





5. **DSM** > **제어판** > **네트워크** > **일반**으로 이동하고 **DNS 서버 수동 구성** 확인란을 선택합니다 . MailPlus Server 의 내부 및 외부 연결이 올바르게 작동할 수 있도록 **기본 DNS Server** 필드에 내부 DNS 서버의 IP 주소를 , **대체 DNS Server** 필드에 외부 DNS 서버의 IP 주소를 입력합니다 . MailPlus Server 가 이메일을 수신하면 두 DNS 서버의 MX 레코드를 확인하고 이메일을 우선 순위가 높은 메일 서버로 발송합니다 .

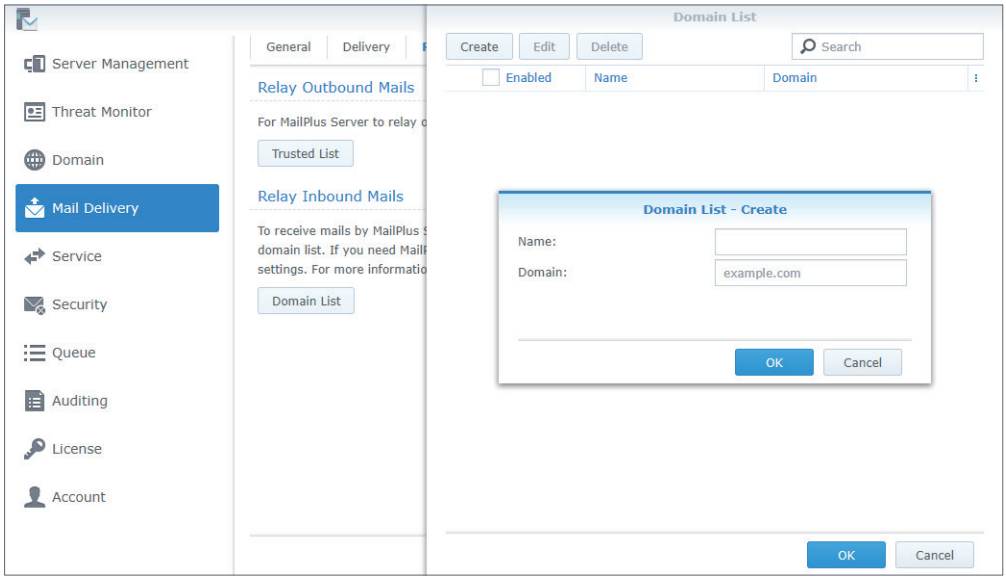


6. MailPlus Server 를 시작하고 **메일 배달** > **릴레이 제어**로 이동합니다 . **인바운드 메일 릴레이** 섹션에서 **도메인 목록** 버튼을 클릭합니다 .




7. **생성** 버튼을 클릭합니다 .

8. 규칙 이름과 도메인을 입력합니다 .




9. **확인**을 클릭하여 설정을 저장합니다 .

**참고 :**

- 이메일은 내부적으로 전송되지만 악성 이메일을 방지하려면 보안 페이지의 **스팸** 및 **안티 바이러스** 탭에서 **보안** 설정을 구성해야 합니다 .
- 보안 설정이 활성화되어 있으므로 **메일 배달** > **보안**에서 이메일을 화이트리스트에 추가하여 차단을 방지할 수 있습니다 .
- 모든 서버의 네트워크 세그먼트는 동일해야 합니다 .

# 8 장 : 도메인 설정

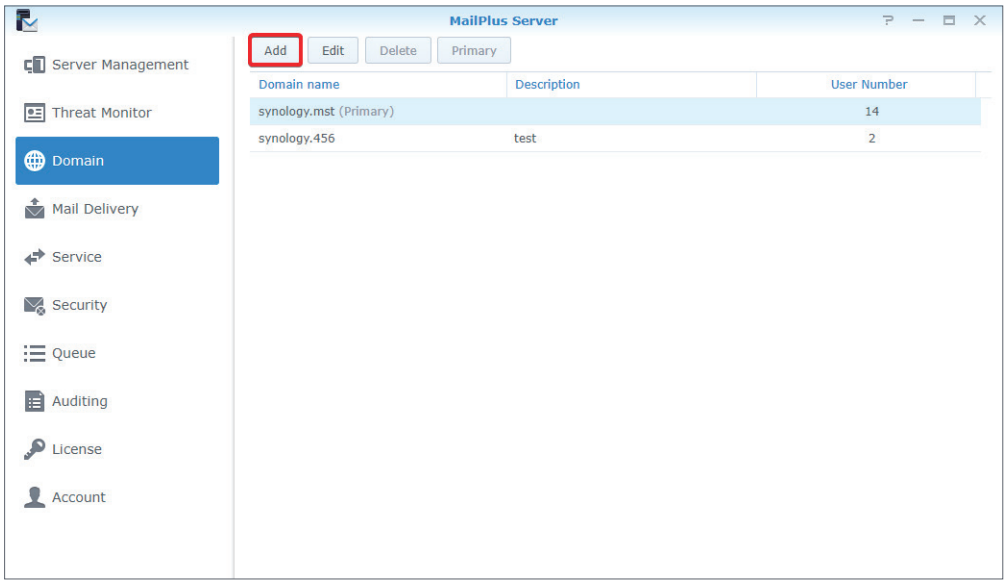
## 도메인

단일 MailPlus Server 에서 이메일 도메인을 여러 개 호스팅하여 도메인에 보낸 이메일을 중앙 집중화할 수 있습니다 . 또한 도메인마다 별칭 , 자동 BCC, 사용 제한 및 책임 부인을 사용자 지정할 수 있습니다 .

### MailPlus Server 에서 도메인 만들기

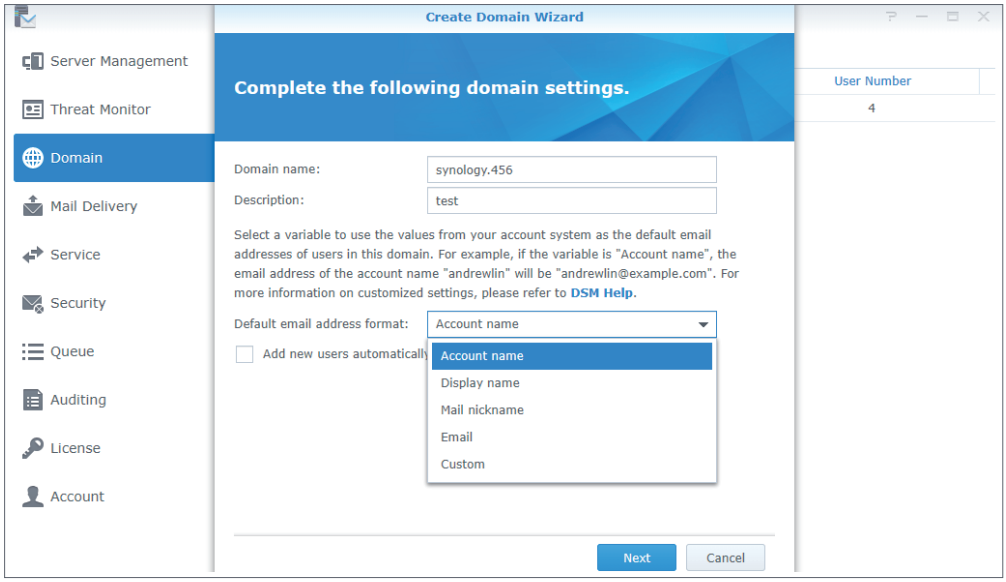
MailPlus Server 에 로그인하고 **도메인**으로 이동하여 새 도메인을 만듭니다 . 이 장에서는 synology.456 를 예로 사용하여 설명합니다 .

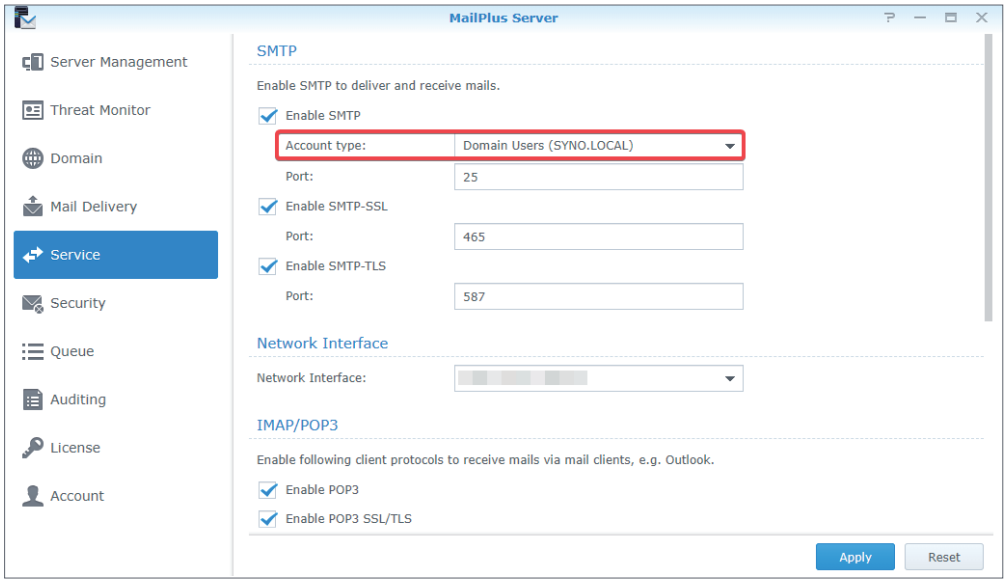
1. **도메인**으로 이동하고 **추가** 버튼을 클릭합니다 .




2. 도메인 이름 synology.456 과 설명을 입력합니다 .

3. 도메인에 구성원을 추가할 경우 MailPlus Server 는 **기본 이메일 주소 형식**의 설정에 따라 계정 시스템에서 정보를 가져옵니다 . **계정 이름** , **표시 이름** , **메일 닉네임** , **이메일** 또는 **서비스** > **SMTP** > **계정 유형**에서 설정한 계정 유형에 따라 **사용자 지정**을 선택할 수 있습니다 .


Create Domain Wizard
Server Management
Threat Monitor
Domain
Mail Delivery
Service
Security
Queue
Auditing
License
Account
Complete the following domain settings.
User Number
4
Domain name:
synology.456
Description:
test
Select a variable to use the values from your account system as the default email addresses of users in this domain. For example, if the variable is "Account name", the email address of the account name "andrewlin" will be "andrewlin@example.com". For more information on customized settings, please refer to DSM Help.
Default email address format:
Account name
Add new users automatically
Account name
Display name
Mail nickname
Email
Custom
Next
Cancel


MailPlus Server
Server Management
Threat Monitor
Domain
Mail Delivery
Service
Security
Queue
Auditing
License
Account
SMTP
Enable SMTP to deliver and receive mails.
Enable SMTP
Account type:
Domain Users (SYNO.LOCAL)
Port:
25
Enable SMTP-SSL
Port:
465
Enable SMTP-TLS
Port:
587
Network Interface
Network Interface:
IMAP/POP3
Enable following client protocols to receive mails via mail clients, e.g. Outlook.
Enable POP3
Enable POP3 SSL/TLS
Apply
Reset

다음 표에서는 계정 유형마다 제공되는 MailPlus Server 기본 설정을 보여줍니다 .

| 계정 유형 | 기본 설정 |
| --- | --- |
| 로컬 사용자 | 계정 이름<br>메일 닉네임 |
| LDAP 사용자 | 계정 이름<br>메일 닉네임 |
| 도메인 사용자 | 계정 이름<br>표시 이름<br>메일 닉네임<br>이메일 |

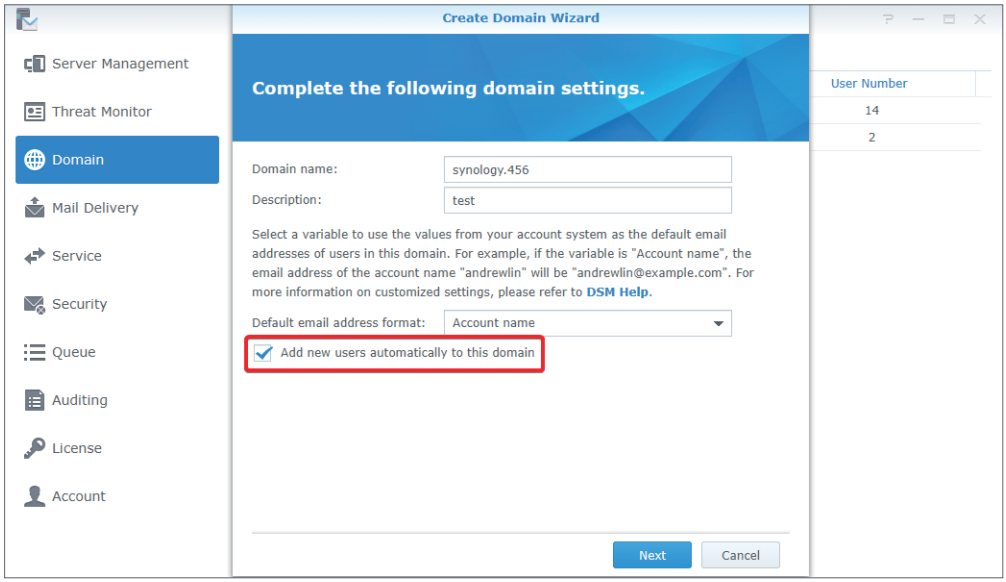
4. 사용자는 위 옵션 이외에 **사용자 지정**을 선택하여 **사용자 지정 변수** 필드에 기본 이메일 주소 형식으로 변수를 입력할 수 있습니다 . 다음 표는 MailPlus Server 가 지원하는 변수를 나타냅니다 .

| 변수 | 값 |
| --- | --- |
| <a> | 계정 이름 |
| <g> | 이름 |
| <i> | 중간 이니셜 |
| <s> | 성 |
| <d> | 표시 이름 |
| <m> | 메일 애칭 |
| <xa> | 계정 이름의 첫 x 문자를 사용합니다 . 예를 들어 x 가 2 면 계정 이름의 첫 두 문자가 사용됩니다 . |
| <xs> | 성의 첫 x 문자를 사용합니다 . 예를 들어 x 가 2 면 성의 첫 두 문자가 사용됩니다 . |
| <xg> | 이름의 첫 x 문자를 사용합니다 . 예를 들어 x 가 2 면 이름의 첫 두 문자가 사용됩니다 . |
| <custom attribute> | 계정 시스템이 지원하는 변수를 입력하여 해당 값을 가져올 수도 있습니다 . |

MailPlus Server 에서 지원되는 변수는 **서비스** > **SMTP** 에서 선택한 계정 시스템에 따라 달라집니다 . 자세한 내용은 다음 표를 참조하십시오 .

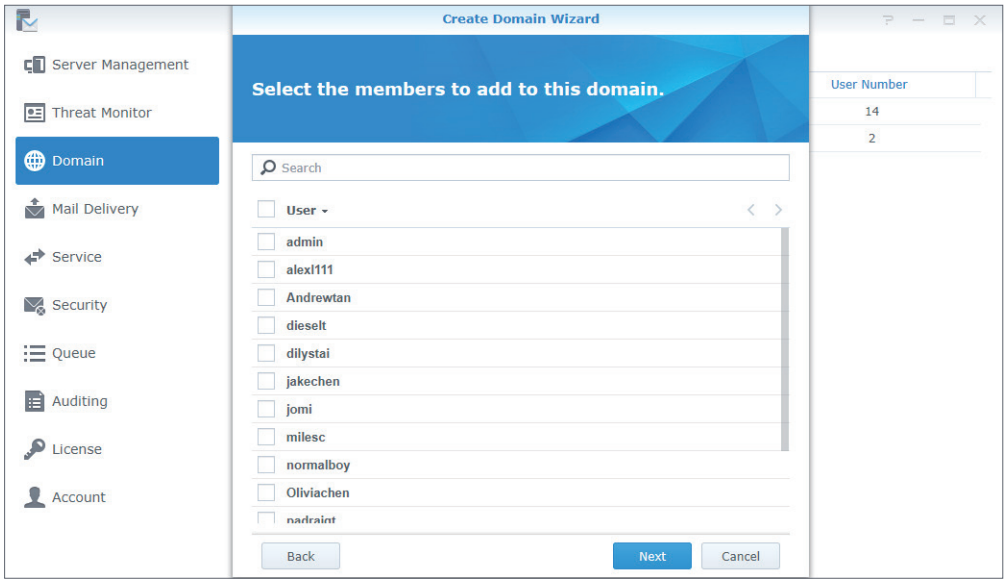
| 변수 | 로컬 사용자 | LDAP 사용자 | 도메인 사용자 |
|---|---|---|---|
| <a> | O | O | O |
| <g> | X | X | O |
| <i> | X | X | O |
| <s> | X | X | O |
| <d> | X | X | O |
| <m> | O | O | O |
| <xa> | O | O | O |
| <xs> | X | X | O |
| <xg> | X | X | O |
| <custom attribute> | X | O | O |

5. 사용자는 **새 사용자를 자동으로 이 도메인에 추가** 확인란을 선택하여 새 사용자를 자동으로 도메인에 추가할 수 있습니다 . MailPlus Server 는 사용자 이메일 주소를 기본 이메일 주소 형식에 따라 작성하도록 정보를 가져옵니다 .




6. 설정 후 **다음**을 클릭합니다 .

7. 이 도메인에 사용자를 추가하고 **다음**을 클릭하여 synology.456 의 구성원을 확인합니다 .




8. **적용**을 클릭하여 설정을 저장합니다 .

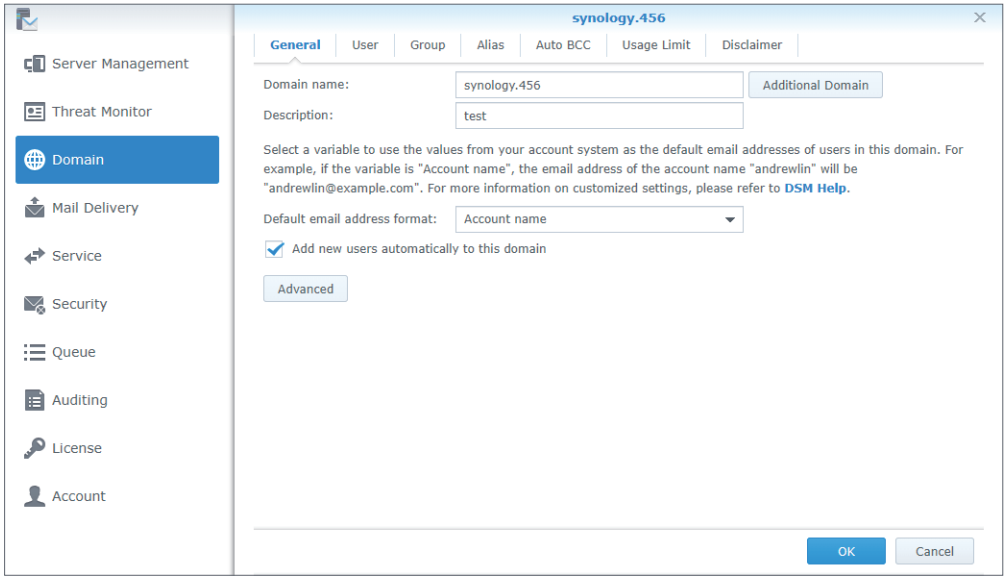
## 도메인 관리

MailPlus Server 는 각 도메인의 관리자와 사용자를 위한 관리 설정을 제공합니다 .

- **일반** : 도메인 이름과 도메인 설명을 편집하고 , 기본 이메일 주소 형식을 변경하고 , 추가 도메인을 만들고 , 아웃바운드 이메일에 DKIM 서명을 활성화하고 , Catch-all 을 활성화하여 존재하지 않는 이메일 주소 또는 특정 도메인에서 활성화되지 않은 이메일 주소로 보낸 이메일을 수신할 수 있습니다 .
- **사용자 계정** : 도메인에 새 구성원을 추가하고 이 도메인에 있는 사용자에 **도메인 관리자** 및 **일반 사용자**와 같은 역할을 선택할 수 있습니다 .
- **그룹 계정** : 이 그룹의 사용자가 같은 역할 설정을 가질 수 있도록 도메인에 구성원을 그룹으로 추가할 수 있습니다 .
- **별칭** : 받는 사람 한 명 또는 여러 명의 별칭을 만들 수 있습니다 . 이메일을 별칭에 보내면 서버는 자동으로 별칭에 있는 모든 사용자에게 배달합니다 . 별칭에 외부 이메일 주소를 포함할 수 있습니다 .
- **자동 BCC**: 시스템에서 보낸 사람 , 받는 사람 또는 모든 메시지의 특정 기준에 따라 BCC( 숨은 참조 ) 를 자동으로 특정 주소에 보내게 할 수 있습니다 .
- **보내기 제한 및 일일 할당량** : 아웃바운드 메시지 수를 제한하고 트래픽 제한을 설정할 수 있습니다 .
- **책임 부인** : 책임 부인을 적용할 조건을 구성하고 콘텐츠를 다양한 요구 사항에 맞게 사용자 지정할 수 있습니다 . 설정한 설정에 따라 책임 부인이 아웃바운드 이메일 콘텐츠 끝에 자동으로 추가됩니다 .

## 도메인의 일반 설정 편집

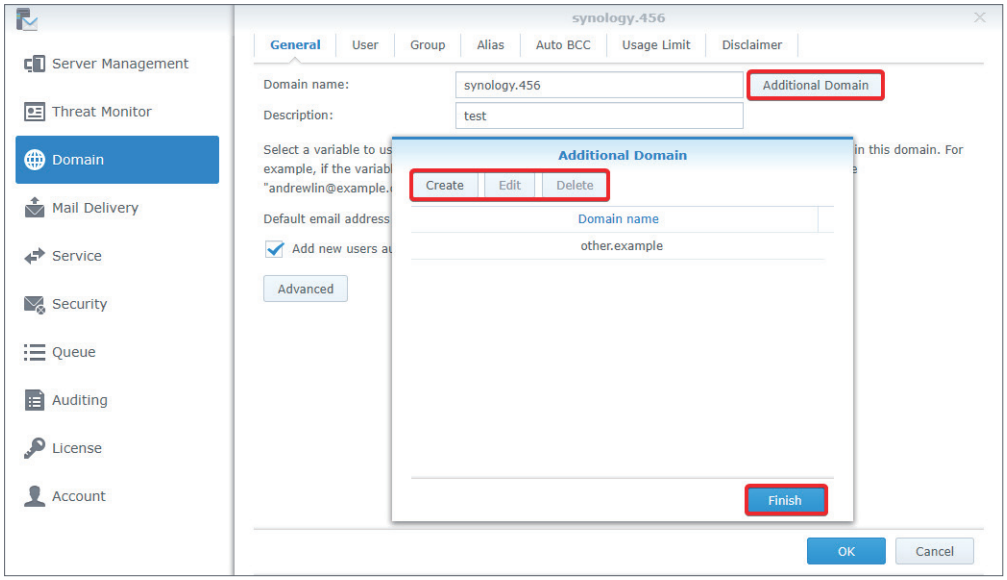
**일반** 탭에서 도메인 정보를 편집하고 , 기본 이메일 주소 형식을 조정하고 , 새 사용자를 자동으로 synology.456 에 추가할 수 있습니다 .




## 추가 도메인 만들기 및 편집

**추가 도메인** 창에서 이메일을 수신할 호스트에 추가 도메인 이름을 만들 수 있습니다 . 추가 도메인 설정은 synology.456 의 설정을 따릅니다 .

1. **도메인** > synology.456 > **일반**으로 이동하고 **추가 도메인** 버튼을 클릭합니다 .
2. **생성** 버튼을 클릭하여 추가 도메인을 만듭니다 . 편집 또는 삭제하려면 대상 도메인을 선택하고 해당 작업 버튼을 클릭하십시오 .
3. **추가 도메인** 페이지에서 만든 추가 도메인을 모두 볼 수 있습니다 . 위 예를 사용하면 synology.456 도메인에서 보낸 이메일 수신 외에도 추가 도메인의 이메일을 수신할 수 있습니다 ( 받는 사람으로 포함된 경우 ).
4. **마침**을 클릭하여 설정을 저장합니다 .



**참고 :**

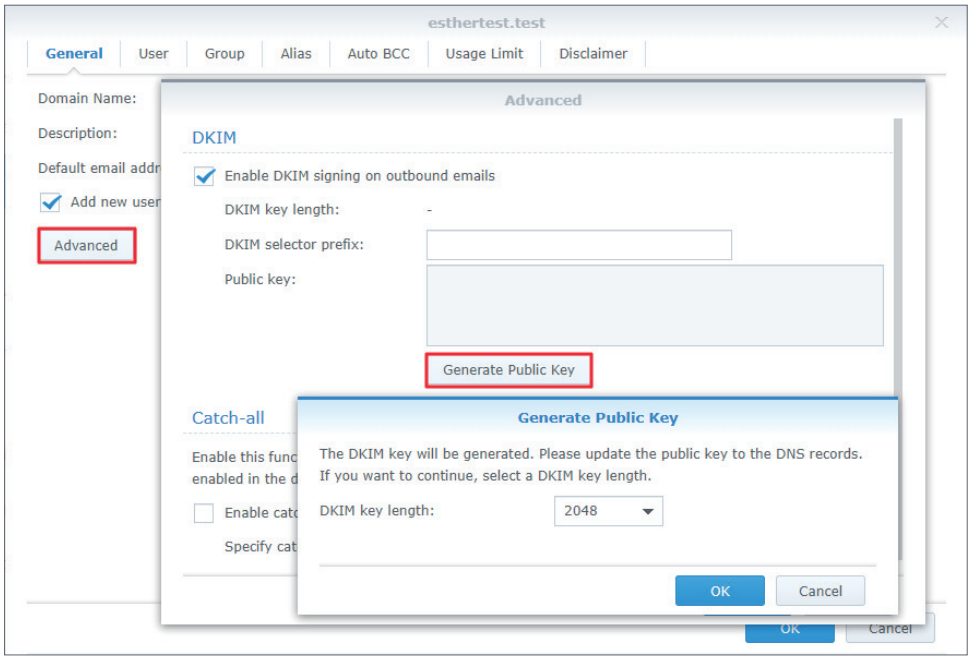
- DNS Server 의 MX 레코드를 조정해야 할 수도 있습니다 .

## 고급 설정 구성

1. **도메인** > synology.456 > **편집** > **일반**으로 이동하고 **고급** 버튼을 클릭합니다 .
2. **고급** 팝업 창에서 synology.456 의 **DKIM** 및 **Catch-all** 설정을 조정할 수 있습니다 .
   - **DKIM**: DKIM 서명을 활성화하여 메시지 수정 및 ID 도용을 방지할 수 있습니다 .
     a. ID 도용을 방지하고 받는 사람이 배달된 메시지를 신뢰하도록 하려면 **DKIM** 섹션에서 **아웃바운드 이메일에서 DKIM 서명 활성화** 확인란을 선택합니다 . 다음과 같이 DKIM 서명을 조정할 수 있습니다 .
        - **DKIM 선택기 접두어** : 접두사가 DKIM 서명에 추가됩니다 . DKIM 선택기 접두사를 원하는 대로 입력할 수 있습니다 .
        - **공개 키** : 공개 키 콘텐츠입니다 . DKIM 서명을 활성화한 경우 시스템에 공개 키와 개인 키가 없으면 키가 자동으로 생성됩니다 .
     b. **공개 키 생성** 버튼을 클릭하여 새로운 공개 키와 개인 키의 집합을 생성합니다 . 기본적으로 시스템은 2048 비트 키를 생성합니다 . (DKIM 키가 거부되면 키 길이를 1024 비트나 512 비트로 변경하십시오 .)

**참고 :**

- **공개 키 생성** 버튼을 클릭하면 기존 키가 삭제됩니다 .



c. **확인**을 클릭하여 설정을 저장합니다 . 또한 DKIM 서명을 다른 수신 서버에서 인증할 수 있도록 하려면 DNS TXT 레코드를 만들어 DKIM 인증을 허용해야 합니다 .

TXT 레코드 값 형식 : **v=DKIM1; k=rsa; p=DKIM 공개 키**

예를 들어 MailPlus Server 도메인이 **example.com** 이고 , DKIM 선택기 접두사가 **abc** 이고 , 시스템에서 생성된 공개 키가 **MIGfMA0GCSqGSIb3DQE** 이면 TXT 레코드는 다음과 같아야 합니다 .

- **TXT 레코드 이름** : abc._domainkey.example.com
- **TXT 레코드 값** : v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQE

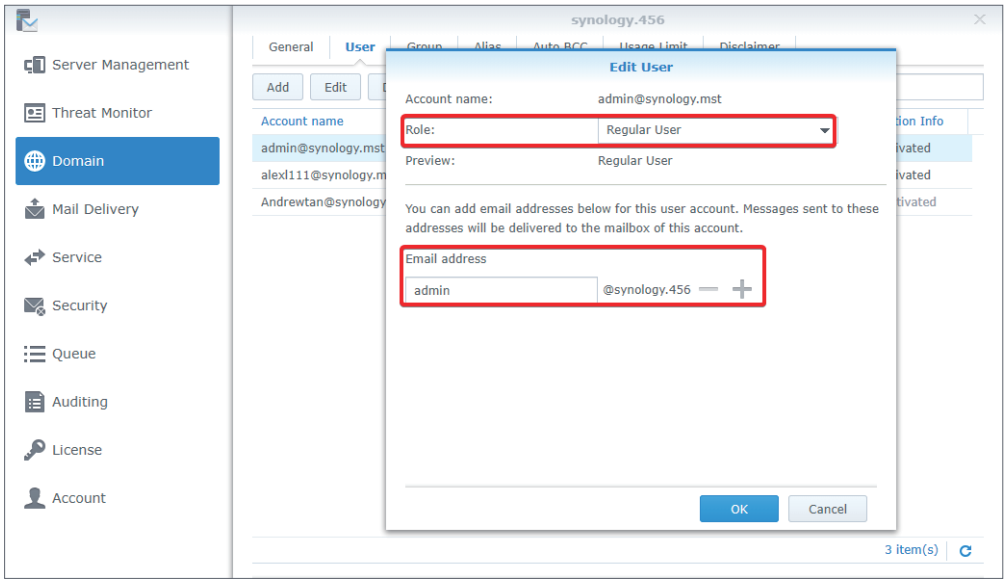
- **Catch-all**: **Catch-all** 을 활성화하면 사용자 계정이 존재하지 않거나 도메인에서 활성화되지 않은 이메일 주소로 보낸 이메일을 수신하도록 범용 사서함 역할을 수행하도록 할 수 있습니다 .

## 도메인에 사용자 계정 추가

1. **도메인**으로 이동하고 **synology.456** 을 선택한 후 **편집**을 클릭합니다 .
2. **사용자** 탭으로 이동하고 **추가**를 클릭합니다 .
3. 사용자 계정을 선택합니다 .
4. 선택한 사용자의 이메일 주소를 확인합니다 .

## 사용자 계정 편집 및 제거

1. **도메인**으로 이동하고 **synology.456** 을 선택한 후 **편집**을 클릭합니다 .
2. **사용자** 탭에서 계정을 선택하고 **편집**을 클릭합니다 .
3. **사용자 편집** 창에서 다음 설정을 조정합니다 .
   - **역할** : 드롭다운 메뉴에서 역할을 선택합니다 .
     - **도메인 관리자** : 도메인 관리자는 도메인 만들기 및 삭제를 제외한 모든 도메인 설정을 관리할 수 있습니다 .
     - **정규 사용자** : 일반 사용자에게는 도메인을 관리할 수 있는 권한이 없습니다 .
     - **그룹 설정을 따름** : 권한은 도메인의 사용자 그룹 설정에 따라 결정됩니다 .
   - **이메일 주소** : 이메일 주소를 여러 개 입력할 수 있습니다 . 해당 주소로 발송된 메시지는 이 계정의 사서함으로 배달됩니다 .



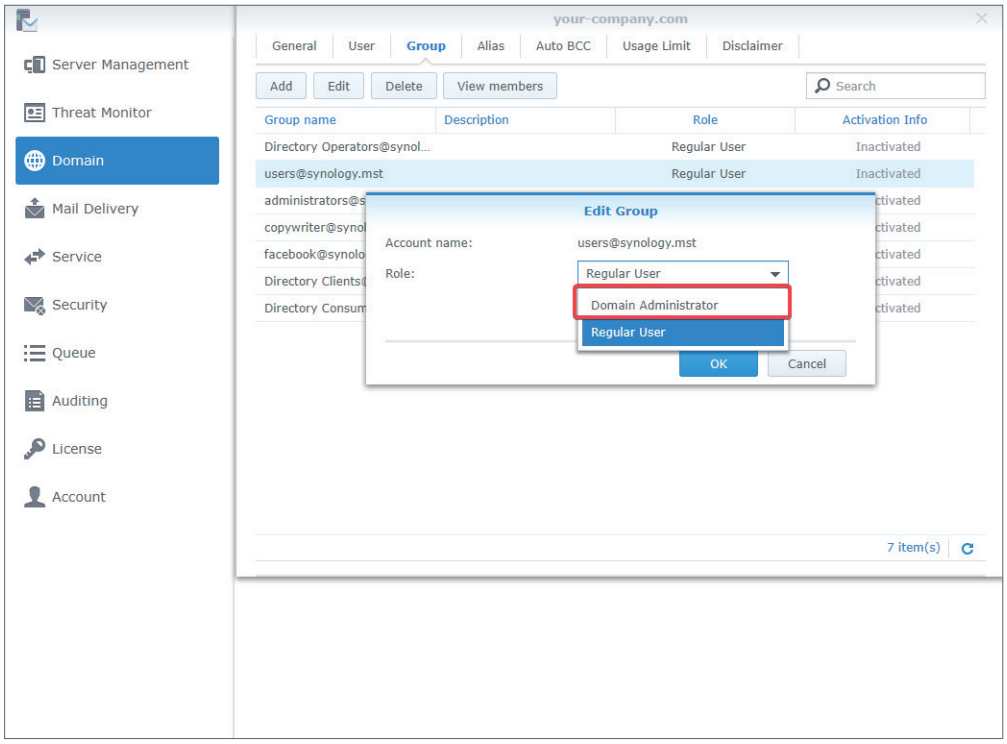

4. 사용자 계정을 제거하려면 대상 사용자 계정을 선택하고 **삭제** 버튼을 클릭합니다 .

## 도메인에 그룹 추가

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **그룹** 탭으로 이동하고 **추가**를 클릭합니다 .
3. 사용자 그룹을 선택하고 **다음**을 클릭합니다 .
4. 구성원의 이메일 주소를 확인합니다 . **적용**을 클릭합니다 .

## 그룹 편집 및 제거

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **그룹** 탭에서 편집할 그룹을 선택한 후 **편집**을 클릭합니다 .
3. **그룹 편집** 창의 **역할** 드롭다운 메뉴에서 **도메인 관리자**를 선택하면 그룹 내 모든 사용자에게 **도메인 관리자** 권한이 부여됩니다 .




4. 제거할 그룹을 선택하고 **삭제** 버튼을 클릭합니다 .

5. **구성원 보기** 버튼을 클릭하면 그룹에 속하는 특정 사용자가 이 도메인에 있지 않은지 확인할 수 있습니다 .

## 별칭 만들기

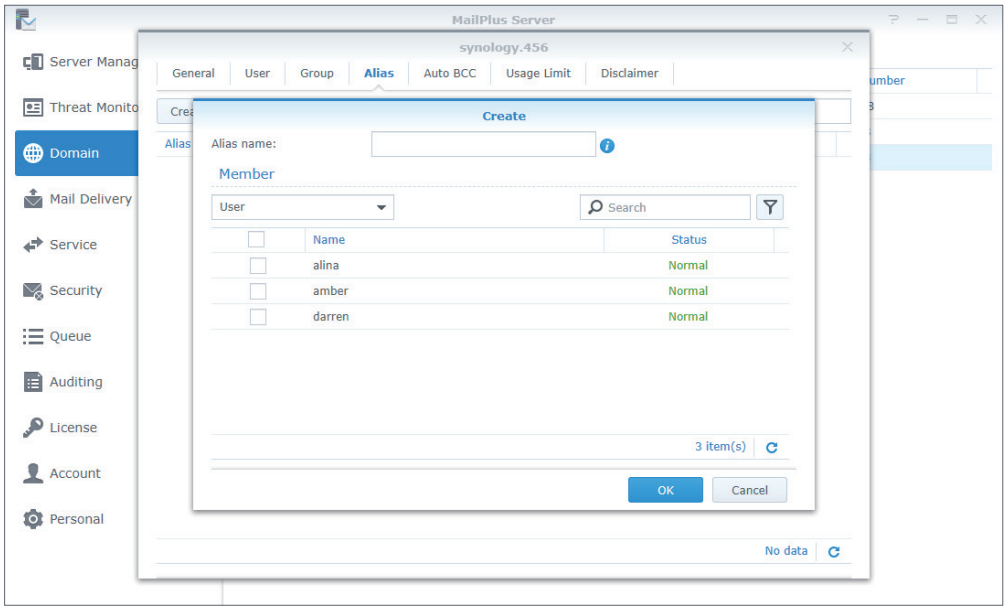
별칭을 만들면 사용자가 별칭 하나를 사용하여 받는 사람 여러 명에게 이메일을 보낼 수 있습니다 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .

2. **별칭**으로 이동하고 **생성** 버튼을 클릭합니다 .

3. **별칭 이름** 필드에 별칭 이름을 입력합니다 .

4. 드롭다운 메뉴에서 선택하여 별칭 , 사용자 , 그룹 또는 외부 사서함을 확인합니다 .




5. 확인란을 선택하여 사용자를 별칭에 추가합니다 .

6. 사용자 계정 , 그룹 계정 및 기타 별칭을 비롯한 소스 두 개 이상에서 사용자를 선택할 수 있습니다 .

7. **확인**을 클릭하여 설정을 저장합니다 .

## 별칭 편집 및 삭제

다음 단계를 참조하여 별칭을 편집 또는 삭제하십시오 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .

2. **별칭**으로 이동하고 수정할 별칭을 선택합니다 . 페이지 오른쪽 위 구석에 있는 검색 창에서 별칭을 검색할 수도 있습니다 .

3. **편집** 또는 **삭제** 버튼을 클릭합니다 .

## 별칭 가져오기 / 내보내기

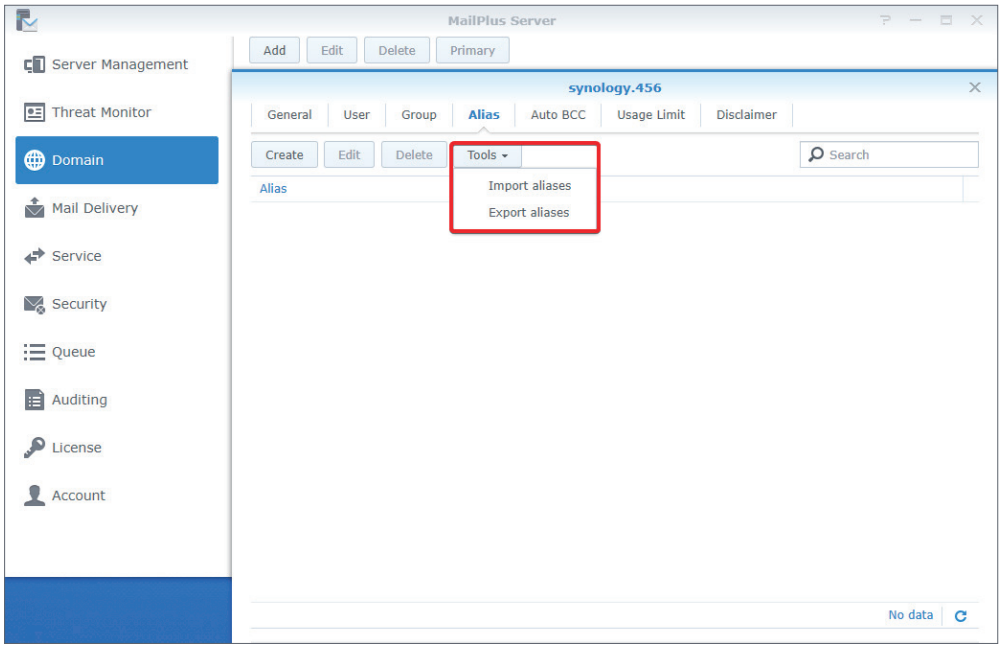
이전에 만든 기존 별칭 목록 또는 별칭 목록을 가져오려면 다음 단계를 참조하십시오 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .

2. **별칭**으로 이동하고 **도구** 버튼을 클릭합니다 .

3. 별칭 가져오기 또는 내보내기를 선택합니다 .

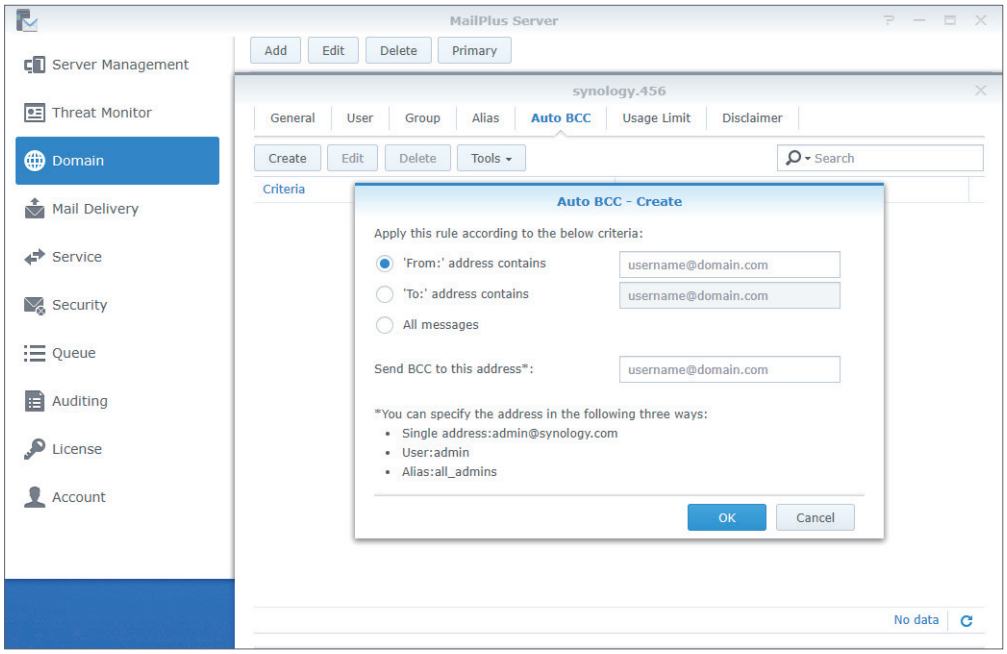
   - **별칭 가져오기** : 가져온 별칭 이름이 이미 있으면 이 별칭을 가져오거나 업데이트할 수 없습니다 .
   - **별칭 내보내기** : 별칭 파일을 내보내고 후위 형식으로 다운로드합니다 .




## 자동 BCC 규칙 만들기

자동 BCC 설정을 사용하면 보낸 사람 , 받는 사람 또는 모든 메시지의 특정 기준에 따라 BCC( 숨은 참조 ) 를 특정 주소에 보낼 수 있습니다 . 다음 단계를 참조하여 자동 BCC 규칙을 만드십시오 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **자동 BCC** 로 이동하고 **생성** 버튼을 클릭합니다 .
3. 자동 BCC 기준을 지정합니다 .
   - **보내는 사람 :' 주소 포함** : 원본 이메일 콘텐츠의 **MAIL FROM** 정보가 여기에 입력한 정보와 일치하면 BCC 가 자동으로 전송됩니다 .
   - **받는 사람 :' 주소 포함** : 원본 이메일 콘텐츠의 **RCPT TO** 정보가 여기에 입력한 정보와 일치하면 BCC 가 자동으로 전송됩니다 .
   - **모든 메시지** : BCC 는 내부 시스템의 알림 이메일을 제외한 모든 이메일에 자동으로 전송됩니다 .
4. **이 주소로 BCC 보내기 *** 필드에 BCC 가 자동으로 전송될 주소를 입력합니다 .
5. 이메일 주소 , 사용자 계정 또는 별칭을 입력할 수 있습니다 .




6. **확인**을 클릭하여 설정을 저장합니다 .

## 자동 BCC 규칙 편집 및 삭제

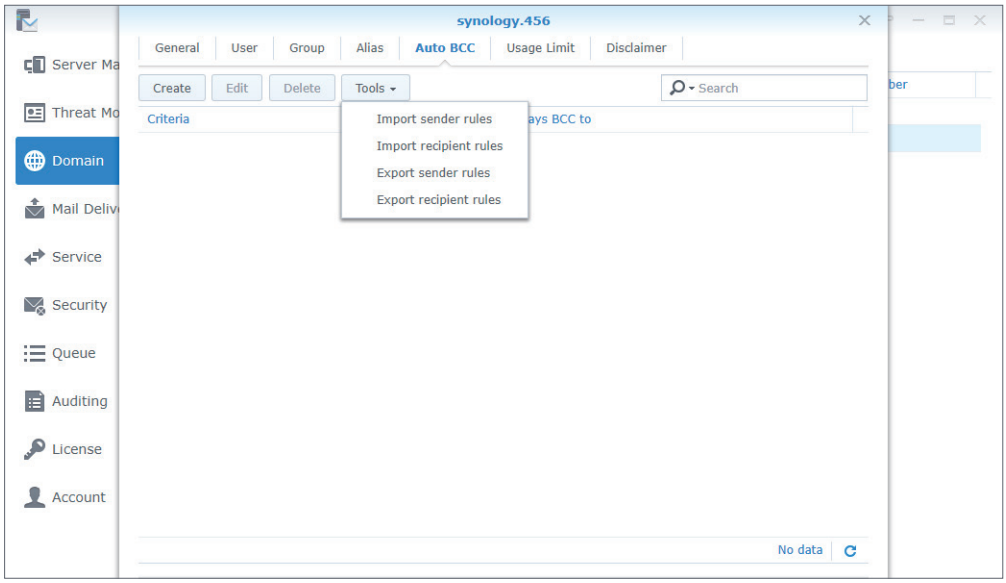
다음 단계를 참조하여 자동 BCC 규칙을 편집 및 삭제하십시오 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **자동 BCC** 로 이동하고 수정할 자동 BCC 규칙을 선택합니다 .
3. **편집** 또는 **삭제** 버튼을 클릭합니다 .

## 자동 BCC 규칙 가져오기 / 내보내기

다음 단계를 참조하여 자동 BCC 규칙을 내보내거나 가져오십시오 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **자동 BCC** 로 이동하고 **도구** 버튼을 클릭합니다 .
3. 보낸 사람 또는 받는 사람 규칙을 가져오거나 내보냅니다 .

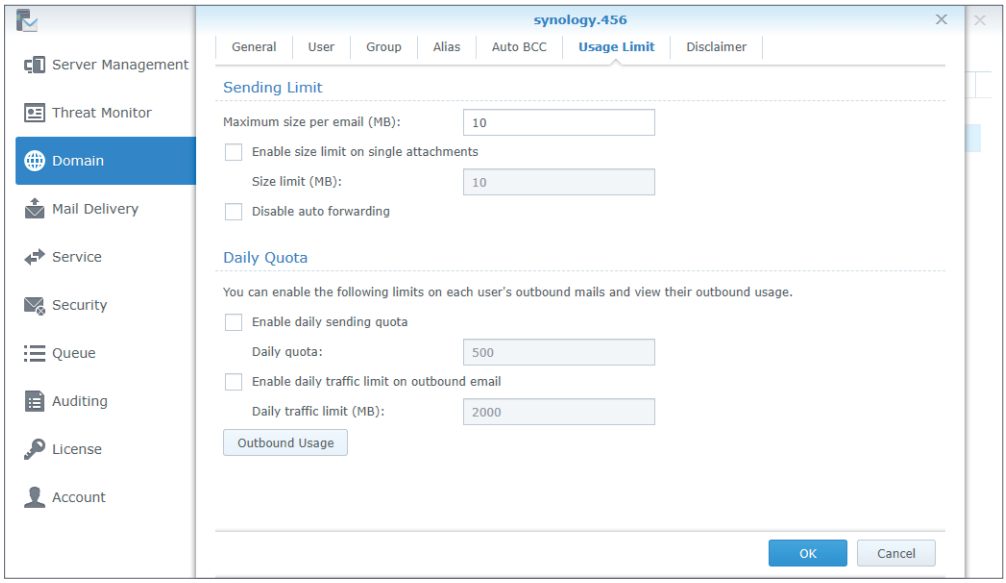



**참고 :**

- 이 기능은 후위 **기본 구성 문서**에 이미 설명되어 있으므로 여기서는 **모든 메시지 규칙 가져오기 및 내보내기**를 사용할 수 없습니다 . **always bcc** 를 참조하십시오 .
- 가져온 파일이 후위 형식인지 확인하십시오 .

## 보내기 제한과 일일 할당량 설정

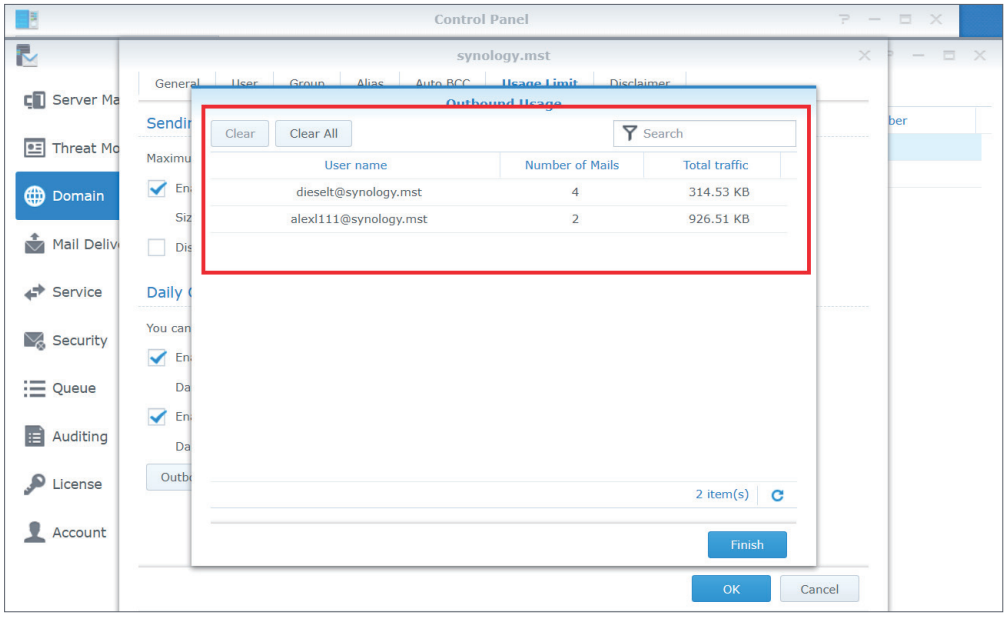
1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **사용량 제한** 탭으로 이동합니다 .
3. **보내기 제한** 섹션에서 다음 설정을 조정합니다 .
   - **이메일당 최대 크기 (MB)**: 아웃바운드 이메일의 크기 제한을 지정합니다 .
   - **단일 첨부 파일에 대한 크기 제한 활성화** : 단일 첨부 파일의 크기 제한을 지정합니다 . 아래 **크기 제한 (MB)** 필드에 값을 입력합니다 .
   - **자동 전달 비활성화**
4. **일일 할당량** 섹션에서 다음 설정을 조정합니다 .
   - **일일 전송 할당량 활성화** : 사용자가 매일 보낼 수 있는 아웃바운드 메시지 수를 제한합니다 .
   - **아웃바운드 이메일에 대한 일일 트래픽 제한 활성화** : 사용자가 매일 보낼 수 있는 아웃바운드 메시지의 총 크기를 제한합니다 .
   - **아웃바운드 사용** : 개별 사용자의 아웃바운드 이메일 사용량을 확인합니다 .




## 아웃바운드 사용

여기에서 기록된 총 아웃바운드 메시지 수를 확인할 수 있습니다 . 사용자가 일일 할당량에 도달하면 사용자가 이메일을 계속 보낼 수 있도록 레코드를 지울 수 있습니다 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **사용량 제한** 탭으로 이동하고 **아웃바운드 사용** 버튼을 클릭합니다 .
3. 목록에서 특정 사용자를 선택합니다 . 페이지 오른쪽 위 구석에 있는 검색 필드에서 사용자를 검색할 수도 있습니다 .
4. **지우기** 버튼을 클릭하여 사용자 아웃바운드 사용 레코드를 지우고 사용 레코드를 재설정합니다 . **모두 제거** 버튼을 클릭하여 목록에 있는 모든 사용자의 사용 레코드를 지웁니다 .




5. **마침**을 클릭하여 설정을 완료합니다 .

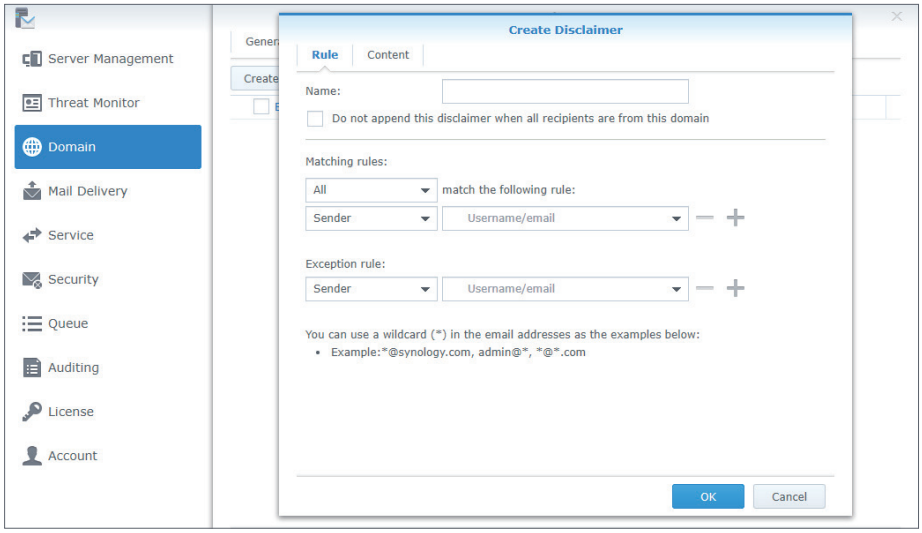
## 책임 부인 만들기

이 책임 부인 기능을 사용하면 사용자가 자동으로 아웃바운드 이메일의 하단 또는 끝에 사용자 지정 텍스트를 추가할 수 있습니다 . 다음 단계를 참조하여 책임 부인을 만드십시오 .

**참고 :**

- 책임 부인과 규칙이 여러 개 있을 수 있지만 이메일 하나에 책임 부인 한 개만 적용할 수 있습니다 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .
2. **책임 부인** 탭으로 이동하고 **생성** 버튼을 클릭합니다 .
3. **책임 부인 생성** 창의 **규칙** 탭으로 이동합니다 .



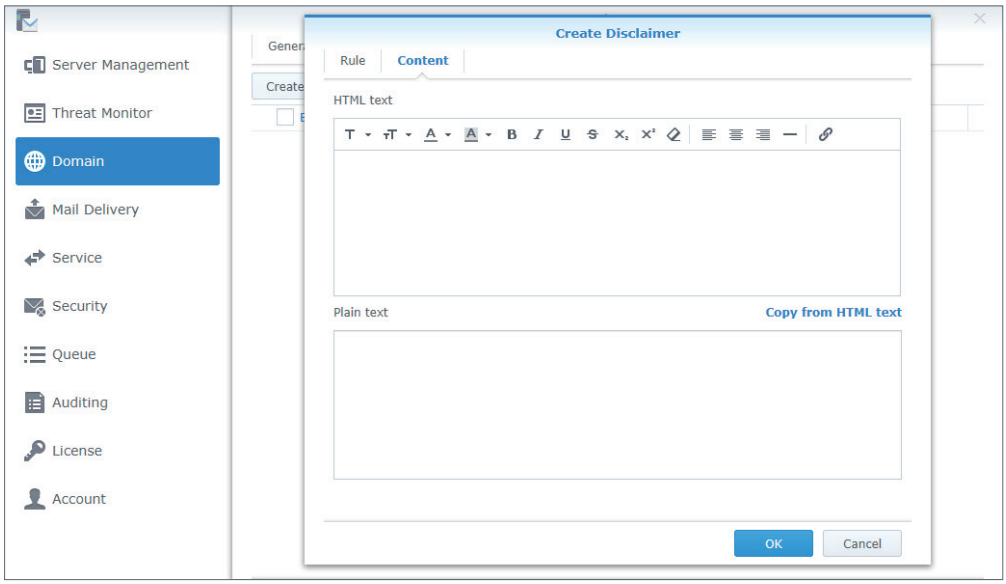

4. **이름** 필드에 책임 부인 이름을 입력합니다 .
5. **모든 받는 사람이 이 도메인에 있는 경우 이 책임 부인 첨부 안 함** 확인란을 선택할지 여부를 선택합니다 .

**참고 :**

- 서버에서 이메일을 내부 이메일 ( 내부 사용자에게 보낸 이메일 ) 로 감지하면 책임 부인이 추가되지 않습니다 .
- 받는 사람 중 한 명이 내부 사용자가 아니면 책임 부인이 계속 추가됩니다 .

6. 다음 옵션을 사용하여 기준을 설정합니다 .
   - **일치 여부 비교 규칙** : 일치시킬 정의에 **모두** 또는 **임의**를 선택합니다 . **모두**를 선택하면 모든 규칙이 충족되는 경우에만 책임 부인이 추가됩니다 . **임의**를 선택하면 규칙이 최소 한 개 이상 충족되면 책임 부인이 추가됩니다 .
   - **다음 규칙과 일치** : **받는 사람** 또는 **보낸 사람**을 기준으로 책임 부인을 추가합니다 . 설정은 와일드 카드 문자 (*) 를 지원합니다 .
   - **예외 규칙**은 **일치 여부 비교 규칙**보다 우선시됩니다 . **예외 규칙**을 만들 때는 **일치 여부 비교 규칙**의 조건이 일치하더라도 책임 부인이 추가되지 않습니다 .
7. 더하기 아이콘 (+) 을 클릭하여 **일치 여부 비교 규칙** 또는 **예외 규칙**을 두 개 이상 만들고 빼기 아이콘 (-) 버튼을 클릭하여 규칙을 제거합니다 .

8. 규칙을 설정한 후 **콘텐츠** 탭으로 이동하여 콘텐츠가 클라이언트 끝에 올바르게 표시되도록 **HTML 텍스트** 콘텐츠와 **일반 텍스트**를 편집합니다 .




9. **일반 텍스트** 콘텐츠를 **HTML 텍스트** 콘텐츠와 동일하게 하려면 **HTML 텍스트에서 복사**를 클릭하여 콘텐츠를 **HTML 텍스트** 편집기에서 **일반 텍스트** 편집기로 복사한 후 모든 HTML 태그를 제거합니다 .

10. **OK**( 완료 ) 을 클릭하여 설정을 완료합니다 .

## 책임 부인 편집 및 삭제

책임 부인 편집 및 삭제 외에 책임 부인이 우선 순위에 따라 적용되면 여기에서 우선 순위 설정을 조정할 수 있습니다 . 다음 단계를 참조하여 책임 부인을 관리하십시오 .

**참고 :**

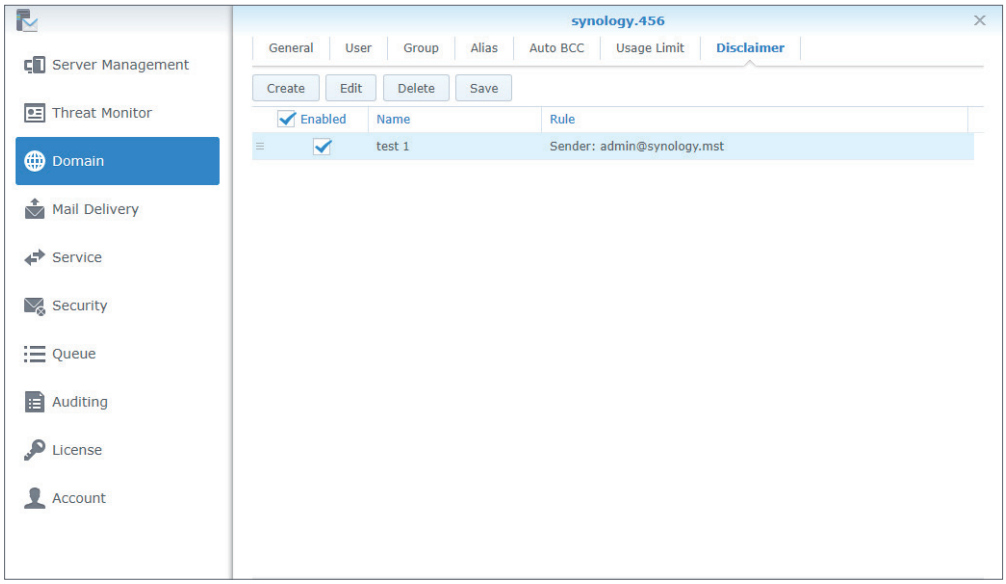
- 시스템은 위에서 아래로 순서로 추가할 책임 부인을 확인합니다 . 책임 부인 기준이 충족되면 책임 부인이 적용되므로 확인이 종료됩니다 .

1. **도메인**으로 이동하고 synology.456 을 선택한 후 **편집**을 클릭합니다 .

2. **책임 부인** 탭으로 이동합니다 . 우선 순위가 높은 책임 부인이 우선 순위가 낮은 책임 부인보다 우선시됩니다 . 우선 순위를 변경하려면 원하는 책임 부인을 선택하고 적절한 위치로 끌어 놓습니다 .

3. 활성화할 책임 부인 규칙을 선택합니다 .

4. 수정할 책임 부인 규칙을 선택하고 **편집** 또는 **삭제** 버튼을 클릭합니다 .




5. **저장**을 클릭하여 설정을 적용합니다 .

# 9 장 : 보안 설정

MailPlus Server 보안 기능은 **스팸** , **안티 바이러스 검사** , **인증** 및 **콘텐츠 보호** 등 4 가지 영역을 다룹니다 . 설정을 조정하여 특정 영역 보호를 강화할 수 있습니다 .

## 스팸

MailPlus Server 는 스팸 메시지의 배달 특성을 기준으로 스팸 감지 표준을 제공합니다 . MailPlus Server 에서 다음과 같은 스팸 방지 기술을 사용할 수 있습니다 .

- **스팸 방지** : 스팸 방지 엔진으로 Rspamd 및 SpamAssassin 을 사용합니다 . 또한 MailPlus Server 는 자동 학습 및 스팸 보고 메커니즘을 통해 필요에 맞게 스팸 메시지를 차단할 수 있습니다 .
- **포스트스크린** : 열려 있는 블랙리스트와 스팸 서버의 보낸 사람 특성에 따라 스팸 서버의 서비스를 거부하여 스팸을 수신할 가능성을 줄입니다 .
- **그레이리스트** : 스팸 서버의 보낸 사람 특성에 따라 작업을 수행합니다 . 그레이리스트는 메시지 배달 속도에 영향을 미치므로 이 기능을 활성화하기 전에 그레이리스트 메커니즘을 숙지하십시오 .

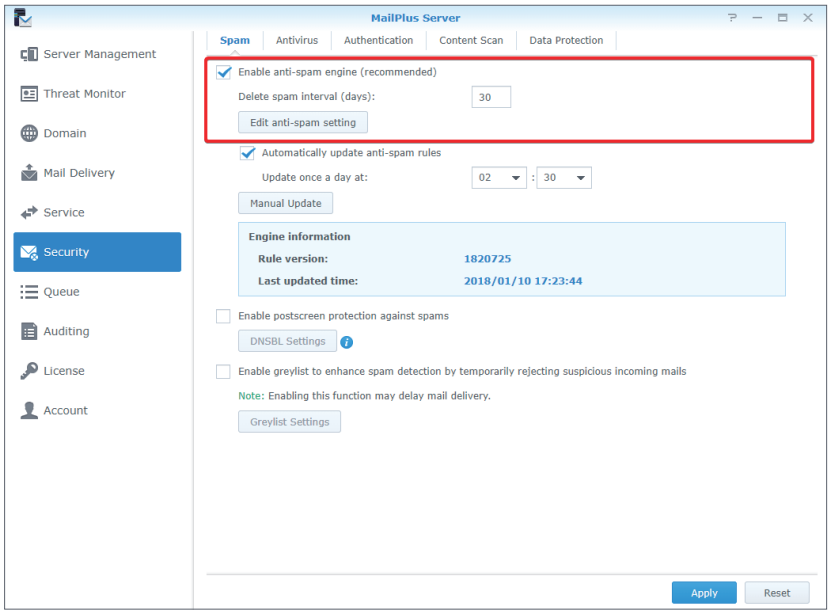
### 스팸 방지 활성화

MailPlus Server 는 스팸 방지 엔진인 Rspamd 를 SpamAssassin 데이터베이스의 규칙과 함께 사용하여 스팸을 감지하고 스팸 점수 임계값에 따라 스팸을 필터링합니다 . 이메일이 사전 설정된 감지 규칙과 일치하면 점수가 추가됩니다 . 임계값을 초과하는 이메일은 스팸으로 표시됩니다 . 다음 단계를 참조하여 스팸 방지를 활성화하십시오 .

1. **보안** > **스팸**으로 이동하여 다음 설정을 조정합니다 .
   - **스팸 방지 엔진 활성화** : 스팸 방지 기능에 대한 자세한 내용은 **스팸 방지 일반 설정** , **스팸 방지 규칙 업데이트** , **스팸 필터 사용자 지정** 및 **자동 학습 및 스팸 보고 설정**을 참조하십시오 .
   - **스팸 삭제 간격 ( 일 )**: 스팸으로 표시된 메시지는 스팸 사서함으로 전송됩니다 . 스팸 메시지는 지정된 일 수 후에 자동으로 삭제됩니다 . 스팸 자동 삭제 간격을 사용자 지정할 수 있습니다 . 기본값은 30 일입니다 .

**참고 :**

- 스팸 방지 엔진이 활성화되지 않더라도 스팸은 여전히 정기적으로 삭제됩니다 .

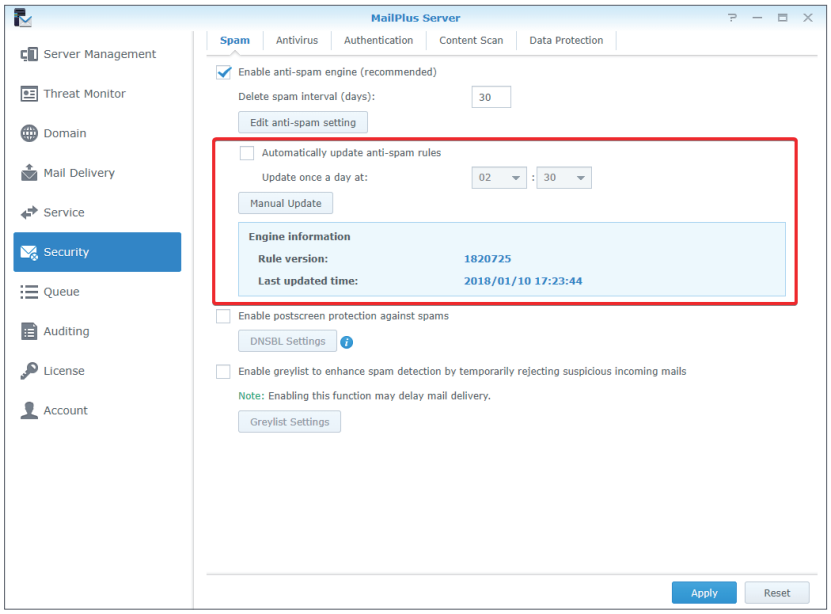



## 스팸 방지 규칙 업데이트

메일 보호 기능이 최신 상태로 유지되도록 스팸 방지 규칙을 정기적으로 업데이트해야 합니다 . 다음 단계를 참조하십시오 .

1. **보안** > **스팸**으로 이동하여 다음 설정을 조정합니다 .

   - **Anti-Spam 규칙 자동 업데이트** : 업데이트 스케줄을 설정하려면 이 옵션을 선택합니다 . 그러면 시스템은 스케줄에 따라 공식 SpamAssassin 웹사이트에서 최신 스팸 방지 규칙을 다운로드합니다 .
   - **하루에 한 번 업데이트할 시간** : 규칙을 다운로드할 일일 스케줄을 설정합니다 .
   - **수동 업데이트** : 스팸 방지 규칙을 즉시 업데이트하려면 이 버튼을 클릭합니다 . 버튼 아래의 **엔진 정보** 섹션에는 최근 업데이트된 시간과 스팸 감지 규칙 버전이 표시됩니다 .



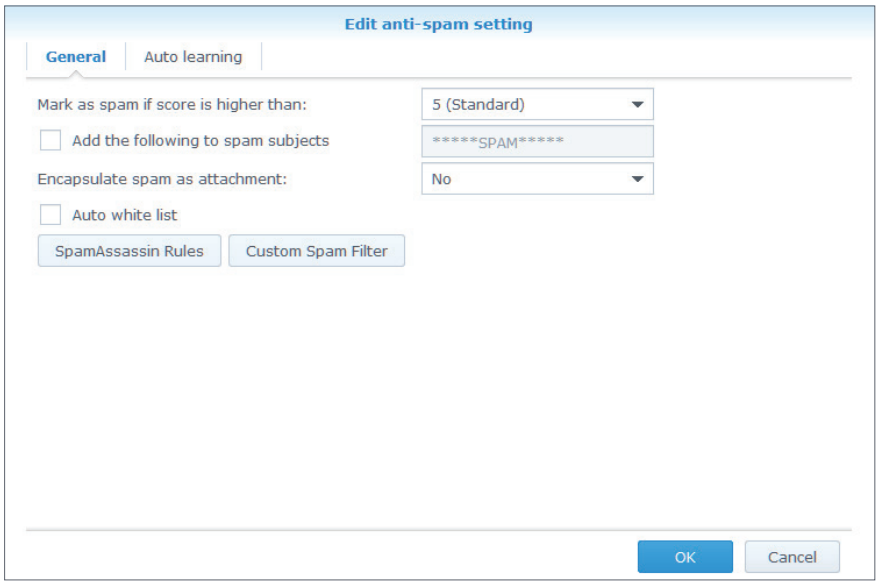
## 스팸 방지 일반 설정

스팸 방지 기능에는 다양한 사용자 지정 가능한 설정이 있습니다 . 필요에 맞게 스팸 방지 엔진을 조정할 수 있습니다 . 다음 단계를 참조하여 일반 스팸 방지 설정을 편집하십시오 .

1. **보안** > **스팸**으로 이동하고 **스팸 방지 설정 편집** 버튼을 클릭합니다 .
2. **스팸 차단 설정 편집** 창의 **일반** 탭으로 이동하여 다음 설정을 조정할 수 있습니다 .
   - **스팸으로 표시할 점수 상한** : 설정한 임곗값을 초과하는 메시지가 스팸으로 표시됩니다 .
   - **스팸 대상에 추가할 항목** : 메시지가 스팸 점수 임곗값을 초과하여 스팸으로 표시되면 스팸 제목에 특정 콘텐츠를 추가하여 사용자에게 알릴 수 있습니다 . **스팸 제목에 다음 추가** 확인란을 선택하고 기본 콘텐츠를 수정합니다 .
   - **스팸을 첨부 파일로 캡슐화** : 스팸으로 표시된 이메일은 새 메시지에 캡슐화된 첨부 파일로 보고됩니다 . 드롭다운 메뉴 옵션은 다음과 같습니다 .

| 옵션 | 설명 |
|---|---|
| **아니요** | 추가 작업 없이 스팸을 신고합니다 . |
| **예** | 스팸을 새 메시지에 캡슐화된 첨부 파일로 보고합니다 . |
| **예 . 일반 텍스트로만** | 웹 버그와 악성 스크립트를 방지하기 위해 스팸을 일반 텍스트로 신고합니다 . 그런 다음 첨부 파일로 캡슐화하여 받는 사람에게 보냅니다 . |

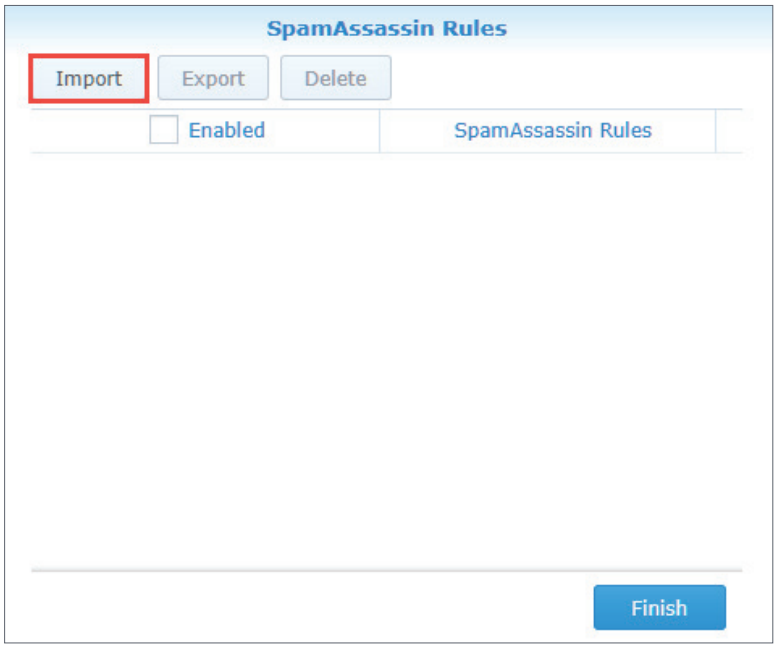
   - **자동 화이트리스트** : 이 기능을 사용하면 시스템은 인바운드 및 아웃바운드 이메일 통신을 분석하여 외부 이메일 주소가 과거에 사용자가 회신했던 주소인지 확인할 수 있습니다 . 이렇게 하면 이메일이 스팸으로 잘못 취급되지 않습니다 .



## SpamAssassin 규칙

1. **보안** > **스팸**으로 이동하고 **스팸 방지 설정 편집** 버튼을 클릭합니다 .
2. **스팸 방지 설정 편집** 창의 **일반** 탭으로 이동하고 **SpamAssassin 규칙** 버튼을 클릭합니다 .
3. **가져오기** 버튼을 클릭하여 SpamAssassin 규칙을 추가합니다 .

> **참고 :**
>
> - 가져온 파일의 확장명은 ".cf" 여야 합니다 . 규칙을 가져오면 규칙이 활성화됩니다 . SpamAssassin 에서 제공하는 **규칙**을 참조하거나 **규칙 지침**에 따라 규칙을 추가할 수 있습니다 .

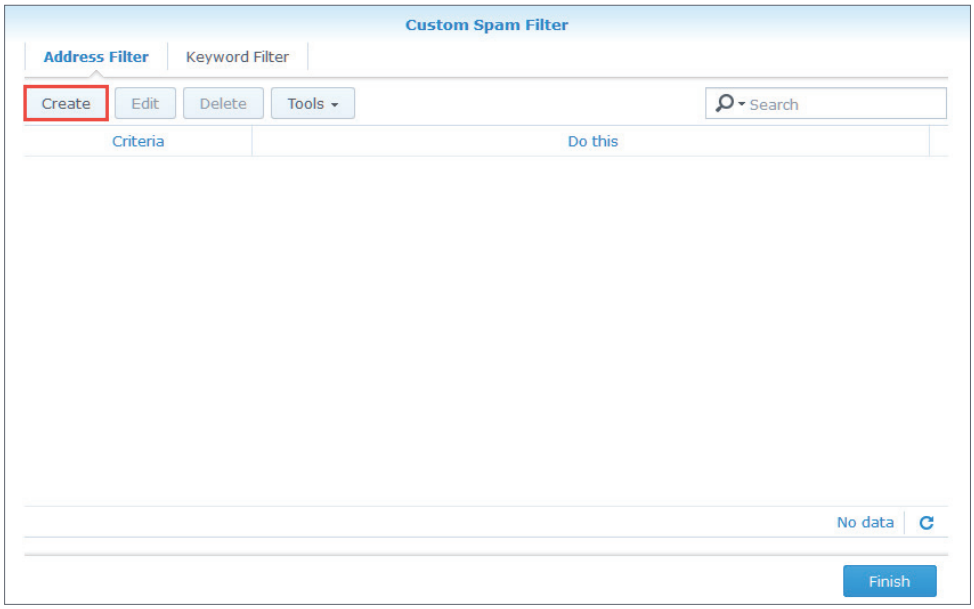



4. 편집할 규칙을 선택하고 **활성화** , **내보내기** 및 **삭제**와 같은 수행할 작업을 선택합니다 .
5. **마침**을 클릭하여 설정을 완료합니다 .

## 스팸 필터 사용자 지정

의심스러운 이메일을 필터링하도록 설정할 수 있는 스팸 필터에는 **주소 필터** 및 **키워드 필터** 등 두 가지 유형이 있습니다 . 필요에 맞게 필터를 사용자 지정할 수 있습니다 . 다음 단계를 참조하여 스팸 필터를 만드십시오 .

1. **보안** > **스팸**으로 이동하고 **스팸 방지 설정 편집** 버튼을 클릭합니다 .
2. **스팸 방지 설정 편집** 창의 **일반** 탭으로 이동하고 **스팸 필터 사용자 지정** 버튼을 클릭합니다 .
3. **스팸 필터 사용자 지정** 창의 **주소 필터** 탭으로 이동하고 **생성** 버튼을 클릭합니다 .

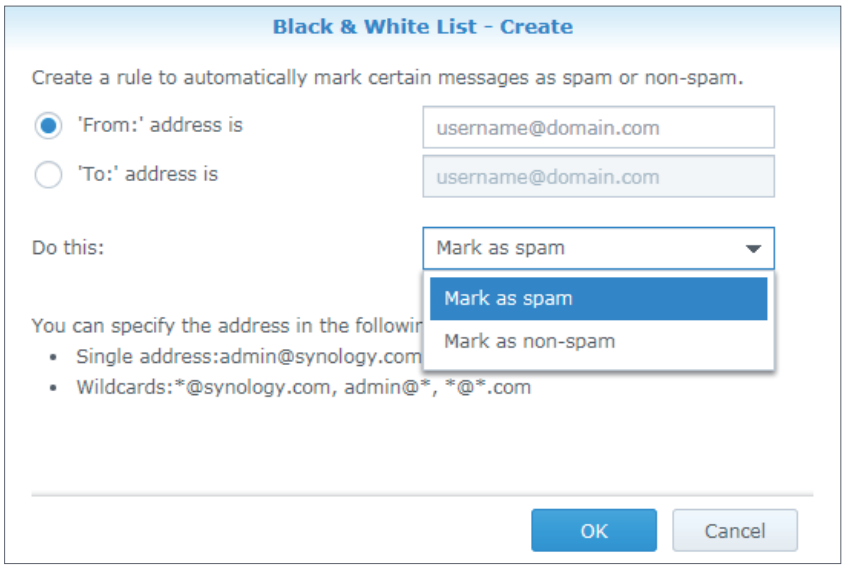



4. 메시지는 보낸 사람과 받는 사람 기준에 따라 스팸 또는 비스팸으로 표시됩니다 . 입력한 주소에 와일드 카드 문자 (*) 를 사용할 수 있습니다 .

5. **수행** 드롭다운 메뉴에서 **스팸으로 표시** 또는 **비스팸으로 표시**를 선택합니다 .

**참고 :**

- 이러한 작업 구성과 관련하여 스팸 점수가 무시됩니다 .



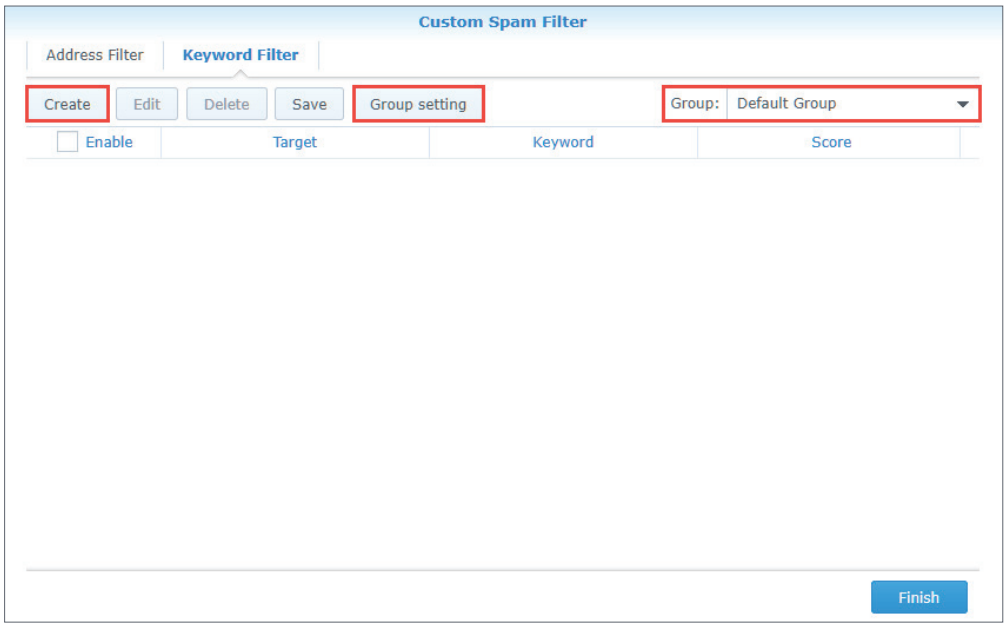

6. **확인**을 클릭하여 설정을 완료합니다 .

7. **스팸 필터 사용자 지정** 창의 **키워드 필터** 탭으로 이동합니다 .

8. **그룹 설정** 버튼을 클릭하여 그룹을 만듭니다 . 그룹을 여러 개 설정하여 키워드 필터를 범주화한 후 그룹별로 필터를 관리할 수 있습니다 .

   - **활성화** 필드의 확인란을 선택하여 전체 그룹을 활성화하거나 비활성화합니다 .
   - 그룹을 생성 , 편집 또는 삭제하려면 그룹을 선택하고 상단 도구 모음의 작업 버튼을 클릭합니다 .

9. 키워드 필터를 만들기 전에 드롭다운 메뉴에서 필터가 포함된 그룹을 선택합니다 .




10. **생성** 버튼을 클릭하여 규칙을 사용자 지정합니다 .

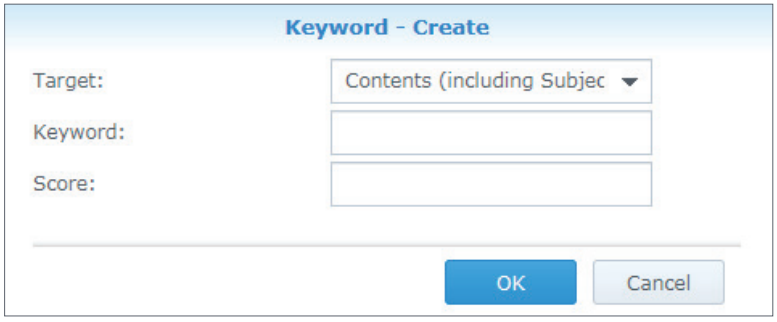
- **대상** : **대상** 드롭다운 메뉴에서 필터링할 다음 옵션을 선택할 수 있습니다 .

| 옵션 | 설명 |
|---|---|
| **제목** | 이메일 제목 |
| **내용 ( 제목 포함 )** | 이메일 콘텐츠 및 제목 |

- **키워드** : 필터링할 키워드를 입력합니다 . 여기서 정규식을 사용할 수 있습니다 . 정규식에 대한 자세한 내용은 **Wikipedia** 를 참조하십시오 .
- **점수** : 키워드가 검색될 때 이메일의 총 스팸 점수에 추가할 포인트 수를 지정합니다 .

**참고 :**

- 총 스팸 점수가 스팸 점수 임곗값을 초과하면 이메일이 스팸으로 표시됩니다 .




**참고 :**

- 이렇게 수정할 경우 스팸 점수 임계값을 다시 조정하려 할 수 있습니다 . **스팸 방지 설정 편집** 창의 **일반** 탭으로 다시 이동하여 스팸 점수 임계값을 조정하십시오 . 스팸 점수 임계값이 높을수록 스팸 기준이 낮아지므로 이메일이 스팸으로 표시될 가능성이 줄어듭니다 . 스팸 점수 임계값이 낮아질수록 스팸 기준이 엄격해지므로 이메일이 스팸으로 표시될 가능성이 높아집니다 .

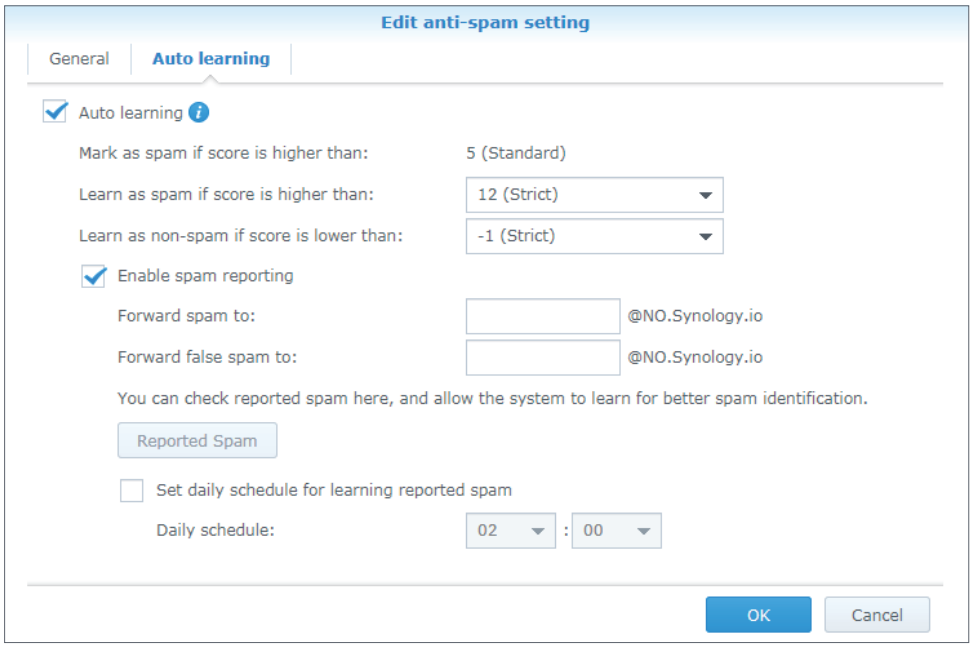
## 자동 학습 및 스팸 보고 설정

스팸 방지 엔진이 실행된 후 전문 알고리즘을 통해 스팸을 보다 정확하게 감지할 수 있도록 MailPlus Server 를 학습시킬 수 있습니다 . 자동 학습 및 스팸 보고를 통해 개별 요구 사항에 맞게 스팸 감지 정확도를 향상시킬 수 있습니다 .

- **자동 학습** : 스팸 방지 엔진에서 스팸을 감지하는 동안 시스템은 이메일을 추가로 분석할 수 있도록 점수를 기준으로 기준에 일치하는 이메일을 자동으로 선택합니다 .
- **스팸 보고** : 사용자는 스팸 방지 엔진이 스팸을 감지하지 못하거나 메시지가 스팸으로 잘못 처리되면 스팸을 보고할 수 있습니다 . 스팸 방지 엔진에 올바르지 않는 범주화를 보고하면 엔진 재학습을 통해 정확도를 향상시킬 수 있습니다 .

다음 단계를 참조하여 자동 학습 및 스팸 보고를 설정하십시오 .

1. **보안** > **스팸**으로 이동하고 **스팸 방지 설정 편집** 버튼을 클릭합니다 .
2. **스팸 방지 설정 편집** 창의 **자동 학습** 탭으로 이동합니다 .



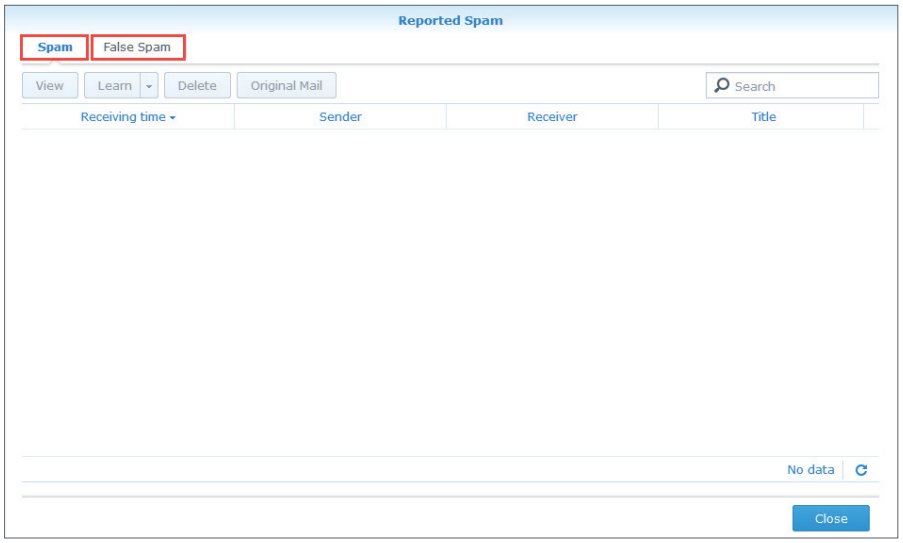

3. **자동 학습** 확인란을 선택하여 다음 설정을 조정합니다 .
   - **스팸으로 표시할 점수 상한** : **일반** 탭에 설정한 스팸 점수 임곗값이 표시됩니다 .
   - **스팸으로 간주할 점수 상한** : 스팸 감지 중에 스팸 점수가 이 값보다 높으면 스팸 방지 엔진은 메시지 콘텐츠의 키워드를 추가로 분석하여 스팸 방지 엔진 데이터베이스를 확장하고 학습 기능을 향상시킵니다 . 이후 동일한 키워드가 감지되면 메시지가 스팸으로 확인될 가능성이 높아집니다 .
   - **비스팸으로 간주할 점수 하한** : 스팸 감지 중에 스팸 점수가 이 값보다 낮으면 스팸 방지는 메시지 콘텐츠의 키워드를 추가로 분석하여 스팸 방지 엔진 데이터베이스를 확장하고 학습 기능을 향상시킵니다 . 이후 동일한 키워드가 감지되면 메시지가 스팸이 아닌 것으로 확인될 가능성이 높아집니다 .
4. **스팸 보고 활성화** 확인란을 선택하여 다음 설정을 조정합니다 .

**참고 :**

- 보고 프로세스는 스팸을 특정 사서함으로 수집하여 학습 프로세스를 진행하는 프로세스입니다 . 따라서 사용자는 스팸 보고를 활성화한 후 다음 두 가지 방법에 따라 스팸과 비스팸을 보고할 수 있습니다 .
  - 사용자가 MailPlus 를 사용하여 메시지를 수신하는 경우 전달 사서함이 이러한 사용자에 이미 구성되어 있습니다 . 사용자는 MailPlus 에서 메시지를 스팸으로 표시하거나 MailPlus 의 스팸 사서함으로 이동하여 메시지를 비스팸으로 표시해야만 합니다 .
  - 사용자가 타사 이메일 클라이언트를 사용하여 메시지를 수신하면 이메일 클라이언트의 **첨부 파일로 전달** 기능을 사용하여 이메일을 첨부 파일로 사서함 보고에 전달해야 합니다 .

- **스팸 전달 대상** : 사용자가 타사 메일 클라이언트를 사용하여 이메일을 수신하고 보고할 때 보고된 스팸이 전달될 이메일 주소를 입력합니다 . 원본 이메일이 첨부 파일로 이 이메일 주소에 전달됩니다 .
- **거짓 스팸 전달 대상** : 사용자가 타사 메일 클라이언트를 사용하여 이메일을 수신하고 보고할 때 보고된 비스팸을 전달할 이메일 주소를 입력합니다 . 원본 이메일이 첨부 파일로 이 이메일 주소에 전달됩니다 .
- **신고된 스팸** : **신고된 스팸** 버튼을 클릭하여 모든 보고된 스팸과 거짓 스팸을 확인합니다 . 이메일 목록에서 이메일을 선택하고 **학습** 버튼을 클릭하면 스팸 방지 엔진이 선택한 이메일 유형의 스팸 감지를 향상시킬 수 있습니다 . 학습된 이메일은 제거됩니다 . 시스템이 스팸 사서함과 스팸이 아닌 사서함의 이메일에서 학습하도록 허용할 수 있습니다 . 다음 스팸 관리를 참조하십시오 .

| 기능 | 설명 |
| --- | --- |
| **보기** | 메시지 콘텐츠를 봅니다 . |
| **학습** | 스팸 방지 엔진이 선택한 이메일에서 신속하게 학습할 수 있습니다 . 이메일을 학습하면 이메일이 목록에서 제거됩니다 . |
| **모두 학습** | 스팸 방지 엔진이 모든 이메일 메시지에서 학습하도록 허용합니다 . **모두 학습**은 **학습** 버튼 옆에 있는 드롭다운 메뉴에 있습니다 . |
| **삭제** | 스팸 방지 엔진이 선택한 이메일을 학습하지 않도록 삭제합니다 . |
| **원래 메일** | 새 브라우저 탭에서 원본 메일을 엽니다 . |
| **검색** | 오른쪽 위 구석에 있는 검색 필드에 키워드 ( 보낸 사람 , 받는 사람 및 제목 ) 를 입력하여 특정 이메일 메시지를 검색합니다 . |




- **보고된 스팸 학습에 대한 일별 일정 설정** : 시스템이 보고된 모든 스팸 및 비스팸 메시지를 자동으로 학습하는 시간을 지정하려면 이 옵션을 선택합니다 .

**참고 :**

- **스팸 전달 대상**에 입력된 이메일 주소는 기존 사용자와 동일한 사용자 이름을 공유할 수 없습니다 . 이 메일 주소는 라이센스 사용자로 계산되지 않으며 이메일 샘플을 받는 데만 사용됩니다 .
- **거짓 스팸 전달 대상**에 입력된 이메일 주소는 기존 사용자와 동일한 사용자 이름을 공유할 수 없습니다 .

5. **확인**을 클릭하여 설정을 완료합니다 .

## 포스트스크린

포스트스크린은 연결 단계 중에 연결 소스를 테스트하고 서비스를 계속할지 여부를 결정합니다 . 포스트스크린에는 다음과 같은 두 가지 주요 기능이 있습니다 .

- 보낸 사람이 SMTP 표준을 따르거나 SMTP 서버 인사말 후에 명령을 보내는지 확인합니다 . 보낸 사람이 SMTP 서버 인사말 전에 명령을 보내면 이 보낸 사람은 차단됩니다 .
- 보낸 사람의 IP 주소를 기준으로 다른 DNSBL 서버를 확인합니다 . 다른 서버에서 보낸 사람의 IP 주소가 블랙리스트에 추가되면 이 보낸 사람은 차단됩니다 .

## DNSBL 설정

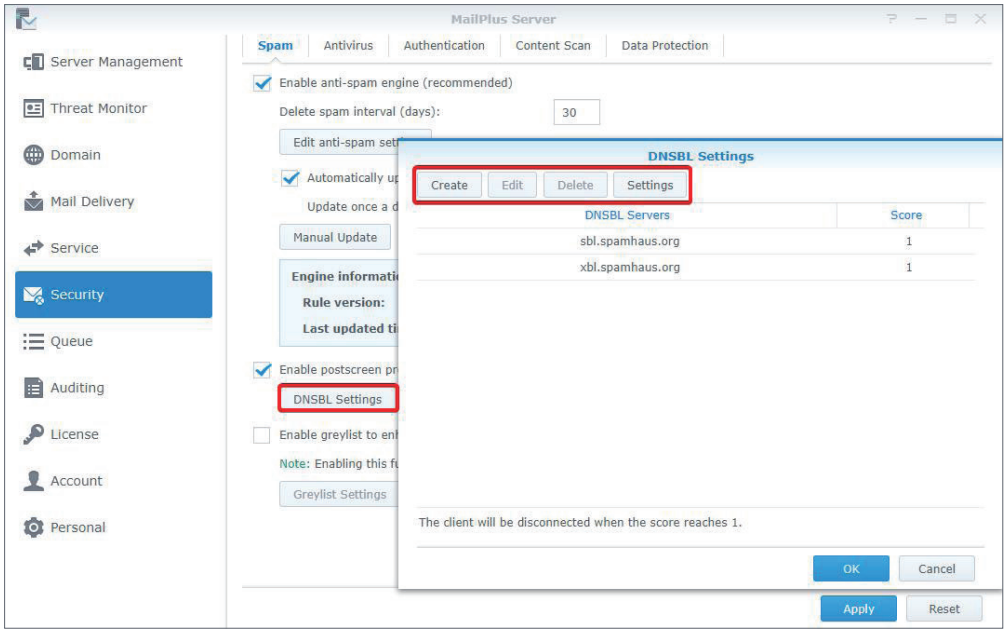
포스트스크린을 사용하면 DNSBL 서버 여러 개를 설정할 수 있습니다 . 서버 검사 중에 기준과 일치하면 스팸 점수가 발생하고 다른 서버에서 발생한 스팸 점수는 누적됩니다 . 총 점수가 **DNSBL 점수 역치**에서 지정된 값을 초과하면 서비스가 거부됩니다 . 아래 단계를 참조하여 DNSBL 설정을 조정하십시오 .

1. **보안** > **스팸**으로 이동하고 **스팸에 대한 포스트스크린 보호 활성화** 확인란을 선택합니다 .
2. **DNSBL 설정** 버튼을 클릭하여 검사해야 하는 서버를 편집합니다 .
3. **설정** 버튼을 클릭하여 서비스를 거부할 수 있도록 **DNSBL 점수 역치**를 지정합니다 .
4. **생성** 버튼을 클릭하여 검사할 서버를 추가합니다 .

**참고 :**

- 여기에 DNSWL(DNS 기반 화이트리스트 ) 서버를 추가하고 해당 **점수** 필드에 음수를 입력할 수 있습니다 .

5. 선택한 DNSBL 서버를 **편집** 또는 **삭제**할 수 있습니다 .




6. **확인**을 클릭하여 설정을 완료합니다 .

## 그레이리스트 활성화

새로운 인바운드 메시지가 있으면 시스템은 이 인바운드 메시지와 동일한 IP 주소 , 보낸 사람 또는 받는 사람의 레코드가 있는지 확인합니다 . 발견된 레코드가 없으면 메시지는 의심스러운 메시지로 간주되고 보낸 사람에게 나중에 메시지를 다시 보내라고 요청하는 오류 메시지가 보낸 사람에게 다시 전송됩니다 . 오류 메시지를 받은 보낸 사람은 SMTP 표준에 따라 나중에 다시 메시지 전송을 시도합니다 . 하지만 대부분의 스팸을 보낸 사람은 메시지 전송을 포기합니다 . 일반 보낸 사람이 잠시 후에 메시지를 다시 보내면 시스템이 수신합니다 . 그레이리스트 메커니즘에서는 이 방식을 사용하여 스팸을 차단합니다 .

그레이리스트를 활성화하면 그레이리스트는 모든 소스의 이메일에 다음 기본 작업을 수행합니다 .

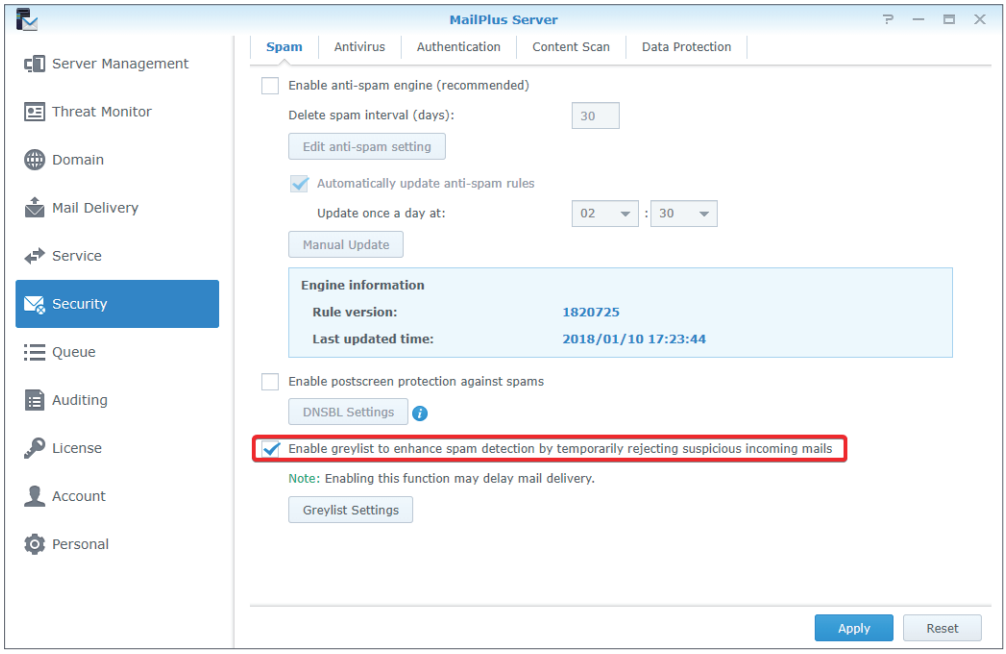
- **화이트리스트** : 테스트를 직접 통과하고 임시 오류 메시지가 다시 전송되지 않습니다 .
- **그레이리스트** : 통신 기록 없이 보낸 사람에게 오류 메시지를 전송합니다 .
- **블랙리스트** : 메시지를 직접 거부합니다 .

**참고 :**

- 그레이리스트 메커니즘으로 인해 합법적인 메시지 배달이 지연될 수 있습니다 . 그레이리스트를 활성화하기 전에 그레이리스트 메커니즘을 완전히 이해했는지 확인하십시오 .

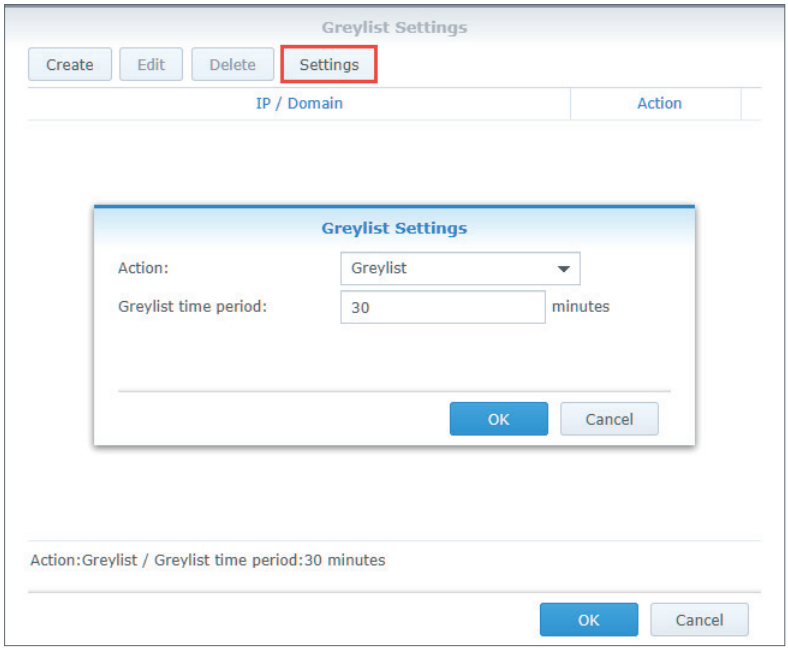
다음 단계를 참조하여 그레이리스트를 활성화하십시오 .

1. **보안** > **스팸**으로 이동하고 **그레이리스트를 활성화하여 의심되는 수신 메일을 일시적으로 거부하여 스팸 감지 강화** 확인란을 선택합니다 .



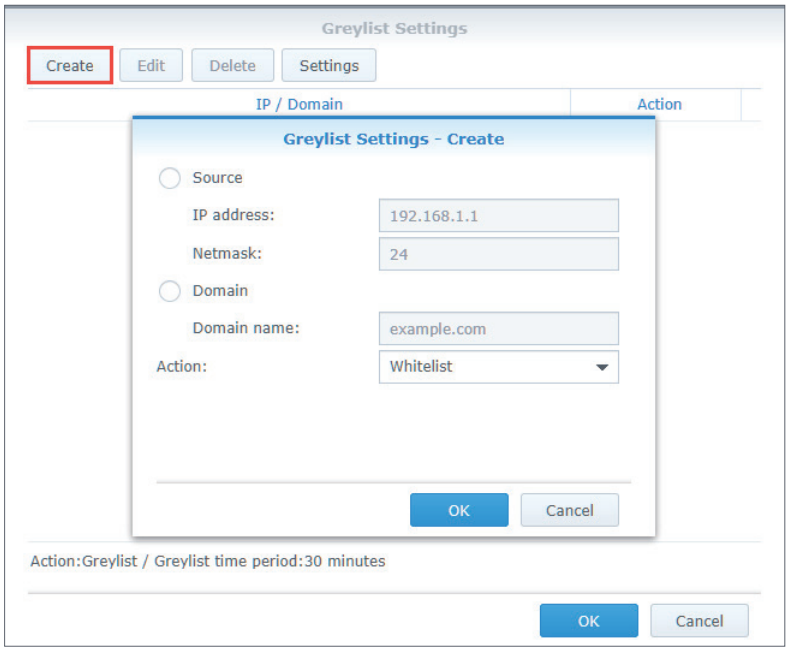

2. **그레이리스트 설정** 버튼을 클릭하여 특정 IP 주소 또는 도메인 이름의 모든 소스 또는 작업에 기본 작업을 설정합니다 .

3. **그레이리스트 설정** 창에서 **설정** 버튼을 클릭하여 모든 소스에 기본 작업을 설정합니다 .




4. **동작** 드롭다운 메뉴에서 기본 작업을 선택합니다 . **회색 목록 간격** 필드에 그레이리스트 지연 시간을 입력합니다 . 이 시간은 모든 그레이리스트 작업에 적용됩니다 .

5. **생성**을 클릭하여 특정 보낸 사람 소스에 다른 작업을 설정합니다 . 특정 사용자에 기본 작업 외 다른 그레이리스트 명령을 설정할 수 있습니다 .




6. 팝업 창에서 보낸 사람 소스를 선택하고 **동작** 드롭다운 메뉴에서 작업을 선택합니다 .

**참고 :**

- 여기서는 메시지의 **MAIL FROM** 에서가 아닌 DNS 를 통해 검색된 IP 주소에서 도메인 소스를 가져옵니다 .

7. **확인**을 클릭하여 설정을 완료합니다 .

# 안티 바이러스 검사

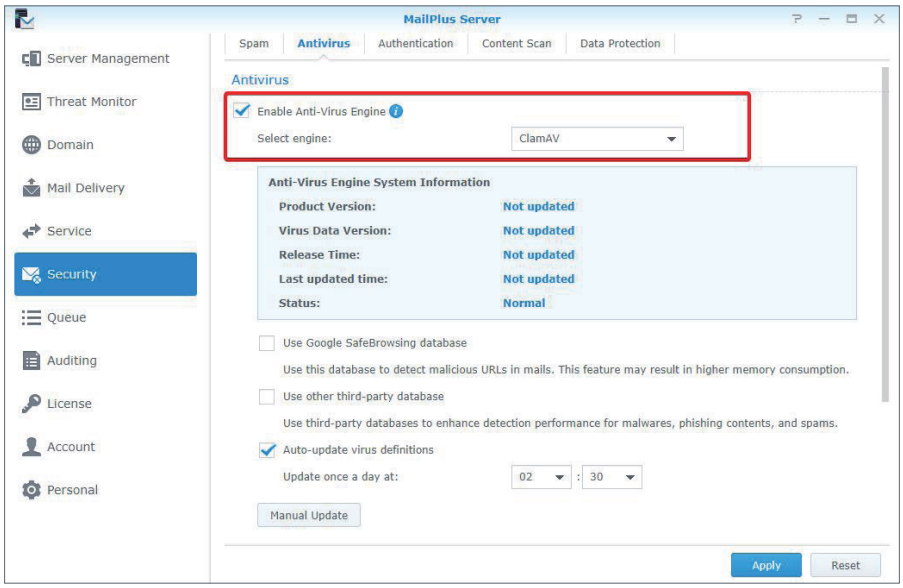
MailPlus Server 는 맬웨어 위협으로부터 보호하기 위해 무료 안티 바이러스 엔진인 ClamAV 와 유료 구독 기반 안티 바이러스 엔진인 McAfee 를 제공합니다 . 바이러스 감지 시 수행할 작업을 설정할 수 있습니다 .

안티 바이러스 감지를 통해 이메일에 악성 소프트웨어나 맬웨어가 포함되어 있는지 검사할 수 있습니다 .

- **ClamAV**: ClamAV 는 MailPlus Server 의 기본 안티 바이러스 시스템으로 , 무료로 서버를 완벽하게 보호합니다 .
- **McAfee**: MailPlus Server 는 유료 안티 바이러스 패키지인 **Antivirus by McAfee** 와 통합되어 있습니다 . **Antivirus by McAfee** 를 구독하고 안티 바이러스 엔진으로 **McAfee** 를 선택하면 편리한 관리 , 안티 바이러스 예약 , 로그 및 고급 설정을 수행할 수 있습니다 . MailPlus Server 는 검사 시간이 증가하지 않도록 20MB 이상의 이메일을 검사하지 않습니다 .

## 안티 바이러스 엔진 활성화

1. **보안** > **안티 바이러스**로 이동하고 **안티 바이러스 엔진 활성화** 확인란을 선택합니다 .

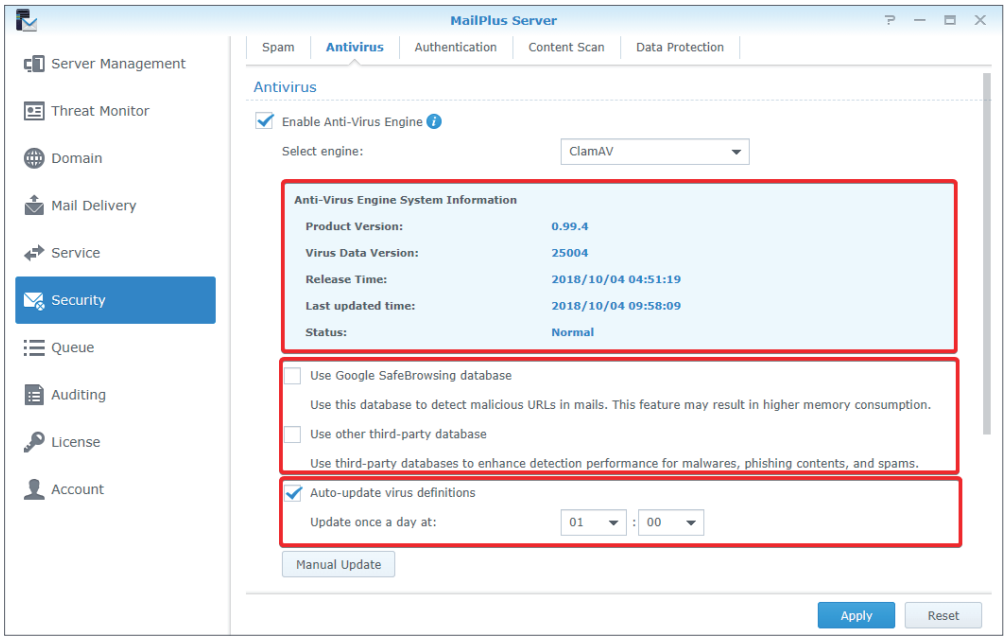



2. **엔진 선택** 드롭다운 메뉴에서 다음 중 하나를 선택합니다 .
   - **ClamAV**: ClamAV 는 MailPlus Server 에서 지원하는 무료 안티 바이러스 엔진입니다 .
   - **McAfee**: McAfee 는 추가 설치가 필요한 구독 기반 안티 바이러스 엔진입니다 . **패키지 센터**로 이동하여 **Antivirus by McAfee** 를 설치하십시오 .
3. 다음 섹션을 참조하여 설정을 완료하십시오 .

## ClamAV

ClamAV 를 안티 바이러스 엔진으로 선택한 경우 다음 단계를 참조하여 설정을 구성하십시오 .

1. **안티바이러스 엔진 시스템 정보**에서 안티 바이러스 엔진 정보를 확인할 수 있습니다 . 안티 바이러스 엔진을 정기적으로 업데이트하십시오 .
2. ClamAV 는 다음 외부 데이터베이스를 사용하여 감지 정확도를 높입니다 .
   - **Google 세이프 브라우징 데이터베이스 사용** : 통합된 Google 세이프 브라우징 데이터베이스를 사용하여 메시지에 악성 링크가 포함되어 있는지 감지합니다 .
   - **다른 타사 데이터베이스 사용** : Sanesecurity 및 기타 **타사 데이터베이스**를 사용하여 바이러스 탐지를 강화합니다 .
3. 바이러스 정의를 자동 또는 수동으로 업데이트할 수 있습니다 .
   - **바이러스 정의 자동 업데이트** : 시스템이 일별 스케줄에 따라 최신 바이러스 정의 파일을 다운로드할 수 있도록 자동 업데이트를 활성화합니다 .
   - **수동 업데이트** : 바이러스 정의를 즉시 업데이트하려면 이 버튼을 클릭합니다 .

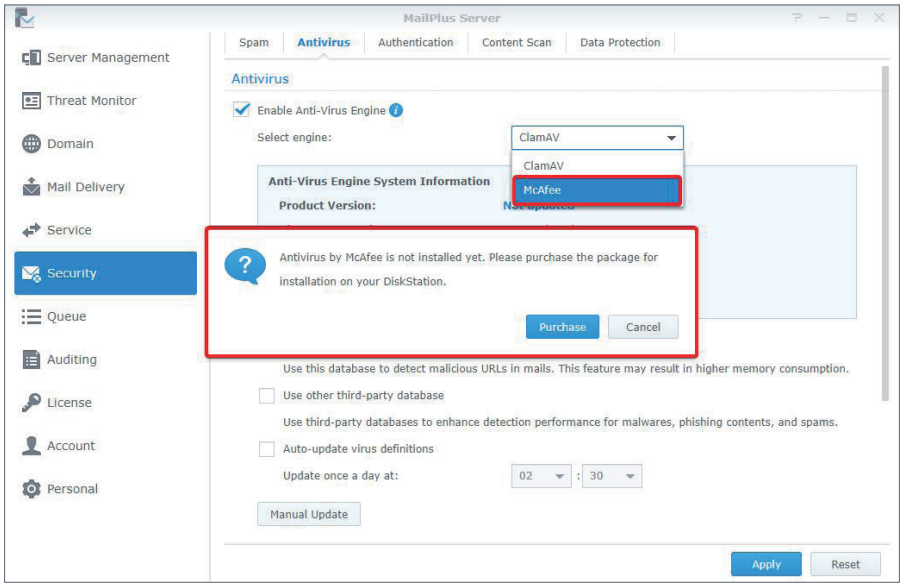



4. **적용**을 클릭하여 설정을 저장합니다 .

## McAfee

안티 바이러스 엔진으로 McAfee 를 선택하려면 **패키지 센터**로 이동하여 패키지를 구매해야 합니다 .

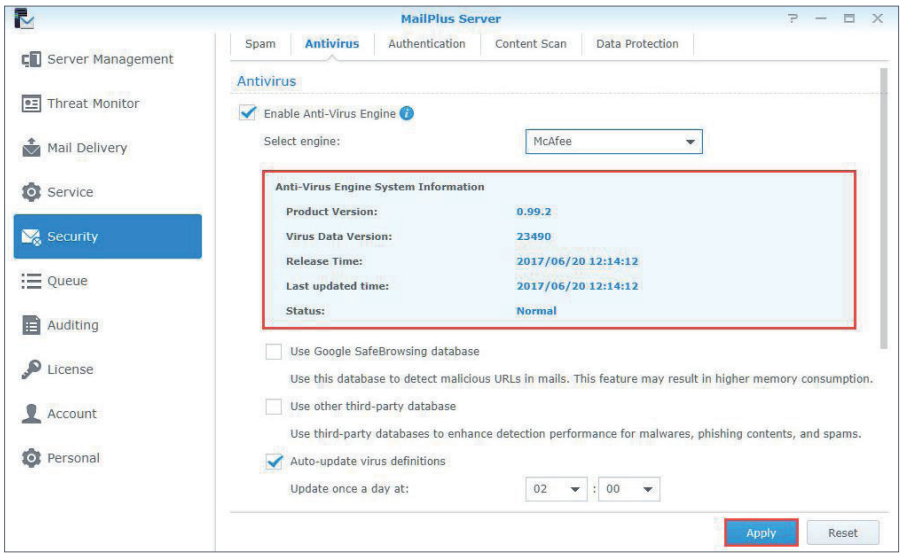
1. McAfee 를 설치하지 않았거나 라이센스가 만료된 경우 **패키지 센터**로 이동하여 **Antivirus by McAfee** 를 설치하고 **Synology 계정**을 사용하여 라이센스를 구매하라는 경고 창이 나타납니다 .




2. **안티 바이러스 엔진 시스템 정보**에서 McAfee 정보를 확인할 수 있습니다 .

**참고 :**

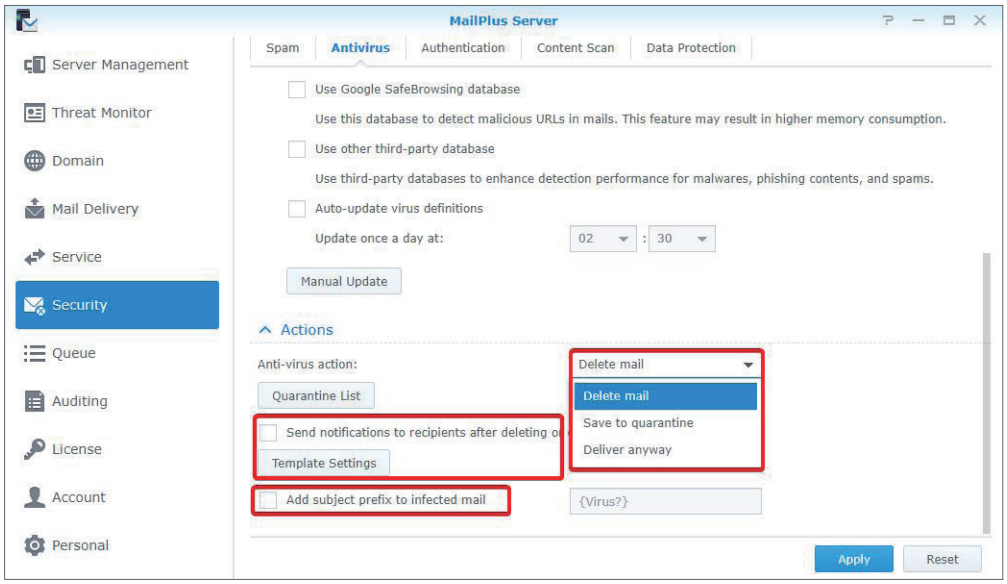
- **Antivirus by McAfee** 패키지에서 McAfee 설정을 구성해야 합니다 .
- 상태가 비정상이면 ( 라이센스 문제 또는 손상된 바이러스 정의 파일 등이 원인 ) **Antivirus by McAfee** 에서 메시지를 검사하지 않습니다 . 문제를 해결하거나 ClamAV 로 다시 전환하십시오 . 사용자가 수동으로 **Antivirus by McAfee** 를 비활성화하면 MailPlus Server 는 자동으로 ClamAV 로 전환합니다 .




3. **적용**을 클릭하여 설정을 저장합니다 .

## 안티 바이러스 작업 설정

1. **보안** > **안티 바이러스**로 이동합니다 .
2. **바이러스 방지 작업** 드롭다운 메뉴에서 바이러스가 포함된 이메일에 수행할 작업을 선택합니다 .
   - **메일 삭제** : 이메일을 삭제합니다 .
   - **검역소에 저장** : 이메일을 차단하고 검역소 섹션에 저장합니다 .
   - **무조건 배달** : 이메일을 전달합니다 .
3. **메일 삭제** 또는 **검역소에 저장**을 선택한 경우 **바이러스를 삭제 또는 격리한 후 수신자에게 알림 전송** 확인란을 선택하면 상황을 알릴 수 있습니다 . 원본 이메일의 받는 사람에게 알림 메시지가 전송됩니다 . 아래 **템플릿 설정** 버튼을 클릭하여 격리된 이메일과 삭제된 이메일에 해당하는 알림 메시지 템플릿을 조정할 수 있습니다 .
4. **무조건 배달**을 선택한 경우 **주제 접두어를 감염된 메일에 추가** 확인란을 선택하면 의심스러운 이메일에 레이블을 지정할 수 있습니다 .

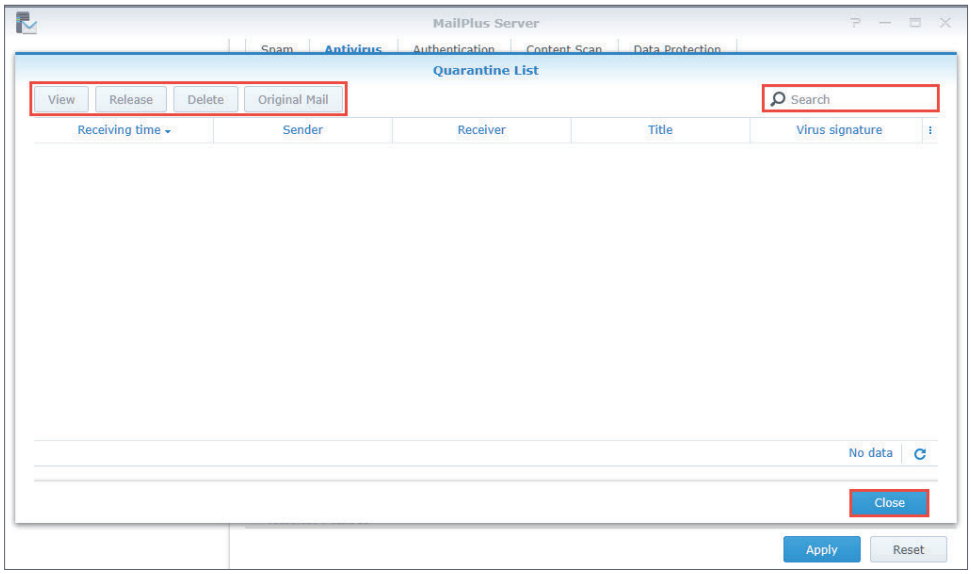



5. **적용**을 클릭하여 설정을 저장합니다 .

## 격리 목록

격리 섹션에 이메일을 저장한 경우 격리된 이메일을 보고 관리할 수 있습니다 . 다음 지침을 참조하여 격리 목록 설정을 조정하십시오 .

1. **보안** > **안티 바이러스**로 이동하고 **격리 목록** 버튼을 클릭합니다 .
2. **격리 목록** 창 오른쪽 위 구석에 있는 검색 창에서 보낸 사람 , 받는 사람 , 제목 및 바이러스 정의를 검색할 수 있습니다 .
3. 격리된 이메일을 선택하고 **보기** 또는 **원본 메일** 버튼을 클릭하여 콘텐츠를 확인합니다 .
4. 이메일 콘텐츠에 따라 다음 작업 중 하나를 선택합니다 .
   - **해제** : 이메일을 받는 사람으로 해제합니다 .
   - **삭제** : 이메일을 삭제합니다 .




5. **닫기**를 클릭하여 설정을 완료합니다 .

# 인증

인증 목적은 사기 메시지를 차단하고 ID 도용으로부터 보호하기 위해 보낸 사람의 ID 를 확인하기 위함입니다 .

- **SPF( 보낸 사람 정책 프레임워크 )**: SPF 메커니즘은 보낸 사람 호스트의 적법성을 확인합니다 . 다양한 도메인의 SPF 레코드는 현재 DNS 에 게시되어 있으며 도메인을 사용하여 이메일을 보낼 수 있는 권한이 있는 호스트의 위치를 제공합니다 . 따라서 네트워크의 호스트에서 메시지를 MailPlus Server 로 배달하면 시스템은 DNS 에서 보낸 사람 도메인의 SPF 레코드를 확인하고 호스트에 이 도메인을 사용하여 이메일을 보낼 수 있는 권한이 있는지 확인합니다 . SPF 인증이 실패하면 SPF 레코드에 따라 **fail** 또는 **softfail** 로 분류되며 시스템은 두 결과를 다르게 처리합니다 .
- **DKIM( 도메인키 식별 메일 )**: DKIM 메커니즘은 암호화 방법으로 보낸 사람 ID 를 확인하여 이메일 콘텐츠 수정 여부를 확인합니다 . DKIM 메커니즘을 사용하면 보낸 사람 호스트는 공개 키와 개인 키 집합을 생성하고 DNS 에 공개 키를 게시하는 동시에 개인 키를 사용하여 이메일에 첨부할 디지털 서명을 만듭니다 . 수신 호스트가 메시지를 받으면 DNS 에서 보낸 사람 도메인의 공개 키를 확인하고 공개 키를 사용하여 서명 , 보낸 사람 ID 및 메시지 수정 여부를 확인합니다 .
- **DMARC(Domain-Based Message Authentication, Reporting & Conformance)**: DMARC 메커니즘은 SPF 및 DKIM 검증 방법을 기반으로 합니다 . 시스템에서 메시지를 수신하면 보낸 사람이 SPF 및 DKIM 확인을 통과했는지 여부를 확인하여 보낸 사람에 사기성이 있는지 확인합니다 .

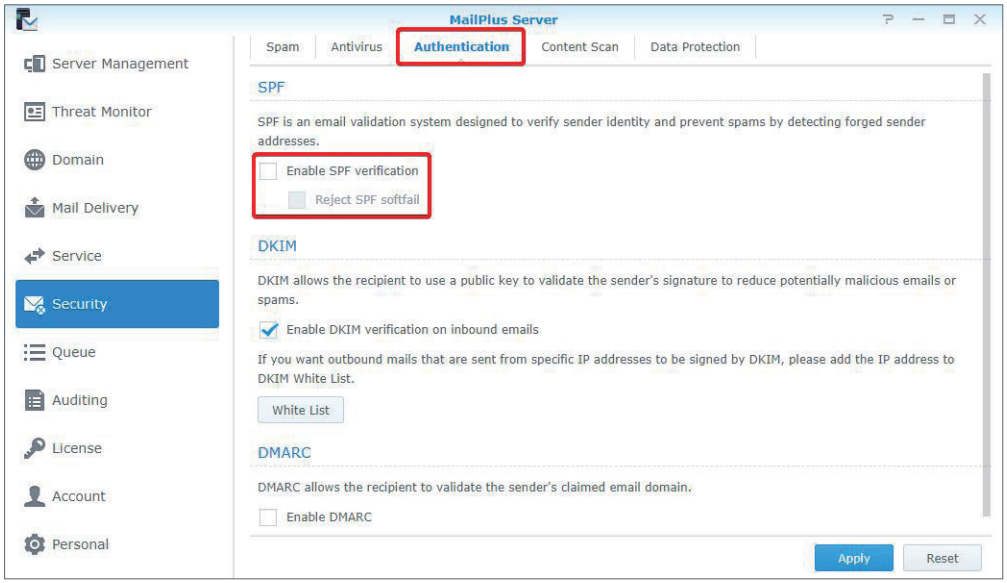
## SPF

SPF 검증을 활성화하면 시스템은 이메일 사기를 방지하기 위해 DNS 에서 보낸 사람 도메인의 SPF 레코드를 확인할 수 있습니다 . SPF 검증이 실패하면 결과는 **fail** 또는 **softfail** 로 식별됩니다 . 아래 단계를 참조하여 SPF 검증 설정을 조정하십시오 .

**참고 :**

- MailPlus Server 가 다른 메일 서버에서 전달된 메시지를 수신하도록 설정된 경우 릴레이 서버 위치가 보낸 사람의 SPF 레코드에 포함되어 있지 않으면 SPF 메커니즘은 릴레이된 메시지를 차단할 수 있습니다 . ( 자세한 내용은 **이 문서**를 참조하십시오 .) 릴레이 서버를 화이트리스트에 추가하거나 SPF 검증을 비활성화하십시오 .

1. **보안** > **인증**으로 이동합니다 .
2. **SPF** 섹션에서 **SPF 검증 활성화** 확인란을 선택합니다 .
   - 검증 결과가 **fail** 이면 메시지가 거부됩니다 .
   - 검증 결과가 **softfail** 이면 **SPF softfail 거부** 확인란을 선택하여 **softfail** 메시지를 거부할 수 있습니다 . 그렇지 않으면 **softfail** 결과의 모든 메시지가 수신됩니다 .

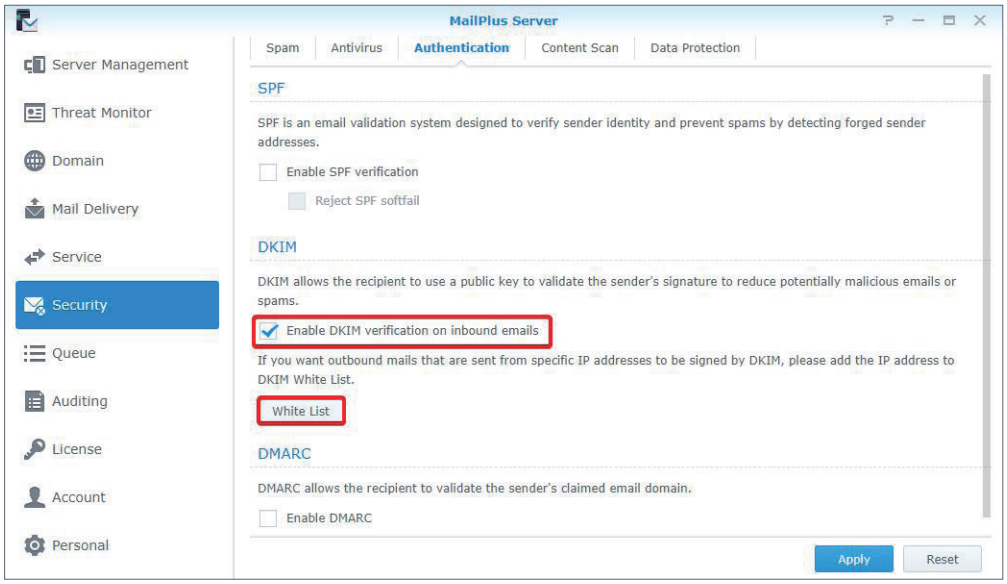



3. **적용**을 클릭하여 설정을 저장합니다 .

## DKIM

DKIM 검증을 활성화하면 메시지 수정을 방지하고 ID 도용으로부터 보호할 수 있습니다 . 아래 단계를 참조하여 DKIM 검증 설정을 조정하십시오 .

1. **보안** > **인증**으로 이동합니다 .
2. 인바운드 메시지의 보낸 사람 ID 를 확인하고 알 수 없는 소스에서 보낸 메시지를 줄이려면 **DKIM** 섹션에서 **인바운드 이메일에서 DKIM 검증 활성화** 확인란을 선택합니다 .
3. **DKIM 확인을 위한 최소 키 길이** 값을 선택합니다 . DKIM 서명의 키 길이가 선택한 값보다 짧으면 DKIM 에서 이메일을 거부합니다 . 최소 키 길이를 늘리면 보안 수준이 낮은 도메인에서 보낸 이메일이 DKIM 검증을 통과할 수 없습니다 .
4. **화이트리스트** 버튼을 클릭하여 특정 보낸 사람이 인증을 통과하고 DKIM 서명을 메시지에 첨부할 수 있도록 화이트리스트에 특정 IP 주소 범위를 추가합니다 . 범위 내 호스트가 아웃바운드 메시지를 보내도록 MailPlus Server 에 연결되면 시스템은 메시지에 DKIM 서명을 첨부합니다 .




5. **적용**을 클릭하여 설정을 저장합니다 .

> **참고 :**
>
> - MailPlus 2.1 이상 버전에서는 DKIM 에서 거부된 이메일이 **스팸** 사서함으로 이동합니다 . MailPlus 클라이언트에서 이러한 이메일이 확인되면 경고가 표시됩니다 .

### DMARC

DMARC 는 SPF 및 DKIM 검증을 기반으로 하므로 도메인에 SPF 를 설정하고 공개 키를 생성하여 아웃바운드 이메일에 DKIM 서명을 활성화한 후에 DMARC 설정을 진행하십시오 . 다음 단계를 참조하여 DMARC 검증을 활성화하십시오 .

1. **보안** > **인증**으로 이동합니다 .
2. **DMARC 활성화** 확인란을 선택하여 DMARC 를 활성화합니다 .

> **참고 :**
>
> - MailPlus 2.1 이상 버전에서는 DMARC 에 의해 격리된 이메일은 **스팸** 사서함으로 이동합니다 . MailPlus 클라이언트에서 이러한 이메일이 확인되면 경고가 표시됩니다 .

## 콘텐츠 보호

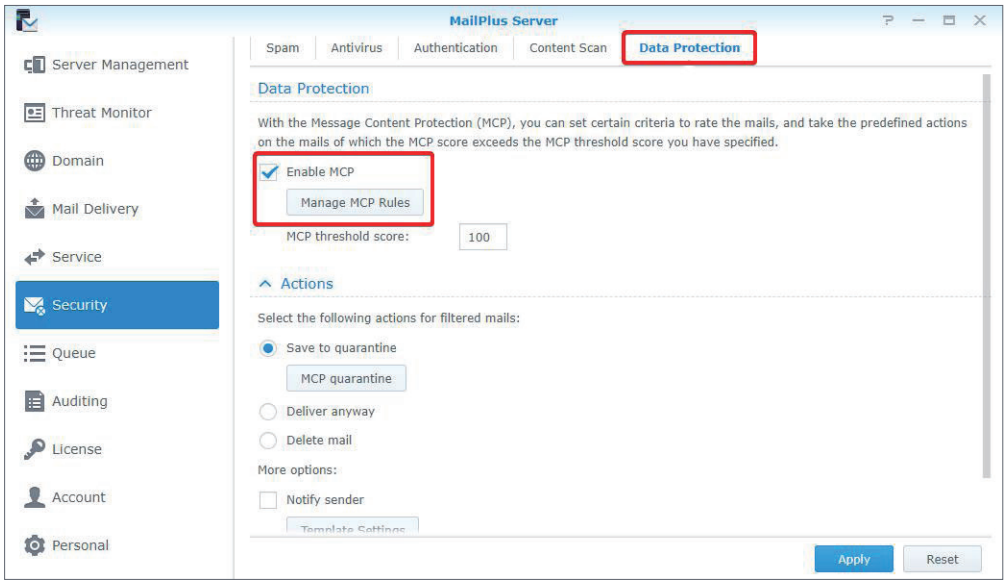
콘텐츠 보호 기능은 사용자 설정에 따라 의심스러운 이메일을 필터링할 수 있습니다 .

- **MCP 규칙** : 원본 이메일의 콘텐츠를 기준으로 검색합니다 . 의심스러운 콘텐츠가 너무 많이 식별되면 이메일은 격리 섹션에 배치되거나 기타 지정된 작업이 수행됩니다 .
- **첨부 파일 필터** : 첨부 파일 형식에 따라 이메일 메시지를 필터링합니다 .
- **콘텐츠 검사** : 이메일 콘텐츠 검사 기능을 강화합니다 . 보안이 강화되도록 피싱 링크나 HTML 태그가 포함된 이메일을 거부하거나 다시 작성합니다 .

## MCP 규칙

MCP(Message Content Protection) 규칙을 설정하고 MCP 임계값 점수를 지정합니다 . 이메일이 규칙 기준과 일치하면 규칙 점수가 총 MCP 점수에 합산됩니다 . 총 점수가 MCP 임곗값 점수를 초과하면 시스템에서 이메일을 필터링하거나 차단합니다 . 다음 단계를 참조하여 MCP 를 활성화하고 관리하십시오 .

1. **보안** > **데이터 보호**로 이동하고 **데이터 보호** 섹션에서 **MCP 활성화** 확인란을 선택합니다 .
2. **MCP 임계값 점수** 필드에 점수를 입력합니다 .
3. **MCP 규칙 관리** 버튼을 클릭하여 새 규칙을 추가합니다 .




4. **MCP 규칙 관리** 창에서 **생성** 버튼을 클릭합니다 .
5. **MCP 규칙 추가** 창에는 다음 항목이 포함됩니다 .
   - **이름** : 규칙 이름을 입력합니다 .
   - **대상** : **대상** 드롭다운 메뉴에서 이메일 섹션을 일치시킬 대상으로 선택합니다 .

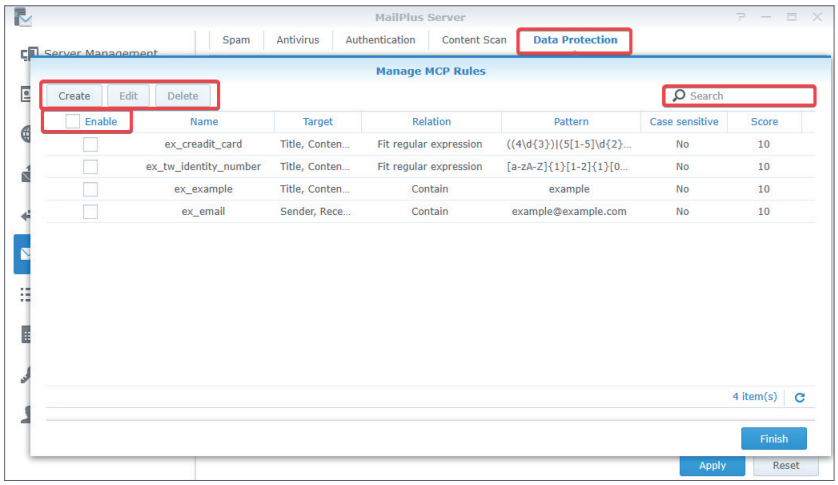
| 섹션 | 설명 |
|---|---|
| **제목** | 이메일 메시지 제목 |
| **내용 ( 제목 포함 )** | 이메일 메시지 콘텐츠 및 제목 |
| **보낸 사람** | 이메일 메시지 보낸 사람 |
| **받는 사람** | 이메일 메시지 받는 사람 |
| **사용자 지정 헤더** | 원본 이메일 메시지의 특정 머리글 |

   - **사용자 지정 헤더** : **대상** 드롭다운 메뉴에서 **사용자 지정 헤더**를 선택하면 **사용자 지정 헤더** 필드가 나타납니다 . 여기에 특정 머리글을 입력합니다 .
   - **관계** : **관계** 드롭다운 메뉴에서 일치 기준을 선택합니다 .

| 기준 | 설명 |
| --- | --- |
| **포함** | 이메일의 대상 섹션에 일치하는 콘텐츠가 포함되면 이메일이 규칙과 일치합니다 . |
| **같음** | 이메일의 대상 섹션이 일치하는 콘텐츠와 동일하면 이메일이 규칙과 일치합니다 . |
| **정규식 맞춤** | 이메일의 대상 섹션에 일치하는 콘텐츠가 포함되면 이메일이 규칙과 일치합니다 . 일치하는 콘텐츠에 정규식을 사용할 수 있습니다 . |

- **패턴** : 규칙에 일치하는 콘텐츠를 입력합니다 .
- **대소문자 구분** : **예** 또는 **아니요**를 선택하여 일치가 대소문자를 구분하는지 결정합니다 .
- **점수** : 이 규칙 기준이 일치하면 생성되는 점수를 지정합니다 .

6. **확인**을 클릭하여 규칙 만들기를 완료합니다 .
7. **MCP 규칙 관리** 창에서 규칙을 생성 , 활성화 , 편집 또는 삭제할 수 있습니다 . 또한 오른쪽 위 구석에 있는 검색 창에서 규칙을 검색할 수 있습니다 .



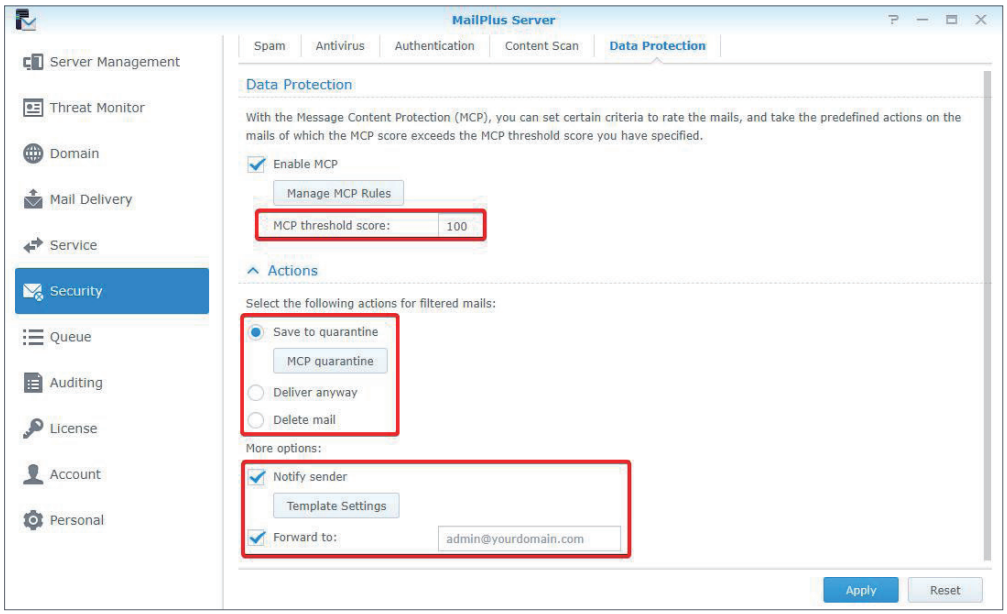

8. **마침**을 클릭하여 설정을 완료합니다 .

## 동작

일치하는 규칙 총점이 **MCP 임계값 점수**를 초과하면 특정 작업이 수행됩니다 . 다음 단계를 참조하여 작업을 설정하십시오 .

1. **보안** > **데이터 보호**로 이동하고 **데이터 보호** 섹션의 **MCP 임계값 점수** 필드에 점수를 입력합니다 .
2. **작업** 섹션에서 **MCP 임계값 점수**가 초과되면 수행할 작업을 설정할 수 있습니다 .
   - **검역소에 저장** : 이메일 메시지를 차단하고 검역소 섹션에 저장합니다 . **MCP 격리** 버튼을 클릭하면 격리 메시지 콘텐츠를 확인할 수 있습니다 . 격리된 메시지를 관리하는 방법에 대한 자세한 내용은 **격리 목록**을 참조하십시오 .
   - **무조건 배달** : 이메일 메시지를 배달합니다 .
   - **메일 삭제** : 이메일 메시지를 삭제합니다 .
   - **기타 옵션** : 보낸 사람에게 알리거나 이메일 메시지를 특정 사서함으로 전달합니다 .

| 기능 | 설명 |
| --- | --- |
| **보낸 사람 알림** | 이메일이 차단되었다는 알림 이메일을 보낸 사람에게 보내 이를 알립니다 . **템플릿 설정** 버튼을 클릭하면 알림 콘텐츠를 설정할 수 있습니다 . |
| **전달할 위치** | 원본 이메일을 특정 사서함으로 전달합니다 . |

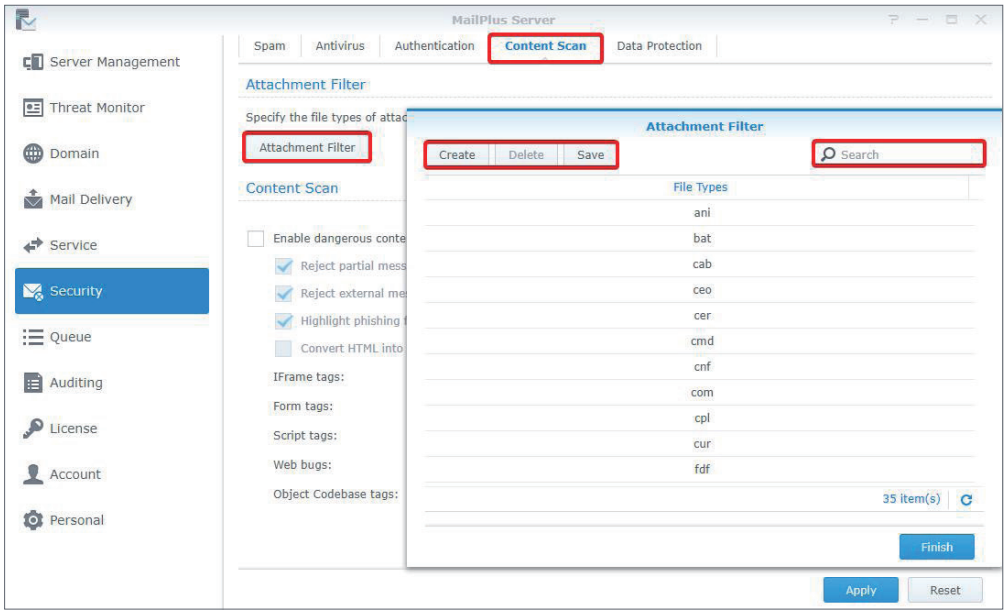



3. **적용**을 클릭하여 설정을 저장합니다 .

## 첨부 파일 필터

이 첨부 파일 필터 기능은 첨부 파일 형식을 기준으로 메시지를 차단합니다 . 다음 단계를 참조하여 첨부 파일 필터를 설정하십시오 .

1. **보안** > **콘텐츠 검사**로 이동합니다 .
2. **첨부 파일 필터** 섹션에서 **첨부 파일 필터** 버튼을 클릭합니다 .
3. **첨부 파일 필터** 창에서 **생성** 버튼을 클릭하여 새 파일 형식을 추가합니다 . **삭제**할 파일 형식을 선택하거나 오른쪽 위 구석에서 특정 파일 형식을 검색할 수 있습니다 .




4. **저장**을 클릭합니다 .

5. **마침**을 클릭하여 설정을 완료합니다 .

## 콘텐츠 검사

콘텐츠 검사 기능은 의심스러운 메시지를 차단하거나 콘텐츠를 수정합니다 . 아래 단계를 참조하여 **콘텐츠 검사** 설정을 조정하십시오 .

> **참고 :**
> - 수정된 콘텐츠가 예상을 충족할 수 없습니다 . 필요에 따라 기능을 활성화했는지 확인하십시오 .

1. **보안** > **콘텐츠 검사**로 이동합니다 .

2. **콘텐츠 검사** 섹션에서 **위험한 콘텐츠 검사 활성화** 확인란을 선택하고 다음 설정을 조정합니다 .

   - **부분 메시지 거부** : 불완전한 메시지 여러 개로 분할된 이메일을 거부합니다 ( 특히 머리글 메시지 / 부분의 Content-Type 값이 있는 이메일 메시지 ).
   - **외부 메시지 본문 거부** : 외부 리소스를 가리키는 이메일을 거부합니다 ( 특히 메시지 / 외부 본문의 Content-Type 값이 있는 이메일 메시지 ).
   - **피싱 사기 강조** : 이메일에서 감지된 피싱 링크를 강조 표시하여 받는 사람에게 알립니다 .
   - **HTML 을 일반 텍스트로 변환** : HTML 형식의 메시지를 일반 텍스트로 변환합니다 .
   - 각 태그에 다음 작업 중 하나를 설정할 수 있습니다 .

| 작업 | 설명 |
|---|---|
| **허용** | 메시지를 배달합니다 . |
| **거부** | 메시지를 거부합니다 . |
| **태그 무효화하기** | 태그를 무효화한 후 메시지를 배달합니다 . |

**참고 :**

- 각 태그의 설정을 지정하십시오 .

# 10 장 : 설정 모니터링

## 서버 상태 모니터링

그래픽 인터페이스를 통해 서버 작업 상태를 빠르게 감독할 수 있습니다 .

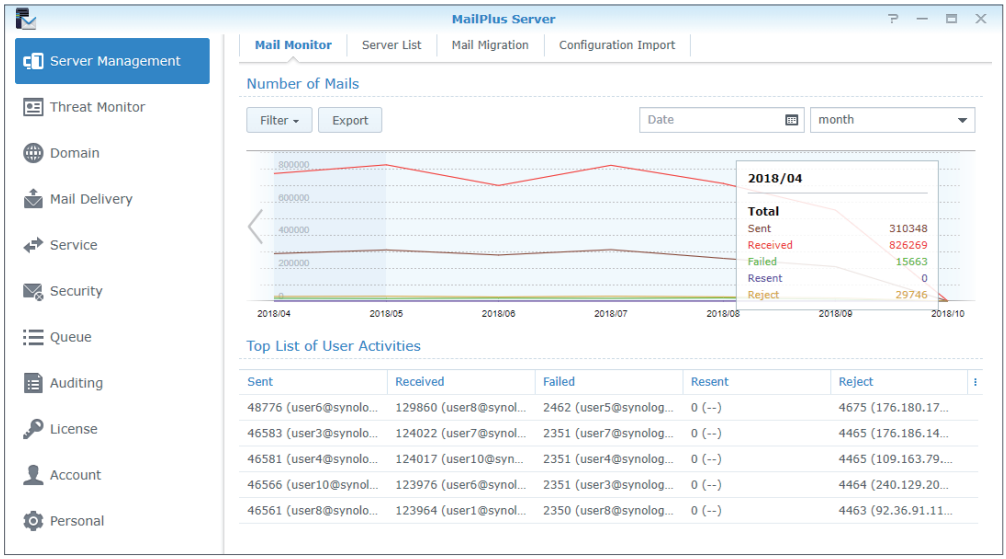
- **메일 트래픽 모니터링** : 특정 시간 간격으로 서버의 메일 트래픽을 모니터링합니다 .
- **위협 모니터링** : 서버의 각 보안 설정에 의해 차단된 이메일 위협 수를 표시합니다 . 모든 위협 소스를 빠르게 식별하고 그에 따라 보안 설정을 조정할 수 있습니다 .
- **서버 목록** : 서버 클러스터 목록 및 해당 작업 상태를 표시합니다 .

### 메일 트래픽 모니터링

**서버 관리**의 **메일 모니터링** 탭에는 지난 기간 동안의 메일 활동 통계가 표시됩니다 . **최상위 사용자 활동 목록** 섹션에 각 트래픽 유형에서 가장 활성화된 이메일 주소 목록이 표시됩니다 . 이메일 트래픽 유형에 대한 자세한 내용은 **메일 로그 보기**를 참조하십시오 .

**참고 :**

- **High-availability 클러스터**를 이미 설정했으면 기본 서버에서 로그를 확인하십시오 .



### 다양한 시간 간격으로 트래픽 모니터링

**시** , **일** , **주** 또는 **월**을 기준으로 MailPlus Server 에서 이메일 트래픽을 모니터링할 수 있습니다 . **메일 수** 차트의 모든 데이터 포인트는 시간 간격 동안의 총 이메일 수 ( 특정 이메일 트래픽 유형 ) 를 나타냅니다 . 아래 단계를 참조하여 시간 간격을 조정하십시오 .

1. **서버 관리** > **메일 모니터링**으로 이동합니다 .
2. **날짜** 필드와 **메일 수** 섹션의 오른쪽 위 구석에 있는 드롭다운 메뉴에서 날짜 및 시간 간격을 선택하면 됩니다 .

### 특정 시간 간격에서 트래픽 모니터링

다음 두 가지 방법을 사용하여 특정 시점을 모니터링할 수 있습니다 .

1. 차트 왼쪽 또는 오른쪽 끝에 커서를 올려놓고 화살표 아이콘을 클릭하여 다른 시점으로 이동합니다 .
2. **메일 수** 섹션의 오른쪽 위 구석에 있는 **날짜** 필드에서 원하는 날짜를 선택합니다 .

**참고 :**

- MailPlus Server 는 서로 다른 시간 동안 메일 데이터를 여러 개 예약합니다 . 사용 가능한 데이터가 있는 시간 간격으로만 전환할 수 있습니다 .

### 특정 시간의 상세 데이터 표시 고정

차트 세부 정보 패널에 표시되는 데이터는 마우스를 다른 시점에 올려놓으면 변경됩니다 . 선택한 시간 간격에 대한 자세한 정보를 보려면 커서를 원하는 시간 간격으로 이동하고 마우스 왼쪽 버튼을 클릭하여 세부 정보 패널을 고정합니다 .

### 특정 트래픽 유형의 데이터 표시 또는 숨기기

1. **서버 관리** > **메일 모니터링**으로 이동합니다 .
2. **메일 수** 섹션에서 **필터** 버튼을 클릭하고 확인란을 선택하여 특정 트래픽 유형의 데이터를 표시하거나 숨깁니다 .

### 특정 시간 간격에서 데이터 내보내기

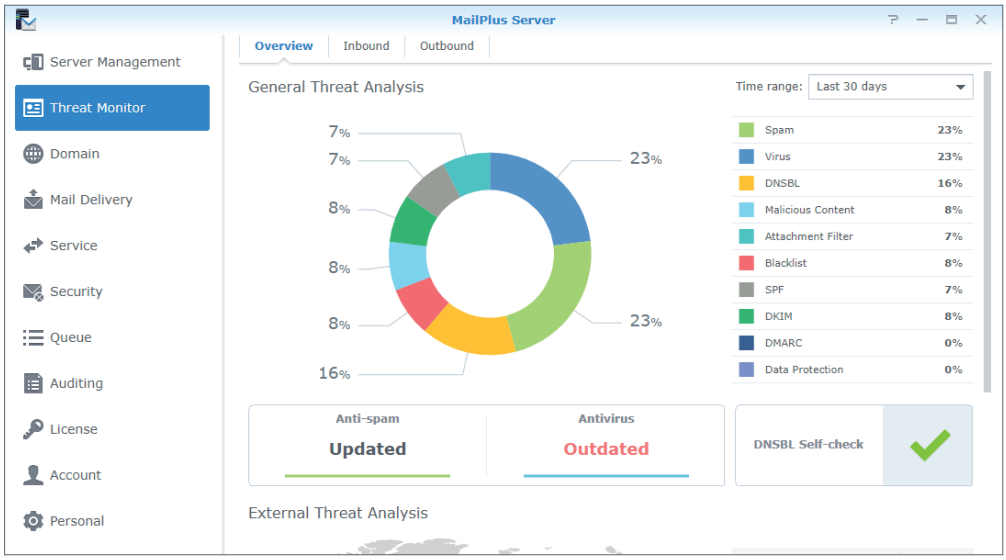
1. **서버 관리** > **메일 모니터링**으로 이동합니다 .
2. **메일 수** 섹션의 차트에서 추가로 조사할 시간 간격을 클릭합니다 .
3. 상단에 있는 **내보내기** 버튼을 클릭합니다 .
4. MailPlus Server 는 데이터를 .html 파일로 내보냅니다 .

## 위협 모니터링

이메일 위협 및 해당 소스에 대한 자세한 내용은 **위협 모니터링**에 표시됩니다 . MailPlus Server 를 보호하도록 위협 분석에 따라 설정을 조정할 수 있습니다 .

**참고 :**

- **High-availability 클러스터**를 이미 설정했으면 기본 서버에서 로그를 확인하십시오 .




## 일반 위협 분석 보기

**일반 위협 분석**은 아웃바운드 이메일과 인바운드 이메일의 위협 데이터 및 통계를 그래프로 표시합니다 . 아래 단계를 참조하여 **일반 위협 분석** 설정을 조정하십시오 .

1. **위협 모니터** > **개요**로 이동합니다 .
2. 위협 데이터 및 통계와 함께 해당 설정이 **일반 위협 분석** 섹션에 표시됩니다 .
   - **시간 범위** : 이 옵션을 선택하면 특정 시간 범위에 대한 위협 통계가 표시됩니다 .
   - **위협 목록** : 각 위협 유형의 백분율 통계를 표시합니다 . 카운트 통계를 확인하려면 특정 유형에 마우스 커서를 올려놓습니다 .
   - **위협 도넛 차트** : 각 위협 유형의 백분율 통계를 표시합니다 . 필요에 맞게 오른쪽 목록에서 위협 유형을 선택하거나 선택 취소합니다 .
   - **스팸 방지 기능** : 스팸 방지 엔진 상태를 표시합니다 . 관련 설정을 수정하려면 클릭하여 해당 페이지로 이동합니다 .
   - **안티 바이러스 기능** : 안티 바이러스 엔진 상태를 표시합니다 . 관련 설정을 수정하려면 클릭하여 해당 페이지로 이동합니다 .
   - **DNSBL 자체 확인** : Synology NAS 가 DNSBL 블랙리스트에 있는지 확인합니다 . 클릭하면 상세 정보를 확인할 수 있습니다 .

## 외부 위협 분석 보기

외부 위협 분석에서는 차단된 인바운드 이메일의 원본과 해당 카운트 통계가 표시됩니다 .

1. **위협 모니터** > **개요**로 이동합니다 .
2. **외부 위협 분석** 섹션에 각 원본의 위협 맵과 카운트 통계가 표시됩니다 .
   - **위협 맵** : 각 원은 위협 원본 영역을 표시합니다 . 영역에서 보다 많은 이메일이 차단되면 원이 확장됩니다 . 카운트 통계를 보려면 마우스 커서를 원 위에 올려놓습니다 .
   - **위협 소스** : 이 목록에서는 차단된 이메일 중 상위 6 개 원본과 해당 카운트를 함께 보여줍니다 .

## 차단된 인바운드 및 아웃바운드 메일 보기

**인바운드** 및 **아웃바운드**에서는 차단된 인바운드 이메일과 아웃바운드 이메일 각각의 통계를 해당 이메일의 상위 보낸 사람 / 받는 사람과 함께 확인할 수 있습니다 .

1. **위협 모니터링**으로 이동합니다 .
2. **인바운드** 또는 **아웃바운드** 탭을 클릭합니다 .
   - **시간 범위** : 특정 기간 동안에 차단된 아웃바운드 이메일이나 인바운드 이메일의 통계를 확인하려는 시간 범위를 선택합니다 .
   - **차단된 메일 통계** : 이 차트에서는 선택한 시간 범위에서 인바운드 이메일 ( **인바운드**에서 ) 또는 아웃바운드 이메일 ( **아웃바운드**에서 ) 에 대한 각 위협 유형의 동향을 보여줍니다 .

> **참고 :**
> - 표시되는 위협 유형을 변경하려면 차트 아래의 범례를 선택하거나 선택 취소합니다 .
> - 각 위협 유형의 카운트 통계를 확인하려면 마우스 커서를 차트 위에 올려놓습니다 .

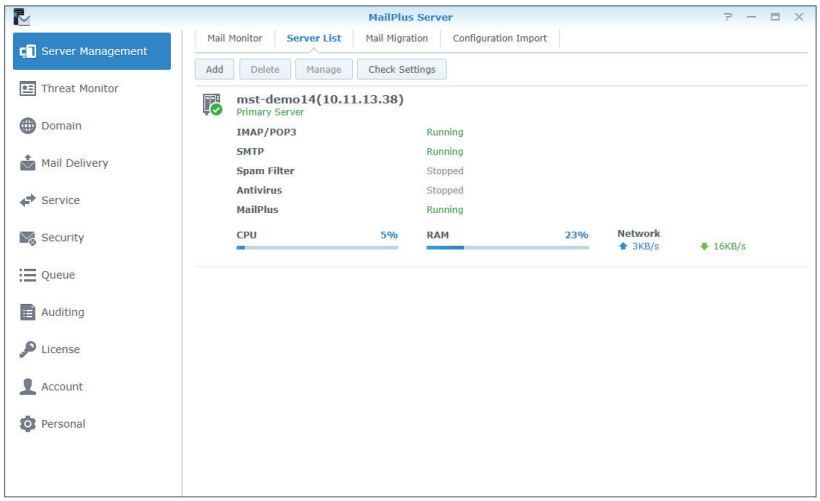
   - **차단된 메일의 상위 송신자** : 이 표에서는 차단된 인바운드 이메일 ( **인바운드**에서 ) 또는 아웃바운드 이메일 ( **아웃바운드**에서 ) 의 보낸 사람 상위 10 명을 카운트 통계와 함께 보여줍니다 . 전체 목록을 보려면 **모두 표시**를 클릭합니다 .
   - **차단된 메일의 상위 수신자** : 이 표에서는 차단된 인바운드 이메일 ( **인바운드**에서 ) 또는 아웃바운드 이메일 ( **아웃바운드**에서 ) 의 받는 사람 상위 10 명을 카운트 통계와 함께 표시합니다 . 전체 목록을 보려면 **모두 표시**를 클릭합니다 .

## 서버 목록

**서버 관리** 페이지의 **서버 목록** 탭에서 CPU, RAM 및 네트워크 사용에 대한 정보 등 MailPlus Server 의 간략한 개요를 확인할 수 있습니다 . 각 MailPlus Server 기능에서 가능한 상태는 다음 목록을 참조하십시오 .

- **실행 중** : 기능이 올바르게 실행 중입니다 .
- **중지됨** : 기능이 활성화되지 않았습니다 .
- **비정상** : 기능이 비정상입니다 .
- **설치되지 않음** : MailPlus 에만 적용됩니다 . 이 상태는 MailPlus 가 설치되어 있지 않음을 나타냅니다 .
- **준비** : 이 상태는 이 기능을 방금 활성화 또는 비활성화했으며 상태를 전환할 수 있음을 나타냅니다 .

- **메일 동기화 중** : MailPlus high-availability 클러스터를 설정하거나 제거하면 시스템에서 이메일을 동기화합니다 . 이 상태는 시스템에서 이메일을 동기화하고 있음을 나타냅니다 .



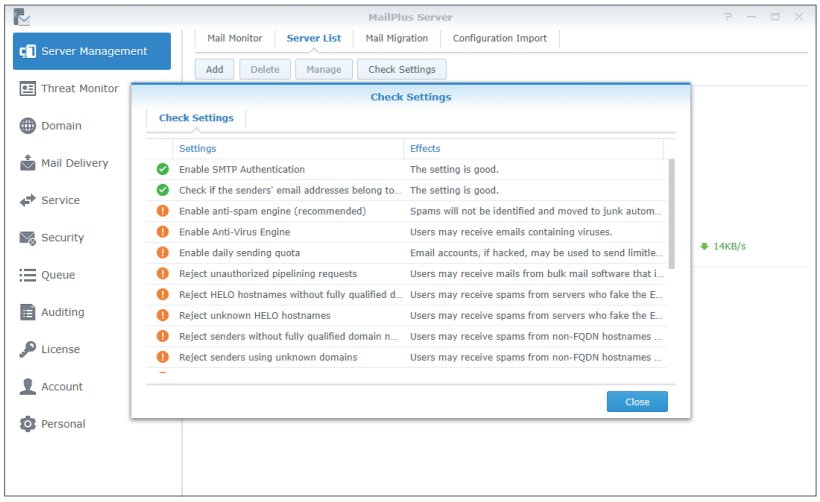

**참고 :**

- **안티 바이러스** 또는 **MCP** 가 활성화된 경우 **스팸 방지** 기능이 활성화되어 있지 않더라도 **스팸 필터**가 활성화됩니다 . 하지만 스팸 검사는 실행되지 않습니다 .

## 설정 확인

**설정 확인**에서 MailPlus Server 설정이 Synology 의 권장 설정과 동일한지 확인할 수 있습니다 . 또한 여기에서 다양한 설정 효과를 확인할 수 있습니다 . 다음 단계를 참조하십시오 .

1. **서버 관리** > **서버 목록**으로 이동합니다 .
2. **설정 확인** 버튼을 클릭합니다 .



# 메일 대기열 모니터링

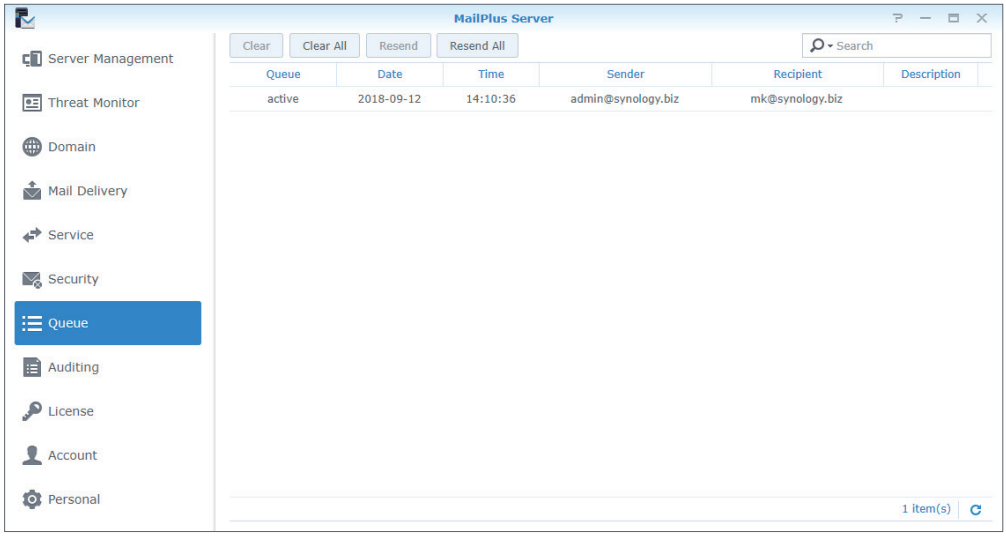
메일 대기열에서 대기 중인 이메일을 확인하고 수행할 작업을 결정할 수 있습니다 .

## 메일 대기열의 메시지 모니터링

**대기열** 페이지에서 다른 서버로 보내기 위해 대기 중이거나 이메일이 거부된 후 다른 서버로 다시 전송될 모든 이메일을 확인할 수 있습니다 .

대기열의 이메일 관련 정보는 다음과 같이 표시됩니다 .

- 이메일이 대기열에 들어온 날짜와 시간
- 이메일 보낸 사람과 받는 사람
- 메시지가 메일 대기열에 대기 중인 이유 ( **설명** 열에 이메일 배달 실패 원인이 표시됨 )




메일 대기열 상태는 다음 세 가지 유형으로 분류됩니다 .

- **보류** : 메시지를 처리해야 합니다 .
- **활성** : 현재 메시지를 처리하고 있습니다 .
- **지연됨** : 메시지를 배달하지 못했으며 나중에 다시 보냅니다 .

**참고 :**

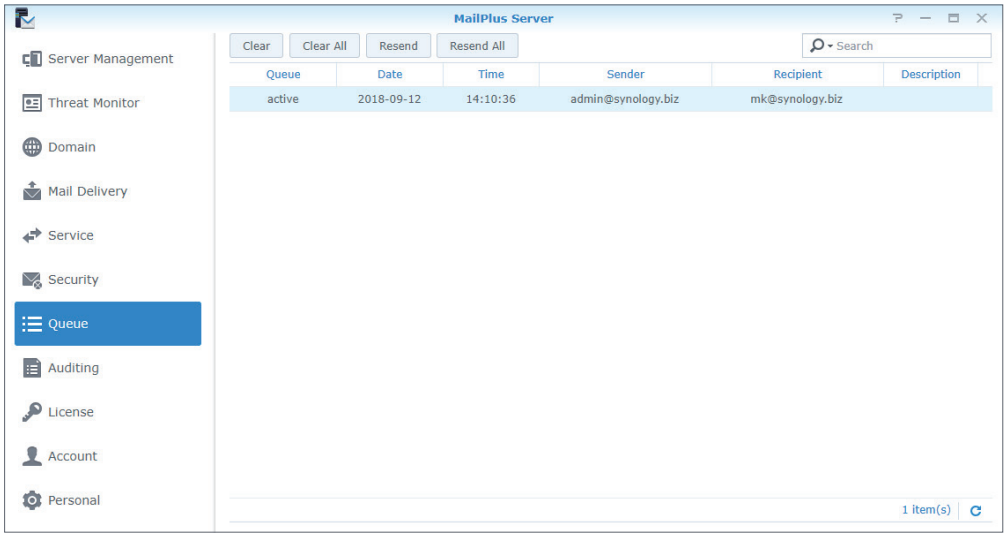
- 다음 5 일 동안 모든 다시 배달 시도가 실패하면 지연된 이메일은 보낸 사람에게 반송됩니다 .

## 메일 대기열의 메시지 관리

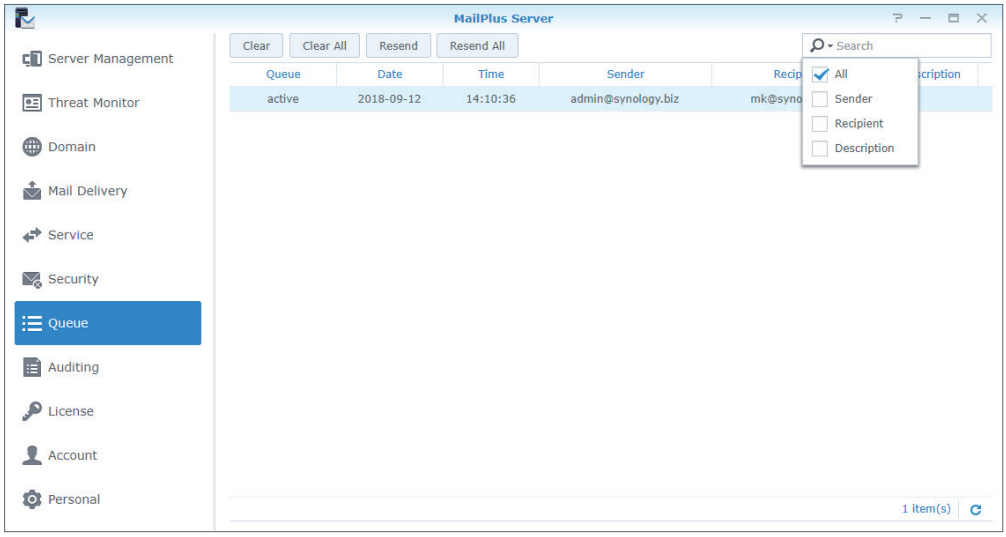
대기열의 메시지를 즉시 다시 배달하거나 배달을 취소할 수 있습니다 . 다음 단계를 참조하여 메일 대기열의 메시지를 관리하십시오 .

1. **대기열**로 이동하여 다음을 수행합니다 .

   - 메시지를 다시 배달하려면 메일 대기열에서 메시지를 선택하고 **재전송** 버튼을 클릭합니다 . 메시지 상태가 **보류**에서 **활성**으로 전환됩니다 .
   - 메시지를 제거하려면 메일 대기열에서 메시지를 선택하고 **지우기** 버튼을 클릭합니다 . 메시지가 대기열에서 제거됩니다 .
   - 모든 메시지를 다시 전송하려면 **모두 재전송** 버튼을 클릭합니다 .
   - 모든 메시지를 제거하려면 **모두 제거** 버튼을 클릭합니다 .




2. 페이지 오른쪽 위 구석에 있는 검색 창에서 메시지를 검색하여 메시지 상태를 확인할 수도 있습니다 .



# 메일 로그 모니터링

메일 로그는 서버의 모든 활동을 기록합니다 . 로그 콘텐츠를 확인하면 근본 문제와 문제 해결책을 찾을 수 있습니다 . 로그 파일이 저장소 공간을 많이 차지할 수 있습니다 .

**감사** 페이지에서 다음 로그 설정을 구성할 수 있습니다 .

- **로그 보기** : 로그에 기록된 메시지를 보고 , 검색하고 , 분석합니다 .
- **로그 보관 및 관리** : 보관 간격 , 백업 , 회전 규칙 및 보조 서버로 로그 전송과 같은 다양한 관리 설정을 구성합니다 .
- **로그 보고서** : 이메일 알림을 통해 로그를 정기적으로 전송하도록 허용합니다 .

## 메일 로그 보기

다음 단계를 참조하여 메일 로그를 확인하십시오 .

1. **감사** > **로그**로 이동합니다 .
2. 상단에 있는 드롭다운 메뉴에서 **메일 로그** 및 **내부 데이터베이스**를 선택합니다 .
3. 메일 로그에는 메시지 ID, 생성된 날짜와 시간 , 보낸 사람 , 받는 사람 , 제목 , 크기 및 각 메시지 상태가 표시됩니다 . 상태는 다음과 같이 분류됩니다 .
   - **수신됨** : 이 상태는 MailPlus 사용자가 메시지를 수신했음을 나타냅니다 . MailPlus 사용자가 다른 MailPlus 사용자에게 메시지를 보내면 로그 레코드 상태는 **수신됨**으로 표시됩니다 . 여러 MailPlus 사용자가 같은 메시지를 수신하면 로그 레코드가 여러 개 생성됩니다 . 하지만 메시지가 MailPlus Server 의 별칭 이메일 주소로 전송되면 별칭에 받는 사람 주소가 여러 개 포함되어 있고 별칭 내 일부 사용자가 다른 서버에 속해 있더라도 별칭 이메일 주소의 로그 레코드가 생성됩니다 . 자동 전달을 활성화하면 **수신됨** 상태의 로그 레코드는 **받은 편지함에 메일 사본 보관** 확인란 선택 여부에 관계없이 생성됩니다 .
   - **전송됨** : 메시지가 다른 서버의 이메일 주소로 전송된 경우 다른 서버의 이메일 주소 여러 개에 받는 사람이 포함되어 있으면 로그 레코드가 여러 개 생성됩니다 .
   - **재전송됨** : 이 상태는 메시지를 다른 서버의 이메일 주소로 재전송하기 위해 여러 번 시도했음을 나타냅니다 . MailPlus Server 1.3.0-0370 이상에서는 더 이상 이 상태를 사용할 수 없습니다 .
   - **실패** : 이 상태는 다른 서버로 전송된 메시지를 배달하지 못했음을 나타냅니다 .

**참고 :**

- **자동 BCC** 규칙 , **자동 전달** 또는 **자동 회신**을 설정한 경우 추가 로그 콘텐츠가 생성될 수 있습니다 .
- **High-availability 클러스터**를 설정했으면 기본 서버에서 로그를 확인하십시오 .

## 보안 로그 보기

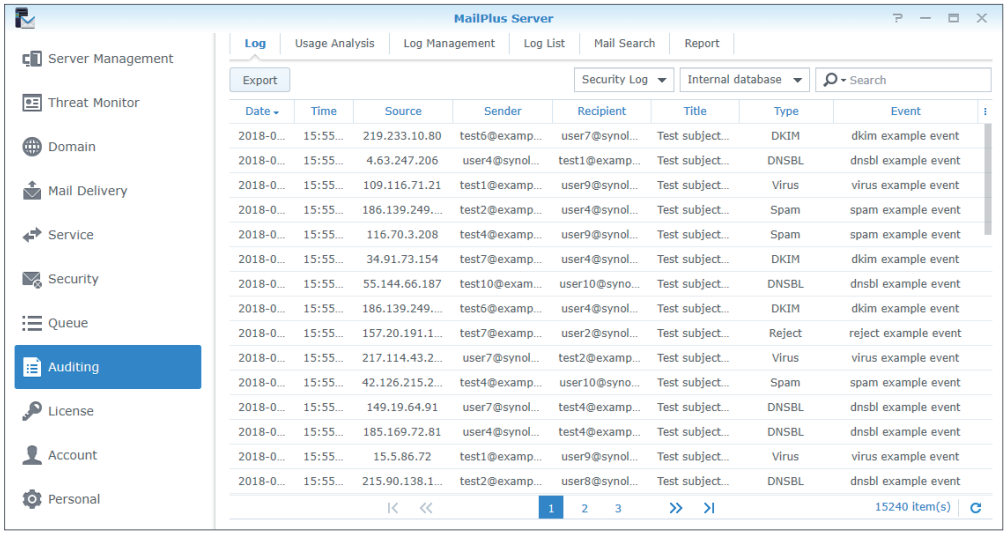
보안 로그에는 소스 , 보낸 사람 , 받는 사람 , 제목 , 유형 및 이벤트 설명과 함께 이벤트가 생성된 시간과 날짜가 표시됩니다 . 보안 로그는 **거부됨** , **스팸** , **바이러스** , **DNSBL**, **악성 콘텐츠** , **첨부 파일 필터** , **블랙리스트** , **SPF**, **DKIM**, **DMARC**, 및 **데이터 보호**로 분류됩니다 . 이 모든 분류 기준은 MailPlus Server 의 보안 설정과 관련됩니다 . **거부됨** 유형은 MailPlus Server 에서 전체 분석을 실행한 후 메시지를 거부했음을 나타냅니다 . 다음 단계를 참조하여 보안 로그를 확인하십시오 .

**참고 :**

- **High-availability 클러스터**를 이미 설정했으면 기본 서버에서 로그를 확인하십시오 .

1. **감사** > **로그**로 이동합니다 .

2. 상단에 있는 드롭다운 메뉴에서 **보안 로그** 및 **내부 데이터베이스**를 선택합니다 .

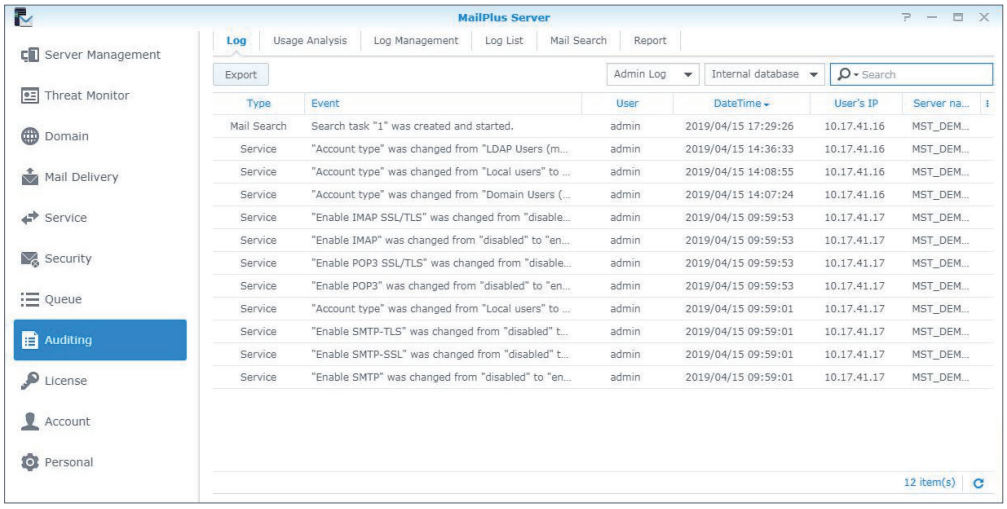



## 관리 로그 보기

관리 로그는 MailPlus Server 설정 변경 사항을 기록합니다 . 각 로그에는 유형 , 사용자 , 시간 및 날짜 , 사용자 IP 주소 및 서버 이름과 함께 간략한 이벤트 설명이 표시됩니다 . 다음 단계를 참조하여 관리 로그를 확인하십시오 .

1. **감사** > **로그**로 이동합니다 .

2. 상단에 있는 드롭다운 메뉴에서 **관리 로그** 및 **내부 데이터베이스**를 선택합니다 .

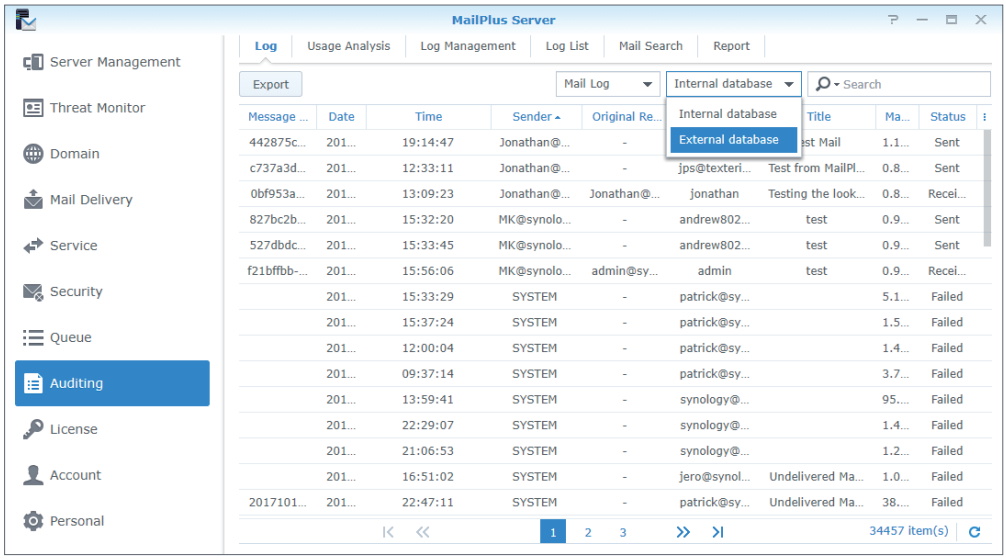


## 외부 데이터베이스 보기

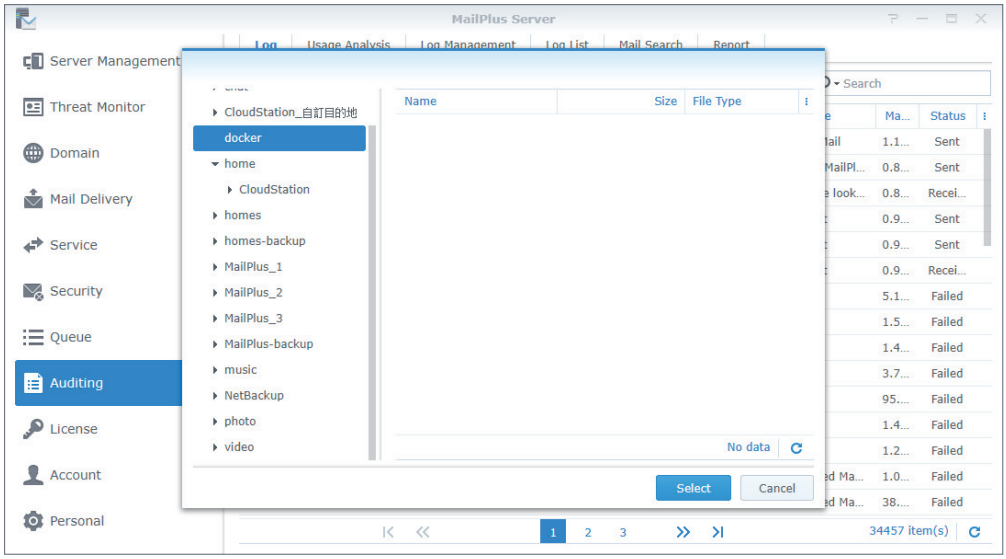
로그를 보관하거나 , 로그 데이터베이스를 생성하거나 , 로그 파일을 다운로드하면 **외부 데이터베이스**에 저장된 로그 콘텐츠를 확인할 수 있습니다 .

다음 단계를 참조하여 외부 데이터베이스를 확인하십시오 .

1. **감사** > **로그**로 이동합니다 .
2. 상단에 있는 드롭다운 메뉴에서 **메일 로그** , **보안 로그** 또는 **관리 로그**를 선택하고 **외부 데이터베이스**를 선택합니다 .



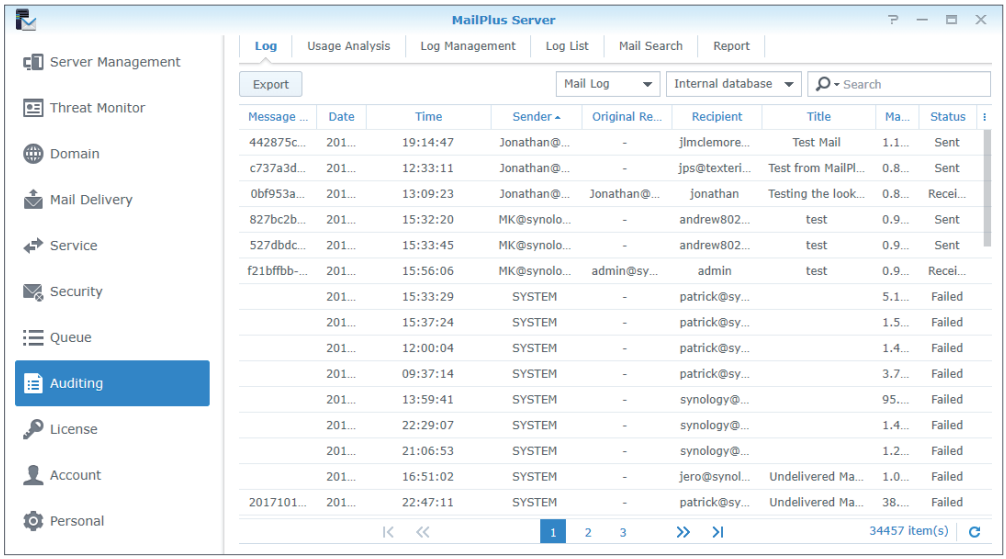

3. Synology NAS 에서 외부 데이터베이스 위치를 확인합니다 .
4. **선택** 버튼을 클릭합니다 .



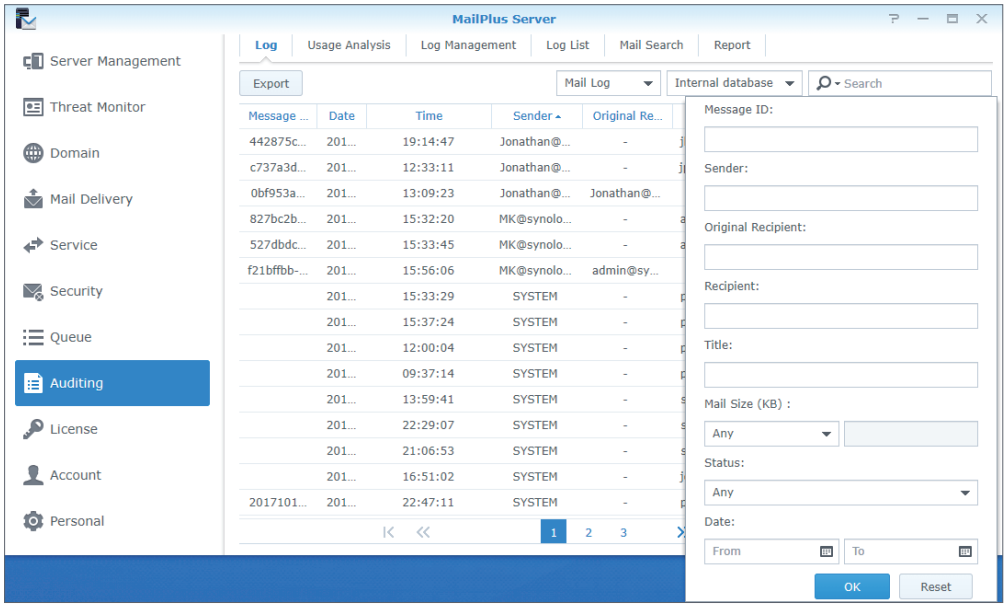
## 로그 검색

**감사** > **로그**에서 간단한 검색 또는 고급 검색을 사용하여 로그를 검색할 수 있습니다 .

- **간단한 검색** : 페이지 오른쪽 위 구석에 있는 검색 필드에 키워드를 입력할 수 있습니다 .
  - **메일 로그**의 경우 입력한 키워드는 **메시지 ID**, **보낸 사람** , **받는 사람** 및 **제목** 열에서 콘텐츠를 검색하는 데 사용됩니다 .
  - **보안 로그**의 경우 입력한 키워드는 **소스** , **보낸 사람** , **받는 사람** , **제목** 및 **이벤트** 열에서 콘텐츠를 검색하는 데 사용됩니다 .
  - **관리 로그**의 경우 입력한 키워드는 **유형** , **이벤트** , **사용자** , **사용자 IP** 및 **서버 이름** 열에서 콘텐츠를 검색하는 데 사용됩니다 .




- **고급 검색** : 페이지 오른쪽 위 구석에 있는 검색 창의 돋보기 아이콘을 클릭할 수 있습니다 . 정밀한 고급 검색을 수행하려면 각 항목에 검색 기준을 설정합니다 . 설정을 완료한 후 **확인**을 클릭합니다 . **상태** 드롭다운 메뉴에서 **도메인 내**를 선택하여 내부 사용자 내에서 보낸 메시지를 검색할 수 있습니다 .

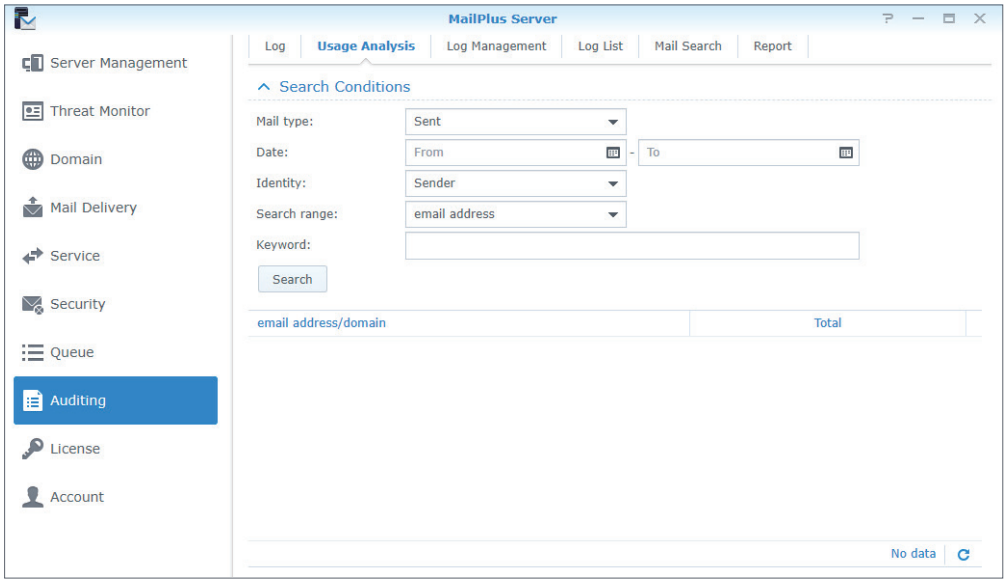


## 로그 콘텐츠 내보내기

**감사** > **로그**에서 로그를 .html 파일로 내보낼 수 있습니다 . 로그 검색 후 **내보내기** 버튼을 클릭하면 검색 결과를 내보낼 수 있습니다 . **로그 검색**을 참조하십시오 .

## 사용 분석

**감사** > **사용 분석**에서 사용 분석을 수행하여 각 이메일 주소 또는 도메인에서 보낸 인바운드 메시지와 아웃바운드 메시지를 분석할 수 있습니다 .

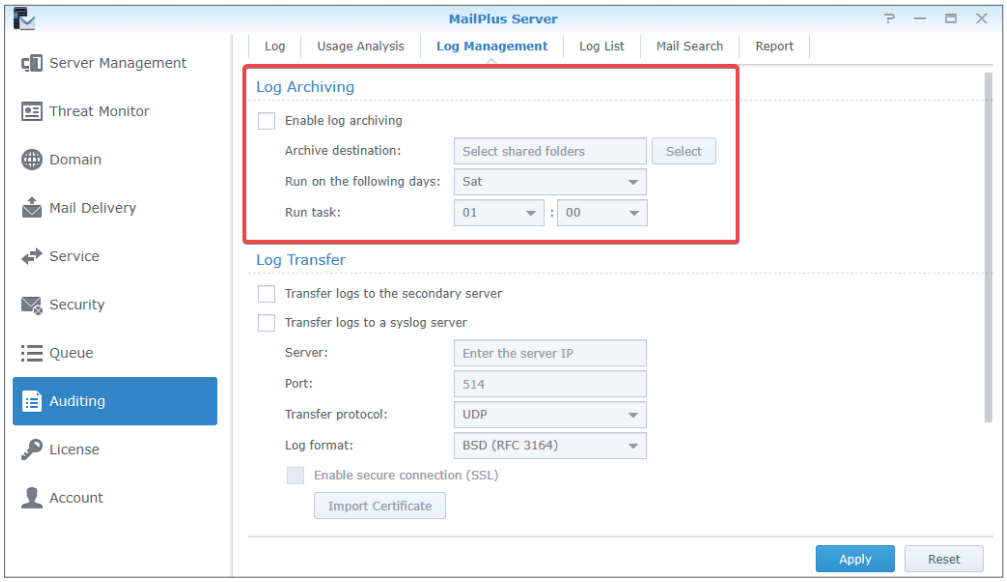



## 로그 보관

로그 보관 설정을 구성할 수 있습니다 . MailPlus Server 는 사용자 정의 스케줄에 따라 메일 로그 , 보안 로그 및 후위 로그를 보관합니다 . 공유 폴더에 액세스할 수 없으면 보관 기능이 자동으로 비활성화됩니다 .

다음 단계를 참조하여 로그를 보관하십시오 .

1. **감사** > **로그 관리**로 이동합니다 .
2. **로그 보관** 섹션에서 **로그 보관 활성화** 확인란을 선택합니다 .
3. **아카이브 대상** 필드 옆에 있는 **선택** 버튼을 클릭하고 보관 파일 대상을 선택합니다 .
4. 보관 작업 실행 시간을 선택합니다 .
5. **적용**을 클릭하여 설정을 저장합니다 .




## 로그를 보조 서버로 전송

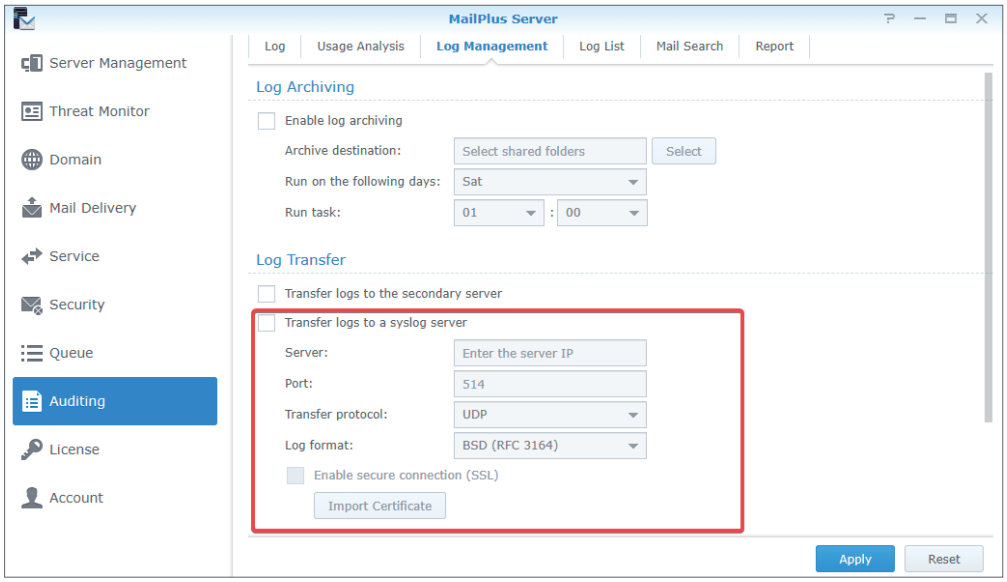
**High-availability 클러스터**를 설정하면 로그가 기본 서버에 수집됩니다 . 복사본을 보조 서버에 보낼 수 있습니다 . 로그를 보조 서버에 보내려면 로그 데이터베이스를 만들어야 합니다 ( **로그 데이터베이스 생성** 참조 ). 다음 단계를 참조하여 로그를 보조 서버로 전송하십시오 .

1. **감사** > **로그 관리**로 이동합니다 .
2. **로그 전송** 섹션에서 **로그를 보조 서버로 전송** 확인란을 선택합니다 .
3. **적용**을 클릭하여 설정을 저장합니다 .

## 후위 로그를 다른 syslog 서버로 전송

다음 단계를 참조하여 후위 로그를 다른 syslog 서버로 전송하십시오 .

1. **감사** > **로그 관리**로 이동합니다 .
2. **로그 전송** 섹션에서 **syslog 서버로 로그 전송** 확인란을 선택합니다 .
3. syslog 서버 정보를 입력합니다 .
4. **보안 연결 (SSL) 활성화** 확인란을 선택한 경우 로그를 보내기 전에 **인증서 가져오기** 버튼을 클릭하여 syslog 서버의 인증서를 가져와야 할 수 있습니다 .
5. **적용**을 클릭하여 설정을 저장합니다 .

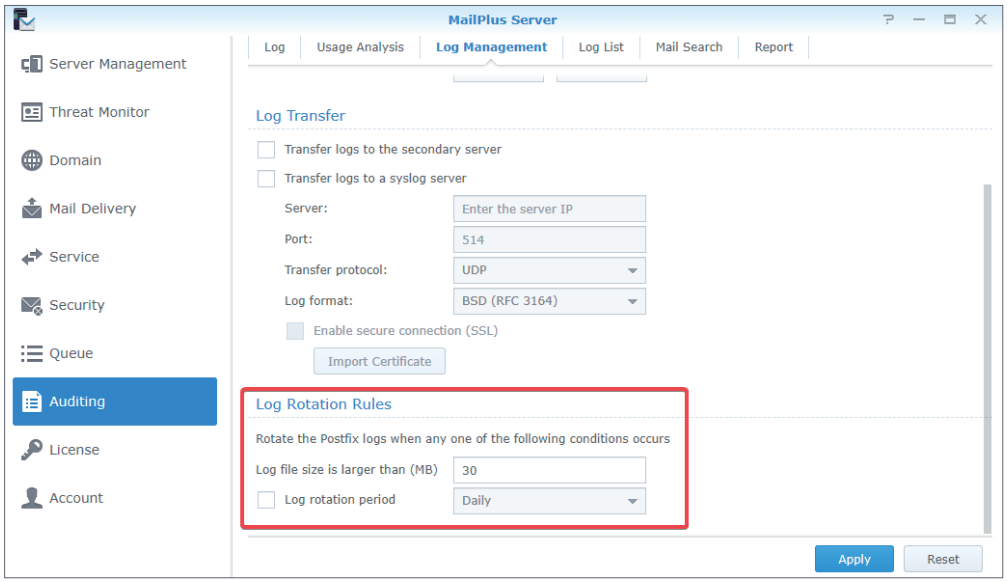



## 로그 회전 규칙 설정

후위 로그의 회전 기간과 파일 크기를 설정할 수 있습니다 . 메일 로그 데이터베이스와 보안 로그 데이터베이스의 최신 항목 4 억 개가 보존됩니다 .

다음 단계를 참조하여 로그 회전 규칙을 설정하십시오 .

1. **감사** > **로그 관리**로 이동합니다 .
2. **로그 회전 규칙** 섹션에서 **로그 파일 크기가 다음보다 큼 (MB)** 필드에 값을 입력합니다 .
3. **로그 회전 규칙** 섹션에서 **로그 회전 주기** 확인란을 선택하고 드롭다운 메뉴에서 회전 기간을 선택합니다 .
4. **적용**을 클릭하여 설정을 저장합니다 .

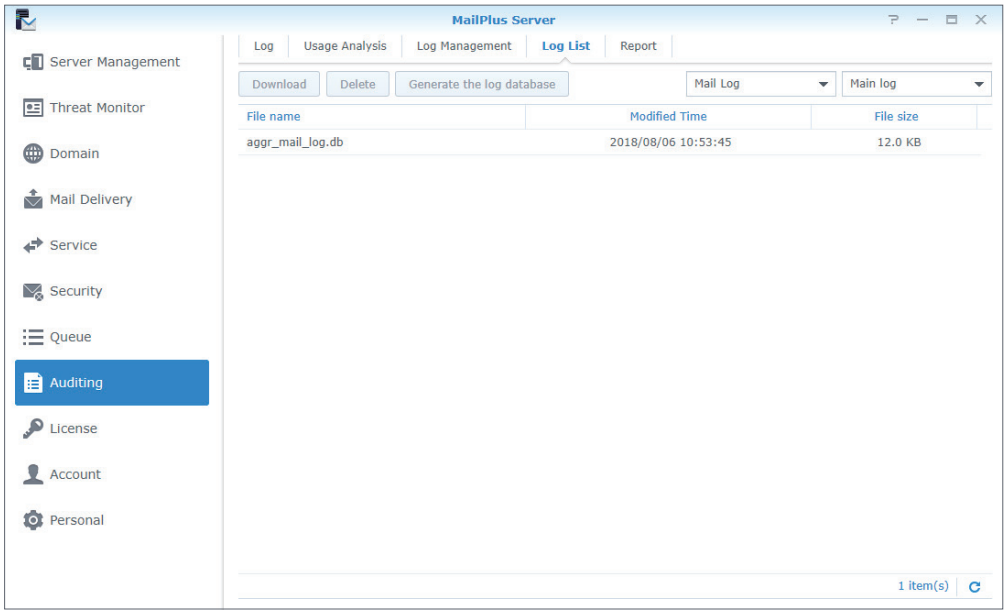


## 로그 파일 다운로드 및 삭제

**감사** > **로그**에서 메일 로그 , 보안 로그 , 관리자 로그 또는 후위 로그를 저장하거나 제거할 수 있습니다 .

다음 단계를 참조하여 로그 파일을 다운로드 및 삭제하십시오 .

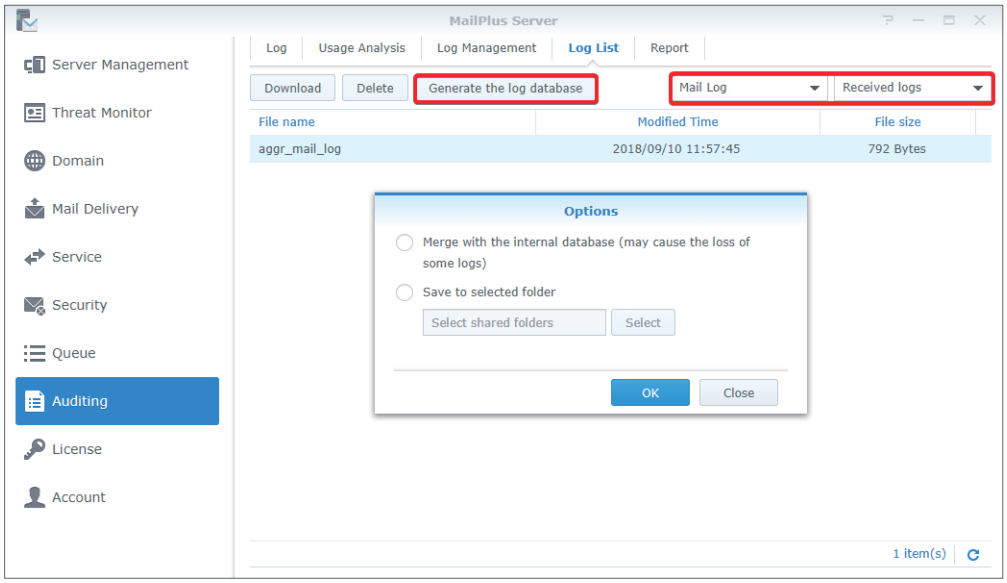
1. **감사** > **로그 목록**으로 이동합니다 .
2. 상단에 있는 드롭다운 메뉴에서 **메일 로그** , **보안 로그** , **관리 로그** 또는 **후위 로그**를 선택합니다 .
3. MailPlus high-availability 클러스터를 설정하고 **로그를 보조 서버로 전송**을 활성화했으면 보조 서버의 드롭다운 메뉴에서 **수신된 로그**를 선택할 수 있습니다 . 그렇지 않으면 **기본 로그**를 선택합니다 .
4. 로그 파일을 선택한 후 **다운로드** 버튼을 클릭하여 파일을 다운로드하거나 **삭제** 버튼을 클릭하여 서버에서 파일을 삭제할 수 있습니다 .




## 로그 데이터베이스 생성

**로그를 보조 서버로 전송을 활성화하면 로그 데이터베이스 생성 기능을 사용하여 수신된 로그 콘텐츠를 데이터베이스 파일로 다시 변환**할 수 있습니다 . **감사** > **로그**에서 **외부 데이터베이스를 확인하여** 로그 데이터베이스의 파일을 확인할 수 있습니다 .

1. **감사** > **로그 목록**으로 이동합니다 .
2. 드롭다운 메뉴에서 **메일 로그** , **보안 로그** 또는 **후위 로그**를 선택합니다 .
3. 드롭다운 목록에서 **수신된 로그**를 선택합니다 .
4. 로그 파일을 선택하고 **로그 데이터베이스 생성** 버튼을 클릭합니다 .
5. **내부 데이터베이스와 병합 ( 일부 로그가 손실될 수 있음 )** 또는 **선택한 폴더에 저장** 옵션을 선택하고 대상 폴더를 선택합니다 .
6. **OK**( 완료 ) 을 클릭하여 설정을 완료합니다 .




**참고 :**

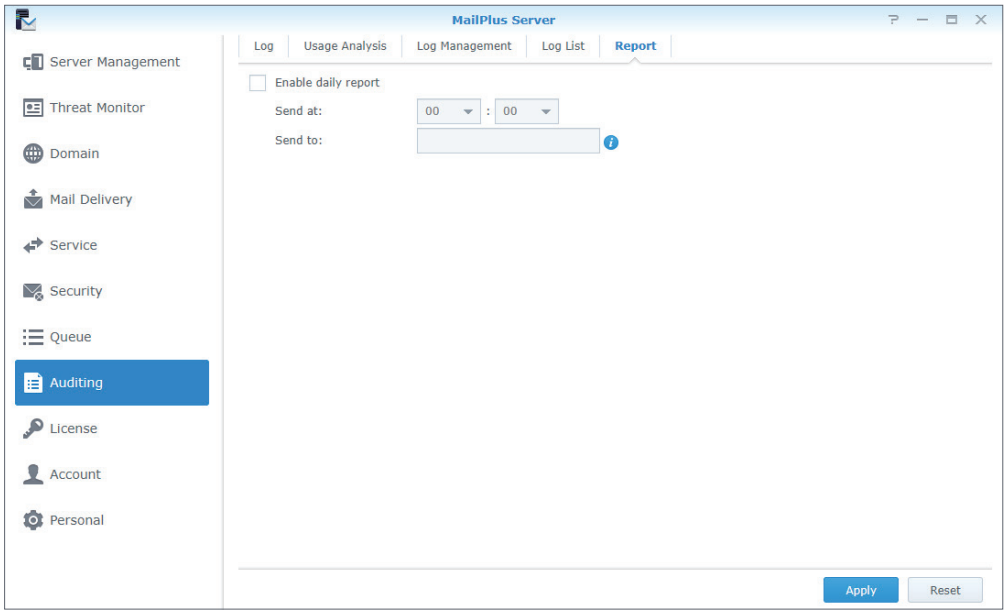
- **관리 로그**의 로그 데이터베이스를 생성할 필요는 없습니다 . **로그를 보조 서버로 전송** 옵션을 활성화하면 두 서버 모두에서 볼 수 있습니다 .
- **로그를 보조 서버로 전송** 옵션을 활성화한 후에 생성된 로그만 다른 서버와 동기화됩니다 .

## 일일 보고서 설정

일일 보고서 기능을 활성화하면 전날의 후위 로그를 특정 이메일 주소로 보낼 수 있습니다 .

다음 단계를 참조하여 일일 보고서를 설정하십시오 .

1. **감사** > **보고서**로 이동합니다 .
2. **일일 보고서 활성화** 확인란을 선택합니다 .
3. 배달 시간을 선택합니다 .
4. **전송 대상** 필드에 일일 보고서의 대상 주소를 입력합니다 . 이메일 주소를 최대 두 개까지 지정할 수 있으며 세미콜론 (;) 으로 구분해야 합니다 .




## 메일 검색 설정

MailPlus Server 에서 인덱싱된 모든 이메일을 찾을 수 있을 뿐만 아니라 검색 결과를 보고 , 삭제하고 , 내보낼 수 있습니다 .

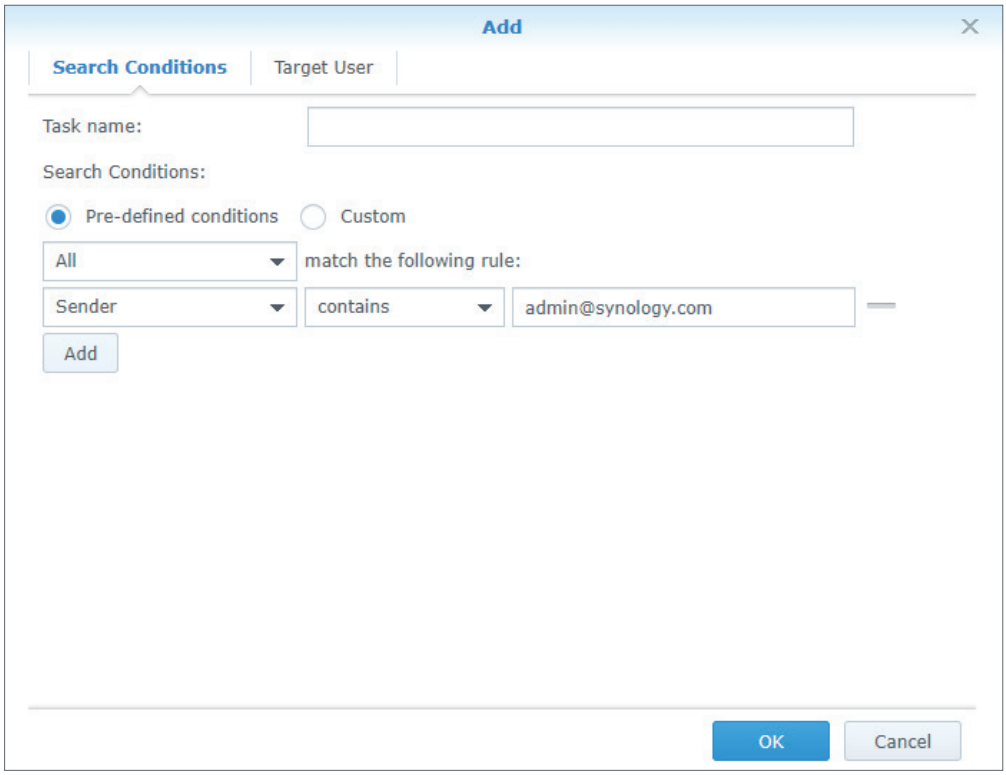
다음 단계를 참조하여 메일 검색 작업을 만드십시오 .

1. **감사** > **메일 검색**으로 이동합니다 .
2. 더하기 (+) 아이콘을 클릭하여 새 작업을 만듭니다 .
3. **작업 이름**을 입력합니다 .
4. **검색 조건**을 설정합니다 .
   - **사전 정의된 조건** : 검색 작업에 검색 조건을 여러 개 추가할 수 있습니다 . 드롭다운 메뉴에서 선택하여 **모든** 조건이나 **임의** 조건과 일치하는 이메일을 찾고 **보낸 사람** , **받는 사람** , **제목** , **키워드** , **메일 크기 (MB)** 또는 입력한 키워드가 **포함** 또는 **제외**된 **날짜**로 조건을 정의합니다 .
   - **사용자 지정** : 검색 연산자와 키워드를 사용하여 검색 조건을 사용자 지정할 수도 있습니다 . 예를 들어 admin@synology.com 주소에서 2018 년 5 월 25 일 이후에 보낸 GDPR 에 대한 이메일을 조회하려면 검색 조건으로 after:2018/05/25 AND from:admin@synology.com AND GDPR 을 입력하면 됩니다 .

| 검색 연산자 | 사용 | 예 |
| --- | --- | --- |
| **from:** | 지정된 보낸 사람의 메시지 | from: 영희 |
| **to:** | 지정된 받는 사람에게 전송된 메시지 | to: 철수 |
| **subject:** | 제목 줄에 특정 단어가 있는 메시지 | subject: 저녁 식사 |

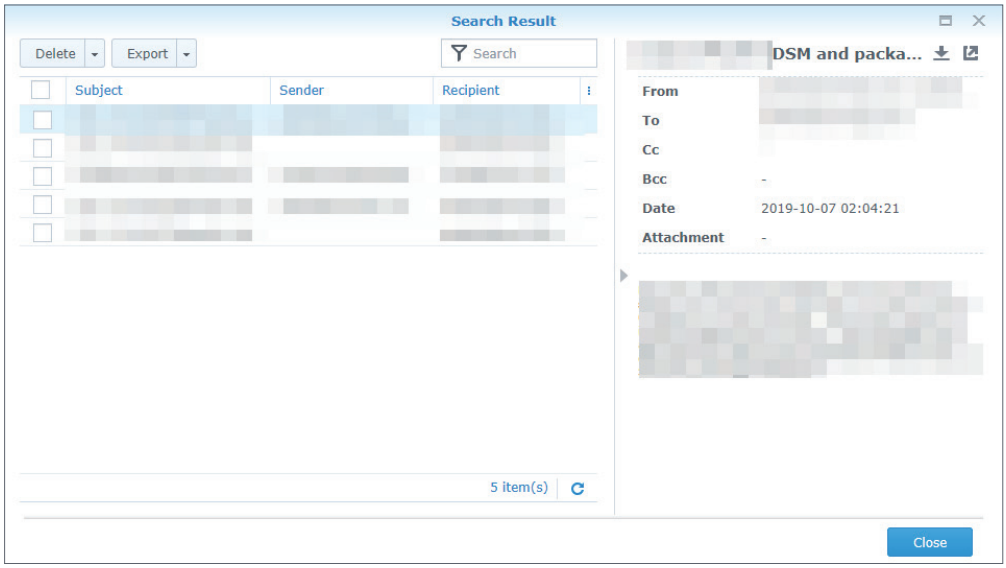
| 검색 연산자 | 사용 | 예 |
| --- | --- | --- |
| **OR** | 지정된 용어 여러 개와 일치하는 메시지 | from: 영희 OR from: 철수 |
| **- 또는 NOT** | 검색 결과에서 제거해야 하는 메시지 | 저녁 식사 - 영화 |
| **( )** | 지정된 용어가 포함된 메시지가 함께 그룹화 | subject:( 저녁 식사 영화 ) |
| **in:** | 지정된 사서함의 메시지 | in:"feature suggestions" |
| **label:** | 특정 레이블이 있는 메시지 | label: 친구 |
| **before: 또는 after:** | 특정 기간 중에 전송된 메시지 | after:2004/04/16 |
| **larger: 또는 smaller:** | 특정 크기보다 크거나 작은 메시지 (MB 단위 ) | larger:10M |
| **filename:** | 특정 파일 또는 파일 형식의 첨부 파일 | filename:pdf |
| **has:attachment** | 첨부 파일이 있는 메시지 | has:attachment |
| **is:starred** | 별표 메시지 | is:starred |
| **is:unread** | 읽지 않은 메시지 | is:unread |

5. **대상 사용자**를 설정합니다 . 대상 사용자를 지정하지 않으면 작업은 기본적으로 모든 사용자를 검색합니다 .
6. **확인** 을 클릭합니다 . 그러면 검색 작업이 즉시 시작됩니다 .
7. 작업을 하고 오른쪽 패널에서 **작업 중지**를 클릭하면 진행 중인 작업을 중지할 수 있습니다 . 작업을 다시 시작하려면 **검색**을 클릭합니다 .
8. 작업을 선택하고 해당 아이콘을 클릭하여 작업을 **편집** , **복사** 또는 **삭제**할 수 있습니다 .




## 메일 검색 결과 보기

1. **감사** > **메일 검색**으로 이동하여 전체 검색 작업을 선택합니다 .
2. 오른쪽 패널에서 **작업 보고서 다운로드** 또는 **결과 보기**를 클릭하여 추가적인 세부정보와 작업을 확인할 수 있습니다 . 작업 보고서를 사용하면 검색된 이메일 개수와 삭제된 이메일 개수를 비롯한 작업 세부 사항을 확인할 수 있습니다 .
3. **결과 보기** 창에서 각 이메일을 확인 , 삭제 또는 내보낼 수 있습니다 . 이메일을 선택하면 해당 이메일 세부정보가 오른쪽 섹션에 나타납니다 . 또한 원본 이메일 또는 이메일 첨부 파일을 다운로드하거나 새 탭에서 이메일을 열 수 있습니다 .



## 메일 검색 결과 내보내기

나중에 필요할 경우를 대비하여 중요한 메일 검색 결과를 항상 내보내 로컬 장치에 백업 파일로 보관하는 것이 좋습니다 .

1. **감사** > **메일 검색**으로 이동하여 전체 검색 작업을 선택합니다 .
2. 작업을 선택하고 오른쪽 패널에서 **결과 보기**를 클릭합니다 .
3. 내보낼 검색 결과를 선택하고 **내보내기**를 클릭합니다 .
4. **내보내기** 버튼 옆에 있는 화살표 아이콘을 클릭하여 메일 목록과 원본 이메일을 모두 내보낼지 또는 메일 목록만 내보낼지 여부를 추가로 지정할 수 있습니다 .
5. 내보낸 메일 목록 **export_list.csv** 라는 파일이며 .csv 파일을 지원하는 편집기로 이 파일을 편집할 수 있습니다 . 감사 작업을 배포하려면 레코드를 파일 여러 개로 분할하면 됩니다 . 내보낸 원본 메일은 **eml** 폴더의 .eml 파일입니다 .

## 메일 검색 결과 가져오기

메일 검색 결과를 내보내 로컬 장치에 저장한 경우 언제든지 메일 목록을 가져와 이메일을 확인할 수 있습니다 .

1. **감사** > **메일 검색**으로 이동합니다 .
2. 휴지통 아이콘 옆에 있는 **작업 가져오기** 아이콘을 클릭합니다 .
3. 메일 목록을 CSV 형식으로 업로드하고 작업 이름을 입력합니다 .
4. **가져오기**를 클릭합니다 .
5. 가져오기가 완료되면 작업 목록 상단에 작업이 표시됩니다 .

# 11 장 : Disaster Recovery

## High-Availability 클러스터

MailPlus Server 에서는 두 가지 솔루션 , 즉 **단일 노드** 구성과 **high-availability** 구성을 제공합니다 . 단일 노드 구성에서 메일 서비스를 실행하려면 Synology NAS 하나가 필요하지만 high-availability 구성에서 예기치 못한 이벤트 시 중단된 메일 서비스를 보장할 수 있는 high-availability(HA) 클러스터를 형성하려면 Synology NAS 두 개가 필요합니다 .

### high-availability(HA) 구성 소개

high-availability(HA) 클러스터는 Synology NAS 두 개로 구성되어 있습니다 . 하나는 " 기본 서버 " 역할을 수행하고 다른 하나는 " 보조 서버 " 역할을 수행합니다 . 사용자와 기타 메일 서버는 MailPlus HA 클러스터의 기본 IP 주소에 연결합니다 . 기본 서버는 MailPlus HA 클러스터의 기본 IP 주소에서 실행되며 모든 서비스 요청을 수신합니다 . 그런 다음 이러한 요청은 기본 서버 또는 보조 서버에 할당되어 처리됩니다 .

양방향 동기화는 메일 데이터와 서버 설정이 일관되게 보존되고 기본 서버와 보조 서버 간에 동기화하기 위해 수행됩니다 . 두 서버가 서로 다른 서비스 요청을 처리하거나 서버 중 하나에서 MailPlus Server 설정을 편집하는 경우 양방향 동기화 기능은 데이터 불일치 가능성을 최소화할 수 있습니다 .

메일 데이터 및 서버 설정과 달리 로그는 HA 구성의 기본 서버에 수집됩니다 . 기본 서버의 로그를 보거나 **로그를 보조 서버로 전송**을 통해 복사본을 전송하십시오 .

HA 구성은 서버 오작동으로 인한 서비스 중단을 최소화합니다 . 기본 서버가 오작동하면 보조 서버가 일시적으로 모든 메일 서비스 요청을 넘겨받습니다 . 기본 서버가 복구되면 대체 작동 기간 중에 처리된 데이터 수정 사항은 기본 서버로 다시 동기화됩니다 . 보조 서버가 오작동하면 기본 서버는 모든 작업 부하를 가정하고 이 기간 중에 처리된 데이터 수정 사항은 보조 서버가 복구된 후에 보조 서버로 동기화됩니다 .

**참고 :**

- MailPlus high-availability 클러스터와 Synology High Availability(SHA) 는 서로 다른 클러스터 시스템이며 동일한 Synology NAS 에서 동시에 실행될 수 없습니다 .
- Synology High Availability 는 MailPlus 2.2 이상에서 지원됩니다 .
- 서비스 지속성이 요구되면 메일 서비스용으로 설계된 MailPlus high-availability 클러스터를 사용하는 것이 좋습니다 . high-availability 클러스터가 복구되면 데이터는 두 서버 사이에서 일관되게 유지되므로 브레인 분할 오류 중에 업데이트된 데이터가 손실되지 않습니다 .
- SHA 에서는 MailPlus 서버 두 개가 하나로 간주되며 무료 라이센스 5 개를 공유합니다 . 반면 MailPlus HA 에서는 라이센스 10 개를 무료로 사용할 수 있습니다 .

## high-availability(HA) 를 구성하기 전에

1. **Synology NAS 두 개를 준비합니다** .

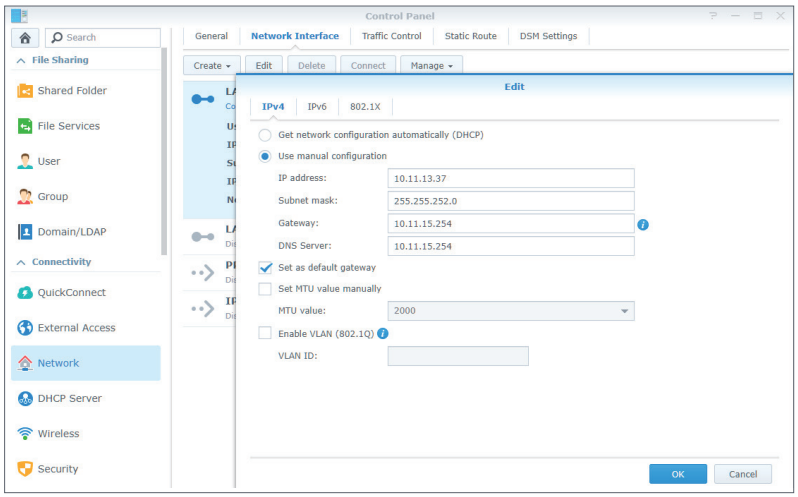
   - 두 Synology NAS 의 **제어판** > **정보 센터** > **Synology 계정**에서 동일한 Synology 계정에 로그인합니다 .
   - **제어판** > **지역 옵션** > **시간**에서 두 Synology NAS 간의 시스템 시간을 동기화합니다 .
   - **패키지 센터**로 이동하여 두 Synology NAS 모두에 **MailPlus Server** 와 **MailPlus** 를 설치하고 초기화합니다 . MailPlus Server 설정 방법에 대한 자세한 내용은 **MailPlus Server 설정** 섹션을 참조하십시오 .
   - MailPlus Server 를 설정하면 **MailPlus** 공유 폴더가 자동으로 Synology NAS 에 추가됩니다 . 클라이언트 사용자가 MailPlus 에 액세스할 수 있도록 보장하려면 권한을 직접 편집하지 않는 것이 좋습니다 . **MailPlus** 공유 폴더의 권한 설정을 기본값으로 설정하십시오 .
   - **제어판** > **권한**에서 대상 사용자 또는 그룹의 권한을 MailPlus Server 와 MailPlus 로 설정합니다 . 설정이 두 Synology NAS 간에 동일해야 합니다 .

**참고 :**

- MailPlus Server 가 있는 볼륨의 크기는 동일해야 합니다 . 또한 모든 인바운드 이메일과 아웃바운드 이메일이 두 볼륨으로 완전 동기화되므로 볼륨 크기가 이메일 저장소 요구 사항을 충족하는지 확인하십시오 .
- 두 볼륨에 SSD 캐시를 탑재한 경우 다음 사항에 유의하십시오 .
  - RAID 1 구성에서는 읽기 - 쓰기 캐시여야 합니다 .
  - 캐시 크기는 동일해야 합니다 .
- HA 클러스터 생성 중에 보조 서버에서 2 단계 검증 기능을 일시적으로 비활성화해야 합니다 .

2. **기본 서버와 보조 서버에 두 가지 고정 IP 주소 집합을 할당합니다** .

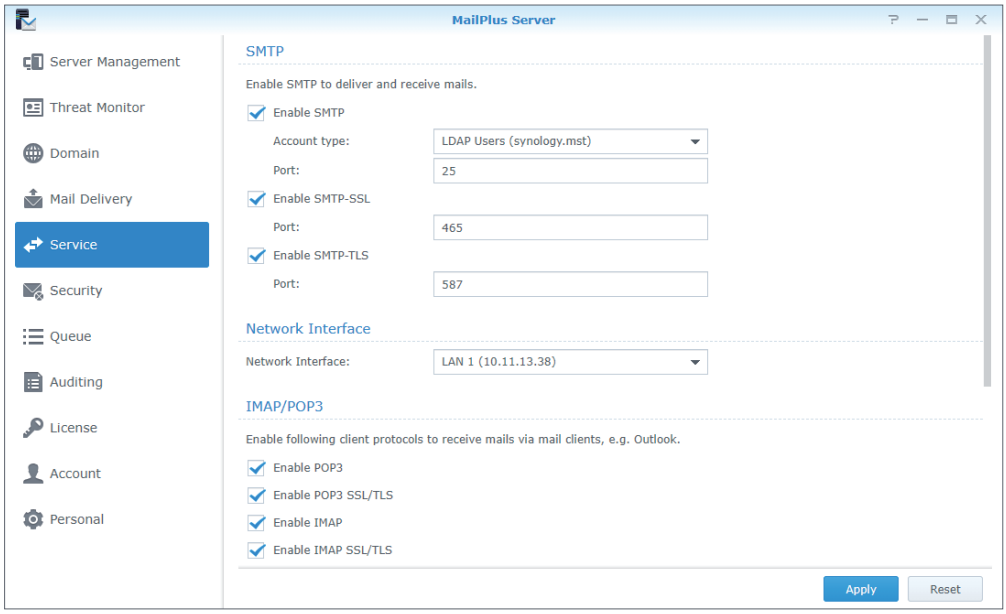
   - 두 Synology NAS 의 IP 주소는 같은 LAN 아래에 있어야 합니다 .
   - IP 주소는 PPPoE 또는 DHCP 를 통해 검색되면 안 됩니다 .
   - 수동으로 네트워크를 구성하려면 IP 주소의 네트워크 카드를 설정해야 합니다 .



3. **두 Synology NAS 모두 동일한 도메인에 가입해야 합니다** .
   - 두 Synology NAS 모두 Windows Active Directory 또는 LDAP 서버에 가입해야 합니다 . Windows Active Directory 에 가입하는 방법에 대한 자세한 내용은 **이 자습서**를 참조하십시오 . LDAP 서버에 가입하는 방법에 대한 자세한 내용은 **이 문서**를 참조하십시오 .
   - 사용자 환경에 Windows Active Directory 또는 LDAP 서버가 없으면 **패키지 센터**로 이동하고 **Synology Directory Server** 또는 **LDAP Server** 를 설치하여 계정 관리에 도메인 또는 LDAP 서버를 설정하면 됩니다 . 자체 호스팅된 LDAP 또는 도메인 서비스를 사용하면 디렉토리를 호스팅하는 Synology NAS 가 비정상적이거나 응답하지 않을 때 메일 서비스가 중단될 위험이 있습니다 .
4. **HA 클러스터의 내부 IP 주소와 외부 IP 주소를 준비합니다** .
   - 두 Synology NAS IP 주수와 동일한 LAN 에 있어야 하는 사용하지 않는 고정 내부 IP 주소와 HA 클러스터의 사용하지 않는 외부 IP 주소를 예약합니다 .
   - 내부 및 외부 클러스터 IP 주소 사이에서 트래픽이 전달되도록 라우터에서 포트 전달 규칙을 구성합니다 .
   - 공용 DNS( 도메인 이름 시스템 ) 서버에 외부 클러스터 IP 주소를 등록합니다 .

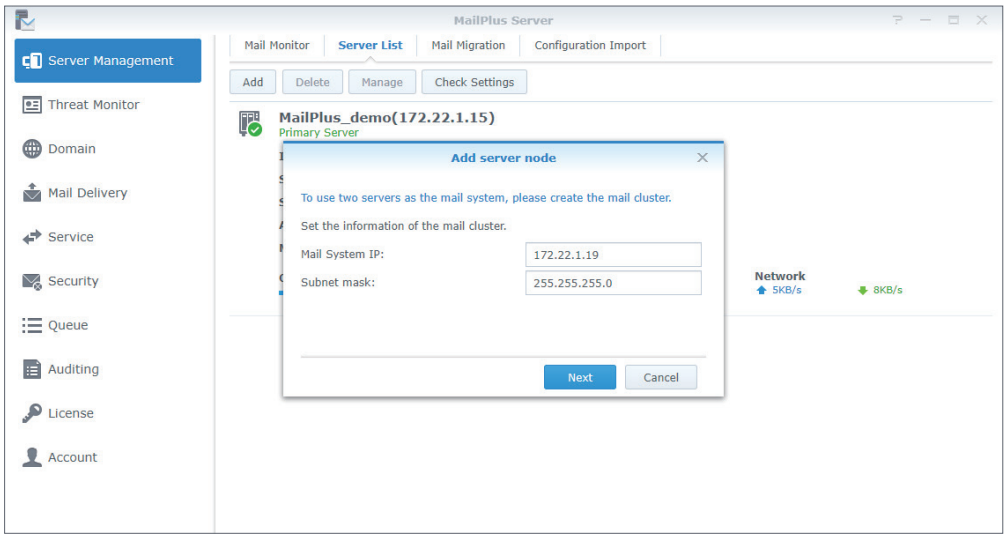
## high-availability(HA) 구성

1. 설정한 후 MailPlus Server 를 시작합니다 .
2. **서비스**로 이동하여 **SMTP** 섹션 아래의 **계정 유형** 드롭다운 메뉴에서 **도메인 사용자** 또는 **LDAP 사용자**를 선택했는지 확인합니다 .




3. **서버 관리** > **서버 목록**으로 이동하고 **추가** 버튼을 클릭합니다 .

4. HA 클러스터의 기본 내부 IP 주소를 입력하고 **다음**을 클릭합니다 .




5. **서버 주소** 필드에 보조 서버의 IP 주소를 입력하거나 **서버 주소** 드롭다운 메뉴에서 보조 서버로 사용할 Synology NAS 를 선택합니다 . 동일한 LAN 아래에 있는 Synology NAS 가 검색되고 이 드롭다운 메뉴에 포함됩니다 .

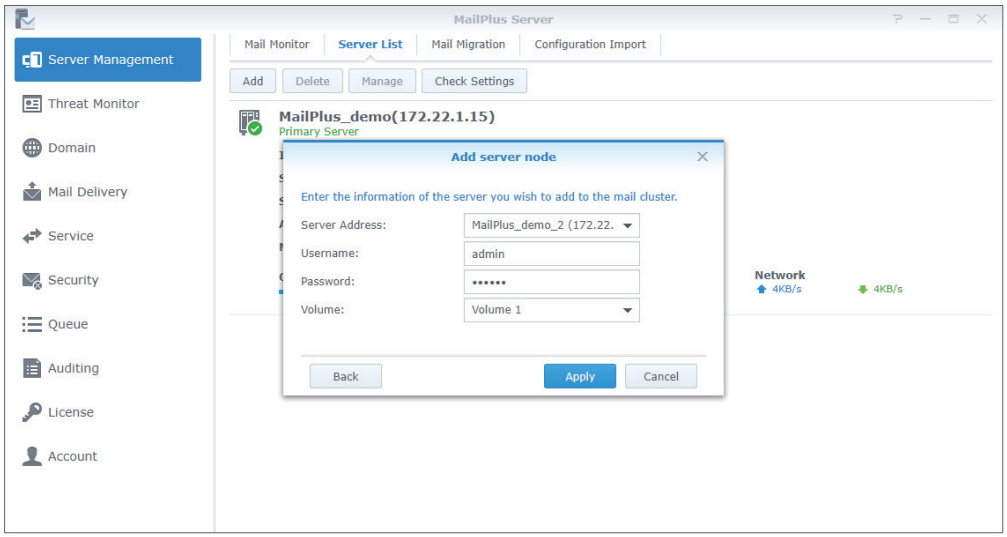
**참고 :**

- 보조 서버를 **네트워크 인터페이스**에 바인딩해야 합니다 . 바인딩된 네트워크 인터페이스의 IP 주소를 입력해야 합니다 .

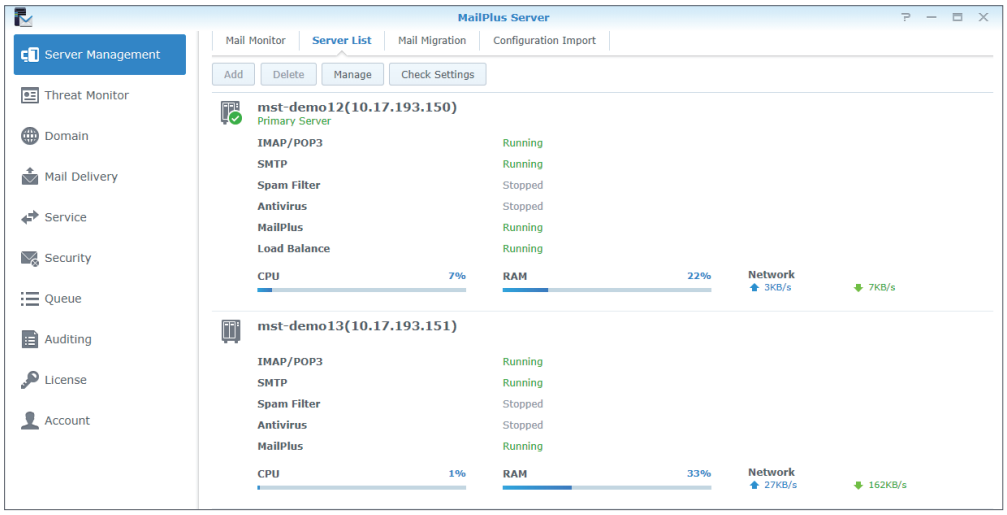
6. **사용자 이름**과 **패스워드** 필드에 보조 서버의 관리자 그룹에 속한 계정 자격 증명을 입력합니다 . HA 클러스터 생성 중에 보조 서버에서 2 단계 검증을 일시적으로 비활성화해야 합니다 .

7. **볼륨** 드롭다운 메뉴에서 보조 서버에 생성된 볼륨의 목록을 찾을 수 있습니다 . 보조 서버에 메일 데이터와 MailPlus 관련 파일을 저장하는 데 사용할 볼륨을 선택합니다 .

8. 설정이 올바른지 확인한 후 **적용**을 클릭합니다 .



9. 설정을 완료하면 이메일이 보조 서버와 동기화됩니다 . 동기화하는 데 필요한 시간은 기본 서버에 저장된 이메일 수에 따라 다릅니다 . 동기화 중에 계속 이메일을 보내거나 받을 수 있습니다 . 동기화가 완료될 때까지 모든 서비스는 기본 서버에서 처리됩니다 . 동기화가 완료되면 기본 서버와 보조 서버가 작업 부하를 공유합니다 .




**참고 :**

- 첫 번째 동기화 중에 MailPlus 서비스를 사용할 수 있지만 서버 부하가 높으므로 속도가 상대적으로 느립니다 . 따라서 오랫동안 MailPlus Server 를 사용하여 이메일 수가 많은 경우 로드 시간이 단축되고 동기화 속도가 향상되도록 **Hyper Backup** 을 사용하여 대부분의 이메일을 보조 서버에 복사하는 것이 좋습니다 . **Hyper Backup** 을 사용하여 이메일을 백업하는 방법에 대한 자세한 내용은 **이메일 백업 및 복원**을 참조하십시오 .

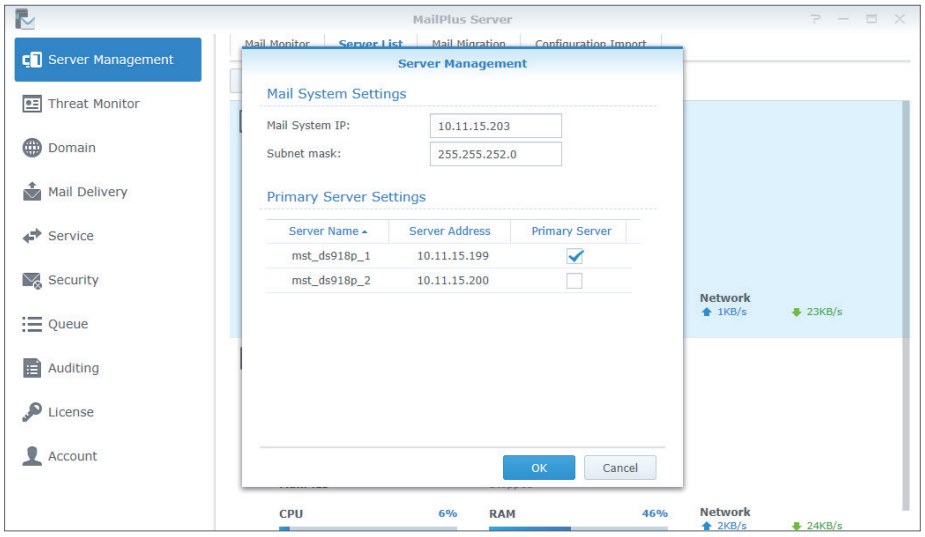
## high-availability(HA) 클러스터 구성 수정

1. 설정한 후 MailPlus Server 를 시작합니다 .
2. **서버 관리** > **서버 목록**으로 이동합니다 .
3. **관리** 버튼을 클릭합니다 .
4. **메일 시스템 설정** 섹션에서 HA 클러스터의 IP 주소와 서브넷 마스크 설정을 수정할 수 있습니다 .

**참고 :**

- 수정된 IP 주소와 서브넷 마스크는 기본 서버 및 보조 서버의 IP 주소와 동일한 LAN 아래에 있어야 합니다 .

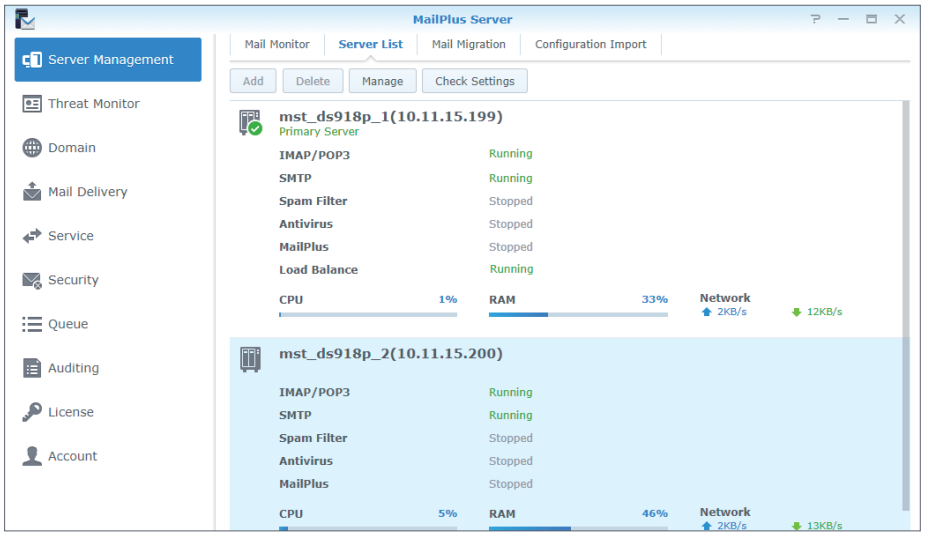
5. **기본 서버 설정** 섹션에서 HA 클러스터의 기본 서버 역할을 수행할 Synology NAS 를 선택할 수 있습니다 . 기본 서버는 HA 클러스터의 내부 IP 주소에서 실행되며 모든 메일 서비스 요청을 수신합니다 . 그러면 이러한 요청은 보조 서버에 할당됩니다 .



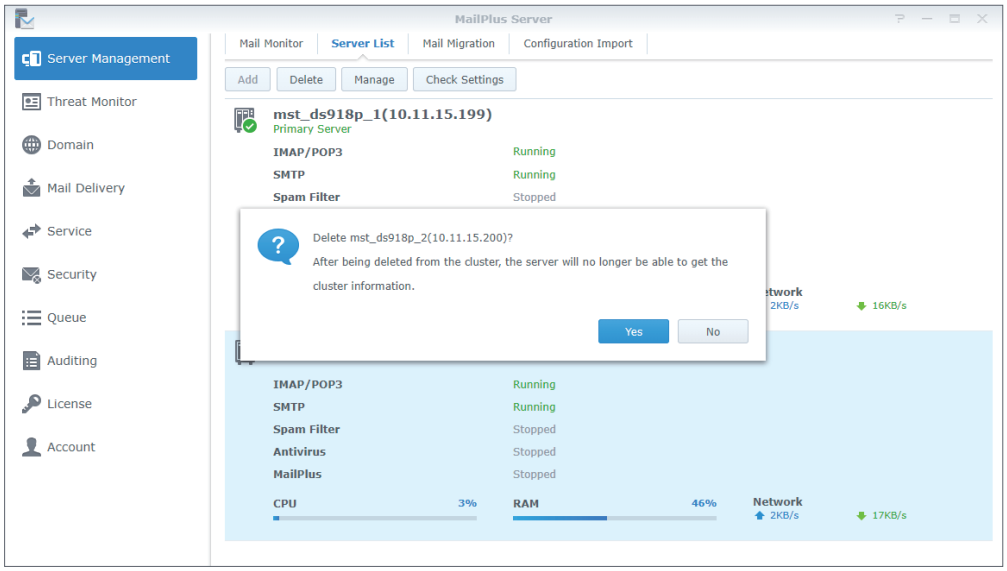

## high-availability(HA) 클러스터 구성 제거

HA 구성을 제거하면 데이터 일관성을 보장하기 위해 메일 데이터가 두 Synology NAS 에서 동기화됩니다 . 구성을 제거한 후에는 HA 클러스터의 내부 IP 주소가 더 이상 Synology NAS 에서 사용되지 않습니다 . 방화벽 장치의 포트 전달과 완충 영역 (DMZ) 설정을 조정하거나 관련 DNS 레코드를 수정해야 할 수 있습니다 . 다음 단계를 참조하여 HA 클러스터에서 Synology NAS 중 하나를 제거하십시오 .

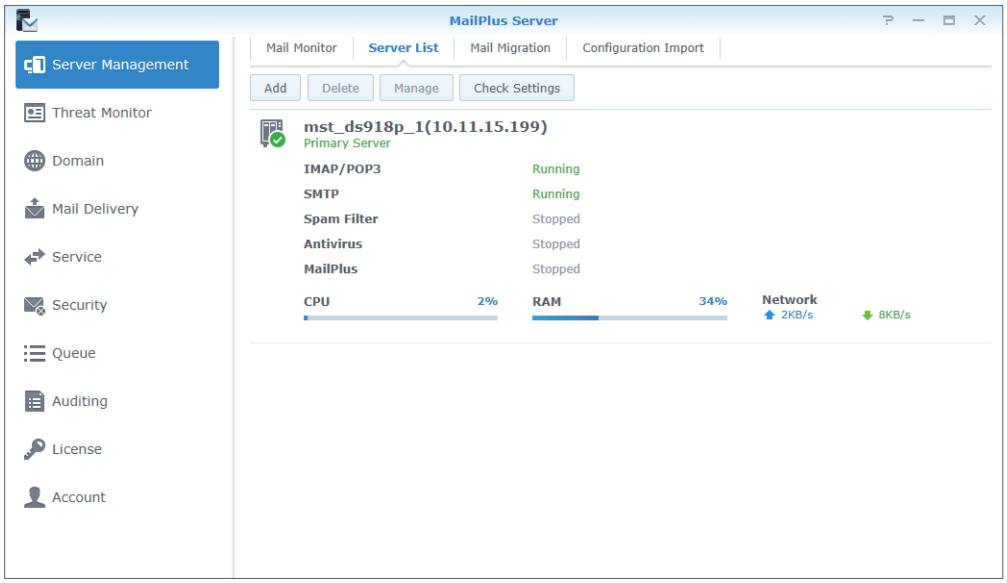
1. 유지하려는 Synology NAS 의 DSM 에 로그인하고 MailPlus Server 를 시작합니다 .
2. **서버 관리** > **서버 목록**으로 이동합니다 .
3. 제거할 Synology NAS 를 선택합니다 .




4. **삭제** 버튼을 클릭합니다 .
5. 팝업 확인 창에서 **예**를 클릭합니다 .




6. 모든 이메일이 동기화되면 HA 클러스터가 해제됩니다 . 유지하려는 서버에서 계속 메일 서비스 요청을 수신하고 처리합니다 . 방화벽 장치의 포트 전달과 완충 영역 (DMZ) 설정을 조정하거나 관련 DNS 레코드를 수정해야 하는지 확인하십시오 .



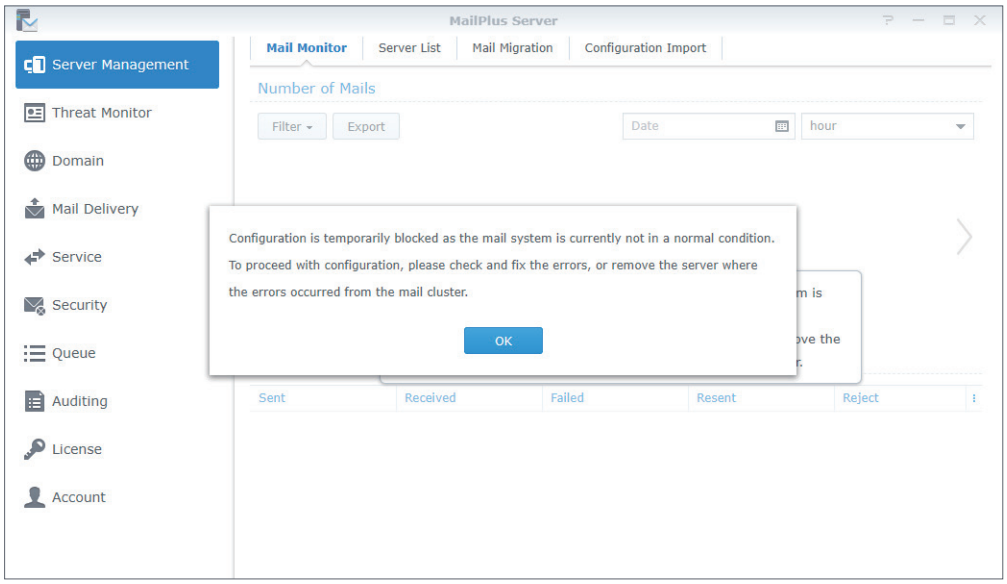

## 서버 오작동

HA 클러스터의 Synology NAS 중 하나가 오작동하면 다른 Synology NAS 가 메일 서비스를 계속 제공합니다 . 다음 섹션에서 언급한 기본 서버와 보조 서버는 전환 후 역할이 아닌 HA 구성에 있는 서버의 원래 역할을 참조합니다 .

### 기본 서버 오작동

원래 기본 서버가 오작동하면 원래 보조 서버가 HA 클러스터의 내부 IP 주소를 넘겨받습니다 . 서비스 요청을 개별적으로 수신 및 처리합니다 . 이러한 상황에서 MailPlus Server 를 원래 보조 서버에서 시작하면 메일 시스템 경고 창이 표시되고 전환 중에 MailPlus Server 설정을 조정할 수 없게 됩니다 .

가능한 빨리 기본 서버를 복구해야 합니다 . 원래 기본 서버를 복구할 수 없으면 **high-availability(HA) 구성 제거**를 참조하여 제거하십시오 . 제거하면 MailPlus Server 는 단일 노드 구성에서 실행됩니다 .




### 보조 서버 오작동

원래 보조 서버가 오작동하면 원래 기본 서버가 HA 클러스터의 내부 IP 주소를 넘겨받고 모든 서비스 요청을 개별적으로 처리합니다 . 가능한 빨리 원래 보조 서버를 복구하십시오 . 원래 보조 서버를 복구할 수 없으면 **high-availability(HA) 구성 제거**를 참조하여 제거하십시오 . 제거하면 MailPlus Server 는 단일 노드 구성에서 실행됩니다 .

## 이메일 백업 및 복원

DSM 의 백업 기능을 사용하여 MailPlus Server 를 백업할 수 있습니다 . MailPlus Server 백업에는 다음이 포함됩니다 .

- **시스템 구성 백업**
- **사서함 및 이메일 백업**

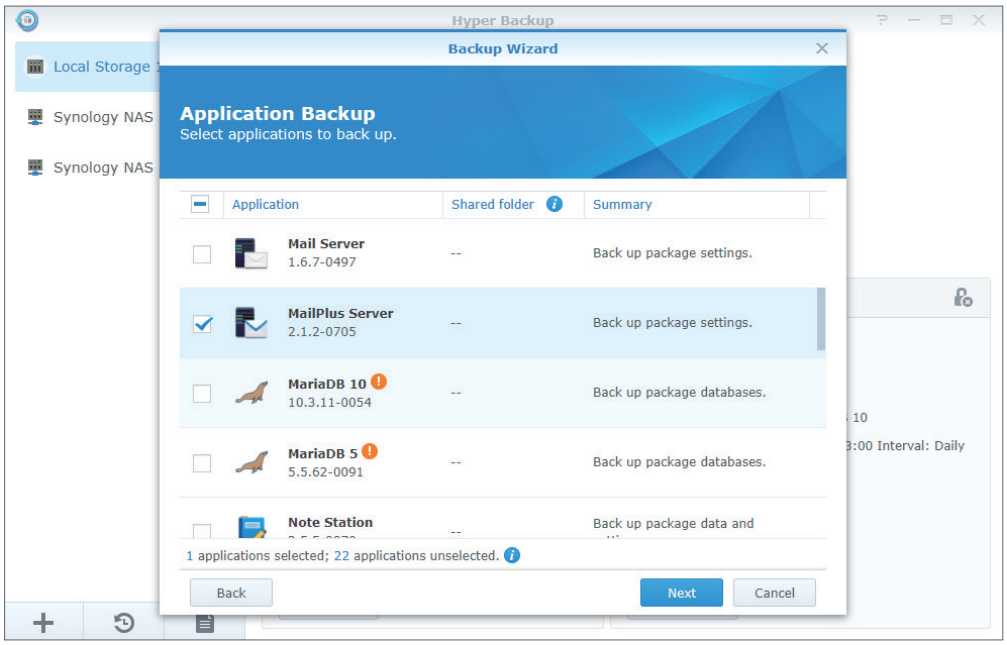
MailPlus Server 의 시스템 설정에서 수정 횟수가 줄어듭니다 . 따라서 **Hyper Backup** 을 사용하여 예약 백업 작업을 실행할 수 있습니다 . 그러나 메일 시스템의 사서함과 이메일 메시지는 지속적으로 변경되므로 실시간 백업이 필요할 수 있습니다 . 따라서 예약 백업만 수행할 때 데이터가 손실되지 않도록 **공유 폴더 동기화**를 사용하여 사서함과 이메일 메시지를 백업하는 것이 좋습니다 .

### 시스템 구성 백업

Hyper Backup 을 사용하여 메일 시스템 구성을 MailPlus 호환 Synology NAS 에 백업합니다 .

1. 원본 Synology NAS 에서 **Hyper Backup** 을 시작합니다 .
2. 왼쪽 아래 구석에 있는 더하기 아이콘 (+) 을 클릭하여 새 데이터 백업 작업을 만듭니다 .

3. 백업 대상 유형을 선택합니다 .
   - **로컬 폴더 및 USB**: 이 옵션은 데이터를 로컬 Synology NAS 또는 외부 USB/SD 저장소 장치에 백업합니다 .
   - **원격 NAS 장치** : 사전에 Hyper Backup Vault 를 원격 대상에 설치 및 실행해야 합니다 .
4. 작업 설정을 지정합니다 . 백업 작업을 만드는 방법에 대한 자세한 내용은 **이 문서**를 참조하십시오 .
5. 시스템에서 백업할 응용 프로그램을 선택하라는 메시지가 나타나면 **MailPlus Server** 를 선택합니다 .




6. 백업 작업 설정이 완료되면 시스템은 MailPlus Server 인터페이스의 왼쪽 패널에서 다음 MailPlus Server 설정을 백업할 수 있습니다 .
   - **도메인**
   - **메일 배달**
   - **서비스**
   - **보안**
   - **감사**
   - **라이센스**
   - **계정**

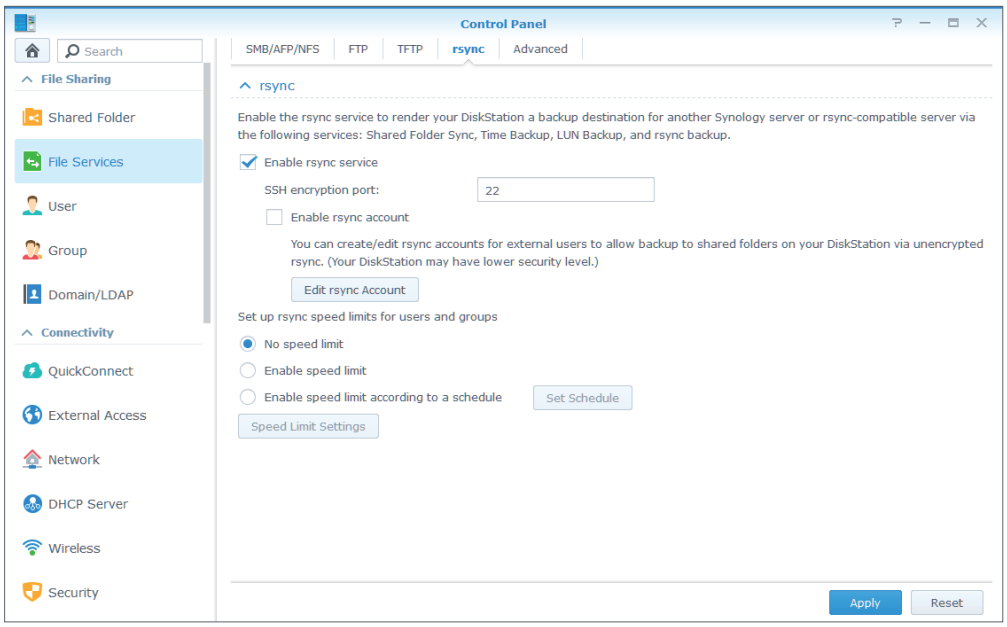
## 사서함 및 이메일 백업

동기화 작업을 통해 전체 사서함과 이메일 메시지를 MailPlus 호환 Synology NAS 에 백업하려면 다음 섹션을 참조하십시오 .

### 공유 폴더 동기화 활성화

대상 Synology NAS 에서 **공유 폴더 동기화**를 활성화해야 합니다 .

1. DSM 에 로그인합니다 .
2. **제어판** > **파일 서비스** > **rsync** 로 이동합니다 .
3. **rsync 서비스 활성화**를 확인란을 선택하여 **공유 폴더 동기화**를 활성화합니다 .




4. **적용**을 클릭합니다 .

### 동기화 작업 생성

원본 Synology NAS 에 로그인하고 다음 단계를 참조하여 동기화 작업을 만듭니다 .

1. **제어판** > **공유 폴더 동기화**로 이동하고 **작업 목록** 버튼을 클릭합니다 .
2. **작업 목록** 창에서 **생성** 버튼을 클릭합니다 .
3. **작업 이름** 필드에 작업 이름을 입력합니다 .
4. 동기화할 공유 폴더를 선택합니다 .
5. 대상 Synology NAS 세부 사항과 다음 동기화 설정을 지정합니다 .
   - **암호화된 공유 폴더 동기화를 위해 SSH 암호화 포트를 사용자 지정** : SSH 전송 암호화에 원하는 암호화 포트를 사용합니다 .
   - **SSH 전송 암호화 활성화** : 전송 중에 데이터를 암호화합니다 . 이 옵션은 높은 보안성을 제공하지만 암호화하지 않고 전송하면 성능이 향상됩니다 .
   - **전송 압축 활성화** : 전송 중에 데이터를 압축합니다 . 이 옵션은 대역폭 사용량을 줄여주지만 CPU 작업 부하를 증가시킵니다 .
   - **블록 수준 동기화 활성화** : 전체 파일 대신 수정된 부분만 동기화합니다 . 이 옵션은 대역폭 사용량을 줄여주지만 CPU 작업 부하를 증가시킵니다 .

6. 메시지가 표시되면 다음 옵션 중 하나를 선택하여 원본에서 대상으로 동기화할 시기를 결정할 수 있습니다 .
   - **수정 시 동기화 실행** : 원본 공유 폴더에서 변경 사항이 발생하면 즉시 동기화합니다 .
   - **수동으로 동기화 실행** : 버튼을 클릭한 경우에만 원본 공유 폴더에서 동기화합니다 .
   - **고급 스케줄** : 설정한 스케줄에 따라 동기화합니다 . **스케줄 계획** 버튼을 클릭하여 동기화 작업 실행 시기를 지정합니다 .
7. **적용**을 클릭합니다 . 이제 작업 목록에서 동기화 작업을 확인할 수 있습니다 . 시스템은 지정된 스케줄에 따라 자동으로 작업을 실행합니다 .

#### 동기화 작업 관리

원본 Synology NAS 에 로그인하고 다음 단계를 참조하여 동기화 작업을 관리합니다 .

1. **제어판** > **공유 폴더 동기화**로 이동하고 **작업 목록** 버튼을 클릭합니다 .
2. **작업 목록** 창에서 작업을 선택하고 다음을 수행합니다 .
   - **편집** 버튼을 클릭하여 작업을 편집합니다 .
   - **삭제** 버튼을 클릭하여 작업을 삭제합니다 .
   - 동기화 작업이 진행되지 않으면 **지금 동기화** 버튼을 클릭하여 작업을 즉시 실행하십시오 .
   - 동기화 작업이 진행 중인 경우 진행 중인 작업을 중지하려면 **취소** 버튼을 클릭하십시오 .
   - 동기화 작업을 처음 실행할 경우 **공유 폴더 동기화**는 **전체 동기화**를 실행합니다 . 이 첫 번째 동기화 작업이 완료된 후에 수정된 부분만 동기화됩니다 . **전체 동기화**를 클릭하면 모든 데이터를 수동으로 다시 동기화할 수 있습니다 .

**참고 :**

- 동기화 작업 스케줄을 **수정 시 동기화 실행**으로 설정한 경우 **취소**를 클릭하면 진행 중인 동기화 작업이 중지됩니다 . 하지만 동기화 작업에 포함된 공유 폴더가 변경되면 공유 폴더 동기화에서 작업을 다시 시작합니다 .
- 양방향 동기화 기능을 사용하면 데이터가 손상될 수 있으므로 Synology Drive, Cloud Station Server 및 Cloud Sync 를 사용하여 백업을 실행하지 마십시오 .
- 대상에 이미 **MailPlus** 공유 폴더가 있는 경우 백업이 완료되면 폴더 이름이 **MailPlus_1** 로 변경됩니다 .
- **MailPlus_1** 의 데이터를 사용하려면 수동으로 데이터를 **MailPlus** 공유 폴더로 이동하십시오 .
- 계정 오류를 방지하려면 대상을 원본 ( 예 : LDAP 서버 또는 Windows Active Directory 도메인 ) 에 사용한 디렉토리 서버와 동일한 디렉토리 서버에 연결하십시오 .

### 시스템 구성 , 사서함 및 이메일 복원

시스템 구성 , 사서함 및 이메일은 대상 Synology NAS 의 로컬 공유 폴더에 저장됩니다 . 다음 단계를 참조하여 시스템 구성 , 사서함 및 이메일을 복원하십시오 .

1. **Hyper Backup** 을 시작합니다 .
2. 로컬 공유 폴더에서 백업한 구성을 복원합니다 . 자세한 내용은 **이 도움말 문서**를 참조하십시오 .
3. 복원 후 복원된 구성은 현재 MailPlus Server 구성을 덮어씁니다 .

4. 백업한 사서함과 이메일을 복원할 필요가 없습니다 . 즉시 사용할 수 있습니다 .

**참고 :**

- 현재 백업 및 복원 기능은 DSM 6.0 이상이 실행되는 MailPlus Server 1.0-164 이상에서 지원됩니다 .

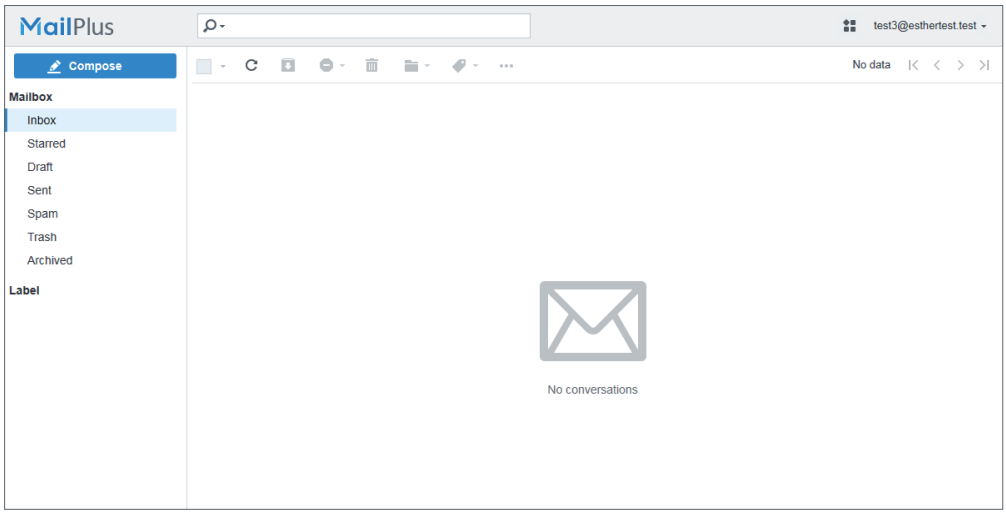
MailPlus 는 클라이언트 사용자에게 이메일을 보고 , 관리하고 , 보낼 수 있도록 사용하기 쉬운 웹메일 서비스를 제공합니다 . MailPlus 설정에 대한 자세한 내용은 **MailPlus 클라이언트 설정** 섹션을 참조하십시오 .

이 장에서는 MailPlus 구성 및 인터페이스 탐색을 설명합니다 . 자세한 내용은 **이 도움말 문서**를 참조하십시오 .

# 12 장 : MailPlus 탐색

## 기본 작업

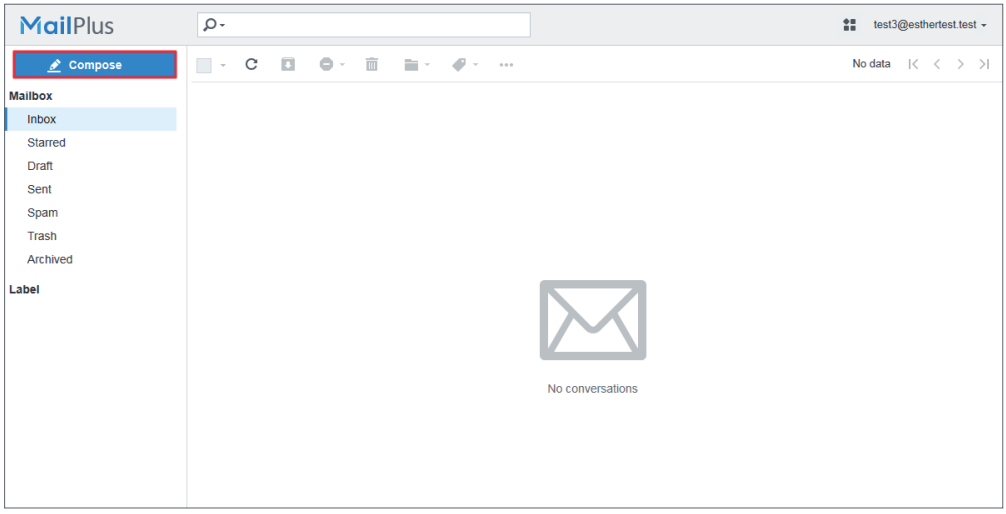
기본적으로 로그인하면 **사서함**이 표시됩니다 .



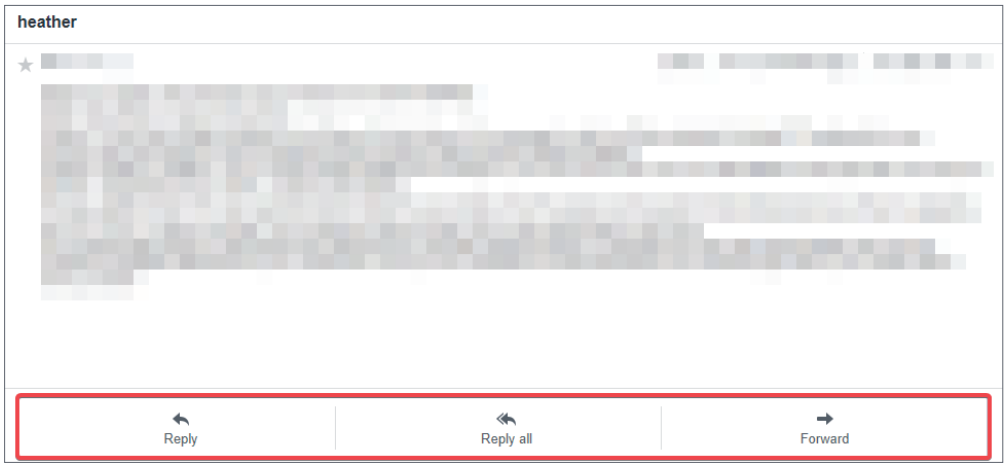

### 이메일 액세스 및 관리

**사서함**에서 다음 작업을 수행할 수 있습니다 .

- **이메일 작성** : 왼쪽 위 구석에 있는 **작성** 버튼을 클릭하여 이메일 초안을 작성합니다 . MailPlus 에서 이메일 초안을 자동으로 저장합니다 . 언제든지 **작성** 창을 닫고 **초안** 상자에서 다시 열어 쓰기를 다시 시작할 수 있습니다 .



- **이메일에 회신** : MailPlus 에서 이메일에 회신하는 방법에는 세 가지가 있습니다 .
  - **회신** : **회신**을 클릭하여 보낸 사람에게 회신합니다 .
  - **모두 회신** : 한 번에 모든 받는 사람 (CC 받는 사람 포함 ) 에게 회신하려면 **모두 회신**을 클릭합니다 .
  - **전달** : 원래 받는 사람 이외의 다른 사람에게 이메일을 보내려면 **전달**을 클릭합니다 .



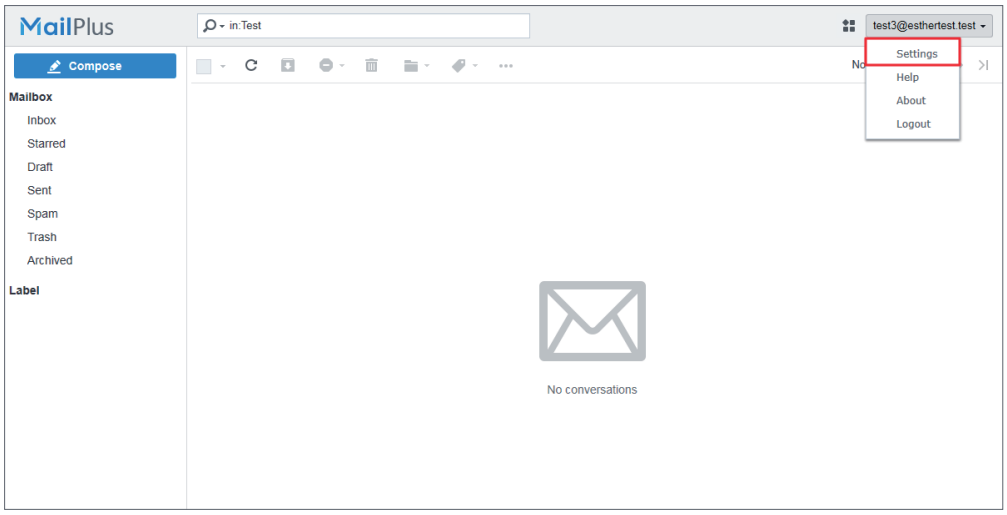

- **사서함별로 이메일 구성** : 필요에 따라 사서함을 여러 개 만들 수 있습니다 . 왼쪽 위 구석에 있는 **사서함**에 커서를 올려놓습니다 . 그러면 사서함 옆에 더하기 아이콘 (+) 이 표시됩니다 . 더하기 (+) 아이콘을 클릭하여 새 사서함을 만듭니다 .
- **레이블별 이메일 관리** : 레이블을 사용자 지정하여 이메일을 분류할 수 있습니다 . 왼쪽 패널에 있는 **레이블**에 커서를 올려놓습니다 . 그러면 레이블 옆에 더하기 아이콘 (+) 이 표시됩니다 . 더하기 (+) 아이콘을 클릭하여 새 레이블을 만듭니다 . 쉽게 식별할 수 있도록 레이블 이름을 입력하고 레이블 색상을 선택합니다 .

# 고급 설정

MailPlus 를 사용하면 클라이언트 사용자는 웹메일 레이아웃 , 자동 회신 / 전달 메시지 , 사서함 설정 및 메일 전달에 사용되는 프로토콜 ( 예 : SMTP 및 OpenPGP) 을 사용자 지정할 수 있습니다 . Synology MailPlus Server 의 MailPlus 관리자가 모든 사용자에게 적용된 일반 설정을 관리할 수 있습니다 . 앱 실행기에서 **연락처**와 관련 설정을 찾을 수 있습니다 **.**

이 장에서는 **SMTP**, **OpenPGP** 및 **블랙리스트 / 화이트리스트**의 구성을 설명합니다 . 다른 설정에 대한 자세한 내용은 **이 도움말 문서**를 참조하십시오 .

오른쪽 위 구석에 있는 계정 이름을 클릭하고 드롭다운 메뉴에서 **설정**을 클릭하여 MailPlus 를 구성합니다 .



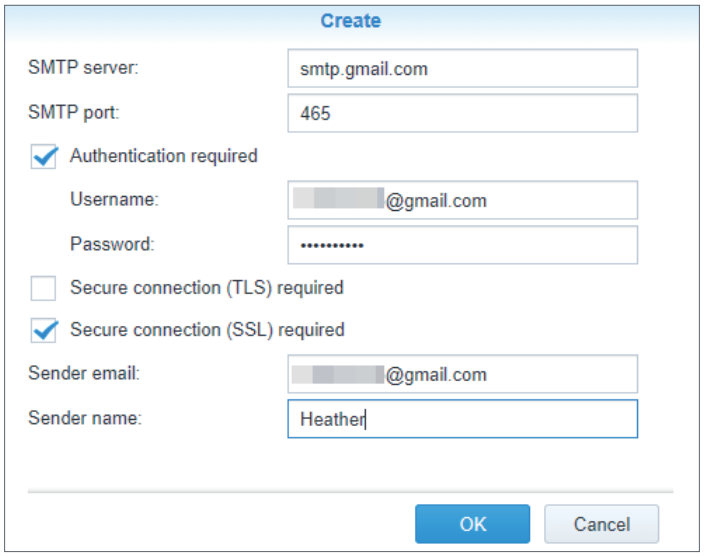

## SMTP 서버 추가

MailPlus 는 메일 전달에 사용되는 SMTP 서버를 여러 개 지원합니다 . SMTP 서버를 추가하지 않으면 MailPlus Server 는 모든 이메일을 배달하도록 자동으로 기본 SMTP 서버로 설정됩니다 . **보낸 사람 이름** 설정만 편집할 수 있습니다 .

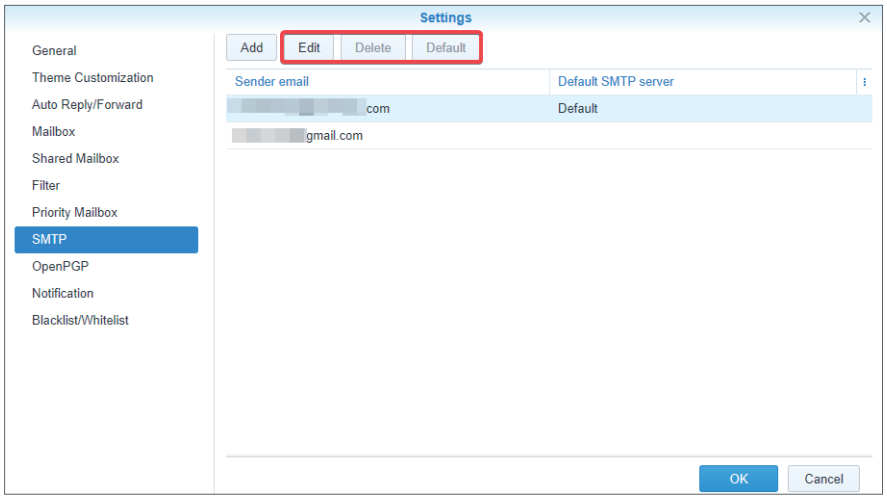
사용자는 MailPlus 에서 이메일을 발송하도록 다른 SMTP 서버를 추가할 수 있습니다 . 예를 들어 Google 의 SMTP 서버를 추가하여 MailPlus 의 Google 계정을 통해 이메일을 보낼 수 있습니다 . 아래 단계를 수행하여 SMTP 서버를 추가하십시오 .

1. **설정** > **SMTP** 로 이동합니다 .
2. 다음 정보를 입력합니다 .
   - **SMTP 서버** : 메일 서비스 공급자의 도움말 문서 또는 자습서에서 SMTP 서버를 찾습니다 .
   - **SMTP 포트** : 포트 번호는 자동으로 SSL/TLS 를 통한 SMTP 연결에 필요한 값으로 업데이트됩니다 . 기본적으로 포트 465 는 SSL 을 통한 SMTP 연결용이고 포트 587 은 TLS 를 통한 SMTP 연결용입니다 . SSL 및 TLS 확인란 중 아무것도 선택하지 않으면 SMTP 연결에 사용되는 표준 포트는 25 입니다 .
   - **인증 필요** : SMTP 서버에 인증이 필요하면 이 확인란을 선택합니다 .
     - **사용자 이름** : 이메일 주소를 입력합니다 .
     - **패스워드** : 이메일 패스워드를 입력합니다 .

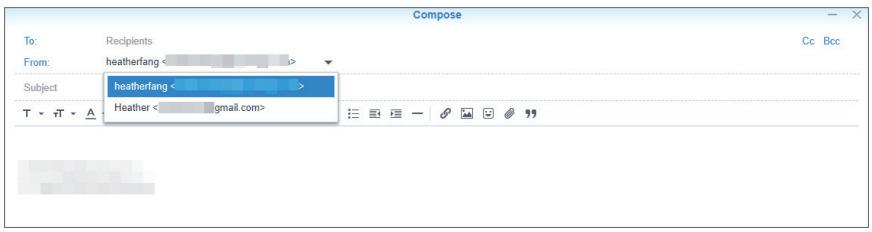
- **보안 연결 (TLS) 필요** : TLS 인증서로 연결을 보호하려면 이 확인란을 선택합니다 .
- **보안 연결 (SSL) 필요** : SSL 인증서로 연결을 보호하려면 이 확인란을 선택합니다 .
- **보낸 사람 이메일** : 이메일 주소를 입력합니다 . **사용자 이름**에 입력한 이메일 주소와 일치하지 않으면 이메일이 스팸으로 표시될 수 있습니다 .
- **보낸 사람 이름** : 받는 사람이 보낸 사람을 인지할 수 있도록 보낸 사람 이름을 입력합니다 .




3. **확인**을 클릭하여 설정을 저장합니다 .
4. 이제 목록에 새로 추가한 SMTP 서버 계정이 나타납니다 .
   - 위에 있는 도구 모음의 버튼을 클릭하여 서버를 편집 , 삭제하거나 기본 SMTP 서버로 설정할 수 있습니다 .



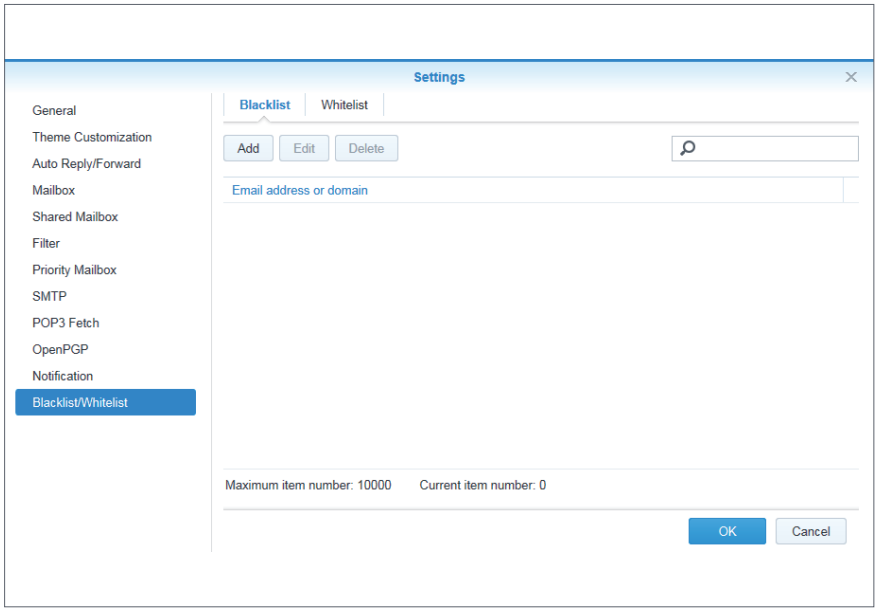

- 이메일을 작성할 경우 **보낸 사람 :** 필드에서 SMTP 서버 간에 전환할 수 있습니다 .



- 다른 사람에게 암호화된 이메일을 보내야 하는 경우 **가져오기** 버튼을 클릭하여 파일 또는 텍스트 입력에서 공개 키를 가져오십시오 .

## 블랙리스트 / 화이트리스트 관리

개인 블랙리스트와 화이트리스트를 만들어 **블랙리스트 / 화이트리스트** 페이지에서 특정 이메일 주소 / 도메인을 차단하거나 허용할 수 있습니다 . 지속적으로 스팸을 보내는 이메일 주소나 도메인을 **블랙리스트**에 추가하면 차단할 수 있습니다 . 마찬가지로 합법적인 이메일이 차단된 경우에는 이메일 주소나 도메인 이름을 **화이트리스트**에 추가하면 됩니다 .




### 이메일 주소 또는 도메인 이름 추가

1. **추가**를 클릭하여 새 항목을 블랙리스트 / 화이트리스트에 추가합니다 .
2. 이메일 주소나 도메인 이름을 지정하고 **확인**을 클릭하여 설정을 저장합니다 .
3. 새로 추가된 이메일 주소나 도메인 이름이 목록에 표시되어야 합니다 .

### 기존 이메일 주소 또는 도메인 이름 삭제

1. 제거할 이메일 주소나 도메인 이름을 클릭한 후 **삭제**를 클릭합니다 .
2. 삭제하려면 **예**를 , 취소하려면 **아니요**를 클릭합니다 .

### 기존 이메일 주소 또는 도메인 이름 편집

1. 편집할 이메일 주소나 도메인 이름을 클릭한 후 **편집**을 클릭합니다 .
2. 원하는 대로 변경한 후 **확인**을 클릭합니다 .
3. 이제 목록에서 이메일 주소나 도메인 이름이 제거됩니다 .


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

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

**SYNOLOGY UK LTD.**
Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL
United Kingdom
전화 : +44 (0)1908048029

**SYNOLOGY FRANCE**
102 Terrasse Boieldieu(TOUR W)
92800 Puteaux
France
전화 : +33 147 176288

**SYNOLOGY GMBH**
Grafenberger Allee 295
40237 Düsseldorf
Deutschland
전화 : +49 211 9666 9666

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

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


Synology®

synology.com