

---

# DaouOffice 시스템 어드민 가이드

Daou Tech., Inc.

# DaouOffice 시스템 어드민 가이드

차례	2
1. 시스템 어드민 시작하기	8
1.1 어드민이란	8
1.2 어드민 접속	9
관리자 설정정보 수정	9
2. 메인홈	11
3. 시스템 관리	13
3.1 개요	13
3.2 장비 관리	13
장비 추가	14
장비 수정	14
장비 삭제	15
3.3 라이선스	15
3.4 업데이트	16
소프트웨어 업데이트	16
업데이트 파일 등록	17
업데이트	17
릴리즈 노트	18
업데이트 Proxy 서버 설정	18
3.5 서비스 설정	19
이메일서버	19
송수신환경	19
기본환경	19
수신도메인변경	20
수신주소변경	20
메일송신옵션	20
송신허용정책	21
송수신실패정책	22
예약메일설정	22
프로세스설정	23
수신서버설정	23

송신서버설정	23
전달서버설정	24
POP서버설정	24
IMAP서버설정	25
이메일 검색 설정	25
성능 튜닝	26
반송 메일	26
메일 첨부 관리	27
TMA 연동	28
TMSe 서버	28
TMSe 연결설정	28
<b>4. 도메인/사이트 관리</b>	<b>30</b>
4.1 도메인 목록	30
도메인 추가	30
도메인 수정	31
도메인 삭제	31
도메인 검색	31
4.2 사이트 목록	32
사이트 추가	32
사이트 수정	34
사이트 삭제	34
사이트 검색	34
사이트 어드민으로 이동	34
4.3 사이트 그룹 목록	35
사이트 그룹 추가	35
사이트 그룹 수정	36
사이트 그룹 삭제	37
사이트 그룹 검색	37
<b>5. 보안 설정</b>	<b>38</b>
5.1 공통	38
안티바이러스	38
인증서	40
기본 인증서	40
자가 인증서	40
신뢰받은 인증서	41
API접근 설정	41
해외 로그인 차단 허용 설정	42
5.2 이메일 보안	42
안티 스팸	42

컨텐츠 필터	43
허용/차단 규칙 추가	43
허용/차단 규칙 수정	45
허용/차단 규칙 삭제	45
허용/차단 규칙의 사용 및 사용안함 설정	45
필터 검색	46
컨텐츠 룰 업데이트	46
접속 단계 차단	47
발송 IP 차단	48
시간당 접속 횟수 제한	48
동시 접속 횟수 제한	49
RBL	50
접속 단계 허용	51
SMTP 단계 차단	51
DNS 검사	52
SPF	52
송신자 차단	53
송신자 시간당 제한	54
수신자 차단	55
수신자 시간당 제한	55
동보 응답 지연	56
SMTP 단계 허용	57
필터 멤버 정책	57
필터 멤버 정책 추가	58
필터 멤버 정책 수정	58
필터 멤버 정책 삭제	58
필터 멤버 정책 사용/사용안함 설정	59
필터 멤버 정책 순서 적용	59
필터 멤버 정책 검색	59
필터 환경 설정	59
필터 정보 관리 서버	59
로컬 도메인, 호스트 허용 정책	60
로컬 베이스안	60
필터 검색	60
메일 정보 필터	61
유출 감시 모니터링	61
정보 보호 필터	62
감시 대상 설정	65
차단 알림메일 설정	65

메일 정보 보호 폴더 관리	66
메일 데이터 보안	66
SSL/TLS 접속설정	67
SMTP	67
POP	68
IMAP	68
5.3 WAS 보안	69
접속차단	69
세션검증	69
HTTPS 설정	70
<b>6. 통계</b>	<b>71</b>
6.1 개요	71
통계 정보 검색	72
통계 결과 다운로드	72
통계 결과 인쇄	72
6.2 이메일	73
요약	73
정상 메일	73
스팸 메일	74
모든 단계	74
접속 단계	74
SMTP 단계	75
컨텐츠 단계	75
피싱 메일	76
바이러스 메일	76
POP	77
IMAP	77
6.3 시스템	78
CPU	78
메모리	78
디스크	78
6.4 통계 보고서	79
통계 보고서 추가	79
통계 보고서 수정	79
통계 보고서 삭제	79
통계 보고서 설정	80
<b>7. 모니터링</b>	<b>81</b>
7.1 개요	81
7.2 실시간 현황	81

7.3 로그	82
이메일 로그	82
이메일 로그 검색	82
스팸메일/정상메일 등록	83
이메일 로그 새로고침	84
로그 설정	85
7.4 시스템현황	85
프로세스 현황	85
리소스 현황	86
메일처리 현황	86
수신 처리 현황	87
필터된 IP 검색	88
큐 현황	88
큐 검색	89
큐 삭제	90
큐 전송	90
7.5 문의 및 지원	90
메일문의	90
경고 메일 설정	91
<b>8. 모빌리티</b>	<b>92</b>
8.1 모바일 앱 버전 관리	92
모바일 앱 버전 추가	92
모바일 앱 버전 추가	93
모바일 앱 버전 삭제	93
모바일 앱 버전 필터링	93
<b>9. 기타 설정</b>	<b>94</b>
9.1 IP 그룹 설정	94
IP 그룹 추가	94
IP 그룹 수정	95
IP 그룹 삭제	95
9.2 초기화	95
9.3 보관 기간 설정	96
9.4 비밀번호 찾기 설정	96
<b>10. 관리자</b>	<b>97</b>
10.1 관리자 목록	97
관리자 추가	97
관리자 수정	98
관리자 삭제	98

관리자 검색 .....	99
10.2 관리자 로그 .....	99
관리자 로그 목록 .....	99
관리 내역 검색 .....	99
<b>그림 차례 .....</b>	<b>100</b>

# 1. 시스템 어드민 시작하기

---

## 1.1 어드민이란

JAVA 기반의 웹 방식의 운영자 Tool로 편리한 서비스 운영을 위해 제공됩니다. 서버 운영에 대한 경험이 없는 운영자도 어드민 페이지에 접속해서 서비스를 쉽게 운영할 수 있습니다.

### 어드민의 주요 기능

- 편리하고 쉬운 웹 기반의 관리자 서버
- 60여 가지 항목의 통계 정보 제공
- 실시간 시스템 모니터링 및 쉽고 편리하게 스팸 차단 룰 설정
- 실시간 로그 모니터링 지원 및 검색 기능 지원
- 각종 환경 설정 파일의 백업 및 복구
- 도메인 별, 그룹 별, 사용자 별 환경 설정 및 메일 서비스 지정
- 이전의 웹 커스터 마이징 사항이었던 것을 기능으로 구현 및 옵션화
- 웹 화면에 유용성을 주어, 관리자의 운영 부담 최소화
- 관리자 별 권한 설정

### 어드민 종류

어드민(관리자 페이지)에는 두 가지 종류가 있습니다.

- 시스템 어드민 - 시스템, 모니터링, 보안 등 시스템 또는 서비스 전체에 영향을 주는 항목을 설정할 수 있습니다. 시스템 어드민에 접근 가능한 사용자를 시스템 관리자라고 하며, 시스템 관리자는 모든 사이트 어드민에도 접속할 수 있는 권한이 있습니다.
- 사이트 어드민 - 시스템에 등록된 각각의 사이트를 관리하는 페이지입니다. 사이트 어드민에 접속할 수 있는 사용자를 사이트 관리자라고 부르며, 각 사이트별로 관리자를 따로 지정할 수 있습니다. 사이트 어드민에서는 특정 사이트에 종속되는 환경 및 서비스를 설정합니다.



## 1.2 어드민 접속

어드민에 접속하기 위해서는 네트워크에 연결된 PC 및 브라우저가 필요합니다.

### 로그인

시스템 어드민 및 사이트 어드민에 로그인하는 방법은 다음과 같습니다.

1. 웹 브라우저의 주소 창에 '`http://hostname:8000`'을 입력합니다. hostname은 DNS에 등록된 Daouoffice 서버의 hostname입니다.
2. 로그인 화면에서 **이메일**과 **패스워드**를 입력합니다.
  - I. 이메일 - 시스템 관리자의 기본 로그인 아이디는 '`mailadm@도메인`'입니다. 기본(default) 도메인의 경우 아이디만 입력해도 로그인이 가능합니다.
  - II. 패스워드 - 해당 계정에 대한 비밀번호를 입력합니다.
3. 아이디와 암호입력이 완료되면 Login을 클릭합니다.



보안을 위하여 mailadm으로 최초 로그인시 관리자 암호 수정화면으로 이동합니다.



시스템 어드민이나 사이트 어드민 모두 로그인 방법은 동일합니다. 단, 관리자의 권한에 따라 보여지는 페이지(시스템 어드민 또는 사이트 어드민)에 차이가 있습니다.



로그인 시 화면 상단에서 언어(한글, 일어)를 설정할 수 있습니다.

### 로그아웃

로그인 된 어드민 페이지에서 화면 오른쪽 상단에 있는 **로그아웃**을 클릭하여 세션을 종료합니다.

## 관리자 설정정보 수정

화면 우측 상단에 있는 로그인 한 사용자의 아이디를 클릭하면, 관리자 정보를 수정할 수 있는 화면으로 바로 이동할 수 있습니다.

수정할 수 있는 항목은 다음과 같습니다.

- 사용자 이름 - 관리자 이름이 자동으로 표기됩니다.
- 언어 - 시스템 어드민에서 사용할 언어를 선택합니다.
- 목록 개수 - 모니터링 등 목록으로 보이는 메뉴에서 한 화면에 출력할 목록 수를 선택합니다.

- 통계 출력 그래프 종류 - 통계 화면에 출력되는 그래프 종류를 선택합니다.
  - 꺾은선 그래프 - 각 항목의 변화 추이를 확인하고 싶을 때 선택합니다.
  - 막대 그래프 - 항목별 비교를 하고 싶을 때 선택합니다.
- 세션 유지 시간 - 관리자가 로그인 후, 정해진 시간동안 입력이 없으면 자동 로그 아웃할 시간을 선택 또는 입력합니다.

## 2. 메인홈

---

메인홈에서는 Daouoffice 서버의 메일 통계 및 시스템 상태를 한 눈에 확인할 수 있습니다.

### 알림

가장 최근에 업데이트된 현황, 스토리지 사용율, 프로세스의 상태가 표시됩니다.

### 정보

Daouoffice가 설치된 날짜와 서버의 라이선스, 버전 정보가 나타납니다.



라이선스 업데이트는 **[시스템 관리 > 라이선스]**에서 수행할 수 있습니다.

### 모니터링 요약

송수신된 메일의 통계와 시스템 상태정보가 나타납니다.

### 메일 트래픽

- 메일 종류 - 정상 메일, 스팸 메일, 피싱 메일, 바이러스 메일
- 시간/기간 - 최근 24시간, 최근 30일간



각 메일 종류별의 상세 통계 정보는 **[통계]**부분을 참조하십시오.

### 시스템 상태 정보

- 메일 프로세스 - 메일 송수신을 하는 데몬의 작동 상태를 보여줍니다.
- 웹 서비스 - 사용자 웹 서비스의 작동 상태를 보여줍니다.
- 부하율 - 시스템 부하율을 보여줍니다.
- CPU 사용율 - CPU의 사용 현황을 보여줍니다.
- Memory - 메모리의 사용 현황을 보여줍니다.

- Disk - 각 파티션 별 디스크 사용 현황을 보여줍니다.



시스템 상태에 대한 좀 더 자세한 정보는 [\[모니터링 > 시스템현황\]](#)을 참조하십시오.

## 3. 시스템 관리

---

### 3.1 개요

Daouoffice 서버가 정상적으로 운영되기 위해서는 각 환경이 우선적으로 설정되어야 합니다. **시스템 관리**에서는 Daouoffice 서버 각각의 환경을 설정할 수 있습니다.

**시스템 관리**메뉴에서 수행할 수 있는 기능은 다음과 같습니다.

- Daouoffice가 설치된 서버 등록
- 라이선스 관리
- 버전 업데이트
- 내부의 중요 파일 백업 및 복구
- 서비스 환경설정

### 3.2 장비 관리

장비 관리에서는 Daouoffice가 설치된 장비 정보를 확인하고, 내부의 장비를 설정 및 관리합니다. Daouoffice는 여러 대의 장비(multi-host)로도 서비스를 할 수 있습니다. Daouoffice가 여러 장비로 구성되어 있는 경우, 각 장비를 모두 등록하여 관리자 화면을 통해 관리할 수 있습니다.

장비 관리 화면의 목록 구성은 다음과 같습니다.

- 장비명 - Daouoffice가 설치된 장비 이름을 FQDN으로 보여줍니다.
- IP - Daouoffice가 설치된 장비의 IP를 보여줍니다.

## 장비 추가

Daouoffice가 설치되어 있는 장비를 추가합니다. Daouoffice가 설치되어 있지 않는 장비는 추가할 수 없습니다.

1. 시스템 어드민의 [시스템 관리 > 장비관리]를 클릭합니다.
2. 장비 목록에서 **추가**를 클릭합니다.
3. 장비 추가 화면에서 각 항목을 입력합니다.
  - I. 장비 명 - 장비 명을 입력합니다. 이 때, 서버의 FQDN을 입력합니다. (예) tims.mydomain.co.kr
  - II. HOST ID - HOST ID를 입력합니다. HOST ID 는 최초 Daouoffice 설치 시 (주)다우기술에서 부여 받은 값을 입력해야 합니다.
  - III. IP - IP를 입력합니다.
  - IV. 가상 IP - Daouoffice 장비를 여러 장비에 설치하여 운영할 때, 다음과 같은 특수한 경우에 백단 장비의 가상 IP를 입력합니다.
    - i. 스토리지와 연결된 백단 장비를 여러 대로 구성하고, 백단 스토리지 장비를 공유합니다.
    - ii. 백단 장비를 L4 스위치에 연결하여 L4 스위치가 백단 장비로 가는 트래픽을 로드 밸런싱 합니다.
    - iii. 이러한 특수한 경우에 L4 스위치는 IP를 부여받고, 앞단 장비는 L4 스위치로 메일 트래픽을 전달합니다. 이때 L4 스위치에 부여한 IP가 백단 장비의 가상 IP 입니다.
  - V. 메일 서버 스토리지 장비로 사용 - 사용자의 메일함과 메일이 저장하기 위한 스토리지 장비를 사용할 지 여부와 각 항목을 설정합니다.
    - i. 사용여부 - 스토리지 장비 사용 여부를 선택합니다.
    - ii. Index FS - IndexFS는 사용자 메일함이 생성되는 디렉터리이므로, 만약 사용자 메일함이 운영될 서버가 아닐 경우에는 입력할 필요가 없습니다. IndexFS는 동시에 여러 곳을 지정할 수 있습니다.
    - iii. Data FS - DataFS는 사용자 메일이 저장되는 디렉터리입니다. 만약 사용자 메일함이 운영될 서버가 아닐 경우에는 입력할 필요가 없습니다. DataFS는 동시에 여러 곳을 지정할 수 있습니다.
  - VI. WAS 스토리지 장비로 사용 - 캘린더, 게시판, 커뮤니티, 주소록에 대한 설정과 첨부파일을 저장하기 위한 스토리지 장비를 사용할 지 여부와 각 항목을 설정합니다.
    - i. 사용여부 - 스토리지 장비 사용 여부를 선택합니다. 캘린더, 게시판, 커뮤니티, 주소록에 대한 설정과 첨부파일을 저장하는 공간이므로, 이 기능을 사용하지 않으면 설정할 필요가 없습니다.
    - ii. Was FS - WAS 스토리지로 사용할 디렉터리를 입력한 후 **추가**를 클릭합니다.
4. 설정이 완료되면, **추가**를 클릭합니다.

## 장비 수정

장비 관리 목록에서 장비 정보를 수정합니다.

1. 시스템 어드민의 [시스템 관리 > 장비관리]를 클릭합니다.
2. 장비 목록에서 수정할 장비의 장비명을 클릭합니다.
3. 장비 수정 화면에서 각 항목을 수정합니다.
4. 수정이 완료되면, **수정**을 클릭합니다.



HOST ID는 수정할 수 없습니다.

## 장비 삭제

장비 관리 목록에서 장비 정보를 삭제합니다.

1. 시스템 어드민의 **[시스템 관리 > 장비관리]**를 클릭합니다.
2. 장비 목록에서 삭제할 장비를 모두 선택한 후, 목록 상단에 있는 **삭제**를 클릭합니다.

## 3.3 라이선스

Daouoffice에서는 기본적으로 메일, 주소록, 자료실, 캘린더, 조직도 기능을 제공합니다. 정규 패키지 외 게시판, 커뮤니티, 첨부파일 미리보기 등의 부가기능을 사용하려면 별도의 라이선스를 구매한 후 등록해야 합니다.

라이선스 현황은 다음과 같습니다.

### 기본 라이선스

- 계정 라이선스: Daouoffice를 이용할 수 있는 계정의 수를 정의합니다.

### 서비스 라이선스

다음의 라이선스를 각각 등록할 수 있습니다. 라이선스를 등록할 때마다 해당하는 기능이 활성화됩니다. 예를 들어, Social 라이선스를 등록하면 게시판, 커뮤니티, 예약/대여, 설문 기능이 활성화되어 보입니다.

- Social: 게시판, 커뮤니티, 예약, 설문
- Mobile: 모바일 웹, 모바일 앱, 동기화, PC 메신저
- Collaboration: Works, 보고, ToDo+

### 기간 라이선스

기간 라이선스는 다음과 같이 Spam과 Virus가 있으며, 기간 라이선스가 종료되면 새로운 필터를 업데이트 할 수 없습니다.

- Spam: 스팸 룰을 업데이트하기 위해 필요한 라이선스입니다.
- Virus: 바이러스 필터를 업데이트하기 위해 필요한 라이선스입니다.

### 부가기능 라이선스

- 보안 메일: 메일을 보낼 때 비밀번호를 설정하여 메일을 발송하는 기능입니다. 수신자는 메일을 확인할 때 비밀번호를 입력해야만 메일을 볼 수 있습니다.
- OTP(One-Time Password): 사용자는Daouoffice에 로그인할 때마다 아이디, 비밀번호 외 일회용 비밀번호

호 인증기를 통해 얻은 OTP 비밀번호를 한 번 더 입력해야 합니다.

- 미리보기: 메일, 게시판, 커뮤니티, 보고서, 설문에 있는 파일을 다운로드하지 않고 바로 볼 수 있는 기능입니다.

라이선스 업데이트 하는 방법은 다음과 같습니다.

1. 새 라이선스를 ㈜다우기술 지원팀으로부터 발급 받습니다.
2. 시스템 어드민의 [시스템 관리 > 라이선스]를 클릭합니다.
3. **파일 선택**을 클릭하여, 로컬 컴퓨터에 있는 라이선스를 찾아 업로드합니다.
4. **등록**을 클릭합니다.



Daouoffice가 여러 대에 설치되어 있다면, 각 장비별로 라이선스를 업로드합니다.



업데이트 후 [모니터링 > 문의및지원 > 경고 메일 설정]에서 경고 메일의 **사용 여부**를 **사용**으로 설정하기를 권장합니다.

## 3.4 업데이트

라이선스 정보를 확인하고, 최신 버전으로 업데이트하거나 업데이트 Proxy 서버를 설정할 수 있습니다.

### 소프트웨어 업데이트

온라인으로 업데이트를 수행할 수 없을 경우, 업데이트 파일을 업로드하여 오프라인으로 업데이트를 진행할 수 있습니다.



Daouoffice가 여러 대 설치되어 있으면 서버별로 버전을 확인하고 업데이트를 수행하시기 바랍니다.

Daouoffice에서 제공하는 제품 버전 정보는 다음과 같습니다.

- 현재 버전 - 현재 설치된 Daouoffice의 버전
- 업데이트 파일 버전 - 업데이트하기 위해 업로드 한 Daouoffice 패키지



## 업데이트 파일 등록

버전을 업데이트하기 위해 먼저 Daouoffice 패키지를 등록합니다.

1. 시스템 어드민의 **[시스템 관리 > 업데이트]**를 클릭합니다.
2. **업데이트 파일 등록**에 있는 **파일 선택**을 클릭하여 ㈜다우기술에서 받은 패키지 파일을 선택한 후 **확인**을 클릭합니다.  
또는, **다운로드 URL 입력**에 패키지를 받을 수 있는 URL을 입력한 후 **확인**을 클릭합니다.



매일 0시(자정) ~ 01시에 에이징 데몬이 구동되며, 업데이트와 관계없이 지정된 시각에 에이징 데몬이 업로드 된 패키지를 삭제합니다. 이점 참고하시기 바랍니다.

## 업데이트

Daouoffice의 최신 버전으로 업데이트합니다. 업데이트하려면 Daouoffice 패키지가 업로드 되어 있어야 합니다.

1. 시스템 어드민의 **[시스템 관리 > 업데이트]**를 클릭합니다.
2. 업데이트 파일 버전을 확인한 후, **업데이트 시작**을 클릭합니다.  
업로드한 파일의 버전이 현재 설치된 버전과 같거나 낮으면 **업데이트 시작**이 보이지 않습니다.
3. 업데이트 확인 메시지 창이 나타납니다. **확인**을 클릭합니다.



업데이트를 수행하는 데 수분~수십 분이 소요될 수 있습니다.



업데이트 후에는 필요에 따라 Daouoffice 서버 재시작이 필요한 경우가 있습니다. 서버를 재시작해야 하는 경우에는 재시작 메시지가 나타납니다.

서버를 재시작하면 Daouoffice 서비스가 수분 정도 중단되니, 이점 유의하시기 바랍니다.



Daouoffice의 버전은 **플랫폼.메이저.마이너**로 이루어집니다. 예를 들어, 버전이 8.4.0이라면 8이 플랫폼 버전, 4는 메이저 버전, 0은 마이너 버전입니다.

메이저 버전 이상이 업데이트된 경우 라이선스를 다시 설치해야 합니다. 라이선스 등록 방법은 [3.3 라이선스](#)를 참조하시기 바랍니다.



패키지를 업로드 한 이후에는 업데이트 화면이 나타납니다. 새로운 패키지를 업로드 하려면 **돌아가기**를 클릭합니다.

## 릴리즈 노트

오프라인 업데이트를 수행한 적이 있는 경우 해당 버전의 릴리즈 노트를 확인할 수 있습니다.



오프라인 업데이트를 수행한 적이 있는 경우에만 **릴리즈 노트**가 나타납니다.

1. 시스템 어드민의 **[시스템 관리 > 업데이트]**를 클릭합니다.
2. 현재 버전 옆에 있는 **릴리즈 노트**를 클릭합니다. 릴리즈 노트가 화면이 나타납니다.

## 업데이트 Proxy 서버 설정

업데이트 proxy서버 설정은 스팸 및 바이러스 필터와 각종 제품 관련 정보를 인터넷을 통해서 업데이트 받을 때에 웹 프록시 서버를 통해서 할 경우에 설정합니다.

프록시 사용시에 아이디와 암호를 필요로 하는 인증 프록시의 경우는 Basic Auth만 지원합니다.



프록시 인증을 사용할 때 암호에서 #문자를 사용할 수 없습니다.

프록시 서버를 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[시스템 관리 > 업데이트]**를 클릭합니다.
2. **업데이트 Proxy 서버 설정**에서 다음 항목을 설정합니다.
  - I. Proxy 서버 사용 - 사용 여부를 선택합니다. 웹 프록시 서버를 통해 필터와 제품을 업데이트할 경우에 설정 하시기 바랍니다. (기본값: 사용안함)
  - II. Proxy 인증 - 프록시 서버 인증의 사용여부를 선택합니다. 인증 방식은 **BASIC**방식입니다. (기본값: 사용안함)
  - III. Proxy 인증설정 - 프록시 서버 인증을 사용할 경우 나타나는 항목입니다. **아이디**와 **암호**를 입력합니다.
  - IV. Proxy 서버정보 - 프록시 서버의 IP와 포트를 입력합니다.
3. **테스트**를 클릭하여 서버 연결을 확인합니다.
4. 설정이 완료되면, **확인**을 클릭합니다.

## 3.5 서비스 설정

### 이메일서버

메일 송수신과 관련된 환경 및 프로세스, 검색 등에 대하여 설정합니다.

#### 송수신환경

##### 기본환경

Daouoffice가 메일을 송수신할 때 적용할 기본 정책을 설정합니다.

1. 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 기본환경]을 클릭합니다.
2. 기본 환경 설정의 항목을 설정합니다.
  - I. 최대 송수신 메일 크기 - 송수신 메일의 최대 크기를 설정합니다. 설정한 메일의 최대 크기보다 큰 메일이 송수신된 경우, 수신이 거부 됩니다.
  - II. 스팸검사 최대 크기 - 스팸을 검사하는 최대 메일크기를 설정합니다. 설정한 메일크기 보다 큰 메일은 스팸 검사를 하지 않습니다. 권장값은 512KB 입니다.
  - III. 최대 수신자 수 - 한 번에 SMTP로 접속할 수 있는 최대 수신자 수를 설정합니다. 최대 2000명까지 지정할 수 있습니다.
  - IV. 최대 HOP 수 - 수신 메일에 허용할 수 있는 최대 HOP 수 입니다. 즉, 메일 헤더의 'Received' 필드의 최대 허용 수입니다. 현재까지 메일이 거쳐온 서버들은 기록하는 것으로서, 제한 값 이상이면 스팸 메일이나 비정상적인 메일일 가능성이 크므로 필터링 규칙에 의해 처리됩니다.
  - V. 최대 세션 수 - 한 번의 SMTP 접속으로 허용하는 메일 통 수를 설정합니다. 보통 스팸 발송기는 한 번의 접속으로 많은 양의 메일을 송신하므로 적절한 값으로 설정하기를 권합니다. 권장값은 20입니다.
  - VI. Greeting 메시지 - SMTP 프로토콜을 알리는 첫 메시지입니다.
  - VII. 첨부 파일명 최대 길이 - 수신 메일에 첨부되는 파일의 이름 길이를 제한합니다.
  - VIII. 최대 첨부파일 수 - 수신 메일에 첨부된 파일의 최대 개수를 제한합니다.
  - IX. 송신자 IP주소 헤더에 추가 - 송신자 IP주소를 x-header로 추가할지 여부를 선택합니다.
  - X. 메일주소 RFC 준수 검사 - 수신메일에 대한 송수신자의 메일주소의 RFC2821 표준 준수 여부를 검사합니다. (권장값: 사용)  
 Daouoffice 자체 사양으로 ID에 연속된 2개의 점(...)은 허용하나 퍼센트(%)나 앰퍼샌드(&)는 허용하지 않습니다. 이 사양은 웹 메일에 한해 적용됩니다. MS Outlook 이나 Outlook Express 등과 같은 PC용 메일 클라이언트에서는 위 사양이 적용되지 않습니다.
  - XI. SMTP 인증 - SMTP 인증 기능의 사용 여부를 선택합니다.  
 CRAM-MD5 암호화 방식을 지원합니다. 단, CRAM-MD5를 사용하려면 도메인의 사용자 비밀번호 암호화가 Clear Text 또는 TWOFISH로 설정되어야 합니다.
  - XII. Mail From 인증 - 메일의 송신자가 로컬 도메인의 사용자인 경우, SMTP 프로토콜 상의 Mail From 명령어에 있는 메일 주소가 존재하는지 검사여부를 선택합니다. 송신자가 존재하는 경우에만 메일이 발송됩니다.

- XIII. 인증 ID와 다른 Mail From 거부 - SMTP Auth 와 Mail From 인증이 다를 경우, 수신을 거부 할지 여부를 선택합니다.
- XIV. 수신자 존재 감추기 - SMTP 상에서 Rcpt To의 메일 주소를 갖는 사용자가 없을 경우, 보통 No Such User 라는 에러메시지를 전달합니다. 사용으로 설정하는 경우, 에러 메시지를 전달하지 않고 무조건 수신합니다. 사용자의 존재 여부를 숨길 때 사용합니다.
- XV. 사용자별 송신 메일 크기 정책 - 사용자 별로 송신 할 수 있는 메일 크기를 다르게 적용할지 여부를 선택합니다. 사용으로 설정한 경우 기본 제한 크기를 입력합니다. 권장값은 100M입니다.  
사용자별 송신 메일 크기는 SMTP 인증을 실시하는 메일 클라이언트 프로그램(예: MS Outlook, MS Express, LiveMail, Eudora, Thunderbird 등)을 이용할 때만 적용됩니다.

3. 설정이 완료되면, **저장**을 클릭합니다.

## 수신도메인변경

메일 수신환경에서 SMTP의 Mail From이나 Rcpt To 명령어에 있는 메일 주소 중 도메인 부분을 변경합니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 수신도메인변경]**을 클릭합니다.
2. 수신 도메인 바꾸기 적용여부를 선택합니다.
3. 사용으로 선택한 경우, 수신 변경 전의 도메인과 변경 후의 도메인을 텍스트 박스에 입력합니다.  
(예) tims.co.kr mydomain.co.kr
4. **추가**를 클릭합니다.
5. 설정이 완료되면, **저장**을 클릭합니다.

## 수신주소변경

메일 수신환경에서 SMTP의 Rcpt To 명령어에 있는 수신자의 메일 주소를 변경합니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 수신주소변경]**을 클릭합니다.
2. 수신 주소 변경 적용여부를 선택합니다.
3. 사용으로 선택한 경우, 수신 변경 전의 메일주소와 변경 후의 메일주소를 텍스트 박스에 입력합니다.(예)aaa@mydomain.co.kr bbb@mydomain.co.kr
4. **추가**를 클릭합니다.
5. 설정이 완료되면, **저장**을 클릭합니다.

## 메일송신옵션

송신 옵션 설정에서는 임의의 메일 서버를 지정하여 메일을 지정한 메일 서버에 발송할 수 있습니다. 메일 송신 옵션을 설정하면 DNS 서버에서 수신자의 메일 서버 주소를 쿼리하지 않고, 설정된 메일 서버로 메일을 발송합니다. 다수의 메일 서버를 지정한 후 다수의 수신자에게 메일을 발송하는 경우 메일을 분산하여 발송하므로 빠른 속도로 메일을 보낼 수 있습니다.

- 분할 수신자 수 - 메일송신시 메일 서버에 한번에 전달하는 사용자의 수입니다.  
(예) 분할 수신자 수가 30명이고 300통의 메일을 발송하는 경우, 30통씩 10번에 나누어서 발송합니다.
- 메일 송신 게이트웨이 서버 - 메일 송신시 메일을 전달할 메일 서버를 입력합니다. 최대 5개까지 입력할 수 있습니다.  
(예) 분할 수신자 수가 30명이고 300통의 메일을 발송하는 경우, 30통씩 메일 서버에 전달됩니다. 다수의 메일

서버가 설정된 경우 메일이 전달되는 순서는 임의로 결정됩니다.

- 도메인별 발송 서버 - 외부 도메인에 메일을 발송할 때, 특정 도메인에 대한 발송 서버를 지정할 수 있습니다. 도메인별로 1개 설정할 수 있으며 최대 10개까지 설정할 수 있습니다.  
(예) 특정 도메인(mydomain.co.kr)에 대한 발송 서버(175.115.93.43)를 지정하면, 메일 주소에 해당 도메인이 있는 경우 지정한 발송 서버로 메일을 전송합니다.

메일 송신 옵션을 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 메일송신옵션]을 클릭합니다.
2. 각 항목을 설정합니다.
  - I. 분할 수신자 수 - 메일 송신시 한번에 메일 서버에 전달하는 사용자의 수를 입력합니다.
  - II. 메일 송신 게이트웨이 서버 목록 - 송신 게이트웨이 역할을 할 서버의 IP 와 포트를 입력하고 추가아이콘(>)을 클릭합니다.
  - III. 도메인별 발송 서버 - 발송 서버를 지정할 도메인과 발송 서버의 IP와 포트를 입력하고, **추가**를 클릭합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.

## 송신허용정책

메일의 송신 허용 환경 정책을 설정합니다. 수신자가 외부 도메인인 경우, 외부 메일 서버로 메일을 송신하게 됩니다. 외부로 메일을 송신할 수 있는 사용자는 인증을 거친 사용자이거나, 외부 송신이 허락된 IP로부터 메일을 송신할 수 있습니다.

1. 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 송신허용정책]을 클릭합니다.
2. 릴레이 설정을 선택합니다. 송신 허용 정책은 다음과 같이 4가지를 지원합니다.
  - I. 모든 릴레이 허용 - 허가되지 않는 사용자에게도 릴레이를 허용합니다.
  - II. 모든 릴레이 불허 - 허가된 사용자에게만 릴레이를 허용합니다.
  - III. 부분 릴레이 허용 - 릴레이를 불허하되 부분적으로 허용합니다. 기본적으로 릴레이를 거부합니다.
  - IV. 부분 릴레이 불허 - 릴레이를 허용하되 부분적으로 불허합니다.  
기본적으로 릴레이를 허용하지만, 불허 IP와 불허 송신자 도메인에 등록되어 있는 경우에는 릴레이를 거부합니다.
3. 각 릴레이 설정 선택에 따른 세부 항목을 설정합니다.
  - I. 세부 설정 - **부분 릴레이 허용** 선택 시 나타나는 항목입니다.
  - II. 허용 IP주소 - **부분 릴레이 허용** 선택 시 나타나는 항목입니다.
    - i. 허용 IP 주소를 등록합니다. 허용 IP 주소에 등록된 IP 에서 송신한 메일은 인증절차 없이 외부로 발송됩니다.
    - ii. 허용 IP 목록에 추가한 IP를 삭제, 검색할 수 있습니다.
  - III. 무조건 불허IP - **부분 릴레이 허용** 선택 시 나타나는 항목입니다.
    - i. 무조건 불허 IP를 등록합니다.
    - ii. 무조건 불허 IP 목록에 추가한 IP를 삭제, 검색할 수 있습니다.
  - IV. 허용 수신자(Mail From) 도메인 - **부분 릴레이 허용** 선택 시 나타나는 항목입니다.
    - i. 허용 송신자(Mail From) 도메인을 등록합니다.
    - ii. 허용 송신자(Mail From) 도메인목록에 추가한 도메인을 삭제, 검색할 수 있습니다.
  - V. 허용 수신자(Rcpt To) 도메인 - **부분 릴레이 허용** 선택 시 나타나는 항목입니다.

- i. 허용 수신자(Rcpt To) 도메인을 등록합니다.
    - ii. 허용 수신자(Rcpt to) 도메인 목록에 추가한 도메인을 삭제, 검색할 수 있습니다.
  - VI. 불허 IP주소 - **부분 릴레이 불허** 선택 시 나타나는 항목입니다.
    - i. 불허 IP 주소를 등록합니다.
    - ii. 불허 IP 주소 목록에 추가한 IP 주소를 삭제, 검색할 수 있습니다.
  - VII. 불허 송신자 도메인 - **부분 릴레이 불허** 선택 시 나타나는 항목입니다.
    - i. 불허 송신자 도메인을 등록합니다.
    - ii. 불허 송신자 도메인 목록에 추가한 도메인을 삭제, 검색할 수 있습니다.
4. 설정이 완료되면, **저장**을 클릭합니다.

## 송수신실패정책

송신되어야 할 메일이 메일 서버의 장애로 인해 송신에 실패할 경우, 메일은 송신 메일 큐에 임시로 보관되며, 송수신 메일 큐에 메일이 쌓이게 됩니다. 송수신 실패 정책에서는 송수신 메일 큐에 쌓여 있는 메일을 처리 하는 방법을 설정합니다.



시스템 부하가 높을 경우 재시도 간격이 정해진 시간보다 더 늦춰지거나, 재시도를 하지 않는 경우가 발생할 수 있습니다. 처리되지 못한 큐에 대해서는 계속 큐 디렉터리에 남아있게 됩니다.

송수신 실패 정책을 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [**시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 송수신실패정책**]을 클릭합니다.
2. 송신 또는 수신 실패 정책을 설정합니다.
  - I. 처리 간격 - 재전송을 시도하려는 처리 간격을 설정합니다.
  - II. 최대 보존 기간 - 송신 또는 수신 실패 큐에 보존될 기간을 설정합니다. 최대값은 7일이며 권장값은 3일입니다. 모두 실패할 경우, 해당 메일은 리턴으로 처리됩니다.  
(예) 처리 간격이 20분에 최대 보존 기간이 1시간인 경우, 1시간 동안 총 5번을 재전송 시도를 합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



최대 보존 기간을 권장값(3일)보다 크게 설정하면 시스템에 심각한 장애를 초래할 수 있습니다. 권장값 설정을 강력히 권고합니다.

## 예약메일설정

예약 메일 발송 주기 및 발송 메일 서버를 설정합니다.

1. 시스템 어드민의 [**시스템 관리 > 서비스 설정 > 이메일서버 > 송수신환경 > 예약메일설정**]을 클릭합니다.
2. 예약 메일을 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. 최대 예약 가능 기간 - 예약 메일 큐를 보존할 최대 시간을 지정합니다. 불필요한 기간 동안의 메일을 저장 해두는 것을 방지하기 적당한 기간으로 설정합니다.
  - II. 송신 간격 - 일정한 시간마다 예약 메일 큐를 체크하여 예약한 시간에 메일을 발송하도록 합니다.

- III. 예약 메일 DB보존 디렉터리 - 예약 메일 발송 정보 DB를 저장할 디렉터리를 지정합니다.
  - IV. 송신 서버명 - 사용할 송신 서버의 호스트 명이나 IP를 입력합니다.
  - V. 송신 SMTP 포트 - 발송 메일 서버의 포트를 지정합니다.
  - VI. 컨넥션 타임아웃 - 발송 메일 서버의 응답 제한 시간을 지정합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.

## 프로세스설정

각 메일 서버 시스템에 관련된 파라미터들을 설정합니다.

### 수신서버설정

수신 서버에서는 메일을 수신하여 사용자 메일함에 전달하거나 수신 큐에 저장합니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스설정 > 수신서버설정]**을 클릭합니다.
2. 수신 서버를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. 최대 쓰레드 개수 - 최대 쓰레드 수를 지정합니다.
  - II. 시작 쓰레드 개수 - 수신 서버가 가동할 때 시작되는 쓰레드의 개수를 지정합니다.
  - III. 쓰레드 당 처리 건수 - 한 쓰레드당 메일 큐를 처리하는 작업 수를 지정합니다. 지정한 수만큼 처리하면, 쓰레드는 자신이 사용하던 리소스를 반환하고, 프로세스를 종료 합니다.
  - IV. 내부 컨넥션 타임아웃 - TCP 접속 후에 설정된 시간동안 프로토콜이 들어오지 않으면 접속을 해제합니다.
  - V. 내부 I/O 타임아웃 - TCP 접속 후에 설정된 시간동안 데이터의 입출력이 없으면 접속을 해제합니다.
  - VI. Busy메시지 응답시간 - SMTP 프로토콜 통신 시, 메시지 응답 처리를 지연시키기 위한 지연시간을 입력합니다.
  - VII. 라우팅 프로토콜 - Daouoffice가 여러 대로 구성되어 있는 경우 메일 수신 시 내부 통신에 사용할 프로토콜을 선택합니다.
  - VIII. 라우팅 포트 - 라우팅 포트를 입력합니다. SMTP 사용 시 25번 포트가 TMTP 사용시 7777번 포트가 자동으로 입력됩니다.
  - IX. MTA timeout - 수신 서버는 SMTP 단계별로 타임아웃을 지정할 수 있습니다. 타임아웃 지정은 **MTA timeout** 탭을 클릭하면 나타나며, 각 단계는 다음과 같습니다.
    - i. connection, greeting, helo, mailfrom, rcptto, receiving\_data, endofsession, rset, handshaking, rcptauth
3. 설정이 완료되면, **저장**을 클릭합니다.

### 송신서버설정

메일을 외부로 발송할 경우, 메일 큐를 송신 큐에 저장합니다. 이 때, 송신 서버에서는 송신큐에 저장된 메일 큐를 처리하는 역할을 합니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스설정 > 송신서버설정]**을 클릭합니다.
2. 송신 서버를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. 최대 쓰레드 개수 - 최대 쓰레드 수를 지정합니다.
  - II. 시작 쓰레드 개수 - 송신 서버가 가동할 때 시작되는 쓰레드의 개수를 지정합니다.
  - III. 외부 I/O 타임아웃 - TCP접속 후에 설정한 시간동안 파일의 입출력이 없으면 접속을 해제합니다.

- IV. 외부 컨넥션 타임아웃 - 상대방 메일 서버에 접속 후, 설정한 시간동안 프로토콜의 입출력이 없으면 접속을 해제합니다.

3. 설정이 완료되면, **저장**을 클릭합니다.

## 전달서버설정

전달 서버는 메일을 사용자의 메일함까지 전달해주는 역할을 하며, 동보로 수신되는 메일이나 512KB 이상의 메일을 처리합니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스설정 > 전달서버설정]**을 클릭합니다.
2. 전달 서버를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. 최대 라우팅 쓰레드 개수 - 최대 라우팅 쓰레드 개수는 메일 전달 또는 리턴 메일을 전담하는 쓰레드의 수를 제한합니다.
    - i. 최대 라우팅 쓰레드 개수를 지정합니다.
    - ii. 개수는 최대 라우티드 쓰레드 수의 25% 정도로 설정하는 것을 권장합니다.
  - II. 최대 라우티드 쓰레드 개수 - 수신 큐에 쌓인 메일을 사용자 메일함에 전달할 때 사용되는 쓰레드 수의 최대 값을 지정합니다.
  - III. 백업 쓰레드 개수 - 백업 쓰레드는 라우티드 쓰레드가 처리하지 못하고 남긴 메일 큐를 처리합니다.
    - i. 백업 쓰레드의 개수를 지정합니다.
  - IV. 쓰레드 당 처리 건수 - 지정된 수만큼 작업 수를 처리하면, 쓰레드는 자신이 사용하던 리소스를 반환하고, 프로세스를 종료 합니다.
    - i. 한 쓰레드당 메일 큐를 처리하는 작업 수를 지정합니다.
  - V. 라우팅 컨넥션 타임 아웃 - TCP 접속이 이루어진 이후에 지정된 시간동안 프로토콜이 없을 경우 접속을 해제합니다.
  - VI. 라우팅 I/O 타임 아웃 - TCP 접속이 이루어진 이후에 지정된 시간동안 데이터의 입출력이 없을 경우 접속을 해제합니다.
  - VII. 재시도 간격 - 수신 큐에 저장된 메시지가 설정된 주기마다 발송을 재시도 합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.

## POP서버설정

POP 서버의 프로세스 파라미터를 확인하고 수정합니다. POP 서버를 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스설정 > POP서버설정]**을 클릭합니다.
2. POP 서버를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. 최대 쓰레드 개수 - POP 서버가 허용할 수 있는 최대 쓰레드 개수를 지정합니다.
  - II. 시작 쓰레드 개수 - POP 서버가 가동될 때의 쓰레드 개수를 지정합니다.
  - III. I/O 타임 아웃 - TCP 접속 후, 설정된 시간동안 파일의 입출력이 없으면 접속을 해제합니다.
  - IV. 포트 - POP 서버의 기본적인 서비스를 제공하는 포트를 지정합니다. 기본값은 110입니다. Daouoffice가 여러 대로 구성되어 있는 경우에는 내부 장비로 서비스 되는 포트를 의미합니다.
  - V. 프록시 포트 - Daouoffice가 여러 대로 구성되어 있는 경우 외부에 서비스를 제공하는 포트입니다. 기본값은 110입니다. Daouoffice가 한 장비로 구성되어 있는 경우 프록시 포트는 의미가 없습니다.
  - VI. 최대 POP 명령어 수 - POP 서버가 인식가능한 명령어를 받을 수 있는 수를 지정합니다.
  - VII. 최대 인식 불가능 명령어 수 - POP 서버가 인식할 수 없는 명령어를 받을 수 있는 수를 지정합니다.



- VIII. 관리자 암호 설정 - POP 서버에 접속할 수 있는 관리자 암호를 설정합니다. POP 프로토콜을 이용하여 사용자 메일함에 접근시 관리자 암호를 입력하면 모든 사용자 아이디로 로그인 가능합니다.
- IX. POP 프록시 IP 설정 - 일반 사용자와 POP서버 간에 중개 역할을 하는 프록시 서버에 접근할 수 있는 IP를 설정합니다.

3. 설정이 완료되면, **저장**을 클릭합니다.



관리자 암호를 사용하면 모든 사용자 아이디로 로그인이 가능하므로 관리자의 각별한 주의가 필요합니다.

## IMAP서버설정

IMAP 서버의 프로세스 파라미터를 확인하고 수정합니다. IMAP 서버를 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스설정 > IMAP서버설정]**을 클릭합니다.
2. IMAP 서버를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. 최대 쓰레드 개수 - IMAP 서버가 허용할 수 있는 최대 쓰레드 개수를 지정합니다.
  - II. 시작 쓰레드 개수 - IMAP 서버가 가동될 때의 쓰레드 개수를 지정합니다.
  - III. I/O 타임 아웃 - TCP 접속 후, 설정된 시간동안 파일의 입출력이 없으면 접속을 해제합니다.
  - IV. 포트 - IMAP 서버의 기본적인 서비스를 제공하는 포트를 지정합니다. 기본값은 143입니다. Daouoffice가 여러 대로 구성되어 있는 경우에는 내부 장비로 서비스 되는 포트를 의미합니다.
  - V. 프록시 포트 - Daouoffice가 여러 대로 구성되어 있는 경우 외부에 서비스를 제공하는 포트입니다. 기본값은 143입니다. Daouoffice가 한 장비로 구성되어 있는 경우 프록시 포트는 의미가 없습니다.
  - VI. 최대 IMAP 명령어 수 - IMAP 서버가 인식가능한 명령어를 받을 수 있는 수를 지정합니다.
  - VII. 최대 인식 불가능 명령어 수 - IMAP 서버가 인식할 수 없는 명령어를 받을 수 있는 수를 지정합니다.
  - VIII. 관리자 암호 설정 - IMAP 서버에 접속할 수 있는 관리자 암호를 설정합니다. IMAP 프로토콜을 이용하여 사용자 메일함에 접근시 관리자 암호를 입력하면 모든 사용자 아이디로 로그인 가능합니다.
  - IX. IMAP 프록시 IP 설정 - 일반 사용자와 IMAP서버 간에 중개 역할을 하는 프록시 서버에 접근할 수 있는 IP를 설정합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



관리자 암호를 사용하면 모든 사용자 아이디로 로그인이 가능하므로 관리자의 각별한 주의가 필요합니다.

## 이메일 검색 설정

웹에서 메일 검색 시, 메일의 검색 범위 및 용량, 첨부파일 검색 포맷을 설정할 수 있습니다.

1. 시스템 어드민의 **[시스템 관리 > 서비스 설정 > 이메일서버 > 이메일 검색 설정]**을 클릭합니다.
2. 검색 엔진의 항목을 설정합니다.
  - I. 허용여부 - 메일 검색 시, 메일의 본문과 첨부파일도 검색할지 허용여부를 선택합니다.
    - i. 본문 검색 허용 - 메일 본문의 내용까지 검색합니다.
    - ii. 첨부 검색 허용 - 첨부 파일의 본문 내용까지 검색합니다.
  - II. 허용용량 - 검색 범위에 포함되는 메일의 크기를 지정합니다. 기본값은 10Mbytes입니다.

- III. 허용 파일 포맷 - 첨부검색 허용까지 검색 시, 첨부 파일 본문 검색이 가능한 첨부 파일 포맷을 선택합니다. 현재 지원하는 첨부 파일 포맷을 다음과 같습니다.
- \*.chm, \*.doc, \*.docx, \*.dwg, \*.htm, \*.hwd, \*.hwp, \*.html, \*.jtd, \*.mdi, \*.mht, \*.msg, \*.pdf, \*.ppt, \*.pptx, \*.rtf, \*.sql, \*.sxc, \*.sxi, \*.txt, \*.wpd, \*.xls, \*.xlsx, \*.xml
  - 파일 포맷을 추가하려면 목록에서 파일 포맷을 선택한 후, 추가아이콘(➤)을 클릭합니다.
  - 파일 포맷을 삭제하려면 추가된 목록에서 삭제하려는 파일 포맷을 선택한 후, 삭제아이콘(⬅)을 클릭합니다.
3. 검색 엔진 설정이 완료되면, **저장**을 클릭합니다.



검색범위를 본문이나 첨부파일내용으로 선택한 후 검색어를 영어로 입력하는 경우 중간문자열 검색이 불가능합니다. 공백문자(space)로 구분하여 첫 문자열을 입력해야 검색이 됩니다. (예) test라는 문자열을 검색하려면 tes 또는 test를 입력합니다. est를 입력하면 검색이 되지 않습니다.



본문이나 첨부 검색을 허용한 이후 수신된 메일부터 검색됩니다. 이전에 수신한 메일은 검색되지 않습니다.

## 성능 튜닝

관리자가 성능과 관련된 옵션을 직접 설정할 수 있습니다. 성능과 관련된 옵션은 다음과 같습니다.

- 사용자 인덱스 생성 주기 - 사용자의 인덱스가 생성되는 주기를 지정합니다. 지정된 수만큼 메일이 수신될 경우 인덱스를 생성합니다.
- 싱글 카피 스토어 - 동보 메일의 경우 원본 파일만 디스크에 저장하고 다른 메일은 원본 파일의 하드 링크를 생성하여 사용합니다.



성능 튜닝 옵션은 시스템에 미치는 영향이 크므로, 성능 튜닝 옵션을 변경할 때는 (주)다우기술의 기술지원 팀에게 문의하시기 바랍니다.

성능 튜닝을 설정하는 방법은 다음과 같습니다.

- 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > 성능 튜닝]을 클릭합니다.
- 사용자 인덱스 생성 주기를 입력합니다.
- 싱글 카피 스토어 사용 여부를 선택합니다.
- 설정이 완료되면, **저장**을 클릭합니다.

## 반송 메일

Daouoffice는 반송하는 메일에 대한 이유(메일 수신자 없음, 메일 용량 초과, 바이러스 메일, 메일 서버 거부 외 다수)를 알려주기 위해 메일을 전송하는 기능을 제공합니다. 반송 메일은 외부로 송신한 메일의 경우에만 적용됩니다.

반송 메일의 변수는 다음과 같습니다.

- \$subject: 반송되는 메일의 제목
- \$reportmta: 반송 메일을 보내는 MTA 호스트명
- \$recipient: 메일 수신자
- \$status: SMTP 상태 코드 (예)4.2.1 <domain> Service not available , closing transmission channel
- \$diagnostic: 실패 이유 (예)550 Don't send spam.

반송 메일 작성 방법은 다음과 같습니다.

1. 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > 반송 메일]을 클릭합니다.
2. 각 항목을 입력합니다.
  - I. 제목 - 반송 메일의 제목을 입력합니다. 기본적으로 설정되어 있는 제목을 사용하길 권합니다.
  - II. 송신자 메일 주소 - 송신자의 메일주소를 입력합니다. 입력하지 않으면 postmaster@기본도메인으로 메일이 발송됩니다.
  - III. 본문 - 메일 변수를 참조하여 메일 본문을 작성합니다.
  - IV. 메일 원문 포함 - 메일 원문을 포함할지 여부를 선택합니다. 사용을 선택하면, 메일 원문은 첨부 파일 형식으로 발송됩니다.
3. 설정이 완료되면, **저장**을 클릭합니다.

## 메일 첨부 관리

메일 첨부과 관련된 설정과 로그아웃 시간을 설정합니다.

1. 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > 메일 첨부 관리]를 클릭합니다.
2. 첨부관리와 자동 로그 아웃 시간을 설정합니다.
  - I. 첨부관리 - 메일의 첨부파일에 대한 옵션을 설정합니다.
    - i. 대용량 첨부 다운로드 만료일 - 대용량 첨부 파일을 다운로드할 수 있는 기간을 입력합니다.
    - ii. 대용량 첨부 다운로드 횟수 - 대용량 첨부 파일을 다운로드할 수 있는 횟수를 입력합니다.
    - iii. 일반 첨부 최대 크기 - 업로드 가능한 일반 첨부 파일의 최대 크기를 입력합니다. 파일 크기 단위는 MB입니다. 최대값은 100MB이며 권장값은 20MB입니다.
    - iv. 대용량 첨부 파일 최대 크기 - 업로드 가능한 대용량 첨부 파일의 최대 크기를 입력합니다. 파일 크기 단위는 MB입니다. 최대값은 1,850MB이며 권장값은 500MB입니다.
    - v. 대용량 첨부 파일함 총 용량 - 첨부 가능한 대용량 파일함의 최대 크기를 입력합니다. 파일 크기 단위는 MB입니다. 최대값은 20,480MB이며, 권장값은 2,000MB입니다.
    - vi. 첨부 업로드 시 Ez Upload 사용 여부 - 메일, 자료실, 게시판 등에서 첨부 파일 업로드 시 드래그&드롭으로 파일을 첨부하는 기능을 사용할 것인지 여부를 선택합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



일반 첨부와 대용량 첨부 최대 크기에 최대값을 설정하면 웹 서비스에 심각한 장애를 초래할 수 있습니다. 권장값 설정을 강력히 권고합니다.

## TMA 연동

(주)다우기술의 아카이빙(Archiving) 서버인 Terrace Mail Archive 서버와의 연동을 설정합니다. Terrace Mail Archive는 이메일 보존 정책에 부합하는 장기간의 신뢰성 있는 메일 저장 기능과 정보보호 기능을 제공하는 이메일 아카이빙 솔루션입니다.

Terrace Mail Archive서버 연동 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [시스템 관리 > 서비스 설정 > 이메일서버 > TMA 연동]을 클릭합니다.
2. TMA 연동의 각 항목을 설정합니다.
  - I. 기본 환경
    - i. 사용 여부 - Terrace Mail Archive 서버와의 연동을 할 것인지를 선택합니다.
    - ii. 저장 상세 옵션 - 스팸 메일과 바이러스 메일 저장 여부를 설정합니다.
    - iii. 아카이브 서버 정보 - 아카이브 서버의 IP와 포트를 입력합니다. 서버 정보 입력이 완료되면, **테스트**를 클릭하여 테스트를 수행합니다.
  - II. 통합로그인
    - i. 사용 여부 - 아카이빙 된 메일을 확인하기 위해 아카이브 센터를 접속할 때, SSO(Single Sign On) 방식을 사용하지 여부를 선택합니다.
    - ii. DES 암호화 KEY - 아카이브 센터에 접속할 때 사용할 암호화 KEY를 입력합니다. SMTP 인증을 HTTP로 요청하면 변수들이 웹 주소상에 보여지므로 보안을 위해 DES key로 암호화하여 입력합니다.  
Terrace Mail Archive 서버에서 설정한 암호화 KEY가 동일하게 입력되어야 합니다.
    - iii. SSL 사용여부 - SSO로 접속시 SSL(Secure Socket Layer) 프로토콜을 사용할 지 여부를 선택합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.

## TMSe 서버

다우오피스와 Terrace Mail Security 기능을 이용하기 위해 각 제품 IP설정과 연동 설정을 진행합니다.

Terrace Mail Security 기능 이용 시 보안센터와 스마트분류 기능을 이용할 수 있습니다.

- 보안센터 : 스팸메일함, APT메일함, 승인보류/승인대기 메일함 제공으로 스팸 또는 표적성 메일을 막아주고 외부로 발송되는 메일은 별도 승인하게 발송되도록 관리할 수 있습니다.
- 스마트분류 : 광고, 소셜, 청구서 메일을 스스로의 관리없이 시스템에서 지정해놓은 상세한 규칙에 의해 자동으로 분류하여 제공합니다.



해당 기능을 이용하려면 TMSe 제품을 별도 구입해야 합니다.

## TMSe 연결설정

기본환경에서 다우오피스와 Terrace Mail Security IP를 설정합니다.

1. **TMSe 연결설정** : TMSe 사용을 위해 연결 할 것인지를 선택합니다. 제품을 구입한 경우 '사용' 선택을 선택하시기 바랍니다.
2. **DO IP 설정** : 다우기술 다우오피스 그룹웨어가 실행되는 장비의 IP를 입력 합니다
3. **TMSe IP 설정** : 다우기술 Terrace Mail Security 가 실행되는 장비의 IP를 입력 합니다. '테스트' 버튼을 선택을 통해 정상적인 연결을 확인합니다. 성공실패 시, IP를 재 확인해주시기 바랍니다.

연동설정에서 스마트분류와 보안센터 메뉴 사용여부를 선택합니다.

1. **TMSe 자동 연동** : 사용 선택 시, TMSe 연결설정에서 기본환경 > IP설정이 정상적으로 동작되면 자동으로 로그인됩니다.
2. **스마트 분류** : 사용 선택 시, 메일 메뉴에 스마트분류함이 보여집니다.
3. **보안센터 메뉴** : 사용 선택 시, 메일 메뉴에 보안센터가 보여집니다. 보안센터 사용에 따라 다우오피스 홈 > 가젯에서도 보안센터 가젯을 이용할 수 있습니다.
4. **승인자 직접 지정** : 연동설정 후에 승인자 직접 지정 사용 선택 시, 외부도메인으로 메일을 발송할 경우 메일 메뉴에 승인자 지정 팝업이 보여집니다.

## 4. 도메인/사이트 관리

---

### 4.1 도메인 목록

#### 도메인 추가

도메인을 추가하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 도메인 목록]**을 클릭합니다.
2. 도메인 목록 상단에 있는 **추가**를 클릭합니다. 도메인 추가화면으로 이동합니다.
3. 도메인 추가화면에서 각 항목의 정보를 입력합니다.
  - I. 도메인 명 - 도메인 명을 FQDN으로 입력합니다. (예) mydomain.co.kr
  - II. 로그인 방법 - 로그인 할 때 사용자를 구별하기 위해 입력해야 하는 정보를 선택합니다.
  - III. 가상도메인 - 해당 도메인이 소유하고 있는 가상의 도메인 주소를 입력한 후 **추가**를 클릭합니다.  
가상도메인이란 위에 입력한 도메인이 사용하는 모든 정보를 동일하게 사용하는 도메인을 의미합니다. 예를 들어, mydomain.com이라는 도메인을 mydomain.co.kr의 가상도메인으로 지정하면, mydomain.com과 mydomain.co.kr이라는 도메인을 같은 도메인으로 취급하여 처리합니다.
  - IV. 사용자 별 가상도메인 - 위에서 지정한 가상도메인은 이 도메인의 모든 사용자에게 똑같이 적용됩니다. 사용자별로 가상도메인을 다르게 설정하고 싶다면, **사용자별 가상도메인**에 해당 도메인을 입력합니다.  
사이트 관리자는 사용자의 가상도메인을 여기에서 입력된 도메인 중에서 선택하여 설정할 수 있습니다.
4. 입력이 완료되면, **저장**을 클릭합니다.



도메인 명, 도메인 웹 주소, 로그인 방법은 필수 입력 항목입니다.

## 도메인 수정

도메인 목록에서 도메인 정보를 수정합니다. 단, 사이트에서 사용 중인 도메인은 수정할 수 없습니다.

1. 시스템 어드민의 [도메인/사이트 관리 > 도메인 목록]을 클릭합니다.
2. 도메인 목록에서 수정하려는 도메인의 이름을 클릭합니다.
3. 도메인 수정화면에서 각 항목의 정보를 수정합니다.
4. 정보 수정이 완료되면, **저장**을 클릭합니다.



도메인명 변경 시, 변경전 도메인의 통계 및 로그 정보는 초기화됩니다.

## 도메인 삭제

추가한 도메인 중 사용하지 않는 도메인을 삭제합니다. 기본 도메인이나 사용 중인 도메인은 삭제할 수 없습니다.

1. 시스템 어드민의 [도메인/사이트 관리 > 도메인 목록]을 클릭합니다.
2. 도메인 목록에서 삭제하려는 도메인을 선택한 후, **삭제**를 클릭합니다.



패키지를 설치할 때 입력한 도메인이 기본 도메인입니다. 기본 도메인에는 바탕색이 있어, 도메인 목록에서 쉽게 찾아볼 수 있습니다.

## 도메인 검색

도메인을 입력하여 등록된 도메인을 검색할 수 있습니다. 등록된 도메인이 많다면, 검색을 이용하여 도메인을 한 번에 찾을 수 있습니다.

1. 시스템 어드민의 [도메인/사이트 관리 > 도메인 목록]을 클릭합니다.
2. 도메인 목록의 우측 상단에 있는 검색창에 검색어를 입력합니다. 검색어에는 도메인 이름을 입력합니다.  
(예) user, mydomain.co.kr
3. 엔터키를 누르거나 **검색**을 클릭합니다.

패키지를 설치할 때 도메인을 입력해야 합니다. 이를 기본 도메인이라고 하며, 기본적으로 도메인 목록에는 기본 도메인이 표시됩니다.

사이트를 추가하려면 먼저 사이트에서 사용하는 도메인이 생성되어 있어야 합니다. **도메인 목록**에서는 기본 도메인 외 추가로 도메인을 추가하거나 추가한 도메인을 수정 또는 삭제할 수 있습니다.

## 4.2 사이트 목록

사이트 현황을 확인하고 관리합니다. 또한, 사이트 어드민으로 이동하여 각 사이트의 게시판, 자료실, 주소록, 조직도 등을 관리할 수 있습니다.

### 사이트 추가

사이트를 추가합니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 목록]**을 클릭합니다.
2. 사이트 목록 상단에 있는 **추가**를 클릭합니다. 사이트 추가화면으로 이동합니다.
3. 사이트 추가화면에서 각 항목의 정보를 입력합니다.
  - I. 사이트 기본정보
    - i. 도메인 명 - 사이트에서 사용할 도메인을 선택합니다. 도메인은 **[도메인/사이트 관리 > 도메인 목록]**에서 확인하거나 추가할 수 있습니다.  
사이트 추가가 완료되면 도메인 정보는 수정할 수 없습니다.
    - ii. 사이트명 - 사이트의 기관이나 회사 이름을 입력합니다.
    - iii. 접속 URL - 사이트를 접속 주소를 입력합니다.
    - iv. 사이트 Indexfs / Datafs - 메일 호스트를 선택하면 해당 호스트의 Indexfs 목록과 Datafs 표시됩니다. Indexfs와 Datafs를 선택한 후, **추가**를 클릭합니다.  
Indexfs는 사용자 메일함이 만들어지는 디렉터리이고, Datafs는 사용자 메일이 저장되는 디렉터리입니다. Indexfs와 Datafs는 동시에 여러 곳을 지정할 수 있습니다.
    - v. 최대 사용자 수 - 사이트에서 사용할 수 있는 최대 사용자 수를 입력합니다. 사이트의 최대 사용자 수는 **[시스템 관리 > 라이선스]**에서 등록된 계정 라이선스의 수를 초과하여 입력할 수 없습니다.
    - vi. 비밀번호 암호화 - 사이트의 사용자 패스워드의 암호화 방법을 선택합니다.
    - vii. 총 할당 계정 용량 - 사이트에서 사용할 수 있는 메일 용량과 자료실 용량의 합을 입력합니다. 이 사이트에서 모든 계정이 사용할 수 있는 메일 용량과 자료실 용량을 합한 값입니다.  
최소 2GB 이상을 입력해야 합니다.
    - viii. 공용 용량 - 전사 자료실, 게시판, 커뮤니티 내 게시판, 보고, 업무에서 첨부파일을 저장할 수 있는 용량을 입력합니다. 공용 용량이 초과되면 사용자가 전사 자료실, 게시판, 커뮤니티내 게시판, 보고, 업무에 파일을 첨부할 수 없도록 설정할 수 있습니다.  
공용 용량은 게시판, 보고서, 업무, 자료실의 사용량으로, 해당 기능을 사용하지 않더라도 있더라도 용량에는 포함됩니다.
    - ix. 공용 용량 초과 경고 발송 - **공용 용량**이 설정되면 나타나는 메뉴입니다. 공용 용량이 초과되면 용량 초과에 대한 알림 메일을 보낼지를 선택합니다. 알림 메일은 사이트 관리자와 시스템 관리자에게 하루에 한번 발송됩니다.
    - x. 공용 용량 초과 경고 비율 - **공용 용량**이 설정되면 나타나는 메뉴입니다. 공용 용량 초과 경고 메일을 발송할 비율을 입력합니다. 예를 들어 **공용 용량 초과 경고 비율**에 90을 입력하면 설정된 공용 용량의 90%가 사용되었을 때 알림 메일이 발송됩니다.
    - xi. 공용 용량 초과시 제재 - **공용 용량**이 설정되면 나타나는 메뉴입니다. 공용 용량이 초과되면 자동으로



전사 자료실, 게시판, 커뮤니티내 게시판, 업무, 보고 등에 첨부파일을 올리지 못하게 할 수 있습니다. 용량 초과 시 첨부파일을 올리지 못하게 하려면 **공용 용량 초과시 제재**를 **사용**으로 설정합니다. 최소 10GB 이상을 입력해야 합니다.

- xii. 사용 기간 - 서비스 이용기간을 선택할 수 있습니다. 구축형 서비스 경우, 무제한으로 설정합니다. 직접 입력을 통해 사용기간이 선택된 경우 해당 기간에만 사용이 가능하니 주의하시기 바랍니다.

## II. 관리자 추가정보

- i. 이름 (한글) - 사이트의 운영 담당자 이름을 입력합니다.
- ii. 아이디 - 사이트어드민의 관리자 권한이 주어져서 서비스에도 접근 가능한 아이디입니다. 관리자 정보는 라이선스 사용자 수에 포함되며 사이트어드민의 계정목록에도 추가됩니다.
- iii. 전화 - 사이트 소유 기관의 운영 관리자 직통 번호를 입력합니다.

## III. 제공 서비스

- i. 메일 서비스 - 이 사이트에서 사용할 수 있는 메일 서비스를 선택합니다.
- ii. 각 메뉴의 사용 여부를 선택합니다. **사용 안함**을 선택하면 사이트 어드민 및 웹 서비스로 접속했을 때, 해당 메뉴가 보이지 않습니다.
- iii. 해외 로그인 차단 - 해외에서의 접속을 허용할지를 선택합니다.  
해외 로그인을 차단하더라도 **[보안 설정 > 해외 로그인 차단 허용 설정]**에서 IP를 등록하면 특정 IP의 접속은 허용할 수 있습니다.

4. 입력이 완료되면, **저장**을 클릭합니다.



**도메인 명, 사이트명, 사이트 Indexfs/Datafs, 최대 사용자 수는 필수 입력항목입니다.**



한 도메인에 여러 사이트를 추가할 수는 있지만, 한 사이트에서 여러 도메인을 사용할 수는 없습니다. 한 도메인에 여러 사이트를 추가한 경우에는 사이트별 통계는 지원하지 않습니다.



사용자를 추가할 때마다 총 할당 계정 용량이 초과되지 않는지 확인합니다. 총 할당 계정 용량이 초과한 순간부터 사용자를 추가할 수 없습니다.

전사 자료실, 게시판, 커뮤니티내 게시판, 보고, 업무에서 사용하는 양을 계산하여, 공용 용량을 초과하지 않는지 하루에 한번 확인합니다. 지정한 공용 용량을 초과한 경우에는 시스템 관리자와 사이트 관리자에게 메일이 발송됩니다.



제공 서비스는 등록된 라이선스에 따라 다르게 보입니다. 예를 들어, Social 서비스 라이선스가 등록되지 않았다면, 게시판, 커뮤니티, 예약, 설문은 나타나지 않습니다.

라이선스에 대한 좀 더 자세한 설명은 [3.3 라이선스](#)를 참조하시기 바랍니다.



해외 로그인 차단을 위한 IP 정보는 매일 자동으로 한 번 업데이트됩니다. 수동으로 업데이트할 수는 없습니다.

## 사이트 수정

사이트 목록에서 사이트 정보를 수정합니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 목록]**을 클릭합니다.
2. 사이트 목록에서 수정하려는 사이트의 이름을 클릭합니다.
3. 사이트 수정화면에서 각 항목의 정보를 수정합니다. 단, 도메인은 수정할 수 없습니다.
4. 정보 수정이 완료되면, **수정**을 클릭합니다.

## 사이트 삭제

등록한 사이트를 삭제합니다.



사이트를 삭제하면, 사이트에 관련된 데이터(메일, 게시판, 커뮤니티, 자료실 데이터)가 모두 삭제됩니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 목록]**을 클릭합니다.
2. 사이트 목록에서 삭제하려는 사이트를 선택한 후, **삭제**를 클릭합니다.

## 사이트 검색

도메인이나 사이트 이름으로 사이트를 검색합니다. 등록된 사이트가 많다면, 검색을 이용하여 사이트를 한번에 찾을 수 있습니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 목록]**을 클릭합니다.
2. 사이트 목록의 우측 상단에 있는 검색창에 검색어를 입력합니다. 검색어에는 도메인 또는 사이트명을 입력해야 합니다.  
(예) iser, mydomain.co.kr, ABC기술
3. 엔터키를 누르거나 **검색**을 클릭합니다.

## 사이트 어드민으로 이동

사이트 어드민으로 이동하면 각 사이트의 메일, 게시판, 자료실, 커뮤니티, 조직도 등에 대한 설정을 확인하거나 변경할 수 있습니다.

사이트 어드민으로 이동하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 목록]**을 클릭합니다.
2. 서비스를 관리하려는 사이트의 **사이트로 이동**을 클릭합니다.



사이트 관리자는 사이트 어드민에만 접근할 수 있습니다. 시스템 관리자는 시스템 어드민과 사이트 어드민 모두 접속할 수 있습니다.

## 4.3 사이트 그룹 목록

하나의 시스템에 두 개 이상의 사이트를 구축하고 해당 사이트를 그룹사의 조직으로 구성할 수 있습니다. 그룹사의 조직도를 공유할 수 있으며, 검색처리를 통해 유연하게 두개의 사이트를 이동할 수 있습니다.

### 사이트 그룹 추가

2개 이상의 사이트 그룹을 생성할 수 있으며, 사이트 그룹을 추가하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 그룹 목록]**을 클릭합니다.
2. 사이트 그룹 목록 상단에 있는 **추가**를 클릭합니다. 사이트 그룹 추가화면으로 이동합니다.
3. 사이트 추가화면에서 각 항목의 정보를 입력합니다.
  - I. 사이트 그룹 기본정보
    - i. 사이트 그룹명 명 - 사이트를 하나로 묶을 **그룹명**을 입력합니다.
    - ii. 사이트 매칭 - **그룹에 포함되는 사이트**를 선택한 후, **화살표**를 클릭하여 추가합니다.
      - 조직도 계층구조 - 상단 들어쓰기/내어쓰기 버튼을 통해 매친된 사이트를 계층구조로 설정할 수 있습니다. 해당 설정 시, 서비스 조직도에도 계층구조로 표현됩니다.
  - II. 검색자 목록
    - i. 검색자 추가 - 1인 다수의 사이트에 소속된 경우, 검색자로 설정할 수 있습니다. **추가**를 클릭하고 각 사이트에서 검색으로 등록되어 있는 사용자를 선택한 후, 화살표를 클릭하여 추가합니다. **확인**을 클릭합니다.
    - ii. 검색자 삭제 - 검색자 목록에서 **삭제할 대상**을 체크한 후, **삭제**를 클릭합니다.
  - III. 검색자 외 조직도 공유
    - i. 조직도 공유자 - 그룹 사이트의 조직도를 조회할 수 있는 **공유 대상자**를 선택합니다.
      - 선택 안함 - 검색자만 조직도를 공유합니다.
      - 지정 사용자 - 사용자, 부서, 직위, 직급, 직책, 사용자 그룹별로 조직도 공유자를 설정할 수 있습니다.
      - 모든 사용자 - 그룹에 소속한 사이트의 모든 사용자들이 조직도를 공유합니다.
    - ii. 공유 범위 - 조직도 공유 대상자에게는 두가지 방법으로 조직도를 공유합니다.

- 조직도와 검색 제공 - 그룹사의 모든 **부서 정보를 공개**합니다.
  - 검색만 제공 - 부서 정보의 트리 구조는 공개하지 않고 **검색으로만 부서 및 사용자를 확인할 수** 있습니다.
4. 사이트 매칭으로 그룹에 포함된 사이트 간 **게시판과 예약/자산 콘텐츠를 공유**할 수 있습니다.
- I. 전사 게시판 공유 탭에서 **추가**를 클릭하면 **전사 게시판 공유 설정** 레이어가 뜹니다.
    - i. 전사 게시판 선택 - 상단에 **사이트 별 생성된 전사 게시판 중 공유할 게시판을 선택**합니다.
    - ii. 공개범위 - 상단에 선택한 A 사이트의 전사게시판을 선택할 사이트와 전사 공개할 것인지 특정인에게만 공개할 것인지 설정할 수 있습니다.
      - **공개** - 상단에 선택한 A 사이트에 전사게시판에 내용을 다른 사이트와 모든 내용을 공유합니다. 기본적으로 읽기만 가능하며, 쓰기가능을 선택하면 쓰기 기능도 함께 공유됩니다.
      - **비공개** - 특정 사용자 또는 부서, 직위 등 전사게시판 내용을 공유할 사용자를 지정할 수 있습니다.
    - iii. 사이트의 전사 게시판은 매칭한 사이트를 기준으로 다수 사이트에 공유할 수 있으며, 여러 공개범위 기준을 통해 추가할 수 있습니다.
5. 전사 예약/자산공유 역시 전사 게시판 공유 방식과 동일하게 추가를 통해 설정할 수 있습니다.



겸직자는 소속된 사이트의 조직도를 확인할 수 있습니다. 단, 소속된 사이트에서 조직도의 접근 금지로 설정되어 있으면 조직도를 확인할 수 없습니다.



겸직자는 그룹웨어에 로그인 후, 좌측 상단의 로고를 클릭하여 자신이 소속한 사이트를 자유롭게 이동할 수 있습니다.



겸직자와 조직도 공유자는 서비스에 로그인 후, 좌측 하단 풀업 조직도를 통해 그룹 사이트의 조직도를 확인할 수 있으며, 모바일 및 PC메신저로 다른 사이트의 사용자와 채팅(대화)가 가능합니다.



전사 게시판 공유, 전사 예약/자산 공유를 추가한 경우 각 사이트 간 공유되었을 알 수 있도록 사이트 어드민 및 서비스페이지에 별도 표기되어 있습니다.

## 사이트 그룹 수정

사이트 그룹 목록에서 사이트 그룹 정보를 수정합니다.

1. 시스템 어드민의 **[도메인/사이트 관리 > 사이트 그룹 목록]**을 클릭합니다.
2. 사이트 그룹 목록에서 수정하려는 사이트 그룹의 이름을 클릭합니다.
3. 사이트 그룹 수정화면에서 각 항목의 정보를 수정합니다.
4. 정보 수정이 완료되면, **수정**을 클릭합니다.

## 사이트 그룹 삭제

등록한 사이트 그룹을 삭제합니다.

1. 시스템 어드민의 [도메인/사이트 관리 > 사이트 그룹 목록]을 클릭합니다.
2. 사이트 그룹 목록에서 삭제하려는 사이트 그룹을 선택한 후, 삭제를 클릭합니다.

## 사이트 그룹 검색

사이트 그룹명으로 검색합니다. 등록된 그룹 사이트가 많다면, 검색을 이용하여 사이트를 한번에 찾을 수 있습니다.

1. 시스템 어드민의 [도메인/사이트 관리 > 사이트 그룹 목록]을 클릭합니다.
2. 사이트 그룹 목록의 우측 상단에 있는 검색창에 검색어를 입력합니다. 검색어에는 사이트 그룹명을 입력해야 합니다.
3. 엔터키를 누르거나 검색을 클릭합니다.

## 5. 보안 설정

---

### 5.1 공통

#### 안티바이러스

수신 또는 송신되는 메일에 바이러스를 포함하고 있는지 검사하여 차단합니다. 검사할 메일의 최대 크기를 설정하여 해당 크기 이하의 메일만 검사하고, 크기 이상의 메일은 통과시킵니다. 바이러스 감염은 사용자들에게 엄청난 악영향을 미칠 수 있으므로, 반드시 바이러스 메일 검사를 권장합니다.



첨부 파일에 암호화 되어 비밀번호가 있는 경우에는 메일을 열수 없으므로, 바이러스 검사가 불가능합니다.

안티바이러스는 다음과 같이 구성되어 있습니다.

- 메일 바이러스 검사 - 송수신되는 메일에 바이러스를 포함하고 있는 지 검사합니다.
- 바이러스 알림 메일 - 바이러스 알림 메일은 바이러스 송수신에 대한 경고 메일이며 처리 방법에 상관없이 알림 메일 수신 대상에 알림 메일을 보냅니다. 바이러스 알림 메일은 지정한 대상(송신자, 수신자, 송수신자)에게 발송됩니다.
- 첨부파일 바이러스 검사 - 메일에 첨부한 파일이 바이러스를 포함하고 있는 지 검사합니다.
- 바이러스 필터 - 바이러스 필터의 업데이트 현황을 확인하고 업데이트 주기를 설정하거나 수동으로 업데이트 할 수 있습니다.

안티바이러스를 사용하기 위해 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [보안 설정 > 공통 > 안티바이러스]를 클릭합니다.
2. 바이러스 검사 항목을 설정합니다.
  - I. 사용 여부(권장: 사용) - 바이러스 검사를 사용할 지 여부를 선택합니다.
  - II. 바이러스 검사할 메일 최대 크기(권장: 5MB) - 바이러스를 검사할 메일의 최대 크기를 입력합니다.

입력한 크기와 같거나 작은 메일에 한해서만 바이러스 검사를 수행합니다.

III. 바이러스 검사 실패 시 처리 정책 - 바이러스 검사 실패 시 처리 정책을 선택합니다.

- i. 전송 - 바이러스 검사 실패한 메일을 전송
- ii. 태그 - 메일의 제목 앞에 특정 문구를 추가하여 전송

IV. 검사에 실패하는 경우는 아래와 같습니다.

- i. 바이러스엔진과 접속이 되지 않는 경우
- ii. 암호가 걸린 압축파일의 경우

3. 바이러스 알림 메일 본문에 들어갈 송신 메일 주소를 입력합니다.

- I. 사용 여부(권장: 사용) - 바이러스 알림 메일을 수신받을지의 사용여부를 선택합니다.
- II. 알림 메일 수신 대상 - 알림 메일을 전송할 수신 대상(수신자, 송신자, 수신자+송신자)을 선택합니다.
- III. 송신자 메일 주소 - 바이러스 알림 메일을 전송할 송신자의 메일주소를 입력합니다.

4. 첨부파일 바이러스 검사 항목을 설정합니다.

- I. 첨부파일 바이러스 검사 여부 - 첨부파일 바이러스 검사를 사용할 지 여부를 선택합니다. 첨부파일이란 메일에 첨부하는 파일뿐만 아니라, 게시판, 커뮤니티에 첨부하는 파일도 모두 포함됩니다.
- II. 바이러스 검사 방식(권장: 업로드 시 검사 사용, 다운로드 시 검사 사용안함) - 첨부파일을 메일, 게시판, 커뮤니티, 자료실에 업로드 또는 다운로드 할 때 바이러스 검사를 진행할지를 선택합니다.  
첨부파일을 다운로드 할 때 바이러스 검사를 하게 되면, 파일을 업로드 한 이후에 추가된 바이러스 패턴도 체크가 된다는 장점이 있지만, 파일을 다운로드 할 때마다 바이러스 검사를 하므로 시간이 더 소요되고 시스템에 부하가 생길 수 있습니다.
- III. 바이러스 검사할 때 최대 첨부 크기 - 바이러스를 검사할 첨부파일의 최대 크기를 입력합니다.

입력한 크기와 같거나 작은 메일에 한해서만 바이러스 검사를 수행합니다.

5. 바이러스 필터가 최근 업데이트 된 시각을 확인하고, 업데이트 주기를 설정합니다.

또는, **업데이트 시각**을 누르면 가장 최신의 바이러스 필터를 수동으로 업데이트 할 수 있습니다.

6. 설정이 완료되면, **저장**을 클릭합니다.



패키지에 바이러스 엔진이 포함되지 않을 수도 있습니다. 바이러스 엔진이 패키지에 포함되지 않는 경우, 규칙의 업데이트 여부를 확인한 시각 정보를 가져올 수 없으므로 바이러스 엔진 업데이트 시각이 표시되지 않습니다.



바이러스 메일에 대처하기 위해서는 업데이트 주기를 **1시간마다**로 권장합니다.



**최근 업데이트 시각**은 가장 최근 바이러스 필터를 업데이트한 날짜와 시각이므로 필터가 업데이트되지 않은 경우, **최근 업데이트 시각**은 변경되지 않습니다.

## 인증서

SSL(Secure Socket Layer) 프로토콜은 웹 상의 보안 통신을 위해 SSL 인증서로 암호화된 정보를 주고받는 프로토콜입니다. SSL 인증서를 통해 HTTPS로 시스템 어드민 및 사용자 페이지에 접속하여 정보를 보호합니다.

SSL 프로토콜의 암호화에 사용할 인증서의 종류는 다음과 같습니다.

- 기본 인증서
- 자가 인증서
- 신뢰받는 인증서

다음은 각각의 인증서를 설정하는 방법에 대해 설명합니다.



Daouoffice가 여러 대로 구성되어 있는 경우 각 장비별로 인증서 등록을 해야 합니다.

### 기본 인증서

(주)다우기술에서 제공하는 기본 인증서입니다. 기본 인증서의 유효기간은 10년입니다.

1. 시스템 어드민의 **[보안 설정 > 공통 > 인증서]**를 클릭합니다.
2. 장비를 선택합니다.
3. **인증서 종류를 기본 인증서로** 선택합니다.
4. **저장**을 클릭합니다.
5. 인증서를 적용하기 위한 웹서버 재시작 진행 여부의 메시지 창이 나타납니다. **확인**을 클릭합니다.

### 자가 인증서

공인인증 기관의 인증을 받지 않고, 자체적으로 발급한 인증서입니다. 자가 인증서의 유효기간은 관리자가 지정할 수 있습니다.

자가 인증서는 공인인증 기관의 인증을 받지 않으므로 비용이 절약됩니다. 그러나, 간혹 상대방 메일 서버가 공인된 인증서가 아닌 이유로 거부할 수도 있고, 아웃룩 등의 메일 클라이언트 프로그램에서는 경고창이 나타날 수도 있습니다.

자가 인증서를 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[보안 설정 > 공통 > 인증서]**를 클릭합니다.
2. 장비를 선택합니다.
3. **인증서 종류를 자가 인증서로** 선택합니다.
4. 자가 인증서를 만드는데 필요한 정보를 입력합니다.
  - I. Common name - 해당 서버의 도메인명을 입력합니다.



- II. Country - 국가를 선택합니다.
- III. 그 외 회사의 정보를 입력합니다.
5. **저장**을 클릭합니다.
6. 인증서를 적용하기 위한 웹서버 재시작 진행 여부의 메시지 창이 나타납니다. **확인**을 클릭합니다.

## 신뢰받은 인증서

인증서 공인 기관(Thawte, Verisign 등)에서 발급한 인증서입니다. 공인 인증 기관의 인증서를 받기 위해서는 private key와 CSR(Certificate signing request)이 필요합니다.

신뢰받은 인증서를 사용하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [**보안 설정 > 공통 > 인증서**]를 클릭합니다.
2. 장비를 선택합니다.
3. **인증서 종류를 신뢰받은 인증서**로 선택합니다.
4. 공인 인증 기관에서 발급 받은 인증서가 없다면, 신뢰받은 인증서를 만드는데 필요한 정보를 입력합니다.
  - I. Common name - 해당 서버의 도메인명을 입력합니다.
  - II. Country - 국가를 선택합니다.
  - III. 그 외 회사의 정보를 입력합니다.
  - IV. 암호화 키의 비트 길이 - 암호화 시 사용하는 키의 길이를 선택합니다. 암호화 키의 길이가 길수록 보안은 강해지지만 성능은 저하됩니다.
5. **Private Key 및 CSR 다운로드 받기**를 클릭합니다.
6. 공인 인증 기관에서 인증서를 발급받기 위해, 다운받은 CSR를 공인인증 기관에 제출합니다.
7. 공인 인증 기관에서 발급받은 인증서를 등록하기 위해 **인증서 등록**을 클릭합니다.
  - I. Private Key - **파일 선택**을 클릭하여, 5번에서 받은 private key를 등록합니다.
  - II. 신뢰받은 인증서 - **파일 선택**을 클릭하여, 공인 인증 기관에서 인증 받은 인증서를 등록합니다.
  - III. 루트 인증서 - 루트 인증서가 필요한 경우, 루트 인증서를 체크하여 인증서를 등록합니다.
  - IV. 체인 인증서 - 체인 인증서가 필요한 경우, 체인 인증서를 체크하여 인증서를 등록합니다. 체인 인증서는 루트 인증기관으로부터 인정을 받은 중계 인증 기관에서 발급하는 인증서입니다., 인증서가 신뢰받은 인증서로 인식되게 하기 위해서 필요합니다. **추가**를 클릭하여, 체인 인증서를 순차적으로 등록합니다. 추가한 체인인증서를 삭제하려면 해당 인증서의 **삭제**를 클릭합니다.
8. **저장**을 클릭합니다.
9. 인증서를 적용하기 위한 웹서버 재시작 진행 여부의 메시지 창이 나타납니다. **확인**을 클릭합니다.

## API접근 설정

Daouoffice에서 제공하는 API(Application Programming Interface)에 접근할 수 있는 IP를 설정합니다.

1. 시스템 어드민의 [**보안 설정 > 공통 > API접근 설정**]를 클릭합니다.
2. **API접근 설정** 여부를 선택합니다.
  - I. 사용안함 - Daouoffice의 API에 접근할 수 없습니다.

- II. 모두허용 - 모든 IP에서 API에 접근할 수 있습니다.
- III. 부분허용 - 일부 허용된 IP만 API에 접근할 수 있습니다.
- 3. 사용여부를 **부분허용**으로 선택한 경우, 허용 IP 주소를 등록합니다.
  - I. 추가 - IP 주소를 입력한 후, 추가아이콘(➤)을 클릭하여 IP 주소 목록에 추가합니다.
  - II. 삭제 - IP 주소 목록에서 삭제하려는 메일주소를 선택한 후, 삭제아이콘(◀)을 클릭합니다.
- 4. 설정이 완료되면, **저장**을 클릭합니다.

## 해외 로그인 차단 허용 설정

해외에서 서비스에 접속을 시도하면, 접속을 차단할 수 있습니다. 해외 로그인을 차단하더라도 허용하려는 IP를 등록하여 특정 IP에서의 접속은 허용할 수 있습니다.



해외 로그인 차단은 [도메인/사이트 관리 > 사이트 목록 > 사이트 상세 정보]의 해외 로그인 차단에서 설정할 수 있습니다.

해외 로그인을 차단할 때 특정 IP를 등록하여 접속을 허용하는 방법은 다음과 같습니다.

- 1. 시스템 어드민의 [보안 설정 > 공통 > 해외 로그인 차단 허용 설정]을 클릭합니다.
- 2. 해외 로그인 차단 허용 설정 사용여부를 선택합니다.
  - I. 사용 - 해외 로그인을 차단할 때도 특정 IP 주소에서의 접속은 허용합니다.
    - i. 해외 로그인 차단 허용 설정을 **사용**으로 선택한 경우, 허용 IP 주소를 등록합니다. 아이피 입력창에 IP 주소를 입력하고 추가아이콘(➤)을 클릭합니다.
  - II. 사용안함
- 3. 설정이 완료되면, **저장**을 클릭합니다.

## 5.2 이메일 보안

### 안티 스팸

수신된 메일은 3단계(접속 단계, SMTP 단계, 콘텐츠 단계)로 처리됩니다. 각 단계별 규칙에 의해 스팸 메일, 스팸성 메일, 바이러스 메일, 정상 메일, 관리자 정의 메일로 분류되고, 분류된 메일은 분류별 처리방법을 따릅니다. 이때 처리 방법들은 메일 주소와 도메인으로 설정되는 수신자 그룹에 따라 다르게 처리할 수 있습니다.

처리 단계별 필터에 의해 메일은 다음과 같이 분류됩니다.

표 5-1 처리단계별 메일 분류

항 목	설 명
스팸 메일	처리 단계 별 필터에 의해 스팸으로 분류되어진 메일
스팸성 메일	스팸성 메일 판단 규칙에 부합되거나, 인공지능 필터의 스팸성 메일 범위에 속한 메일
바이러스 메일	바이러스 필터에 의해서 바이러스로 분류된 메일
정상메일	허용 규칙에 의해 통과되거나, 스팸, 바이러스 메일이 아닌 메일
관리자 정의 메일	관리자가 정의한 규칙에 부합되는 메일

메일 처리 단계별에 따른 필터의 종류는 다음과 같습니다.

## 컨텐츠 필터

수신 메일 본문 내용(Contents)에 특정 문자열이나 단어를 포함하는 경우에 해당 메일을 필터링하기 위한 허용 및 차단 규칙을 설정할 수 있습니다. 일반 문자열뿐만 아니라 정규식을 이용하여 다양한 차단 조건을 만들 수 있습니다.

스팸검사를 할 수 있는 메일의 최대 크기는 512Kbytes입니다.

## 허용/차단 규칙 목록 구성

관리자가 설정한 규칙으로 메일 내용(Contents)에 특정단어나 문자열을 포함하면 차단하거나 허용할 수 있습니다. 허용/차단 규칙의 목록의 항목 구성은 다음과 같습니다.

- 필터명 - 허용/차단 규칙명입니다.
- 상세 내용 - 허용/차단 규칙의 상세한 규칙 내용입니다.
- 메일 분류 - 해당 필터에 처리된 메일 분류입니다.
- 사용 여부 - 설정한 필터가 사용중인지 여부를 보여줍니다.



필터에 의해 처리된 메일 분류 설명은 표 5-1 처리단계별 메일 분류를 참조하시기 바랍니다.

## 허용/차단 규칙 추가

메일 내용(Contents)에 특정단어나 문자열을 포함하면 차단하거나 허용합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 컨텐츠 필터]를 클릭합니다.
2. 차단 규칙 또는 허용 규칙을 선택합니다.
3. 규칙 목록 화면에서 추가를 클릭합니다.
4. 규칙 추가 화면이 나타납니다. 각 규칙 항목을 설정합니다.
  - I. 필터명 - 규칙 필터명을 입력합니다. 필터명은 영문, 숫자, '-', '\_'만 입력할 수 있으며, 최대 64byte까지 가능합니다. 필수입력 항목입니다.
  - II. 사용 여부 - 해당 차단 규칙을 사용할 것인지 여부를 선택합니다.
  - III. 연산 종류
    - i. 하나의 조건이라도 만족(OR) - 수신 된 메일이 조건 중 하나만 만족해도 메일분류에서 선택한 메일로

#### 처리

- ii. 모든 조건을 만족(AND) - 수신 된 메일이 조건 모두를 만족해야 **메일분류**에서 선택한 메일로 처리
- IV. 조건 - 허용/차단 규칙으로 필터링할 항목과 항목에 대한 조건을 입력하고, 비교 방법을 선택합니다.스팸  
검사의 메일 최대 크기는 512Kbytes입니다.

필터링 항목은 다음과 같습니다.

- i. 제목 - 메일 Header의 Subject를 비교합니다.
- ii. 본문내의 URL - 메일 본문이나 HTML에 포함되어있는 URL 링크(http:// 시작하는 주소)를 비교합니  
다.
- iii. 송신자(ENV) - SMTP 프로토콜 단계에서의 Mail From을 비교합니다.
- iv. 수신자(ENV) - SMTP 프로토콜 단계에서의 Rcpt To를 비교합니다.
- v. 송신자(Header) - 메일 Header의 송신자(From)를 비교합니다.
- vi. 수신자(Header) - 메일 Header의 수신자(To)를 비교합니다.
- vii. 동보 수신자(Cc-Header) - 메일 Header의 참조수신자(Cc)를 비교합니다.
- viii. 헤더 전체 - 메일 Header 모두를 비교합니다.
- ix. 헤더값 - 특정 Header의 필드를 지정하여 입력한 값을 비교합니다.  
(예) Message-id: xxxx Header Message-Id에 'xxxx'를 포함하고 있으면 필터링
- x. Content-Type - 메일 Header의 Content-type을 비교합니다.
- xi. 본문 - 메일의 본문에 특정 내용을 포함되어 있는지 비교합니다.
- xii. 메일 크기 - 첨부파일을 포함한 메일의 전체크기를 비교합니다.
- xiii. IP - 메일의 발송 IP를 비교합니다. IP 입력방법은 다음의 예와 같습니다.

(예)

하나의 IP로 입력: 192.168.0.1

IP 범위로 입력: 192.168.0.1-192.168.0.35

서브넷 마스크로 입력: 192.168.0.1/24

- xiv. 첨부 파일명 - 메일에 첨부된 파일명을 비교합니다.
- xv. 첨부 파일 본문 - 첨부 파일의 본문의 내용을 비교합니다. 지원하는 파일 형식은 다음과 같습니다.  
zip, txt, rtf, htm, html, xml, pdf, mht, hwd, doc, ppt, xls, hwp, chm, dwg, sxw, sxc, sxi, mdi,  
msg, eml, xlsx, pptx, docx, jtd

조건방법은 다음과 같습니다.

- xvi. 포함하면/포함하지 않으면 - 조건 항목의 문자열을 메일 항목이 포함하는/포함하지 않는 경우 필터링  
합니다.
- xvii. 일치하면/일치하지 않으면 - 조건 항목의 문자열을 메일 항목과 비교하여 정확히 일치하는/일치하지  
않는 경우 필터링합니다. 단, IP가 비교 대상인 경우에는 일치하는 경우로만 비교합니다.
- xviii. 시작하면/시작하지 않으면 - 조건 항목의 문자열로 메일 항목이 시작하면/시작하지 않으면 필터링하  
입니다.
- xix. 끝나면/끝나지 않으면 - 조건 항목의 문자열로 메일 항목이 끝나면/끝나지 않으면 필터링합니다.
- xx. 맞으면/맞지 않으면(정규식) - 조건 항목의 문자열을 정규식으로 변환하여 메일 항목과 비교했을 때  
맞으면/맞지 않으면 필터링합니다. (정규식 문자는 별도 입력이 필요가 없습니다.)  
이 비교는 대소 구분을 하지 않습니다.
- xxi. 맞으면/맞지 않으면(정규식, 대소구분) - 조건 항목의 문자열을 정규식으로 변환하여 메일 항목과 비  
교했을 때 맞으면/맞지 않으면 필터링합니다.  
이 비교는 대소 구분을 합니다.

xxii. 존재하지 않으면 - 조건 항목이 메일 항목으로 존재하지 않으면 필터링합니다.

xxiii. 보다 크면/보다 작으면 - 조건 항목에서 설정한 메일 크기보다 크면/작으면 필터링합니다.

5. 규칙 설정이 완료되면, **추가**를 클릭하여 규칙을 저장합니다.



첨부 파일 본문필터를 사용하게 되면 필터링 성능이 저하될 수 있으며 시스템 메모리 사용량이 늘어날 수 있습니다. 따라서 이 필터를 사용할 경우 충분히 모니터링 해야 하고, 메모리 사용량이 늘거나 부하가 높은 경우는 사용을 중지해주시기 바랍니다.



필터링 항목 중 본문내의 URL, 수신자(ENV, Header), 송신자(ENV, Header) 필터링은 필터 처리 시, 대소문자를 구분하지 않습니다.

## 허용/차단 규칙 수정

허용/차단 규칙 목록에 있는 규칙을 수정합니다. 수정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터]를 클릭합니다.
2. 차단 규칙 또는 허용 규칙을 선택합니다.
3. 규칙 목록에서 수정하려는 규칙의 필터명을 클릭합니다.
4. 규칙 수정 화면이 나타납니다. 각 규칙 항목을 수정합니다.
5. 수정이 완료되면, 수정을 클릭합니다.

## 허용/차단 규칙 삭제

허용/차단 규칙 목록에 있는 규칙을 삭제합니다. 삭제하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터]를 클릭합니다.
2. 차단 규칙 또는 허용 규칙을 선택합니다.
3. 규칙 목록에서 삭제할 규칙을 선택한 후, 목록 상단에 있는 삭제를 클릭합니다.

## 허용/차단 규칙의 사용 및 사용안함 설정

규칙을 필터링에서 사용하기 위해 작동시킵니다. 또는, 사용으로 설정된 규칙을 필터링에서 중지하기 위해 규칙을 중지합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터]를 클릭합니다.
2. 차단 규칙 또는 허용 규칙을 선택합니다.
3. 규칙 목록에서 사용으로 설정할 규칙을 선택한 후, **사용**을 클릭합니다.  
사용으로 설정된 규칙을 중지하려면, **사용안함**을 클릭합니다.
4. 규칙 사용여부 설정의 변경완료 메시지 창이 나타납니다. **확인**을 클릭합니다.
5. 규칙 목록의 **사용 여부** 항목이 사용(🟢) 또는 사용안함(🔴)으로 변경된 것을 확인합니다.

## 필터 검색

해당 규칙이 속해 있는 단계별필터를 검색하여, 어떤 패턴이 어떤 규칙이 속해 있는지 검색할 수 있습니다.



필터 검색에 대한 자세한 설명은 [필터 검색](#)을 참조하십시오.

허용/차단 규칙 목록에서 필터 검색하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터]**를 클릭합니다.
2. **차단 규칙** 또는 **허용 규칙**을 선택합니다.
3. 규칙 목록에서 **검색**을 클릭합니다.
4. 검색 화면에서 검색 범위 및 검색 조건을 선택합니다.
5. **검색**을 클릭하면, 검색 결과 목록이 나타납니다

## 콘텐츠 룰 업데이트

(주)다우기술에서 다음과 같이 실시간으로 차단하는 패턴 필터를 제공합니다.

- **테라스 패턴 필터** - (주)다우기술이 실시간으로 제공하는 패턴 필터로, 메일 내용(Contents)에 특정 단어나 문자열을 포함하면 스팸 메일로 처리하는 패턴 필터입니다.
- **스팸 핑거 프린트** - (주)다우기술에서 제공한 스팸 핑거 프린트 알고리즘에 의해 이미지 스팸 및 URL을 포함한 스팸을 차단합니다. 이미지 스팸이나 스팸 URL정보를 Hash 정보화하여 저장하고, 메일의 Hash 정보와 비교하여 스팸처리를 합니다.
- **테라스 인공지능 필터** - (주)다우기술에서 제공하는 베이시안(baysian)알고리즘에 기반하여 스팸을 차단합니다. 메일의 내용을 자동으로 분석하여 단어나 문구별로 스팸 지수를 부여합니다. 스팸 지수 범위에 따라 정상 메일, 스팸성 메일, 스팸 메일로 구분되어 처리합니다.

인공 지능 필터가 메일을 분류하는 기준값(스팸 지수)을 설정할 수 있습니다. 화살표 아이콘(➡)을 마우스로 조절하여 기준 값을 설정합니다. 권장 값은 50입니다.

권장 값보다 스팸 지수를 작게 설정하면 스팸을 차단할 확률은 높아지지만, 정상 메일이 차단될 수 있습니다. 따라서, 정상 메일이 차단되면 스팸 지수를 높게 조절해야 합니다. 예를 들어, 스팸성 메일의 설정 범위가 30~80인 경우, 메일의 스팸 지수가 다음과 같은 경우 각각 지수에 따라 메일이 구분됩니다.

- 스팸지수 30 이하 - 정상 메일
- 스팸지수 30~80 - 스팸성 메일
- 스팸지수 80이상 - 스팸 메일

## 패턴 필터 사용 설정

(주)다우기술에서 제공하는 패턴 필터의 사용여부 및 스팸 지수 기준을 설정합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터 > 콘텐츠 룰 업데이트]**를 클릭합니다.
2. 각 패턴 필터의 사용 여부를 선택합니다.

3. 스팸 지수 기준 값을 화살표 아이콘(📈)을 마우스로 조절하여 설정합니다.
4. 패턴 필터 설정을 저장하려면, **저장**을 클릭합니다.

## 패턴 필터 업데이트 주기 설정

각 필터 규칙의 업데이트 시각 및 업데이트 주기를 설정할 수 있습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터 > 콘텐츠 룰 업데이트]**를 클릭합니다.
2. 업데이트 주기 설정에서 각 패턴마다 **업데이트 주기**를 선택합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



스팸 메일, 스파이웨어 등에 대처하기 위해서는 업데이트 주기를 **1시간마다**로 권장합니다.



**최근 업데이트 시각**은 가장 최근 각 패턴을 업데이트한 날짜와 시각이므로 패턴이 업데이트되지 않은 경우 **최근 업데이트 시각**은 변경되지 않습니다.

## 패턴 필터 수동 업데이트

각 패턴별로 수동으로 업데이트를 할 수 있습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터 > 콘텐츠 룰 업데이트]**를 클릭합니다.
2. 수동으로 업데이트하기 위해 각 패턴의 **업데이트 시각**을 클릭합니다.



바이러스 필터의 업데이트 시각을 확인하거나, 수동으로 업데이트 하려면 [안티바이러스](#)부분을 참조하시기 바랍니다.

## 접속 단계 차단

외부 메일 서버가 TCP 통신을 통해 시스템에 접속하려는 발송 IP를 접속 단계에서 제한하여, 스팸 메일을 방지할 수 있습니다.

접속단계의 필터 종류는 다음과 같습니다.

- 발송 IP 차단 - 등록된 IP의 SMTP 접속 차단
- 시간당 접속 횟수 제한 - 단위 시간동안 한 IP로부터의 SMTP 접속 횟수 제한
- 동시 접속 횟수 제한 - 한 IP로부터의 동시 접속 회수를 제한
- RBL - RBL(Realtime Spam Black List) 서버가 제공하는 IP를 차단

다음은 각 필터를 설정하는 방법에 대해 살펴봅니다.

## 발송 IP 차단

Daouoffice에 접속하려는 특정 발송 IP를 차단하기 위해 IP를 등록합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 차단 > 발송 IP차단]을 클릭합니다.
2. 발송 IP차단 **사용 여부**를 선택합니다.
3. 차단 IP로 입력할 IP의 입력 형식을 선택합니다.
4. IP를 입력한 후, 추가아이콘(➤)를 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘(✖)를 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
5. 거부 메시지의 코드 및 메시지를 작성합니다. 다음은 권장 사항입니다.
  - I. 코드 - 550
  - II. 메시지 - Your IP is blocked.
6. 설정이 완료되면, **저장**을 클릭합니다.



IP 그룹은 시스템 어드민의 [기타 설정 > IP 그룹 설정]에서 설정한 그룹입니다.

## 시간당 접속 횟수 제한

단위 시간 동안 기준치 이상의 메일을 보내는 IP를 차단하는 규칙에 대해 설정합니다.

예를 들어,

- 단위 시간: 30초, 접속건수: 10, 수신 메일수: 100, 수신자 인증 실패 횟수: 10, 차단 시간: 1시간으로 설정된 경우 30초 동안 특정 IP의 접속건수가 10번을 초과하거나, 특정 IP에서 발송된 메일의 수신자 수가 100명을 초과하거나, 수신자의 인증이 10회 초과 실패할 경우 → 해당 IP의 접속을 1시간 동안 차단하고 메일이 서버에 접속할 경우 거부 메시지를 발송자에게 보냅니다.

시간당 접속 횟수 차단은 기본 설정과 세부 설정으로 구분되어 있습니다.

- 기본 설정 - 시간당 접속 횟수 차단의 기본 설정입니다.
- 세부 설정 - 특정 IP에 대해서 시간당 접속 횟수 제한 수를 다르게 적용하고 싶을 때 설정하는 기능입니다. 기본 설정과 다르게 적용할 시간당 접속 횟수를 입력하고, 설정을 적용할 대상(IP)을 입력합니다.

시간당 접속 횟수 차단을 설정하는 방법은 다음과 같습니다.

## 기본 설정

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 차단 > 시간당 접속 횟수 제한]을 클릭합니다.
2. 시간당 접속 횟수 차단 **사용 여부**를 선택합니다.



3. 단위 시간을 설정합니다. 권장 값은 1분입니다.
4. 차단 규칙을 설정합니다.
  - I. 접속건수 (권장 값: 30건)
  - II. 수신 메일 수 (권장 값: 30건)
  - III. 수신자 인증 실패 횟수 (권장 값: 10회)
5. 차단 시간을 설정합니다.
6. 거부 메시지의 코드 및 메시지를 작성합니다. 다음은 권장 사항입니다.
  - I. 코드 - 421
  - II. 메시지 - Your IP is filtered by IP Rate Control.
7. 설정이 완료되면, **저장**을 클릭합니다.

## 세부 설정

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 차단 > 시간당 접속 횟수 제한]**을 클릭합니다.
2. **세부 설정** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. 시간당 접속 횟수 차단 **사용 여부**를 선택합니다.
5. 단위 시간을 설정합니다. 권장 값은 1분입니다.
6. 차단 규칙을 설정합니다.
  - I. 접속건수 (권장 값: 30건)
  - II. 수신 메일 수 (권장 값: 30건)
  - III. 수신자 인증 실패 횟수 (권장 값: 10회)
7. 차단 시간을 설정합니다.
8. 특정 IP를 등록합니다. IP의 입력 형식을 선택합니다.
9. IP를 입력한 후, 추가아이콘(➤)을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘(⏏)을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
10. 설정이 완료되면, **추가**를 클릭합니다.



IP 그룹은 시스템 어드민의 **[기타 설정 > IP 그룹 설정]**에서 설정한 그룹입니다.

## 동시 접속 횟수 제한

동시 접속으로 인한 메일 서버의 부하를 방지하기 위해 한 IP로부터의 동시 접속 횟수를 제한합니다. 신뢰된 IP에서 대량으로 메일을 발송하는 경우에는 해당 IP를 접속 단계 허용 IP에 등록합니다.

동시 접속 횟수 차단은 기본 설정과 세부 설정으로 구분되어 있습니다.

- 기본 설정 - 동시 접속 횟수 차단 기본 설정입니다.
- 세부 설정 - 특정 IP에 대해서 동시 접속 횟수 제한 수를 다르게 적용하고 싶을 때 설정하는 기능입니다. 기본 설정과 다르게 적용할 동시 접속 횟수를 입력하고, 설정을 적용할 대상(IP)을 입력합니다.

## 기본 설정

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 차단 > 동시 접속 횟수 제한]을 클릭합니다.
2. 동시 접속 횟수 차단의 **사용 여부**를 선택합니다.
3. IP당 동시에 접속할 수 있는 **최대 제한 접속수**를 입력합니다. 권장값은 10입니다.
4. 거부 메시지의 코드 및 메시지를 작성합니다. 다음은 권장 사항입니다.
  - I. 코드 - 421
  - II. 메시지 - You made too many connections.
5. 설정이 완료되면, **저장**을 클릭합니다.

## 세부 설정

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 차단 > 동시 접속 횟수 제한]을 클릭합니다.
2. **세부 설정** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. 동시 접속 횟수 차단의 세부 설정 **사용 여부**를 선택합니다.
5. IP당 동시에 접속할 수 있는 **최대 제한 접속수**를 입력합니다. 권장값은 10입니다.
6. IP를 입력한 후, 추가아이콘(➤)을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘(⏏)을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
7. 설정이 완료되면, **추가**를 클릭합니다.



IP 그룹은 시스템 어드민의 [기타 설정 > IP 그룹 설정]에서 설정한 그룹입니다.

## RBL

RBL(Real-time Spam Black Lists) 서버는 스팸 발송 IP를 블랙 리스트로 관리합니다. 블랙 리스트에 있는 IP의 접속을 막아 스팸 메일을 원천 차단할 수 있습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 차단 > RBL]을 클릭합니다.
2. RBL의 **사용 여부**를 선택합니다.
3. 처리방법을 선택합니다.
  - I. 전송 - 해당 메일을 사용자에게 전송합니다.
  - II. 수신 거부 - 해당 메일을 전송하지 않고 수신거부합니다.
  - III. 삭제 - 해당 메일을 전송하지 않고 바로 삭제합니다.

- IV. 태그 - 해당 메일 제목 앞에 태그를 추가하거나 메일 헤더에 X-header를 추가하여 메일을 전송합니다. **태그 설정**에서 X-header 및 태그를 설정합니다.
4. RBL DNS 설정을 선택합니다.
  - I. **기본 RBL** - 환경설정에서 설정한 DNS 서버를 이용하여 쿼리하게 됩니다. 최대 5개까지 등록 가능하지만, 성능을 위해서 1개 이상을 등록하지 않는 것이 좋습니다.
  - II. **사용자 지정 RBL** - 사용자가 설치한 RBL DNS 서버를 지정할 수 있습니다.
5. 거부 메시지를 등록합니다. 처리방법을 수신거부로 하는 경우 사용되는 메시지입니다. 영구 차단하기 위해서는 코드를 500번대 에러로 입력하기를 권합니다.
6. 설정이 완료되면, **저장**을 클릭합니다.

## 접속 단계 허용

메일을 발송하는 특정 IP가 접속 단계에서 차단되는 것을 방지할 수 있습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 접속 단계 허용]**을 클릭합니다.
2. 접속 단계 허용의 **사용 여부**를 선택합니다.
3. 허용으로 등록할 IP의 입력 형식을 선택합니다.
4. IP를 입력한 후, 추가아이콘(➤)을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘(⏏)을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
5. 설정이 완료되면, **저장**을 클릭합니다.



IP 그룹은 시스템 어드민의 **[기타 설정 > IP 그룹 설정]**에서 설정한 그룹입니다.

## SMTP 단계 차단

SMTP 프로토콜의 형식을 제한하여 스팸 메일을 방지할 수 있습니다. SMTP 단계의 차단 필터 종류는 다음과 같습니다.

- DNS 검사 - EHLO 명령어 뒤에 도메인, 송신자의 도메인, 수신자의 도메인 유효성을 검사 한 후, 이에 위배 시에 차단
- SPF - 송신자 도메인을 SPF로 불법 도메인 검사 후, 차단
- 송신자 차단 - 송신자 차단 목록에 있는 송신자가 보낸 메일을 차단
- 송신자 시간당 제한 - 단위 시간동안 기준치 이상의 메일을 보내는 송신자를 설정한 시간동안 차단
- 수신자 차단 - 수신자 차단 목록에 있는 수신자가 보낸 메일을 차단
- 수신자 시간당 제한 - 단위 시간동안 기준치 이상의 메일을 받는 수신자를 설정 시간동안 차단
- 동보 메일 응답 지연 - 설정된 수 이상의 메일을 동보 발송하는 경우, 수신 속도를 조절하여 수신 메일의 수를 제한

다음은 각 필터를 설정하는 방법에 대해 살펴봅니다.

## DNS 검사

SMTP 프로토콜 상에서 도메인의 DNS 검사 여부를 설정합니다. 단, DNS 검사는 상당한 검사 시간을 요하므로 가급적 사용을 권하지 않습니다.

DNS 검사하여 차단하는 방법에 대한 설명은 다음과 같습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > DNS 검사]를 클릭합니다.
2. 각 검사 대상을 설정합니다.
  - I. EHLO DNS 검사
    - i. 사용 여부 - EHLO DNS 검사 사용여부를 선택합니다.
    - ii. 검사 방식 - 검사 방식을 선택합니다.
    - iii. Soft Fail시의 처리 - Soft Fail은 DNS 서버가 응답이 없는 경우 등 서버가 실패되는 경우입니다. 이러한 경우에도 수신 거부를 할 것인지를 선택합니다.
  - II. 송신자 DNS 검사
    - i. 사용 여부 - 송신자 DNS 검사 사용여부를 선택합니다.
    - ii. Soft Fail시의 처리 - Soft Fail은 DNS 서버가 응답이 없는 경우 등 서버가 실패되는 경우입니다. 이러한 경우에도 수신 거부를 할 것인지를 선택합니다.
  - III. 수신자 DNS 검사
    - i. 사용 여부 - 수신자 DNS 검사 사용여부를 선택합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



발송 IP와 EHLO 도메인 IP의 일치 여부는 C Class 주소까지만 검사합니다. 즉, 발송 IP와 EHLO도메인 IP의 C Class 주소가 같으면 허용합니다. C Class란 IP 주소의 4byte중 앞에 3byte(네트워크ID)가 같은 네트워크를 의미합니다.(예) 192.168.10.x



Outlook 이나 Outlook Express등과 같은 PC용 메일 클라이언트에서 발송되는 메일 경우에는 EHLO의 도메인이 정상적이지 않습니다. 따라서, EHLO DNS 검사 기능을 사용할 경우에는 PC용 메일 클라이언트에서 발송되는 메일이 차단될 수 있습니다. Terrace Mail Watcher를 외부 송신 메일 서버로 사용할 경우에는 EHLO DNS 검사 기능 사용을 권하지 않습니다.

## SPF

SMTP 프로토콜 중 송신자의 도메인을 SPF(Sender Policy Framework) 검사하여 불법 도메인에서 발송된 메일을 차단합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > SPF]를 클릭합니다.
2. SPF 검사의 **사용 여부**를 선택합니다.
3. **검사 방식**을 선택합니다.
4. **처리 정책**을 선택합니다.

- I. 기본정책 따름 - KISA 권장값입니다. 기본정책 사용시 처리 방법은 아래와 같습니다.
    - i. Invalid, Neutral, Softfail, None, Temperror, Permerror - 태그
    - ii. Pass - 사용 안함
    - iii. Fail - 거부
  - II. 개별 정책 지정(고급 기능) - SPF 결과 값에 따라 개별 정책을 지정할 수 있습니다.
5. 설정이 완료되면, **저장**을 클릭합니다.

#### 개별 정책 지정 구분 및 처리 방법

- SPF 결과
  - Pass - 조회가 성공하여 SPF 레코드를 찾았으며, 레코드에서 발송 시스템이 도메인 사용이 인증되었음을 확인하였습니다.
  - Fail - 조회결과 SPF 레코드를 찾았지만 SMTP 트랙잭션 중에 SMTP 클라이언트의 도메인 사용권한이 레코드에서 명시적으로 거부되었습니다.
  - Softfail - 조회 결과 일치하는 SPF 레코드를 찾았으며, 레코드에서 SMTP 클라이언트의 도메인 사용인증이 거부되었지만 거부가 덜 명확해서 바로 실패로 확인되지는 않았습니다.
  - Invalid - SPF 레코드에 잘못된 형식의 값이 등록되어 쿼리시 잘못된 값이 들어옵니다.
  - Neutral - SPF 레코드에서 SMTP 클라이언트의 도메인 사용인증을 요구하지 않습니다. 메시지는 받으며, 사양에 따라 none 과 같이 처리합니다.
  - None - 일치하는 SPF 레코드를 찾지 못했기 때문에 SPF 처리가 수행되지 않았습니다.
  - Temperror - SPF 레코드에서 SMTP 레코드를 찾지 못했기 때문에 SPF 처리가 수행되지 않았습니다.
  - Permerror - SPF 처리 중에 SPF 레코드의 구문 오류입니다. 중첩된 SPF 레코드 처리중의 DNS 실패 또는 중첩된 SPF 레코드 처리 중에 SPF 처리 제한 초과 등의 영구적인 오류가 발생합니다.
- 처리 방법
  - 태그 - 메일 헤더 또는 메일 제목에 이미 설정된 태그 문구가 삽입되어 사용자에게 전송됩니다
  - 거부 - 메일을 사용자의 메일함으로 전송하지 않습니다.
  - 통과 - 메일을 사용자의 메일함으로 전송합니다.
  - 사용안함 - 해당 카테고리를 사용하지 않습니다.



태그는 미리 정의되어 있어 관리자가 태그를 따로 지정할 수 없습니다.

## 송신자 차단

특정 사용자가 발송한 메일을 SMTP 프로토콜 단계에서 차단하도록 설정합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 송신자 차단]**를 클릭합니다.
2. 송신자 차단 **사용 여부**를 선택합니다.
3. 차단할 송신자의 메일 주소 또는 도메인을 입력한 후, 추가아이콘(➤)을 클릭하여 목록에 추가합니다.  
(예) 메일주소: test@xxx.com 도메인: @xxx.com, @yyy.co.kr
4. 설정이 완료되면, **저장**을 클릭합니다.

## 송신자 시간당 제한

특정 송신자가 일정시간 동안 기준치 이상의 메일을 발송한 경우에 해당 송신자를 일정시간 동안 차단합니다.

예를 들어,

- 단위 시간이 30초, 단위 시간 동안 송신 메일 수: 10, 차단 시간: 1시간으로 설정된 경우→ 특정 송신자가 30초 동안 10통 이상 메일을 발송하는 경우 해당 송신자로부터 오는 메일을 1시간 동안 차단합니다.

송신자 시간당 제한은 기본 설정과 세부 설정으로 구분되어 있습니다.

- 기본 설정 - 송신자 시간당 제한의 기본 설정입니다.
- 세부 설정 - 특정 IP에 대해서 단위 시간 동안 송신자 메일 수 제한과 차단 시간을 다르게 적용하고 싶을 때 설정하는 기능입니다. 세부 설정을 적용할 대상(IP)을 입력합니다.

송신자 시간당 제한을 설정하는 방법은 다음과 같습니다.

### 기본 설정

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 송신자 시간당 제한]을 클릭합니다.
2. 송신자 시간당 제한의 **사용 여부**를 선택합니다.
3. **단위 시간**을 설정합니다. 권장값은 1분입니다.
4. **송신 메일수**를 입력합니다. 권장값은 30입니다.
5. **차단 시간**을 설정합니다.
6. 거부 메시지의 코드 및 메시지를 작성합니다. 다음은 권장 사항입니다.
  - I. 코드 - 421
  - II. 메시지 - Your sent too many messages.
7. 설정이 완료되면, **저장**을 클릭합니다.


### 세부 설정

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 송신자 시간당 제한]을 클릭합니다.
2. **세부 설정** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. 송신자 시간당 제한의 **사용 여부**를 선택합니다.
5. **단위 시간**을 설정합니다. 권장값은 1분입니다.
6. **송신 메일수**를 입력합니다. 권장값은 30입니다.
7. **차단 시간**을 설정합니다.
8. IP를 입력한 후, 추가아이콘(➤)을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘(✖)을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.

9. 설정이 완료되면, **추가**를 클릭합니다.

## 수신자 차단

특정 수신자에게 수신되는 메일을 SMTP 프로토콜 단계에서 차단하도록 설정합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 수신자 차단]**을 클릭합니다.
2. 수신자 차단 **사용 여부**를 선택합니다.
3. 차단할 수신자의 메일 주소 또는 도메인을 입력한 후, 추가아이콘()을 클릭하여 목록에 추가합니다.  
(예) 메일주소: test@xxx.com 도메인: @xxx.com, @yyy.co.kr
4. 설정이 완료되면, **저장**을 클릭합니다.

## 수신자 시간당 제한

특정 수신자가 일정시간 동안 기준치 이상의 메일을 수신한 경우에 해당 수신자를 일정시간 동안 차단합니다.

예를 들어,

- 단위 시간이 30초, 단위 시간 동안 수신 메일 수: 10, 차단 시간: 1시간으로 설정된 경우→ 특정 수신자가 30초 동안, 수신하는 메일이 10개를 초과할 경우 해당 수신자에게 오는 메일을 1시간 동안 차단합니다.

수신자 시간당 제한은 기본 설정과 세부 설정으로 구분되어 있습니다.

- 기본 설정 - 수신자 시간당 제한의 기본 설정입니다.
- 세부 설정 - 특정 IP에 대해서 단위 시간 동안 수신자 메일 수 제한과 차단 시간을 다르게 적용하고 싶을 때 설정하는 기능입니다. 세부 설정을 적용할 대상(IP)을 입력합니다.

## 기본 설정

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 수신자 시간당 제한]**을 클릭합니다.
2. 기본 설정 탭에서 수신자 시간당 제한의 **사용 여부**를 선택합니다.
3. **단위 시간**을 설정합니다. 권장값은 1분입니다.
4. **수신 메일수**를 입력합니다. 권장값은 30입니다.
5. **차단 시간**을 설정합니다.
6. 거부 메시지의 코드 및 메시지를 작성합니다. 다음은 권장 사항입니다.
  - I. 코드 - 421
  - II. 메시지 - You sent too many messages to specific receiver
7. 설정이 완료되면, **저장**을 클릭합니다.

## 세부 설정

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 수신자 시간당 제한]**을 클릭합니다.
2. **세부 설정** 탭을 클릭합니다.
3. **추가**를 클릭합니다.

4. 수신자 시간당 제한의 **사용 여부**를 선택합니다.
5. **단위 시간**을 설정합니다. 권장값은 1분입니다.
6. **수신 메일수**를 입력합니다. 권장값은 30입니다.
7. **차단 시간**을 설정합니다.
8. IP를 입력한 후, 추가아이콘(➤)을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘(⏏)을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
9. 설정이 완료되면, **추가**를 클릭합니다.

## 동보 응답 지연

설정된 수 이상의 메일을 동보 발송하는 경우 응답 지연을 통해 수신 속도를 조절합니다.

동보 메일 응답 지연은 기본 설정과 세부 설정으로 구분되어 있습니다.

- 기본 설정 - 동보 메일 응답 지연의 기본 설정입니다.
- 세부 설정 - 특정 IP에 대해서 동보 메일의 응답 지연을 다르게 적용하고 싶을 때 설정하는 기능입니다. 적용할 대상(IP)을 입력합니다.



## 기본 설정

1. 시스템 어드민의 [**보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 동보 응답 지연**]을 클릭합니다.
2. 동보 메일 응답 지연의 **사용 여부**를 선택합니다.
3. **수신자 형태**를 선택합니다.
  - I. 모든 수신자
  - II. 유사 ID 수신자: ID 패턴이 비슷한 수신자 (예) aa, a1, a2,...
4. **제한 수신자 수**를 입력합니다. 권장값은 10명입니다.
  - I. 제한 수신자 수 - 동보메일을 보낼 수 있는 최대 수신자 수입니다.
5. **지연 시간**을 설정합니다. 권장값은 2초입니다.
  - I. 지연 시간 - SMTP 프로토콜 응답을 지연시키는 시간입니다.
6. 설정이 완료되면, **저장**을 클릭합니다.

## 세부 설정




1. 시스템 어드민의 [**보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 차단 > 동보 응답 지연**]을 클릭합니다.
2. **세부 설정** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. **사용 여부**를 선택합니다.
5. **수신자 형태**를 선택합니다.
  - I. 모든 수신자



- II. 유사 ID 수신자 : ID 패턴이 비슷한 수신자 (예) aa, a1, a2, ...
6. **제한 수신자 수**를 입력합니다. 권장값은 10명입니다.
  - I. 제한 수신자 수 - 동보메일을 보낼 수 있는 최대 수신자 수입니다.
7. **지연 시간**을 설정합니다. 권장값은 2초입니다.
  - I. 지연 시간 - SMTP 프로토콜 응답을 지연시키는 시간입니다.
8. IP를 입력한 후, 추가아이콘()을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘()을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 파일 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 파일 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
9. 설정이 완료되면, **추가**를 클릭합니다.

## SMTP 단계 허용

메일을 발송하는 특정 IP 또는 특정 메일 주소, 도메인이 SMTP 단계에서 차단되는 것을 방지할 수 있습니다. 메일을 발송하는 특정 IP 또는 특정 메일 주소, 도메인이 실시간 패턴필터 단계에서 차단되는 것을 방지할 수 있습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > SMTP 단계 허용]**을 클릭합니다.
2. 접속 단계 허용의 **사용 여부**를 선택합니다.
3. 허용할 메일 주소 또는 도메인을 입력합니다. 메일 주소/도메인을 입력한 후, 추가아이콘()을 클릭하여 목록에 추가합니다.
4. 허용 IP를 입력한 후, 추가아이콘()을 클릭하여 목록에 추가합니다.
  - I. IP 삭제 - IP 목록에서 삭제하려는 IP를 선택한 후, 삭제아이콘()을 클릭합니다.
  - II. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - III. IP 목록 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - IV. IP 목록 내보내기 - IP 목록에서 **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
5. 설정이 완료되면, **저장**을 클릭합니다.

## 필터 멤버 정책

메일 수신 시 특정 사용자 또는 도메인 그룹에 대해 특정 멤버로 규정하여 기본 정책과 다른 처리 방법을 적용할 수 있습니다. 적용 대상(멤버)에 따라 네 가지 메일 카테고리에 대한 처리 방법을 다르게 설정할 수 있습니다.

- 스팸 메일
- 스팸성 메일
- 바이러스 메일
- 관리자 정의 메일

Daouoffice가 최초 설치되면 기본적으로 3개의 정책이 설정되어 있습니다.

- DEFAULT - 특정 멤버 정책에 포함되지 않는 수신자들에게 제공하는 기본 멤버 정책입니다. Default 정책은 처

리 방법만 수정 가능합니다.

- OUTBOUND - 내부 도메인을 제외한 모든 외부 도메인으로 송수신되는 메일에 대한 처리 방법입니다. 관리 편의성을 위해 제공되는 정책이므로, 관리자가 수정, 삭제할 수도 있습니다.
- SYSTEM - 시스템의 부하를 줄이기 위해 대용량 메일을 처리하는 고객센터에서 유용하게 사용할 수 있는 정책입니다. 접속 단계 또는 SMTP 단계에서 스팸이나 바이러스를 대량 발송하는 것을 수신 거부(reject)를 통해 원천 봉쇄할 수 있습니다. system 정책을 사용할 때는 모든 송수신 메일에 대해서, 최우선 순위로 적용 받게 됩니다. 이 경우에는 사용자가 수신을 허용한 발송자도 차단될 수 있으므로, 반드시 확인 후에 사용하시기 바랍니다.

## 필터 멤버 정책 추가

필터 멤버 정책을 추가합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]을 클릭합니다.
2. 멤버 정책 화면에서 **추가**를 클릭합니다.
3. 정책 추가 화면에서 각 항목을 설정합니다.
  - I. 정책명 - 정책 명을 입력합니다. 최대 64bytes까지 입력 가능합니다.
  - II. 사용 여부 - 정책의 **사용 여부**를 선택합니다.
  - III. 메일 주소/도메인 - 해당 정책을 적용할 메일 주소 및 도메인을 추가합니다.
  - IV. 처리 방법 - 각 메일 카테고리 별로 메일 처리방법을 설정합니다.
    - i. 전송 - 메일을 수신자에게 전송합니다.
    - ii. 차단 등급 - 차단 등급을 선택합니다.
    - iii. 태그 - 적용할 태그 입력 방식을 선택합니다.
    - iv. 치료 후 전송 - 바이러스를 치료한 후 전송합니다.
    - v. 삭제 - 메일이 수신되는 즉시 삭제합니다. **system** 정책에서만 선택할 수 있습니다.
    - vi. 수신 거부 - 메일을 사용자의 메일함으로 전송하지 않고, 송신자에게 다시 보냅니다. **system** 정책에 서만 선택할 수 있습니다.
    - vii. 멤버 정책 따름 - 접속 단계 또는 SMTP 단계에서 특정 차단 규칙에 의해 메일이 분류될 때, 해당 메일의 수신자가 속한 멤버의 정책에 따라 처리합니다. **system** 정책에서만 선택할 수 있습니다.
4. 멤버 정책의 항목 설정이 완료되면, **추가**를 클릭합니다.

## 필터 멤버 정책 수정

멤버 정책을 수정합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]을 클릭합니다.
2. 멤버 정책 목록에서 수정할 필터 멤버 정책명을 클릭합니다.
3. 멤버 정책 정보를 수정합니다.
4. 멤버 정책의 항목 수정이 완료되면, **수정**을 클릭합니다.

## 필터 멤버 정책 삭제

멤버 정책을 삭제합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]을 클릭합니다.
2. 멤버 정책 목록에서 삭제할 멤버정책을 선택한 후, **삭제**를 클릭합니다.

## 필터 멤버 정책 사용/사용안함 설정

멤버 정책의 사용 여부를 설정합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]을 클릭합니다.
2. 멤버 정책 목록에서 사용으로 설정할 멤버 정책을 선택한 후, **사용**을 클릭합니다.  
또는, 멤버 정책 목록에서 사용안함으로 설정할 필터를 선택한 후, **사용안함**을 클릭합니다.
3. 멤버 정책 사용여부 설정의 변경 완료 메시지 창이 나타납니다. **확인**을 클릭합니다.
4. 멤버 정책 목록의 사용 여부 항목에서 사용(○) 또는 사용안함(⊗)으로 변경된 것을 확인합니다.

## 필터 멤버 정책 순서 적용

여러 정책에 속한 멤버(메일 주소, 도메인)들의 메일처리 방법은 우선 순위가 가장 높게 설정된 정책을 적용 받습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]을 클릭합니다.
2. 멤버 정책 목록에서 순위를 변경할 멤버 정책을 선택합니다.
3. **위로** 또는 **아래로**를 클릭하여 순서를 변경합니다.

## 필터 멤버 정책 검색

멤버 정책에 포함된 메일주소 또는 도메인들 대상을 검색할 수 있습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]을 클릭합니다.
2. 멤버 정책 목록 상단 입력창에 검색어를 입력한 후, **검색**을 클릭합니다.

## 필터 환경 설정

필터 환경을 설정합니다. 필터 환경 설정은 다음과 같이 구성되어 있습니다.

- 필터 정보 관리 서버 - 필터링 된 IP 정보를 수집하고 공유할 것인지 설정합니다.
- 로컬 도메인, 호스트 허용 정책 - 로컬 도메인이나 로컬 호스트의 IP에서 발송한 메일은 스팸 필터룰에 차단하지 않을 것인지 설정합니다.
- 로컬 베이시안 - 사용자 신고에 기반하여 관리자가 교육한 룰을 이용하여 메일을 차단할 것인지 설정합니다.

## 필터 정보 관리 서버

Daouoffice를 여러 장비에 설치하여 운영하는 경우 특정 서버를 지정하여 필터링 된 IP 정보를 수집하고 공유할 수 있습니다. 필터 정보 관리 서버를 설정하면 각 서버에서 필터링 된 IP 정보를 지정한 서버에서 수집하고 관리하지만 모든 Daouoffice 서버에 동일하게 적용하여 필터링 합니다. 필터 정보 관리 서버를 설정하지 않는 경우 각 서버 내부의 필터링 정보만을 참조합니다.



Daouoffice를 단독으로 설치한 경우에는 필터 관리 서버 설정이 필요하지 않습니다.

필터 정보 관리 서버를 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 필터 환경 설정]**을 클릭합니다.
2. **관리 방식**을 설정합니다.
  - I. 개별 관리 - 서버 별로 필터링 된 IP 정보를 수집하고 필터링 합니다. 필터링 된 IP 정보는 다른 Daouoffice 서버와 공유하지 않습니다.
  - II. 외부 관리 -서버 지정 - 특정 서버를 지정하여 필터링 된 IP 정보를 공유하고 필터링 합니다.
3. **타임 아웃**을 설정합니다.
  - I. 설정된 시간동안 필터 정보 관리 서버와 통신이 이루어지지 않으면 필터링 정보를 무시하고 메일을 수신합니다.
  - II. 초 단위로 타임아웃을 설정합니다. (권장: 5초)
4. 설정이 완료되면, **저장**을 클릭합니다.



필터 정보 관리서버의 **관리 방식**을 **외부 관리 서버**로 지정할 때, 각 장비의 필터 규칙과 시간이 같아야 합니다. 이 조건이 만족되지 않으면 필터 정보 관리 서버가 오작동을 할 수 있습니다.

## 로컬 도메인, 호스트 허용 정책

로컬 도메인이 사용중인 IP 또는 로컬 호스트의 IP에서 발송한 메일은 스팸 필터룰에 의해 차단하지 않고 무조건 수신하도록 설정할 수 있습니다. 로컬 도메인이 사용중인 IP는 다음과 같습니다.

- **[시스템 관리 > 장비관리]**에 등록된 IP
- **[기타 설정 > IP 그룹 설정]**에 등록된 IP

로컬 도메인 호스트 허용 정책을 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 필터 환경 설정]**을 클릭합니다.
2. **로컬 도메인, 호스트 허용 정책**의 사용 여부를 선택합니다.
3. **저장**을 클릭합니다.

## 로컬 베이시안

로컬 베이시안이란 사용자가 스팸으로 신고한 메일을 관리자가 교육하여 해당 룰을 시스템에 직접 적용하는 것을 의미합니다. 사용자 신고에 기반하여 관리자가 교육한 룰을 이용하여 스팸처리를 합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 필터 환경 설정]**을 클릭합니다.
2. **로컬 베이시안**의 사용 여부를 선택합니다.
3. **저장**을 클릭합니다.

## 필터 검색

필터 검색에서는 어떤 패턴이 어떤 규칙에 속해 있는지를 검색할 수 있습니다. 즉, 해당 패턴이 속해 있는 단계별 필터를 검색하여 필터를 관리합니다.

- 검색 범위 - 필터 검색 범위는 메일이 처리되는 각 단계별로 선택하여 검색할 수 있습니다. 검색하려는 검색 범위

를 선택합니다.

- 필터 종류 - 검색할 필터종류가 차단 규칙 또는 허용 규칙인지를 선택합니다.
- 검색어 - 검색하려는 검색어를 입력합니다. 검색어에 입력할 수 있는 형태는 차단/허용 규칙 추가에서 입력할 수 있는 패턴들과 동일한 형태인 IP, 메일 주소 또는 도메인, 일반 문자열(URL, 헤더 내용)을 입력할 수 있습니다.
  - 필터명 포함 - 콘텐츠 단계 또는 메일정보필터 단계에서 설정한 필터 명을 검색할 경우 체크합니다.
  - IP범위 포함 - 검색어에 입력한 IP가 특정 범위에 포함되어 있는지를 검색합니다. 이 경우 검색어에 IP형식으로 입력해야 합니다.

필터를 검색하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 필터 검색]**을 클릭합니다.
2. **검색 범위와 필터 종류**를 선택하고, 검색어를 입력합니다.
3. **검색**을 클릭합니다.



검색한 결과 목록의 **검색어**에서 상세 내용을 클릭하면, 해당 검색어가 포함된 규칙 등으로 이동하여 상세한 필터 내용을 확인할 수 있습니다.

## 메일 정보 필터

### 유출 감시 모니터링

유출 감시 모니터링은 기업 내부 정보가 메일을 통해 유출되는 것을 감시하는 기능입니다. 송수신되는 메일 중 주요 정보를 포함하는 메일에 대한 규칙을 설정하여 필터링할 수 있습니다. 필터링 된 메일을 모니터링 함으로써 내부 정보의 유출을 방지할 수 있습니다. 단, 메일 모니터링은 개인 사생활 보호를 위해 반드시 사용자의 동의가 있어야 합니다.

**[보안 설정 > 이메일 보안 > 메일 정보 필터 > 정보 보호 필터]**에서 처리 방법이 **특정 폴더에 보관**인 경우, 관리자가 지정한 폴더에 규칙에 부합되는 메일이 해당 폴더에 보관됩니다. **유출 감시 모니터링**에서는 이처럼 특정 폴더에 보관된 메일을 모니터링하여 내부 정보 유출을 감시할 수 있습니다. 단, 유출 감시 모니터링은 폴더 보관 기간 동안만큼의 모니터링이 가능합니다.



유출 감시 모니터링 폴더 기간 설정은 **유출 감시 모니터링** 목록에서 **설정**을 클릭하면, **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 메일 정보 보호 폴더 관리]**로 이동됩니다.

### 유출 감시 모니터링 검색

유출 감시 모니터링에서는 기본 검색과 고급 검색으로 필터링된 메일을 검색할 수 있습니다. 검색 결과는 최근 1000개까지 나타납니다.

기본 검색은 지정된 검색조건을 토대로 최근 1000개 내에서 메일을 검색합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 유출 감시 모니터링]**을 클릭합니다.
2. 유출 감시 모니터링 목록의 좌측 상단에서 검색 범위를 선택합니다.
3. 검색 조건을 선택하고, 검색어를 입력합니다.
4. **검색**을 클릭합니다.

검색할 날짜와 검색 항목을 이용하여 전체 메일을 검색합니다. 단, 날짜 지정은 검색하려는 저장 폴더의 보관기관 기준 이내로 가능합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 유출 감시 모니터링]**을 클릭합니다.
2. 유출 감시 모니터링 목록의 우측 상단에서 **고급 검색**을 체크합니다.
3. 고급 검색 조건 설정화면이 나타나면, 각 항목을 선택 또는 입력합니다.
4. **검색**을 클릭합니다.

## 유출 감시 모니터링 삭제

폴더에 보관되어 있는 메일 정보를 삭제할 수 있습니다. 삭제된 메일은 다시 복구할 수 없습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 유출 감시 모니터링]**을 클릭합니다.
2. **보관 폴더명**에서 삭제하려는 메일이 있는 폴더를 선택합니다.
3. 목록에서 삭제하려는 메일을 선택한 후, **삭제**를 클릭합니다.

## 유출 감시 모니터링 전송

폴더에 보관되어 있는 메일의 재전송을 시도할 수 있습니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 유출 감시 모니터링]**을 클릭합니다.
2. **보관 폴더명**에서 전송하려는 메일이 있는 폴더를 선택합니다.
3. 목록에서 전송하려는 메일을 선택한 후, **전송**을 클릭합니다.

## 정보 보호 필터

수신 메일 본문 내용(Contents)에 주요 문자열이나 단어를 포함하는 경우에 해당 메일을 필터링하기 위한 규칙을 설정할 수 있습니다. 일반 문자열뿐만 아니라 정규식을 이용하여, 다양한 조건을 설정할 수 있습니다.

다음은 정보 보호 필터 구성 및 관리하는 방법에 대해 살펴봅니다.

## 정보 보호 필터 추가

정보 보호 필터를 추가합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 정보 보호 필터]**를 클릭합니다.
2. 정보 보호 필터 화면에서 **추가**를 클릭합니다.
3. 정보 보호 필터 추가 화면에서 각 항목을 입력합니다.
  - I. 필터명 - 다른 필터와 구분할 수 있는 필터 이름을 입력합니다.

- II. 사용여부 - 필터의 사용여부를 선택합니다.
- III. 연산종류 - 연산 종류를 선택합니다.
- IV. 처리방법 - 조건에 해당하는 메일의 처리 방법을 선택합니다.
  - i. 특정 폴더에 보관/전송 - [보안 설정 > 이메일 보안 > 메일 정보 필터 > 메일 정보 보호 폴더 관리]에서 설정한 특정 폴더로 필터링된 메일을 저장하고, 메일의 원래 수신자에게 전송합니다. 메일은 보관 기간 동안만 존재합니다.
  - ii. 특정 메일 주소로 전달/전송 - 지정한 특정 메일 주소로 메일을 전달하고, 메일의 원래 수신자에게 전송합니다.
  - iii. 특정 폴더에 보관 - [보안 설정 > 이메일 보안 > 메일 정보 필터 > 메일 정보 보호 폴더 관리]에서 설정한 특정 폴더로 필터링된 메일을 수신자에게 전달은 하지 않고 저장만 합니다. 메일은 보관 기간동안만 존재합니다.
  - iv. 특정 메일 주소로 전달 - 수신자에게 메일을 전송하지 않고, 지정한 특정 메일 주소로만 메일을 전달합니다.
- V. 조건 - 필터링 대상, 조건 입력, 조건 방법을 선택하여 정보 보호 필터링 조건을 설정합니다.
  - i. 제목 - 메일 Header의 Subject를 비교합니다.
  - ii. 본문 내의 URL - 메일 본문이나 HTML에 포함되어 있는 URL 링크(http:// 로 시작하는 주소)를 비교합니다.
  - iii. 송신자(ENV) - SMTP 프로토콜 단계에서의 Mail From을 비교합니다.
  - iv. 수신자(ENV) - SMTP 프로토콜 단계에서의 Rcpt To를 비교합니다.
  - v. 송신자(Header) - 메일 Header의 송신자(From)를 비교합니다.
  - vi. 수신자(Header) - 메일 Header의 수신자(To)를 비교합니다.
  - vii. 동보 수신자(Cc-Header) - 메일 Header의 참조 수신자(Cc)를 비교합니다.
  - viii. 헤더 전체 - 메일 Header의 모두를 비교합니다.
  - ix. 헤더값 - 특정 Header의 필드를 지정하여 입력한 값을 비교합니다.  
(예) Message-id : xxxx Header의 Message-Id에 'xxxx'를 포함하고 있으면 필터링
  - x. Content-Type - 메일 Header의 Content-type을 비교합니다.
  - xi. 본문 - 메일의 본문에 특정 내용을 포함되어 있는지 비교합니다.
  - xii. 메일 크기 - 첨부 파일을 포함한 메일의 전체 크기를 비교합니다.
  - xiii. IP - 메일의 발송 IP를 비교합니다. IP의 입력 방법은 다음의 예와 같습니다.
  - xiv. 첨부 파일명 - 메일에 첨부된 파일명을 비교합니다.
  - xv. 첨부 파일 본문 - 첨부 파일의 본문의 내용을 비교합니다. 지원하는 파일 형식은 다음과 같습니다.  
(zip, txt, rtf, htm, html, xml, pdf, mht, hwd, doc, ppt, xls, hwp, chm, dwg, sxw, sxc, sxi, m di, msg, eml, xlsx, pptx, docx, jtd)
  - xvi. 개인정보 - 본문에 주민등록번호, 계좌번호 등과 같이 개인을 식별할 수 있는 정보가 포함되어 있는지 확인합니다.  
필터링 대상을 개인정보로 선택할 때는 메일 본문에 포함되어 있는 개인정보의 수를 1부터 1000까지 지정할 수 있습니다. 단, 개인정보를 여러 개 추가할 때는 개인정보의 수를 지정할 수 없습니다.  
조건을 필터링할 방법을 선택합니다.
  - xvii. 포함하면/포함하지 않으면 - 조건 항목의 문자열을 메일 항목이 포함하는/포함하지 않는 경우 필터링합니다.
  - xviii. 일치하면/일치하지 않으면 - 조건 항목의 문자열을 메일 항목과 비교하여 정확히 일치하는/일치하지 않는 경우 필터링합니다. 단, IP가 비교 대상인 경우에는 일치하는 경우로만 비교합니다.
  - xix. 시작하면/시작하지 않으면 - 조건 항목의 문자열로 메일 항목이 시작하면/시작하지 않으면 필터링함

니다.

- xx. 끝나면/끝나지 않으면 - 조건 항목의 문자열로 메일 항목이 끝나면/끝나지 않으면 필터링합니다.
- xxi. 맞으면/맞지 않으면(정규식) - 조건 항목의 문자열을 정규식으로 변환하여 메일 항목과 비교했을 때 맞으면/맞지 않으면 필터링합니다. 정규식 문자는 별도 입력이 필요가 없습니다. 이 비교는 대소 구분을 하지 않습니다.
- xxii. 맞으면/맞지 않으면(정규식, 대소구분) - 조건 항목의 문자열을 정규식으로 변환하여 메일 항목과 비교했을 때 맞으면/맞지 않으면 필터링합니다. 이 비교는 대소 구분을 합니다.
- xxiii. 존재하지 않으면 - 조건 항목이 메일 항목으로 존재하지 않으면 필터링합니다.
- xxiv. 보다 크면/보다 작으면 - 조건 항목에서 설정한 메일 크기보다 크면/작으면 필터링합니다.

4. 필터 추가 설정이 완료되면, **추가**를 클릭합니다.



**첨부 파일 본문 필터**를 사용하게 되면 필터링 성능이 저하될 수 있으며 시스템 메모리 사용량이 늘어날 수 있습니다. 따라서 이 필터를 사용할 경우 충분히 모니터링해야 하고, 메모리 사용량이 늘거나 부하가 높은 경우는 사용을 중지해주시기 바랍니다.

## 정보 보호 필터 수정

정보 보호 필터 목록에 있는 필터를 수정합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 정보 보호 필터]**를 클릭합니다.
2. 정보 보호 필터 화면에서 수정하려는 필터명을 클릭합니다.
3. 정보 보호 필터 수정 화면에서 필터 정보를 수정합니다.
4. 필터 수정이 완료되면, **수정**을 클릭합니다.

## 정보 보호 필터 삭제

정보 보호 필터 목록에 있는 필터를 삭제합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 정보 보호 필터]**를 클릭합니다.
2. 정보 보호 필터 화면에서 삭제하려는 필터를 선택한 후, **삭제**를 클릭합니다.

## 정보 보호 필터 사용/사용안함

정보 보호 필터의 사용 여부를 설정합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > 메일 정보 필터 > 정보 보호 필터]**를 클릭합니다.
2. 필터 목록에서 사용으로 설정할 필터를 선택한 후, **사용** 또는 **사용안함**을 클릭합니다.
3. 필터 사용여부 설정의 변경완료 메시지 창이 나타납니다. **확인**을 클릭합니다.
4. 필터 목록의 사용 여부 항목에서 사용(●) 또는 사용안함(⊘)으로 변경된 것을 확인합니다.



## 정보 보호 필터 검색

필터를 검색합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 메일 정보 필터 > 정보 보호 필터]를 클릭합니다.
2. 필터 목록에서 검색을 클릭합니다.
3. [보안 설정 > 이메일 보안 > 안티 스팸 > 필터 검색]으로 이동합니다.

## 감시 대상 설정

정보 보호 필터를 적용시킬 대상을 설정합니다. 감시 대상을 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 메일 정보 필터 > 감시 대상 설정]을 클릭합니다.
2. 고급 설정 화면에서 다음 사항을 설정합니다.
  - I. 저장 대상 설정 - 필터링 된 저장 메일대상을 선택합니다.
    - i. 전체 저장 - 필터 조건에 상관없이 모든 메일이 저장 및 전송됩니다.
    - ii. 특정 필터에 적용된 메일만 저장(권장) - 메일 정보 필터에 등록된 규칙에 해당하는 메일만 저장됩니다.
  - II. 저장 상세 옵션 - 저장 상세 옵션을 선택합니다. (옵션 모두 선택 권장)
    - i. 스팸메일을 저장하지 않음 - 스팸으로 판단되는 메일을 정보감시 대상에서 제외하여 저장하지 않습니다.
    - ii. 바이러스를 저장하지 않음 - 바이러스로 판단되는 메일을 정보감시 대상에서 제외하여 저장하지 않습니다.
  - III. 송수신 구분- 송신메일 또는 수신메일을 적용할 것인지 선택합니다.
  - IV. 압축 설정 - 설정압축 설정을 선택합니다.
    - i. 메일 정보 보호에 저장되는 메일을 확인하기 위해 압축된 메일을 하나씩 해제하면, 서버의 부하가 올라갑니다. 따라서, 서버 부하를 막기 위해 압축하지 않음을 권장합니다.
  - V. 개인정보 옵션 - 메일에 개인정보가 포함되었는지를 확인하기 위해 검출 조건을 설정합니다.
    - i. 연속된 숫자에서 검출 - 연속된 숫자 사이에 개인정보가 있으면, 해당 정보를 검출합니다.
    - ii. 제외문자 설정 - 메일에 개인정보가 포함되었는지 확인할 때 제외문자를 설정할 수 있습니다. 제외문자를 뺀 나머지 문자에서 개인정보가 포함되었는 지 확인합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.

## 차단 알림메일 설정

사용자가 보내는 메일이 정보 보호 필터에 의해 차단되었다는 사실을 알려주기 위해, 메일의 송신자에게 알림메일을 전송하는 기능입니다.



정보 보호 필터의 처리방법이 특정 폴더에 보관/전송이거나 특정 메일 주소로 전달/전송이면 메일이 정보 보호 필터에 해당하더라도 메일을 수신자에게 전송하기 때문에, 이때에는 차단 알림메일이 발송되지 않습니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 메일 정보 필터 > 차단 알림메일 설정]을 클릭합니다.
2. 사용여부를 선택합니다.
  - I. 사용 - 정보 보호 필터가 메일을 차단하면 송신자에게 알림 메일을 보냅니다.
  - II. 사용안함
3. 알림 메일의 제목과 송신자 메일 주소를 입력합니다.
4. 차단 알림메일의 변수를 확인합니다. 이 변수는 알림메일에 기본적으로 포함되는 항목으로 관리자가 수정할 수 없습니다.
  - I. \$subject - 정보 보호 필터에 의해 차단된 메일의 제목
5. 알림메일의 내용을 확인하고, 필요 시 내용을 수정합니다.
6. 차단된 메일의 원문을 알림메일에 포함할지를 선택합니다.
7. 설정이 완료되면, **저장**을 클릭합니다.

## 메일 정보 보호 폴더 관리

유출 감시 모니터링에 사용되는 저장 폴더를 추가 및 삭제하고, 보관기간을 설정합니다. 메일 정보 보호 폴더는 최대 5개까지 설정할 수 있으며, 디스크의 상태를 고려하여 보관 기간을 설정해야 합니다.

### 메일 정보 보호 폴더 추가

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 메일 정보 필터 > 메일 정보 보호 폴더 관리]를 클릭합니다.
2. **추가**를 클릭합니다.
3. 새 폴더 입력 필드란에 폴더 정보를 입력합니다.
  - I. 폴더명 - 폴더명을 입력합니다. 영문, 숫자입력만 가능합니다.
  - II. 보관기간 - 보관기간을 입력합니다. 최대 메일 보관 기간은 365일로 제한합니다.
4. 폴더 추가가 완료되면, **저장**을 클릭합니다.

### 메일 정보 보호 폴더 삭제

메일 정보 보호 폴더를 삭제합니다. 폴더를 삭제할 경우, 해당 폴더로 메일을 보관으로 지정한 필터를 우선적으로 삭제해야 합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 메일 정보 필터 > 메일 정보 보호 폴더 관리]를 클릭합니다.
2. 폴더 목록에서 삭제하려는 폴더의 **삭제**를 클릭합니다.
  - I. 사용 중인 폴더를 삭제하려면, 먼저 해당 폴더로 저장하도록 설정된 필터를 삭제해야 합니다.
3. 폴더 삭제가 완료되면, **저장**을 클릭합니다.

## 메일 데이터 보안

메일 보안과 관련하여 메일 압축 및 암호화, 무결성을 설정합니다.

1. 시스템 어드민의 [보안 설정 > 이메일 보안 > 메일 데이터 보안]을 클릭합니다.

2. 각각의 보안 메일의 사용여부를 설정합니다.
  - I. 메일 압축 설정 - 디스크 리소스 효율성을 높이기 위해 수신된 메일을 압축하여 보관합니다.
  - II. 메일 암호화 설정 - 수신된 메일을 암호화하여 저장합니다. 불법적인 침입에 의한 메일 도취를 예방할 수 있습니다.
  - III. 무결성 검토 설정 - 수신한 메일의 위조 및 변조 여부를 확인하여, 메일의 무결성을 확고히 합니다. 무결성 검토를 사용하면, 웹메일에서 메일 읽기 화면에 **변조 여부 확인**버튼이 표시됩니다. **변조 여부 확인**버튼을 클릭하여 메일의 변조 여부를 확인할 수 있습니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



메일 압축 설정 혹은 메일 암호화 설정을 사용하면, 하드웨어의 사양에 따라 메일의 로딩 속도가 저하되거나, 시스템 부하가 올라갑니다. 충분한 모니터링 과정을 확인한 후에 기능 사용을 권장합니다.

## SSL/TLS 접속설정

### SMTP

SMTP 프로토콜에 이용되는 TLS, SSL, Submission에 대해 설정합니다.

1. 시스템 어드민의 **[보안 설정 > 이메일 보안 > TLS 접속 차단 > SMTP]**를 클릭합니다.
2. 수신메일과 송신메일 각각 TLS를 설정합니다.
  - I. 사용 안함 - 암호화를 하지 않고 통신
  - II. TLS 지원 - 상대방이 암호화 지원할 경우만 암호화 통신. 그 외는 보통 통신
3. SSL 사용 여부와 포트번호를 설정합니다.
  - I. SSL 포트 설정 - SMTP 프로토콜에서 암호화된 정보로 주고 받을 지 설정합니다.
  - II. SSL 포트 번호 - SSL 포트를 사용하는 경우, 포트 번호를 입력합니다. 기본 포트 번호는 465입니다.
4. Submission 포트 사용여부와 포트번호를 설정합니다.
  - I. Submission port 설정 - Submission port는 송신전용으로 사용하는 포트입니다. Submission port 기능을 사용할 지 여부를 선택합니다.
  - II. Submission port 번호 - 기본적으로 Submission port에서 사용하는 port 번호는 587로 지정되어 나타납니다.
5. 설정이 완료되면, **저장**을 클릭합니다.



수신메일을 사용안함, 송신메일을 TLS 지원으로 설정하는 경우 MS Outlook에서 **[도구 > 계정설정 > 전자 메일 계정 > 사용자계정 > 인터넷 전자메일 설정 > 기타설정 > 고급]**에서 보내는 메일서버(SMTP)의 암호화된 다음 연결 방식 사용을 자동으로 설정하시기 바랍니다. 암호화된 다음 연결 방식 사용을 자동으로 설정해야 수신메일, 송신메일에 따라 MS Outlook이 자동으로 TLS를 지원할 수 있습니다.

## POP

POPS는 POP 프로토콜 정보를 암호화하여 통신하는 기능입니다. POP과 POPS 접근 IP를 설정하여 외부에 서비스하고자 하는 프로토콜을 지정할 수 있습니다.

1. 시스템 어드민인의 **[보안 설정 > 이메일 보안 > TSL 접속 차단 > POP]**을 클릭합니다.
2. POPS 서버 포트 및 POP 접근 IP를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. POPS 서버 포트 - POPS 프로토콜에서 사용하는 포트를 지정합니다. 기본값은 995입니다.
  - II. POP접근 IP 설정 - 외부에서 POP 프로토콜로 접근 가능한 IP를 설정합니다.
  - III. POPS접근 IP 설정 - 외부에서 POPS 프로토콜로 접근 가능한 IP를 설정합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



외부에 POP만 서비스 하고자 할 경우, POP 접근 IP는 0.0.0.0 - 255.255.255.255로 POPS 접근 IP는 공백으로 설정합니다. 외부에 POP과 POPS 모두 서비스 하고자 할 경우, POP 및 POPS 접근 IP 모두 0.0.0.0 - 255.255.255.255로 설정합니다. 외부에 POPS만 서비스 하고자 할 경우, POP 접근 IP는 공백으로 POPS 접근 IP는 0.0.0.0 - 255.255.255.255로 설정합니다.



POP 서버에 대한 설정은 **[시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스 설정 > POP서버설정]**에서 할 수 있습니다.

## IMAP

IMAPS는 IMAP 프로토콜 정보를 암호화하여 통신하는 기능입니다. IMAP과 IMAPS 접근 IP를 설정하여 외부에 서비스하고자 하는 프로토콜을 지정할 수 있습니다.

1. 시스템 어드민인의 **[환경 설정 > 메일서버 > IMAP 서버설정]**을 클릭합니다.
2. IMAPS 서버 포트 및 IMAP/IMAPS접근 IP를 설정합니다. 각 항목 설명은 다음과 같습니다.
  - I. IMAPS서버 포트 - IMAPS 프로토콜에서 사용하는 포트를 지정합니다. 기본값은 993입니다.
  - II. IMAP접근 IP 설정 - 외부에서 IMAP 프로토콜로 접근 가능한 IP를 설정합니다.
  - III. IMAPS접근 IP 설정 - 외부에서 POPS 프로토콜로 접근 가능한 IP를 설정합니다.
3. 설정이 완료되면, **저장**을 클릭합니다.



외부에 IMAP만 서비스 하고자 할 경우, IMAP 접근 IP는 0.0.0.0 - 255.255.255.255로 IMAPS 접근 IP는 공백으로 설정합니다. 외부에 IMAP과 IMAPS 모두 서비스 하고자 할 경우, IMAP 및 IMAPS 접근 IP 모두 0.0.0.0 - 255.255.255.255로 설정합니다. 외부에 IMAPS만 서비스 하고자 할 경우, IMAP 접근 IP는 공백으로 IMAPS 접근 IP는 0.0.0.0 - 255.255.255.255로 설정합니다.



IMAP 서버에 대한 설정은 [시스템 관리 > 서비스 설정 > 이메일서버 > 프로세스 설정 > IMAP서버설정]에서 할 수 있습니다.

## 5.3 WAS 보안

### 접속차단

Daouoffice 서비스에 접근할 수 있는 IP를 설정합니다.

1. 시스템 어드민의 [보안 설정 > WAS 보안 > 접속 차단]을 클릭합니다.
2. 접근 설정의 사용여부를 선택합니다.
  - I. 모두허용 - 서비스에 접속하는 IP를 모두 허용합니다. 즉, IP와 관계없이 서비스에 접속할 수 있습니다.
  - II. 부분허용 - 허용한 IP에서의 접근만 허용합니다. 허용하지 않은 IP에서 서비스에 접속하면 페이지가 정상적으로 표시되지 않습니다.
3. 사용여부를 **부분허용**으로 선택한 경우 허용 IP 주소를 등록하고, 링크 허용 여부를 설정합니다.
  - I. 추가 - IP 주소를 입력한 후, **추가아이콘**(➤)을 클릭하여 IP 주소 목록에 추가합니다. 허용된 IP 외에서 Daouoffice 서비스에 접근하면 페이지가 정상적으로 표시되지 않습니다.
  - II. 삭제 - IP 주소 목록에서 삭제하려는 IP 주소를 선택한 후, **삭제아이콘**(◀)을 클릭합니다.
  - III. 대용량 첨부 파일 링크 허용 - 접근 설정 사용여부가 **부분허용**이고 메일 수신자가 허용된 IP에서 접근하지 않거나 Daouoffice 사용자가 아니라면, 대용량 첨부 파일을 확인할 수 없습니다. IP와 관계없이 대용량 첨부파일 링크를 허용하려면 **대용량 첨부 파일 링크 허용**에 체크합니다.
  - IV. 수신 확인 링크 허용 - 접근 설정 사용여부가 **부분허용**이고 메일 수신자가 허용된 IP에서 접근하지 않거나 Daouoffice 사용자가 아니라면, 수신을 확인할 수 없습니다. IP와 관계없이 수신 확인 링크를 허용하려면 **수신 확인 링크 허용**에 체크합니다.
  - V. 보안 메일 링크 허용 - 접근 설정 사용여부가 **부분허용**이고 메일 수신자가 허용된 IP에서 접근하지 않거나 Daouoffice 사용자가 아니라면, 보안 메일을 확인할 수 없습니다. IP와 관계없이 보안 메일 링크를 허용하려면 **보안 메일 링크 허용**에 체크합니다.
4. 설정이 완료되면, **저장**을 클릭합니다.

### 세션검증

사용자가 로그인하면 사용자의 접근 IP 와 세션 ID를 로그아웃할 때까지 임시저장합니다. 사용자가 로그아웃하지 않은 상태일 때 다른 IP에서 같은 세션 ID로 접근하려고 하면 해당 IP를 차단합니다. 사용자가 로그아웃하면 접근 IP와 세션 ID 정보는 삭제됩니다.

1. 시스템 어드민의 [보안 설정 > WAS 보안 > 세션 검증 보안]을 클릭합니다.
2. 세션 ID/IP 일치 여부 검사의 사용여부를 선택합니다.
  - l. 사용, 사용안함(기본값)
3. 저장을 클릭합니다.

## HTTPS 설정

서비스에 로그인할 때는 http를 통해 접속하더라도 사용자의 정보를 보호하기 위해 자동으로 https로 바꿔 접속합니다. 로그인이 완료되면 다시 http로 바꿔 접속하는데, 로그인 후에도 https 프로토콜을 사용할지를 설정합니다.

1. 시스템 어드민의 [보안 설정 > WAS 보안 > HTTPS 설정]을 클릭합니다.
2. 로그인 후 https 접속을 유지할지를 선택합니다.
  - l. 사용, 사용안함(기본값)
3. 저장을 클릭합니다.

## 6. 통계

---

### 6.1 개요

통계 정보를 통해 송수신 메일의 추이를 볼 수 있으며, 과도한 트래픽을 유발시키는 주요 원인을 확인하여 서비스 관리를 도와줍니다.

#### 통계 종류

통계 결과 정보는 통계 종류에 따라 추이 분석과 순위 분석으로 확인할 수 있습니다.

- 추이 분석 - 선택한 기간 동안의 메일 추이 분석
- 순위 분석 - 선택한 기간 동안의 순위 항목 트래픽 분석

제공하는 통계 종류는 다음과 같습니다.

- 요약 - 정상, 스팸, 피싱, 바이러스 메일 처리에 대한 요약 통계를 메일별로 보여줍니다.
- 정상 메일 - 허용 규칙에 의해 통과되거나, 스팸/바이러스 메일이 아닌 메일의 통계를 보여줍니다.
- 스팸 메일 - 관리자(또는 사용자)의 차단 규칙 또는 테라스 패턴(패턴필터, 인공지능 필터, 핑거 프린트, 로컬 베이스안)에 의해 차단되거나 스팸으로 처리된 메일의 통계를 메일의 처리 단계별로 보여줍니다.
- 피싱 메일 - 개인의 신용 정보를 유출해 갈 수 있는 공격형 스팸 메일에 대한 통계를 보여줍니다.
- 바이러스 메일 - 바이러스 엔진에 의해 필터링된 바이러스 메일의 통계를 보여줍니다.
- POP - POP의 사용량 통계 정보입니다.
- IMAP - IMAP의 사용량 통계 정보입니다.
- CPU - 장비별 CPU 사용량 추이입니다.
- 메모리 - 장비별 메모리 사용량 추이입니다.
- 디스크 - 장비별 디스크 사용량 추이입니다.

## 통계 정보 검색

통계 정보를 확인하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[통계]**를 클릭합니다.
2. 왼쪽 화면의 통계 종류 메뉴에서 확인하려는 통계 정보를 클릭합니다.
3. 통계 조건을 선택합니다.
  - I. 도메인 선택 - 도메인을 선택하거나 도메인 정보를 직접 입력합니다.
  - II. 그래프 종류 - 꺾은선 그래프, 막대 그래프 중에서 그래프 종류를 선택합니다.
  - III. 기간 - 검색 기간을 선택합니다.
4. 통계 조건 선택이 완료되면, **검색**을 클릭합니다.

## 통계 결과 다운로드

검색한 통계 결과를 CSV, HTML, EXCEL 파일 형식으로 다운로드 할 수 있습니다.

1. 시스템 어드민의 **[통계]**를 클릭합니다.
2. 왼쪽 화면의 통계 종류 메뉴에서 확인하려는 통계 정보를 클릭합니다.
3. 통계 조건을 입력하여 통계를 검색합니다.
4. 통계 결과의 하단의 표에서 다운받으려는 파일 형식을 선택합니다.
  - I. CSV, HTML, EXCEL
5. **저장**을 클릭하여 파일을 열거나 저장합니다.



통계 결과를 EXCEL 파일 형식으로 확인할 때는 MS Excel에서 매크로 보안을 낮게 지정해야 합니다.

매크로 보안을 지정하는 방법은 아래와 같습니다.

MS Excel 2003에서는 **[도구 > 옵션 > 보안]** 탭에 있는 **매크로 보안**버튼을 클릭하여 **보안 수준을 낮음**으로 지정합니다.

MS Excel 2007에서는 **[오피스 단추 > Excel 옵션 > 보안 센터]**를 클릭합니다.

MS Excel 2010에서는 **[파일 > 옵션 > 보안센터]**를 클릭합니다. **보안 센터 설정**버튼을 클릭하여 **매크로 설정을 모든 매크로 포함**으로 지정합니다.

## 통계 결과 인쇄

조회한 통계 결과를 프린터를 통해 인쇄합니다.

1. 시스템 어드민의 **[통계]**를 클릭합니다.



2. 왼쪽 화면의 통계 종류 메뉴에서 확인하려는 통계 정보를 클릭합니다.
3. 통계 조건을 입력하여 통계를 검색합니다.
4. 화면 우측 상단에 있는 **인쇄**를 클릭하면 인쇄 창이 나타납니다.
5. 인쇄 창에서 **인쇄버튼**을 클릭하여 통계 결과를 인쇄합니다.



통계 결과에서 데이터가 있을 경우에는 각 범주 별로 색이 구분되어 인쇄됩니다. 인쇄 시 범주 별로 색이 구분 안될 경우, 익스플로어의 [도구 > 인터넷 옵션 > 고급 > 인쇄] 에서 **배경색 및 이미지 인쇄**를 선택하고 인쇄하면 정상적으로 출력됩니다.

## 6.2 이메일

이메일 통계에서는 메일의 처리 형태와 처리 전 과정을 분석하여 통계 결과를 확인 할 수 있습니다.

### 요약

정상 메일, 스팸 메일, 피싱 메일, 바이러스 메일 처리에 대한 요약 통계의 기간별 추이를 볼 수 있습니다. 수신메일과 송신메일로 구분하여 요약 통계를 확인할 수 있습니다.

### 정상 메일

정상 메일에서는 허용 규칙에 의해 통과된 허용 메일이거나, 스팸 혹은 바이러스 메일로 분류되지 않은 메일의 통계를 확인할 수 있습니다.

#### 추이 분석

- 정상메일 - 스팸/바이러스 메일이 아닌 메일
- 허용 규칙에 의해 처리된 메일

#### 순위 분석

- [허용 메일] 필터 명 - 허용 규칙 필터명의 기간별 순위
- [정상 메일] 발송 IP - 발송 IP의 기간별 순위
- [정상 메일] 송신자 메일 주소 - 송신자 메일 주소의 기간별 순위

- [정상 메일] 수신자 메일 주소 - 수신자 메일 주소의 기간별 순위
- [정상 메일] 송신자 도메인 - 송신자 도메인의 기간별 순위

## 스팸 메일

관리자(또는 사용자)의 차단 규칙 또는 테라스 패턴(패턴필터, 인공지능 필터, 핑거 프린트, 로컬 베이시안)에 의해 차단되거나 스팸으로 처리된 메일의 통계를 메일의 처리 단계별로 보여줍니다.

스팸 메일은 다음과 같은 단계로 처리되며, 모든 단계 및 각 단계별로 통계를 확인할 수 있습니다.

1. 접속단계
2. SMTP 단계
3. 콘텐츠 단계

## 모든 단계

스팸 처리의 모든 단계에 대한 통계를 기간별 추이로 확인할 수 있습니다.

- 접속 단계
- SMTP 단계
- 콘텐츠 단계

## 접속 단계

### 추이 분석

스팸 처리 단계 중 접속 단계의 규칙들에 의해 차단된 접속 횟수의 통계를 확인할 수 있습니다.

- 발송 IP 차단
- 시간당 접속 횟수 제한
- RBL
- 동시 접속 횟수 제한

### 순위 분석

스팸 처리 단계 중 접속 단계의 규칙들에 의해 차단된 상위 100개의 항목별 발송 IP 목록을 확인할 수 있습니다.

- [발송 IP 차단] 발송 IP - 발송 IP 차단 규칙에 의해 차단된 발송 IP들의 순위
- [시간당 접속 횟수 제한] 발송 IP - 시간당 접속 횟수 제한 규칙에 의해 차단된 발송 IP들의 순위
- [동시 접속 제한] 발송 IP - 동시 접속 횟수 제한 규칙에 의해 차단된 발송 IP들의 순위
- [RBL] 발송 IP - RBL (Realtime Spam BlackList) 서버가 제공하는 IP에 의해 차단된 발송 IP들의 순위

## SMTP 단계

### 추이 분석

스팸 처리 단계 중 SMTP 프로토콜 단계의 규칙들에 의해 차단된 SMTP 세션의 건수를 통계로 확인할 수 있습니다.

- DNS 검사 - EHLO 도메인, 송신자 도메인, 수신자 도메인
- SPF 검사
- 송신자 - 송신자 차단, 송신자 시간당 제한
- 수신자 - 수신자 차단, 수신자 시간당 제한
- 동보 응답 지연
- 송수신 기본 정책 - 최대 메일 크기, 최대 HOP 수, 최대 수신자 수, 최대 허용 세션 수, 외부 송신 릴레이 IP
- 메일 서버 거부

### 순위 분석

SMTP 프로토콜 단계의 규칙들에 의해 차단된 도메인, 송신자, 수신자의 상위 100개 목록을 확인할 수 있습니다.

- [EHLO DNS 검사] - EHLO의 도메인 유효성을 검사한 후, 위배 시에 차단
  - 발송 IP
  - 송신자 도메인
- [SPF 검사] - SPF 검사에서 위반하는 메일을 차단
  - 발송 IP
  - 송신자 도메인
  - 송신자 메일 주소
- [송신자 도메인 DNS 검사] 송신자 메일 주소 - 송신자의 도메인을 DNS 검사하여 유효치 않을 경우 차단
- [수신자 도메인 DNS 검사] 수신자 메일 주소 - 수신자의 도메인을 DNS 검사하여 유효치 않을 경우 차단
- [송신자 차단] 송신자 메일 주소 - 송신자 차단 목록의 송신자가 보낸 메일을 차단
- [수신자 차단] 수신자 메일 주소 - 수신자 차단 목록의 수신자가 보낸 메일을 차단
- [송신자 시간당 제한] 송신자 메일 주소 - 단위시간 동안 기준치 이상의 메일을 보내는 송신자를 설정 시간 동안 처리
- [수신자 시간당 제한] 수신자 메일 주소 - 단위시간 동안 기준치 이상의 메일을 받는 수신자를 설정 시간 동안 차단

## 컨텐츠 단계

### 추이 분석

스팸 메일 처리 단계 중 컨텐츠 단계의 필터링 항목(제목, 본문, 헤더 등) 규칙들에 의해 스팸 메일로 분류된 메일 통수와 기간별 추이를 확인할 수 있습니다.

- 스팸 메일

- 스팸성 메일
- 관리자 정의 메일

## 순위 분석

스팸 메일 처리 단계 중 콘텐츠 단계의 규칙들에 의해 분류된 스팸 메일의 항목별 상위 100개 목록을 확인할 수 있습니다.

- 발송 IP
- 송신자 메일 주소
- 처리 방법 - 멤버 정책 설정 시, 지정한 처리 방법(전송, 삭제, 차단등급, 태그)
- 수신자 메일 주소
- 필터 종류
- 필터명



처리 방법은 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 필터 멤버 정책]**에서의 처리방법입니다. 자세한 설명은 **필터 멤버 정책**을 참조하십시오.

## 피싱 메일

개인 정보를 불법적으로 알아내어 이용하려는 공격형 스팸 메일을 피싱 메일이라 합니다. 피싱 차단 규칙에 의해 걸려진 메일에 대한 통계를 확인할 수 있습니다.

### 추이 분석

피싱메일의 기간별 통계를 확인할 수 있습니다.

### 순위 분석

발송 IP, 송신자 메일 주소, 수신자 메일 주소의 순위로 통계를 분석할 수 있습니다.

## 바이러스 메일

바이러스 필터(엔진)에 의해 처리된 바이러스 메일의 통계 결과를 확인할 수 있습니다.

### 추이 분석

차단된 바이러스 메일 개수의 기간별 결과를 확인할 수 있습니다.

## 순위 분석

바이러스 필터에 의해 차단된 바이러스 메일의 항목별 순위 100개 목록을 확인할 수 있습니다.

- 발송 IP
- 송신자 메일 주소
- 수신자 메일 주소
- 바이러스 명

## POP

POP 사용량에 대한 추이를 지정한 기간별로 확인할 수 있습니다.

### 추이 분석

POP에 로그인한 수와 메일을 열람한 수의 추이를 확인할 수 있습니다.

- POP 로그인 - POP에 로그인 한 수
- POP 메일 열람 - POP을 통해 메일을 열람한 수

### 순위 분석

POP 사용에 대한 항목 별 순위 100개 목록을 확인할 수 있습니다.

- [로그인] 주소별 순위
- [로그인] IP 별 순위
- [메일 열람] 주소별 순위
- [메일 열람] IP 별 순위

## IMAP

IMAP 사용량에 대한 추이를 지정한 기간별로 볼 수 있습니다.

### 추이 분석

IMAP으로 로그인한 수를 기간별 추이로 확인할 수 있습니다.

### 순위 분석

IMAP 사용에 대한 항목 별 순위를 확인할 수 있습니다.

- [로그인] 주소별 순위
- [로그인] IP별 순위

## 6.3 시스템

장비의 CPU, 메모리, 디스크 통계를 기간별로 확인할 수 있습니다. 시스템 통계는 추이분석만 제공합니다.

### CPU

장비별 CPU 사용량의 추이를 지정한 기간별로 확인할 수 있습니다.

- System
- User
- I/O Wait
- Idle

### 메모리

메모리 사용량에 대한 추이를 지정한 기간별로 확인할 수 있습니다.

- Physical 메모리
- Swap 메모리



메모리 사용량이 80% 이상이 지속될 경우 적절한 조치를 해야 합니다.

### 디스크

도메인별 디스크 사용량에 대한 추이를 지정한 기간별로 확인할 수 있습니다. 특히 저장소 사용량이 80% 이상인 경우 해당 부분에 대한 적절한 조치를 해야 합니다.

## 6.4 통계 보고서

관리자는 시스템 어드민에 로그인 하지 않고서도 송수신 메일의 다양한 통계를 정기적으로 받아 확인할 수 있습니다.

다음은 통계 보고서 설정을 추가, 수정, 삭제하는 방법에 대해 설명합니다.

### 통계 보고서 추가

통계 보고서를 추가하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [통계 > 통계보고서]를 클릭합니다.
2. 통계 보고서 목록에서 **추가**를 클릭합니다.
  - I. 종류 - 보고서의 종류를 선택합니다. 보고서 종류는 [통계]에 있는 통계목록입니다.
  - II. 기간 - 보고서 내용을 확인할 통계 기간을 선택합니다.
  - III. 발송 시간 - 보고서를 수신자에게 발송할 시간을 선택합니다.
  - IV. 언어 - 보고서의 언어를 설정합니다.
  - V. 보고서 수신자 - 보고서를 수신할 수신자의 메일 주소를 설정합니다.
3. 설정이 완료되면, **추가**를 클릭합니다.

### 통계 보고서 수정

통계 보고서 목록에서 통계 보고서 설정을 수정합니다.

1. 시스템 어드민의 [통계 > 통계보고서]를 클릭합니다.
2. 통계 보고서 목록에서 수정하려는 통계 보고서의 이름을 클릭합니다.
3. 각 항목을 수정합니다.
4. 수정이 완료되면, **수정**을 클릭합니다.

### 통계 보고서 삭제

통계 보고서 목록에서 통계 보고서 삭제합니다.

1. 시스템 어드민의 [통계 > 통계보고서]를 클릭합니다.
2. 통계 보고서 목록에서 삭제하려는 통계 보고서를 선택한 후, **삭제**를 클릭합니다.

## 통계 보고서 설정

통계 보고서의 발송자를 설정할 수 있습니다.

1. 시스템 어드민의 [통계 > 통계보고서]를 클릭합니다.
2. 통계 보고서 목록 상단에 있는 **설정**을 클릭합니다.
3. 보고서 발송자 설정 화면이 나타납니다. 발송자 이름과 메일주소를 각각 입력합니다.
4. 입력이 완료되면, **확인**을 클릭합니다.



## 7. 모니터링

---

### 7.1 개요

시스템 어드민에서는 보다 원활한 서비스 제공을 위해 웹 방문자 수, 송수신 메일 처리, 시스템의 현황 및 처리 내역을 확인할 수 있는 기능을 제공합니다.

모니터링이 가능한 주요 사항은 다음과 같습니다.

- 메일 송수신 처리 현황 파악
- 송수신과 트래픽 감지
- 처리 메일 추적
- 시스템현황 파악
- 송수신 장애 감지

### 7.2 실시간 현황

실시간 현황에서는 웹 메일의 메일 수신 상태를 실시간으로 모니터링하여 정상 메일과 스팸 메일, 피싱 메일, 바이러스 메일 및 차단 메일의 비율 및 수신 현황을 확인 할 수 있습니다.

- 오늘 메일현황 - 24시간 동안의 메일 유입량 누적치를 보여줍니다.
- 30일간 메일현황 - 최근 30일간의 메일 수신량을 하루 단위로 보여줍니다.

## 7.3 로그

### 이메일 로그

이메일 로그에서는 송수신 메일을 처리하고 있는 상황을 실시간으로 모니터링을 할 수 있습니다. 로그 분석을 통해 실시간으로 서비스 트래픽을 확인하여, 메일 송수신을 저해하는 메일을 즉시 스팸 메일로 등록할 수 있습니다.

단, 부하를 줄이기 위해 실시간 로그 모니터링은 최근 1000개의 로그로 제한합니다.

메일 분류에 따른 모니터링 항목은 다음과 같습니다.

- 전체메일 - 송수신되는 모든 메일을 모니터링 합니다.
- 정상메일 - 송수신 되는 메일 중에서 정상 메일에 대해 모니터링 합니다.
- 스팸메일 - 송수신 되는 메일 중에서 스팸 메일에 대해 모니터링 합니다.
- 피싱메일 - 송수신된 스팸 메일 중에서 공격형 피싱 메일만 모니터링 합니다.
- 바이러스메일 - 송수신된 메일 중에서 바이러스 메일만 모니터링 합니다.
- 에러메일 - 송수신된 메일 중에서 에러가 발생한 메일만 모니터링 합니다. 확인할 수 있는 에러 표기는 다음과 같으며, 목록의 이유항목에 나타납니다.
  - connection-reset - 연결이 끊어진 경우
  - connection-refused - 연결이 거부된 경우
  - time-out - 응답 시간이 지난 경우
- WebMail - 사용자가 웹 메일에서 메일을 사용한 내역을 보여줍니다. 각 표시되는 내역은 로그인, 메일 읽기, 이동, 복사, 삭제, 전송, 편지함 생성, 수정, 삭제입니다. 단, 메일 읽기, 메일 전송 이외에는 해당 메일의 제목을 볼 수 없습니다.
- IMAP - MAP이 메일을 처리한 내역을 보여줍니다.
  - 메일의 복사, 이동, 삭제, 예약
  - 메일함 생성, 수정, 삭제
- POP - POP이 메일을 처리한 내역을 보여줍니다.
  - 로그인, 메일 다운로드, 메일 삭제

### 이메일 로그 검색

이메일 로그를 검색할 수 있습니다. 이메일 로그 검색 결과가 1000개를 초과할 경우, 최근 1000개까지만 나타납니다.



검색 결과는 시스템의 부하를 줄이기 위해 최근 1000개만 출력하고 보관 기간이 지난 메일은 자동 삭제합니다.



이메일 로그의 검색 대상은 로그 보관기간을 설정한 기간의 송수신 로그입니다. 이메일 로그 보관기간을 확인하거나 변경하려면, 화면 상단에 있는 **설정**을 클릭합니다.

## 기본 검색

기본 검색하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[모니터링 > 로그 > 이메일 로그]**를 클릭합니다.
2. 모니터링하려는 하위 메뉴를 클릭합니다.
3. 이메일 로그 목록의 우측 상단에서 검색 대상을 선택합니다.
4. 검색 조건을 선택합니다.
  - I. 정확하게 - 검색 대상과 검색어가 동일한 메일 로그를 검색합니다.
  - II. 포함해서 - 검색 대상에서 검색어가 포함된 메일 로그를 모두 검색합니다.
5. 검색어를 입력합니다.
6. **검색**을 클릭합니다.

## 고급 검색

고급 검색에서는 검색 일자와 조건을 상세하게 설정하여 이메일 로그를 검색합니다.

1. 시스템 어드민의 **[모니터링 > 로그 > 이메일 로그]**를 클릭합니다.
2. 모니터링하려는 하위 메뉴를 클릭합니다.
3. 이메일 로그 목록의 우측 상단에 있는 **고급검색**을 체크합니다.
4. 고급 검색 조건이 나타나면, 각 항목을 입력 또는 설정합니다.
5. **검색**을 클릭합니다.



검색 항목은 이메일 로그의 하위메뉴에 따라 다르게 나타납니다.

## 스팸메일/정상메일 등록

이메일 로그 모니터링 목록에서 정상(스팸)으로 처리된 메일을 스팸(정상) 메일로 처리할 수 있습니다.

추가된 규칙은 시스템 어드민의 **[보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터 > 차단 규칙]** 또는 **[보안 설정 > 이메일 보안 > 안티 스팸 > 콘텐츠 필터 > 허용 규칙]**에서 확인할 수 있습니다.

스팸메일 또는 정상메일 등록은 다음과 같은 하위 메일 메뉴에서 수행할 수 있습니다.

- 전체메일 - 스팸메일 또는 정상메일 등록
- 정상메일 - 스팸메일 등록
- 스팸메일, 피싱메일 - 정상메일 등록

## 스팸 메일로 등록

정상으로 처리된 메일을 스팸 메일로 등록합니다.

1. 시스템 어드민의 [모니터링 > 로그 > 이메일 로그]를 클릭합니다.
2. 모니터링하려는 하위 메뉴를 클릭합니다.
  - I. 전체메일, 정상메일, 피싱메일, 바이러스메일, 에러메일
3. 이메일 로그 목록의 **정상/스팸신고** 항목에서 **스팸신고**를 클릭합니다.
4. **스팸 메일로 등록** 화면이 나타납니다.
5. 해당 항목을 선택합니다.
  - I. 다우기술 관리자에게 보고 - 다우기술의 스팸메일 관리자에게 신고합니다. 관리자는 해당 메일을 검토한 후, 차단 규칙을 새로 만들어 배포합니다.
  - II. 차단 규칙에 추가 - 송신자, 제목의 차단 규칙을 입력한 후, 메일 처리 방법을 선택합니다.
6. 스팸 메일 설정이 완료되면, **확인**버튼을 클릭합니다.



메일 처리 방법에 대한 설명은 [표 5-1 처리단계별 메일 분류](#)를 참조하십시오.

## 정상 메일로 등록

정상으로 처리된 메일을 스팸 메일로 등록합니다.

1. 시스템 어드민의 [모니터링 > 로그 > 이메일 로그]를 클릭합니다.
2. 모니터링하려는 하위 메뉴를 클릭합니다.
  - I. 전체메일, 정상메일, 피싱메일, 바이러스메일, 에러메일
3. 이메일 로그 목록의 **정상/스팸신고** 항목에서 **정상신고**를 클릭합니다.
4. **정상 메일로 등록** 화면이 나타납니다.
5. 해당 항목을 선택합니다.
  - I. 다우기술 관리자에게 보고 - 다우기술의 스팸메일 관리자에게 신고합니다. 관리자는 해당 메일을 검토한 후, 차단 규칙을 새로 만들어 배포합니다.
  - II. 허용 규칙에 추가 - 추가할 규칙 항목을 선택한 후, 송신자, 제목의 허용 규칙을 입력합니다.
6. 스팸 메일 설정이 완료되면, **확인**버튼을 클릭합니다.

## 이메일 로그 새로고침

내부적으로 설정한 시간 간격으로 이메일 로그 정보를 자동 갱신되거나, **새로고침**을 클릭하여 메일 로그 정보를 새로 불러옵니다.



이메일 로그 새로고침의 시간 설정을 확인하거나 변경하려면, 화면 상단에 있는 **설정**을 클릭합니다.

## 로그 설정

서비스의 로그 환경을 설정할 수 있습니다.

1. 시스템 어드민의 **[모니터링 > 로그 > 로그 설정]**을 클릭합니다.
2. 로그 설정의 각 항목을 설정합니다.
  - I. 메일 로그
    - i. 보존 기간 - 메일 송수신과 관련된 로그를 보존하는 기간을 설정합니다. 로그는 최대 365일까지 저장할 수 있습니다. 로그 보관이 너무 길면 디스크 용량도 많이 차지하고 검색 시에 시스템에 부하가 발생합니다. 권장값은 30일입니다.
    - ii. 제목 표시 여부 - 제목 표시 여부 설정은 개인 정보 보호를 위해서 사용하는 기능입니다. 메일 로그에서 제목 부분의 표시 여부를 설정합니다. 메일 로그의 제목 표시 여부 확인은 시스템 어드민의 **[모니터링 > 이메일 로그]**에서 확인할 수 있습니다.
    - iii. 디버그 로그 옵션 - 시스템에 이상이 있다고 판단되는 경우, 전문적인 지원팀의 필요에 의해서 확인하는 로그입니다.
  - II. 실시간 메일 로그 모니터링
    - i. 사용 여부 - 시스템 어드민의 **[모니터링 > 이메일 로그]**에서 실시간 로그를 보여줄 것인지에 대한 여부를 결정합니다.
    - ii. 로그 자동 갱신 간격 - **[모니터링 > 이메일 로그]**에서 메일 로그의 목록을 자동으로 갱신할 시간을 설정합니다. 시간 간격이 너무 짧으면 CPU에 부하를 주므로 30초로 권장합니다.
    - iii. 로그 본문 보기 - 로그 본문 보기에 대해 설정합니다.
3. 설정이 완료되면 **저장**을 클릭합니다.

## 7.4 시스템현황

장비의 현황을 체크하여 장비별 프로세스와 시스템의 현재 상황을 모니터링 할 수 있습니다.

### 프로세스 현황

서버별 프로세스의 현황에 대해 모니터링을 할 수 있습니다. 확인 가능한 프로세스는 tpopd, t4imapd, WEBMAIL, tmtad, tremoted, tmss-routed, search, notifier입니다.

1. 시스템 어드민의 **[모니터링 > 시스템현황 > 프로세스 현황]**을 클릭합니다.
2. **서버선택**에서 모니터링할 서버를 선택합니다.
3. 장비의 프로세스 상황을 확인할 수 있습니다. 프로세스 현황의 주요 기능과 사용법은 다음과 같습니다.
  - I. 시작/중지 - 선택한 프로세스를 시작하거나 중지시킵니다.

- II. 재시작 - 선택한 프로세스를 재시작합니다. (단, WEBMAIL, searcher, notifier는 제외)
- III. 재설정 - 선택한 프로세스를 중단 없이 새로운 설정값을 적용합니다. (단, WEBMAIL, searcher, notifier는 제외)

## 리소스 현황

서버 장비의 현재 리소스 현황을 모니터링 할 수 있습니다. 리소스란 서버에서 가용할 수 있는 자원을 말하며, 시스템 부하율 및 디스크 사용량을 표시합니다

### 시스템 부하율

시스템 부하율을 수치 및 신호등 표시로 보여줍니다.

- 수치 - 기본적으로 시스템 부하율이 10 이하 일 경우, 현재 시스템은 매우 안정되게 운영되고 있는 것으로 합니다.
- 신호등 표시 - 시스템 상태를 보여줍니다.
  - 정상 - 녹색
  - 주의 - 노랑
  - 긴급 - 빨강

### 디스크 리소스

디스크 사용량은 시스템의 전체 디스크량을 보여줍니다. 각 파티션 마다의 사용량/ 전체 사용량(%)로 표기합니다. 그리고, 각 사용량에 따라 신호등 색상 표시로 현재의 상태를 확인할 수 있습니다.

### 보고서 작성

로그 보존 기간 내의 시스템 상태정보에 대해 날짜를 선택하여 보고서를 다운로드할 수 있습니다.

## 메일처리 현황

수신 메일 서버에서 현재까지 처리한 메일 및 필터링된 IP수 등 메일서버의 현황을 항목별로 확인할 수 있습니다.

확인하려는 메일 서버를 선택하면 해당 메일 서버의 메일처리 현황 정보가 나타납니다. 메일처리 현황에서의 항목은 다음과 같습니다.

**표 7-1** 메일 처리 현황 항목

항 목	설 명
서버 실행 시간	수신 메일 서버가 시작된 후, 중지되기 전까지 총 실행 시간입니다.
실행 중인 쓰레드	수신 메일 서버에서 실행하는 쓰레드 수입니다.
현재까지 처리한 메일	수신 메일 서버가 시작 된 후, 현재까지 송수신한 메일 수입니다.

항 목	설 명
처리할 메일	수신 큐에 저장된 메일 수입니다.
내부로 송신한 메일	수신메일 서버가 메일을 수신한 후, 전달 메일 서버에 메일을 전달한 메일입니다.
IP 필터링	접속단계 차단, SMTP 단계 차단, 바이러스 필터에서 필터링 룰에 의해 필터링 된 IP의 수입니다. IP 필터링, 바이러스 필터링
IP 차단	필터링 룰에 의해 차단된 IP의 수입니다.
바이러스 차단	바이러스 메일을 처리한 수입니다.
스팸 차단	필터 관리 중 스팸 콘텐츠 필터에 의해 처리된 전체 메일 수 와 각각 처리된 메일 수입니다. 삭제, 저장, 경고, 로깅, 반송, 통과, 태그

## 수신 처리 현황

수신 메일 서버의 각 쓰레드 상태표시 및 각 쓰레드가 실행하고 있는 상황을 확인할 수 있습니다.

### 쓰레드 상태 표시

확인하려는 메일 서버를 선택하면 해당 메일 서버의 수신처리 현황 정보가 나타납니다.

**표 7-2** 수신 처리 현황 항목

항 목	설 명
대기 중	쓰레드가 실행되지 않은 상태
접속 중	메일을 보내기 위해 TCP단에서 접속을 시도하는 단계
SMTP Greeting 상태	접속 후, EHLO 또는 HELO 프로토콜을 받기 전 상태
Mail From 상태	Mail From 프로토콜을 받은 상태
Rcpt To 상태	Rcpt to 프로토콜을 받은 상태
Data 상태	Data 프로토콜을 받은 상태 혹은 콘텐츠를 받고 있는 상태
Quit 상태	Quit 프로토콜을 받은 상태
New Session 상태	Quit 프로토콜 대신 rset 프로토콜을 받아서 새 세션을 연 상태
접속 종료 상태	Quit 프로토콜을 받고 난 후, TCP 단에서 접속 종료하는 단계
인증 전 상태	수신자 인증을 하기 전 단계 수신자가 있는지 없는지를 체크하는 단계
인증 후 상태	수신자 인증을 하고 난 후 단계. 수신자가 있으면 다음 단계로 이동하고, 수신자가 없으면 메일을 반송
시간당 제한 IP 처리 중	수신된 메일이 시간당 제한에 걸려 해당 IP를 차단하는 단계
IP 차단 처리 중	접속한 IP를 검사하여 차단하는 단계
RBL 검사 중	메일 접속 시, 해당 메일의 IP 주소를 이용하여 RBL 룩업하는 단계
송신자 DNS 검사 중	송신자 메일에 있는 도메인을 DNS 룩업하는 단계
수신자 DNS 검사 중	수신자 메일에 있는 도메인을 DNS 룩업하는 단계

항 목	설 명
송신자 시간당 제한 처리 중	수신된 메일의 송신자 주소가 시간당 제한에 걸려 해당 IP를 차단하는 단계
동시 접속 수 제한 처리 중	메일 전송 시, 동시에 여러 쓰레드에 접속하여 메일을 발송하려는 소스 IP를 차단하는 단계

## 쓰레드 ID별 상태 확인

각 쓰레드 ID별로 시작시간, 현재 상황, 접속 IP를 확인할 수 있습니다.

- 쓰레드 ID - tmtad 프로세스의 쓰레드 ID입니다. 쓰레드 ID는 고유의 ID를 가집니다.
- 시간 - 쓰레드가 처음 생성된 시간입니다.
- 현재 상황 - 쓰레드의 현재 상태를 보여줍니다. (예) 대기중, 접속중 등
- 접속 IP - 발송 IP - 메일의 발송 IP입니다.

## 필터된 IP 검색

접속 단계, SMTP 단계, 바이러스 필터에 의해 차단된 IP 목록을 확인하고, 차단된 IP를 해제할 수 있습니다.

1. 시스템 어드민의 [모니터링 > 시스템현황 > 필터된 IP검색]을 클릭합니다.
2. 검색할 서버를 선택합니다.
3. 필터 IP에 검색하려는 IP를 입력합니다.
4. 검색을 클릭합니다.



필터된 내역을 확인 후, 해당 IP 필터를 해제하려면 **필터해제**버튼을 클릭합니다.

## 큐 현황

송수신되는 메일이 메일 서버의 이상으로 바로 전달되지 않을 경우 큐에 임시 저장하게 됩니다. 관리자는 큐 모니터링에서 큐에 저장된 메일 목록을 확인하고, 재전송 및 삭제를 수행할 수 있습니다.

큐 모니터링은 다음과 같이 분류됩니다.

- 수신 메일 큐 - 수신 메일 큐에 저장되는 경우는 다음과 같습니다.
  - 메일 용량이 큰 메일(512K 이상)
  - 동보 메일 - 수신 메일 큐에 저장한 후 처리
  - 내부 메일 서버에 이상이 있는 경우, 메일이 전달되지 못하고 수신 메일 큐에 임시 저장
- 송신 메일 큐 - 송신 메일 큐에 저장되는 경우는 다음과 같습니다.



- 외부로 발송하는 메일
- 외부 메일 서버에 이상이 있는 경우, 메일이 전달되지 못한 경우 송신 메일 큐에 임시 저장

## 큐 모니터링 목록 구성

정상적으로 처리되지 않은 메일의 목록을 확인할 수 있습니다. 큐 모니터링 목록 위에 해당 큐의 총 수가 표시됩니다.

큐 모니터링 목록의 항목 구성은 다음과 같습니다.

- 시간/발송IP - 메일 처리 시각(YYYY/MM/DD HH:mm)과 메일을 발송한 IP입니다.
- 송신자 - SMTP 프로토콜(mail from)상의 송신자입니다.
- 수신자 - SMTP 프로토콜(rcpt to)상의 수신자입니다.
- 제목 - 메일 본문입니다. 메일 제목을 클릭하면 메일 본문을 확인할 수 있습니다.
- 설명(처리 이유) - 메일이 정상적으로 처리되지 못한 이유가 나타납니다.

## 큐 검색

단순 검색 또는 고급 검색으로 큐를 검색할 수 있습니다.

### 단순 검색

검색 조건과 범위를 선택하여 큐를 검색합니다. 큐 검색은 최근 수신된 상위 1000개의 큐 중에서 원하는 큐 정보를 검색할 수 있습니다.

1. 시스템 어드민의 **[모니터링 > 시스템현황 > 큐현황]**을 클릭합니다.
2. **수신메일 큐** 또는 **송신메일 큐**를 클릭합니다.
3. 큐 목록 우측 상단에서 검색 범위를 선택합니다.
  - I. 제목 - 메일 본문의 제목
  - II. 발송 IP - 메일의 발송 IP입니다.
  - III. 송신자 - SMTP 프로토콜(mail from)상의 송신자입니다.
  - IV. 수신자 - SMTP 프로토콜(rcpt to) 상의 수신자입니다.
4. 검색 조건을 선택하고, 검색어를 입력합니다.
5. **검색**을 클릭합니다.

### 고급 검색

날짜와 여러 검색조건으로 큐를 검색합니다. 고급검색은 상위 1000개 이외의 전체 큐에 대해 검색합니다. 단, 시스템의 부하를 주지 않기 위해서 검색 결과는 1000개만 보여줍니다.

1. 시스템 어드민의 **[모니터링 > 시스템현황 > 큐현황]**을 클릭합니다.
2. **수신메일 큐** 또는 **송신메일 큐**를 클릭합니다.
3. 큐 목록 우측 상단에서 **고급 검색**을 체크합니다.
4. 상세 검색 조건 항목을 선택하고, 검색 조건에 해당하는 검색어를 입력합니다.

- I. 시작 시점/종료 시점 - 메일이 처리된 일자 범위를 선택합니다.
  - II. 검색 방식 - 검색 조건(정확하게, 포함하여)을 선택합니다.
  - III. 송신자 - SMTP 프로토콜(mail from)상의 송신자입니다.
  - IV. 수신자 - SMTP 프로토콜(rcpt to) 상의 수신자입니다.
  - V. 제목 - 메일 제목입니다.
  - VI. 발송 IP - 메일의 발송 IP입니다.
5. 검색을 클릭합니다.

## 큐 삭제

큐에 보관되어 있는 메일 정보를 삭제할 수 있습니다. 삭제된 메일은 복구할 수 없습니다.

1. 시스템 어드민의 [모니터링 > 시스템현황 > 큐현황]을 클릭합니다.
2. 수신메일 큐 또는 송신메일 큐를 클릭합니다.
3. 메일목록에서 삭제하려는 메일을 선택합니다.
4. 목록 상단에 있는 삭제를 클릭합니다.

## 큐 전송

큐에 보관되어 있는 메일을 재전송할 수 있습니다. 메일을 전송하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [모니터링 > 시스템현황 > 큐현황]을 클릭합니다.
2. 수신메일 큐 또는 송신메일 큐를 클릭합니다.
3. 메일목록에서 전송하려는 메일을 선택합니다.
4. 목록 상단에 있는 전송을 클릭합니다.

## 7.5 문의 및 지원

### 메일문의

시스템 운영 중 생긴 의문점을 ㈜다우기술의 고객지원팀에게 메일을 전송하여 문의합니다. 접수된 문의사항은 신속하게 처리되어 메일 또는 전화로 답변드리겠습니다.

문의하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [모니터링 > 문의 및 지원 > 메일문의]를 클릭합니다.
2. 문의 사항을 입력합니다.

- I. 제목 - 문의 제목을 입력합니다.
  - II. 질문자 메일주소 - 질문자의 메일 주소를 입력합니다. 문의에 대한 답변을 받기 위해 정확하게 입력하도록 합니다.
  - III. 본문 - 문의 내용을 작성합니다.
3. 작성이 완료되면, **확인**을 클릭합니다.

## 경고 메일 설정

시스템의 이상 현상이 발생하였을 경우, 경고하는 메일을 지정한 수신자에게 자동으로 보내는 기능을 설정합니다.

### 경고 메일이 발송되는 경우

경고 메일이 발송되는 경우는 다음과 같습니다.

- 수신 큐에 메일이 2,000 이상 쌓였을 경우
- 송신 큐에 메일이 2,000 이상 쌓였을 경우
- 디스크 사용률이 80% 이상인 경우 (디스크 공간 및 Inode 사용률)
- 테라스 패턴 필터를 3일동안 업데이트 못 한 경우
- 테라스 인공지능 필터를 3일동안 업데이트 못 한 경우
- 테라스 핑거프린트 필터를 3일동안 업데이트 못 한 경우
- 바이러스 필터를 7일 동안 업데이트 못한 경우
- 작동하지 않는 프로세스가 있을 경우
- 여러 장비로 서비스 할 때, 응답 없는 장비가 있는 경우
- 장비의 라이선스가 만료된 경우
- 스팸 라이선스, 바이러스 라이선스의 만료일이 30일 남은 경우
- 통계 파일이 1일치 이상 쌓이는 경우
- 로그 모니터링이 정상적으로 실행되고 있지 않는 경우
- 바이러스 엔진이 정상적으로 실행되고 있지 않는 경우
- 웹 메일 엔진에서 사용하는 힙 메모리 영역이 부족한 경우



경고 메일 체크 주기는 1시간(60분)입니다. 단, 디스크 사용률은 12시간에 한번씩 확인합니다.

경고 메일을 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[모니터링 > 문의 및 지원 > 경고 메일 설정]**을 클릭합니다.
2. 경고 메일 **사용 여부**를 선택합니다.
3. **메일 주소**를 입력합니다.
4. 경고 메일 발송자의 이름과 메일주소를 입력합니다.
5. 설정이 완료되면, **저장**을 클릭합니다.

## 8. 모빌리티

### 8.1 모바일 앱 버전 관리

모바일 디바이스별(PC, iPhone, 안드로이드 폰 등)로 최신 패키지를 업로드하여 사용자가 접속했을 때 모바일 앱의 업데이트 상황을 알리고, 업데이트를 유도합니다.



시스템 어드민의 [도메인/사이트 관리 > 사이트 목록]에서 사이트명을 클릭합니다. 사이트 수정화면의 **제공 서비스**에 있는 **모빌리티**가 **사용인** 경우에만, PC메신저와 모바일 웹 그리고 모바일 앱을 사용할 수 있습니다. 그러므로, 모빌리티를 사용하지 않는 경우에는 모빌리티에 관련된 정보를 설정할 필요가 없습니다.

### 모바일 앱 버전 추가

버전을 추가하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [모빌리티 > 모바일 앱 버전 관리]를 클릭합니다.
2. 디바이스 버전 목록 상단에 있는 **추가**를 클릭합니다. 버전 추가화면으로 이동합니다.
3. 각 항목을 입력 또는 설정합니다.
  - I. 디바이스 - 디바이스 종류를 선택합니다.
    - i. PC - 새로운 버전의 PC 메신저를 배포할 때 선택합니다.
    - ii. iPhone - iOS 기반의 아이폰용 앱을 배포할 때 선택합니다.
    - iii. Android - 안드로이드 기반의 스마트폰용 앱을 배포할 때 선택합니다.

안드로이드용 앱을 배포할 때는 **In-house**와 **Market**을 선택할 수 있습니다. **In-house**는 앱 패키지를 내부 서버에 올리고, 사용자가 URL로 서버에 있는 패키지를 다운로드하는 방식입니다. **Market**은 안드로이드 마켓 등 외부 서버에 앱 패키지를 올리고 사용자가 마켓에서 직접 다운로드하는 방식입니다.
  - II. 중요도 - 업로드하려는 패키지의 중요도를 선택합니다. 사용자가 업데이트 내역을 확인하고 바로 업데이트

하길 바라면 **상**을 선택합니다.

III. 버전 - 업로드 하는 패키지의 버전을 입력합니다.

IV. 업데이트 메시지 - 업데이트 할 때 사용자에게 노출되는 메시지를 작성합니다. 다국어로 서비스를 원한다면, **항목추가**를 클릭하여 각각의 언어로 업데이트 메시지를 작성합니다.

V. 패키지 업로드 - **파일 찾기**를 클릭하여 업로드할 패키지를 내 컴퓨터에서 선택합니다.

VI. 업데이트 내용 - 업데이트 된 항목을 기술합니다. 다국어로 서비스를 원한다면, **항목추가**를 클릭하여 각각의 언어로 업데이트 항목을 작성합니다.

VII. 비고 - 기타 관리자 입장에서 필요한 내용이 있는 경우 알아볼 수 있도록 해당 내용을 기록합니다.

4. 설정이 완료되면, **저장**을 클릭합니다.

## 모바일 앱 버전 추가

추가한 버전을 수정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 **[모빌리티 > 모바일 앱 버전 관리]**를 클릭합니다.
2. 디바이스 버전 목록에서 수정하려는 항목을 클릭합니다.
3. 각 항목을 수정합니다.
4. 수정이 완료되면, **수정**을 클릭합니다.

## 모바일 앱 버전 삭제

더 이상 제공하지 않는 앱 버전이 있거나, 잘못된 패키지를 업로드한 경우 모바일 앱 버전을 삭제할 수 있습니다.

1. 시스템 어드민의 **[모빌리티 > 모바일 앱 버전 관리]**를 클릭합니다.
2. 디바이스 버전 목록에서 삭제하려는 항목을 선택한 후, 목록 상단에 있는 **삭제**를 클릭합니다.

## 모바일 앱 버전 필터링

모바일 앱 버전을 디바이스 종류별로 필터링할 수 있습니다.

1. 시스템 어드민의 **[모빌리티 > 모바일 앱 버전 관리]**를 클릭합니다.
2. 디바이스 버전 목록 위에 있는 **전체분류** 드롭다운 박스를 클릭합니다.

확인하려는 디바이스를 선택합니다.

- I. PC, iPhone, Android

## 9. 기타 설정



---

### 9.1 IP 그룹 설정

내부적으로 사용하는 IP를 그룹으로 등록하면, 보안설정 등의 메뉴에서 IP를 쉽게 등록할 수 있습니다.

#### IP 그룹 추가

IP그룹 추가하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [기타 설정 > IP 그룹 설정]을 클릭합니다.
2. **추가**를 클릭합니다.
  - I. 그룹명을 입력합니다. 그룹명은 2bytes 이상 32bytes 이하로 입력합니다.
  - II. IP입력 종류를 선택합니다.
    - i. 하나의 IP 입력 - IP 형식에 맞게 입력을 합니다.
    - ii. IP 범위로 입력 - 0.0.0.0 - 255.255.255.255 내의 IP 범위를 입력합니다.
    - iii. 서브넷 마스크로 입력 - 서브넷 마스크 형식으로 IP를 입력합니다.
  - III. IP 입력 후, 추가아이콘()을 클릭하여 IP 목록에 추가합니다.
  - IV. IP 삭제 - IP 목록에서 IP를 삭제하려면, IP를 선택한 후 삭제아이콘()을 클릭합니다.
  - V. IP 검색 - IP 목록에서 IP를 검색하려면, 목록 하위에 IP를 입력한 후 **검색**을 클릭합니다.
  - VI. IP 목록 파일 가져오기 - **가져오기**를 클릭하여, IP 목록을 한 번에 추가합니다.
  - VII. IP 목록 파일 내보내기 - **내보내기**를 클릭하여, IP 목록을 파일로 다운로드합니다.
3. IP 그룹 설정이 완료되면, **추가**를 클릭합니다.

## IP 그룹 수정

IP그룹 목록에서 IP그룹을 수정합니다.

1. 시스템 어드민의 [기타 설정 > IP 그룹 설정]을 클릭합니다.
2. IP 그룹 목록에서 수정할 IP 그룹명을 클릭합니다.
3. IP 그룹 정보를 수정합니다.
4. 수정이 완료되면, 수정을 클릭합니다.

## IP 그룹 삭제

IP 그룹 목록에서 IP그룹을 삭제합니다.

1. 시스템 어드민의 [기타 설정 > IP 그룹 설정]을 클릭합니다.
2. 목록에서 삭제할 IP 그룹을 선택한 후, 삭제를 클릭합니다.

## 9.2 초기화

시스템이 설치된 이후 내부 DB에 저장된 각종 데이터를 설치 시점으로 초기화를 할 수 있습니다.



초기화 기능을 수행한 후에는 기존 정보는 삭제되어 더 이상 확인할 수 없으므로, 초기화 실행에 유의하시기 바랍니다.

초기화할 수 있는 데이터는 다음과 같습니다.

- 통계 - 통계 관련 모든 정보를 초기화합니다.
- 모니터링 - 로그, 큐, 관리자 로그 관련 모든 정보를 초기화합니다.
- 보안설정 - 모든 단계 필터와 멤버 정책을 설치 시의 값으로 초기화합니다.
- 메일 정보 필터 - 유출 감시 모니터링, 정보 보호 필터의 모든 내용을 초기화합니다.

초기화를 하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [기타 설정 > 초기화]를 클릭합니다.
2. 초기화하려는 항목 옆에 있는 초기화를 클릭합니다.

## 9.3 보관 기간 설정

PC 메신저, 모바일 앱으로 대화한 내용 및 서비스 알림의 보관 기간을 설정합니다.

보관 기간을 설정하는 방법은 다음과 같습니다.

1. 시스템 어드민의 [기타 설정 > 보관 기간 설정]을 클릭합니다.
  - I. 알림 보관 기간 - 서비스의 알림을 보관하는 기간을 선택합니다. 기본 값은 3개월입니다.
  - II. 대화내용 보관기간 - PC 메신저, 모바일 앱에서 대화한 내용 및 첨부파일을 저장하는 기간을 설정할 수 있습니다.
    - i. 시스템 설정 - 시스템 관리자에 의하여 시스템 및 사이트에 일괄 적용되며 기본값은 1년입니다.
    - ii. 사이트 별 설정 - 각 사이트별 관리자에 의해 설정될 수 있으며 사이트 별로 메시지만 삭제하거나 첨부파일을 관리자가 직접 삭제할 수 있습니다.
2. 설정이 완료되면, **저장**을 클릭합니다.



직접입력을 선택하면 오른쪽 입력박스에 최대 999까지 입력하여 설정할 수 있습니다.

## 9.4 비밀번호 찾기 설정

비밀번호 찾기 기능을 사용할 것인지 설정합니다.

옵션값을 <사용>으로 설정하면, 사용자는 비밀번호를 분실해도 찾을 수 있습니다.



# 10. 관리자

---

## 10.1 관리자 목록

여러 명의 관리자를 지정하여 서비스를 관리할 수 있습니다.

### 관리자 종류

관리자에는 두 가지 종류가 있습니다.

- 시스템 관리자 - 시스템 전체를 관리하는 시스템 어드민의 접근권한을 갖습니다. 시스템 관리자는 각 사이트의 사이트 어드민으로 이동하여, 계정관리, 부서관리, 메일, 자료실, 캘린더 등도 관리할 수 있습니다.
- 사이트 관리자 - 특정 사이트(도메인)에 한하여 계정관리, 부서관리, 메일, 자료실, 캘린더 등을 관리할 수 있습니다. 사이트 관리자는 사이트 어드민에만 접근할 수 있습니다.



관리자 목록에서 항목명(아이디, 사용자 이름, 도메인, 관리자 종류)을 클릭하면, 정렬 순서를 변경할 수 있습니다.

## 관리자 추가

관리자를 새로 추가합니다.

1. 시스템 어드민의 **[관리자]**를 클릭합니다.
2. 관리자 목록 위에 있는 **추가**를 클릭합니다.
3. 관리자 추가화면에서 각 항목을 설정합니다.
  - i. 관리자 종류 - 관리자 종류를 선택합니다.
    - i. 시스템 관리자 - 시스템 전체에 대한 권한을 가지며, 모든 사이트를 관리할 수 있습니다.

- ii. 사이트 관리자 - 특정 사이트(도메인)에 대한 서비스 설정 권한을 가집니다.
  - II. 관리자 ID - 관리자를 지정합니다. 이 때, 관리자는 이미 회사에서 생성된 계정이어야 합니다. **사용자 검색**을 클릭하여, 아이디 또는 이름으로 사용자를 검색합니다.
  - III. 사용자 이름 - 관리자 아이디를 지정하면, 해당 아이디의 사용자 이름이 자동적으로 표기됩니다.
  - IV. 언어 - 어드민에서 사용할 언어를 선택합니다.
  - V. 목록 개수 - 모니터링, 규칙 등 목록으로 보이는 메뉴에서 한 화면에 출력할 목록 수를 선택합니다.
  - VI. 통계 출력 그래프 종류 - 통계 화면에 출력되는 그래프 종류를 선택합니다.
    - i. 꺾은선 그래프 - 각 항목의 변화 추이를 확인하고 싶을 때 선택합니다.
    - ii. 막대 그래프 - 항목별 비교를 하고 싶을 때 선택합니다.
  - VII. 세션 유지 시간 - 관리자가 로그인 후, 정해진 시간동안 입력이 없으면 자동 로그 아웃할 시간을 선택 또는 입력합니다.
4. 입력이 완료되면, **추가**를 클릭합니다.

## 관리자 수정

관리자 목록에서 관리자 정보를 수정합니다.

1. 시스템 어드민의 **[관리자]**를 클릭합니다.
2. 관리자 목록에서 수정하려는 관리자 아이디를 클릭합니다.
3. 관리자 수정화면으로 이동합니다. 정보를 수정합니다.
4. 수정이 완료되면, **수정**을 클릭합니다.



회사를 추가하면 mailadm이 시스템 관리자로 자동으로 등록됩니다. 이 계정은 수정할 수 없습니다.

## 관리자 삭제

관리자 목록에서 관리자 정보를 삭제합니다.

1. 시스템 어드민의 **[관리자]**를 클릭합니다.
2. 관리자 목록에서 삭제하려는 관리자를 선택한 후, 목록 상단에 있는 **삭제**를 클릭합니다.



사이트를 추가하면 mailadm이 시스템 관리자로 자동으로 등록됩니다. 이 계정은 삭제할 수 없습니다.

## 관리자 검색

관리자 목록에서 관리자를 검색합니다.

1. 시스템 어드민의 **[관리자]**를 클릭합니다.
2. 관리자 목록 오른쪽 상단에서 검색 항목을 선택합니다.
  - I. 아이디, 사용자 이름
3. 검색창에 검색어를 입력하고, **검색**을 클릭합니다.

## 10.2 관리자 로그

관리자는 시스템 관리자와 사이트 관리자로 나뉘어 관리됩니다. 각 관리자가 로그인한 후, 화면을 통해서 작업한 내역에 대한 로그를 저장 및 모니터링하여 관리의 혼선을 방지하고, 각 관리자의 책임 소재를 분명히 할 수 있습니다.

관리자 로그의 목록 구성 및 검색방법은 다음과 같습니다.

### 관리자 로그 목록

관리자들이 작업한 내역을 처리 시간 순으로 확인할 수 있습니다. 관리자 로그 목록 항목은 다음과 같습니다.

- 시간 - 관리자가 '관리 내역'을 처리한 시간
- 관리자 ID - 해당 작업을 실행한 관리자의 ID
- 접속 IP - 해당 작업을 실행한 관리자의 접속 IP
- 관리 내역 - 관리자가 실행한 내역 경로
- 재시도 - 관리자가 실패한 작업 내역인 경우 재시도

### 관리 내역 검색

관리자 ID 및 접속 IP로 관리 내역을 검색할 수 있습니다.

1. 시스템 어드민의 **[관리자 > 관리자 로그]**를 클릭합니다.
2. 관리자 목록 오른쪽 상단에서 검색 항목을 선택합니다.
  - I. 관리자 ID, 접속 IP
3. 검색어를 입력한 후, **검색**을 클릭합니다.

# DaouOffice 시스템 어드민 가이드