중소기업 기술 유출 방지 IT 보안 가이드라인

실무자 편

국가정보원 중소벤처기업부

중소기업 기술 유출 방지
IT 보안 가이드라인

2023.12

들어가며

2023년 기준, 대한민국의 중소기업은 국내 전체 기업의 99.9%를 차지하며 우리 경제 전반을 책임지고 있습니다. 하지만 많은 중소기업이 정보보호에 투자할 재정적 여유가 부족해 보안 시스템을 갖추지 못하고 있거나, 보안 책임자가 부재한 상황에 놓여 있습니다.

「중소기업 기술 유출 방지 IT 보안 가이드라인」은 이처럼 보안 사각지대에 있는 중소기업을 위해 작성되었습니다. 정보보호 전문가가 부족한 중소기업의 현실을 고려하여 업무상 많이 활용되는 IT장비의 보안 설정에 대해 쉽고 자세히 설명하고자 노력하였습니다. 중소기업에서 많이 사용하는 제품을 위주로 작성하였고, 추가 비용 없이 따라할 수 있는 기본적인 내용을 담았습니다.

해킹에 의한 기술 유출은 매년 증가하고 있습니다. 중소기업도 예외는 아니며, 그렇기 때문에 이제 보안은 선택이 아닌 필수라고 할 수 있습니다. 앞으로 중소기업은 임직원들에게 안전한 근무 환경을 제공하면서 해킹을 통한 기술 유출을 예방해야 할 것입니다.

본 가이드라인을 통해 모든 중소기업의 정보보안 역량이 향상되기를 희망합니다.

목차

1

가이드라인 개요

제1장은 「가이드라인 개요」로 본 가이드라인에 대하여 전체적으로 소개합니다. 가이드라인의 작성 배경과 이를 통해 얻고자 하는 기대 효과에 대하여 서술하며, 가이드라인의 구성을 설명하여 이를 어떻게 활용하면 좋을지 안내합니다.

가이드라인 작성 배경

한국인터넷진흥원에 따르면 민간 분야에 대한 사이버 침해 신고는 최근 5년간 계속 증가하고 있습니다. 2019년 418건이었던 신고건수는 매년 증가하여 2022년에는 1,142건이 집계되었고, 올해 2023년에는 상반기에만 890건이 집계되어 관련 피해가 상당할 것으로 예상됩니다.

기업을 향한 해킹 공격은 대부분 산업기술을 탈취하려는 목적으로 일어나고 있습니다. 21세기 글로벌 경쟁시대에 산업기술은 기업과 국가 경쟁력을 좌우하는 핵심 요소로 작용하고 있으며, 산업기술 유출은 피해 기업은 물론 국가경쟁력까지 훼손할 수 있습니다.

현재 사이버 침해사고로 인한 피해는 대부분 중소기업에 집중되어 있습니다. 그 이유는 다수의 중소기업이 정보보안 전문 인력과 관련 예산을 갖추지 못한 경우가 많기 때문입니다. 이는 우리 중소기업이 해킹을 통한 산업기술 유출에 매우 취약한 상태임을 의미합니다.

해킹에 의한 산업기술 유출 위협으로부터 우리 중소기업을 지키고, 국내산업의 경쟁력을 강화하기 위해서는 기술 보호에 대한 국가적·국민적 관심이 절실히 필요합니다. 본 가이드라인은 이러한 문제의식 속에서 작성되었습니다. 중소기업이 보안에 투자할 재정적 여력이 부족하다는 점에 중점을 두어, 별도의 비용 없이 기존에 사용하고 있는 IT 장비에 대한 보안 설정 방법에 대하여 안내합니다. 본 가이드라인을 통해 중소기업 내 IT 인프라 보안 역량이 향상되기를 기원합니다.

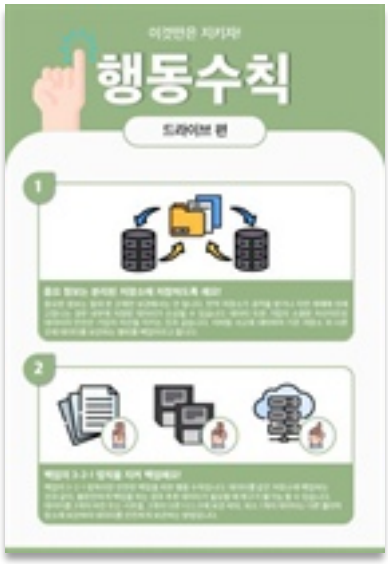
2023년 12월
산업기밀보호센터

가이드라인 구성

01. 내용 구성

행동 수칙

「행동 수칙」은 업무 중 IT 장비를 다룸에 있어서 알아 두어야 할 일반적인 행동 지침을 포스터로 설명하고 있습니다. 기술적인 내용보다는 사용자의 행동에 초점을 두어, 업무를 수행하면서 기억하면 좋을 기본적인 보안 수칙 위주로 작성되었습니다. 이를 출력하여 배부하거나, 보기 좋은 곳에 게시하여 기업 임직원에게 지속적으로 노출한다면 모든 구성원의 보안 인식 향상에 도움이 될 것입니다.



가이드라인 구성

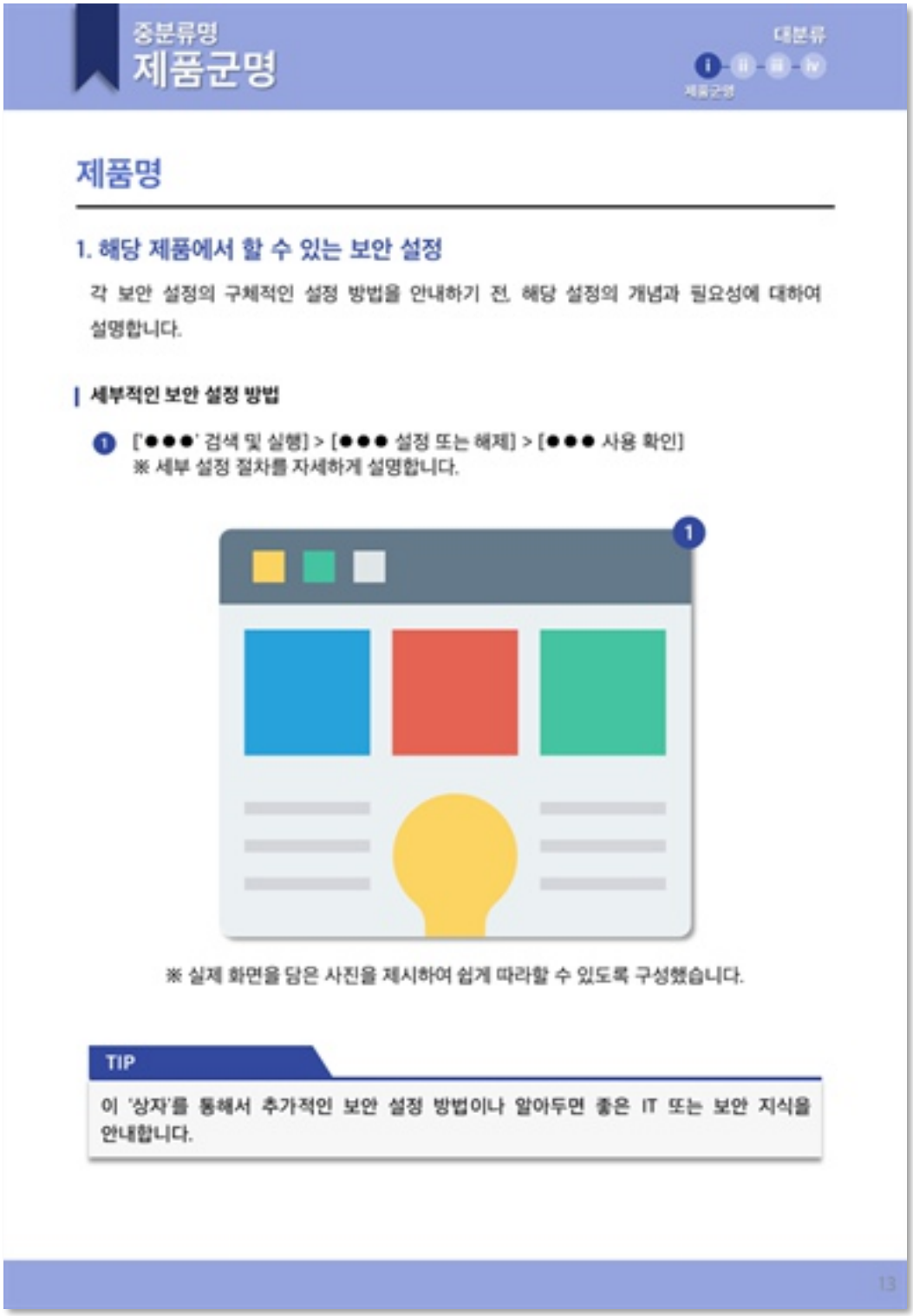
설정 방안

「설정 방안」은 IT 제품에 대한 설명과 함께, 개별적인 장비에서 할 수 있는 보안 설정 방법을 상세하게 안내합니다. 해당 제품에 대한 기술적인 지식이 없는 사람도 바로 따라 할 수 있도록 실제 화면을 담았고, 설정 방법 또한 자세하게 서술하였습니다.

우선 목차를 통해 기업 내에서 사용하고 있는 IT 장비를 찾아, 해당 부분에서 다루는 설정을 모두 적용하기를 권장합니다. 설정 방안에서 제시하는 보안 설정은 필수적이고 기본적인 조치입니다. 제품이 기본적으로 제공하는 보안 기능을 최대한 활용하여 발생할 수 있는 보안 문제를 기술적으로 예방할 수 있게 하고자 하였습니다.

가이드라인 구성

가이드라인 구성 예시



가이드라인의 기대 효과

사람들은 일반적으로 해킹 사고를 막기위해 고가의 장비나 전문적인 도움이 필요하다고 인식하며, 정보보호는 나와 관련 없는 일이라 생각합니다. 하지만 알려진 것 이상으로 침해사고는 주변에서 빈번하게 일어나고 있으며, 이는 기본적인 보안조치 만으로도 충분히 예방이 가능합니다.

본 가이드라인은 별도의 보안 장비나 전문 인력 없이 누구나 따라할 수 있는 내용들로 구성되어 있습니다. 가이드라인을 통해 기업의 보안 수준을 빠르게 끌어올릴 수 있기를 희망하며, 정보보호의 중요성에 대한 인식이 널리 퍼지기를 기대합니다.

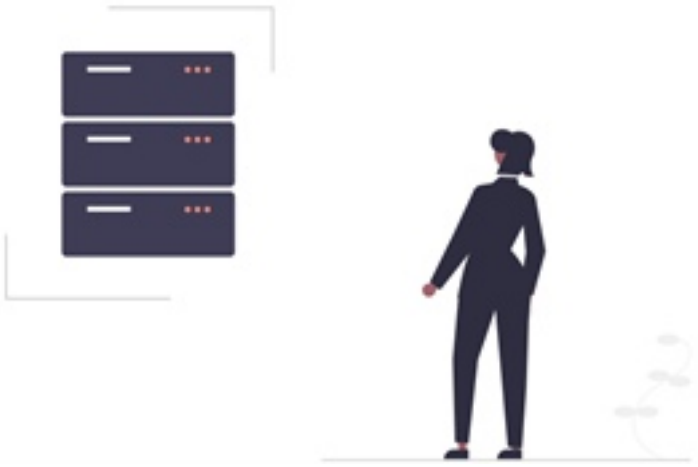
2

정보보호 실무자 보안수칙

제2장은 「정보보호 실무자 보안수칙」으로 기업 내 전산담당자 또는 정보보호담당자가 수행해야 할 사항에 대해 다룹니다. 기술적인 서버, DB, 저장소와 같은 기업 내 IT 인프라 장비와 소프트웨어에서 적용해야 할 보안 설정에 대하여 설명합니다. 본 장에서 권장하는 사항을 준수한다면 기업 내 IT 인프라의 전체적인 보안수준을 높일 수 있을 것입니다.

제2장 정보보안 실무자 보안수칙

I. 서버



이것만은 지키자!

행동수칙

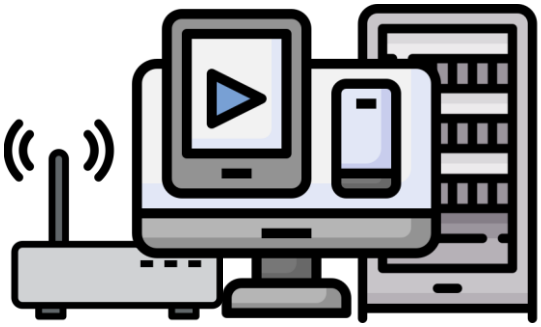
공통 편

1

비밀번호를 주기적으로 변경해요!

공격자의 공격(무차별 대입 공격, 사전 공격 등)에 의해 비밀번호가 노출될 수 있으므로, 비밀번호를 주기적으로 변경하여 사이버 침해사고를 예방하여야 합니다.

2



소프트웨어를 주기적으로 업데이트해요!

소프트웨어 업데이트는 소프트웨어 공급자가 제공하는 가장 저렴하고 효과적인 보안 수단입니다. 서버의 부하가 적은 시간대에 정기적인 업데이트 일정을 설정하여 업데이트를 진행해야 합니다.

이번 장에서는 서버용 운영체제인 윈도우즈 서버와 리눅스에 대하여 다룹니다. 운영체제에서 제공하는 파일 권한 관리, 시스템 계정 관리와 같은 보안 설정을 통해서 서버를 안전하게 관리하는 방법에 대해서 설명합니다.

서버 운영체제란 무엇인가요?

서버 운영체제는 서버용 컴퓨터를 작동시키고 관리하기 위한 시스템 소프트웨어입니다. 서버 컴퓨터 또한 개인용 PC와 마찬가지로 윈도우와 같은 운영체제가 필요하며, 서버에서 제공하는 서비스 또한 운영체제를 통해 작동됩니다.

서버 관리가 중요한 이유는 무엇인가요?

서버 시스템은 조직 내 IT 인프라의 핵심으로 많은 인원이 서버를 통해 업무를 수행합니다. 따라서 서버 시스템이 손상되는 경우 업무 수행에 지장을 줄 수 있습니다. 또한 서버 컴퓨터는 영업데이터 같은 중요 정보를 처리하기 때문에 관리 미흡으로 인해 정보가 유출되는 경우 회사에 큰 피해를 가져올 수 있습니다.

가이드라인에서 다루는 제품 확인하기

Windows Server 2022

▲ 윈도우즈 서버 2022

▲ 리눅스

윈도우즈 서버(Windows Server)

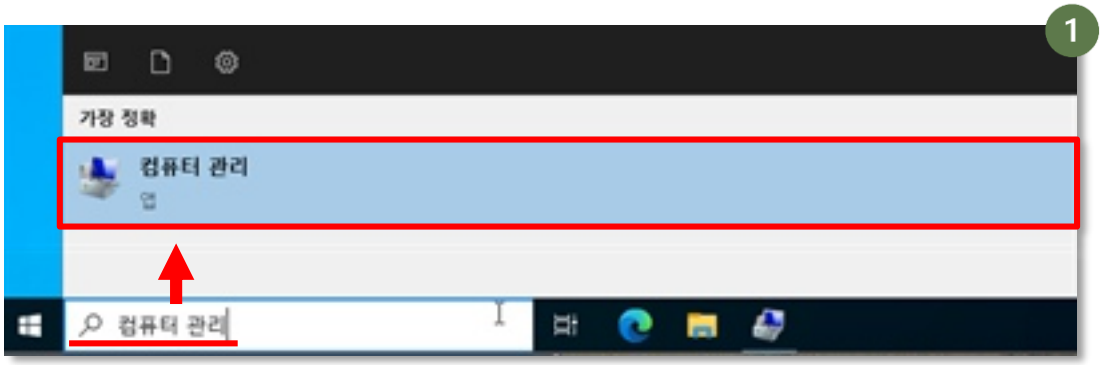
1. 관리자 계정 보안설정하기

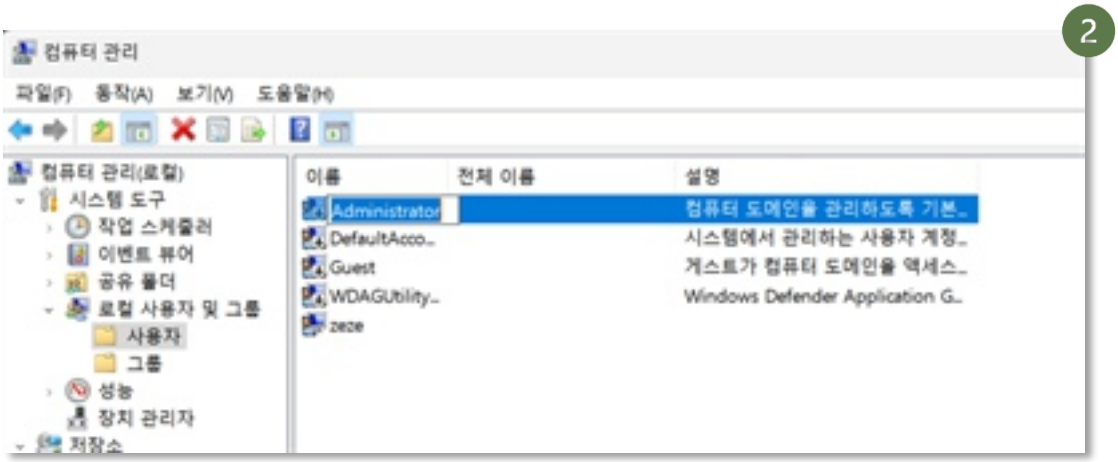
서버의 관리자 계정은 공격자들이 주요 목표로 삼는 대상입니다. 관리자 계정은 시스템에서 모든 작업을 수행할 수 있는 권한을 가지고 있습니다. 공격자가 관리자 계정을 탈취한 경우 시스템을 완전히 제어할 수 있기 때문에 관리자 계정은 특별한 관리가 필요합니다.

관리자 계정 이름 변경하기

관리자 계정의 존재를 숨기는 것 만으로도 보안에 큰 도움이 됩니다. 윈도우 서버의 기본 관리자 계정명인 'Administrator'를 추측하기 힘든 다른 이름으로 변경해야 합니다.

1. ['컴퓨터 관리' 검색 및 실행]
2. [시스템 도구] > [로컬 사용자 및 그룹] > ['사용자' 클릭] > ['Administrator' 클릭] > ['F2' 누르기] > [계정 이름 변경]



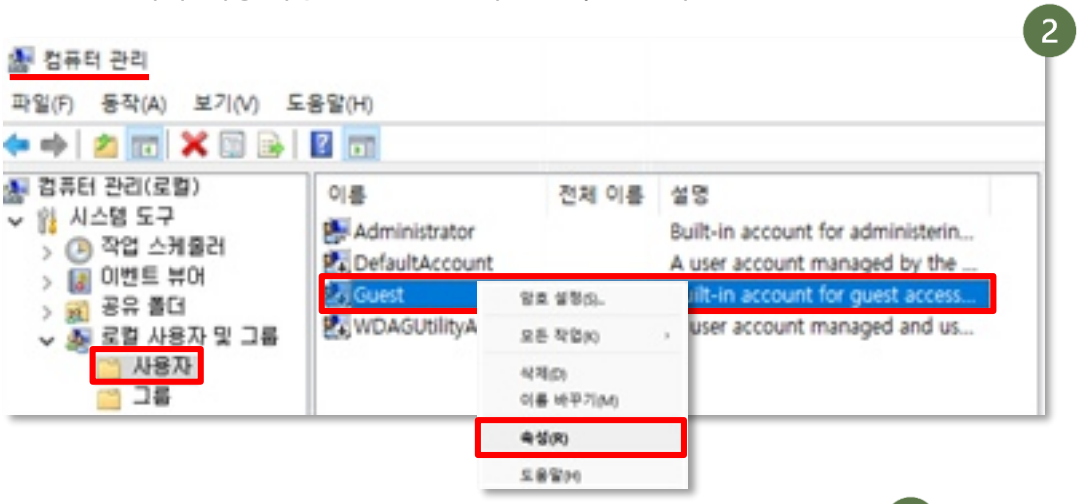


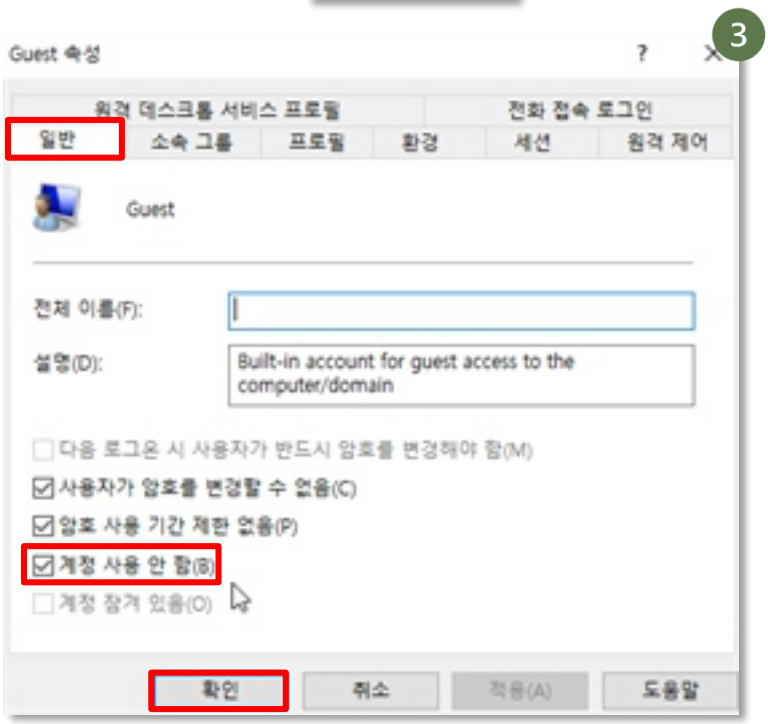
윈도우즈 서버(Windows Server)

게스트 계정 사용 안 함 설정하기

Guest 계정은 외부 사용자가 시스템에 잠시 접근할 수 있게 해주는 손님용 계정입니다. 시스템 설치시 기본으로 주어지는 기능 중 하나이지만, 공격을 위해 악용되는 경우가 많기 때문에 비활성화 하여야 합니다.

1. ['컴퓨터 관리' 검색 및 실행]
2. [시스템 도구] > [로컬 사용자 및 그룹] > ['사용자' 클릭] > ['Guest' 계정 우클릭 후 '속성' 클릭]
3. [일반 탭에서 '계정 사용 안 함(B)' 선택] > ['확인' 클릭]





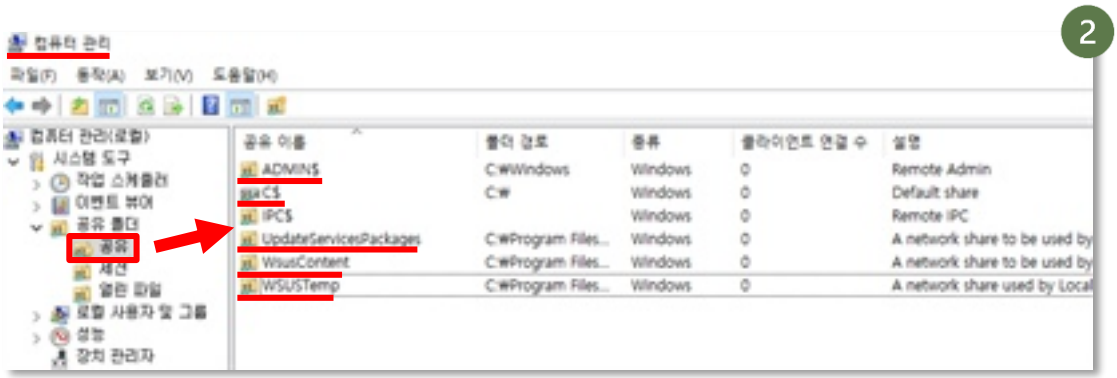
윈도우즈 서버(Windows Server)

2. 공유 폴더 사용 금지하기

공유 폴더는 같은 네트워크 안의 컴퓨터들과 파일을 공유할 수 있는 기능입니다. 서버 PC는 일반적으로 공유 폴더 기능 사용이 권장되지 않으니 비활성화 해야 합니다.

공유 폴더 사용 금지하기

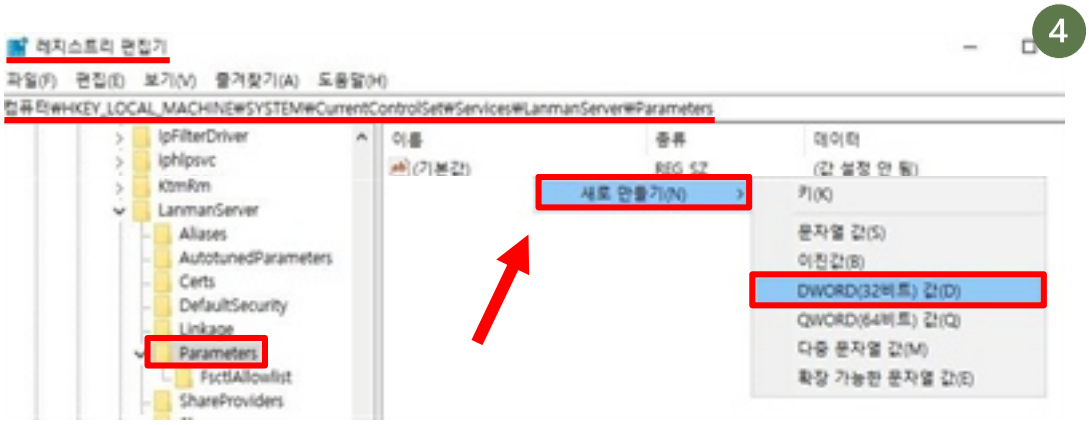
1. ['컴퓨터 관리' 검색 및 실행]
2. [시스템 도구] > [공유 폴더] > ['공유' 클릭] > ['IPC$'를 제외한 모든 항목 삭제]



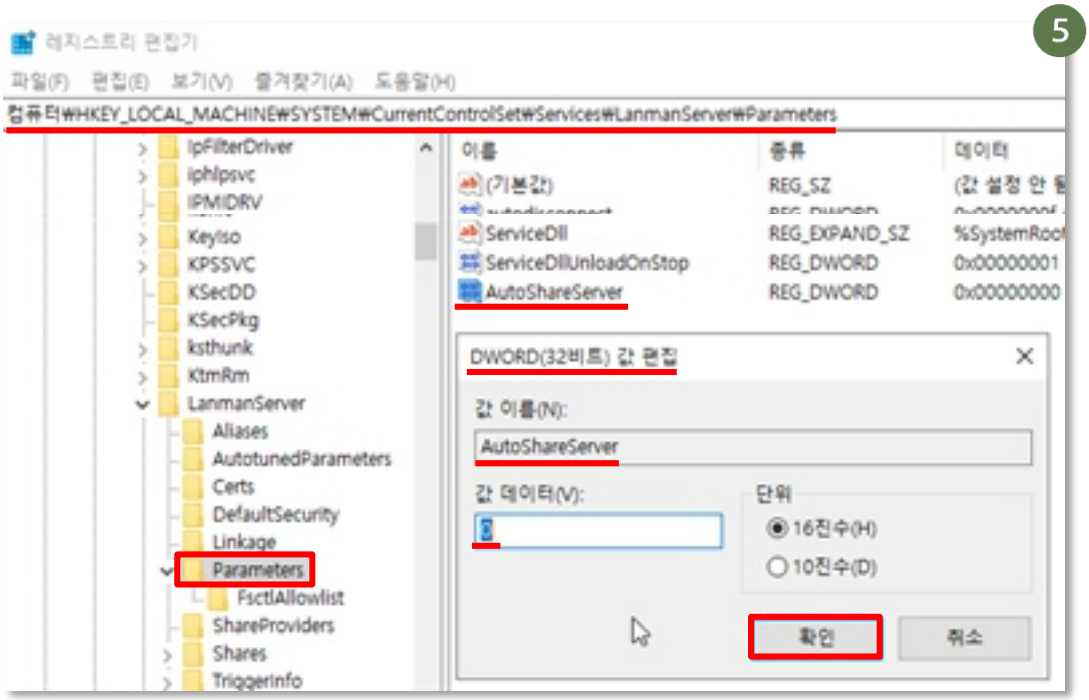
3. ['레지스트리 편집기' 검색 및 실행]

윈도우즈 서버(Windows Server)

4 ['컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' 이동] > [마우스 우클릭 후 '새로 만들기' 클릭] > ['DWORD(32비트) 값' 클릭] > [새 파일 이름 'AutoShareServer'로 변경]



5 ['AutoShareServer' 값 데이터 '0'으로 변경] > ['확인' 클릭]



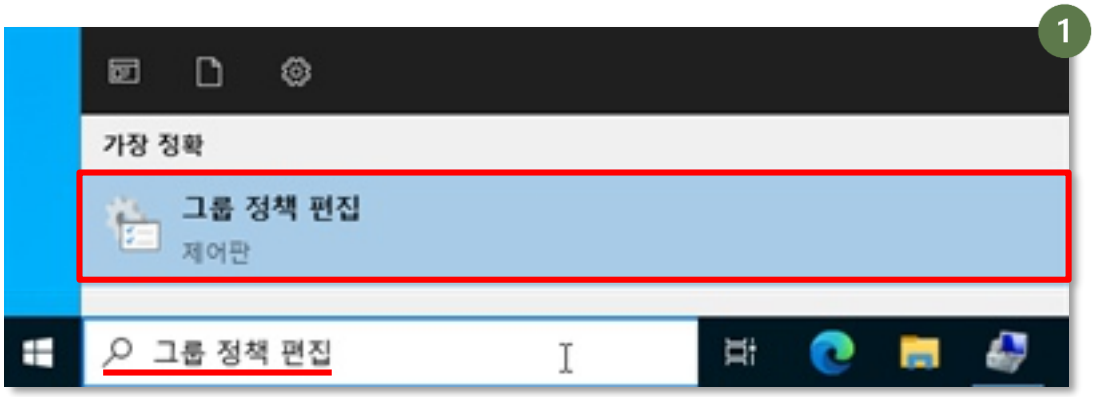
윈도우즈 서버(Windows Server)

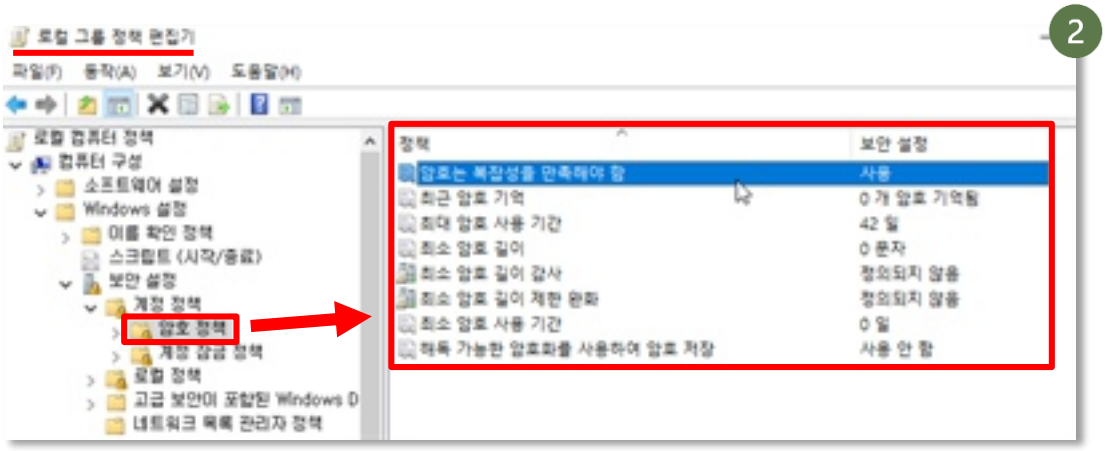
3. 안전한 계정정책 사용하기

시스템 계정이 안전하게 관리될 수 있도록 계정정책을 설정해야 합니다. 복잡한 비밀번호를 갖도록 강제하거나, 원격 로그인을 금지하여 계정을 안전하게 관리할 수 있습니다.

안전한 비밀번호 정책 설정하기

1. ['그룹 정책 편집' 검색 및 실행]
2. [컴퓨터 구성] > [Windows 설정] > [보안 설정] > [계정 정책] > ['암호 정책' 클릭] > [암호 정책들을 다음 페이지 표 기준에 맞게 설정]



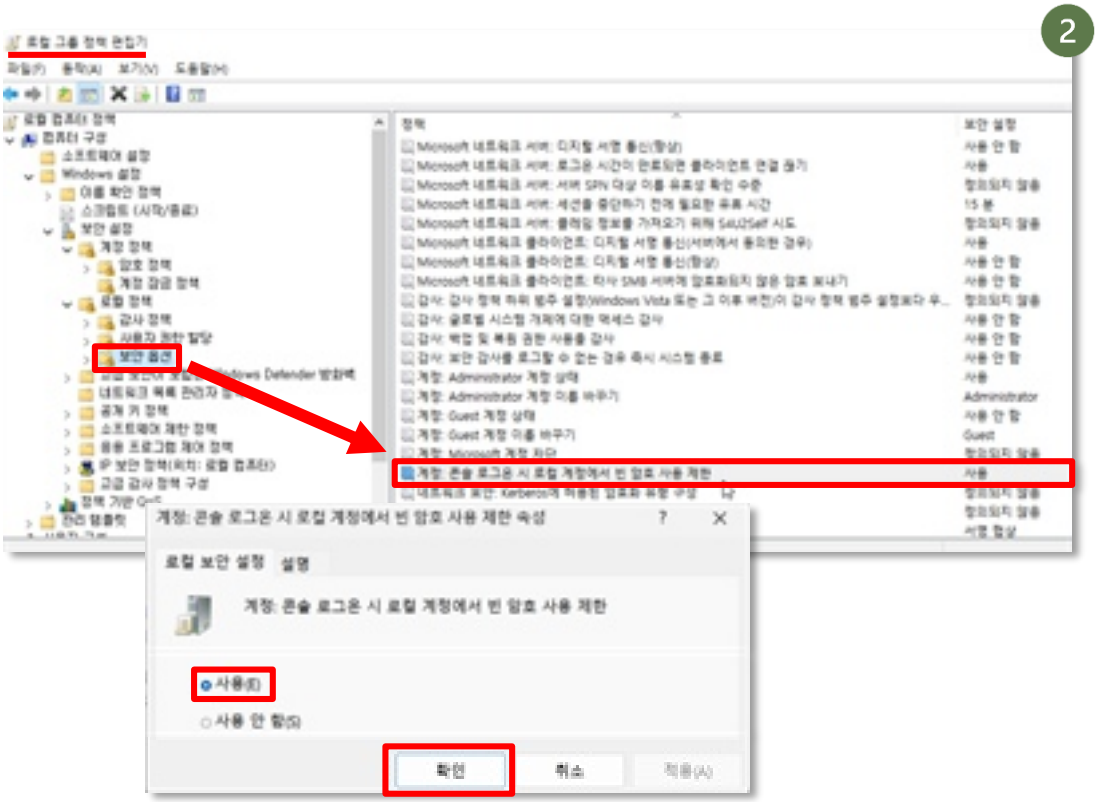


윈도우즈 서버(Windows Server)

설정항목	안전한값	상세설명
암호 복잡성 설정	활성화	영문, 숫자, 특수문자 중 2종류와 10자리 이상 조합, 또는 3종류 이상 최소 8자리 이상 조합을 사용하게 하는 설정
최근 암호 기억 속성	24개 이상	기존에 사용했던 비밀번호를 재사용하지 못하게 하는 설정
최대 암호 사용 기간	90일 이상	같은 비밀번호를 변경없이 사용할 수 있는 최대 기간 설정
최소 암호 사용 기간	1일 이상	비밀번호 변경 후 다시 변경할 수 있는 간격을 두게 하는 설정
최소 암호 길이 설정	10자 이상	비밀번호의 최소 길이 조건을 두게 하는 설정

원격 로그인 제한하기

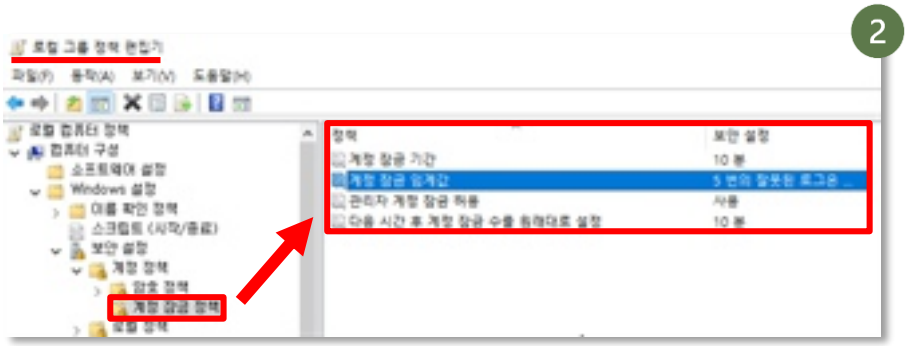
1. ['그룹 정책 편집' 검색 및 실행]
2. [컴퓨터 구성] > [Windows 설정] > [보안 설정] > [로컬 정책] > ['보안 옵션' 클릭] > ['계정: 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한' 클릭] > ['사용' 선택] > ['확인' 클릭]

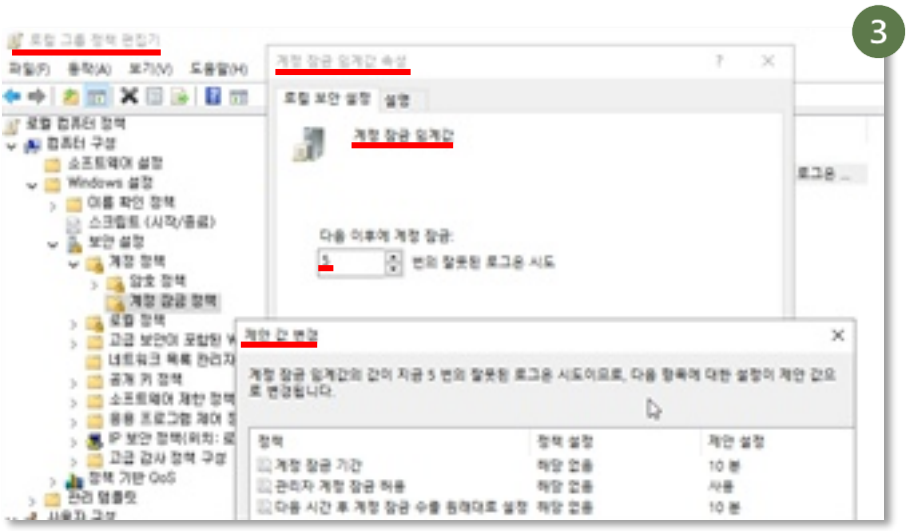


윈도우즈 서버(Windows Server)

계정 잠금 정책 사용하기

1. ['그룹 정책 편집' 검색 및 실행]
2. [컴퓨터 구성] > [Windows 설정] > [보안 설정] > [계정 정책] > ['계정 잠금 정책' 클릭]
3. [제안 값 변경 창에서 암호 정책들을 하단의 표 기준에 맞게 설정]



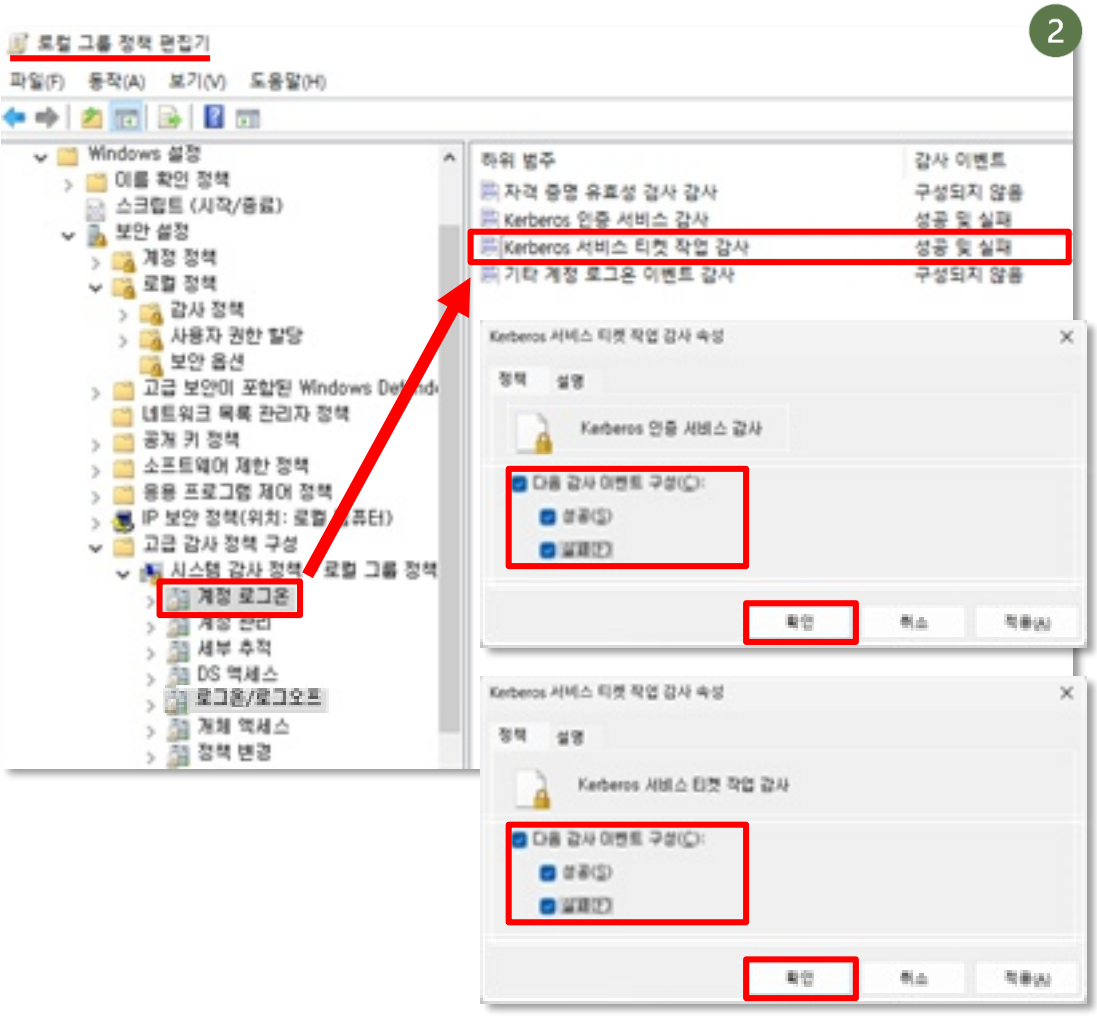


설정 항목	안전한 값	상세 설명
계정 잠금 임계값	5회 이하	최대 로그인 시도 횟수를 설정. 임계값 초과시 일정 시간 동안 계정 잠금
계정 잠금 기간	30분 이상	로그인 시도 횟수 초과시 계정 잠금 시간 설정
관리자 계정 잠금 허용	사용	관리자 계정에 계정 잠금 정책이 적용되는지 여부 설정
다음 시간 후 계정 잠금 수를 원래대로 설정	60분 이상	실패한 로그온 시도 횟수가 초기화 될 때까지 걸리는 시간을 설정

윈도우즈 서버(Windows Server)

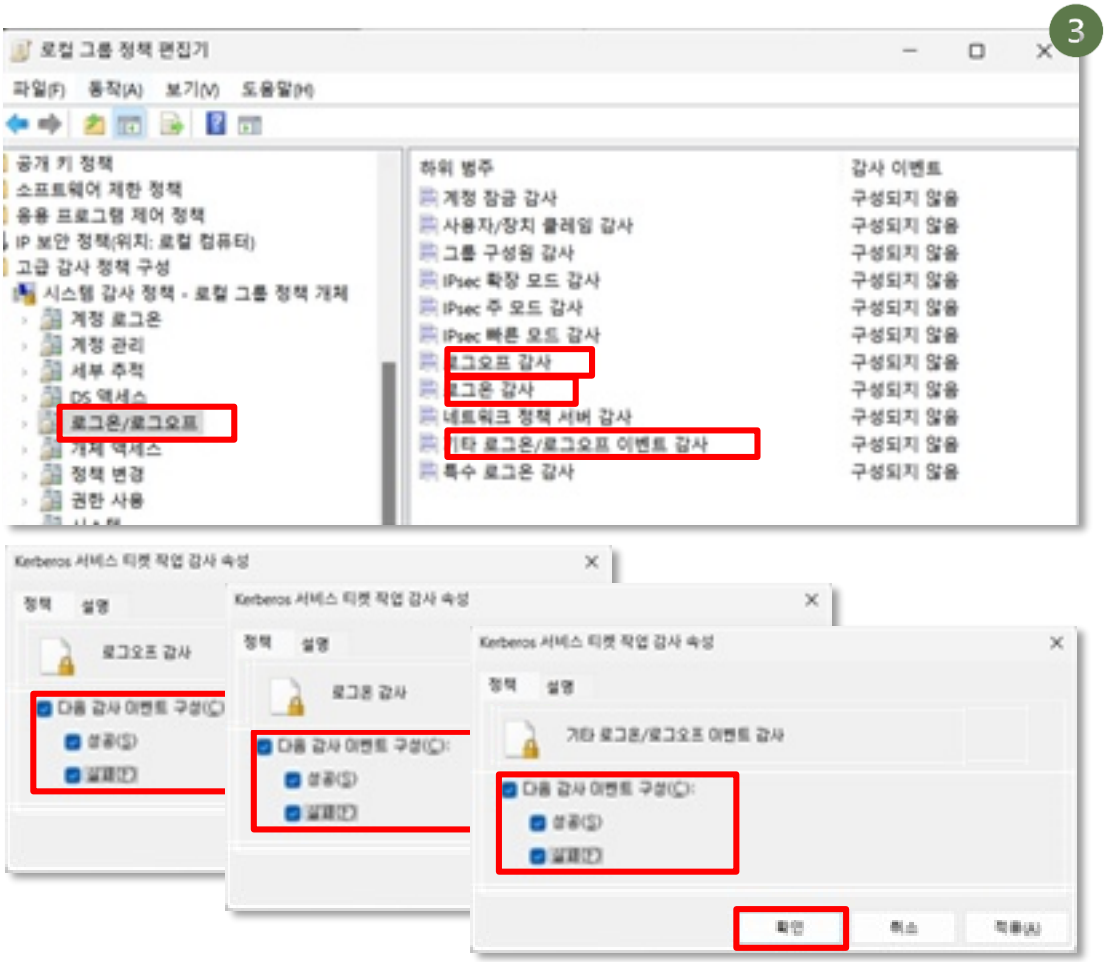
계정 로그인 시도 감지하고 기록 남기기

1. ['그룹 정책 편집' 검색 및 실행]
2. [컴퓨터 구성] > [Windows 설정] > [보안 설정] > [고급 감사 정책 구성] > [시스템 감사 정책-로컬 그룹 정책] > ['계정 로그온' 클릭] > ['Kerberos 인증 서비스 감사', 'Kerberos 서비스 티켓 작업 감사' 클릭] > ['다음 감사 이벤트 구성' 모두 선택] > ['확인' 클릭]



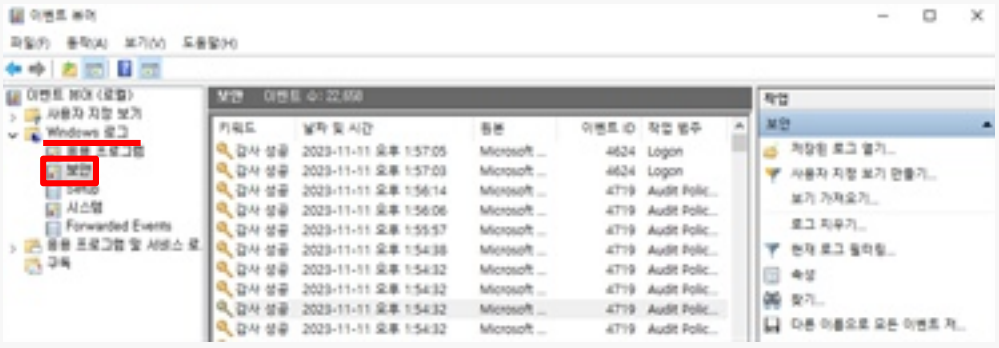
윈도우즈 서버(Windows Server)

3 [컴퓨터 구성] > [Windows 설정] > [보안 설정] > [고급 감사 정책 구성] > [시스템 감사 정책-로컬 그룹 정책] > ['로그온/로그오프' 클릭] > ['로그오프 감사', '로그온 감사', '기타 로그온/로그오프 이벤트 감사' 클릭] > ['다음 감사 이벤트 구성' 모두 선택] > ['확인' 클릭]



저장된 로그 보는 법

계정 정책을 통해 기록된 로그는 이벤트 뷰어의 [Windows 로그] > [보안]에서 확인할 수 있습니다.



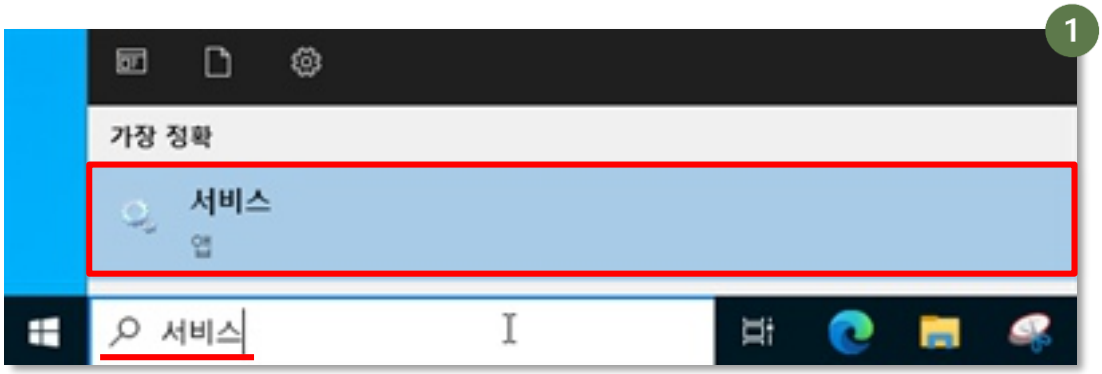
윈도우즈 서버(Windows Server)

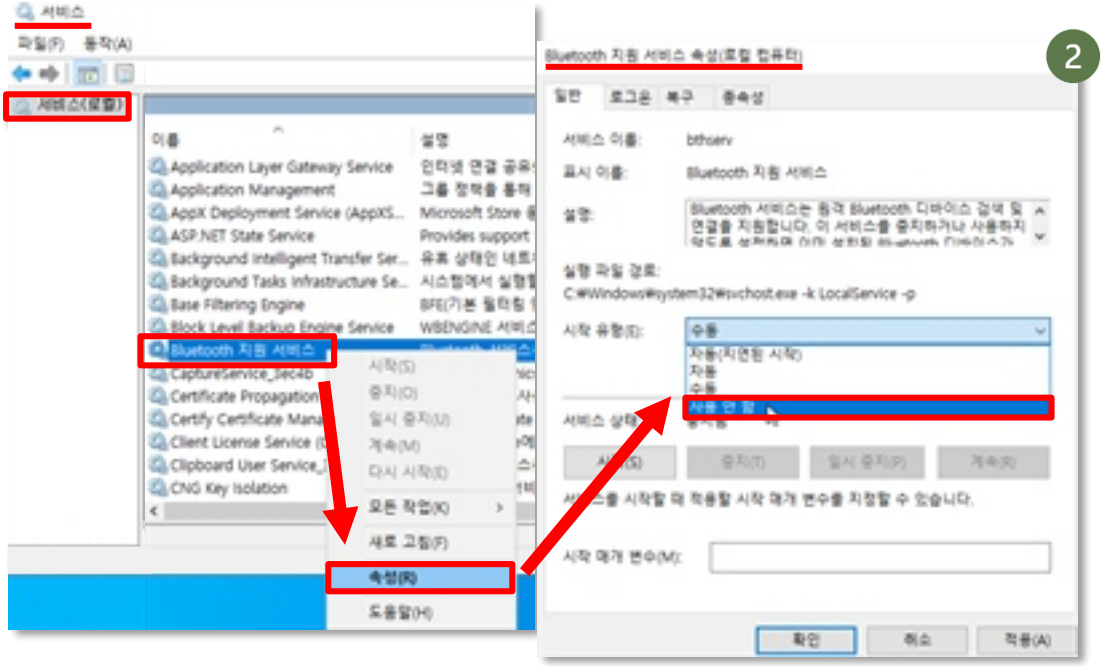
4. 안전한 시스템 설정하기

서버 운영체제에서 제공하는 보안 기능을 활성화하고, 서버 운영에 필요하지 않은 기능을 비활성화하여 시스템의 보안성을 높일 수 있습니다.

일반적으로 불필요한 기능 끄기

1. ['서비스' 검색 후 실행]
2. [다음 페이지 표에 기재된 서비스 목록 참고하여 '사용 안 함' 설정]



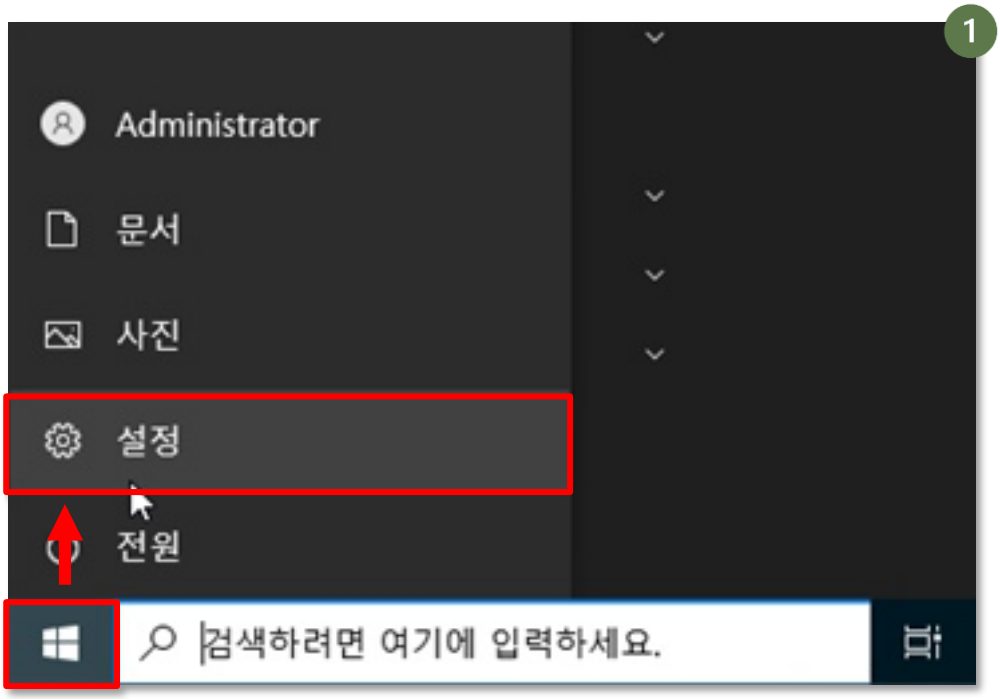


윈도우즈 서버(Windows Server)

사용 중지 필요 서비스명	상 세 설 명
Bluetooth 지원 서비스	서버 PC가 블루투스 기능을 이용하지 않는 경우 불필요
Clipbook	Clipbook 기능을 별도로 이용하지 않는 경우 불필요
Distributed Link Tracking Client Server	액티브 디렉터리를 이용하지 않는 경우 불필요
Netmeeting Remote Serial Number	넷미팅 기능을 이용하지 않는 경우 불필요
Print Spooler	서버 PC가 출력기기에 연결되지 않는 경우 불필요
Remote Registry	원격 레지스트리 설정 기능을 이용하지 않는 경우 불필요

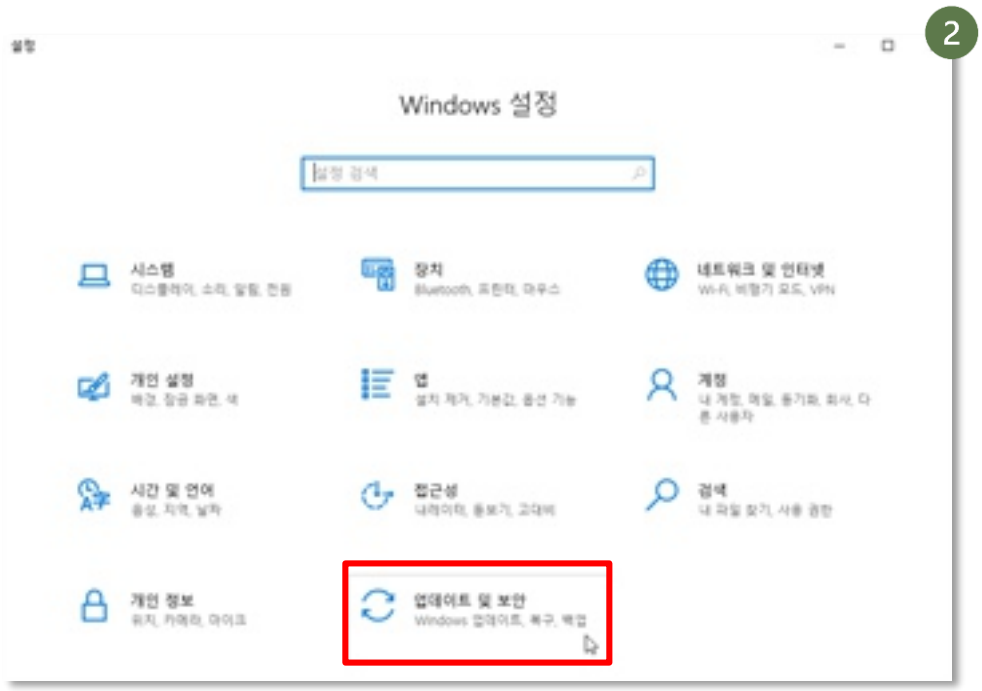
윈도우 보안 설정 활성화 하기

1 ['시작' 클릭] > ['설정' 클릭]

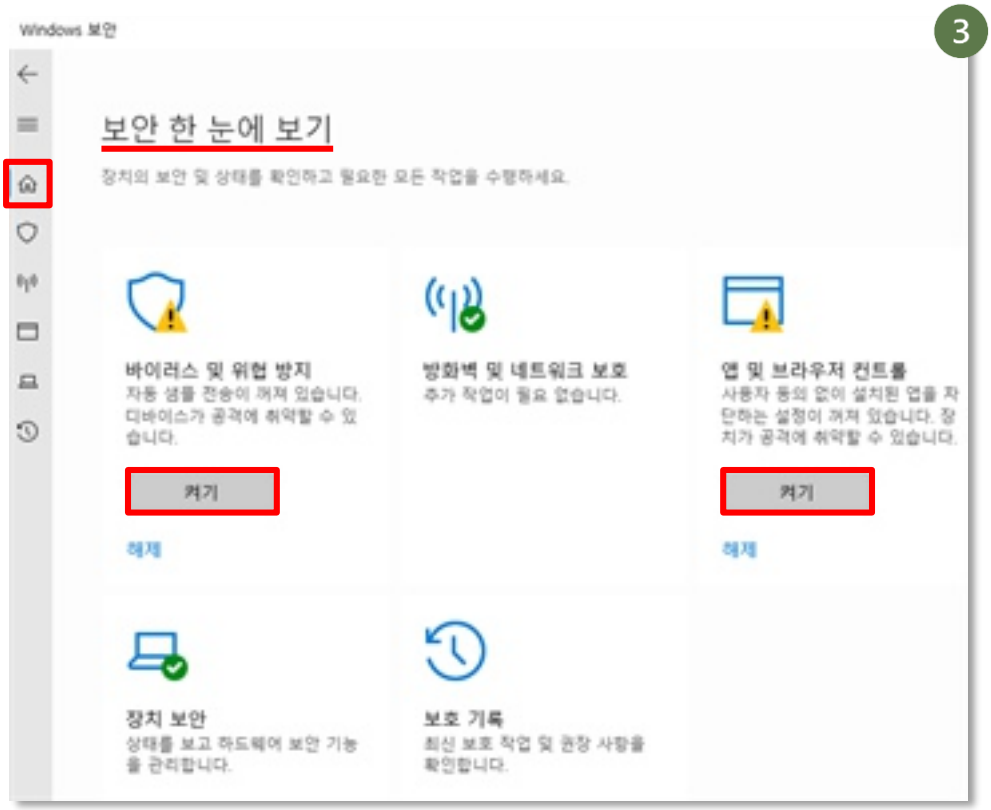


윈도우즈 서버(Windows Server)

2 ['업데이트 및 보안'클릭]



3 ['보안 한 눈에 보기'의 모든 보안설정 활성화]



리눅스(Linux)

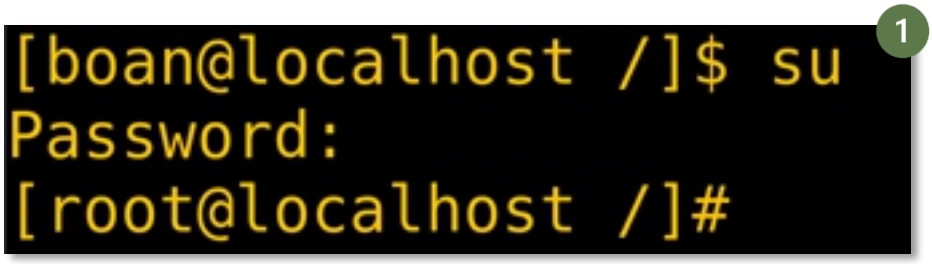
0. 관리자 권한으로 변경하기

리눅스 서버의 보안 설정들은 기본적으로 root 권한을 필요로 합니다. 이를 위해 su 명령어를 사용해 root 계정으로 전환할 수 있습니다. 하지만 root 계정은 리눅스에서 가장 높은 권한을 가지기 때문에 보안 위협의 대상이 될 수 있습니다. 따라서 설정을 마친 이후에는 다시 일반 사용자 계정으로 전환해야 합니다.

root 계정으로 전환하기

1. ['터미널' 실행] > ['su' 명령어를 통한 root 계정 전환] > [root 패스워드 입력]
   *입력 중인 패스워드는 안 보이는게 정상

```
$ su
```

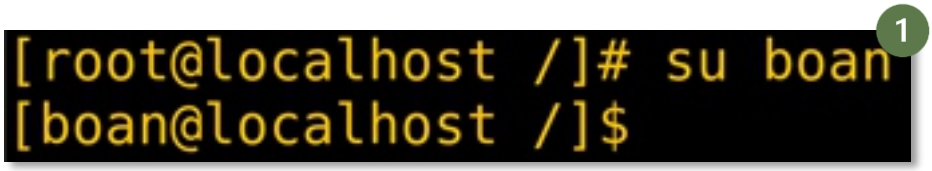


사용자 계정으로 다시 전환하기

보안 설정이 모두 끝난 후 root 권한을 반납해야 합니다.

1. ['터미널' 실행] > ['su' 명령어를 통한 사용자 계정 전환]

```
# su [사용자 계정 이름]
```



리눅스(Linux)

root 권한은 필요할 때만 사용하기

리눅스 서버에 항상 root 계정으로 로그인하는 것은 굉장히 위험합니다.

root 계정은 리눅스 시스템에서 가장 높은 권한을 가지는데, 이는 시스템의 모든 파일에 접근, 수정, 삭제가 가능함을 의미합니다. root 권한은 매우 강력하기 때문에 시스템 관리에 필요한 경우에만 사용하는 것이 바람직합니다.

사용자 계정 추가하기

1. ['터미널' 실행] > [하단의 'useradd' 명령어를 통한 사용자 계정 추가] > [하단의 'passwd' 명령어를 통한 비밀번호 설정] > [비밀번호 입력] > [비밀번호 재입력]

```
# useradd [사용자 계정 이름]
# passwd [사용자 계정 이름]
```

1

```
[root@localhost /]# useradd boanlove
[root@localhost /]# passwd boanlove
Changing password for user boanlove.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Useradd 명령어의 추가 설정 옵션

- useradd -d [디렉터리 경로] [사용자 계정 이름]: 홈 디렉터리를 지정할 수 있습니다.
- useradd -g [그룹 ID] [사용자 계정 이름]: 사용자가 소속될 그룹을 지정할 수 있습니다.
- useradd -u [사용자 ID] [사용자 계정 이름]: 사용자 고유번호를 지정할 수 있습니다.

리눅스(Linux)

사용자 계정 삭제하기

1. ['터미널' 실행] > [하단의 'userdel' 명령어를 통한 사용자 계정 삭제] > ['su' 명령어를 통한 삭제 확인]

```
# userdel -r [사용자 계정 이름]
# su [사용자 계정 이름]
```

```
[root@localhost /]# userdel -r boanlove
[root@localhost /]# su boanlove
su: user boanlove does not exist
```

계정 삭제가 필요한 경우

직원이 퇴사하거나 특정 프로젝트가 종료된 뒤 불필요해진 계정을 적절히 관리하지 않으면, 계정이 시스템 내에 계속 남아있습니다. 공격자는 이렇게 방치된 계정을 이용해 회사 시스템에 무단으로 접근하여 데이터를 유출하는 등 악의적인 행위를 할 수 있습니다.

리눅스(Linux)

1. 계정 보안 설정하기

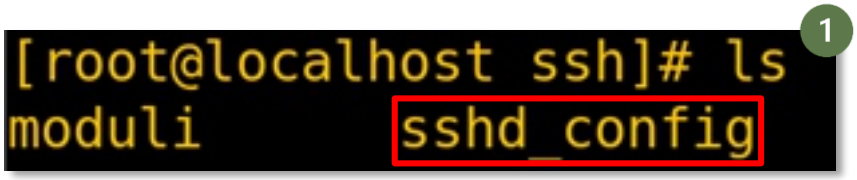
계정은 서버에 접근하는 수단입니다. 서버의 민감한 데이터를 안전하게 관리하기 위해서는 계정 보안을 설정해야 합니다. 이번 장에서는 서버의 계정 보안을 위해 할 수 있는 원격 접속의 제한, 비밀번호 복잡성 설정에 관해 설명합니다.

root 계정의 원격 접속 제한 설정하기

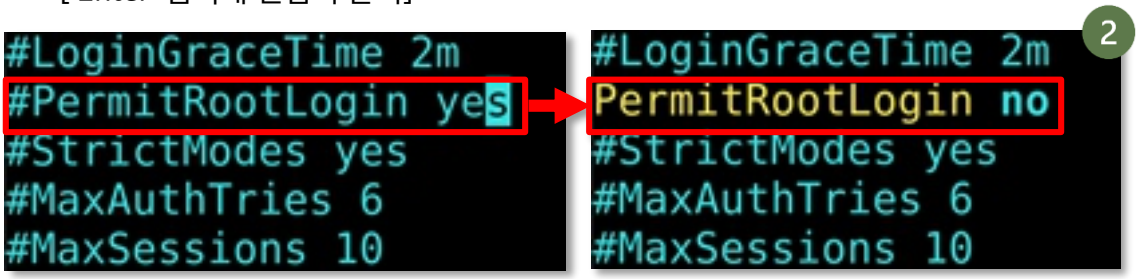
ssh 서비스의 설정 파일인 sshd_conf 파일을 수정하여 root 계정의 원격 접속을 제한할 수 있습니다.
* ssh 서비스를 사용하지 않는다면, 다음 항목으로 넘어가시면 됩니다.

1. ['터미널' 실행] > [하단의 'ls' 명령어로 /etc/ssh/ 경로에 sshd_config 파일 확인] > [하단의 'vi' 명령어로 'sshd_conf' 파일 열기]

```
# ls -l /etc/ssh/sshd_conf
# vi /etc/ssh/sshd_config
```



2. ['/PermitRootLogin'를 입력하여 옵션 검색] > ['i'를 통해 입력모드 진입] > [PermitRootLogin 설정 값을 'no'로 변경] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]



root 계정을 보호해야 하는 이유

리눅스 시스템에서 root 계정은 가장 높은 권한을 가진 계정입니다. 이 계정을 통해 시스템 설정 변경, 파일 수정 및 삭제, 사용자 계정 관리 등 모든 작업을 수행할 수 있기 때문에 원격에서 무단으로 접근할 수 있다면, 시스템 전체가 위험에 처하게 될 수 있습니다.

그렇기 때문에 root 계정의 원격 접속을 제한하는 것은 서버의 보안성을 높이는 첫걸음입니다.

리눅스(Linux)

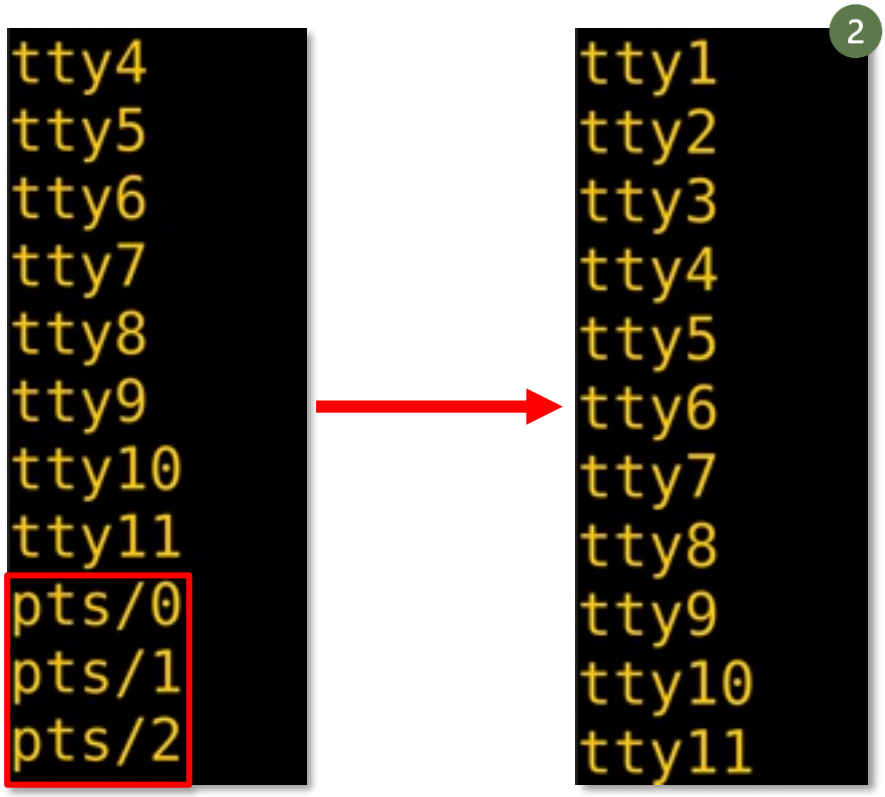
telnet 계정의 원격 접속 제한설정하기

securetty 파일을 수정하여 원격 접속에 사용되는 telnet 서비스를 제한할 수 있습니다.

1. ['터미널' 실행] > [하단의 'ls' 명령어로 /etc 경로에 'securetty' 파일 확인] > [하단의 'vi' 명령어로 'securetty' 파일 열기]

```
# vi /etc/securetty
```

2. ['/pts'를 입력하여 검색] > ['i'를 통해 입력모드 진입] > ['pts/n' 값 전부 삭제] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]



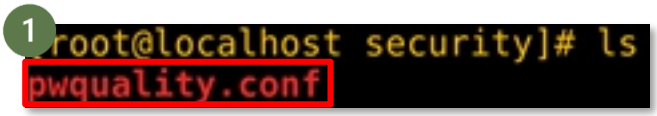
리눅스(Linux)

비밀번호 복잡성 설정하기

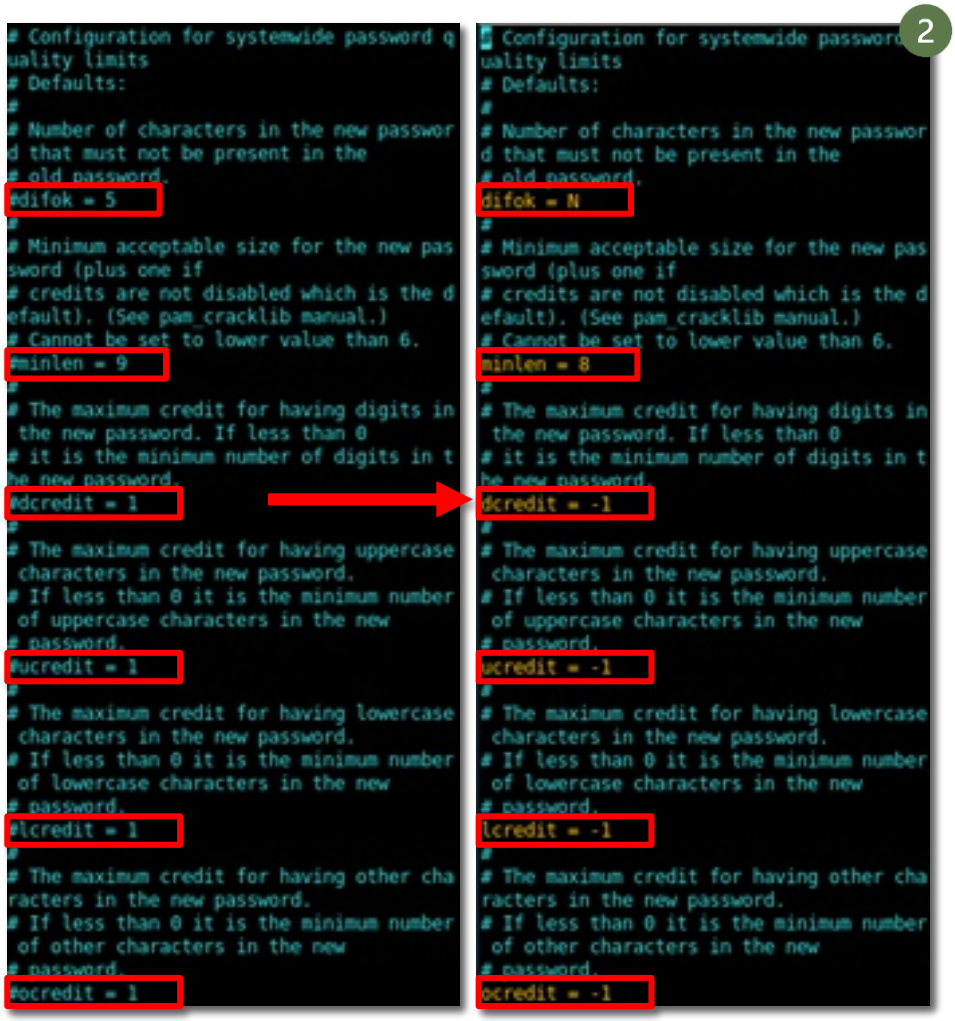
비밀번호 복잡성 설정을 통해 계정의 보안성을 더욱 높일 수 있습니다.

1. ['터미널' 실행] > [하단의 'ls' 명령어로 /etc/security 경로에 'pwquality.conf' 파일 확인] > [하단의 'vi' 명령어로 'pwquality.conf' 파일 열기]

```
# vi /etc/security/pwquality.conf
```



2. ['i'를 통해 입력모드 진입] > [각각의 항목 맨 앞 '#'을 제거하여 주석 제거 및 하단의 표를 참고하여 값 변경] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]



리눅스(Linux)

권장 값	기능	설명
difok=N	**기존 비밀번호와 비교**	기본값 10(50%))
minlen=8	**최소 비밀번호 길이 설정**	최소 8자리 이상 설정
dcredit=-1	**최소 숫자 요구**	최소 숫자 1자 이상 요구
ucredit=-1	**최소 대문자 요구**	최소 대문자 1자 이상 요구
lcredit=-1	**최소 소문자 요구**	소문자 최소 1자 이상 요구
ocredit=-1	**최소 특수문자 요구**	최소 특수문자 1자 이상 요구

리눅스(Linux)

계정 잠금 임계값 설정하기

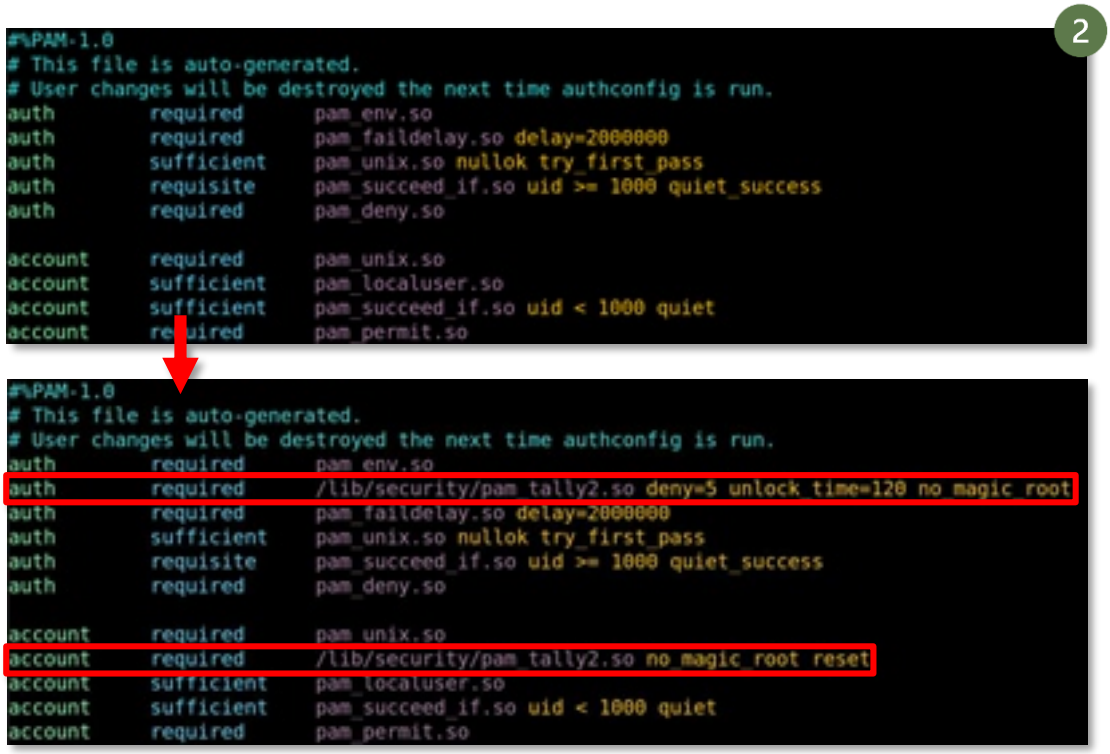
1. ['터미널' 실행] > [하단의 'ls' 명령어로 /etc/pam.d 경로에 'system-auth' 파일 확인] 혹은 ['common-auth' 파일 확인] > [하단의 'vi' 명령어로 'system-auth' 혹은 'common-auth' 파일 열기]

```
# ls /etc/pam.d
# vi /etc/pam.d/system-auth
```

2. [하단의 설정 값 추가] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]
   * auth, account 옵션의 두번째 줄에 설정 값 추가하기

추가할 설정 값

```
auth required /lib/security/pam_tally2.so deny=5 unlock_time=120 no_magic_root
account required /lib/security/pam_tally2.so no_magic_root reset
```



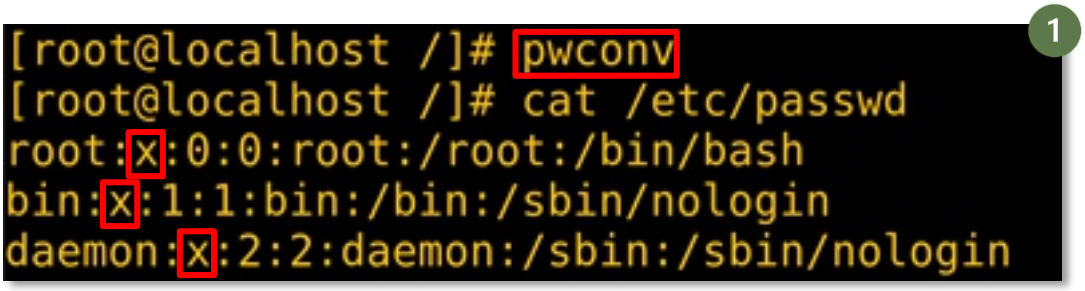
리눅스(Linux)

옵션	설명
no_magic_root	root에게는 패스워드 잠금 설정을 적용하지 않음
deny=5	5회 입력 실패 시 패스워드 잠금
unlock_time	계정 잠김 후 자동 계정 잠김 해제 시간(단위: 초)
reset	접속 시도 성공 시 실패한 횟수 초기화

비밀번호 파일 보호하기

1. ['터미널' 실행] > [하단의 'pwconv' 명령어로 패스워드 암호화 저장] > [하단의 'cat' 명령어로 'passwd' 파일의 두번째 필드 값이 'x' 인지 확인]

```
# pwconv
# cat /etc/passwd
```



비밀번호 파일 보호의 필요성

일부 오래된 시스템의 경우 /etc/passwd 파일에 비밀번호가 평문으로 저장되어 있는 경우가 있습니다. 사용자 계정 비밀번호가 암호화되어 있지 않다면, 공격자가 비밀번호 파일을 탈취하였을 때 그 안의 비밀번호도 쉽게 확인할 수 있습니다.

만약 비밀번호가 암호화되어 저장되어 있다면 공격자에 의해 비밀번호 파일이 탈취되어도 비밀번호를 알아볼 수 없기 때문에 계정의 보안을 지킬 수 있습니다.

리눅스(Linux)

2. 파일 권한 관리하기

중요한 파일이나 디렉터리에 적절한 소유자와 권한을 설정해 허용되지 않은 접근을 방지하고, 데이터를 보호할 수 있습니다. 이번 항목에서는 파일 소유자와 권한을 확인하는 법과 이를 관리하는 법 그리고 관리해야 하는 파일에 대하여 설명하겠습니다.

파일의 소유자 및 권한을 확인하는 방법

1 ['터미널' 실행] > [하단의 'ls' 명령어로 파일의 소유자 및 권한 확인]

```
# ls -l [파일 경로 및 이름]
```

예시 (/etc/passwd)

```
[root@localhost /]# ls -l /etc/passwd
-rw-r--r--. 1 root root 2304 Nov 22 22:38 /etc/passwd
```

1

리눅스에서 권한이란?

리눅스에서의 권한은 파일이나 디렉토리에 대한 사용자의 접근 수준을 설정하는 것입니다. 이러한 권한을 통해 해당 파일이나 디렉토리를 누가 볼 수 있고, 수정할 수 있으며, 실행할 수 있는지를 결정합니다. 아래는 리눅스 권한을 읽는 법과 영문, 숫자 표기법입니다.

	파일 유형	파일 소유자 권한			파일 소유 그룹 권한			기타 사용자 권한		
영문 표기법	-	r	w	x	r	w	x	r	w	x
숫자 값	-: 파일 d: 디렉토리	4	2	1	4	2	1	4	2	1
숫자 표기법		7			7			7		
권 한		읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행

리눅스(Linux)

파일의 소유자 및 권한 변경하기

1. ['터미널' 실행] > [하단의 'chown' 명령어로 파일 소유자 변경] > [하단의 'chmod' 명령어로 파일 권한 변경]

```
# chown [소유자] [파일 경로 및 이름]
# chmod [권한] [파일 경로 및 이름]
```

예시 (/etc/passwd)

1
```
[root@localhost /]# chown root /etc/passwd
[root@localhost /]# chmod 644 /etc/passwd
```

권한 변경이 권장되는 파일 목록		
설정 파일	권장 값	상 세 설 명
/etc/passwd	소유자: root 권한: 644이하	사용자의 ID, 패스워드, UID, GID, 홈 디렉터리, 쉘 정보를 담고 있는 파일
/etc/shadow	소유자: root 권한: 400이하	시스템에 등록된 모든 계정의 패스워드를 암호화된 형태로 저장 및 관리 하고 있는 파일
/etc/hosts	소유자: root 권한: 600이하	IP 주소와 호스트 네임을 매핑하는 파일. 인터넷 통신 시 주소를 찾기 위해 참조
/etc/rsyslog.conf	소유자: root 권한: 640이하	시스템 로그 기록의 종류, 위치 및 Level을 설정할 수 있는 파일
/etc/services	소유자: root 권한: 644이하	서비스 관리를 위해 사용되는 파일. 서버에서 사용하는 모든 포트(port)들에 대해 정의

권한 설정 시 유의사항

리눅스에서는 권한을 설정할 때 숫자로 권한을 판단합니다. 권한을 어느 권한 이하로 설정할 때는 숫자 전체로 판단하지 않고 각 자릿수 별로 권한을 비교하여, 모든 자리의 권한을 이전보다 낮게 해야 합니다. 따라서 600보다 낮은 권한 설정의 예시로 400은 될 수 있지만, 420은 될 수 없습니다. 두 번째 자리는 그룹의 권한인데 0에서 2(실행)로 변경되는 것은 그룹의 권한이 낮아진 것이 아니라 오히려 높아진 것이기 때문입니다.

권한 설정 시 이 점을 유의하시길 바랍니다.

리눅스(Linux)

3. crond 관련 파일 관리하기

리눅스 서버에서 crond 관련 파일은 시스템의 주기적인 작업을 관리하는 역할을 합니다. crond 관련 파일에 잘못된 설정이 되어 있으면 시스템이 마비되거나 데이터가 유출될 수 있습니다. 이를 막기 위해 crond 관련 파일의 권한을 관리하는 방법을 안내합니다.

crontab 명령어 권한 설정하기

1 ['터미널' 실행] > [하단의 'ls' 명령어로 소유자 및 권한 확인] > [하단의 'chmod' 명령어로 SUID 제거]

```
# ls -l /usr/bin/crontab
# chmod 750 /usr/bin/crontab
```

1

```
root@localhost /]# ls -l /usr/bin/crontab
-rwsr-xr-x. 1 root root 57656 Aug  8  2019 /usr/bin/crontab
[root@localhost /]# chmod 750 /usr/bin/crontab
[root@localhost /]# ls -l /usr/bin/crontab
-rwxr-x---. 1 root root 57656 Aug  8  2019 /usr/bin/crontab
```

SUID란?

SUID는 리눅스 기반 시스템에서 특정 파일이 실행될 때, 해당 파일이 그 소유자의 권한으로 실행 되도록 하는 특별한 파일 권한입니다. 만약 어떤 파일이 root의 소유이고 SUID가 설정되어 있다면, root 권한을 얻은 채로 파일이 실행됩니다.

이러한 SUID의 특성 때문에, 공격자는 SUID가 설정된 파일을 통해 root 권한을 획득하여 공격에 활용할 수 있습니다. 특히 crontab 명령어와 같이 시스템의 중요한 작업을 제어하는 명령어가 SUID가 설정되어 있다면, 공격에 다양하게 활용될 수 있으므로 crontab 명령어의 권한을 조정해야 합니다.

리눅스(Linux)

crond 관련 파일의 소유자 및 권한 변경하기

1. ['터미널' 실행] > [하단의 'chown' 명령어로 소유자 변경] > [하단의 'chmod' 명령어로 권한 변경]

```
# chown root [crond 관련 파일]
# chmod 640 [crond 관련 파일]
```

예시 (/etc/crontab)

1
```
[root@localhost /]# chown root /etc/crontab
[root@localhost /]# chmod 640 /etc/crontab
```

권한 변경이 권장되는 파일 목록		
설정 파일	**권장 값**	**상 세 설 명**
/etc/crontab	**소유자: root 권한: 640이하**	예약작업을 등록하는 파일
/etc/cron.hourly	**소유자: root 권한: 640이하**	시간,일, 주, 월 단위별로 실행스크립트를 등록하는 파일
/etc/cron.daily		
etc/cron.weekly		
/etc/cron.monthly		
/var/spool/cron/	**소유자: root 권한: 640이하**	사용자별 설정된 cron 작업 목록
cron.allow	**소유자: root 권한: 640이하**	crontab 명령어 허용 및 차단 사용자 등록
cron.deny		

이번 장에서는 외부의 공격으로부터 웹사이트를 보호할 수 있는 웹 서버 보안 설정 방안에 대해 다루겠습니다. 다양한 환경에서의 설정 방법을 다루어, 웹 서비스를 안전하게 제공할 수 있도록 구성했습니다.

웹 서버란 무엇인가요?

웹 서버는 인터넷을 통해 필요한 정보를 찾고, 공유하고, 사용할 수 있게 하는 컴퓨터 시스템 중 하나입니다. 웹 서버는 HTTP(HyperText Transfer Protocol)라는 통신 규약을 사용하는데, 웹 브라우저로부터 이 HTTP 요청을 받아들여 사용자에게 웹 페이지를 전달해 줍니다.

웹 서버 보안은 왜 해야 하나요?

웹 서버에는 회사의 중요한 문서부터 일반 사용자의 개인 정보까지 다양한 데이터가 저장되어 있습니다. 웹 서버가 공격받으면, 웹사이트나 웹 기반의 서비스가 중단되고 정보가 유출되는 등 사용자와 기업 모두에게 악영향을 끼칠 수 있습니다. 웹 서버 보안은 기업의 정보를 안전하게 보호하고, 사용자의 신뢰를 얻기 위한 중요한 조치입니다.

가이드라인에서 다루는 제품 확인하기

▲ IIS(internet Information Service)　▲ 엔진엑스(Nginx)　▲ 아파치(Apache)

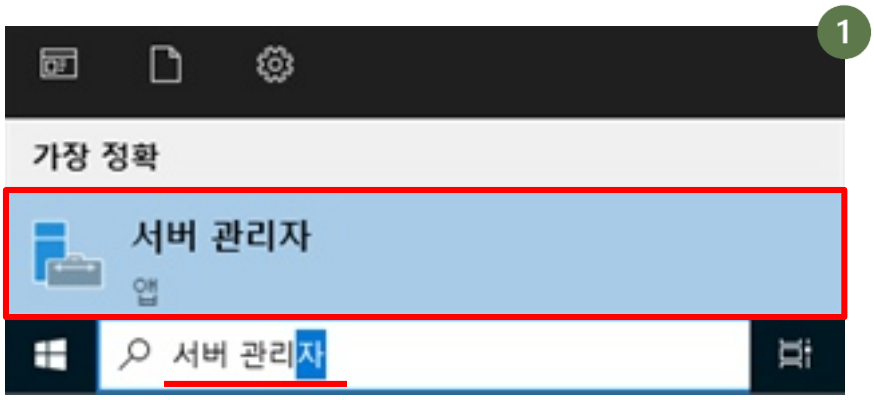
IIS(Internet Information Service)

1. 디렉터리 계층정보 감추기

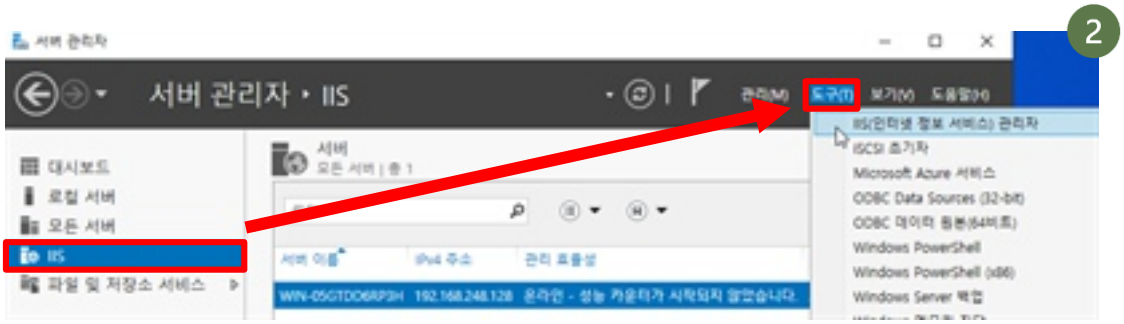
디렉터리 리스팅은 웹 서버의 디렉터리 구조가 외부에 노출되는 것을 말합니다. 디렉터리 리스팅 기능이 활성화 되어있으면, 누구나 웹 서버 안의 파일에 접근할 수 있습니다. 웹 서버에 저장된 데이터가 유출되는 것을 막기 위해서는 디렉터리 리스팅 기능을 비활성화해야 합니다

계정 환경 설정하기

1 ['서버 관리자' 검색 및 실행]

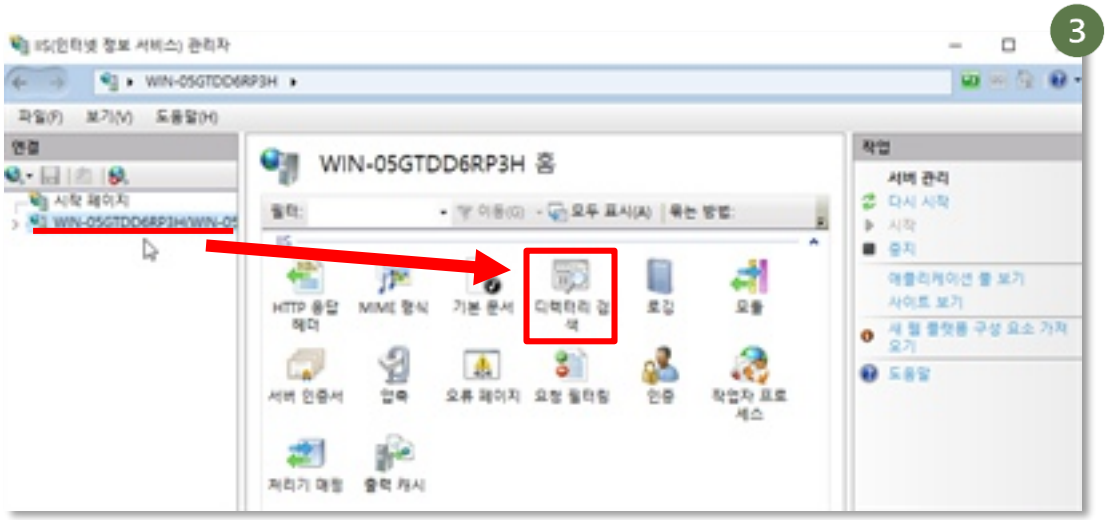


2 [IIS] > [도구] > ['IIS(인터넷 정보 서비스) 관리자' 선택]



IIS(Internet Information Service)

3 ['연결'에서 관리할 웹사이트 선택] > ['디렉터리 검색' 클릭]



4 ['사용 안 함' 설정]

디렉터리 계층정보가 무엇인가요?

인터넷 홈페이지는 컴퓨터의 파일을 저장하는 공간과 같습니다. 이 파일들은 우리가 올린 사진, 글, 비디오 등 다양한 정보를 담고 있는데, 이때 이 파일들은 디렉터리라고 불리는 폴더 안에 정리되어 있습니다.

만약 누군가가 홈페이지의 디렉터리 계층정보를 알게 된다면, 그 안에 저장된 파일에 쉽게 접근할 수 있게 되어 데이터 유출 사고가 일어날 수 있습니다.

IIS(Internet Information Service)

2. 회사 웹 사이트에 암호화 통신 적용하기

HTTPS는 웹 서버와 이용자 사이의 통신을 암호화해주며, 정보가 중간에 수정되지 않았음을 보장해주는 인터넷 보안 기술입니다. HTTPS를 사용하지 않는 홈페이지에서는 누군가 웹 통신을 도청할 수 있습니다. 따라서 HTTPS를 사용해 이용자와 주고받는 정보가 다른 사람들에게 노출되지 않도록 해야 합니다. 이번 항목에서는 웹 사이트에 HTTPS를 적용하는 방법을 안내합니다.

HTTPS를 꼭 적용해야 하나요?

개인정보를 취급하는 사이트는 HTTPS를 의무적으로 적용해야 합니다. 다음 항목 중 하나라도 해당한다면, HTTPS 적용을 권장해 드립니다.

① 회원가입/로그인 기능을 사용한다.

② 예약 서비스 또는 상품 판매 서비스를 제공한다.

③ 입력 폼 등을 사용해 개인정보를 수집한다.

④ 사용자가 게시글이나 댓글을 작성할 수 있다.

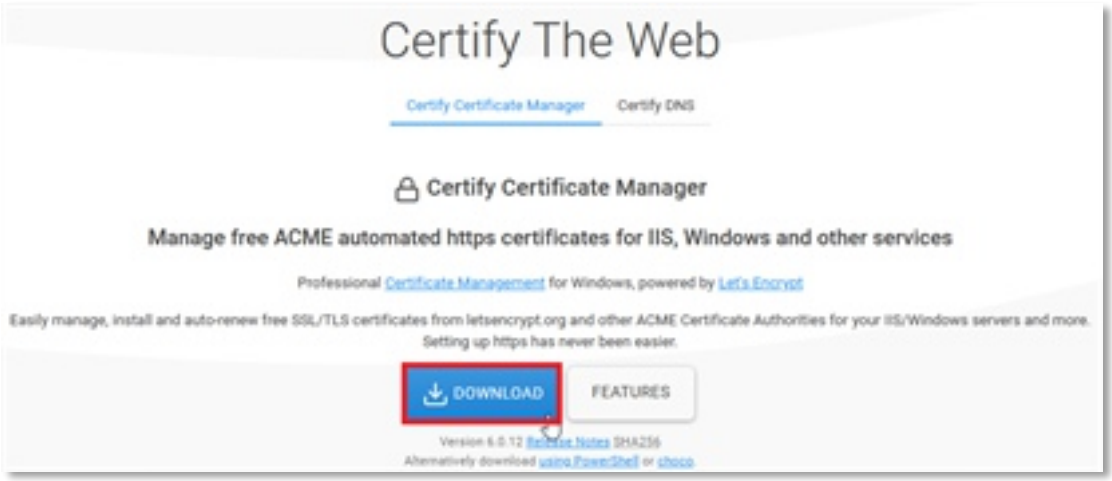
또한, 구글과 같은 검색 엔진에서 HTTPS를 사용하는 홈페이지를 더 먼저 보여주기 때문에 HTTPS를 사용하면 검색엔진에 회사 홈페이지를 더 자주 노출할 수 있습니다.

IIS(Internet Information Service)

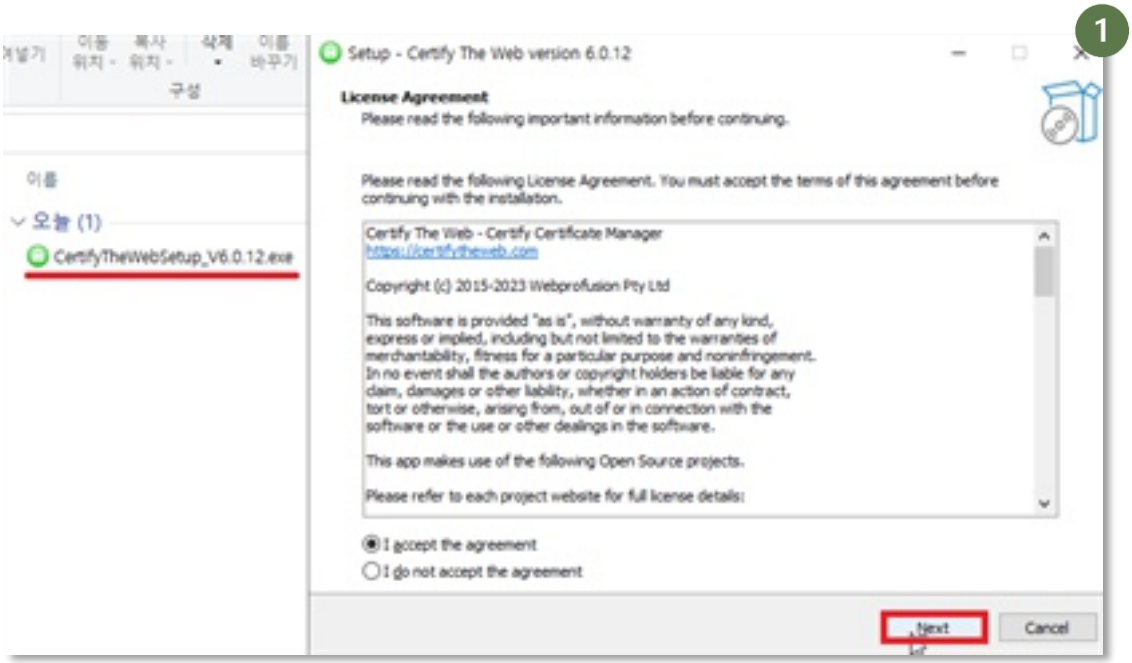
도메인 인증서 발급받기

도메인 인증 기관에서 회사 홈페이지의 도메인 인증서를 발급받을 수 있습니다. 이후 인증서를 통해 HTTPS를 회사 홈페이지에 적용할 수 있습니다.

Certify The Web 홈페이지에서 Certificate Manager 다운로드
https://certifytheweb.com/ - 공식 홈페이지 다운로드 링크

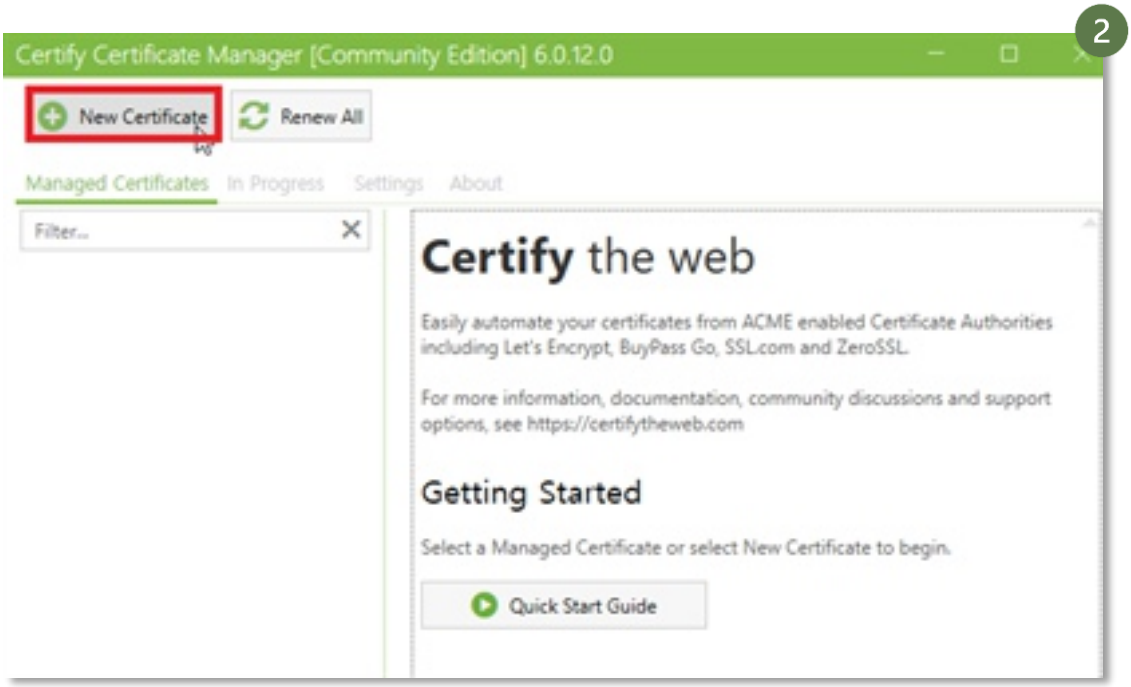


1 ['CertifyTheWeb' 설치]

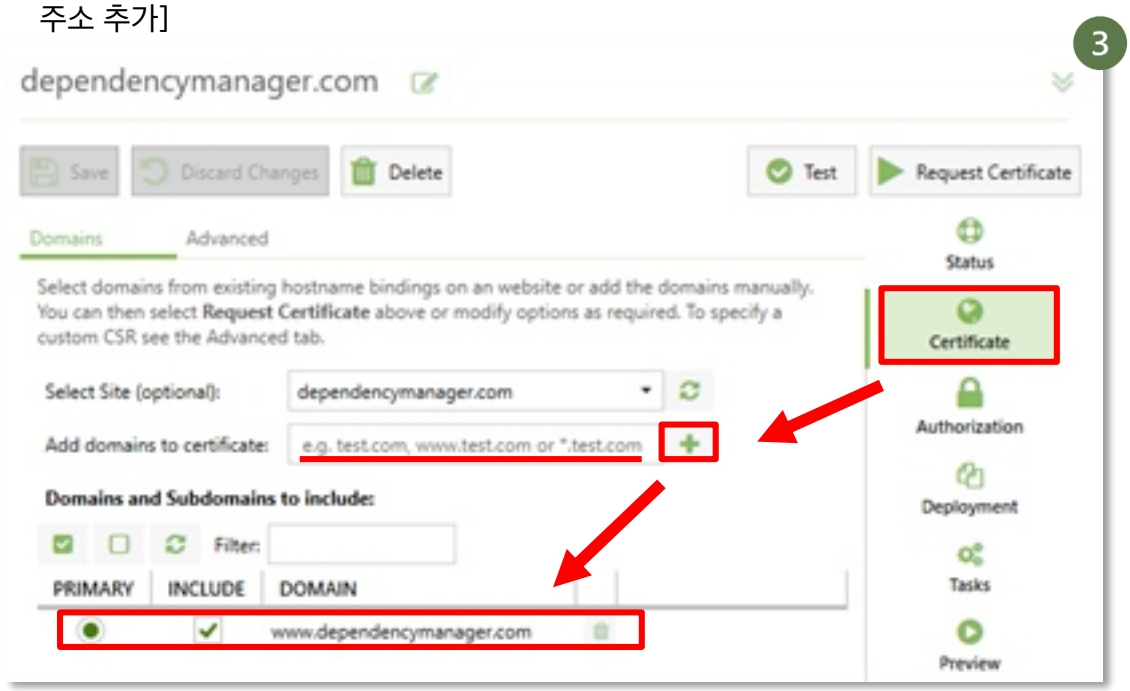


IIS(Internet Information Service)

2 ['New Certificate' 클릭해 인증서 발급 시작]

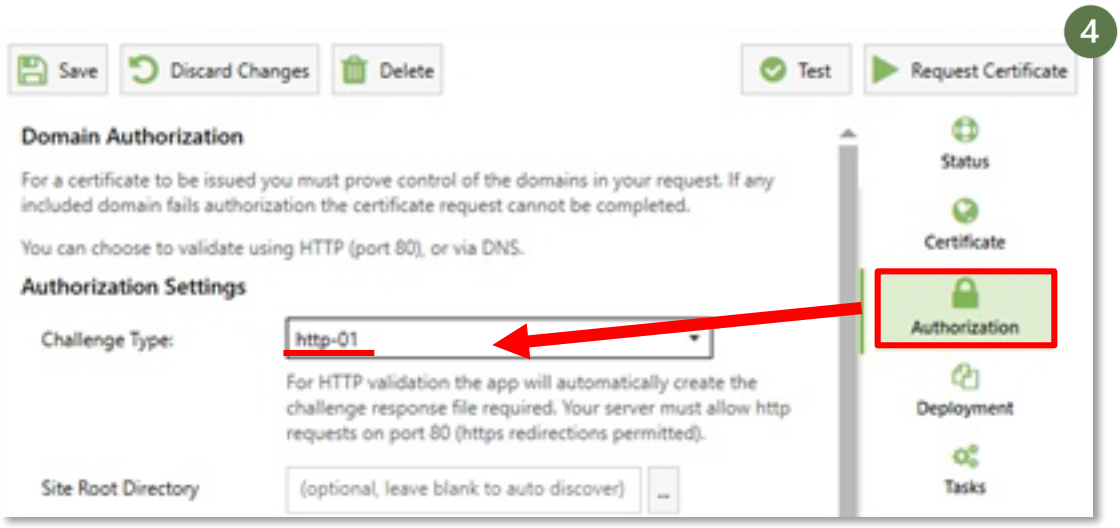


3 [우측 'Certificate' 탭 선택] > ['Add domains to certificate' 클릭해 인증 받을 도메인 주소 추가]

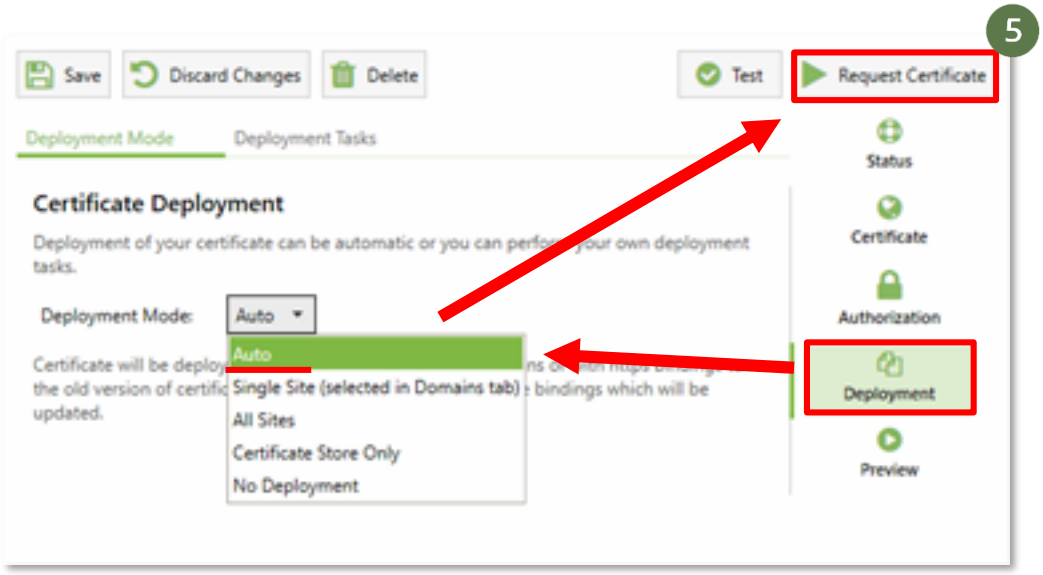


IIS(Internet Information Service)

4 [우측 'Authorization' 탭 선택] > [도메인 검증 방식 'http-01' 또는 'dns-01' 선택]



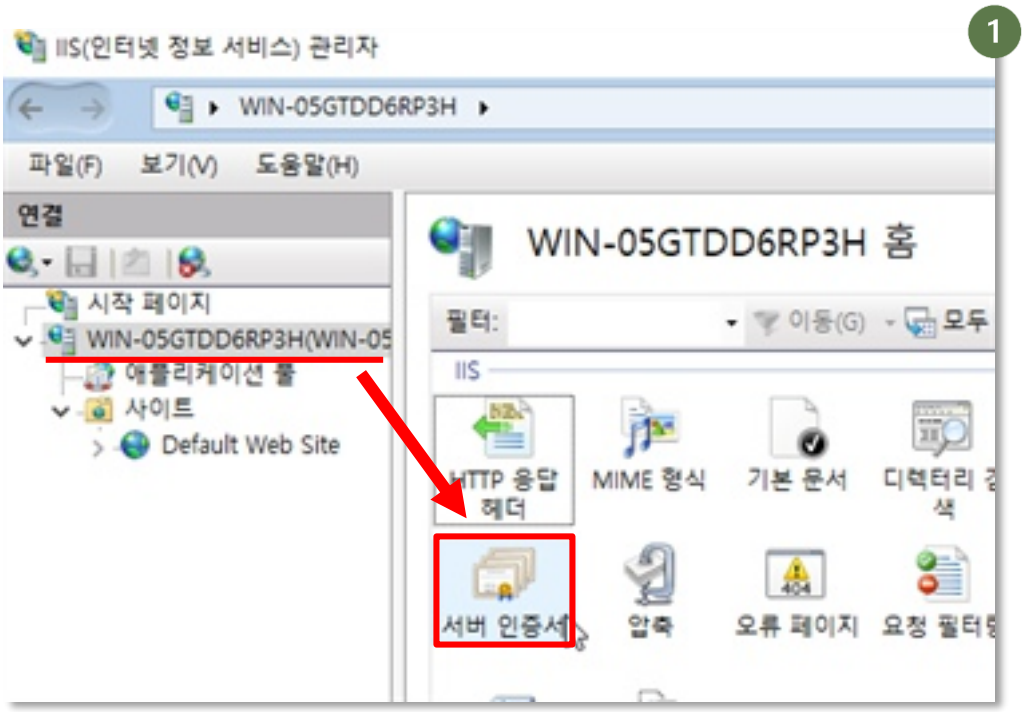
5 [우측 'Deployment' 탭 선택] > [Deployment Mode 'Auto' 선택] > [우측 상단 'Request Certificate' 클릭]



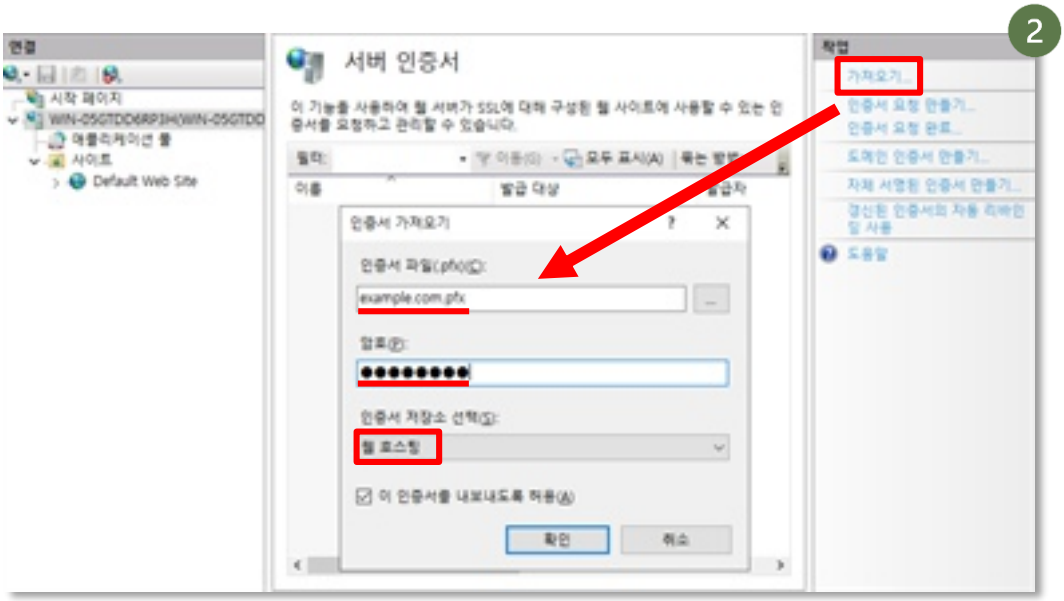
IIS(Internet Information Service)

서버 인증서 등록하기

1. [IIS(인터넷 정보 서비스) 관리자 실행] > [좌측 '대상 웹 서버' 선택]> ['서버 인증서' 선택]



2. [우측 '가져오기...' 선택] > [발급받은 인증서 파일 경로 및 암호 입력] > [인증서 저장소 '웹 호스팅' 선택]

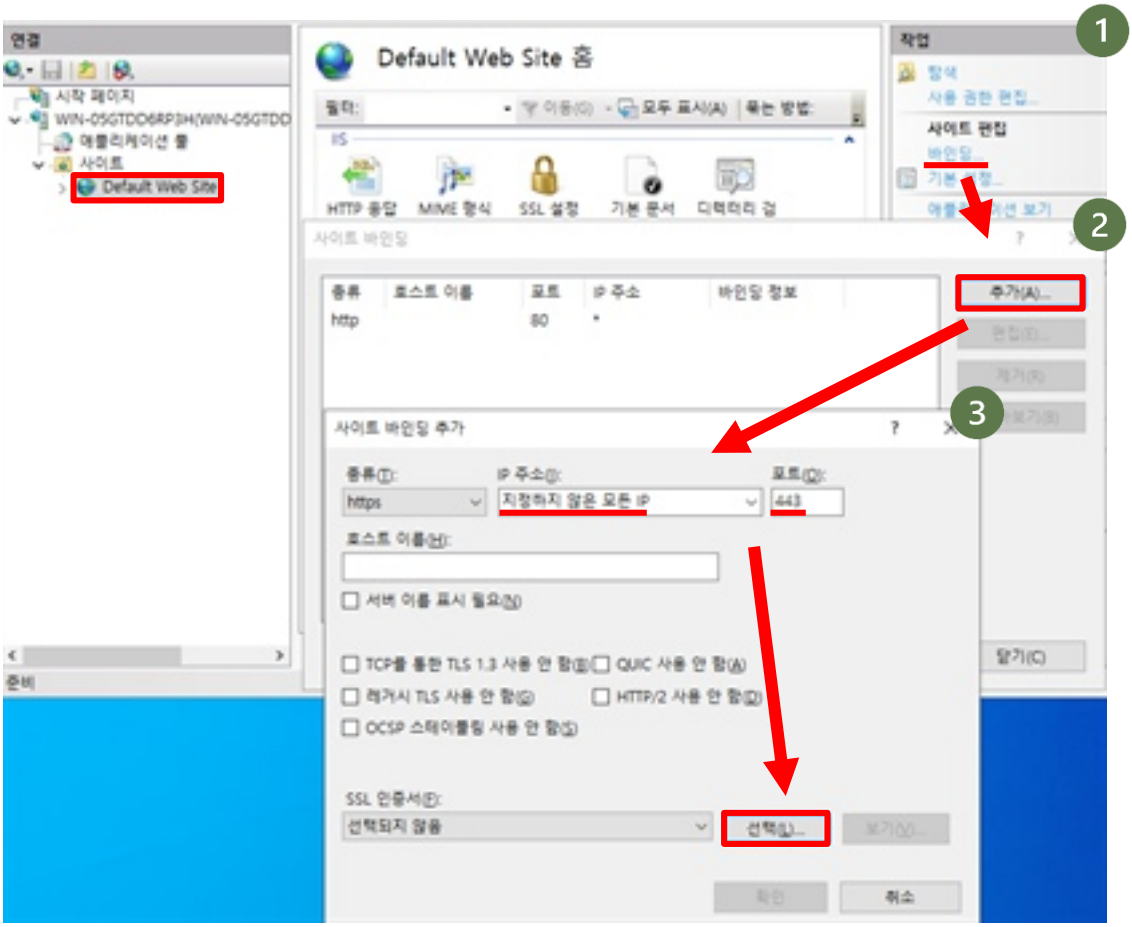


IIS(Internet Information Service)

사이트와 인증서 연결하기

웹 서버에 등록한 인증서를 이용해 HTTPS를 활성화합니다. 이제 웹 서버와 이용자 사이의 웹 통신은 암호화가 적용되어 도청으로부터 안전합니다.

1. [좌측 웹 서버 하위 '사이트'에서 설정할 사이트 선택] > [오른쪽 '바인딩...' 클릭]
2. [사이트 바인딩에서 '추가...' 클릭]
3. [종류 'HTTPS' 선택] > [IP 주소 '지정하지 않은 모든 IP' 선택] > [포트번호 '443' 선택] > [선택 클릭]

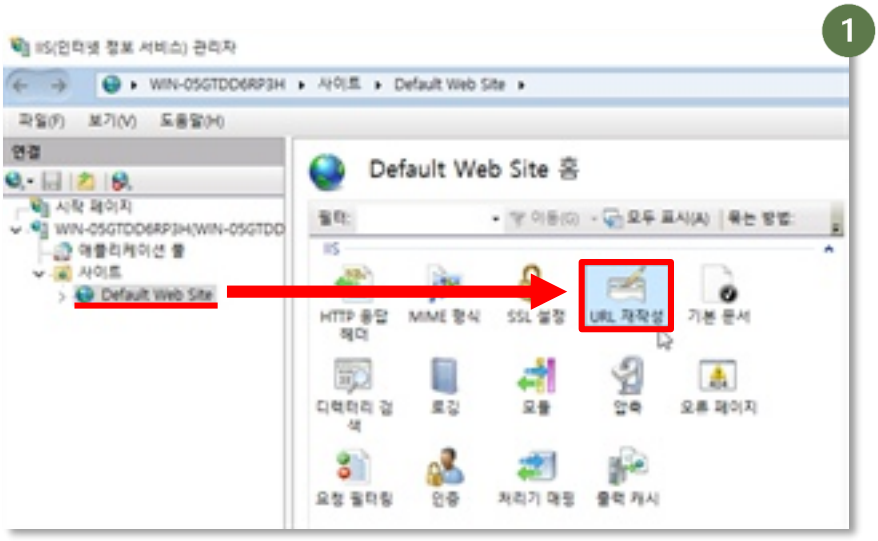


IIS(Internet Information Service)

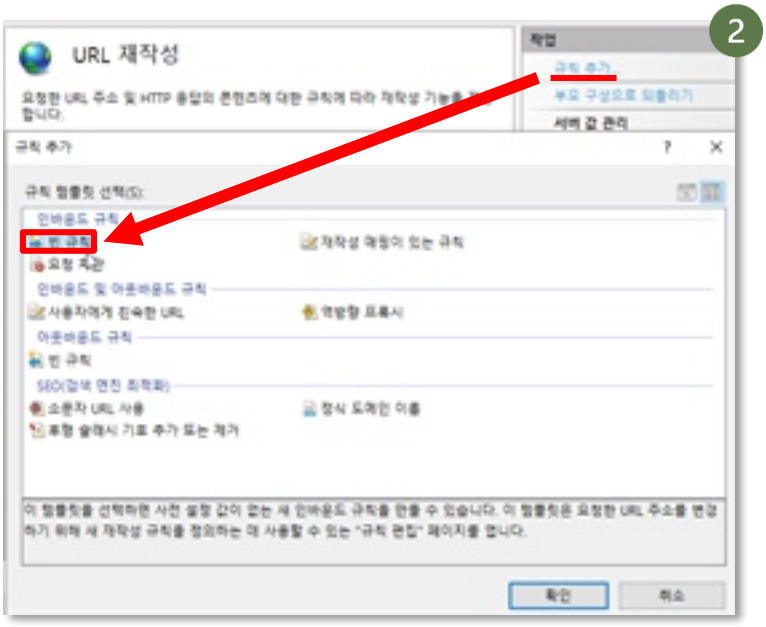
안전한 연결 방식으로 재 연결 설정하기

이용자가 홈페이지에 HTTP 요청을 하더라도 안전한 연결방식인 HTTPS로 자동 연결될 수 있도록 규칙을 만듭니다.

1. [하단 링크 참고해 'URL Rewrite 모듈' 다운로드 및 설치] > [IIS 관리자 실행] > [왼쪽 '사이트' 선택] > ['URL 재작성' 선택]

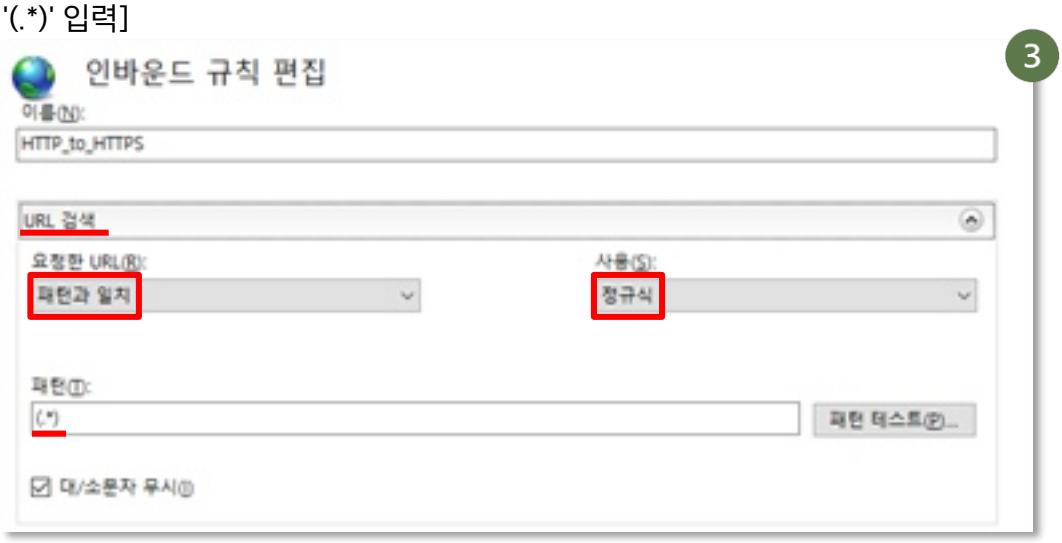


2. [오른쪽 작업에서 '규칙 추가' 선택] > [인바운드 규칙에서 '빈 규칙' 선택]
https://www.iis.net/downloads/microsoft/url-rewrite - URL Rewrite 모듈 다운로드주소

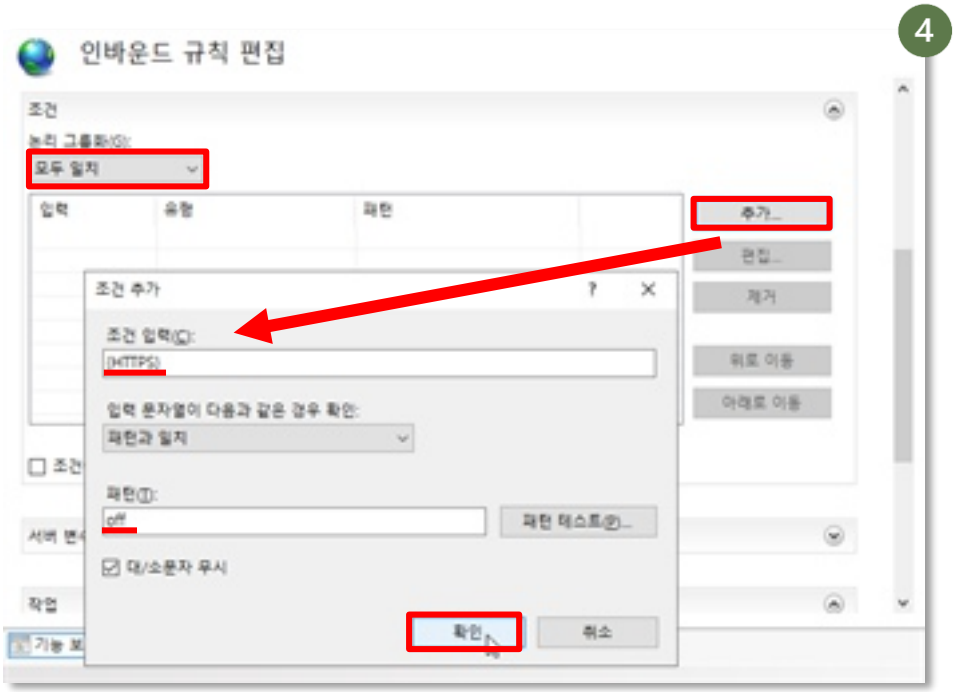


IIS(Internet Information Service)

3 [URL 검색] > [요청한 URL 값 '패턴과 일치' 선택] > [사용 값 '정규식' 선택] > [패턴 값 '(.*)' 입력]

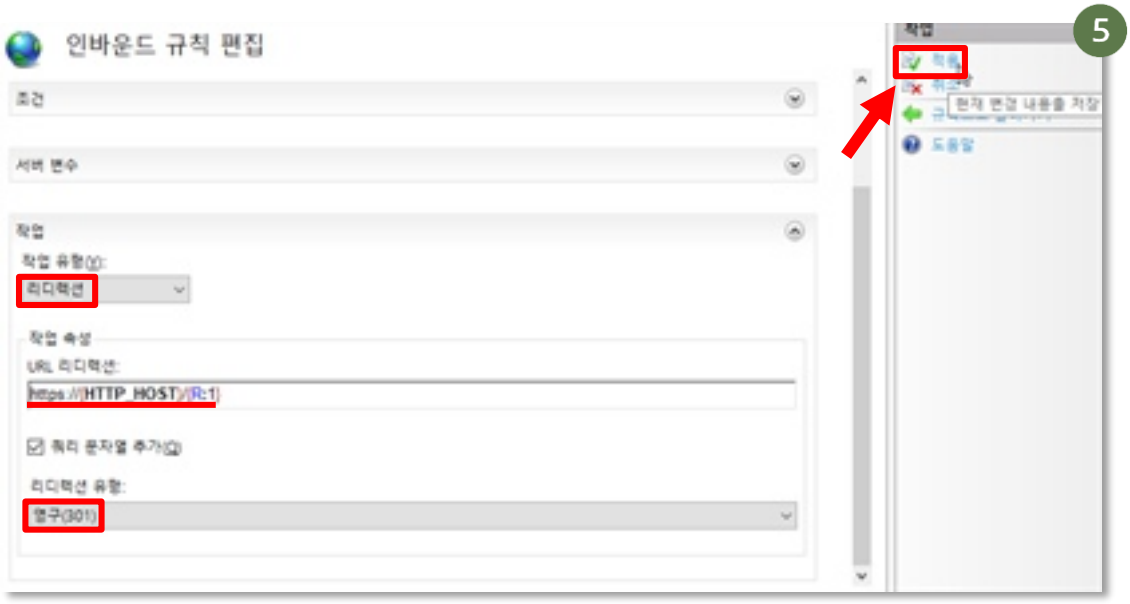


4 [조건 논리 그룹화 '모두 일치' 선택] > ['추가...' 선택] > [조건 입력 '{HTTPS}' 입력] > [패턴 'off' 입력] > ['확인' 클릭]



IIS(Internet Information Service)

5 [작업 값 '리디렉션' 선택] > [작업 유형 '리디렉션' 선택] > [작업 속성의 URL 리디렉션 'https://{HTTP_HOST}/{R:1}' 입력] > ['쿼리 문자열 추가' 체크] > [리디렉션 유형 '영구{301}' 선택] > [우측 상단 '적용' 클릭]



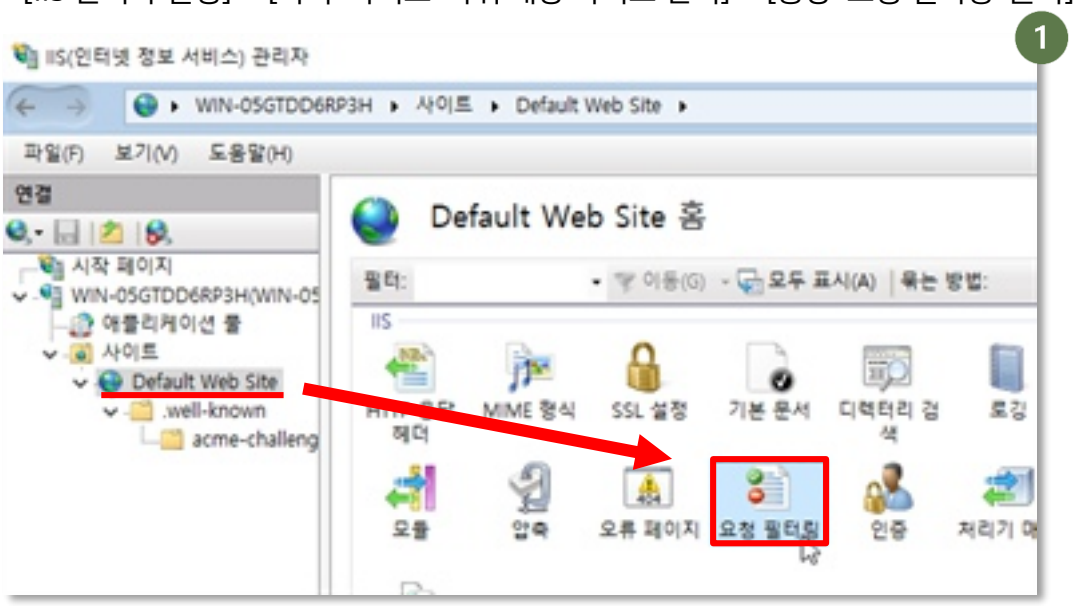
IIS(Internet Information Service)

3. 부적절한 요청 검사하기

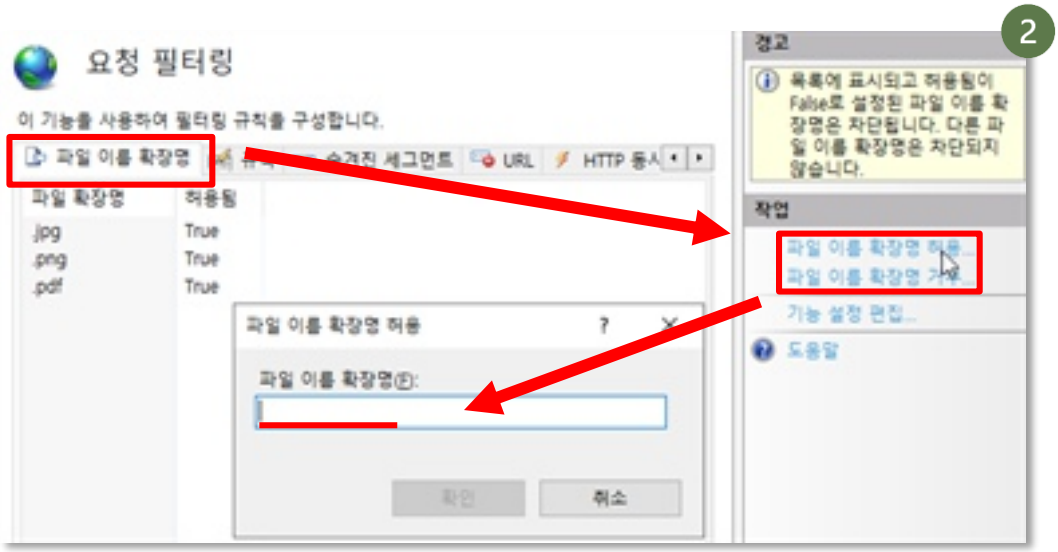
요청 필터링 기능 활용하기

요청 필터링은 이용자가 보낸 검색어 입력, 파일 업로드 등의 요청을 검사해 비정상 요청을 차단하는 기능입니다. 이를 통해 웹사이트가 허용하지 않은 작업을 거부할 수 있습니다.

1 [IIS 관리자 실행] > [좌측 '사이트' 하위 대상 사이트 선택] > [중앙 '요청 필터링' 클릭]



2 [좌측 상단 '파일 이름 확장명' 선택] > [우측 작업의 '파일 이름 확장명 허용.../거부...' 선택] > ['파일 이름 확장명' 값에 하단의 표 참고하여 허용 또는 거부할 확장명 입력]

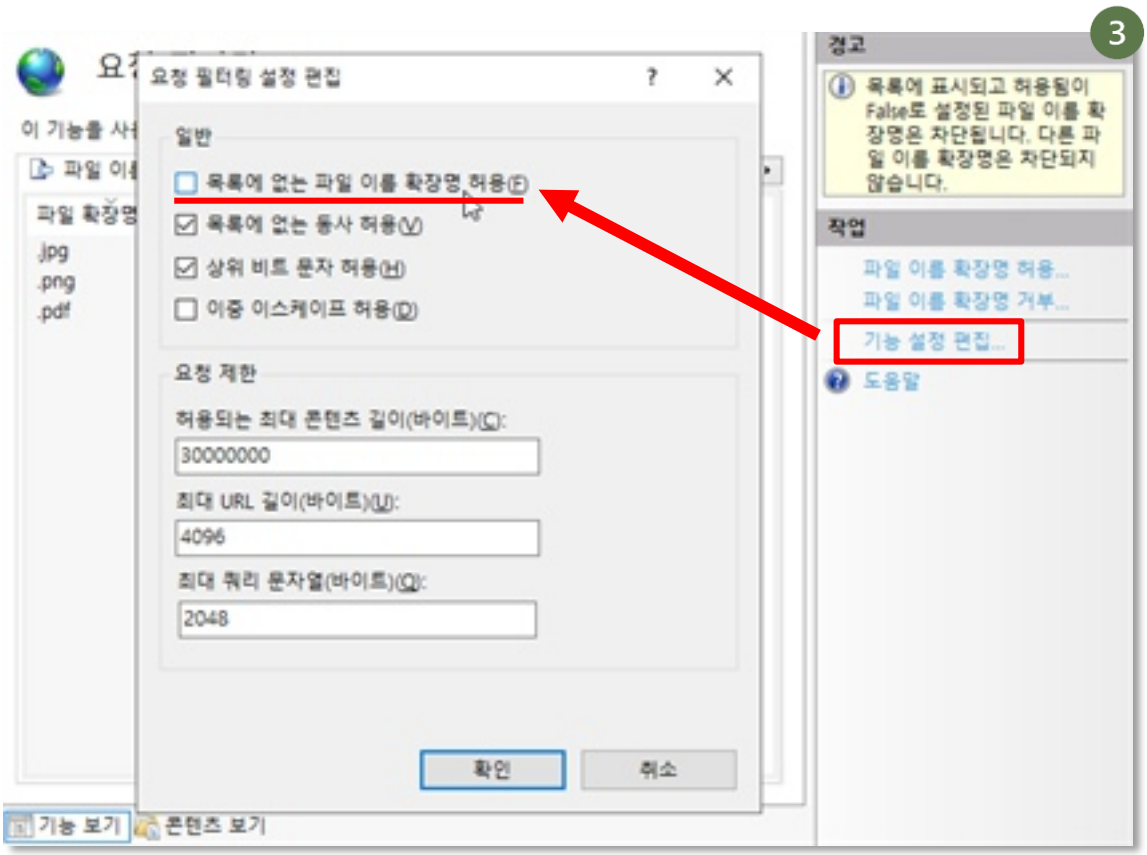


IIS(Internet Information Service)

일반적으로 허용 또는 거부해야 하는 확장자 명은 아래 표를 참조하시길 바랍니다.

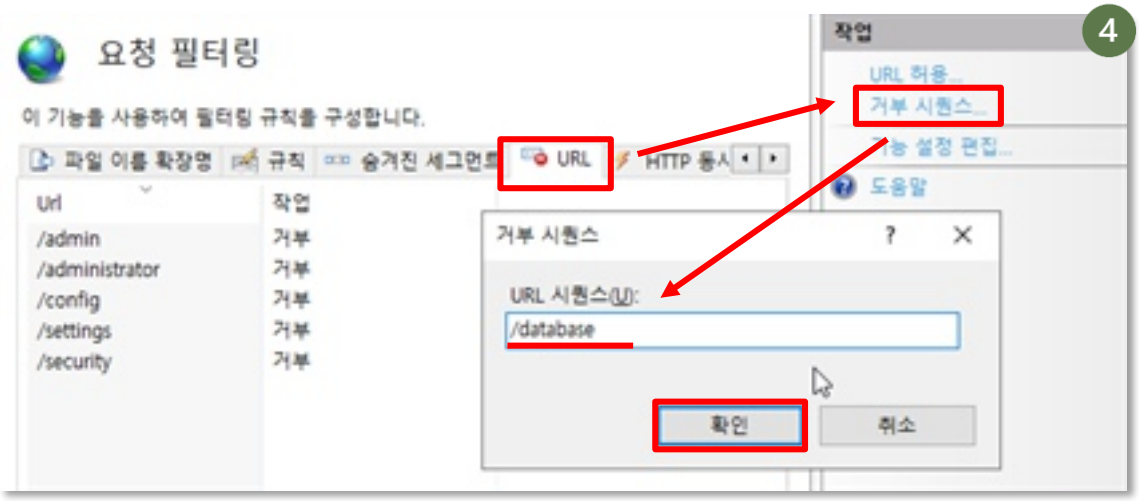
확장자명	허용/거부	상세 설명
.jpg / .jpeg / .png / .gif	필요시 허용	이미지 파일 확장자명으로, 허용 시 이용자들은 홈페이지에 사진이나 그래픽 이미지를 업로드 가능
.pdf / .doc / .docx / .txt	필요시 허용	문서 파일 확장자명으로, 허용 시 이용자들은 홈페이지에 텍스트 문서나 문서 파일을 업로드 가능
.mp3 / .wav / .ogg	필요시 허용	오디오 파일 확장자명으로, 허용 시 이용자들은 홈페이지에 음악 파일을 업로드 가능
.exe / .bat / .msi	거부	실행 파일 확장자명으로, 허용 시 공격자가 홈페이지에 악성 프로그램 업로드 가능
.php / .asp / .cgi	거부	서버 스크립트 파일 확장자명으로, 허용 시 웹 서버에 대한 해킹에 악용 가능
.zip / .rar	거부	압축 파일 확장자명으로, 허용 시 공격자가 홈페이지에 악성 파일을 압축하여 업로드 가능

3 [우측 작업 '기능 설정 편집...' 선택] > ['목록에 없는 파일 이름 확장명 허용' 체크 해제]



IIS(Internet Information Service)

4 [요청 필터링에서 'URL' 탭 선택] > [작업 '거부 시퀀스...' 선택] > [거부할 URL 시퀀스 추가] > ['확인' 클릭]



하단의 예시를 참고해 거부할 URL 시퀀스를 추가하는 것을 권장합니다.

확장자명	허용/거부	효과
/admin, /administrator, /login/admin, /admin-panel	거부	관리자 페이지 접근 방지
/config, /settings, /setup, /configurations, /install	거부	웹 애플리케이션 설정 파일 접근 방지
/security, /secure, /ssl, /auth, /password	거부	웹사이트 보안 정보 탈취 시도 차단
/database, /db, /sql, /mysql, /phpmyadmin	거부	데이터베이스 관련 작업 시도 차단
/iis, /server, /web-server, /apache, /nginx	거부	웹 서버의 정보 탈취 시도 차단
/files, /uploads, /documents, /download	거부	웹 서버에 업로드된 파일 접근 방지

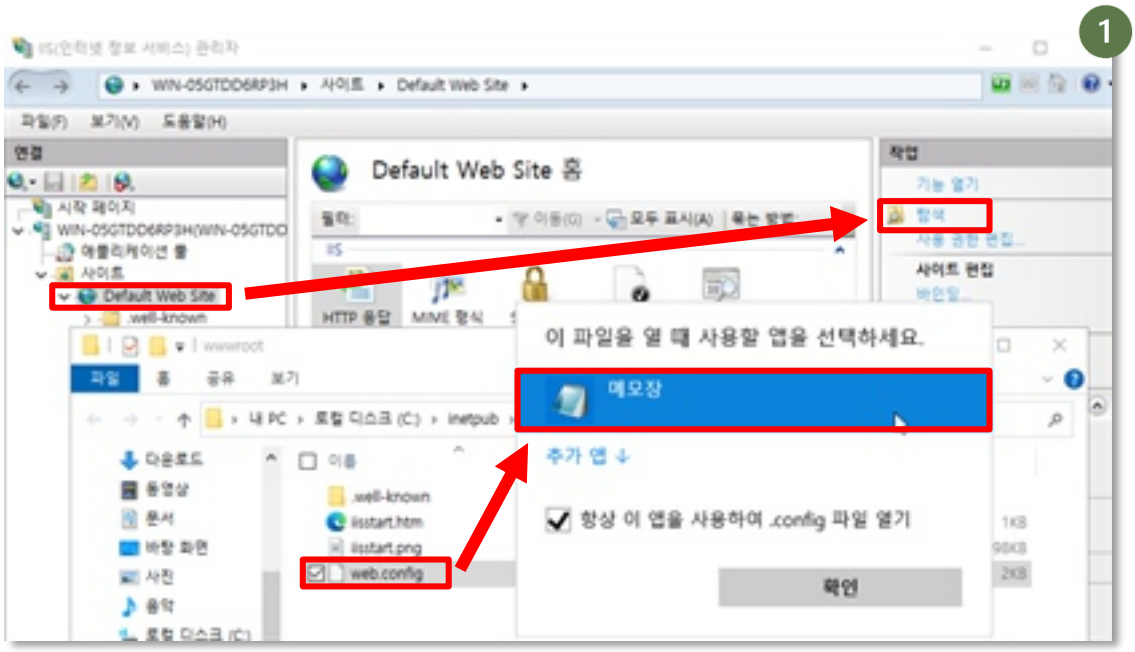
IIS(Internet Information Service)

4. 서버 정보 숨기기

HTTP 서버 헤더에서 서버 정보 숨기기

HTTP 응답 헤더 중 '서버 헤더'는 웹 서버 종류와 버전 정보를 알려줍니다. 공격자는 서버 헤더에서 제공하는 웹 서버 정보를 수집해 공격에 활용할 수 있기 때문에, 이를 알려주지 않도록 설정해야 합니다.

1. [IIS 관리자 실행] > [좌측 '사이트' 하위 대상 사이트 선택] > [우측 작업 '탐색' 클릭해 루트 디렉터리 열기] > ['web.config' 파일 메모장으로 실행]



IIS(Internet Information Service)

② [<system.webserver>에 하단의 코드를 작성 후 저장]

```
<system.webServer> ## 하단의 코드 추가
  <httpProtocol>
    <customHeaders>
      <remove name="Server" />
      <add name="Content-Security-Policy" value="default-src 'self'; script-src 'self';
object-src 'none';" />
      <add name="X-Content-Type-Options" value="nosniff" />
    </customHeaders>
  </httpProtocol>
```

설정 코드	용도
<remove name="Server" />	서버 헤더를 감추는 코드
<add name="Content-Security-Policy" value="default-src 'self';" />	모든 리소스의 출처를 현재 도메인으로 제한하는 코드
<add name="X-Content-Type-Options" value="nosniff" />	브라우저가 컨텐츠 유형 훔쳐보는 것을 막는 코드

엔진엑스(NGINX)

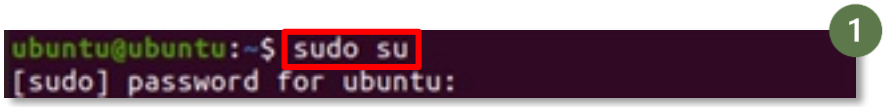
0. NGINX 설치 디렉터리 확인하기

NGINX의 설정을 변경하기 위해서는 먼저 관리자 권한으로 전환한 뒤, NGINX 설치 위치를 알아내야 합니다. 일반적으로 NGINX는 '/etc/nginx' 및 '/usr/share/nginx' 디렉터리에 설치됩니다. 하지만 구체적인 경로는 설치 방법과 버전에 따라 다를 수 있습니다. 따라서 다음에서 소개하는 명령어를 통해 설치 경로를 확인해야 합니다.

관리자 권한으로 전환하기

1 ['터미널' 실행] > ['su' 명령어를 통한 root 계정 전환] > [root 패스워드 입력]

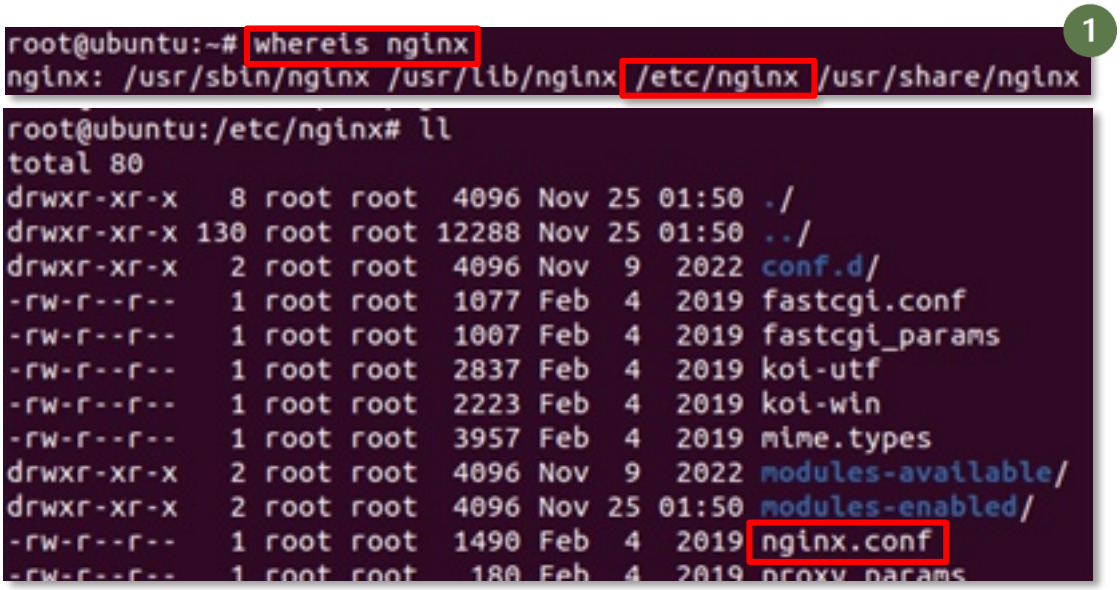
```
$ sudo su
```



NGINX 설치 위치 확인하기

1 ['터미널' 실행] > ['whereis' 명령어를 통한 NGINX 설치위치 확인]

```
# whereis nginx
```



엔진엑스(NGINX)

1. 소스 파일 쓰기 권한 제거하기

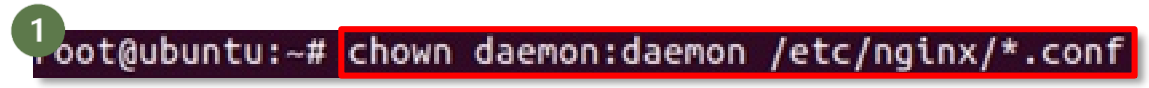
이용자가 웹 서버의 설정 파일 및 웹 사이트 소스 파일을 임의로 수정 또는 삭제할 수 있으면 홈페이지 변조, 백도어 삽입과 같은 웹 사이트에 대한 공격을 수행할 수 있습니다. 그 결과 웹 서버에 저장된 데이터가 유출되거나, 시스템이 오작동해 사용 불능 상태에 빠질 수 있습니다.

daemon으로 파일 소유자 변경하기

daemon은 일반적으로 시스템에서 제한된 권한을 가진 사용자로, 최소한의 권한만을 부여받아 동작합니다. 만약 Nginx가 특정 파일을 실행해야 하는 경우, 이를 위해 daemon 사용자에게 제한적인 권한만을 부여함으로써 보안을 강화할 수 있습니다.

1 ['터미널' 실행] > [하단의 'chown' 명령어 실행]

```
# chown daemon:daemon /[Nginx 설치 경로]/*.conf
```



파일 또는 디렉터리를 만든 사용자에게만 권한 부여하기

1 ['터미널' 실행] > [하단의 'chmod' 명령어를 통해 소유자에게만 권한 부여]

```
# chmod 700 /[Nginx 설치 경로]/*.conf
```

리눅스에서 권한이란?

리눅스에서의 권한은 파일이나 디렉토리에 대한 사용자의 접근 수준을 설정하는 것입니다. 이러한 권한을 통해 해당 파일이나 디렉토리를 누가 볼 수 있고, 수정할 수 있으며, 실행할 수 있는지를 결정합니다. 아래는 리눅스 권한을 읽는 법과 영문, 숫자 표기법입니다.

	파일 유형	파일 소유자 권한			파일 소유 그룹 권한			기타 사용자 권한		
영문 표기법	-	r	w	x	r	w	x	r	w	x
숫자 값	-: 파일 d: 디렉토리	4	2	1	4	2	1	4	2	1
숫자 표기법		7			7			7		
권 한		읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행

엔진엑스(NGINX)

2. NGINX 관리자 권한 구동 여부 점검하기

NGINX 프로세스는 관리자 권한이 아닌 서비스 전용 계정의 권한으로 운영되어야 합니다. 웹 프로세스가 관리자 권한을 가지고 있으면 시스템에 침입한 공격자가 시스템 전체를 제어할 수 있어 큰 피해를 입을 수 있습니다. 따라서 웹 프로세스에 최소한의 권한만을 부여하고 서비스를 격리하는 것이 보안 측면에서 중요합니다.

관리자 권한이 뭔가요?

관리자 권한은 시스템 전체를 제어하고 변경할 수 있는 권한을 의미합니다. root 사용자는 시스템에 대한 모든 권한을 가지고 있어 파일 시스템의 모든 파일에 접근할 수 있고, 시스템 설정을 변경할 수 있으며, 사용자 계정을 관리할 수 있습니다. 따라서 관리자 권한을 부주의하게 사용할 경우 시스템에 심각한 문제를 일으킬 수 있습니다.

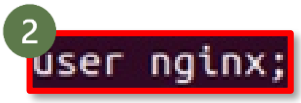
관리자 계정이 아닌 서비스 전용 계정으로 구동되도록 변경하기

1 ['터미널' 실행] > ['vi' 명령어 실행해 'nginx.conf' 파일 열기]

```
# vi /[nginx 설치 디렉터리]/nginx.conf
```

2 ['user' 지시어 수정] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
# user [서비스 전용 계정] [서비스 전용 그룹(생략가능)];
```



3 ['터미널'에 'service nginx restart' 명령어 입력] > [서비스 다시 시작]

```
# service nginx restart
```

엔진엑스(NGINX)

3. 로그파일 권한 제한하기

로그파일은 시스템 및 애플리케이션의 활동을 기록하는 중요한 도구입니다. 그러나 로그파일은 그 특성상 시스템의 중요한 정보도 함께 담고 있습니다. 따라서 로그파일에 대한 권한 관리가 중요합니다. 로그파일에 저장된 정보가 공격자에게 노출되면, 시스템의 취약점을 찾아내거나 공격을 계획하는 데 활용될 수 있습니다.

nginx.conf 파일에서 로그파일 위치 확인하기

로그 파일의 위치를 확인하기 위해 Nginx의 설정 파일인 nginx.conf를 열어서 해당 파일에서 error_log 또는 access_log라는 문자열을 포함하는 모든 라인을 출력합니다.

1 ['터미널' 실행] > [하단의 'cat' 명령어 입력]

```
# cat /[nginx 설치 디렉터리]/nginx.conf | grep 'error_log\|access_log'
```

1

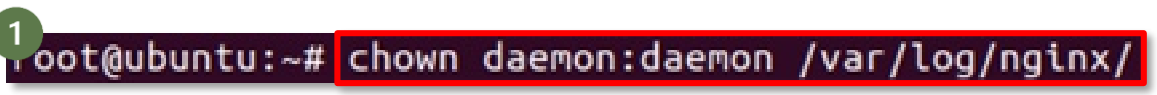
로그 폴더 소유자 변경하기

Nginx 로그 디렉터리 및 하위 디렉터리 전체의 소유자를 daemon 사용자, 그룹을 daemon으로 변경합니다.

1 ['터미널' 실행] > [하단의 'chown' 명령어 입력]

```
# chown daemon:daemon /[nginx 로그 디렉터리]
```

1



엔진엑스(NGINX)

로그 폴더 권한 변경하기

1 ['터미널' 실행] > [하단의 'chmod' 명령어 입력]

```
# chmod 750 /[nginx 설치 디렉터리]/logs/
```

1
```
root@ubuntu:~# chmod 750 /var/log/nginx
```

로그 파일 권한 변경하기

1 ['터미널' 실행] > [하단의 'chmod' 명령어 입력]

```
# chmod 640 /[nginx 설치 디렉터리]/logs/[로그파일]
```

1
```
root@ubuntu:~# chmod 640 /var/log/nginx/access.log
root@ubuntu:~# chmod 640 /var/log/nginx/error.log
```

권장하는 권한		
항목	권장 값	권한 의미
로그 폴더	750 이하	소유자에게 읽기, 쓰기, 실행 권한을, 그룹에는 읽기와 실행 권한을 부여하고, 기타 사용자에게는 어떠한 권한도 주지 않음
로그 파일	640 이하	소유자에게 읽기와 쓰기 권한을, 그룹에는 읽기 권한을 부여하고, 기타 사용자에게는 어떠한 권한도 주지 않음

리눅스에서 권한이란?

리눅스에서의 권한은 파일이나 디렉토리에 대한 사용자의 접근 수준을 설정하는 것입니다. 이러한 권한을 통해 해당 파일이나 디렉토리를 누가 볼 수 있고, 수정할 수 있으며, 실행할 수 있는지를 결정합니다. 아래는 리눅스 권한을 읽는 법과 영문, 숫자 표기법입니다.

	파일 유형	파일 소유자 권한			파일 소유 그룹 권한			기타 사용자 권한		
영문 표기법	-	r	w	x	r	w	x	r	w	x
숫자 값	-: 파일 d: 디렉토리	4	2	1	4	2	1	4	2	1
숫자 표기법		7			7			7		
권 한		읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행

엔진엑스(NGINX)

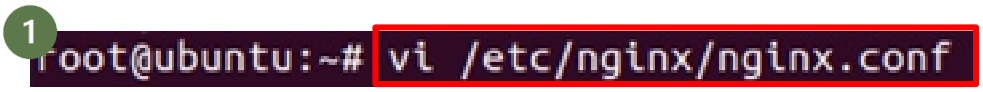
4. 암호화 통신 규약 변경하기

NGINX는 HTTPS 통신 규약 중 'SSLv3'를 기본 암호화 통신 규약으로 사용합니다. 'SSLv3'는 현재 여러 문제점이 발견되어 사용을 권장하지 않습니다. 따라서 SSL보다 안전한 버전인 TLS 통신 규약을 사용하도록 설정합니다.

TLS 통신 규약 사용 설정 하기

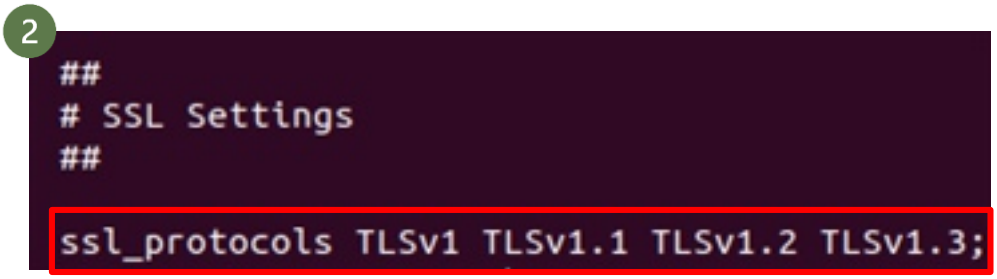
1. ['터미널' 실행] > ['vi' 명령어 실행해 'nginx.conf' 파일 열기]

```
# vi /[nginx 설치 디렉터리]/nginx.conf
```



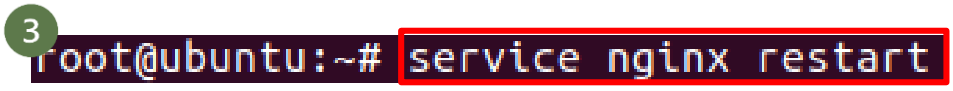
2. ['/http'를 입력하여 http {} 블록 검색] > ['i'를 통해 입력모드 진입] > ['ssl_protocols' 이하 내용 삽입] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
http { } 블록 검색
ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
```



3. ['터미널'에 'service nginx restart' 명령어 입력] > [서비스 다시 시작]

```
# service nginx restart
```



엔진엑스(NGINX)

5. HTTP 메소드 제한하기

보안을 강화하기 위해 웹 통신에서 잘 사용되지 않는 메소드인 PUT, DELETE 등을 비활성화해야 합니다. 이러한 메소드가 활성화되어 있으면 공격자가 서버의 파일을 임의로 삭제하거나 업로드하여 시스템에 피해를 줄 수 있습니다.

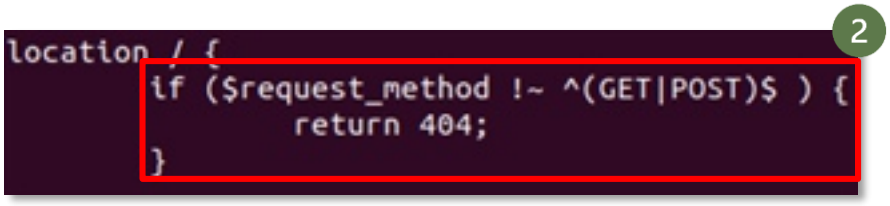
불필요한 메소드 비활성화하기

1. ['터미널' 실행] > ['vi' 명령어 실행해 'nginx.conf' 파일 열기]

```
# vi /[nginx 설치 디렉터리]/nginx.conf
```

2. ['/location'를 입력하여 location / {} 블록 검색] > ['i'를 통해 입력모드 진입] > ['if' 이하 내용 삽입] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
location / { } 블록 찾기
if ($request_method !~ ^(GET|POST)$ ) {
return 404;
}
```



3. ['터미널'에 'service nginx restart' 명령어 입력] > [서비스 다시 시작]

```
# service nginx restart
```

엔진엑스(NGINX)

메소드명	권장설정	상 세 설 명
GET	허용	데이터를 요청할 때 사용하는 메소드
POST	허용	데이터를 요청하거나 변경할 때 사용하는 메소드
HEAD	허용	데이터를 요청하는 경우 HTTP Header 정보만 전송하는 메소드로 해당 자원이 존재하는 지 확인할 때 사용
PUT	비허용	데이터를 생성할 때 사용하는 메소드로 웹 서버에 임의의 파일 생성 가능
DELETE	비허용	데이터를 삭제할 때 사용하는 메소드
OPTIONS	비허용	응답가능한 HTTP 메소드 정보를 요청하는 메소드
TRACE	비허용	요청한 내용을 그대로 반환하는 메소드

엔진엑스(NGINX)

WebDAV 모듈 비활성화하기

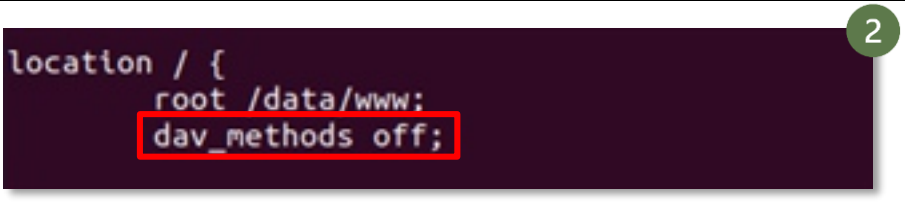
WebDAV는 외부에서 웹 서버에 저장된 파일을 편집하고 관리할 수 있는 프로토콜입니다. 외부 이용자가 웹 서버에 저장된 파일을 수정할 수 있게 설정되어 있으면, 공격자가 웹 서버의 데이터를 유출하거나, 웹 서버에 악성 프로그램을 업로드할 수 있습니다.

1 ['터미널' 실행] > ['vi' 명령어 실행해 'nginx.conf' 파일 열기]

```
# vi /[nginx 설치 디렉터리]/nginx.conf
```

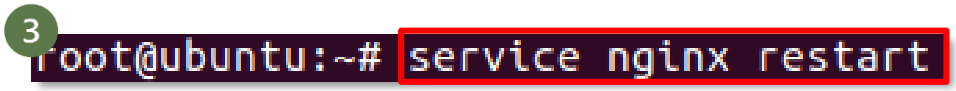
2 ['/location'를 입력하여 location / {} 블록 검색] > ['i'를 통해 입력모드 진입] > [수정 후 내용 삽입] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
location / { } 블록 찾기
<수정 전>
location / {
        root            /data/www;
        dav_methods  PUT  DELETE  MKCOL  COPY  MOVE;
    }

<수정 후>
location / {
        root            /data/www;
        dav_methods off
        }
```



3 ['터미널'에 'service nginx restart' 명령어 입력] > [서비스 다시 시작]

```
# service nginx restart
```



엔진엑스(NGINX)

6. 기본 페이지 변경하기

NGINX 기본 페이지에는 서버 버전과 같은 시스템 정보가 들어있습니다. 공격자는 이와 같은 시스템 정보를 수집해 공격에 활용할 수 있기 때문에 다른 페이지로 기본 페이지를 변경하여 웹 서비스를 제공해야 합니다.

기본 페이지 변경하기

1. ['터미널' 실행] > ['vi' 명령어 실행해 'nginx.conf' 파일 열기]

```
# vi /[nginx 설치 디렉터리]/nginx.conf
```

1
```
root@ubuntu:~# vi /etc/nginx/nginx.conf
```

2. ['/location'를 입력하여 location / {} 블록 검색] > ['i'를 통해 입력모드 진입] > [수정 후 내용 삽입] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

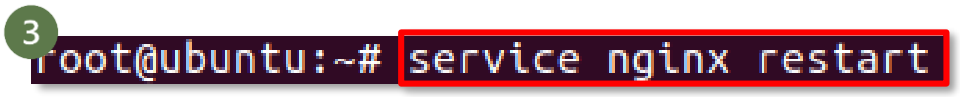
```
location / { } 블록 찾기
<수정 전>
location / {
        root html;
        index index.html;
        }

<수정 후>
location / {
        root html;
        index example_main.html;
}
```

2
```
location / {
        root html;
        index example.html;
}
```

엔진엑스(NGINX)

3 ['터미널'에 'service nginx restart' 명령어 입력] > [서비스 다시 시작]

```
# service nginx restart
```



7. 서버 정보 숨기기

HTTP 응답 헤더 중 '서버 헤더'는 웹 서버 종류와 버전 정보를 알려줍니다. 공격자는 서버 헤더에서 제공하는 웹 서버 시스템 정보를 수집해 공격에 활용할 수 있기 때문에, 이를 알려주지 않도록 설정해야 합니다.

server_tokens 지시자 설정 변경하기

server_tokens 지시자를 설정한 경우 서버의 응답에 Nginx 버전이 전송되기 때문에 server_tokens 지시자 사용을 off로 설정해야 합니다.

1 ['터미널' 실행] > ['vi' 명령어 실행해 'nginx.conf' 파일 열기]

```
# vi /[nginx 설치 디렉터리]/nginx.conf
```

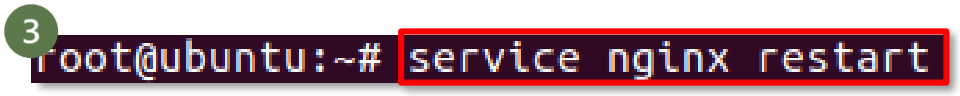
엔진엑스(NGINX)

② ['/http'를 입력하여 http {} 블록 검색] > ['i'를 통해 입력모드 진입] > ['server_tokens 'off'로 수정] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
http { } 블록 검색
server_tokens off;
```

③ ['터미널'에 'service nginx restart' 명령어 입력] > [서비스 다시 시작]

```
# service nginx restart
```



아파치(Apache)

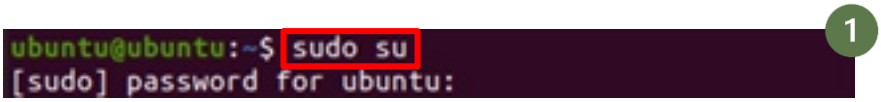
0. Apache 설치 디렉터리 확인하기

이번 장의 보안 설정을 위해 먼저 관리자 권한으로 전환한 뒤, Apache의 설치 위치를 알아내야 합니다. 일반적으로 Apache는 '/etc/apache2/' 및 '/usr/share/apache2' 디렉터리에 설치됩니다. 하지만 구체적인 경로는 설치 방법과 버전에 따라 다를 수 있습니다. 따라서 다음에서 소개하는 명령어를 통해 설치 경로를 확인해야 합니다.

관리자 권한으로 전환하기

1. ['터미널' 실행] > ['su' 명령어를 통한 root 계정 전환] > [root 패스워드 입력]

```
sudo su
```

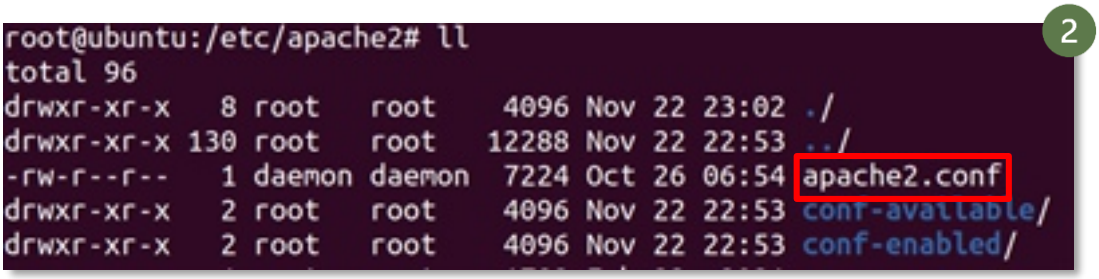


Apache 설치 위치 확인하기

1. ['터미널' 실행] > [하단의 'whereis' 명령어로 Apache 실행 파일 위치 확인]

```
whereis apache2
apache2: /etc/apache2 /usr/share/apache2
```

2. [주요 설정 파일인 /etc/apache2 내부의 apache2.conf]



아파치(Apache)

1. 소스 파일 쓰기 권한 제거하기

이용자가 웹 서버의 설정 파일 및 웹 사이트 소스 파일을 임의로 수정 또는 삭제할 수 있으면 홈페이지 변조, 백도어 삽입과 같은 웹 사이트에 대한 공격을 수행할 수 있습니다. 그 결과 웹 서버에 저장된 데이터가 유출되거나, 서버가 오작동해 사용 불능 상태에 빠질 수 있습니다.

daemon으로 소유자 변경하기

daemon은 일반적으로 시스템에서 제한된 권한을 가진 사용자로, 최소한의 권한만을 부여받아 동작합니다. 만약 Apache가 특정 파일을 실행해야 하는 경우, 이를 위해 daemon 사용자에게 제한적인 권한만을 부여함으로써 보안을 강화할 수 있습니다.

1. ['터미널' 실행] > [하단의 'chown' 명령어를 통해 Daemon으로 소유자 변경]

```
chown -R daemon:daemon /[apache 설치 경로]/*.conf
```

파일 또는 디렉터리를 만든 사용자에게만 권한 부여하기

Apache 설치 경로 안에 있는 모든 '.conf' 파일들의 권한을 700으로 변경합니다. 700은 숫자로 표현된 권한 값으로, 파일 소유자에게만 읽기, 쓰기, 실행 권한을 부여하고, 그룹과 다른 사용자에게는 어떠한 권한도 주지 않는 설정입니다.

1. ['터미널' 실행] > [하단의 'chmod' 명령어를 통해 소유자에게만 권한 부여]

```
chmod 700 /[apache 설치 경로]/*.conf
```

1
```
root@ubuntu:~# chown -R daemon:daemon /etc/apache2/*.conf
root@ubuntu:~# chmod 700 /etc/apache2/*.conf
```

아파치(Apache)

2. 디렉터리 정보 노출 감추기

디렉터리 리스팅은 웹 서버의 디렉터리 구조가 외부에 노출되는 것을 말합니다. 디렉터리 리스팅 기능이 활성화 되어있으면, 누구나 웹서버 안의 파일에 접근할 수 있습니다. 이를 통해 웹서버에 저장된 데이터가 유출될 수 있으므로 디렉터리 리스팅 기능을 비활성화 해야 합니다.

설정 파일에서 디렉터리 리스팅 설정 코드 추가하기

텍스트 편집 명령어인 vi를 사용하여 Apache의 설정 파일인 'apache2.conf'를 열어줍니다. 해당 파일에서 <Directory> 블록 내부에 Options -Indexes 코드를 삽입합니다.

1. ['터미널' 실행] > [하단의 'vi' 명령어 실행해 'apache2.conf' 파일 열기]

```
vi /[apache 설치 디렉터리]/apache2.conf
```

1
```
root@ubuntu:~# vi /etc/apache2/apache2.conf
```

2. ['/<Directory />'를 입력하여 <Directory /> 블록 검색] > ['i'를 통해 입력모드 진입] > [하단의 'Options' 내용 삽입] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
<Directory /> </Directory> 블록 찾기
Options -Indexes 코드 삽입
```

2
```
<Directory />
        Options -Indexes
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>
```

3. ['터미널'에 'service apache2 restart' 명령어 입력] > [서비스 다시 시작]

```
service apache2 restart
```

3
```
root@ubuntu:~# service apache2 restart
```

아파치(Apache)

3. 로그파일 관리하기

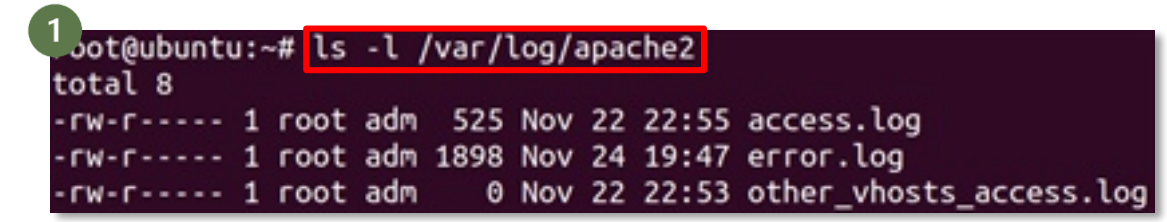
로그 파일은 시스템 및 애플리케이션의 활동을 기록하는 중요한 도구입니다. 그러나 로그파일은 그 특성상 시스템의 중요한 정보도 함께 담고 있습니다. 따라서 로그 파일에 대한 권한 관리가 중요합니다. 로그 파일에 저장된 정보가 공격자에게 노출되면, 시스템의 취약점을 찾아내거나 공격을 계획하는 데 활용될 수 있습니다.

로그파일 소유자 변경하기

일반적으로 Apache 로그 파일은 /var/log/apache2에 위치합니다. 'ls -l' 명령어를 통해 해당 경로에서 전체 로그 파일을 확인합니다. 아래 명령어를 실행하여 /var/log/apache2/ 폴더와 하위 파일 및 폴더의 소유자를 변경할 수 있습니다

1. ['터미널' 실행] > [하단의 'ls -l' 명령어 실행해 전체 로그파일 확인]

```
ls -l /var/log/apache2/
```



2. [하단의 'chown' 명령어 실행해 로그파일 소유자 변경]

```
chown -R [apache 사용자]:[apache 그룹] /var/log/apache2/
```

3. ['터미널'에 'service apache2 restart' 명령어 입력] > [서비스 다시 시작]

```
service apache2 restart
```

아파치(Apache)

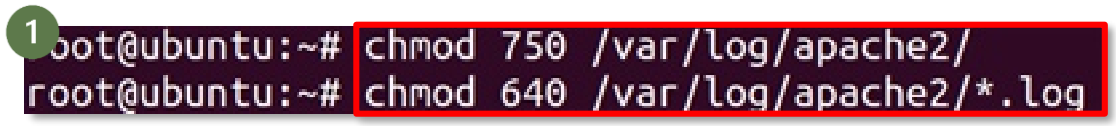
로그 폴더 및 로그파일 권한 변경하기

로그 폴더에 대해 750 권한을 부여합니다. 750은 숫자로 표현된 권한 값으로, 소유자에게 읽기, 쓰기, 실행 권한을, 그룹에는 읽기와 실행 권한을 부여하고, 기타 사용자에게는 어떠한 권한도 주지 않음을 의미합니다.

로그 파일에 대해서는 640 권한을 부여합니다. 640은 숫자로 표현된 권한 값으로, 사용자에게 읽기와 쓰기 권한을 주고, 그룹에는 읽기 권한을 주며, 기타 사용자에게는 어떠한 권한도 주지 않음을 의미합니다.

1. ['터미널' 실행] > [하단의 'chmod' 명령어 실행해 대상 폴더 및 파일 권한 변경] > [하단의 'chown' 명령어 실행해 로그파일 소유자 변경]

```
chmod 750 /var/log/apache2/
chmod 640 /var/log/apache2/*.log
```



2. ['터미널'에 'service apache2 restart' 명령어 입력] > [서비스 다시 시작]

```
service apache2 restart
```

아파치(Apache)

4. HTTP 메소드 사용 제한하기

보안을 강화하기 위해 웹 통신에서 잘 사용되지 않는 메소드인 PUT, DELETE 등의 메소드 사용을 비활성화해야 합니다. 이러한 메소드가 활성화되어 있으면 공격자가 서버의 파일을 임의로 삭제하거나 업로드하여 시스템에 피해를 줄 수 있습니다.

불필요한 메소드 비활성화하기

PUT 메소드는 웹 서버에 파일을 생성할 수 있고, DELETE는 웹 서버의 파일을 삭제할 수 있어 사용을 제한해야 합니다. 또한 OPTIONS, TRACE 메소드는 웹 서버에서 허용한 메소드 정보를 알 수 있어 공격자에게 불필요한 정보를 줄 수 있어 사용되어서는 안됩니다.

1 ['터미널' 실행] > [하단의 'vi' 명령어 실행해 'apache2.conf' 파일 열기]

```
vi /[apache 설치 디렉터리]/apache2.conf
```

아파치(Apache)

2 ['/<Directory />'를 입력하여 <Driectory /> 블록 검색] > ['i'를 통해 입력모드 진입] > [하단의 'LimitExcept' 내용 삽입] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
<Directory /> </Directory> 블록 찾기
아래 코드 삽입
<LimitExcept PUT DELETE OPTIONS TRACE>
        Order deny,allow
        Deny from all
    </LimitExcept>
```

2

```
<Directory />
        Options -Indexes
        Options FollowSymLinks
        AllowOverride None
        Require all denied
        <LimitExcept PUT DELETE OPTIONS TRACE>
                Order deny,allow
                Deny from all
        </LimitExcept>
</Directory>
```

3 ['터미널'에 'service apache2 restart' 명령어 입력] > [서비스 다시 시작]

```
service apache2 restart
```

3

```
root@ubuntu:~# service apache2 restart
```

메소드명	권장설정	상 세 설 명
GET	허용	데이터를 요청할 때 사용하는 메소드
POST	허용	데이터를 요청하거나 변경할 때 사용하는 메소드
HEAD	허용	데이터를 요청하는 경우 HTTP Header 정보만 전송하는 메소드로 해당 자원이 존재하는 지 확인할 때 사용
PUT	비허용	데이터를 생성할 때 사용하는 메소드로 웹 서버에 임의의 파일 생성 가능
DELETE	비허용	데이터를 삭제할 때 사용하는 메소드
OPTIONS	비허용	응답가능한 HTTP 메소드 정보를 요청하는 메소드
TRACE	비허용	요청한 내용을 그대로 반환하는 메소드

아파치(Apache)

5. 심볼릭 링크 사용 제한하기

심볼릭 링크의 기능을 악용하는 경우 관리자 권한을 탈취하는 형태의 공격이 가능합니다. 관리자 권한은 시스템 전체를 제어할 수 있어 공격에 악용되면 심각한 문제를 일으킬 수 있습니다. 이를 막기 위해 웹 서버에서 심볼릭 링크 사용을 제한해야 합니다.

심볼릭 링크란 무엇인가요?

심볼릭 링크는 컴퓨터에서 중요한 파일이나 폴더에 빠르게 접근할 수 있도록 도와주는 기능으로 마치 컴퓨터에서의 바로 가기 아이콘과 비슷한 역할을 합니다. 심볼릭 링크를 사용하면 복잡한 디렉터리 구조에서도 필요한 파일에 쉽게 접근할 수 있습니다. 그러나 이 기능을 사용할 때는 보안상 주의가 필요하며 신중하게 다뤄야 합니다.

예를 들어, 관리자 권한이 필요한 파일에 심볼릭 링크가 걸려 있다면, 해당 심볼릭 링크를 통해 관리자가 아닌 사람도 접근할 수 있는 보안 취약점이 발생할 수 있습니다.

설정 파일에서 FollowSymLinks 옵션 지우기

이 설정 시 **주의할 점은 서버 루트(/)가 아닌 웹 루트(var/~)**의 FollowSymLinks 옵션을 지워야 한다는 점입니다.

1. ['터미널' 실행] > [하단의 'vi' 명령어 실행해 'apache2.conf' 파일 열기]

```
vi /[apache 설치 디렉터리]/apache2.conf
```

아파치(Apache)

2 ['/<Directory /var>'를 입력하여 <Directory /var> 블록 검색] > ['I'를 통해 입력모드 진입] > [하단의 'FollowSymLinks' 내용 삭제] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
<Directory /var> </Directory> 블록 찾기
(서버 루트(/)가 아니어야 함)

FollowSymLinks 코드 지우기
# Options Indexes FollowSymLinks
```

3 ['터미널'에 'service apache2 restart' 명령어 입력] > [서비스 다시 시작]

```
service apache2 restart
```

아파치(Apache)

6. 서버 정보 숨기기

HTTP 응답 헤더 중 '서버 헤더'는 웹 서버 종류와 버전 정보를 알려줍니다. 공격자는 서버 헤더에서 제공하는 웹 서버 시스템 정보를 수집해 공격에 활용할 수 있기 때문에, 이를 알려주지 않도록 설정해야 합니다.

보안 설정파일 내 ServerTokens 수정하기

서버의 버전 정보를 감추기 위해서는 [apache 설치 디렉터리] 아래 'conf-available' 폴더의 'security.conf' 파일을 수정해야 합니다. 파일 내용 중 'ServerTokens' 설정 값을 수정하여 서버 정보의 공개 범위를 결정할 수 있습니다. 웹 서버의 제품 정보만의 노출을 허용하는 최소 설정 값인 Prod로 설정하는 것이 권장됩니다.

1. ['터미널' 실행] > [하단의 'vi' 명령어 실행해 'security.conf' 파일 열기]

```
vi /[apache 설치 디렉터리]/conf-available/security.conf
```

2. ['/ServerTokens'를 입력하여 ServerTokens 옵션 검색] > ['i'를 통해 입력모드 진입] > [하단의 'ServerTokens' 설정 값 수정] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
ServerTokens 설정 값을 Prod로 수정하기
ServerTokens Prod
```

3. ['터미널'에 'service apache2 restart' 명령어 입력] > [서비스 다시 시작]

```
service apache2 restart
```

이번 장에서는 회사에서 많이 사용하는 DBMS에 대한 보안 설정 방안을 설명하고자 합니다. 최소한의 보안 설정을 통해 데이터베이스의 보안을 향상하는 방안을 간단하고 쉽게 설명하겠습니다.

DBMS란 무엇인가요?

여러분들이 사용하는 포털사이트(네이버, 다음 등)의 아이디와 비밀번호, 은행 계좌 정보, 신용카드 거래 명세서와 같은 정보들을 데이터(Data)라고 합니다. 이 외에도 수많은 데이터들은 데이터의 집합인 데이터베이스(DataBase, DB)에 저장되어 관리되고, 이러한 데이터베이스에 저장된 정보들을 체계적으로 관리하고 운영할 수 있게 도와주는 소프트웨어가 바로 DBMS(Data Base Management System)입니다.

DBMS 보안은 왜 해야 할까요?

DBMS 보안은 공격자로부터 회사의 중요 정보를 안전하게 보호하는 데 필수적입니다. 회사의 데이터베이스에는 사내의 기밀, 사용자와 고객의 개인 정보와 같은 매우 중요한 정보들이 저장되어 있습니다. 따라서, 외부 유출이나 해킹 공격 등의 위협 으로부터 회사의 정보 자산을 안전하게 보호하기 위해서는 DBMS 보안이 매우 중요합니다.

가이드라인에서 다루는 제품 확인하기

▲ MS SQL ▲ Postgre SQL ▲ MySQL

가이드라인에서 다루는 소프트웨어 확인하기

데이터베이스를 관리하기 위한 방법은 대표적으로 DB 서버에 직접 접속한 뒤 쿼리문을 사용하는 것과 시각적이고 직관적인 UI 전용 소프트웨어를 사용하는 것이 있습니다. 본 가이드라인에서는 위 2가지 방법을 사용한 항목별 보안 조치 사항과 각 DBMS 별로 특화된 전용 소프트웨어 설치 방법을 설명합니다.

▲ MS SQL의 SSMS

▲ Postgre SQL의 pgAdmin

▲ MySQL의 MySQL Workbench

MS-SQL

0. SSMS 설치하기

Microsoft SQL은 SSMS(SQL Server Management Studio)라는 전용 UI 소프트웨어를 제공합니다. 본 가이드라인에서는 SSMS를 사용한 항목별 보안 조치 사항을 설명하며, 이번 장에서는 SSMS를 설치하고 기본 설정하는 방법을 설명합니다.

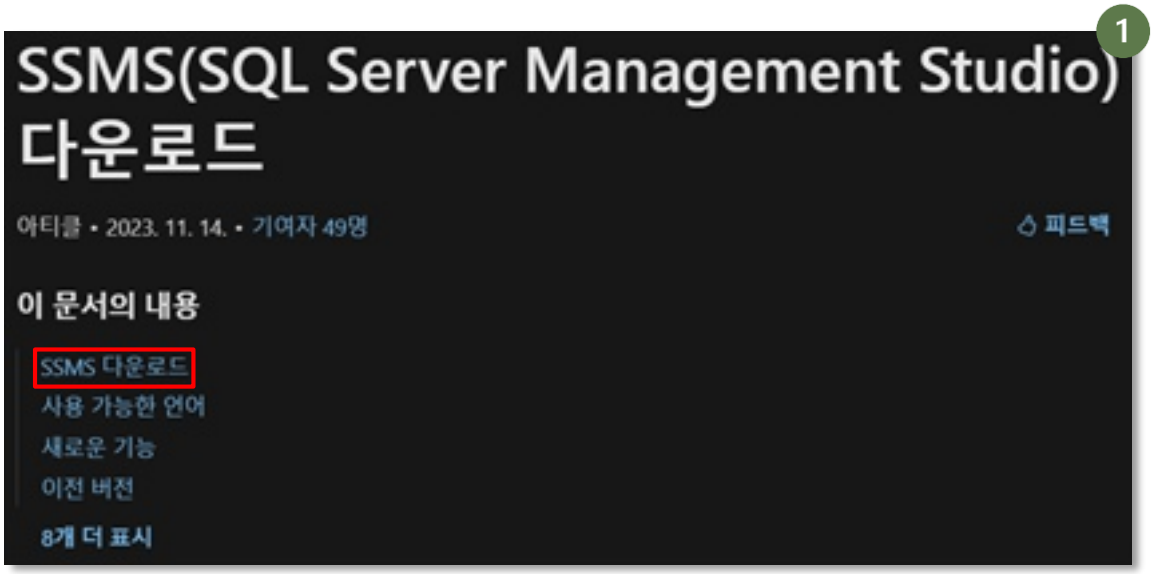
SSMS(SQL Server Management Studio)란?

SSMS(SQL Server Management Studio)는 Microsoft SQL Server를 관리하기 위한 인터페이스 환경입니다. 데이터베이스 관리자와 개발자가 하나의 인터페이스에서 SQL Server를 구성하고 개발 및 유지, 관리를 할 수 있도록 설계되었으며, UI를 기본으로 제공하여 보다 쉽게 DB를 관리할 수 있습니다.

https://learn.microsoft.com/ko-kr/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16 - SSMS 다운로드 링크

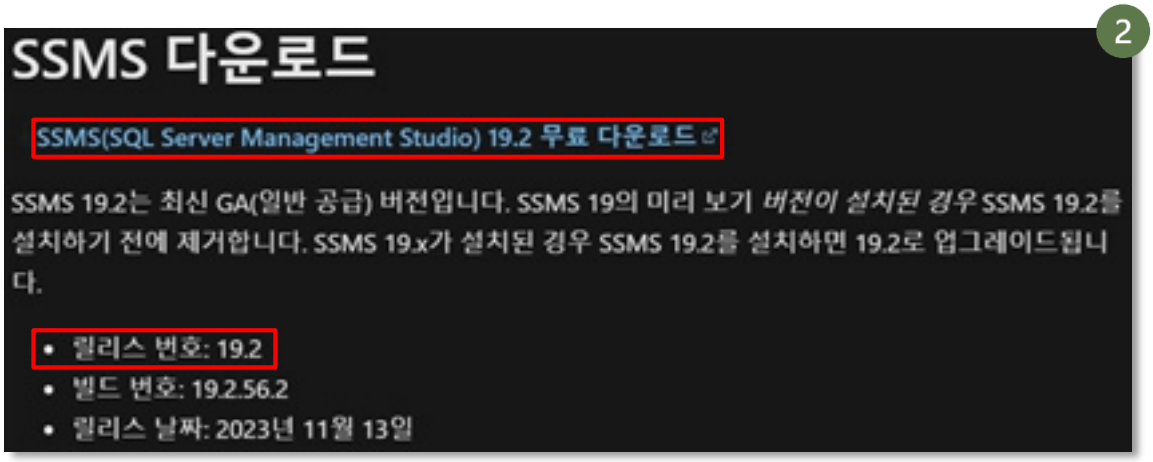
SSMS (SQL Server Management Studio) 설치하기

1. [위 다운로드 링크 클릭] > ['SSMS 다운로드' 클릭]

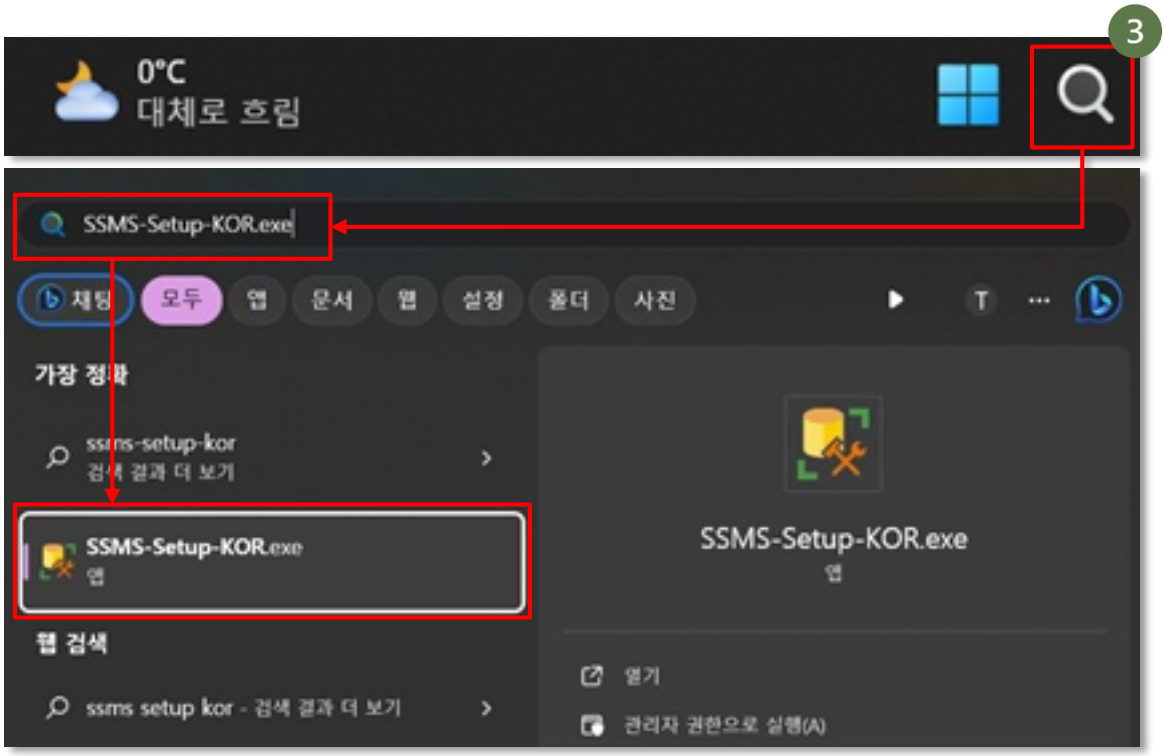


MS-SQL

2 ['무료 다운로드' 링크 클릭 후 파일 다운로드 (릴리스 번호: 19.2)]
* 2023.12.11 기준 최신 버전: 19.2

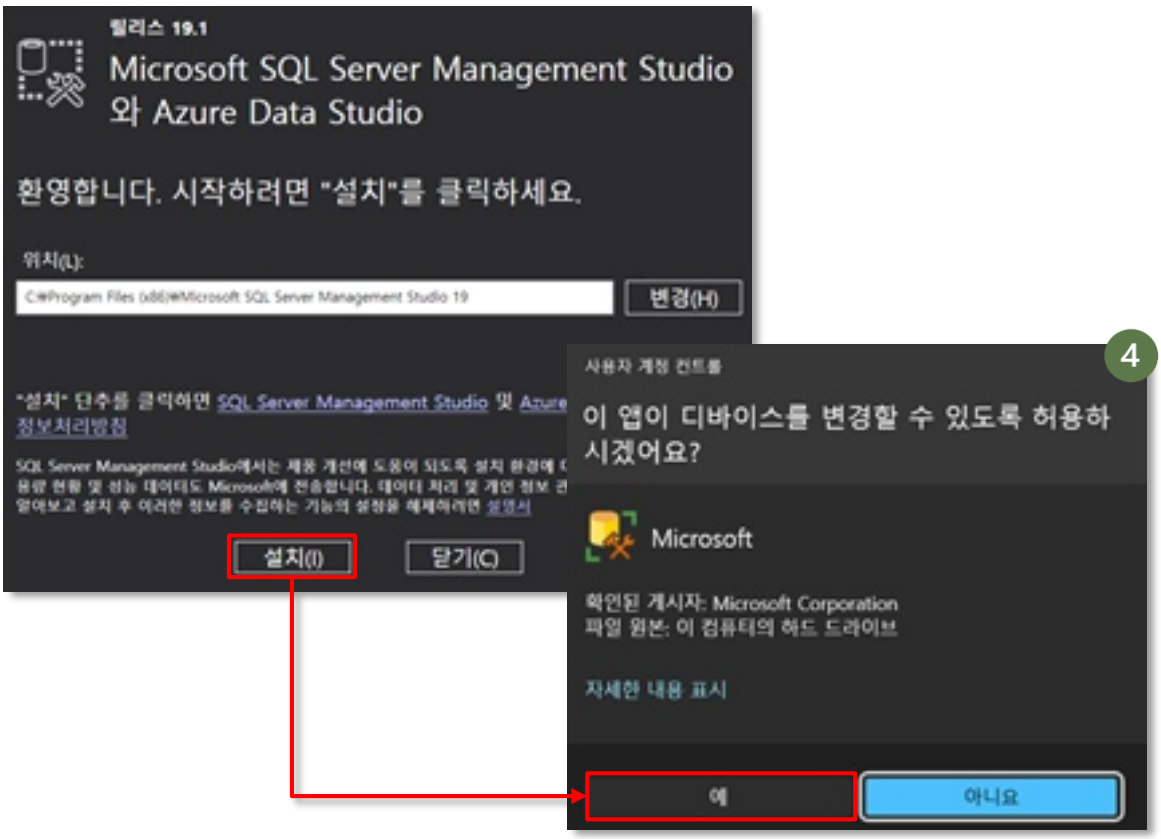


3 [다운로드 완료 후 윈도우 검색창에 'SSMS-Setup-KOR' 검색 후 실행]

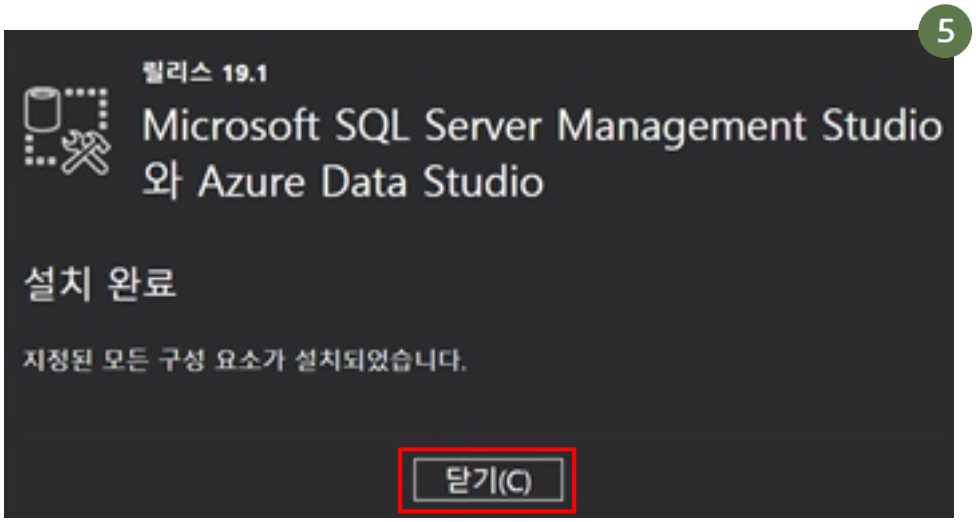


MS-SQL

4 [설치화면에서 '설치(I)' 클릭] > [알림창의 '예' 클릭]

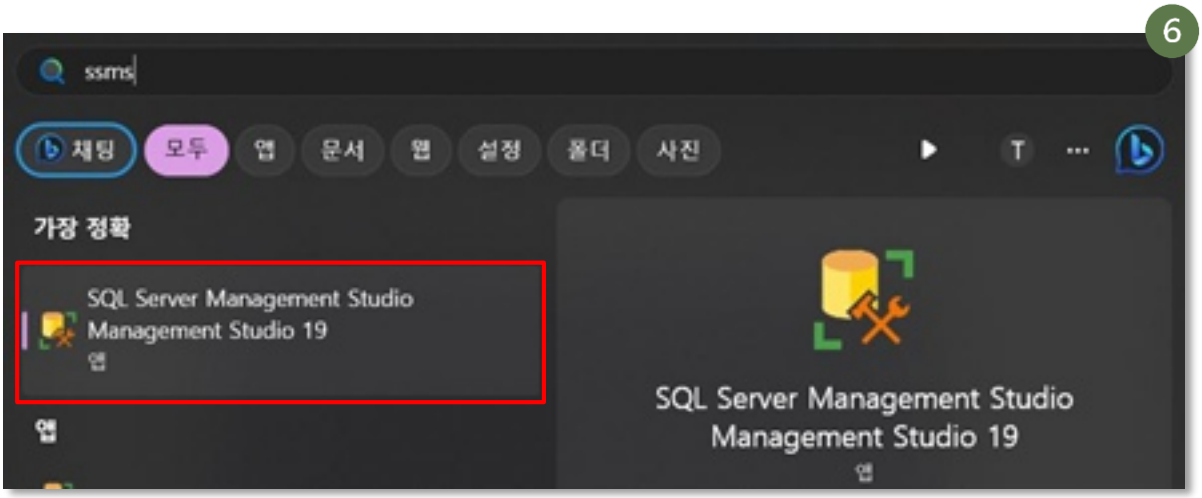


5 [설치완료 후 '닫기' 클릭]

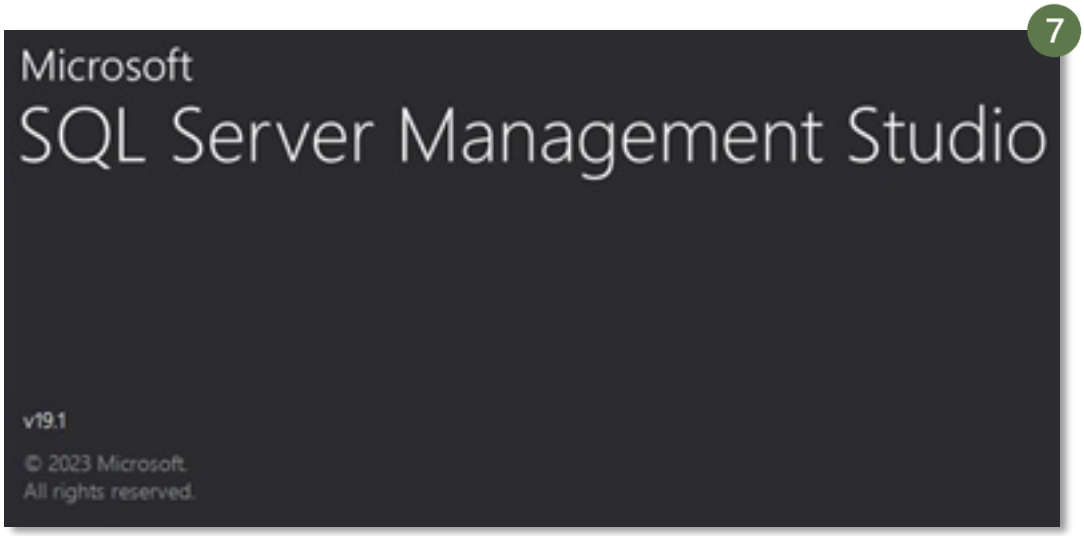


MS-SQL

6 [윈도우 검색창에 'ssms' 검색]

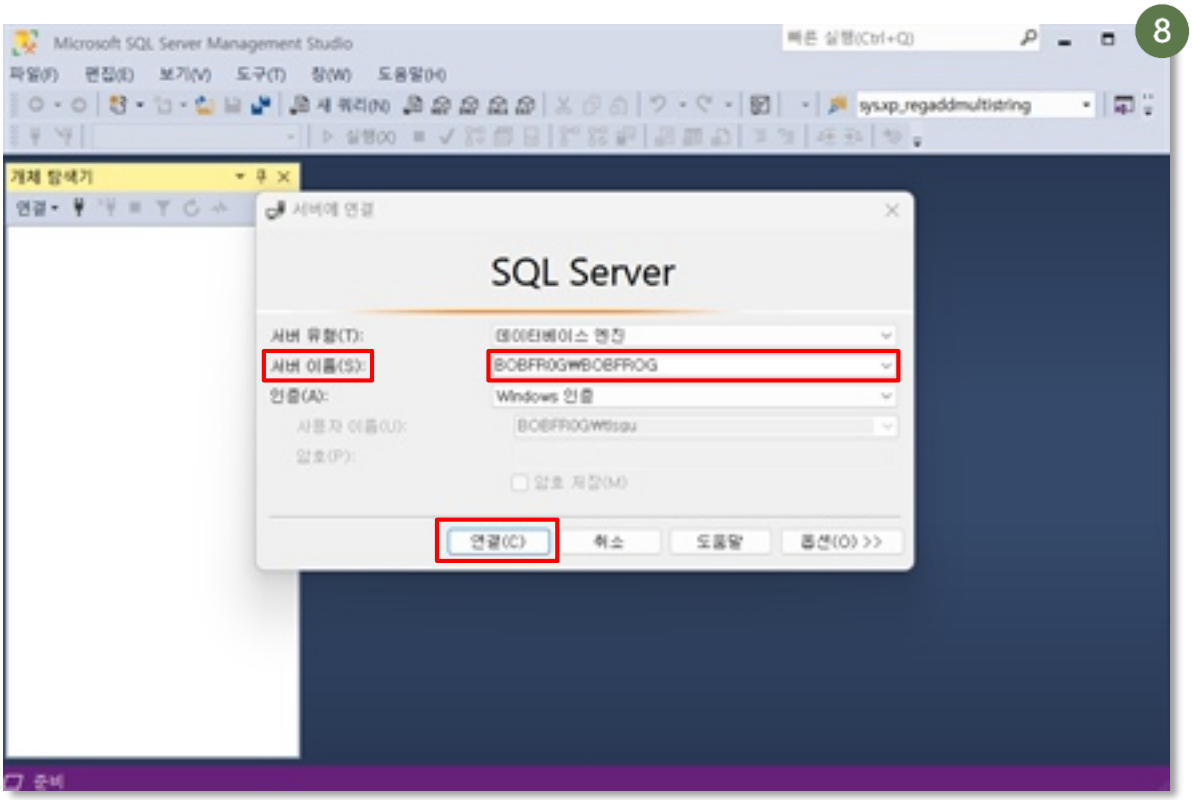


7 ['SQL Server Management Studio Management Studio 19' 실행]



MS-SQL

8 [SSMS 메인 화면에서 서버 이름 확인 후 '연결(C)' 클릭]



기존에 MS SQL설치 된 경우

기존에 설치되어 있는 MS SQL DB가 존재한다면 이를 SSMS에서 자동으로 인식, 연결이 가능합니다.

MS-SQL

1. 포트 관리하기

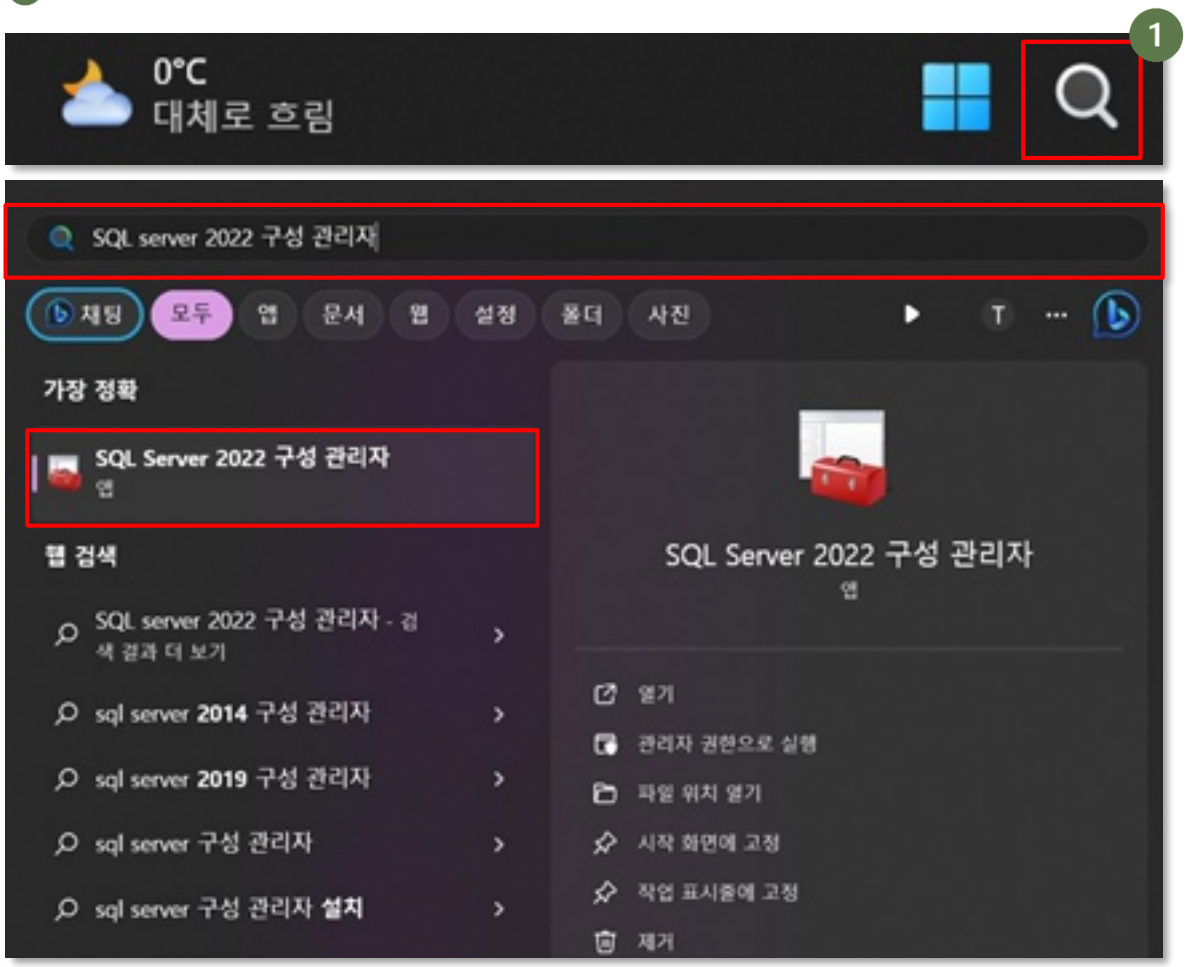
MS SQL 데이터베이스는 설치 시 기본적으로 1433번 포트를 사용합니다. 하지만 해당 포트는 널리 알려져 있어 외부 공격에 취약할 수 있습니다. 따라서, 보안을 강화하기 위해 별도의 포트 번호를 설정하여 사용해야 합니다.

포트(Port)란?

포트는 컴퓨터가 네트워크를 통해 정보를 주고받을 때 사용하는 통로를 의미합니다.

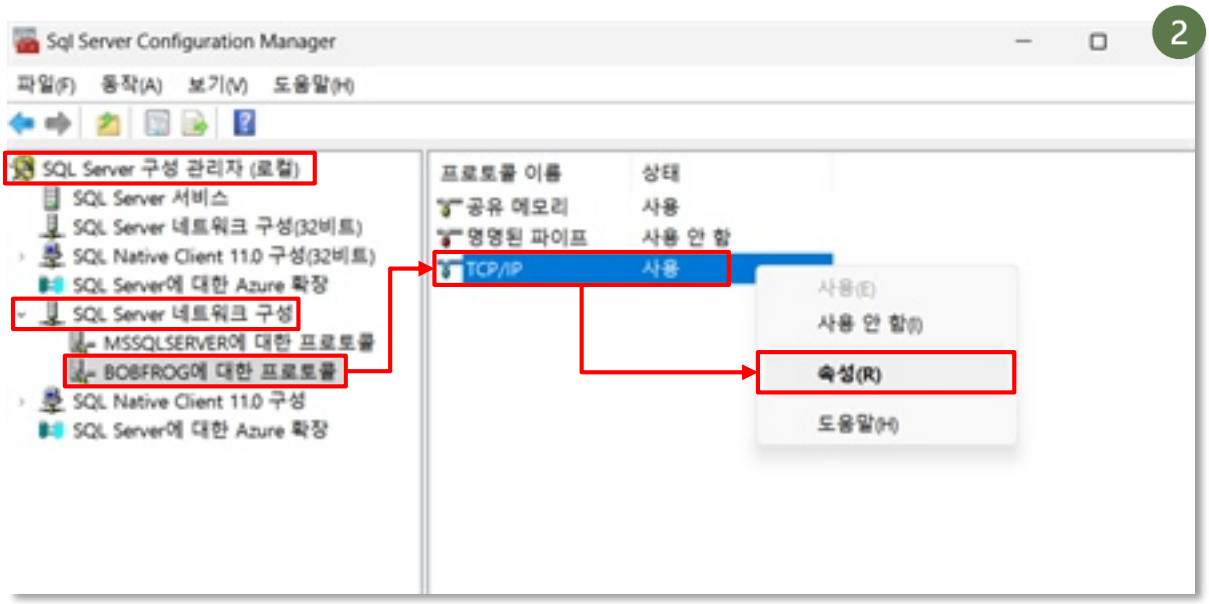
기본 포트번호 변경하는 방법

1. [윈도우 검색창에 'SQL Server 2022 구성 관리자' 검색 후 클릭]

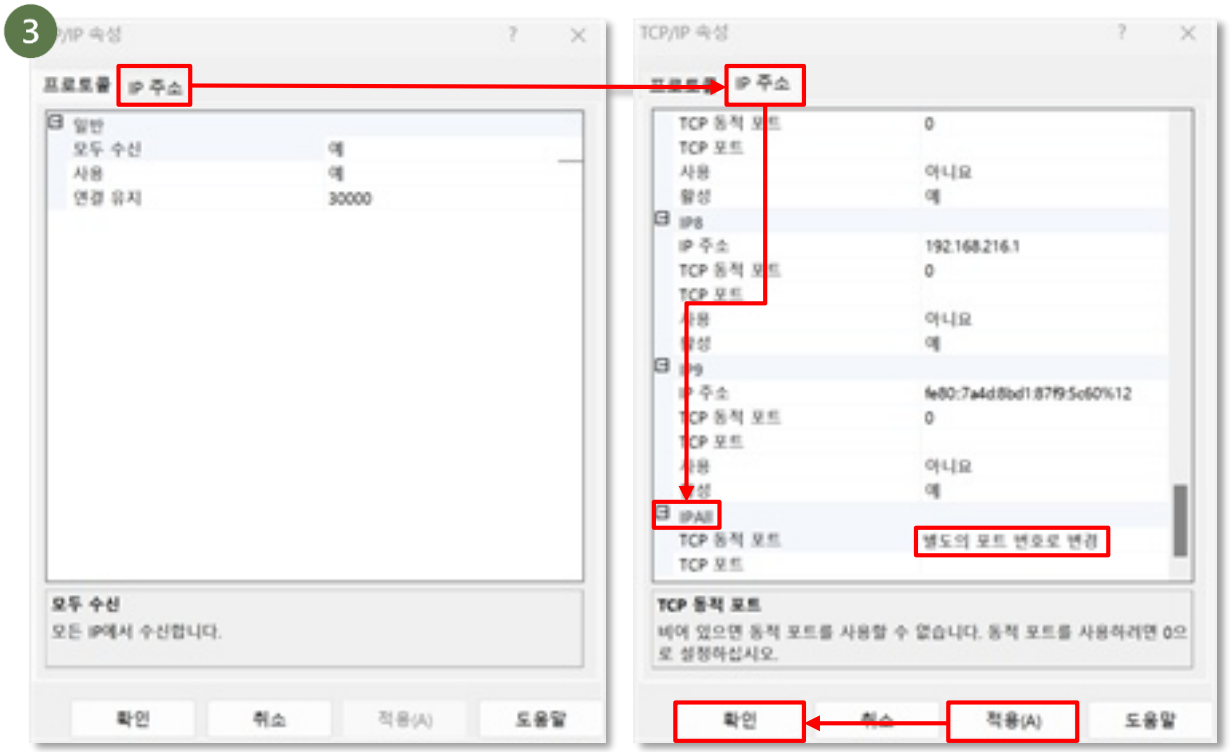


MS-SQL

2 [좌측의 'SQL Server 구성 관리자(로컬)'] > ['SQL Server 네트워크 구성'] > [하위 항목에서 '(서버명)에 대한 프로토콜' 클릭] > ['TCP/IP' 우클릭 후 '속성' 선택]



3 ['IP 주소' 선택] > ['IPALL' 부분의 'TCP 동적 포트' 부분을 별도의 포트 번호로 변경] > [변경 후 '적용' 클릭] > ['확인' 클릭]



MS-SQL

2. 일반 계정 관리하기

직원이 회사를 떠나거나, 테스트를 목적으로 계정을 생성한 뒤에 계정을 삭제하지 않는 경우가 종종 있습니다. 데이터베이스에 현재 사용하지 않는 계정이 존재할 경우, 공격자의 접근 통로가 되어 데이터 조회, 변경, 삭제 등의 침해사고가 발생할 수 있습니다. 따라서, 해당 계정들은 사용 여부를 검토한 뒤 삭제하는 것을 권장합니다.

삭제하면 안되는 MS SQL 기본 계정 목록

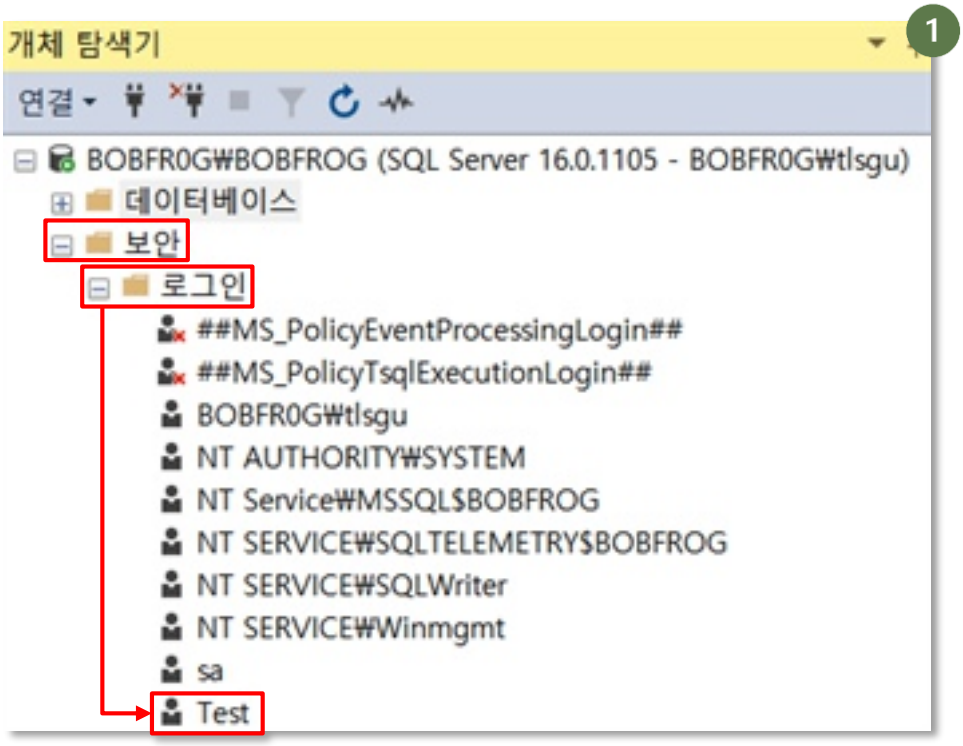
MS SQL에는 관리를 목적으로 생성되는 기본 계정들이 있습니다. 계정 삭제 시 아래의 계정들은 삭제하지 않도록 주의해야 합니다.

삭제하면 안되는 MS SQL 기본 계정 목록	
계 정 명	상 세 설 명
##MS_PolicyEventProcessingLogin##	SQL Server의 정책 평가와 관련된 작업을 수행하는 데 사용
##MS_PolicyTsqlExecutionLogin##	SQL Server의 정책 평가와 관련된 작업을 수행하는 데 사용
NT AUTHORITY\SYSTEM	Windows 시스템 계정. SQL Server에 대한 광범위한 권한을 가지며 일반적으로 서버 작업에 사용
NT Service\MSSQLSERVER	SQL Server 및 SQL Server Agent 서비스를 실행하는 데 사용
NT Service\SQLSERVERAGENT	SQL Server 및 SQL Server Agent 서비스를 실행하는 데 사용
NT SERVICE\SQLTELEMETRY	SQL Server와 관련된 다른 서비스를 실행하는 데 사용
NT SERVICE\SQLWriter	SQL Server와 관련된 다른 서비스를 실행하는 데 사용
NT SERVICE\Winmgmt	Windows Management Instrumentation (WMI) 서비스를 위한 계정
sa	데이터베이스의 모든 측면을 관리

MS-SQL

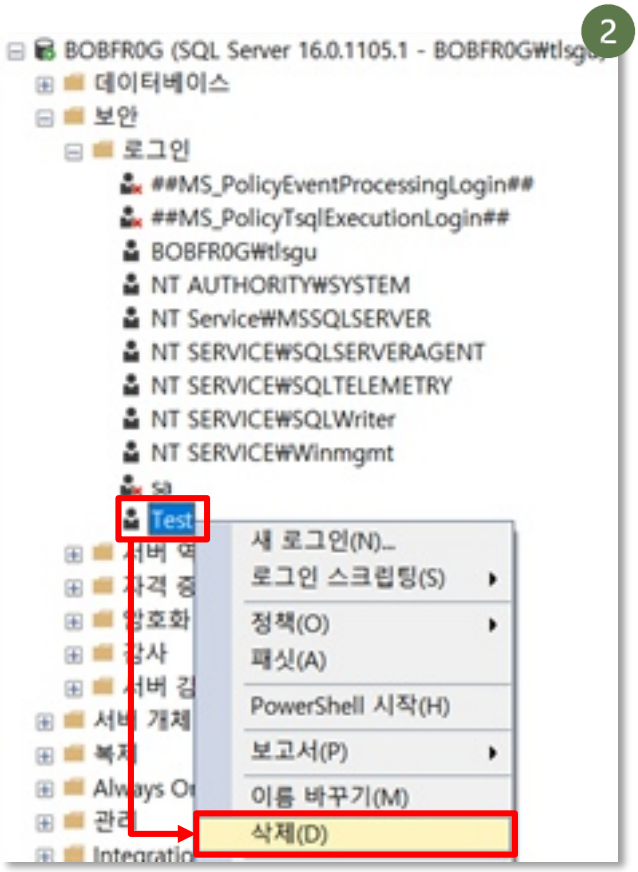
사용하지 않는 계정 삭제하는 방법 - UI 방식

1. [SSMS 개체탐색기] > [보안] > [로그인]



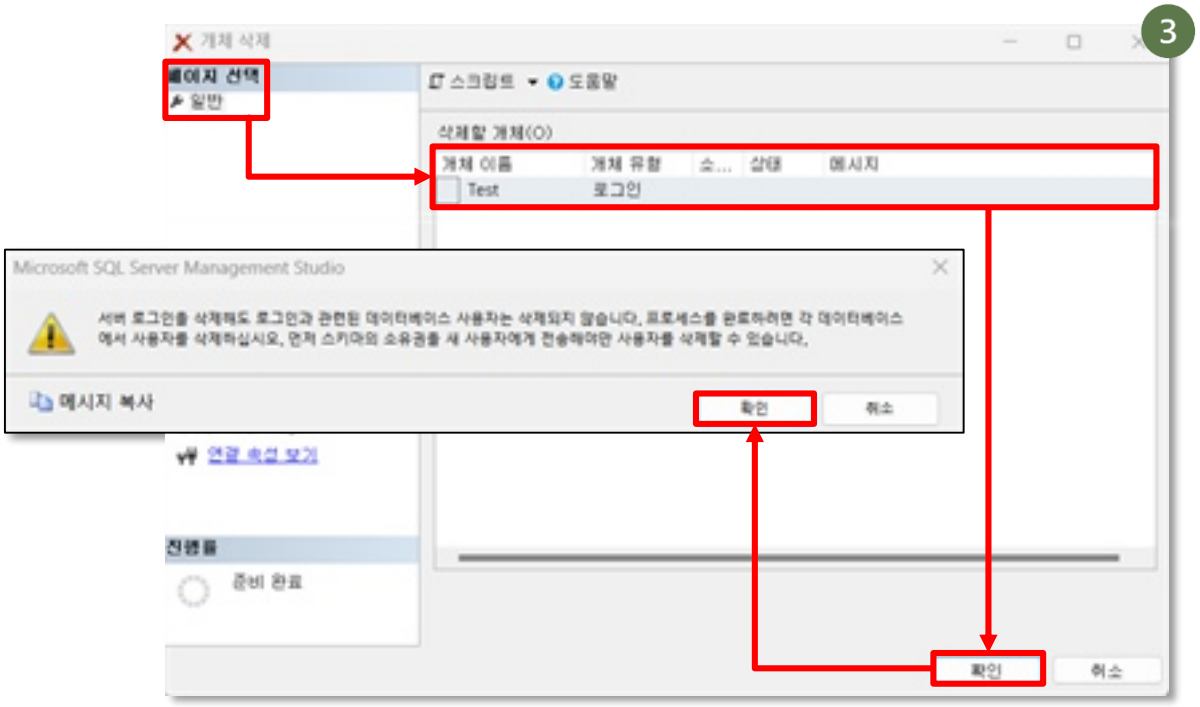
MS-SQL

② [해당 계정 우클릭 후 '삭제' 선택]



MS-SQL

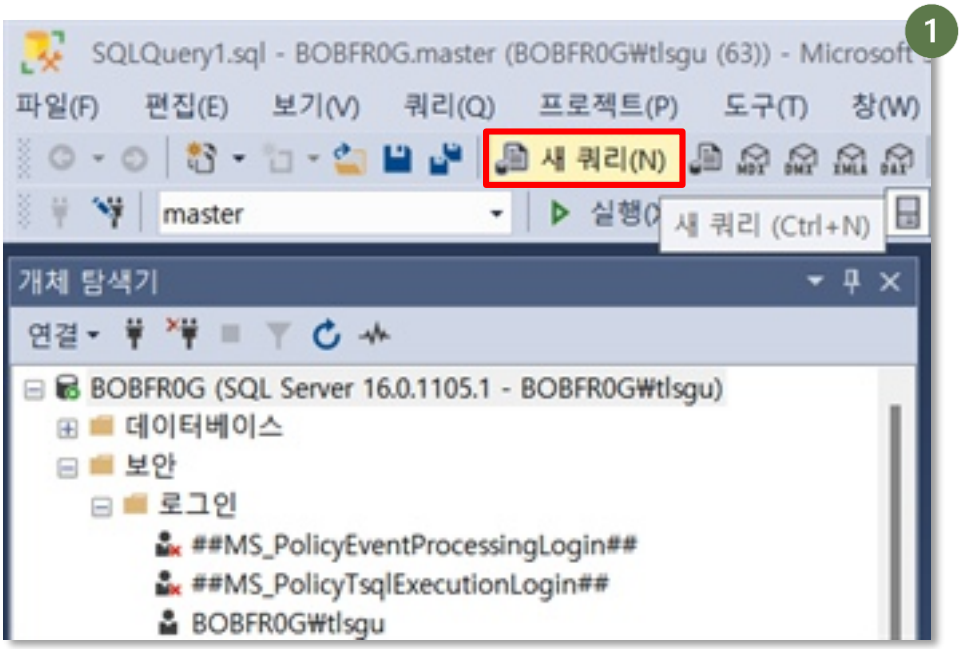
③ [삭제할 계정 체크 후 '확인' 클릭]



MS-SQL

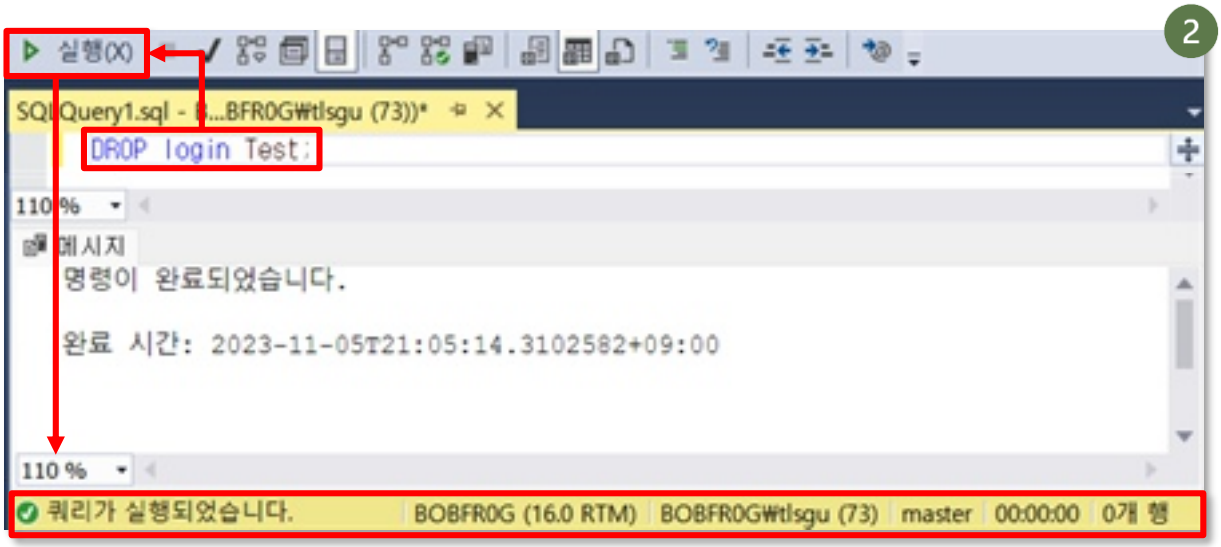
사용하지 않는 계정 삭제하는 방법 - 쿼리문 방식

1 [SSMS 메뉴바에서 '새 쿼리' 클릭]



2 [쿼리 창에 아래 쿼리문 작성] > [실행] > [결과 확인]

```
DROP login [삭제할 계정명];
```



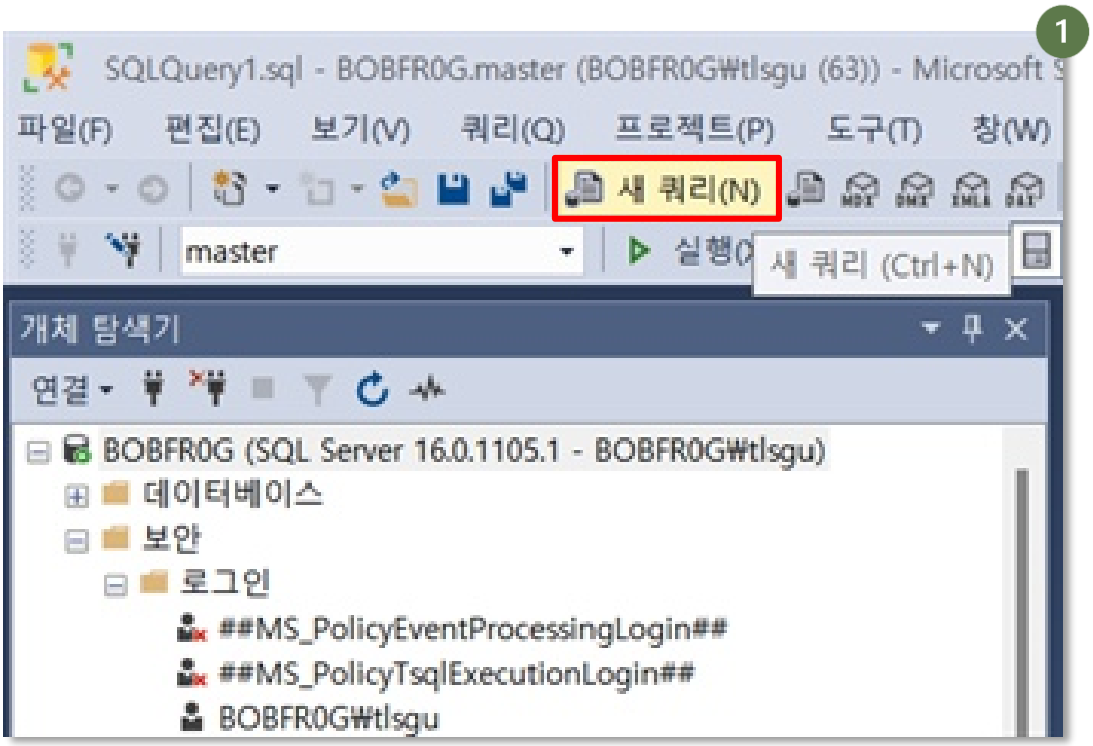
MS-SQL

3. SYSADMIN 권한 관리하기

SYSADMIN이란 SQL 서버와 데이터베이스에 대한 최상위 관리 권한입니다. 해당 권한이 일반 사용자 계정에 부여될 경우, 보안 설정을 변경하거나 데이터베이스를 손상시키는 등의 보안 위협을 초래할 수 있습니다. 따라서, 데이터베이스 서버의 안전한 운영을 위해 'SYSADMIN' 권한은 관리자 계정에만 부여하거나 최소화 해야 합니다.

SYSADMIN 권한 사용자 확인하기

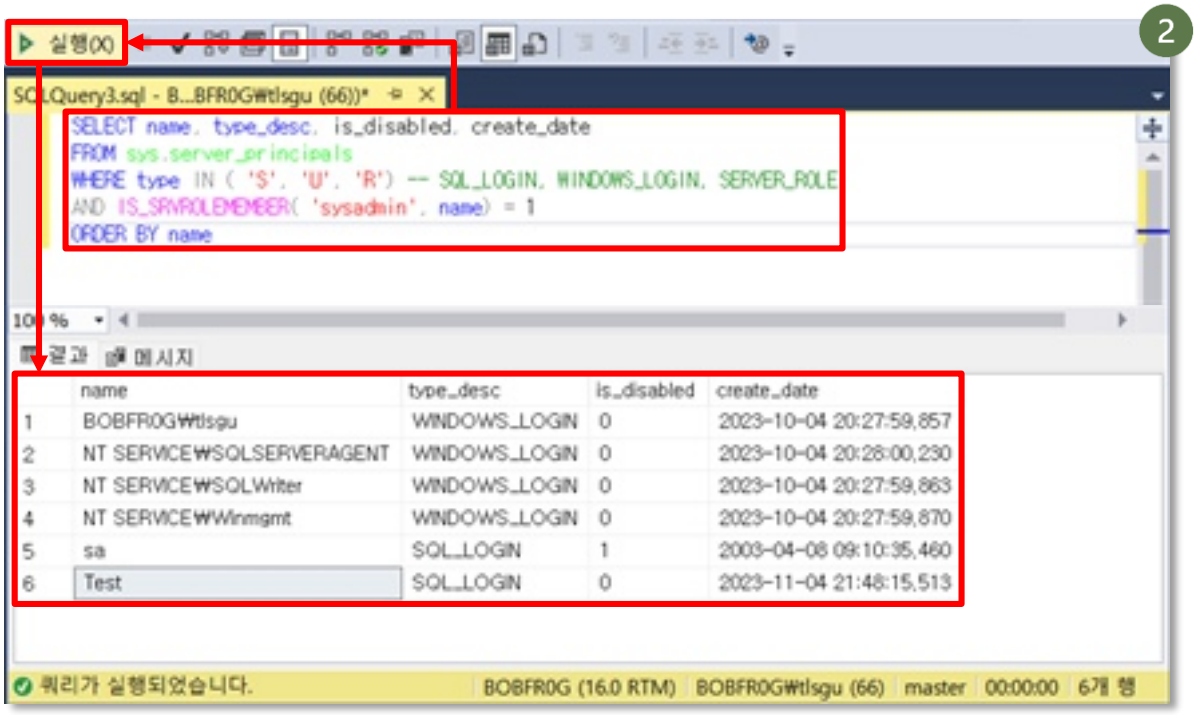
1 [SSMS 메뉴바에서 '새 쿼리' 클릭]



MS-SQL

② [쿼리 창에 아래 쿼리문 작성] > [실행] > [sysadmin 권한 사용자 확인]

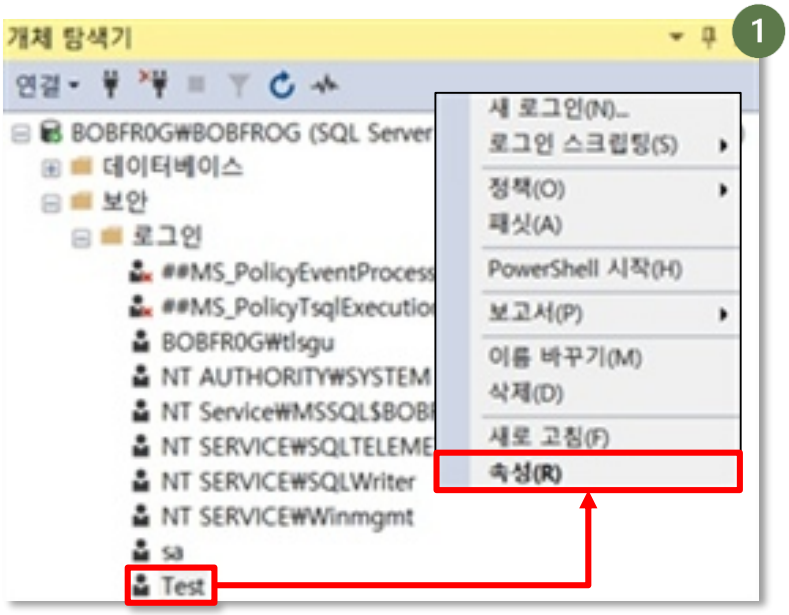
```
SELECT name, type_desc, is_disabled, create_date FROM sys.server_principals
WHERE type IN ( 'S', 'U', 'R') -- SQL_LOGIN, WINDOWS_LOGIN, SERVER_ROLE
AND IS_SRVROLEMEMBER( 'sysadmin', name) = 1 ORDER BY name
```



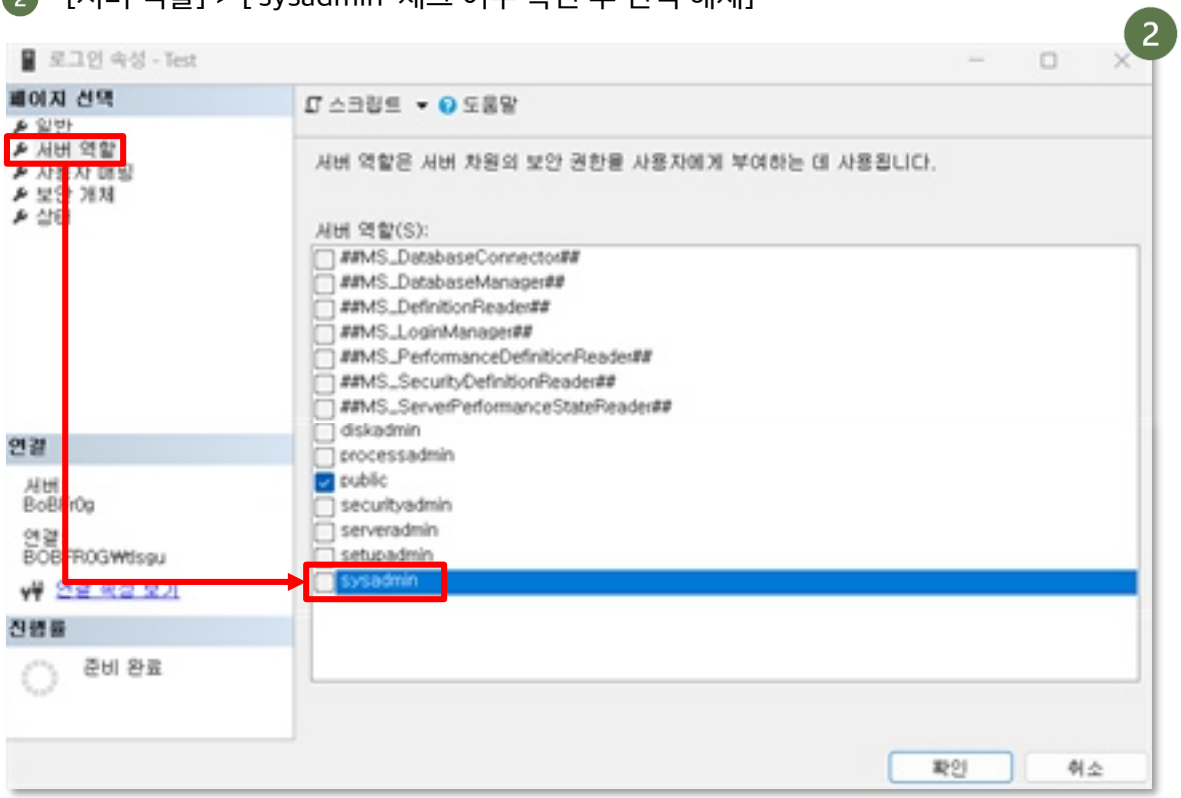
MS-SQL

SYSADMIN 권한 해제하기 - UI 방식

1. [SSMS 실행] > [개체탐색기] > [보안] > [로그인] > [권한 불필요 계정 확인] > [해당 계정 우클릭 후 '속성' 선택]



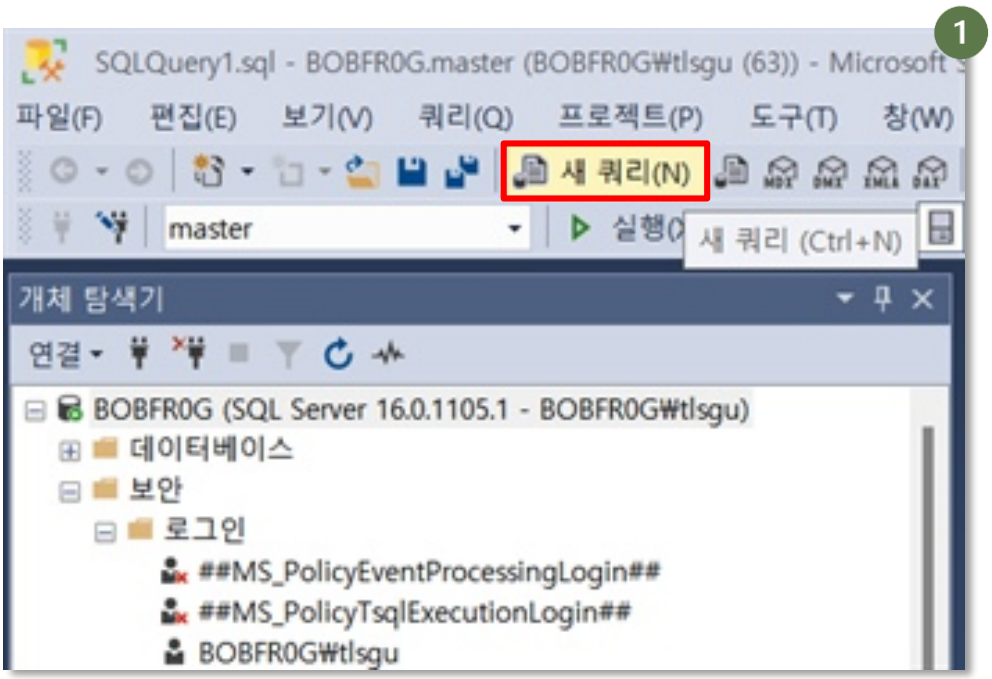
2. [서버 역할] > ['sysadmin' 체크 여부 확인 후 선택 해제]



MS-SQL

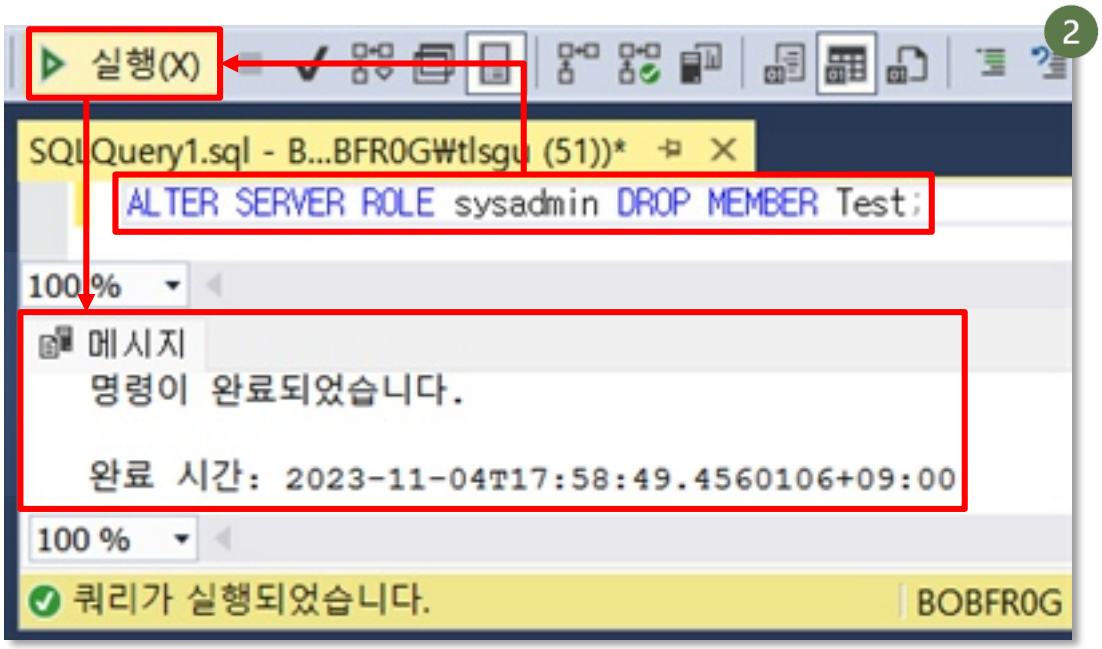
SYSADMIN 권한 해제하기 - 쿼리문 방식

1 [SSMS 메뉴바에서 '새 쿼리' 클릭]



2 [쿼리 창에 아래 쿼리문 작성] > [실행] > [결과 확인]

```
ALTER SERVER ROLE sysadmin DROP MEMBER [권한 불필요 계정명];
```



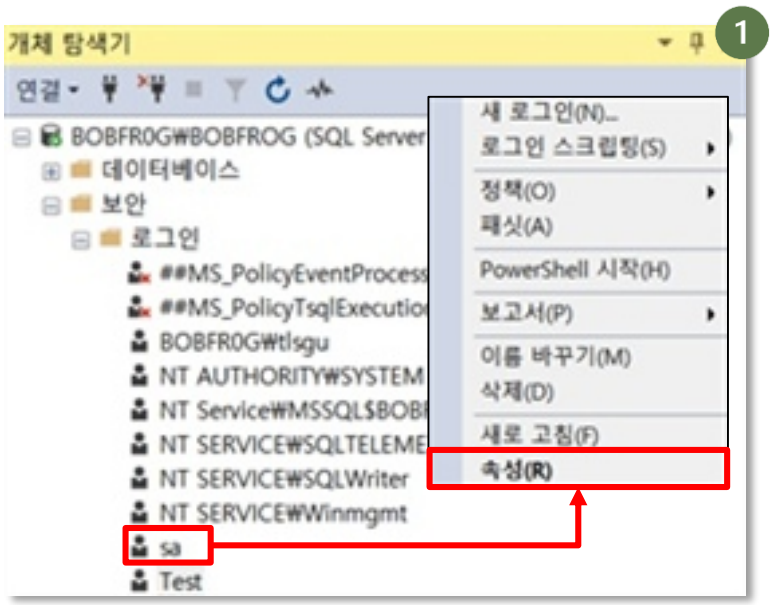
MS-SQL

4. sa 계정 관리하기

sa 계정은 MS-SQL 설치 시 기본적으로 설치되는 계정이며 sysadmin 권한을 가지고 있습니다. 서버 내 최고 권한인 sysadmin 권한을 가진 계정인 만큼 해커의 목표가 되기 쉽고, 탈취당했을 경우 심각한 피해를 유발할 수 있습니다. 따라서, 해당 계정을 비활성화하여 접근을 방지하고 데이터베이스의 보안을 강화해야 합니다.

sa 계정 비활성화 하기 - UI 방식

1. [SSMS 개체탐색기] > [보안] > [로그인] > ['sa' 계정 우클릭 후 '속성' 선택]

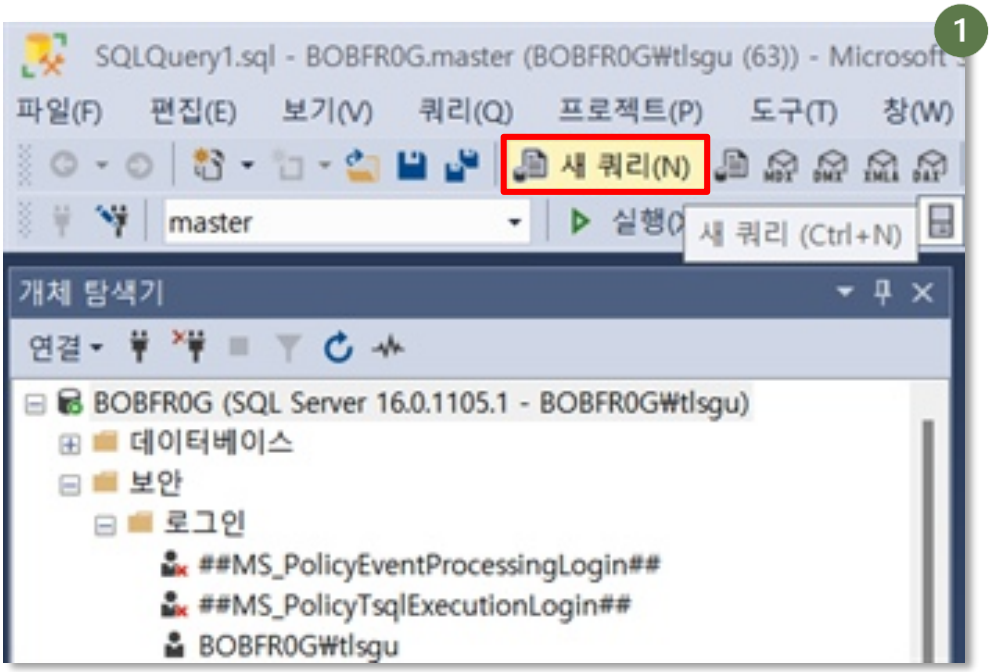


2. [상태] > [데이터베이스 엔진 연결 권한 '거부' 클릭] > [로그인 설정 '사용 안 함' 선택]

MS-SQL

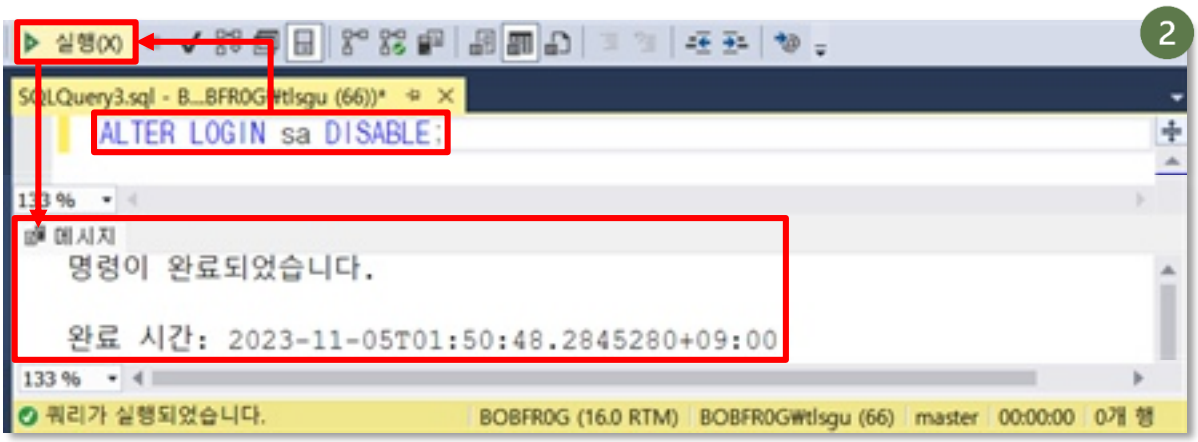
sa 계정 비활성화 하기 - 쿼리문 방식

1. [SSMS 메뉴바에서 '새 쿼리' 클릭]



2. [쿼리 창에 아래 쿼리문 작성] > [실행] > [결과 확인]

```
ALTER LOGIN sa DISABLE;
```



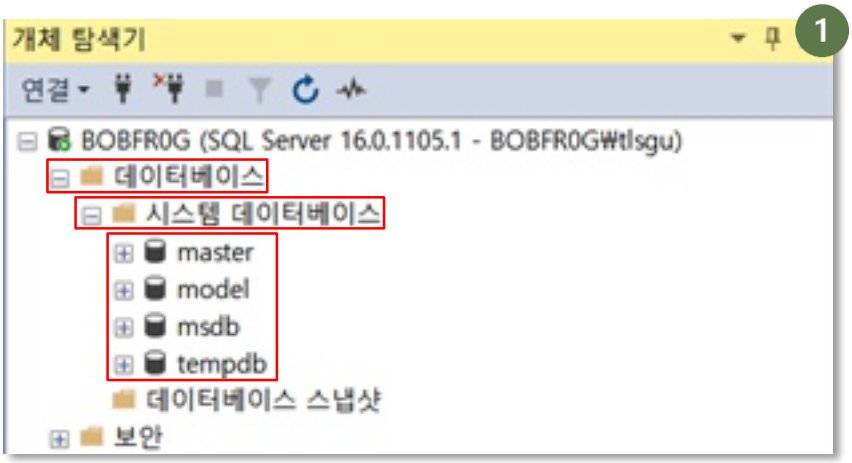
MS-SQL

5. Guest 계정 관리하기

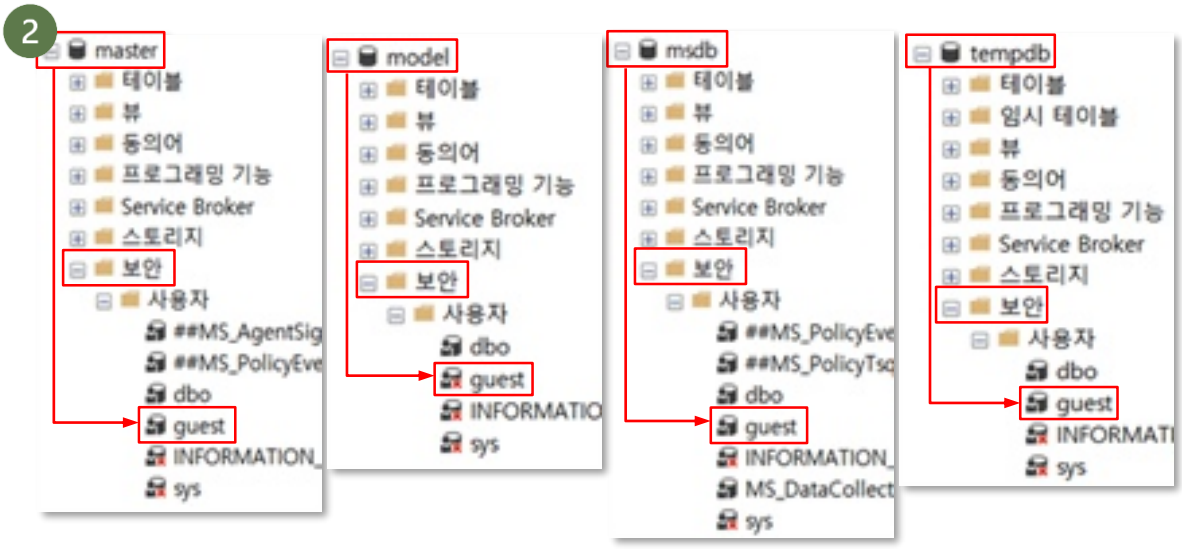
Guest 계정은 모든 SQL 사용자가 게스트 권한을 가지고 접근할 수 있도록 해주는 특별한 로그인 계정입니다. 해당 계정은 인증되지 않은 사용자들에게도 접근을 허용하기 때문에, 데이터베이스의 보안을 강화하기 위해 게스트 권한을 삭제하는 것을 권장합니다.

Guest 계정 비활성화하기 - UI 방식

1. [SSMS 개체탐색기] > [데이터베이스] > [시스템 데이터베이스]

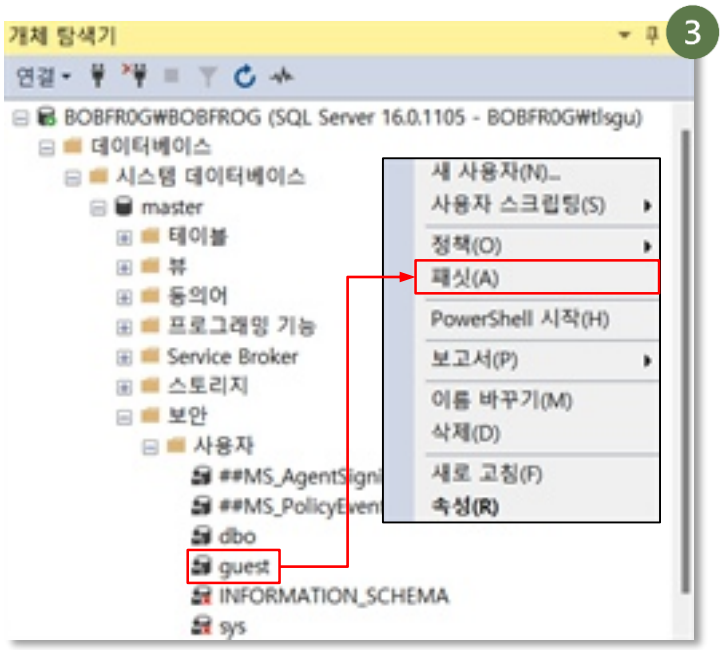


2. [각 데이터베이스(master, model, msdb, tempdb) 별 '보안' 클릭] > [사용자] > ['guest' 계정 확인]

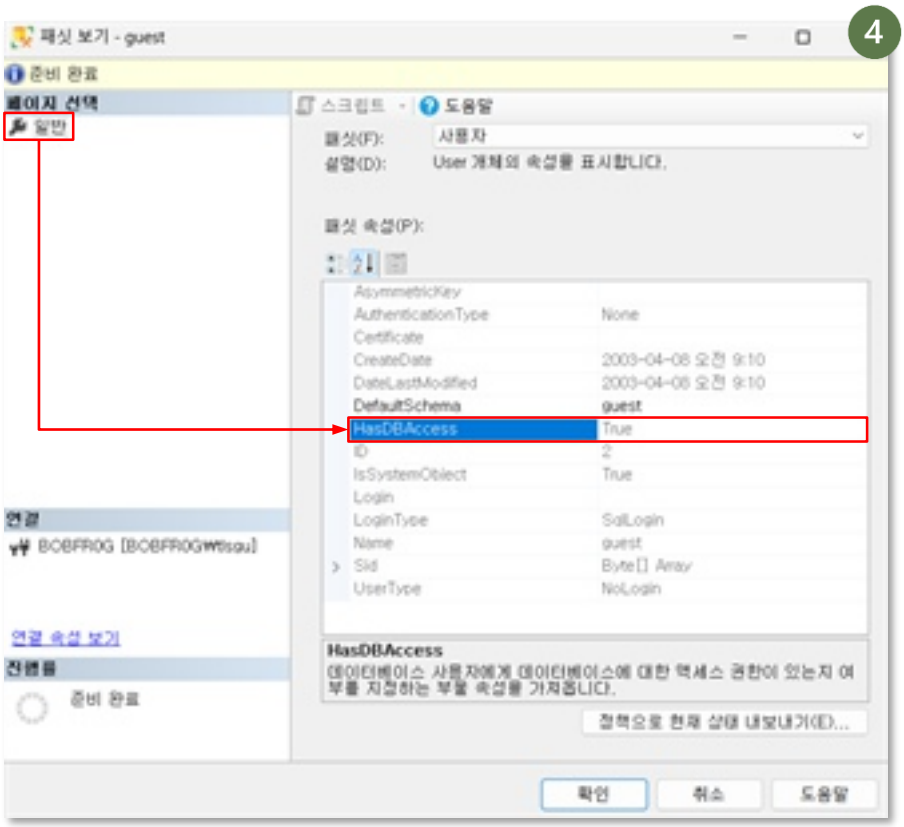


MS-SQL

3 ['guest' 우클릭 후 '패싯' 선택]



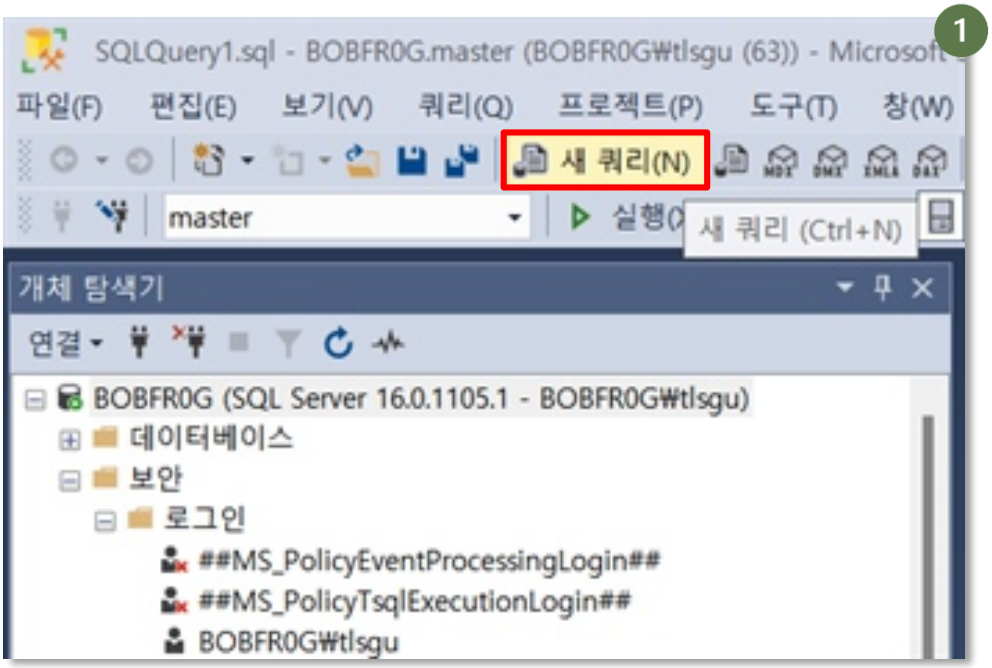
4 ['패싯속성'의 'HasDBAccess' 옵션을 'False'로 설정] > ['확인' 클릭]



MS-SQL

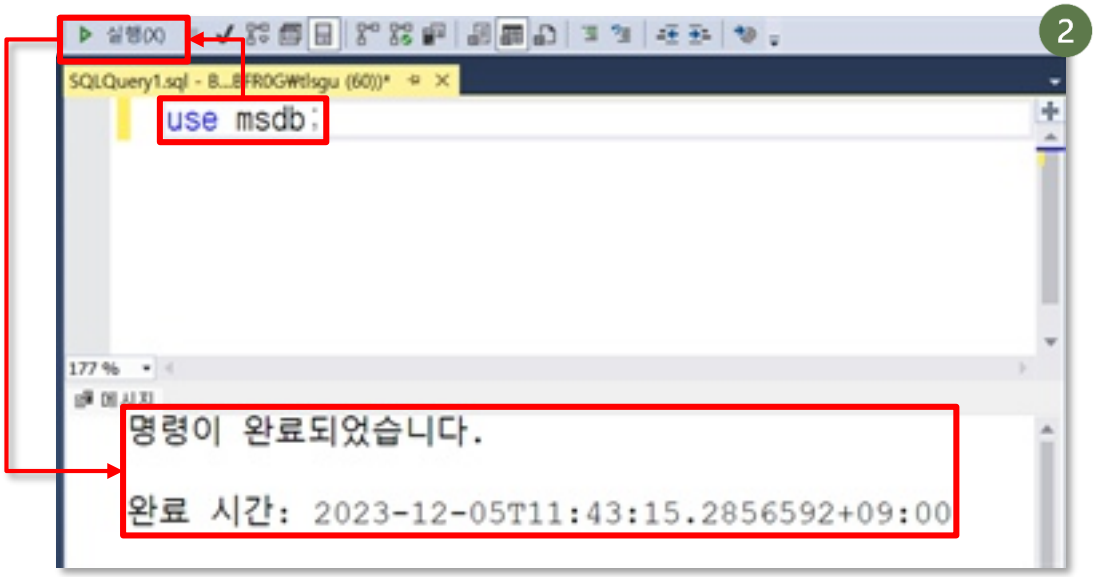
Guest 계정 비활성화하기 - 쿼리문 방식

1 [SSMS 메뉴바에서 '새 쿼리' 클릭]



2 [쿼리 창에 아래 쿼리문 작성] > [실행] > [DB접속]

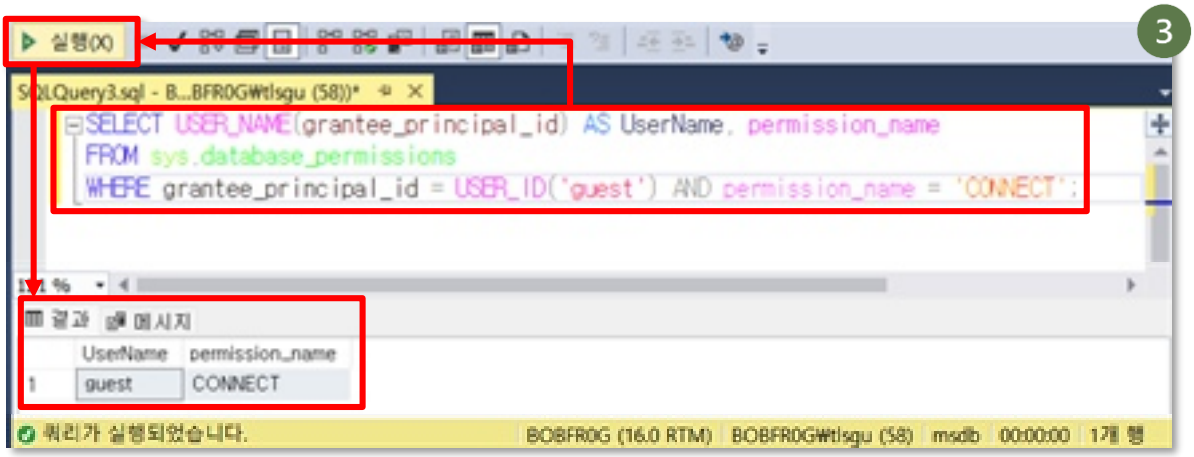
```
use [DB명];
```



MS-SQL

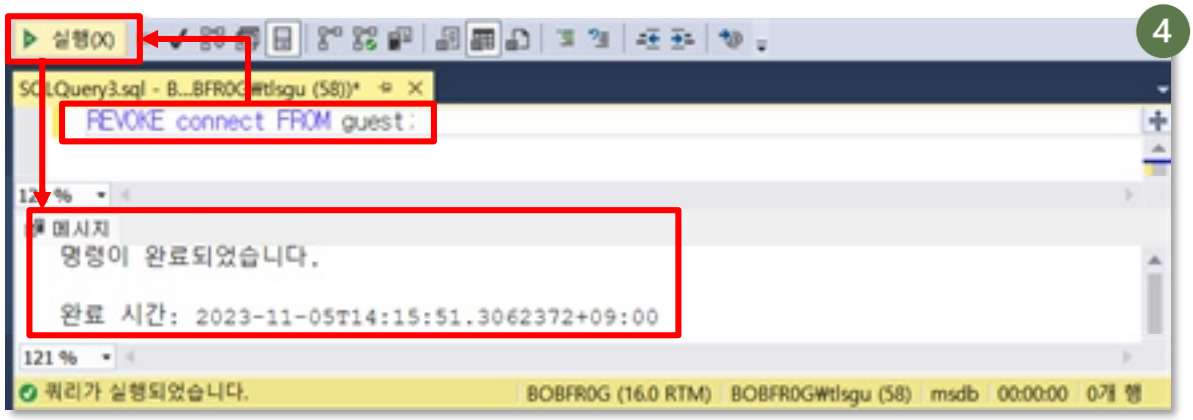
③ [쿼리 창에 아래 쿼리문 작성] > [실행] > ['guest' 계정 확인]

```
[2] SELECT USER_NAME(grantee_principal_id) AS UserName, permission_name
FROM sys.database_permissions
WHERE grantee_principal_id = USER_ID('guest') AND permission_name = 'CONNECT';
```



④ ['guest' 계정 존재 시 쿼리 창에 아래 쿼리문 작성] > [실행] > [결과 확인]

```
REVOKE connect FROM guest;
```



참 고 사 항

MS SQL Server 2022 기준 master와 tempdb 데이터베이스는 guest 계정 활성화가 기본값이기 때문에 변경이 불가능 합니다. 따라서, msdb의 guest 계정에 대해서만 비활성화를 진행하면 됩니다.

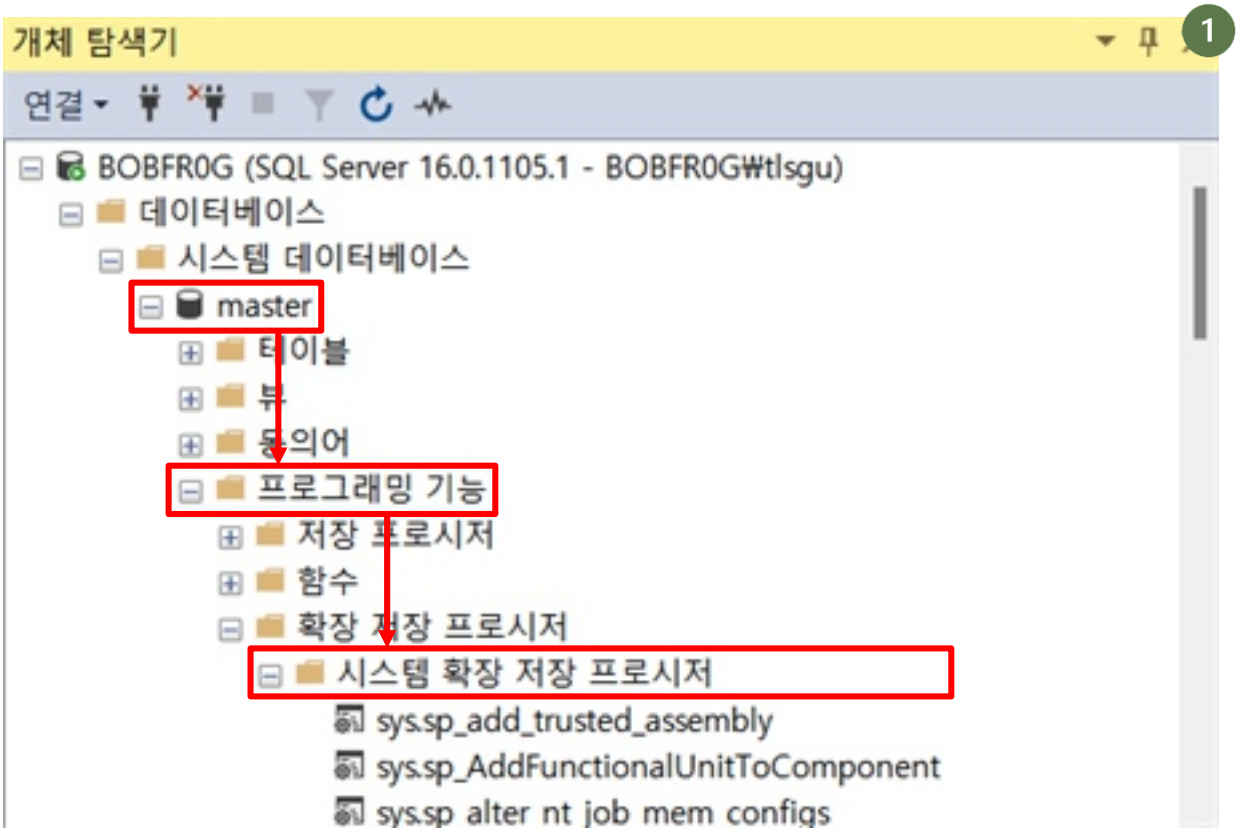
MS-SQL

6. SSMS의 시스템 접근 제한하기

SSMS에서 사용할 수 있는 일종의 내장함수인 '레지스트리 확장 저장 프로시저'를 사용하면 사용자는 윈도우 시스템 설정까지 접근할 수 있습니다. 응용 프로그램이 시스템의 설정에 접근하고 수정까지 할 수 있는 것은 과도한 권한을 가지고 있는 것이기 때문에 위험합니다. 따라서 '레지스트리 확장 저장 프로시저'의 접근 권한을 제한해야 합니다.

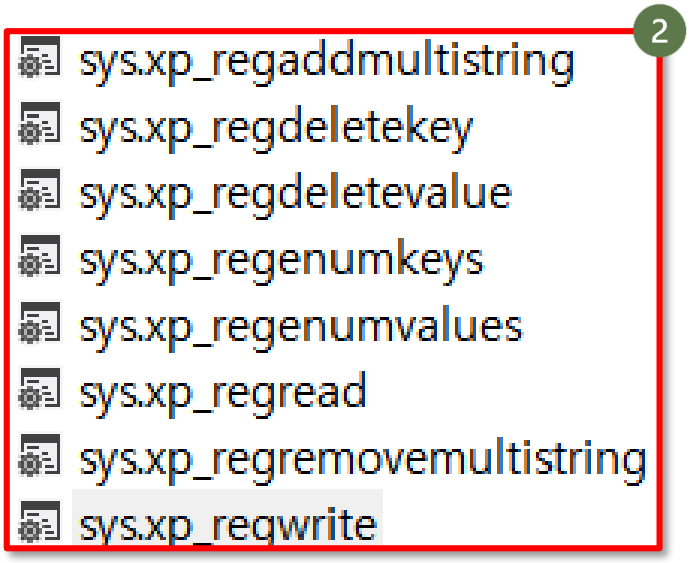
레지스트리 프로시저 항목 확인하기

1. [SSMS 개체탐색기] > [데이터베이스] > [시스템 데이터베이스] > ['master' DB] > [프로그래밍 기능] > [확장 저장 프로시저] > [시스템 확장 저장 프로시저]



MS-SQL

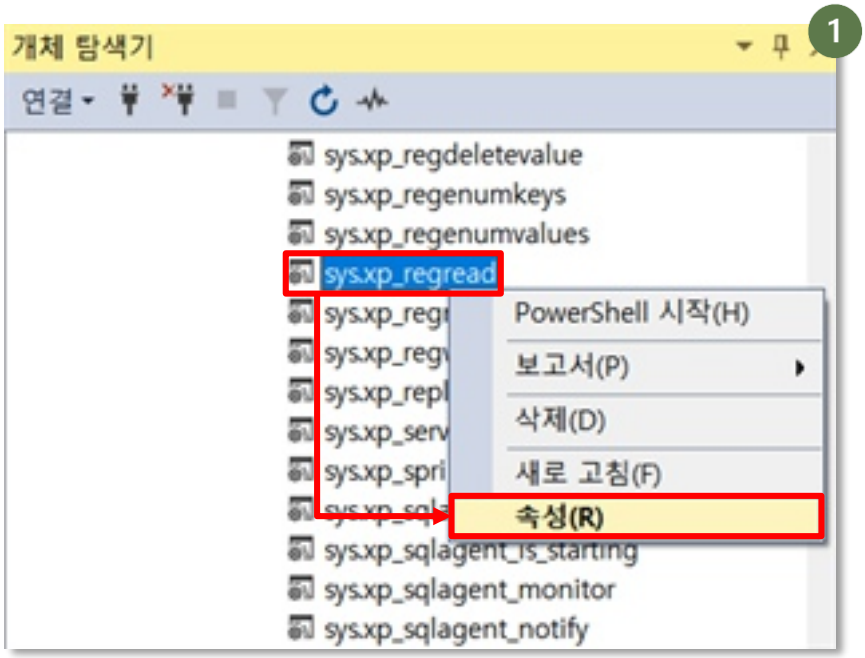
2 [레지스트리 관련 8개 프로시저 항목 확인]



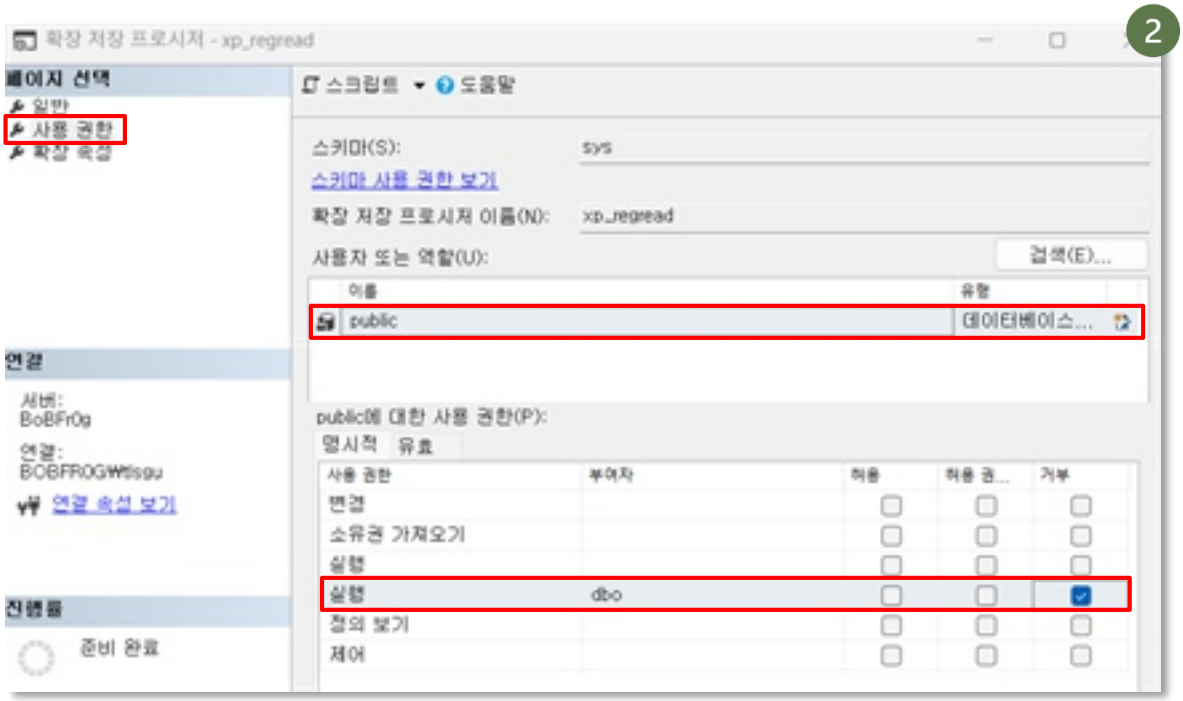
MS-SQL

레지스트리 프로시저의 public 권한 해제하기 - UI 방식

1 [각각의 레지스트리 프로시저 '우클릭' 후 '속성' 선택]



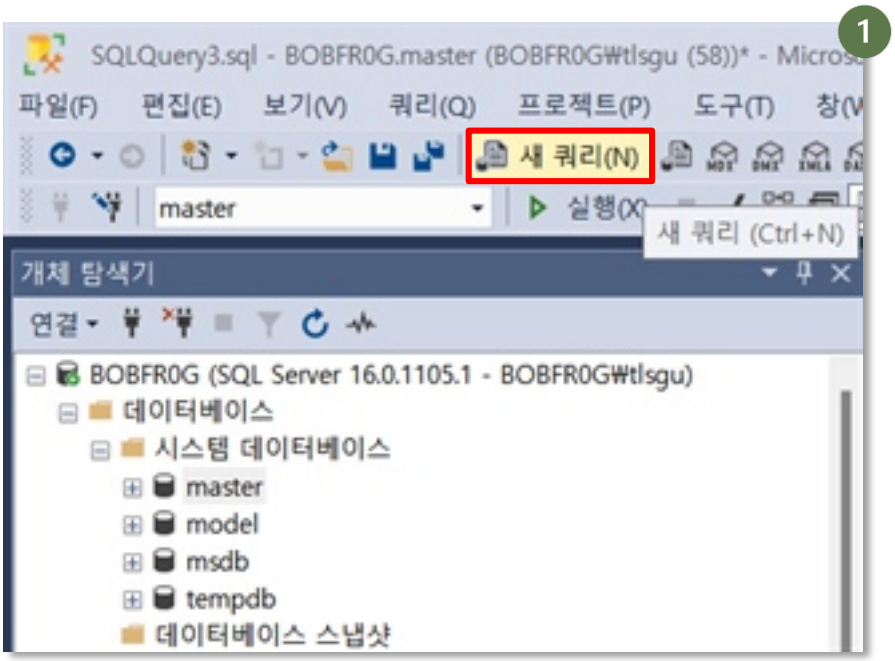
2 ['사용 권한' 클릭] > ['public'에 대한 사용 권한 에서 '거부' 선택]



MS-SQL

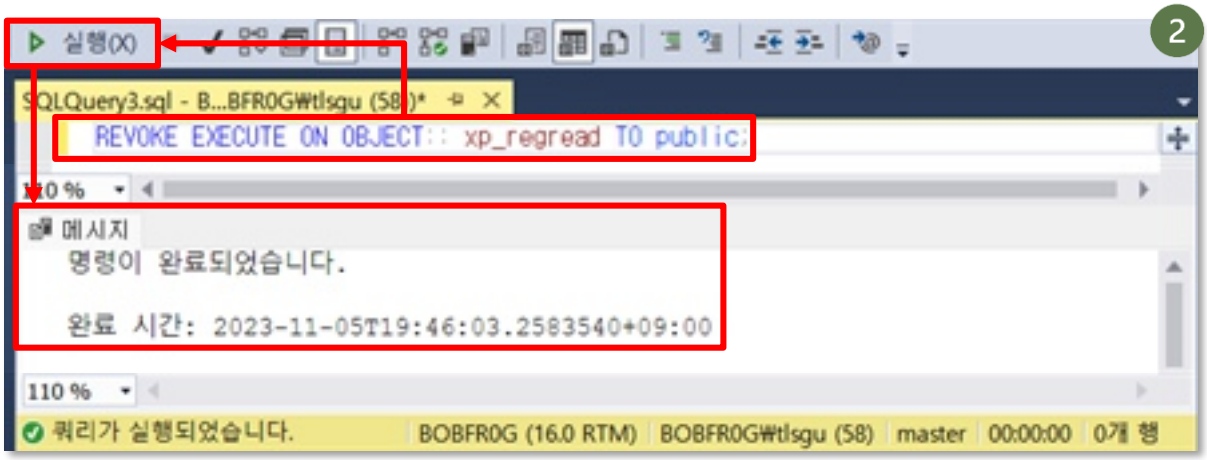
레지스트리 프로시저의 public 권한 해제하기 - 쿼리문 방식

1 [SSMS 메뉴바에서 '새 쿼리' 클릭]



2 [쿼리 창에 아래 쿼리문 작성] > [실행] > [결과 확인]

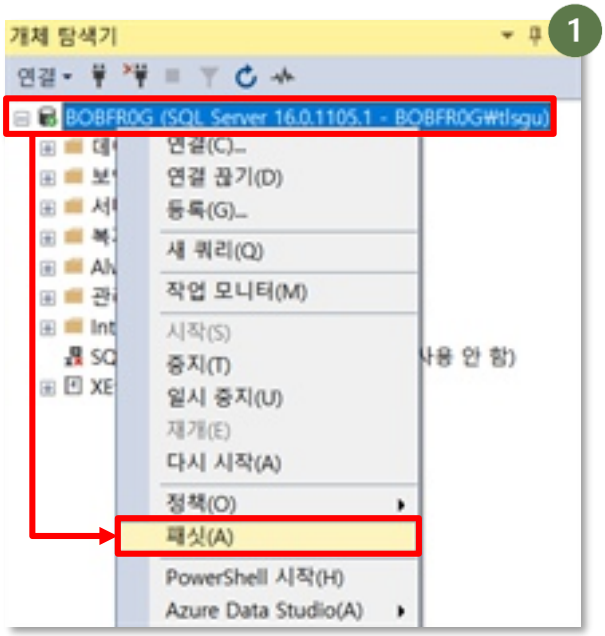
```
REVOKE EXECUTE ON OBJECT:: [레지스트리 관련 프로시저명] TO public;
```



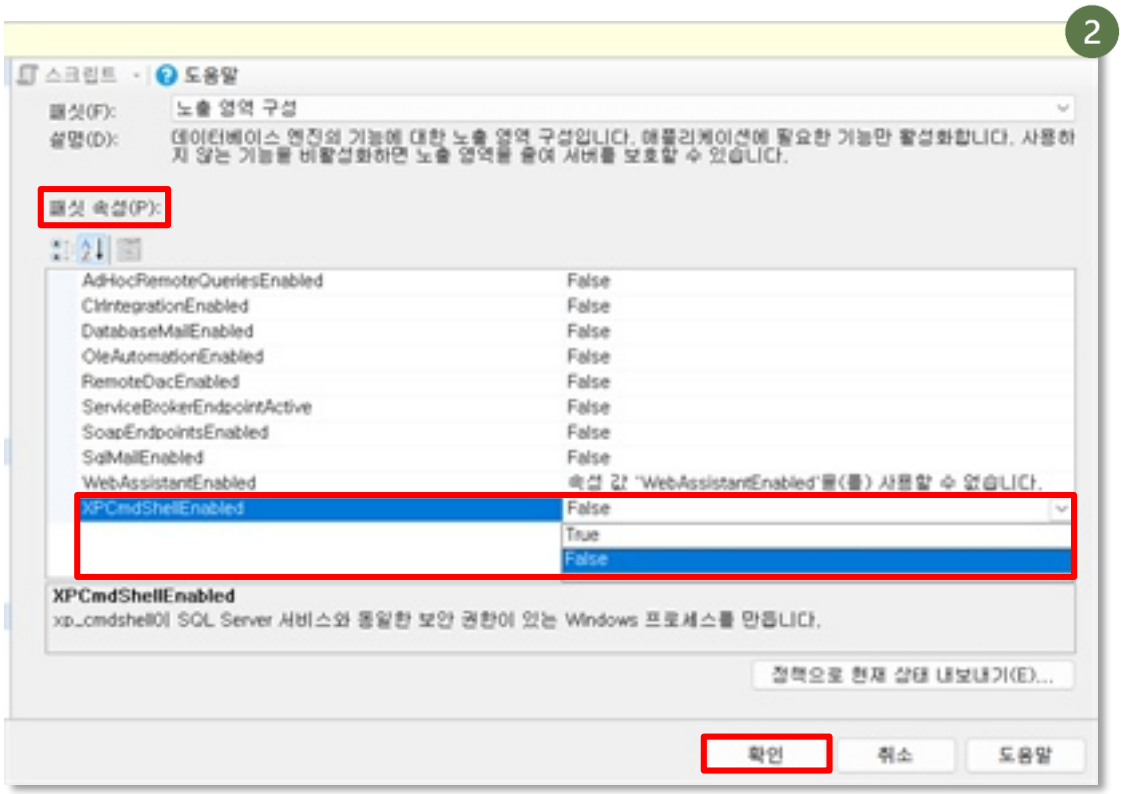
MS-SQL

xp_cmdshell 사용 제한하기

1 [SSMS 개체탐색기] > ['로컬 PC' 이름 우클릭 후 '패싯' 선택]



2 ['패싯 속성'의 'XPCmdShellEnabled' 옵션 'False' 설정] > ['확인' 클릭]



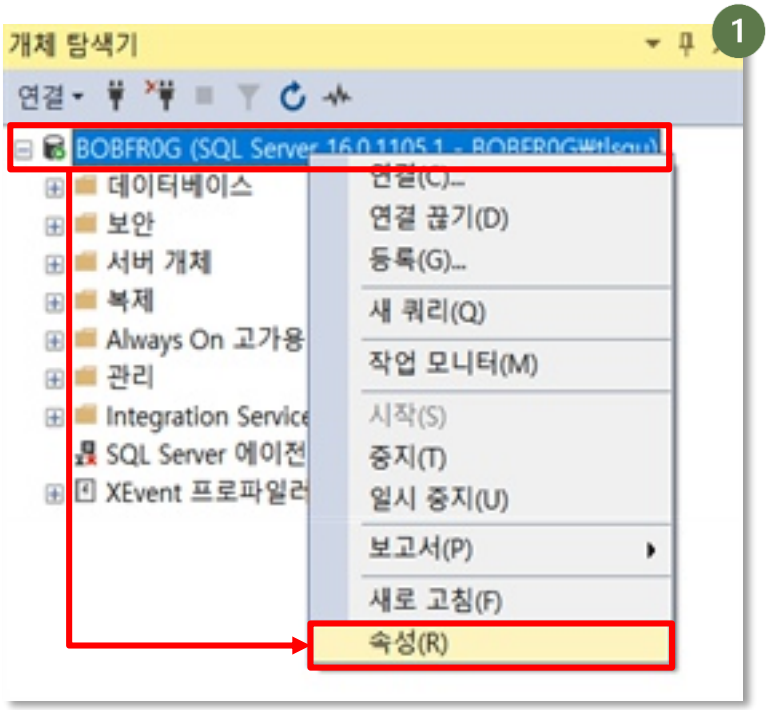
MS-SQL

7. 데이터베이스 로그 활성화

데이터베이스 로그를 남기는 것으로 데이터의 이동, 사용자의 활동, 시스템의 오류 등 중요한 운영 데이터를 기록할 수 있습니다. 이는 추후 데이터베이스에서 발생한 침해사고 및 비정상적인 활동을 추적하는 데 중요한 역할을 합니다.

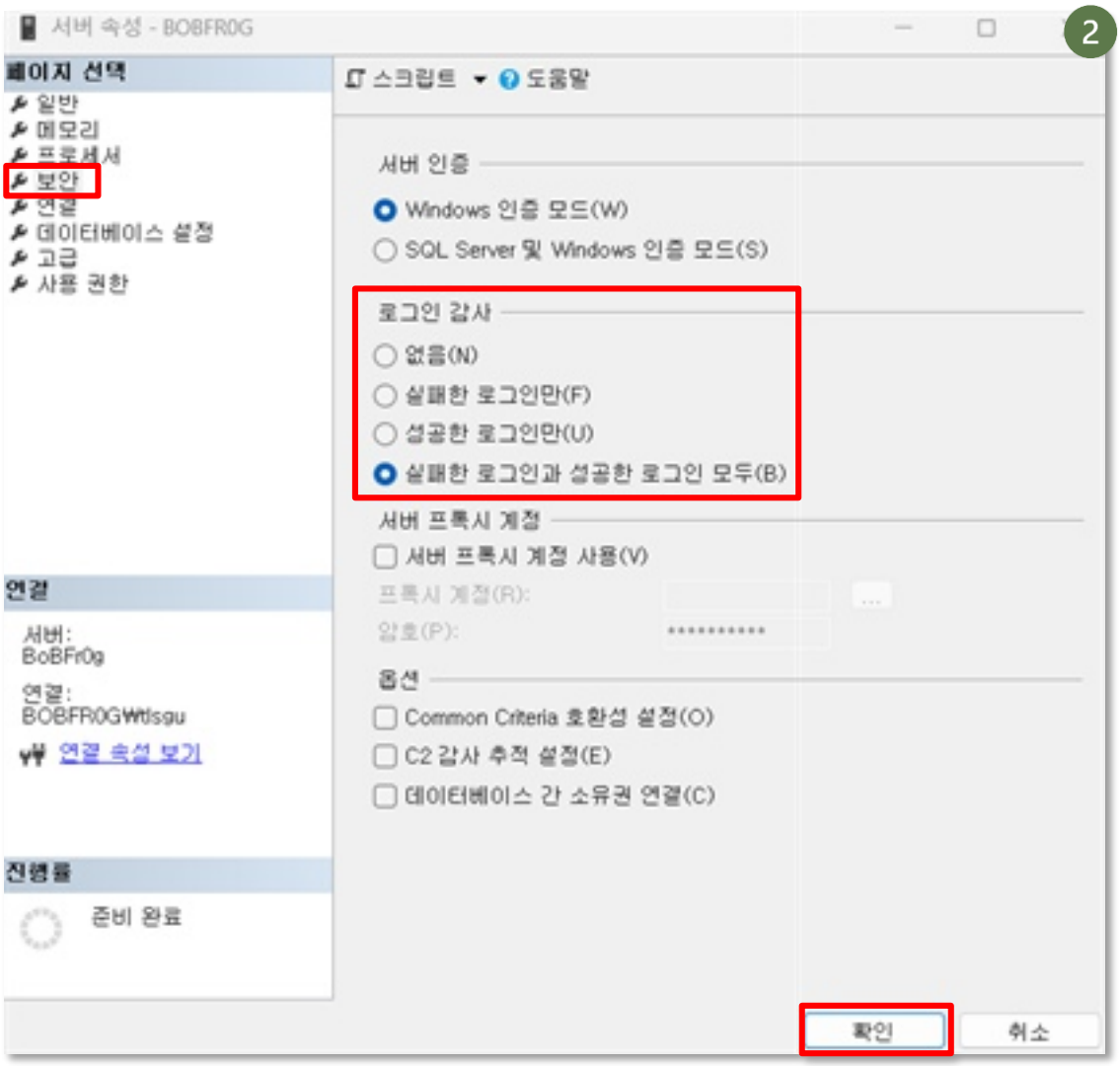
로그 기록 활성화 및 조건 설정

1. [SSMS 개체탐색기] > ['로컬 PC' 이름 '우클릭' 후 '속성' 선택]



MS-SQL

② [보안] > ['로그인 감사' 옵션 '실패한 로그인과 성공한 로그인 모두' 선택] > ['확인' 클릭]



로그(Log) 란?

시스템, 네트워크, 소프트웨어 애플리케이션 또는 다른 디지털 환경에서 발생하는 모든 이벤트의 기록입니다. 로그 파일은 사용자의 활동, 시스템의 오류, 기타 중요한 운영 데이터를 자동으로 기록하여, 문제 발생 시 원인 분석에 도움을 주고, 시스템의 성능을 모니터링하며, 보안 사고의 감지와 대응, 그리고 컴플라이언스 준수에 중요한 역할을 합니다.

Postgre-SQL

0. pgAdmin 설치하기

PostgreSQL은 pgAdmin이라는 전용 UI 소프트웨어를 제공합니다. 본 가이드라인에서는 pgAdmin을 사용한 항목별 보안 조치 사항을 설명하며, 이번 장에서는 pgAdmin을 설치하고 기본 설정하는 방법을 설명합니다.

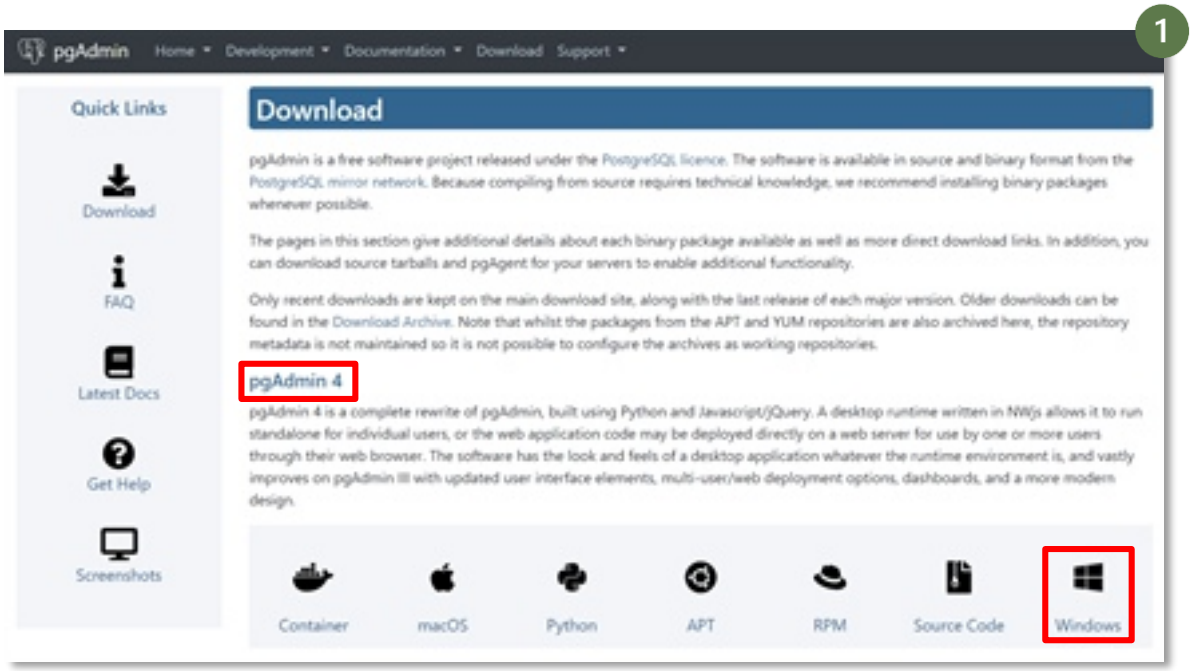
pgAdmin 이란?

pgAdmin은 PostgreSQL 데이터베이스를 관리하기 위한 사용자 인터페이스 도구입니다. 사용자 친화적인 인터페이스를 통해 데이터베이스 관리를 간소화하며, SQL 쿼리 작성, 실행, 저장을 위한 효율적인 환경을 제공합니다.

https://www.pgAdmin.org/download/ - pgAdmin 다운로드 링크

pgAdmin 설치하기

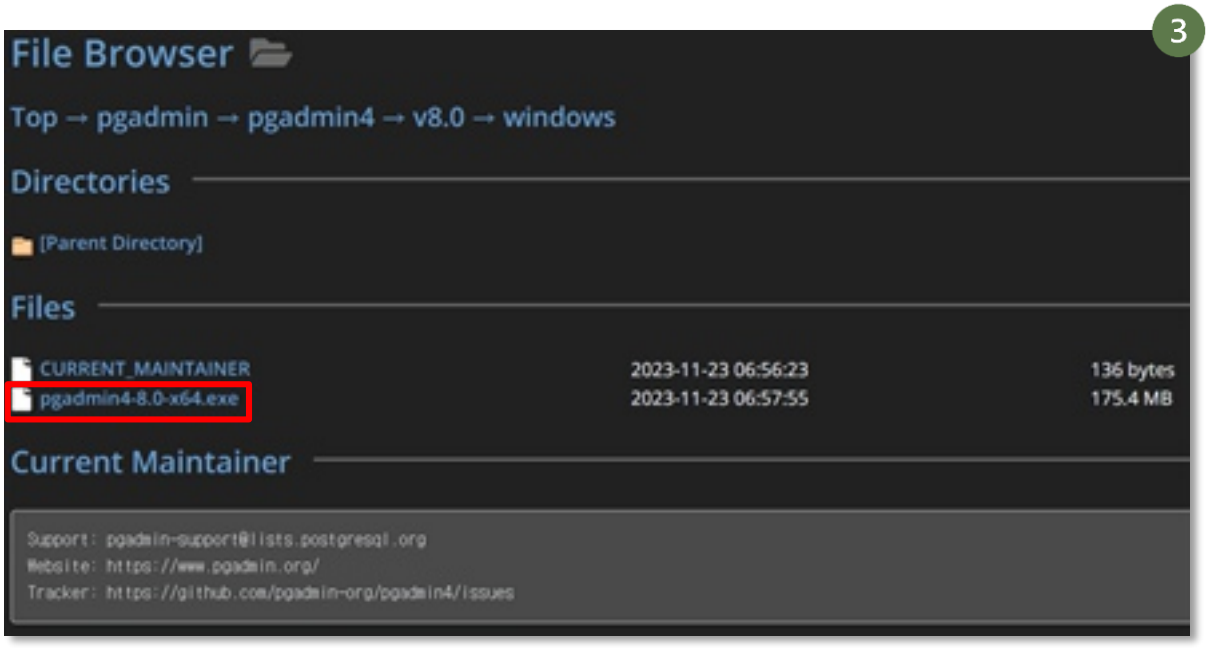
1. [pgAdmin 4에서 해당하는 운영체제를 선택하여 클릭]
   - 본 가이드라인에서는 Windows 운영체제를 사용합니다.



Postgre-SQL

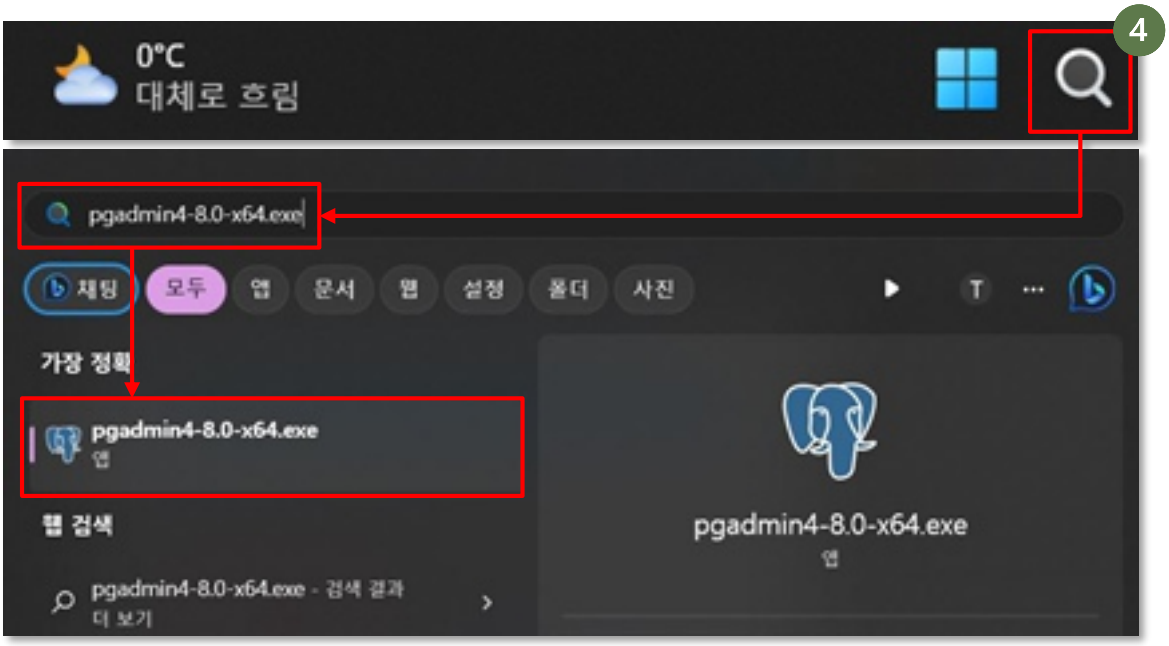
2 ['pgAdmin 4 v8.0' 클릭 (released Nov. 23, 2023)]

3 ['pgAdmin-4-8.0-x64.exe'를 클릭하여 설치파일 다운로드]

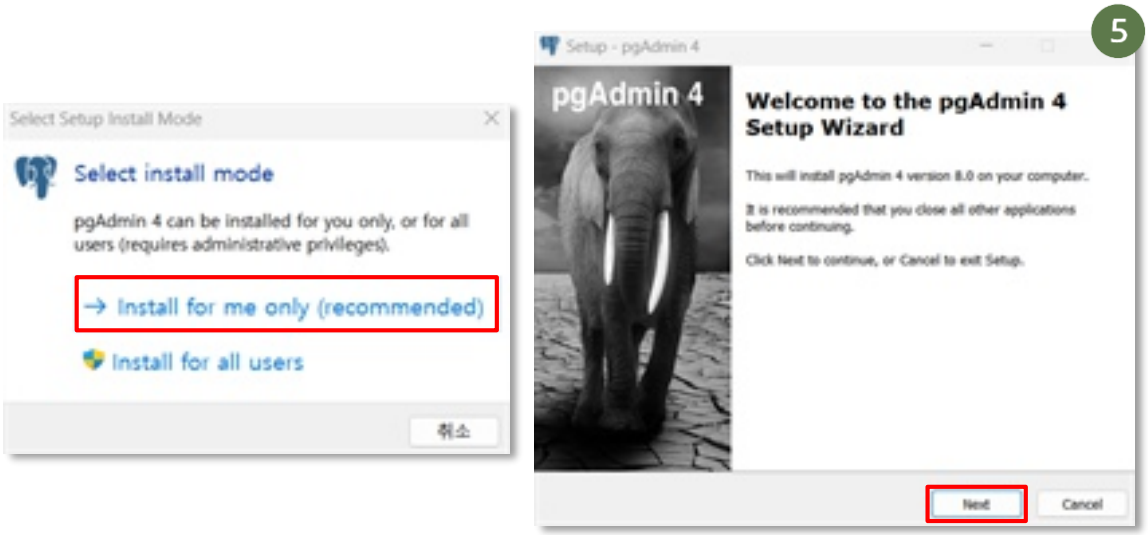


Postgre-SQL

4 [다운로드 완료 후 윈도우 검색창에 'pgAdmin-4-8.0-x64.exe ' 검색 후 실행]

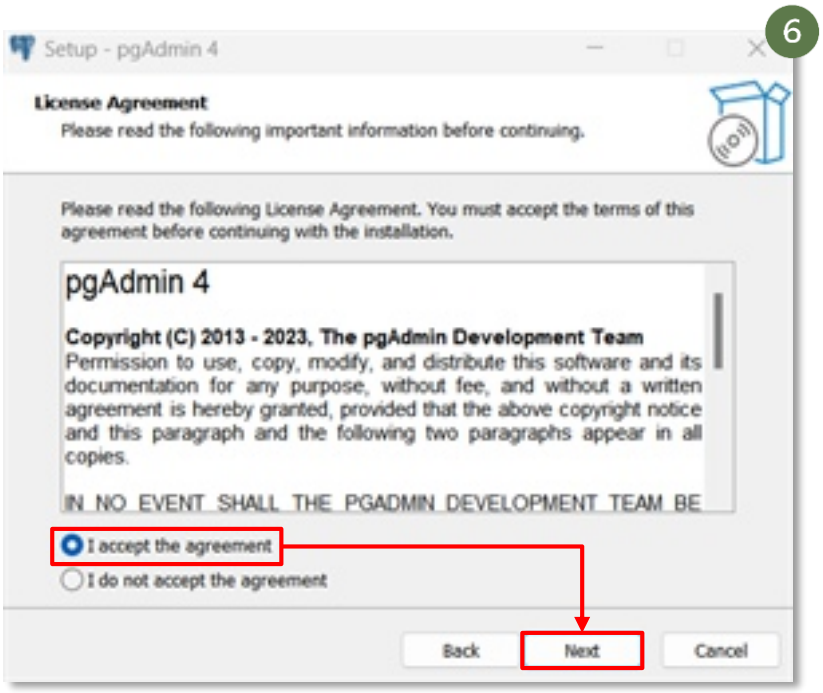


5 [설치 화면에서 'Install for me only (recommended) 클릭] > [다음 화면에서 'Next' 클릭]

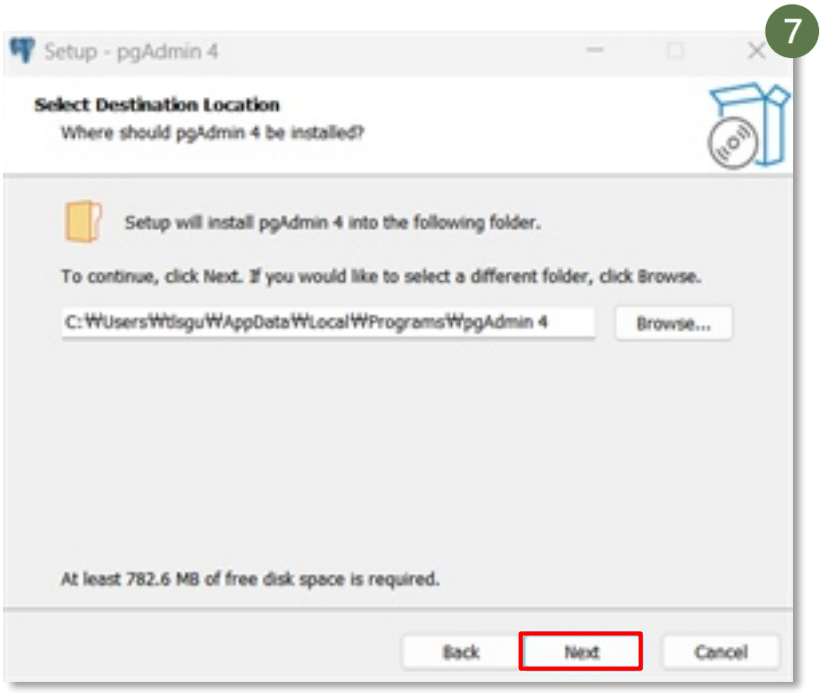


Postgre-SQL

6 [다음 화면에서 'I accept the agreement' 체크 후 'Next' 클릭]

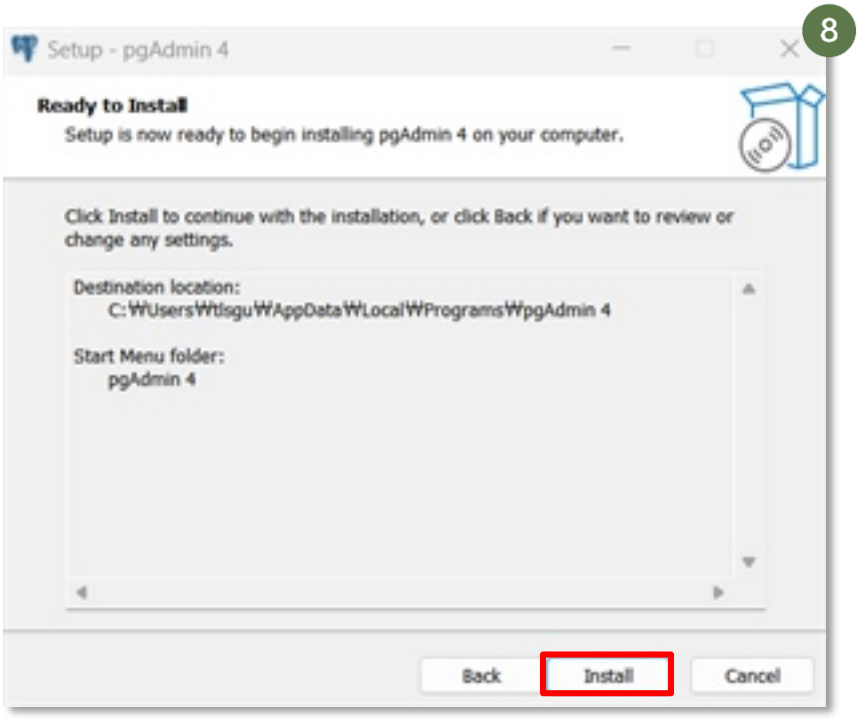


7 [다음 화면에서 'Next' 클릭]



Postgre-SQL

8 [다음 화면에서 'Install' 클릭하여 pgAdmin4 설치 시작]

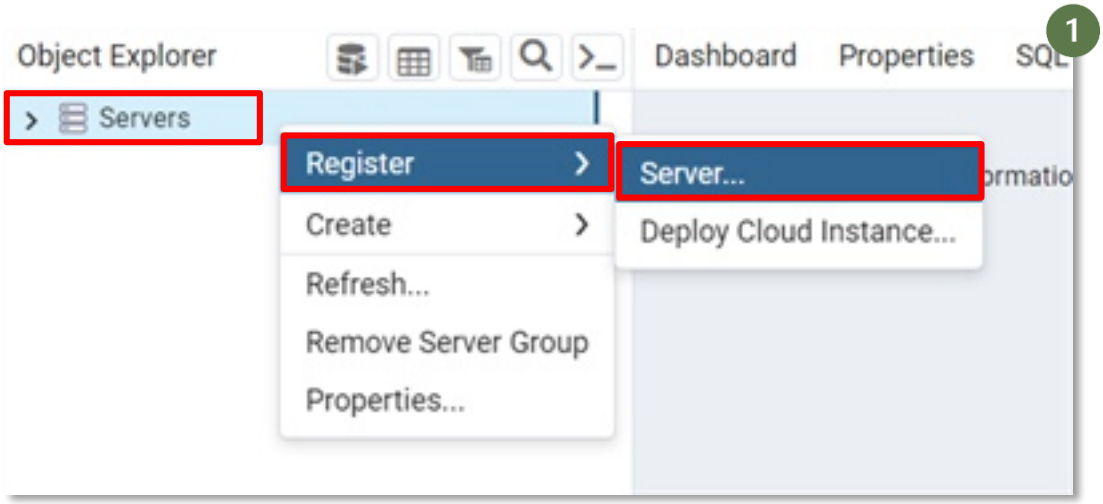


9 [설치완료 후 'Finish' 클릭]

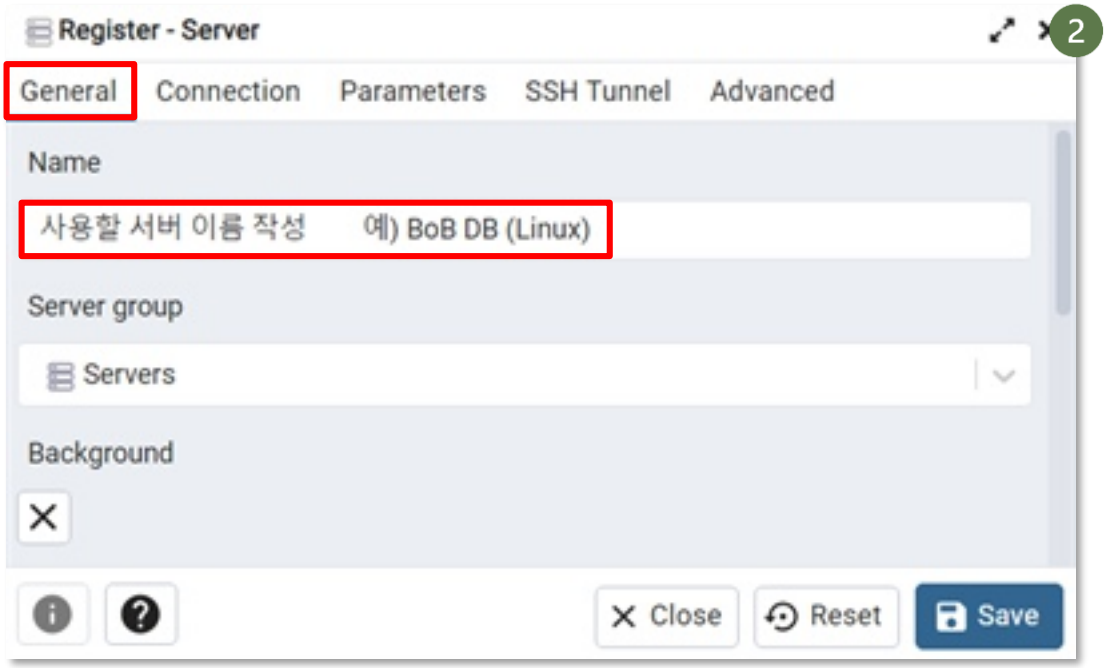
Postgre-SQL

pgAdmin 과 PostgreSQL 데이터베이스 초기 접속 설정하기

1 [pgAdmin 실행] > ['Servers' 우클릭] > ['Register' 선택] > ['Server...' 선택]

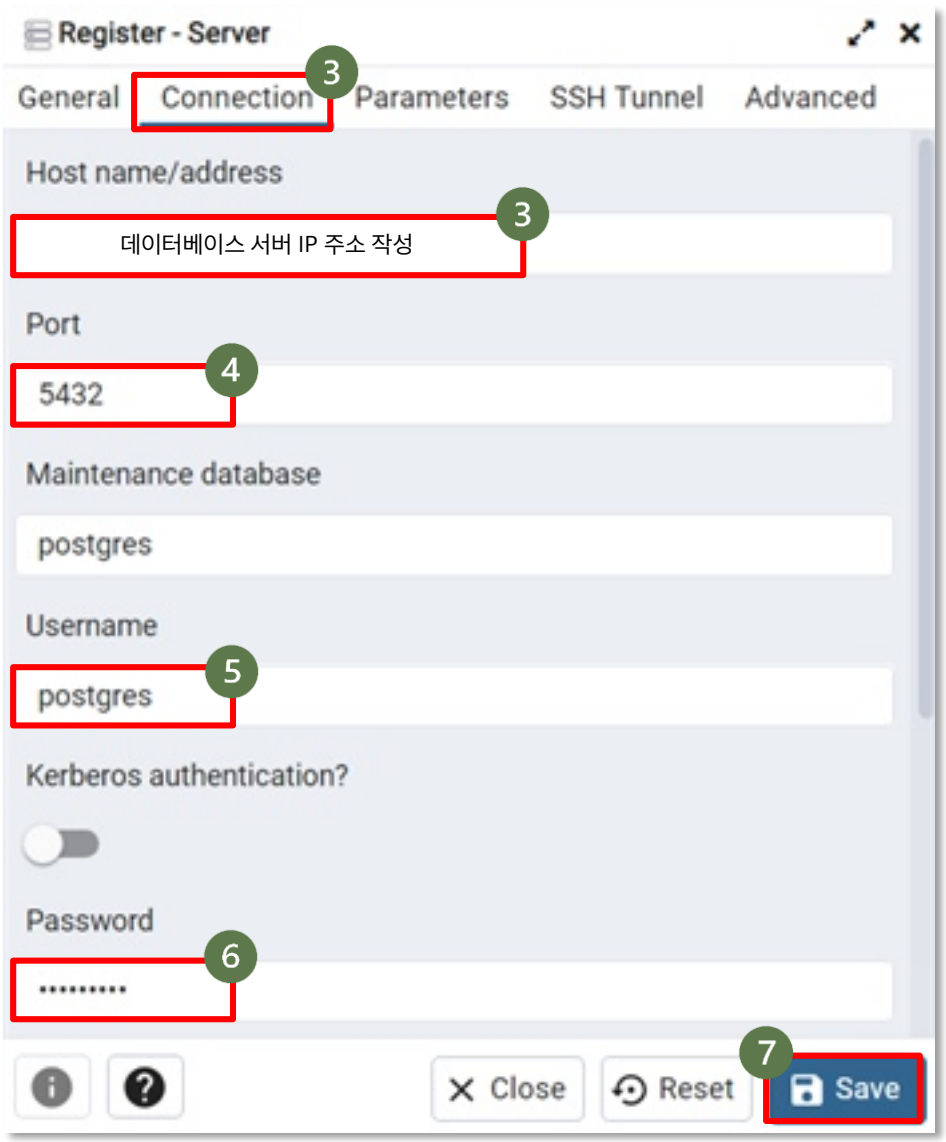


2 ['General' 클릭] > ['Name'에 사용할 서버 이름 입력]



Postgre-SQL

3. ['Connection' 탭 클릭] > ['Host Name/address' 부분에 데이터베이스 서버 IP 작성]
   - 데이터베이스 서버 IP 주소 확인하는 법은 다음 장 참고
4. ['Port' 부분에 5432 작성]
5. ['Username' 부분에 'postgres' 작성]
6. ['Password' 부분에 postgres 계정의 비밀번호 작성]
   - PostgreSQL 데이터베이스 설치 시 별도로 postgres 계정에 비밀번호를 설정하지 않았을 경우에는 기본적으로 postgres 계정에 비밀번호가 설정되지 않으므로 3, 4번 항목의 'Password' 부분을 입력하지 않아도 됩니다.
7. [작성완료 후 'Save' 클릭]



Postgre-SQL

데이터베이스 IP 주소 확인하기

데이터베이스와 pgAdmin을 서로 연동하기 위해서는 데이터베이스의 IP 주소가 필요합니다.
아래의 방법을 통해 데이터베이스의 IP를 확인할 수 있습니다.

운영체제	사용도구	명령어	명령어 실행 방법
Linux 계열	터미널	ifconfig	터미널에서 바로 입력
Window 계열	명령 프롬프트	ipconfig	1. 윈도우 키 + R ('실행' 창) 2. 'cmd' 입력 후 명령어 입력

- Linux 계열 예시

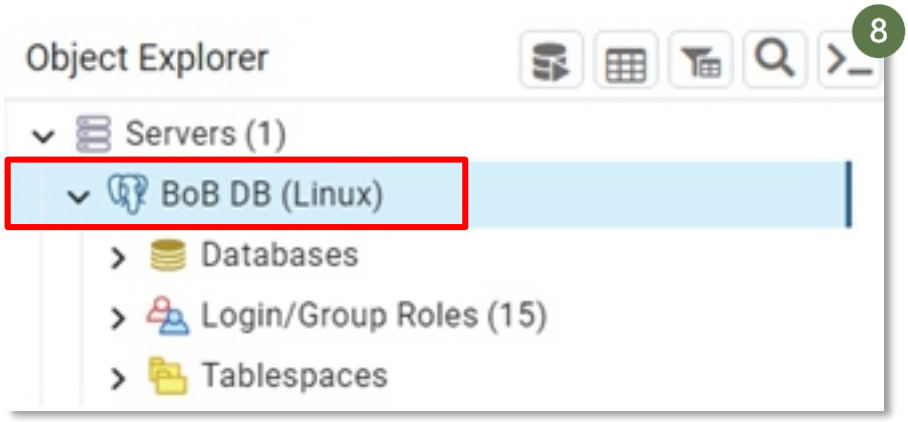
```
root@BoBFr0g:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.28.   .    netmask 255.255.240.0  broadcast 172.28.31.255
        inet6 fe80::215:5dff:fe02:2b0b  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:02:2b:0b  txqueuelen 1000  (Ethernet)
        RX packets 307  bytes 307585 (307.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118  bytes 10467 (10.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Window 계열 예시

```
C:\Users\     >ipconfig

Windows IP 구성


이더넷 어댑터 이더넷 3:

   연결별 DNS 접미사. . . . :
   링크-로컬 IPv6 주소 . . . . . : fe80::2ec:733c:e8f0:e290%20
   IPv4 주소 . . . . . . . . . . : 192.168.   .
   서브넷 마스크 . . . . . . . . : 255.255.255.0
   기본 게이트웨이 . . . . . . . :
```

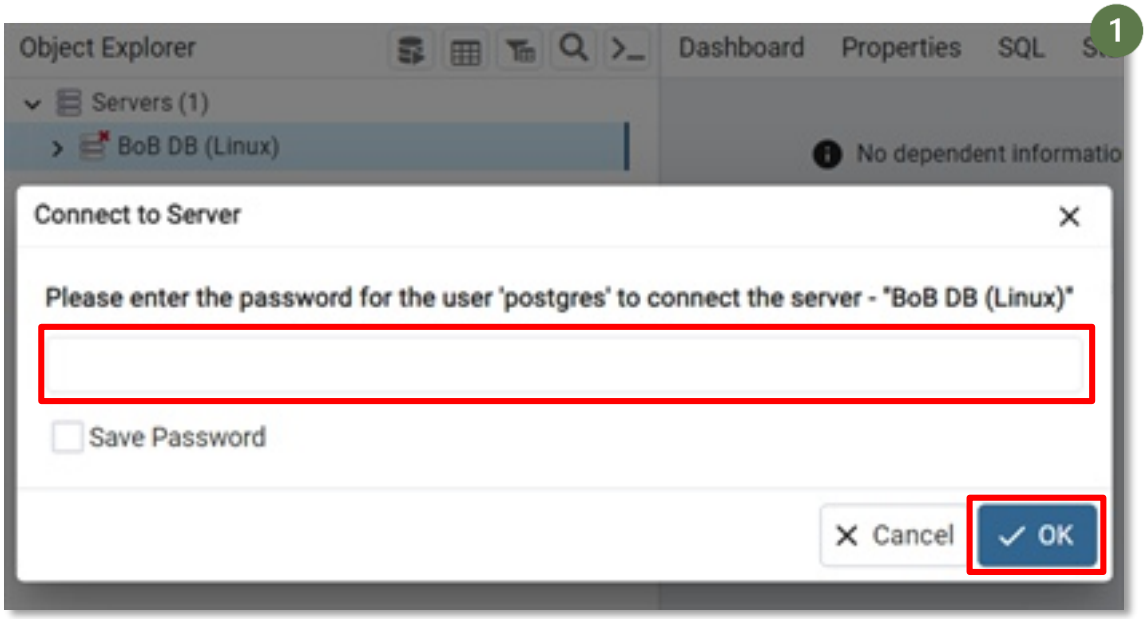
Postgre-SQL

8 [다음 화면에서 'Install' 클릭하여 pgAdmin4 설치 시작]



데이터베이스 재접속시

1 [pgAdmin4 실행 후 접속 계정에 맞는 비밀번호 입력 뒤 'OK'를 클릭하여 접속]



Postgre-SQL

1. 포트 관리하기

PostgreSQL 데이터베이스는 설치 시 기본적으로 5432번 포트를 사용합니다. 하지만 해당 포트는 널리 알려져 있어 외부 공격에 취약할 수 있습니다. 따라서 보안을 강화하기 위해 별도의 포트 번호를 지정하여 데이터베이스를 운영해야 합니다.

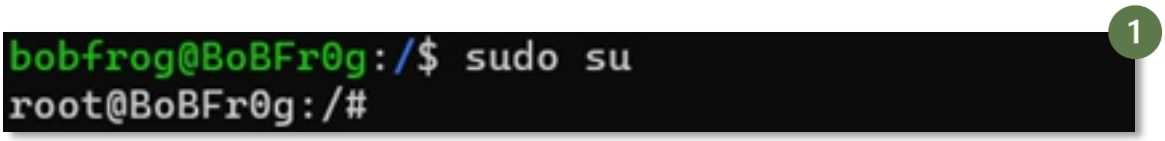
포트(Port)란?

포트는 컴퓨터가 네트워크를 통해 정보를 주고받을 때 사용하는 통로를 의미합니다.

PostgreSQL 데이터베이스 접속 방법

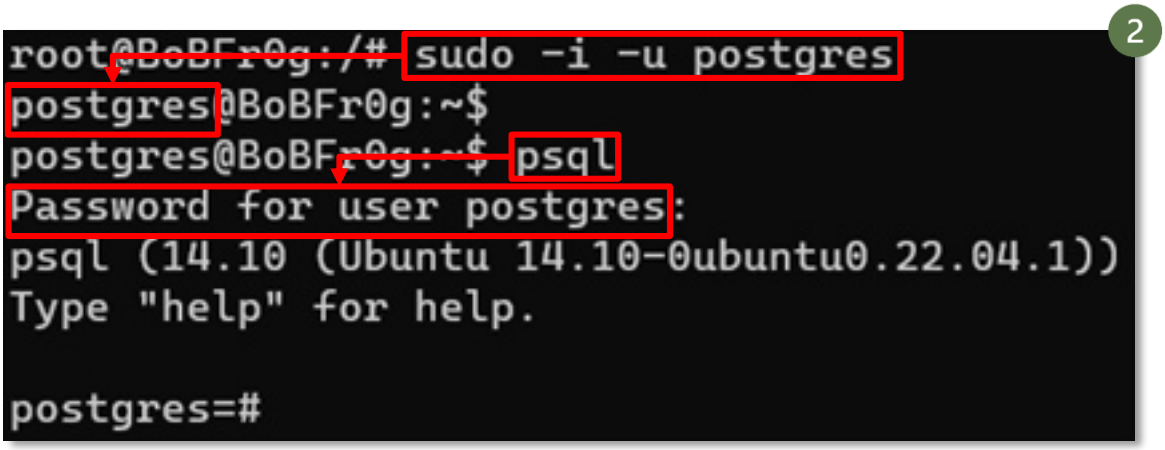
1. [PostgreSQL 서버에서 root 변경 명령어로 root 접속] (Ubuntu 기준)

```
$ sudo su
```



2. [root 접속 후 PostgreSQL 접속 명령어 입력] > [비밀번호 입력 후 MySQL 데이터베이스 접속]

```
# sudo -i -u postgres
(postgres 로 전환 후)
$ psql
```

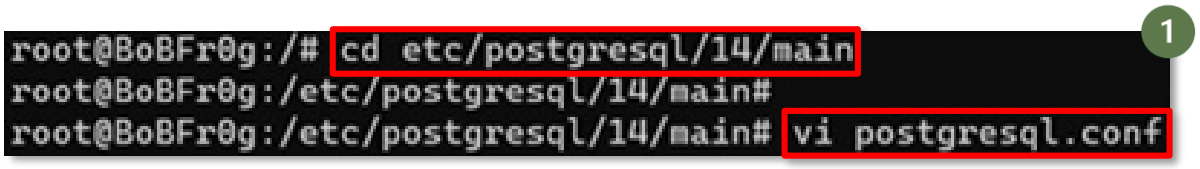


Postgre-SQL

기본 포트번호 변경하는 방법

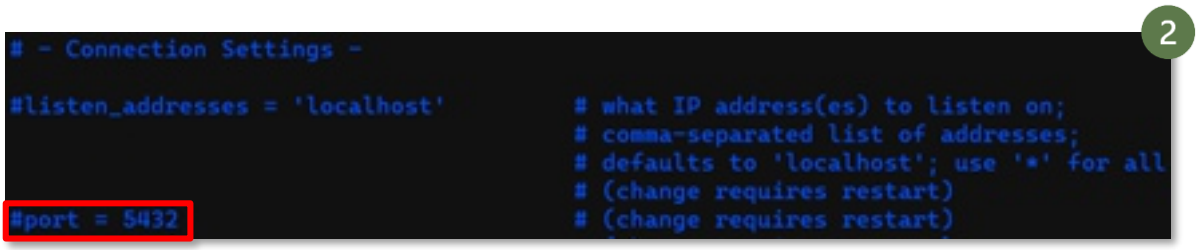
1. ['cd' 명령어를 통해 PostgreSQL 설정 파일 디렉토리로 이동] > [하단의 'vi' 명령어를 실행해 'postgresql.conf' 파일 열기]

```
# cd etc/postgresql/14/main
# vi postgresql.conf
```



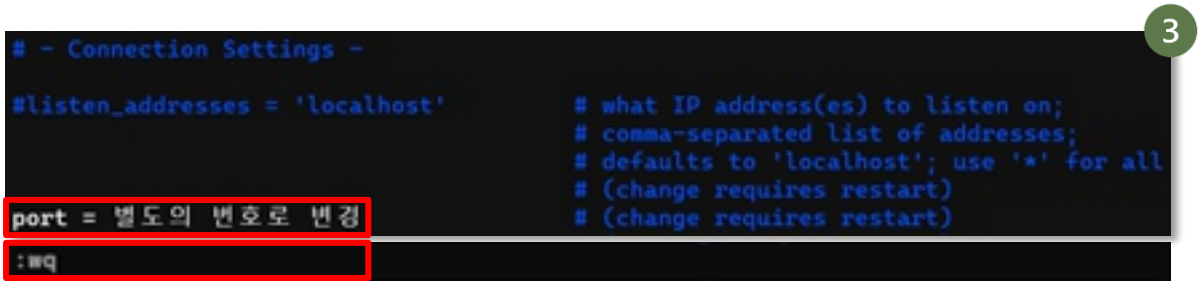
2. ['/port'를 입력하여 port 항목 검색]

```
/port
```



3. ['i'를 통해 입력모드 진입] > [주석('#') 제거 후 별도의 포트번호로 수정] > [이후 키보드 ESC] > [':wq' 입력] > ['Enter' 입력]

```
#port = 5432 에서 # 삭제
port = 임의의 포트 번호 입력
```



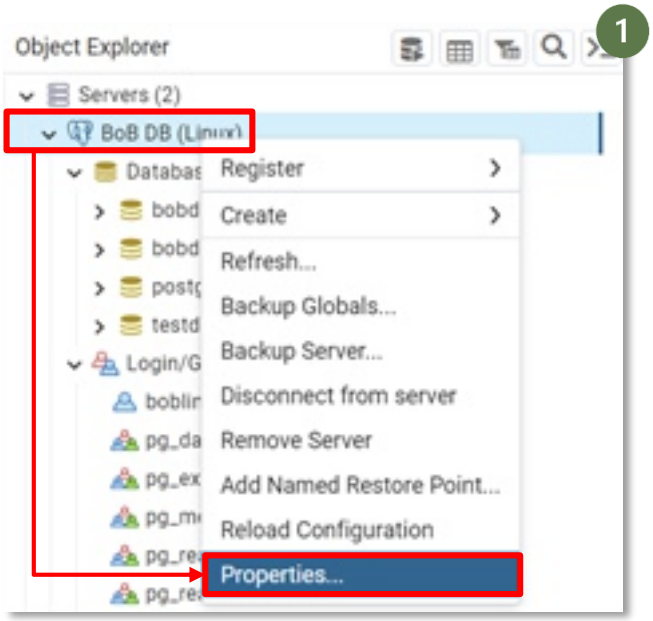
4. [터미널에 'service mysql restart' 명령어 입력] > [서비스 다시 시작]

```
service mysql restart
```

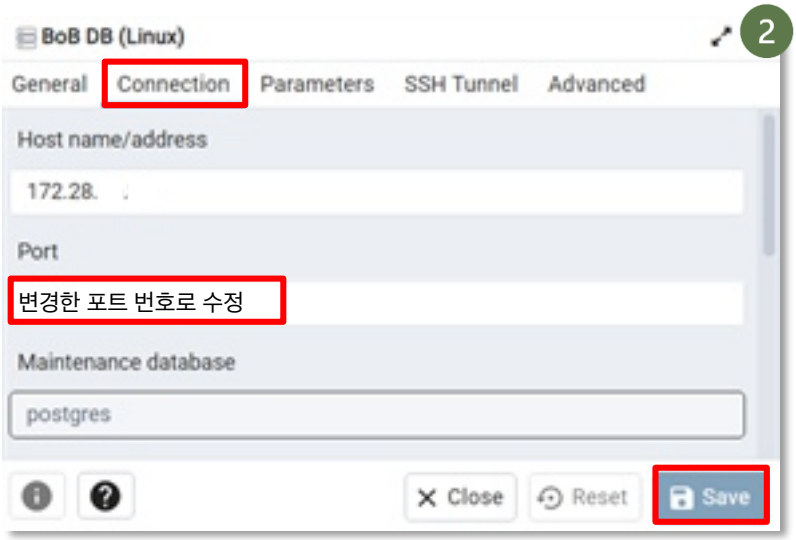
Postgre-SQL

데이터베이스 포트 번호 변경 후 pgAdmin4 재설정 하기

1. [pgAdmin 'Object Explorer'] > [포트 번호를 변경할 데이터베이스 우클릭] > ['Properties...' 선택]



2. ['Connection' 클릭 후 수정된 포트 번호로 'Port' 항목 수정] > [수정 후 'Save' 클릭]



설정 파일 디렉토리 이동 시 유의사항

설정 파일 디렉토리로 이동할 때 (cd /etc/postgresql/14/main) '14' 부분은 PostgreSQL 버전에 따라 변경해야 합니다.

(ex. 13버전일 경우 'cd /etc/postgresql/13/main')

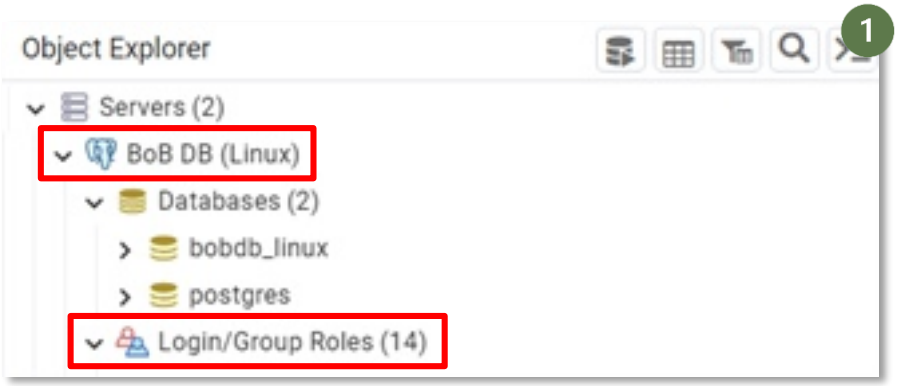
Postgre-SQL

2. 일반 계정 관리하기

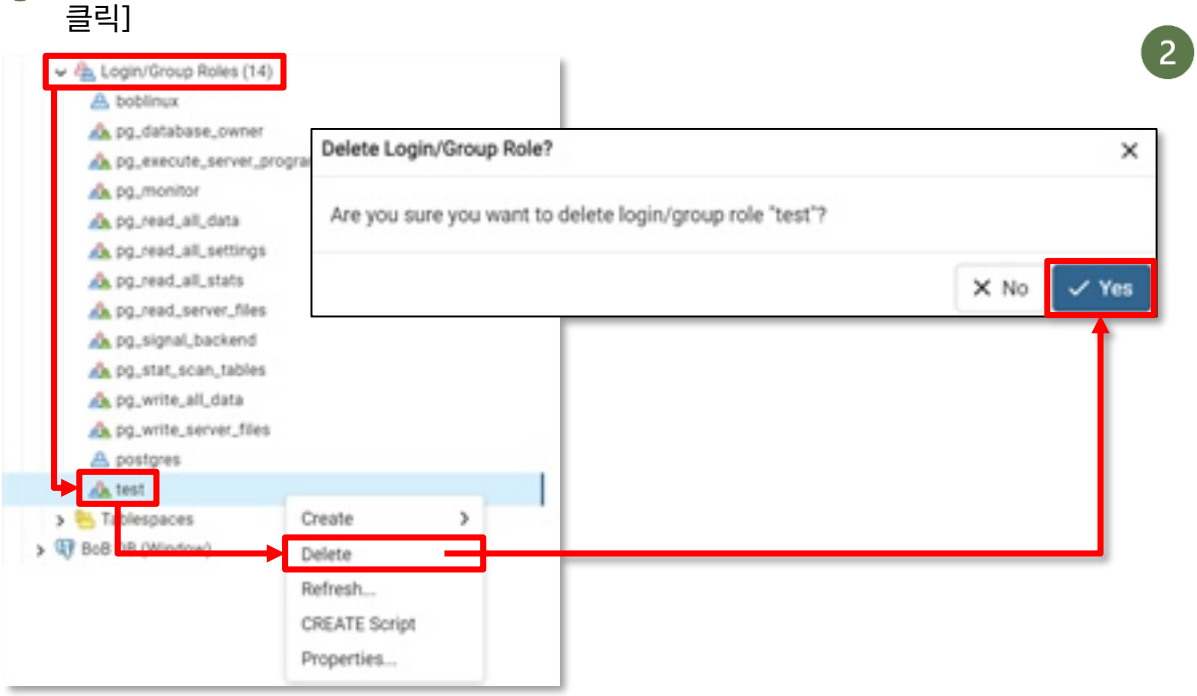
직원이 회사를 떠난 뒤 그 계정을 삭제하지 않았거나, 테스트 목적으로 계정을 생성한 뒤에 이를 삭제하지 않아 데이터베이스에 불필요한 계정이 남아있을 수 있습니다. 공격자는 이러한 계정을 탈취하여 무단으로 데이터 조회, 변경, 삭제와 같은 작업을 수행할 수 있습니다. 따라서 주기적으로 계정 사용 여부를 검토한 뒤 불필요한 계정은 삭제할 것을 권장합니다.

불필요한 계정 삭제하는 방법 - UI 방식

1. [pgAdmin 'Object Explorer'] > [사용 중인 데이터베이스 선택] > ['Login/Group Roles' 클릭]



2. [하위 항목에서 사용하지 않는 계정 확인] > [해당 계정 우클릭 후 'Delete' 선택] > ['Yes' 클릭]



Postgre-SQL

불필요한 계정 삭제하는 방법 - 쿼리문 방식

1. [PostgreSQL 데이터베이스 접속] > ['\du' 명령어를 통해 사용하지 않는 계정 확인]
   - '\du' 명령어의 '\' 은 역슬래시로, 키보드의 '₩' (혹은 '\') 버튼으로 입력 가능합니다.

```
# \du
```

```
postgres=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 boblinux  |                                                            | {}
 newtest   |                                                            | {}
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 test      |                                                            | {}
```

2. [계정 확인 후 'DROP USER' 쿼리문을 실행하여 사용하지 않는 계정 삭제]
   - 명령어 실행 후 'DROP ROLE' 문구가 나온다면 정상적으로 삭제 된 것입니다.

```
# DROP USER [계정명];
```

```
postgres=# DROP USER test;
DROP ROLE
postgres=#
```

Postgre-SQL

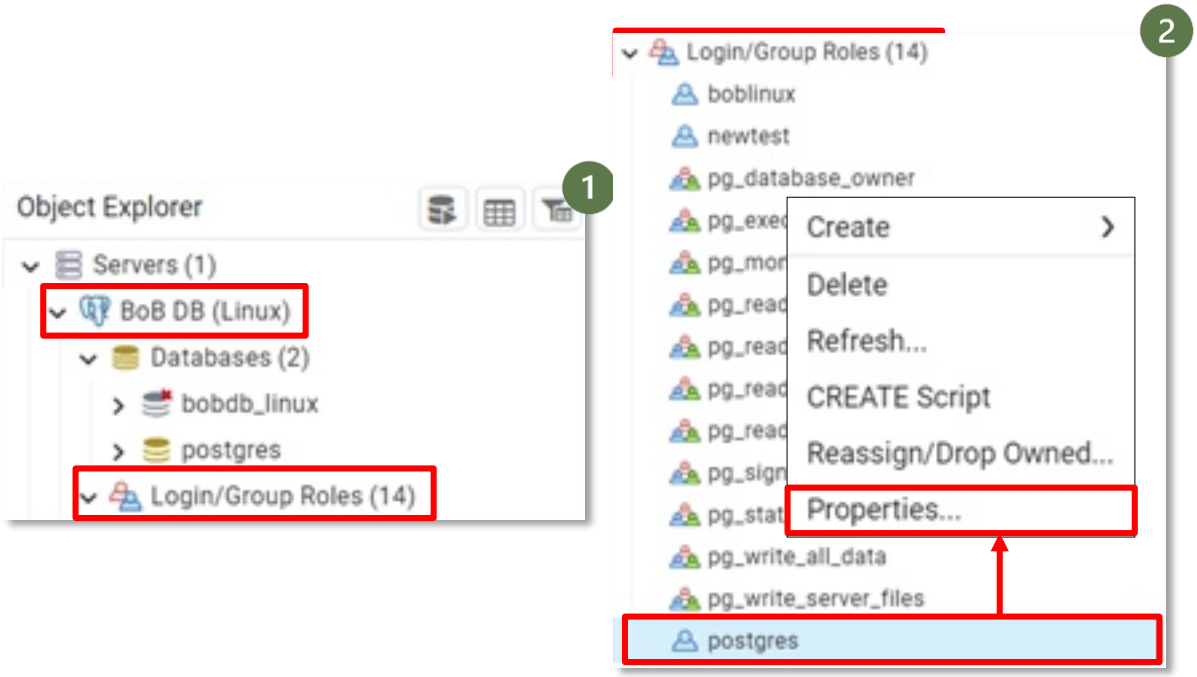
3. 취약한 비밀번호 관리하기

비밀번호가 계정명과 동일하거나 너무 짧은 비밀번호를 사용하는 등 안전하지 않은 비밀번호를 사용하는 경우, 비인가자가 데이터베이스에 쉽게 접근해 침해 사고가 발생할 수 있습니다. 따라서 비밀번호 설정 시 비밀번호의 복잡성을 추가하고 검증하는 절차가 필요합니다.

취약한 비밀번호 예시	취약한 이유
aaabbb, 123123	동일한 문자의 반복
qwerty, asdfgh	키보드 상에서 연속한 위치에 존재하는 문자들의 집합
gildong	개인정보를 바탕으로 구성된 패스워드
iloveyou	사전적 단어로 구성된 패스워드
root123, postgresql	컴퓨터 용어, 기업 등의 특정 명칭을 포함하는 패스워드
admin	시스템에서 초기에 설정되어 있는 패스워드

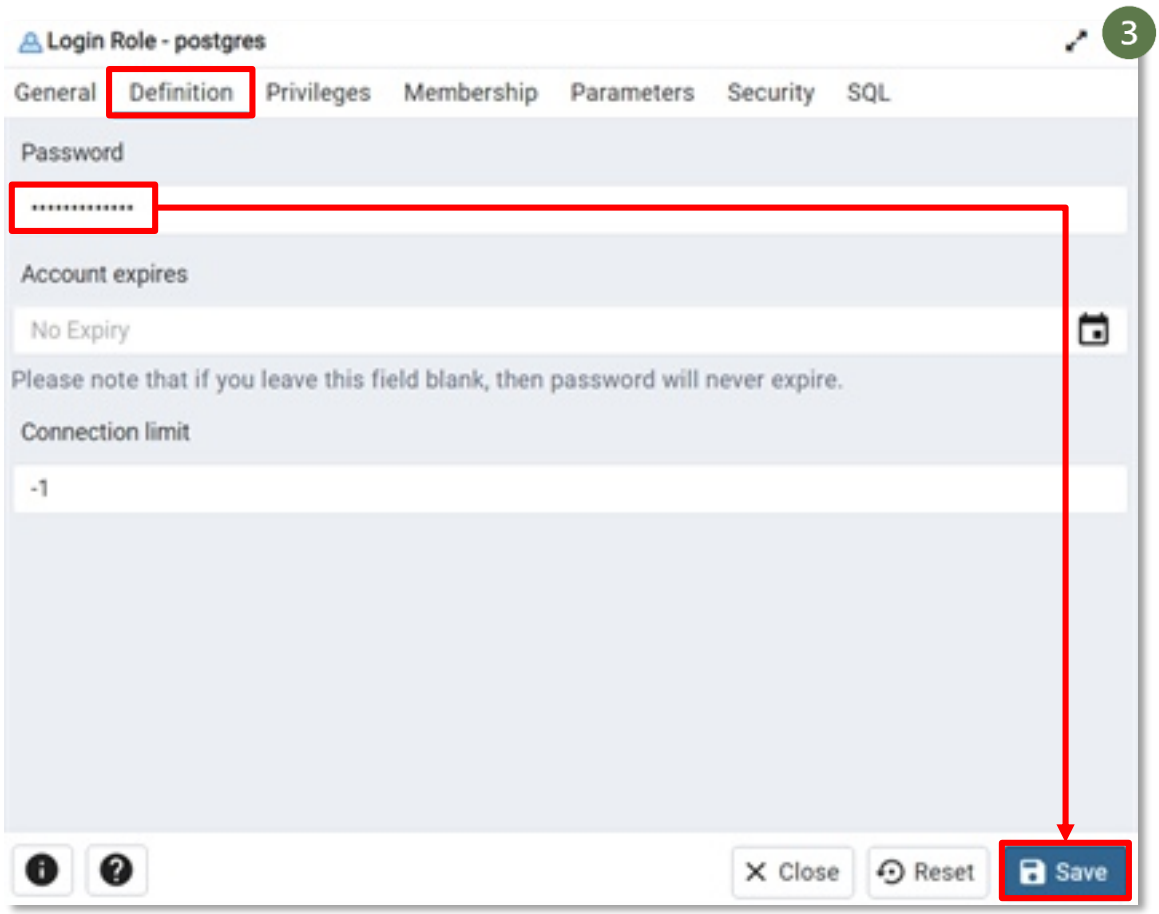
비밀번호 설정/변경 방법 - UI 방식

1. [pgAdmin 'Object Explorer'] > [사용 중인 데이터베이스 선택] > ['Login/Group Roles' 클릭]
2. [하위 항목에서 비밀번호를 바꿀 계정 확인] > [해당 계정 '우클릭' 후 'Properties...' 선택]



Postgre-SQL

3 ['Definition' 클릭] > [“Password” 항목에 문자와 숫자, 특수문자를 조합한 최소 8자 이상의 비밀번호 설정하기] > [설정 후 'Save' 클릭]



안전한 비밀번호 설정하기

안전한 비밀번호를 설정하는 것은 곧, 회사의 정보 자산을 안전하게 지키는 것입니다. 특히 데이터베이스의 경우, 고객들의 개인정보 및 회사 임직원의 정보 등 안전하게 지켜야 할 정보들이 많이 저장되어 있기 때문에 비밀번호 설정에 더욱 신경을 써야 합니다.

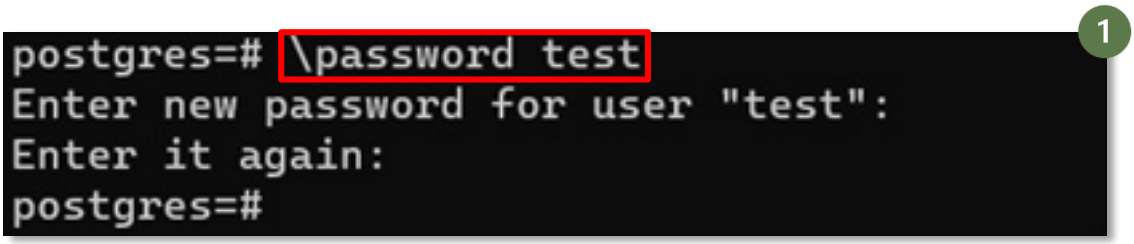
- 비밀번호 설정 시 문자와 숫자, 특수문자를 포함한 최소 8~12자 이상으로 설정하기
- 같은 문자, 혹은 숫자를 연속으로 사용하지 않기
- 회사 임직원 이름, 혹은 회사명 등 유추하기 쉬운 단어는 사용하지 않기
- 한 번 사용했던 비밀번호는 다시 쓰지 않기

Postgre-SQL

비밀번호 설정/변경 방법 - 쿼리문 방식

1. [Postgre SQL 데이터베이스 접속] > ['\password' 명령어를 통해 비밀번호 변경]
   - 아래 명령어의 '\' 은 역슬래시로, 키보드의 '₩' (혹은 '\') 버튼으로 입력 가능합니다.

```
# \password [계정명]
```



비밀번호 설정 시 유의사항

비밀번호 입력 및 변경 시 글씨가 보이지 않는 것이 정상입니다.

Postgre-SQL

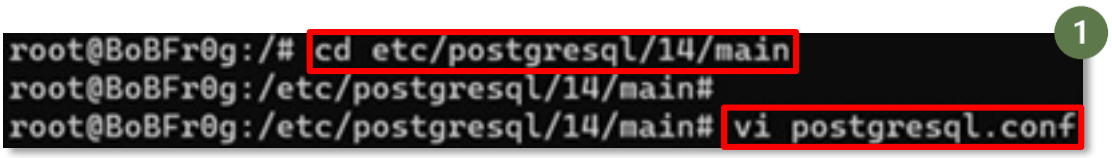
비밀번호 복잡성 조건 수정

PostgreSQL 서버 설정 파일 수정을 통해 비밀번호 복잡성 조건을 추가할 수 있습니다. 아래는 설정 파일 수정을 통해 추가되는 비밀번호 복잡성 조건입니다.

- 비밀번호 길이가 8자 이상인가?
- 비밀번호에 숫자와 문자가 포함되어 있는가?
- 비밀번호에 특수문자가 포함되어 있는가?

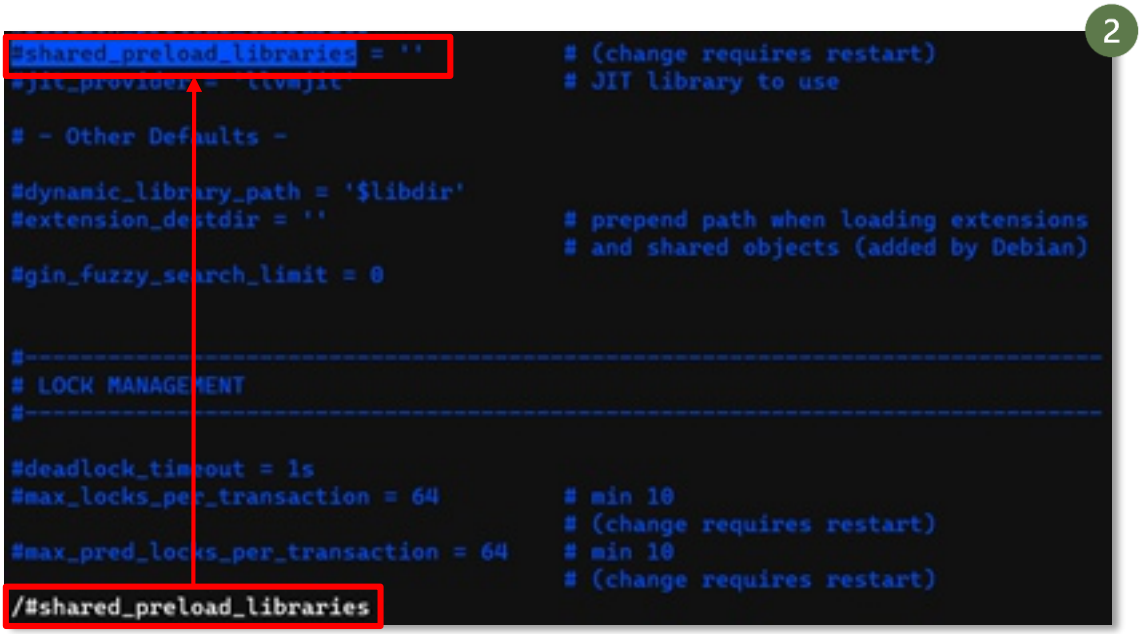
1. ['cd' 명령어를 통해 PostgreSQL 설정 파일 디렉토리로 이동] > [하단의 'vi' 명령어를 실행해 'postgresql.conf' 파일 열기]

```
# cd /etc/postgresql/14/main
# vi postgresql.conf
```



2. ['/#shared_preload_libraries'를 입력해 항목 검색]

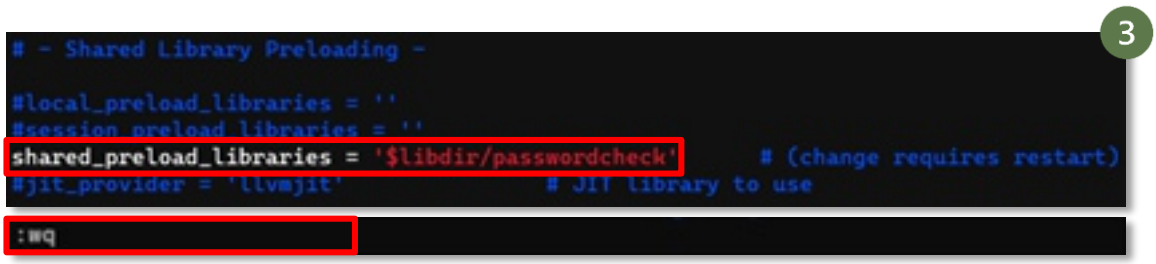
```
/#shared_preload_libraries
```



Postgre-SQL

3 ['i'를 통해 입력모드 진입] > [주석('#') 제거 후 '_' 부분에 '$libdir/passwordcheck' 작성] > [이후 키보드 ESC] > [':wq' 입력] > ['Enter' 입력]

```
#shared_preload_libraries = ' ' 에서 # 삭제
shared_preload_libraries = '$libdir/passwordcheck'
```



4 [터미널에 'service mysql restart' 명령어 입력] > [서비스 다시 시작]

```
service mysql restart
```

비밀번호 복잡성 조건이란?

비밀번호 복잡성 조건은 사용자가 설정한 비밀번호가 일정 수준 이상 복잡하게끔 만드는 보안 설정입니다. 이를 통해 비밀번호는 강력해지고 유추하기 어려워지며, 악의적인 사용자들로부터 계정을 보호할 수 있습니다.

Postgre-SQL

4. 사용자 계정 권한 관리하기

PostgreSQL에는 다양한 권한이 존재합니다. 예를 들어, Superuser 권한은 모든 작업을 제한 없이 수행할 수 있으며 Create Role 권한은 새 계정을 생성하고 권한을 할당할 수 있습니다. 이러한 권한이 불필요한 계정에 부여되어 있다면, 악의적인 사용자가 데이터베이스에서 계정을 조작하거나 데이터를 변경할 수 있으므로 계정에 부여된 불필요한 권한을 관리해야 합니다.

항 목 명	상 세 설 명
Can login?	사용자가 데이터베이스에 로그인 할 수 있는 권한을 의미
Superuser?	데이터베이스 시스템 내에서 가장 높은 수준의 권한을 의미
Create roles?	데이터베이스 사용자에게 역할을 부여할 수 있는 권한을 의미
Create databases?	데이터베이스를 생성할 수 있는 권한을 의미

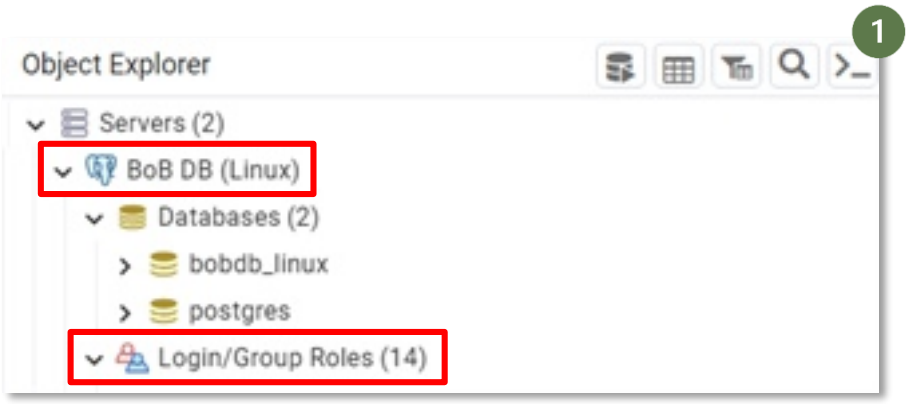
사용하는 계정에 맞는 적절한 권한 부여를 통해 불필요한 권한 사용을 막고 최소한의 권한을 사용하여 보안을 높여야 합니다. 또한, 필요한 권한이 있을 시에는 관리자를 통해 직접 권한을 요청하고 이를 승인해주는 방식을 사용하여 오직 관리자만이 권한을 부여할 수 있도록 해야 합니다.

	Can login?	Superuser?	Create roles?	Create database?
관리자	O	O	O	O
개발자	O	X	X	O
일반 사용자	O	X	X	X
사용하지 않는 계정	X	X	X	X

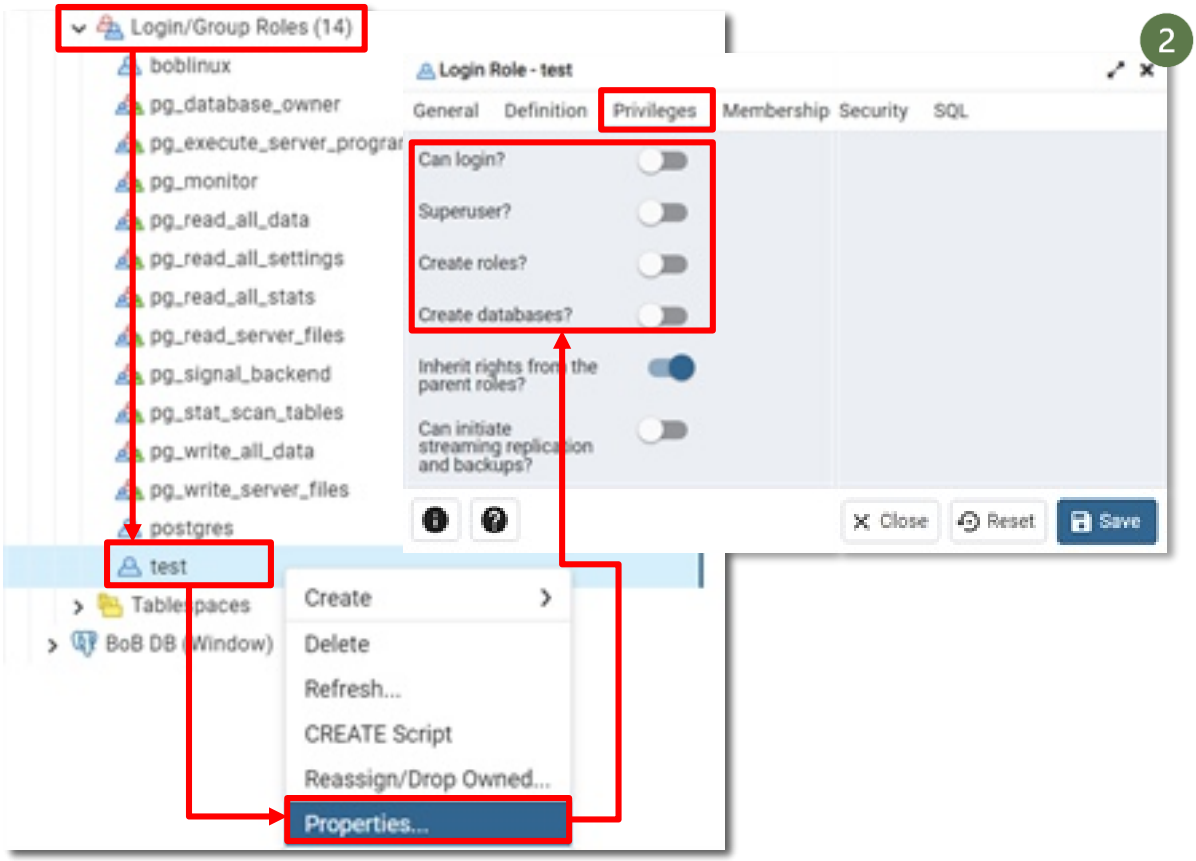
Postgre-SQL

계정 별 불필요한 권한 비활성화 하기 - UI 방식

1. [pgAdmin 'Object Explorer'] > [사용 중인 데이터베이스 선택] > ['Login/Group Roles' 클릭]



2. [권한을 변경할 계정 선택] > [해당 계정 우클릭 후 'Properties' 혹은 '속성' 선택] > ['Privileges' 클릭] > [해당 탭에서 아래 4개 중 불필요한 권한 비활성화] > ['Save' 클릭]

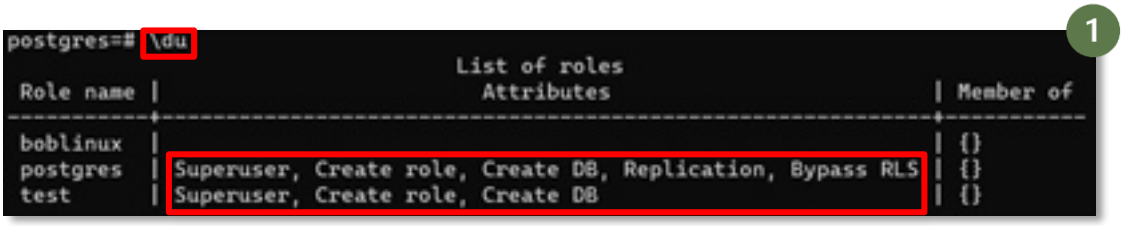


Postgre-SQL

계정 별 불필요한 권한 비활성화 하기 - 쿼리문 방식

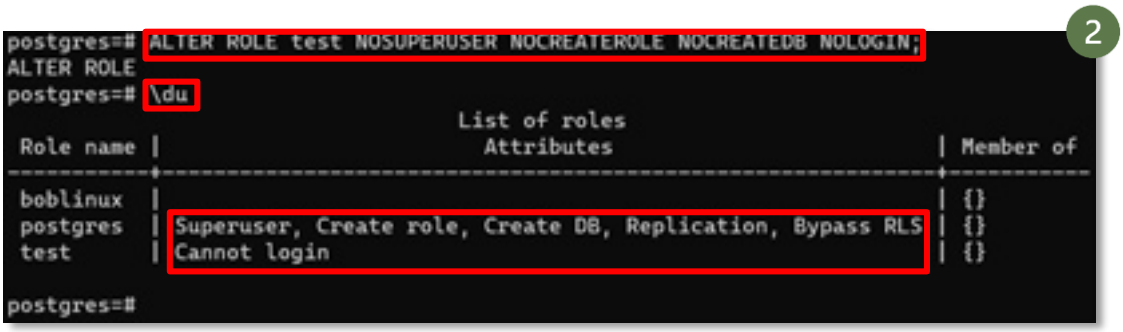
1. [PostgreSQL 데이터베이스 접속] > ['\du' 명령어로 사용자 별 권한 확인]
   - 아래 명령어의 '\' 은 역슬래시로, 키보드의 '₩' (혹은 '\') 버튼으로 입력 가능합니다.

```
# \du
```



2. [권한 설정 확인 후 'ALTER ROLE' 쿼리문을 실행하여 불필요한 권한 삭제]

```
# ALTER ROLE [사용자명] [삭제할 권한명];
```



예시에서 사용된 권한 알아보기	
권 한 명	**상 세 설 명**
NOSUPERUSER	사용자는 슈퍼유저 권한을 갖지 않습니다. 즉, 시스템 전체의 최고 권한을 부여하는 슈퍼유저가 아닌 일반 사용자로 취급됩니다.
NOCREATEROLE	사용자는 데이터베이스 역할을 생성할 수 없습니다. 데이터베이스 역할은 특정 권한을 가진 사용자 그룹을 나타내며, 이 권한을 가진 사용자는 다른 사용자에 대한 권한을 관리할 수 있습니다.
NOCREATEDB	사용자는 데이터베이스를 생성할 수 없습니다. 데이터베이스 생성 권한이 없는 사용자는 새로운 데이터베이스를 만들거나 소유할 수 없습니다.
NOLOGIN	사용자는 로그인할 수 없습니다. 로그인 권한이 없는 사용자는 시스템에 로그인할 수 없으며, 주로 시스템에 대한 작업을 수행하지 않는 사용자에게 권한을 부여합니다.

Postgre-SQL

5. 데이터베이스 권한 관리하기

PostgreSQL에서 새 데이터베이스를 만들면 기본적으로 public 스키마가 포함됩니다. 특정 스키마를 지정하지 않고 테이블을 생성하면 public 스키마에 위치하게 됩니다. public 스키마는 모든 사용자가 접근할 수 있어, 데이터 노출이나 시스템 자원의 과도한 사용과 같은 보안 문제가 발생할 수 있습니다.

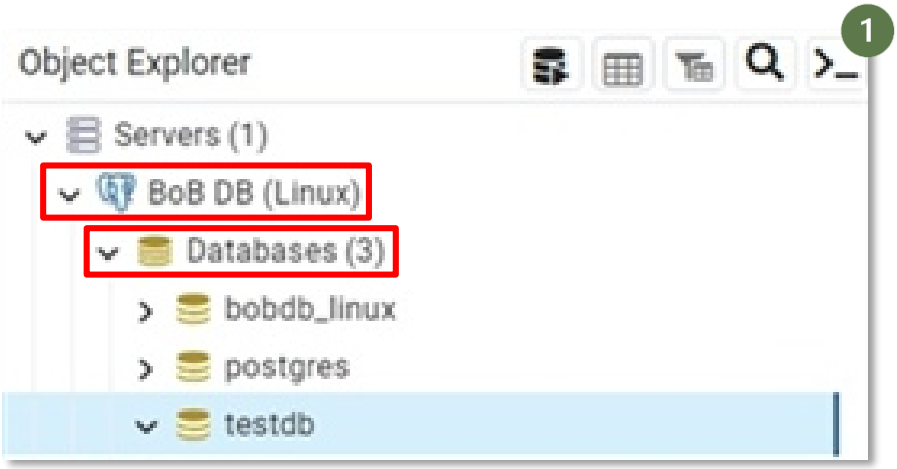
스키마(schema)에 Public 권한이 들어가면 안되는 이유

스키마(Schema)는 데이터베이스에서 어떤 종류의 데이터가 저장되고 그 데이터가 어떻게 구성되는지에 대한 전반적인 계획이나 설계를 말합니다.

public 권한을 허용한다는 것은 모든 사용자와 역할이 해당 스키마에 접근할 수 있게 된다는 의미입니다. 이러한 경우, 모든 사용자들이 해당 스키마 내에 저장되어 있는 정보들을 확인할 수 있고, 이로 인한 보안 사고의 위험이 존재합니다. 따라서, 스키마에 public 권한이 포함되어서는 안됩니다.

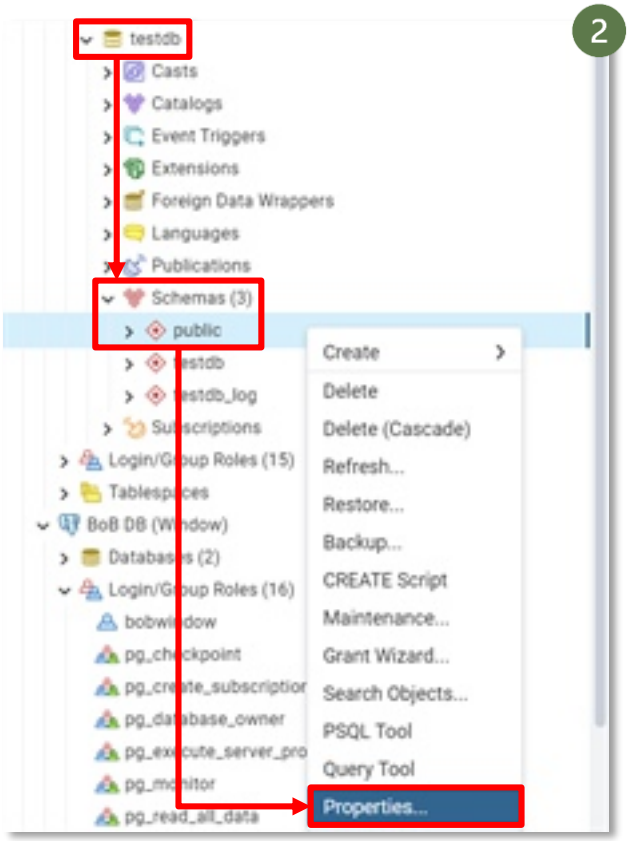
DB의 Public Schema 접근 권한 해제하기 - UI 방식

1. [pgAdmin 'Object Explorer'] > [사용 중인 데이터베이스 선택] > ['Databases' 클릭]

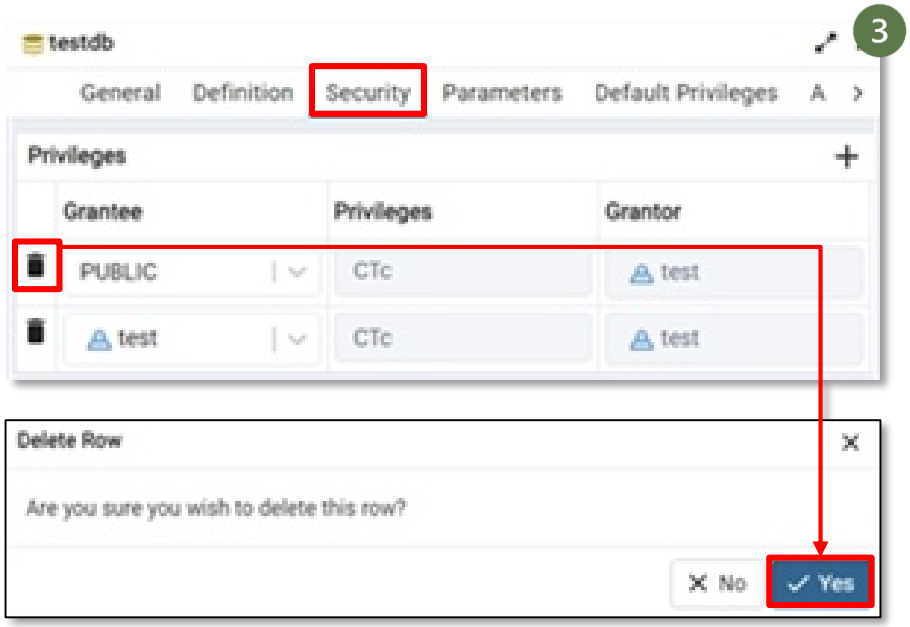


Postgre-SQL

2 [하위 항목의 개별 DB 선택] > ['Schemas' 클릭] > ['Public' 항목 우클릭 후 'Properties' 선택]



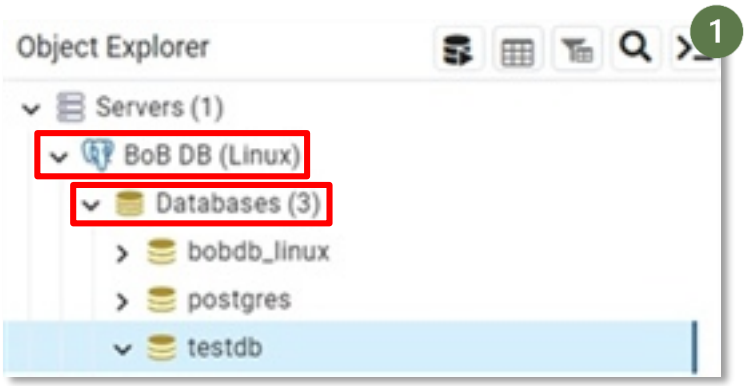
3 ['Security' 클릭] > ['Privileges' 부분의 PUBLIC 항목 삭제] > ['Yes' 클릭]



Postgre-SQL

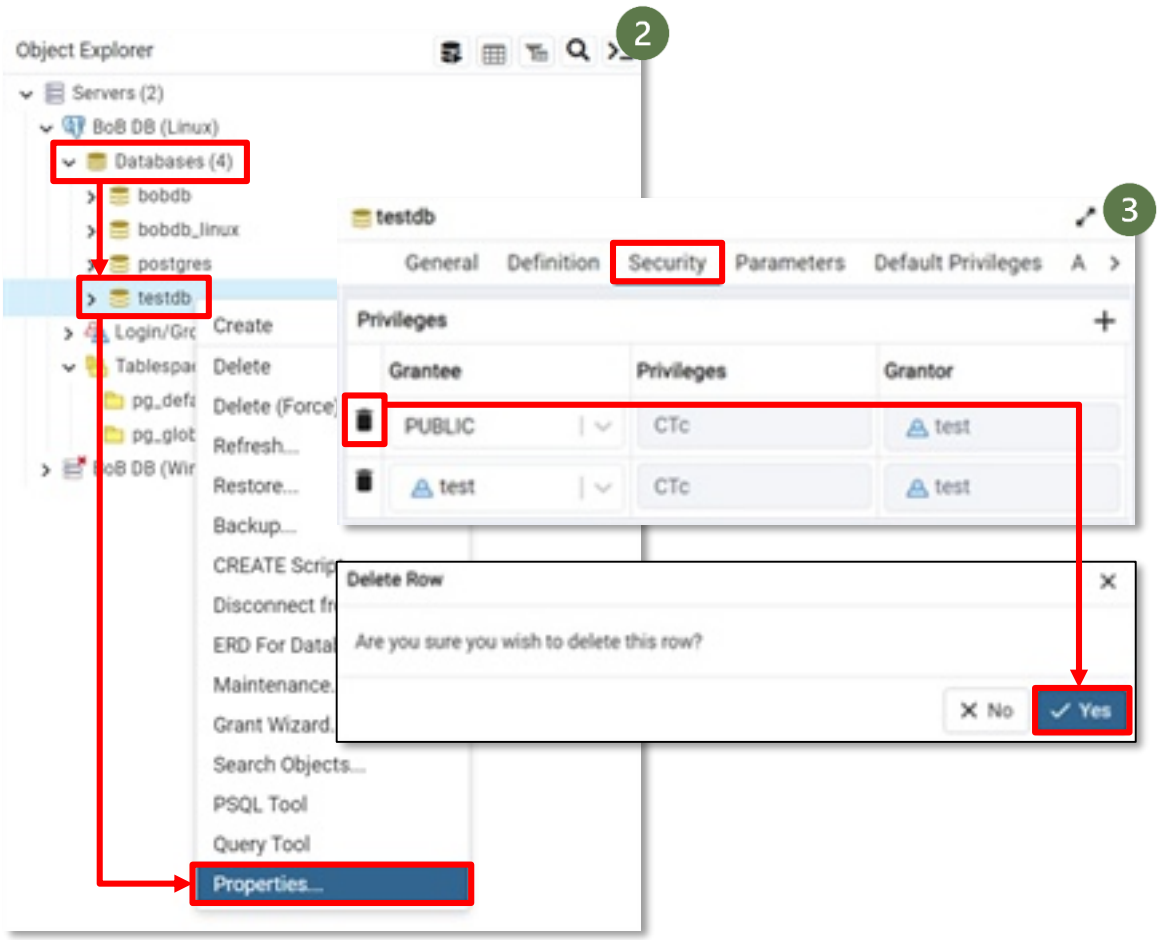
DB의 Public 접근 권한 해제하기 - UI 방식

1. [pgAdmin Object Explorer] > [사용 중인 데이터베이스 선택] > ['Databases' 클릭]



2. [하위 항목의 개별 DB 선택] > [개별 DB 우클릭 후 'Properties' 클릭]

3. ['Security' 클릭] > ['Privileges' 부분의 PUBLIC 항목 삭제] > ['Yes' 클릭]



Postgre-SQL

DB의 Public Schema 접근 권한 해제하기 - 쿼리문 방식

1. [PostgreSQL 데이터베이스 접속] > ['\c' 명령어를 통해 개별 데이터베이스로 접속]
   - 아래 명령어의 '\' 은 역슬래시로, 키보드의 '₩' (혹은 '\') 버튼으로 입력 가능합니다.

```
# \c [DB명] postgres
```

```
postgres=# \c testdb postgres
You are now connected to database "testdb" as user "postgres".
testdb=# \dn+
                              List of schemas
    Name    |  Owner   |  Access privileges   |      Description
------------+----------+----------------------+------------------------
 public     | postgres | postgres=UC/postgres+| standard public schema
            |          | =UC/postgres         |
 testdb     | test     |                      |
 testdb_log | test     |                      |
(3 rows)
```

1

2. ['REVOKE' 쿼리문을 통해 Public Schema 사용 및 접근 권한 삭제]

```
# REVOKE all on schema public from PUBLIC;
```

```
testdb=# REVOKE all on schema public from PUBLIC;
REVOKE
testdb=# \dn+
                              List of schemas
    Name    |  Owner   |  Access privileges   |      Description
------------+----------+----------------------+------------------------
 public     | postgres | postgres=UC/postgres | standard public schema
 testdb     | test     |                      |
 testdb_log | test     |                      |
(3 rows)
```

2

Postgre-SQL

DB의 Public 접근 권한 해제하기 - 쿼리문 방식

1. [PostgreSQL 데이터베이스 접속] > ['\c' 명령어를 통해 개별 데이터베이스로 접속]
   - 아래 명령어의 '\' 은 역슬래시로, 키보드의 '₩' (혹은 '\') 버튼으로 입력 가능합니다.

```
# \c [DB명] postgres
```

```
postgres=# \c testdb postgres
You are now connected to database "testdb" as user "postgres".
testdb=# \dn
    List of schemas
    Name     |  Owner
-------------+----------
 public      | postgres
 testdb      | test
 testdb_log  | test
(3 rows)
```

1

2. ['REVOKE' 쿼리문을 통해 데이터베이스의 Public 접근 권한 삭제]

```
# REVOKE all on database [DB명] from PUBLIC;
```

```
testdb=# REVOKE all on database testdb from PUBLIC;
REVOKE
testdb=# \c testdb newtest
Password for user newtest:
connection to server on socket "/var/run/postgresql/.s.PGSQL.5530" failed:
 FATAL:  permission denied for database "testdb"
DETAIL:  User does not have CONNECT privilege.
Previous connection kept
```

2

Postgre-SQL

DB의 Public Schema 접근 권한 해제하기 - 쿼리문 방식

1. [PostgreSQL 데이터베이스 접속] > ['\c' 명령어를 통해 template1 데이터베이스로 접속]
   - 아래 명령어의 '\' 은 역슬래시로, 키보드의 '₩' (혹은 '\') 버튼으로 입력 가능합니다.

```
\c template1 postgres
```

```
postgres=# \c template1 postgres
You are now connected to database "template1" as user "postgres".
template1=# \dn+
                           List of schemas
  Name   |  Owner   |  Access privileges   |      Description
---------+----------+----------------------+------------------------
 public  | postgres | postgres=UC/postgres+| standard public schema
         |          | =UC/postgres         |
(1 row)
```

1

2. ['REVOKE' 쿼리문을 통해 추후 생성될 데이터베이스에 대한 Public 접근 권한 삭제]

```
# REVOKE all on schema public from PUBLIC;
```

```
template1=# REVOKE all on schema public from PUBLIC;
REVOKE
template1=# \dn+
                           List of schemas
  Name   |  Owner   |  Access privileges   |      Description
---------+----------+----------------------+------------------------
 public  | postgres | postgres=UC/postgres | standard public schema
(1 row)
```

2

PostgreSQL - template DB란?

PostgreSQL에서 “템플릿 데이터베이스(template DB)”는 새로운 데이터베이스를 생성할 때 기본 구조로 사용되는 특별한 종류의 데이터베이스로, PostgreSQL에는 두 가지 템플릿 데이터베이스가 있습니다.

Postgre-SQL

6. 안전한 사용자 인증 방식 사용하기

PostgreSQL은 사용자의 안전한 데이터베이스 접속을 위해 'scram-sha-256'이라는 암호화 방식을 지원하며, 이를 사용해 데이터베이스에 안전하게 접속할 수 있습니다.

scram-sha-256 방식이란?

scram-sha-256은 PostgreSQL 데이터베이스에서 사용할 수 있는 비밀번호 암호화 및 인증 방식입니다. scram-sha-256은 비밀번호를 보관하고 인증하는 과정이 복잡하고 비밀번호를 추측하기 어렵게 하는 기능이 추가되어 더욱 안전하게 비밀번호를 관리할 수 있습니다.

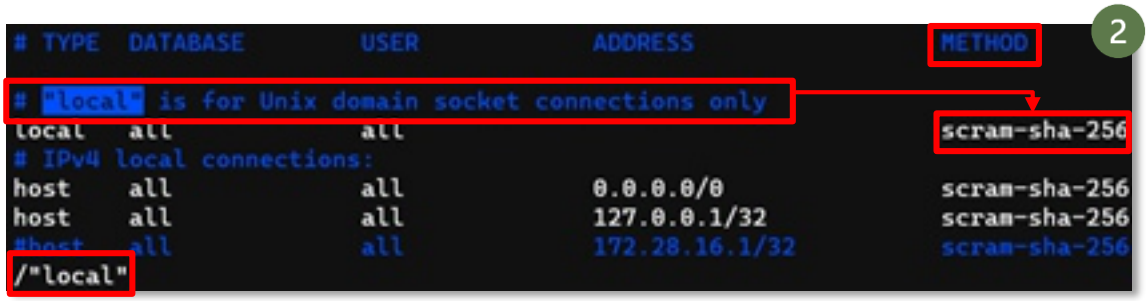
scram-sha-256 방식 설정하기 - 명령어 방식

1. [터미널 실행] > ['cd' 명령어를 통해 PostgreSQL 설정 파일 디렉토리로 이동] > [하단의 'vi' 명령어를 실행해 'pg_hba.conf' 파일 열기]

```
# cd /etc/postgresql/14/main
# vi pg_hba.conf
```

2. ['/"local"'를 입력하여 설정 항목 검색] > ['local is for Unix domain socket connections only' 항목의 'METHOD' 부분을 'scram-sha-256'으로 입력]

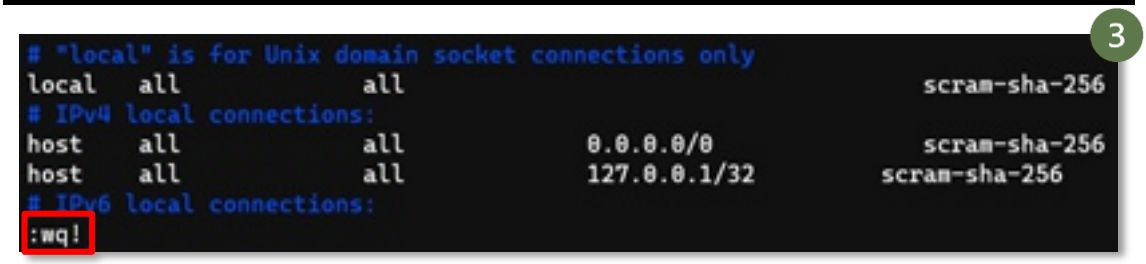
```
/"local"
local    all    all    scram-sha-256
```



Postgre-SQL

3 [키보드 'ESC'] > [':wq!' 입력] > ['Enter' 입력해 편집기 닫기]

```
:wq!
```



4 [터미널에 'service postgresql restart' 명령어 입력] > [서비스 다시 시작]

```
# service postgresql restart
```

설정 파일 디렉토리 이동 시 주의사항

설정 파일 디렉토리로 이동할 때 (cd /etc/postgresql/14/main) '14' 부분은 PostgreSQL 버전에 따라 변경해야 합니다.

(ex. 13버전일 경우 'cd /etc/postgresql/13/main')

Postgre-SQL

7. 안전한 비밀번호 저장 방식 사용하기

PostgreSQL은 사용자 비밀번호를 안전하게 암호화하여 관리하기 위해 'scram-sha-256' 이라는 암호화 방식을 지원하며, 이를 사용해 비밀번호를 안전하게 저장할 수 있습니다.

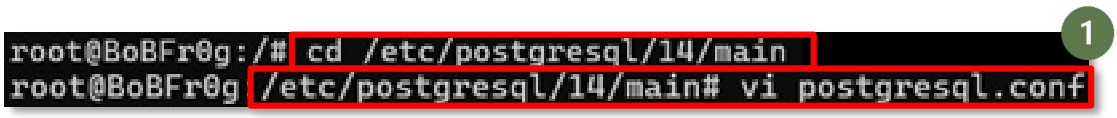
scram-sha-256 방식이란?

scram-sha-256은 PostgreSQL 데이터베이스에서 사용할 수 있는 비밀번호 암호화 및 인증 방식입니다. scram-sha-256은 비밀번호를 보관하고 인증하는 과정이 복잡하고 비밀번호를 추측하기 어렵게 하는 기능이 추가되어 더욱 안전하게 비밀번호를 관리할 수 있습니다.

scram-sha-256 방식 설정하기 - 명령어 방식

1. [터미널 실행] > ['cd' 명령어를 통해 PostgreSQL 설정 파일 디렉토리로 이동] > [하단의 'vi' 명령어를 실행해 'postgresql.conf' 파일 열기]

```
# cd /etc/postgresql/14/main
# vi postgresql.conf
```



설정 파일 디렉토리 이동 시 주의사항

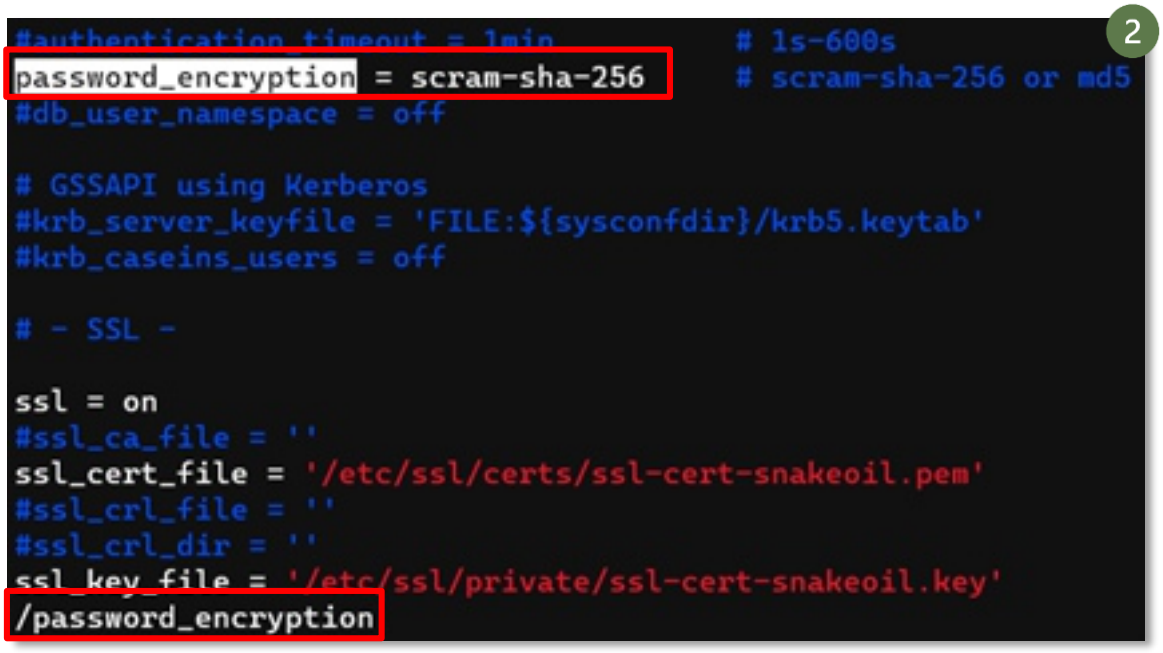
설정 파일 디렉토리로 이동할 때 (cd /etc/postgresql/14/main) '14' 부분은 PostgreSQL 버전에 따라 변경해야 합니다.

(ex. 13버전일 경우 'cd /etc/postgresql/13/main')

Postgre-SQL

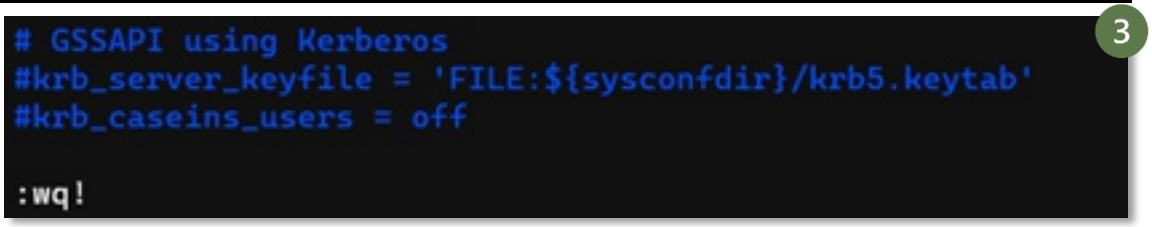
2 ['/password_encryption'를 입력하여 설정 항목 검색] > ['i'를 통해 입력모드 진입] > ['password_encryption' 주석 제거(# 제거)] > [하단과 같이 'scram-sha-256' 추가]

```
/password_encryption
password_encryption = scram-sha-256
```



3 [':wq!' 입력] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기]

```
:wq!
```



4 [터미널에 'service postgresql restart' 명령어 입력] > [서비스 다시 시작]

```
# service postgresql restart
```

Postgre-SQL

8. 데이터 디렉토리 권한 관리하기

PostgreSQL의 데이터 디렉토리에 권한 설정이 취약하게 되어있는 경우 인가되지 않은 사용자가 파일을 자유롭게 생성, 삭제, 수정할 수 있습니다. 이 과정에서 중요 서버 설정 파일이 손상되는 등 보안 위험을 초래할 수 있습니다. 따라서, 권한 설정을 통해 접근 권한을 제한해야 합니다.

데이터 디렉토리 권한 설정하기 - 명령어 방식

1 [하단의 'chmod' 명령어를 통해 데이터 디렉토리 권한 변경]

```
# chmod 700 /var/lib/postgresql/(버전)/main
```

```
root@BoBFr0g:/# chmod 700 /var/lib/postgresql/14/main
root@BoBFr0g:/# ls -l /var/lib/postgresql/14
total 4
drwx------ 19 postgres postgres 4096 Nov 30 20:37 main
root@BoBFr0g:/#
```

1

700 권한이란?

700은 숫자로 표현된 권한 값으로, 소유자에게 읽기, 쓰기, 실행 권한을 부여하며, 그룹과 기타 사용자에게는 어떠한 권한도 주지 않음을 의미합니다.

리눅스에서 권한이란?

리눅스에서의 권한은 파일이나 디렉토리에 대한 사용자의 접근 수준을 설정하는 것입니다. 이러한 권한을 통해 해당 파일이나 디렉토리를 누가 볼 수 있고, 수정할 수 있으며, 실행할 수 있는지를 결정합니다. 아래는 리눅스 권한을 읽는 법과 영문, 숫자 표기법입니다.

	파일 유형	파일 소유자 권한			파일 소유 그룹 권한			기타 사용자 권한		
영문 표기법	-	r	w	x	r	w	x	r	w	x
숫자 값	- : 파일 d : 디렉토리	4	2	1	4	2	1	4	2	1
숫자 표기법		7			7			7		
권 한		읽기	쓰기	실행	읽기	쓰기	실행	읽기	쓰기	실행

Postgre-SQL

9. Postgre SQL 서버 환경 설정파일 권한 관리하기

PostgreSQL의 핵심 환경 설정 파일의 권한이 취약하게 설정되어 있는 경우 해커에 의해 권한이 변경될 수 있으며, 이를 통해 서버 장애 및 여러 보안 문제를 일으킬 수 있습니다. 따라서, 적절한 권한 설정을 통해 접근 권한을 제한해야 합니다.

핵심 서버 환경 설정파일	상 세 설 명	권장 파일 권한
postgresql.conf	PostgreSQL 서버의 주요 설정 파일로, 데이터베이스의 동작과 성능에 관련된 다양한 설정을 포함합니다.	600
pg_hba.conf	사용자가 어떤 방식으로 데이터베이스에 접근할 수 있는지 세부적으로 제어하는 설정 파일	600
pg_ident.conf	실제 시스템 사용자 이름과 PostgreSQL 사용자 이름 간의 매핑을 정의	600
pg_ctl.conf	서버를 시작, 중지, 재시작하는데 사용되는 명령어 및 유틸리티에 대한 설정을 관리합니다. * 해당 파일은 버전에 따라 없을 수도 있습니다.	600
start.conf	PostgreSQL 서버가 시스템 시작 시 어떤 방식으로 실행될지를 정의 * 해당 파일은 버전에 따라 없을 수도 있습니다.	600

Postgre-SQL

서버 환경 설정파일 권한 설정하기 - 명령어 방식

1 ['cd' 명령어를 통해 postgresql 설정 파일 디렉토리로 이동]

```
# cd /etc/postgresql/14/main
```

```
root@BoBFr0g:/# cd /etc/postgresql/14/main
```

2 ['ls -l' 명령어를 통해 설정 파일들의 권한 확인]

```
# ls -l
```

```
root@BoBFr0g:/etc/postgresql/14/main# ls -l
total 60
drwxr-xr-x 2 postgres postgres  4096 Nov  6 19:43 conf.d
-rw-r--r-- 1 postgres postgres   315 Nov  6 19:43 environment
-rw------- 1 postgres postgres   143 Nov  6 19:43 pg_ctl.conf
-rw------- 1 postgres postgres  5104 Dec  5 16:21 pg_hba.conf
-rw------- 1 postgres postgres  1636 Nov  6 19:43 pg_ident.conf
-rw------- 1 postgres postgres 29043 Dec  5 16:22 postgresql.conf
-rw------- 1 postgres postgres   317 Nov  6 19:43 start.conf
```

3 [하단의 'chmod' 명령어를 통해 설정 파일들의 권한 변경]

```
# chmod 600 (서버 환경 설정파일명)
```

```
root@BoBFr0g:/etc/postgresql/14/main# chmod 600 pg_ctl.conf
root@BoBFr0g:/etc/postgresql/14/main# chmod 600 pg_hba.conf
root@BoBFr0g:/etc/postgresql/14/main# chmod 600 pg_ident.conf
root@BoBFr0g:/etc/postgresql/14/main# chmod 600 postgresql.conf
root@BoBFr0g:/etc/postgresql/14/main# chmod 600 start.conf
```

Postgre-SQL

10. 로그 관리하기

데이터베이스 로그를 활성화하는 것은 중요한 보안조치 입니다. 로그는 데이터베이스의 모든 것을 기록하고, 이를 통해 데이터의 무결성을 보장합니다. 또한, 데이터베이스에서 발생한 침해사고 및 비정상적인 활동을 추적하는 데 중요한 역할을 합니다.

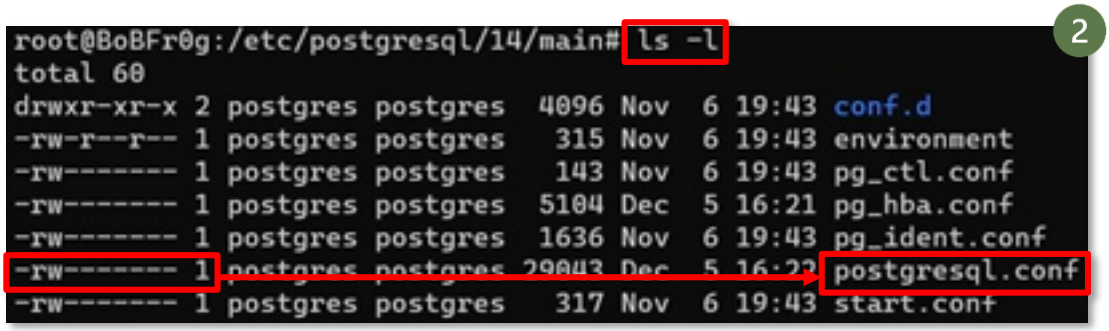
로그 활성화하기

1. ['cd' 명령어를 통해 postgresql 설정 파일 디렉토리로 이동]

```
# cd /etc/postgresql/14/main
```

2. ['ls -l' 명령어를 통해 postgresql.conf 파일 권한 확인]

```
# ls -l
```



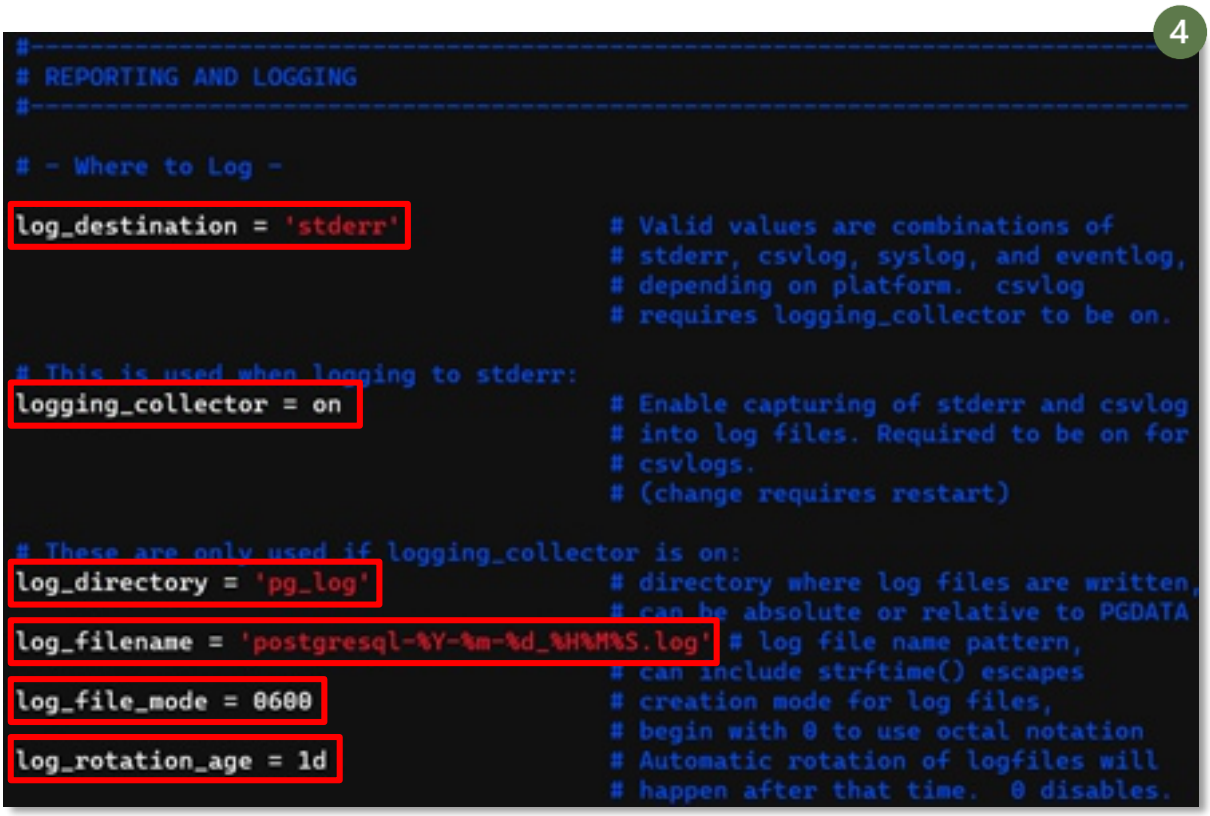
3. ['vi' 명령어를 통해 postgresql.conf 파일 열기]

```
# vi postgresql.conf
```

Postgre-SQL

4 [하단의 표를 참고해 'Where to Log' 항목의 로그 활성화 설정]

Where to Log		
설정 항목	권장 설정	상세 내용
log_destination	주석(#) 제거	Log 파일 생성 방식 설정
logging_collector	주석(#) 제거 후 설정 값 'on' 변경	Log 파일 수집 및 생성 설정
log_directory	주석(#) 제거 후 설정 값 'pg_log' 변경	Log 파일 생성 경로 설정
log_filename	주석(#) 제거	Log 파일명 설정
log_file_mode	주석(#) 제거	Log 파일 권한 설정
log_rotation_age	주석(#) 제거	Log 파일의 생성 주기 설정



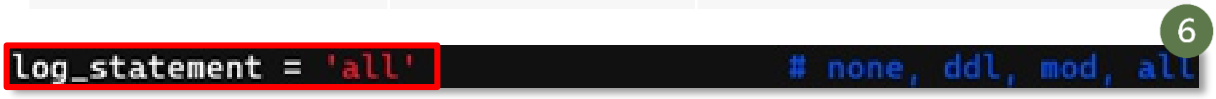
Postgre-SQL

5 [하단의 표를 참고해 'When to Log' 항목의 로그 활성화 설정]

When to Log		
설정 항목	권장 설정	상세 내용
log_min_duration_statement	주석(#) 제거 후 설정 값 '100' 설정	Log 파일에 기록될 쿼리문의 임계값 설정

6 [하단의 표를 참고해 'What to Log' 항목의 로그 활성화 설정]

What to Log		
설정 항목	권장 설정	상세 내용
log_statement	주석(#) 제거 후 설정 값 'all' 설정	Log 파일에 기록되는 쿼리 로그 수준을 설정합니다.



7 [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력해 편집기 닫기] > ['터미널'에 'service postgresql restart' 명령어 입력] > [서비스 다시 시작]

```
service postgresql restart
```

MY-SQL

0. MySQL Workbench 설치하기

MySQL은 MySQL Workbench라는 전용 UI 소프트웨어를 제공합니다. 본 가이드라인에서는 MySQL Workbench를 사용한 항목별 보안 조치 사항을 설정합니다. 아래에서는 먼저 MySQL Workbench 설치 및 기본 설정하는 방법을 안내합니다.

MySQL Workbench란?

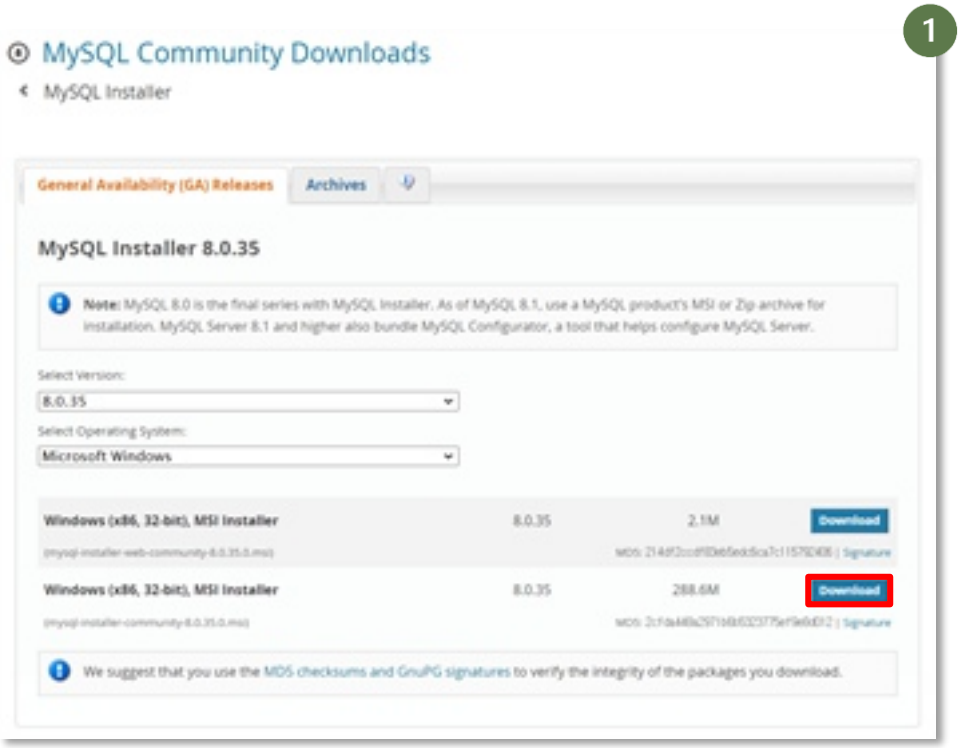
MySQL Workbench는 MySQL 데이터베이스를 관리하기 위한 인터페이스 환경입니다. 사용자 친화적인 인터페이스를 통해 SQL 쿼리 작성, 실행, 저장 및 데이터베이스 관리 작업을 편리하게 수행할 수 있습니다.

https://dev.mysql.com/downloads/windows/installer/ - Workbench 다운로드 링크

MySQL Workbench 설치하기

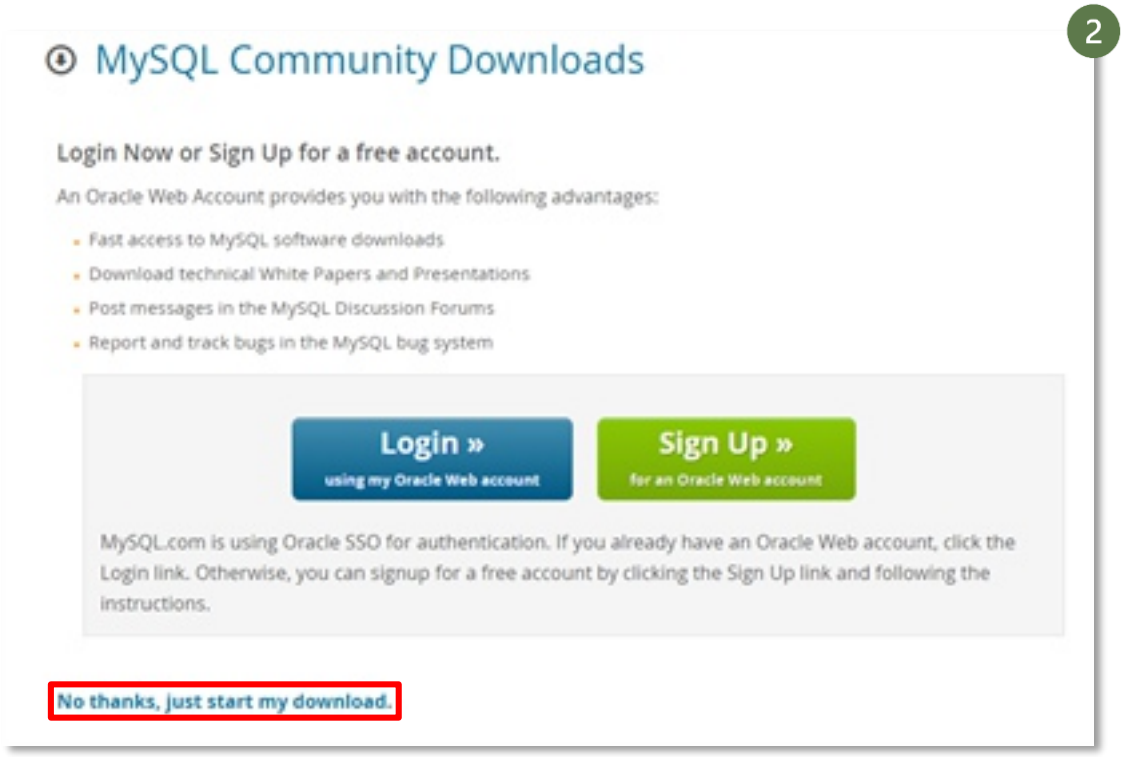
MySQL Workbench는 기본적으로 MySQL과 함께 설치됩니다. 만약 설치되어 있지 않다면 아래의 과정을 통해 직접 설치할 수 있습니다.

1. [위 다운로드 링크 클릭] > ['Windows (x86, 64-bit), MSI Installer' 옆의 'Download' 클릭]
   * 2023년 12월 기준 최신 버전: 8.0.35

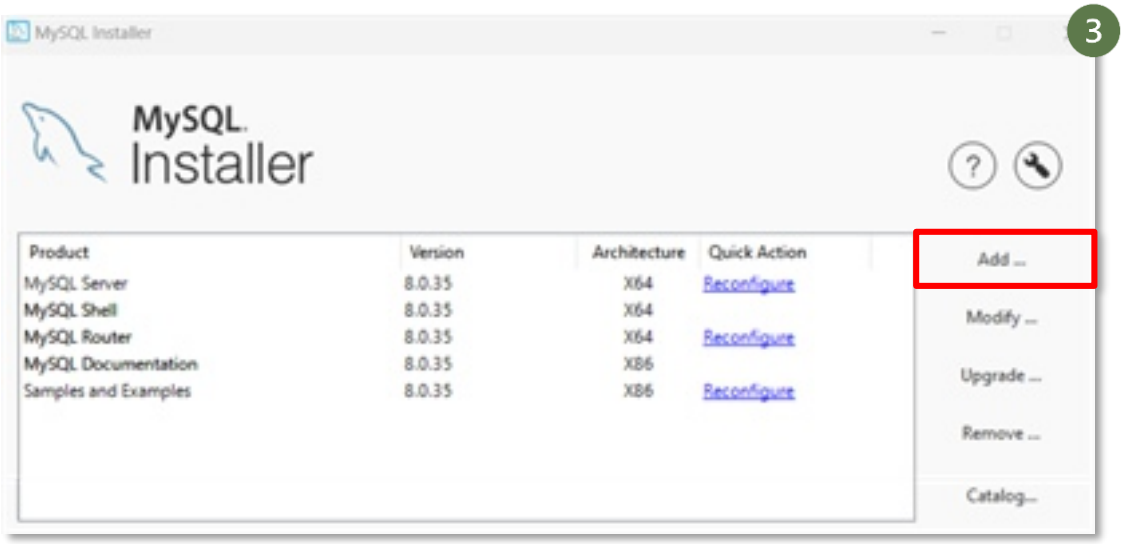


MY-SQL

2 [다음 화면에서 'No thanks, just start my download.' 클릭 후 파일 다운로드]



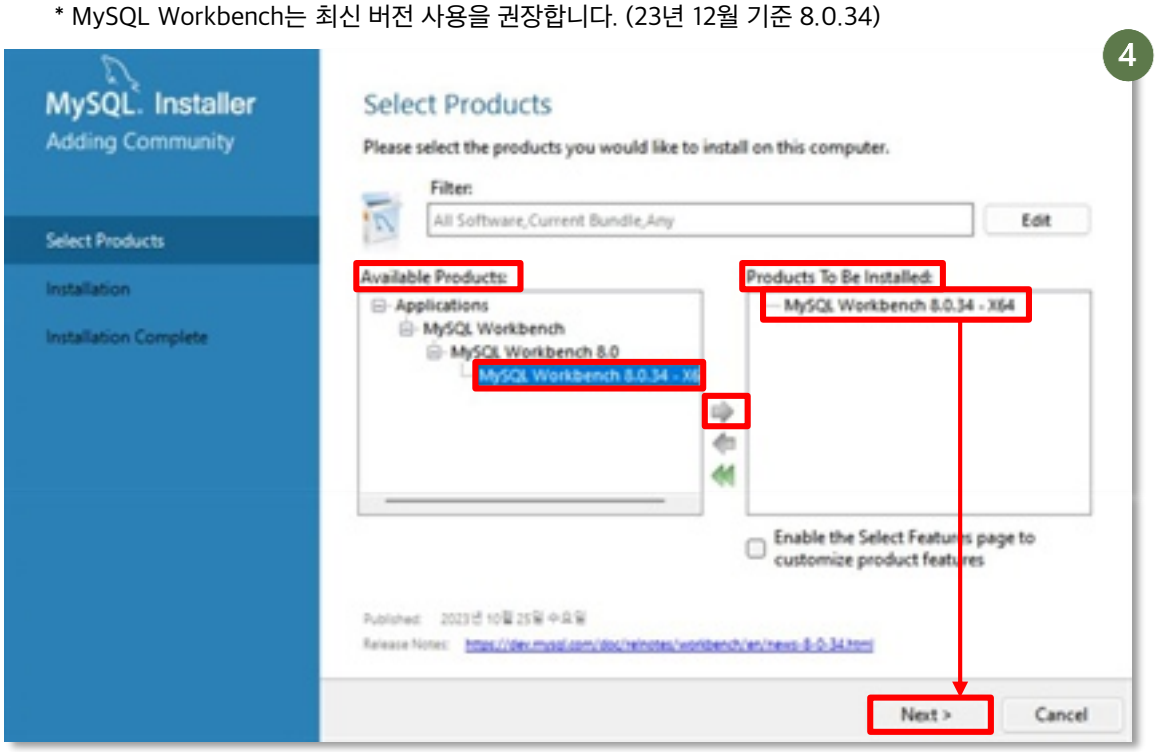
3 [다음 화면에서 'Add ...' 클릭]



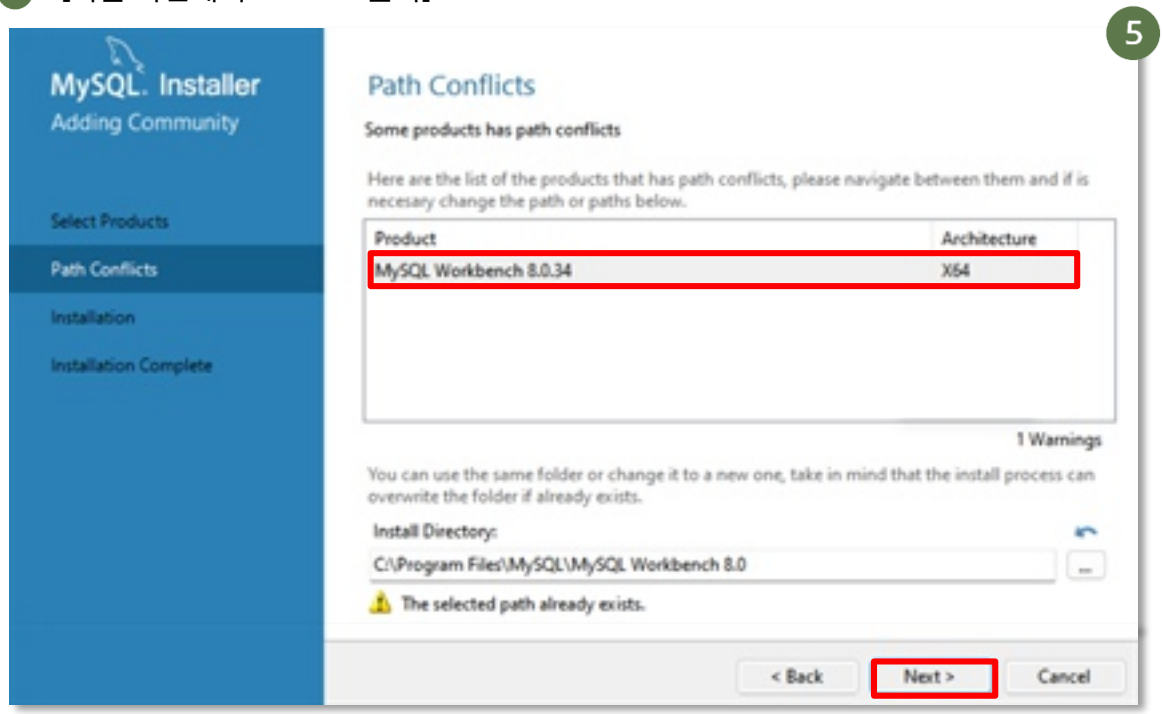
MY-SQL

4 [다음 화면의 'Available Products' 항목에서 'MySQL Workbench 8.0.xx -X64' 클릭 후 'Products To Be Installed'로 이동] > ['Next >' 클릭]

* MySQL Workbench는 최신 버전 사용을 권장합니다. (23년 12월 기준 8.0.34)

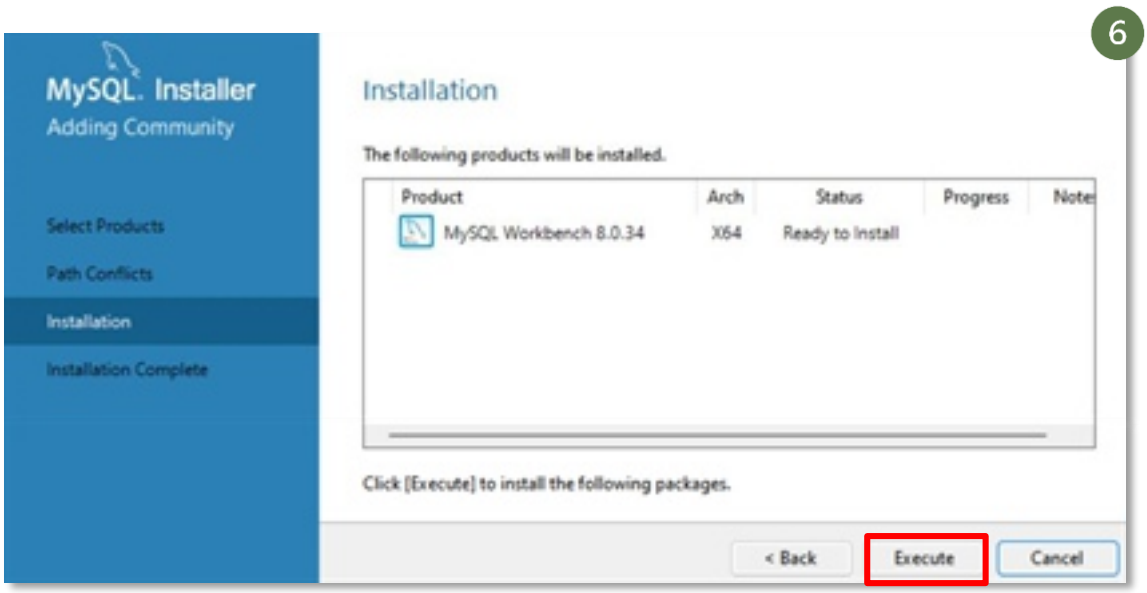


5 [다음 화면에서 'Next >' 클릭]

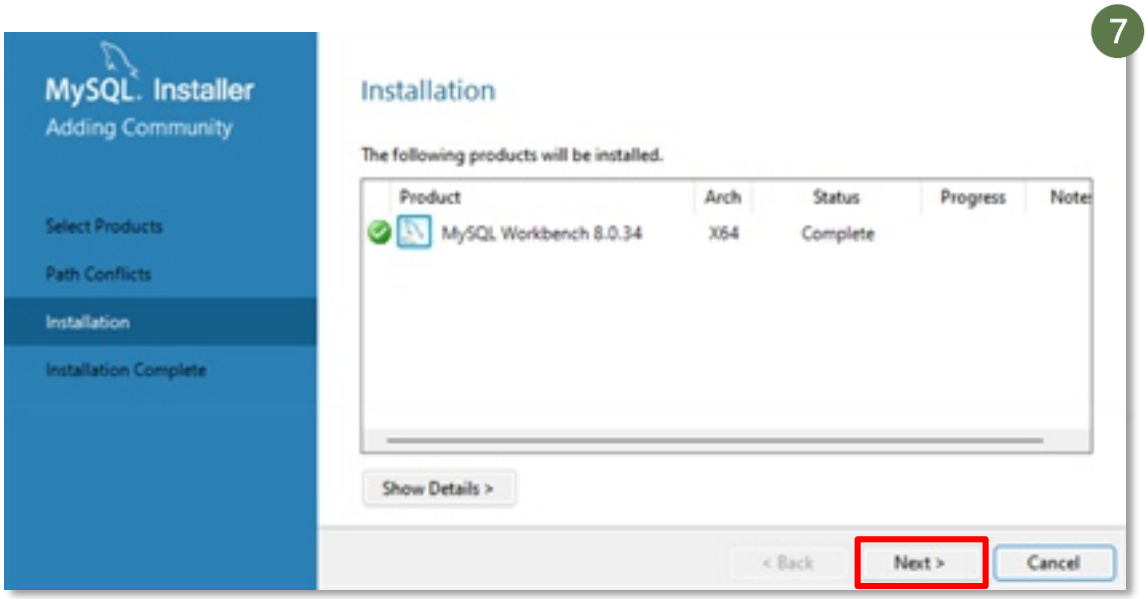


MY-SQL

6 [다음 화면에서 'Execute' 클릭]

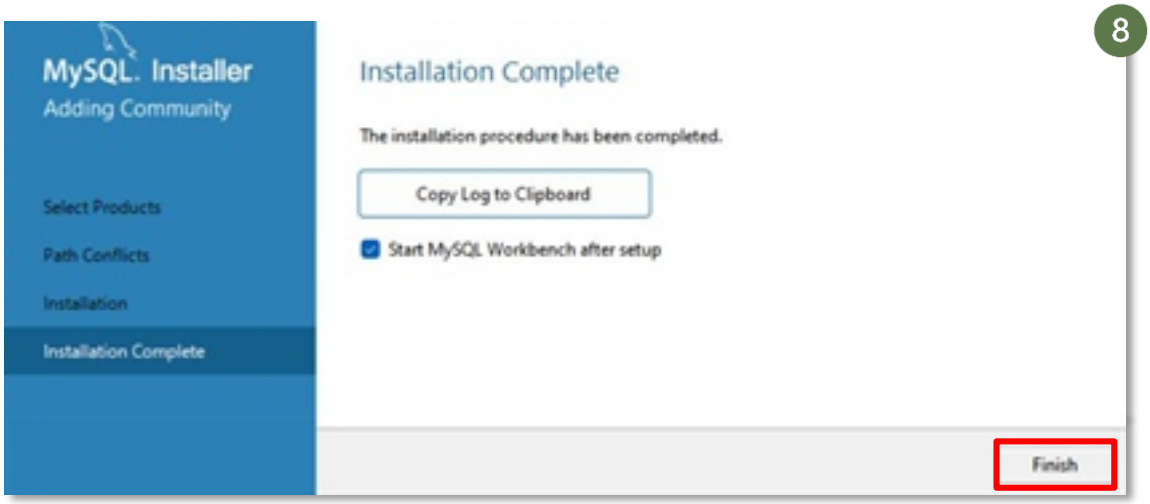


7 [설치 완료 후 'Next >' 클릭]

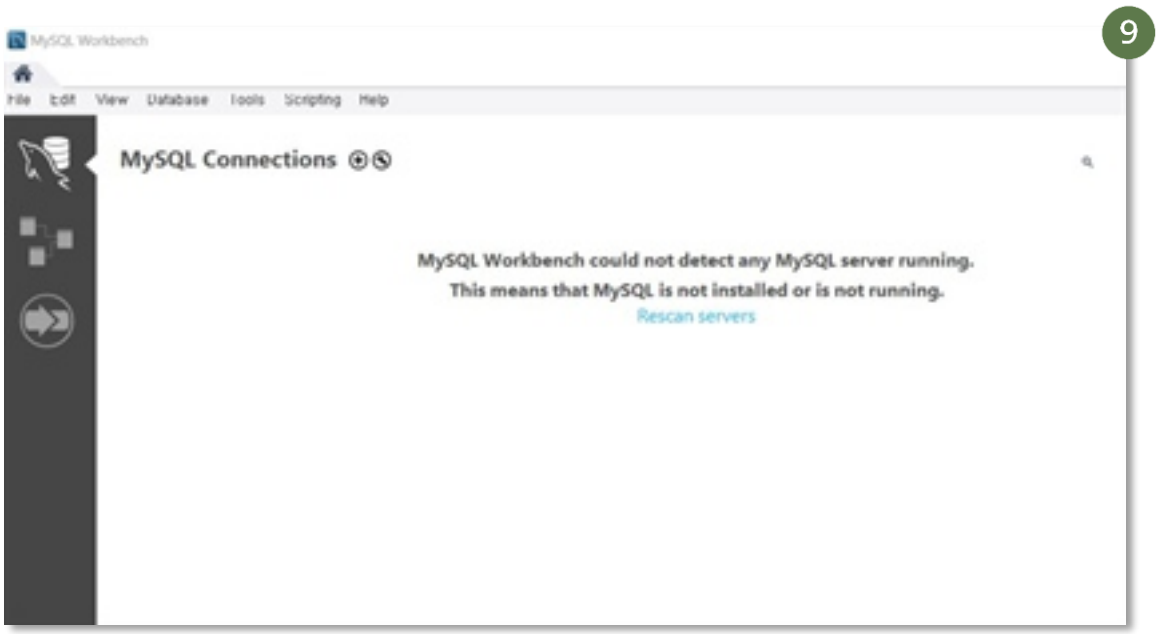


MY-SQL

8 [설치 완료 후 'Finish' 클릭]



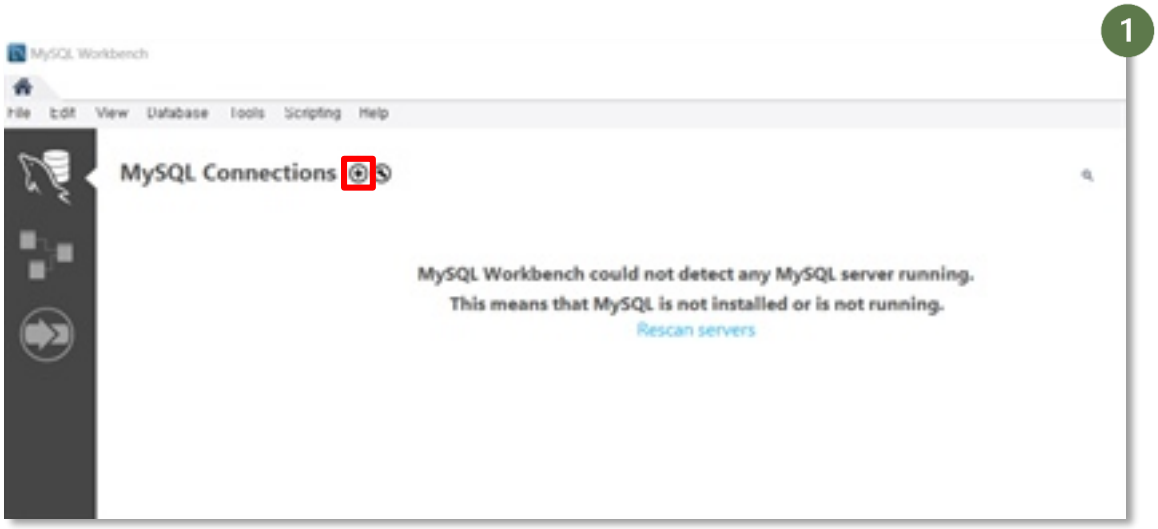
9 [MySQL Workbench 시작 시 메인 화면]



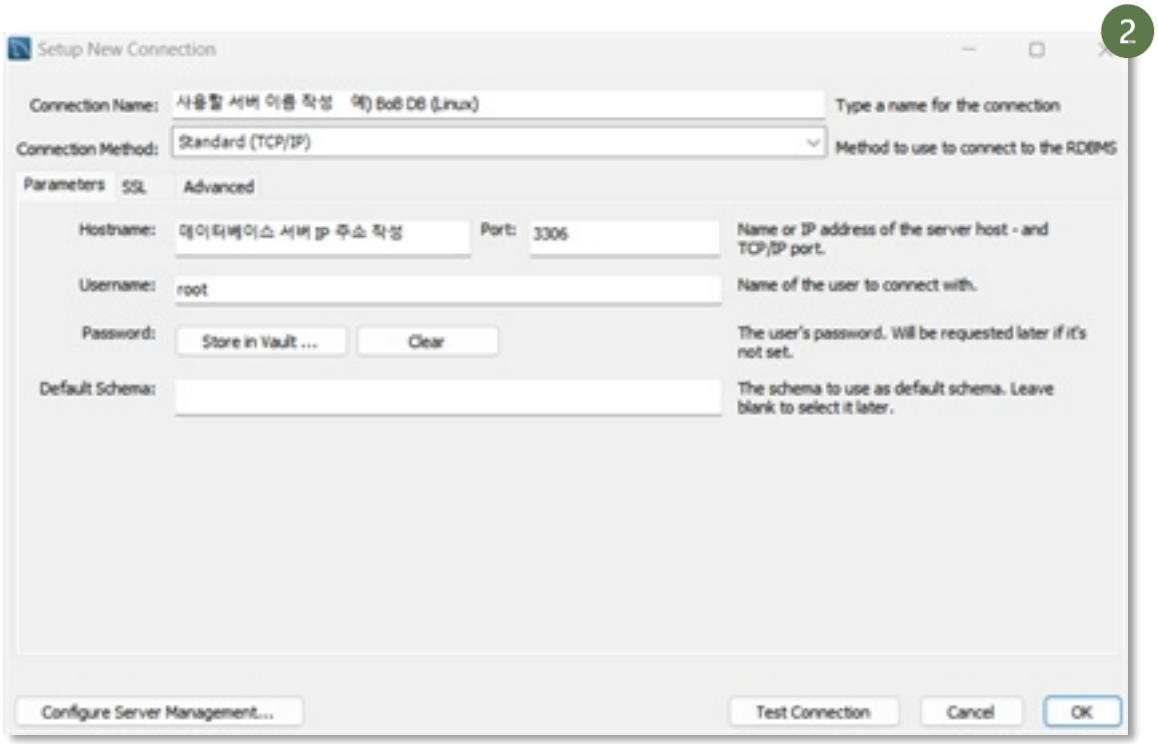
MY-SQL

MySQL Workbench 와 MySQL 데이터베이스 초기 접속 설정하기

1 [메인 화면의 '+' 버튼 클릭]



2 ['Setup New Connection' 화면에서 초기 접속 설정]
* 세부 설정 항목은 다음 장에서 설명



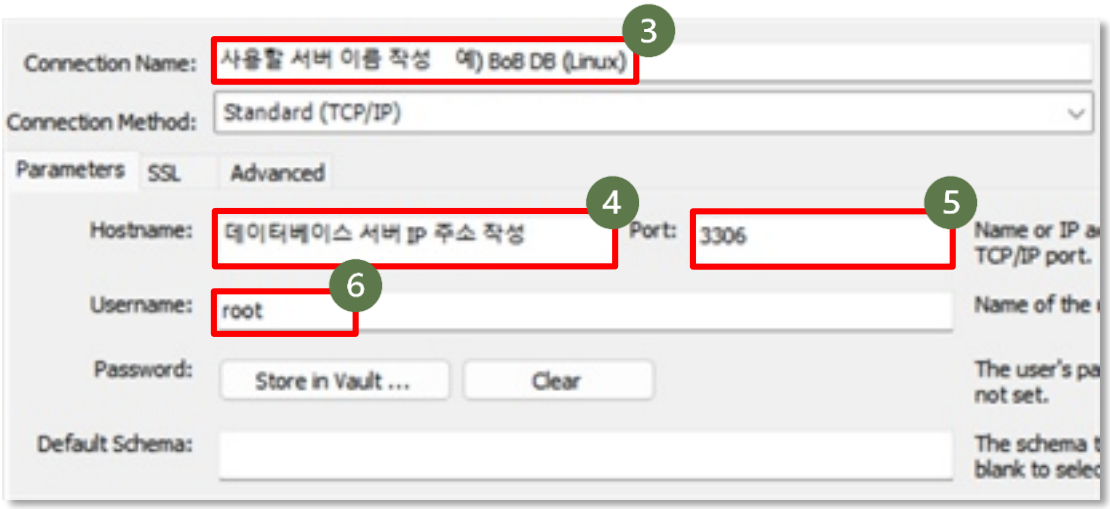
MY-SQL

3 ['Connection Name'에는 사용할 서버 이름 입력]

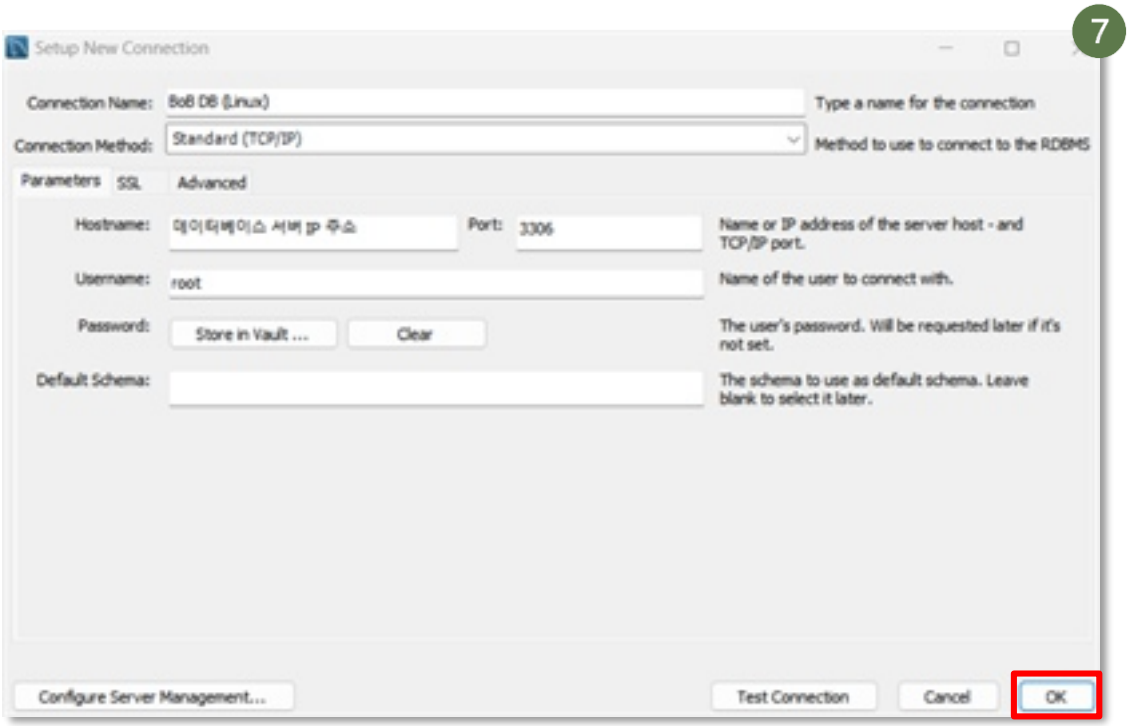
4 ['Hostname'에는 데이터베이스 서버 IP 주소 입력]

5 ['Port'에는 3306 입력]

6 ['Username'에는 root 입력]

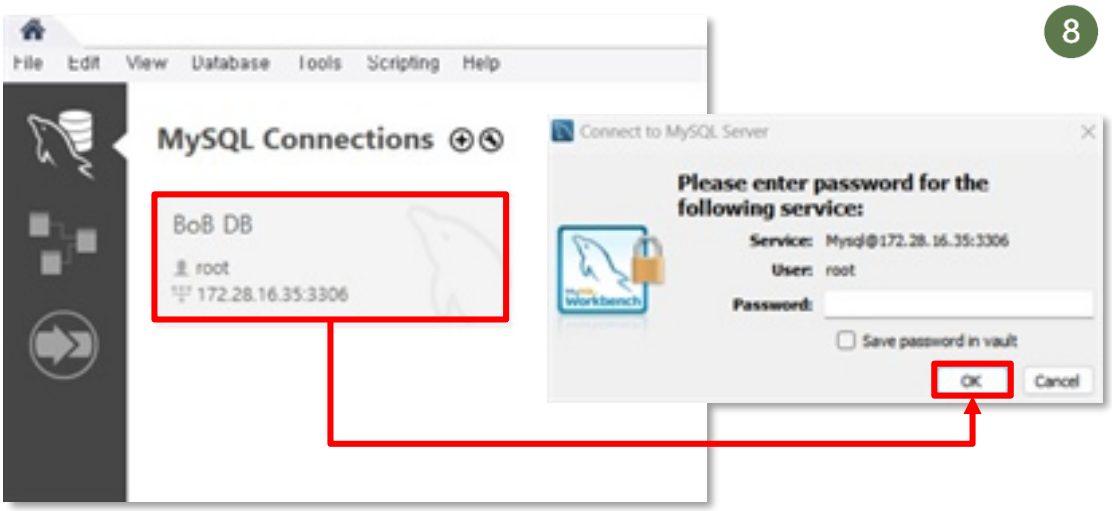


7 ['Username'에는 'root' 입력] > ['OK' 클릭]

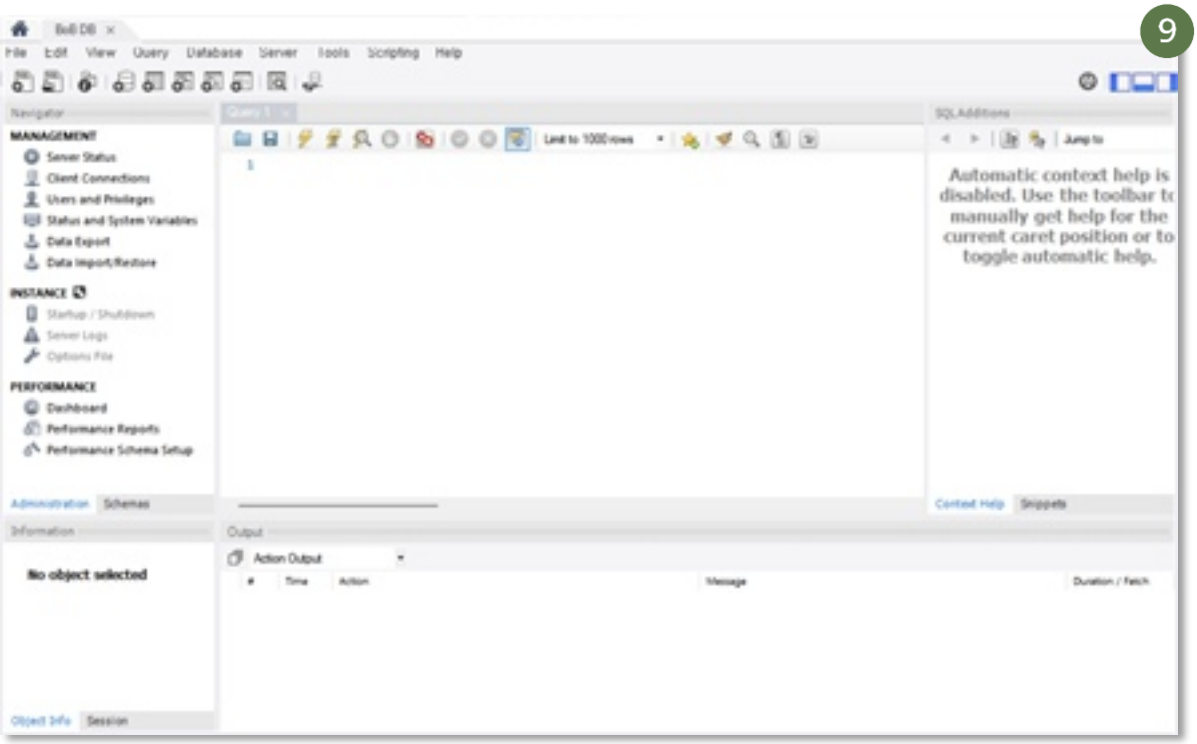


MY-SQL

8 [설정 완료 후 메인 화면에서 설정한 연결 클릭] > ['Connect' 화면에서 'OK' 클릭]



9 [MySQL Workbench 로 MySQL 데이터베이스 접속 시 초기화면]



MY-SQL

1. 포트 관리하기

MySQL 데이터베이스는 설치 시 기본적으로 3306번 포트를 사용합니다. 하지만 해당 포트는 널리 알려져 있어 외부 공격에 취약할 수 있습니다. 따라서, 보안을 강화하기 위해 별도의 포트 번호를 설정하여 사용해야 합니다.

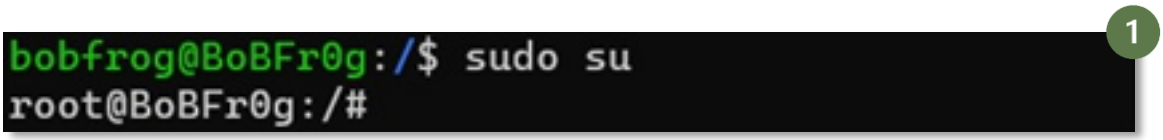
포트(Port)란?

포트는 컴퓨터가 네트워크를 통해 정보를 주고받을 때 사용하는 통로를 의미합니다.

MySQL 데이터베이스 접속하기

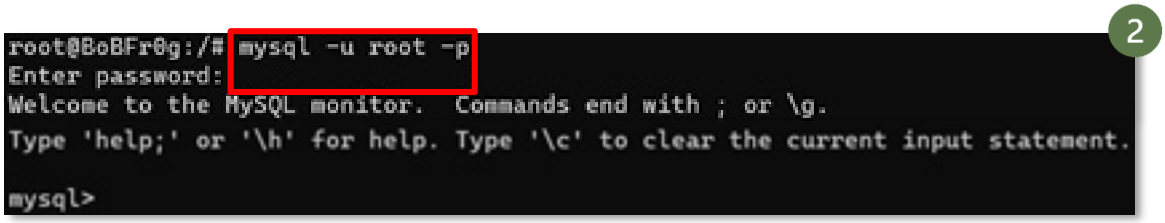
1. [MySQL 서버 'su' 명령어를 통한 root 계정 전환]

```
$ sudo su
```



2. [root 접속 후 mysql 접속 명령어 입력] > [비밀번호 입력 후 MySQL 데이터베이스 접속]

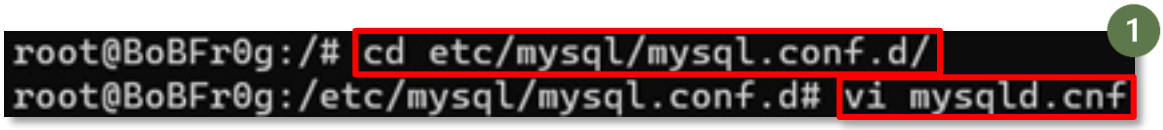
```
# mysql -u root -p
```



기본 포트번호 변경하기

1. [MySQL 설정 파일 디렉토리로 이동] > [하단의 'vi' 명령어를 사용하여 'mysqld.cnf' (혹은 'mysql.cnf') ' 파일 열기]

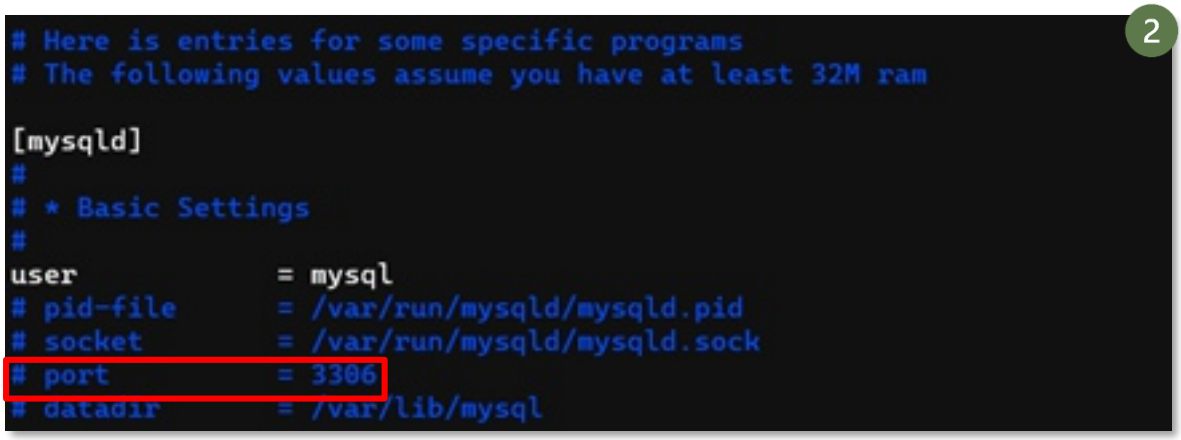
```
# cd /etc/mysql/mysql.conf.d/
# vi mysqld.cnf
```



MY-SQL

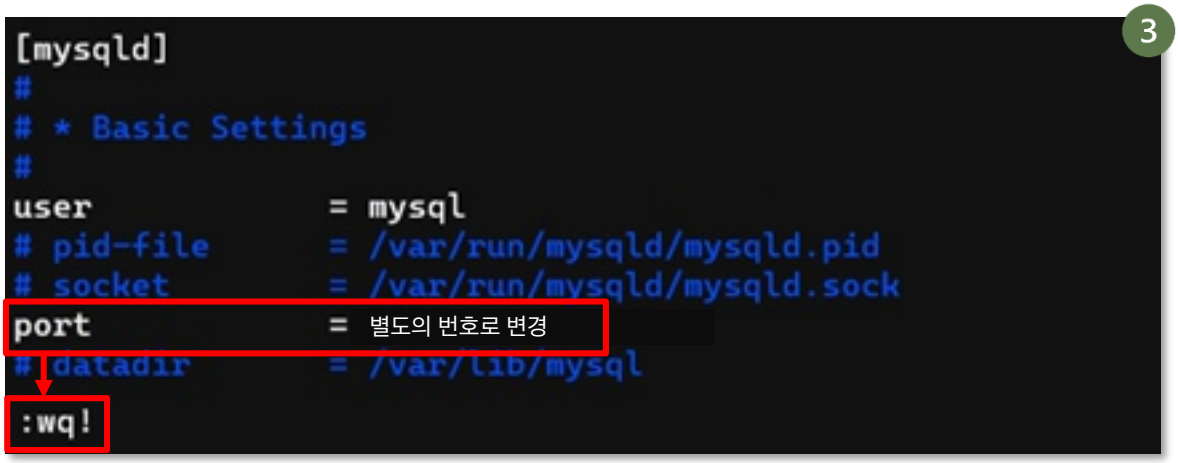
② ['/port'를 입력하여 port 옵션 검색]

```
/port
```



③ ['i'를 통해 입력모드 진입] > [주석('#') 제거 후 별도의 포트번호로 수정] > [이후 키보드 'ESC'] > [':wq' 입력] > ['Enter' 입력]

```
port = 임의의 포트 번호 입력
```



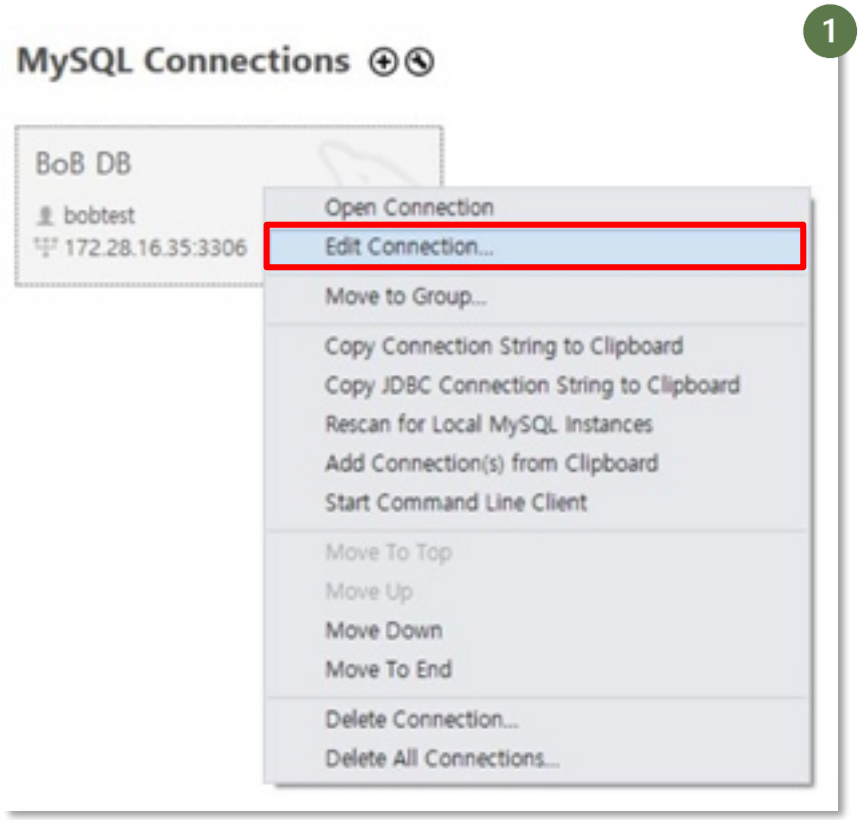
④ [터미널에 'service mysql restart' 명령어 입력] > [서비스 다시 시작]

```
# service mysql restart
```

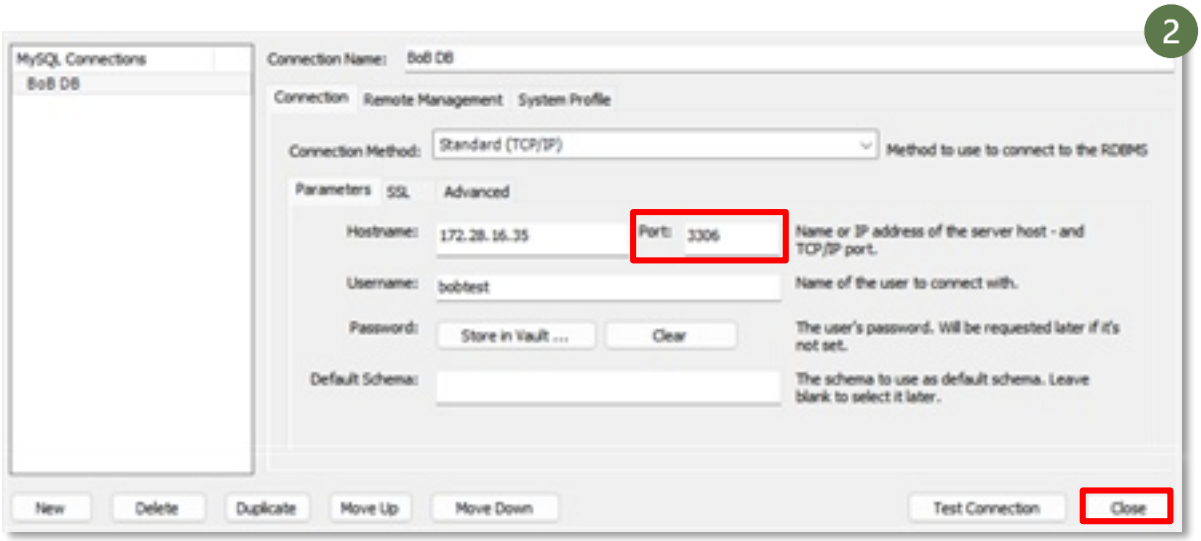
MY-SQL

데이터베이스 포트 번호 변경 후 MySQL Workbench 재설정하기

1 [메인 화면의 연결 설정 우클릭] > ['Edit Connection...' 선택]



2 [설정 화면의 'Port' 부분을 변경한 포트 번호로 변경] > ['Close' 클릭]



MY-SQL

2. 일반 계정 관리하기

직원이 회사를 떠난 뒤 또는 테스트 목적으로 계정을 생성한 뒤에 그 계정을 삭제하지 않아 데이터베이스에 불필요한 계정이 남아있을 수 있습니다. 공격자는 이러한 계정을 탈취하여 무단으로 데이터 조회, 변경, 삭제와 같은 작업을 수행할 수 있습니다. 따라서 주기적으로 계정 사용 여부를 검토한 뒤 불필요한 계정은 삭제할 것을 권장합니다.

삭제하면 안되는 MySQL 기본 계정 목록

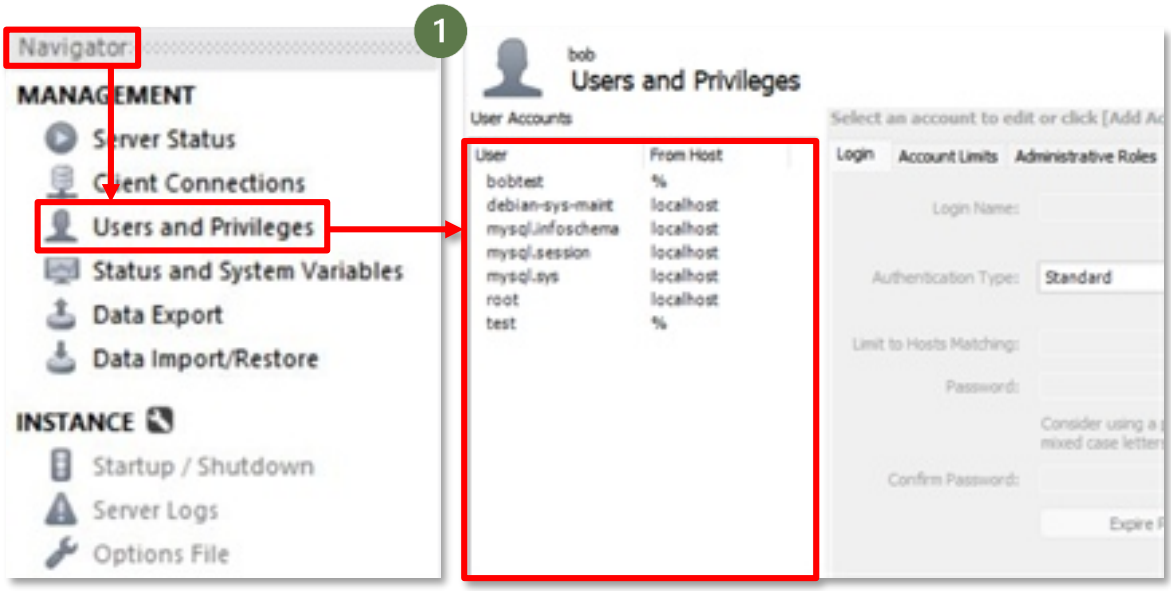
MySQL에는 관리를 목적으로 생성되는 기본 계정들이 있습니다. 계정 삭제 시 하단의 계정들은 삭제하지 않도록 주의해야 합니다.

계 정 명	상 세 설 명
mysql.infoschema	MySQL 서버에서 정보 스키마(INFORMATION_SCHEMA)를 관리하는 데 사용합니다.
mysql.session	MySQL 서버가 시스템 유지 관리 작업을 수행할 때 사용합니다.
mysql.sys	MySQL 서버의 내부 작업과 관련된 시스템 객체를 관리하는 데 사용합니다
debian-sys-maint	Debian 및 Ubuntu와 같은 Debian 기반 Linux 시스템에서 MySQL 데이터베이스 서버를 관리하기 위해 특별히 생성된 사용자 계정입니다.
root	MySQL 데이터베이스 시스템의 모든 측면을 관리할 수 있는 시스템의 관리자 계정입니다.

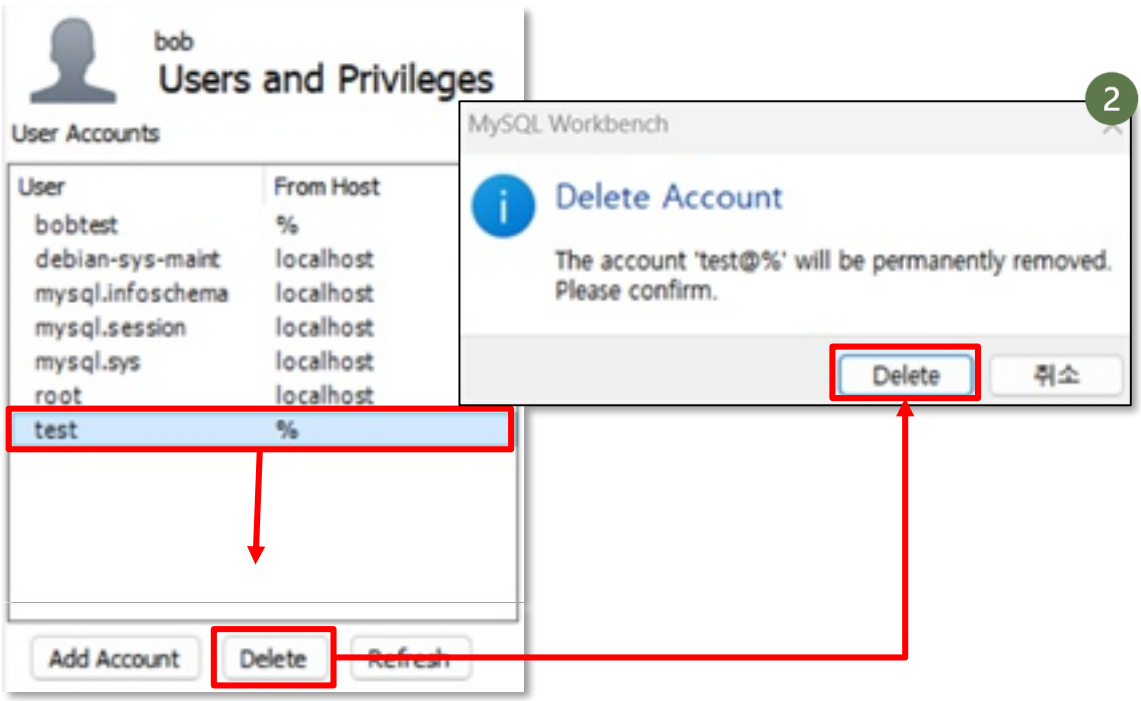
MY-SQL

사용하지 않는 계정 삭제하기 - UI 방식

1 [MySQL Workbench (관리자)] > ['Navigator'] > ['MANAGEMENT' 탭의 'Users and Privileges' 선택]



2 ['User Accounts' 부분에서 사용하지 않는 계정 확인 후 'Delete' 클릭]

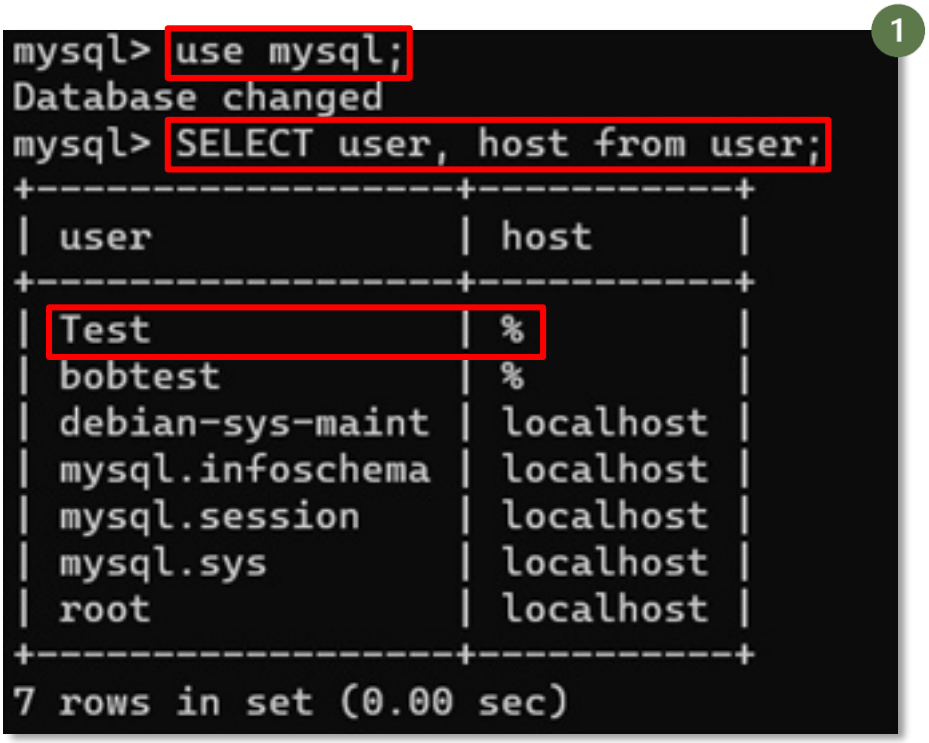


MY-SQL

사용하지 않는 계정 삭제하기 - 쿼리문 방식

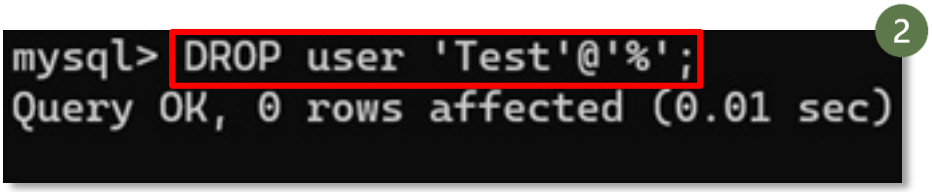
1. ['use' 쿼리문을 통해 'mysql' 데이터베이스로 전환] > ['SELECT' 쿼리문을 통해 계정 정보 확인]

```
> use mysql;
> SELECT user, host FROM user;
```



2. ['DROP' 쿼리문을 실행하여 불필요한 계정 삭제]

```
> DROP user '[삭제할 계정명]'@'[호스트명]';
```



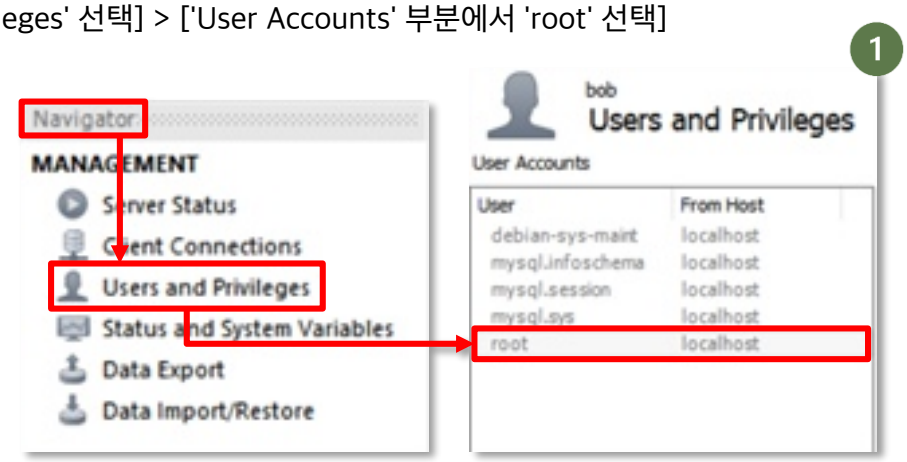
MY-SQL

3. root 계정 비밀번호 설정하기

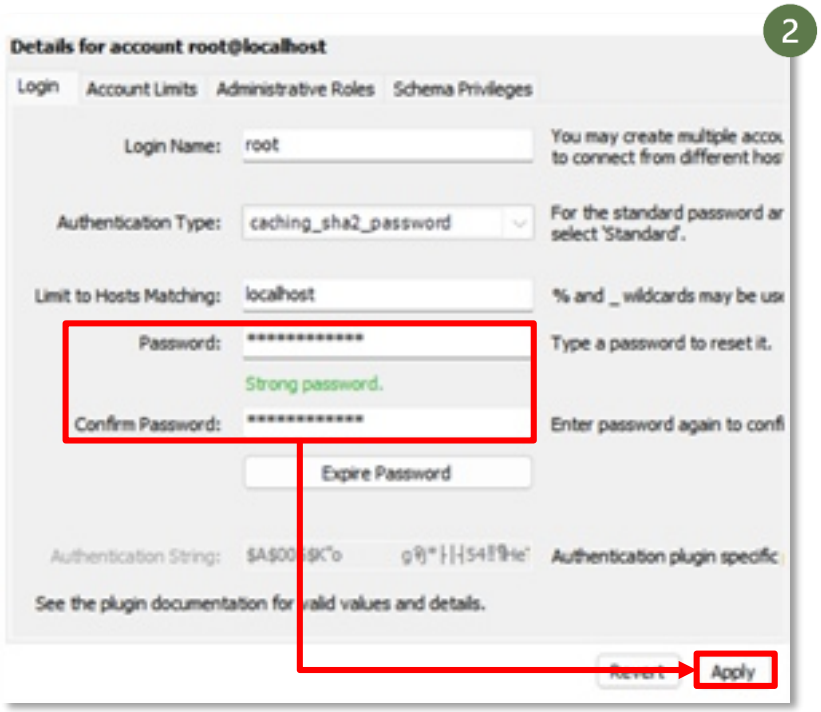
MySQL 데이터베이스 설치 시, 초기 root 계정의 비밀번호가 설정되어 있지 않습니다. root 계정은 데이터베이스에 대한 모든 권한을 가지고 있어 주된 공격 대상이 되므로 반드시 비밀번호를 설정해야 합니다.

root 계정 비밀번호 설정하기 - UI 방식

1. [MySQL Workbench (관리자)] > ['Navigator'] > ['MANAGEMENT' 탭의 'Users and Privileges' 선택] > ['User Accounts' 부분에서 'root' 선택]



2. ['Login' 클릭 후 'Password'에 root 비밀번호 설정] > [설정 후 'Apply' 클릭]

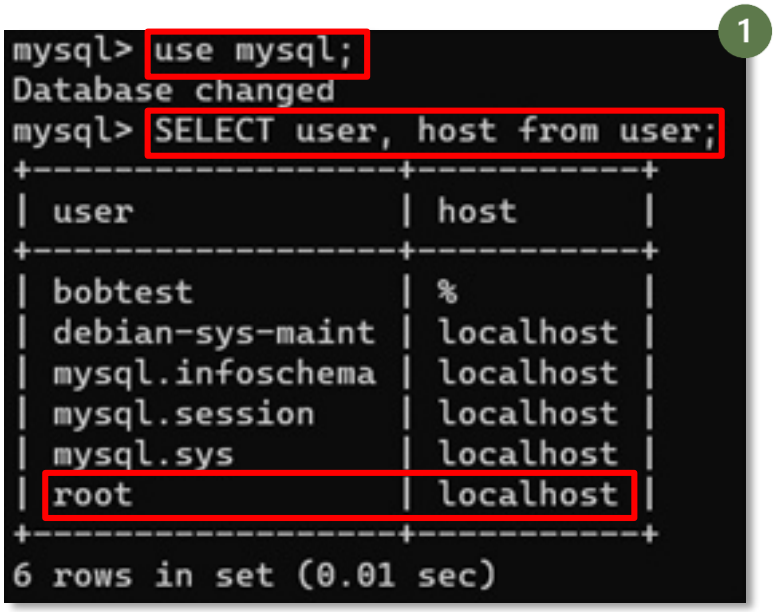


MY-SQL

root 계정 비밀번호 설정하기 - 쿼리문 방식

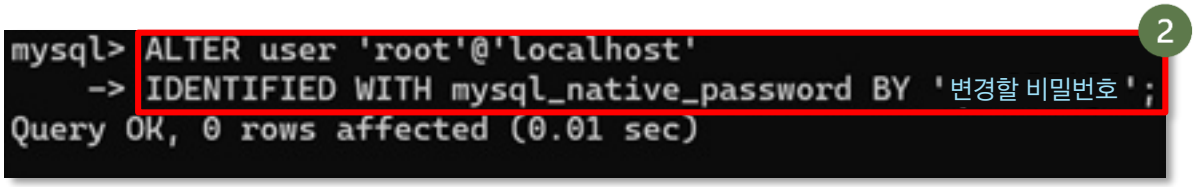
1. ['use' 쿼리문을 통해 'mysql' 데이터베이스로 전환] > ['SELECT' 쿼리문을 통해 계정 정보 확인]

```
> use mysql;
> SELECT user, host FROM user;
```



2. [root 계정 확인 후 'ALTER' 쿼리문을 통해 root 비밀번호 변경]

```
> ALTER user 'root'@'localhost'
IDENTIFIED WITH mysql_native_password BY '[변경 비밀번호]';
```



MY-SQL

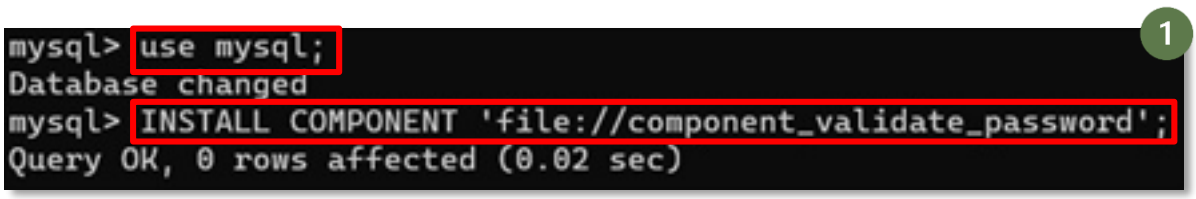
4. 비밀번호 관리하기

길이가 짧거나, 구성이 간단한 비밀번호를 사용할 수 있으면 공격자는 비밀번호를 쉽게 알아낼 수 있습니다. 이를 막기 위해 비밀번호 설정 시 복잡성을 검증하도록 정책을 설정할 수 있습니다.

비밀번호 복잡도 설정하기

1. ['use' 쿼리문을 통해 'mysql' 데이터베이스로 전환] > [하단의 쿼리문을 통해 비밀번호 검증 구성 요소 설치]
   * MySQL 8.0 부터는 기본적으로 비밀번호 검증 구성 요소를 사용할 수 있습니다.

```
> use mysql;
> INSTALL COMPONENT 'file://component_validate_password';
```



MySQL의 비밀번호 복잡도 설정 중 권장하는 설정 사항은 다음 5가지 입니다.

비밀번호 복잡도 설정 항목 별 권장 값

validate_password 옵션명	권장 값	상 세 설 명
length	**8 이상**	비밀번호 설정 시 필요한 최소 길이를 설정하는 항목입니다.
mixed_case_count	**1 이상**	비밀번호 설정 시 필요한 최소 대문자/소문자의 개수를 설정하는 항목입니다.
number_count	**1 이상**	비밀번호 설정 시 필요한 최소 숫자의 개수를 설정하는 항목입니다.
Policy	**MEDIUM**	비밀번호 설정 시 설정된 비밀번호를 점검하는 강도를 설정하는 항목입니다. **LOW: 비밀번호의 최소 길이만 점검합니다.** **MEDIUM: 비밀번호의 최소 길이, 숫자, 대문자/소문자 및 특수문자 포함 여부를 점검합니다.** **STRONG: 비밀번호의 최소 길이는 4, dictionary 항목에 포함된 문자열의 포함 여부를 점검합니다.**
special_char_count	**1 이상**	비밀번호 설정 시 필요한 특수문자의 개수를 설정하는 항목입니다.

MY-SQL

② [설치 후 'SHOW GLOBAL' 쿼리문을 통해 비밀번호 복잡도 확인]

```
> SHOW GLOBAL VARIABLES LIKE 'validate_password%';
```

```
mysql> SHOW GLOBAL VARIABLES LIKE 'validate_password%';
+--------------------------------------------------+--------+
| Variable_name                                    | Value  |
+--------------------------------------------------+--------+
| validate_password.changed_characters_percentage  | 0      |
| validate_password.check_user_name                | ON     |
| validate_password.dictionary_file                |        |
| validate_password.length                         | 8      |
| validate_password.mixed_case_count               | 1      |
| validate_password.number_count                   | 1      |
| validate_password.policy                         | MEDIUM |
| validate_password.special_char_count             | 1      |
+--------------------------------------------------+--------+
8 rows in set (0.00 sec)
```

③ [필요 부분에 따라 'SET GLOBAL' 쿼리문을 통해 설정 값 수정]

```
> SET GLOBAL [변경할 복잡도 항목]=[수정값];
ex) > SET GLOBAL validate_password.special_char_count=3;
```

```
mysql> SET GLOBAL validate_password.special_char_count=3;
Query OK, 0 rows affected (0.00 sec)

mysql> SHOW GLOBAL VARIABLES LIKE 'validate_password%';
+--------------------------------------------------+--------+
| Variable_name                                    | Value  |
+--------------------------------------------------+--------+
| validate_password.changed_characters_percentage  | 0      |
| validate_password.check_user_name                | ON     |
| validate_password.dictionary_file                |        |
| validate_password.length                         | 8      |
| validate_password.mixed_case_count               | 0      |
| validate_password.number_count                   | 1      |
| validate_password.policy                         | MEDIUM |
| validate_password.special_char_count             | 3      |
+--------------------------------------------------+--------+
8 rows in set (0.06 sec)
```

MY-SQL

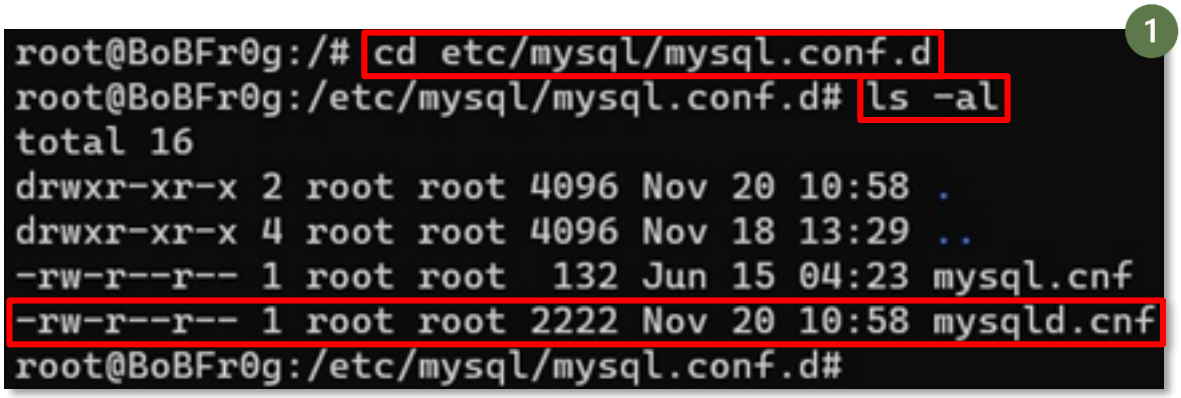
5. 서버 환경 설정파일 관리하기

데이터베이스 서버의 핵심 환경 설정 파일에 모든 사용자가 접근 가능한 경우, 누군가에 의해 서버 설정이 회사 데이터베이스 운영 정책과 다르게 변경될 수 있습니다. 이는 서버 장애를 일으키는 등 정상적인 서버 운영에 지장을 줄 수 있습니다. 따라서 관리자만 설정파일에 접근할 수 있도록 권한을 설정할 것을 권장합니다.

서버 환경 설정 파일 권한 확인하기

1 [MySQL 설정 파일 디렉토리로 이동] > ['ls -al' 명령어를 통해 환경 설정파일 권한 확인]

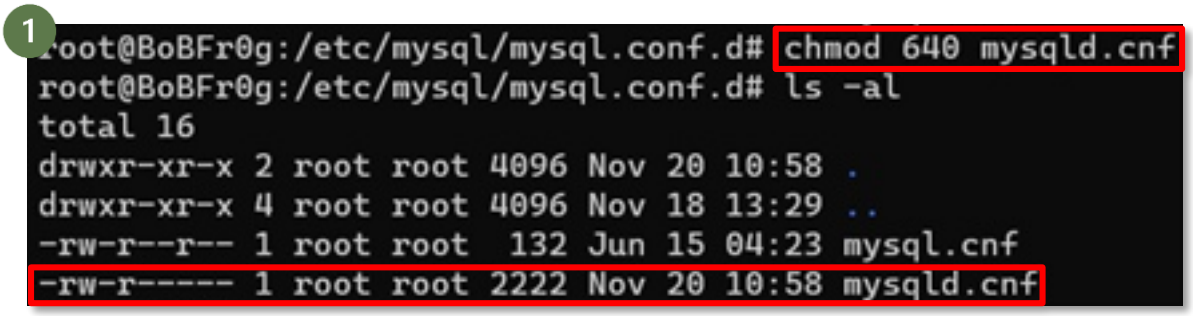
```
# cd etc/mysql/mysql.conf.d
# ls -al
```



서버 환경 설정 파일 권한 변경하기

1 ['chmod' 명령어를 통해 환경 설정파일 권한 확인]

```
# chmod 640 mysqld.cnf
```



MY-SQL

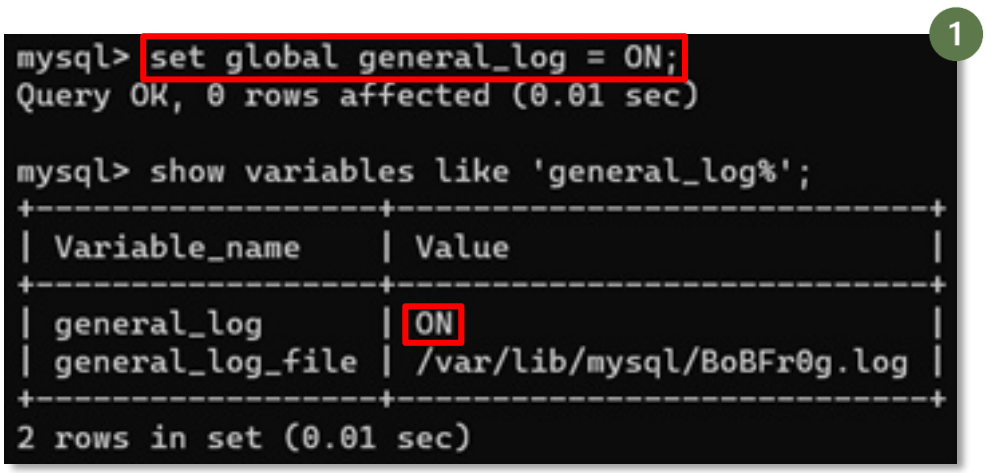
6. 데이터베이스 로그 활성화

데이터베이스 로그에는 데이터 이동, 사용자 활동, 시스템 오류 등 중요한 운영 데이터가 기록됩니다. 이는 추후 데이터베이스에서 발생한 침해사고 및 비정상적인 활동을 추적하는데 중요한 역할을 합니다.

로그 기록 활성화 및 조건 설정하기

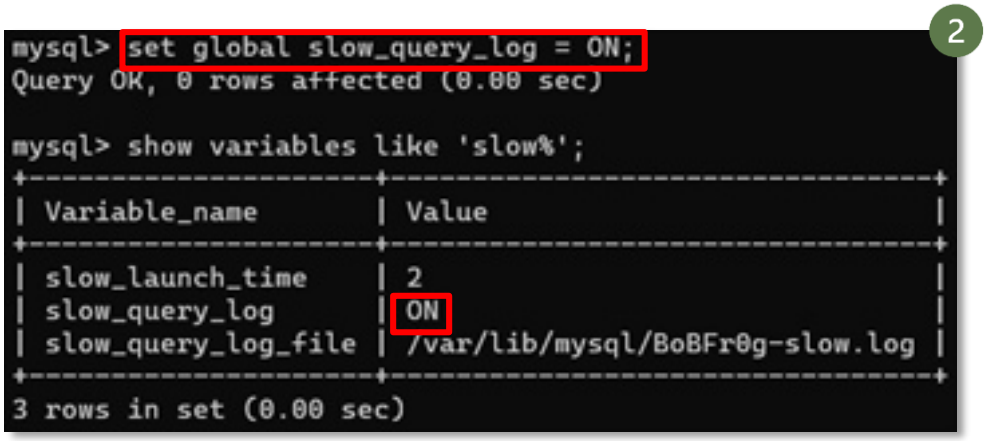
1. ['use' 쿼리문을 통해 'mysql' 데이터베이스로 전환] > ['SET GLOBAL' 쿼리문을 통해 'general_log' 활성화]

```
> use mysql;
> SET GLOBAL general_log=ON;
```



2. ['SET GLOBAL' 쿼리문을 통해 'slow_query_log' 활성화]

```
> SET GLOBAL slow_query_log=ON;
```

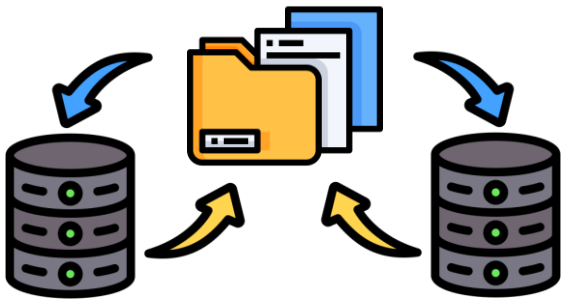


이것만은 지키자!

행동수칙

나스 편

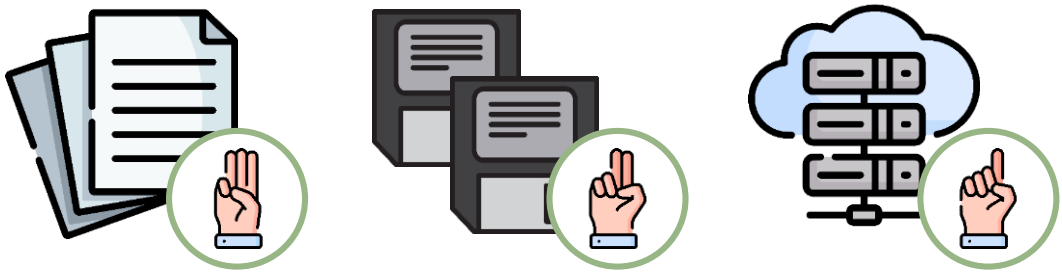
1



중요한 데이터는 분리된 저장 공간에도 저장하도록 해요!

중요한 데이터는 절대로 한 곳에서만 보관하는 일이 없도록 해야 합니다. 유일한 저장 공간이 공격을 받거나 자연 재해로 고장이 나면 저장된 데이터가 손상될 수 있습니다. 데이터 또한 기업의 소중한 자산이므로 데이터의 안전은 회사의 자산을 지키는 것과 같습니다. 이처럼 사고에 대비하여 데이터를 다른 공간에 추가적으로 보관하는 행위를 백업이라고 합니다.

2



“백업의 3-2-1 법칙”을 지켜 백업해요!

“백업의 3-2-1 법칙”이란 안전한 백업을 위한 행동 수칙으로, 백업 데이터의 3개의 버전 또는 사본을, 2개의 다른 디스크에 보관 하되, 최소 1개의 데이터는 물리적으로 다른 장소에 보관하는 방법입니다. 데이터를 기존 저장 공간과 동일한 저장소에 백업을 하면, 경우에 따라 복구가 불가능할 수 있기 때문입니다.

회사에서 데이터를 보관하는 방법으로 저장소를 활용하는 경우가 많습니다. 저장소를 구축하는 방법은 SAN 방식, NAS 방식, 클라우드 방식 등이 존재합니다. 중소기업과 같은 소규모 조직에서는 주로 NAS를 활용한 저장소 구축이 많은 편입니다. 본 장에서는 NAS의 개념과, 널리 사용되는 NAS 제품인 시놀로지와 큐냅의 보안설정 방법에 대하여 안내합니다.

NAS란 무엇인가요?

NAS는 Network Attached Storage의 약자로 다수의 저장장치(HDD 또는 SSD)를 연결하여 파일 서버 형태로 사용할 수 있게끔 만들어진 작은 컴퓨터 장비입니다. 대규모의 스토리지 네트워크를 구축하는 것은 비용이 많이 들기 때문에, 소규모 조직의 경우 NAS를 통해 저장소를 구축하는 경우가 많습니다. NAS는 저렴한 비용으로 직접 회사에서 관리할 수 있는 저장소를 확보할 수 있어 인기가 높습니다.

NAS 보안은 왜 해야할까요?

회사가 보유한 정보는 회사의 소중한 자산입니다. 회사가 갖는 지적재산, 영업비밀, 고객정보와 같은 데이터는 기업 경영에 있어서 핵심적인 가치를 가지므로, 데이터의 손실과 유출은 회사에 큰 재정적 손해를 불러올 수 있습니다. 따라서 데이터를 안전하게 관리하는 것이 매우 중요합니다. 본 장에서는 NAS가 제공하는 기능을 활용하여 저장된 데이터를 안전하게 관리하는 방법을 안내합니다.

가이드라인에서 다루는 제품 확인하기

Synology®

▲ Synology

QNAP®

▲ QNAP

시놀로지(Synology)

1. 외부 부정 접속 차단하기

NAS는 인터넷과 연결할 수 있어, NAS의 IP주소 혹은 URL을 알고 있다면 외부에서도 NAS 저장소에 접근할 수 있습니다. 그렇기 때문에 회사용 NAS의 경우 인터넷을 통한 직접 접속은 차단하고 내부에서만 운영할 것을 권고하고 있습니다. 불가피하게 인터넷과 연결해야 하는 경우에는 철저한 관리가 필요합니다.

방화벽 활성화하기

① ['제어판' 실행] > ['보안' 클릭] > ['방화벽' 클릭] > ['일반'의 '방화벽 활성화' 선택] > [우측 하단 '적용' 클릭]

시놀로지에서 인터넷 연결 차단하기

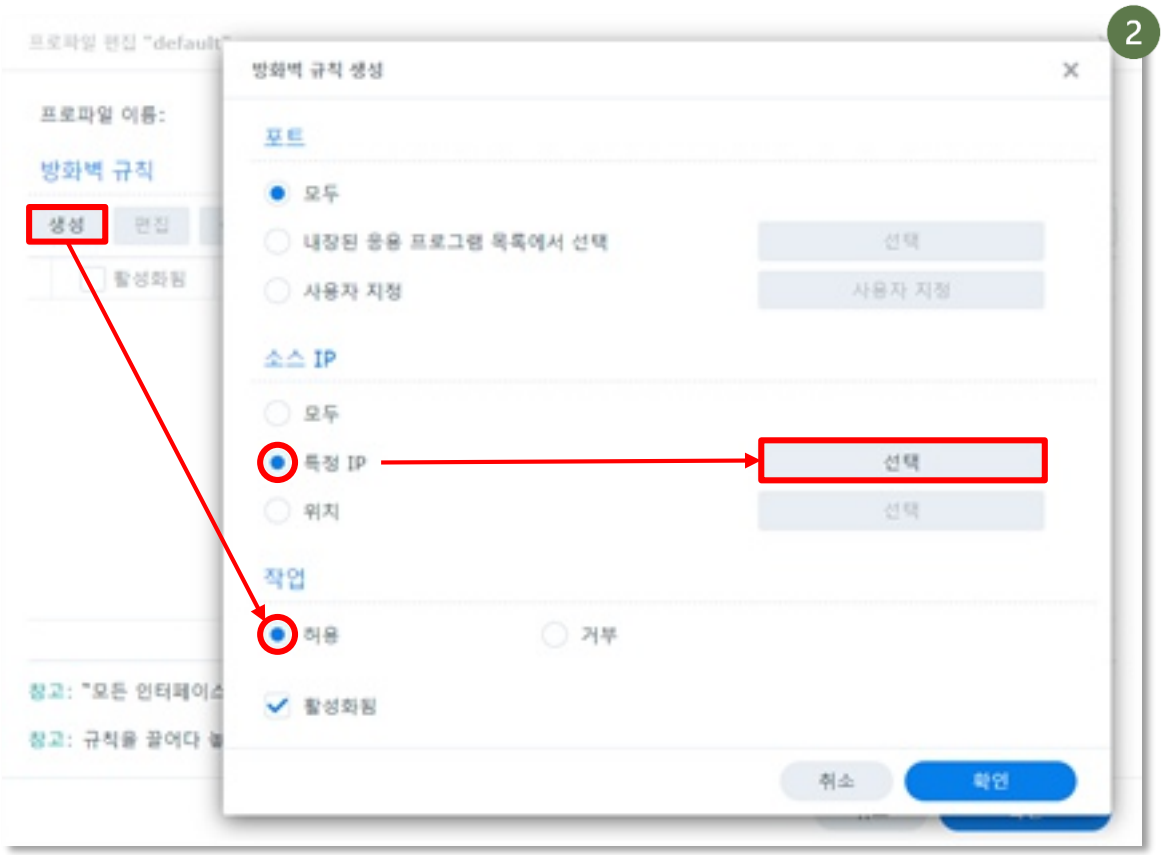
시놀로지 NAS의 경우 'QUICK CONNECT', 'DDNS', '라우터 구성' 기능을 통해 NAS를 외부 인터넷과 연결할 수 있도록 하고 있습니다. 조직 내 저장소 관리 정책이 인터넷 연결을 차단하기로 하였다면, NAS DSM의 [제어판] > [연결성] > [외부 엑세스]에서 설정을 바꿀 수 있습니다.

시놀로지(Synology)

방화벽으로 등록된 IP만 접근 허용하기

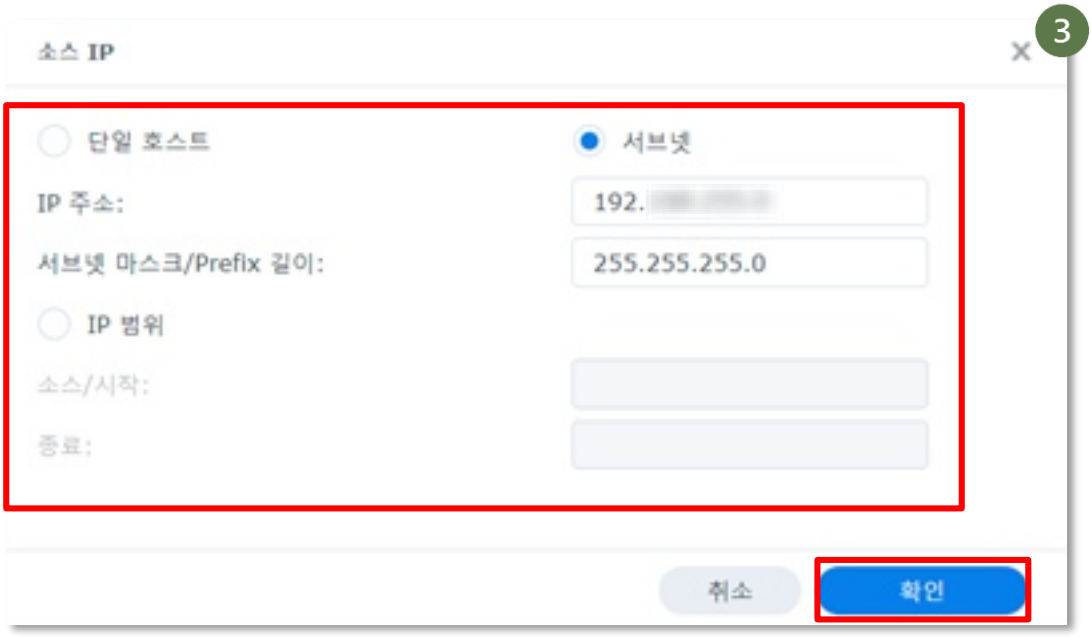
1 ['방화벽 프로파일'의 '규칙 편집' 클릭]

2 [방화벽 규칙의 '생성' 클릭] > ['작업'의 '허용' 선택] > ['소스 IP'의 '특정 IP' 선택 후 '선택' 클릭]

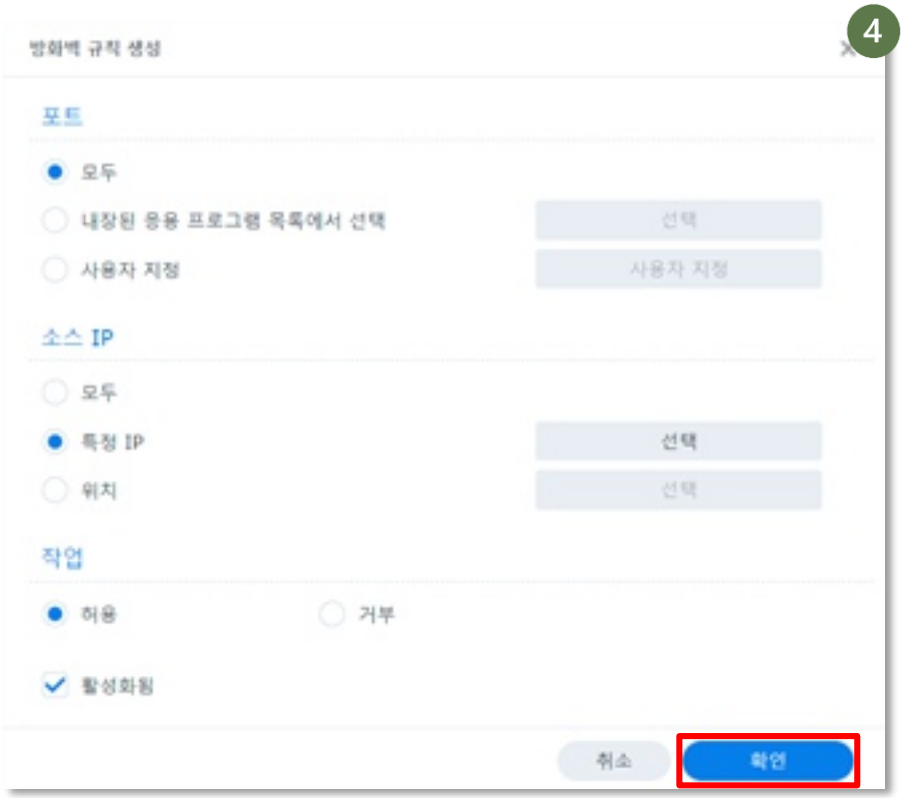


시놀로지(Synology)

3 ['개별IP', 'IP대역', '네트워크(서브넷)' 중 선택하여 입력] > [하단의 '확인' 클릭]

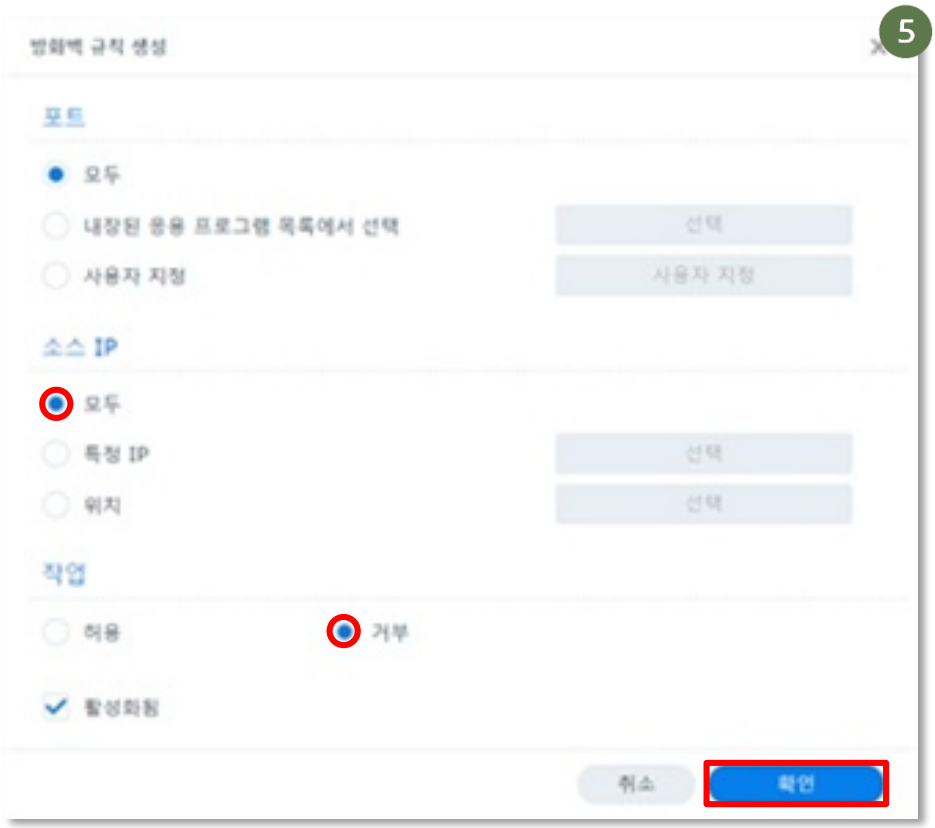


4 [방화벽 규칙 생성 '확인' 클릭으로 완료]



시놀로지(Synology)

5 [방화벽 규칙 생성] > ['소스 IP'를 '모두'로 설정한 후 '작업'을 '거부'로 선택] > [우측 하단의 '확인'을 클릭] * 규칙은 위에 있는 규칙이 먼저 적용되므로 순서에 주의

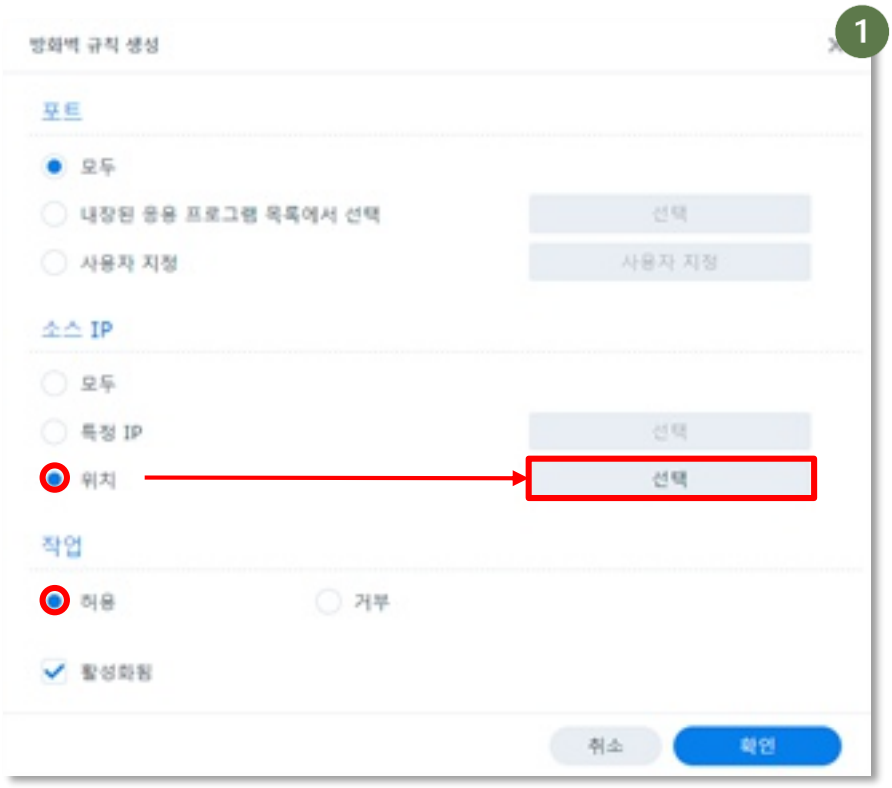


6 [우측 하단의 '확인'을 클릭]

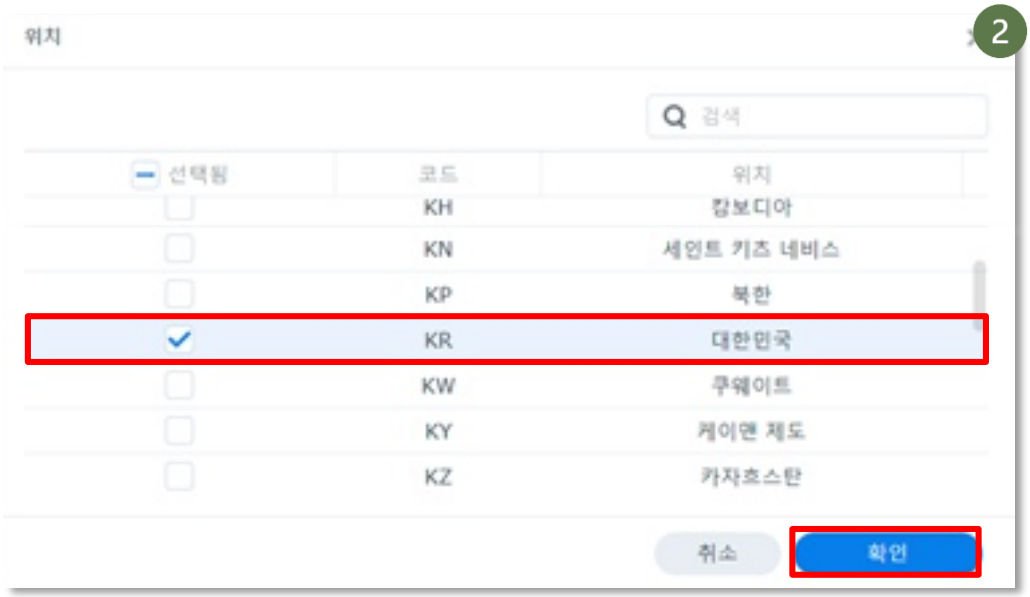
시놀로지(Synology)

방화벽으로 등록된 국가만 접근 허용하기

1 [방화벽 규칙] > ['작업'의 '허용' 선택] > ['소스 IP'의 '위치' 선택 후 '선택' 클릭]

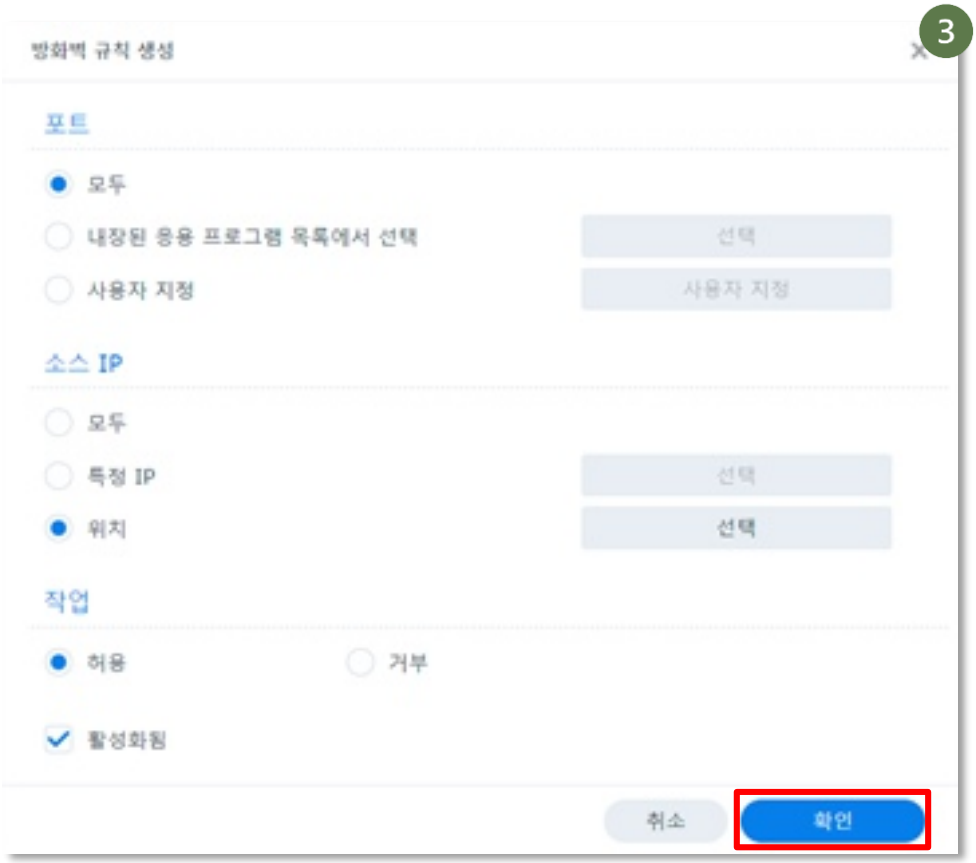


2 ['대한민국' 체크한 후 '확인' 클릭] > [우측 하단 '확인' 클릭]



시놀로지(Synology)

3 [이전 페이지에서 '확인' 클릭]

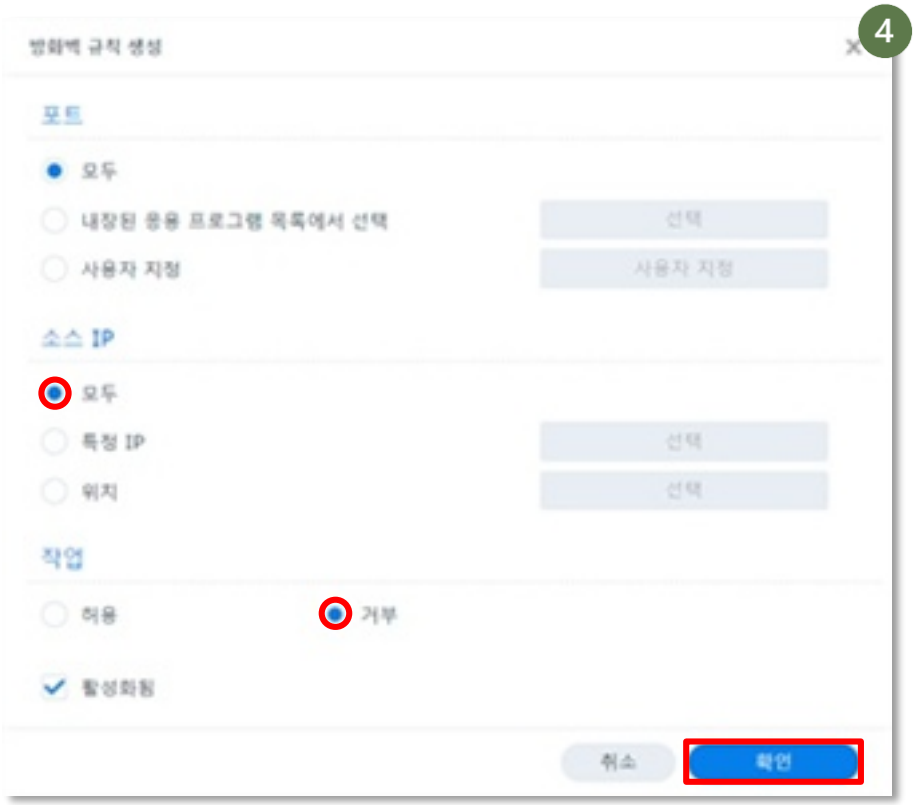


방화벽 규칙 설정

방화벽은 회사 내 정책에 따라 다양한 규칙을 가질 수 있습니다. 앞서 살펴본 2가지 규칙은 가장 대표적인 규칙입니다. 추가로 특정 서비스에만 접근할 수 있게 하거나(포트별 설정), 수상한 IP가 계속 접속을 시도하는 경우 그 IP만을 차단할 수도 있습니다.

시놀로지(Synology)

4 [방화벽 규칙 생성] > ['소스 IP'를 '모두'로 설정한 후 '작업'을 '거부'로 설정] > [우측 하단의 '확인'을 클릭] * 규칙은 위에 있는 규칙이 먼저 적용되므로 순서에 주의



5 [우측 하단의 '확인'을 클릭]

시놀로지(Synology)

2단계 인증 강제 적용하기

2단계 인증은 사용자가 로그인을 시도하는 경우 휴대전화를 통해 본인이 로그인을 하고 있음을 인증하는 기술입니다. 2단계 인증을 적용하면 비밀번호만으로는 바로 NAS에 접속할 수 없기 때문에 타인의 계정을 도용한 부정 접속을 방지할 수 있습니다. 따라서 모든 구성원이 2단계 인증을 수행하도록 정책을 변경할 것을 권장합니다.

※ 정책 설정 후 각 사용자는 개별적으로 2단계 인증 설정을 해야 합니다.

1. ['제어판' 실행] > ['보안' 클릭] > ['계정' 클릭] > ['2단계 인증'에서 '다음 사용자에게 2단계 인증 적용' 체크] > ['모든 사용자' 체크 후 '적용' 클릭]

2단계 인증 설정

2단계 인증 강제 설정 시, NAS에 접근하는 모든 계정은 2단계 인증을 등록하기 전까지 로그인할 수 없습니다. 모든 구성원은 아래 3가지 중 하나의 방법으로 2단계 인증을 등록해야 합니다.

① 로그인 승인: Secure Signin 애플리케이션 이용
② 검증 코드(OTP): Secure Signin 애플리케이션 이용
③ 하드웨어 보안키: USB 키, 패스키 등 이용

시놀로지(Synology)

서비스 거부(DoS) 보호 설정하기

DoS 공격이란 특정 서버, 컴퓨터와 같은 IT 장비를 사용하지 못하게 할 목적으로 과도한 양의 데이터 또는 요청을 보내 혼잡한 상태를 유도하는 공격 방법입니다. 저장소의 경우 필요할 때 바로 사용할 수 있어야 하는 장비이므로 DoS 공격을 방지할 수 있도록 설정할 것을 권장합니다.

1 ['제어판' 실행] > ['보안' 클릭] > ['보호' 클릭] > [하단의 'DoS 보호 활성화' 체크] > ['적용' 클릭]

시놀로지(Synology)

2. 자동 업데이트 활성화하기

보안 업데이트 자동 설치하기

인터넷을 통한 접속을 허용한 경우, 외부 공격자는 NAS가 자체적으로 가지고 있는 결함을 악용하여 공격을 시도할 수 있습니다. NAS의 판매사는 이러한 위험을 막기 위해 결함을 발견하면 프로그램을 수정하여 배포합니다. 따라서 항상 최신 버전의 소프트웨어를 설치하는 것이 중요합니다. 이를 위해 '자동 업데이트'를 활성화 해야 합니다.

1 ['제어판'의 '업데이트 및 복원' 클릭] > ['DSM 업데이트'에서 '상태' 확인]

2 ['업데이트 설정'] > ['중요 보안 문제와 버그를 수정한 중요 업데이트 자동 설치(권장)' 선택] > ['확인' 클릭]

시놀로지(Synology)

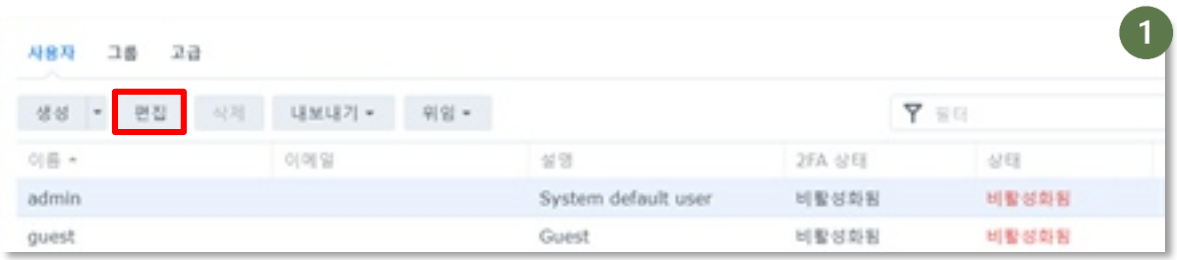
3. 계정 보안 설정하기

시놀로지 NAS에는 'admin'이라는 관리자 계정이 기본적으로 생성되어 있습니다. 기본 'admin' 계정은 비밀번호가 존재하지 않아 비밀번호 없이도 로그인이 가능합니다. 따라서 기본 admin 계정이 활성화되어 있는 경우 공격자는 바로 admin 계정에 로그인할 수 있으며, 설령 admin의 비밀번호를 변경하였더라도 여러번 로그인 시도를 하여 로그인에 성공할 수 있습니다.

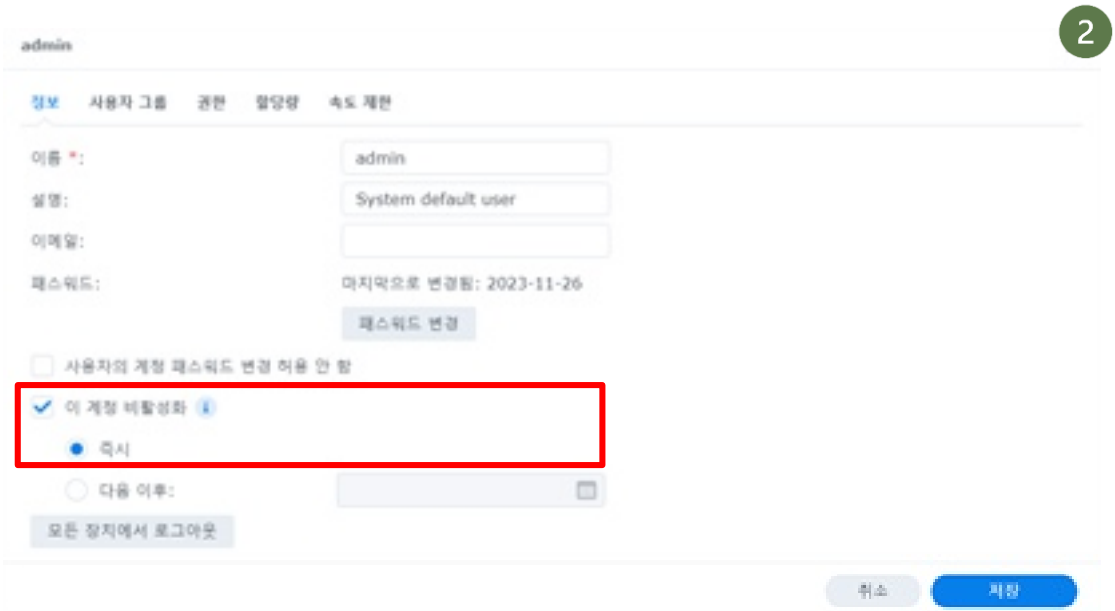
기본 관리 계정 비활성화하기

기본 admin 계정은 완전히 비활성화하고, 관리자 계정임을 추측하기 어렵도록 ID를 설정하여 관리자 계정으로 사용하기를 권장합니다.

1 [사용자 및 그룹] > ['admin' 계정 클릭 후 '편집' 클릭]



2 ['이 계정 비활성화' 선택] > ['즉시' 선택] > [하단의 '저장' 클릭]



시놀로지(Synology)

비밀번호 정책 설정하기

관리자는 NAS 계정에 대한 비밀번호 규칙을 지정할 수 있습니다.

1. ['제어판'의 '사용자 및 그룹'] > [우측 상단의 '고급' 클릭] > ['패스워드 설정'의 '패스워드 강도 규칙 적용' 선택] > [다음 페이지의 '권장하는 규칙'에 맞게 설정 변경]

2. ['제어판'의 '사용자 및 그룹'] > [우측 상단의 '고급' 클릭] > ['패스워드 만료'의 '패스워드 만료 활성화' 선택] > [다음 페이지의 '권장하는 규칙'에 맞게 설정 변경]

시놀로지(Synology)

권장하는 규칙	
항목	권장 값
패스워드에서 사용자 이름 및 설명 제외	활성화
대소문자 혼합 포함	활성화
숫자 문자 포함	활성화
특수 문자 포함	활성화
최소 패스워드 길이	8자 이상
패스워드 만료 활성화	활성화
최대 패스워드 유효 기간	90일 미만
최소 패스워드 유효 기간	1일

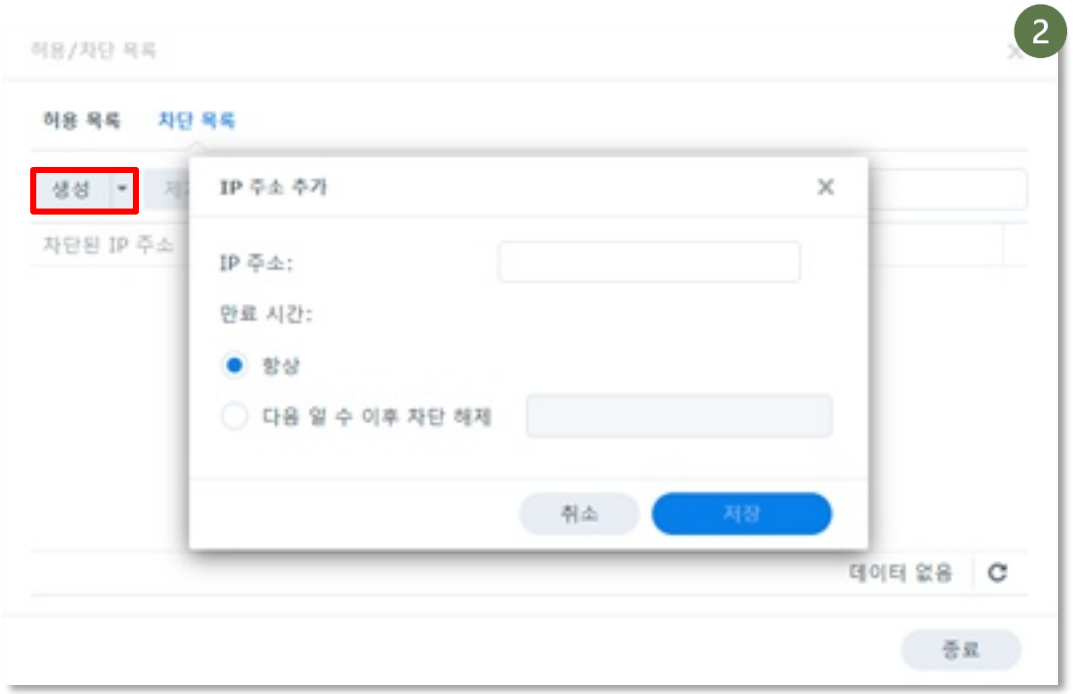
시놀로지(Synology)

로그인 실패횟수 초과시 IP 차단하기

로그인에 여러 번 실패한 경우 계정 보호를 위해 해당 IP를 차단할 수 있습니다.

1. ['제어판'의 '보안'] > ['보호' 클릭] > ['자동 차단'에서 '자동 차단 활성화' 선택] > ['로그인 시도 횟수'를 10회 이하로 설정하기를 권장]

2. [하단의 '허용/차단 목록'의 '생성'을 통해 직접 차단할 아이피 추가]



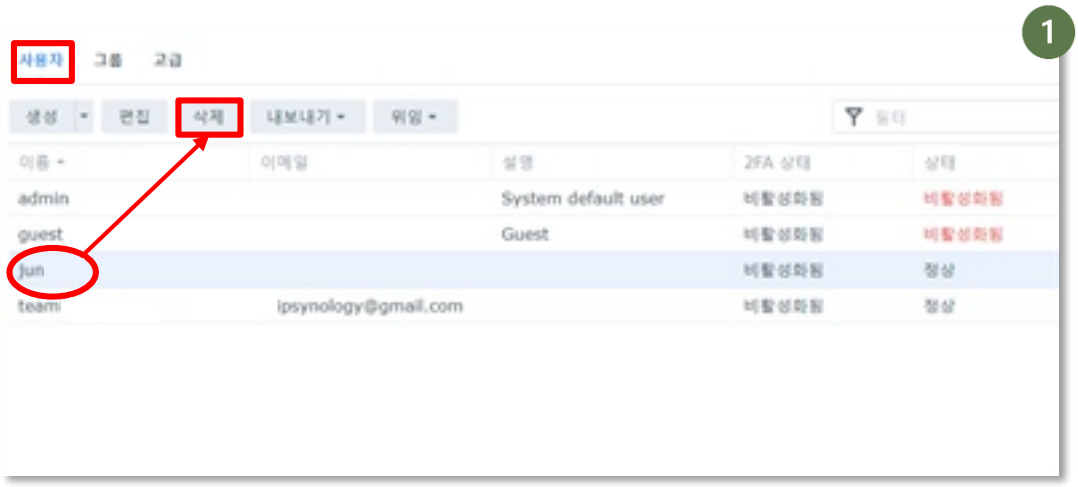
시놀로지(Synology)

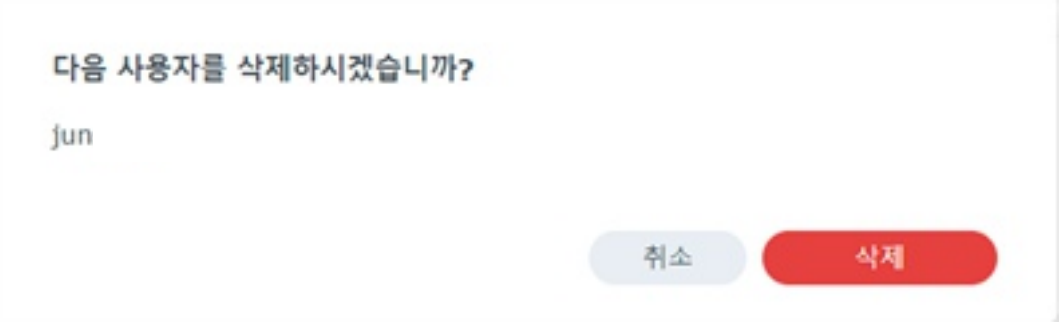
4. 계정 권한 관리하기

일반 계정 및 게스트용 계정에 불필요하게 많은 권한이 주어져 있다면 공격자가 이러한 계정을 해킹한 뒤 공격하거나, 권한 없는 내부자가 영업비밀을 유출하는 등 많은 문제가 발생할 수 있습니다. 따라서 관리자는 임직원들의 권한이 필요 이상으로 주어져 있지 않은지 반드시 확인해야 합니다.

퇴사자 계정 삭제하기

1. [제어판의 '사용자 및 그룹'] > ['사용자' 클릭] > [삭제 대상 계정 클릭 후 '삭제' 클릭]



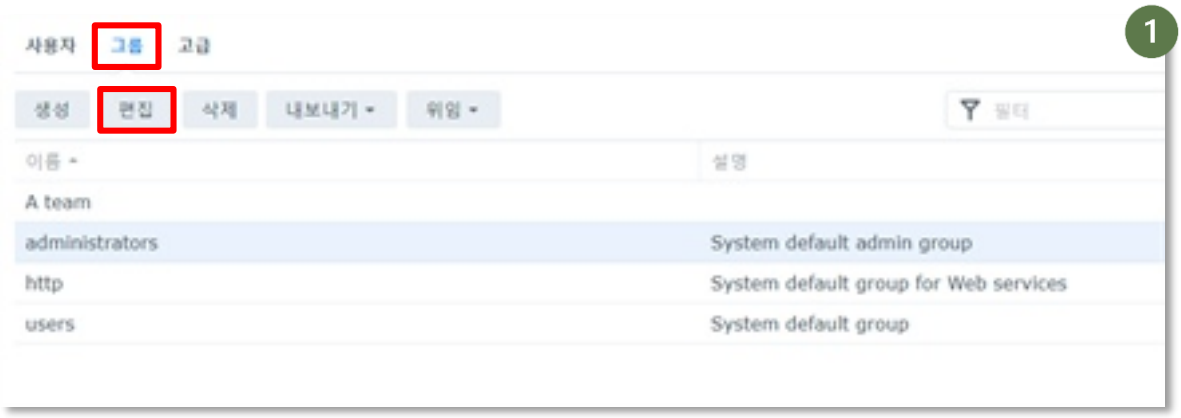


시놀로지(Synology)

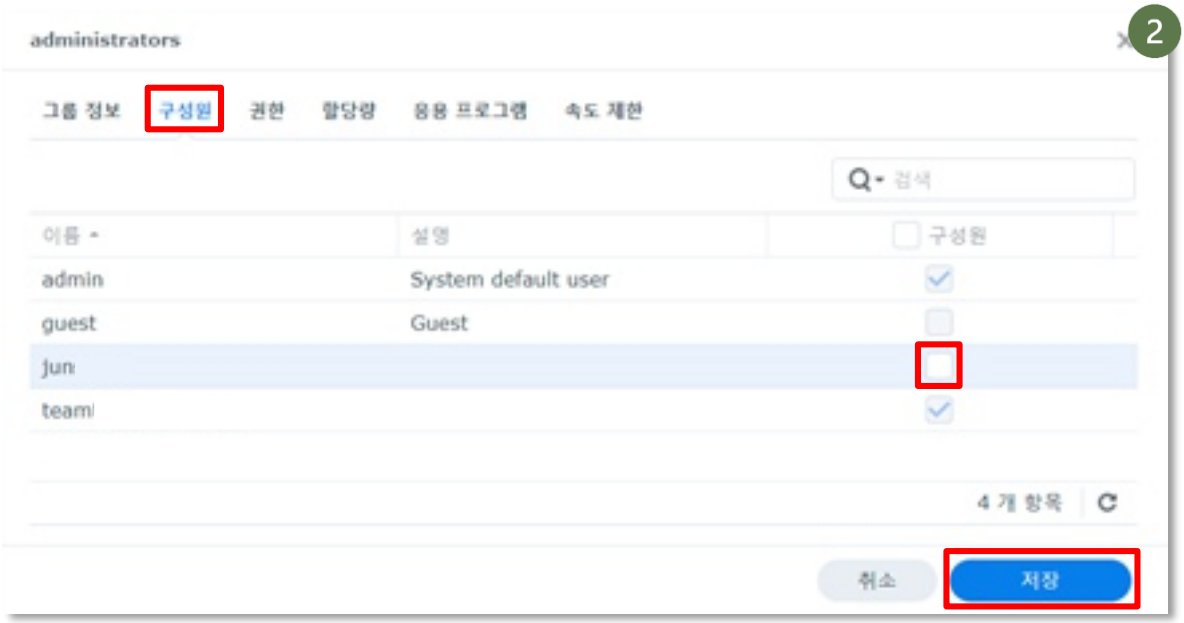
관리자 그룹 관리하기

관리자 계정은 기본적으로 높은 권한을 가지고 있어 부정 접속이 성공하면 큰 피해가 발생할 수 있습니다.

1 [제어판의 '사용자 및 그룹'] > ['그룹' 클릭] > ['administrators' 그룹 클릭 후 '편집' 클릭]



2 ['구성원' 클릭 후 관리자 그룹에서 해제할 인원의 선택 해제] > ['저장' 클릭]



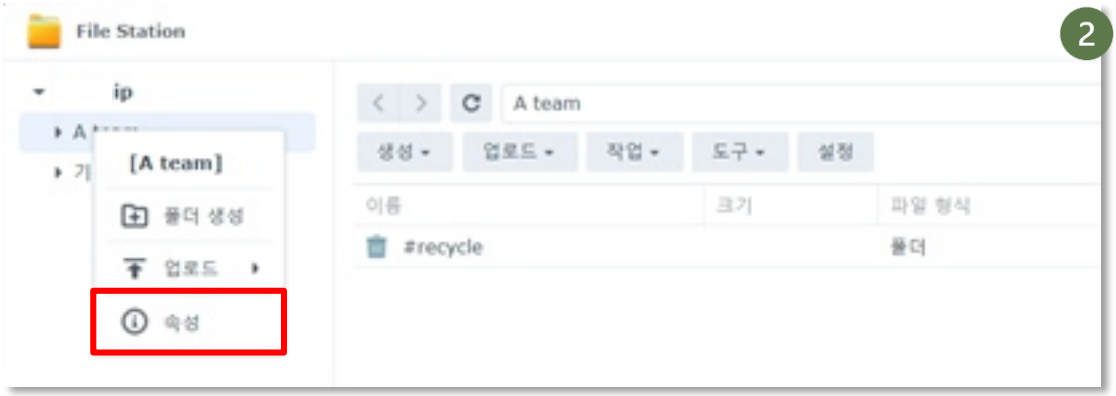
시놀로지(Synology)

공유 폴더 접근 권한 제한하기

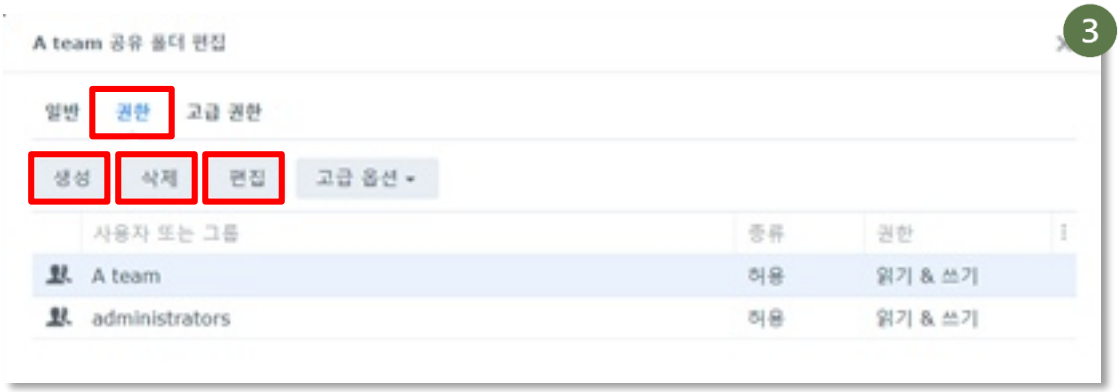
공유 폴더에 관리/읽기 및 쓰기 권한을 특정 사용자 또는 그룹에만 부여할 수 있습니다. 특정 인원에게 과도한 권한이 주어지면 보안에 취약하므로 적절히 관리해야 합니다.

1 ['File Station' 클릭]

2 [좌측 디렉터리 표시에 권한을 관리할 공유 폴더 우클릭] > ['속성' 클릭]

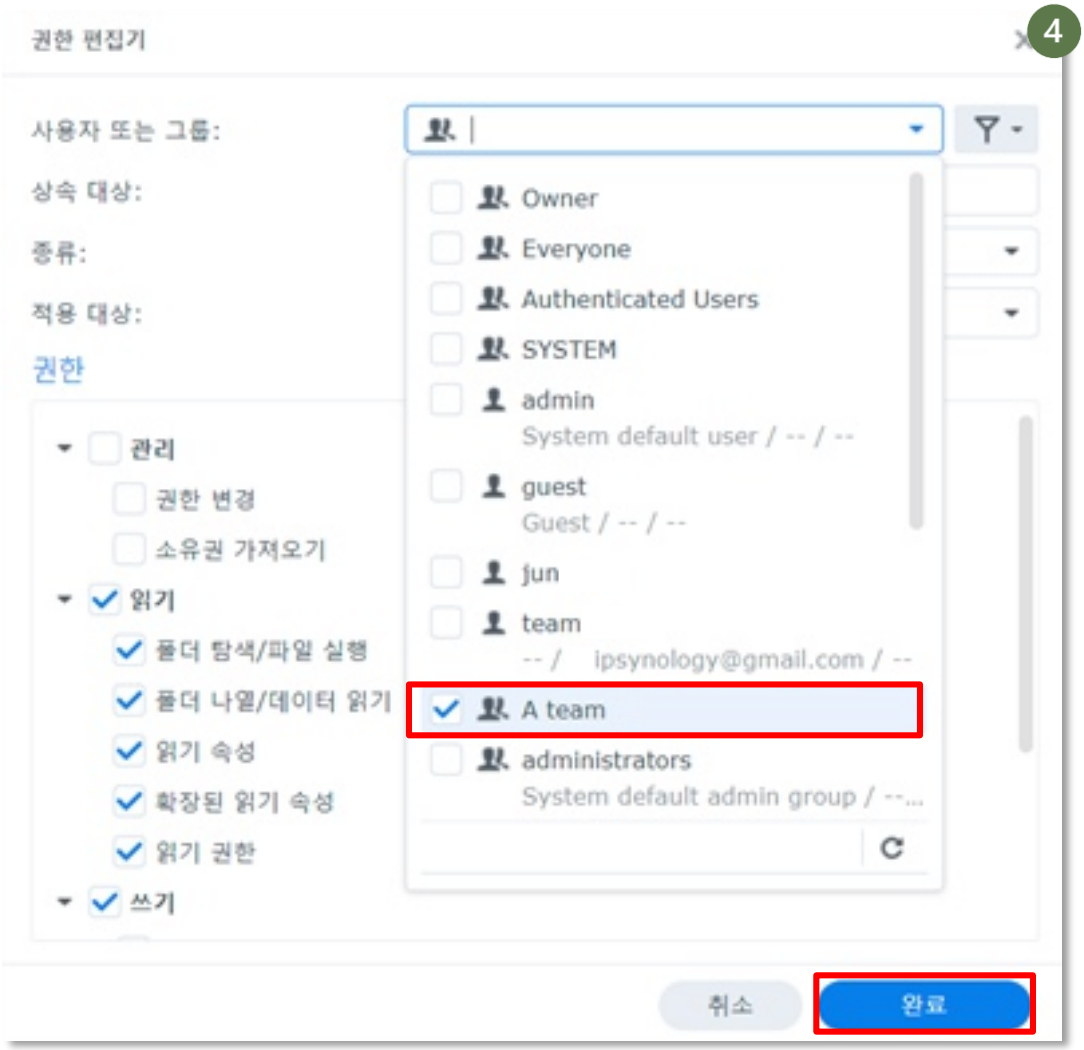


3 ['권한' 클릭] > [부여된 권한을 관리하거나 삭제 및 추가]



시놀로지(Synology)

4 ['사용자 또는 그룹' 에서 권한을 부여하거나 제거할 대상자 선택] > ['권한'에서 폴더에 대한 관리, 읽기, 쓰기에 대한 권한 관리 가능] > [최종적으로 '완료' 클릭]



그룹에 사용자 추가 또는 제거

새로 그룹을 생성/삭제하거나, 그룹에 인원을 추가/제거하는 설정은 [제어판] > [그룹]에서 할 수 있습니다. 자세한 과정은 위의 '관리자 그룹 관리'와 동일합니다.

시놀로지(Synology)

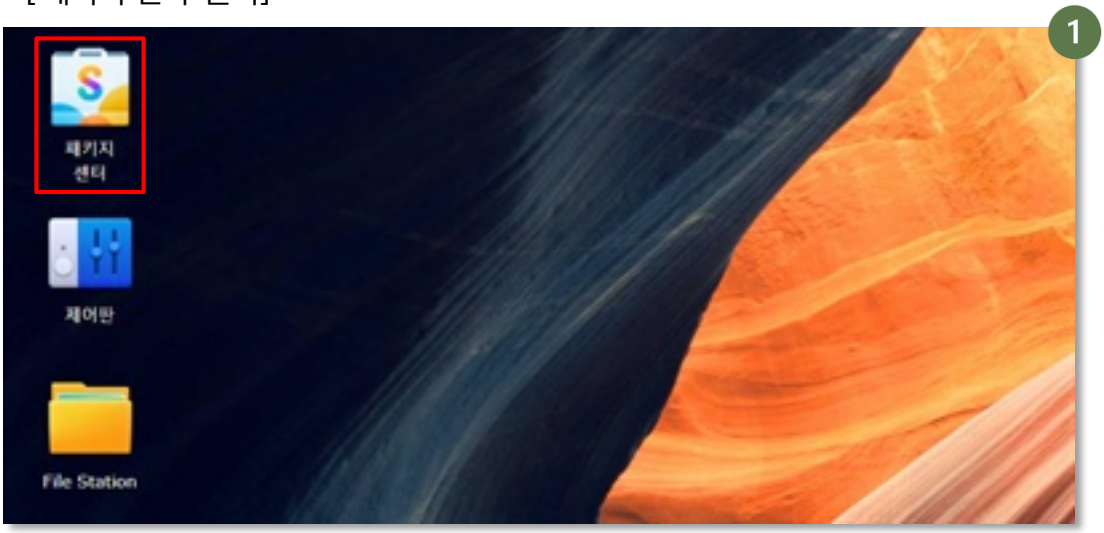
5. 보안 애플리케이션 설치하기

시놀로지에서 제공하는 보안 애플리케이션(백신)을 설치할 것을 권장합니다. 그리고 기본적으로 내장되어 있는 '보안 어드바이저'를 통해 현재 NAS 설정이 취약한지 확인하고 조치할 수 있습니다.

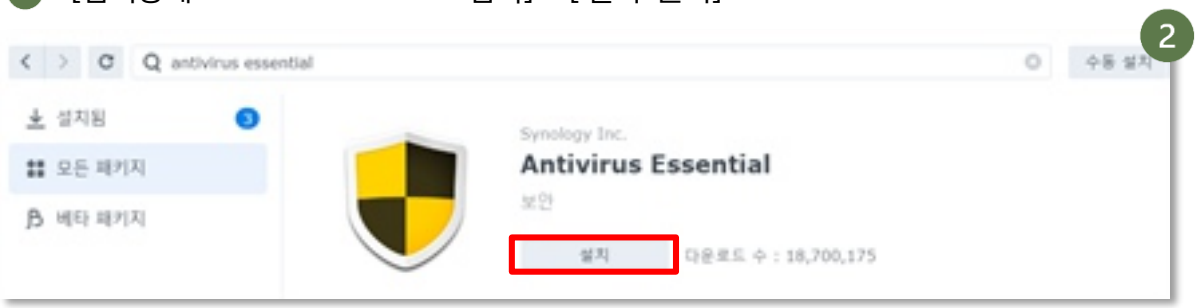
Antivirus Essential 설치하기

Antivirus Essential은 시놀로지에서 제공하는 무료 바이러스 백신입니다. 최근 NAS를 노리는 랜섬웨어 공격이 다수 발생하고 있기 때문에 백신을 설치하여 예방할 것을 권장합니다.

1 ['패키지 센터' 클릭]

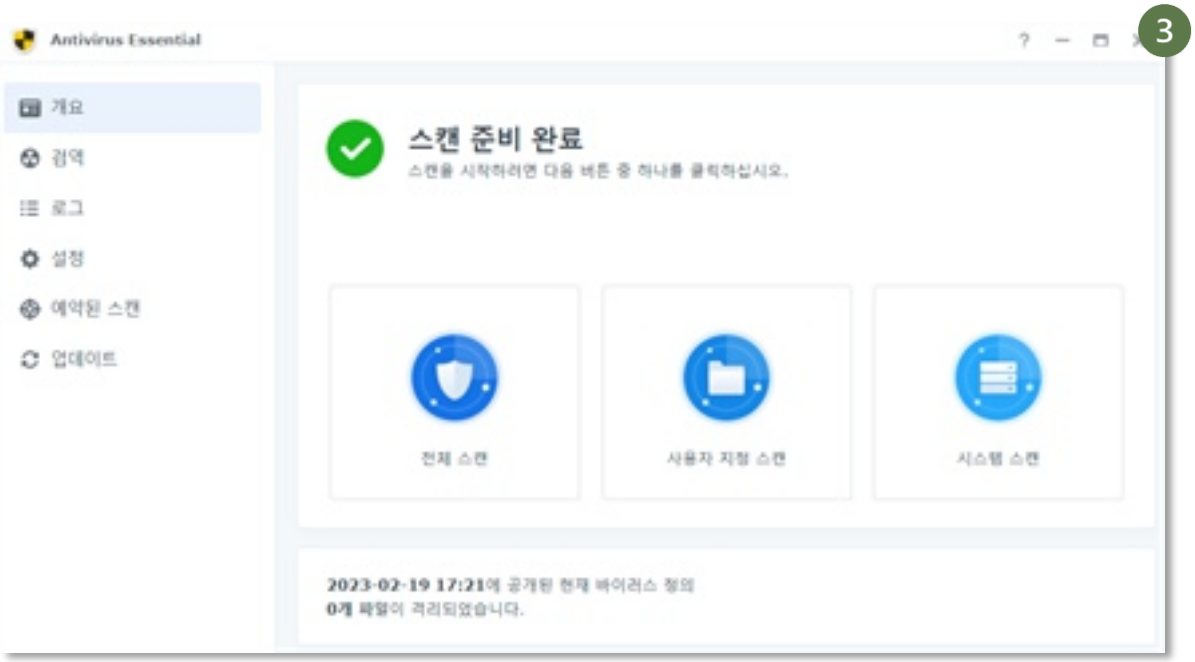


2 [검색창에 'Antivirus Essential' 입력] > ['설치' 클릭]



시놀로지(Synology)

3 [바탕화면에서 좌측 상단 '메인 메뉴' 클릭 후 'Antivirus Essential' 실행] > ['스캔'을 통해 바이러스 검사 가능]

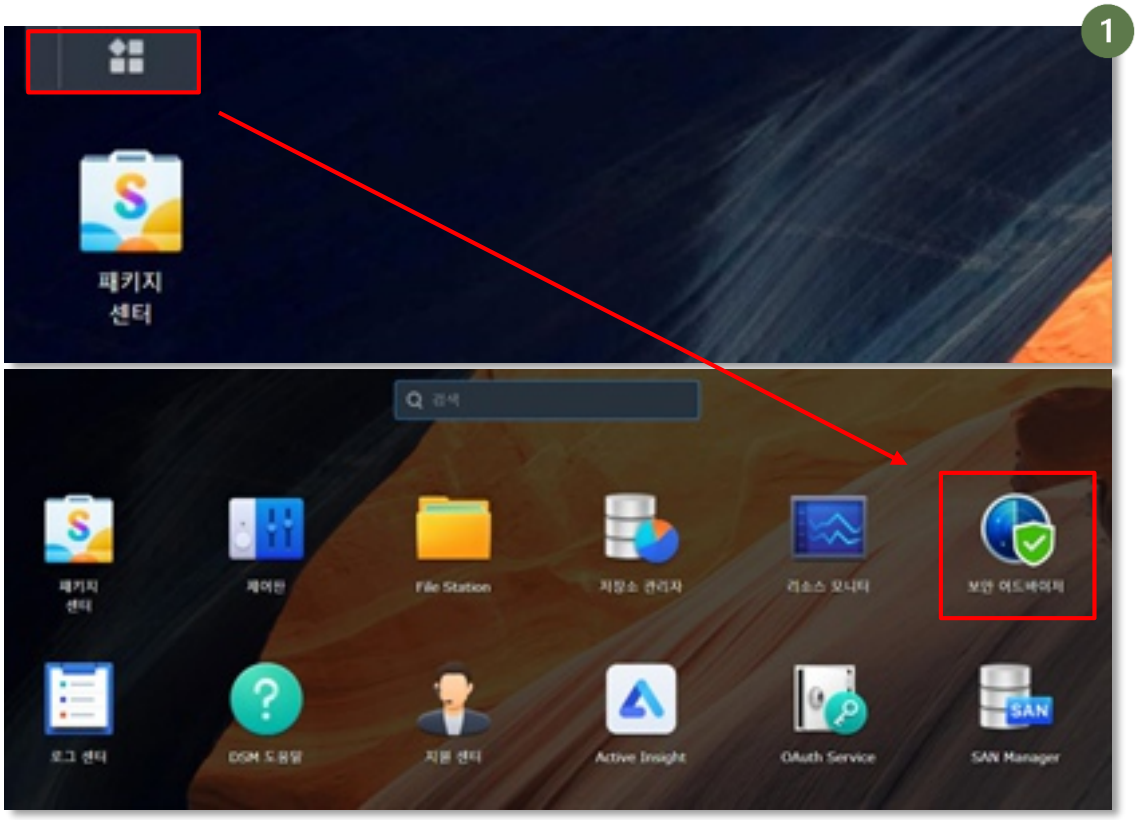


시놀로지(Synology)

보안 어드바이저 활용하기

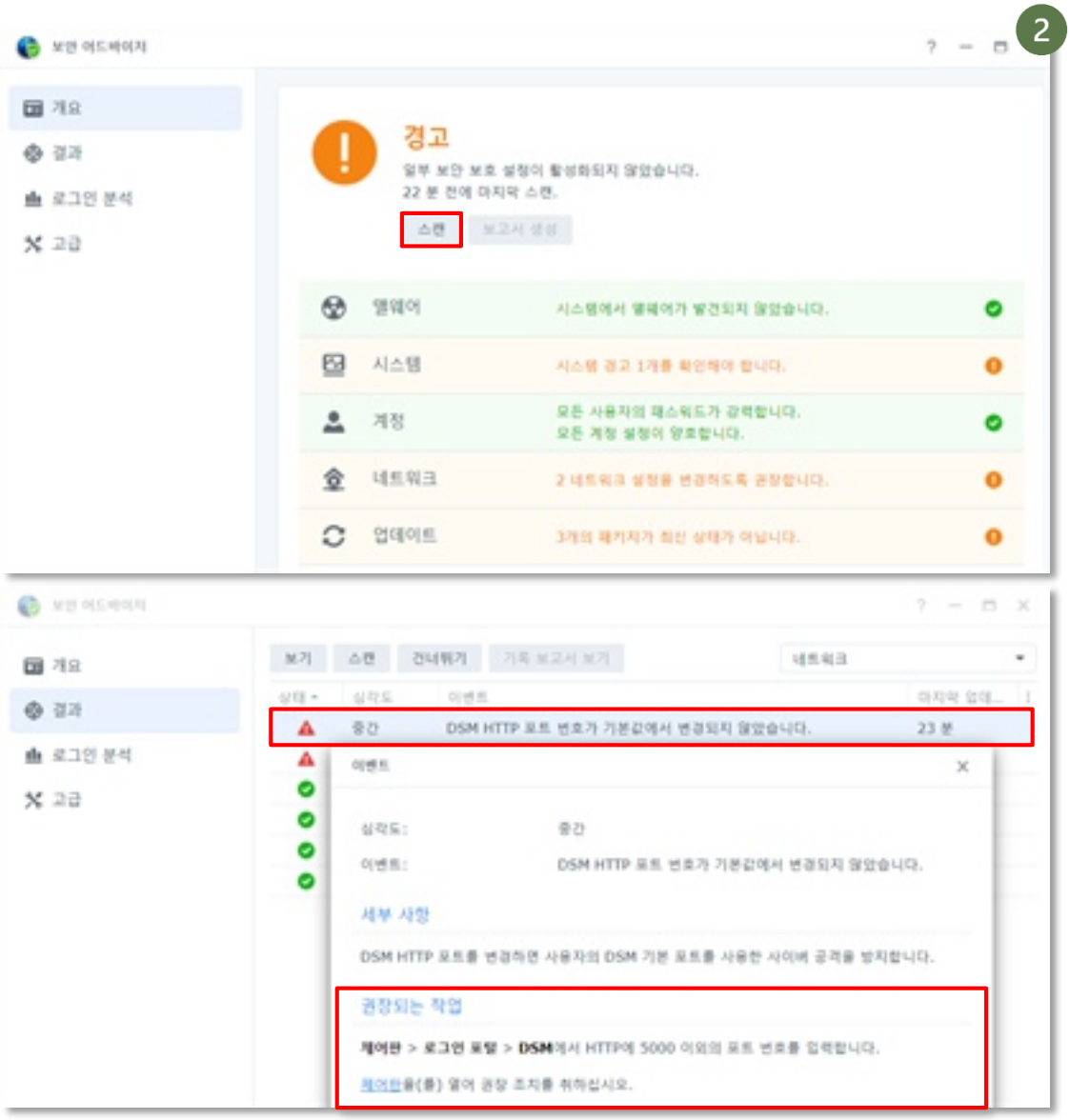
보안 어드바이저는 시놀로지가 기본적으로 제공하는 보안 애플리케이션입니다.
보안 어드바이저는 현재 NAS의 설정 상태를 검사한 뒤. 바람직한 보안 설정을 추천합니다.

1. ['바탕 화면'에서 '메인 메뉴' 클릭] > ['보안 어드바이저' 클릭]



시놀로지(Synology)

2 ['스캔'후 문제가 있는 설정에 대한 조치 방법 확인]



시놀로지(Synology)

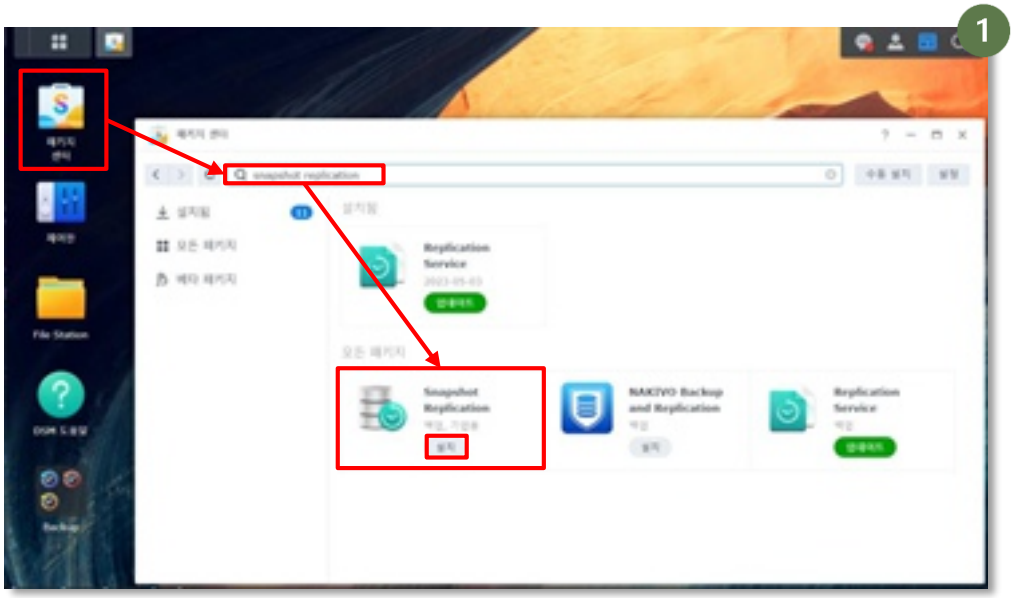
6. 스냅샷 기능

'스냅샷'은 특정 시점에 NAS가 가진 데이터 상태를 기억하는 기술로, 단순 데이터 백업에 비해 생성시간 및 저장용량이 적어 편리합니다. 실수로 데이터를 삭제하거나, 랜섬웨어와 같은 악성 프로그램에 의하여 데이터가 손실된 경우 저장해 놓은 시점으로 되돌아가 데이터를 복구할 수 있습니다.

스냅샷 기능 설치하기

시놀로지에서 스냅샷 기능을 사용하려면 NAS의 파일 시스템이 'BTRFS'이어야 합니다. 또한 제품별로 스냅샷 기능이 포함되어 있지 않은 경우가 있으므로 사전에 확인해야 합니다.

1 ['패키지 센터' 클릭] > [검색창에 'Snapshot Replication' 입력] > ['설치' 클릭]



스냅샷과 백업의 차이

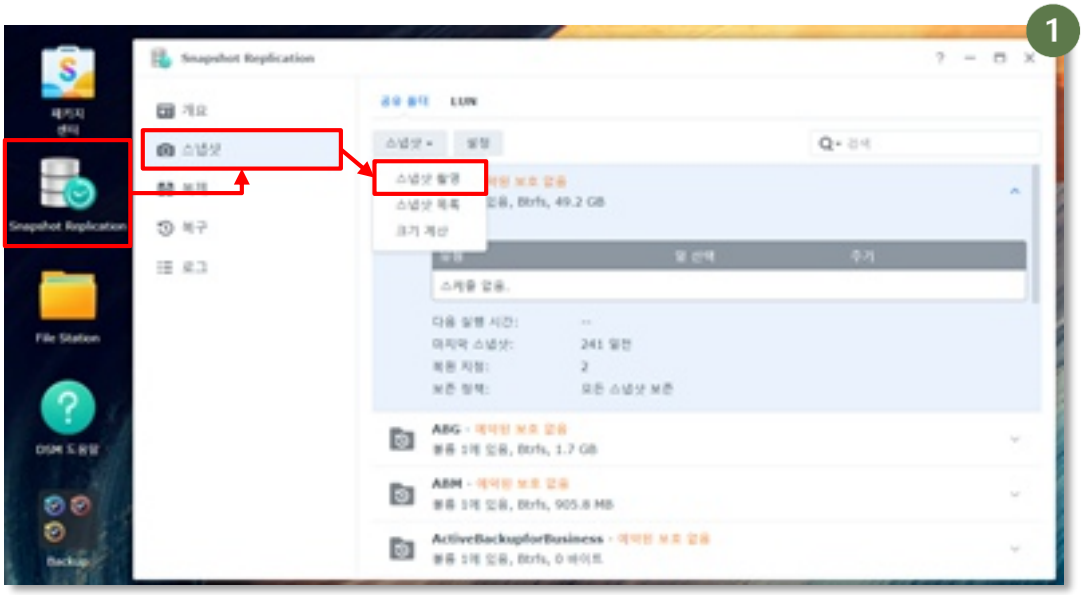
스냅샷 기술은 특정 시점의 데이터 상태를 기억하고 있다가 해당 시점으로 되돌리는 기술로, 데이터 자체를 여러 사본으로 만들어 별도 장소에 저장하는 '백업' 기술과는 차이가 있습니다. 스냅샷은 빠르고 용량을 적게 차지한다는 장점이 있지만, 스냅샷 이미지 자체가 손상되거나 NAS가 물리적으로 고장나는 경우 복구할 수 없다는 단점이 있습니다. 따라서 스냅샷은 백업에 비해 데이터의 안전성은 떨어진다는 한계가 있습니다.

시놀로지에서는 'Hyper Backup'이라는 프로그램을 통해 백업을 지원하고 있습니다.
해당 프로그램 또한 패키지 센터에서 다운로드 할 수 있습니다.

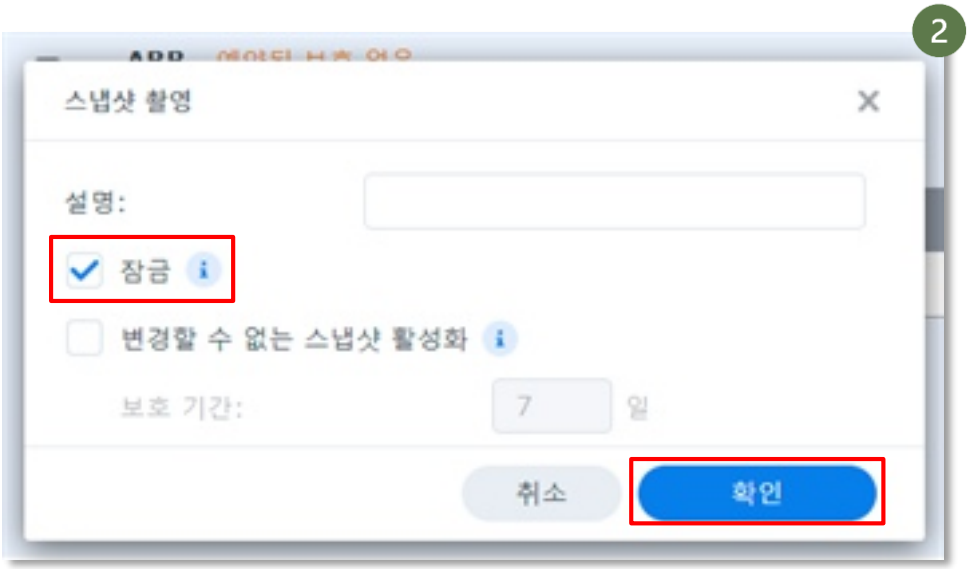
시놀로지(Synology)

스냅샷 촬영 및 촬영 예약하기

1 ['Snapshot Replication'을 클릭하여 실행] > [우측 메뉴에서 '스냅샷' 선택] > ['공유 폴더' 클릭] > ['스냅샷' 클릭] > ['스냅샷 촬영' 선택]



2 [스냅샷이 자동으로 삭제되지 않도록 '잠금' 선택> ['확인' 클릭]



시놀로지(Synology)

3 ['스냅샷' 메뉴에서 '설정' 클릭] > ['스케줄' 클릭] > ['스냅샷 예약 활성화' 선택] > [스냅샷을 촬영할 주기(1일, 1주, 특정 요일 선택가능) 및 촬영 시간 선택]

4 [상단 메뉴바의 '보존' 클릭] > ['보존 정책 활성화' 선택] > ['유지할 최신 스냅샷 수'를 128로 입력> ['확인' 클릭]

시놀로지(Synology)

스냅샷 예약 시 주의할 점

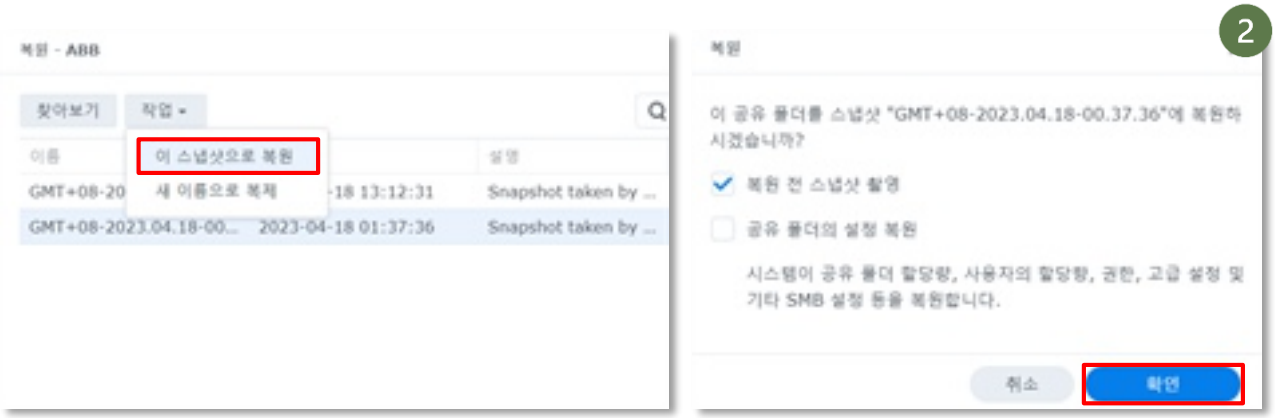
① 스냅샷 촬영시간은 새벽으로 설정하는 것이 좋습니다. 스냅샷 촬영은 부하량이 많아 작업이 수행되는 중에는 NAS 사용이 자유롭지 못할 수 있습니다. 업무 중 NAS에 저장된 데이터에 접근할 수 없다면 업무 수행에 지장을 초래할 수 있습니다. 그러므로 업무 시간 외에 스냅샷을 촬영하도록 예약하는 것이 좋습니다.

② 스냅샷 저장 개수가 일정량을 넘지 않도록 제한하는 것이 좋습니다. 스냅샷도 저장공간을 차지하기 때문에 스냅샷이 너무 많이 쌓이면 데이터를 저장할 공간이 모자랄 수 있습니다. 저장 개수를 제한하면 새로 스냅샷을 촬영할 때 가장 오래된 스냅샷부터 삭제합니다. 이로써 데이터 저장 공간을 너무 많이 차지하지 않으면서 복구 시점을 현재와 가깝게 할 수 있습니다.

스냅샷으로 데이터 복구하기

1. [좌측 메뉴에서 '복구' 선택] > ['공유 폴더' 클릭] > [복구할 공유폴더 클릭 후 상단의 '복원' 클릭]

2. [복구 시점 선택 후 '작업' 클릭] > ['이 스냅샷으로 복원' 선택] > ['확인' 클릭]



시놀로지(Synology)

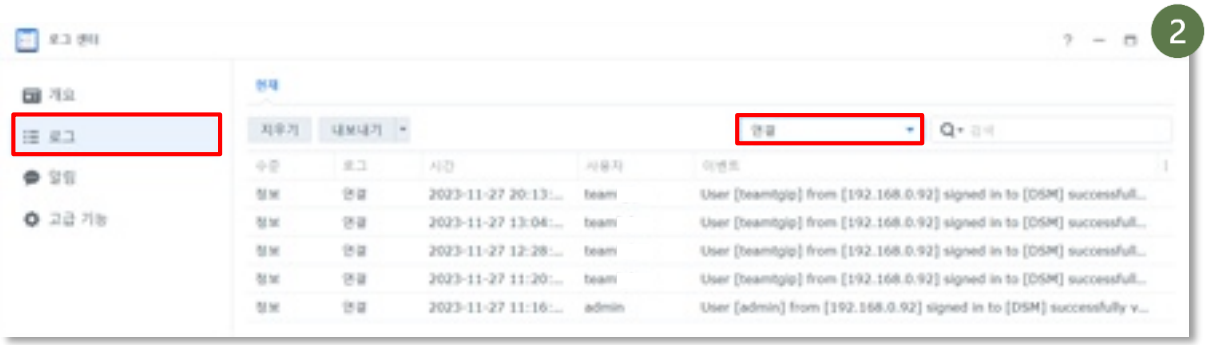
7. 로그 관리

저장소에 누가, 언제, 어떤 파일을 올리고 받아갔는지 추적하는 방법을 안내합니다. 특히 자료 유출, 악성 파일 업로드 시 책임자를 추적하는 데 도움이 될 수 있습니다.

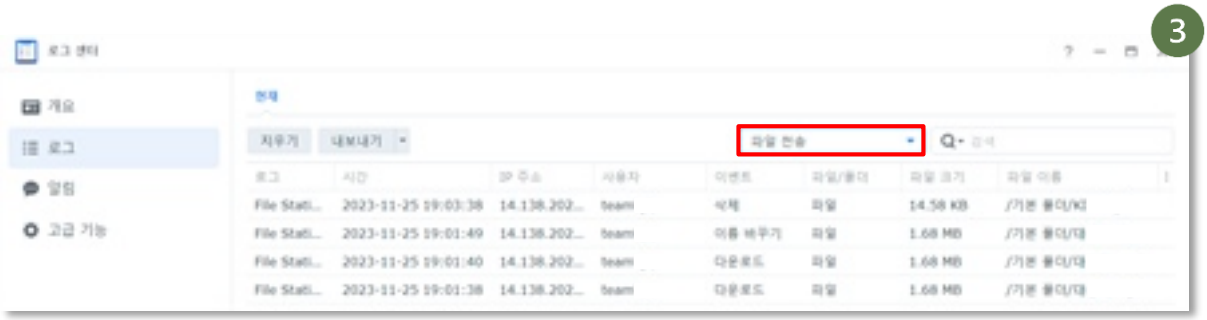
로그관리

1 ['메인 메뉴' 클릭] > ['로그 센터' 클릭]

2 ['메뉴'에 '로그' 클릭] > [우측 상단 메뉴를 '연결'로 설정하면 NAS의 접속한 명세(시간, IP, 계정) 확인 가능]



3 [우측 상단 메뉴를 '파일 전송'으로 설정하면 파일 업로드, 다운로드 명세 확인 가능]



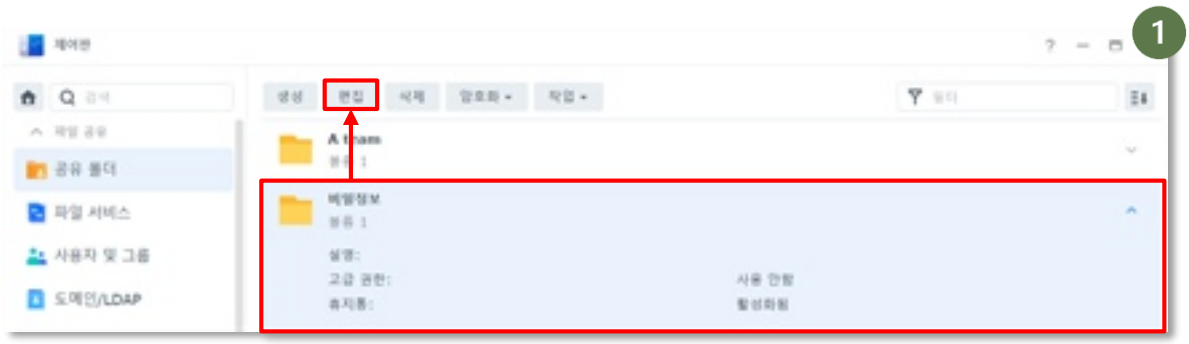
시놀로지(Synology)

8. 데이터 암호화하기

데이터가 외부로 유출되어도 그 내용이 암호화되어 있다면 민감한 정보를 타인이 알게되는 것을 막을 수 있습니다. 데이터 암호화란 일상적으로 사용되는 문자(평문)를 '암호키'라고 하는 값과 계산해 암호문으로 변환하여 알아볼 수 없게 만드는 기술입니다. 암호문은 암호키를 가진 사람만이 그 내용을 알 수 있어 정보의 비밀을 유지할 수 있습니다.

공유폴더 암호화하기

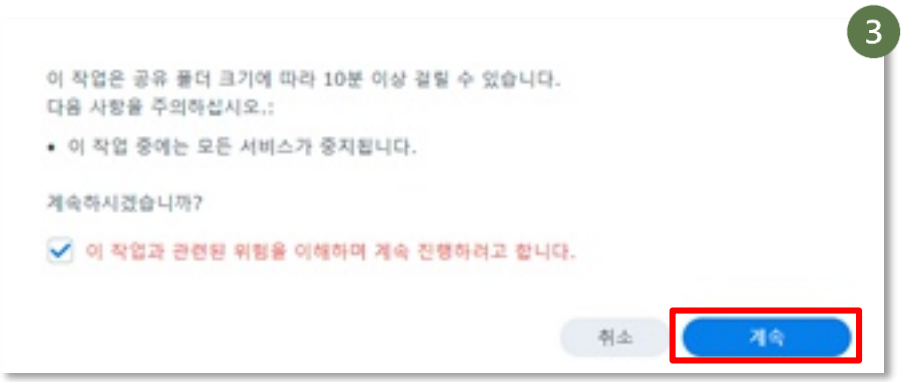
1 [제어판의 '공유 폴더'] > [암호화 할 폴더를 선택한 후 '편집' 클릭]



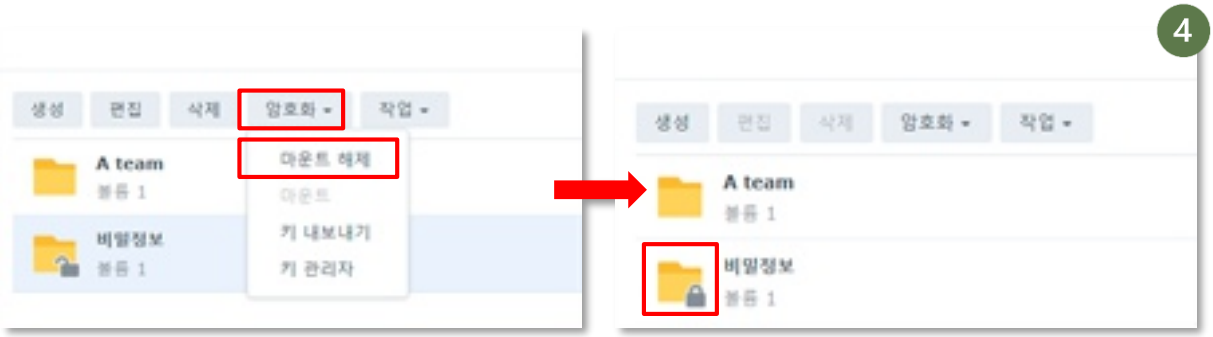
2 ['암호화' 클릭 후 '이 공유 폴더 암호화' 선택] > [복호화 키 입력(임의의 비밀번호)]

시놀로지(Synology)

3 [암호화 동의를 위해 '계속' 클릭]

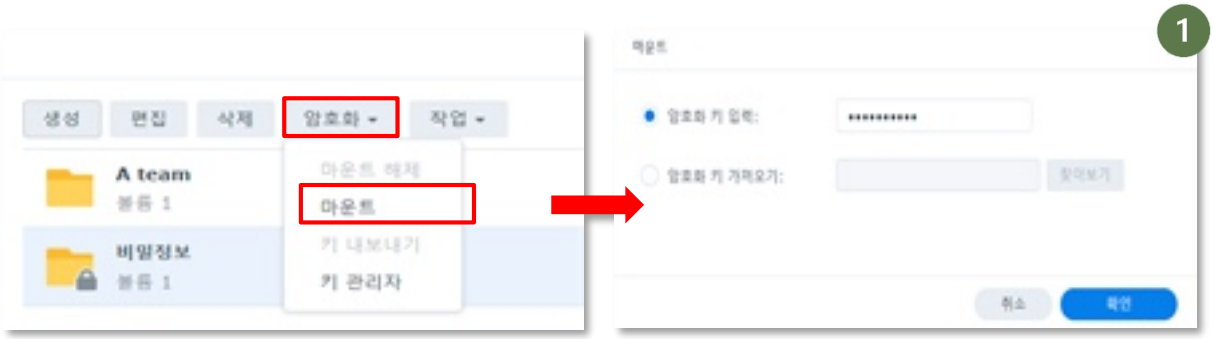


4 [완료 후 우측 상단 '암호화' 클릭] > ['마운트 해제'를 클릭하여 암호화 완료 (마운트 해제까지 수행하여 암호화 완료)]



공유폴더 복호화하기

1 [복호화를 위해서 '마운트' 클릭한 후 '복호화 키' 입력해 복호화 완료]



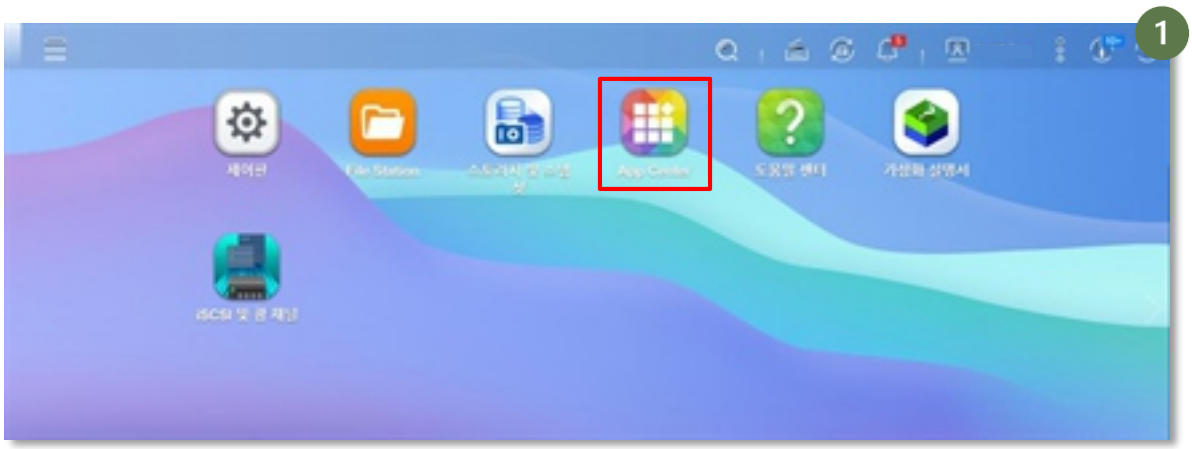
큐냅(QNAP)

1. 외부 부정 접속 차단하기

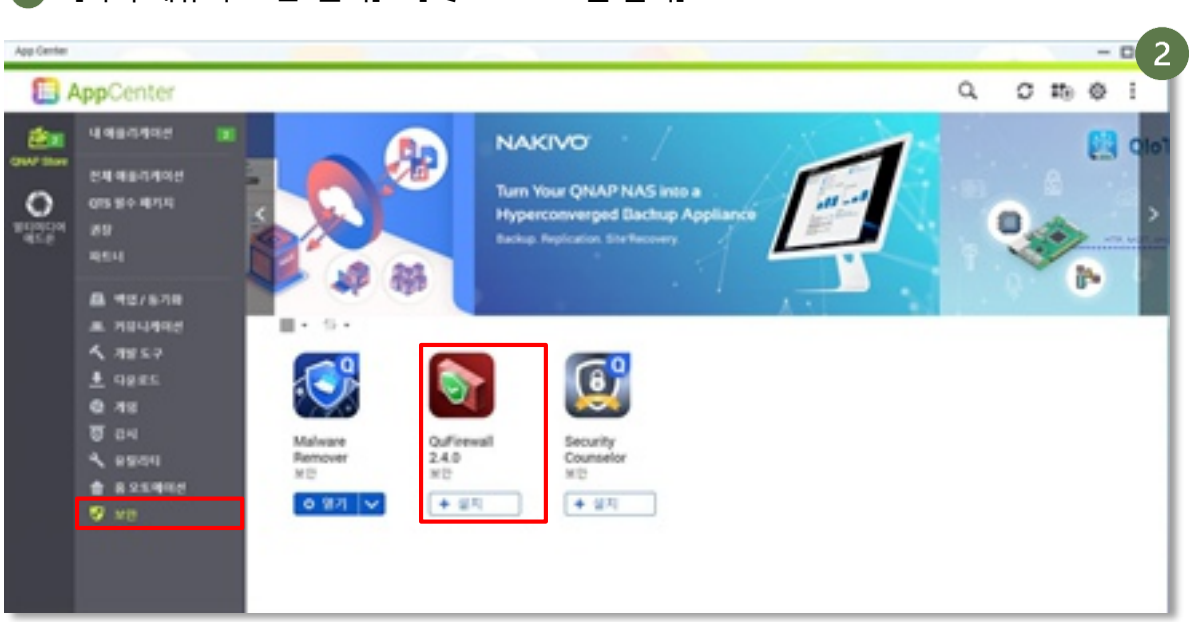
NAS는 인터넷과 연결되어 NAS의 IP주소 혹은 URL을 알고 있다면 외부에서도 NAS 저장소에 접근할 수 있습니다. 그렇기 때문에 회사용 NAS의 경우 인터넷을 통한 직접 접속은 차단하고 내부에서만 운영할 것을 권고하고 있습니다. 불가피하게 인터넷과 연결해야 하는 경우에는 철저한 관리가 필요합니다.

방화벽 'QuFirewall' 설치하기

1 ['메인 메뉴' 클릭 후 'App Center' 클릭]



2 [좌측 메뉴의 '보안' 클릭] > ['QuFirewall'을 설치]

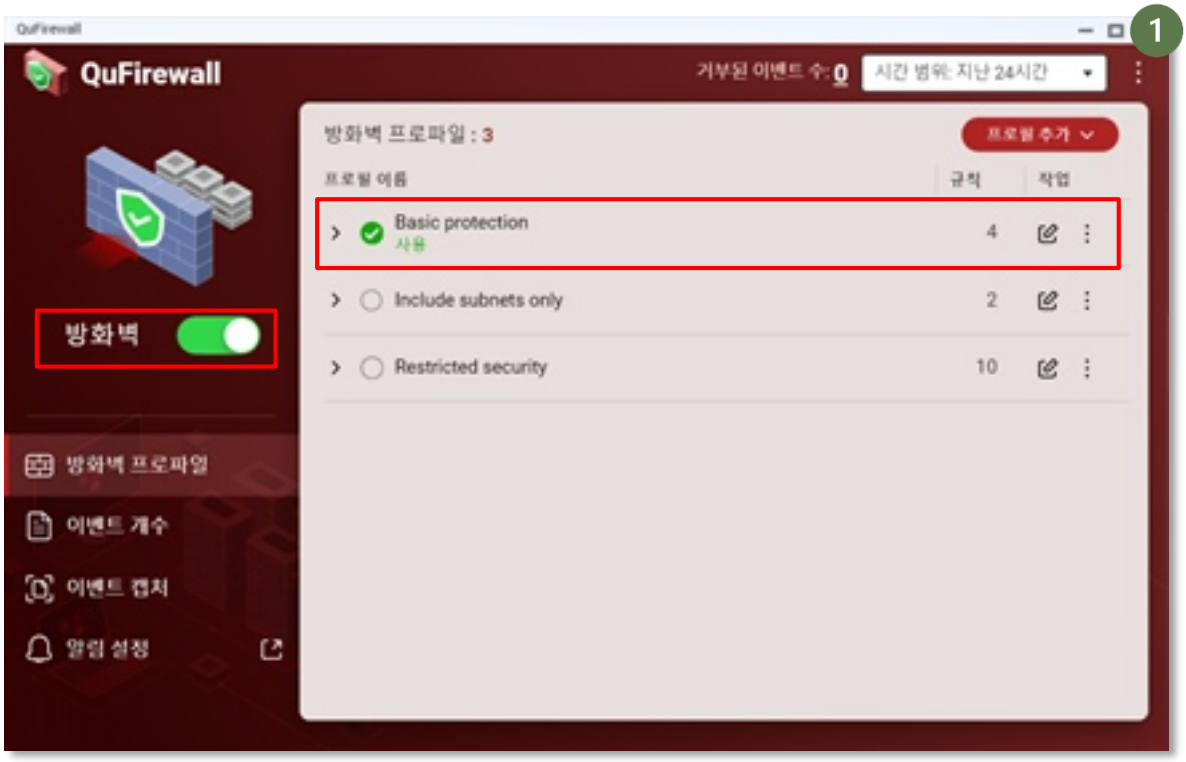


큐냅(QNAP)

방화벽 활성화 확인하기

1 [방화벽 '활성화' 확인] > [프로필 'Basic protection(기본 보호)' 권장]

※ 기본 보호 설정 하에서는 동일 인트라넷(내부망) 및 동일 지역(국가)의 접근은 허용됩니다.



큐냅에서 인터넷 연결 차단하기

NAS와 연결된 라우터 장치에 'DMZ', '포트포워딩', 'UPnP'와 같은 기능이 활성화되어 있다면 NAS 장비가 인터넷에 노출될 수 있습니다. 따라서 NAS를 인터넷에 노출시키지 않으려면 라우터에 해당 기능이 비활성화되어 있는지 확인해야 합니다.

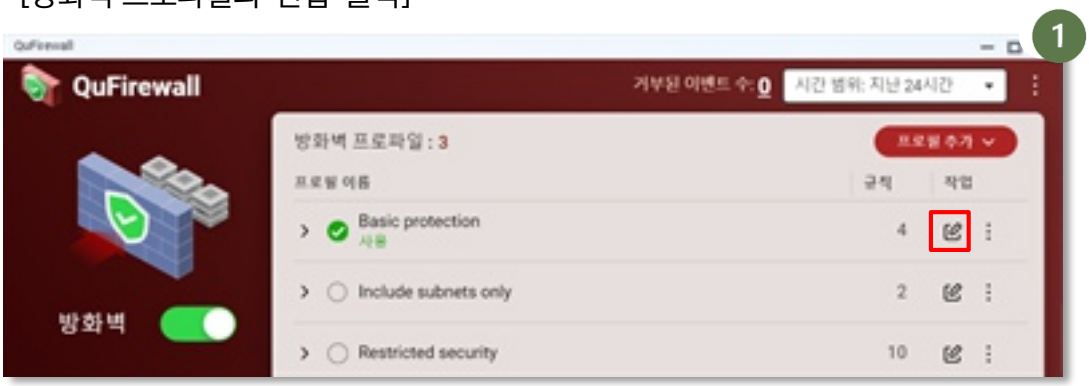
큐냅 NAS에서 확인할 수 있는 설정 방법은 다음과 같습니다. (myQNAPcloud를 통해 설정)

['자동 라우터 구성 UPnP 포트포워딩' 비활성화]: 우측 상단 메뉴의 '자동 라우터 구성' 클릭
['게시된 서비스 기능' 비활성화]: 'Published Service' 메뉴에서 '공개'를 모두 해제
['myQNAPcloud Link 액세스 제어'를 '비공개' 또는 '사용자지정' 설정]: '액세스 제어' 메뉴 클릭

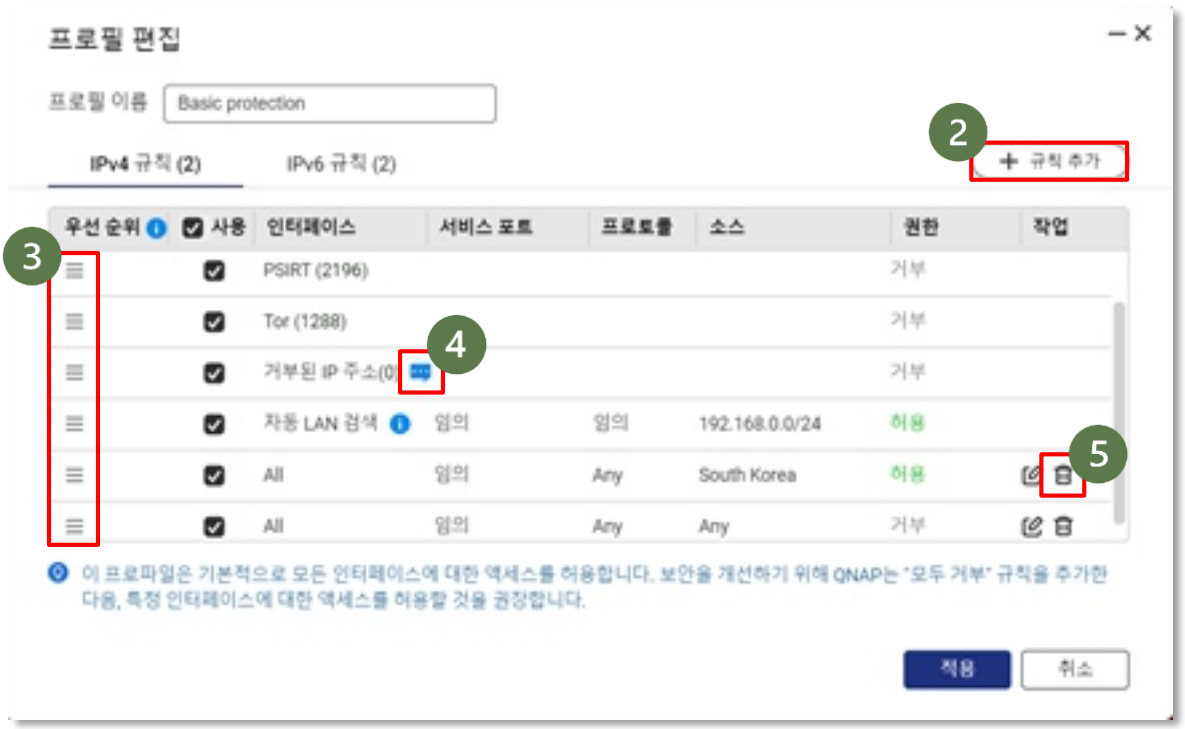
큐냅(QNAP)

방화벽 규칙 편집하기

1. [방화벽 프로파일의 '편집' 클릭]



2. 특정 IP, 네트워크(서브넷) 또는 국가에 대한 접근 허용 및 차단 설정 가능
3. 규칙의 순서 변경 가능, 규칙은 위에서 부터 적용
4. 관리자가 직접 거부할 IP주소를 추가 가능
5. 지역 설정을 삭제하면 내부 인트라넷에서의 접근만을 허용하므로 보안 강화 가능



큐냅(QNAP)

6 [규칙의 순서를 변경하거나 새 규칙 추가 가능]

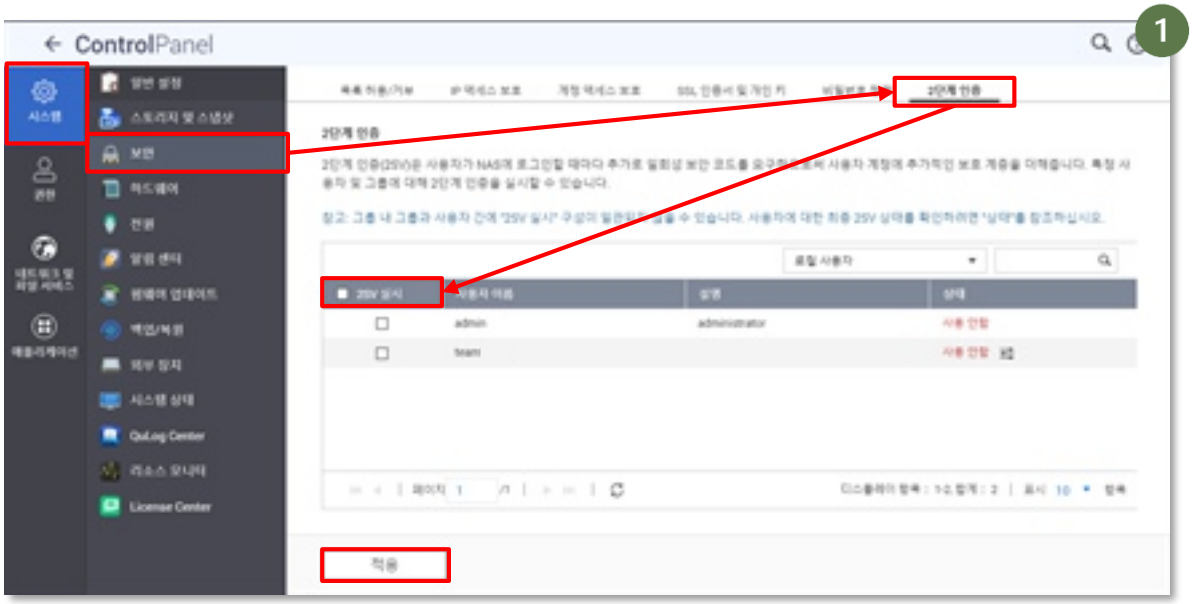
큐냅(QNAP)

2단계 인증 강제 적용하기

2단계 인증은 사용자가 로그인을 시도하는 경우, 휴대전화를 통해 본인이 로그인을 하고 있음을 인증하는 기술입니다. 2단계 인증을 적용하면 비밀번호만으로는 바로 NAS에 접속할 수 없기 때문에, 타인의 계정을 도용한 부정 접속을 방지할 수 있습니다. 따라서 모든 구성원이 2단계 인증을 수행하도록 정책을 변경할 것을 권장합니다.

* 정책 설정 후 각 사용자는 개별적으로 2단계 인증 설정을 해야 합니다.

1. ['제어판' 실행] > ['시스템' 클릭] > ['보안' 클릭] > ['2단계 인증'에서 모든 사용자 선택 후 '적용' 클릭] > [모든 구성원에게 2단계 인증을 적용 권장]



2단계 인증 설정 방법

2단계 인증 강제 설정 시, NAS에 접근하는 모든 계정은 2단계 인증을 등록하기 전까지 로그인할 수 없습니다. 모든 구성원은 아래 2가지 중 하나의 방법으로 2단계 인증을 등록해야 합니다.

① Google OTP 애플리케이션 이용
② Microsoft Authenticator 애플리케이션 이용

큐냅(QNAP)

2. 자동 업데이트 활성화하기

인터넷을 통한 접속을 허용한 경우, 외부 공격자는 NAS가 자체적으로 가지고 있는 결함을 악용하여 공격을 시도할 수 있습니다. NAS 판매사는 이러한 위험을 막기 위해 결함을 발견하면 프로그램을 수정하여 배포합니다. 따라서 항상 최신 버전의 소프트웨어를 설치하는 것이 중요합니다. 이를 위해 NAS의 '자동 업데이트'가 활성화되어 있는지 확인해야 합니다.

자동 업데이트 설정하기

1. ['제어판'의 펌웨어 업데이트' 클릭] > ['업데이트 확인'을 클릭하여 최신 버전인지 확인] > [최신 버전이 아니라면 업데이트 수행]

2. ['펌웨어 업데이트 설정'에서 '펌웨어 자동으로 업데이트' 선택] > ['펌웨어 업데이트 유형'을 권장 설정인 '보안 업데이트'와 '품질 업데이트'로 선택]

큐냅(QNAP)

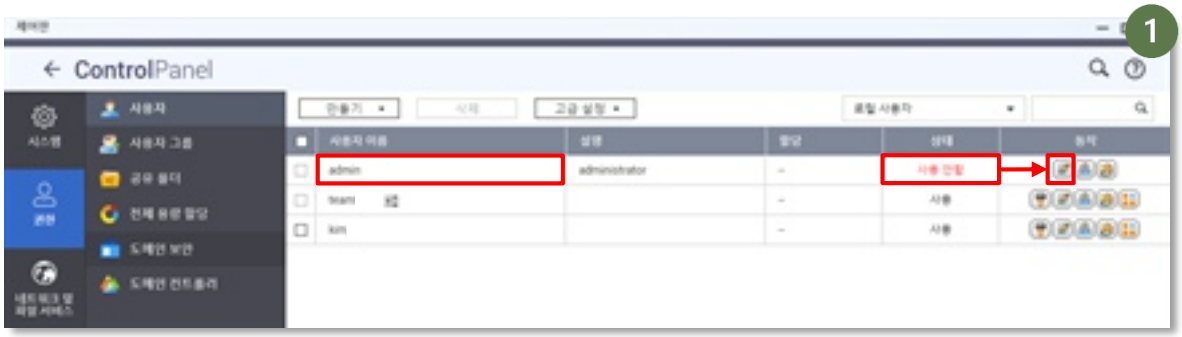
3. 계정 보안 설정하기

QNAP NAS에는 'admin'이라는 관리자 계정이 기본으로 생성되어 있습니다. 기본 admin 계정이 활성화되어 있는 경우 공격자가 해당 계정으로 접속을 시도할 수 있습니다.

기본 관리 계정 비활성화하기

기본 admin 계정은 완전히 비활성화하고, 관리자 계정임을 추측하기 어렵게 ID를 설정하여 관리자 계정으로 사용하기를 권장해 드립니다.

1. ['제어판' 실행] > ['권한' 클릭] > ['사용자' 클릭] > [admin 상태가 '사용 안함'으로 되어있는지 확인]



2. [계정이 활성화 되어 있다면 '계정 프로필 편집'을 클릭] > ['이 계정 사용 안함' 선택]

큐냅(QNAP)

비밀번호 정책 설정하기

관리자는 NAS 계정에 대한 비밀번호 규칙을 지정할 수 있습니다.

1. ['제어판' 실행] > ['시스템' 클릭] > ['보안' 클릭] > [우측 상단의 '비밀번호 정책' 클릭] > [하단의 '권장하는 규칙'에 맞게 설정 변경]

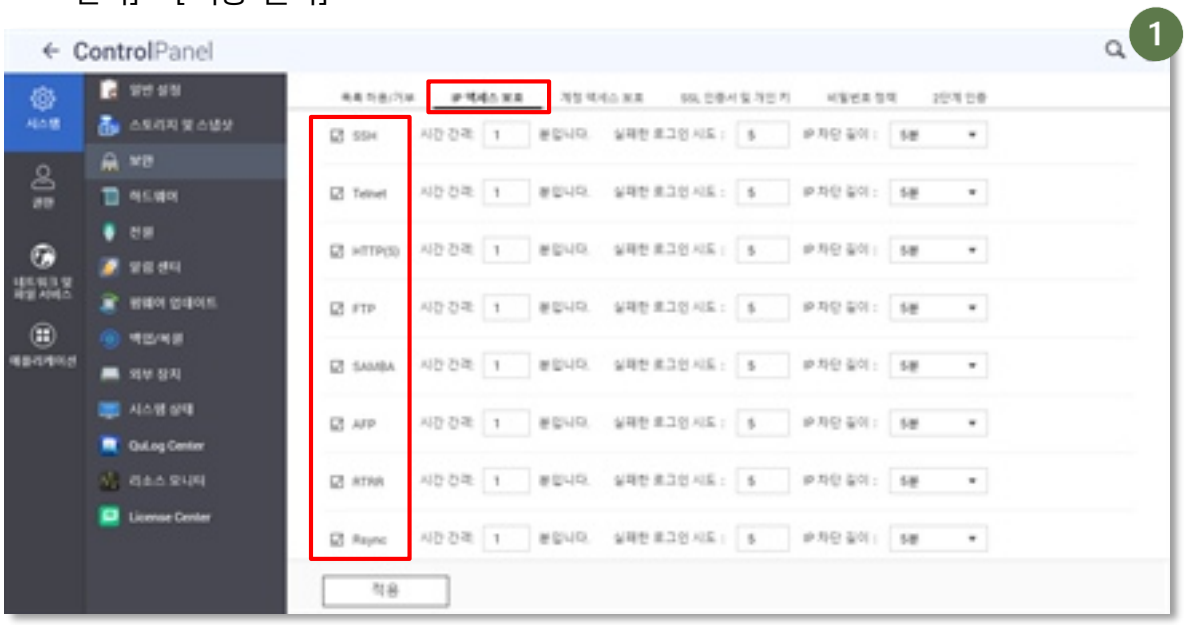
권장하는 규칙	
항목	권장 값
영문 대소문자 혼합 포함	최소 1개의 대문자 및 1개의 소문자
숫자 문자 포함	활성화
특수 문자 포함	활성화
연관된 사용자 이름 또는 반대 순서의 이름과 동일하지 않아야 함	활성화
최소 길이	8자 이상
최대 비밀번호 사용 기간	90일 미만

큐냅(QNAP)

로그인 실패횟수 초과시 IP 차단 및 계정 잠금 설정하기

로그인에 여러 번 실패한 경우 계정 보호를 위해 해당 IP를 차단할 수 있으며, 정해진 시간 동안 그 계정에 대한 로그인을 막을 수 있습니다.

1. ['제어판' 실행] > ['시스템' 클릭] > ['보안' 클릭] > ['IP 액세스 보호' 클릭 후 모든 서비스 선택] > ['적용' 클릭]



2. ['계정 액세스 보호' 클릭] > ['관리자 그룹에 속하지 않는 모든 사용자' 선택] > [모든 서비스 선택] > ['적용' 클릭]

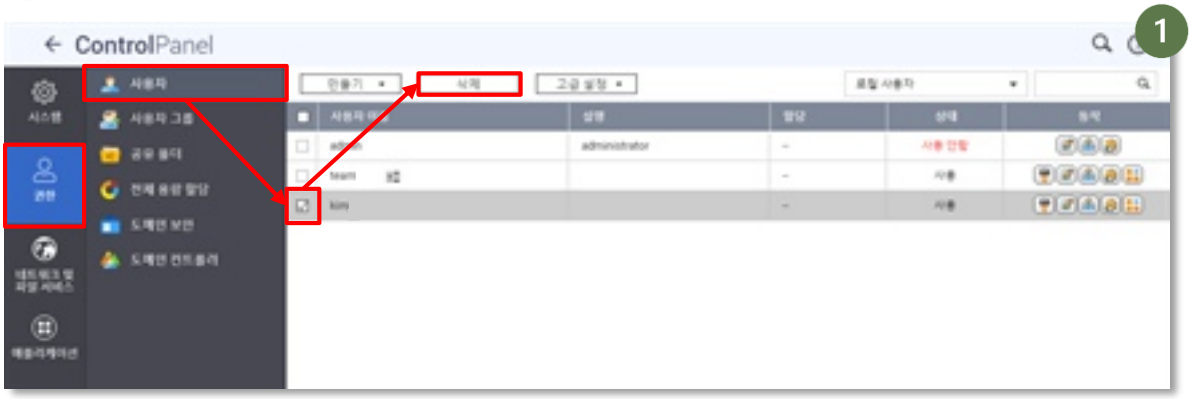
큐냅(QNAP)

4. 계정 권한 관리하기

일반 계정 및 게스트용 계정에 불필요하게 많은 권한이 주어져 있다면 공격자가 이러한 계정을 해킹한 뒤 공격하거나, 권한 없는 내부자가 영업비밀을 유출하는 등 많은 문제가 발생할 수 있습니다. 따라서 관리자는 임직원들의 권한이 필요 이상으로 주어져 있지 않은지 반드시 확인해야 합니다.

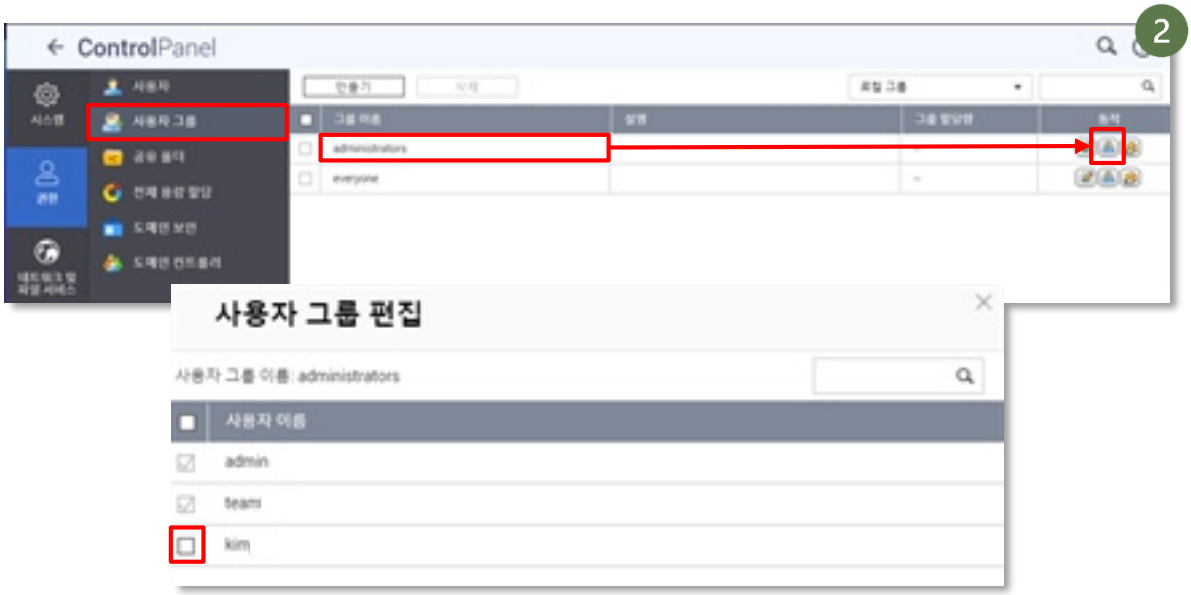
퇴사자 계정 삭제하기

1. [제어판의 '권한' 클릭] > ['사용자' 클릭] > [삭제 대상 계정 체크 후 '삭제' 클릭]



관리자 그룹 관리하기

2. [제어판의 '권한' 클릭] > ['사용자 그룹' 클릭] > ['administrators'의 '사용자 그룹 편집' 클릭] > [권한을 해제할 계정을 선택 해제한 후 '적용' 클릭]



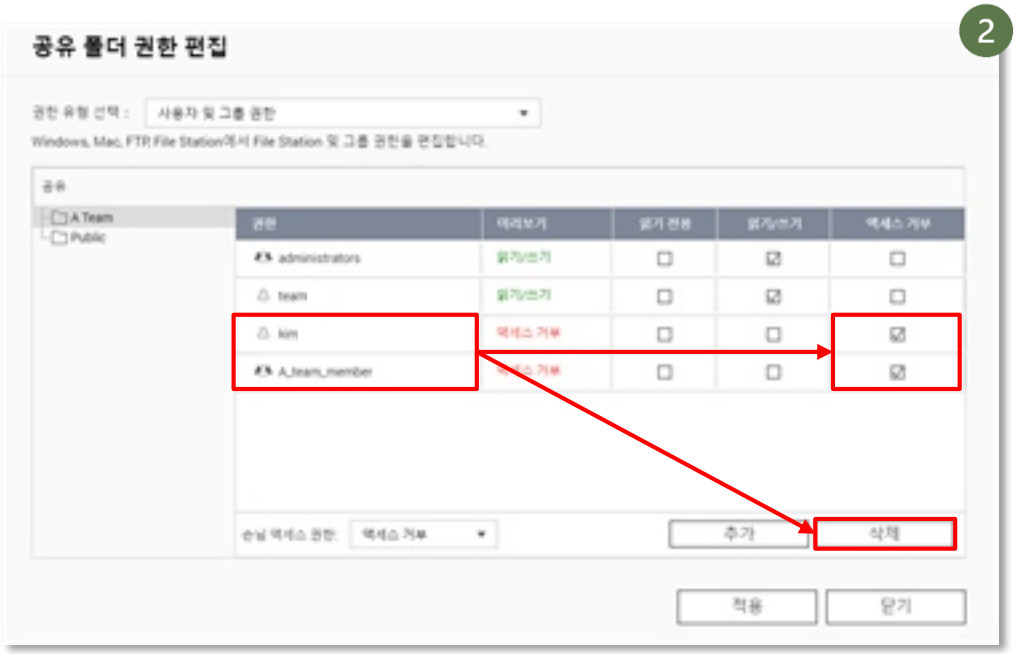
큐냅(QNAP)

공유 폴더 접근 권한 제한하기

공유 폴더에 관리/읽기 및 쓰기 권한을 특정 사용자 또는 그룹에만 부여할 수 있습니다. 특정 인원에게 과도한 권한이 주어지면 보안에 취약하므로 이를 적절히 관리해야 합니다.

1 ['제어판'의 '권한' 클릭] > ['공유 폴더' 클릭] > ['공유 폴더 권한 편집' 클릭]

2 [권한을 해제할 사용자 또는 그룹을 '삭제' 하거나 '엑세스 거부' 선택]



그룹에 사용자 추가 또는 제거

새로 그룹을 생성/삭제하거나, 그룹에 인원을 추가/제거하는 설정은
[권한] > [사용자 그룹] 에서 할 수 있습니다.
자세한 과정은 위의 '관리자 그룹 관리'와 동일합니다.

큐냅(QNAP)

5. 보안 애플리케이션

큐냅에서 제공하는 보안 애플리케이션(백신)을 사용할 것을 권장합니다. 그리고 'Security Counselor'를 통해서 NAS의 설정이 취약한지 확인하고 조치할 수 있습니다.

Security Counselor 설치

Security Counselor는 큐냅에서 제공하는 보안 애플리케이션 입니다. 현재 NAS의 설정 상태를 검사한 뒤, 바람직한 보안 설정을 추천합니다.

1 ['APP Center' 클릭] > [좌측 메뉴의 '보안' 클릭] > ['Security Counselor' 설치]

큐냅(QNAP)

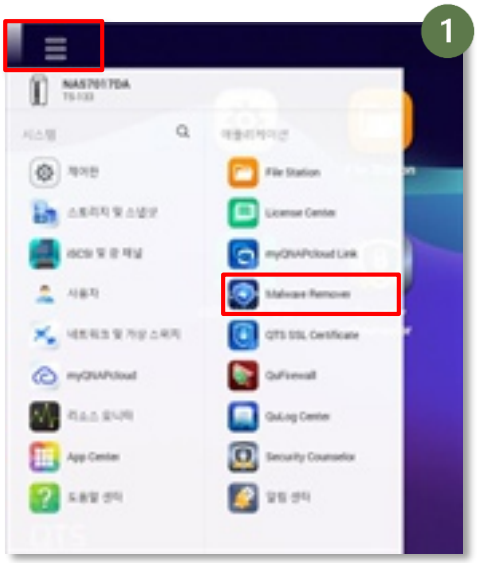
2 ['스캔' 후 문제가 있는 설정의 조치 방법 따르기]

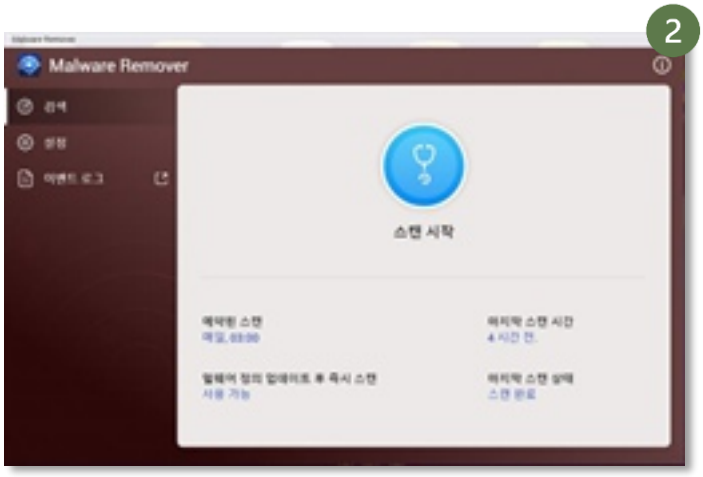
Malware Remover

Malware Remover은 큐냅에서 제공하는 무료 바이러스 백신입니다. 최근 NAS를 노리는 랜섬웨어 공격이 다수 발생하고 있기 때문에 백신을 통해 예방할 것을 권장합니다.

1 ['메인 메뉴' 클릭] > ['애플리케이션'의 'Malware Remover' 클릭]

2 ['스캔 시작'을 통해 검사 수행]





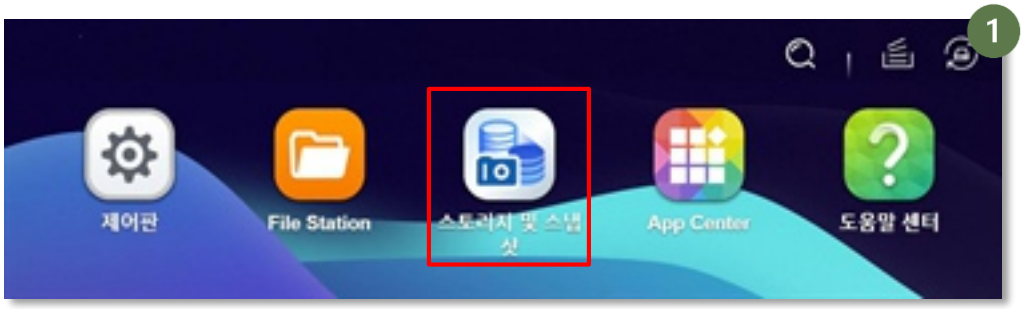
큐냅(QNAP)

6. 스냅샷 기능 사용하기

'스냅샷'은 특정 시점에 NAS가 가진 데이터 상태를 기억하는 기술입니다. 실수로 데이터를 삭제하거나, 랜섬웨어와 같은 악성 프로그램에 의하여 데이터가 손실된 경우 저장해 놓은 시점으로 되돌아가 데이터를 복구할 수 있습니다.

스토리지 스냅샷 촬영하기

1 ['스토리지 및 스냅샷' 클릭]

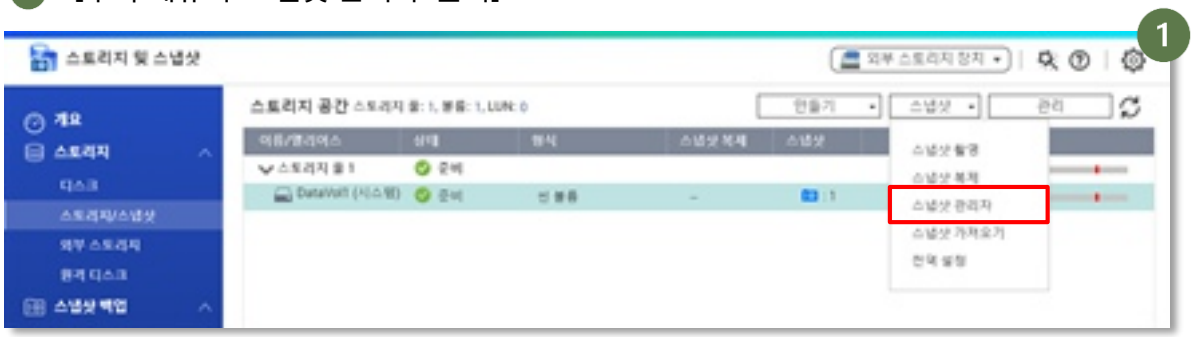


2 [좌측 메뉴 '스토리지'의 '스토리지/스냅샷' 클릭] > [스냅샷 촬영을 원하는 드라이브 클릭] > [우측 상단 '스냅샷' 클릭] > ['스냅샷 촬영' 클릭]

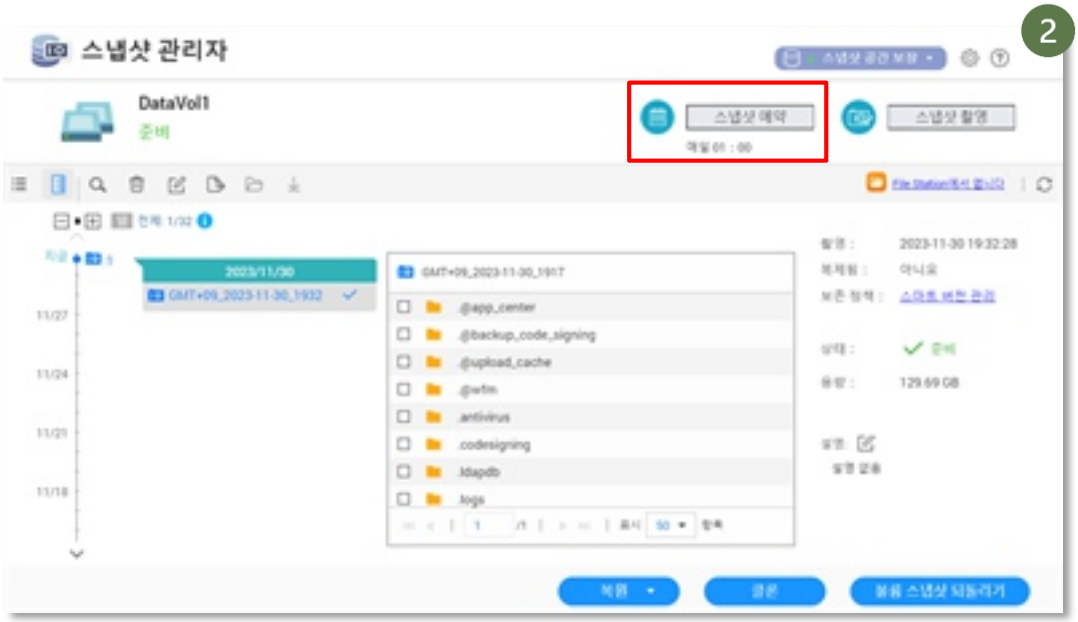
큐냅(QNAP)

스토리지 스냅샷 예약하기

1 [우측 메뉴의 '스냅샷 관리자' 클릭]



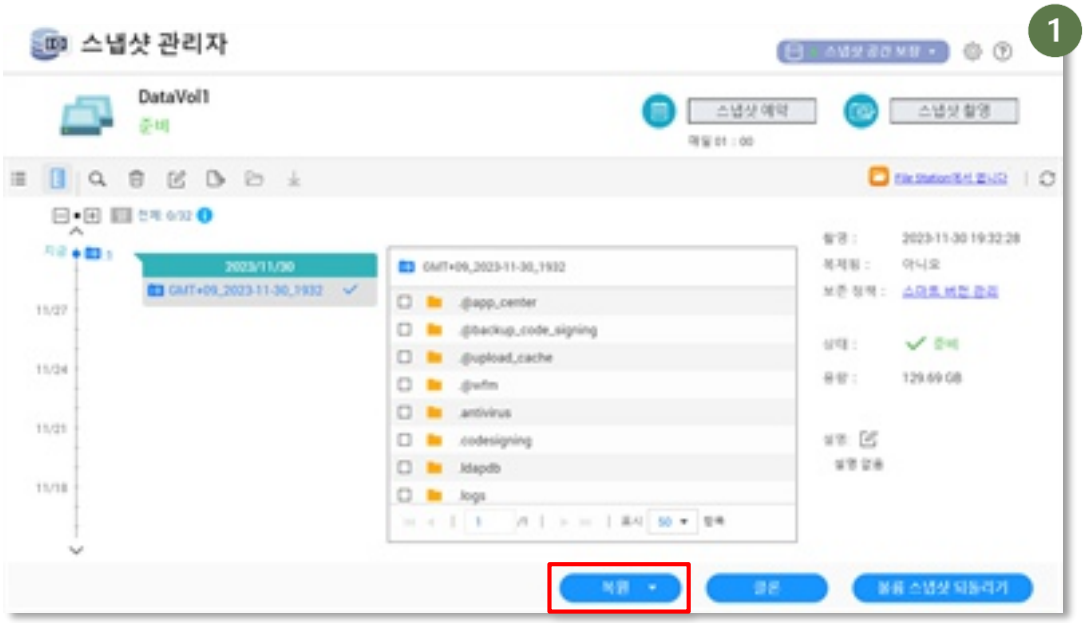
2 ['스냅샷 예약' 에서 스냅샷을 자동으로 촬영할 시간 설정 가능]



큐냅(QNAP)

스토리지 스냅샷 복원하기

1 [스냅샷 복원: '스냅샷 관리자'에서 복원할 시점의 스냅샷을 클릭한 후 하단의 '복원' 클릭]
* 스냅샷 복원의 경우 해당 시점으로 파일의 상태를 되돌리기 때문에 주의하여 실행합니다.



스냅샷과 백업의 차이

스냅샷 기술은 특정 시점의 데이터 상태를 기억하고 있다가 해당 시점으로 되돌리는 기술로, 데이터 자체를 여러 사본으로 만들어 별도 장소에 저장하는 '백업' 기술과는 차이가 있습니다. 스냅샷은 빠르고 용량을 적게 차지한다는 장점이 있지만, 스냅샷 이미지 자체가 손상되거나 NAS가 물리적으로 고장나는 경우 복구할 수 없다는 단점이 있습니다. 따라서 스냅샷은 백업에 비해 데이터의 안전성은 떨어진다는 한계가 있습니다.

QNAP에서는 Qsync라는 자체 소프트웨어를 통해 백업을 지원하고 있습니다.

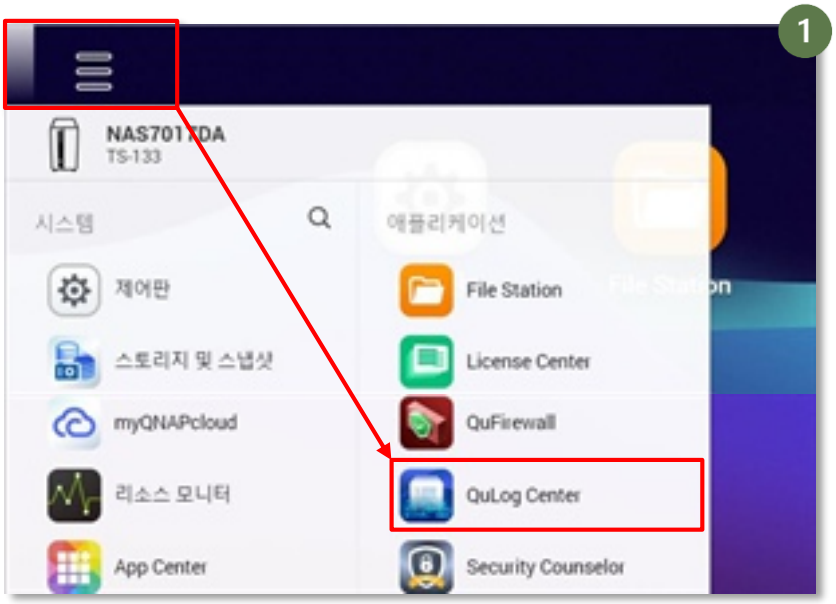
큐냅(QNAP)

7. 로그 관리 설정하기

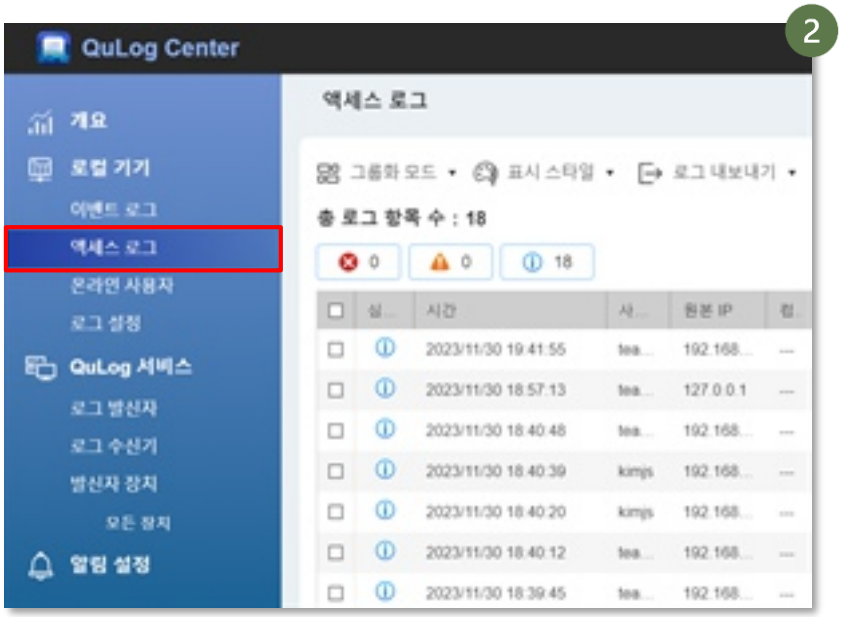
엑세스 로그 기능 사용하기

저장소에 누가, 언제, 어떤 파일을 올리고 받아갔는지 추적하는 방법을 안내합니다. 특히 자료 유출 시 책임자를 추적하는 데 도움이 될 수 있습니다.

1 ['메인 메뉴' 클릭] > ['QuLog Center' 클릭]



2 ['메뉴'에 '액세스 로그' 클릭]



큐냅(QNAP)

3 [우측 상단 '고급 검색'의 '동작'을 '삭제됨', '읽기', '쓰기', '복사됨', '이동됨', '추가됨' 등으로 지정하면 파일 추가/변경/삭제와 관련된 로그 확인 가능]

큐냅(QNAP)

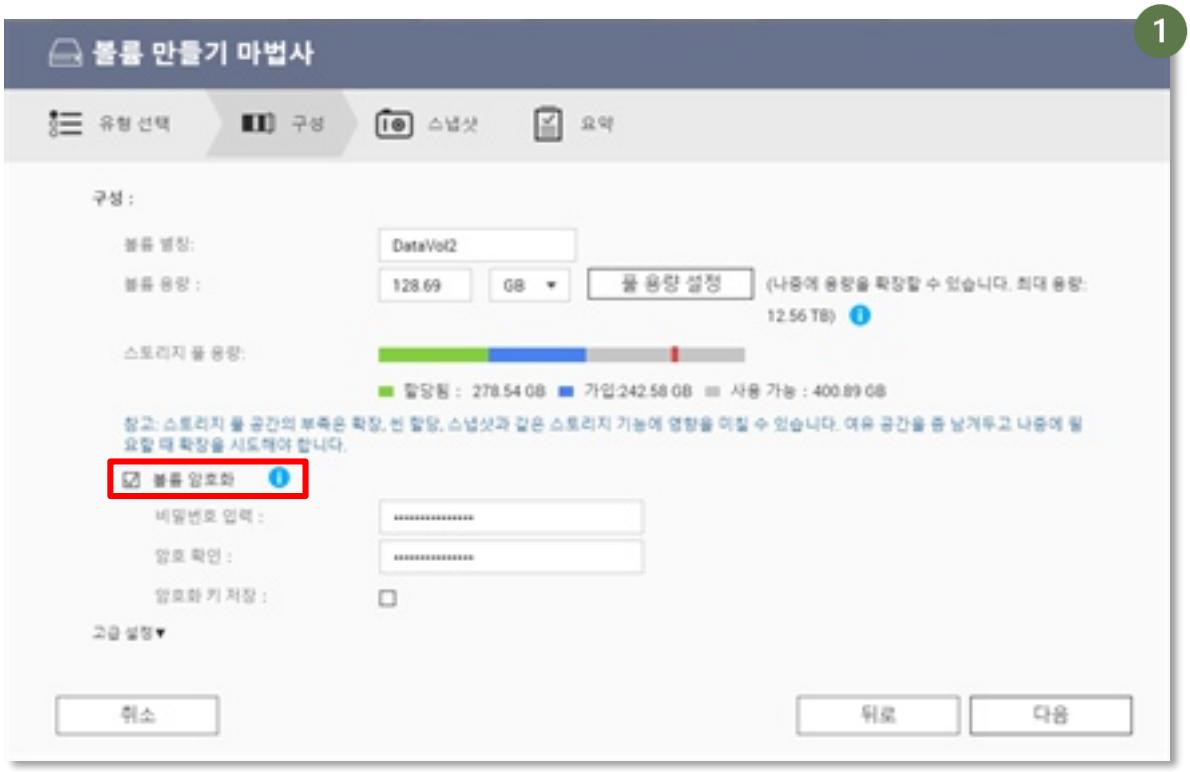
8. 데이터 암호화하기

데이터가 외부로 유출되어도 그 내용이 암호화되어 있다면 민감한 정보를 타인이 알게 되는 일을 막을 수 있습니다. 데이터 암호화란 일상적으로 사용되는 문자(평문)를 '암호키'라고 하는 값과 함께 계산해 암호문으로 변환하여 알아볼 수 없게 만드는 기술입니다. 암호문은 암호키를 가진 사람만이 그 내용을 알 수 있어 정보의 비밀을 유지할 수 있습니다.

디스크 볼륨 암호화하기

'볼륨' 단위로 암호화하는 방법입니다. 볼륨 생성 시에만 설정할 수 있기 때문에, 볼륨이 생성된 이후에는 볼륨 암호화를 할 수 없습니다.

1. [볼륨 생성 시 '볼륨 만들기 마법사'의 '구성'에서 '볼륨 암호화' 선택] > [디스크에 접근할 수 있는 비밀번호 입력 후 볼륨 만들기 절차 진행]



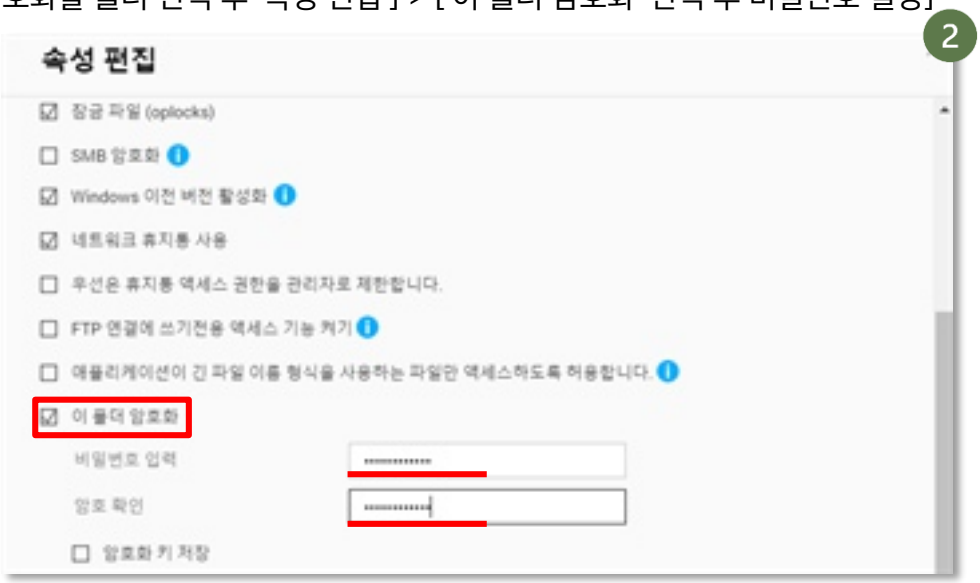
큐냅(QNAP)

공유 폴더 암호화하기

'공유 폴더' 단위로 암호화하는 방식입니다.

1 ['제어판' 실행] > [권한] > [공유 폴더]

2 [암호화할 폴더 선택 후 '속성 편집'] > ['이 폴더 암호화' 선택 후 비밀번호 설정]

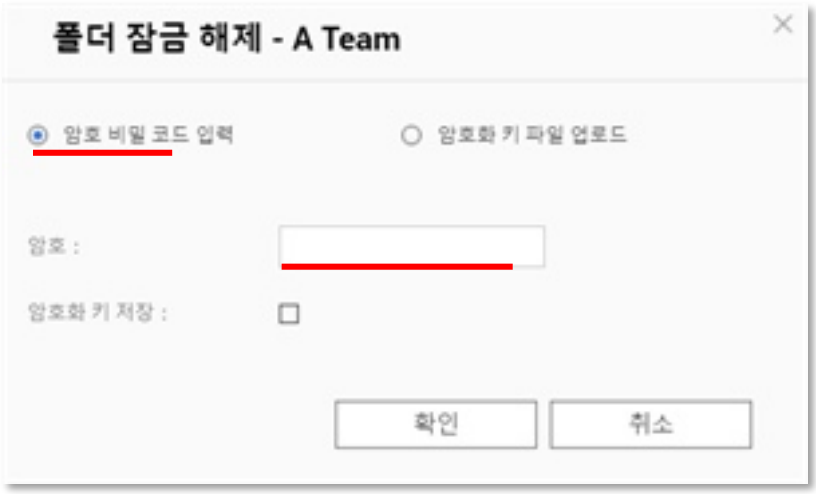


3 [암호화 방법: '열린 자물쇠' 아이콘 클릭 후 '잠금' 메뉴 '확인' 클릭]

큐냅(QNAP)

공유 폴더 복호화하기

1 [암호화 해제 방법: '잠긴 자물쇠' 아이콘 클릭 후 비밀번호 입력]

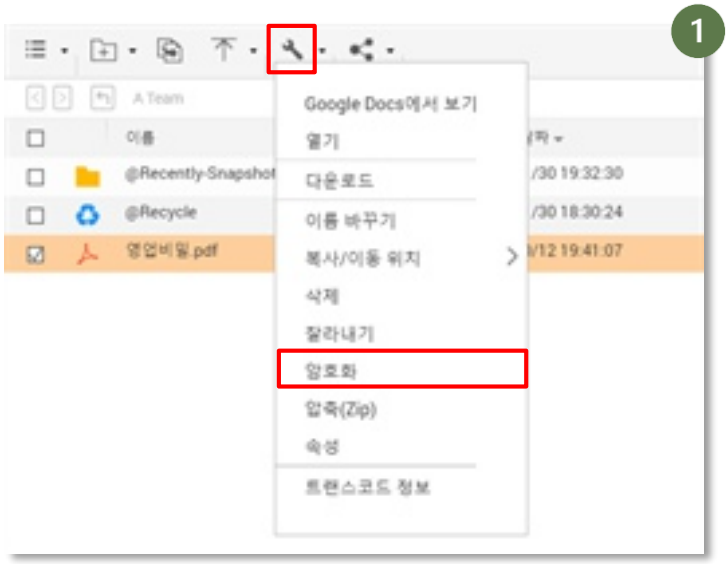


큐냅(QNAP)

파일 암호화하기

'개별 파일' 단위로 암호화하는 방식입니다.

1. [암호화 할 파일 클릭] > [상단 메뉴의 '작업 더보기' 클릭] > ['암호화' 클릭]



2. [비밀번호 입력 후 '확인' 클릭]

3. [암호화 해제 방법: '작업 더보기'에서 '암호 해독' 클릭 후 비밀번호 입력]

제2장 정보보안 실무자 보안수칙

II. 사무용 IT 장비

이번 장에서는 기업에서 공유기를 안전하게 사용할 수 있는 보안 설정 방안을 소개합니다. 공유기 보안 설정을 통해 회사 내 공유기를 안전하게 보호할 수 있습니다. 제품별로 할 수 있는 기본적인 보안 설정들에 대해 알아보겠습니다.

공유기 보안이 왜 필요한가요?

회사에서 무선 네트워크 도입을 위해 공유기를 이용하는 경우가 많습니다. 회사의 다양한 기기를 공유기에 연결하는 만큼 사이버 위협에 취약합니다. 따라서 회사의 보안을 위해 공유기를 안전하게 관리해야 합니다.

공유기의 비밀번호를 설정했는데도 추가적인 보안이 필요한가요?

공유기에 비밀번호를 설정하는 것만으로는 충분히 안전하지 않습니다. 회사 내의 정보들이 오가는 네트워크 장비인 만큼 공유기 비밀번호 설정 외에도 기기에서 제공하는 보안 기능들을 최대한 활용해야 합니다.

가이드라인에서 다루는 제품 확인하기

ipTIME The World Best Network Equipments

▲ ipTIME

tp-link

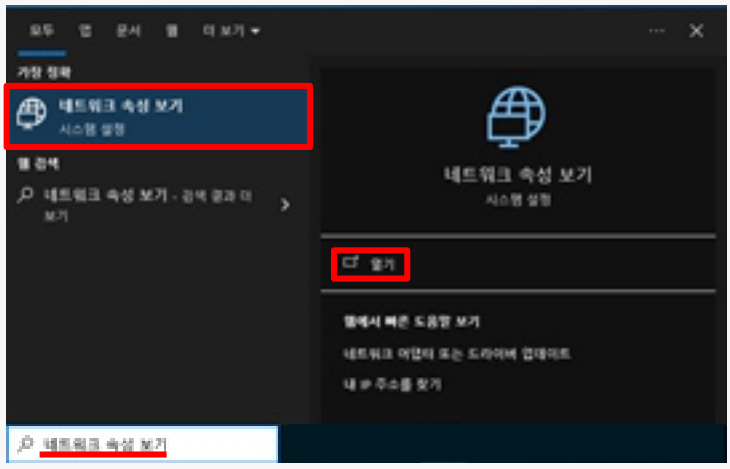
▲ TP-Link

관리자 페이지 접속 주소 알아보기

대부분의 공유기 보안 설정을 하기 위해서는 관리자 페이지로 접속해야 합니다. 이때, 제조사마다 설정해 놓은 기본 페이지 주소가 있지만, 접속이 되지 않을 경우 해당 주소를 찾아야 합니다.

Windows 10

[검색] > [네트워크 속성 보기'] > ['열기' 클릭] > ['기본 게이트웨이 주소' 확인]



Windows 11

[검색] > [네트워크 속성 보기] > ['열기' 클릭] > ['기본 게이트웨이 주소' 확인]

ipTIME

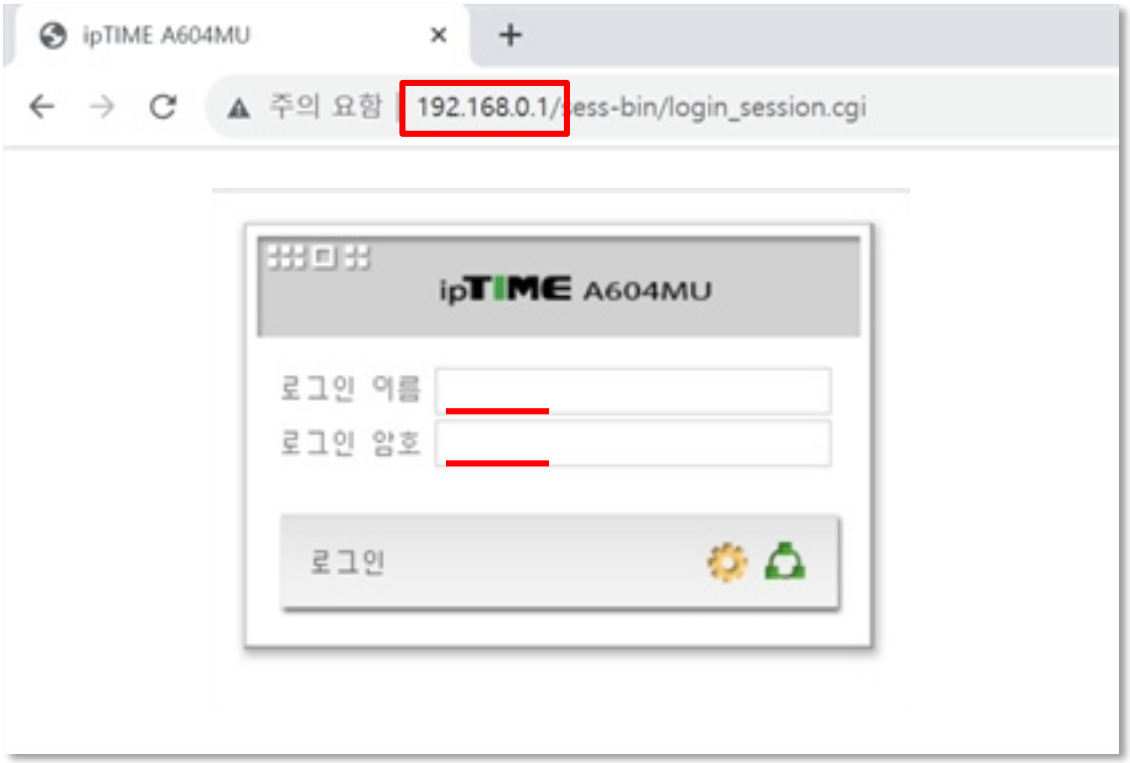
0. 관리자 페이지 접속하기

ipTIME 공유기의 경우 기본 접속 주소는 192.168.0.1입니다. 기기 내 설정이 다를 경우, 기본 게이트웨이를 주소로 관리자 페이지에 접속하실 수 있습니다.

브라우저에서 관리자 페이지 접속하기

1. [브라우저에서 'https://192.168.0.1 (관리자 페이지 접속 주소 기본값) 혹은 기본 게이트웨이 주소' 입력]

   * ipTIME의 초기 로그인 이름, 로그인 비밀번호는 admin / admin 입니다.



ipTIME

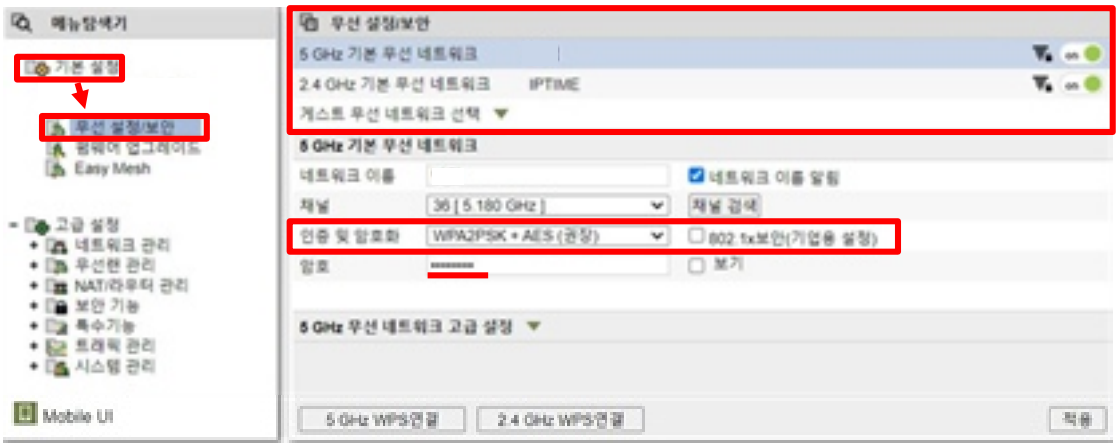
1. 공유기 비밀번호 관리하기

ipTIME 공유기 제품의 경우 초기 비밀번호가 없기 때문에 비밀번호를 별도로 설정하지 않을 경우 누구든지 제한 없이 접속할 수 있습니다. 이번 항목에서는 공유기의 비밀번호를 설정하는 방법에 대해 안내하겠습니다.

무선 네트워크 연결 시 비밀번호 설정하기

5 GHz 와 2.4 GHz 기본 무선 네트워크에 각각 비밀번호를 설정해야 합니다. 적용 완료 후 우측 상단 안테나 모양의 아이콘에 자물쇠 아이콘이 추가된 것을 확인할 수 있습니다.

1. [메뉴탐색기] > [기본 설정] > [무선 설정/보안] > ['WPA2PAK + AES (권장)' 선택] > [비밀번호입력]



바람직한 공유기 설치 위치

공유기의 경우 관리자 비밀번호와 공유기 비밀번호를 설정하더라도 실제 기기에서 초기화 버튼을 눌러 비밀번호를 초기화할 수 있습니다. 따라서 공유기는 쉽게 접근할 수 없는 장소에 두어야 합니다.

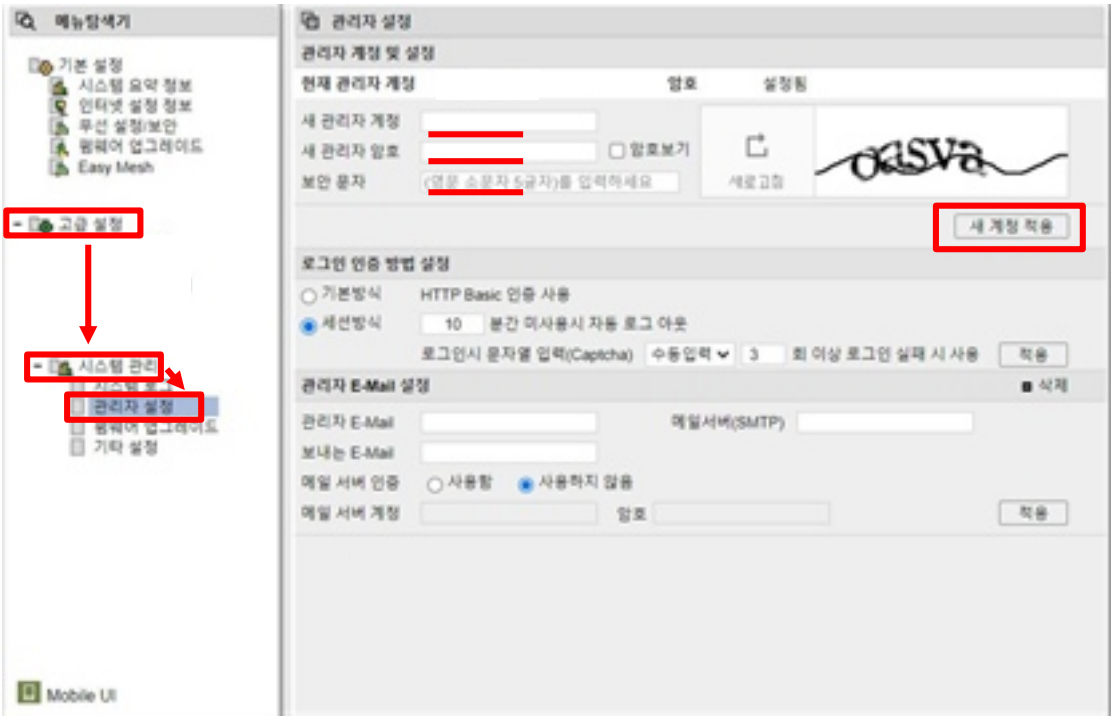
ipTIME

2. 관리자 계정 비밀번호 설정하기

관리자 비밀번호가 기본값으로 설정되어 있다면, 공유기에 연결된 이용자라면 누구든지 관리자 페이지에 접속해 공유기 설정을 변경할 수 있습니다. 이를 막기 위해 관리자 비밀번호를 변경해야 합니다.

계정 환경 설정하기

1. [메뉴 탐색기] > [고급 설정] > [시스템 관리] > ['관리자 설정' 클릭] > [관리자 계정 및 설정] > [새로 생성할 관리자 계정 ID와 암호를 입력] > [우측 '보안문자' 입력] > ['새 계정 적용' 클릭]



비밀번호 설정 시 유의사항

새로운 관리자 계정 생성 시 관리자 비밀번호는 영문, 숫자, 특수문자를 조합한 8자리 이상으로 설정해야 안전합니다.

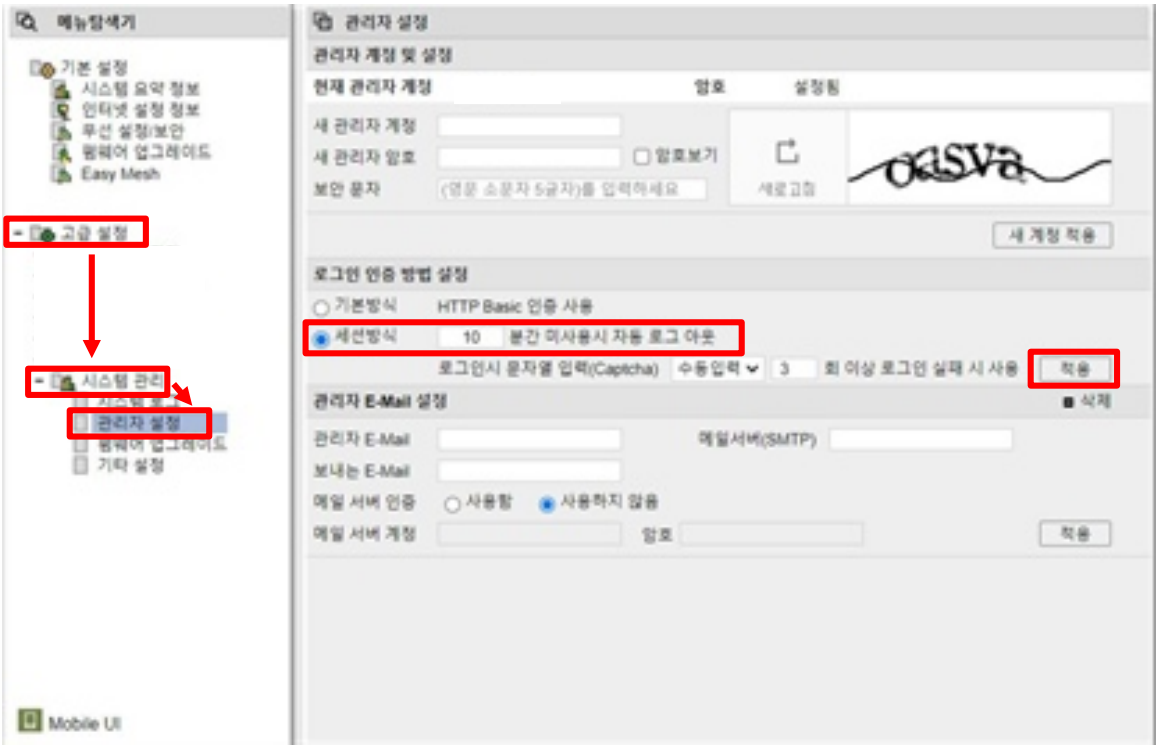
ipTIME

3. 자동 로그아웃 기능 설정하기

관리자가 관리자 페이지에 로그인 후 일정 시간 동안 작업이 없으면 자동으로 로그아웃이 되도록 하는 기능을 설정합니다. 해당 기능을 설정하면 관리자가 로그인 후 자리를 비우더라도 관리자가 아닌 사람이 관리자 페이지에 접근할 가능성을 낮출 수 있습니다.

로그인 후 미사용시 자동 로그아웃 설정하기

1. [설정] > [고급 설정] > [시스템 관리] > ['관리자 설정' 클릭] > [로그인 인증 방법 설정] > ['세션방식' 클릭] > [미사용 시 자동 로그아웃을 '10분 이하' 로 값 입력] > ['로그인 시 문자열 입력' 수동입력 - 3회 이상 로그인 실패 시 사용'으로 값 선택] > ['적용' 클릭]



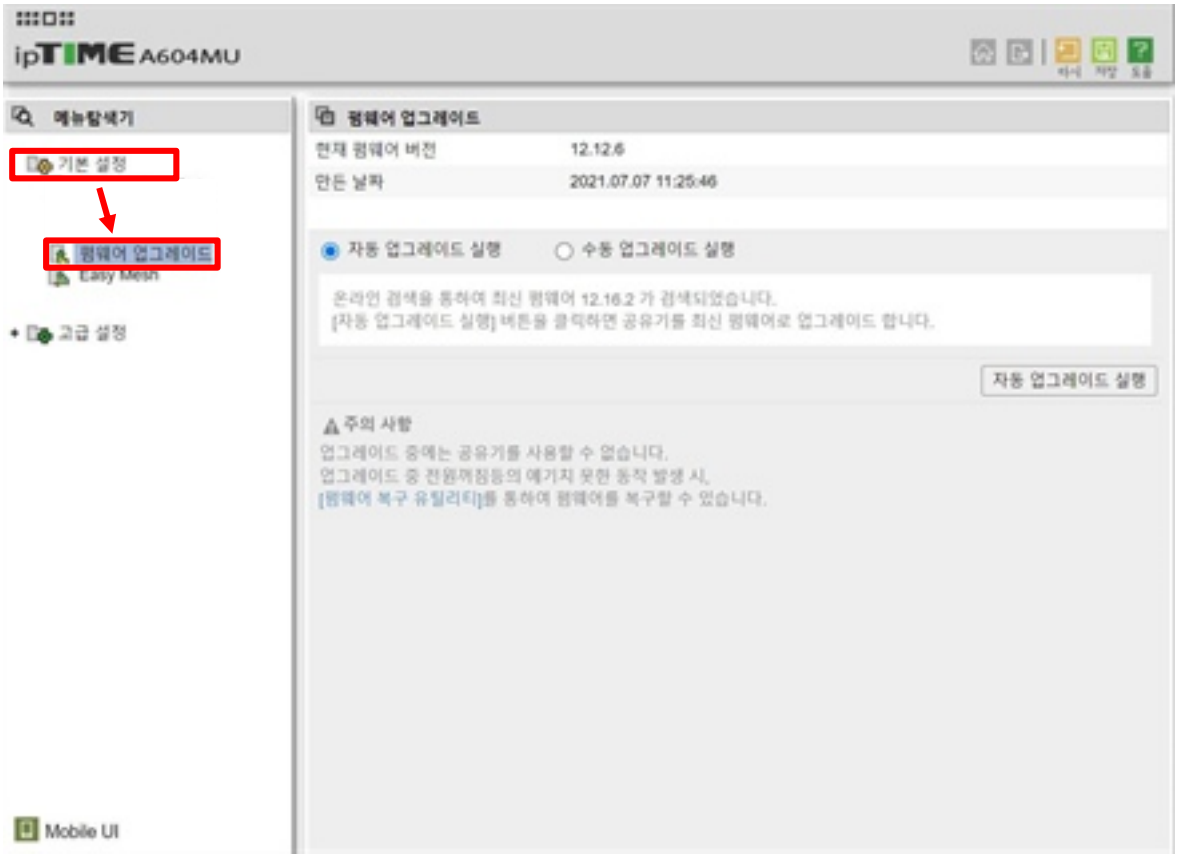
ipTIME

4. 공유기 보안 상태 설정하기

펌웨어 업그레이드 확인하기

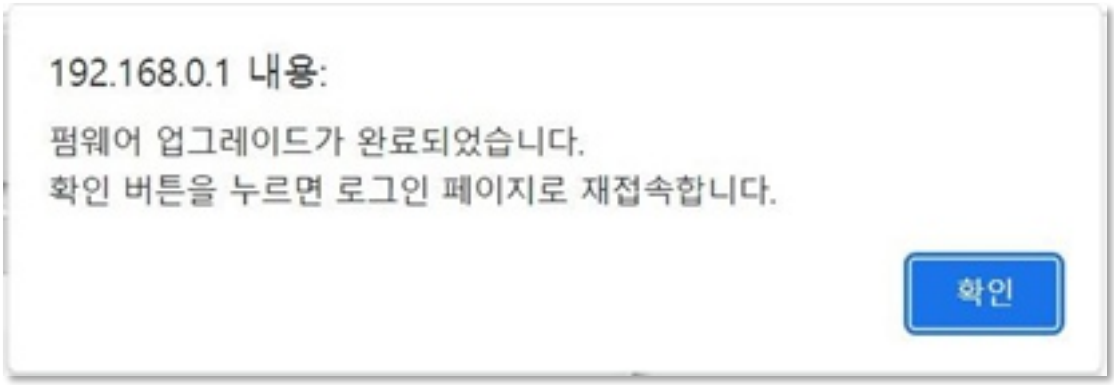
ipTIME 관리자 페이지에 접속해 공유기 펌웨어의 업데이트 상태를 확인할 수 있습니다.

1 [기본 설정] > ['펌웨어 업그레이드' 클릭] > ['자동 업그레이드 실행' 클릭]

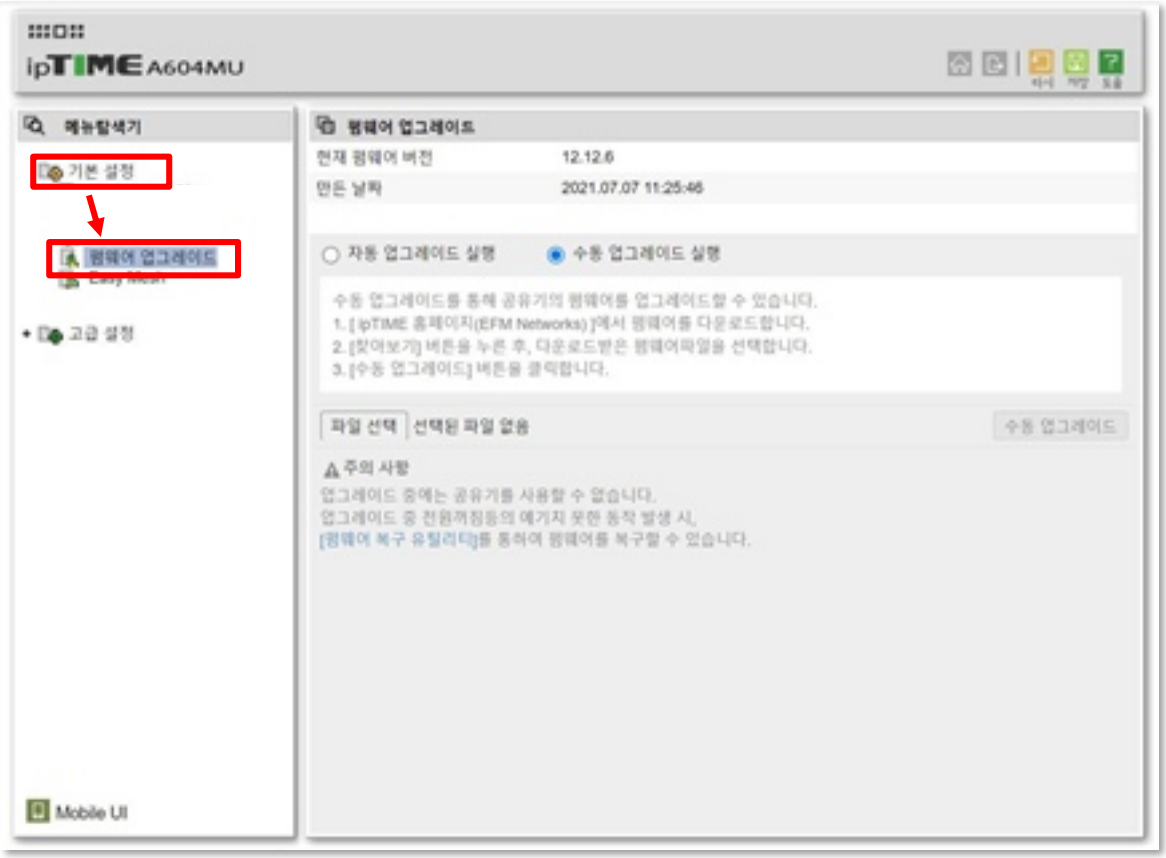


ipTIME

펌웨어 업그레이드가 완료되면 팝업창과 함께 로그인 페이지로 재접속하는 것을 확인할 수 있습니다.



자동 업그레이드가 아닌 수동으로도 업그레이드를 실행할 수 있습니다. 수동 업그레이드를 실행할 경우 로컬 파일을 업로드하는 방식을 통해 업그레이드를 진행할 수 있습니다.



ipTIME

ipTIME 보안 검사기로 점검하기

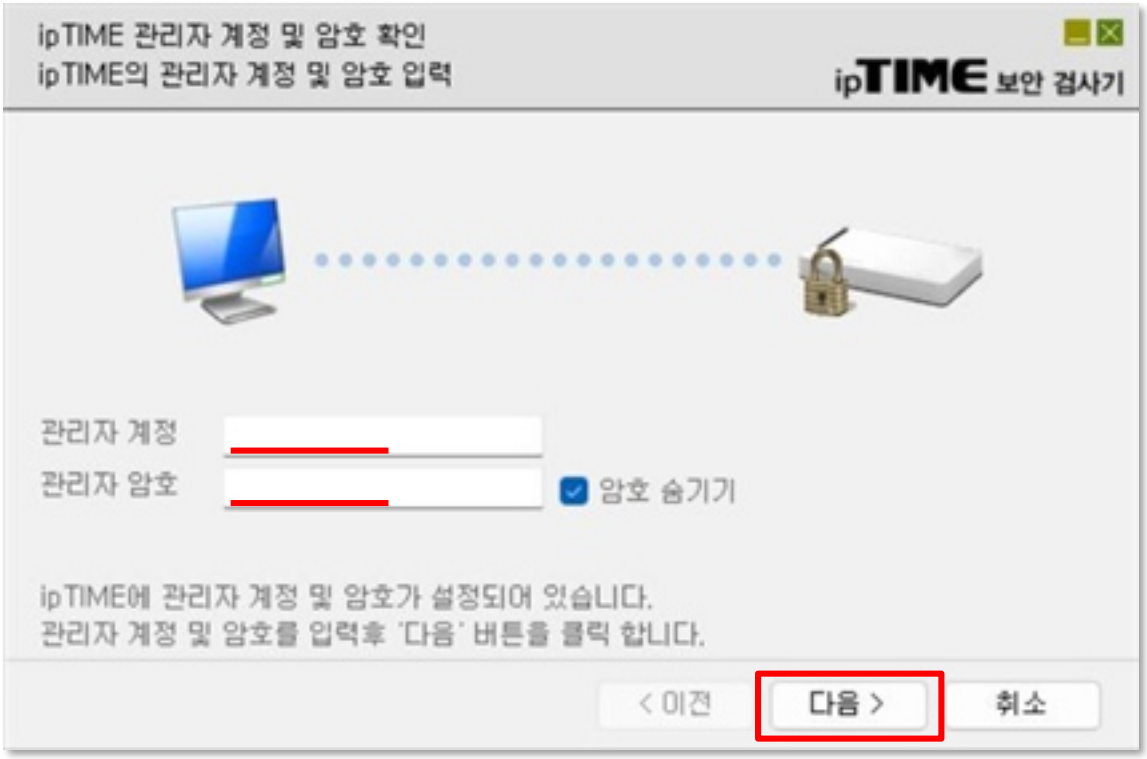
ipTIME에서는 ipTIME 보안 검사기 프로그램을 제공하고 있습니다. 이 프로그램을 통해 PC와 연결된 ipTIME 공유기의 보안 상태를 검사할 수 있습니다.

ipTIME 보안 검사기 프로그램은 ipTIME 공식 홈페이지에서 다운로드할 수 있습니다.

https://iptime.com/iptime/?pageid=4&page_id=126&dffid=3&mod=document&keyword=업그레이드&uid=16239 - IPTIME 보안 검사기 다운로드 링크

ipTIME

ipTIME에 관리자 계정 및 비밀번호가 설정되어 있다면, 관리자 계정과 비밀번호를 입력해야 검사를 시작할 수 있습니다.

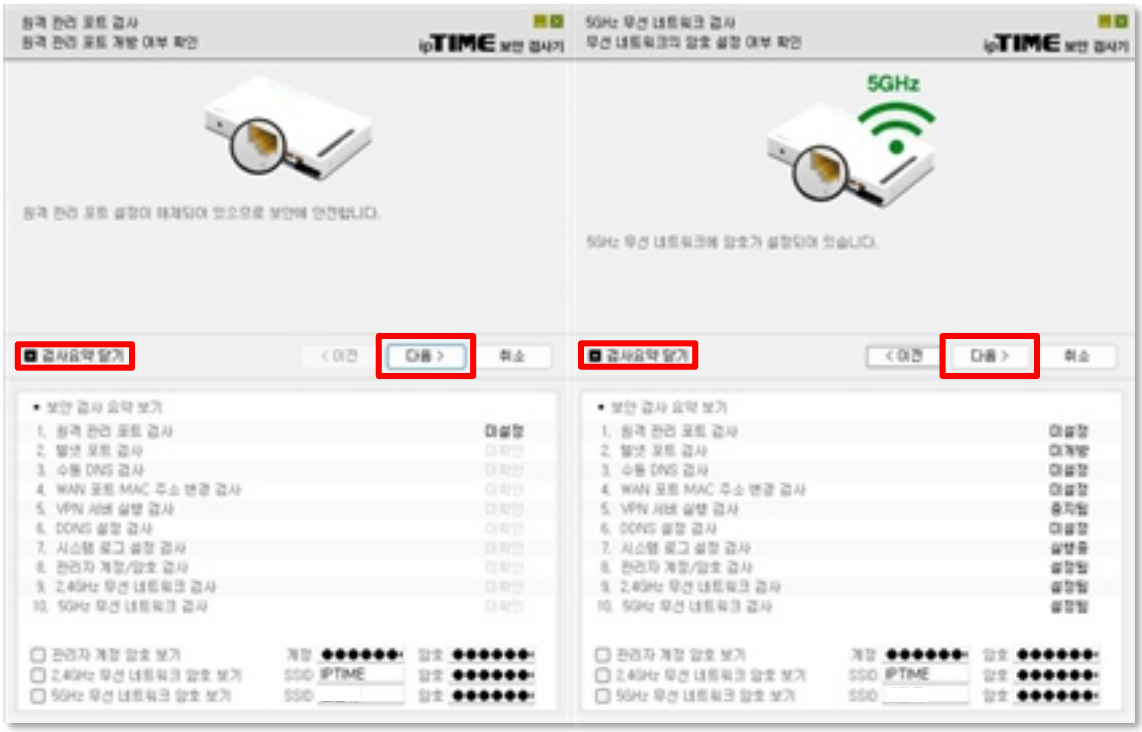


공유기와 PC 프로그램 간 연결이 완료되었다면, 다음과 같은 보안 검사를 진행할 수 있습니다.

보안 검사 항목	
원격 관리 포트 검사	DDNS 설정 검사
텔넷 포트 검사	시스템 로그 설정 검사
수동 DNS 검사	관리자 계정/암호 검사
WAN 포트 MAC 주소 변경 검사	2.4GHz 무선 네트워크 검사
VPN 서버 실행 검사	5GHz 무선 네트워크 검사

ipTIME

보안 검사기의 항목별 검사를 진행하면서, 왼쪽 하단의 검사요약 보기를 통해 전체 검사 결과를 간단하게 확인하게 확인할 수 있습니다.



권장 보안 검사 항목별로 설정 권장사항은 다음과 같습니다.

권장 보안 검사 항목별 권장사항	
원격 관리 포트 검사	직접 설정한 경우가 아니라면 '사용하지 않음' 선택
수동 DNS 검사	직접 설정한 경우가 아니라면 '수동 DNS 설정 해제' 선택
WAN 포트 MAC 주소 변경 검사	1. 직접 설정한 경우, '변경된 WAN 포트 MAC 주소를 그대로 사용함' 선택 2. 직접 설정한 경우가 아니라면, '변경된 WAN 포트 MAC 주소 해제' 선택
VPN 서버 실행 검사	직접 실행한 경우가 아니라면 'VPN 서버 실행 중단' 선택 - 직접 등록한 사용자 계정이 아닐 경우 '등록된 사용자 계정' 삭제
DDNS 설정 검사	직접 등록한 주소가 아니면 '등록된 DDNS 호스트' 삭제
시스템 로그 설정 검사	공유기 보안 확인을 위해 '시스템 로그 실행' 선택
관리자 계정/암호 검사	관리자 비밀번호가 없거나 기본 설정인 경우, 새로운 계정/비밀번호 입력

ipTIME

10가지 항목의 보안 검사가 완료되면 보안에 취약한 항목의 개수를 확인할 수 있습니다. 또한, 검사요약 보기 버튼을 통해 자세한 내용을 확인할 수 있습니다.

TP-Link

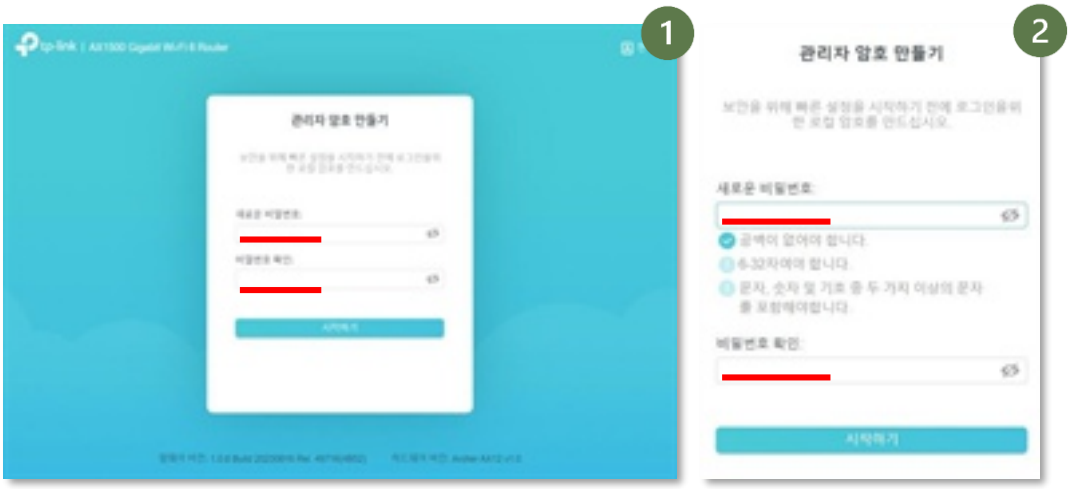
0. 관리자 페이지 접속하기

TP-Link 공유기의 경우 기본 접속 주소는 192.168.0.1입니다. 하지만, 기기 내 설정이 다를 경우, 기본 게이트웨이를 주소로 관리자 페이지에 접속하실 수 있습니다.

브라우저에서 관리자 페이지 접속하기

TP-Link 공유기 설치 이후 처음 관리자 페이지에 접속한 경우, 관리자 비밀번호를 만든 후에 공유기 설정 페이지로 들어갈 수 있습니다.

1. [사용하는 브라우저에서 '192.168.0.1 (관리자 페이지 접속 주소 기본값) 혹은 회사 게이트웨이 주소' 입력]
2. [관리자 암호 만들기] > ['새로운 비밀번호' 입력] > ['비밀번호 확인' 입력] > [로컬 암호로 로그인]



TP-Link

공유기 최초 설정 시 유의사항

관리자 페이지에 최초로 접속해 관리자 비밀번호를 설정하는 경우, 공유기 접속 비밀번호 또한 설정할 수 있습니다. 이때, 무선 공유기 비밀번호는 문자, 숫자 및 기호를 포함한 10자 이상의 안전한 비밀번호로 변경할 것을 권장합니다.

TP-Link

1. 공유기 비밀번호 관리하기

공유기에 비밀번호를 설정하지 않을 경우 누구든지 제한 없이 접속할 수 있습니다. 이번 항목에서는 공유기의 비밀번호를 설정하는 방법에 대해 안내하겠습니다.

보안 설정 및 비밀번호 설정하기

1 보안 설정: [무선] > [무선 설정] > [보안] > ['WPA2-PSK[AES]' 선택]
비밀번호 설정: [무선] > [무선 설정] > ['비밀번호' 입력]

Wi-Fi 보안 표준

WPA2-PSK[AES] 보안 방식은 Wi-Fi Alliance에서 표준으로 지정한 강력한 무선 네트워크 보안 표준입니다.

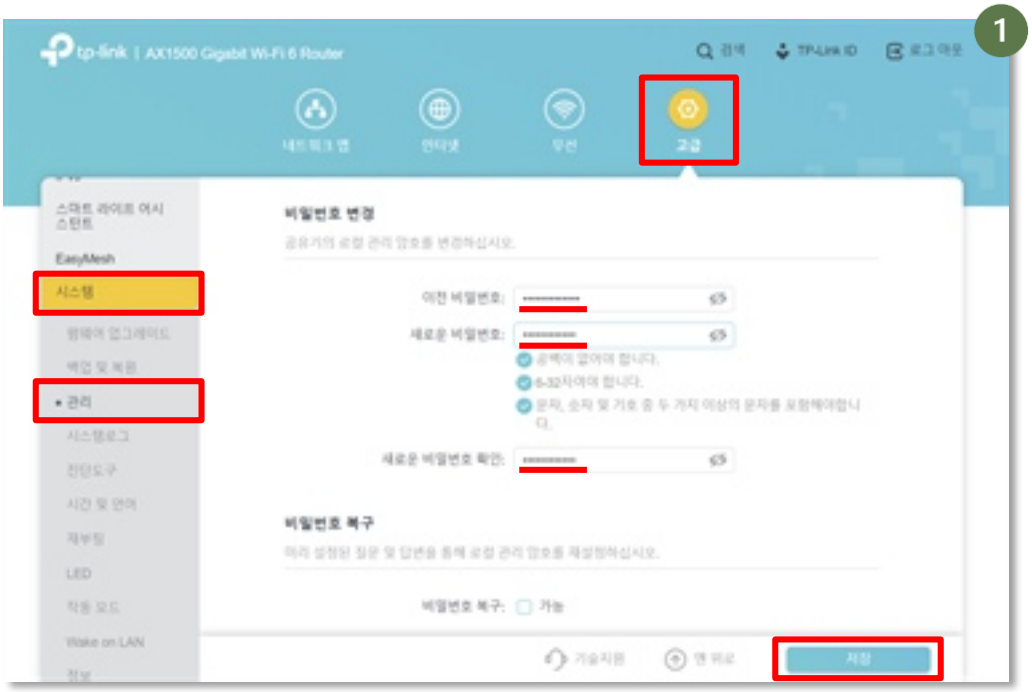
TP-Link

2. 관리자 계정 비밀번호 설정하기

관리자 비밀번호가 기본값으로 설정되어 있다면, 공유기에 연결된 이용자라면 누구든지 관리자 페이지에 접속해 공유기 설정을 변경할 수 있습니다. 이를 막기 위해 관리자 비밀번호를 변경해야 합니다.

공유기 로컬 관리 암호 변경하기

1. [고급] > [시스템] > ['관리' 클릭] > [비밀번호 변경] > [새로운 비밀번호 입력] > [오른쪽 하단 '저장' 클릭]



비밀번호 설정 시 유의사항

TP-Link 공유기에서는 기본적으로 비밀번호 설정 시 다음과 같이 제한을 두고 있습니다.

① 공백이 없어야 합니다.
② 6-32자여야 합니다.
③ 문자, 숫자 및 기호 중 두 가지 이상의 문자를 포함해야 합니다.

하지만 이 외에도, 동일한 문자나 숫자(예:1111,aaaa 등)나 반복된 문자나 숫자(예:1234,qwer 등) 로 설정하지 않는 것을 권장합니다.

TP-Link

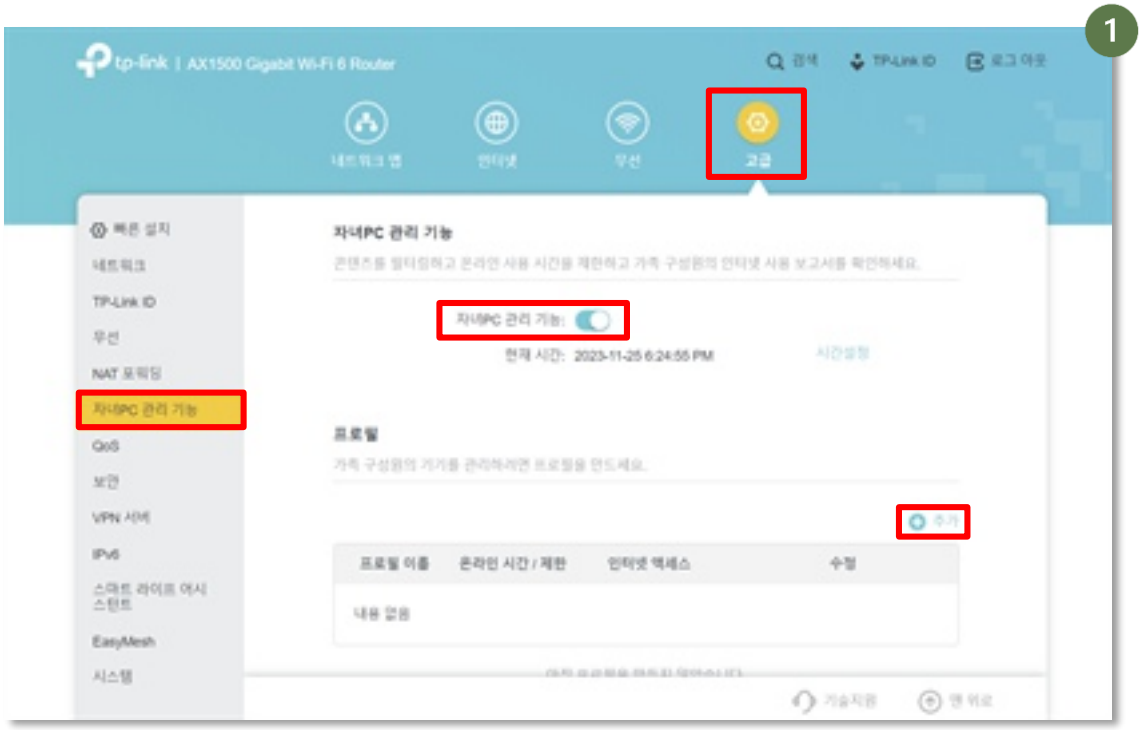
3. 공유기 보안 상태 설정하기

공유기에서 기본적으로 제공하는 보안설정을 활용하여 공유기의 보안성을 높일 수 있습니다.

자녀 PC 관리기능 활용하기

TP-Link에서 제공하는 '자녀 PC 관리 기능'을 이용하면 공유기에 연결된 기기에 대해 시간과 콘텐츠를 기준으로 접근 제한 설정을 할 수 있습니다. 이를 통해 회사 PC 사용자가 허용되지 않은 사이트에 접속하거나, 지정된 시간 외에 인터넷을 사용하는 것을 막을 수 있습니다.

1 [고급] > [자녀PC 관리 기능] > ['자녀 PC 관리 기능' 활성화] > ['추가' 클릭]

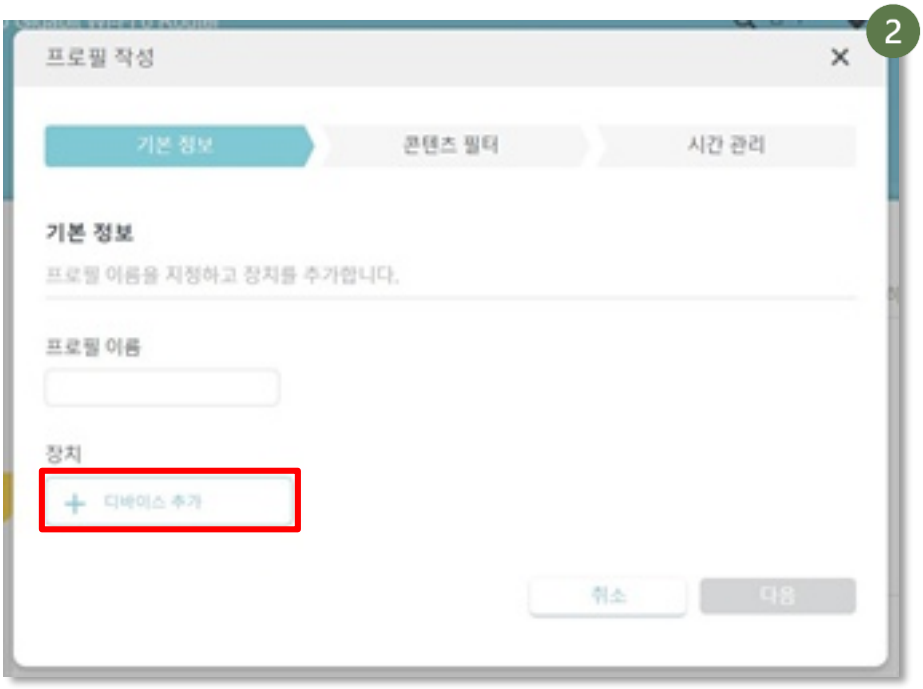


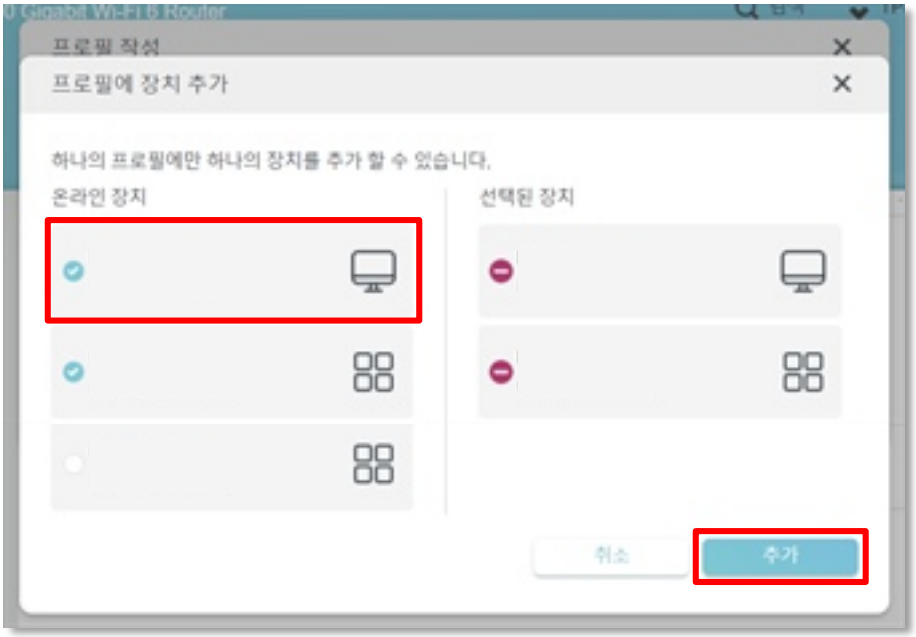
TP-Link

관리 대상 기기 추가하기

기본 정보에서는 관리할 PC를 추가할 수 있습니다. 현재 네트워크에 연결되어 있는 장치가 표시됩니다.

2 ['디바이스 추가' 클릭] > [추가할 '온라인 장치' 클릭] > ['추가' 클릭]

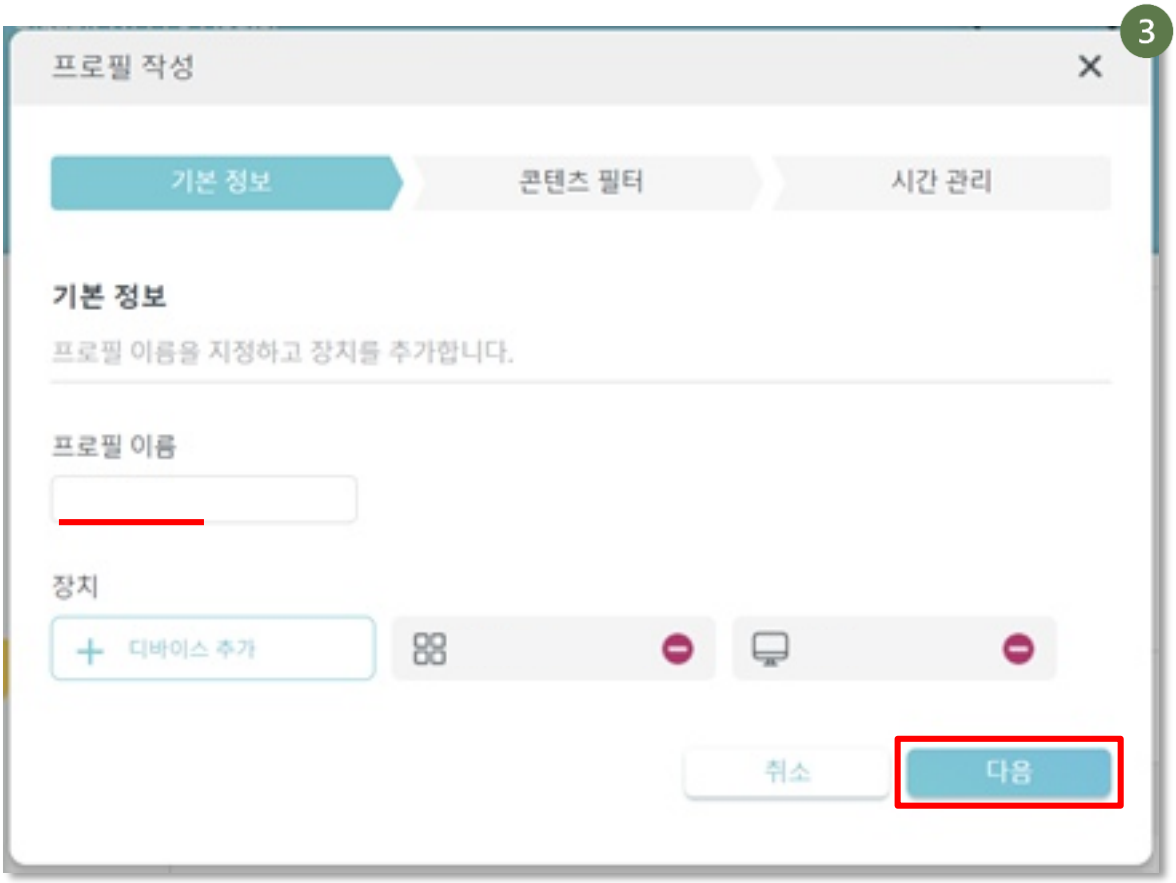




TP-Link

관리 대상 기기 프로필 추가하기

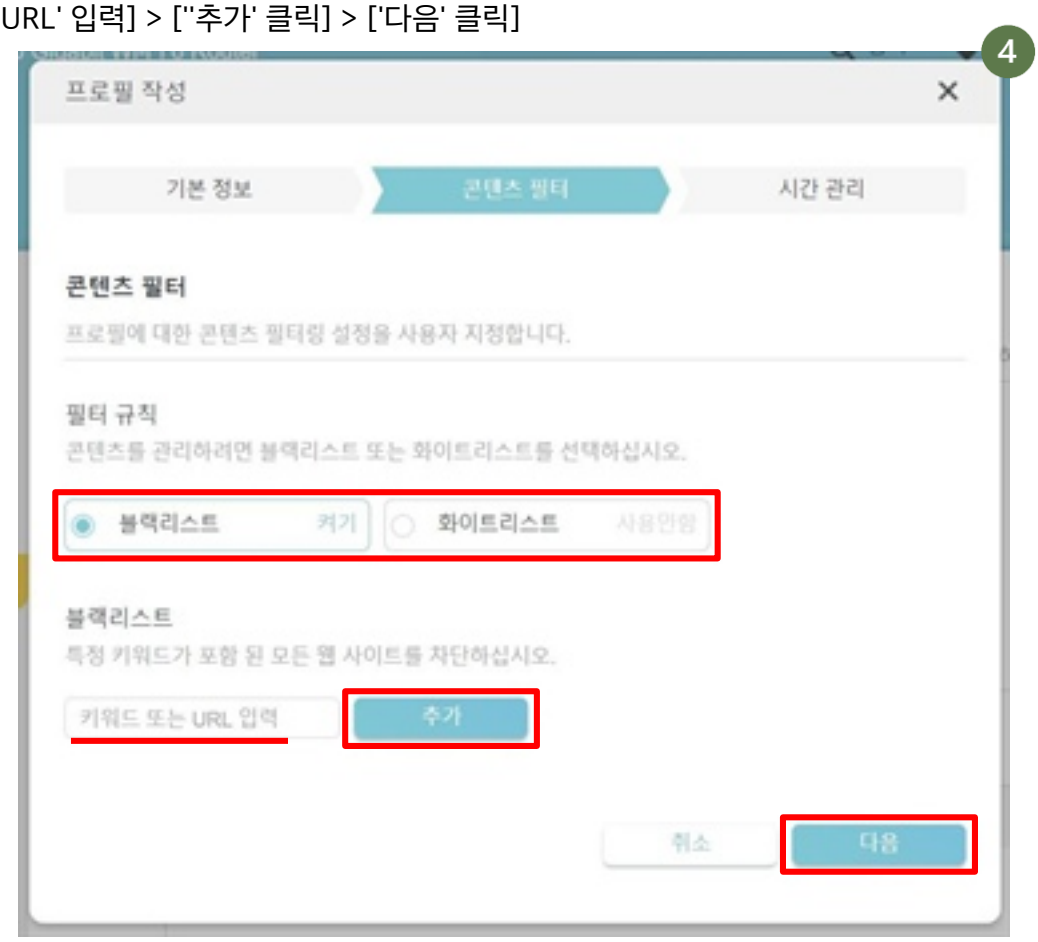
3 ['프로필 이름' 입력] > ['다음' 클릭]



TP-Link

콘텐츠 필터 기능 이용하기

4 [필터 규칙 (블랙리스트/화이트리스트) 클릭] > [차단/허용할 사이트에 대한 '키워드 또는 URL' 입력] > ['추가' 클릭] > ['다음' 클릭]



콘텐츠 필터 기능이 무엇인가요?

콘텐츠 필터 기능은 특정 키워드가 포함된 웹 사이트를 차단하는 블랙리스트 기능과 특정 키워드가 포함된 웹 사이트만 허용할 수 있는 화이트리스트 기능을 제공하고 있습니다.

블랙리스트 방식은 기본 정책이 모두 허용인 상황에서 예외적으로 차단 대상을 지정하는 방식입니다.

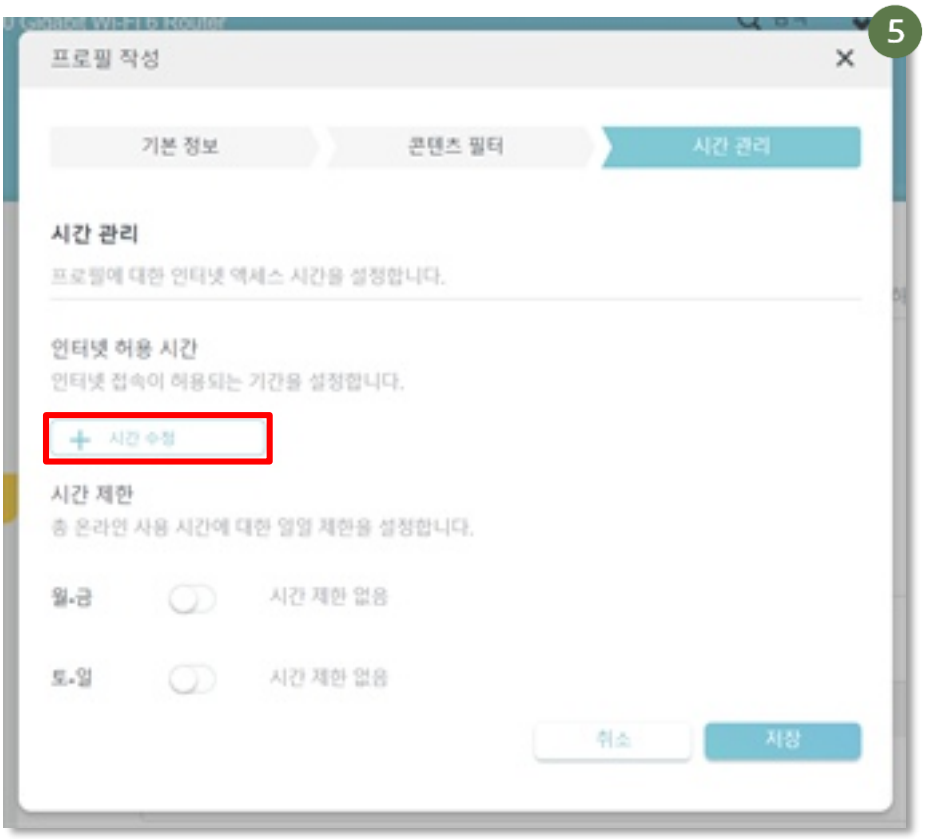
화이트리스트 방식은 기본 정책이 모두 차단인 상황에서 예외적으로 허용 대상을 지정하는 방식입니다.

차단하거나 허용할 사이트에 대한 키워드 또는 URL을 필요에 따라 입력해 추가하여 관리하는 PC가 특정 웹사이트 접근하는 것을 제한할 수 있습니다.

TP-Link

시간 관리 기능 이용하기

5 [시간 관리] > [인터넷 허용 시간] > ['시간 수정' 클릭]



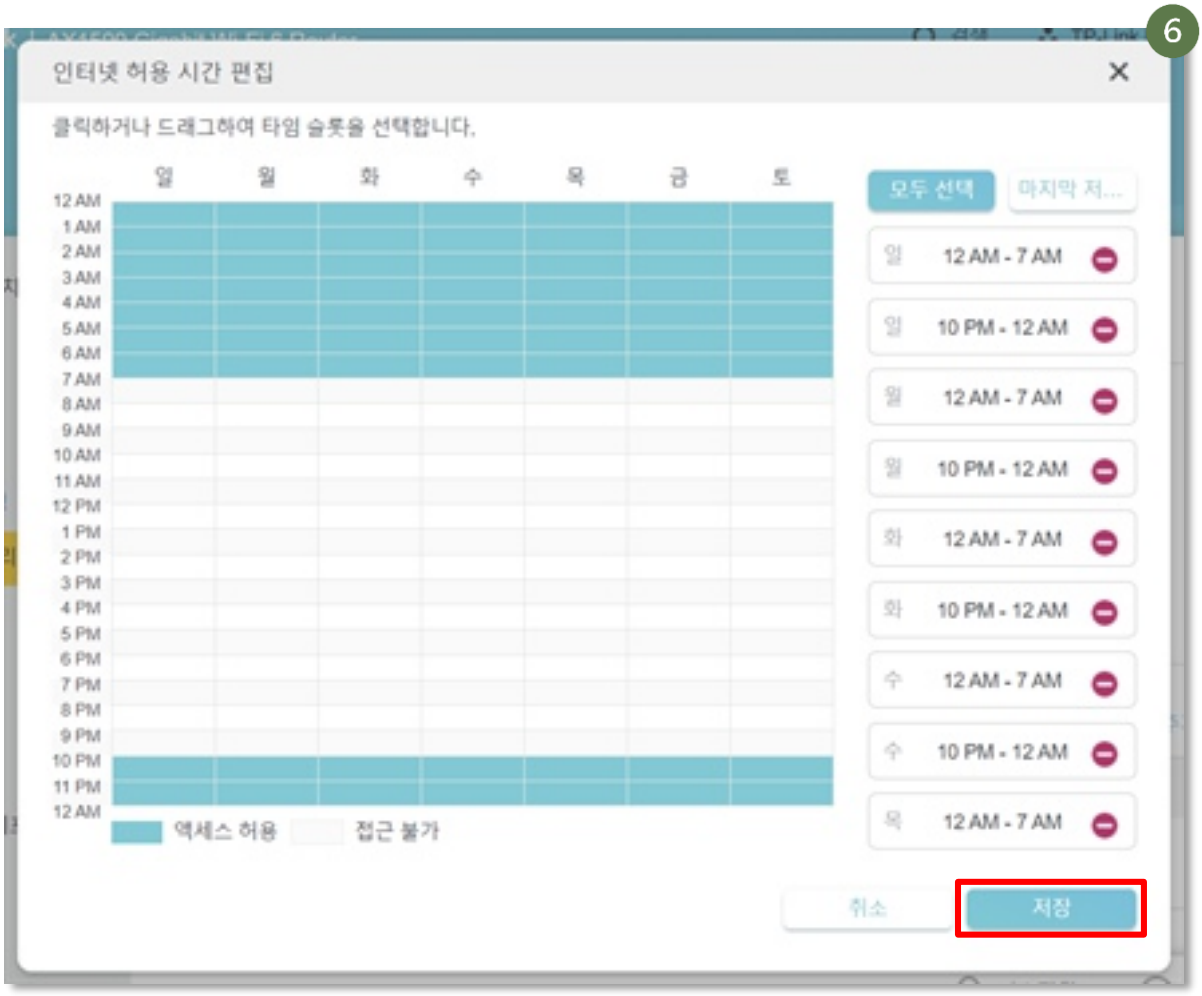
시간 관리 기능이란?

시간 관리 기능을 통해 공유기에 연결된 기기가 인터넷에 접속할 수 있는 시간대를 설정하여, 업무 시간 외 인터넷 접속을 제한할 수 있습니다.

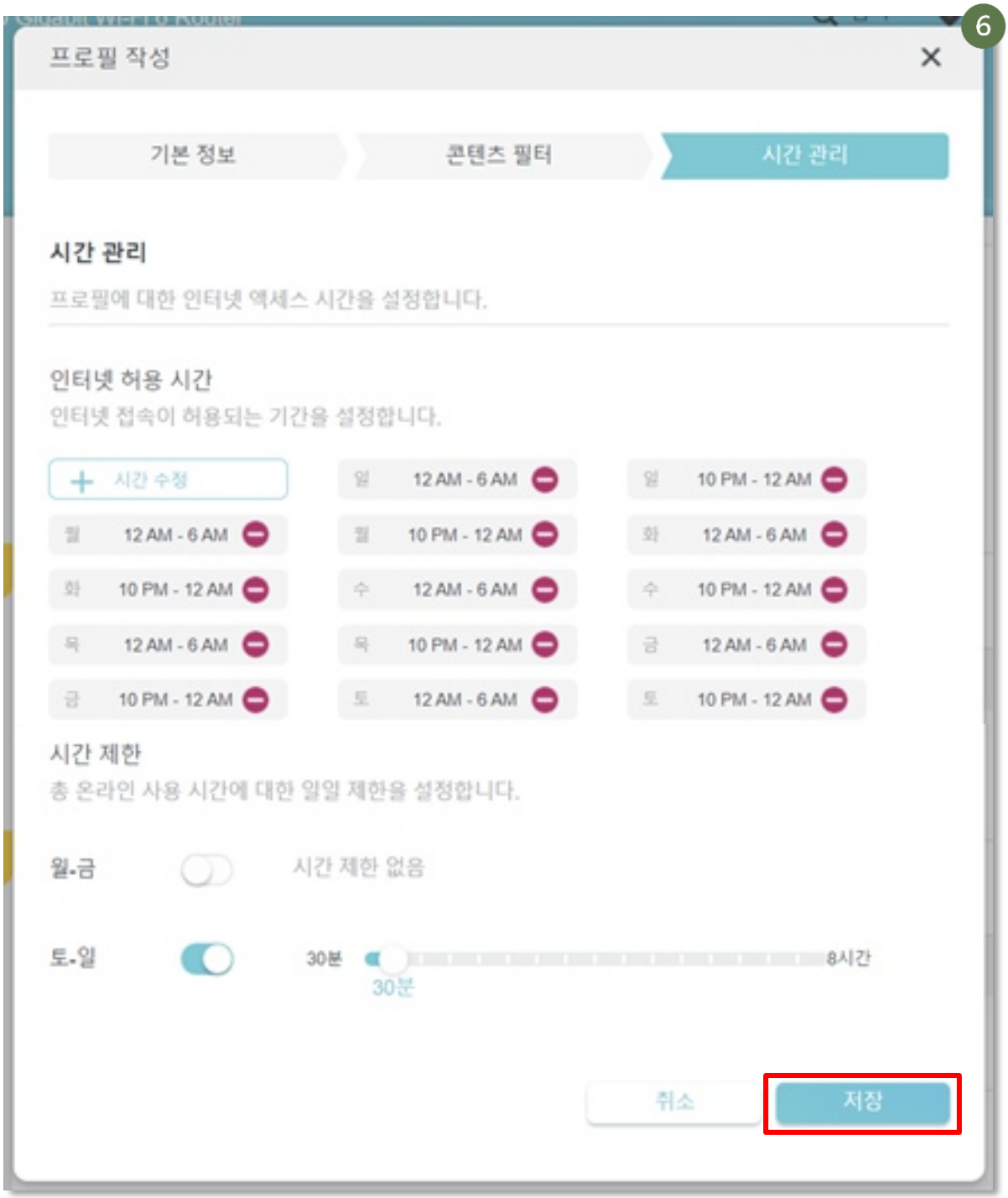
인터넷 허용 시간을 설정하지 않을 경우 시간표가 설정되지 않아 해당 프로필은 모든 시간대에 인터넷에 접근할 수 없습니다. '월-금', '토-일'과 같은 사전 설정을 이용해도 좋습니다.

TP-Link

6 [시간 수정] > [인터넷 허용 시간 편집] > ['타임 슬롯' 클릭] > ['저장' 클릭] > [한 번 더 '저장' 클릭]

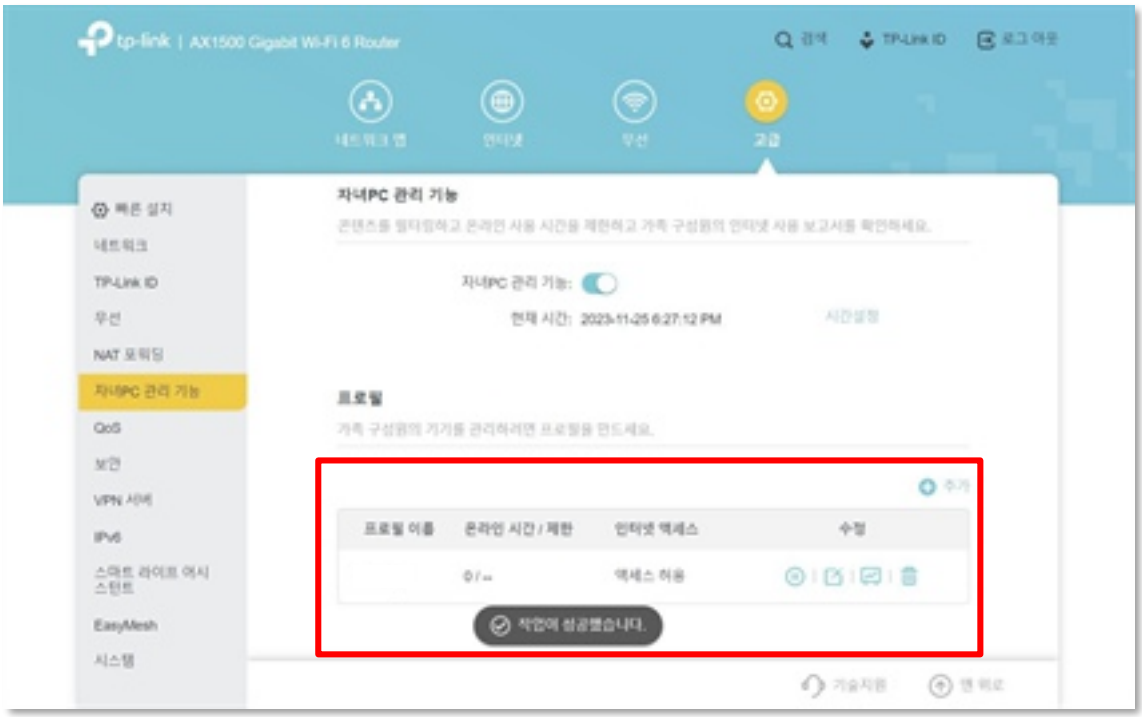


TP-Link


6
프로필 작성
기본 정보
콘텐츠 필터
시간 관리
시간 관리
프로필에 대한 인터넷 액세스 시간을 설정합니다.
인터넷 허용 시간
인터넷 접속이 허용되는 기간을 설정합니다.
+ 시간 수정
일 12 AM - 6 AM
일 10 PM - 12 AM
월 12 AM - 6 AM
월 10 PM - 12 AM
화 12 AM - 6 AM
화 10 PM - 12 AM
수 12 AM - 6 AM
수 10 PM - 12 AM
목 12 AM - 6 AM
목 10 PM - 12 AM
금 12 AM - 6 AM
금 10 PM - 12 AM
토 12 AM - 6 AM
토 10 PM - 12 AM
시간 제한
총 온라인 사용 시간에 대한 일일 제한을 설정합니다.
월-금
시간 제한 없음
토-일
30분
8시간
30분
취소
저장

TP-Link

설정을 마치면, 다음과 같이 기기가 추가된 것을 확인할 수 있습니다.

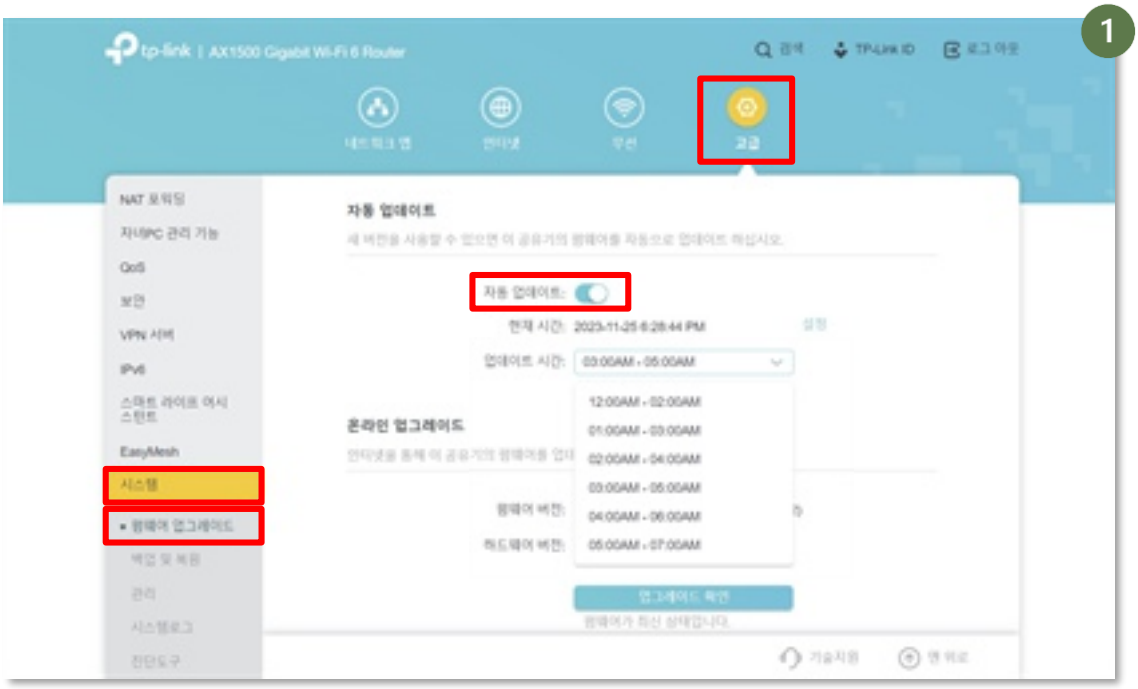


TP-Link

펌웨어 업그레이드 확인하기

자동 업데이트 기능을 활성화하여 제조사에서 제공하는 펌웨어 업데이트를 자동화할 수 있습니다. 업데이트 시간이 근무 환경에 지장이 가지 않도록 자동 업데이트 시간을 새벽 시간대에 설정하는 것을 권장합니다.

1. [고급] > [시스템] > [펌웨어 업그레이드] > [자동 업데이트] > ['자동 업데이트' 활성화] > ['업데이트 시간' 선택]

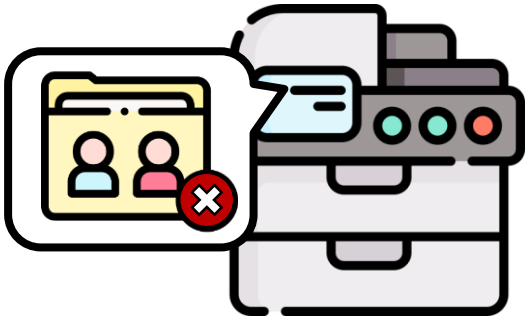


이것만은 지키자!

행동수칙

복합기 편

1



출력매체(복합기 등) 내 공유 폴더를 사용하지 않아요!

공유 폴더를 통해 민감한 정보가 의도하지 않은 사람에게 전달되거나, 악성코드가 공유 폴더 네트워크를 통해 전파될 위험이 있습니다. 중요한 정보는 개인 폴더나 보안이 강화된 공간에 보관해야 합니다.

2

USB와 같은 이동식 저장매체를 사용하지 않아요!

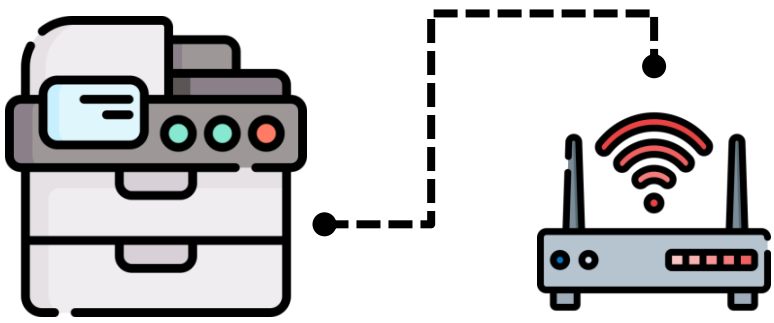
이동식 저장매체는 분실, 도난 등으로 데이터가 유출될 수 있고 잠재적인 보안 위협이 될 수 있습니다. 중요한 데이터는 안전한 내부 네트워크, 클라우드 서비스를 통해 관리해야 합니다.

이것만은 지키자!

행동수칙

복합기 편

3



복합기 네트워크를 공유기로 연결해요!

복합기를 공유기와 연결하여 사용하면, 복합기가 회사 내부 네트워크에서만 작동하게 되어 외부의 불필요한 접근을 차단할 수 있습니다. 이를 통해 해킹 및 데이터 유출 위험을 줄이고, 회사의 중요 정보를 보호할 수 있습니다.

이번 장에서는 회사에서 문서 출력을 위해 사용하는 기기인 복합기를 안전하게 사용하는 방법을 안내합니다. 대표적인 복합기 제조사인 신도리코, 캐논, 삼성의 복합기 보안 설정을 다룹니다.

복합기란 무엇인가요?

복합기는 여러 사무용 기기의 기능을 한데 모은 제품을 말합니다. 예를 들어 문서의 복사와 스캔 기능, 컴퓨터 파일 인쇄 기능, 팩스 전송 기능 등을 한 기계에서 모두 할 수 있습니다.

복합기 보안은 왜 해야할까요?

회사에서 사용되는 문서는 영업에 관한 중요한 정보를 담고있는 경우가 많습니다. 복합기 보안이 중요한 이유도 복합기가 회사의 문서를 처리하고 저장하는 장비이기 때문입니다. 복합기는 복사, 인쇄, 스캔, 팩스 등 다양한 작업을 처리하면서 그 문서를 일시적으로 저장합니다. 이렇게 저장된 데이터를 적절하게 관리하지 않으면 외부로 유출될 위험이 있습니다.

가이드라인에서 다루는 제품 확인하기

▲ 신도리코(Sindoh)　▲ 캐논(Canon)　▲ 삼성(Samsung)

신도리코(Sindoh)

1. 관리자 패스워드 설정하기

복합기의 관리자 기본 패스워드를 변경하는 것은 필수입니다. 복합기의 초기 관리자 아이디, 패스워드는 누구나 쉽게 알아낼 수 있습니다. 따라서 최초 사용 시 기본 패스워드를 반드시 변경해야 하며, 또한 주기적으로 변경해야 합니다.

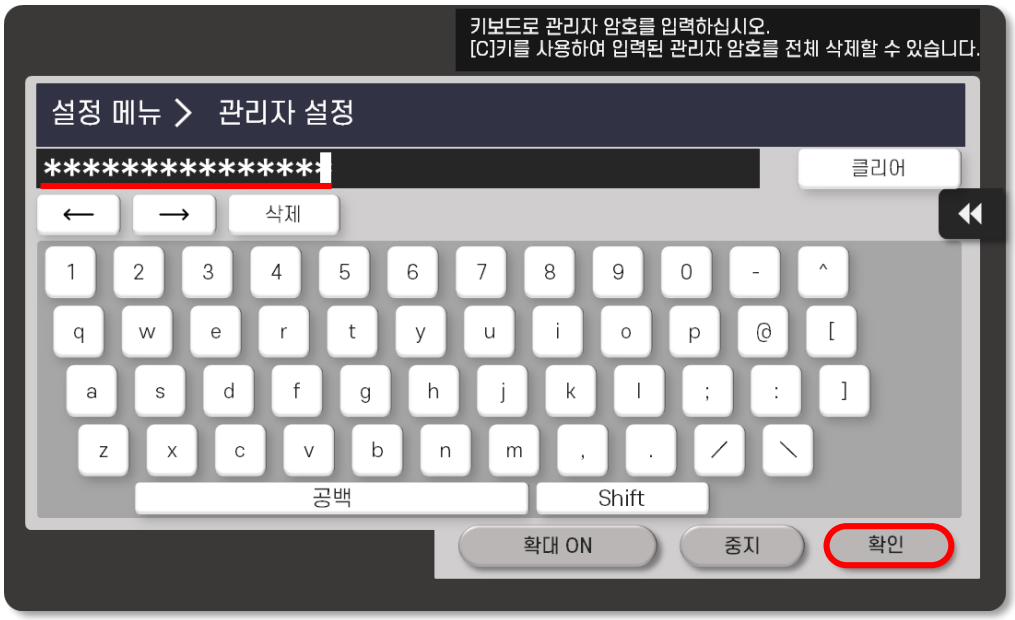
기본 관리자 패스워드 변경하기

1 ['유틸리티' 선택]

2 ['관리자 설정' 선택]

신도리코(Sindoh)

3 [관리자 암호 입력] > ['확인' 선택]

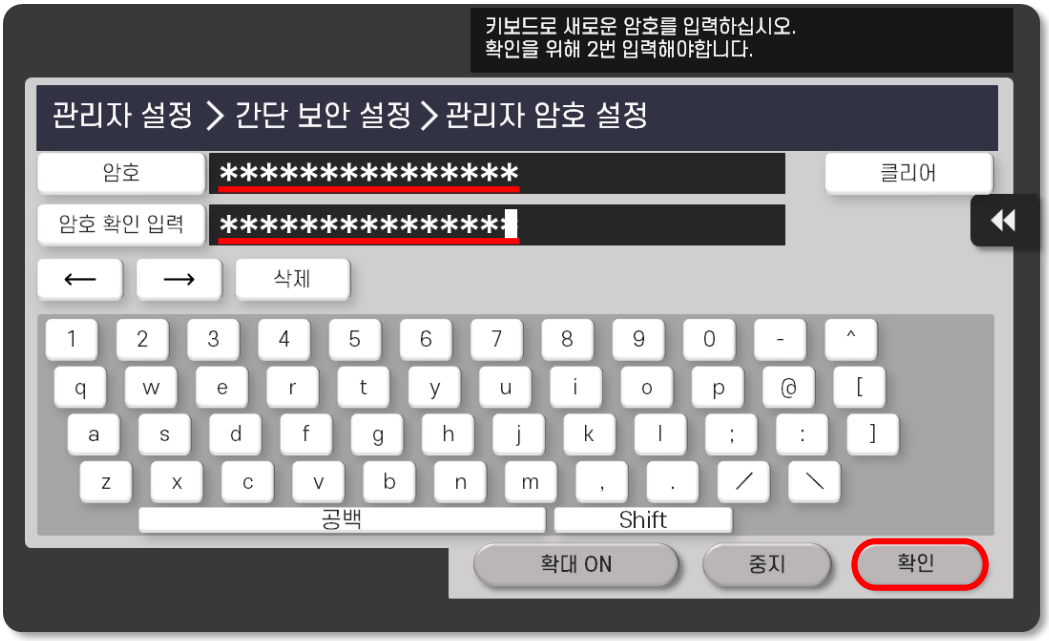


4 [관리자 설정] > [2페이지 넘어가기] > ['보안 설정' 선택]

신도리코(Sindoh)

5 [2페이지 넘어가기] > ['간단 보안 설정' 선택]

6 [관리자 암호 설정] > [암호 입력] > [암호 확인 입력] > ['확인' 선택]



신도리코의 기본 관리자

신도리코의 기본 관리자 패스워드는 '12345678123456 78'로, 관리자 패스워드를 재설정하여 보안 위협을 막아야 합니다.

신도리코(Sindoh)

2. 저장 문서 관리하기

복합기에는 출력, 스캔한 문서가 남아있을 수 있습니다. 문서 자동 삭제 설정은 복합기의 저장 공간에 저장된 문서를 주기적으로 정리하는 기능입니다. 이를 통해 의도치 않은 문서 유출 사고를 막을 수 있습니다.

문서 자동 삭제 설정하기

1 ['유틸리티' 선택]

2 ['관리자 설정' 선택]

신도리코(Sindoh)

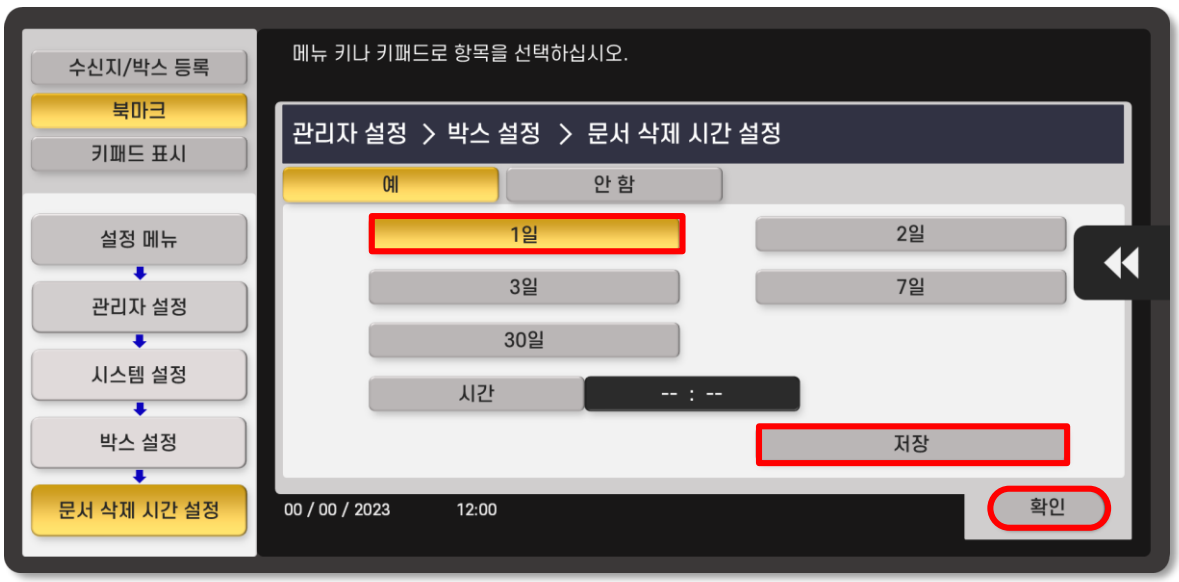
3 ['시스템 설정' 선택]

4 ['박스 설정' 선택]

신도리코(Sindoh)

5 [2페이지 넘어가기] > ['문서 삭제 시간 설정' 선택]

6 ['예' 선택] > ['1일' 선택] > ['저장' 선택] > ['확인' 선택]



신도리코(Sindoh)

3. 이동식 저장매체 관리하기

복합기에 이동식 저장매체(USB)를 연결하여 자료를 전송하거나, 문서를 출력할 수 있습니다. 하지만 이동식 저장매체는 악성코드의 유입과 문서 유출의 주요 경로 중 하나이기 때문에 복합기에 연결할 수 없도록 하는 것이 바람직합니다.

이동식 저장매체 사용 제한하기

1 ['유틸리티' 선택]

신도리코(Sindoh)

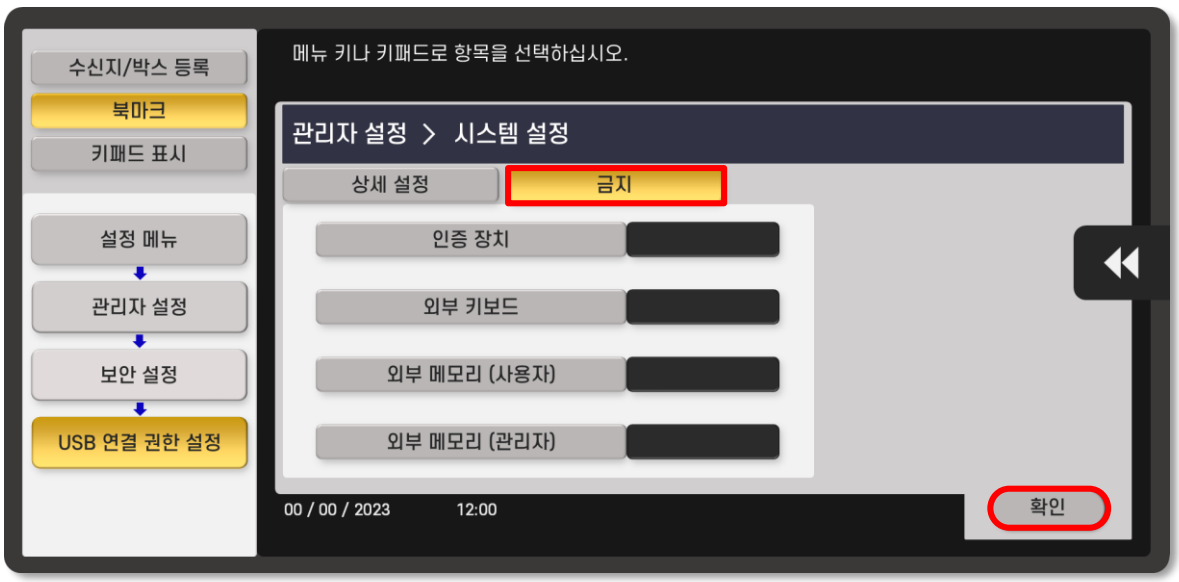
② ['관리자 설정' 선택]

③ [2페이지 넘어가기] > ['보안 설정' 선택]

신도리코(Sindoh)

4 ['USB 연결 권한 설정' 선택]

5 [USB 연결 권한 설정 '금지' 선택] > ['확인' 선택]



캐논(Canon)

1. 관리자 패스워드 설정하기

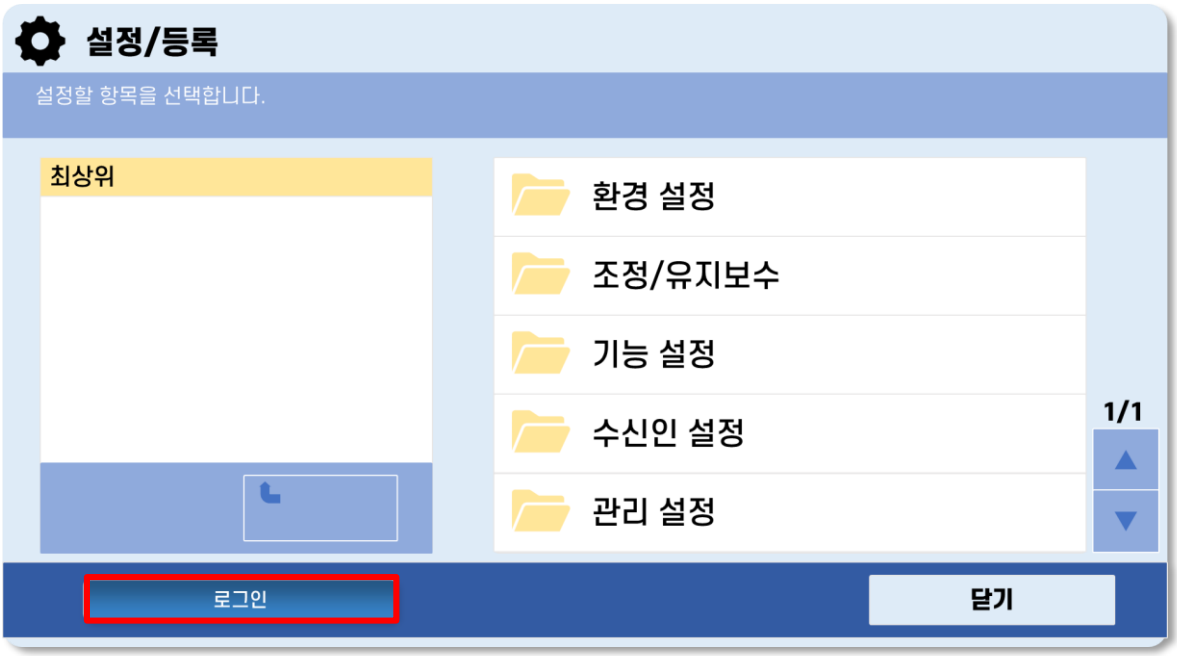
복합기의 관리자 기본 패스워드를 변경하는 것은 필수입니다. 복합기의 초기 관리자 아이디, 패스워드는 누구나 쉽게 알아낼 수 있습니다. 따라서 최초 사용 시 기본 패스워드를 반드시 변경해야 하며, 또한 주기적으로 변경해야 합니다.

기본 관리자 패스워드 변경하기

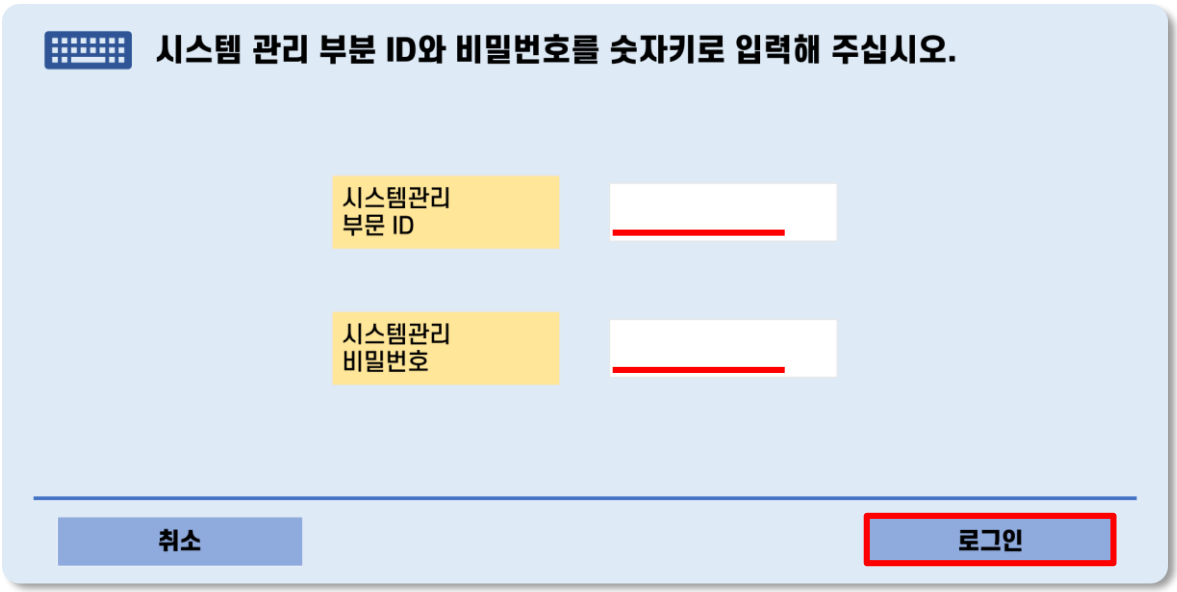
1. ['설정/등록' 누르기]

캐논(Canon)

2 ['로그인' 선택]

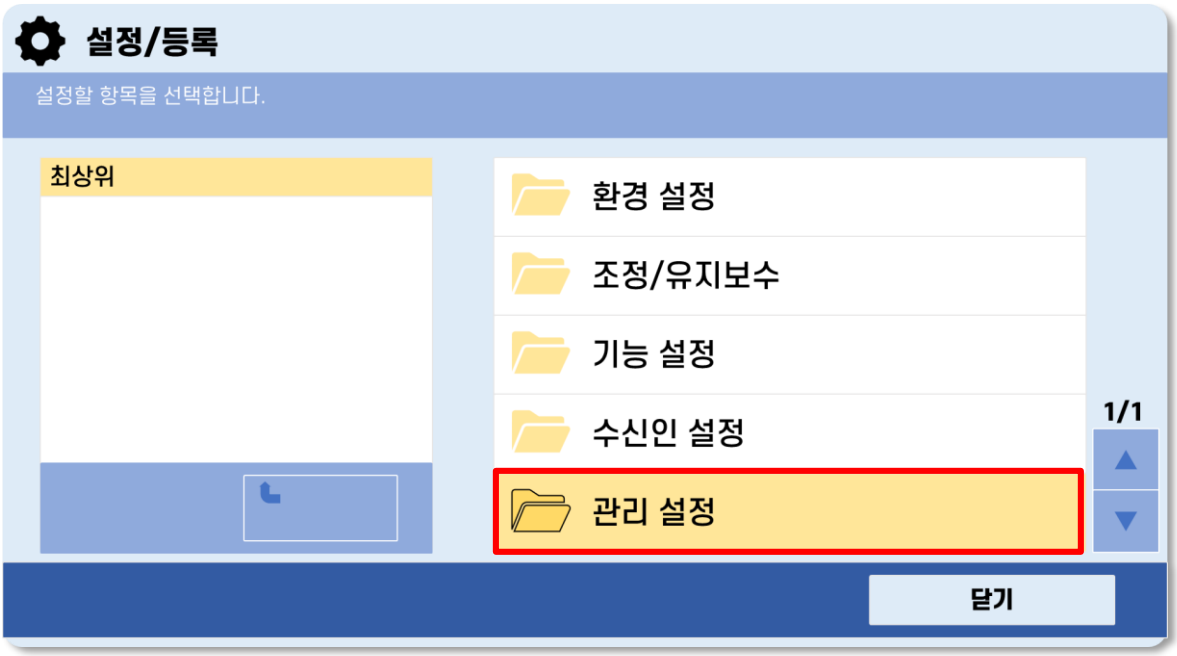


3 [시스템관리 ID, 비밀번호 입력] > ['로그인' 선택]

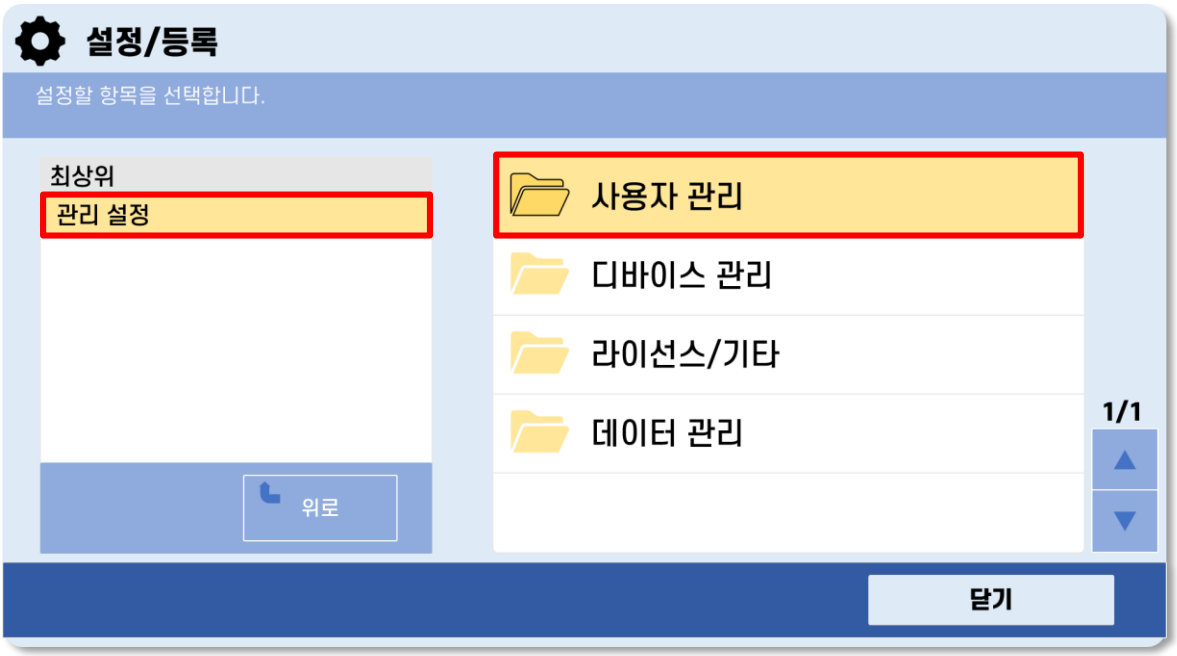


캐논(Canon)

4 ['관리 설정' 선택]

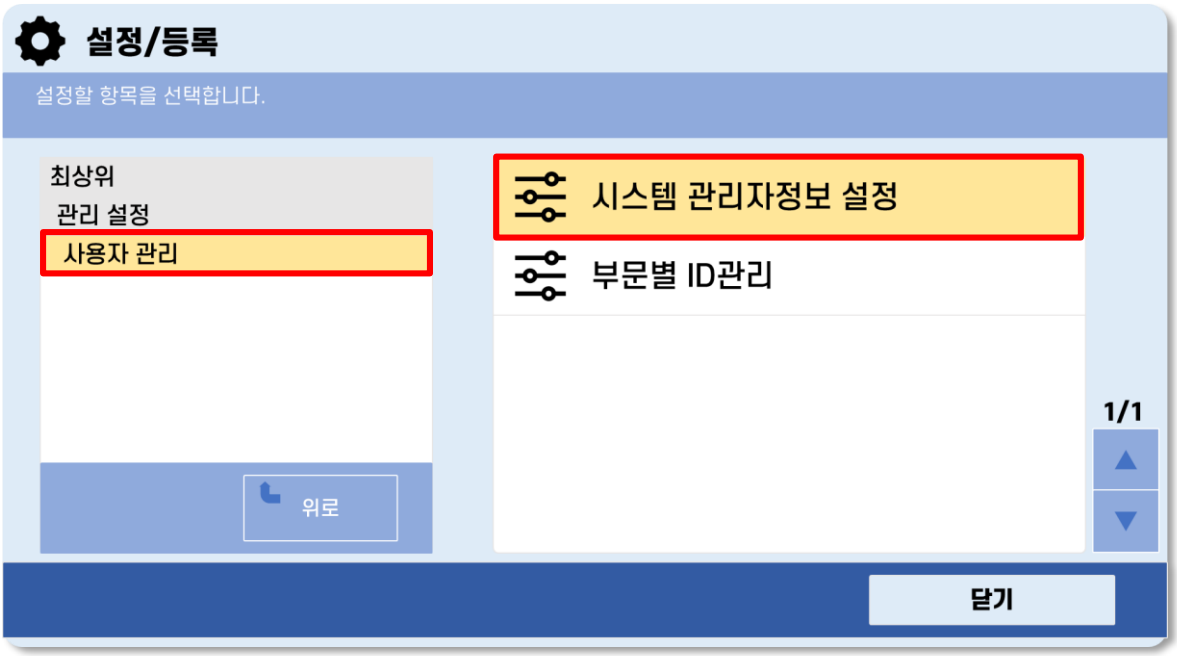


5 ['사용자 관리' 선택]



캐논(Canon)

6 ['시스템 관리자정보 설정' 선택]



7 [시스템관리 ID/비밀번호 입력] > ['확인' 선택]

캐논의 기본 관리자

캐논의 기본 관리자 ID와 패스워드는 '7654321'로, 관리자 패스워드를 재설정하여 보안 위협을 막아야 합니다.

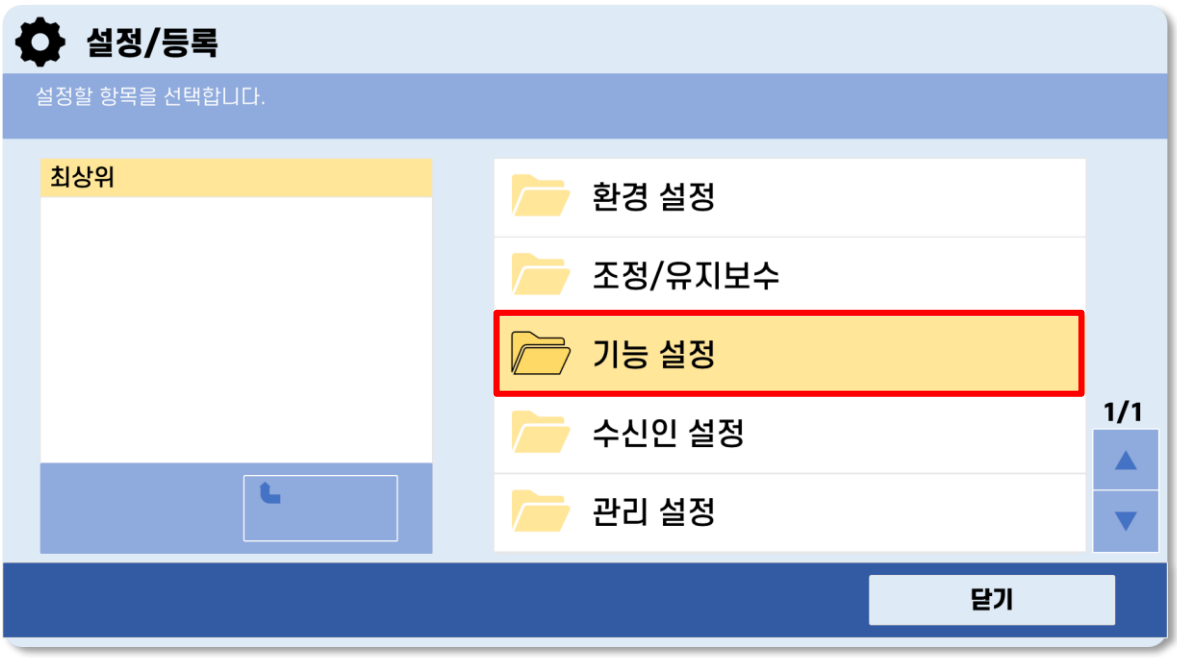
캐논(Canon)

2. 저장 문서 관리하기

복합기에는 출력, 스캔한 문서가 남아있을 수 있습니다. 문서 자동 삭제 설정은 복합기의 저장 공간에 저장된 문서를 주기적으로 정리하는 기능입니다. 이를 통해 의도치 않은 문서 유출 사고를 막을 수 있습니다.

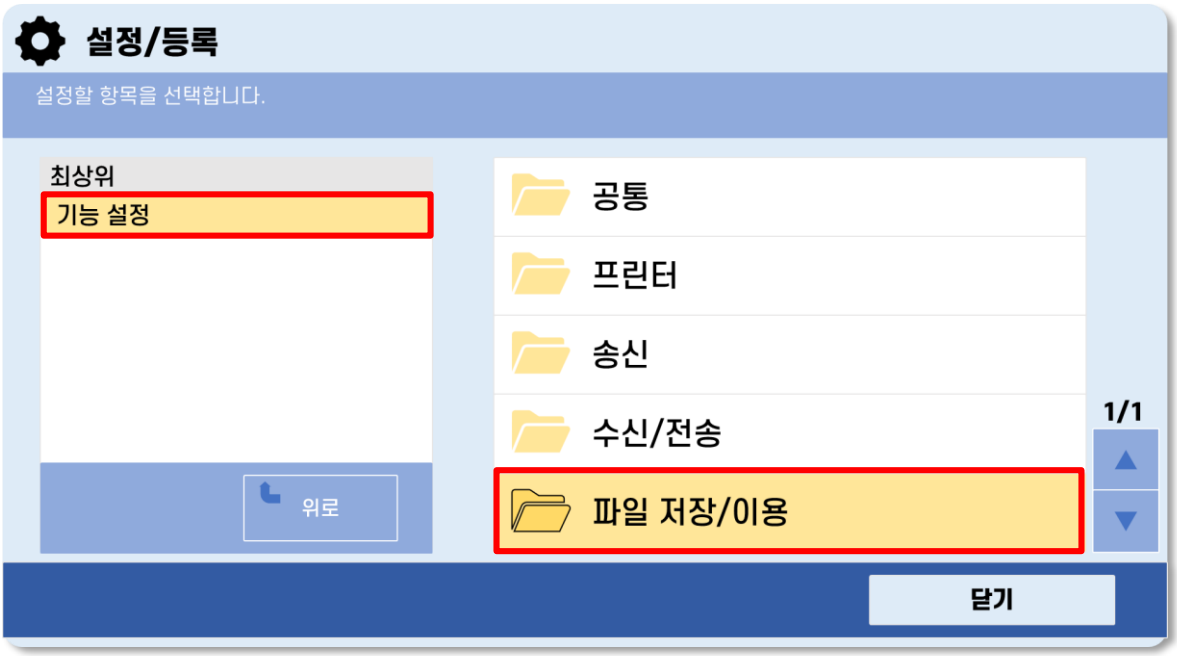
문서 자동 삭제 설정하기

1. [관리자로 접속] > ['설정/등록' 선택] > ['기능 설정' 선택]

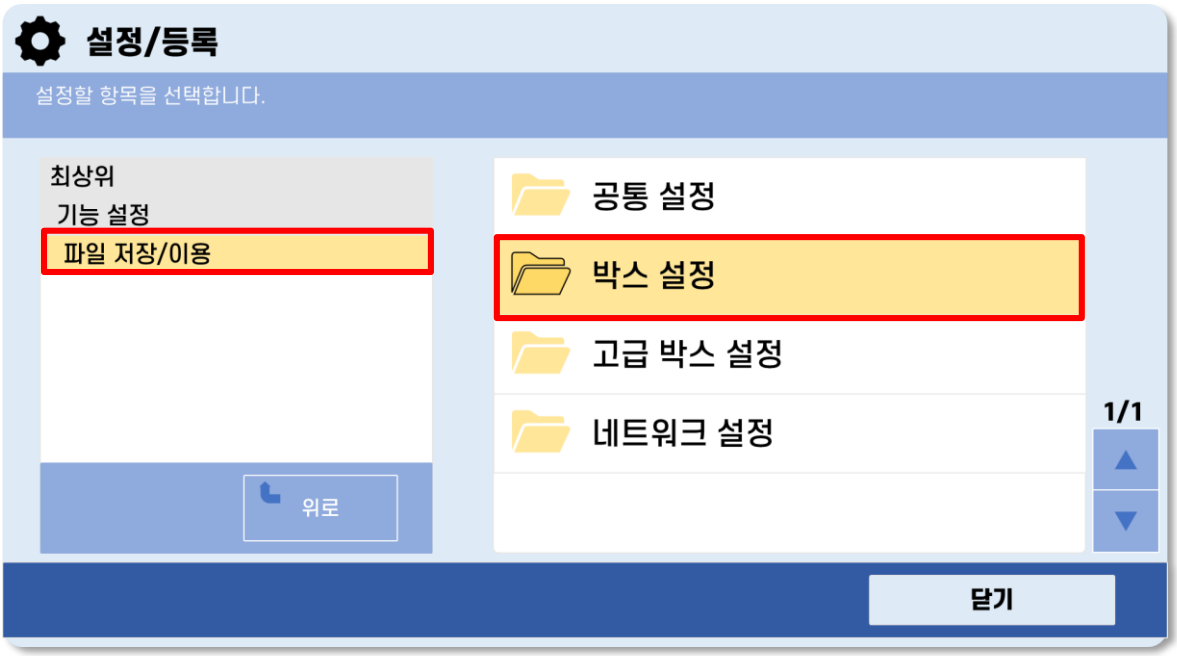


캐논(Canon)

② ['파일 저장/이용' 선택]

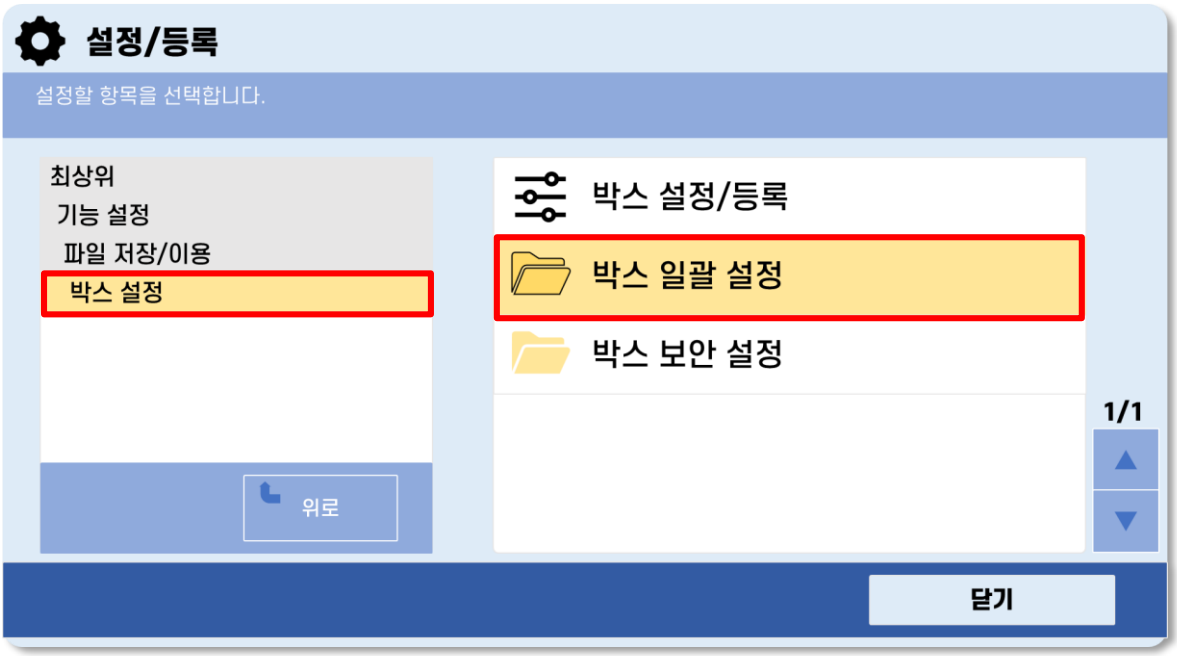


③ ['박스 설정' 선택]



캐논(Canon)

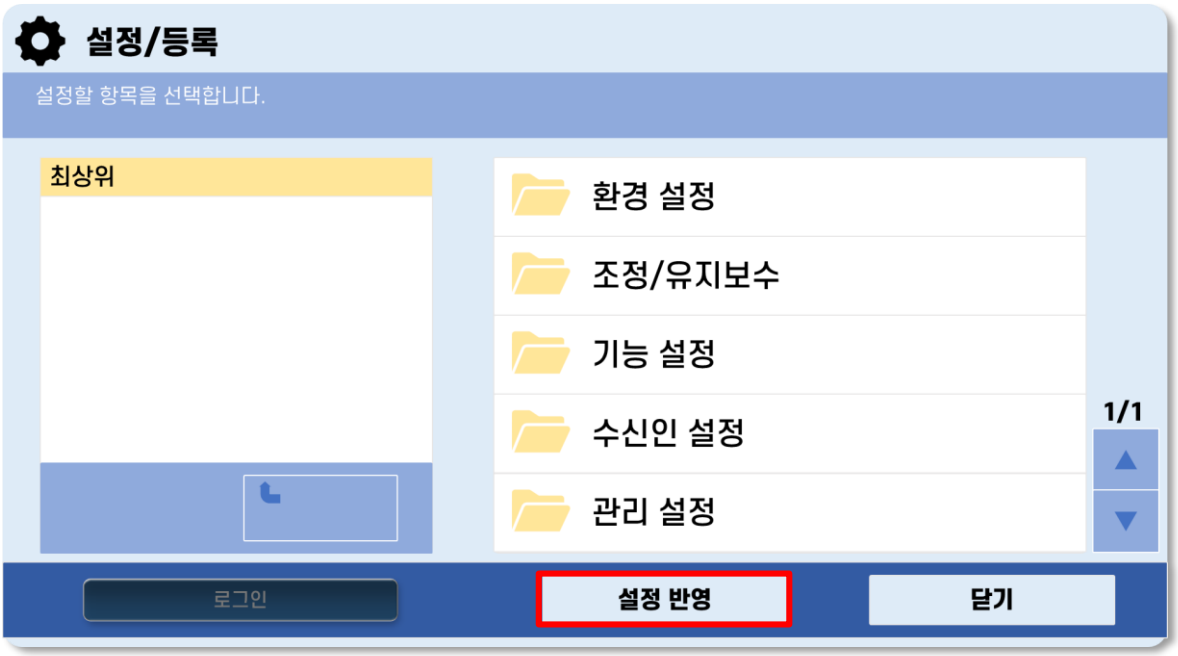
4 ['박스 일괄 설정' 선택]



5 [파일 자동 삭제까지의 시간 '1일' 입력] > [프린터 드라이버로부터 저장 시 인쇄 '해제' 선택] > ['확인' 선택]

캐논(Canon)

6 ['설정 반영' 선택]



저장 문서 관리 미흡과 관련된 피해 사례

기업의 민감한 정보를 보호하기 위해 문서의 적절한 저장과 관리가 필요합니다.

실제로 전자장비 제조업체인 A사의 사례를 보면, 회사의 출입구나 정보관리 서버에 대한 해킹 시도 흔적이 없음에도 불구하고, 회사 기밀이 경쟁사에 유출되었습니다.

이 사건의 조사 결과, 해커가 사내 네트워크에 침입하여 복합기에 저장된 문서를 통해 기밀 정보를 한 번에 유출했음이 밝혀졌습니다. 이러한 사례를 통해, 저장 문서 관리의 중요성을 알 수 있습니다.

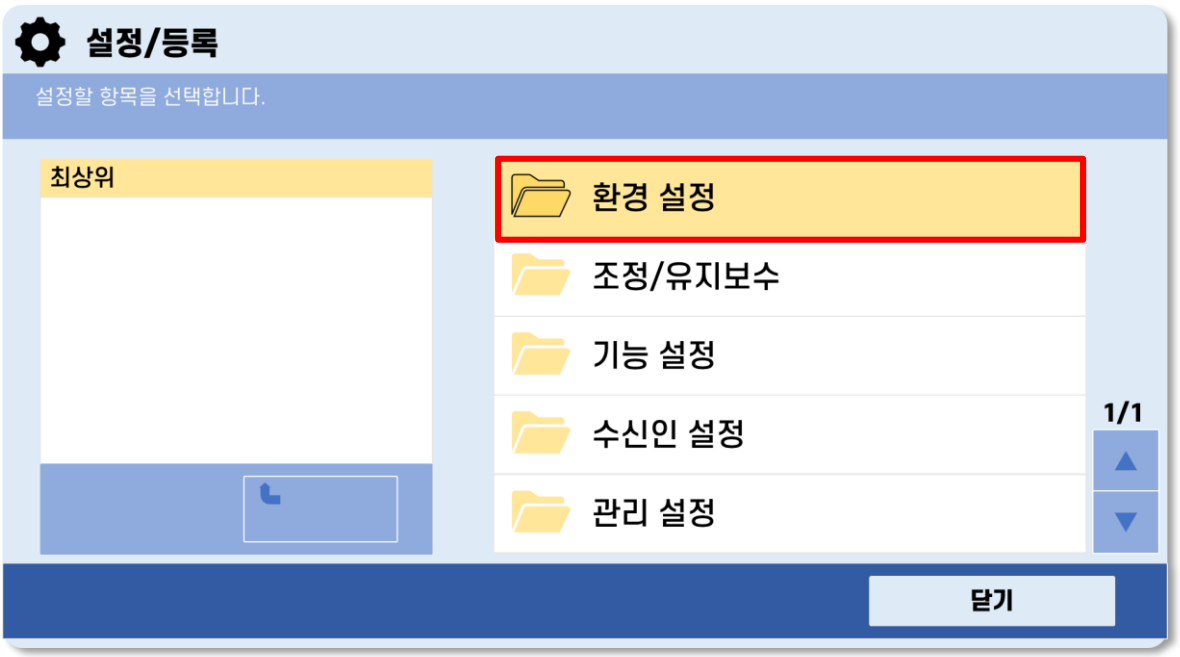
캐논(Canon)

3. 이동식 저장매체 관리하기

복합기에 이동식 저장매체(USB)를 연결하여 자료를 전송하거나, 문서를 출력할 수 있습니다. 하지만 이동식 저장매체는 악성코드의 유입과 문서 유출의 주요 경로 중 하나이기 때문에 복합기에 연결할 수 없도록 하는 것이 바람직합니다.

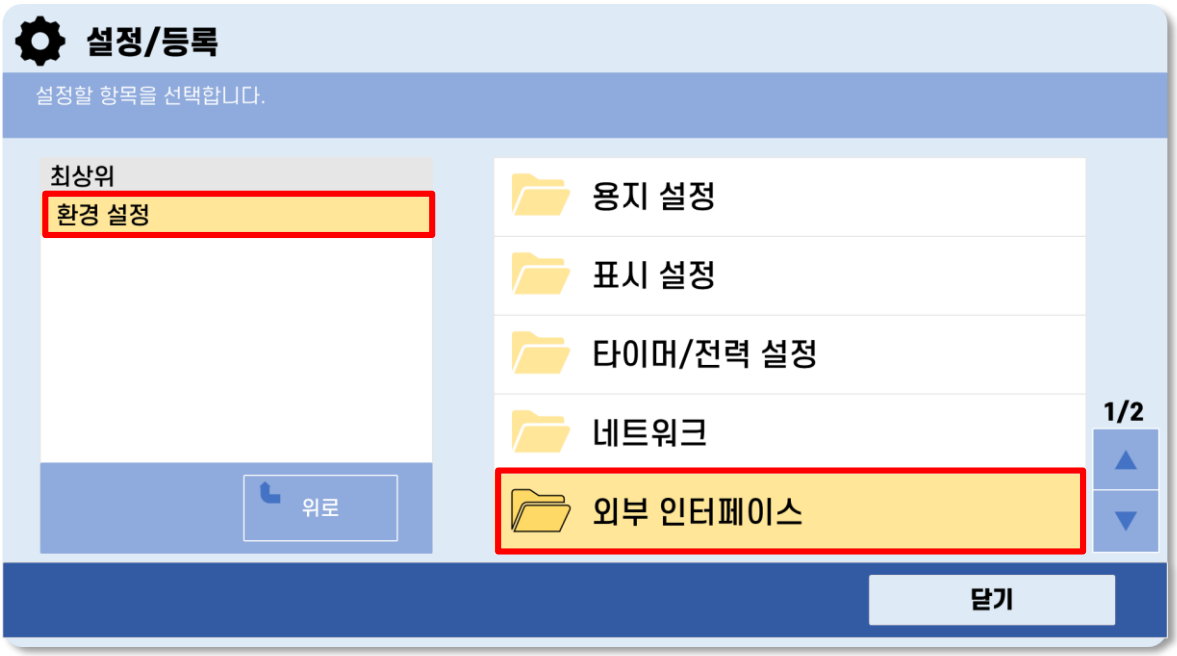
이동식 저장매체 사용 제한하기

1. [관리자로 접속] > ['환경 설정' 선택]



캐논(Canon)

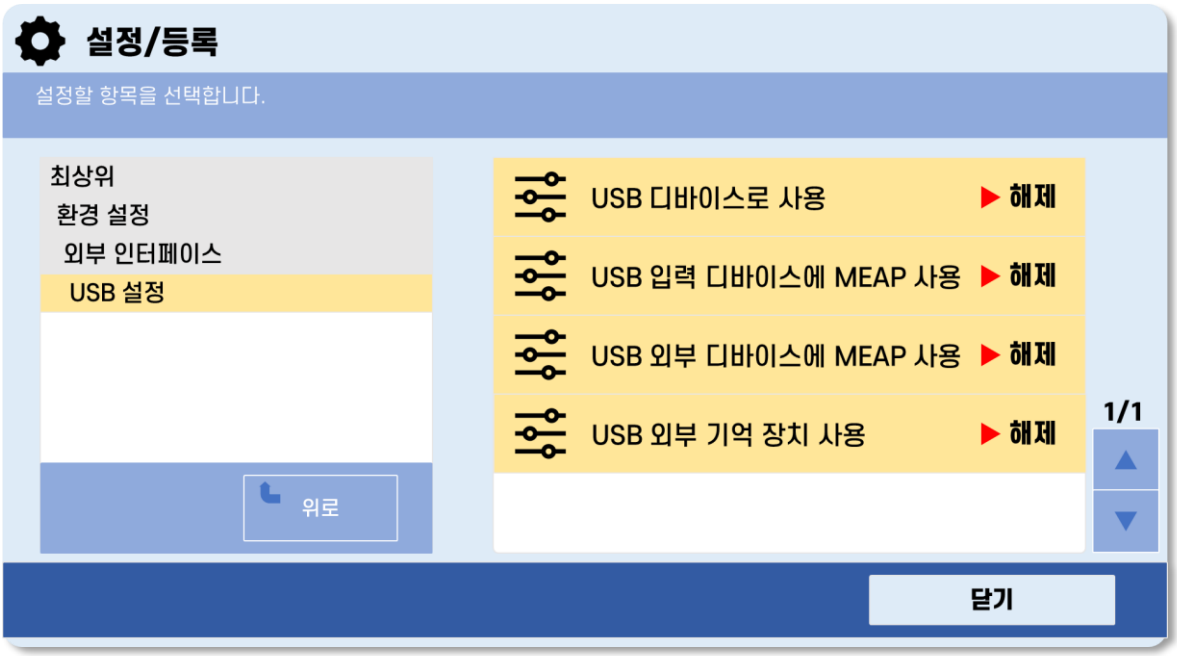
2 ['외부 인터페이스' 선택]



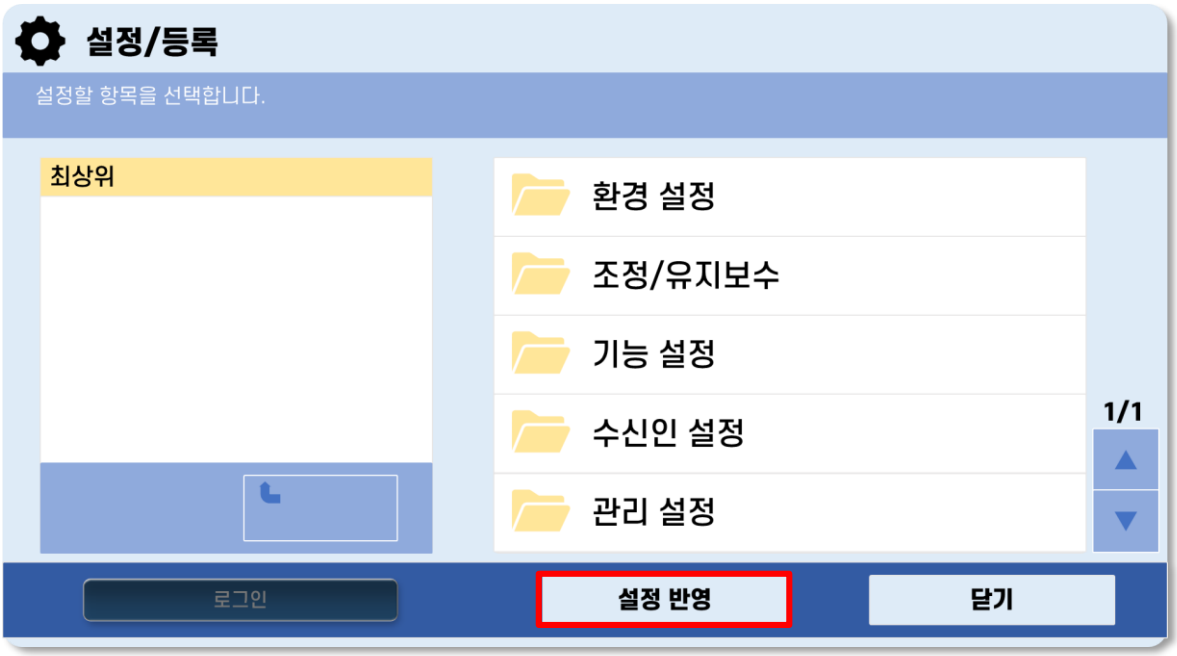
3 ['USB 설정' 선택]

캐논(Canon)

4 [USB 디바이스로 사용 '해제' 선택] > [USB 입력 디바이스에 MEAP 사용 '해제' 선택] > [USB 외부 디바이스에 MEAP 사용 '해제' 선택] > [USB 외부 기억 장치 사용 '해제' 선택]



5 ['설정 반영' 선택]



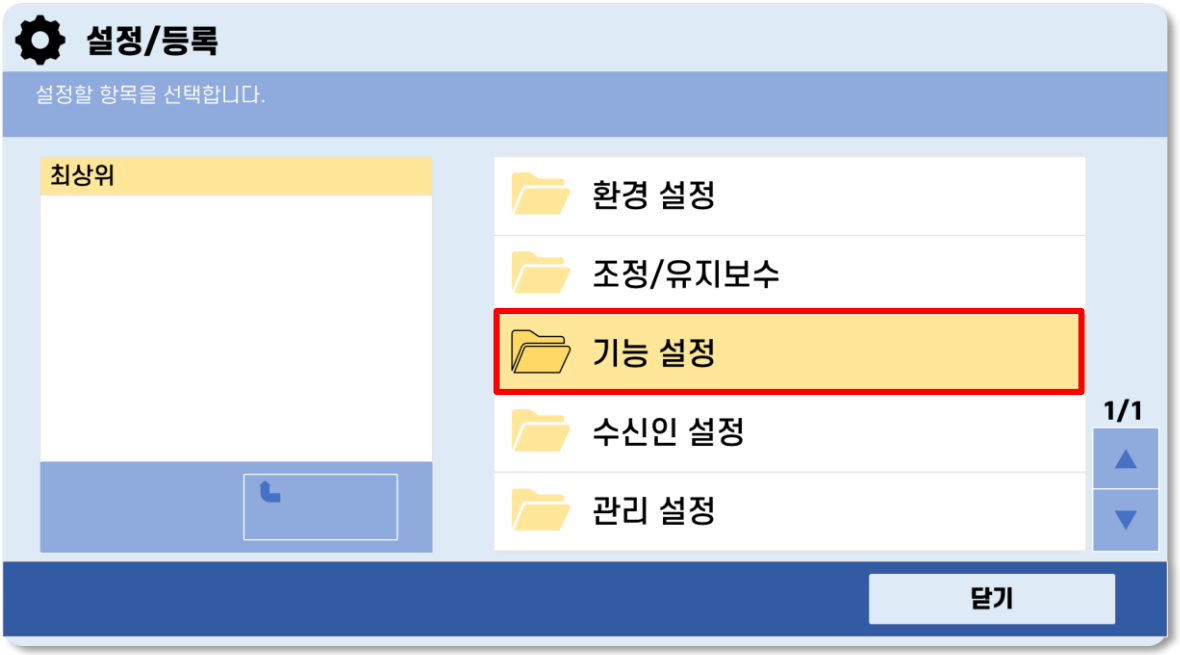
캐논(Canon)

4. 보안 인쇄 설정하기

보안 인쇄 기능은 사용자가 인쇄를 요청한 후 비밀번호를 입력하기 전까지 문서가 인쇄되지 않도록 하는 캐논의 보안 기능입니다. 이를 통해 인쇄 중인 문서를 다른 사용자들로부터 보호할 수 있습니다. 보안 인쇄 기능을 설정하여 기업의 문서 보안을 유지하는 방법을 알아보겠습니다.

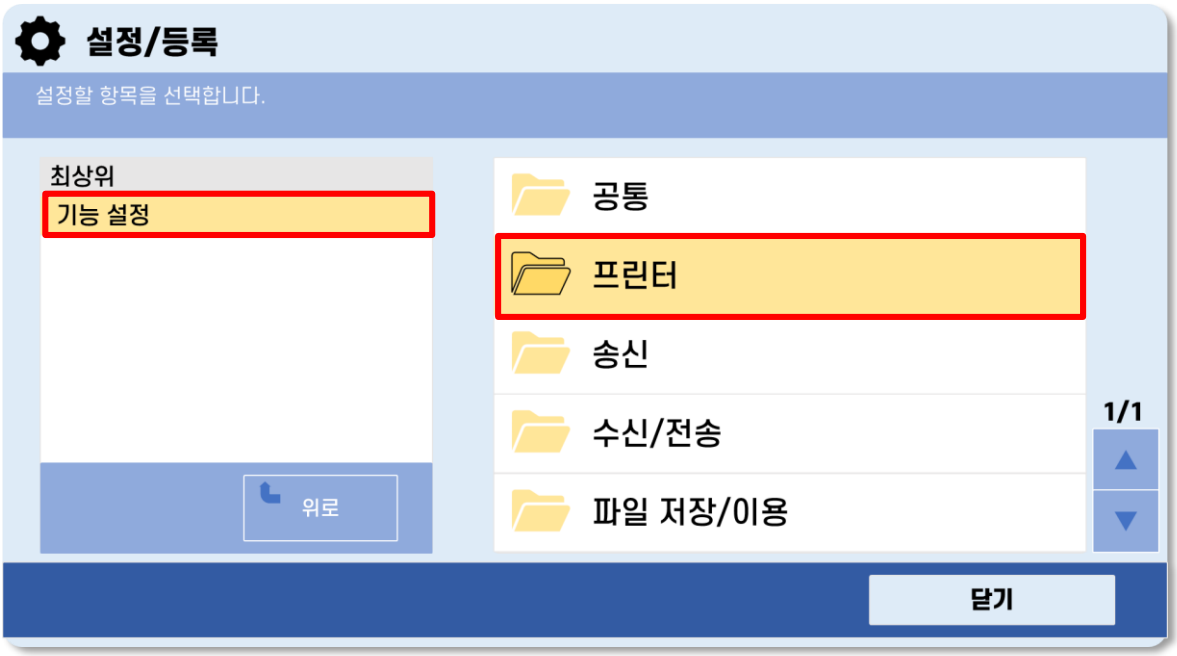
프린터 작업 제한 설정하기

1. [관리자로 접속] > ['기능 설정' 선택]

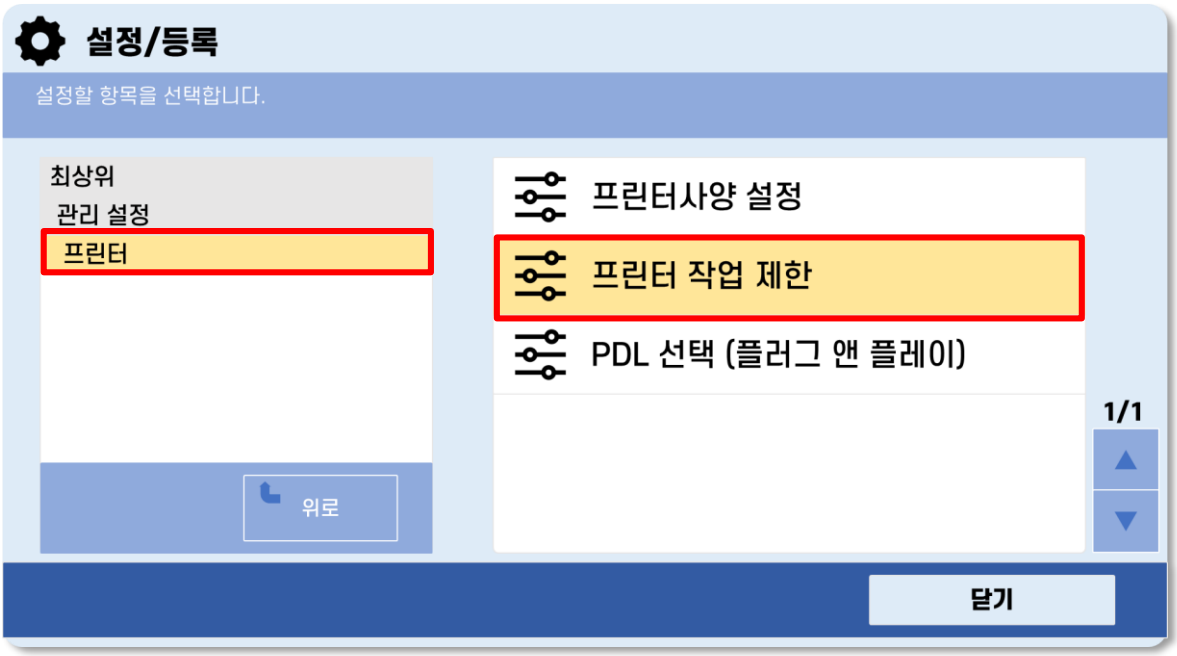


캐논(Canon)

2 ['프린터' 선택]

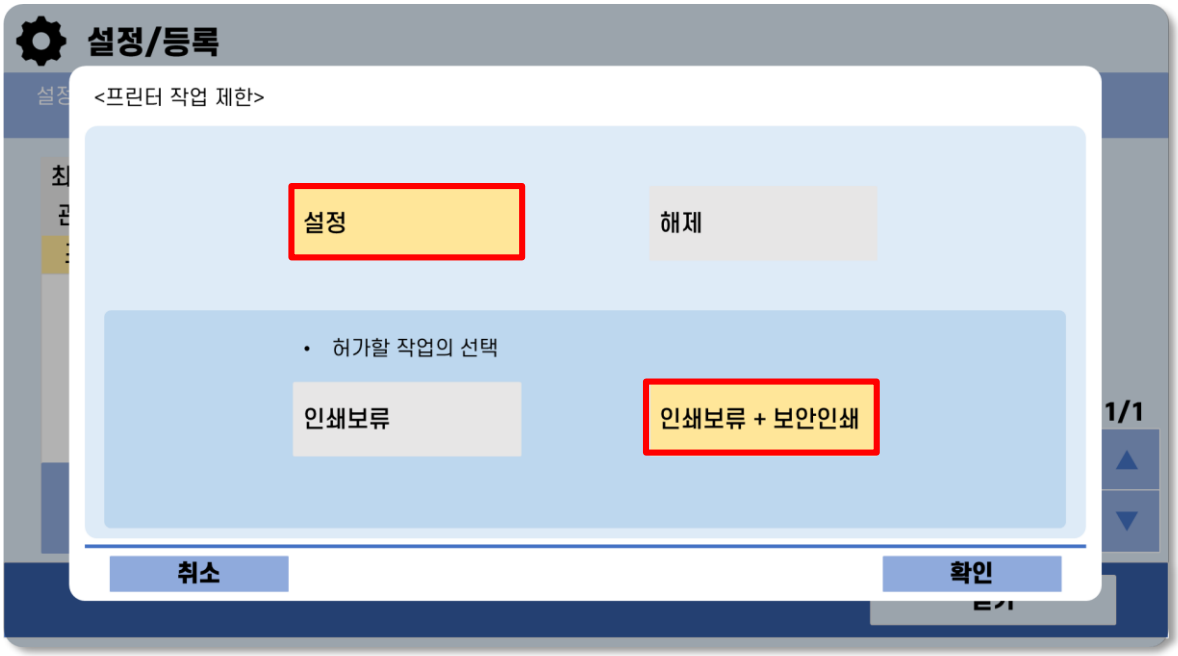


3 ['프린터 작업 제한' 선택]

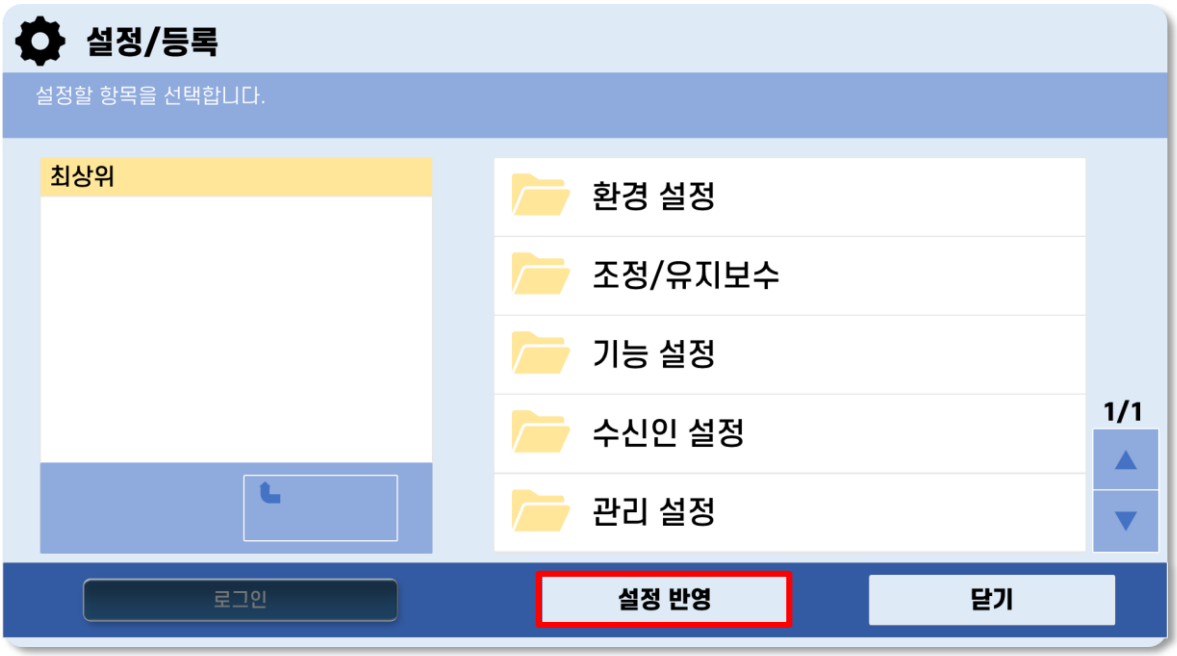


캐논(Canon)

4 [설정] > [허가할 작업의 선택 '인쇄보류 + 보안인쇄' 선택] > ['확인' 선택]



5 ['설정 반영' 선택]



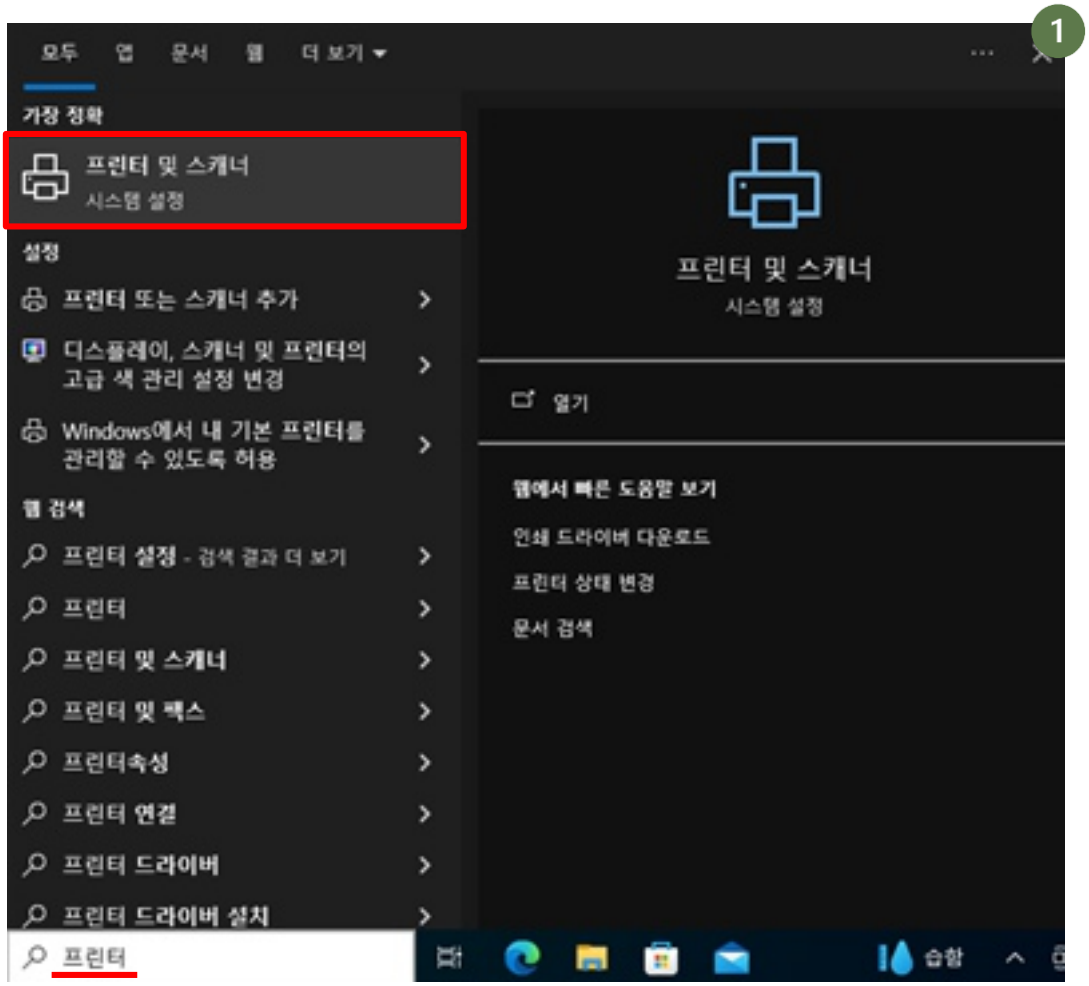
삼성(Samsung)

0. SyncThru™ Web Service 접속하기

삼성의 복합기와 프린터는 'SyncThru™ Web Service'라는 관리 웹서비스를 제공합니다. 이 서비스를 통해 PC에서도 복합기의 상태를 확인하거나 설정을 변경할 수 있습니다. 본 항목은 'SyncThru™ Web Service'에 접속하는 방법을 안내합니다.

복합기의 IP 주소 확인하기

1 ['프린터 및 스캐너' 검색 및 실행]



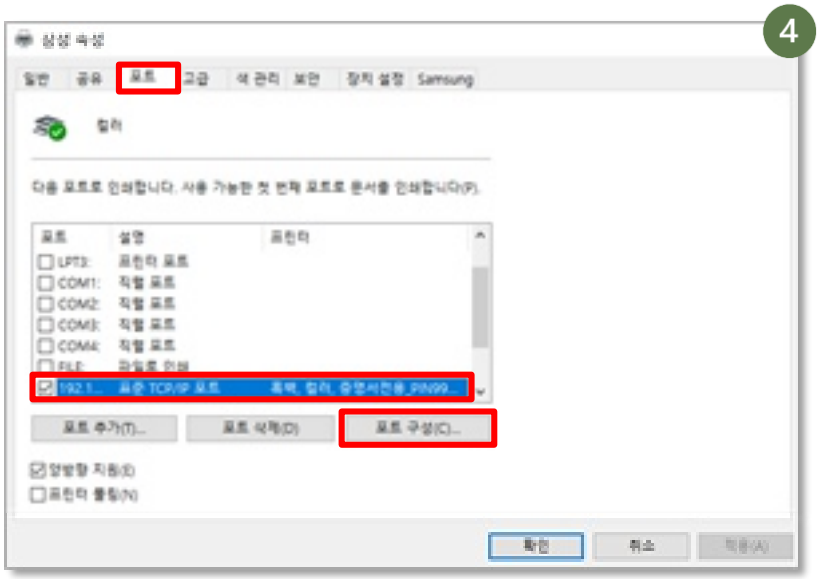
삼성(Samsung)

② ['프린터 및 스캐너'에서 삼성 복합기 선택 후 '관리' 클릭]

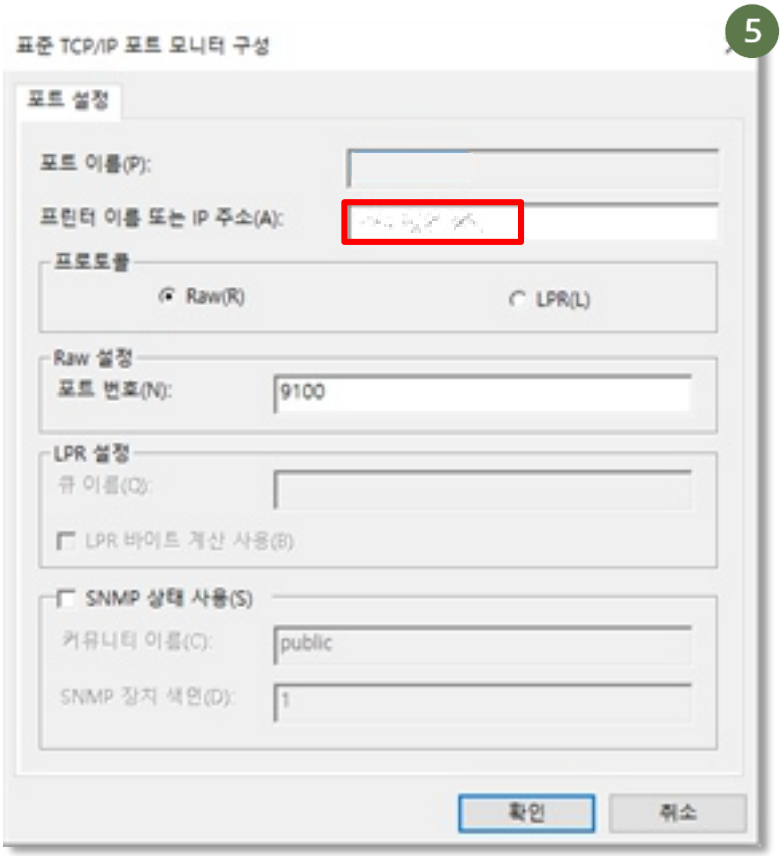
③ ['프린터 속성' 클릭]

삼성(Samsung)

4 ['프린터 속성'의 '포트' 탭 클릭] > ['표준 TCP/IP 포트' 클릭 후 '포트 구성' 클릭]



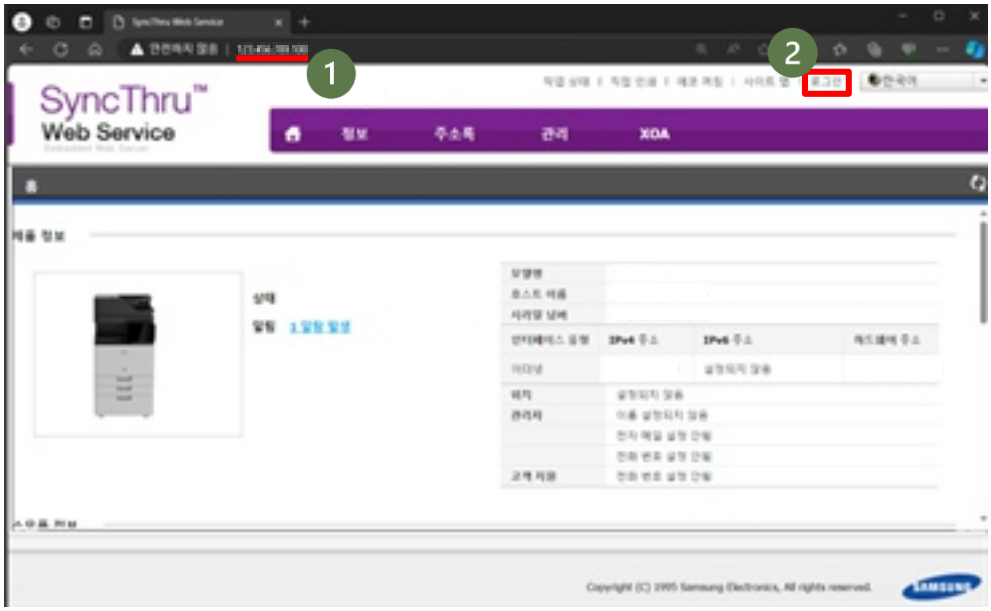
5 ['프린터 이름 또는 IP 주소' 란에서 IP 주소 확인]



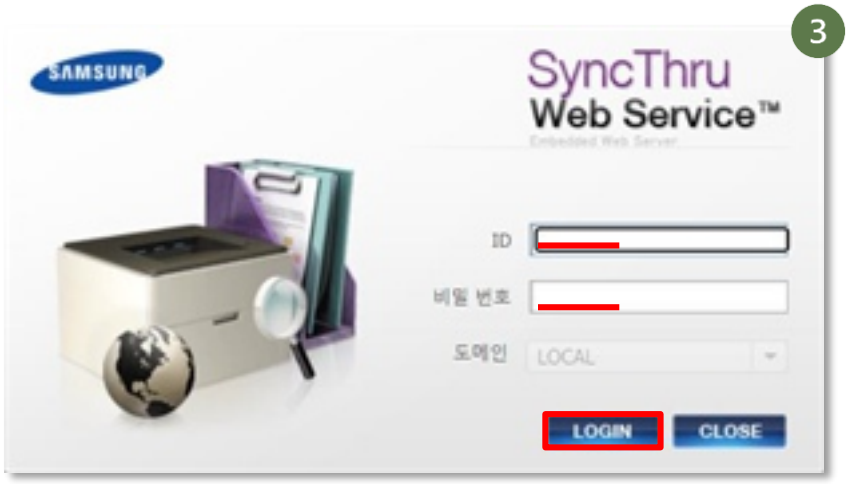
삼성(Samsung)

관리자 페이지 로그인 하기

1. [복합기 IP 주소 웹 브라우저에 검색]
2. [우측 상단의 '로그인' 클릭]



3. [관리자 계정으로 로그인]



삼성의 기본 관리자 계정

삼성의 기본 관리자 계정은 [ID: 'admin' PW: 'sec00000' 혹은 'admin@123']으로, 복합기 설정을 위해서는 로그인이 필요합니다.

삼성(Samsung)

1. 관리자 패스워드 설정하기

복합기의 관리자 기본 패스워드를 변경하는 것은 필수입니다. 복합기의 초기 관리자 아이디, 패스워드는 누구나 쉽게 알아낼 수 있습니다. 따라서 최초 사용 시 기본 패스워드를 반드시 변경해야 하며, 또한 주기적으로 변경해야 합니다.

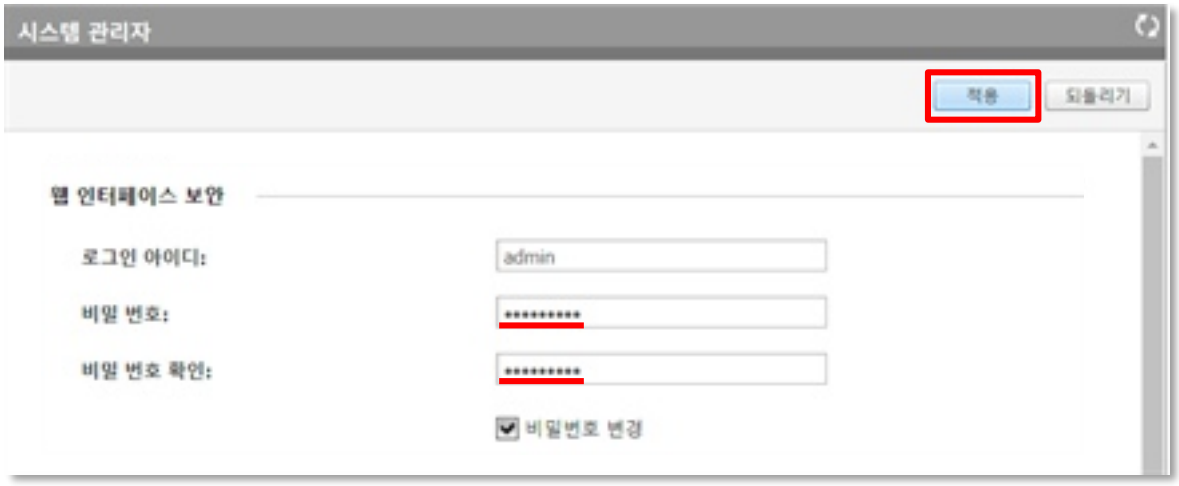
기본 관리자 패스워드 변경하기

1. [관리자 페이지] > ['보안' 탭 클릭]

2. ['시스템 관리자' 클릭] > [웹 인터페이스 보안] > ['비밀번호 변경' 체크박스 선택]

삼성(Samsung)

3 ['비밀 번호' 입력] > ['비밀 번호 확인' 입력] > ['적용' 클릭]



삼성복합기의 기본 관리자

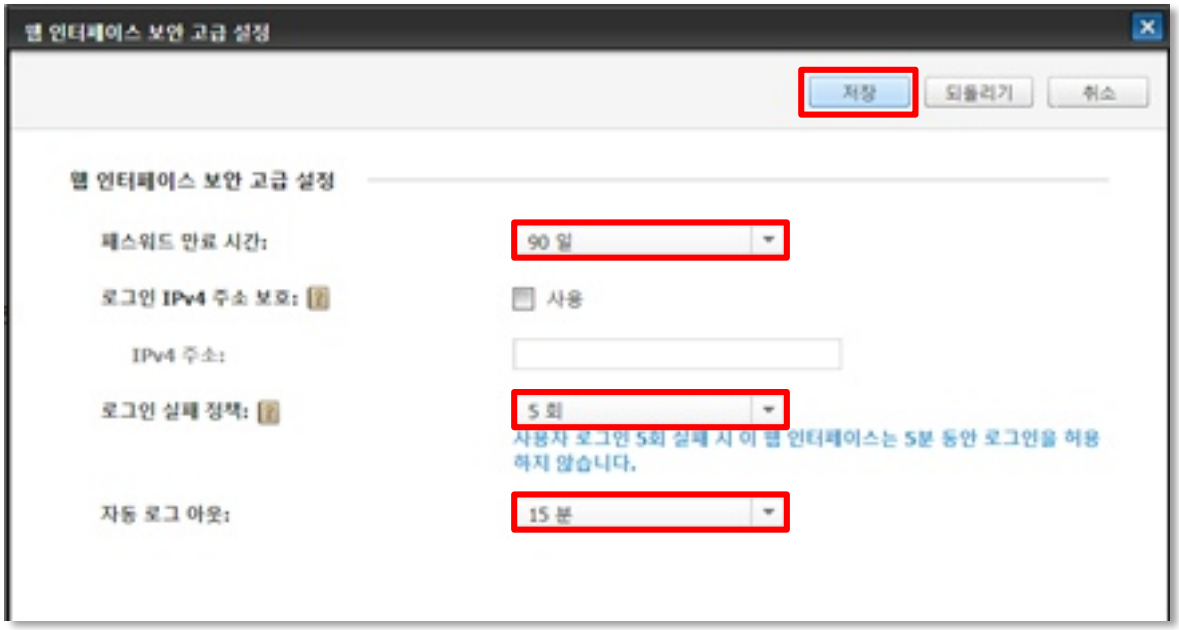
삼성의 기본 관리자 계정은 [ID: 'admin' PW: 'sec00000' 혹은 'admin@123']으로, 관리자 패스워드를 재설정하여 보안 위협을 막아야 합니다.

삼성(Samsung)

패스워드 세션기간/로그인 정책 설정하기

1. [관리자 페이지] > ['보안' 탭 클릭] > ['시스템 관리자' 클릭] > [웹 인터페이스 보안] > ['고급' 클릭]

2. [웹 인터페이스 보안 고급 설정] > [패스워드 만료 시간 '90일' 선택] > [로그인 실패 정책 '5회' 선택] > [자동 로그 아웃 '15분' 선택] > ['저장' 클릭]



웹 인터페이스 보안 고급 설정

웹 인터페이스 보안 고급 설정의 패스워드 만료 시간, 로그인 실패 정책, 자동 로그 아웃은 회사 내규에 따라 더 강화된 보안 설정을 하셔도 무방합니다.

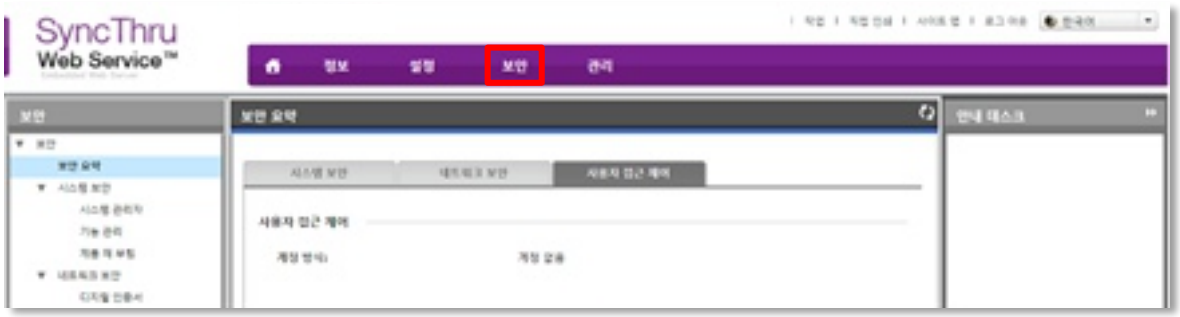
삼성(Samsung)

2. 이동식 저장매체 관리하기

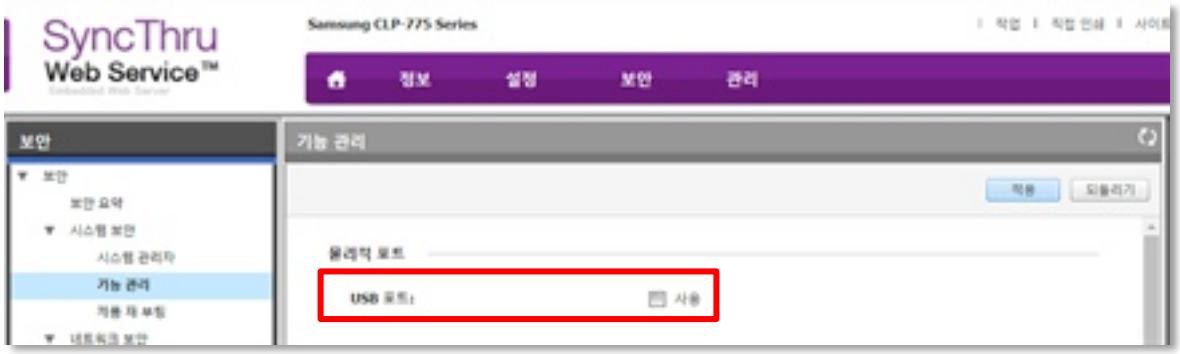
복합기에 이동식 저장매체(USB)를 연결하여 자료를 전송하거나, 문서를 출력할 수 있습니다. 하지만 이동식 저장매체는 악성코드의 유입과 문서 유출의 주요 경로 중 하나이기 때문에 복합기에 연결할 수 없도록 하는 것이 바람직합니다.

이동식 저장매체 사용 제한하기

1. [관리자 페이지] > ['보안' 탭 클릭]



2. [기능 관리] > [물리적 포트] > [USB 포트 '사용' 체크박스 해제] > ['적용' 클릭]



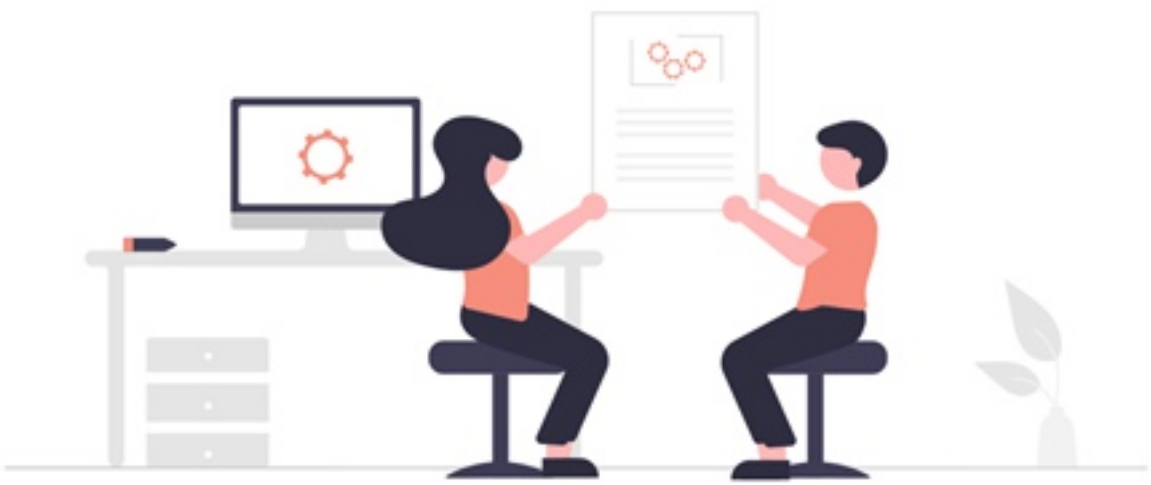
이동식 저장 매체의 보안 위협

이동식 저장 매체의 사용은 복합기 보안에서 중요한 사안입니다. 이동식 저장 매체는 이동성이 편리하지만 그만큼 위험도가 높습니다.

예를 들어 USB와 같은 이동식 저장매체를 통해 악성코드가 복합기로 전파되면 복합기 내에 있는 중요 정보가 삭제되거나 유출될 수 있습니다. 또한 이동식 저장매체를 통해 복합기에 저장된 문서를 무단으로 복사하는 경우, 회사의 민감한 정보가 유출될 위험이 있습니다.

제2장 정보보안 실무자 보안수칙

Ⅲ. 사무용 소프트웨어

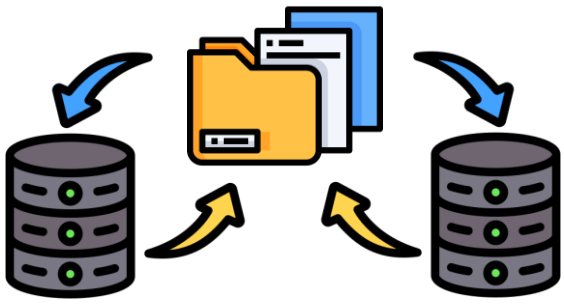


이것만은 지키자!

행동수칙

드라이브 편

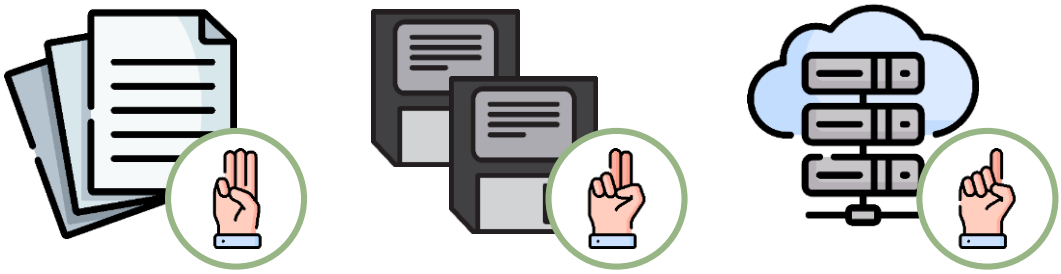
1



중요한 데이터는 분리된 저장 공간에도 저장하도록 해요!

중요한 데이터는 절대로 한 곳에서만 보관하는 일이 없도록 해야 합니다. 유일한 저장 공간이 공격을 받거나 자연 재해로 인해 고장이 나면 저장된 데이터가 손상될 수 있습니다. 데이터 또한 기업의 소중한 자산이므로 데이터의 안전은 회사의 자산을 지키는 것과 같습니다. 이처럼 사고에 대비하여 데이터를 기존 저장 공간과 다른 공간에 중복하여 보관하는 행위를 백업이라고 합니다.

2



"백업의 3-2-1 법칙"을 지켜 백업해요!

"백업의 3-2-1 법칙"이란 안전한 백업을 위한 행동 수칙으로, 백업 데이터의 3개의 버전 또는 사본을, 2개의 다른 디스크에 보관하되, 최소 1개의 데이터는 물리적으로 다른 장소에 보관하여 데이터를 보관하는 방법입니다. 데이터를 기존 저장 공간과 동일한 저장소에 백업하는 것과 같이 불완전하게 백업을 하면, 경우에 따라 복구가 불가능할 수 있기 때문입니다.

클라우드 컴퓨팅의 눈부신 발전으로 오늘날에는 산업 현장에서도 클라우드를 많이 이용하게 되었습니다. 이번에는 클라우드 서비스 중에서도 가장 많이 이용되는 서비스인 '드라이브(저장소)'의 보안에 대하여 다룹니다.

드라이브란 무엇인가요?

'드라이브'는 SaaS(Software as a Service) 서비스 중 하나로, 일정 비용을 지불하고 클라우드에서 관리하는 저장 장치의 일정 공간을 빌려 자신의 저장소처럼 이용할 수 있는 서비스입니다. 인터넷을 통해 멀리 있는 저장소에 데이터를 전송하고, 데이터가 필요하면 다시 인터넷을 통해 받아오는 형태로 데이터 저장 및 인출이 이루어집니다.

드라이브 보안을 왜 신경써야 할까요?

드라이브는 업무 자료를 저장하기 위해 주로 이용되고 있어 중요한 정보가 많이 저장되어 있습니다. 그렇기 때문에 드라이브를 안전하게 지키는 것이 매우 중요합니다. 그러나 드라이브 사용자들은 모든 보안 책임을 클라우드가 진다고 생각해 보안에 잘 신경쓰지 않는 경향이 있습니다. 하지만 사용자도 데이터 관리 및 보안에 책임이 있기 때문에, 데이터 유출 시 사용자가 손실을 감수해야 합니다.

가이드라인에서 다루는 제품 확인하기

▲ 구글 드라이브(Google Drive)

▲ 원 드라이브(OneDrive)

▲ 드롭박스(Dropbox)

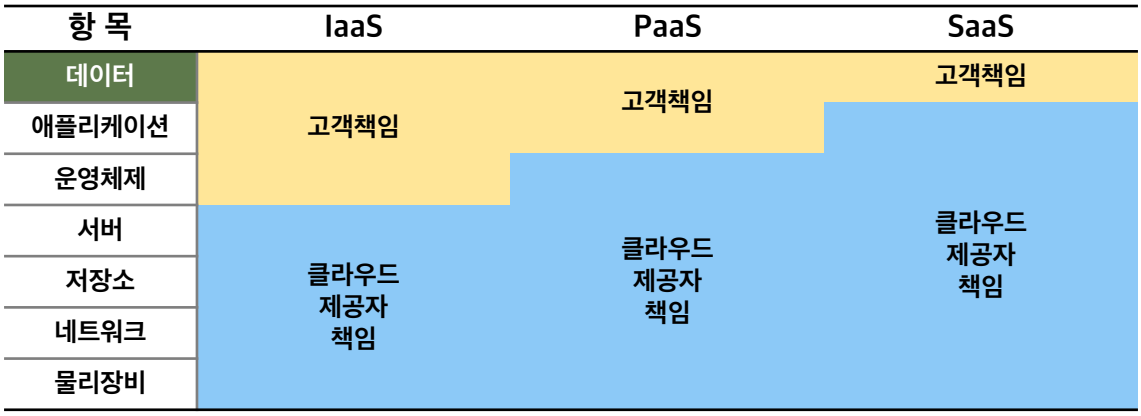
드라이브(저장소) 보안 알아보기

1. 책임공유모델

클라우드에서의 보안

클라우드가 생기기 전에는 회사에서 하드웨어(서버, 스토리지 등)부터 소프트웨어까지 모두 자체적으로 설치하고 운영하여야 했습니다. 따라서 시스템의 보안 책임 또한 그 시스템을 소유한 회사의 것이었습니다.

하지만 클라우드가 도입되고 회사는 더 이상 시스템을 구축할 필요 없이 클라우드 서비스 제공자의 시스템을 빌려서 이용할 수 있게 되었습니다. 이에 따라 해당 시스템의 보안 책임이 누구에게 있는지 모호해지는 문제가 생기게 되었습니다. 이 문제를 해결하기 위해 '책임 공유 모델'이 등장했습니다. 이는 클라우드를 이용하면서 나타날 수 있는 보안 문제는 클라우드 서비스 제공자와 사용자 모두에게 그 책임이 있고, 구체적인 상황에서 특정 문제를 누구의 책임으로 할 것인지 합의한 것을 의미합니다.



AWS에서 제시하는 책임 공유 모델

많은 사람들은 클라우드 이용 과정에서 나타나는 보안 책임이 전적으로 클라우드 서비스 제공자에게 있다고 생각합니다. 하지만 서비스 종류별로 사용자가 직접 관리해야 하는 보안 요소가 존재하며, 데이터의 관리는 어떤 서비스에서도 전적으로 사용자의 책임이라는 것을 알아야 합니다.

드라이브(저장소) 보안 알아보기

클라우드 저장소 사용 시 관리해야 하는 보안 영역

클라우드 저장소의 경우 책임공유모델에서 SaaS에 해당합니다. 따라서 SaaS에 저장되는 데이터에 대한 보안 책임은 그 서비스를 이용하는 사용자에게 있습니다.

계정 및 권한관리

① 퇴사자 계정 제거하기
② 불필요한 권한 제거하기
③ 2단계 인증 설정하기
④ 비밀번호 규칙 설정하기

데이터관리

⑤ 외부 접근 통제 설정하기
⑥ 로그 관리하기
⑦ 데이터 암호화하기

드라이브(저장소) 보안 알아보기

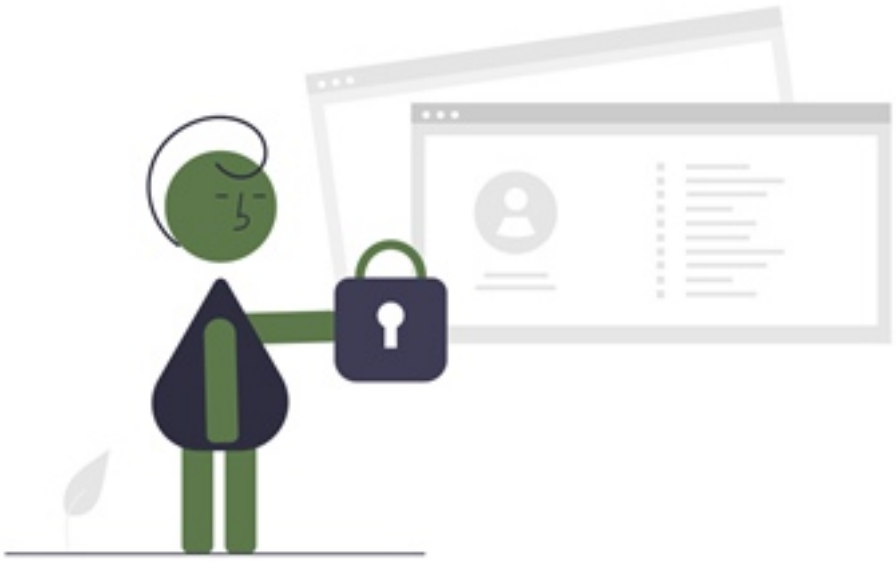
2. 중요정보 사용자 암호화

암호 및 암호키 관리의 중요성

데이터 암호화란 일상적으로 사용되는 문자(평문)를 '암호키'라고 하는 값과 함께 계산해 암호문으로 변환하는 기술입니다. 암호문은 암호키를 가진 사람만이 그 내용을 읽을 수 있어 정보의 비밀을 유지할 수 있습니다. 단 데이터를 암호화하더라도 암호키가 외부로 유출된다면 타인이 데이터을 읽을 수 있게되어 데이터의 비밀을 지킬 수 없습니다. 따라서 암호키에 대한 관리도 중요합니다.

시스템이 공격받아 기업이 갖고 있는 중요한 정보가 외부로 유출되어도, 사용자가 사전에 정보를 암호화하였다면 누구도 이를 알아볼 수 없어 유출된 정보의 비밀을 지킬 수 있습니다.

중요한 정보가 유출되는 경우 기업 경영이 심각하게 저해될 수 있습니다. 따라서 중요한 정보는 클라우드 저장소에 업로드 하기 전 데이터를 암호화하기를 권장드립니다.



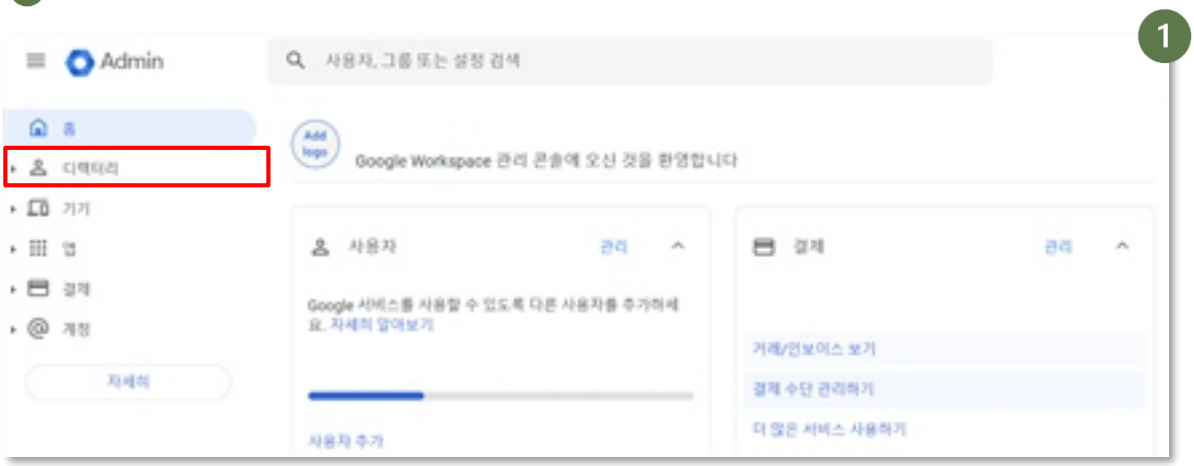
구글 드라이브(Google Drive)

1. 퇴사자 계정 제거하기

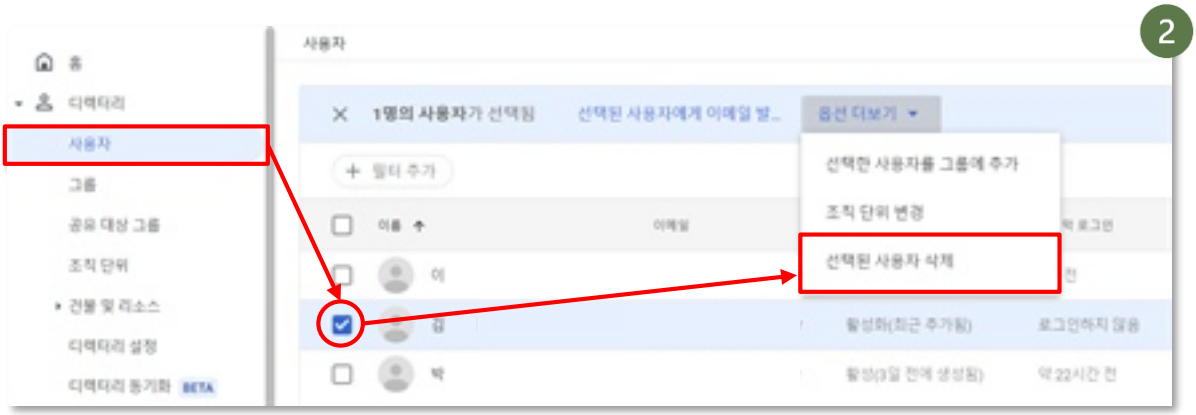
회사 임직원이 퇴사하거나 직무를 변경한 경우, 즉시 데이터에 대한 접근을 막아 정보 유출을 방지해야 합니다. 따라서 관리자는 임직원의 지위 변동 시 신속히 권한을 회수하거나 계정을 삭제해야 합니다.

관리 콘솔로 계정 삭제하기

① [구글 워크스페이스 관리 콘솔 접속] > [좌측 메뉴의 '디렉터리'의 '사용자' 선택]



② ['사용자' 화면에서 삭제할 계정을 선택] > [우측 상단 '옵션 더 보기' 클릭] > ['선택한 사용자 삭제' 선택] > [삭제 대상 계정의 이메일 및 데이터 이전 여부 결정 후 계정 삭제]



구글 워크스페이스에 접속하는 이유

기업용 구글 드라이브는 '구글 워크스페이스'의 일부로 포함되어 있습니다. 따라서 구글 워크스페이스 내 '관리 콘솔'에서 할 수 있는 설정 방법에 대하여 다룹니다. 본 가이드라인에서 설명하는 구글 워크스페이스의 라이선스는 'Business Standard' 입니다.

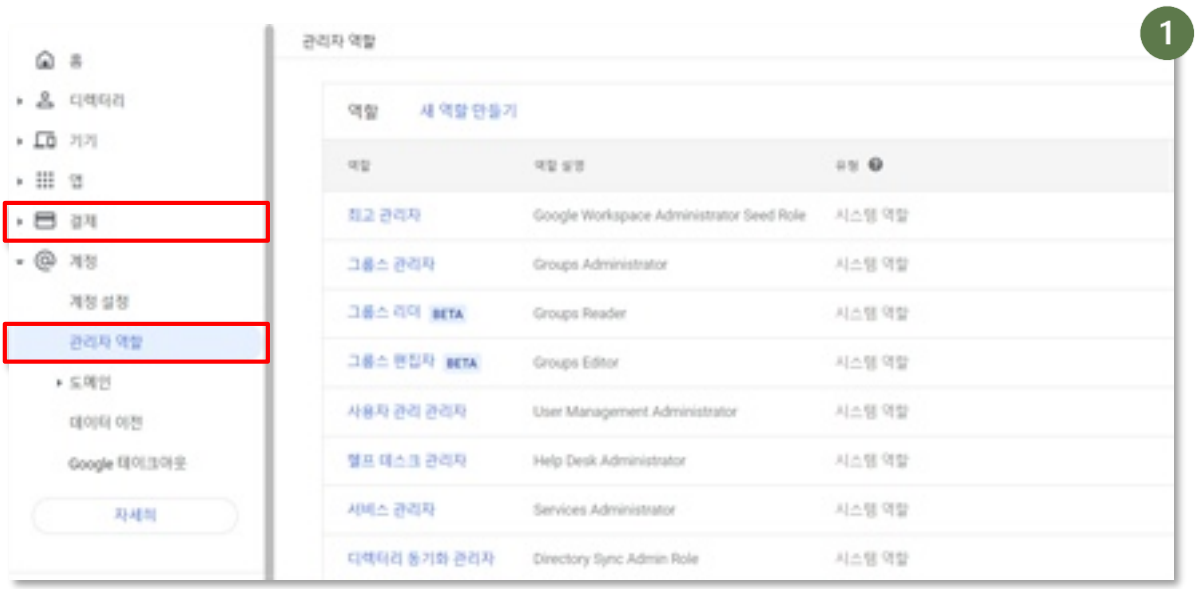
구글 드라이브(Google Drive)

2. 불필요한 권한 제거하기

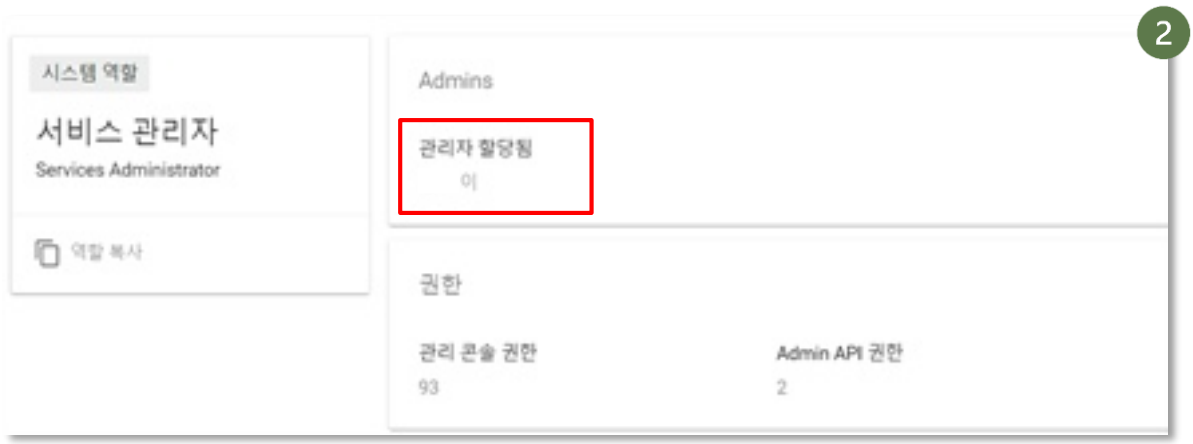
일반 계정 및 게스트용 계정에 불필요하게 많은 권한이 설정되어 있다면 공격자가 계정을 해킹한 뒤 공격하거나, 권한 없는 내부자가 영업비밀을 유출할 수 있습니다. 따라서 관리자는 임직원들의 권한이 필요 이상으로 부여되어 있지 않은지 반드시 확인해야 합니다.

관리자 그룹 관리하기

1. [관리 콘솔 좌측 메뉴에서 '계정'의 '관리자 역할' 선택] > ['관리자 역할' 화면에서 각 관리자의 역할을 클릭]

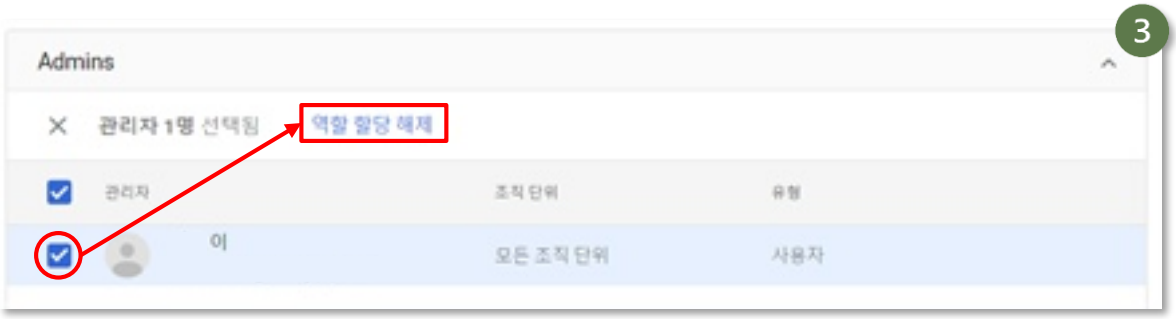


2. [각 관리자 역할에서 'Admins' 상자를 통해 누구에게 관리자 역할이 할당 되었는지 확인] > [적절하지 않은 계정이 있다면 'Admins' 상자 클릭]



구글 드라이브(Google Drive)

3 ['Admins' 화면에서 역할 할당을 해제할 계정을 선택] > ['역할 할당 해제' 클릭]



관리자의 역할

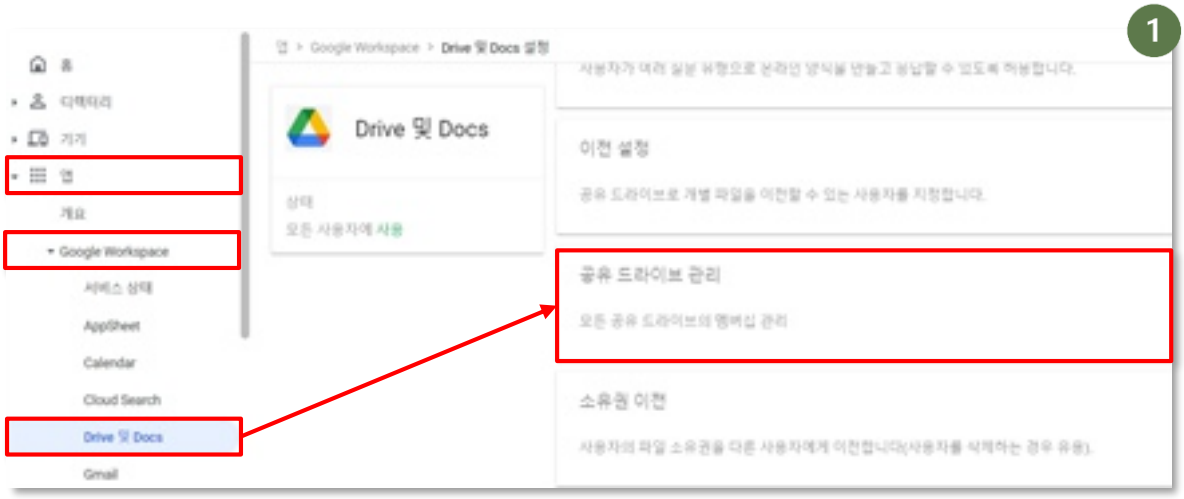
구글 워크스페이스에는 초기 설정으로 다양한 관리자 역할이 생성되어 있습니다. 각 관리자는 역할에 따라 권한 수준이 다르게 되어 있습니다.

따라서 최고 관리자는 각 임직원의 역할에 맞게 적절한 수준의 권한을 부여할 수 있습니다. 그리고 필요에 따라 조직에서 특별한 관리자 역할을 직접 생성하여 권한을 부여할 수도 있습니다. ('관리자 역할' > '새 역할 만들기')

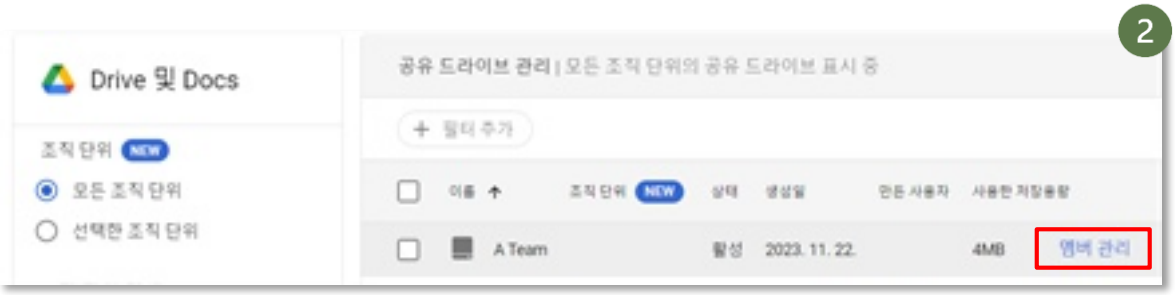
구글 드라이브(Google Drive)

공유 드라이브 접근 권한 제거하기

1 [관리 콘솔 좌측 메뉴에서 '앱' 의 'Google Workspace' - 'Drive 및 Docs' 선택] > ['공유 드라이브 관리' 상자를 클릭]

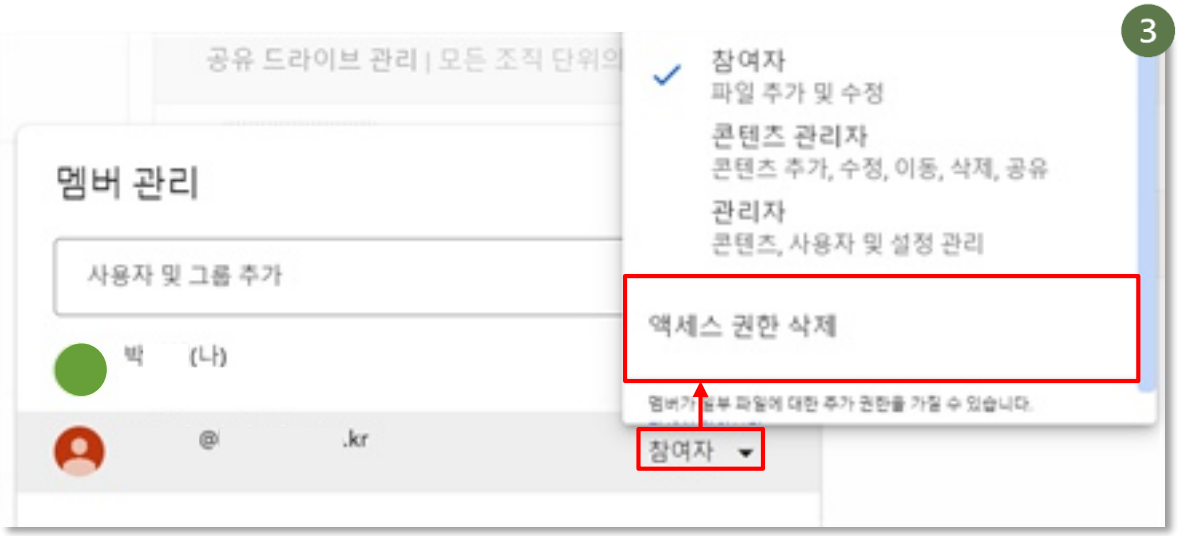


2 [접근 권한을 관리할 공유 드라이브의 '멤버 관리' 클릭]



구글 드라이브(Google Drive)

3 [권한을 삭제할 사용자 선택 후 '액세스 권한 삭제' 클릭]



공유 드라이브 접근 권한 변경하기

위 메뉴에서 공유 드라이브에 대한 접근 권한을 완전히 제거할 수도 있지만,
사용자마다 '액세스 권한'을 다양하게 부여할 수 있습니다.

권한의 종류는 '댓글 작성자', '참여자', '콘텐츠 관리자', '관리자'가 있고, 오른쪽으로 갈수록 권한이 높아집니다. 드라이브 사용 권한 또한 너무 많은 권한이 부여되지 않도록 관리하여야 합니다.

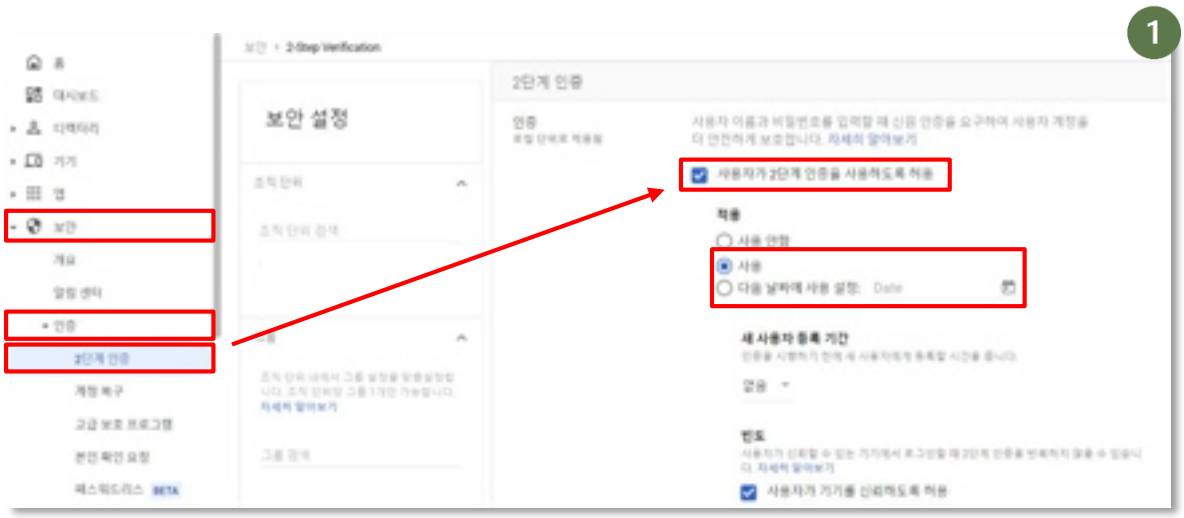
구글 드라이브(Google Drive)

3. 2단계 인증 설정하기

2단계 인증은 사용자가 로그인을 시도하는 경우, PC외 다른 기기를 통해 본인이 로그인을 하고 있음을 인증하는 기술입니다. 이를 통해 계정정보가 노출되어도 공격자가 로그인할 수 없도록 보안 조치를 할 수 있습니다.

관리 콘솔에서 2단계 인증 적용하기

1. [관리 콘솔 메뉴에서 '보안' 탭] > ['인증'에서 '2단계 인증' 선택] > ['사용자가 2단계 인증을 사용하도록 허용' 선택] > [2단계 인증을 강제 적용하려는 경우 '적용'에 '사용' 또는 '다음 날짜에 사용 설정' 선택]



구글 드라이브(Google Drive)

4. 비밀번호 설정 규칙 관리

구글 워크스페이스에 로그인하는 사용자에 대한 비밀번호 규칙을 지정할 수 있습니다.

조직에서 사용할 비밀번호 정책 구성하기

1. [관리 콘솔 메뉴의 '보안' 탭] > ['인증'에서 '비밀번호 관리' 클릭] > [아래 사진에 맞게 비밀번호 정책 설정]

권장하는 규칙	
항목	권장 값
안전한 비밀번호 적용	활성화
최소 비밀번호 길이	8자 이상
비밀번호 재사용 설정	비활성화
최대 비밀번호 사용 기간	90일 미만

구글 드라이브(Google Drive)

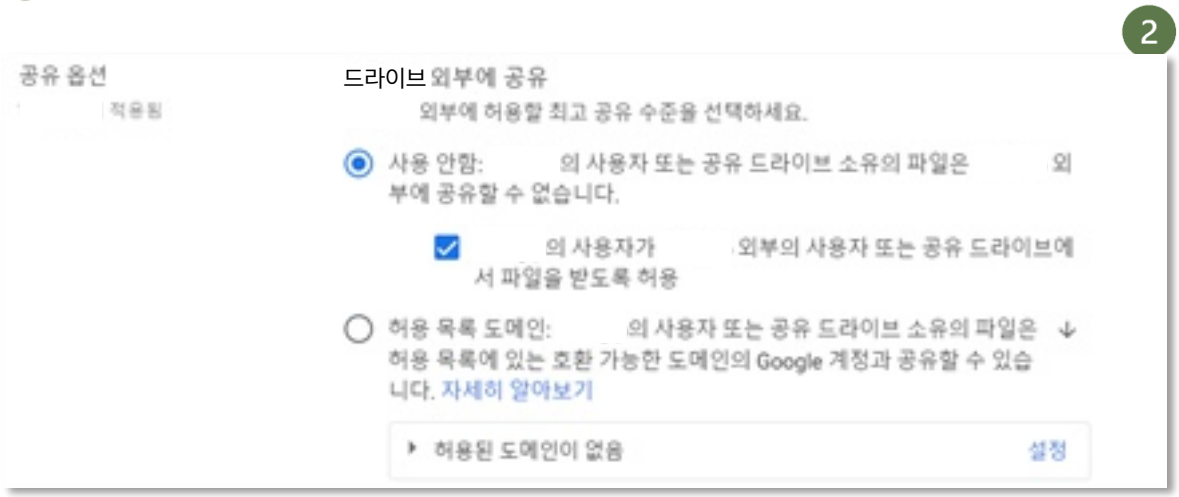
5. 외부 공유 금지하기

협력사 또는 고객에게 자료를 전달하기 위해서 회사 공유 드라이브에 접속할 수 있게 하는 경우가 있습니다. 이는 데이터 유출에 매우 취약합니다. 따라서 드라이브 외부 공유는 최대한 자제하여야 합니다.

외부 공유 설정 비활성화하기

1. [관리 콘솔 메뉴 '앱' 에서 'Google Workspace'-'Drive 및 Docs' 선택] > ['공유 설정' 상자 클릭]

2. ['공유 옵션' 클릭 후 '외부에 공유' 에서 '사용 안 함' 선택]



구글 드라이브(Google Drive)

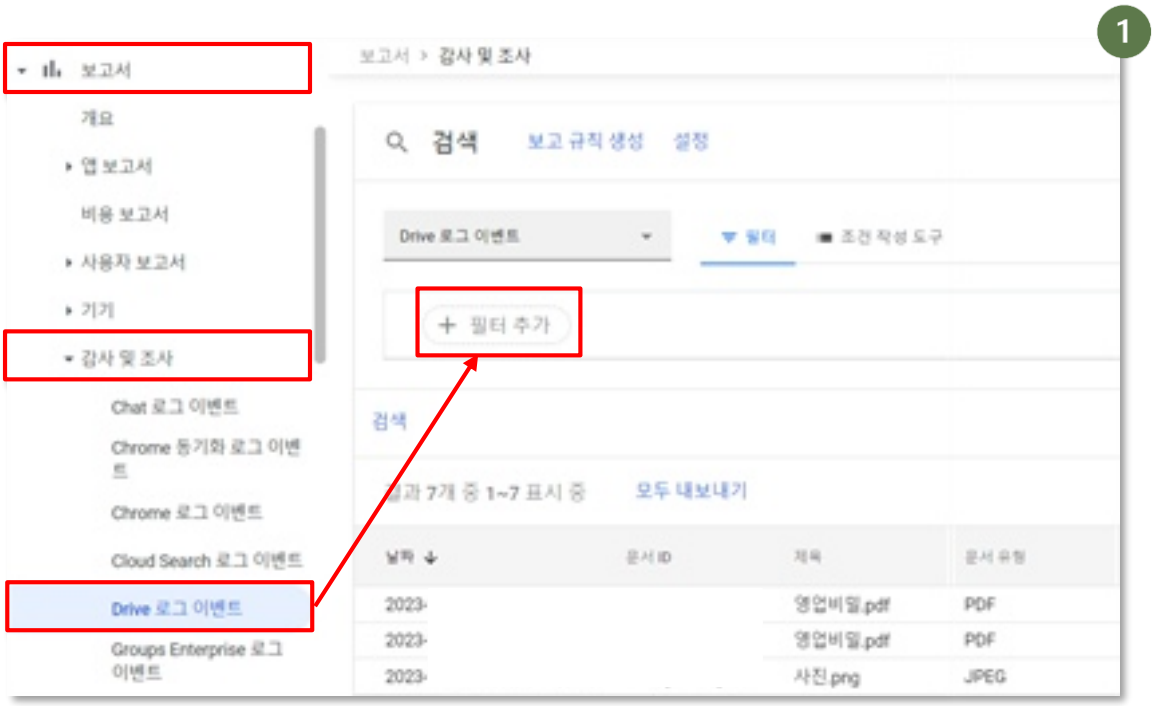
6. 로그 관리

공유 드라이브에 누가, 언제, 어떤 파일을 올리고 받아갔는지 추적하는 방법을 안내합니다.

특히 자료 유출 시 책임자를 추적하는 데 도움이 될 수 있습니다.

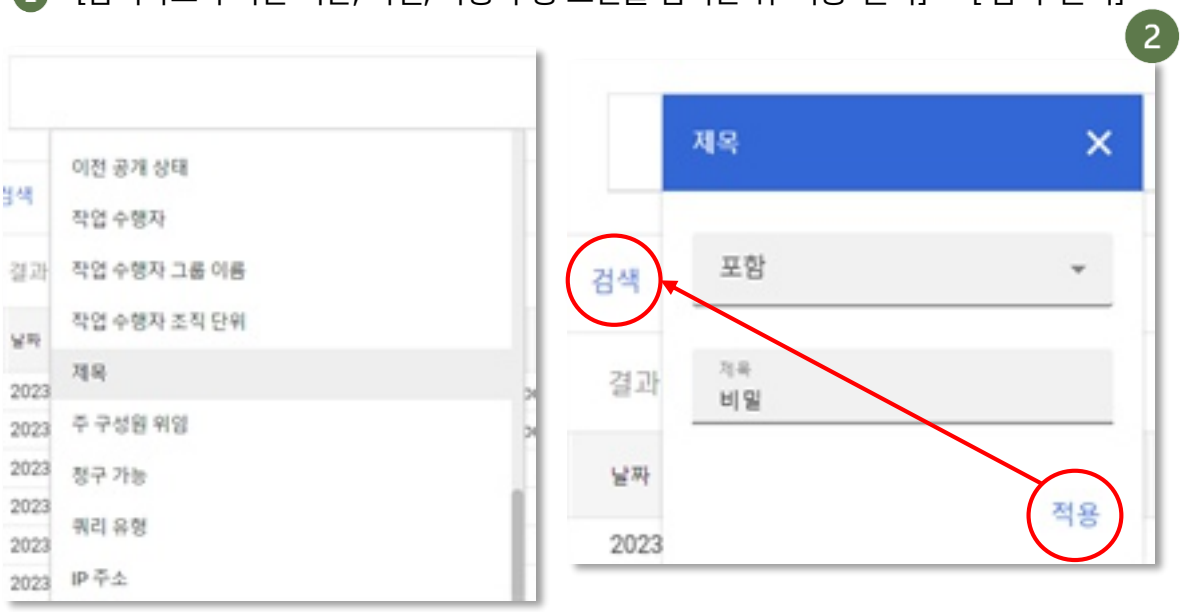
파일 관련 로그 확인하기

1. [관리 콘솔 메뉴의 '보고서'에서 '감사 및 조사' - 'Drive 로그 이벤트' 선택] > ['필터 추가' 클릭]



구글 드라이브(Google Drive)

2 [탐색하고자 하는 시간, 파일, 사용자 등 조건을 입력한 뒤 '적용' 클릭] > ['검색' 클릭]



3 [검색 결과로 나타난 로그 확인 (제목(파일명), 이벤트(보기, 업로드 …), 수행자, IP 등]

원 드라이브(OneDrive)

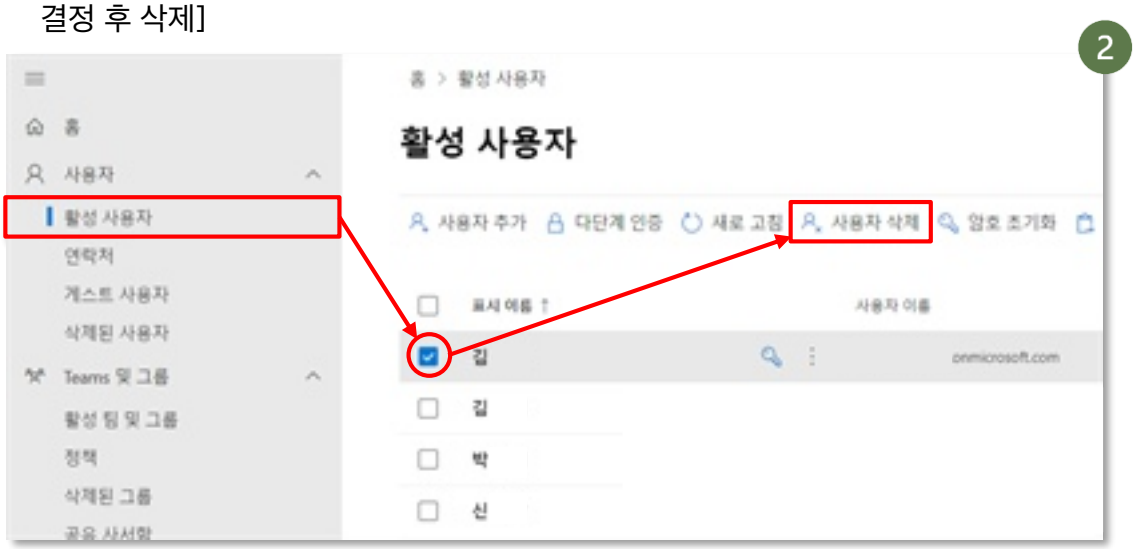
1. 퇴사자 계정 제거하기

회사 임직원이 퇴사하거나 직무를 변경한 경우, 즉시 데이터에 대한 접근을 막아 정보 유출을 방지해야 합니다. 따라서 관리자는 임직원의 지위 변동 시 신속히 권한을 회수하거나 계정을 삭제해야 합니다.

활성 사용자 계정 삭제하기

1. ['Microsoft 365 관리 센터' 접속]

2. [좌측 메뉴 '사용자'에서 '활성 사용자'선택] > ['활성 사용자' 화면에서 삭제할 계정을 선택] > [우측 상단 '사용자 삭제' 클릭] > [삭제 대상 계정의 이메일 및 데이터 이전 여부 결정 후 삭제]



관리 센터에 접속하는 이유

기업용 원 드라이브는 '마이크로소프트 365' 서비스의 일부로 포함되어 있습니다. 따라서 마이크로소프트 365 관리자 설정에서 할 수 있는 설정 방법에 대하여 다룹니다. 본 가이드라인에서 설명하는 마이크로소프트 365의 라이선스는 'Business Standard' 입니다.

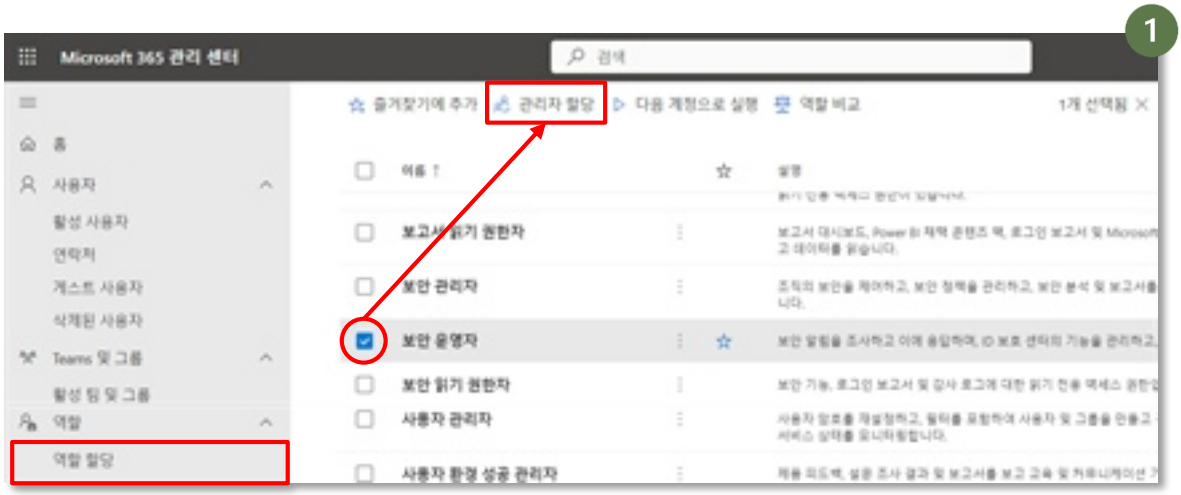
원 드라이브(OneDrive)

2. 불필요한 권한 제거하기

일반 계정 및 게스트용 계정에 불필요하게 많은 권한이 설정되어 있다면 공격자가 계정을 해킹한 뒤 공격하거나, 권한 없는 내부자가 영업비밀을 유출할 수 있습니다. 따라서 관리자는 임직원들의 권한이 필요 이상으로 부여되어 있지 않은지 반드시 확인해야 합니다.

관리자 그룹 관리하기

1 [관리 센터 좌측 메뉴에서 '역할'의 '역할 할당' 선택] > ['관리자 할당' 화면에서 각 관리자의 역할 선택 후 '관리자 할당' 클릭]



원 드라이브(OneDrive)

2 [각 관리자 역할에서 누구에게 관리자 역할이 할당되었는지 확인] > [적절하지 않은 계정이 있다면 이름 선택 후 '제거' 클릭]

관리자의 역할

원 드라이브에는 초기 설정으로 다양한 관리자 역할이 생성되어 있으며, 각 관리자는 역할에 따라 권한 수준이 다르게 설정되어 있습니다. 따라서 최고 관리자는 각 임직원의 역할에 맞게 적절한 수준의 권한을 부여할 수 있습니다.

원 드라이브(OneDrive)

3. 2단계 인증 설정하기

2단계 인증은 사용자가 로그인을 시도하는 경우, PC외 다른 기기를 통해 본인이 로그인을 하고 있음을 인증하는 기술입니다. 이를 통해 계정정보가 노출되어도 공격자가 로그인할 수 없도록 보안 조치를 할 수 있습니다.

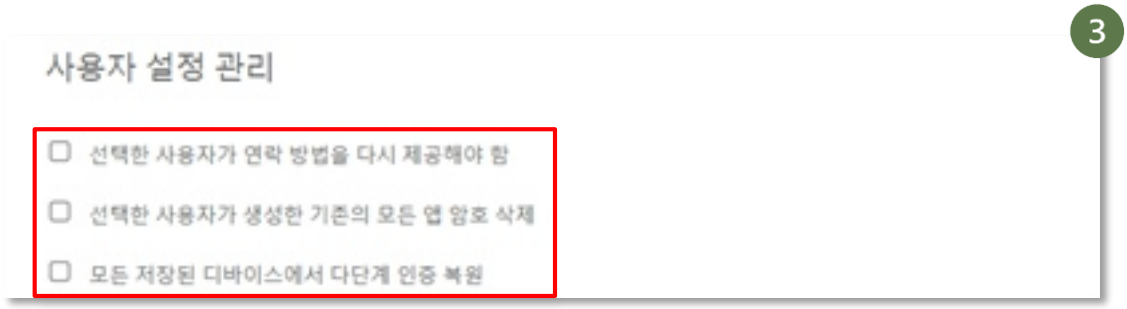
다단계 인증 기능 활용하기

1 [관리 센터 메뉴에서 '사용자'에서 '활성 사용자' 선택] > ['다단계 인증' 클릭]

2 [열린 창에서 다단계 인증을 적용할 계정 선택 후 '사용' 클릭]

원 드라이브(OneDrive)

3 [우측의 '사용자 설정 관리'에서 추가로 적용할 규칙 선택(선택 사항)]



설정에 대한 설명	
설정 항목	**상세 내용**
선택한 사용자가 연락 방법을 다시 제공해야 함	선택한 계정의 2단계 인증 계정 정보를 초기화하여 다시 설정하게 하는 설정입니다.
선택한 사용자가 생성한 기존의 모든 앱 암호 삭제	앱 암호란 microsoft365를 웹 브라우저가 아닌 전용 프로그램을 통해 사용할 때, 해당 프로그램을 사용하기 위한 비밀번호입니다. 본 설정은 기존에 생성된 앱 암호를 초기화하는 것 입니다.
모든 저장된 디바이스에서 다단계 인증 복원	해당 계정이 연결된 모든 기기에서 2단계 인증을 수행하도록 하는 설정입니다.

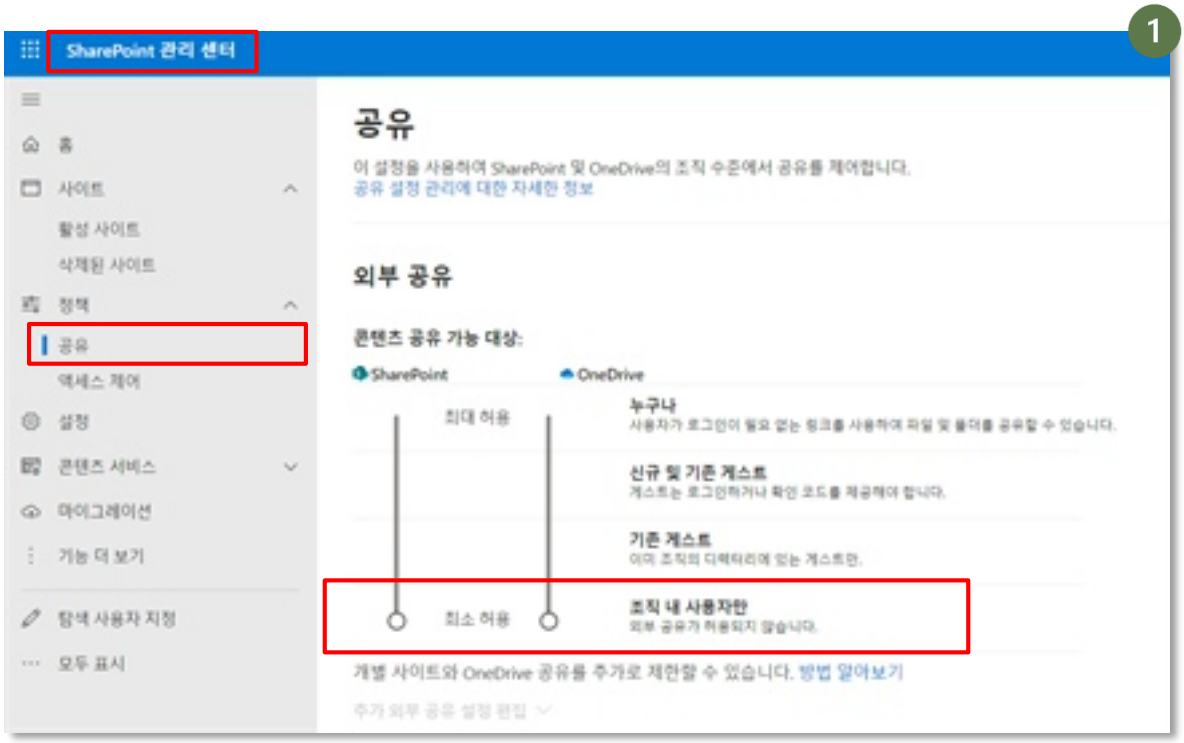
원 드라이브(OneDrive)

4. 외부 접근 차단하기

협력사 또는 고객에게 자료를 전달하기 위해서 회사 공유드라이브에 접속할 수 있게 하는 경우가 있습니다. 이는 데이터 유출에 매우 취약합니다. 따라서 드라이브 외부 공유는 최대한 자제하여야 합니다.

외부 접근 차단하기

1. [메뉴의 '관리 센터'의 'SharePoint'를 클릭해 'SharePoint 관리 센터' 접속] > [좌측 메뉴의 '정책'에서 '공유' 선택] > [외부 공유의 '컨텐츠 공유 가능 대상'을 SharePoint와 OneDrive 모두 '최소 허용' 선택]



2. [하단 파일 및 폴더 링크의 '사용자가 SharePoint 및 OneDrive에서 파일 및 폴더를 공유할 때 기본적으로 선택 되는 링크의 유형'을 '조직 내 사용자만'으로 선택] > [최하단의 '저장' 클릭]

원 드라이브(OneDrive)

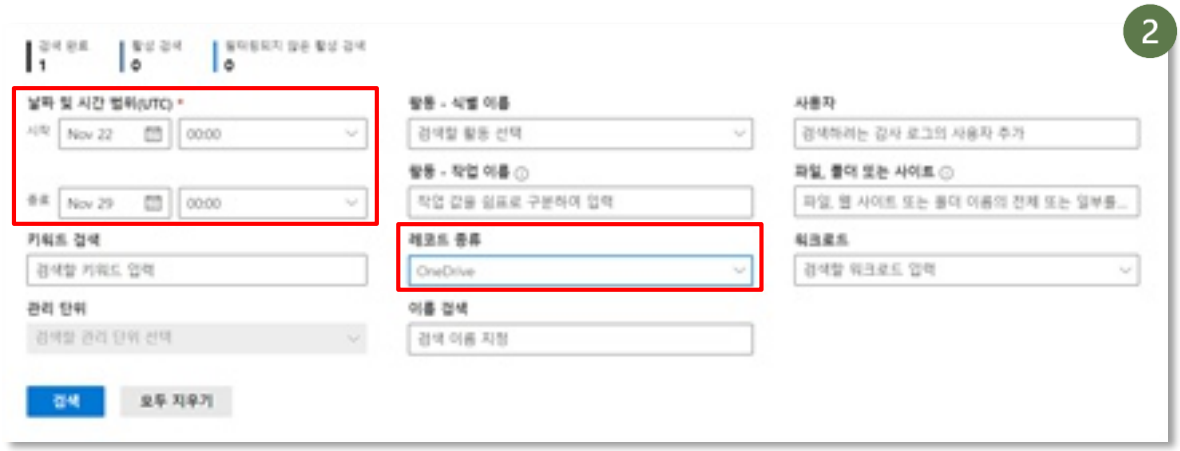
5. 로그 관리하기

공유 드라이브에 누가, 언제, 어떤 파일을 올리고 받아갔는지 추적하는 방법을 안내합니다.
특히 자료 유출 시 책임자를 추적하는 데 도움이 될 수 있습니다.

로그 관리하기

1. [메뉴의 '관리 센터'의 '보안'을 클릭해 'Microsoft Defender' 접속] > [좌측 메뉴 에서 '감사' 선택] > [상단의 '새로지정' 클릭]

2. [검색할 날짜 및 시간 범위 지정] > ['레코드 종류' 'OneDrive'로 지정] > [검색 수행 후 결과 확인]



드롭박스(Dropbox)

1. 퇴사자 계정 제거하기

회사 임직원이 퇴사하거나 직무를 변경한 경우, 즉시 데이터에 대한 접근을 막아 정보 유출을 방지해야 합니다. 따라서 관리자는 임직원의 지위 변동 시 신속히 권한을 회수하거나 계정을 삭제해야 합니다.

불필요한 계정 삭제하기

1. [드롭박스 관리콘솔 접속] > [좌측 메뉴의 '팀원' 선택]

2. ['팀원' 화면에서 삭제할 계정을 선택] > [우측 '⋯' 클릭] >
['삭제' 선택] > [삭제 대상 계정의 이메일 및 데이터 이전 여부 결정 후 삭제]

드롭박스 관리콘솔 라이선스

이번에는 드롭박스 내 '관리 콘솔'에서의 설정 방법에 대하여 다룹니다. 본 가이드라인에서 설명하는 드롭박스의 라이선스는 'Business' 입니다.

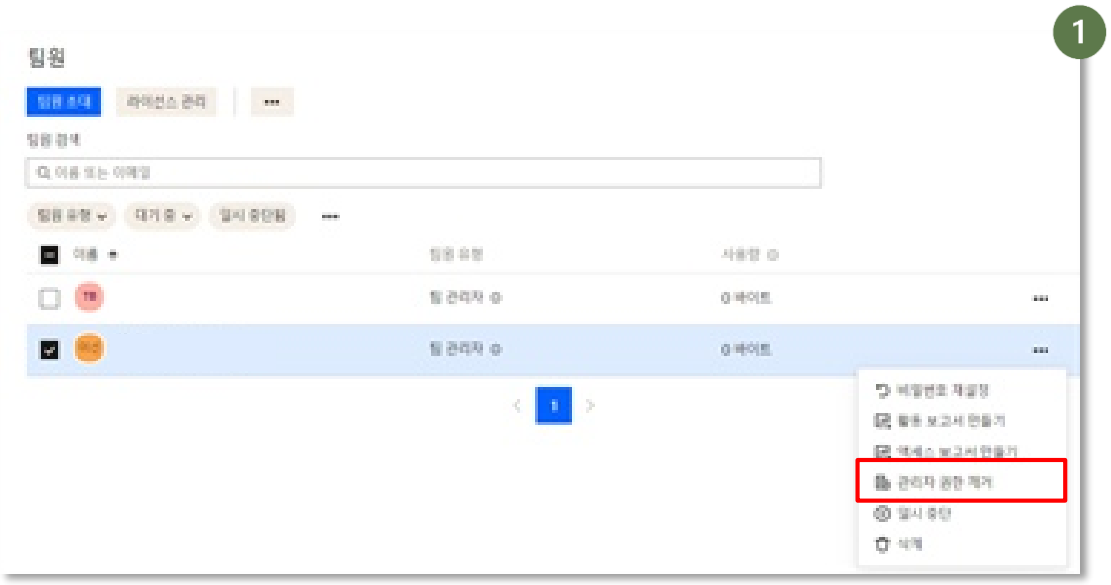
드롭박스(Dropbox)

2. 불필요한 권한 제거하기

일반 계정 및 게스트용 계정에 불필요하게 많은 권한이 설정되어 있다면 공격자가 계정을 해킹한 뒤 공격하거나, 권한 없는 내부자가 영업비밀을 유출할 수 있습니다. 따라서 관리자는 임직원들의 권한이 필요 이상으로 부여되어 있지 않은지 반드시 확인해야 합니다.

팀 관리자 권한 관리하기

1. [관리 콘솔 좌측 메뉴에서 '팀원' 선택] > ['팀원 유형'이 '관리자' 되어 있는 사람 중 관리자 권한을 해제할 사람을 선택] > [우측 ··· 클릭] > ['관리자 권한 제거' 선택]



관리자의 유형

드롭박스에는 관리자의 유형을 8개로 나누어 제공하고 있습니다. 이는 팀 관리자, 사용자 관리자, 지원 관리자, 청구 관리자, 콘텐츠 관리자, 규정준수 관리자, 보고 관리자, 보안 관리자의 총 8개 입니다. 각 관리자 마다 권한이 서로 다르기 때문에 회사 임직원의 역할에 따라 너무 많은 권한이 부여되지 않도록 하여야 합니다.

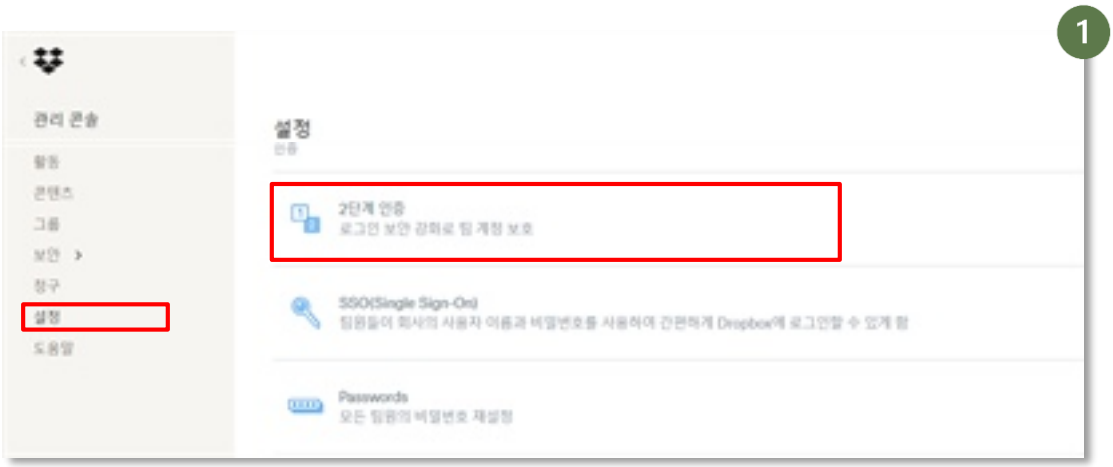
드롭박스(Dropbox)

3. 2단계 인증 설정하기

2단계 인증은 사용자가 로그인을 시도하는 경우, PC외 다른 기기를 통해 본인이 로그인을 하고 있음을 인증하는 기술입니다. 이를 통해 계정정보가 노출되어도 공격자가 로그인할 수 없도록 보안 조치를 할 수 있습니다.

2단계 인증 필수사항으로 지정하기

1 [관리 콘솔 메뉴에서 '설정' 선택] > ['인증'에서 '2단계 인증' 클릭]



2 [2단계 인증 '필수 사항' 선택] > ['저장' 클릭]

정책 변경 후 팀원은 모두 2단계 인증 수단을 지정하여야 로그인 가능]

드롭박스(Dropbox)

4. 외부 접근 차단하기

협력사 또는 고객에게 자료를 전달하기 위해서 회사 공유드라이브에 접속할 수 있게 하는 경우가 있습니다. 이는 데이터 유출에 매우 취약합니다. 따라서 드라이브 외부 공유는 최대한 자제하여야 합니다.

모든 공유설정 비활성화 하기

1. [관리 콘솔 메뉴의 '설정' 선택 > ['콘텐츠'의 '공유' 클릭]

2. ['팀 외부 사람과 공유'에서 아래 사진과 같이 비활성화 (모두 '꺼짐' 및 '해제'로 변경)] > [최하단의 '저장' 클릭]

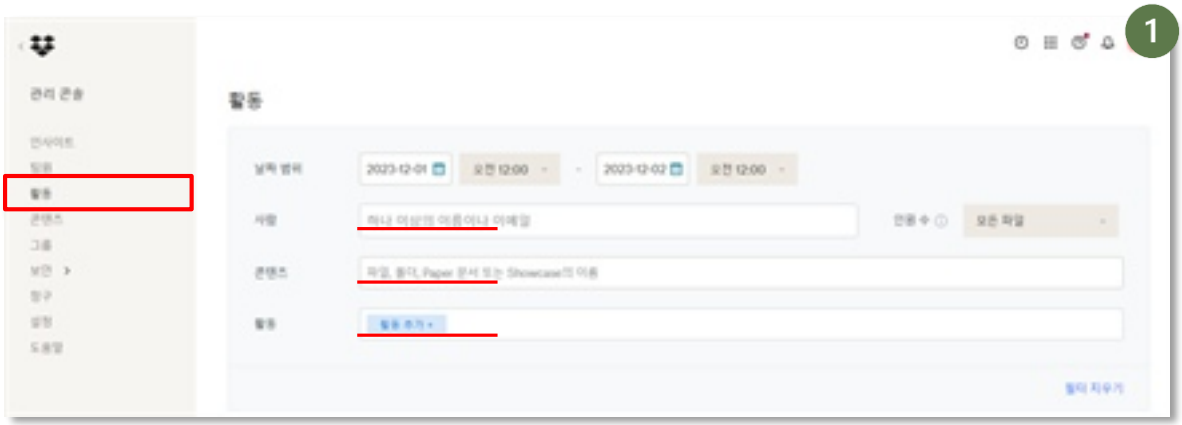
드롭박스(Dropbox)

5. 로그 관리

공유 드라이브에 누가, 언제, 어떤 파일을 올리고 받아갔는지 추적하는 방법을 안내합니다.
특히 자료 유출 시 책임자를 추적하는 데 도움이 될 수 있습니다.

멤버 활동 로그 확인하기

1. [관리 콘솔 메뉴의 '활동' 선택] > [검색 조건 입력 (사람, 기간, 파일명 등)] > [검색 수행 후 결과 확인] > [파일 관련 로그 외에도 팀원의 활동에 관한 다양한 로그 확인 가능]



2. (로그인 로그 예시)

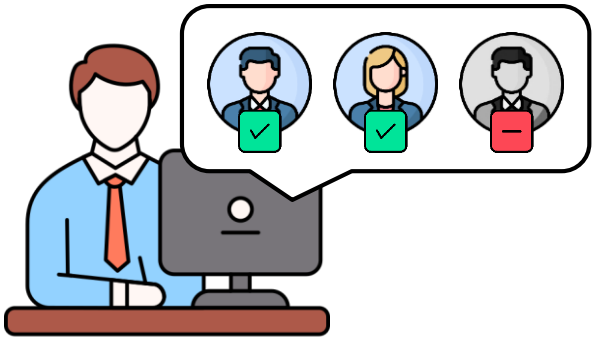
로그 데이터 분석하기	
항목	주의해야 할 로그 데이터
날짜 정보	근무 시간 및 날짜 외에 로그인 시도
활동 분석	기존과 다른 방법을 이용한 로그인 시도
로그인 성공 여부	여러 번의 실패한 로그인 시도
액세스 디바이스 정보	특정 사용자가 기존과 다른 디바이스로 로그인 시도
위치 정보	한 계정으로 여러 지역에서 동시에 로그인 시도

이것만은 지키자!

행동수칙

협업툴 편

1



퇴사자의 계정을 삭제해요!

퇴사자의 계정 정보를 퇴사 즉시 삭제하거나 변경하지 않으면, 퇴사자가 회사의 중요 정보에 계속 접근할 수 있게 되어 위험할 수 있습니다. 이로 인해 회사의 중요 데이터 유출, 무단 접근 등의 위험을 초래할 수 있으므로 퇴사자 관리는 필수입니다. 퇴사자 관리는 기업의 정보 보안을 유지하고, 비즈니스 연속성을 보장하는 데 매우 중요한 역할을 합니다.

USB와 같은 저장매체를 사용하지 않아요!

이동식 저장매체는 분실, 도난 등으로 데이터가 유출되거나 알려지지 않은 보안 위협이 존재할 수 있습니다. 중요한 데이터는 내부 네트워크, 클라우드 서비스를 통해 안전하게 공유, 저장해야 합니다.

이번 편에서는 팀 단위 업무의 편리를 위해 사용하는 협업 도구인 협업툴을 안전하게 사용하는 방법을 안내합니다. 대표적인 협업툴인 슬랙, 네이버웍스, 플로우에 대한 보안 설정을 다룹니다.

협업툴이란 무엇인가요?

팀원들이 함께 작업을 수행하고 공동의 목표를 달성하기 위해 사용하는 디지털 도구를 의미합니다. 이 도구를 통해 프로젝트 관리, 문서 공유, 실시간 커뮤니케이션, 일정 관리 등 다양한 기능을 제공하여 팀의 생산성을 향상하고, 작업의 효율성을 높일 수 있습니다. 슬랙, 네이버웍스, 플로우 등이 대표적인 예시로, 원격으로 작업하는 팀원들 사이의 소통을 원활하게 하며, 정보를 효과적으로 공유할 수 있게 돕습니다.

협업툴 보안을 왜 해야 할까요?

협업 도구의 보안은 회사의 중요 정보를 보호하고, 악의적인 사이버 공격을 방지하는 데 필수적입니다. 이 도구들은 회사의 중요한 데이터를 저장하고 공유하는 공간이므로, 외부 유출이나 해킹 공격 등의 위협으로부터 안전하게 보호할 필요가 있습니다.

가이드라인에서 다루는 제품 확인하기

slack NAVER WORKS flow

▲ 슬랙(Slack) ▲ 네이버웍스(NAVER WORKS) ▲ 플로우(flow)

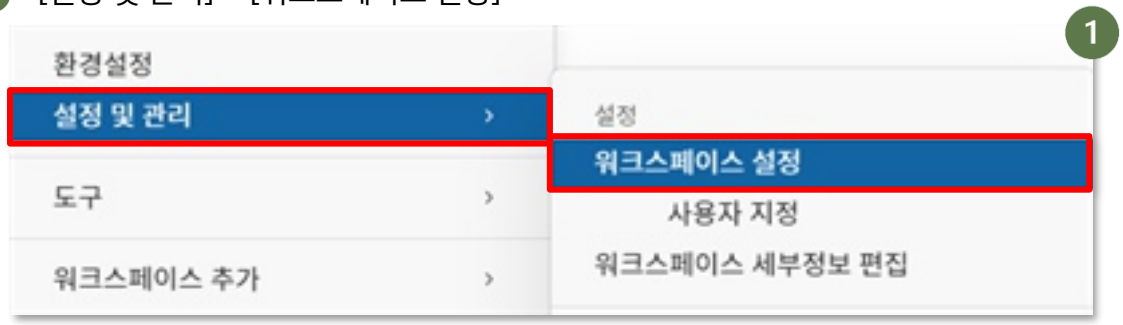
슬랙(Slack)

1. 계정 로그인 관리 설정하기

협업 툴은 회사의 중요한 사업 정보를 공유하고 관리하는 플랫폼입니다. 이런 정보는 민감한 데이터를 포함할 수 있으며, 허락 없이 이를 확인하거나 수정하는 것을 방지할 필요가 있습니다. 계정 로그인 관리를 통해 사용자의 인증을 확인하고, 무단 접근을 방지함으로써 정보를 보호해야 합니다.

워크스페이스 2단계 인증 활성화 하기

1. [설정 및 관리] > [워크스페이스 설정]



2. [인증] > [워크스페이스의 2단계 인증(2FA)] > ['워크스페이스를 위한 2단계 인증' 활성화]

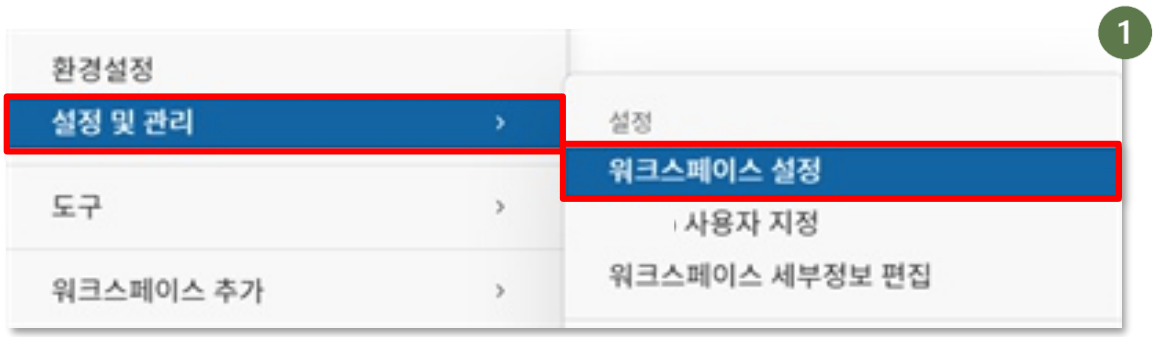
2단계 인증(2FA)이란?

사용자의 아이디와 비밀번호 외에 다른 인증 수단을 추가로 요구하는 보안 방식입니다. 일반적으로 휴대전화로 전송되는 일회용 코드가 이에 해당하며, 이를 통해 무단 접근을 방지하고 보안을 강화합니다.

슬랙(Slack)

자동 로그아웃 기간 설정하기

1 [설정 및 관리] > [워크스페이스 설정]



2 [인증] > [세션 기간 활성화]

세션 기간이란?

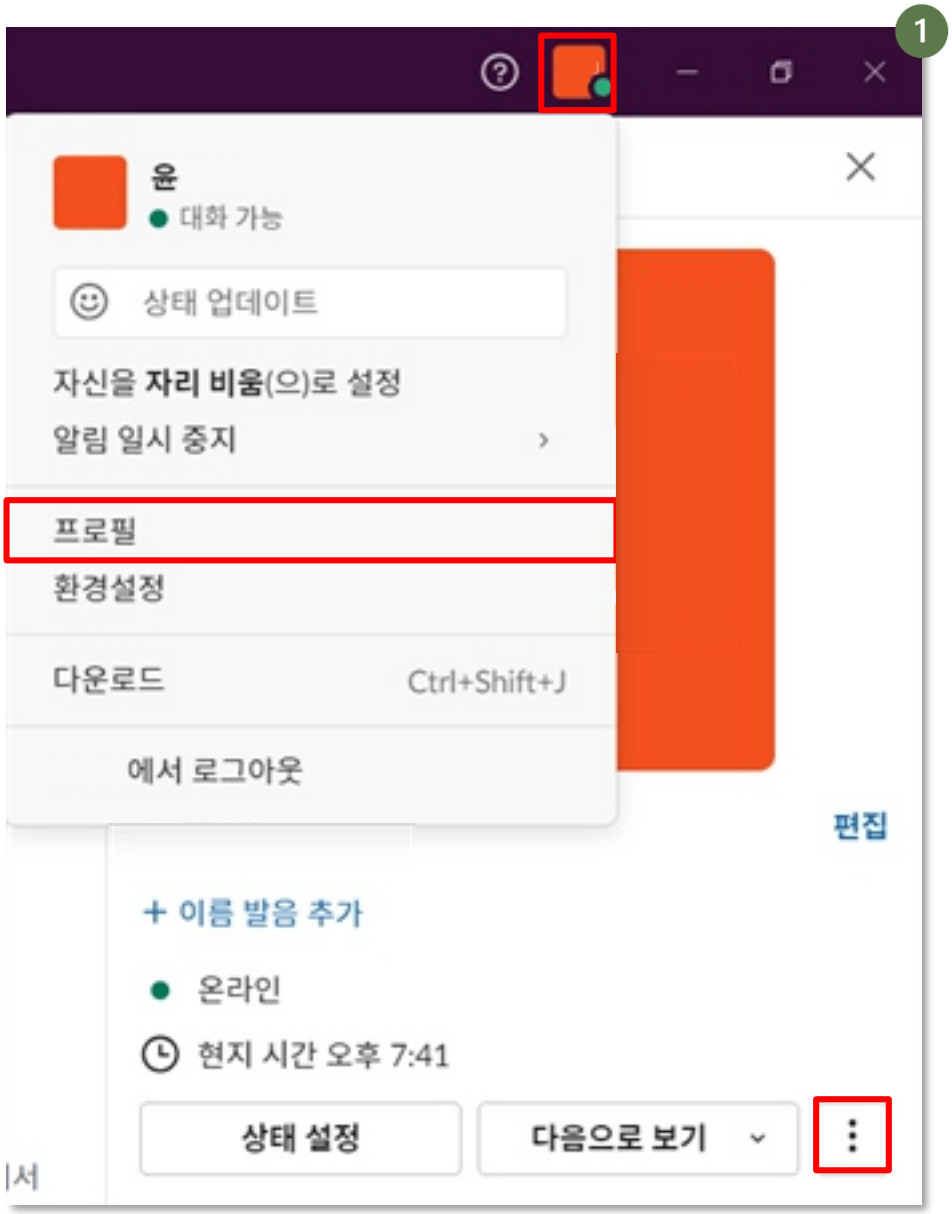
사용자가 웹사이트나 애플리케이션에 로그인한 후 일정 시간 동안 활동 없이 그대로 두었을 때, 자동으로 로그아웃되는 시간입니다. 이는 사용자 계정의 보안을 위해 사용되는 기능으로, 만약 사용자가 로그아웃 하는 것을 잊어버렸을 경우, 누군가 그 계정을 잘못 사용하는 것을 막기 위한 것입니다.

세션 기간이 설정되면, 사용자가 설정된 시간 동안 아무런 활동을 하지 않으면 자동으로 로그아웃되어, 계정 정보를 보호할 수 있습니다.

슬랙(Slack)

기기가 분실된 경우 로그아웃하기

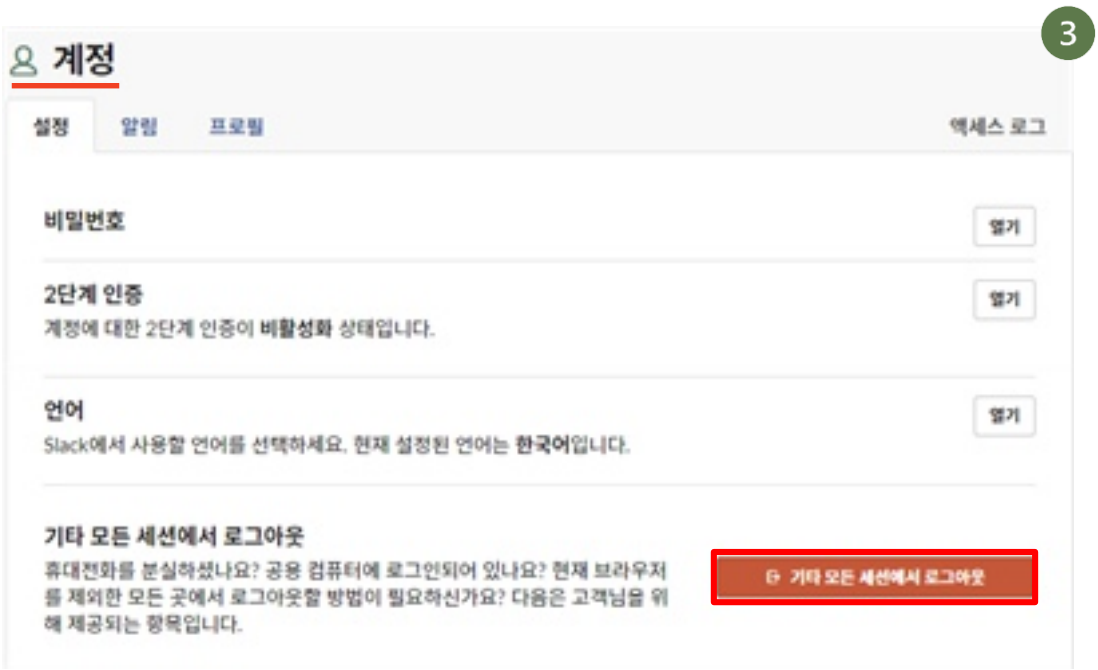
1 [데스크톱 상단 프로필 선택] > [프로필] > [하단 ' ⋮ ' 클릭]



슬랙(Slack)

2 [계정 설정]

3 [계정] > [설정] > [기타 모든 세션에서 로그아웃]



분실된 기기의 로그아웃 왜 필요할까요?

협업툴을 사용하는 장치가 분실된 경우 해당 기기를 통해 기업의 중요 정보가 유출될 위험이 있습니다. 이를 방지하기 위해 분실 즉시 멤버 로그아웃을 설정하여 분실된 장치를 통한 사고 발생 가능성을 줄이고 회사의 보안 위협을 최소화 할 수 있습니다..

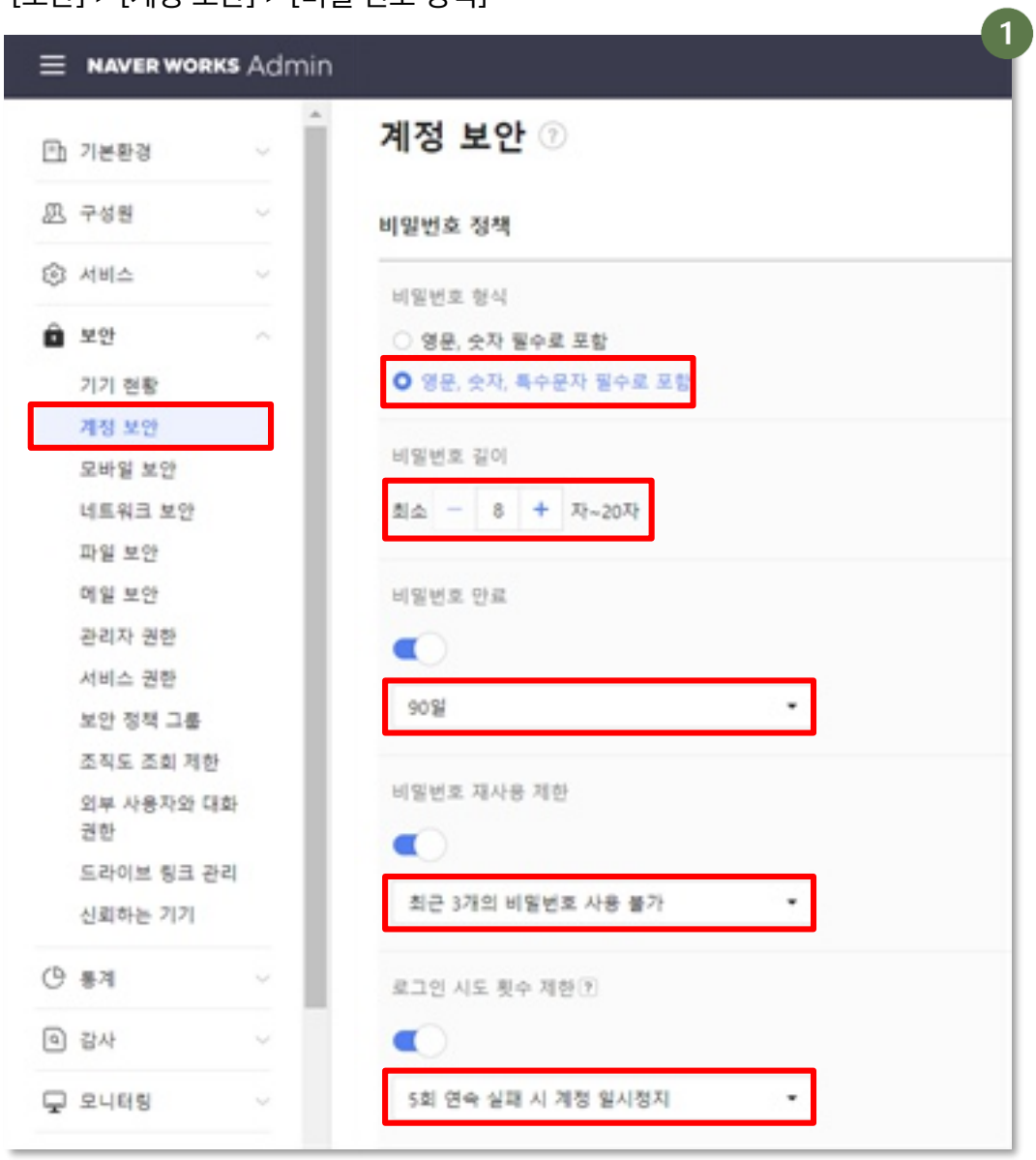
네이버웍스(NAVER WORKS)

1. 계정 로그인 관리 설정하기

협업 툴은 회사의 중요한 사업 정보를 공유하고 관리하는 플랫폼입니다. 이런 정보는 민감한 데이터를 포함할 수 있으며, 허락 없이 이를 확인하거나 수정하는 것을 방지할 필요가 있습니다. 계정 로그인 관리를 통해 사용자의 인증을 확인하고, 무단 접근을 방지함으로써 정보를 보호해야 합니다.

안전한 비밀번호 정책 설정하기

1 [보안] > [계정 보안] > [비밀 번호 정책]

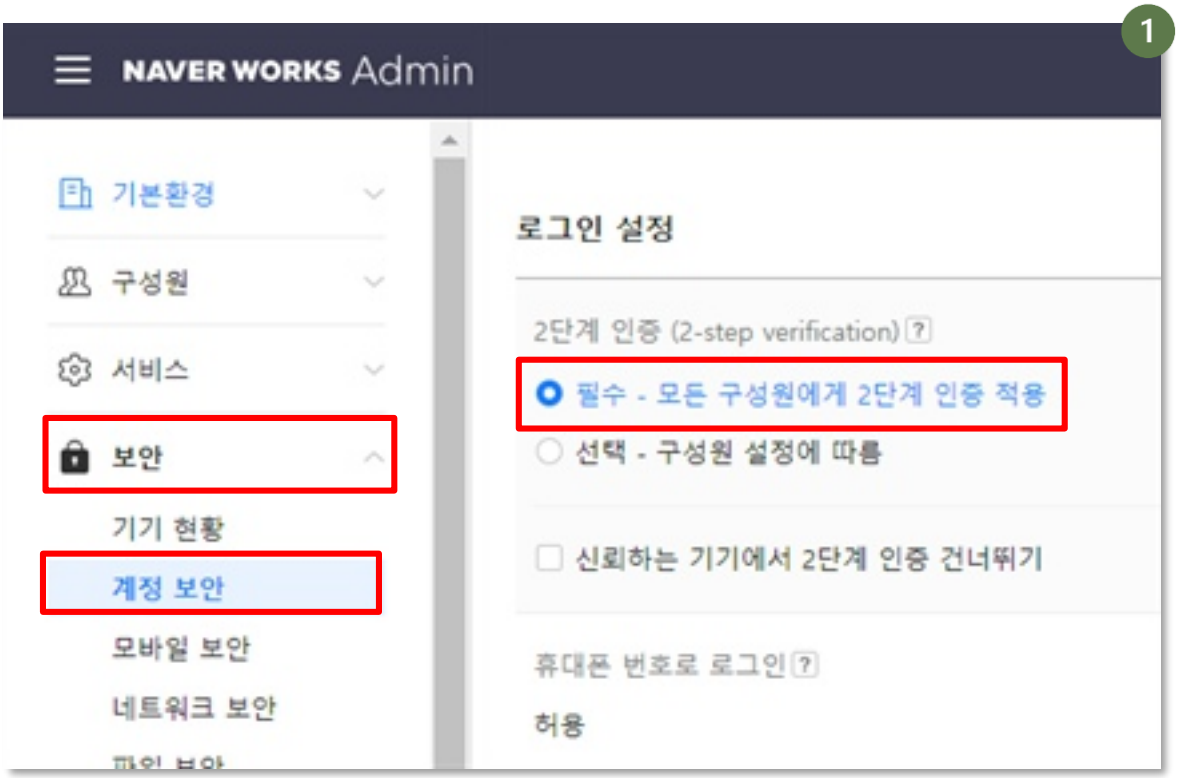


네이버웍스(NAVER WORKS)

설정항목	안전한값	상세설명
비밀번호 형식	영문, 숫자, 특수문자 포함	비말번호 구성을 영문, 숫자, 특수문자를 모두 포함하도록 제한
비밀번호 길이	8자 이상	비밀번호의 최소 길이 조건을 두는 설정
비밀번호 만료	90일 이상	같은 비밀번호를 변경없이 사용할 수 있는 최대 기간 설정
비밀번호 재사용 제한	3개 이상	사용자가 동일한 비밀번호를 반복 사용하는 것을 막기 위한 설정
로그인 시도 횟수 제한	5회 이하	계정 유출을 막기위해 연속으로 비밀번호를 틀리면 계정을 일시정지하는 설정

2단계 인증 활성화하기

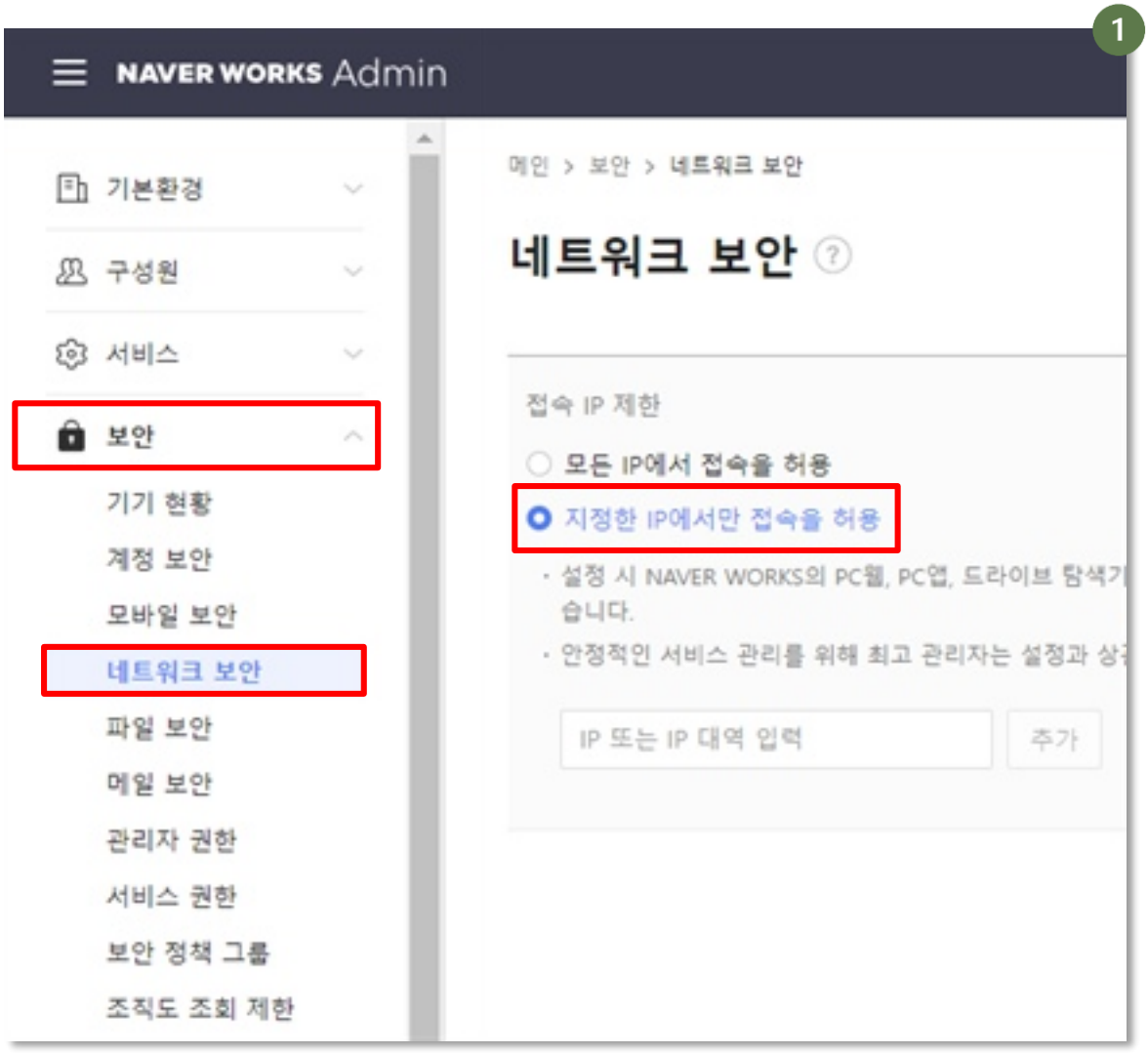
1. [보안] > [계정 보안] > [로그인 설정] > [2단계 인증] > [필수] > [모든 구성원에게 2단계 인증 적용]



네이버웍스(NAVER WORKS)

접속 IP 제한 설정하기

1 [보안] > [네트워크 보안] > [접속 IP 제한] > ['지정한 IP에서만 접속을 허용' 설정]



접속 IP 제한 설정이 필요한 이유?

접속 IP 제한 설정은 특정 IP주소에서만 시스템에 접근을 허용하여 기업의 중요 정보를 보호하고 불필요한 침입을 방지할 수 있는 기능입니다.

이는 허가되지 않은 접근을 효과적으로 방지하며, 특히 원격 근무나 다양한 위치에서 작업하는 경우 발생할 수 있는 위협을 방지하는 데 사용합니다.

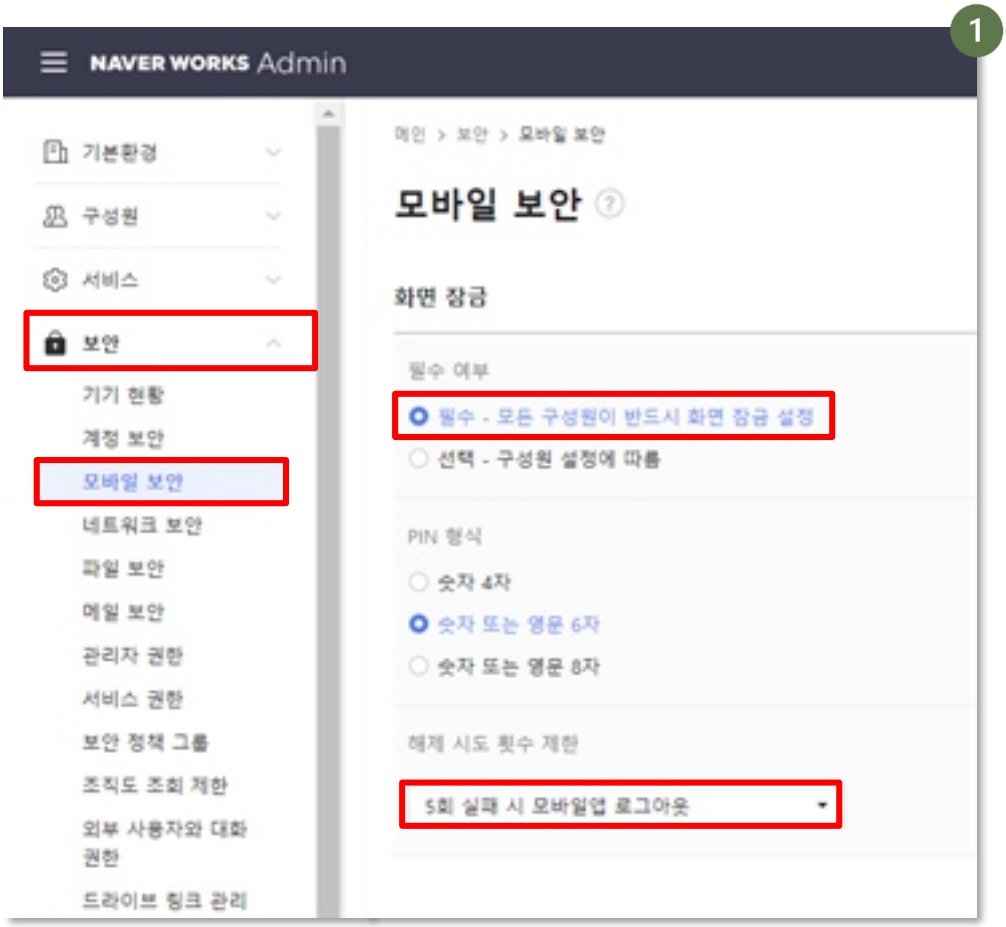
네이버웍스(NAVER WORKS)

2. 모바일 보안 설정하기

모바일을 통해 협업툴을 실행할 경우 본의 아니게 회사의 중요 정보가 노출될 수 있습니다. 모바일 화면 잠금 설정을 통해 이를 막을 수 있습니다. 잠금 설정을 통해 잘못된 사람에게 기기가 넘어가거나, 잃어버렸을 때 불법적인 접근을 막을 수 있습니다.

화면 잠금 설정하기

1 [보안] > [모바일 보안] > [화면 잠금] > [하단의 권장하는 규칙을 참고하여 설정]



권장하는 규칙	
항목	권장 값
필수 여부	필수- 모든 구성원이 반드시 화면 잠금 설정
해제 시도 횟수 제한	5회 실패 시 모바일앱 로그아웃 설정

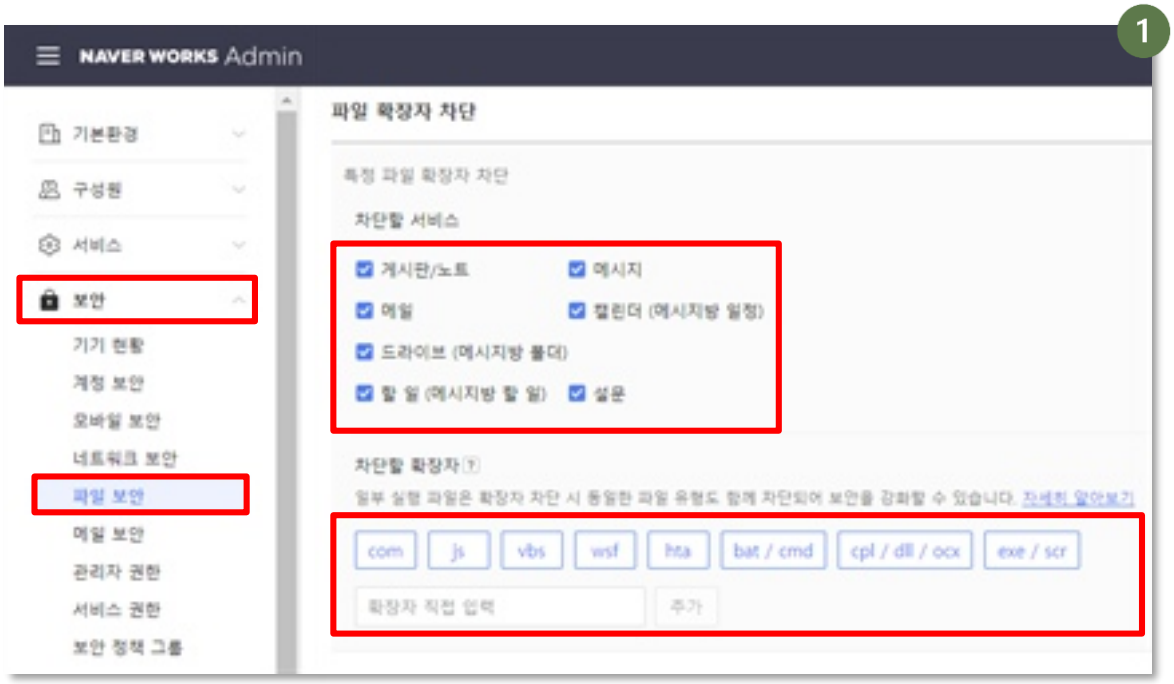
네이버웍스(NAVER WORKS)

3. 파일 보안 설정하기

협업툴은 회사내 다양한 부서와 직원들이 함께 작업하고 정보를 공유하는 도구입니다. 이런 공유 공간에서 파일 보안 설정이 소홀하다면 회사 내부에서만 공유되어야 하는 중요한 문서나 데이터가 외부로 유출될 수 있습니다.

파일 확장자 관리하기

1. [보안] > [파일 보안] > [파일 확장자 차단] > [특정 파일 확장자 차단] > [차단할 서비스/확장자 선택]



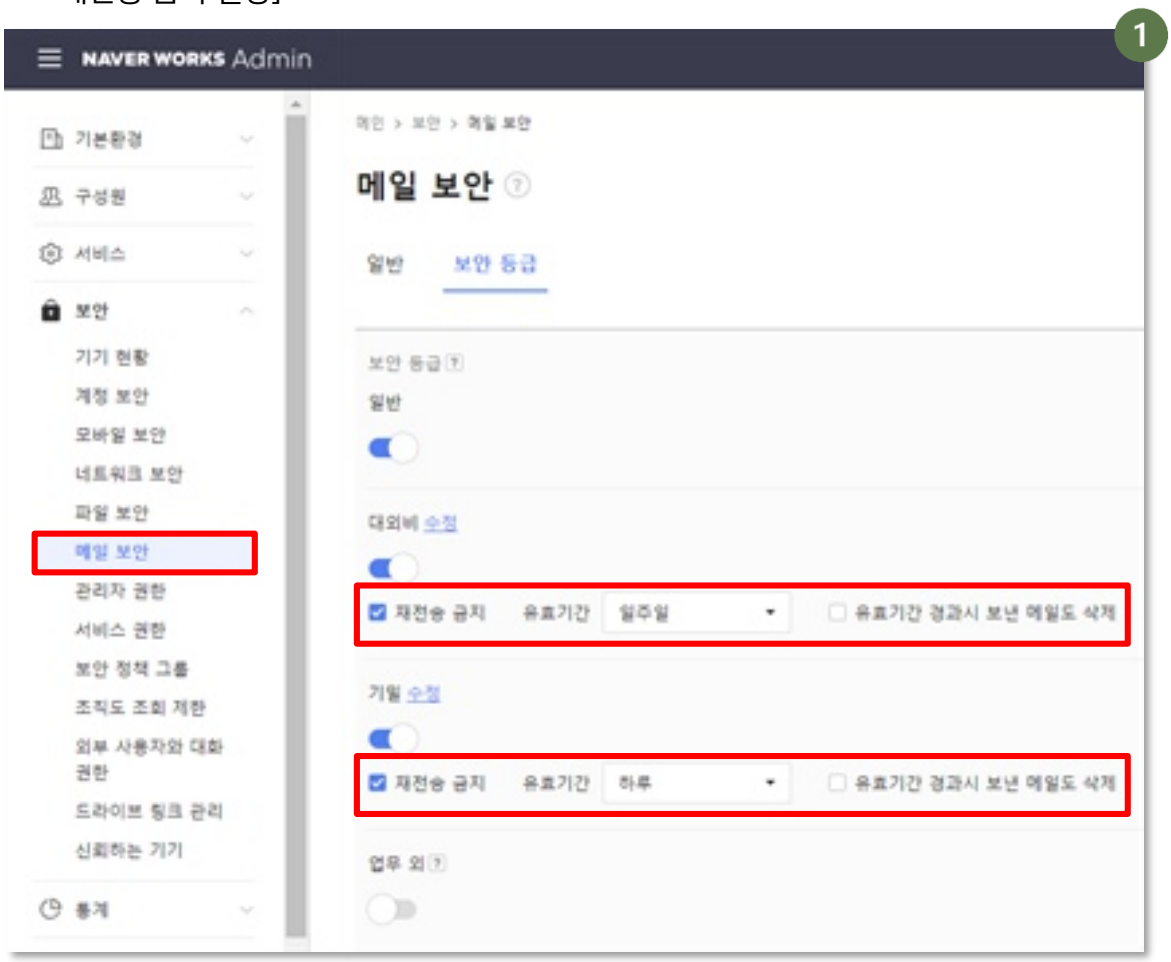
확장자 관리가 필요한 이유

협업툴에서 파일 확장자를 제한하는 것은 악성 코드나 바이러스의 유입을 막는 중요한 보안 조치입니다. 일부 파일 확장자(.exe, .bat 등)를 통해 악성 코드가 실행 될 수 있습니다. 따라서, 이러한 위험성을 줄이기 위해 협업 툴에서 특정 확장자의 파일 업로드를 제한하는 것이 필요합니다.

네이버웍스(NAVER WORKS)

문서의 보안 등급 설정하기

1 [보안] > [메일 보안] > [보안 등급] > [일반/대외비/기밀 등급 설정] > [유효기간 및 재전송 금지 설정]



각 설정별 의미

일반: 메일의 유효기간이 설정되지 않으며 항상 재전송할 수 있습니다. 보안 등급을 지정하지 않은 메일은 '일반' 등급으로 적용됩니다.

대외비, 기밀: 보안상 중요한 메일을 보낼 때 사용할 수 있는 보안 등급입니다. 회사 정책에 맞춰 등급 명과 등급별 설정을 변경할 수 있습니다.

등급별 설정: '유효기간', '재전송 금지', '유효기간 경과 시 보낸 메일도 삭제'에 대한 설정을 할 수 있습니다.

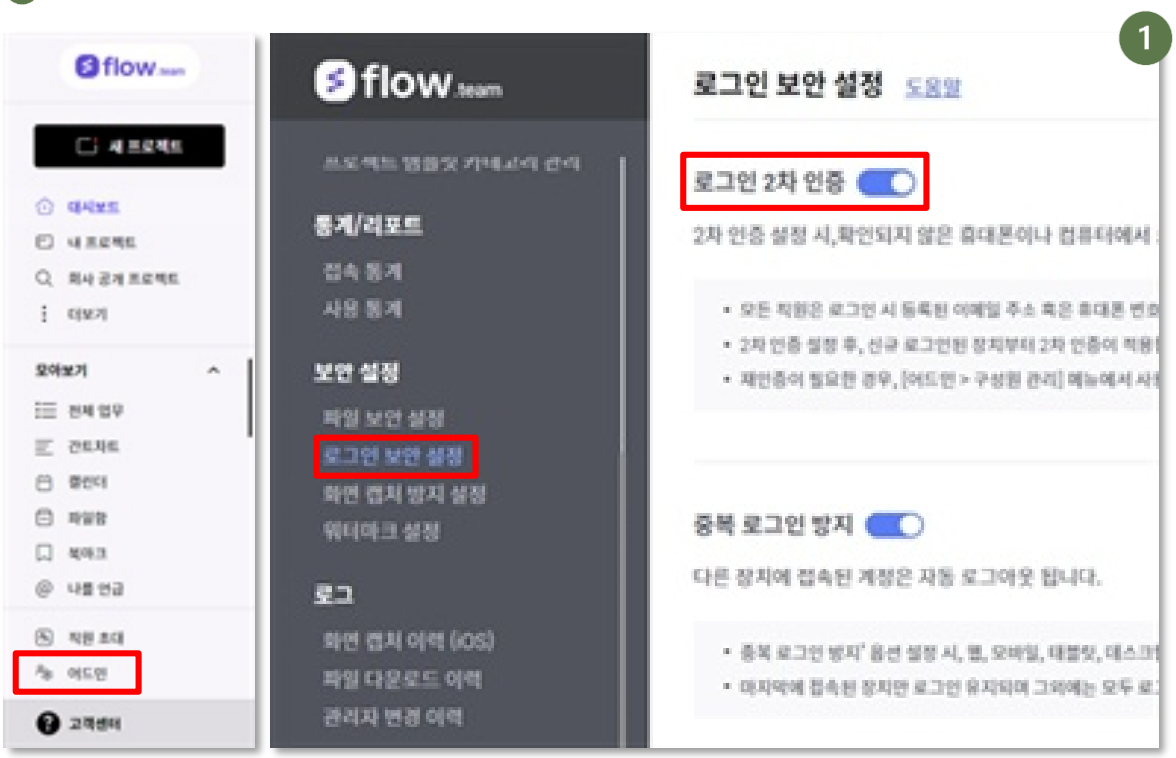
플로우(flow)

1. 계정 로그인 관리 설정하기

협업 툴은 회사의 중요한 사업 정보를 공유하고 관리하는 플랫폼입니다. 이런 정보는 민감한 데이터를 포함할 수 있으며, 허락 없이 이를 확인하거나 수정하는 것을 방지할 필요가 있습니다. 계정 로그인 관리를 통해 사용자의 인증을 확인하고, 무단 접근을 방지함으로써 정보를 보호해야 합니다.

2차 인증 설정하기

1 [어드민] > [보안 설정] > [로그인 보안 설정] > ['로그인 2차 인증' 활성화]



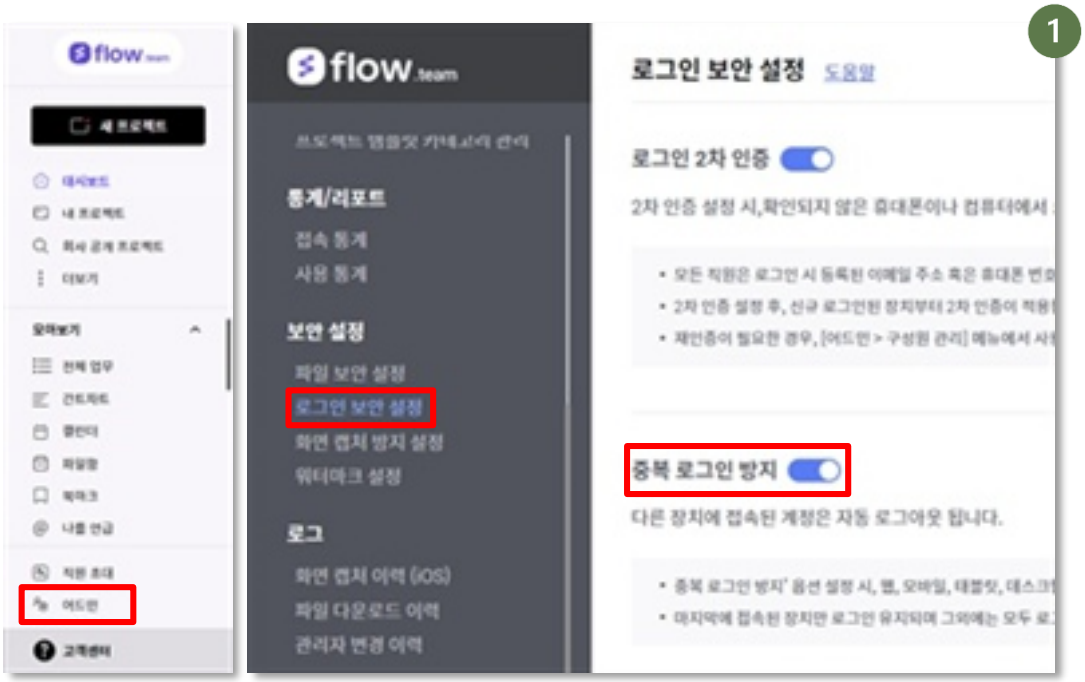
로그인 2차 인증이란?

사용자의 아이디와 비밀번호 외에 다른 인증 수단을 추가로 요구하는 보안 방식입니다. 일반적으로 휴대전화로 전송되는 일회용 코드가 이에 해당하며, 이를 통해 무단 접근을 방지하고 보안을 강화합니다.

플로우(flow)

중복 로그인 방지 설정하기

1 [어드민] > [보안설정] > [로그인 보안 설정] > ['중복 로그인 방지' 활성화]



로그인 IP 설정하기

1 [어드민] > [보안설정] > [로그인 보안 설정] > ['로그인 IP 설정' 활성화]

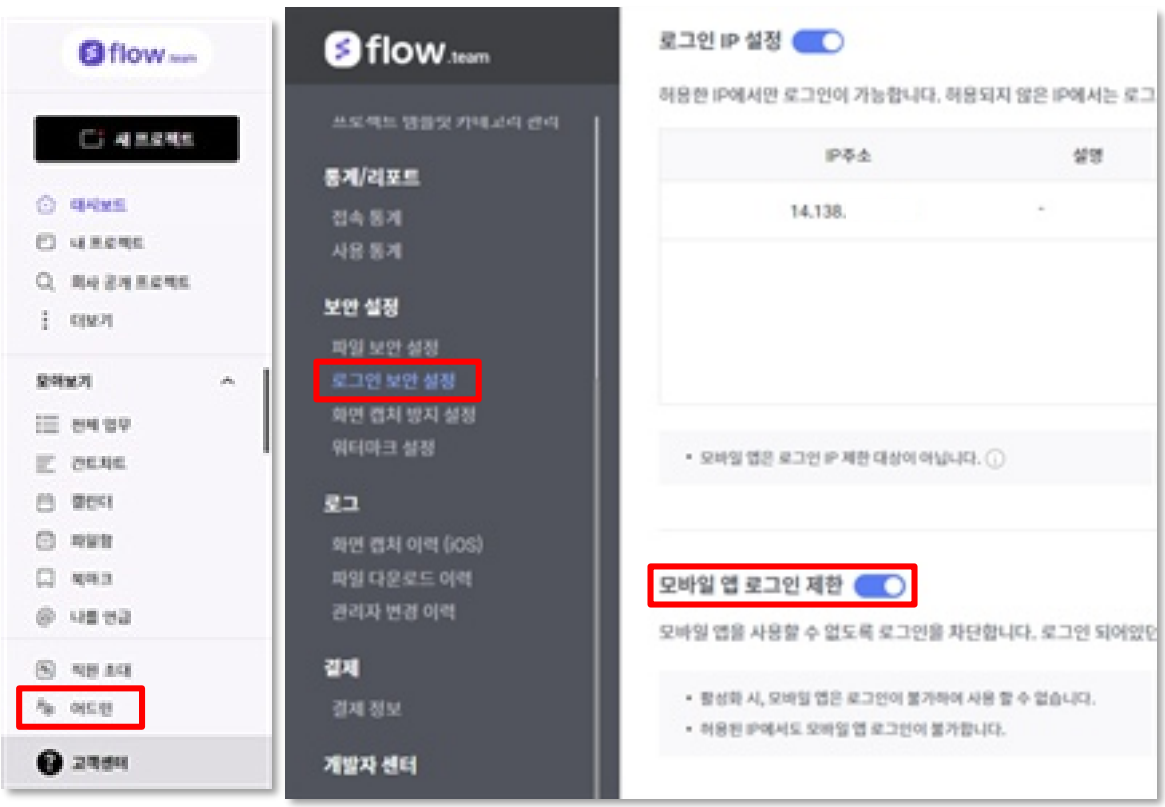
플로우(flow)

IP기반 서비스 접근

IP 주소는 주소와 비슷한 역할을 합니다. 만약 누군가가 우리 집으로 오려면 정확한 주소를 알아야 하듯이, 서버에 접근하려면 해당 서버의 IP 주소를 알아야 합니다.
보안을 강화하기 위해서는 불필요한 접근을 차단하는 것이 중요합니다. 서비스 접근 IP를 별도로 설정하면, 특정한 IP 주소에서만 서비스에 접근할 수 있도록 제한할 수 있습니다.

모바일 앱 로그인 제한

1. [어드민] > [보안 설정] > [로그인 보안 설정] > ['모바일 앱 로그인 제한' 활성화]



플로우(flow)

2. 파일 보안 설정하기

협업툴은 회사내 다양한 부서와 직원들이 함께 작업하고 정보를 공유하는 도구입니다. 이런 공유 공간에서 파일 보안 설정이 소홀하다면 회사 내부에서만 공유되어야 하는 중요한 문서나 데이터가 외부로 유출될 수 있습니다.

지정된 IP에서만 다운로드 허용

1 [어드민] > [보안 설정] > [파일 보안 설정] > ['지정된 IP에서만 다운로드 허용' 활성화]

플로우(flow)

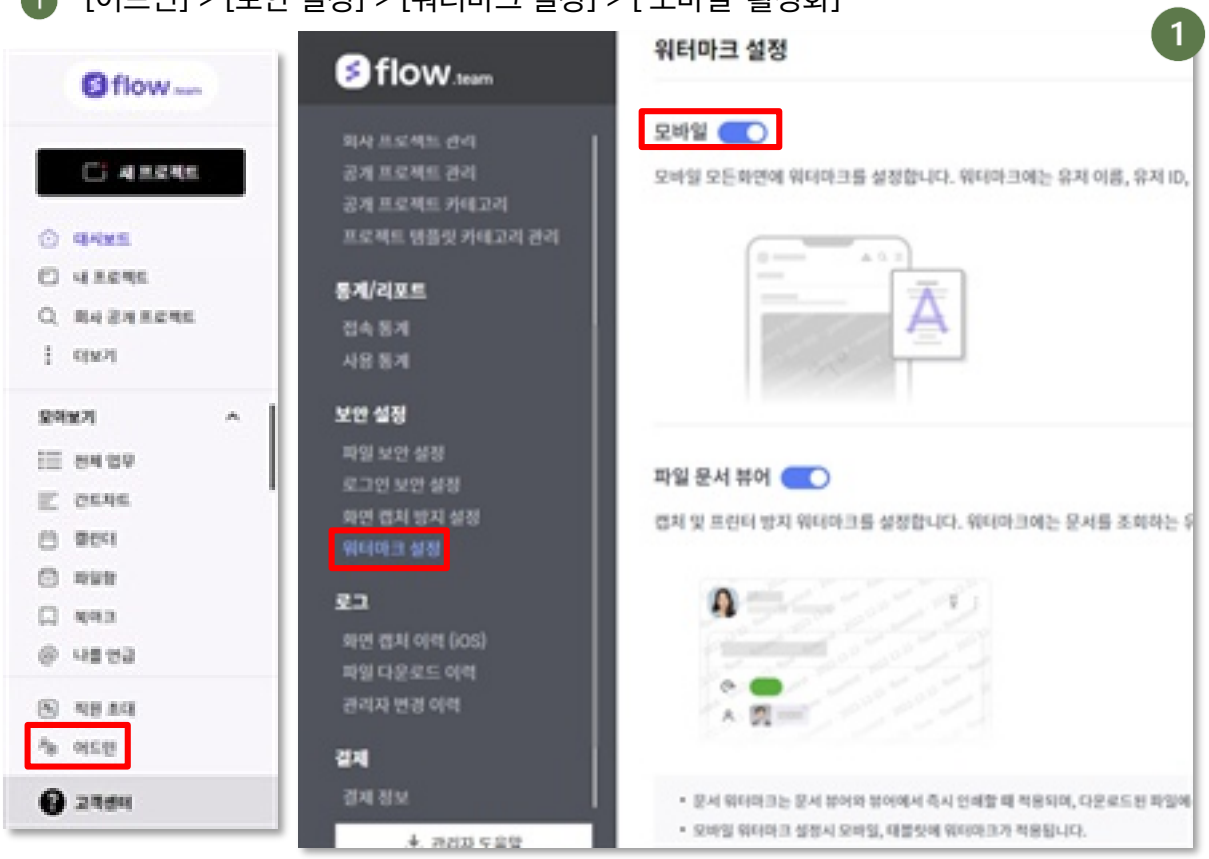
이미지 파일 조회 제한 설정하기

1 [어드민] > [보안 설정] > [파일 보안 설정] > ['이미지 파일 조희 제한' 활성화]

플로우(flow)

모바일 워터마크 설정하기

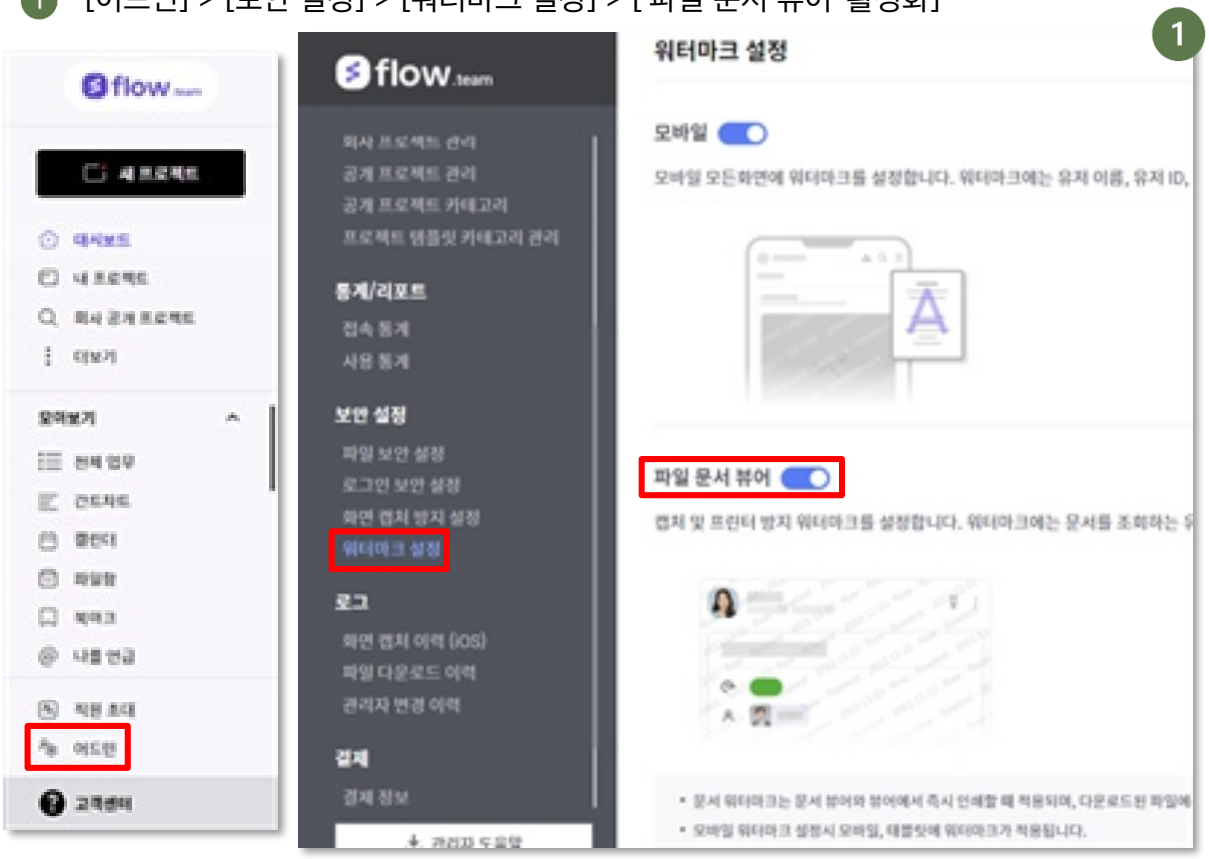
1 [어드민] > [보안 설정] > [워터마크 설정] > ['모바일' 활성화]



플로우(flow)

문서 뷰어 워터마크 설정하기

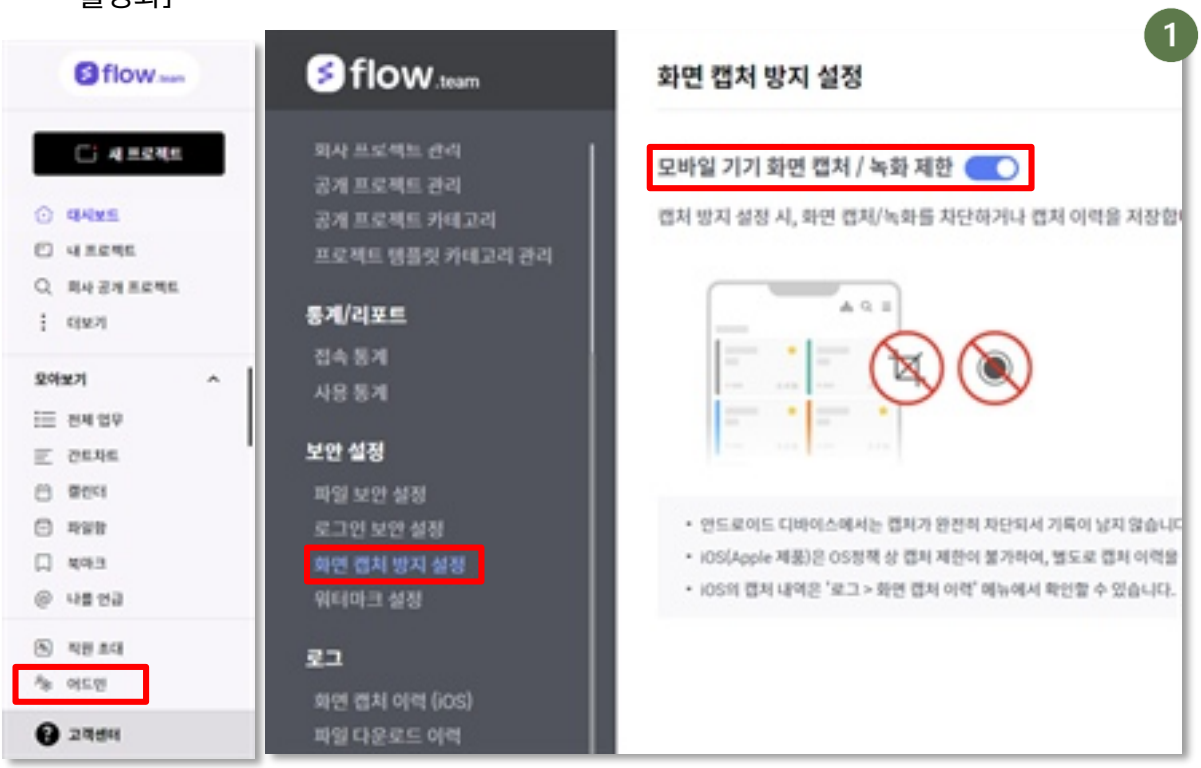
1 [어드민] > [보안 설정] > [워터마크 설정] > ['파일 문서 뷰어' 활성화]



플로우(flow)

모바일 워터마크 설정하기

1 [어드민] > [보안 설정] > [화면 캡처 방지 설정] > ['모바일 기기 화면 캡처 / 녹화 제한' 활성화]



이번 편에서는 중소기업들이 그룹웨어를 이용하며 추가적인 비용을 들이지 않고도 데이터 보안을 강화하는 방법을 쉽고 간단하게 소개합니다. 10인 미만 기업을 위한 서비스를 운영하고 있는 제품들의 보안에 대해 안내합니다.

그룹웨어란 무엇인가요?

그룹웨어는 기업 내에서 업무 협업을 용이하게 하기 위한 소프트웨어 플랫폼으로, 업무관리, 커뮤니케이션, 일정 관리, 문서 공유 등을 통합적으로 제공하는 시스템입니다.

그룹웨어 보안을 왜 해야 할까요?

그룹웨어 보안은 기업 정보와 개인정보의 유출 방지를 위해 매우 중요합니다. 중요한 사내 데이터를 보호하고 안전하게 유지하기 위해서는 강력한 보안 정책이 필요합니다.

가이드라인에서 다루는 제품 확인하기

DAOUoffice hiworks mailplug

▲ 다우오피스(DAOUoffice) ▲ 하이웍스(hiworks) ▲ 메일플러그(mailplug)

다우오피스(DAOUoffice)

1. 보안 설정하기

동시접속 제한 설정하기

동시접속 제한 설정을 통해, 다른 브라우저나 PC 환경에서 로그인 시 기존 접속이 로그아웃 되도록 설정할 수 있습니다.

1 [관리자페이지] > [보안관리] > [로그인] > ['동시접속 제한' 체크]

자동 로그아웃 설정하기

자동 로그아웃 기능 설정을 통해 일정 시간 동안 동작이 없을 경우 자동으로 로그아웃 되도록 설정할 수 있습니다.

1 [관리자페이지] > [보안관리] > [로그인] > ['자동 로그아웃' 체크] > ['5분' 선택]

다우오피스(DAOUoffice)

서비스 접근 IP 설정하기

허용된 IP 주소에서만 서비스에 접속할 수 있도록 설정할 수 있습니다.

1. [관리자페이지] > [보안관리] > [로그인] > [서비스 IP 접근설정 사용여부 '부분 허용' 체크] > [허용할 IP 입력 및 추가']

비밀번호 변경 주기 설정하기

사용자들이 주기적으로 비밀번호를 변경하도록 설정할 수 있습니다.

1. [관리자페이지] > [보안관리] > [비밀번호] > [비밀번호 관리] > [비밀번호 변경 주기 '3개월' 선택 및 '강제 변경' 체크]

다우오피스(DAOUoffice)

2. 모바일 기기 관리하기

동시접속 제한 설정하기

PC 뿐만 아니라 모바일 앱을 통해서도 다우오피스에 접속할 수 있습니다. 아래 설정을 통해 그룹웨어에 접속할 수 있는 모바일 기기를 별도로 지정할 수 있습니다.

1. [관리자페이지] > [보안관리] > [모바일 접속차단(MAM)] > [모바일 앱 접속차단 설정(MAM) '사용' 체크] > [하단 모바일 앱 접속기기 관리에 허용할 모바일 기기 추가]

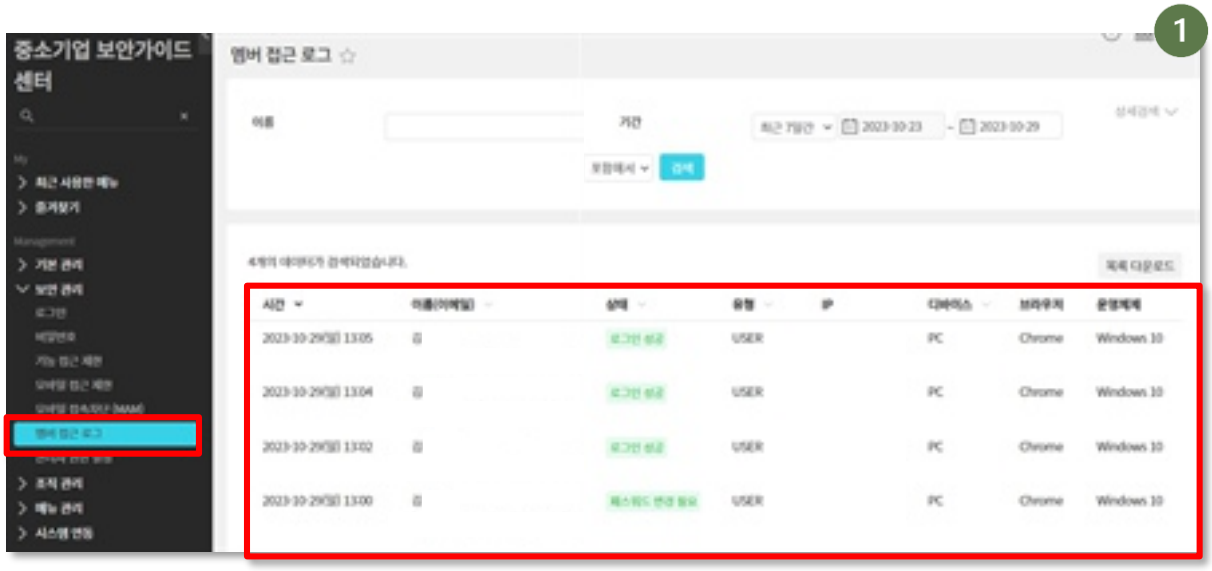
다우오피스(DAOUoffice)

3. 로그 확인하기

그룹웨어 사용자 로그인 기록 확인하기

3개월 이내 사용자들의 로그인 기록 및 접속 기간, IP, 디바이스 명, 브라우저 종류, 운영체제 종류 등을 확인하여 부적절한 접근이 있었는지 확인할 수 있습니다.

1 [관리자페이지] > [보안관리] > [멤버 접근 로그] > [데이터 확인]



로그 데이터 분석하기	
항목	주의해야 할 로그 데이터
시간 기반 분석	근무 시간 외에 로그인 시도
계정 로그인 기록	한 계정으로 여러 지역에서 동시에 로그인 시도
로그인 성공 여부	여러 번의 실패한 로그인 시도
IP 주소 확인	사용자가 자주 접속하는 지역 이외의 IP 주소로 로그인 시도
디바이스 / 브라우저 / 운영체제 정보	특정 사용자가 기존과 다른 디바이스, 브라우저, 운영체제를 사용하는 경우

메일플러그(mailplug)

1. 접근 제한 설정하기

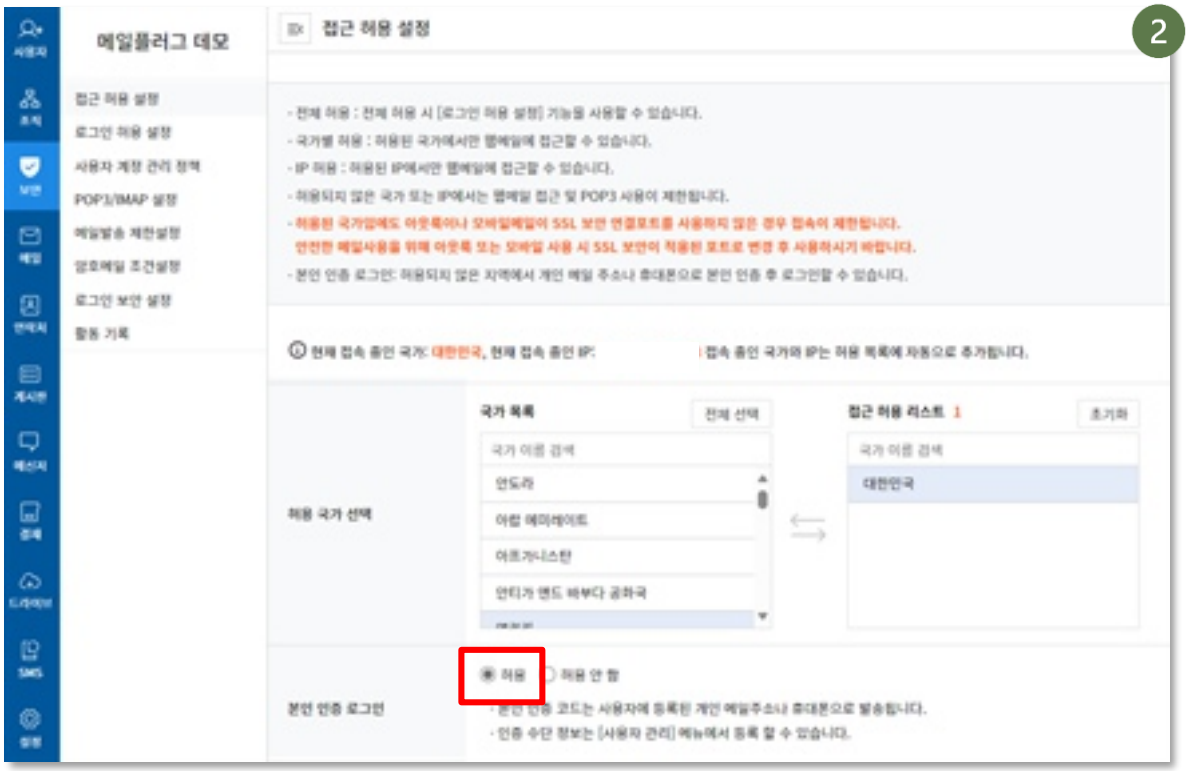
접근 허용 설정하기

허용된 국가에서만 메일플러그에 로그인할 수 있도록 설정할 수 있습니다. 또한 허용되지 않은 지역에서 로그인 시, 등록된 사용자의 휴대전화 번호/개인 메일 주소로 인증코드를 받아 인증 후 메일플러그에 로그인하도록 설정할 수 있습니다.

1. [관리자] > [보안] > [접근 허용 설정] > [접근 허용 방식 '국가별 허용' 체크] > [접근 허용 국가 추가]

메일플러그(mailplug)

2 [관리자] > [보안] > [접근 허용 설정] > [본인 인증 로그인 '허용' 체크]



메일플러그(mailplug)

2. 사용자 계정 관리 정책 설정하기

사용자 계정 관리 정책 설정하기

불필요한 계정을 최소한으로 보관하기 위해서 일정 기간 동안 로그인 기록이 없을 시, 휴면 계정으로 전환되도록 설정할 수 있습니다. 또한 예외 사용자 설정을 통해 정상/휴면/중지 계정으로의 전환을 지정할 수 있습니다.

1. [관리자] > [보안] > [사용자 계정 관리 정책] > ['최근 3개월간 로그인하지 않으면 휴면 계정으로 전환합니다.' 선택] > ['휴면 전환 후 3개월 지난 계정은 사용 중지합니다.' 체크] > [예외 사용자 필요시 체크 및 지정]

휴면 계정과 사용 중지 계정의 차이가 무엇인가요?

휴면: 사용자가 직접 비밀번호 변경 후, 휴면을 해제해 로그인할 수 있습니다.
사용 중지: 관리자가 정상상태로 변경하지 않으면 로그인할 수 없습니다.

메일플러그(mailplug)

사용만료일 설정하기

외부자에게 임시로 그룹웨어 계정을 발급해야 할 경우에는 사용만료일 설정을 통해 사용기간 만료 후 계정이 자동으로 정지되도록 설정할 수 있습니다.

1 [관리자] > [보안] > [사용자 계정 관리 정책] > [사용만료일 설정 기능 필요시 체크]

메일플러그(mailplug)

3. 이메일 프로토콜 설정하기

POP3/IMAP 사용 설정하기

이메일 서버에서 클라이언트로 이메일을 가져오는 데 사용되는 프로토콜인 POP3/IMAP 사용 여부를 설정할 수 있습니다. 사용 설정 후 30일동안 연동이 없는 사용자는 '사용 안 함'으로 전환됩니다.

1 [관리자] > [보안] > [POP3/IMAP 설정] > [POP3/IMAP 기능 필요 시 '사용' 체크]

POP3와 IMAP이 무엇인가요?

POP3와 IMAP은 이메일 서버와 클라이언트 간 통신을 위해 사용되는 프로토콜입니다.
POP3는 단방향 통신을 지원합니다. 이메일 클라이언트에서 이메일을 다운로드하면 서버에 복사본이 남지 않습니다. 따라서 여러 기기에서 이메일을 확인할 때 이메일이 각 기기에 독립적으로 다운로드됩니다.
IMAP은 양방향 통신을 지원합니다. 클라이언트에서 이메일을 읽거나 삭제하면 서버에서도 그 상태가 반영됩니다. 이메일 서버에 메일함이 유지되어 있어 여러 기기 간에 메일함이 동일하게 유지됩니다.

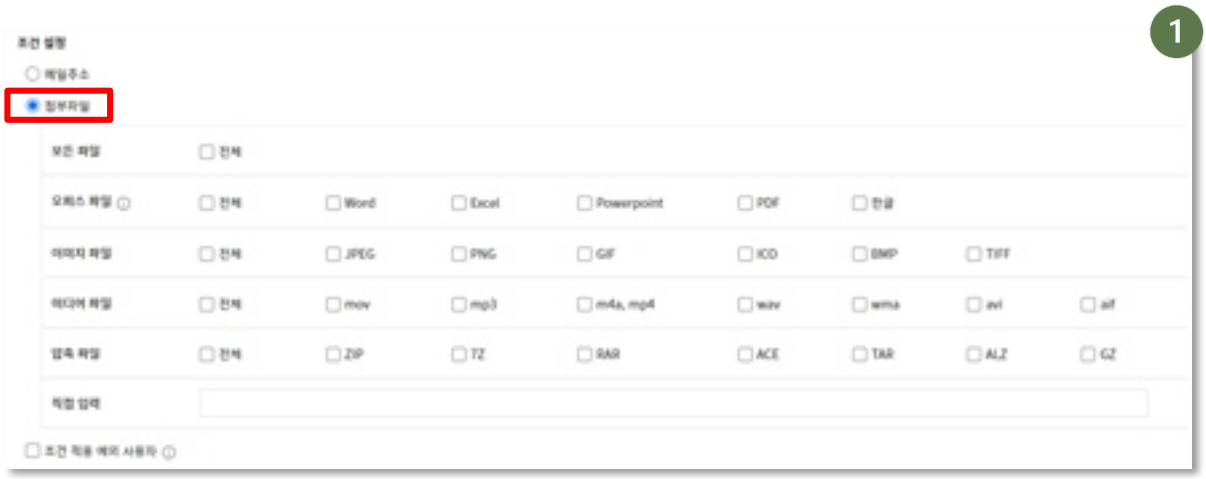
메일플러그(mailplug)

4. 메일발송 제한 설정하기

첨부파일 조건 설정하기

메일 첨부파일에 허용되지 않은 파일 종류(확장자)가 포함되어 있으면 메일 발송이 제한되도록 설정할 수 있습니다. 조건 적용 예외 사용자로 등록된 사용자는 제한설정에 영향을 받지 않습니다.

1 [관리자] > [보안] > [메일 발송 제한 설정] > [허용할 첨부파일 유형 선택]



메일플러그(mailplug)

5. 암호메일 조건 설정하기

암호메일 조건 설정하기

첨부파일/외부 발송 여부에 따라 암호메일을 강제하도록 설정할 수 있습니다. 조건 적용 예외 사용자로 등록된 사용자는 제한설정에 영향을 받지 않습니다.

1. [관리자] > [보안] > [암호메일 조건설정] > [하단의 권장하는 규칙을 참고하여 설정]

메일플러그(mailplug)

6. 로그인 보안 설정하기

로그인 환경 설정하기

동시접속 제한 설정을 통해, 다른 브라우저나 PC 환경에서 로그인 시 기존 접속이 로그아웃 되도록 설정할 수 있습니다. 또한 일정 횟수 이상 잘못된 비밀번호로 로그인을 시도하면 설정한 시간 또는 관리자에 의해 해제될 때까지 로그인이 차단되도록 설정할 수 있습니다.

1 [관리자] > [보안] > [로그인 보안 설정] > [하단의 권장하는 규칙을 참고하여 설정]

권장하는 규칙	
항목	권장 값
동시 로그인	허용 안 함
로그인 차단	사용
접속 차단 시간	관리자에 의해 해제될 때까지

메일플러그(mailplug)

비밀번호 정책 설정하기

비밀번호가 설정한 조건으로 조합되어야 입력 및 수정이 가능하도록 설정할 수 있습니다. 또한 비밀번호 변경 주기를 설정하여 사용자들이 주기적으로 비밀번호를 변경하도록 설정할 수 있습니다.

2 [관리자] > [보안] > [로그인 보안설정] > [하단의 권장하는 규칙을 참고하여 설정]

권장하는 규칙	
항목	권장 값
비밀번호 보안 수준	높음: 영문, 숫자, 특수문자 3종을 모두 조합하여 9자리 이상
비밀번호 변경 주기	30일 이하

메일플러그(mailplug)

2단계인증(OTP 로그인) 정책 설정하기

아이디/비밀번호 입력 후 본인 소유의 휴대전화 OTP 앱을 통해 QR코드 인증까지 완료하여야 로그인할 수 있는 2단계인증을 설정할 수 있습니다.

3 [관리자] > [보안] > [로그인 보안설정] > [하단의 권장하는 규칙을 참고하여 설정]

권장하는 규칙	
항목	권장 값
2단계 인증 로그인 정책	사용
신규 사용자 등록 시 2단계 인증 사용 여부	2단계 인증(OTP) 사용

2단계 인증이란?

사용자의 아이디와 비밀번호 외에 다른 인증 수단을 추가로 요구하는 보안 방식입니다. 일반적으로 휴대전화로 전송되는 일회용 코드가 이에 해당하며, 이를 통해 무단 접근을 방지하고 보안을 강화합니다.

하이웍스(hiworks)

1. 보안 설정하기

비밀번호 변경 정책 설정하기

비밀번호 변경 주기를 설정하여 사용자들이 주기적으로 비밀번호를 변경하도록 설정할 수 있습니다.

1 [관리자페이지] > [보안] > [비밀번호 변경 정책] > ['적용함' 체크 및 기간 선택]

하이웍스(hiworks)

2단계 인증 사용 설정하기

아이디/비밀번호 입력 후 일회용 인증 번호를 입력해야 로그인이 되도록 설정할 수 있습니다.

1 관리자페이지] > [보안] > [2단계 인증]

3

침해사고 발생 시 대처 방법

본장에서는 기업 내 침해사고 발생 시 대처 방법에 대해 다룹니다. 침해사고가 발생했을 때 신고할 수 있는 주요 기관인 경찰청, 한국인터넷진흥원, 중소벤처기업부에서의 신고 방법에 대해 설명하며, 이외에도 도움을 받을 수 있는 정부기관에 대해 안내합니다.

침해사고 대응하기

침해사고를 완전히 예방하는 것은 어려우며, 큰 피해를 막기 위해서는 침해사고가 발생했을 때 신속하고 정확한 대응이 이루어져야 합니다. 이번 편에서는 침해사고가 발생했을 때 신고할 수 있는 주요 기관과 그 신고 방법에 대해 살펴보겠습니다.

침해사고가 발생했을 때 꼭 신고해야 할까요?

기업에서 침해사고가 발생하면, 그 즉시 이 유관기관 혹은 **한국인터넷진흥원**에 알려야 합니다. 빠르게 대응할수록 기업의 피해를 줄일 수 있고, 업무 복귀시점을 앞당길 수 있습니다.

신고 기관별 차이점이 있나요?

경찰청은 **정보통신망을 통한 모든 형태의 범죄** 행위에 대한 신고를 받을 수 있습니다. 이는 정보통신망 침해 범죄 뿐만 아니라 정보통신망을 이용한 범죄, 불법 컨텐츠 범죄 등도 포함됩니다.

한국인터넷진흥원(KISA)는 유출된 정보의 유형에 상관 없이 **정보통신망 침해 범죄**에 대한 신고를 처리하고 있습니다.

중소벤처기업부는 사고의 종류에 상관 없이 **중소기업기술에 대한 범죄** 행위에 대한 신고를 받습니다.

중소기업의 기술이 정보통신망 침해로 인해 유출되었을 경우, 세 기관에 모두 신고가 가능합니다. 중요한 것은, '**빠른 신고를 통해 적절한 초동대응을 하는 것**' 입니다.

가이드라인에서 안내하는 신고 사이트 확인하기

▲ 경찰청
사이버범죄 신고시스템

▲ 한국인터넷진흥원
인터넷침해사고대응지원센터

▲ 중소벤처기업부
중소기업 기술보호 울타리

경찰청

사이버범죄 신고시스템

지원 대상

정보통신망* 침해 범죄를 당한 **모든 기업**

* 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체제

지원 내용

사이버 상에서 일어나는 범죄행위에 대한 형사처벌

피해 유형

☑ 해커 또는 외부인이 컴퓨터에 침입해서 기업 데이터를 유출한 경우 (단순침입 포함)

☑ 해커가 기업 컴퓨터 시스템에 악성 프로그램을 유포해서 장애를 일으킨 경우

☑ 해커가 시스템이나 데이터 프로그램을 훼손, 삭제, 변경한 경우

신고 방법 ecrm.police.go.kr (사이버범죄 신고 시스템)

- 온라인: [ECRM 홈페이지 하단 신고하기] > ['긴급한 사안이 아닙니다.' 선택] > ['오프라인 사안이 아닙니다.' 선택] > [범죄유형-'해킹' 선택]
- 오프라인: 가까운 경찰서 직접 방문

긴급신고 112(무료)

민원상담 182(유료)

한국인터넷진흥원

인터넷 침해사고 대응 지원 센터

지원 대상

- 정보통신망* 침해 범죄를 당한 **모든 기업**
- 중소기업기술 침해 행위를 당한 **중소기업****

* 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체제

** 「중소기업기본법」 제2조에 해당하는 중소기업

지원 내용

- 침해사고 발생 원인 및 침투경로 분석
- 재발방지를 위한 원인제거 지원
- 임직원 대상 온라인/오프라인 보안교육 진행

피해 유형

☑ 컴퓨터 시스템에 외부에서 접속한 흔적이 있는 경우
☑ 비정상적인 네트워크 성능 저하 및 특정 또는 모든 웹 사이트 접속이 어려운 경우
☑ 컴퓨터 파일이 바이러스에 의해 암호화된 경우

신고 방법 boho.or.kr (KISA 인터넷 보호나라)

- 온라인: [홈페이지 상단 정보보호 서비스] > ['중소기업 피해지원' 선택]
  > [하단 '신고하기' 선택]

	해킹 · 스팸개인정보침해 신고 118(무료)
	KISA 대표번호 1433-25(유료)

중소벤처기업부

중소기업 기술보호 울타리

지원 대상

- 중소기업기술 침해 행위를 당한 **중소기업***

  * 「중소기업기본법」 제2조에 해당하는 중소기업

지원 내용

- 중소기업 기술침해에 대한 행정조사
- 침해내용(검토)에 따라 타부처 및 분쟁 조정제도 이관
- 가해기업에 대한 시정 권고 및 공표
- 행정조사 결과 기술피해가 인정되는 경우, 지원심사를 거쳐 법무지원단을 통한 민사소송 비용지원

피해 유형

☑ 기업기술이 타인에 의해 부정한 방법으로 취득 · 사용되는 피해를 입은 경우

신고 방법 mss.go.kr (중소벤처기업부) ultari.go.kr (중소기업 기술보호 울타리)

- 온라인: [중소벤처기업부 홈페이지(www.mss.go.kr)] > [민원·신고] > [신고센터] > [기술침해행위 신고]
- 오프라인: 세종특별자치시 가름로 180 중소벤처기업부 기술보호과 기술침해조사팀 (서면 접수)

중소벤처기업부 기술보호과 기술침해조사팀
044-204-7786~7

유관기관 알아두기

침해사고 발생 시 도움을 받을 수 있는 유관기관 한 눈에 확인하기

보안 분야 전문가가 아니라면, 침해사고가 발생했을 때 적절한 대응 방법을 정확히 알기는 어려울 것입니다. 따라서 망설이지 말고, 즉시 아래의 전화번호로 연락하여 신속한 조치를 취하는 것이 필요합니다.

기관명	지원내용	연락처 · 홈페이지
국가정보원 NATIONAL INTELLIGENCE SERVICE	• 국내 첨단기술을 보호하고 산업보안활동을 수행	• 111 • www.nis.go.kr
중소벤처기업부	• 중소기업지원 정책	• 1357 • www.mss.go.kr
산업통상자원부	• 산업기술유출방지 및 보호에 관한 법률 및 정책	• 1577-0900 • www.motie.go.kr
공정거래위원회	• 산업기술 유출범죄 전문 수사 및 예방 • 기업지원활동	• 1670-0007 (공정위 상담안내) • www.ftc.go.kr
특허청	• 부정경쟁방지 및 영업비밀 보호에 관한 법률 및 정책	• 1544-8080 • www.kipo.go.kr
	• 지적재산권 침해 및 기술(영업비밀) 유출범죄 전문수사	• 1666-6464 • www.ippolice.go.kr
개인정보보호위원회	• 개인정보 사고 발생 시 신고 및 문의 처리	• 02-2100-3025 (대표전화) • 1833-6972 (개인정보분쟁조정위원회) • www.pipc.go.kr
KISA 한국인터넷진흥원	• 침해사고 발생 시 초기대응 및 지원	• 1433-25 (대표전화) • 118 (해킹 · 스팸개인정보침해) • www.kisa.or.kr
대·중소기업 농어업협력재단	• 중소기업 기술보호 역량강화 • 지원사업 및 피해구제에 대한 상담 기능 수행	• 02-368-8700 • www.win-win.or.kr
K-ip care 한국지식재산보호원 Korea Intellectual property Protection Agency	• 기업의 영업비밀 보호 및 체계적인 관리 One-Stop 지원	• 02-2183-5800 • www.koipa.re.kr
경찰청	• 산업기술 유출범죄 전문 수사 및 예방 • 기업지원활동	• 182 • ecrm.police.go.kr (사이버범죄 신고시스템)
한국산업기술보호협회 The Korean Association for Industrial Technology Security	• 산업기술 유출방지 및 보호에 관한 정책지원 및 중소기업 지원	• 02 -3489-7014 • www.kaits.or.kr

중소기업 기술 유출 방지
IT 보안 가이드라인

2023년 12월 발행
발행처 산업기밀보호센터

본 가이드라인은 공공의 목적을 위하여 한국인터넷진흥원의 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드, 중소기업 정보보호 실무 가이드, 클라우드 취약점 점검 가이드 및 각 제품의 사용 안내서 등을 기반으로 제작되었습니다.

중소기업
기술 유출 방지
IT 보안
가이드라인