POSTECH VPN 서비스 이용 가이드

2025. 04.

학술정보처 정보기술팀

일시	구분
2018. 1.	제정
2019. 10	개정
2023. 10	개정
2024. 05	개정
2025. 04	개정

문의처: 학술정보처 정보기술팀

T. 054-279-2515

E-mail: hemos@postech.ac.kr

목차

Ⅰ. 개요 **4**

1. VPN 이란? 4
2. VPN 서비스 목적 4
3. VPN 고정 IP 사용 4

Ⅱ. VPN 접속 방법 **5**

1. 웹사이트를 통한 접속 5
2. VPN 클라이언트 프로그램을 통한 접속 6
3. 리눅스 환경 VPN 접속 방법 8
4. 모바일 디바이스를 통한 접속 10
5. VPN 이중인증 13

Ⅲ. VPN 연결 장애 시 대응 방법 **19**

1. 클라이언트 접속 장애 19
2. Linux 접속 장애 19
3. 이차인증 오류 발생 19

I. 개요

1. VPN(Virtual Private Network: 가상사설망)이란?

가. 인터넷과 같은 공중망(Public Network)을 마치 전용선으로 사설망을 구축한 것처럼 사용할 수 있는 방식

나. VPN 을 통해 대학 외부에서도 대학 내부 네트워크를 이용하는 것과 동일한 환경을 제공

다. VPN 을 통해 송수신되는 데이터는 암호화되어 외부 위협에 대해 안전성 확보

2. VPN 서비스 목적

가. 대학 외부에서 대학 내 정보시스템을 안전하게 이용할 수 있는 환경 제공

3. VPN 고정 IP 사용

가. 필요성

1) VPN 접속 시 일반적으로는 사설 IP 를 임의로 할당 받기 때문에 VPN 접속할 때마다 할당 받는 IP 가 달라짐
2) VPN 고정 IP 를 신청하면 VPN 접속 시 항상 동일한 사설 IP 할당 가능
3) 리눅스 등 시스템에 접속 시 할당 받은 고정 IP 만 접속 가능하도록 설정 가능하여 보안 강화 가능

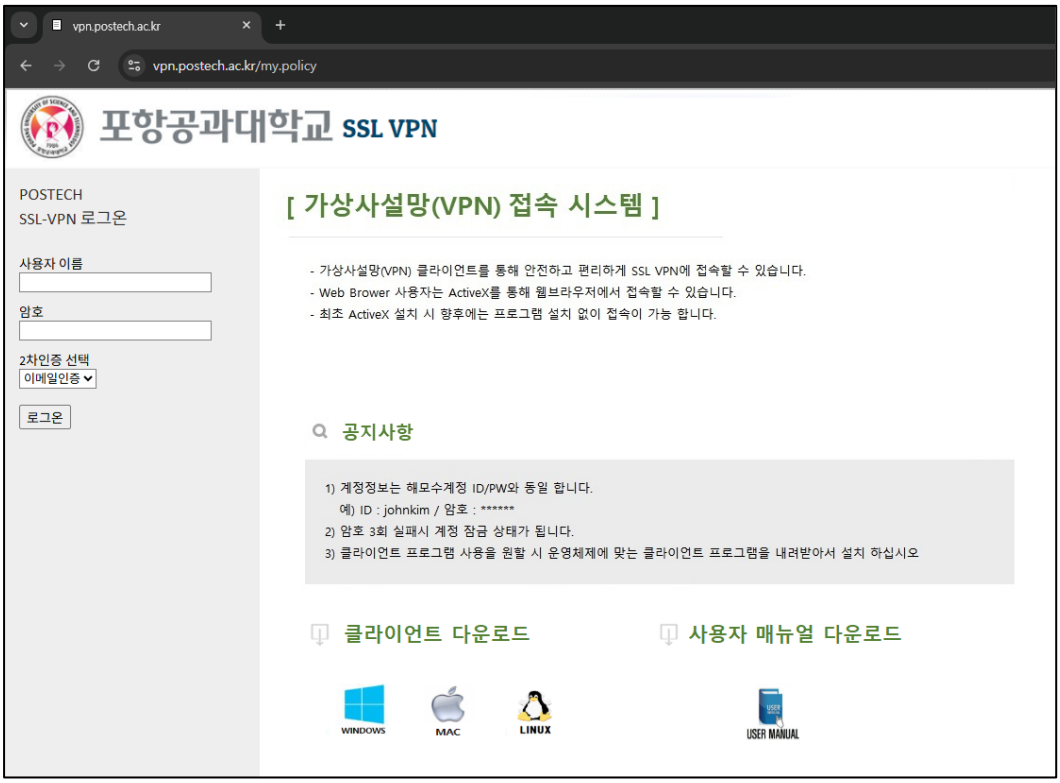
나. 신청 방법

1) HEMOS 사이트(https://hemos.postech.ac.kr) – Service Application 메뉴 – Access/Network – Static IP for VPN(VPN 용 고정 IP 신청)에서 신청
   * 신청 시 사유 작성 필수.

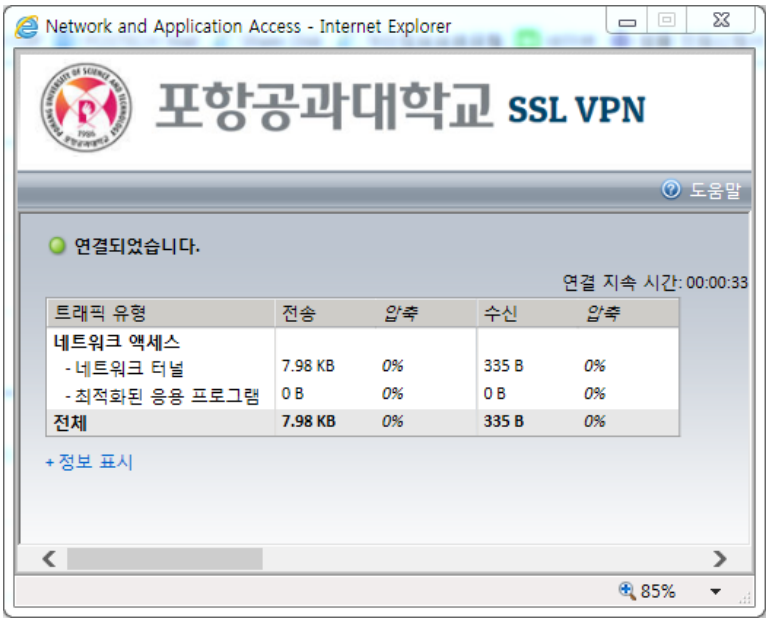
II. VPN 접속방법

1. 웹사이트를 통한 접속

1-1. 대학 VPN 사이트(https://vpn.postech.ac.kr) 접속



1-2. HEMOS 계정 입력 및 2 차인증 방법 선택 후 로그인하여 서비스 이용



2. VPN 클라이언트 프로그램을 통한 접속

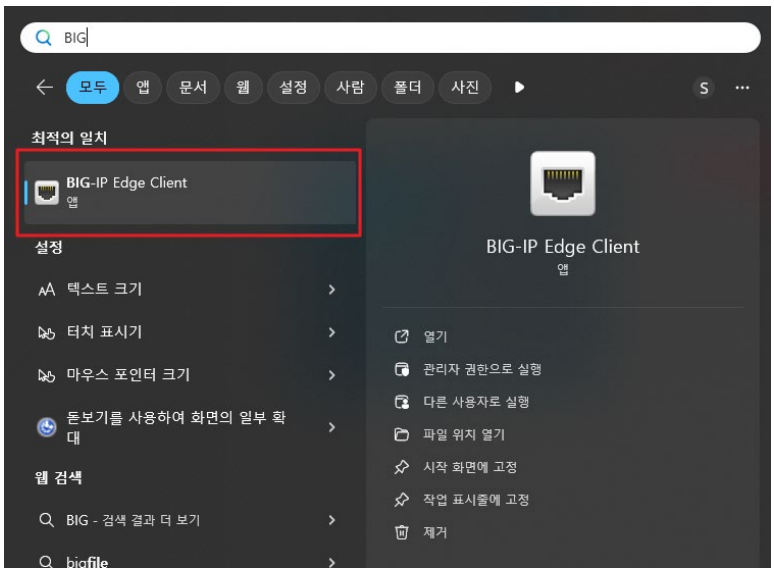
2-1. 대학 VPN 사이트 (https://vpn.postech.ac.kr) 접속

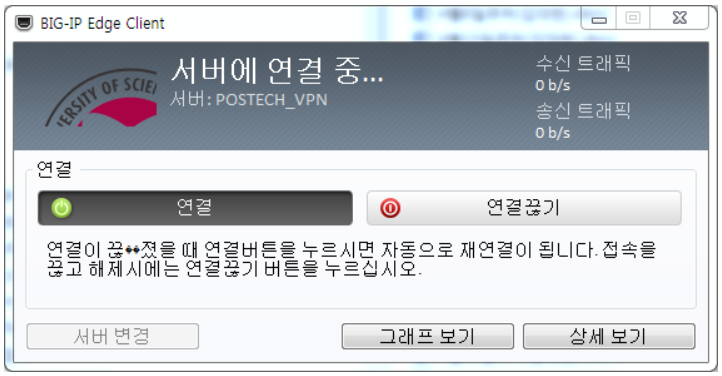
2-2. VPN 접속 클라이언트 설치

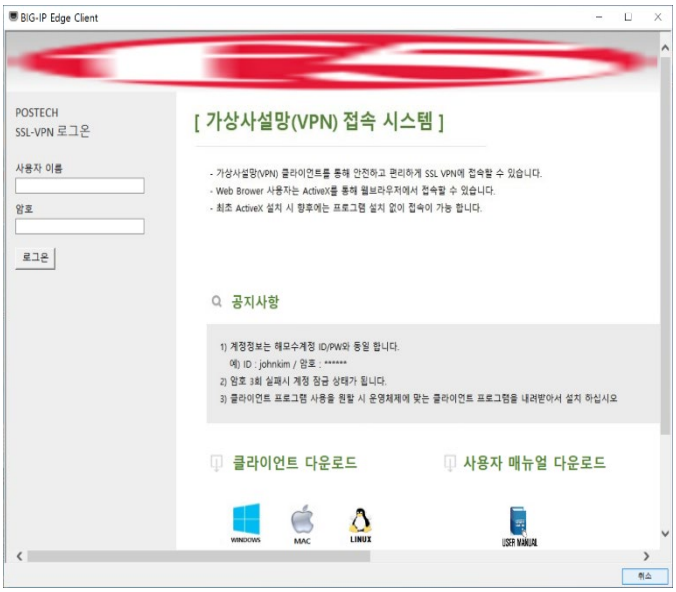


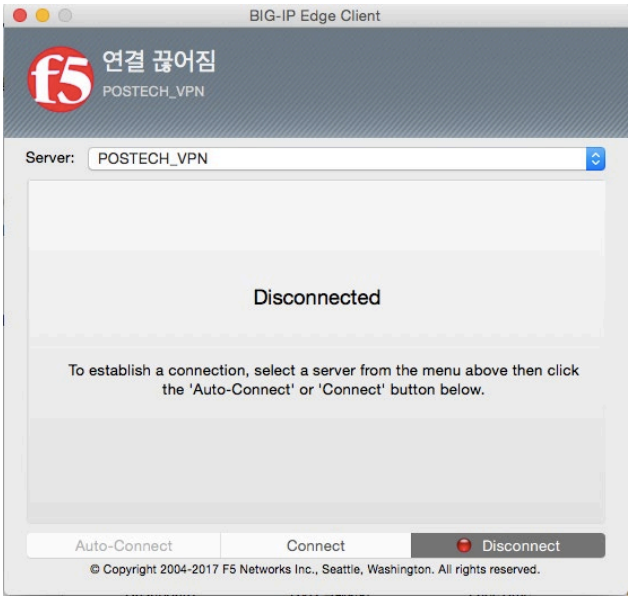
* OS 에 맞는 클라이언트 프로그램 설치 (윈도우, Mac OS, Linux)

2-3. 접속 클라이언트 프로그램 (BIG-IP Edge Client) 실행









[윈도우 클라이언트]

[Mac OS 클라이언트]

2-4. HEMOS 계정 입력 및 2 차인증 방법 선택 후 로그인하여 서비스 이용

3. 리눅스 환경 VPN 접속 방법

3-1. 리눅스 클라이언트 프로그램 다운로드: https://vpn.postech.ac.kr 에서 Client Program 다운

3-2. 프로그램 설치하기

- 다운받은 Linux.gz 파일을 압축 해제.
- Terminal 실행 후 root 계정으로 전환 (명령어 : su)
- Root 계정 전환 후 Linux.gz 파일을 압축해제한 디렉토리로 경로 이동
- 압축해제한 디렉토리의 하위 디렉토리에서 OS 에 맞는 파일을 설치.

(1) CentOS

- linux_f5cli.x86_64.rpm 설치 (명령어 : sudo yum localinstall linux_f5cli.x86_64.rpm)

(2) Ubuntu

- OS 비트 확인 (명령어 : getconf LONG_BIT)

```
root@[redacted] /home/[redacted] # getconf LONG_BIT
64
```

* 64 비트 : linux_f5cli.x86_64.deb 설치 (명령어 : sudo dpkg -i linux_f5cli.x86_64.deb)
* 32 비트 : linux_f5cli.armhf.deb 설치 (명령어 : sudo dpkg -i linux_f5cli.armhf.deb)

3-3. VPN 접속

* 명령어 : f5fpc -s

- hostname : https://vpn.postech.ac.kr
- username : HEMOS ID
- password : HEMOS PW

```
root@ubuntu:/home/test/Downloads/linux_sslvpn# f5fpc -s
Enter server hostname: https://vpn.postech.ac.kr
Enter username: test
Enter password:
Operation in progress
```

3-4. VPN 연결 확인

* 명령어 : f5fpc --i

- Connection Status: session established 되면 VPN 연결 성공

```
root@ubuntu:/home/test/Downloads/linux_sslvpn# f5fpc --i
Connection Status: session established
Favorites Information:

----------------------
fav-Id   fav-Type  fav-Status       fav-Name
377      vpn        established     /Common/ob_na
```

3-5. VPN 연결 종료

* 명령어 : f5fpc -o

- Disconnected successfully 가 출력되면 연결 끊김

```
root@ubuntu:/home/test/Downloads/linux_sslvpn# f5fpc -o
Disconnected successfully
```

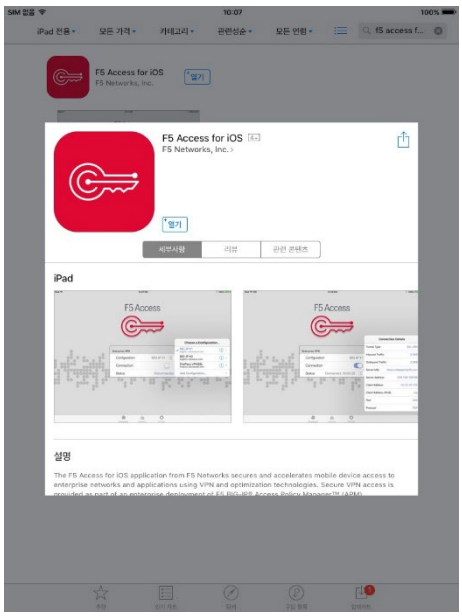
4. 모바일 디바이스를 통한 접속

가. 모바일 스토어(Play 스토어 또는 앱스토어) 접속

나. "F5 Access" 어플리케이션 검색하여 설치



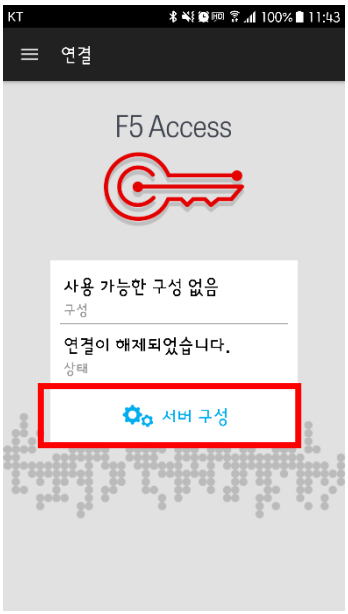
[안드로이드 용]



[iPhone 용]

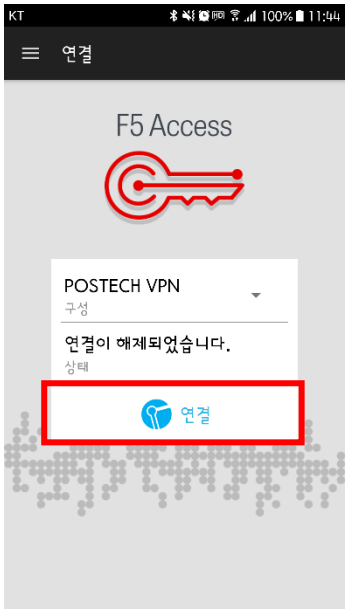
다. VPN 서버 구성 (https://vpn.postech.ac.kr 입력) 및 접속

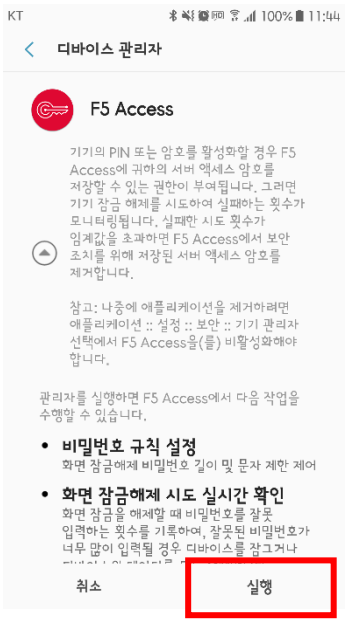
1) 안드로이드



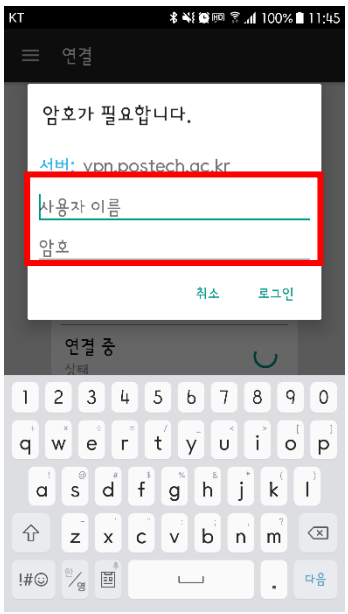


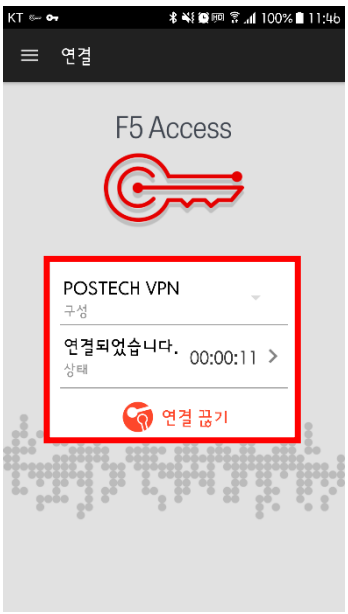



KT 100% 11:44
연결
F5 Access
POSTECH VPN
구성
연결이 해제되었습니다.
상태
연결


KT 100% 11:44
디바이스 관리자
F5 Access
기기의 PIN 또는 암호를 활성화할 경우 F5 Access에 귀하의 서버 액세스 암호를 저장할 수 있는 권한이 부여됩니다. 그러면 기기 잠금 해제를 시도하여 실패하는 횟수가 모니터링됩니다. 실패한 시도 횟수가 임계값을 초과하면 F5 Access에서 보안 조치를 위해 저장된 서버 액세스 암호를 제거합니다.
참고: 나중에 애플리케이션을 제거하려면 애플리케이션 :: 설정 :: 보안 :: 기기 관리자 선택에서 F5 Access을(를) 비활성화해야 합니다.
관리자를 실행하면 F5 Access에서 다음 작업을 수행할 수 있습니다.
비밀번호 규칙 설정
화면 잠금해제 비밀번호 길이 및 문자 제한 제어
화면 잠금해제 시도 실시간 확인
취소
실행


KT 100% 11:44
연결
F5 Access
PIN 또는 암호 변경
화면 잠금 암호 또는 PIN이 설정되지 않았거나 회사 정책에 부합되지 않습니다. 회사 정책에 부합되는 PIN이나 암호를 만드십시오.
취소
확인


KT 100% 11:45
연결
암호가 필요합니다.
서버: vpn.postech.ac.kr
사용자 이름
암호
취소
로그인
연결 중
상태

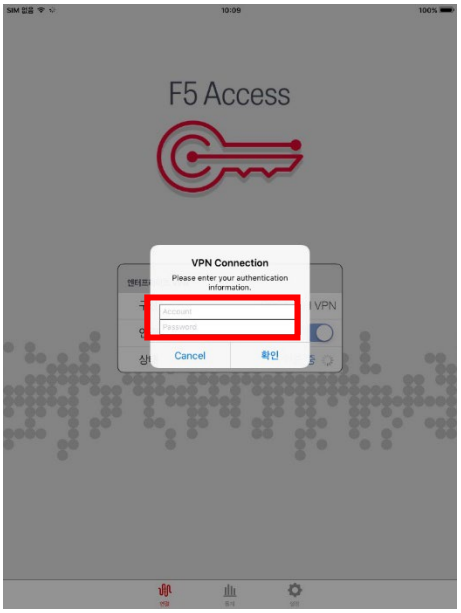

KT 100% 11:46
연결
F5 Access
POSTECH VPN
구성
연결되었습니다.
00:00:11
상태
연결 끊기

2) IOS


F5 Access
엔터프라이즈 VPN
구성
새로 추가
상태
연결 끊어짐


F5 Access
취소
구성
저장
설명
POSTECH VPN
서버
https://vpn.postech.ac.kr
웹 로그온
인증서 사용
사용자이름
패스워드
필요 시 연결


F5 Access
엔터프라이즈 VPN
구성
POSTECH VPN
연결
상태
연결 끊어짐


F5 Access
VPN Connection
Please enter your authentication information.
Account
Password
Cancel
확인


F5 Access
구성
POSTECH VPN
연결됨: 00:00:07

5. VPN 이중인증

5-1. 추진 배경

- 교육부 정보보안 기본지침 제 57 조(원격근무 보안)에 의거 VPN 이용 시 보안성 강화한 사용자 인증 필요

5-2. 이중인증 방법

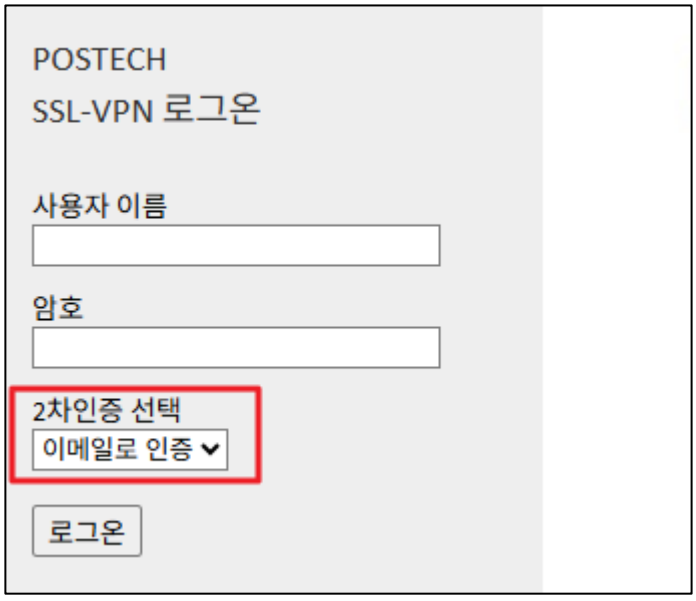
- 대상: 대학 VPN 이용자 전체

(1) 이메일 인증 방식

- OTP 를 이메일로 수신하여 입력

[인증 절차]

① ID/PW 입력 후 '이메일로 인증'을 선택합니다.



② OTP 코드를 메일로 수신 받습니다.



③ OTP 코드를 입력한 후 VPN 서비스를 사용합니다.



(2) MS Authenticator 앱 인증 방식

- 어플리케이션을 실행하여 생성된 OTP 코드를 기입

※ 앱 인증의 경우 최초 로그인 시 MS Authenticator 앱에서 등록이 필요합니다.

- MS Authenticator 앱이 설치되어 있지 않을 경우 (2)-1 부터 시작
- MS Authenticator 앱이 설치되어 있을 경우 (2)-2 부터 시작

(2)-1. MS Authenticator 앱이 설치되어 있지 않을 경우



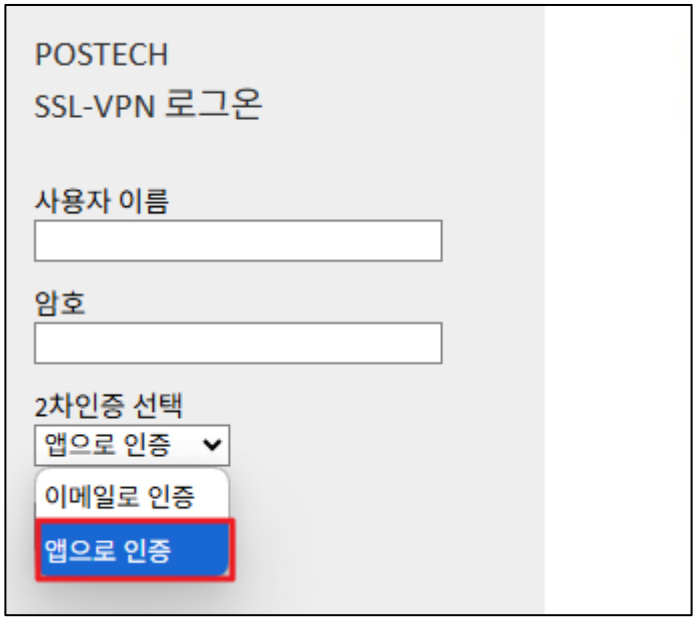
모바일 스토어(플레이스토어 또는 앱스토어) 접속

"MS Authenticator" 어플리케이션 검색하여 설치

(2)-2. MS Authenticator 앱이 설치되어 있을 경우

[PC 에서 인증]

① VPN 홈페이지 접속 후 ID/PW 를 입력하고 '앱으로 인증'을 선택합니다.



② 화면에 QR 코드 팝업 후 등록 절차 실시

- MS Authenticator 어플 실행 > Authenticator > + 버튼(계정 추가 버튼) 클릭 > 기타 계정 > 화면의 QR 코드 촬영 > OTP 생성 ID 확인

- MS Authenticator 어플 실행 > 우측 하단 QR 코드 아이콘 클릭 > 화면의 QR 코드 촬영 > OTP 생성 ID 확인



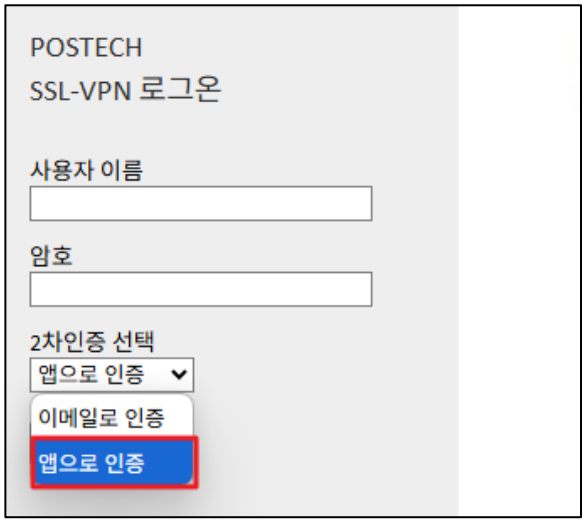
③ QR 코드 등록 후 VPN 홈페이지 접속하여 다시 로그인 시도

④ ID/PW 입력 후 MS Authenticator 어플 내 OTP 코드 6 자리 입력



[모바일에서 인증]

① VPN 홈페이지 접속 후 ID/PW 를 입력하고 '앱으로 인증'을 선택합니다.



② 화면에 QR 코드 팝업 후 등록 절차 실시

②-1) QR 코드 팝업 페이지 내 account, key(secret) 항목 복사

②-2) MS Authenticator 어플 실행 > Authenticator > + 버튼(계정 추가 버튼) 클릭 > 기타 계정 > Enter Code manually > 복사한 account/key(secret)을 계정이름/비밀키 항목에 입력 > OTP 생성 ID 확인



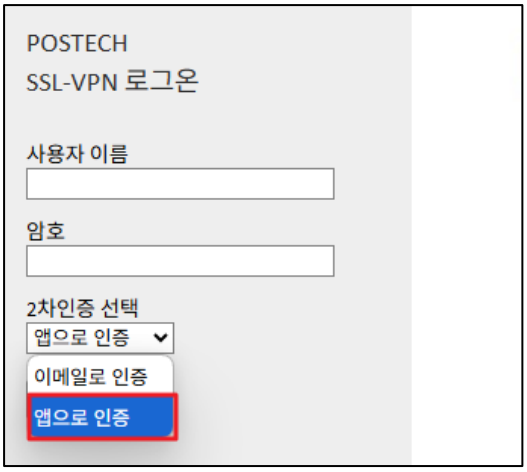
③ QR 코드 등록 후 VPN 홈페이지 접속하여 다시 로그인 시도

④ ID/PW 입력 후 MS Authenticator 어플 내 OTP 코드 6 자리 입력



(2)-3. MS Authenticator 앱 사용자 등록이 완료된 후

⑤ VPN 홈페이지 접속 후 ID/PW 를 입력하고 '앱으로 인증'을 선택합니다.



② MS Authenticator 어플 내 OTP 코드 6 자리 입력 후 서비스 사용



III. VPN 연결 장애 시 대응방법

1. 클라이언트 접속 장애

가. 클라이언트 버전 문제로 인해 연결 장애가 발생할 수 있음.

- 클라이언트 프로그램 삭제 및 재설치 후 재접속 시도.
- 웹사이트를 통한 VPN 접속 시도.

2. Linux 접속 장애

가. Linux 내에서의 VPN 접속이 되지 않을 때, Linux 내의 VPN 패키지 버전 노후로 인해 해당 현상이 발생할 수 있음.

- https://vpn.postech.ac.kr 의 클라이언트 다운로드를 통해 최신 VPN 패키지를 설치 후 VPN 재접속 시도.

나. 최신 VPN 패키지 설치 후 같은 증상 발생 시, Linux OS 버전의 최신화 진행 후 VPN 접속 진행.

3. 이차인증 오류 발생

가. 이메일 이차인증 시스템 오류: 재학생의 경우 MS 클라우드 메일 시스템을 이용하고 있어 메일 시스템 상황에 따라 OTP 코드 발송이 늦는 경우가 다소 발생하고 있음.

- 여러 번 시도를 통해 메일을 수신 받거나 앱 인증 방식을 적용
- 아래의 항목에 해당하시는 경우에는 관리자(security@postech.ac.kr)에게 인증 초기화 요청을 보내어 새로 등록하도록 하여야 함
  (1) QR 코드 촬영 전에 QR 코드 있는 화면을 꺼버렸어요.
  (2) QR 코드에서의 account, key 를 입력 전에 잊어버렸어요.
  (3) OTP 인증 어플을 삭제해버렸어요.
  (4) OTP 인증 계정을 삭제해버렸어요.
  (5) 스마트폰을 바꾸면서 어플을 새로 받아야해요.