

SecuwaySSL U v2.0

사용자 매뉴얼

목 차

1. Windows 설치 및 접속

1-1. 브라우저 Client 설치

1-1-1. Internet Explorer	5P
1-1-2. Chrome	9P
1-1-3. Opera	14P
1-1-4. Firefox	19P
1-1-5. Edge	23P

1-2. 프로그램 설치

1-2-1. CS	27P
---------------------------	-----

1-3. Windows 접속 방식

1-3-1. ID/PW 접속	28P
1-3-2. ID/PW CS 접속	31P
1-3-3. ID/PW APP OTP 접속	34P
1-3-4. ID/PW SMS OTP 접속	37P
1-3-5. ID/PW 인증서 접속	39P
1-3-6. ID/PW QR CODE 접속	44P

2. Mac 설치 및 접속

2-1. Mac Client 설치

2-1-1. Mac	47P
----------------------------	-----

2-2. Mac 접속 방식

2-2-1. ID/PW 접속	52P
2-2-2. ID/PW OTP 접속	53P
2-2-3. ID/PW 인증서 접속	55P

목 차

3. Mobile 설치 및 접속

3-1. Mobile Client 설치

3-1.1 .iOS	60P
3-1.2. Android	64P

3-2. iOS 접속 방식

3-2-1. ID/PW 접속	66P
3-2-2. ID/PW OTP 접속	67P
3-2-3. ID/PW 인증서 접속	69P

3-3. Android 접속 방식

3-3-1. ID/PW 접속	72P
3-3-2. ID/PW OTP 접속	74P
3-3-3. ID/PW 인증서 접속	76P

4. 임베디드 설치 및 접속

4-1. Linux Client 설치

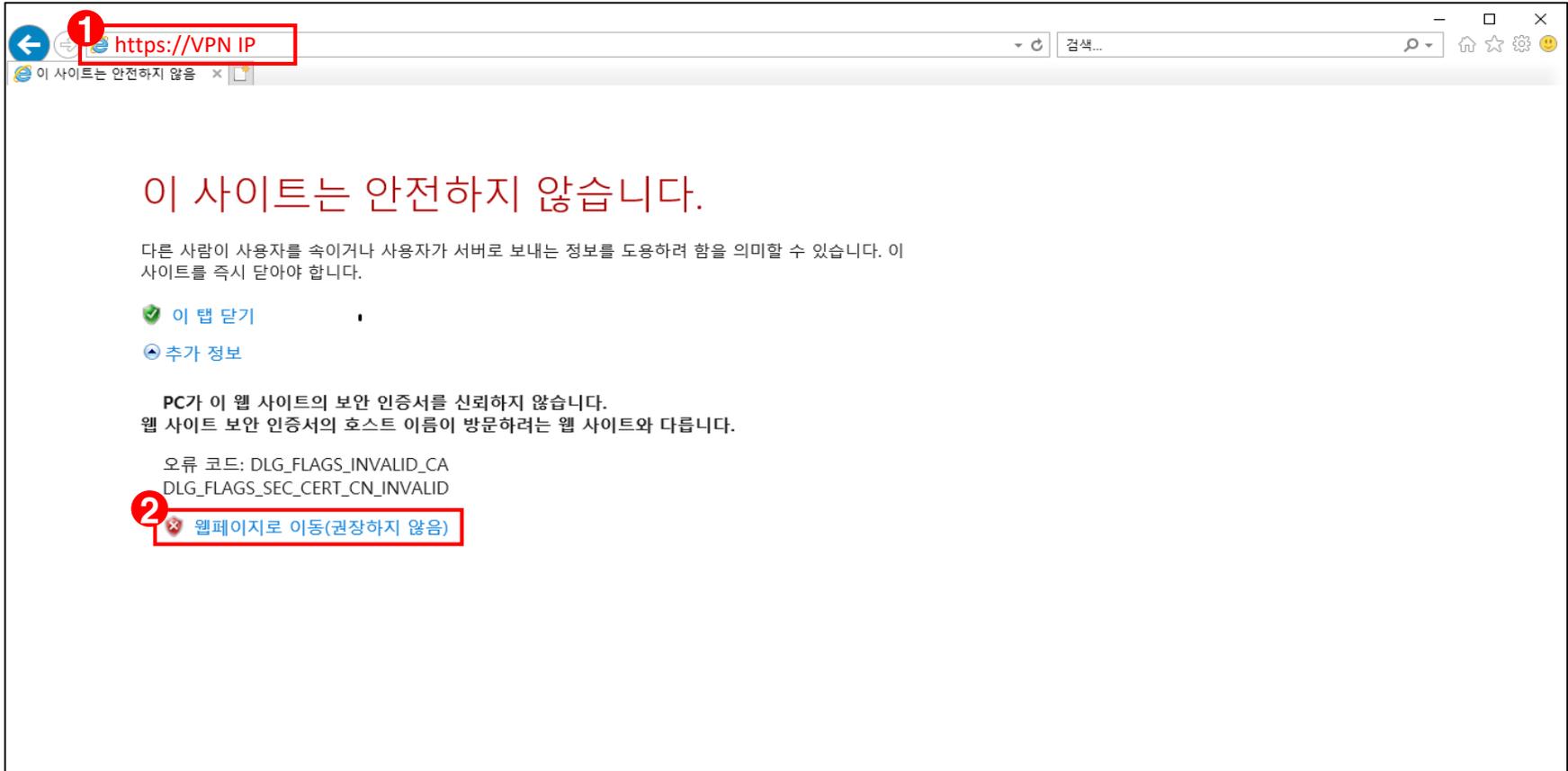
4-1-1. Linux	78P
------------------------------------	-----

4-2. Linux 접속 방식

4-2-1. ID/PW 접속	80P
---------------------------------------	-----

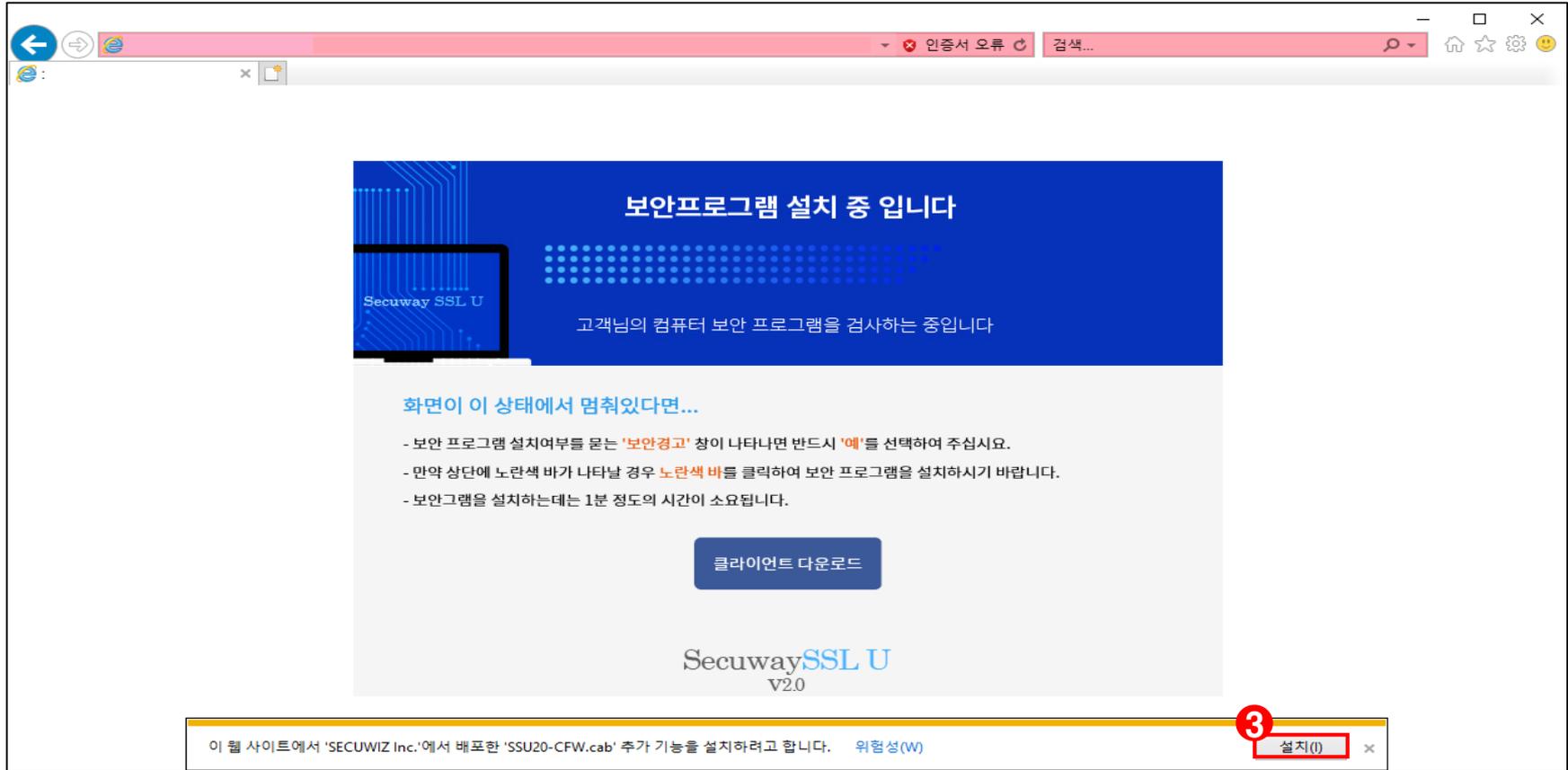
1-1-1 Internet Explorer #1

1. 사용자가 VPN에 접속하기 위해서는 주소 창에 VPN 관리페이지에서 설정한 WAN IP를 입력합니다.
접속하면 보안 인증서가 없는 경우 보안 인증서와 관련된 문제가 있음을 알리는 경고 화면이 생성됩니다.
2. "웹사이트를 이동(권장하지 않음)" 을 클릭합니다.



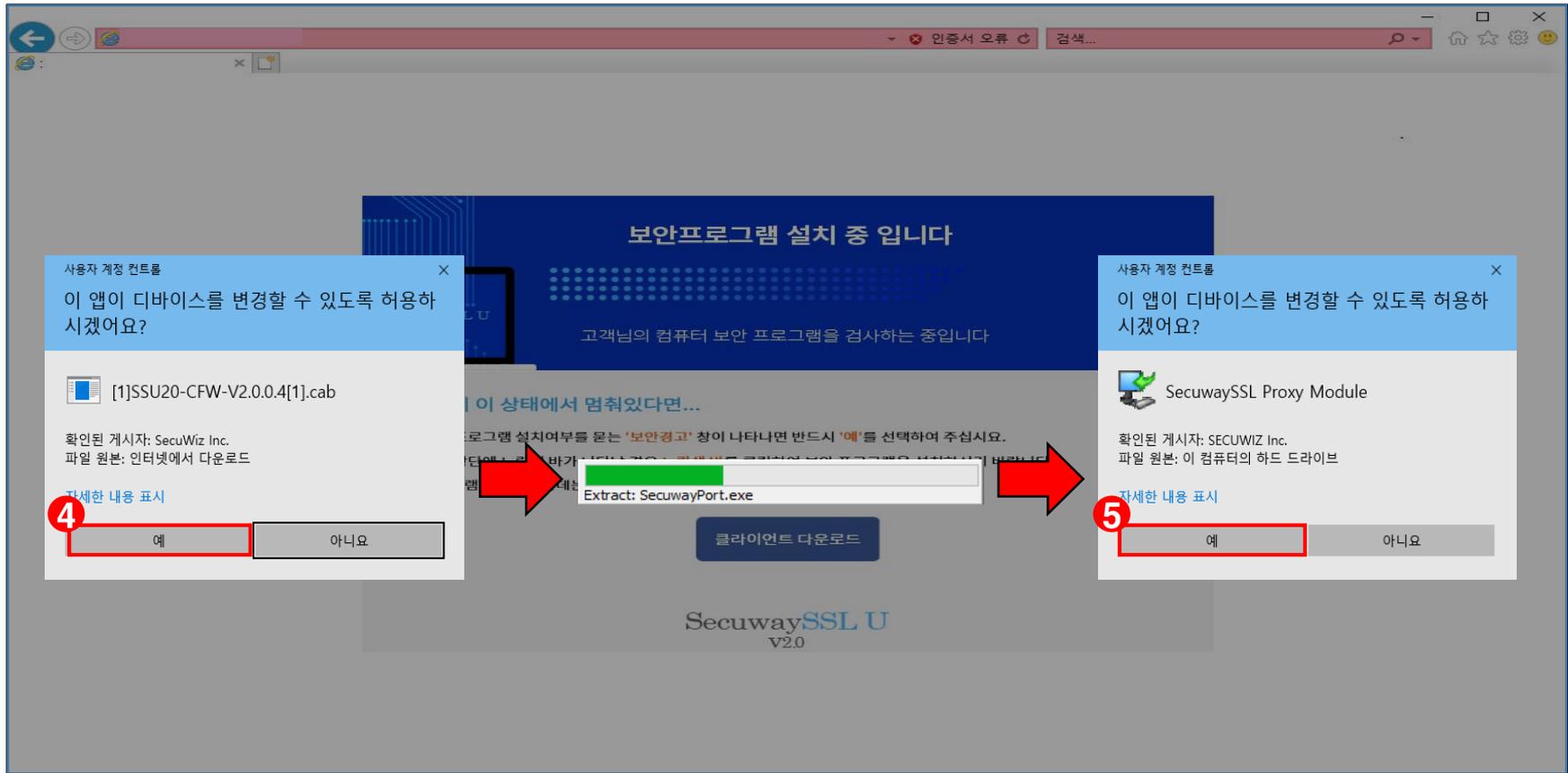
1-1-1 Internet Explorer #2

3. 인터넷 브라우저 하단에 "이 웹 사이트에서 'SECUWIZ Inc.'에서 배포한 'SSU20-CFW.cab' 추가 기능을 설치 하려고 합니다." 라는 경고 메시지가 나타나면 "설치" 를 클릭하여 Active X 설치를 진행합니다.



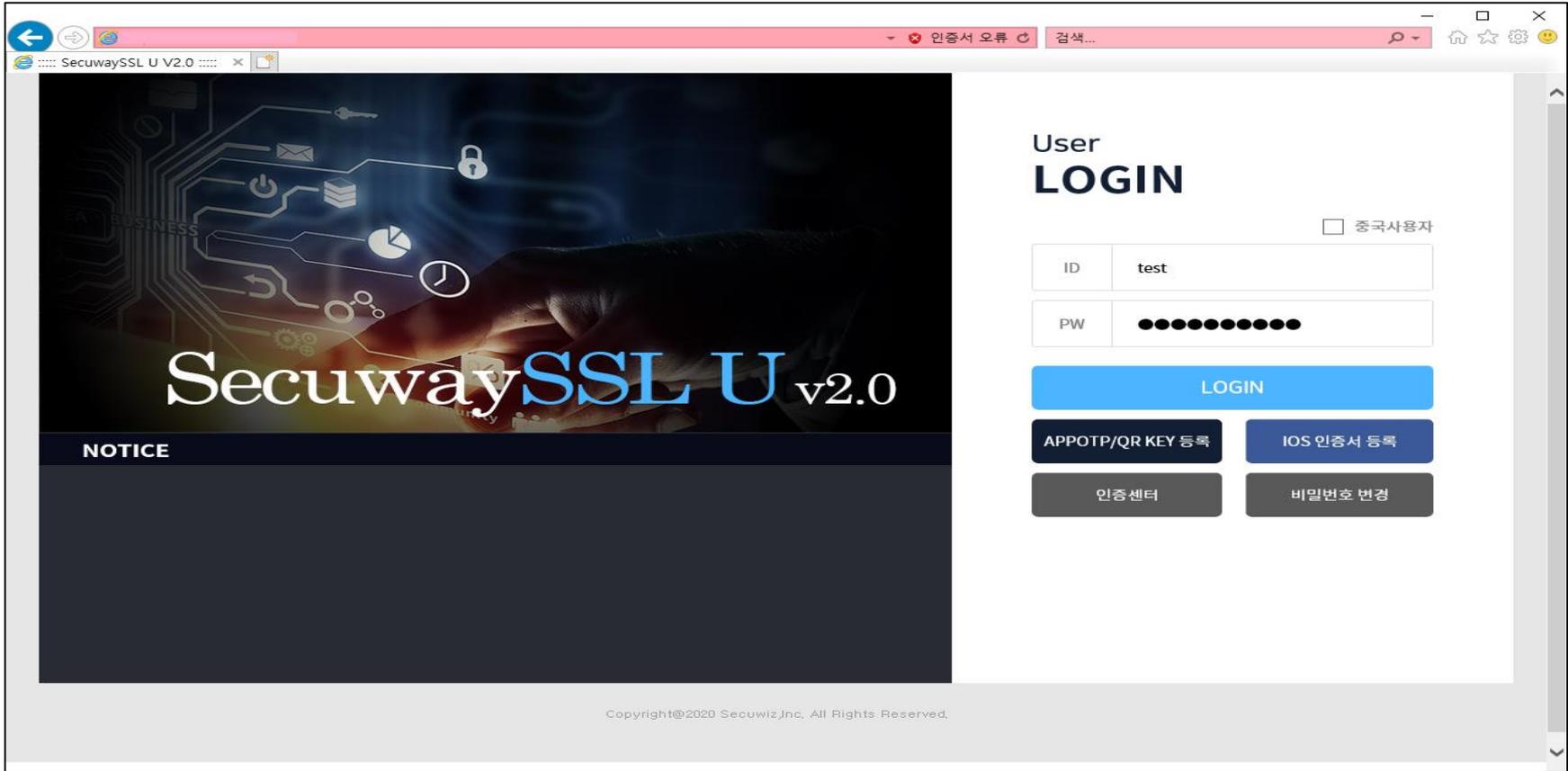
1-1-1 Internet Explorer #3

- 4. ActiveX를 이용한 SecuwaySSL U Client 프로그램 설치를 위한 보안 경고 메시지가 나타나면 “예” 버튼을 클릭하여 프로그램 설치를 진행합니다 .
- 5. 설치가 진행되고 다시 프로그램 허용 창이 생성되며 “예” 를 클릭합니다.



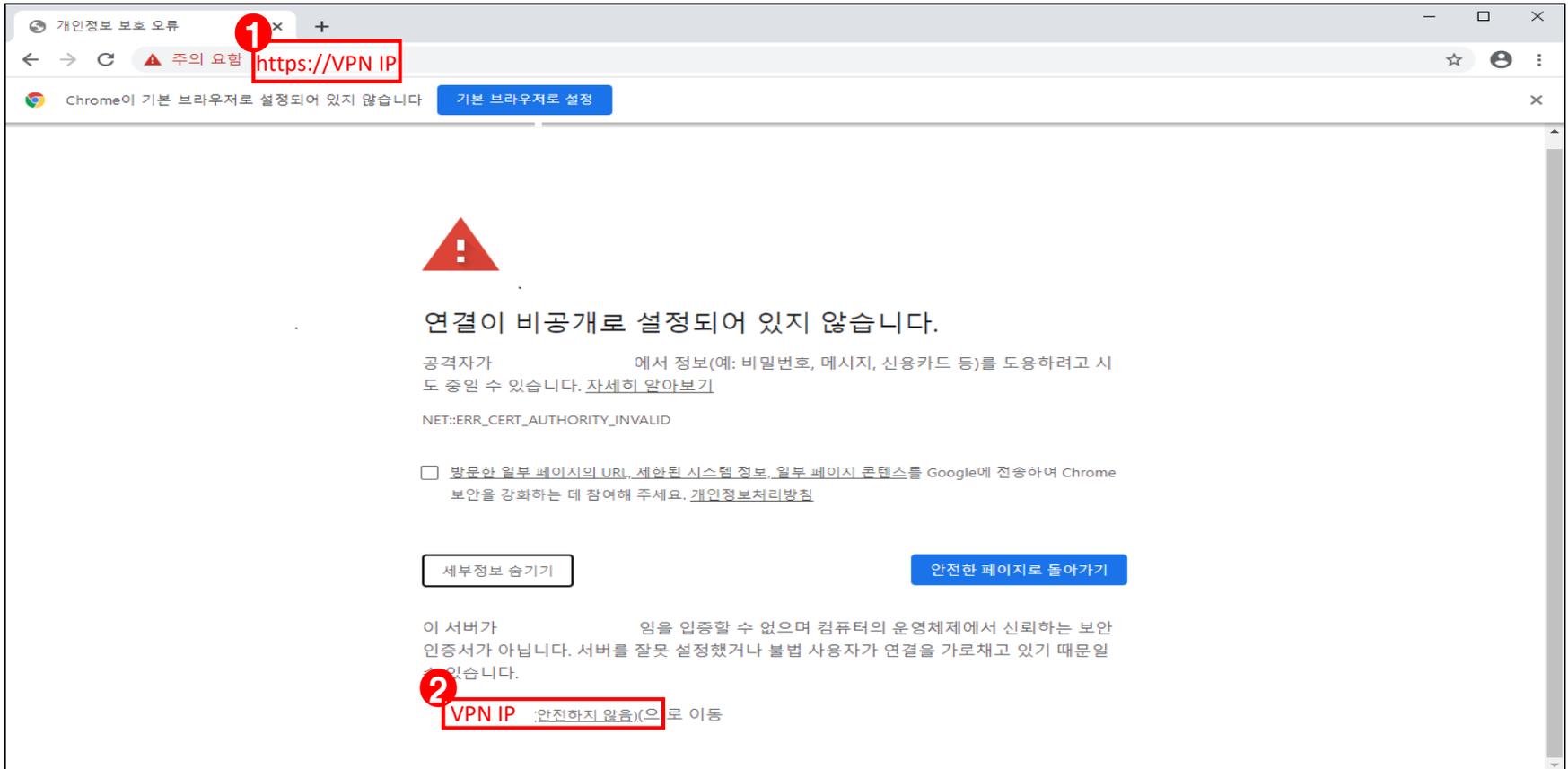
1-1-1 Internet Explorer #4

6. SecuwaySSL U Client 설치가 끝나면 로그인 화면으로 전환됩니다.



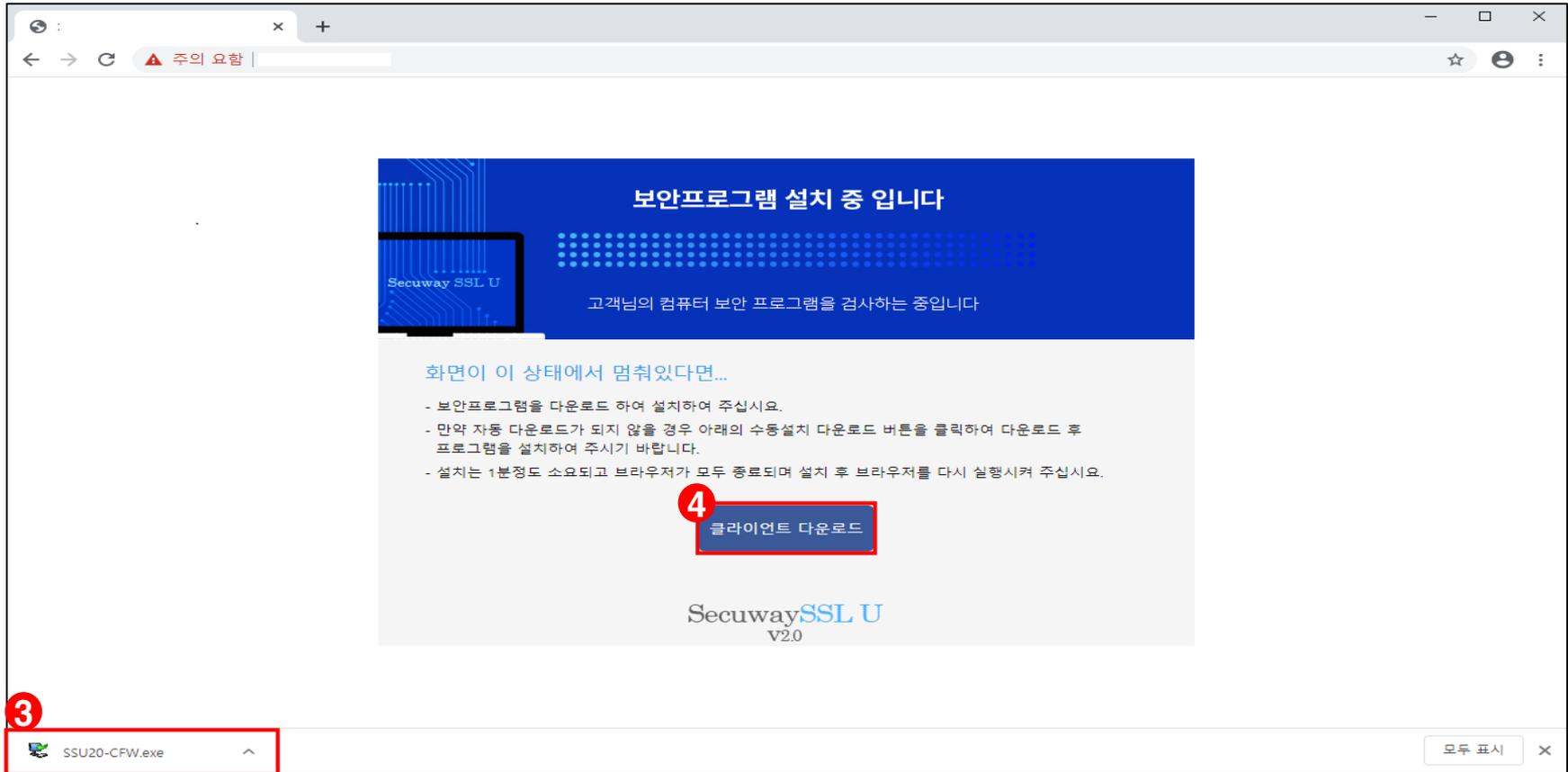
1-1-2 Chrome #1

1. 사용자가 VPN에 접속하기 위해서는 주소 창에 VPN 관리페이지에서 설정한 WAN IP를 입력합니다. 접속하면 보안 인증서가 없는 경우 보안 인증서와 관련된 문제가 있음을 알리는 경고 화면이 생성됩니다.
2. "서버IP(안전하지 않음)"을 클릭합니다.



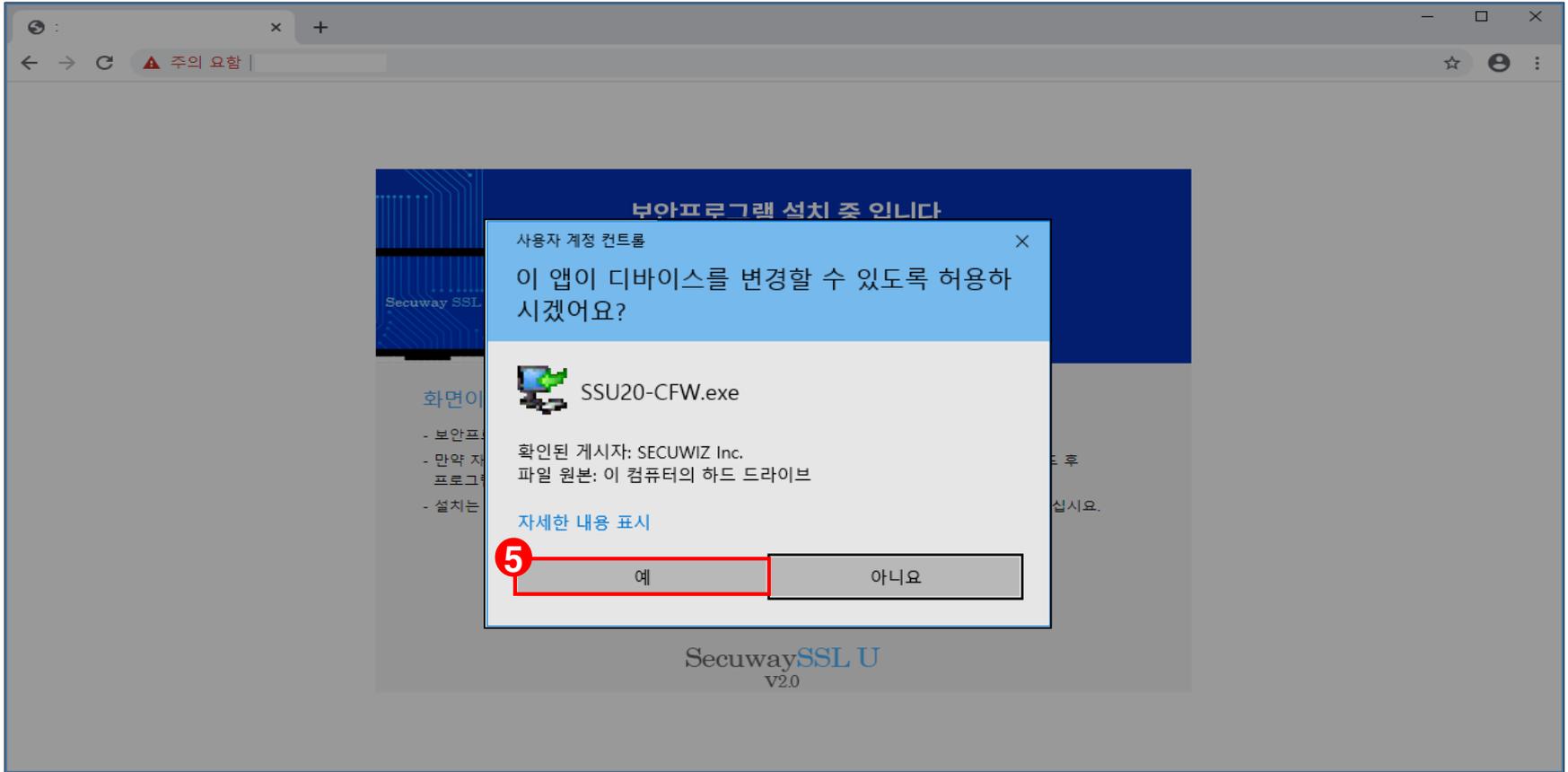
1-1-2 Chrome #2

- 3. 보안프로그램 설치 중 화면으로 전환되며 브라우저 하단에 자동으로 프로그램이 다운됩니다.
- 4. 자동 다운로드가 되지 않으면 "**클라이언트 다운로드**" 버튼을 클릭하여 설치합니다.



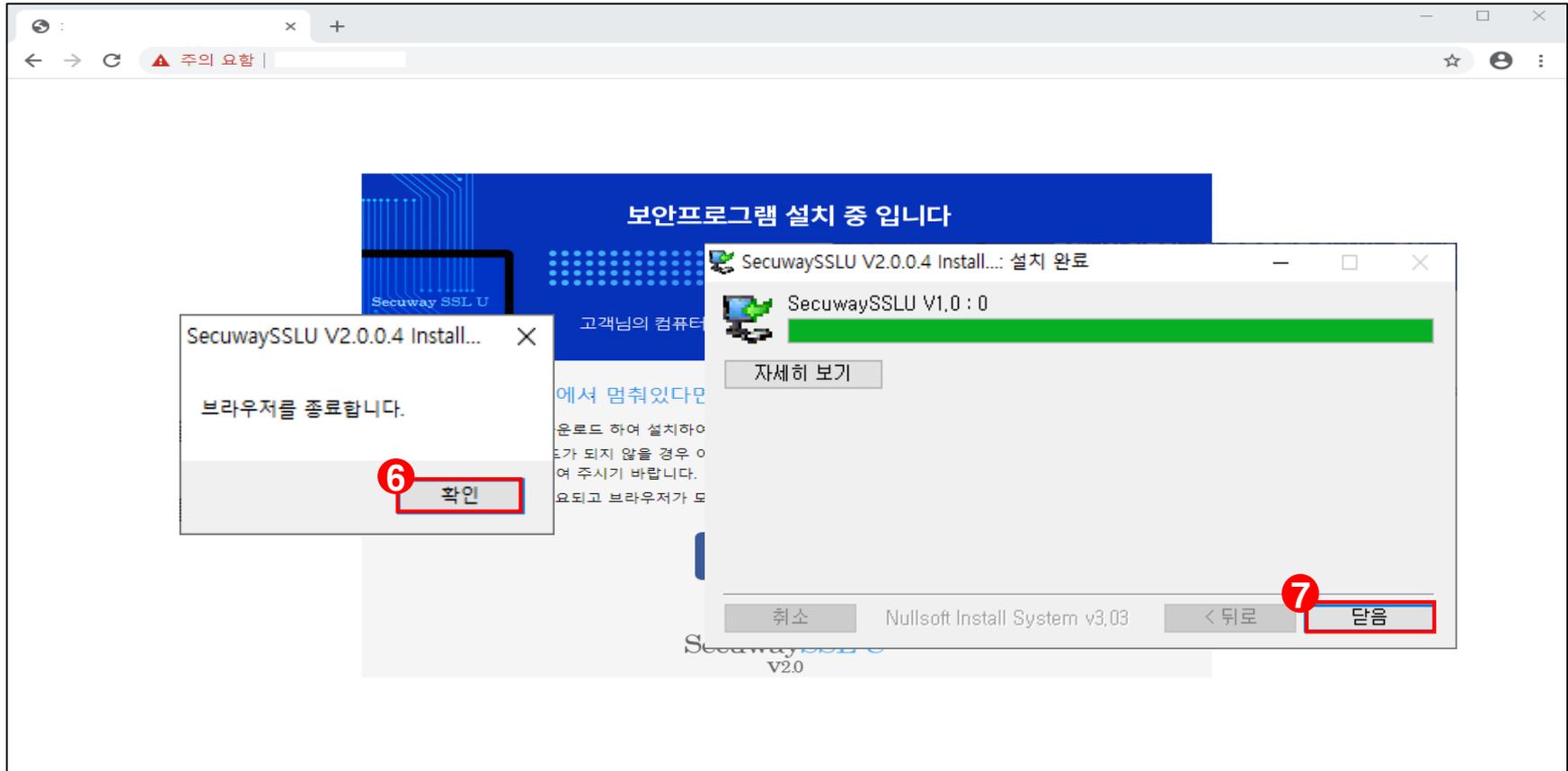
1-1-2 Chrome #3

- 5. SecuwaySSL U Client 프로그램 설치를 위한 보안 경고 메시지가 나타나면 “예” 버튼을 클릭하여 프로그램 설치를 진행합니다.



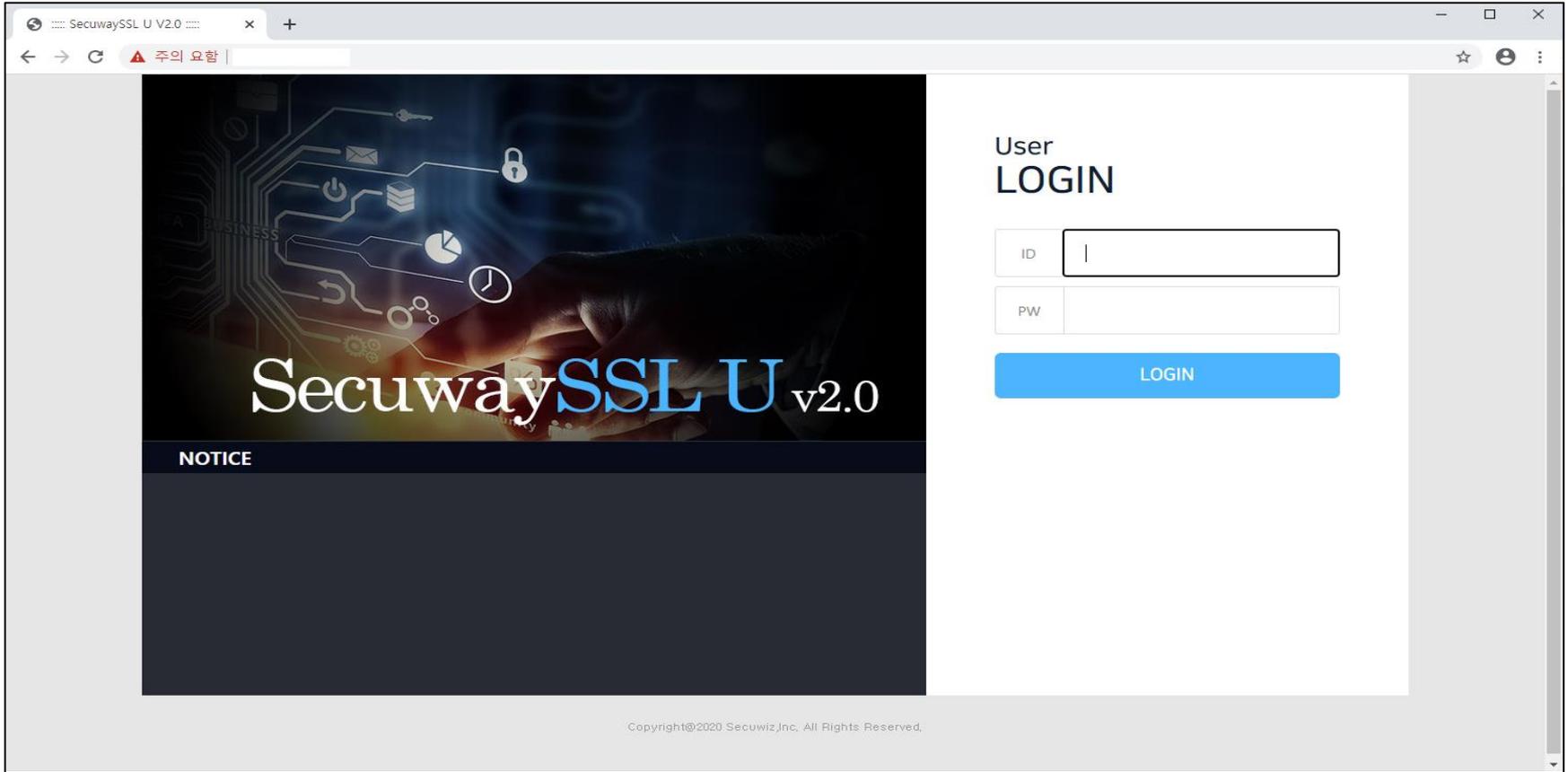
1-1-2 Chrome #4

- 6. "브라우저를 종료합니다." 메시지가 생성되면 "확인" 을 클릭합니다.
- 7. 모든 브라우저가 닫힌 후 설치가 진행이 되며, 완료되면 "다음" 을 클릭합니다.



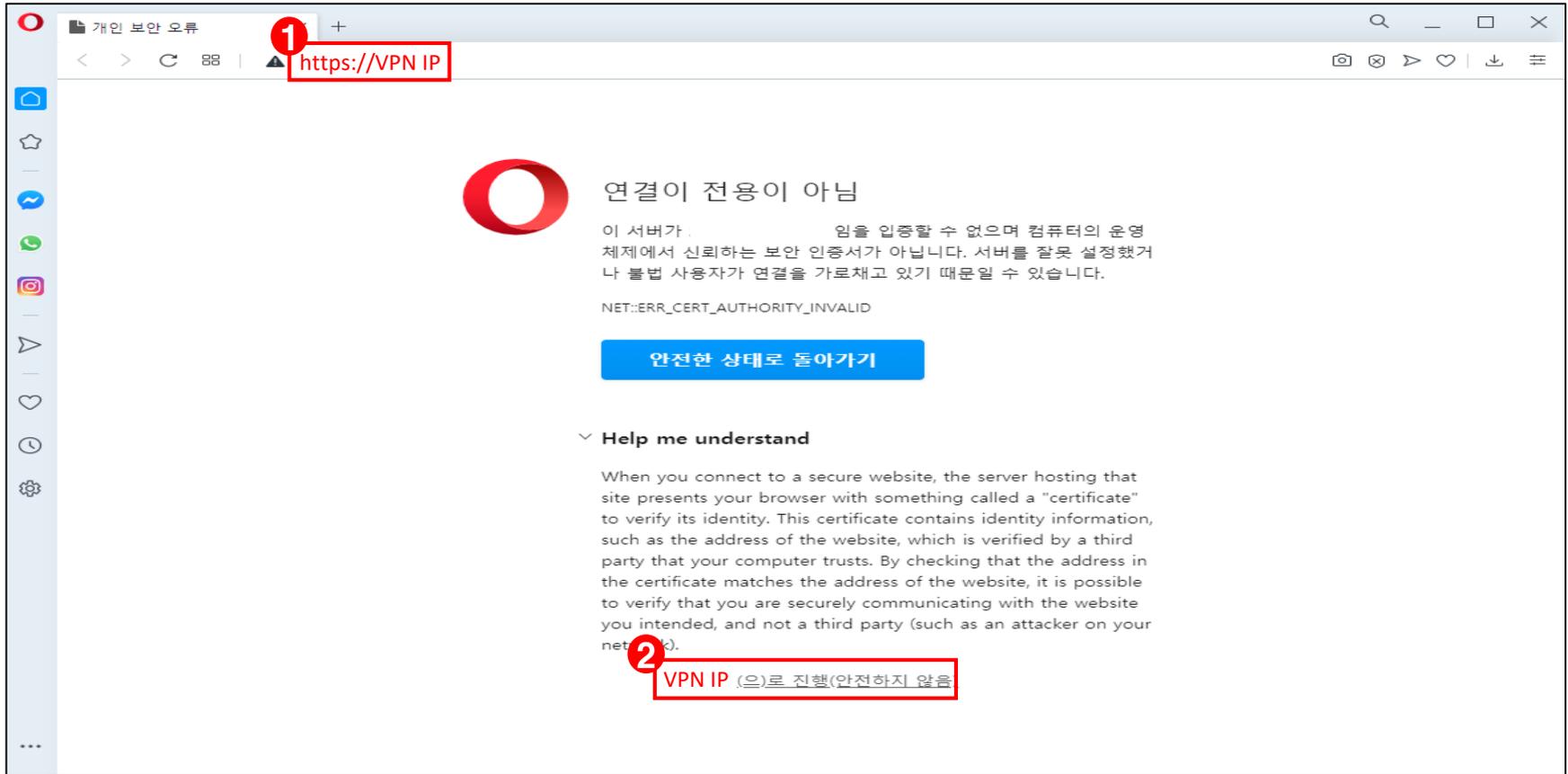
1-1-2 Chrome #5

8. SecuwaySSL U Client 설치가 완료되면 로그인 페이지로 접속이 가능합니다.



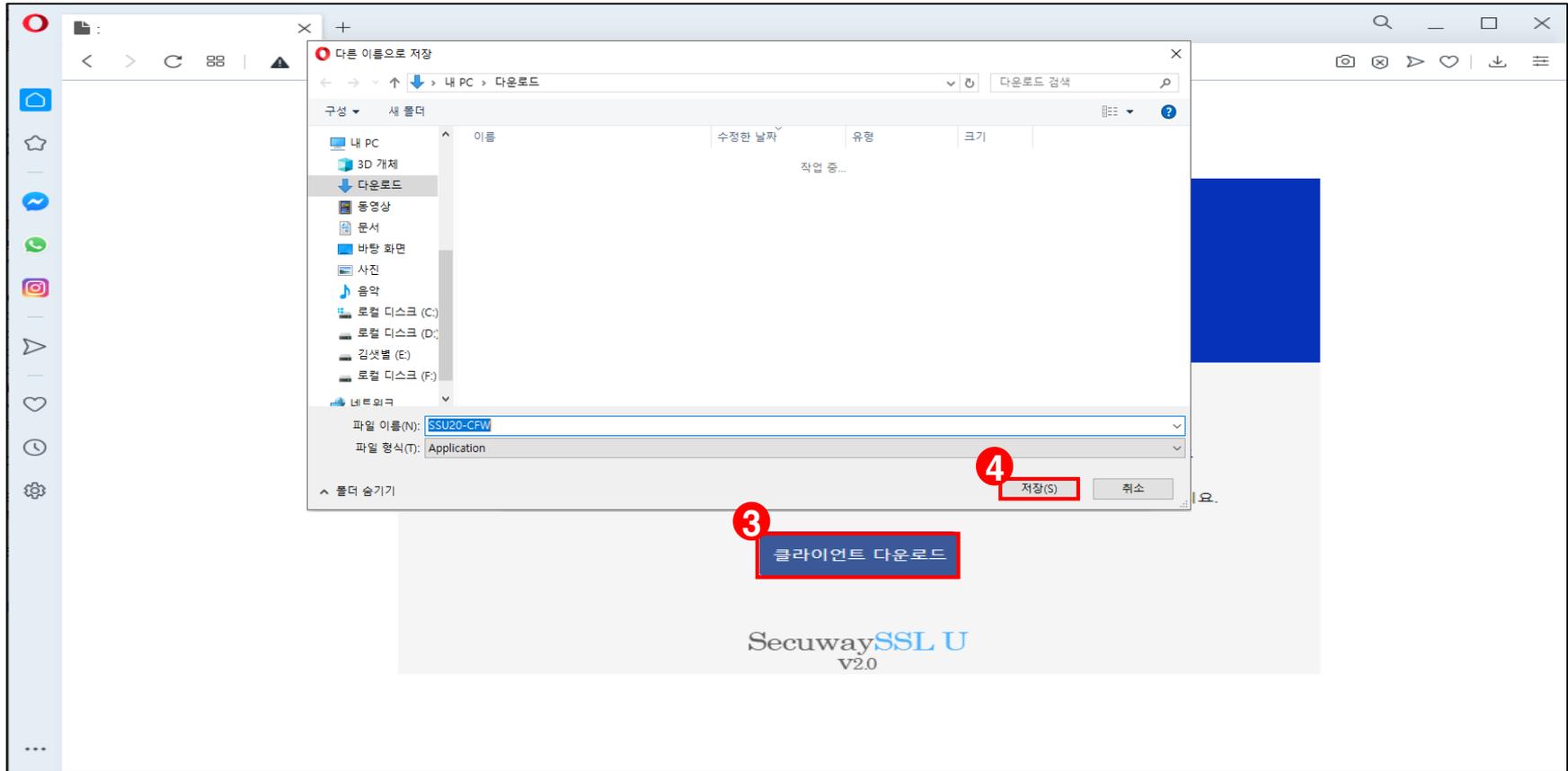
1-1-3 Opera #1

1. 사용자가 VPN에 접속하기 위해서는 주소 창에 VPN 관리페이지에서 설정한 WAN IP를 입력합니다. 접속하면 보안 인증서가 없는 경우 보안 인증서와 관련된 문제가 있음을 알리는 경고 화면이 생성됩니다.
2. "서버IP으로 진행(안전하지 않음)" 을 클릭합니다.



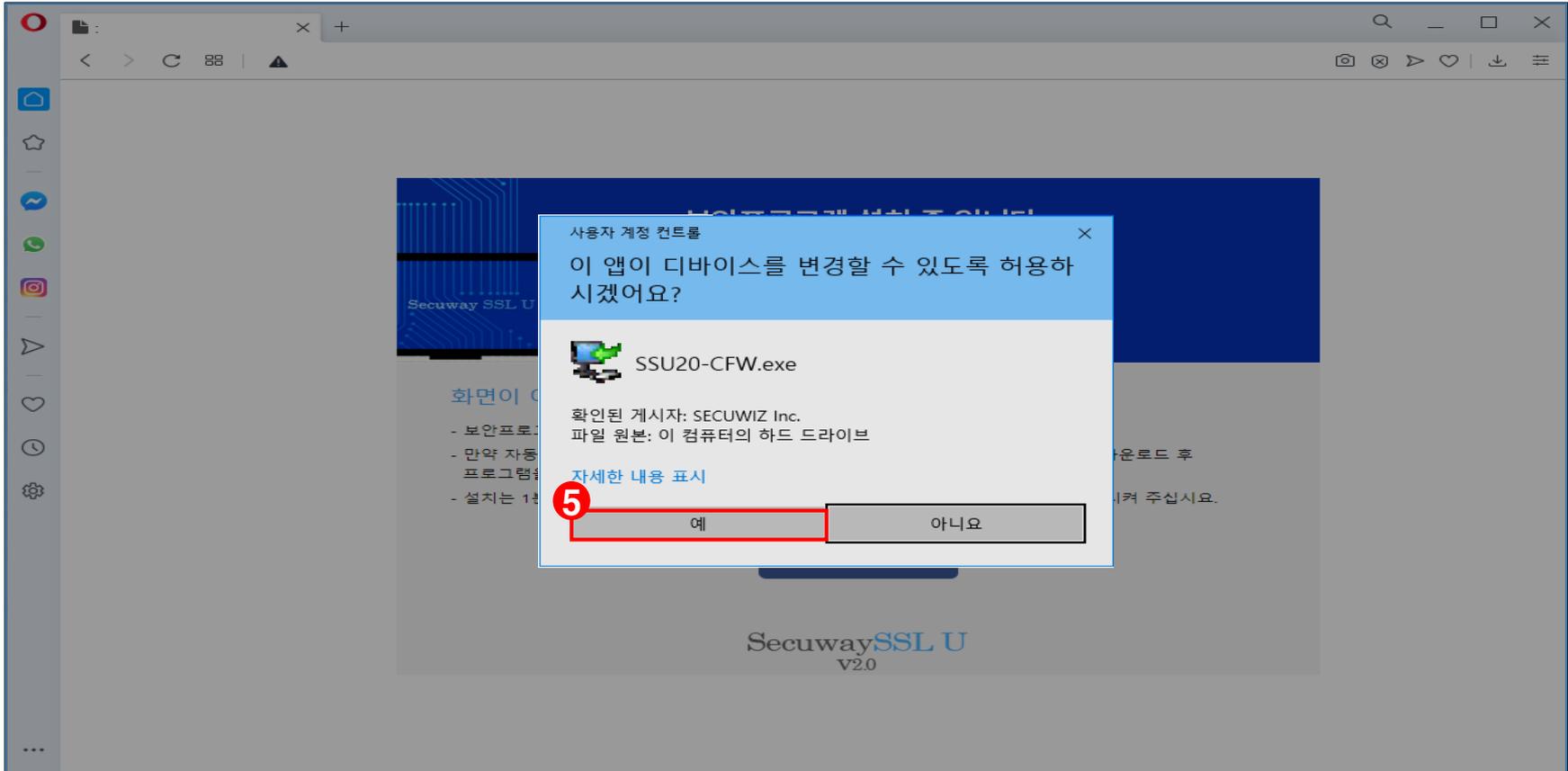
1-1-3 Opera #2

- 3. "클라이언트 다운로드" 를 클릭하여 다운로드합니다.
- 4. 다른 이름으로 저장으로 경로가 생성되고 "저장" 을 클릭하고 저장 받은 파일을 실행합니다.



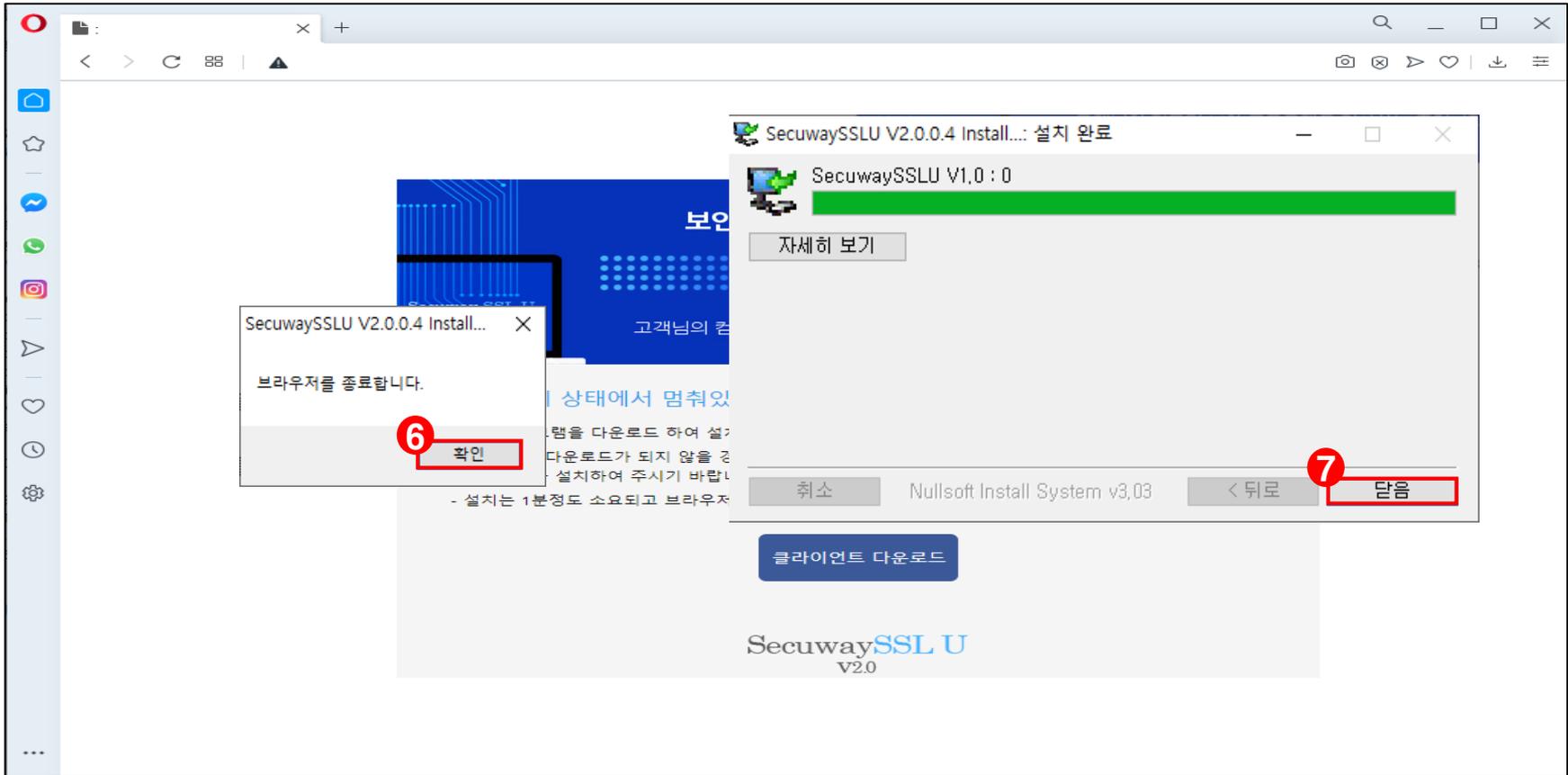
1-1-3 Opera #3

- 5. SecuwaySSL U Client 프로그램 설치를 위한 보안 경고 메시지가 나타나면 "예" 버튼을 클릭하여 프로그램 설치를 진행합니다



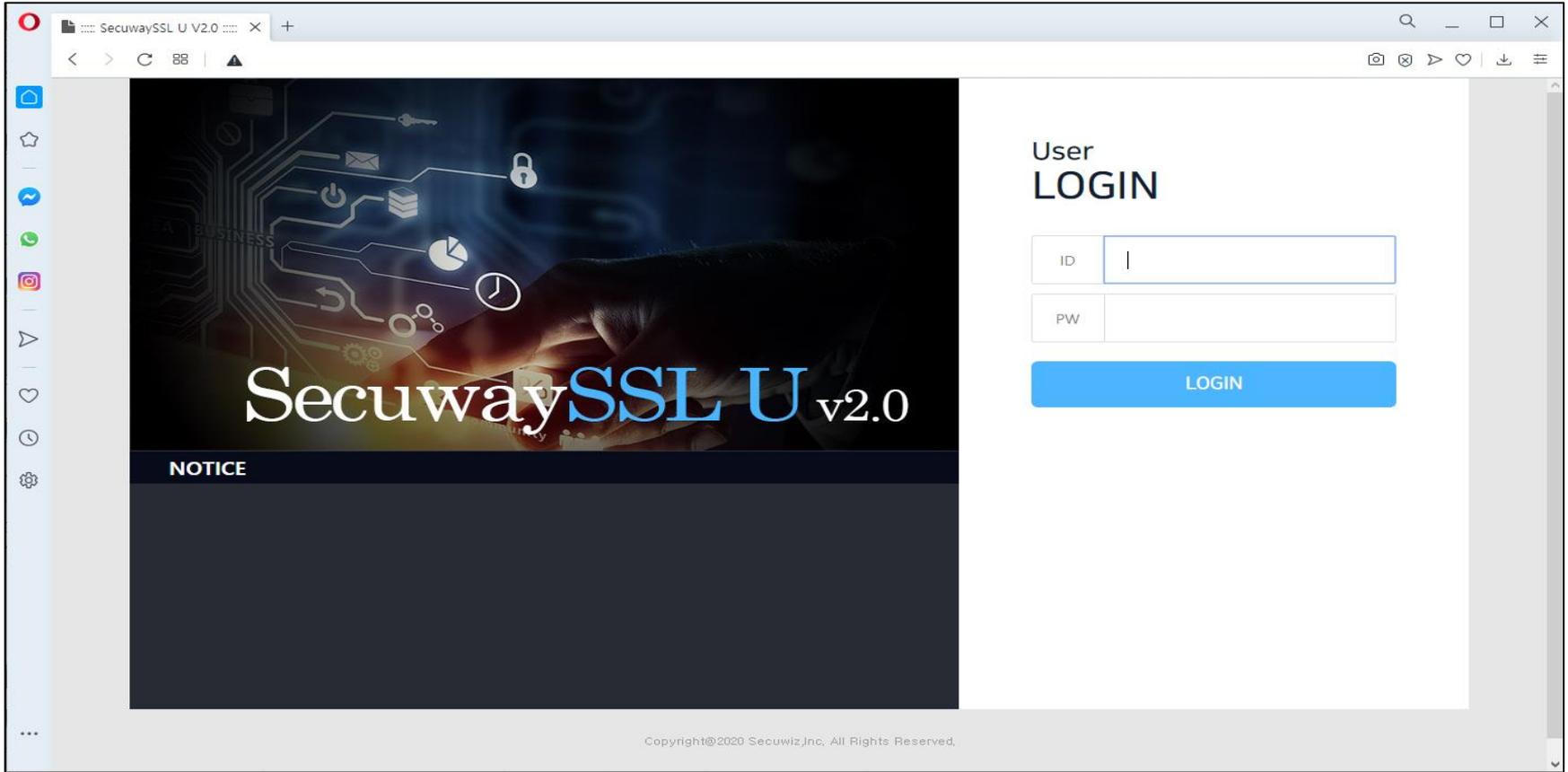
1-1-3 Opera #4

- 6. "브라우저를 종료합니다." 메시지가 생성되면 "확인" 을 클릭합니다.
- 7. 모든 브라우저가 닫힌 후 진행 창이 생성되며, 완료되면 "다음" 을 클릭합니다.



1-1-3 Opera #5

8. SecuwaySSL U Client 설치가 완료되면 로그인 페이지로 접속이 가능합니다.



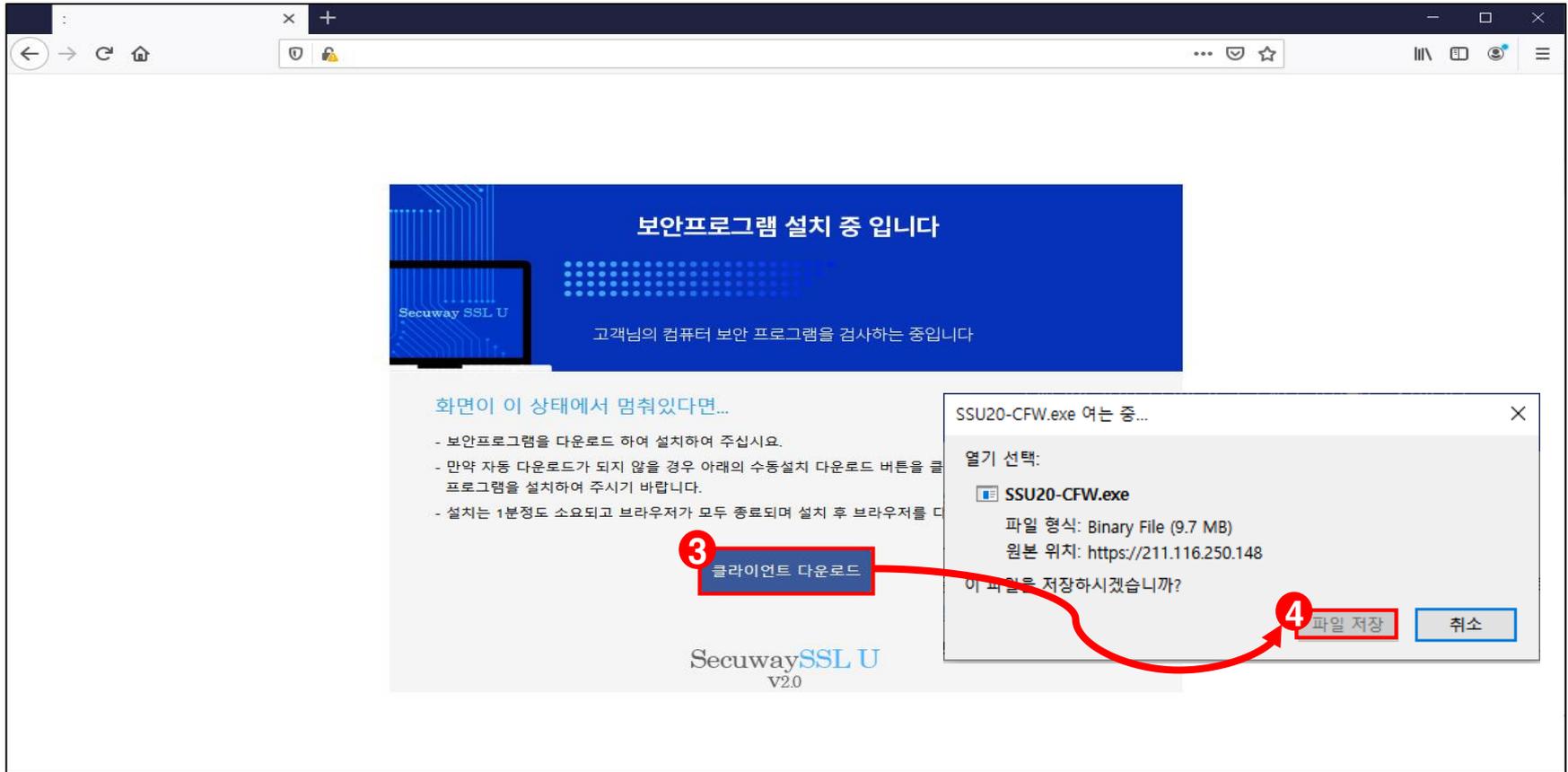
1-1-4 Firefox #1

1. 사용자가 VPN에 접속하기 위해서는 주소 창에 VPN 관리페이지에서 설정한 WAN IP를 입력합니다. 접속하면 보안 인증서가 없는 경우 보안 인증서와 관련된 문제가 있음을 알리는 경고 화면이 생성됩니다.
2. "위험을 감수하고 계속" 을 클릭합니다.



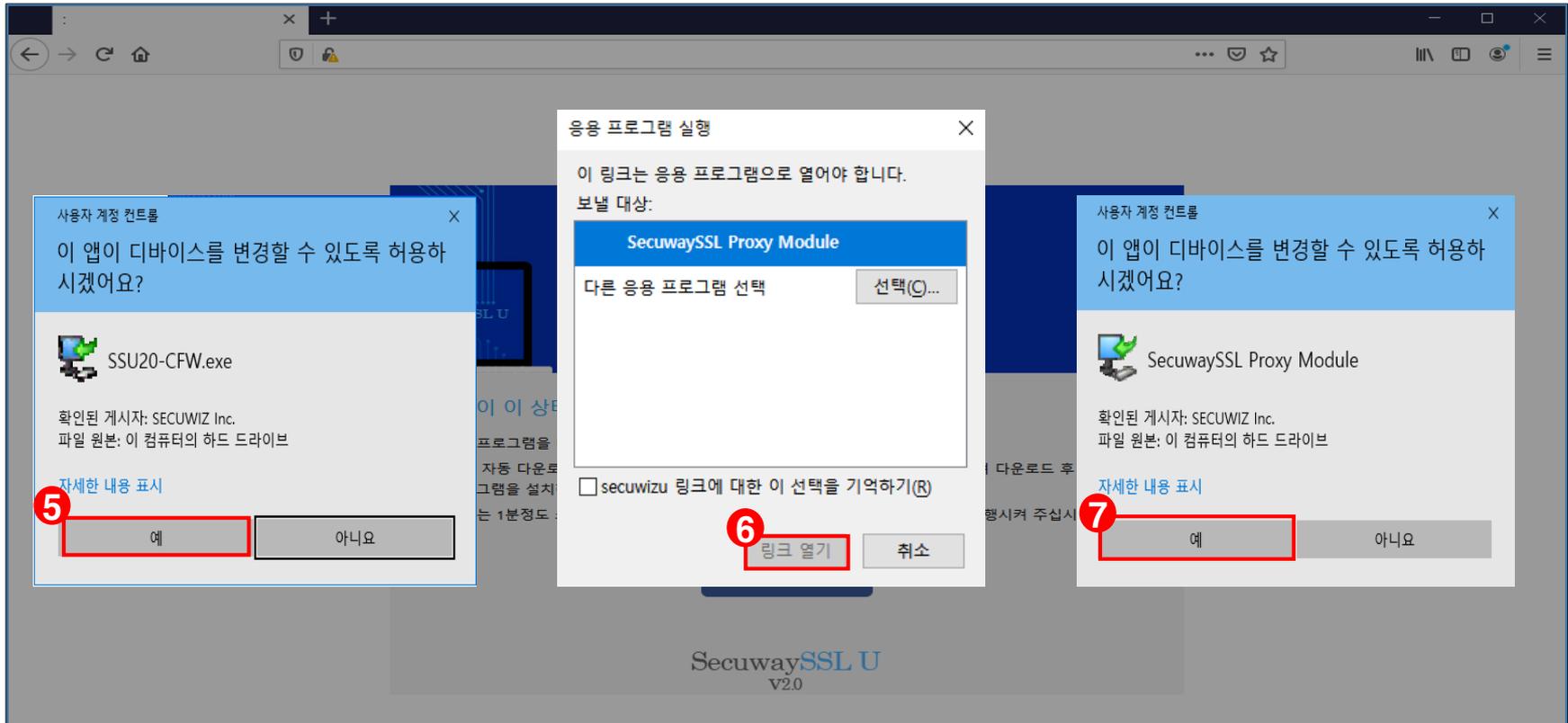
1-1-4 Firefox #2

- 3. "클라이언트 다운로드" 를 클릭하여 다운로드합니다.
- 4. 다른 이름으로 저장으로 경로가 생성되고 "파일 저장" 을 클릭하여 저장하고 실행합니다.



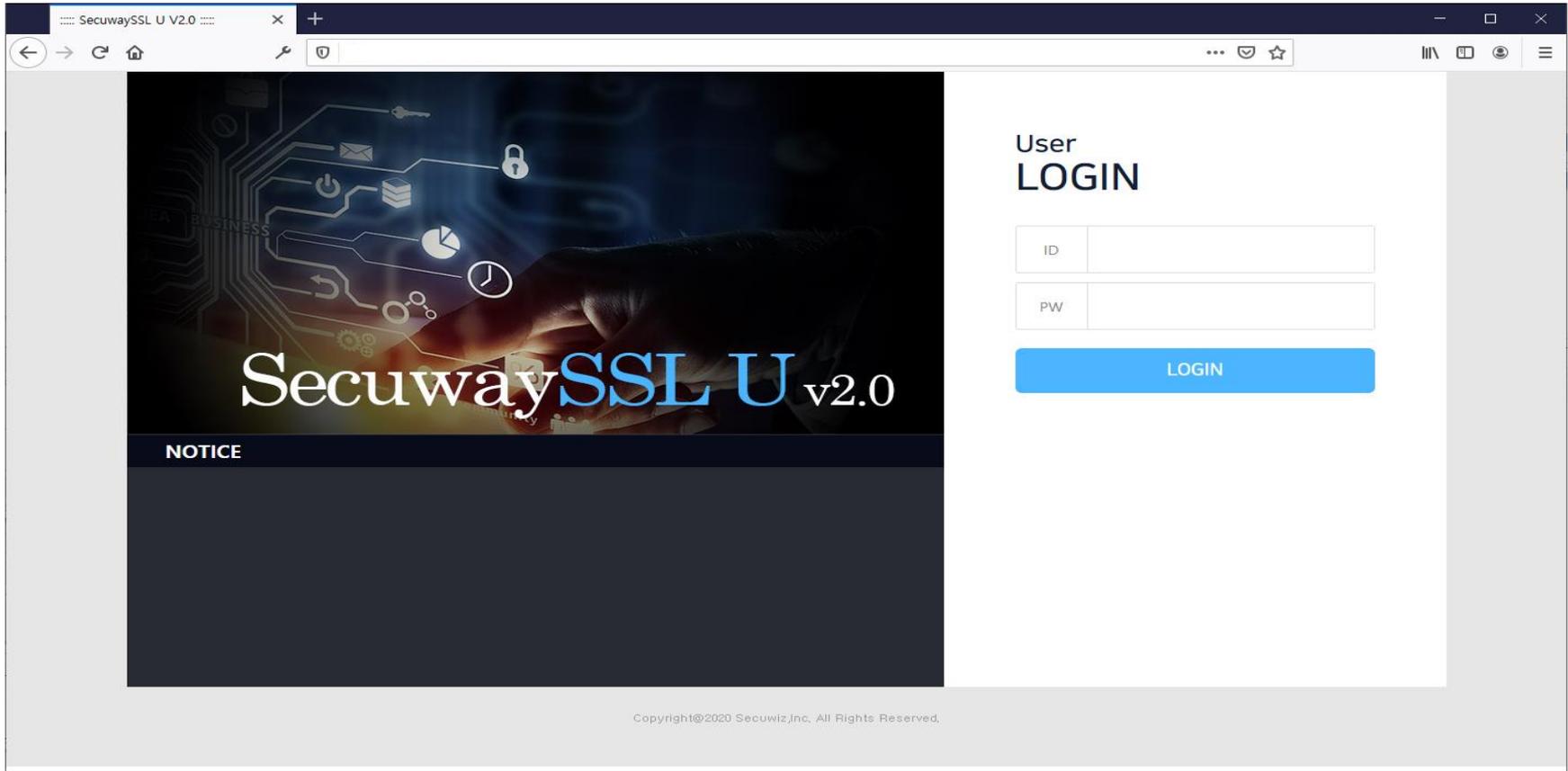
1-1-4 Firefox #3

- 5. SecuwaySSL U Client 프로그램 설치를 위한 보안 경고 메시지가 나타나면 “예” 버튼을 클릭하여 프로그램 설치를 진행합니다.
- 6. 응용프로그램 실행창이 생성되고 “링크 열기” 를 클릭합니다.
- 7. 다시 경고 창이 생성되고 “예” 를 클릭합니다.



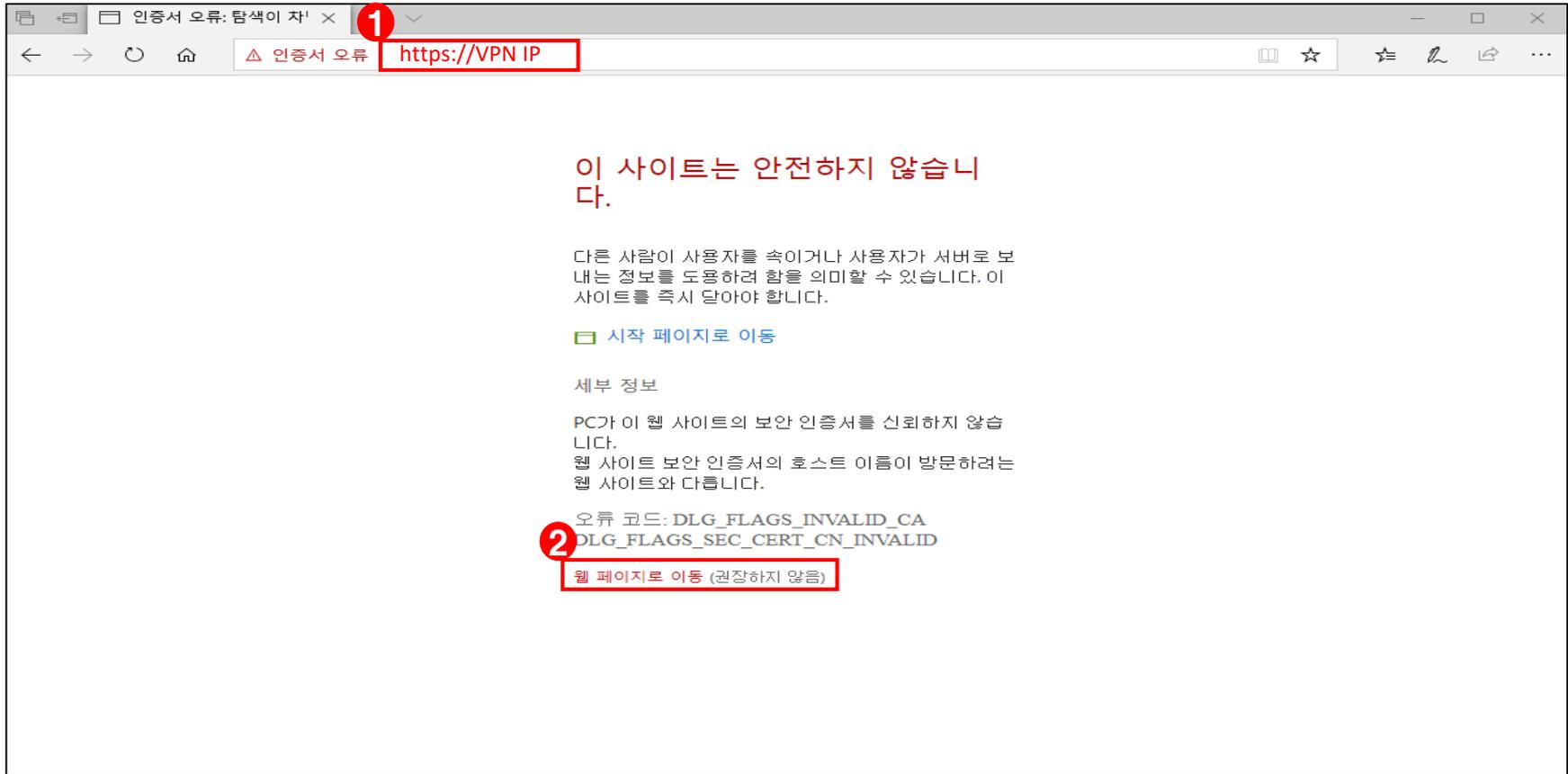
1-1-4 Firefox #4

8. SecuwaySSL U Client 설치가 완료되면 로그인 페이지로 접속이 가능합니다.



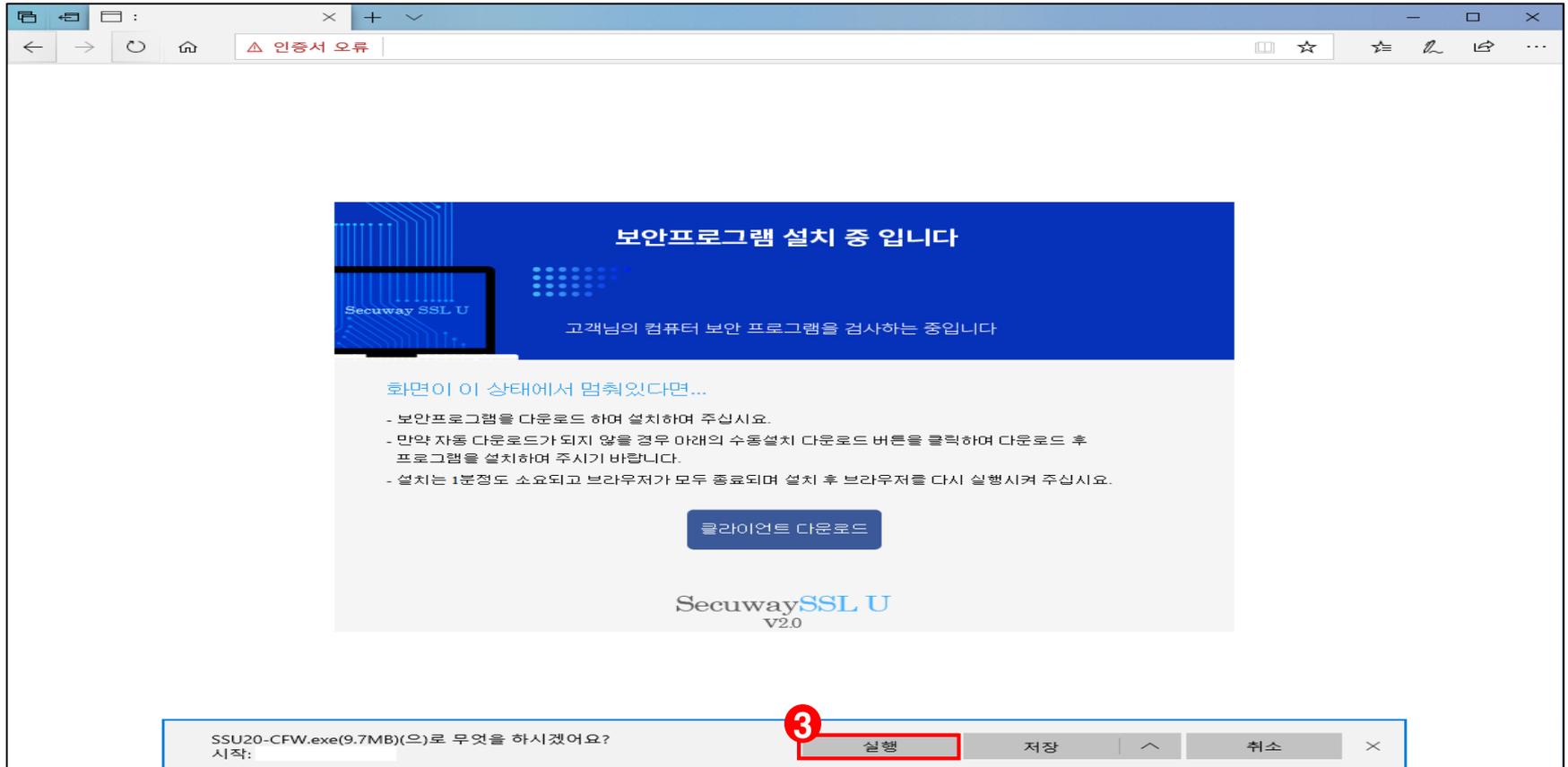
1-1-5 Edge #1

1. 사용자가 VPN에 접속하기 위해서는 주소 창에 VPN 관리페이지에서 설정한 WAN IP를 입력합니다. 접속하면 보안 인증서가 없는 경우 보안 인증서와 관련된 문제가 있음을 알리는 경고 화면이 생성됩니다.
2. “웹 페이지로 이동(권장하지 않음)” 을 클릭합니다.



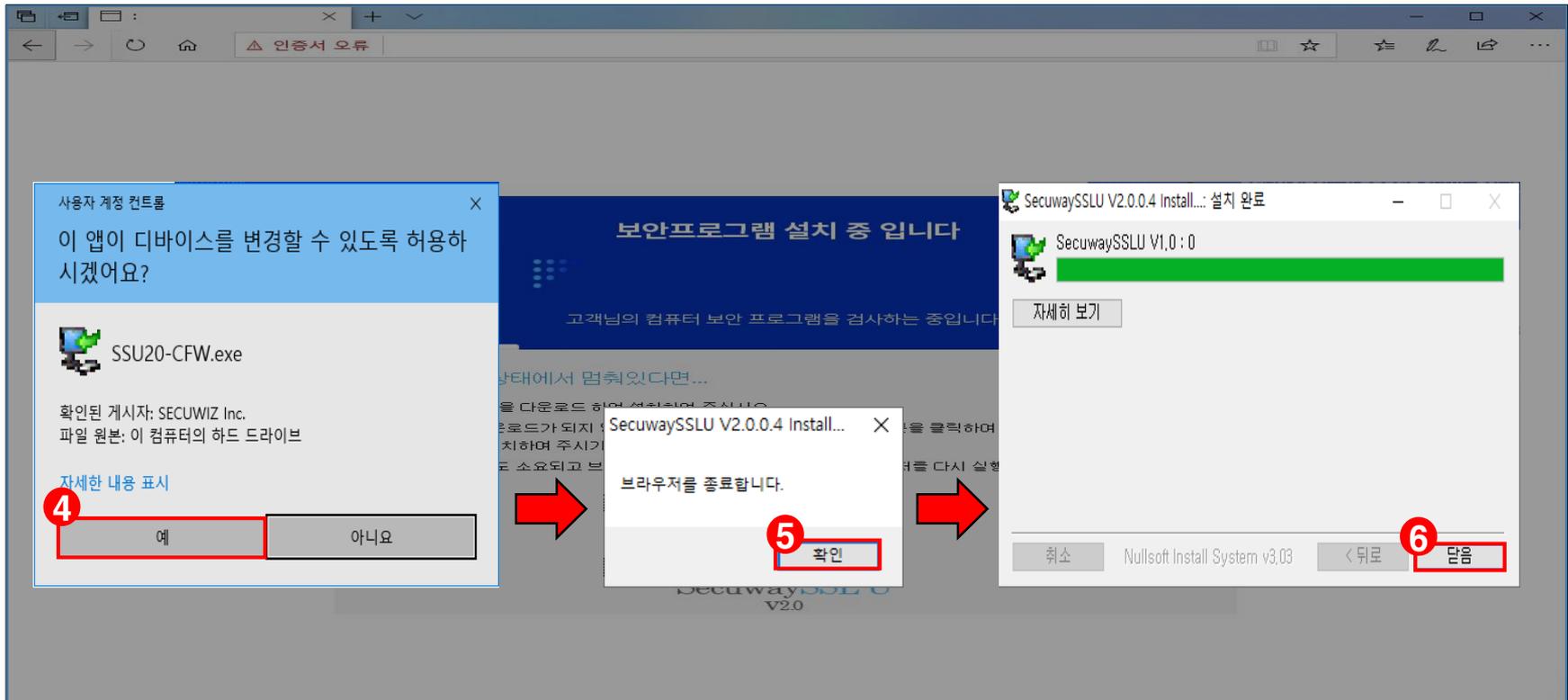
1-1-5 Edge #2

3. 브라우저 하단에 보안프로그램 설치가 생성되고 "실행" 을 클릭합니다.



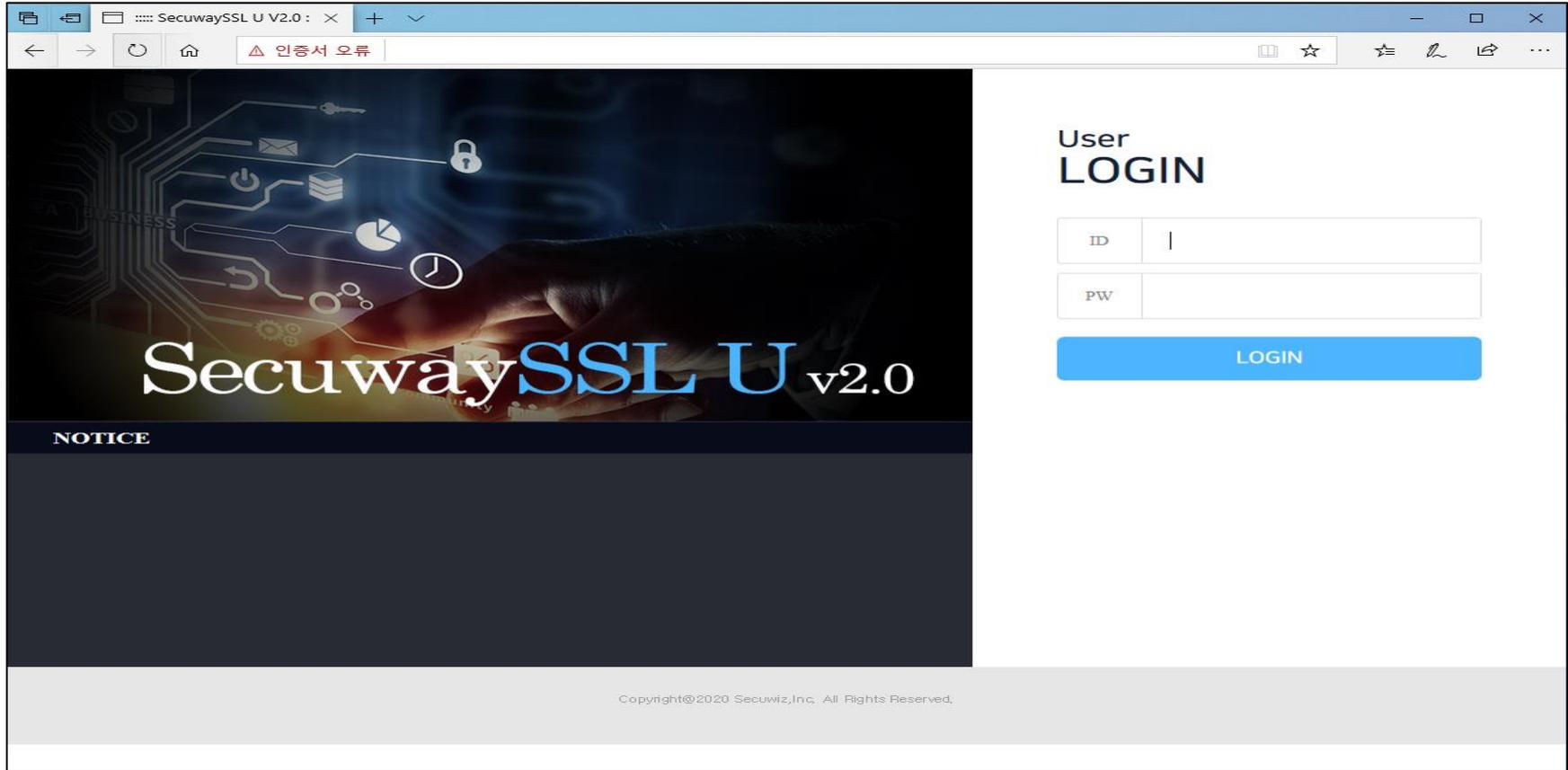
1-1-5 Edge #3

- 4. SecuwaySSL U Client 프로그램 설치를 위한 보안 경고 메시지가 나타나면 “예” 버튼을 클릭하여 프로그램 설치를 진행합니다.
- 5. 브라우저를 종료하는 메시지가 생성되고 “확인” 을 클릭합니다.
- 6. 설치가 완료되면 “다음” 를 클릭합니다.



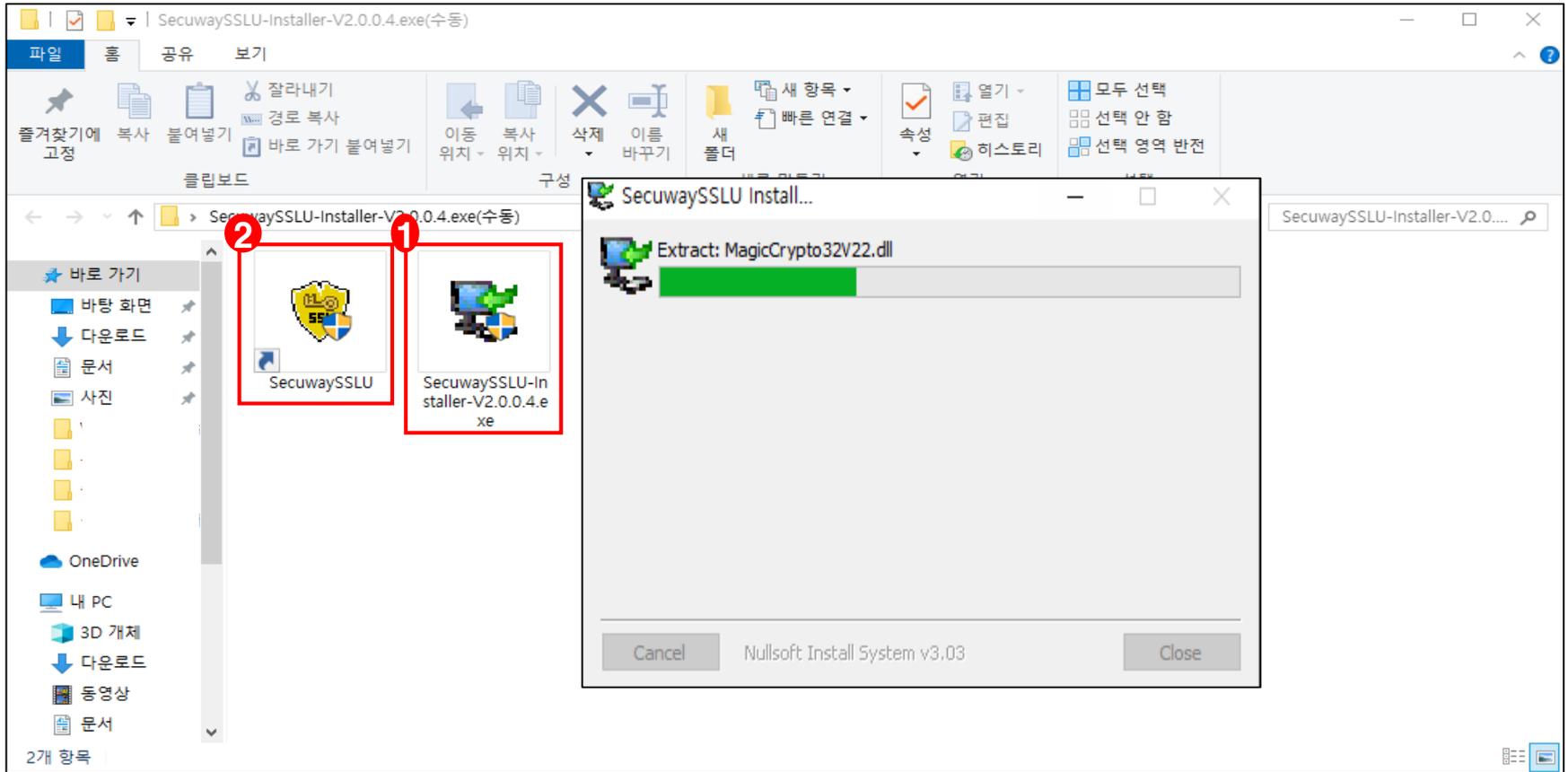
1-1-5 Edge #4

7. SecuwaySSL U Client 설치가 완료되면 로그인 페이지로 접속이 가능합니다.



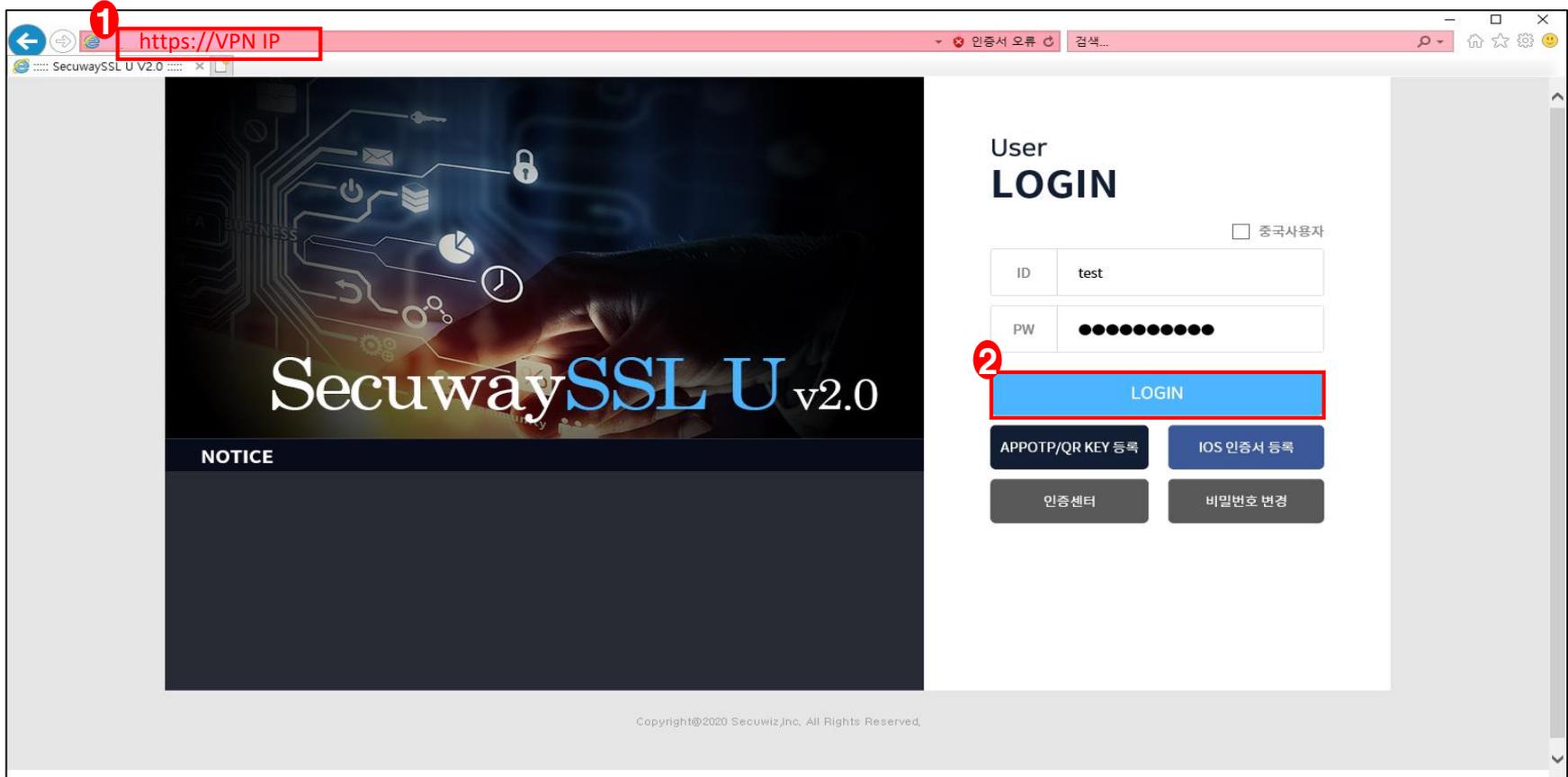
1-2-1 CS 프로그램

1. CS 프로그램을 더블 클릭하여 프로그램을 실행합니다. 설치 창이 생성되고 설치가 진행됩니다.
2. 설치가 완료되면 SecuwawySSLU 아이콘이 생기며 클라이언트 설치가 완료됩니다.



1-3-1 ID/PW 브라우저 접속 #1

1. 인터넷 브라우저의 주소 창에 VPN IP 주소 또는 URL을 입력합니다.
2. 사용자 계정 정보를 입력하고 "**LOGIN**" 을 클릭합니다.



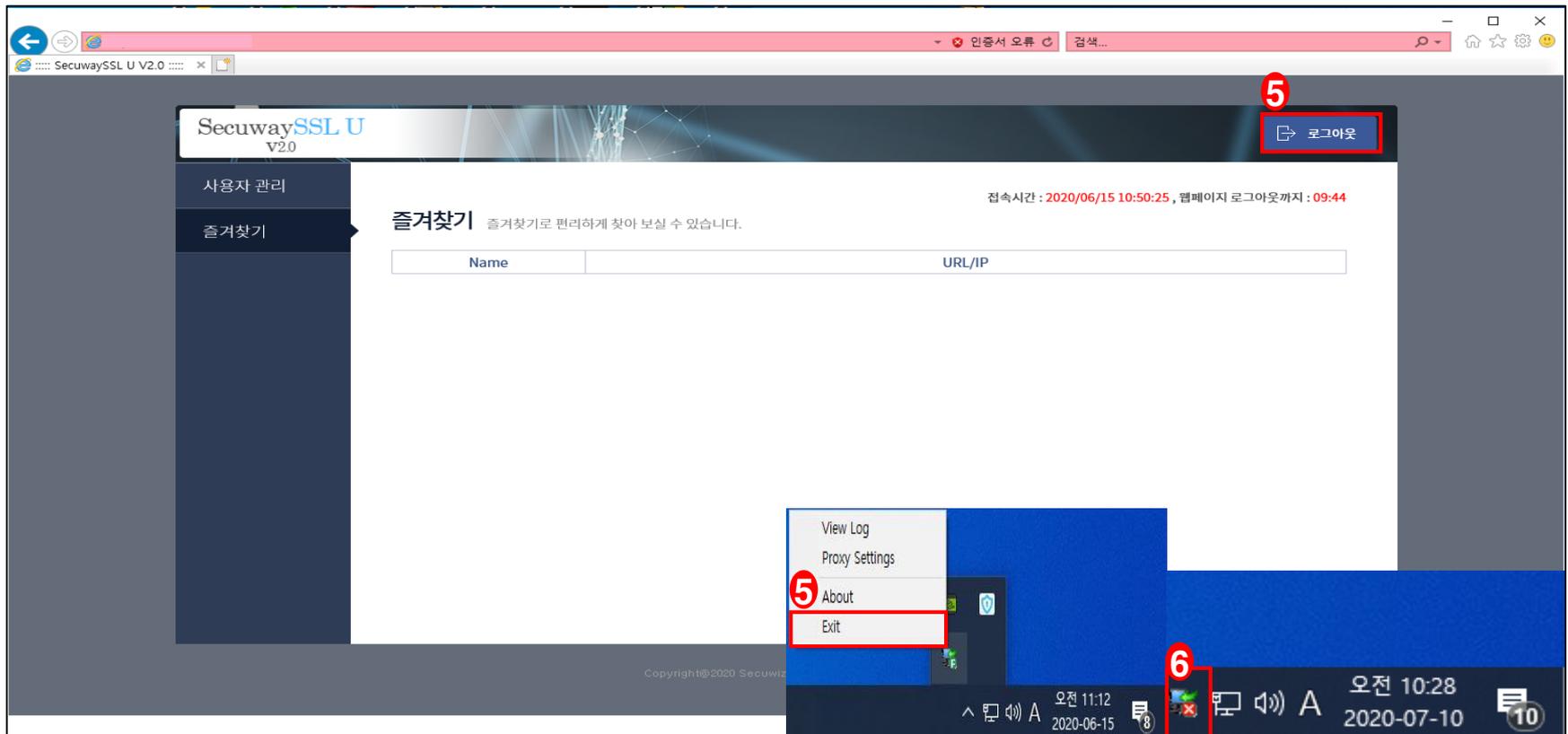
1-3-1 ID/PW 브라우저 접속 #2

- 3. 로그인하면 아래 사진과 같이 오른쪽 아래 트레이 아이콘이 생성되며 노란색에서 파란색으로 아이콘 이미지가 변경되면서 VPN에 접속됩니다.
- 4. VPN에 접속되면 아래 사진과 같은 페이지로 이동하게 되고 트레이 아이콘 표시에 마우스를 옮기게 되면 할당 받은 가상IP 확인이 가능합니다.



1-3-1 ID/PW 브라우저 접속 #3

- 5. 접속을 종료하려면 로그인한 페이지에서 "**로그아웃**"을 클릭하거나 트레이 아이콘에서 "**Exit**"를 클릭하여 접속을 종료합니다.
- 6. 종료하면 트레이 아이콘이 X표시로 변하고 없어지며 VPN 접속이 종료됩니다.



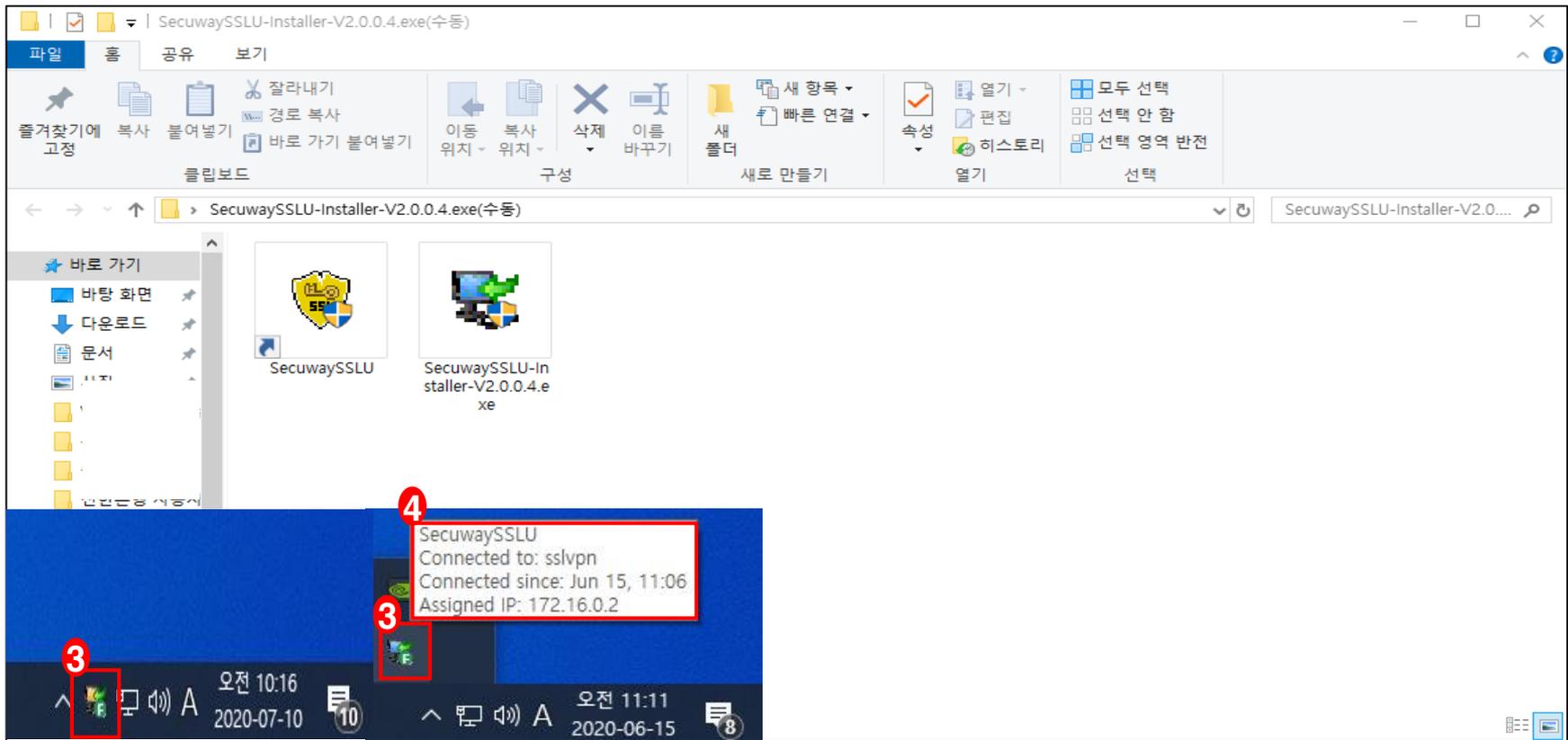
1-3-2 ID/PW CS 접속 #1

1. CS프로그램을 실행합니다.
2. 접속 주소에 https://서버IP 입력하고 "확인"을 클릭합니다.
3. ID/PW 입력하는 창으로 변경이 되면 ID/PW 입력 후 "확인"을 클릭합니다.



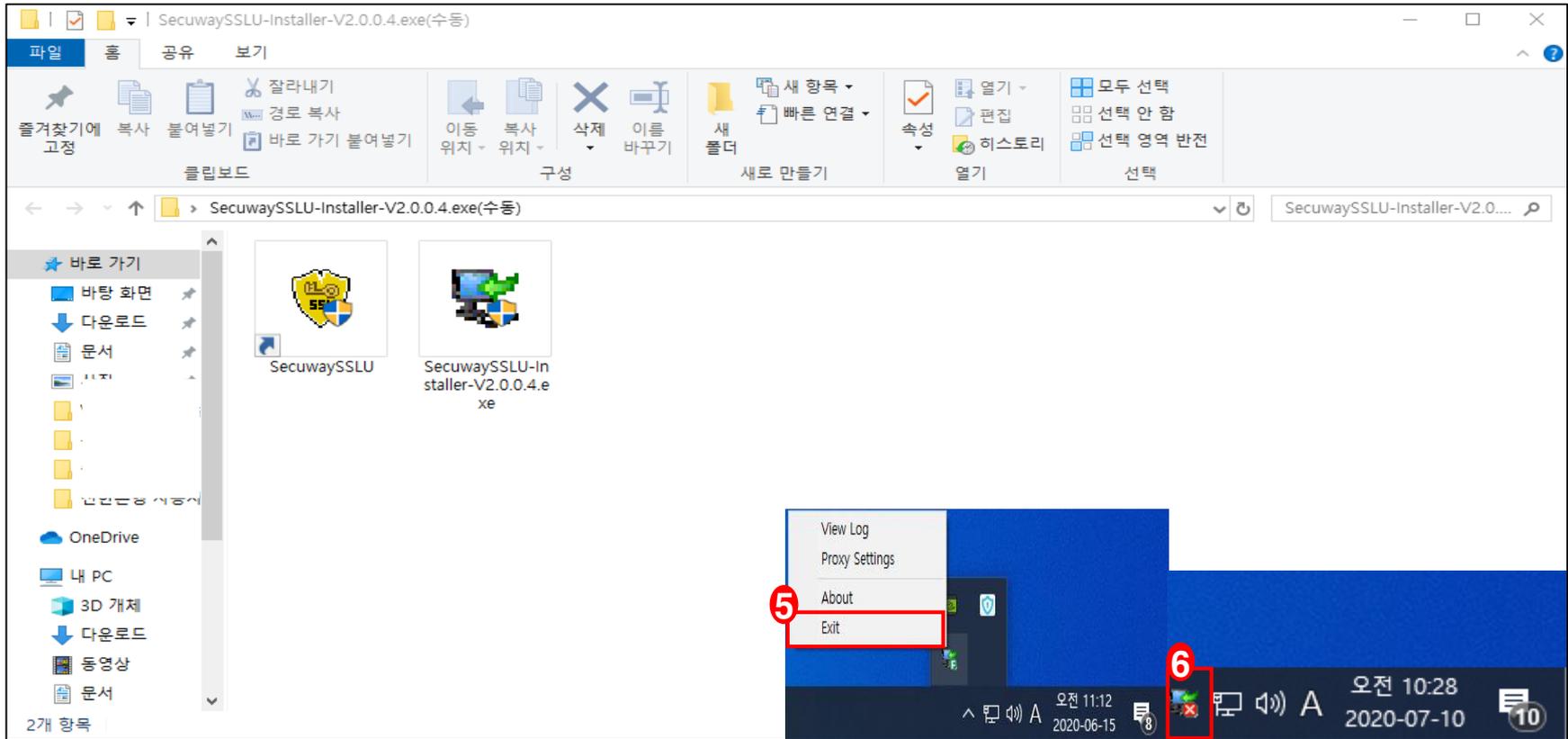
1-3-2 ID/PW CS 접속 #2

- 3. 로그인하면 아래 사진과 같이 오른쪽 아래 트레이 아이콘이 생성되며 노란색에서 파란색으로 아이콘 이미지가 변경되면서 VPN에 접속됩니다.
- 4. VPN에 접속되면 아래 사진과 같은 페이지로 이동하게 되고 트레이 아이콘 표시에 마우스를 옮기게 되면 할당 받은 가상IP 확인이 가능합니다.



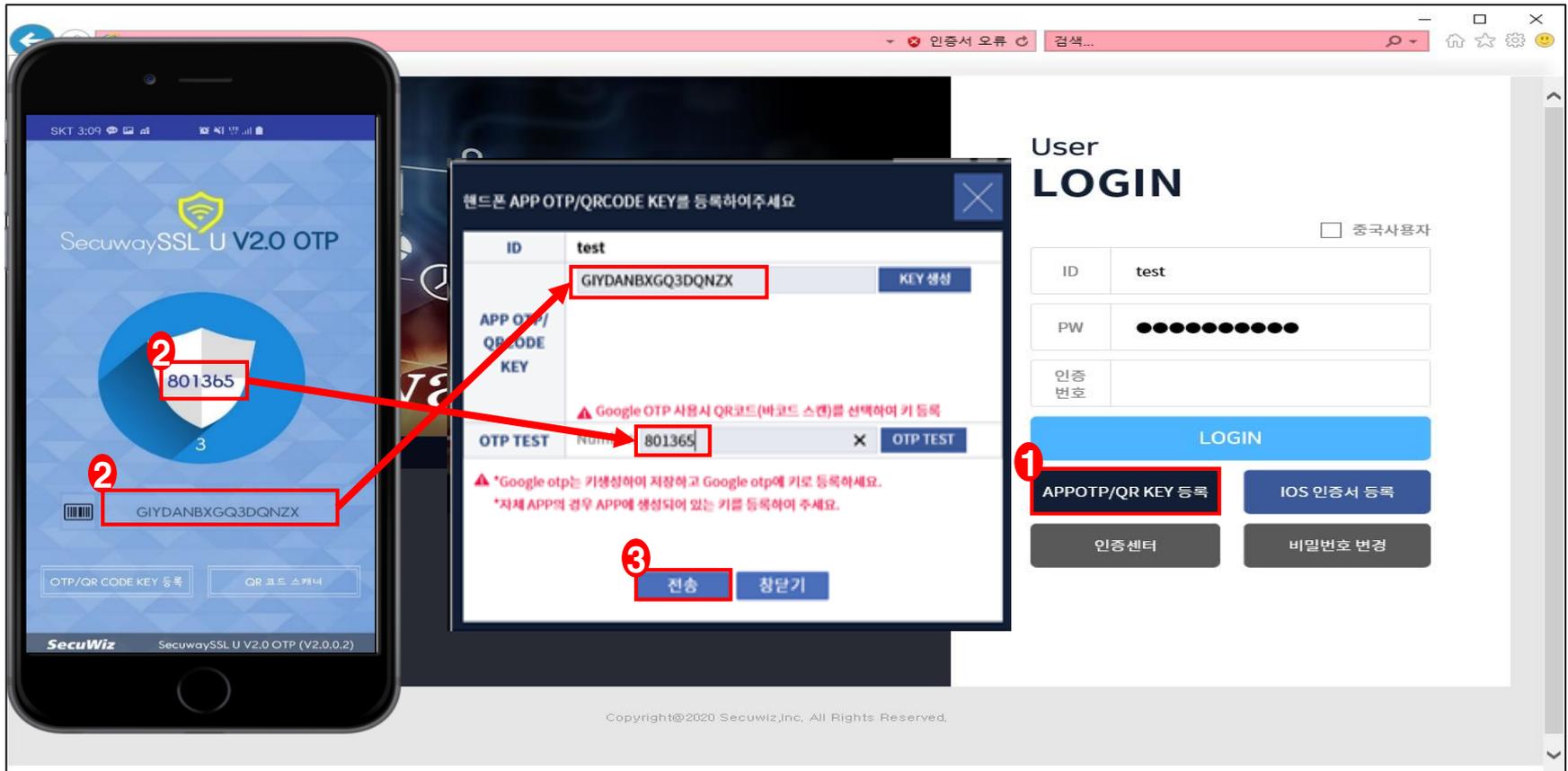
1-3-2 ID/PW CS 접속 #3

- 5. 트레이 아이콘에서 "Exit"를 클릭하여 접속을 종료합니다.
- 6. 종료하면 트레이 아이콘이 'X' 표시로 변하고 없어지며 VPN 접속이 종료됩니다.



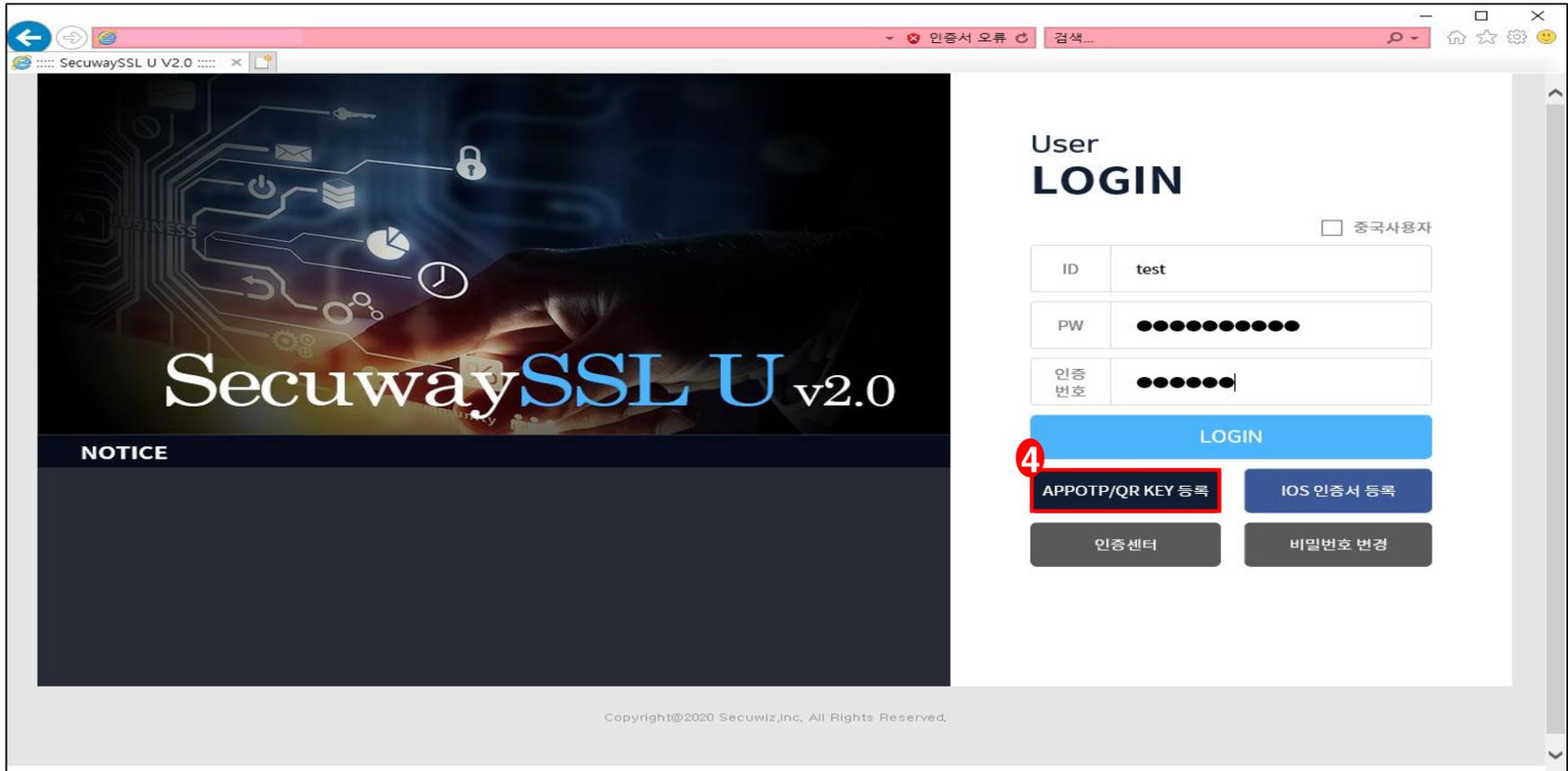
1-3-3 ID/PW APP-OTP 접속 #1

1. 로그인페이지에서 ID/PW를 입력하고 “**APPOTP/QR KEY 등록**” 을 클릭합니다.
2. SecuwaySSL U V2.0 OTP 앱을 실행시켜 OTP Key와 인증번호를 등록 창에 동일하게 입력합니다.
3. “**전송**” 을 클릭하면 OTP Key가 등록됩니다.



1-3-3 ID/PW APP-OTP 접속 #2

4. ID/PW/OTP 입력 후 “**LOGIN**” 을 클릭하여 로그인합니다.



1-3-3 ID/PW APP-OTP 접속 #3

1. OTP Key와 인증번호는 동일하게 입력합니다.
2. 기타검증에는 이름, 핸드폰번호, EMAIL, 주민번호를 같이 입력하여 등록합니다.
3. 각각 등록 할 때 서버에 등록되어 있는 이름, 핸드폰번호, EMAIL, 주민번호를 입력합니다.
4. 기타 검증은 등록할 때만 사용되며 다음 로그인 시 검증하지 않습니다.

핸드폰 APP OTP/QRCODE KEY를 등록해주세요

ID	test
APP OTP/QRCODE KEY	<input type="text"/> KEY 생성
▲ Google OTP 사용시 QR코드(바코드 스캔)를 선택하여 키 등록	
OTP TEST	Number: <input type="text"/> OTP TEST
기타검증	이름: <input type="text"/> *"없이"
▲ *Google otp는 키생성하여 저장하고 Google otp에 키로 등록하세요. *자체 APP의 경우 APP에 생성되어 있는 키를 등록하여 주세요.	
<input type="button" value="전송"/> <input type="button" value="창닫기"/>	

[ID+PW+이름]

핸드폰 APP OTP/QRCODE KEY를 등록해주세요

ID	test
APP OTP/QRCODE KEY	<input type="text"/> KEY 생성
▲ Google OTP 사용시 QR코드(바코드 스캔)를 선택하여 키 등록	
OTP TEST	Number: <input type="text"/> OTP TEST
기타검증	핸드폰번호: <input type="text"/> *"없이"
▲ *Google otp는 키생성하여 저장하고 Google otp에 키로 등록하세요. *자체 APP의 경우 APP에 생성되어 있는 키를 등록하여 주세요.	
<input type="button" value="전송"/> <input type="button" value="창닫기"/>	

[ID+PW+핸드폰번호]

핸드폰 APP OTP/QRCODE KEY를 등록해주세요

ID	test
APP OTP/QRCODE KEY	<input type="text"/> KEY 생성
▲ Google OTP 사용시 QR코드(바코드 스캔)를 선택하여 키 등록	
OTP TEST	Number: <input type="text"/> OTP TEST
기타검증	EMAIL: <input type="text"/> *"없이"
▲ *Google otp는 키생성하여 저장하고 Google otp에 키로 등록하세요. *자체 APP의 경우 APP에 생성되어 있는 키를 등록하여 주세요.	
<input type="button" value="전송"/> <input type="button" value="창닫기"/>	

[ID+PW+EMAIL]

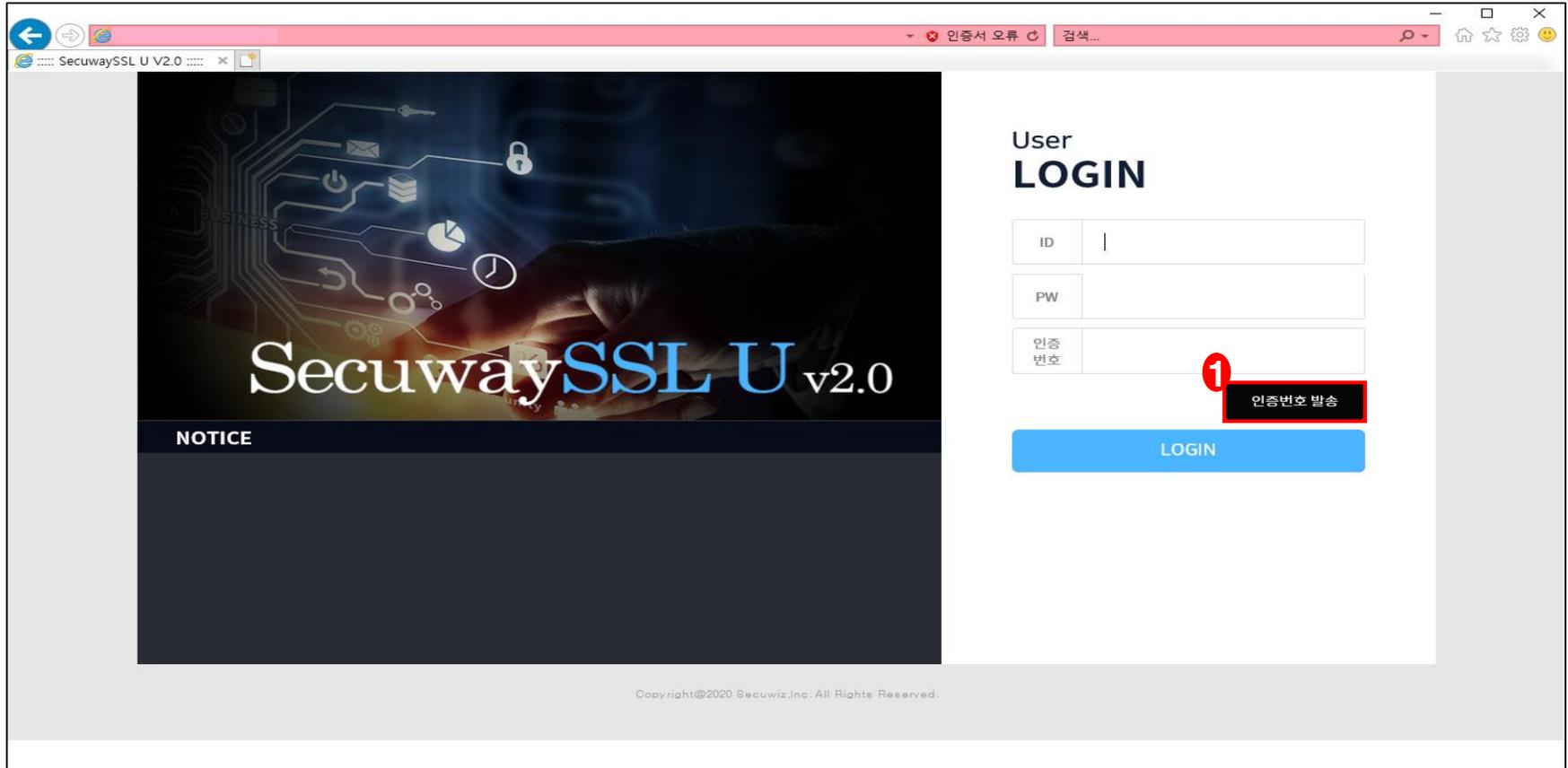
핸드폰 APP OTP/QRCODE KEY를 등록해주세요

ID	test
APP OTP/QRCODE KEY	<input type="text"/> KEY 생성
▲ Google OTP 사용시 QR코드(바코드 스캔)를 선택하여 키 등록	
OTP TEST	Number: <input type="text"/> OTP TEST
기타검증	주민번호: <input type="text"/> *"없이"
▲ *Google otp는 키생성하여 저장하고 Google otp에 키로 등록하세요. *자체 APP의 경우 APP에 생성되어 있는 키를 등록하여 주세요.	
<input type="button" value="전송"/> <input type="button" value="창닫기"/>	

[ID+PW+주민번호]

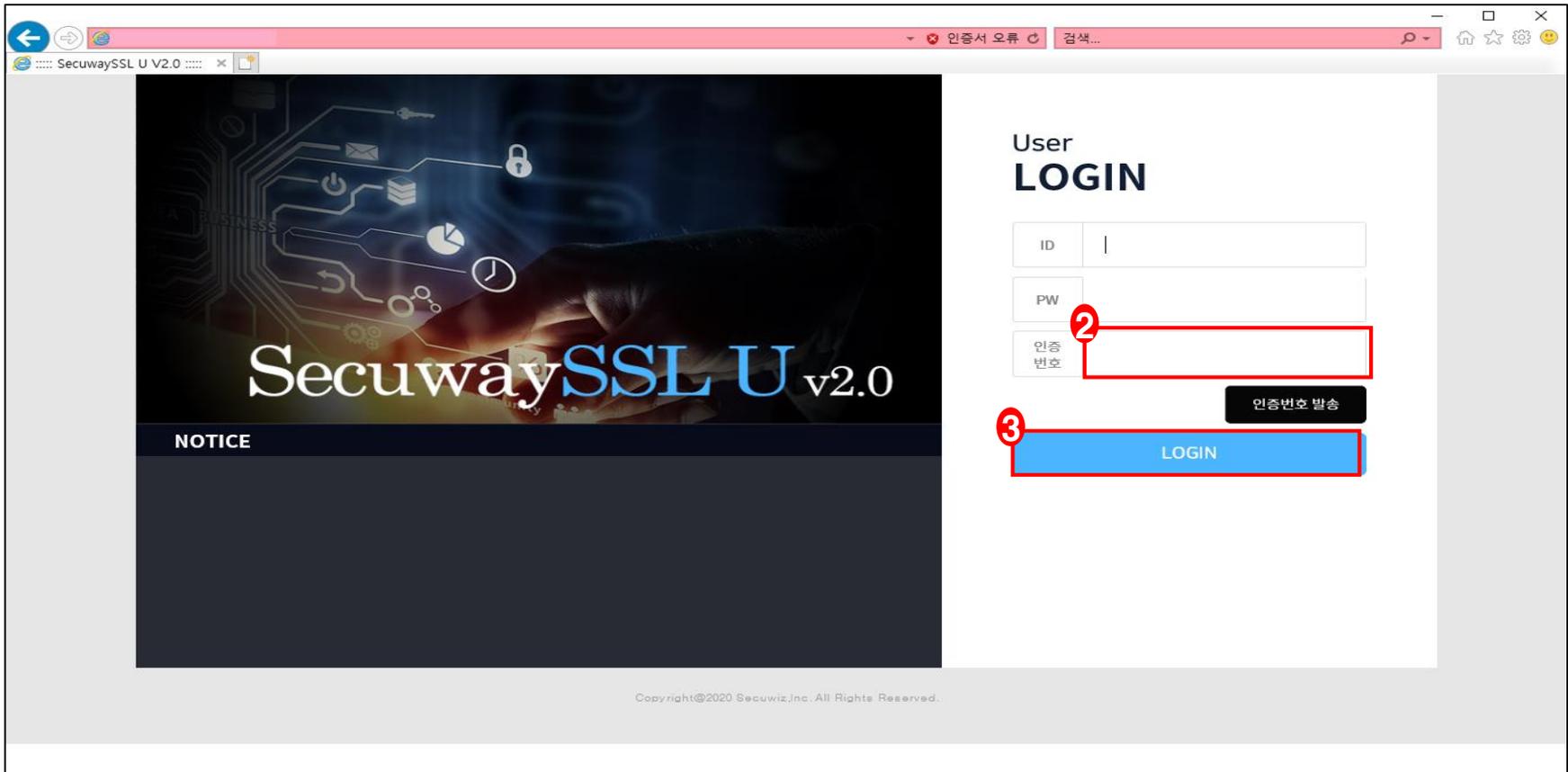
1-3-4 ID/PW SMS-OTP 접속 #1

1. ID/PW 입력 후 "인증번호 발송" 을 클릭하면 VPN에 등록되어 있는 핸드폰번호로 인증번호를 메시지로 전송합니다.



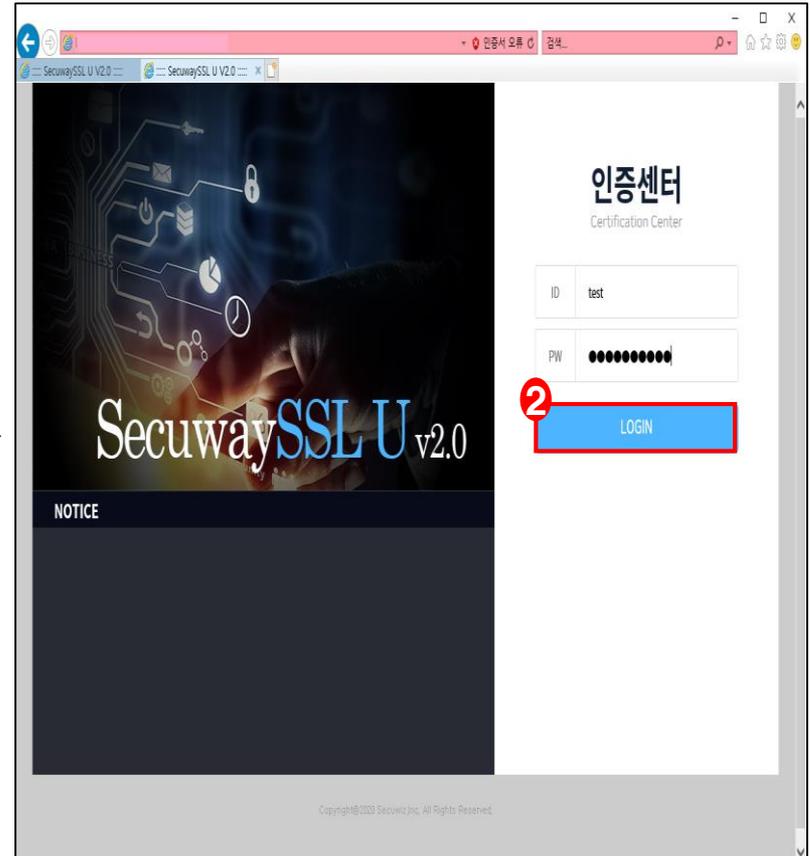
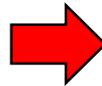
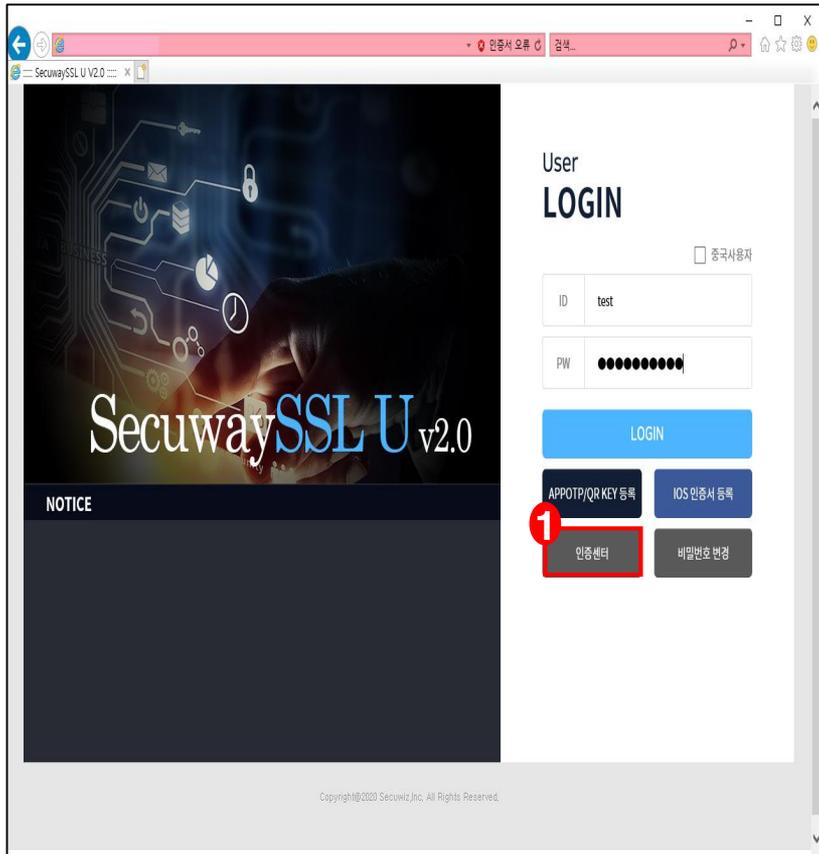
1-3-4 ID/PW SMS-OTP 접속 #2

- 2. "인증번호가 발송되었습니다." 라는 안내 메시지 창이 생성되고 사용자는 인증번호 7자리를 문자 메시지로 수신 받으며 인증번호는 3분 이내 입력 해야 됩니다.
- 3. 인증번호 입력란이 생성되면 인증번호를 입력한 후 "**LOGIN**" 버튼을 클릭하여 VPN에 접속됩니다.



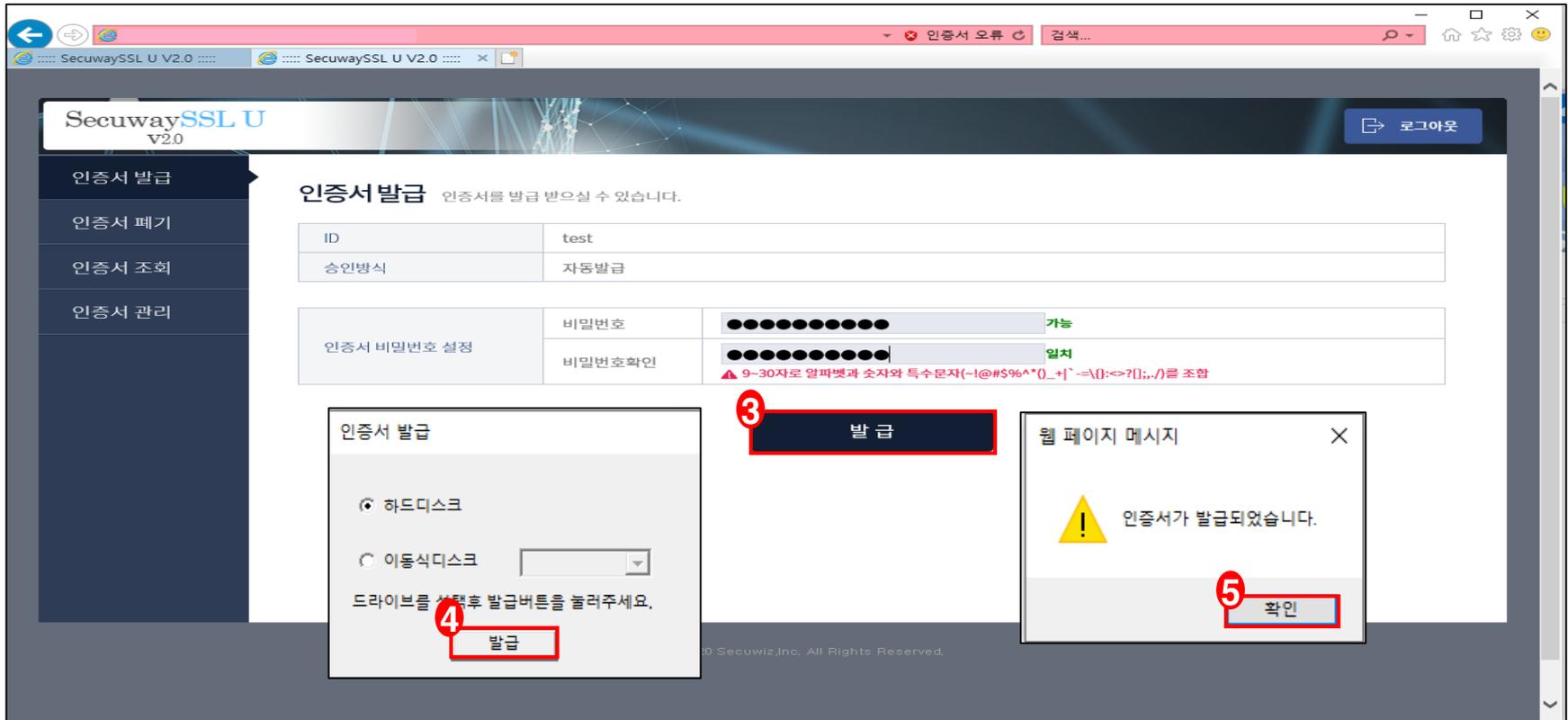
1-3-5 ID/PW 사설 인증서 접속 #1

1. 사용자 로그인페이지에서 인증 센터를 클릭합니다.
2. 계정정보를 입력하고 "**LOGIN**" 을 클릭합니다.



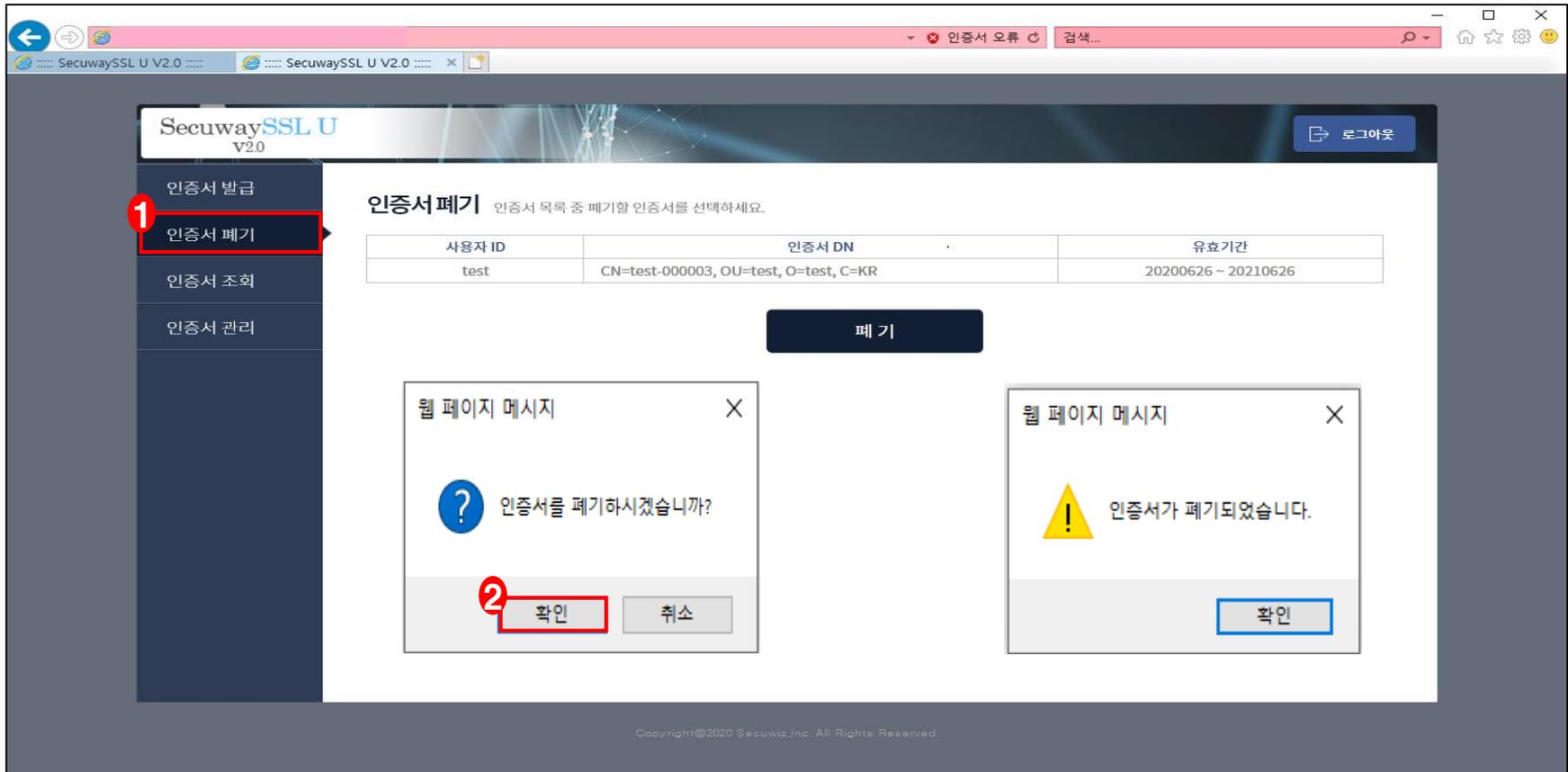
1-3-5 ID/PW 사설 인증서 접속 #2

- 3. 인증 센터에서 로그인하면 아래 사진과 같은 페이지로 접속되며 인증서 발급에서 인증서 비밀번호를 입력하고 "발급" 을 클릭합니다
- 4. 그리고 인증서 다운받을 드라이브 위치를 선택하고 "발급" 을 클릭하면 인증서가 발급됩니다.
- 5. 인증서가 발급되었고 "확인" 을 클릭합니다.



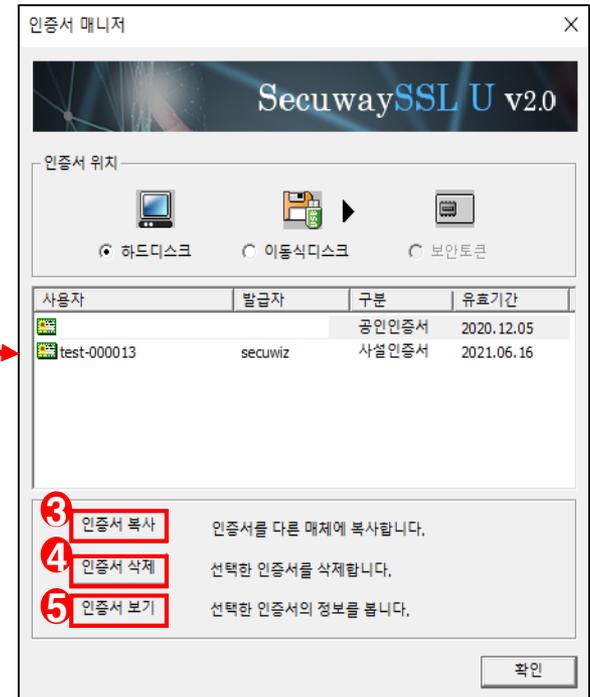
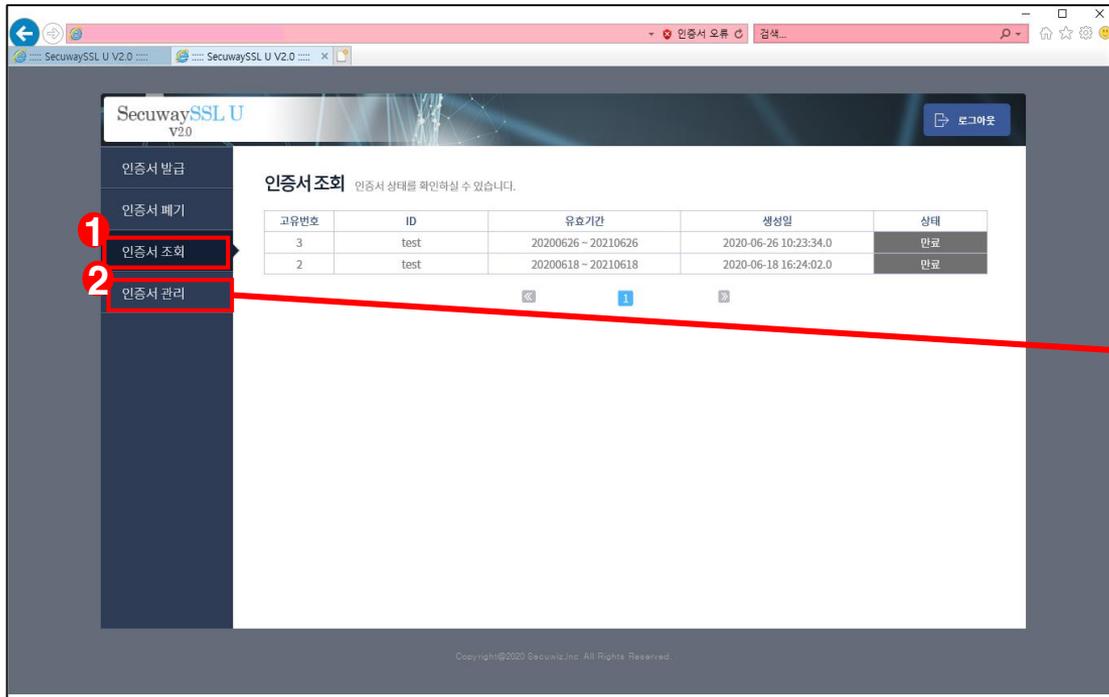
1-3-5 ID/PW 사설 인증서 접속 #3

1. “**인증서 폐기**” 버튼을 클릭하면 현재 사용중인 인증서를 볼 수 있고 폐기할 수 있습니다.
2. “**폐기**” 를 클릭하면 인증서 폐기 경고 창이 나오게 되며 “**확인**” 을 클릭하면 폐기가 됩니다.
3. 사용중인 인증서를 폐기할 수 있으며 한번 폐기된 인증서는 복구되지 않습니다.



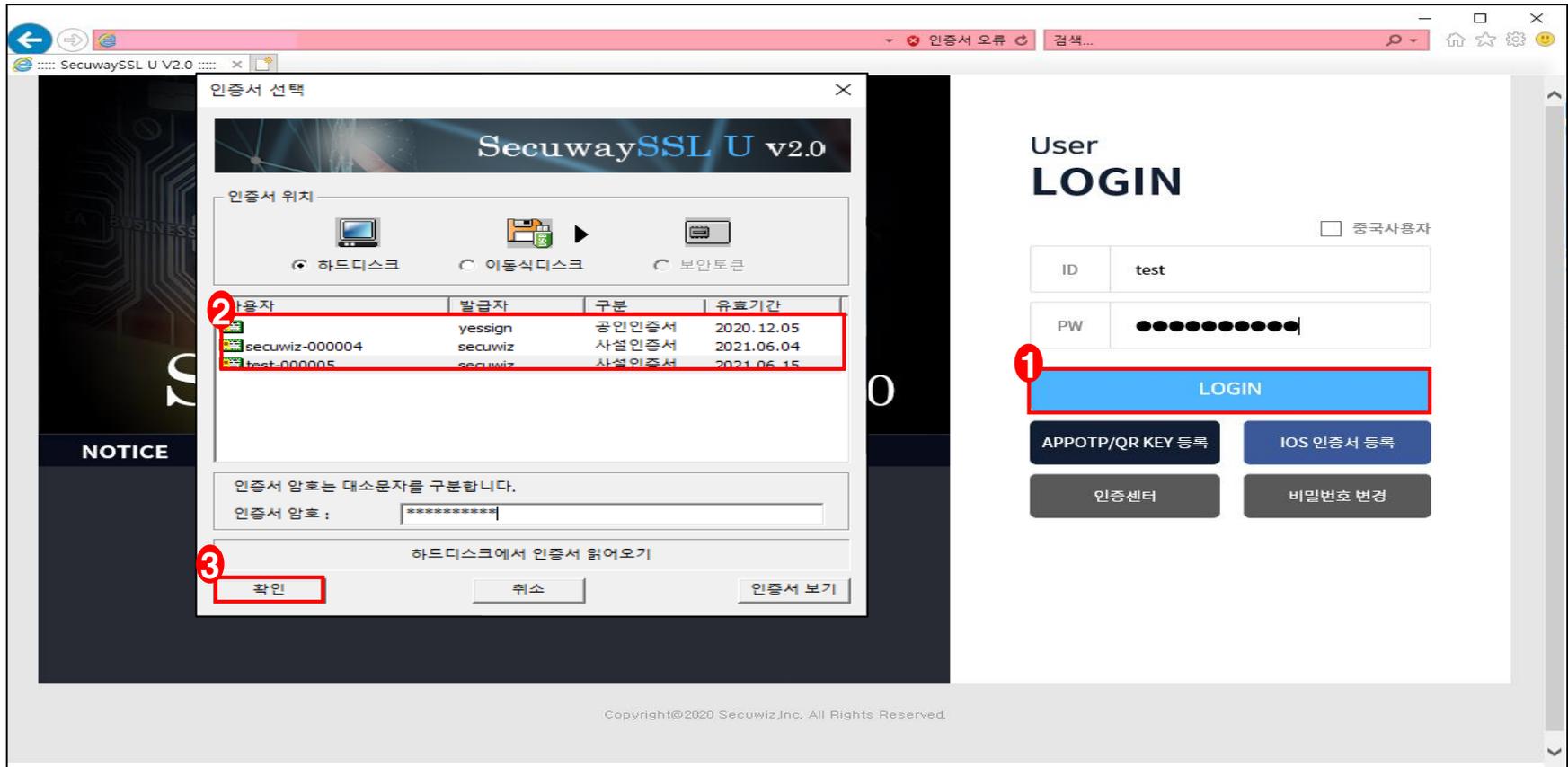
1-3-5 ID/PW 사설 인증서 접속 #4

1. 인증서 조회 페이지는 발급받은 인증서를 조회할 수 있습니다.
2. 인증서 관리를 클릭하면 오른쪽 사진과 같이 인증서 매니저 창이 생성됩니다.
3. 인증서 복사: 인증서를 다른 매체에 복사합니다.(ex 하드디스크->이동식디스크)
4. 인증서 삭제: 선택한 인증서를 삭제합니다.
5. 인증서 보기: 선택한 인증서의 정보를 확인합니다.



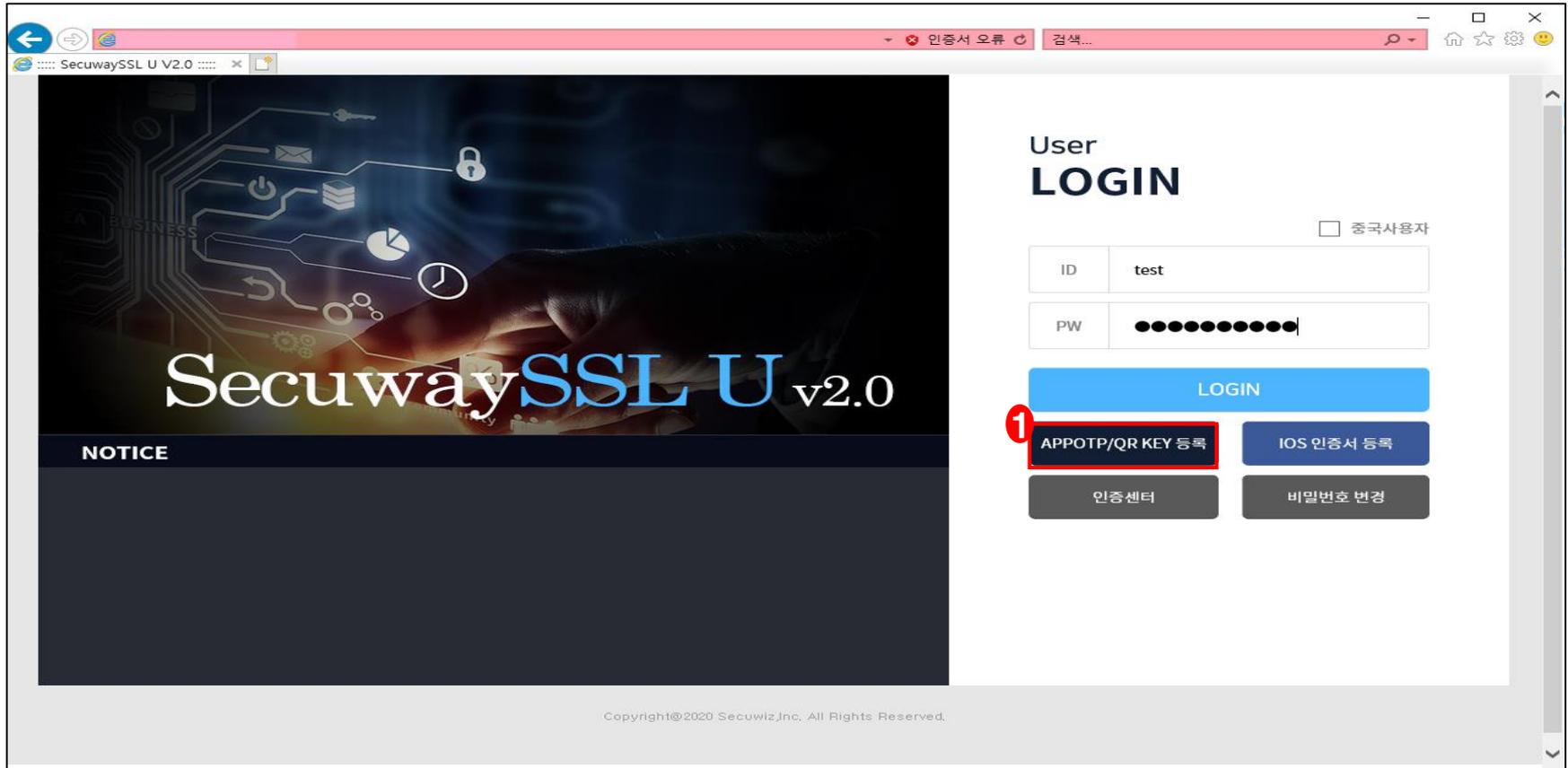
1-3-5 ID/PW 공인, 사설 인증서 접속 #5

1. 로그인 페이지에서 ID/PW를 입력하고 "**LOGIN**" 을 클릭합니다.
2. 인증서 선택이 생성되고 (공인/사설) 중 인증서를 선택합니다.
3. 인증서 암호를 입력하고 "**확인**" 을 클릭하여 로그인합니다.



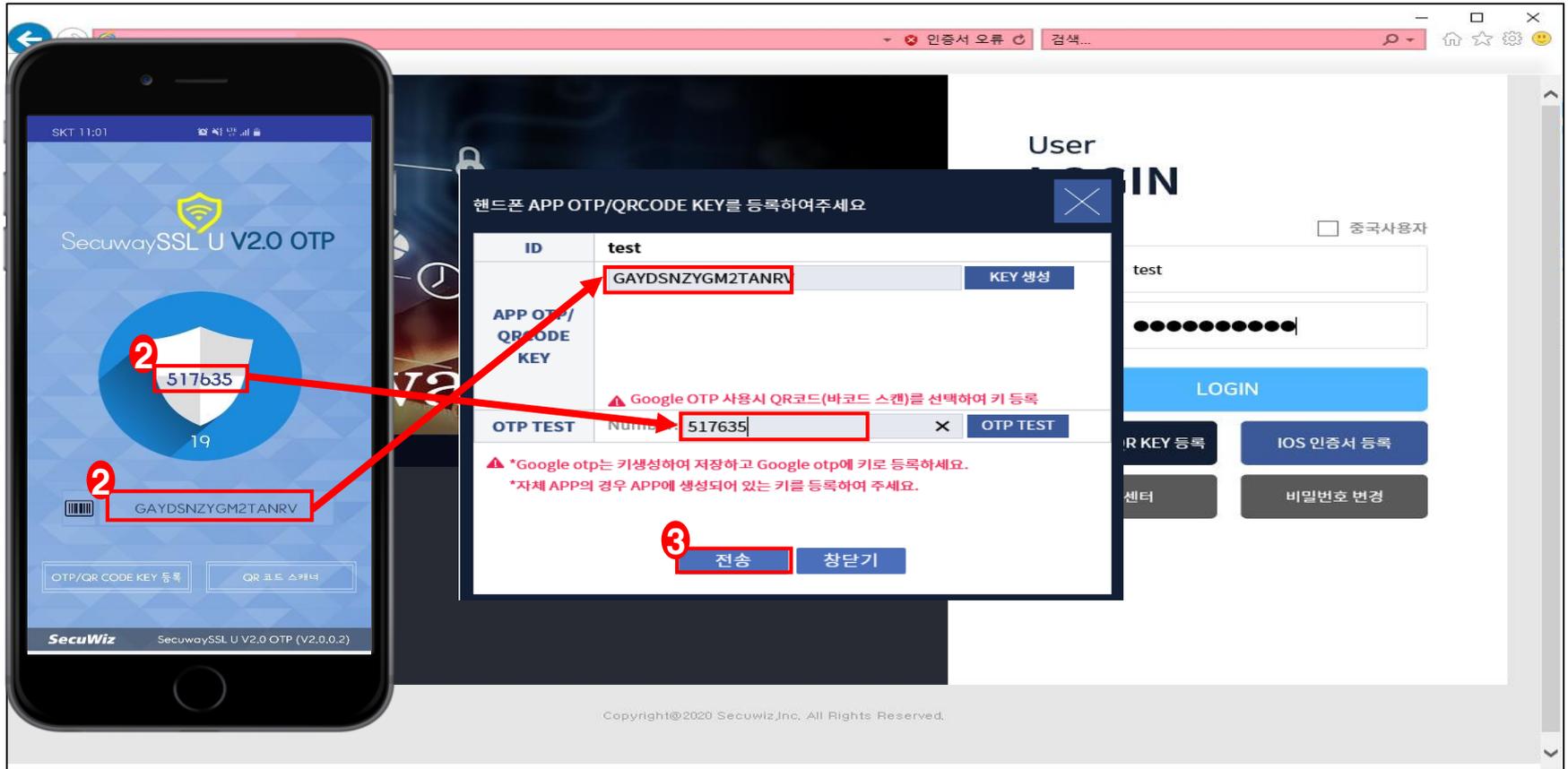
1-3-6 ID/PW QR CODE 접속 #1

1. 로그인페이지에서 ID/PW를 입력하고 "APPOTP/QR KEY" 등록을 클릭합니다.



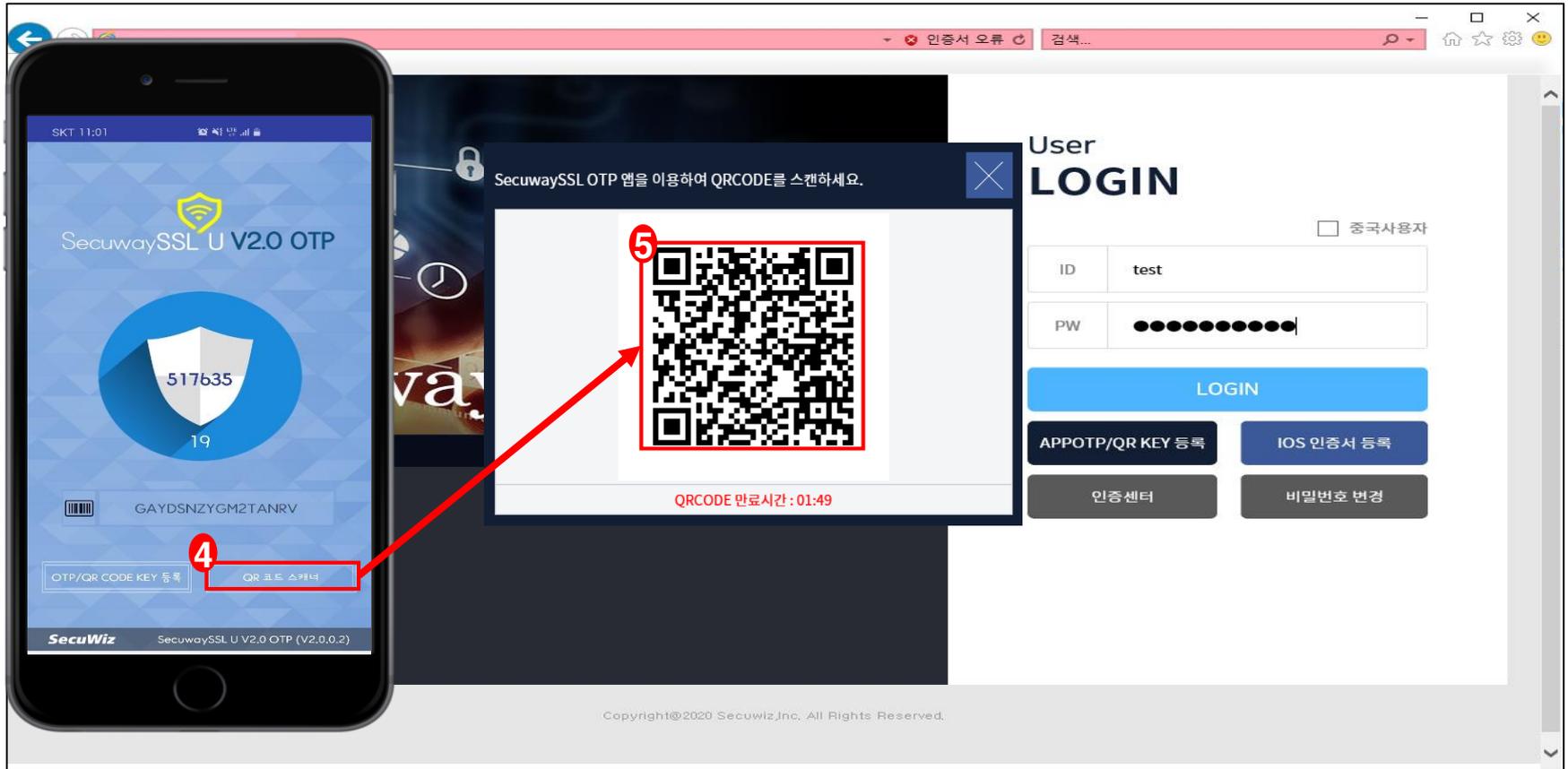
1-3-6 ID/PW QR CODE 접속 #2

- 2. 핸드폰 SecuwaySSL U V2.0 OTP 앱을 실행시켜 사진과 같이 OTP Key와 인증번호를 입력합니다.
- 3. 입력을 완료했다면 "전송" 버튼을 클릭합니다.



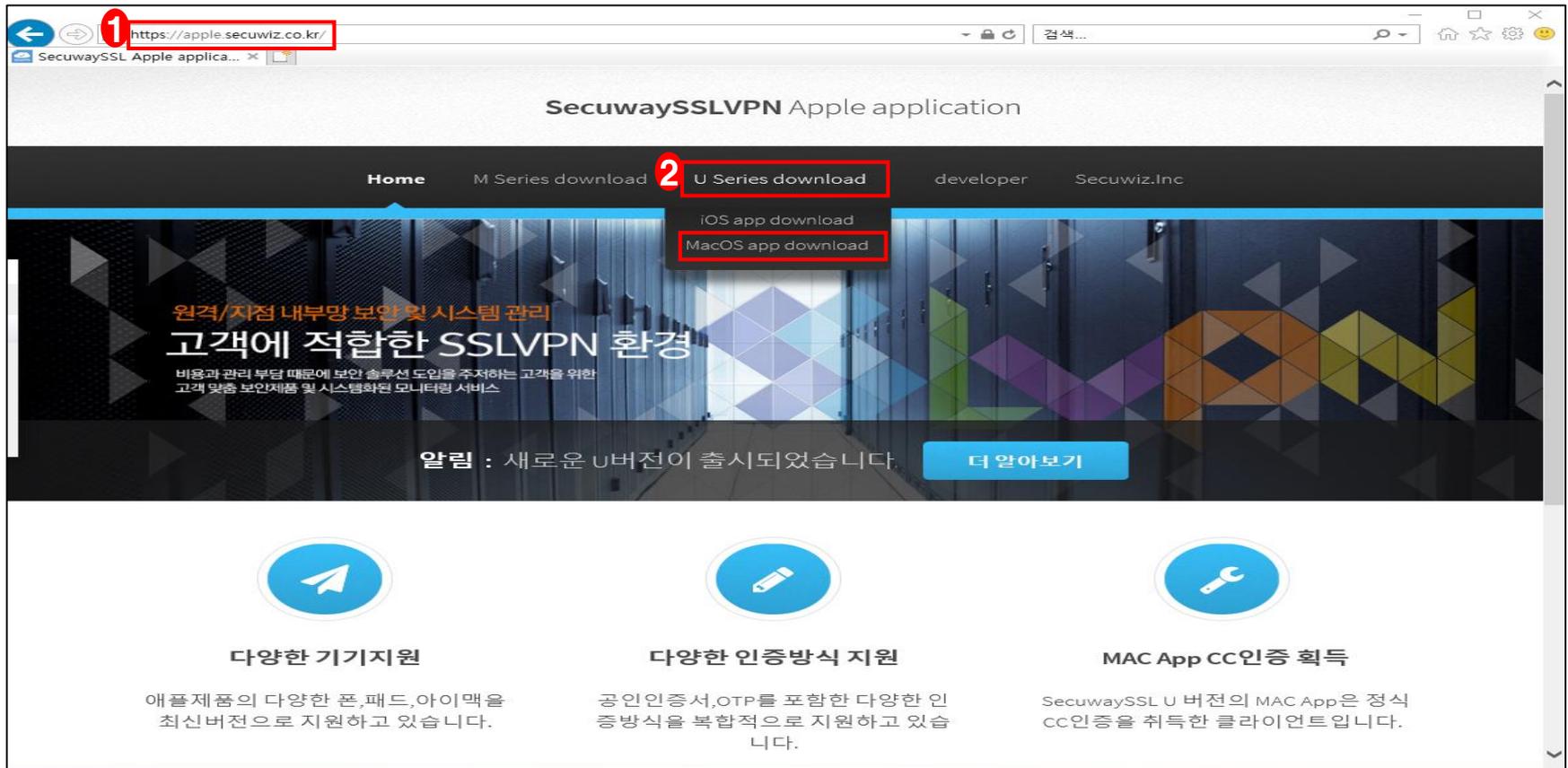
1-3-6 ID/PW QR CODE 접속 #3

- 4. "**LOGIN**" 버튼을 클릭하면 QR CODE가 생성됩니다. OTP 앱에서 QR 코드 스캐너를 누릅니다.
- 5. "**QR 코드스캐너**" 를 클릭하면 카메라로 전환되고 화면 QR CODE에 맞추게 되면 인증이 되면서 로그인 됩니다.



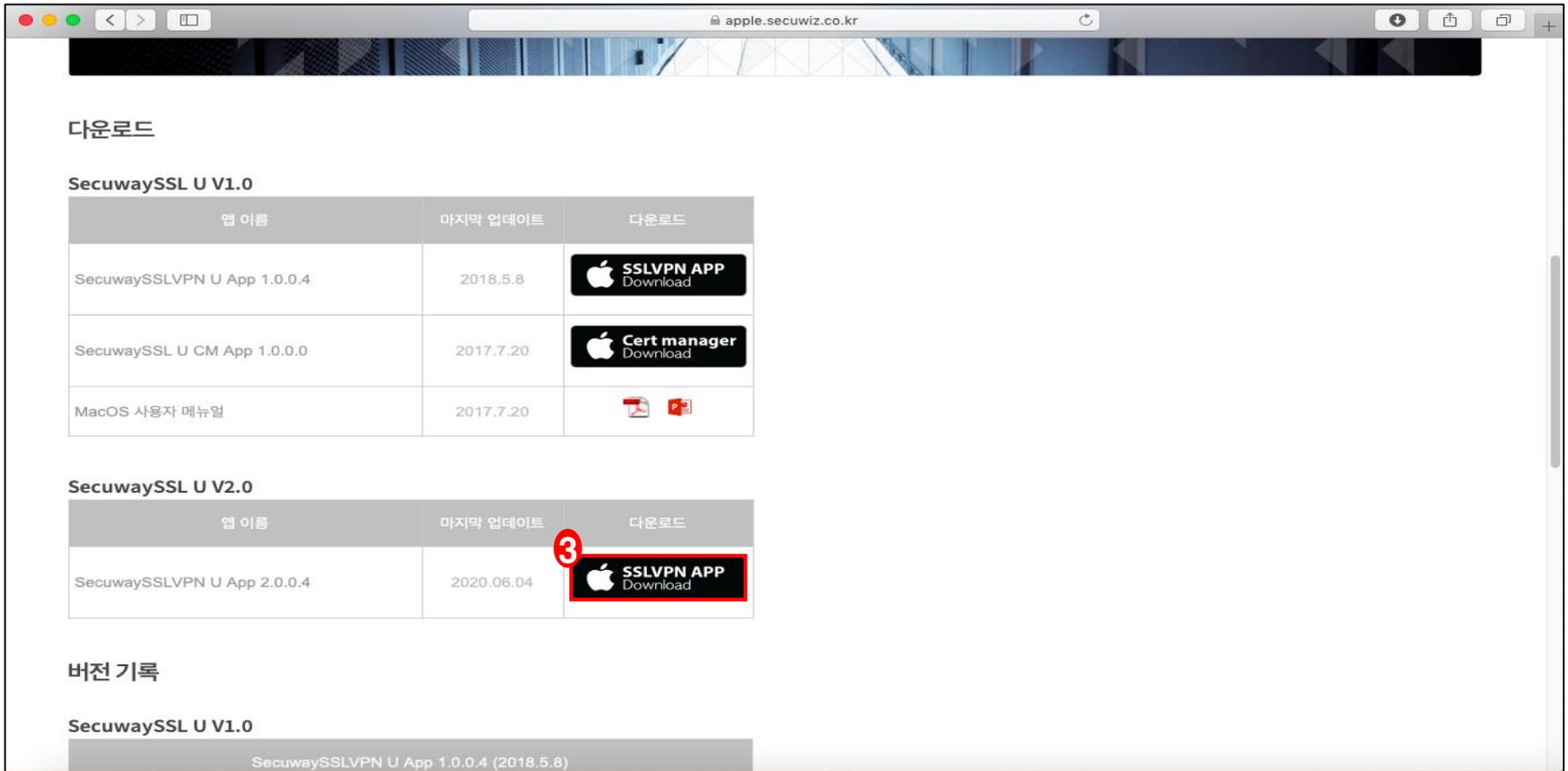
2-1-1 Mac #1

1. 주소 창에서 <https://apple.secuwiz.co.kr>을 입력합니다.
2. U Series Download – MacOS app download 메뉴를 클릭합니다.



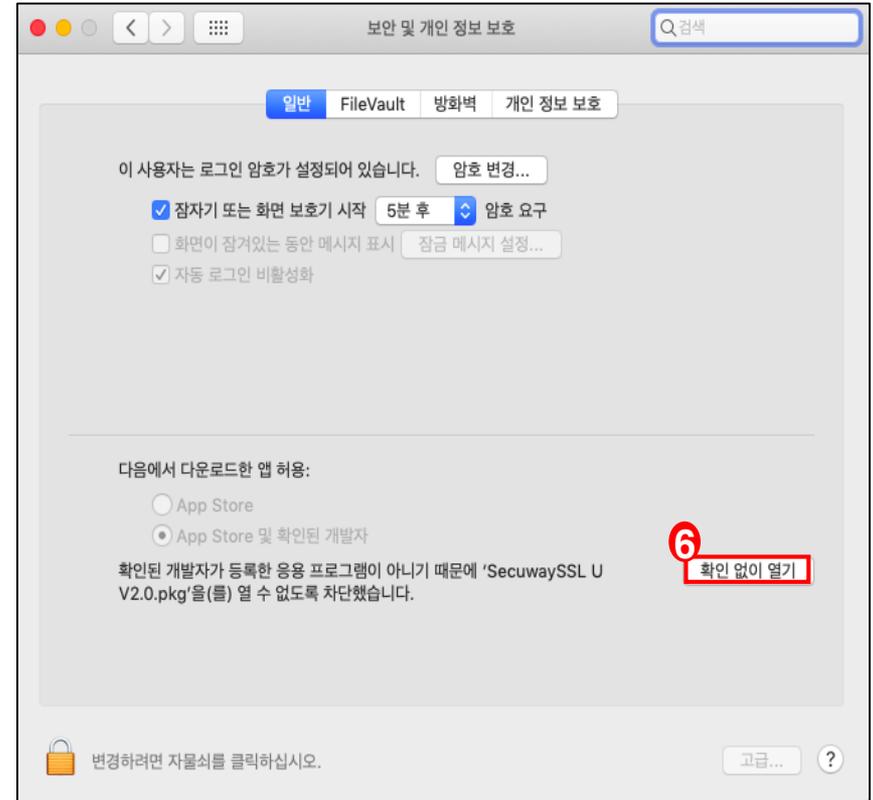
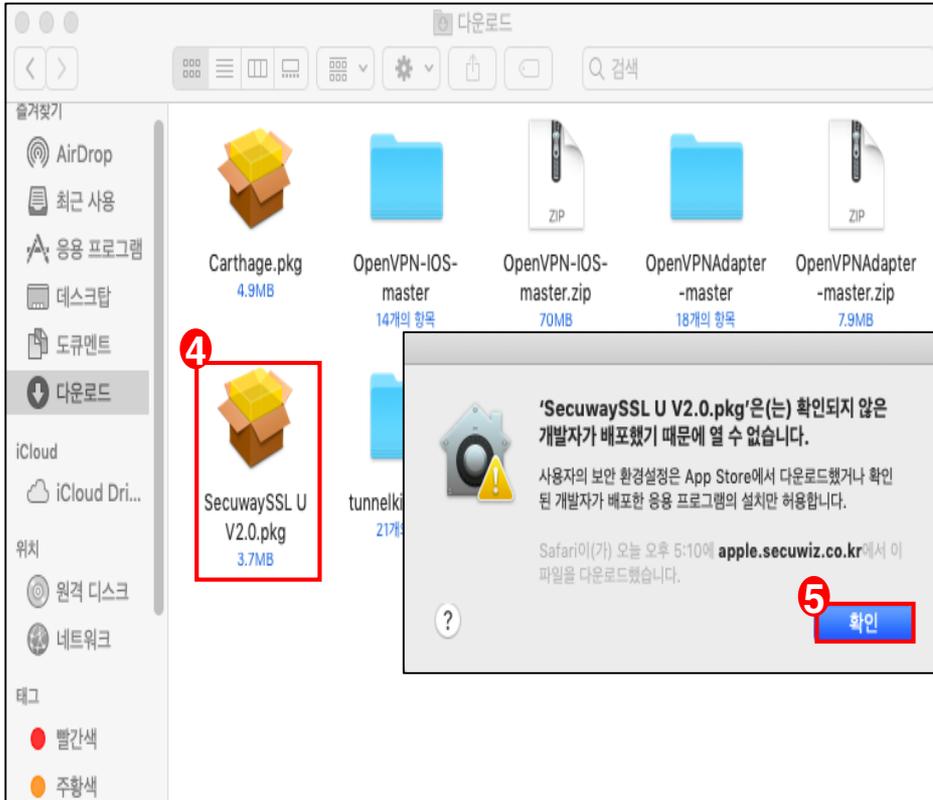
2-1-1 Mac #2

3. SecuwaySSL U APP 2.0.0.4 – SSLVPN APP Download 를 클릭하여 다운받습니다.



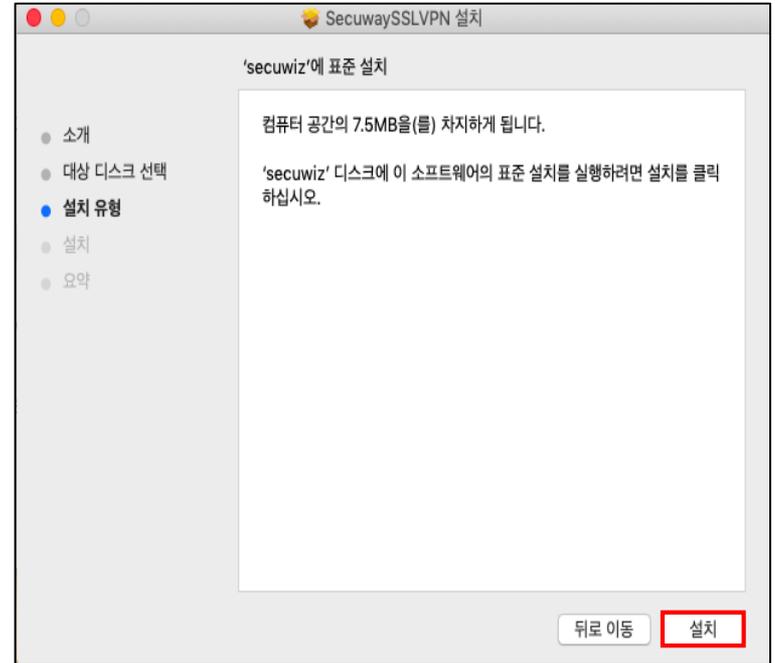
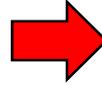
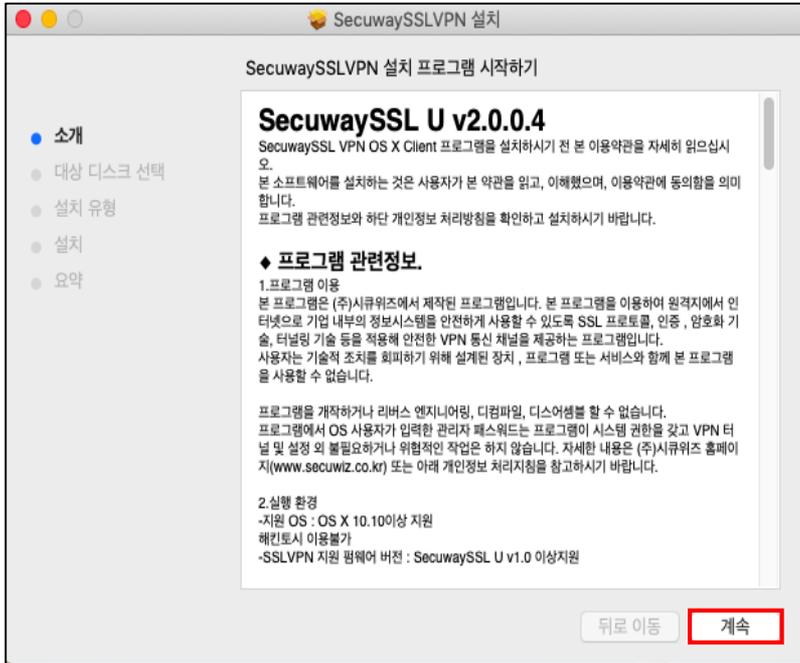
2-1-1 Mac #3

- 4. 다운받은 경로에 위치에서 SecuwaySSL U V2.0.pkg 파일을 실행합니다.
- 5. 'SecuwaySSL U V2.0.pkg'은(는) 확인되지 않은 개발자가 배포했기 때문에 열 수 없습니다. 라는 메시지 창이 생성됩니다.
- 6. 시스템 환경설정-보안 및 개인 정보 보호 에서 "확인 없이 열기" 를 클릭합니다.



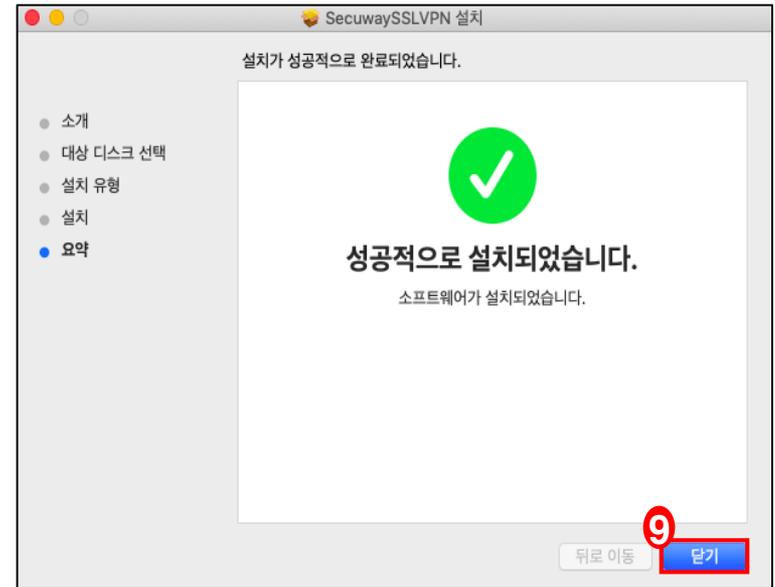
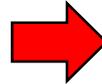
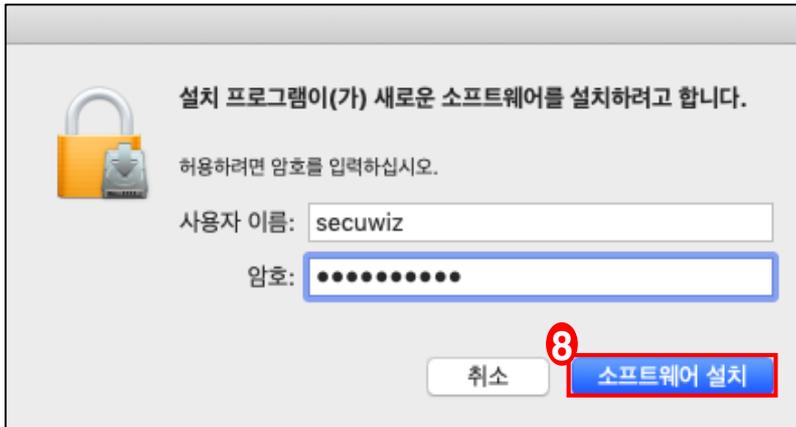
2-1-1 Mac #4

7. 아래 사진과 같이 계속 버튼을 클릭하여 순차적으로 설치를 진행합니다.



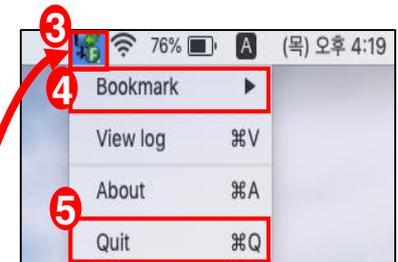
2-1-1 Mac #5

8. Mac의 사용자 이름과 암호를 입력하고 "소프트웨어 설치" 를 클릭합니다.
9. 설치가 완료되면 "닫기" 를 클릭합니다.



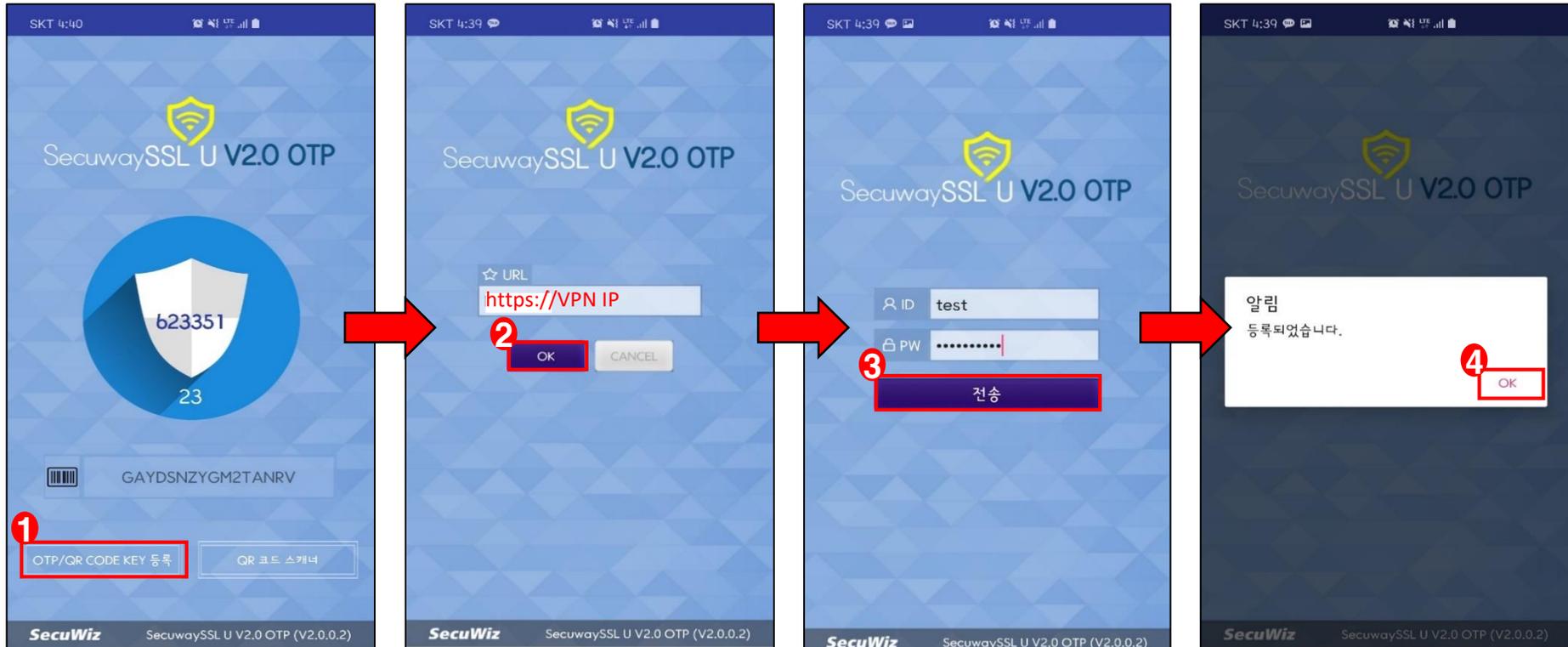
2-2-1 ID/PW 접속

1. 앱이 실행되면 주소 창에 `https://VPN접속IP` 를 입력하고 “**접속**” 을 클릭합니다.
2. 사용자 ID/PW/OS 비밀번호를 입력 후 “**로그인**” 버튼을 클릭합니다.
3. VPN에 정상 접속되면 화면 오른쪽 상단에 트레이 아이콘이 생깁니다.
4. Bookmark 를 클릭하면 서버에 등록된 즐겨찾기 리스트를 볼 수 있습니다.
5. Quit를 통해 VPN접속을 해제할 수 있습니다.



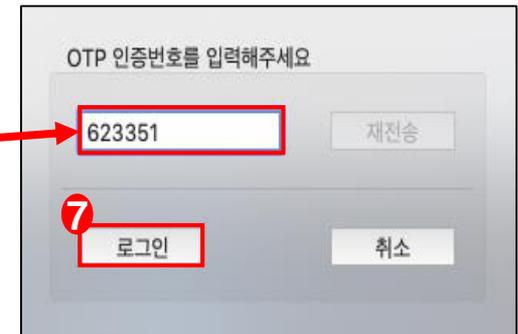
2-2-2 ID/PW APP-OTP 접속 #1

1. OTP 앱을 실행시켜서 "OTP/QR CODE KEY 등록" 을 클릭합니다.
2. VPN 접속IP를 입력하고 "OK" 를 클릭합니다.
3. 계정정보를 입력하고 "전송" 을 클릭합니다.
4. 등록이 완료되고 "OK" 를 클릭합니다.



2-2-2 ID/PW APP-OTP 접속 #2

5. SecuwaySSL U V2.0 Client를 실행하고 계정 정보를 입력하고 "**OTP**" 를 클릭합니다.
6. OTP 인증번호 입력 창에서 OTP 인증번호를 입력합니다.
7. "**로그인**" 을 클릭합니다.



2-2-3 ID/PW 인증서 접속 #1

1. 주소 창에서 <https://apple.secuwiz.co.kr> 입력합니다.
2. U Series Download- MacOs app download 메뉴를 클릭합니다.

1. 주소 창에서 <https://apple.secuwiz.co.kr> 입력합니다.

2. U Series Download- MacOs app download 메뉴를 클릭합니다.

SecuwaySSLVPN Apple application

Home M Series download U Series download developer Secuwiz.Inc

iOS app download
MacOS app download

원격/지점 내부망 보안 및 시스템 관리
고객에 적합한 SSLVPN 환경
비용과 관리 부담 때문에 보안 솔루션 도입을 주저하는 고객을 위한
고객 맞춤 보안제품 및 시스템화된 모니터링 서비스

알림 : 새로운 U버전이 출시되었습니다. [더 알아보기](#)

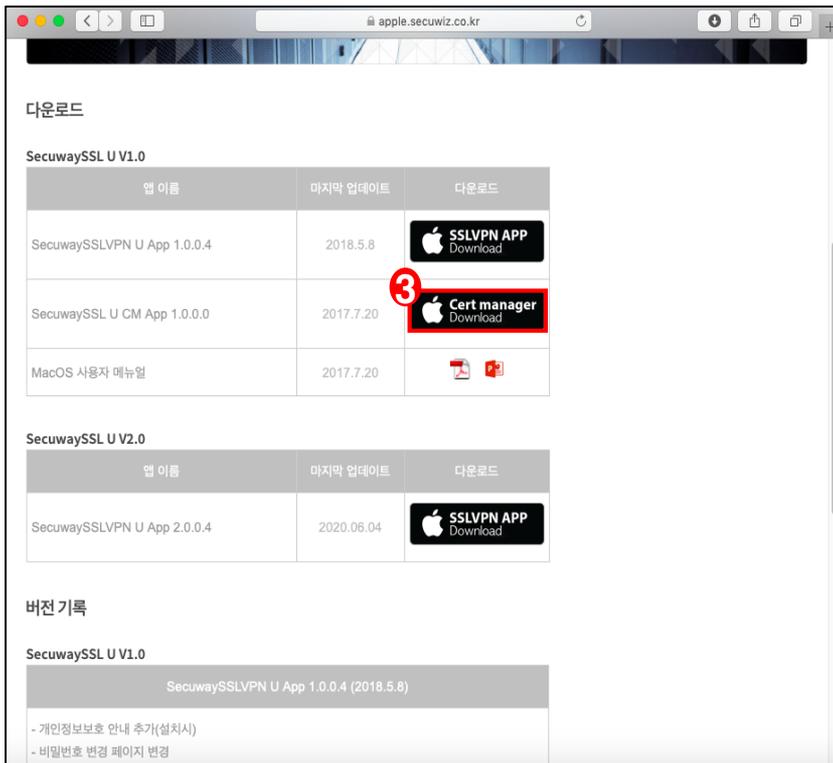
다양한 기기지원
애플제품의 다양한 폰,패드,아이맥을 최신버전으로 지원하고 있습니다.

다양한 인증방식 지원
공인인증서,OTP를 포함한 다양한 인증방식을 복합적으로 지원하고 있습니다.

MAC App CC인증 획득
SecuwaySSL U 버전의 MAC App은 정식 CC인증을 취득한 클라이언트입니다.

2-2-3 ID/PW 인증서 접속 #2

3. SecuwaySSL U CM App 1.0.0.0 – Cert manager 클릭하여 다운로드합니다.
4. 받은 파일을 설치하고 SecuwaySSL CM을 실행하면 SecuwayPKI 페이지가 생성됩니다.
5. VPN 접속 주소와 계정 정보를 입력하여 “로그인” 클릭합니다.



앱 이름	마지막 업데이트	다운로드
SecuwaySSLVPN U App 1.0.0.4	2018.5.8	
SecuwaySSL U CM App 1.0.0.0	2017.7.20	
MacOS 사용자 매뉴얼	2017.7.20	

버전 기록

SecuwaySSL U V1.0

SecuwaySSLVPN U App 1.0.0.4 (2018.5.8)
--

- 개인정보보호 안내 추가(설치시)
- 비밀번호 변경 페이지 변경



URL: 주소저장

인증센터
Secuway PKI

Beyond the Security

로그인

Copyright©2016 SecuWiz, Inc. All Rights Reserved

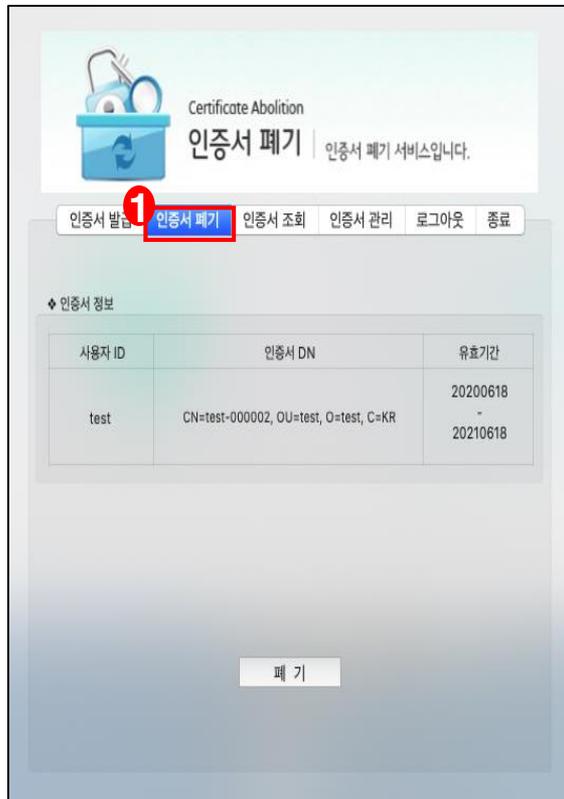
2-2-3 ID/PW 인증서 접속 #3

6. 인증서 발급 창이 생성되고 인증서 암호를 입력하고 “**발급**” 을 클릭합니다.
7. 인증서를 저장할 수 있고 저장 받을 디스크를 선택합니다.
8. 인증서 다운로드가 완료되고 “**확인**” 을 클릭합니다.



2-2-3 ID/PW 인증서 접속 #4

1. “인증서 폐기” 클릭하면 사용중인 인증서를 폐기 할 수 있습니다. 한번 폐기된 인증서는 복구되지 않습니다.
2. “인증서 조회” 클릭하면 발급 받은 인증서를 조회할 수 있습니다.
3. “인증서 관리” 클릭하면 다운 받은 인증서를 복사/삭제/보기를 할 수 있습니다.



[인증서 폐기]



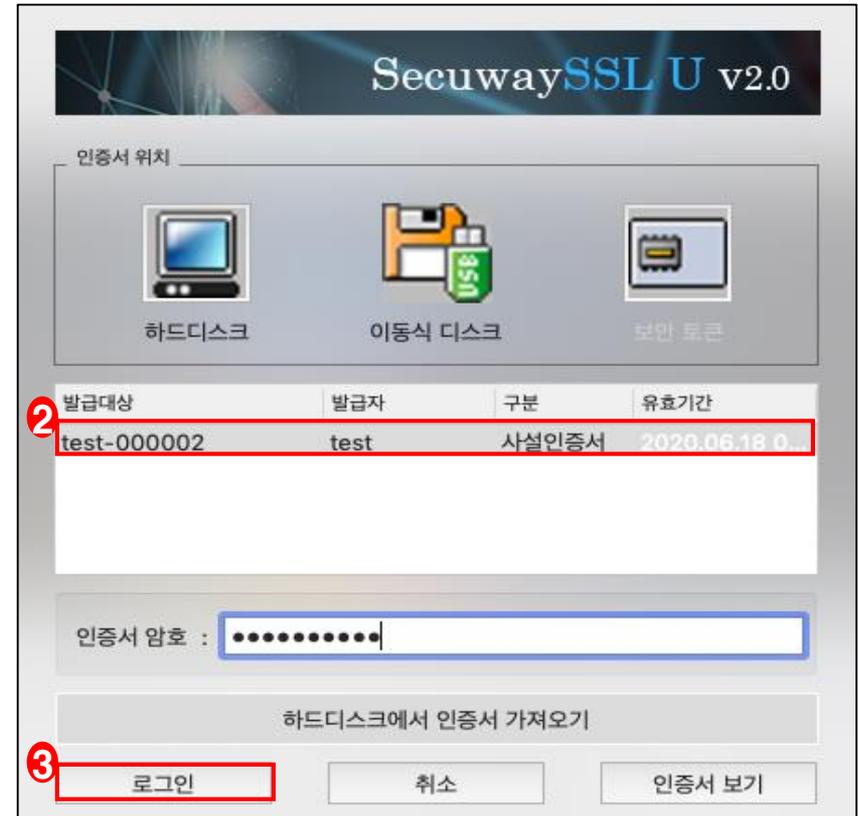
[인증서 조회]



[인증서 관리]

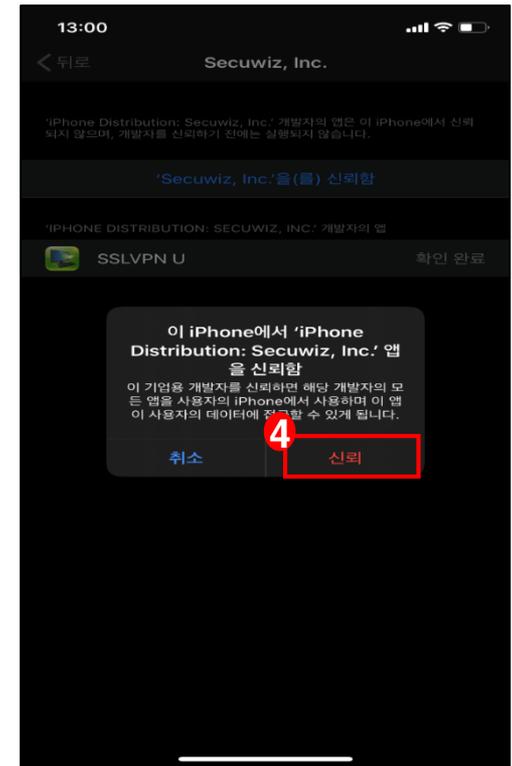
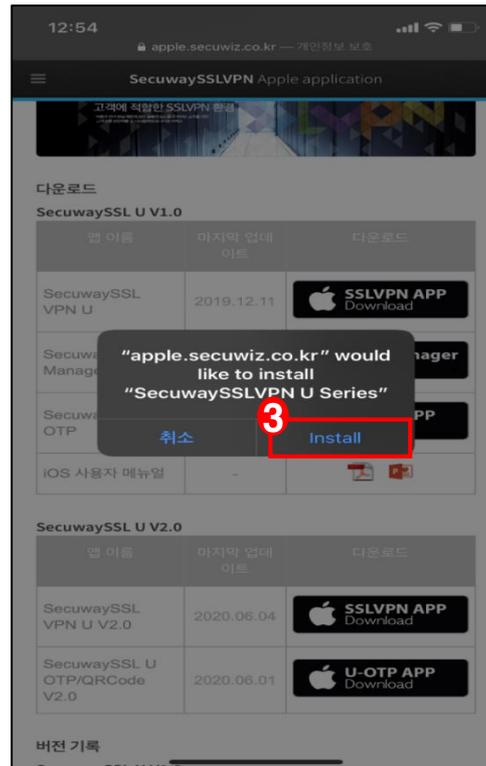
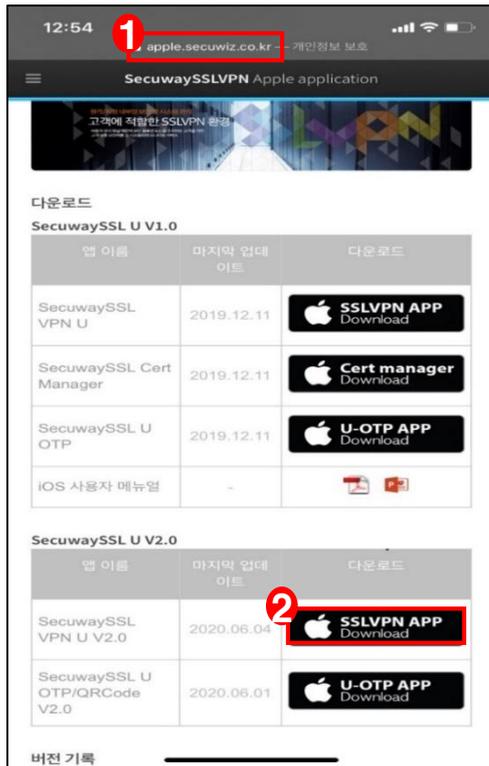
2-2-3 ID/PW 인증서 접속 #5

1. SecuwaySSL U V2.0 Client를 실행하여 계정정보를 입력하고 “로그인” 을 클릭합니다.
2. 인증서를 선택 창이 나타나며 (공인,사설) 인증서 중에서 선택합니다.
3. 인증서 암호를 입력하고 “로그인” 을 클릭합니다.



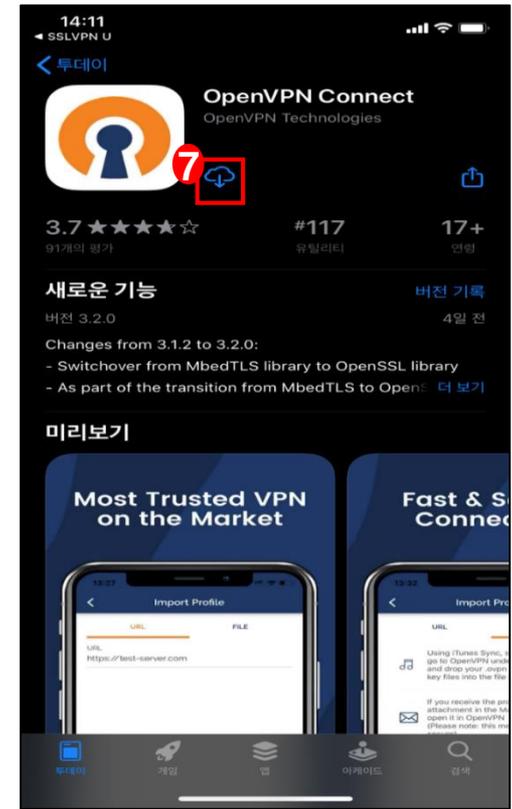
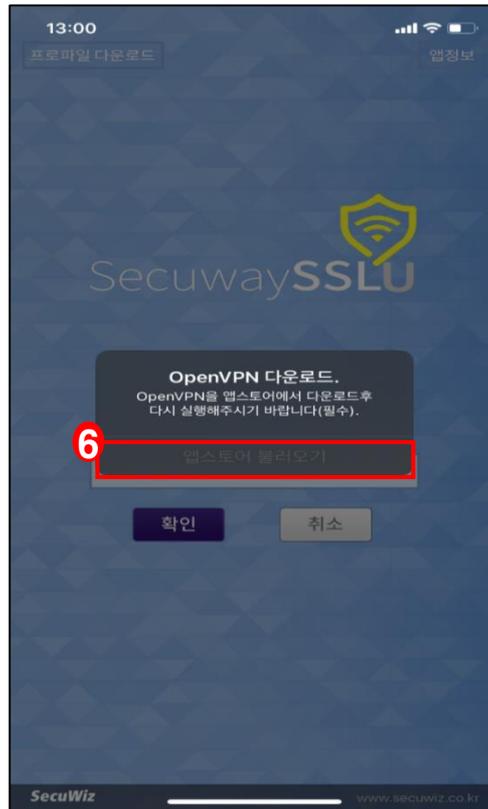
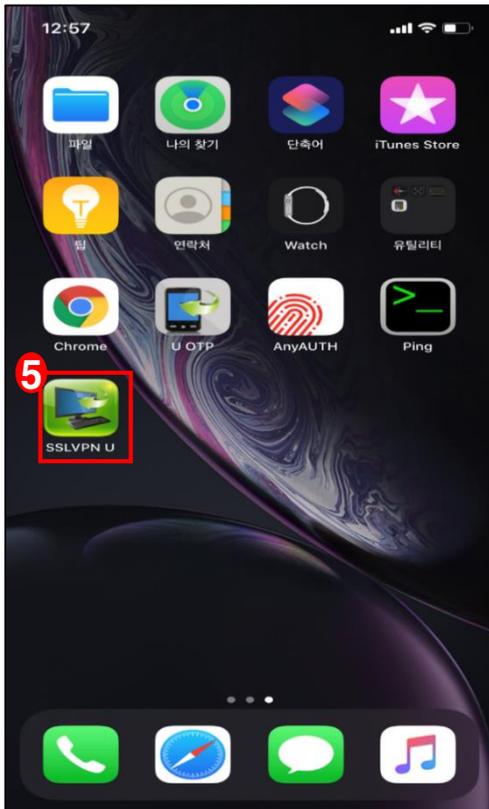
3-1-1 iOS #1

1. 주소 창에 <https://apple.secuwiz.co.kr> 입력합니다.
2. U Serise download - iOS app download 메뉴로 들어가 SecuwaySSL U V2.0을 다운로드합니다.
3. 확인 창이 나오면 "install" 을 클릭합니다.
4. 설치 완료되면 "설정-일반-프로파일 및 기기관리-secuwiz, Inc" 에 들어가서 "신뢰" 를 클릭합니다.



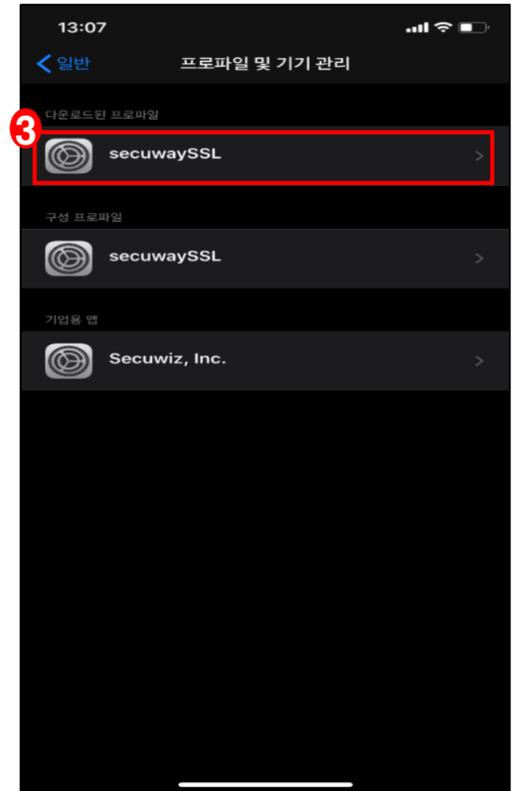
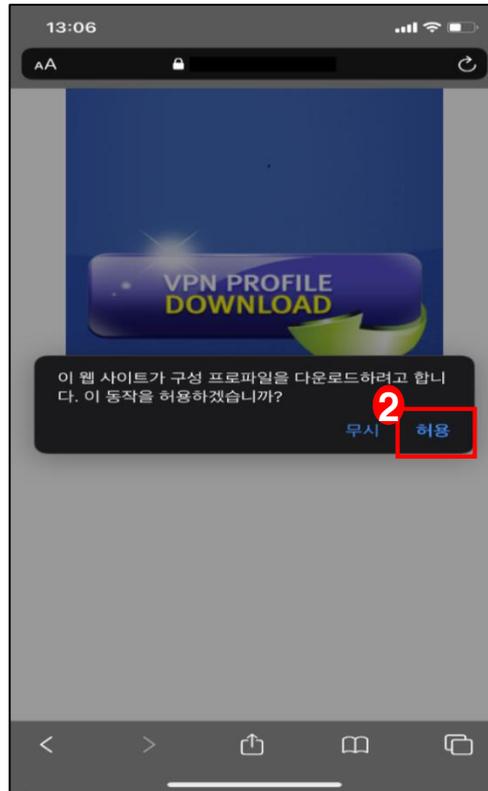
3-1-1 iOS #2

- 5. SSLVPN U 앱을 실행합니다.
- 6. OpenVPN 다운로드 경고창이 나오고 “앱스토어 불러오기” 를 클릭합니다.
- 7. 앱스토어로 이동되고 다운로드 합니다.



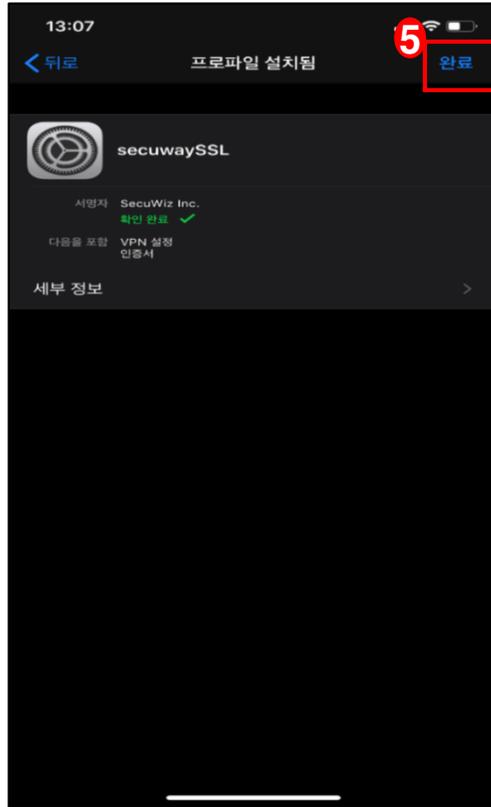
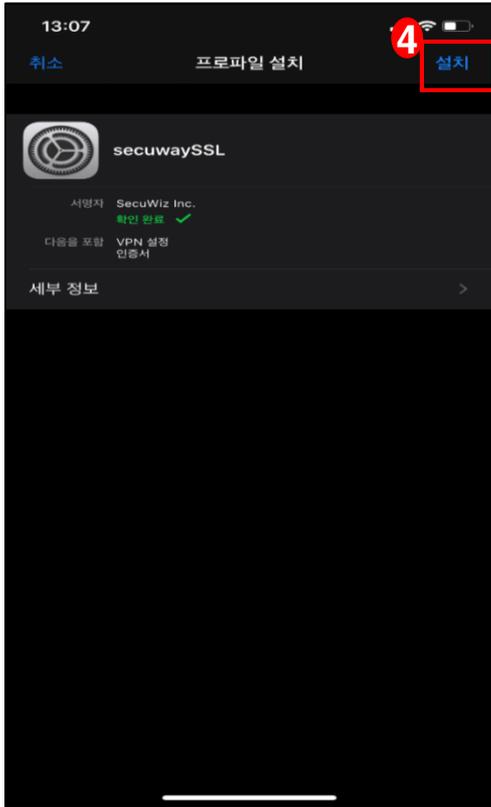
3-1-1 iOS #3

1. safari 앱을 실행하고 주소 창에 https://서버IP 를 입력합니다. 로그인 페이지가 나오고 ID , PW를 입력하고 "LOGIN" 을 클릭합니다.
2. VPN PROFILE DOWNLOAD를 클릭하면 창이 나오고 "허용" 을 클릭합니다.
3. "설정-일반-프로파일 및 기기관리 - secuwaySSL" 의 경로로 들어갑니다.



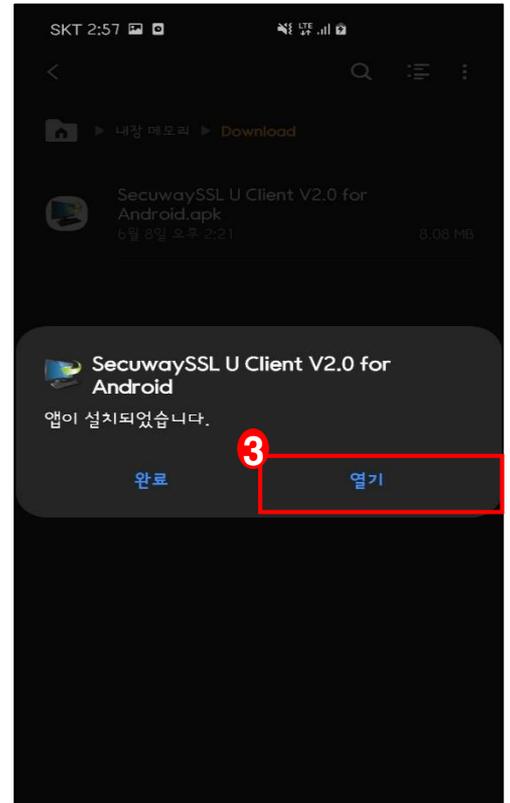
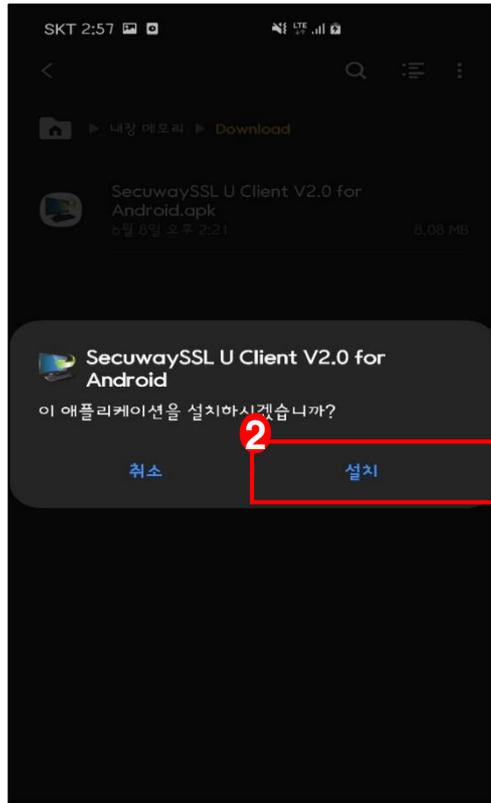
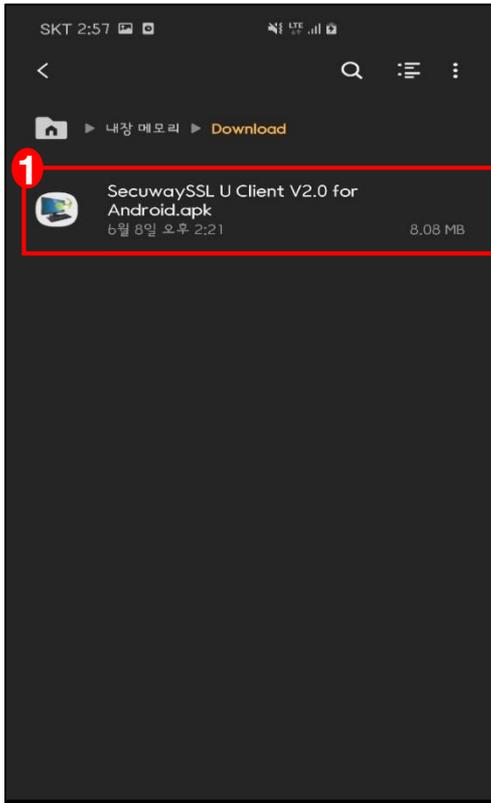
3-1-1 iOS #4

- 4. SecuwaySSL의 프로파일을 설치합니다.
- 5. 프로파일 설치가 되면 “완료” 를 클릭합니다.
- 6. SecuwaySSLU 앱을 실행하여 로그인을 진행합니다.



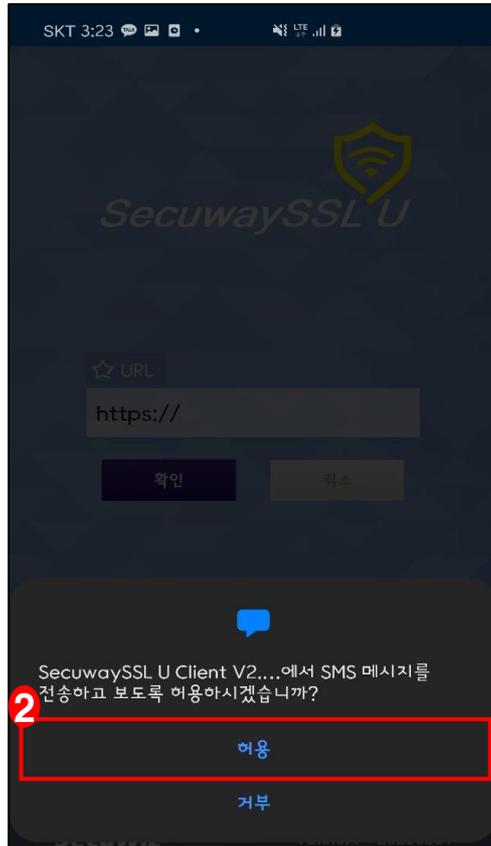
3-1-2 Android #1

1. 스마트폰 혹은 태블릿PC를 PC와 연결하거나 전송하여 설치 파일을 임의의 경로로 이동시킵니다.
2. “설치” 를 클릭합니다.
3. 설치가 완료되고 “열기” 를 클릭합니다.



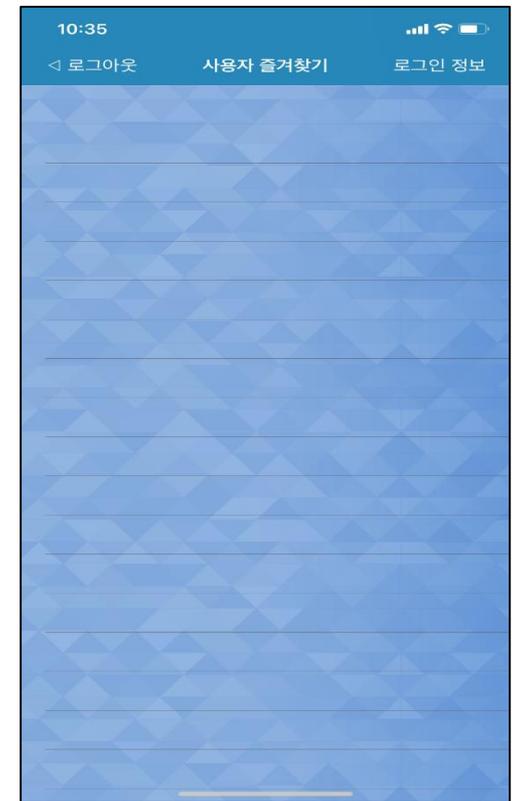
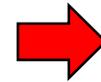
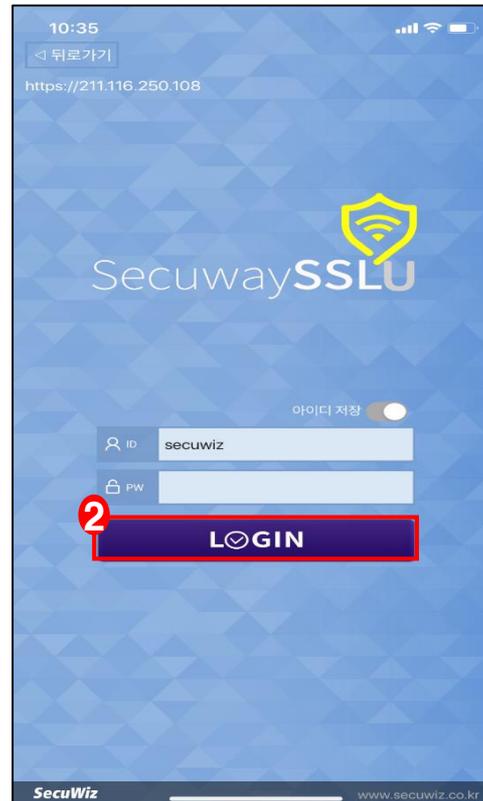
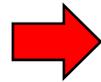
3-1-2 Android #2

1. 액세스 할건지 메시지 창이 나오고 "허용" 을 클릭합니다.
2. SMS 메시지 전송을 허용 할건지 묻고 "허용" 을 클릭합니다.
3. 로그인 페이지가 생성됩니다.



3-2-1 ID/PW iOS 접속

1. SecuwaySSL U 앱을 실행시키고 주소 창에 `https://VPN IP`를 입력하고 “**확인**”을 클릭합니다.
2. 사용자 ID/PW 를 입력하고 “**로그인**” 을 클릭합니다.
3. 접속 페이지가 생성되며 로그인 됩니다.



3-2-2 ID/PW iOS OTP 접속 #1

1. 웹페이지에서 ID/PW를 입력하고 "**APPOTP/QR KEY등록**" 을 클릭합니다.
2. OTP키와 인증번호를 입력하는 창이 팝업됩니다.
3. SecuwaySSL U-OTP 앱을 실행시켜서 키와 인증번호를 창에 입력하고 "**전송**" 을 클릭합니다.

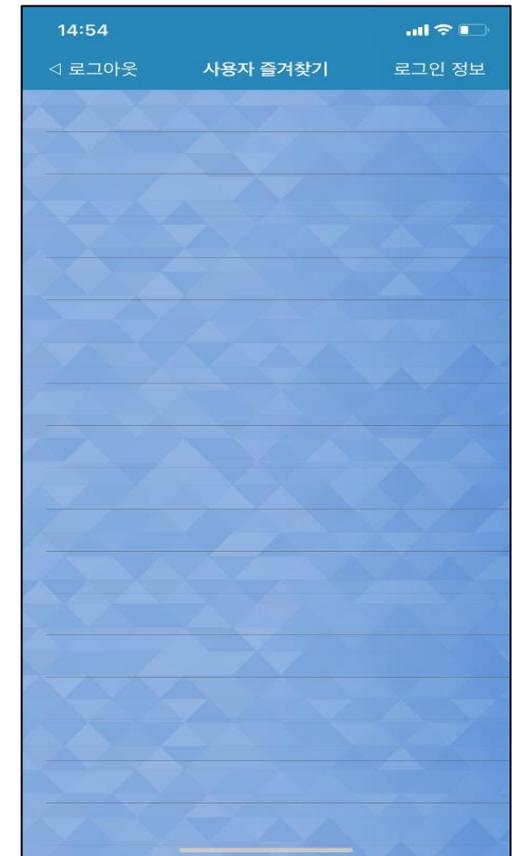
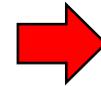
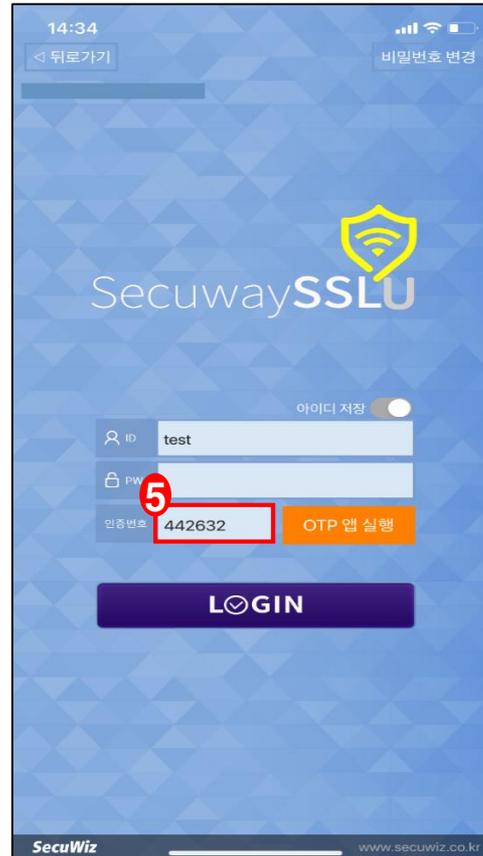
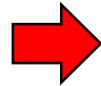
The image illustrates the first step of the iOS connection process. It shows three main components:

- Mobile App:** The SecuwaySSL U-OTP app interface on an iPhone. A red box labeled '2' highlights the key 'GUZD-SMZT-GE3D-IMJQ' and the OTP '442632'.
- Registration Popup:** A dialog box titled '핸드폰 APP OTP/QR코드 KEY를 등록하여주세요'. It contains a table with ID 'test' and key 'GUZDSMZTGE3DIMJQ'. Below the table, there is an 'OTP TEST' field with the value '442632'. A red box labeled '3' highlights the '전송' (Send) button.
- Web Login Page:** A 'User LOGIN' page with fields for ID ('test') and PW. A red box labeled '1' highlights the 'APPOTP/QR KEY 등록' button.

Copyright©2020 Secuwiz,Inc. All Rights Reserved.

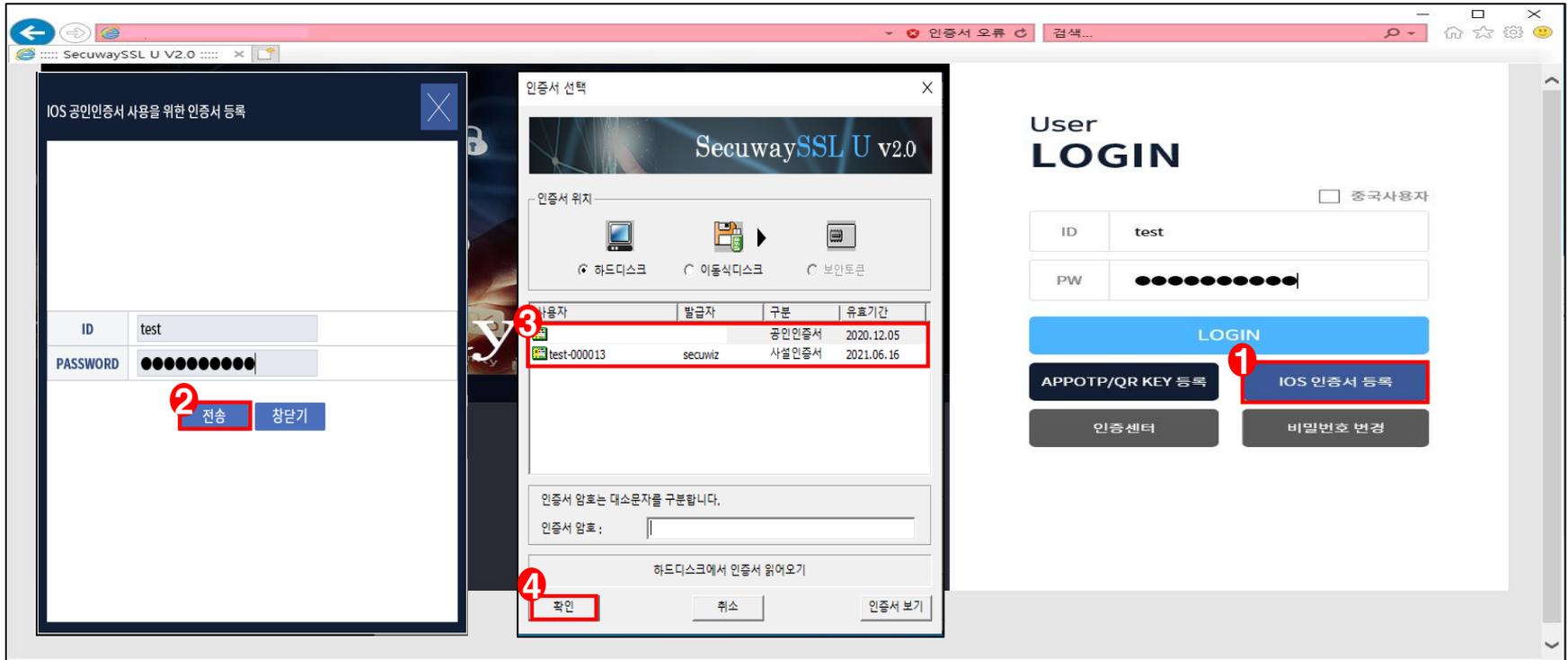
3-2-2 ID/PW iOS OTP 접속 #2

4. 인증번호를 누르면 자동으로 복사가 됩니다.
5. SecuwaySSLU 앱으로 다시 와서 계정을 입력하고 인증번호를 붙여 넣고 "**LOGIN**" 을 클릭합니다.



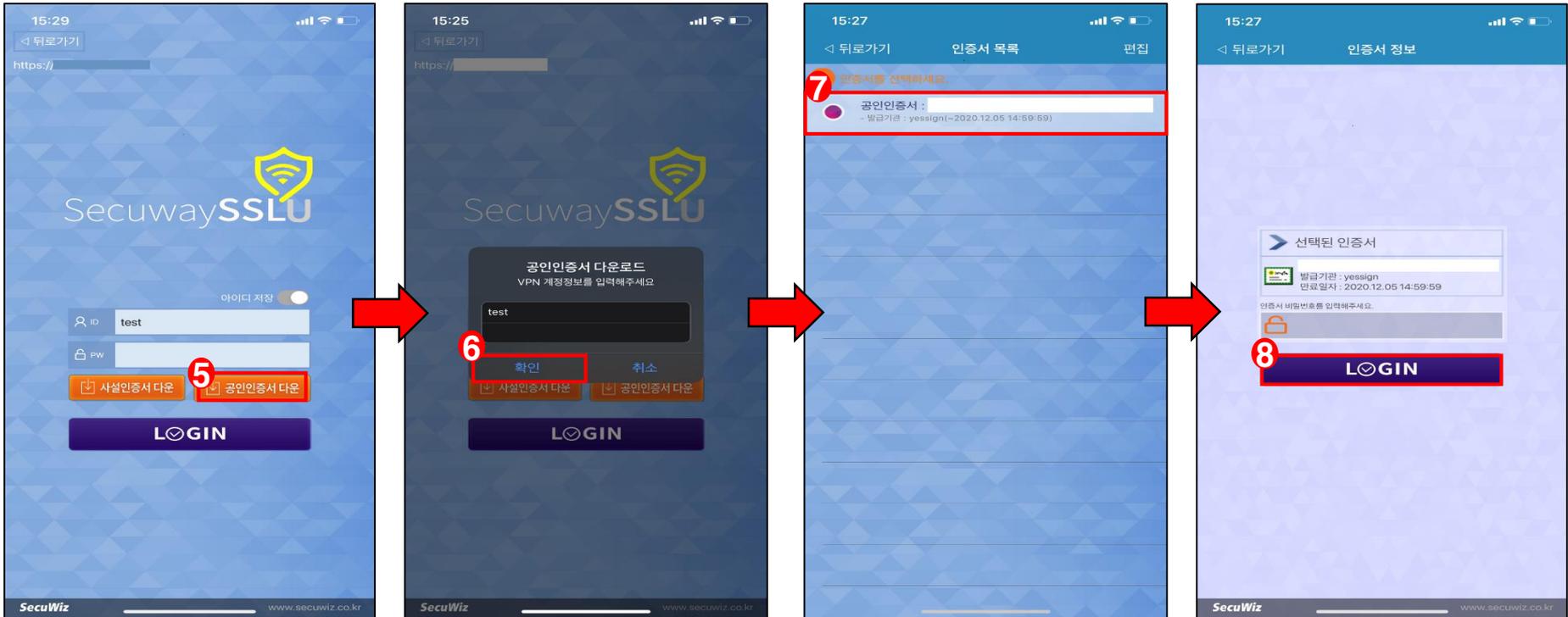
3-2-3 ID/PW iOS 인증서 접속 #1

1. 브라우저 로그인 페이지에서 “iOS 인증서 등록” 을 클릭합니다.
2. 등록을 위한 사용자 ID/PW를 입력하고 “전송” 을 클릭합니다.
3. 인증서 선택에서 공인인증서를 선택합니다.
4. 인증서 암호를 입력하고 “확인” 을 클릭합니다.



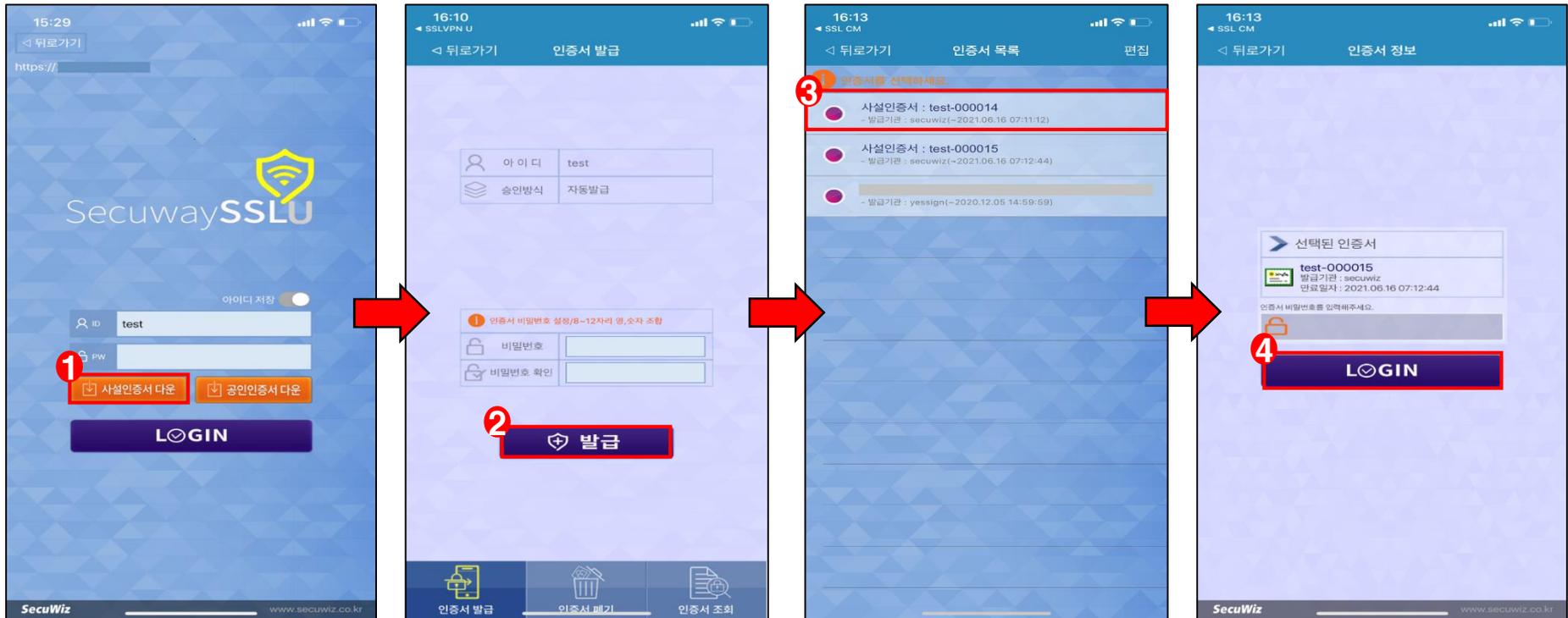
3-2-3 ID/PW iOS 인증서 접속 #2

- 5. SecuwaySSLU 앱을 실행해서 “공인인증서 다운” 을 클릭합니다.
- 6. VPN 계정정보를 입력하고 “확인” 을 클릭합니다.
- 7. 다운받은 공인인증서를 선택합니다
- 8. 인증서 암호를 입력하여 “LOGIN” 을 클릭합니다



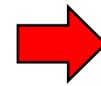
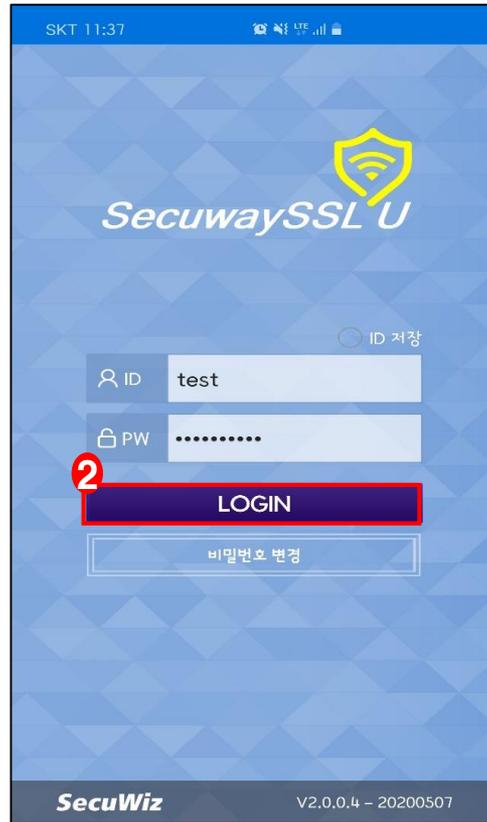
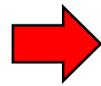
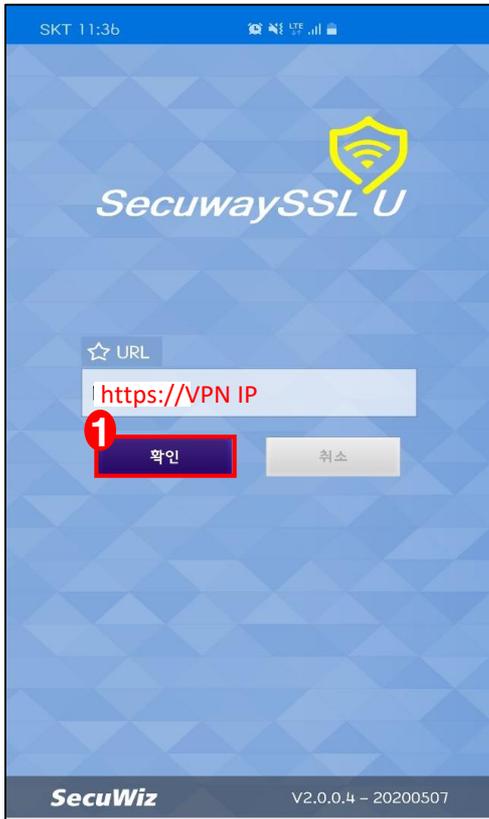
3-2-3 ID/PW iOS 인증서 접속 #3

1. SecuwaySSLU앱에서 ID/PW를 입력하고 “사실인증서 다운” 을 클릭합니다.
2. 계정정보를 입력하고 “발급” 을 클릭합니다.
3. 발급 받은 사실인증서를 선택합니다.
4. 인증서 암호를 입력하여 “LOGIN” 을 클릭하시면 로그인 됩니다.



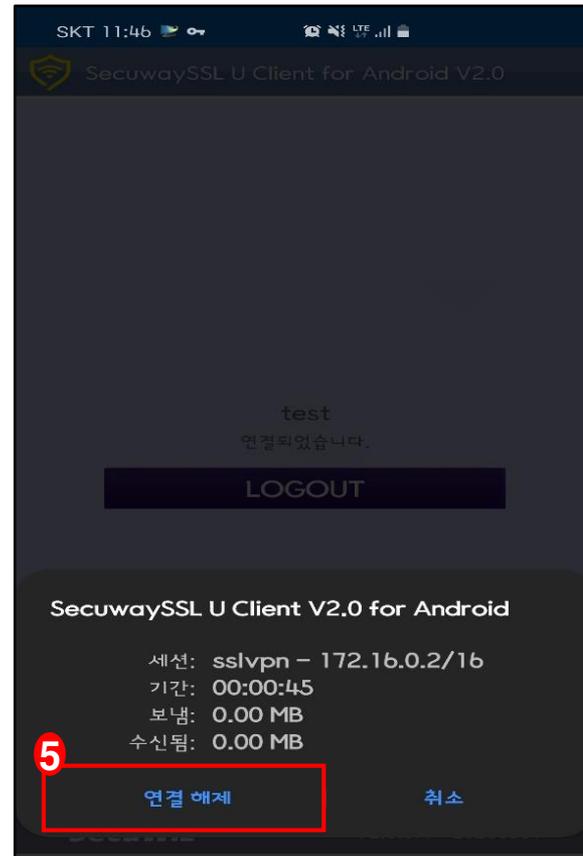
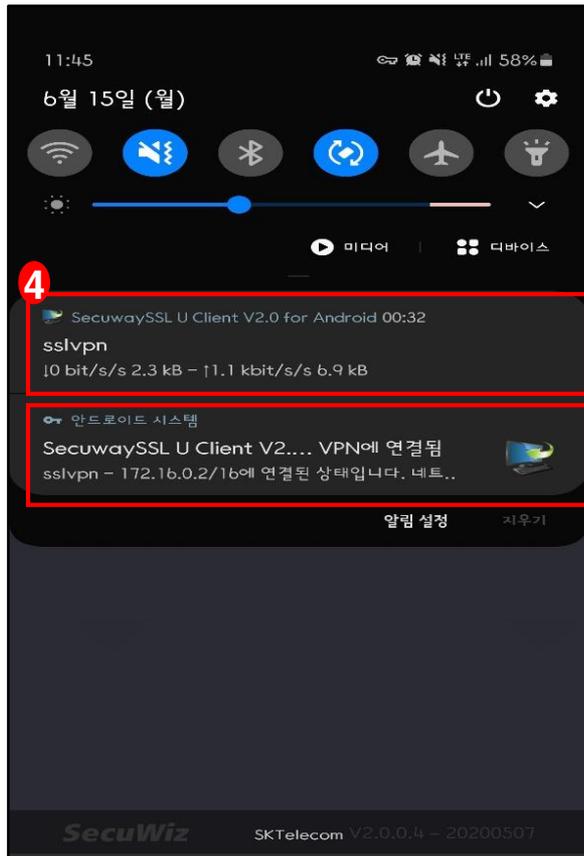
3-3-1 ID/PW Android 접속 #1

1. SecuwaySSL U 앱을 실행시키고 주소 창에 https://서버IP를 입력하고 "**확인**" 을 클릭합니다.
2. 사용자 ID , PW 를 입력하고 "**LOGIN**" 을 클릭합니다.
3. 연결되었습니다. 라고 표시되며 VPN 접속됩니다



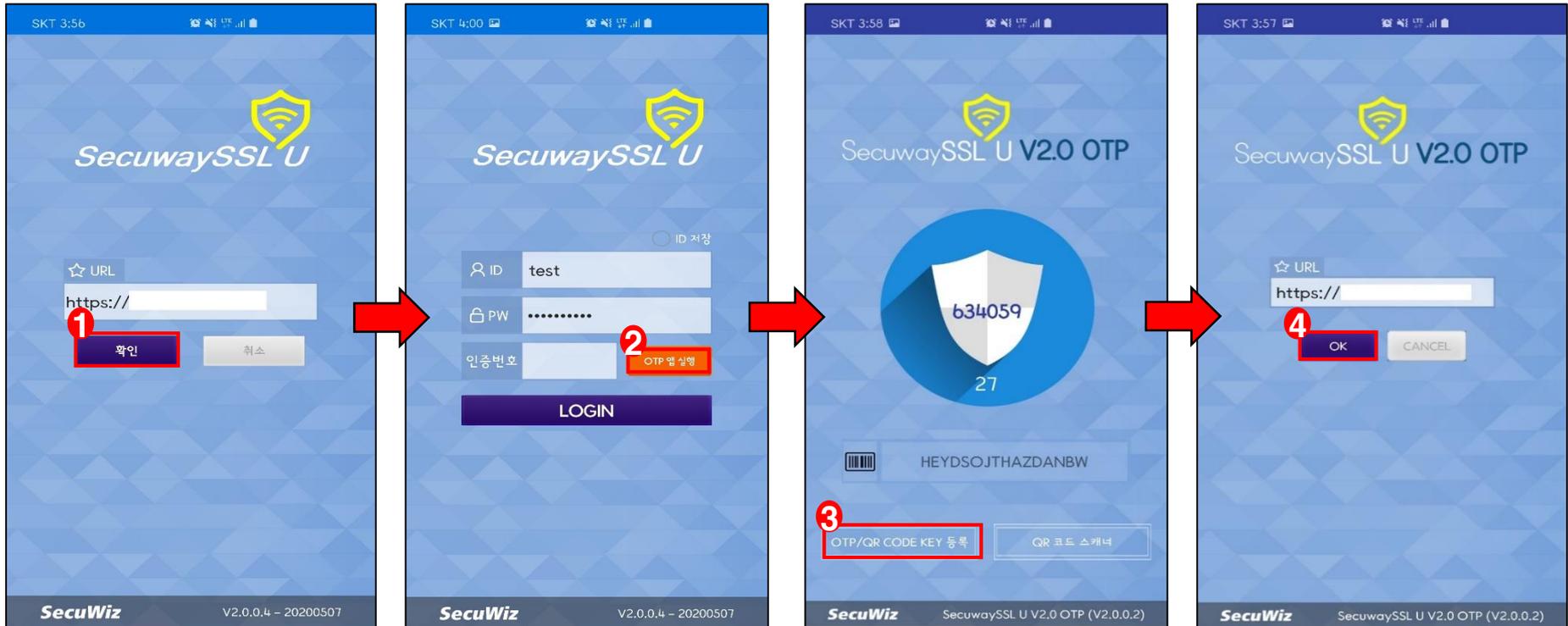
3-3-1 ID/PW Android 접속 #2

- 4. 상단에 SecuwaySSL U client 아이콘이 나타나며 클릭하여 정보를 볼 수 있습니다.
- 5. "연결 해제"를 클릭하여 VPN 접속을 해제할 수 있습니다.



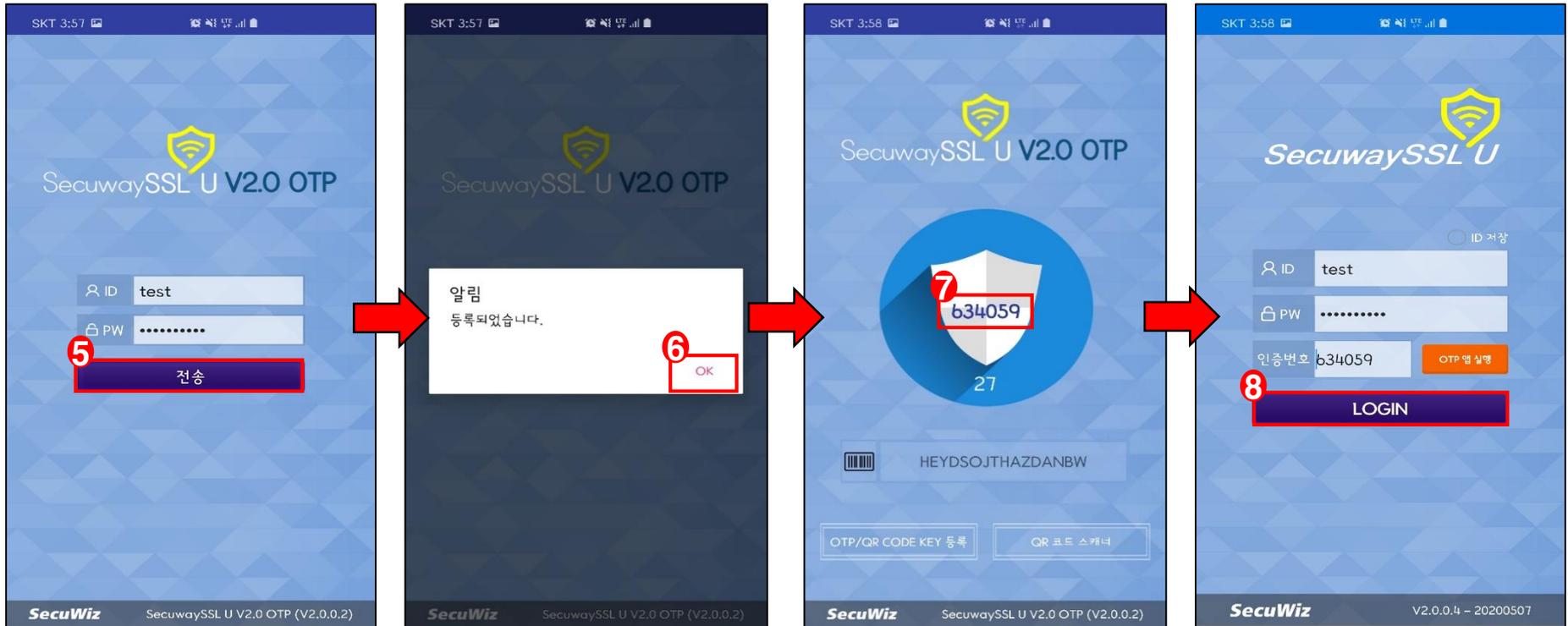
3-3-2 ID/PW Android OTP 접속 #1

1. 주소 창에 https://서버IP 를 입력하고 "확인" 을 클릭합니다.
2. "OTP 앱 실행" 을 클릭합니다.
3. OTP 앱에서 "OTP/QR CODE KEY 등록" 을 클릭합니다.
4. 주소 창에 https://서버IP 를 입력하고 "OK" 를 클릭합니다



3-3-2 ID/PW Android OTP 접속 #2

- 5. 계정을 입력하고 "전송"을 클릭합니다.
- 6. 등록이 완료되고 "OK"를 클릭합니다.
- 7. 인증번호를 클릭하면 자동으로 인증번호가 저장됩니다.
- 8. 다시 SecuwaySSL U앱에서 인증번호를 붙여 넣고 "LOGIN" 을 클릭합니다



3-3-3 ID/PW Android 인증서 접속 #1

1. SecuwaySSLU 인증센터 앱을 실행합니다.
2. 서버 주소와 계정정보를 입력하고 "로그인" 을 클릭합니다.
3. 사설 인증서 암호를 새로 입력하고 "발급" 을 클릭합니다.
4. 발급 되었고 "확인" 을 클릭합니다.



3-3-3 ID/PW Android 인증서 접속 #2

1. 계정정보를 입력하고 “**LOGIN**” 을 클릭합니다.
2. 인증서 선택을 할 수 있으며 공인 , 사설 인증서 중 선택합니다.
3. 인증서 암호를 입력하고 “**확인**” 을 클릭하면 VPN 연결됩니다.



4-1-1 Linux #1

1. 파일을 경로에 다운받고 tar 명령어를 이용하여 파일의 압축을 해제합니다. (옵션 zvf)
2. cd 명령어를 이용하여 conf 디렉터리로 이동합니다.
3. 디렉터리 안에 있는 client.info 라는 파일을 수정하기 위해 vi 명령어를 사용합니다.

```
root@localhost:/home/sslvpn/conf
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
[root@localhost sslvpn]# ls
SSU20-CFL-V2.0.0.3.tgz
[root@localhost sslvpn]# tar zxvf SSU20-CFL-V2.0.0.3.tgz
SecuwaySSLU_client
conf/
conf/client.info
libMagicCrypto.so
log/
sbin/
sbin/sslvpn
[root@localhost sslvpn]# cd conf/
[root@localhost conf]# vi client.info
```


4-2-1 ID/PW 접속

1. Client.info 에서 VPN 접속 정보를 확인합니다.
2. ./SecuwaySSLU_client 명령어로 VPN 접속 가능합니다.
 - ps -ef | grep SecuwaySSLU_client (프로세스 정보 확인) , route -nn (라우팅 정보확인)
3. Killall 명령어를 통해 VPN 접속 해제합니다.

```
root@localhost:/home/sslvpn
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
[root@localhost sslvpn]# pwd
/home/sslvpn
[root@localhost sslvpn]# cd conf
[root@localhost conf]# cat client.info
userid: test
userpw:
vpn_ip:
vpn_port: 443
crypto: yes
log_size: 50
site-to-site: no

[root@localhost conf]# cd -
/home/sslvpn
[root@localhost sslvpn]# ./SecuwaySSLU_client
SecuwaySSL U V2.0 start...
SecuwaySSL client connected!!
[root@localhost sslvpn]# ps -ef | grep SecuwaySSLU_client
root      4323      1  0 16:32 pts/0    00:00:00 ./SecuwaySSLU_client
root      4349    3075  0 16:32 pts/0    00:00:00 grep --color=auto SecuwaySSLU_client
[root@localhost sslvpn]# route -nn
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.2    0.0.0.0         UG    100    0      0 ens32
10.10.16.97     172.16.0.1     255.255.255.255 UGH   0      0      0 tun0
172.16.0.0      0.0.0.0        255.255.0.0     U     0      0      0 tun0
192.168.2.0     0.0.0.0        255.255.255.0   U     100    0      0 ens32
192.168.122.0   0.0.0.0        255.255.255.0   U     0      0      0 virbr0
[root@localhost sslvpn]# killall SecuwaySSLU_client
```

감사합니다.