사용하기 전에

Q. SSL VPN 이란 무엇인가요?

- VPN 은 가상 사설망(Virtual Private Network)의 약자로, 외부에서 접근할 수 없는 사설망에 내 PC 나 네트워크를 연결시키는 방법을 말합니다.
- 사설망과의 연결은 가상 터널을 통해 이루어지며, 이 가상 터널을 SSL 암호화로 보호하는 것이 SSL VPN 입니다.
- 가상 터널을 통해 사설망과 연결된 사용자 PC 는 사설망의 라우팅 및 ACL 정책에 따라 내부 서버에 접근할 수 있습니다.

Q. 네이버 클라우드 플랫폼의 SSL VPN 서비스는 무엇인가요?

- SSL VPN 서비스는 외부에서 네이버 클라우드 플랫폼 내부에 구성된 고객의 네트워크로 암호화된 보안 접속 통신을 제공하는 서비스입니다.
- SSL VPN 환경이 구축되어 있으면, 언제 어디서든 외부에서 도/감청 위협없이 내부 네트워크로 접근을 할 수 있습니다.

Q. SSL VPN 서비스 사용 절차는 어떻게 되나요?

- 콘솔에 접속한 후에 다음 단계를 통해 간단하게 신청한 후 바로 사용할 수 있습니다.

1. 콘솔 접속: 네이버 클라우드 플랫폼 콘솔에 접속합니다.
2. SSL VPN 서비스 설정: SSL VPN 에 외부 접속을 허용할 최대 ID 수, 인증방식, VPN 아이디 정보를 등록합니다. VPN 아이디는 최대 10 개까지 등록할 수 있습니다.
3. SSL VPN 서비스 신청: SSL VPN 서비스를 신청합니다. 서비스 신청 즉시 이용이 가능합니다.
4. 클라이언트 설치: 네이버 클라우드 플랫폼 자료실에서 SSL VPN Agent 를 다운로드하여 외부 접속용 PC 에 설치합니다.
5. 접속: 외부 접속용 PC 에 설치된 Agent 를 실행한 후 등록된 VPN 아이디를 이용해 접속합니다.

Q. SSL VPN 에 접속하면 모든 접속은 내부 네트워크를 경유하게 되나요?

- SSL VPN 은 분할 터널링(Split Tunneling)을 지원하여 내부 사설망으로 향하는 접속에 대해서만 VPN 터널링을 수행합니다.
- 내부 사설망으로 향하지 않는 접속(인터넷 접속, 타 네트워크로의 접속 등)은 기존과 같이 사용자 PC 의 라우팅을 따릅니다.

Q. SSL VPN 를 콘솔에서 생성했더니 SSL VPN IP pool 이라는 게 보이는데 이게 뭔가요?

- SSL VPN 은 가상의 터널을 통해 사용자의 PC 와 대상 네트워크를 연결하는 서비스로, SSL VPN IP pool 은 대상 네트워크로부터 사용자 PC 가 부여받는 IP 주소입니다.
- 사용자 PC 는 28 비트의 네트워크 대역에서 비어있는 IP 주소를 자동으로 할당받습니다.
- 사용자 PC 는 대상 VM 에 접속할 때 해당 SSL VPN IP 주소를 사용하기 때문에, 사용자는 미리 ACG 에 해당 SSL VPN IP pool 을 허용 처리해 두어야 합니다.

Q. 사용자 계정 수는 뭔가요?

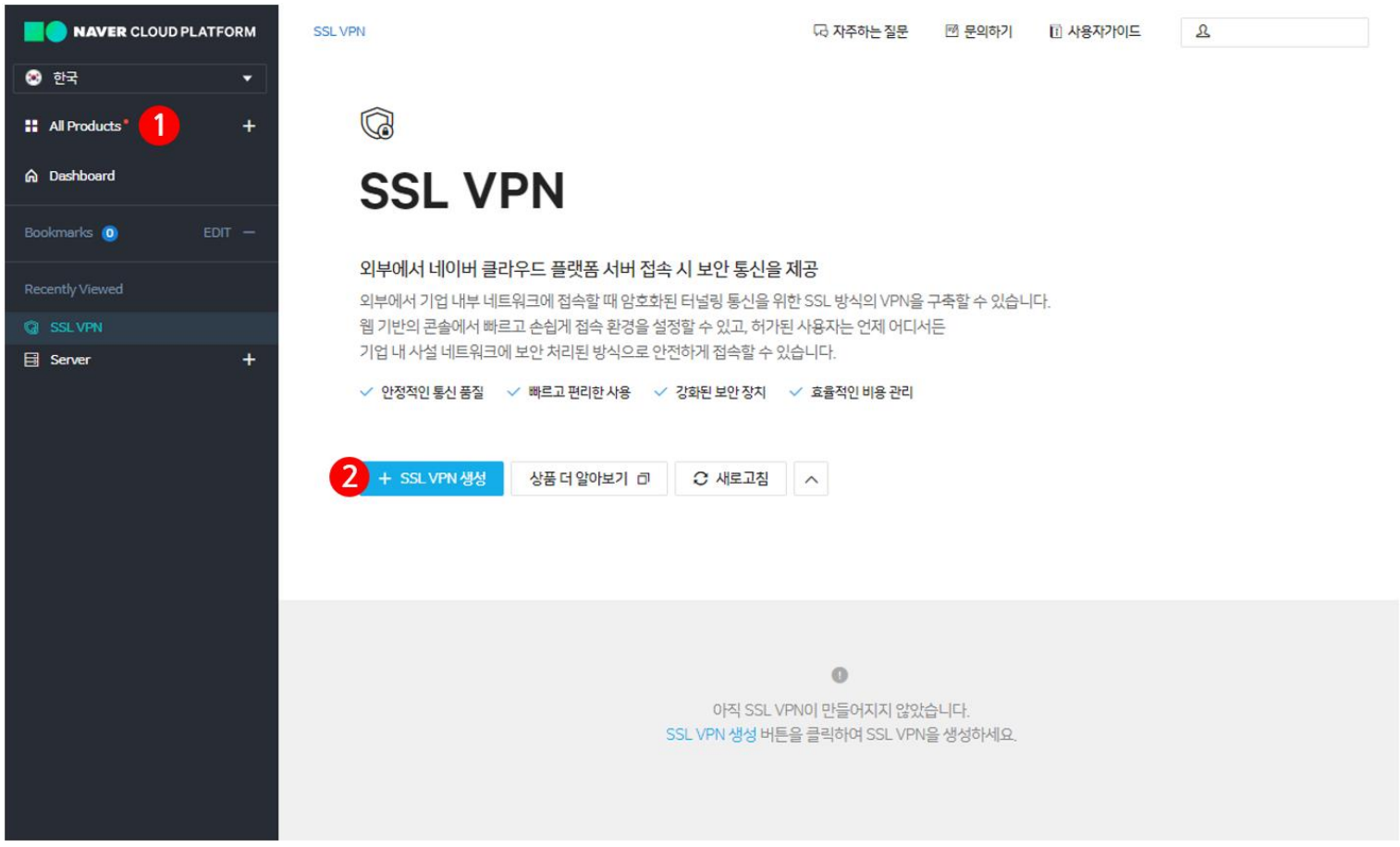
- 사용자는 SSL VPN 생성 시 최대 3/5/10 개의 VPN 아이디를 생성할 수 있는 상품을 선택할 수 있습니다.
- 이후 선택한 개수 내에서 자유롭게 VPN 아이디를 생성/삭제할 수 있으며, 사용자 계정 수는 이 내용을 보여주는 항목입니다.
- 예를 들어 '사용자 계정 수 (2/3)'와 같이 표기되어 있으면 사용자가 VPN 아이디 3 개를 생성할 수 있는 상품을 선택했으며, 그 중 2 개를 만들어 사용하고 있다는 의미입니다. 즉, 이 사용자는 1 개의 VPN 아이디를 더 만들어서 사용할 수 있습니다. VPN 아이디가 더 필요한 경우, 추가로 SSL VPN 상품을 생성 후 사용하시면 됩니다.

Q. 일차인증방식과 이차인증방식의 차이점은 뭔가요?

- SSL VPN 접속 시 인증하는 방식의 차이입니다.
- 일차인증은 ID/PW 만을 통해 인증받고 로그인할 수 있는 방식입니다.
- 이에 반해 이차인증는 MFA(Multi-Factor Authentication) 방식으로, ID/PW 를 통해 인증한 후에 OTP 를 통해 한 번 더 인증을 받아야 로그인할 수 있는 방식입니다.
- OTP 를 이용한 인증방식은 ID/PW 만을 이용한 인증방식보다 보안상 안전합니다.
- SSL VPN 의 OTP 는 사용자가 입력한 메일과 SMS 를 통해 전달됩니다.

SSL VPN 서비스 신청

Step 1. 콘솔 접속

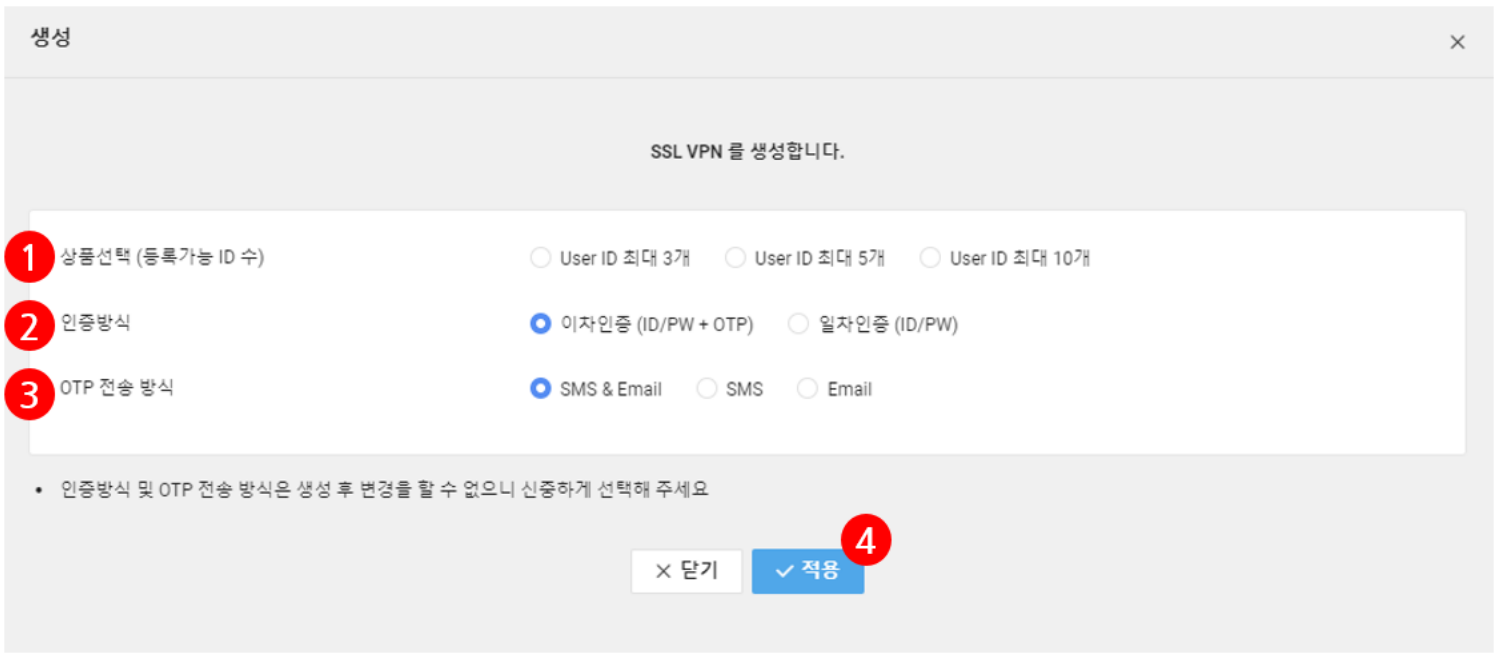


① 콘솔에 접속 후, **Security > SSL VPN** 을 클릭합니다.

② 왼쪽 상단 혹은 화면 중앙의 **SSL VPN 생성**을 클릭합니다.

- SSL VPN 은 필요에 따라서 2 개 이상의 상품을 추가로 신청할 수 있습니다.

Step 2. 스펙 및 인증방식 선택



① SSL VPN 생성 팝업 창이 열리면 먼저 생성 가능한 ID 수(3 개/5 개/10 개)로 구분된 스펙을 선택합니다.

② VPN 서비스 인증방식에서 일차인증 또는 이차인증 인증을 선택합니다.

- 일차인증은 ID/PW 로 인증하는 방식입니다. 간단하지만 이차인증보다 보안성이 낮습니다.
  이차인증은 ID/PW 로 인증한 후 OTP 로 추가 인증하는 방식입니다. OTP 는 사용자 이메일 및 휴대전화번호로 전달됩니다.
  일차인증보다 보안성이 높습니다.
  단, 이차인증을 사용하려면 이메일 및 휴대전화번호 정보 수집을 위한 개인정보 활용에 동의해야 합니다.

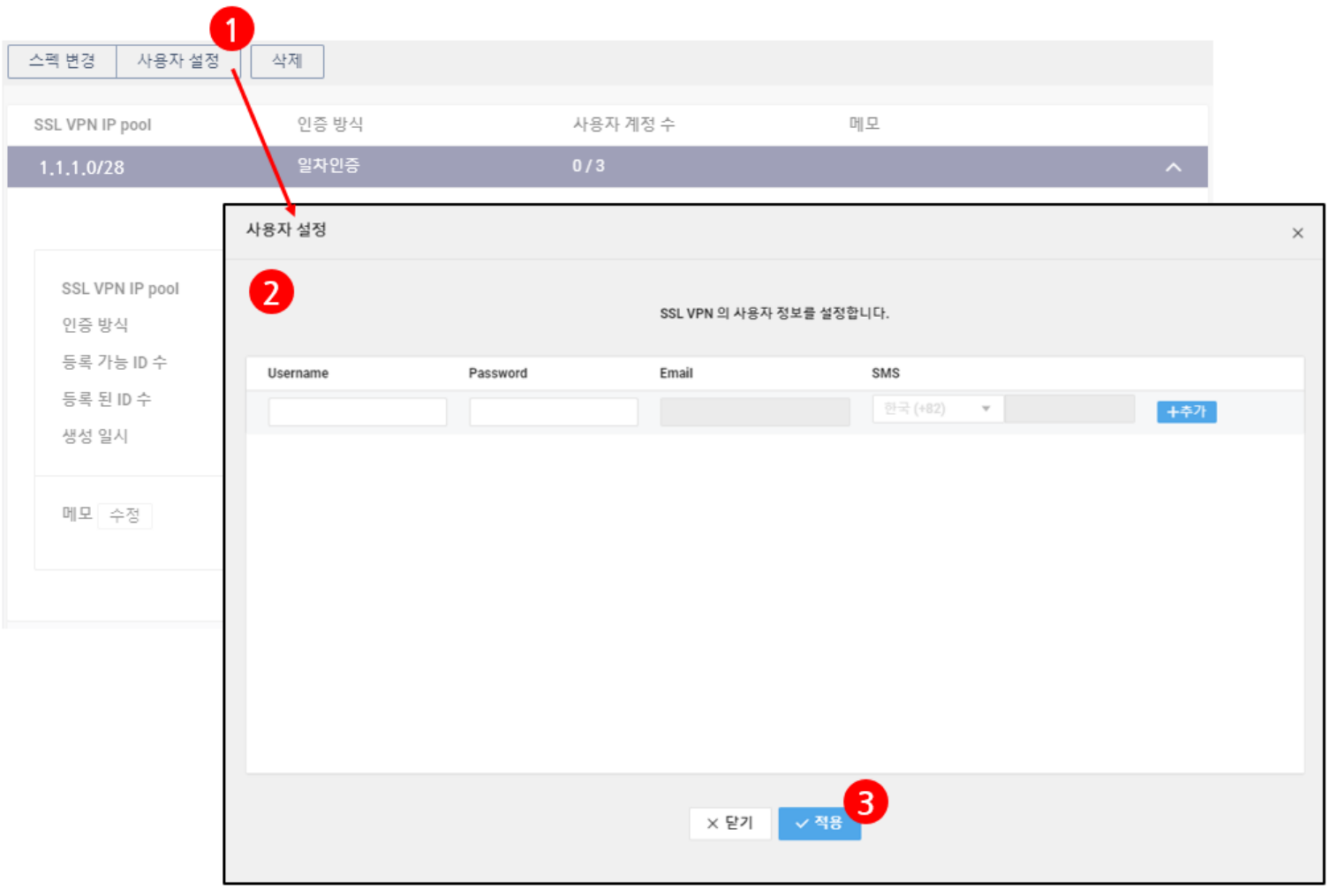
- 인증방식은 SSL VPN 서비스 생성 후에는 변경할 수 없으므로 신중하게 선택해야 합니다.
  (인증방식을 바꾸고 싶다면 SSL VPN 서비스 삭제 후 재생성합니다)
  스펙은 **스펙 변경**을 클릭하여 언제든지 변경할 수 있습니다. 단, 스펙에 따라 요금이 변경되므로 본인에게 맞는 스펙을 선택해야 합니다.
  ③ 인증방식을 이차인증으로 사용하시는 경우 ID/PW 입력 이후 OTP 를 어떤 디바이스로 전송 받을지 결정합니다. SMS, Email 을 선택할 수 있습니다.

  ④ **생성**을 클릭하면 SSL VPN 상품 신청이 완료됩니다.

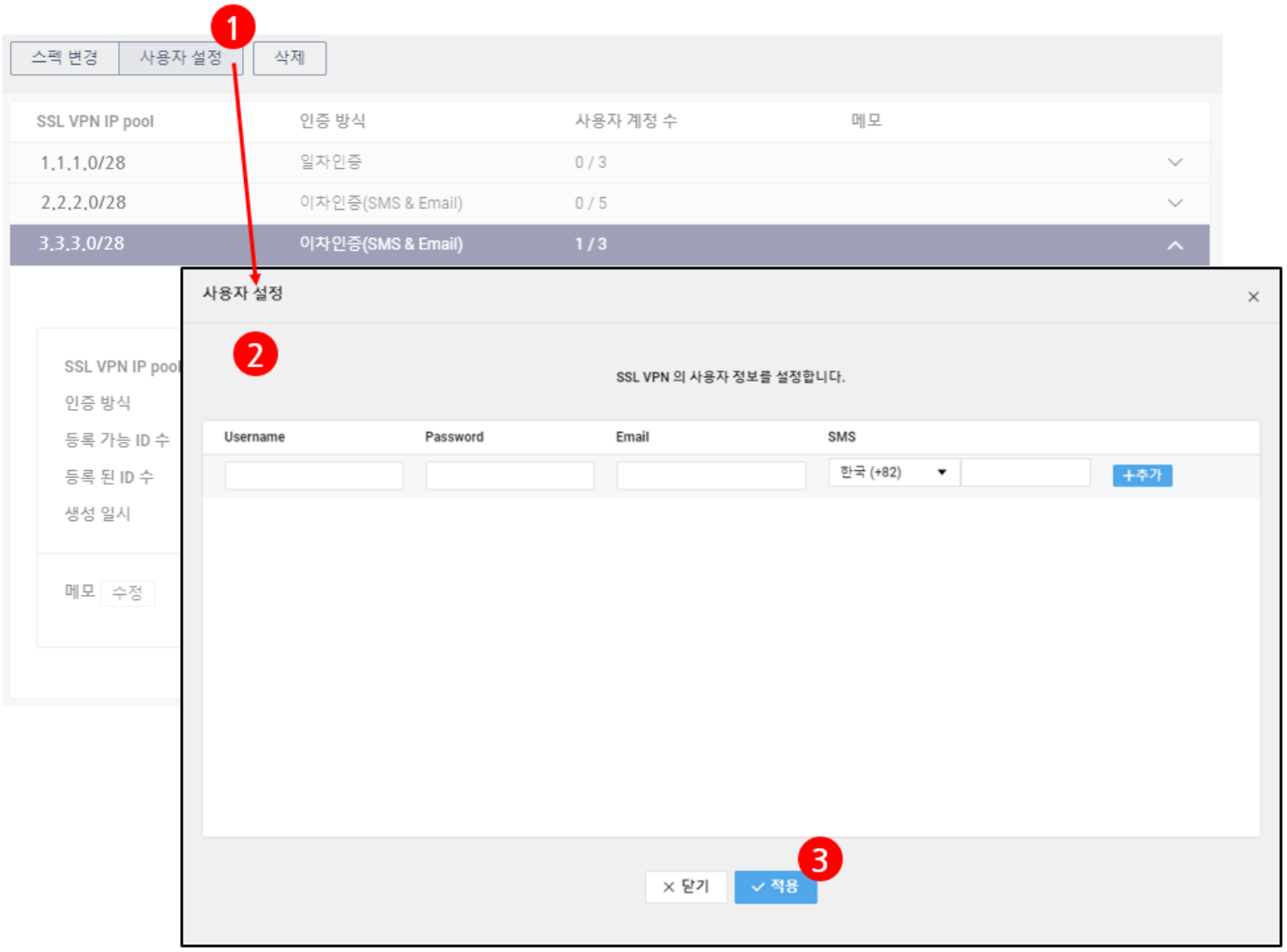
Step 3. 사용자 설정

인증방식에 따라 다음과 같이 사용자를 설정합니다.

- 일차인증



- 이차인증



① 설정할 상품을 선택한 후 **사용자 설정**을 클릭합니다.

② SSL VPN 을 사용할 사용자의 Username 및 부가 정보를 입력하고 **추가**를 클릭합니다.

- SSL VPN 생성 창에서 일차인증을 선택했다면 username, 비밀번호를 입력하고, 이차인증을 선택했다면 username, 비밀번호 외에도 메일 주소 및 휴대전화번호를 함께 입력합니다.
- 선택한 스펙에 따라 생성 가능한 username 개수도 달라집니다.
- 보안을 위해 비밀번호는 8 자 이상이어야 하며, 영문자 소문자, 대문자, 특수문자, 숫자 중 3 개 항목이 1 자 이상씩 포함되어야 합니다.

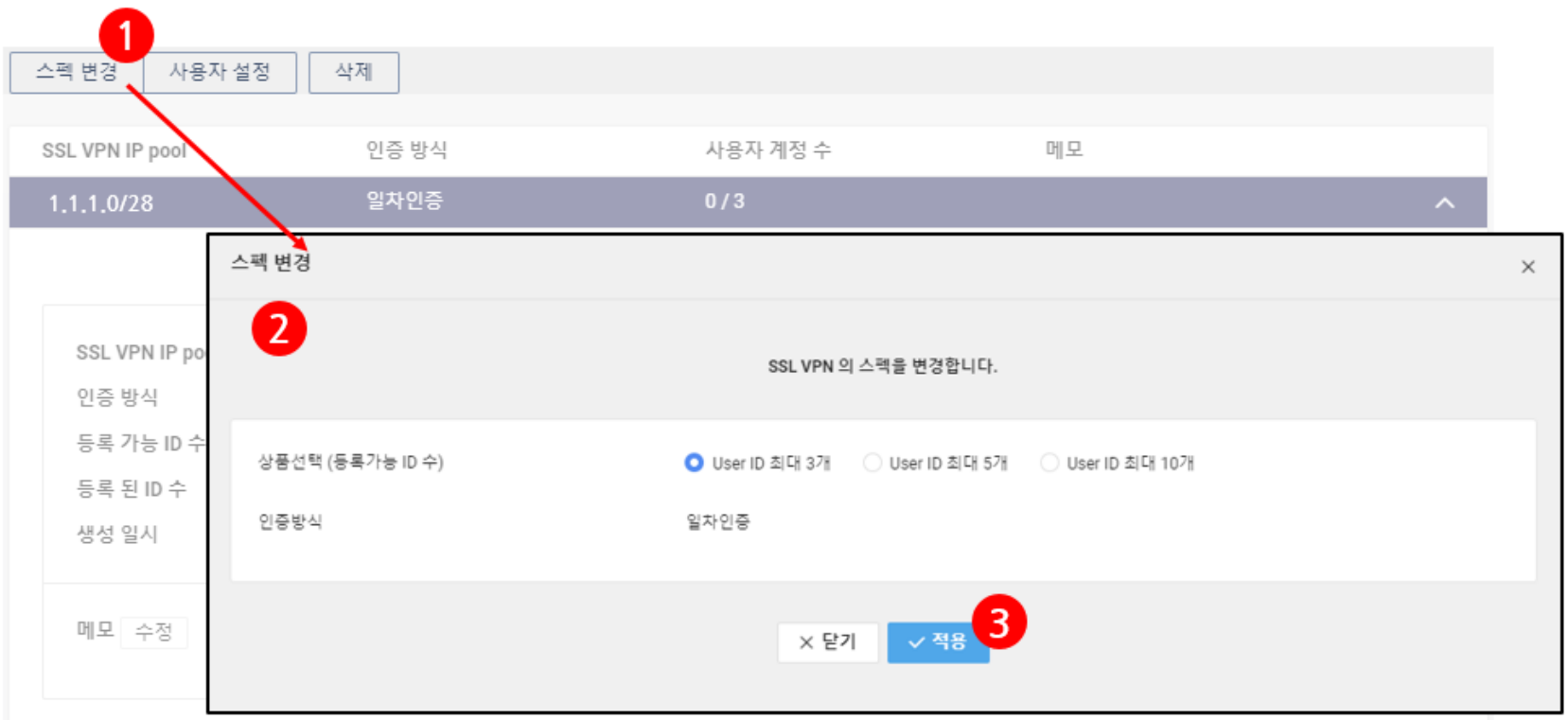
③ 설정을 마쳤으면 **적용**을 클릭해 서비스에 반영합니다.

username 을 제외한 모든 설정은 수정 가능하며, username 의 추가/삭제 또한 **사용자 설정**에서 언제든지 가능합니다.

SSL VPN 서비스 변경

현재 선택된 스펙(등록 가능한 ID 수) 변경

Step 1. 콘솔 접속



① 설정할 상품을 선택한 후 상단의 **스펙 변경**을 클릭합니다.

Step 2. 스펙 선택

② 변경할 스펙을 선택합니다. 현재 스펙보다 등록 가능 ID 수가 더 적은 스펙으로 변경하려면, 현재 등록된 ID 수가 변경할 스펙의 ID 수와 같거나 더 적어야 합니다.

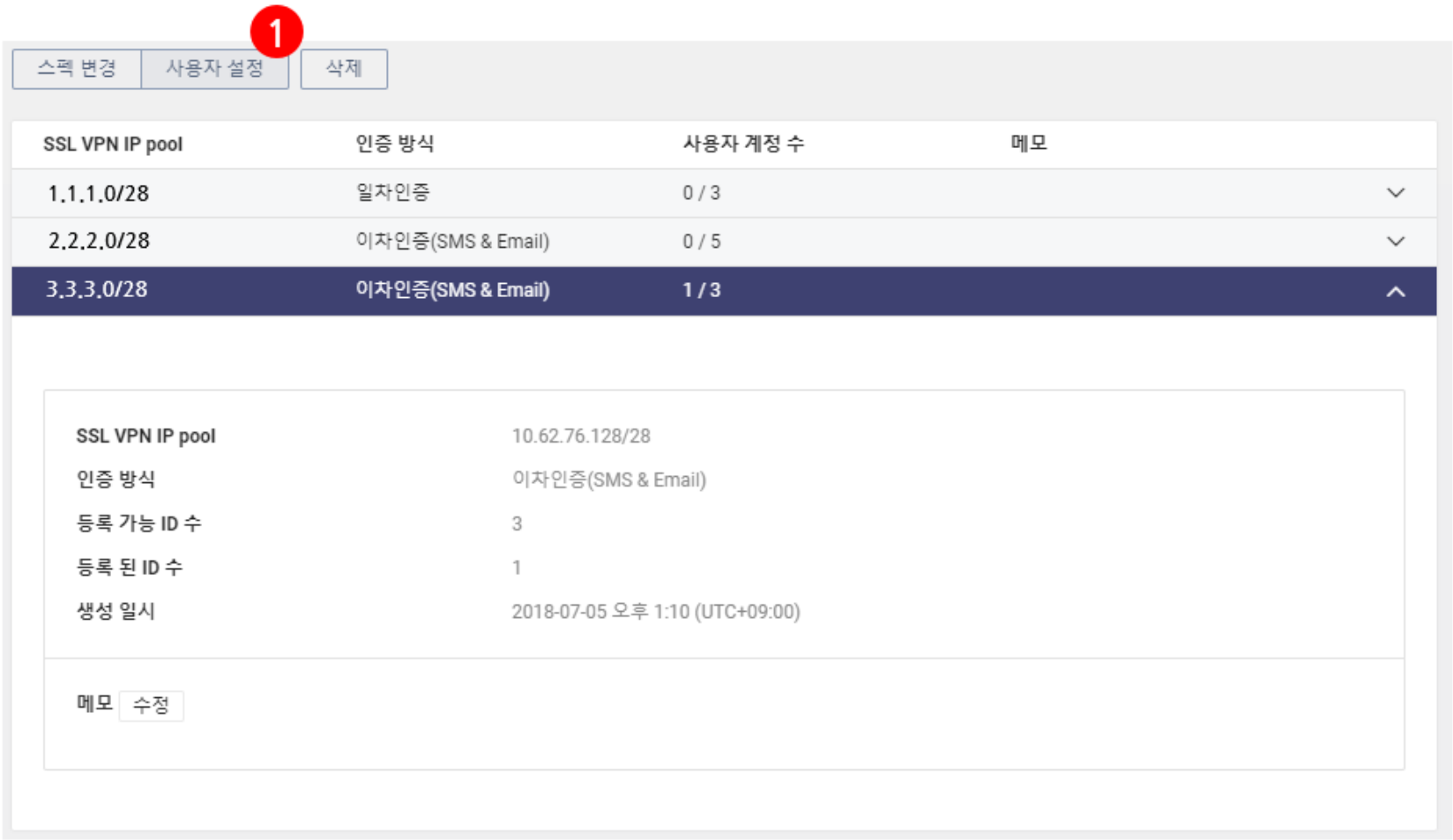
③ **변경**을 클릭합니다.

10개 이상의 ID가 필요할 때

10 개 이상의 ID 가 필요한 경우에는 SSL VPN 상품을 추가로 생성합니다.

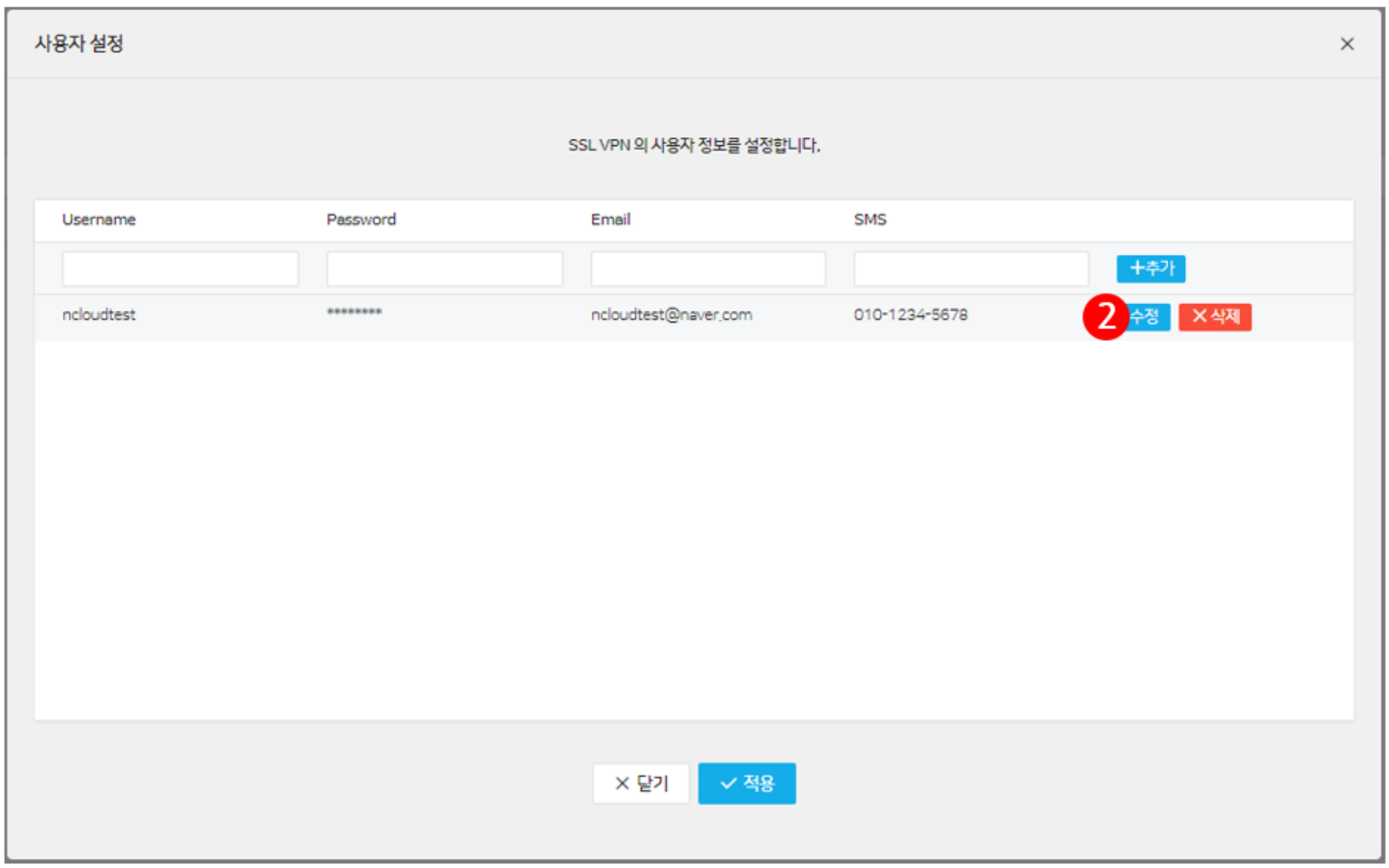
등록한 ID의 정보 변경

Step 1. 콘솔 접속



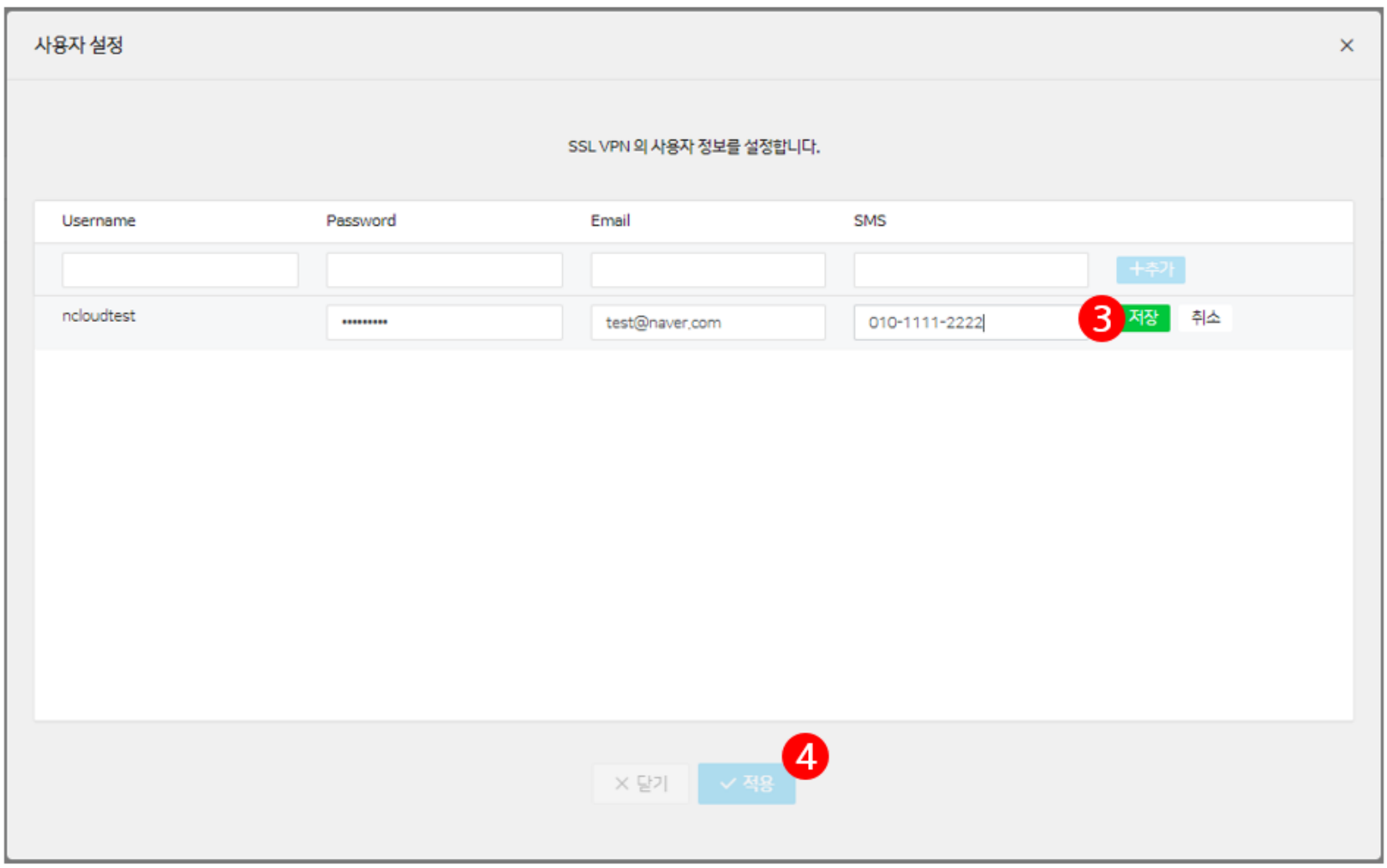
① 설정할 상품을 선택한 후 상단의 **사용자 설정**을 클릭합니다.

Step 2. 정보 변경



② 변경하고 싶은 ID 오른쪽의 **[수정]** 버튼을 클릭한 후에 정보를 설정합니다.

Step 3. 저장 및 적용



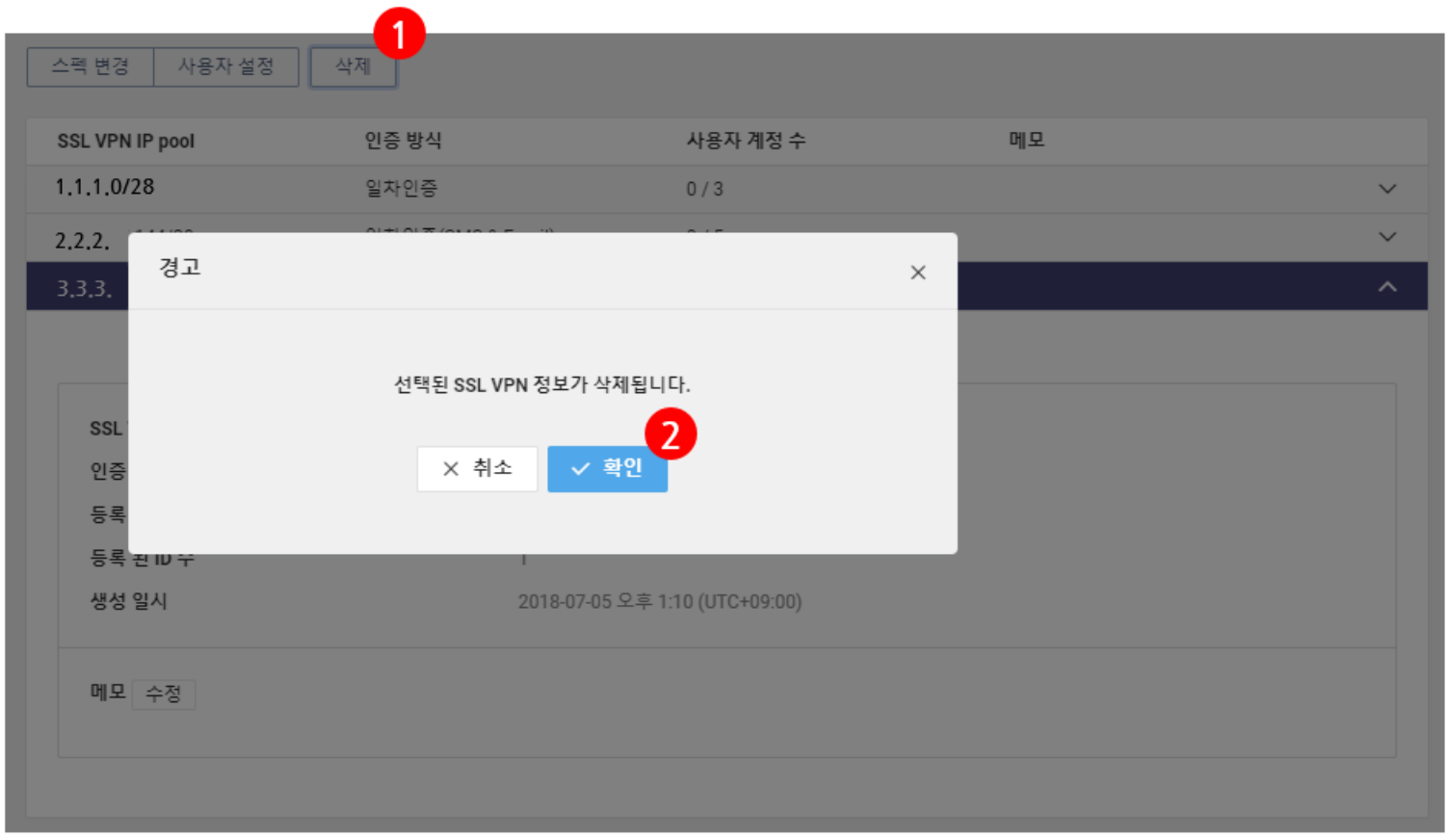
③ **저장**을 클릭하면 정보가 저장됩니다. 변경한 정보을 저장하지 않으려면 **취소**를 클릭합니다.

④ 변경이 필요한 모든 ID 의 정보를 저장한 후 하단의 **적용**을 클릭합니다.

인증방식 변경 – 일차인증/이차인증

한 번 선택한 인증방식은 변경할 수 없습니다. 따라서 최초 SSL VPN 생성 시 인증방식을 신중하게 선택해야 합니다.

SSL VPN 서비스 삭제



① 삭제할 상품을 선택한 후 왼쪽 위의 **SSL VPN 삭제**를 클릭합니다.

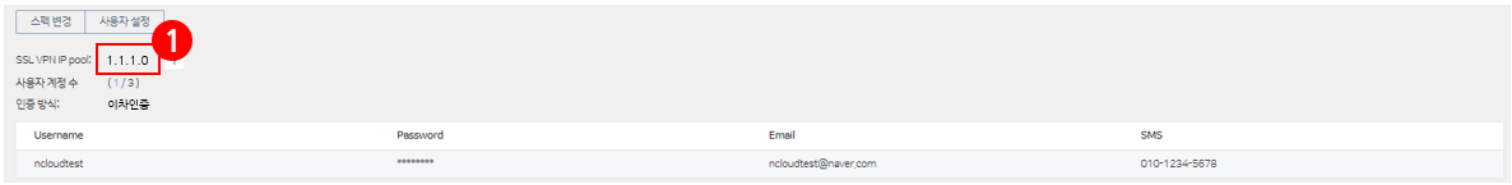
② 경고 문구를 확인하고 **확인**을 클릭하면 선택한 SSL VPN 서비스가 삭제됩니다.

주의

SSL VPN 서비스를 삭제하면 해당 상품에서 등록한 모든 username 정보가 함께 삭제됩니다. 이 정보는 복구할 수 없으며, 다시 SSL VPN 서비스를 사용하려면 모든 정보를 다시 입력해야 합니다.

SSL VPN IP pool을 ACG에 등록하기

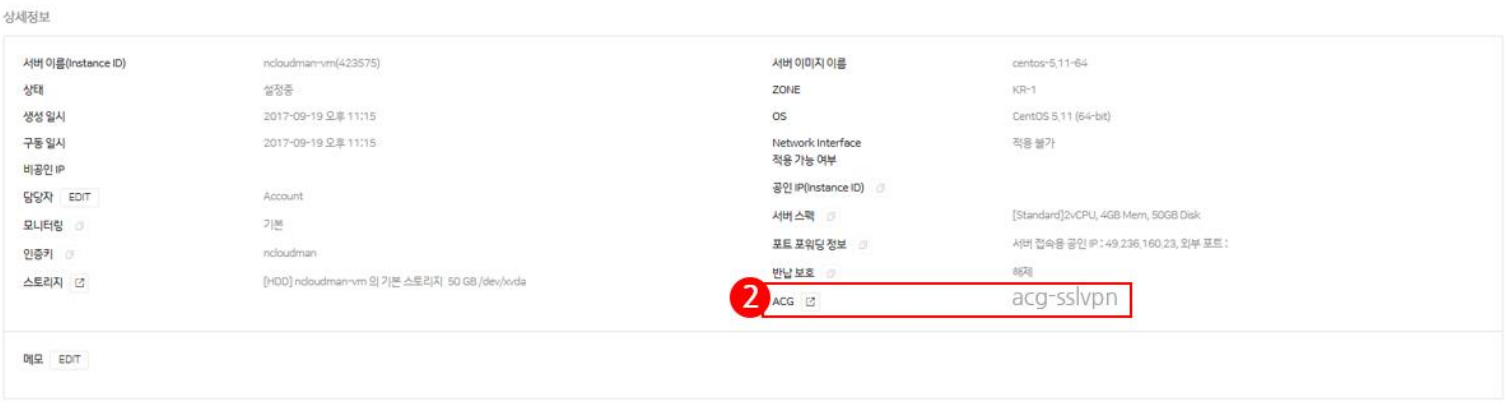
Step 1. SSL VPN IP pool 확인



① SSL VPN 상품 상단에 표기된 SSL VPN IP pool 을 확인합니다.

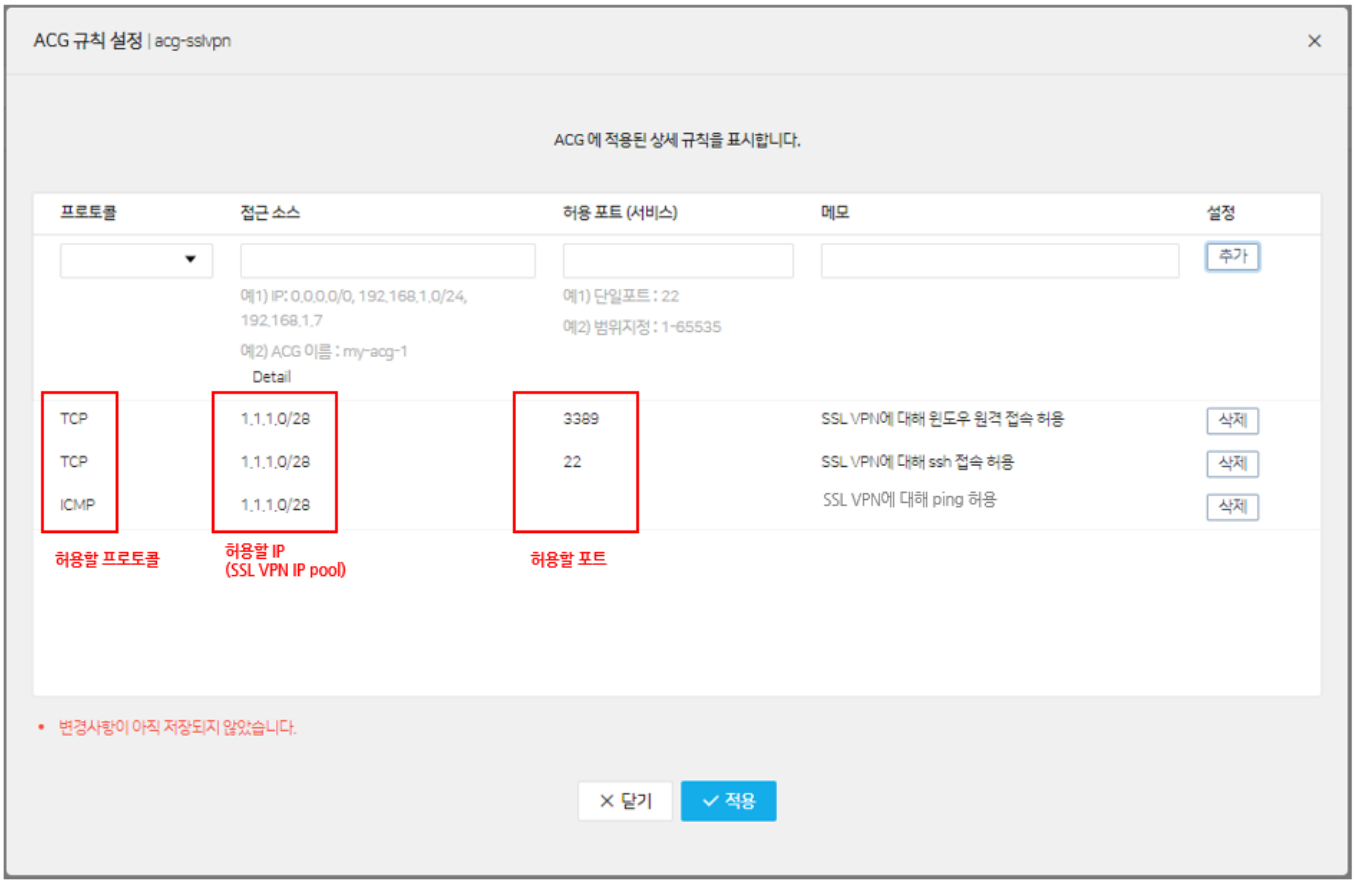
- 일반적으로 28 비트(16 개)의 IP 블록으로 할당되어 있습니다.

Step 2. 접속하고자 하는 VM의 ACG 확인



② SSL VPN 을 통해 접속하고자 하는 서버 VM 에 어떤 ACG 가 적용되어 있는지 확인합니다.

Step 3. ACG에 등록



③ **Server > ACG** 메뉴에서 SSL VPN IP pool 을 등록합니다.

참고

접속 형태에 따라 아래 프로토콜 및 포트를 ACG 에 등록합니다.

- ping: ICMP 프로토콜 등록
- ssh: TCP 프로토콜의 포트 22 등록
- 윈도우 원격 접속(RDP): TCP 프로토콜의 포트 3389 등록

SSL VPN Agent 설치

참고

다른 VPN 접속이 활성화되어 있는 상태에서는 다른 접속 환경과 충돌이 발생할 수 있으므로 VPN Agent 설치를 권장하지 않습니다.

Step 0. 네트워크 점검

SSL VPN 의 원활한 사용을 위해 방화벽, NAC 등에서 sslvpn-kr-01.ncloud.com 의 443 포트로 접근이 허용되어 있는지 확인해 주세요. 접근이 허용되어 있지 않으면 Agent 설치 및 서비스 이용에 제약이 있을 수 있습니다.

Step 1. Agent 다운로드

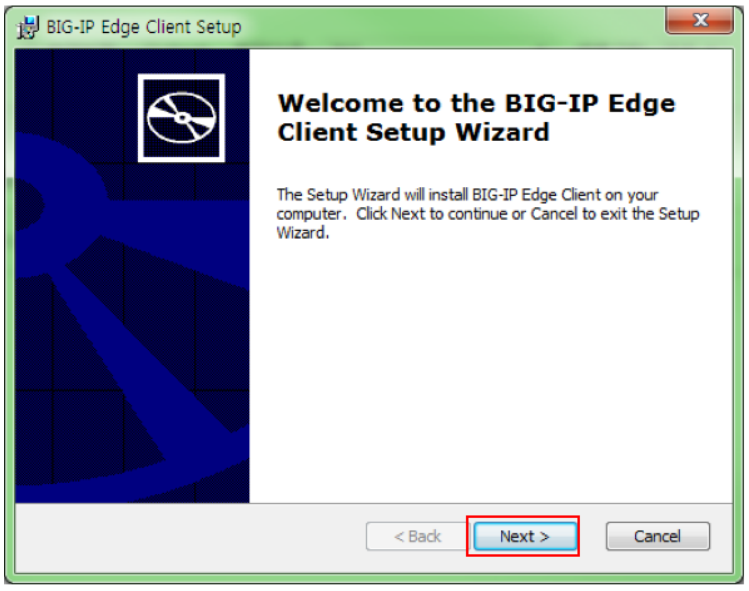
① 설명서(Windows Agent, Mac OS Agent)에서 SSL VPN Agent 를 다운로드합니다.

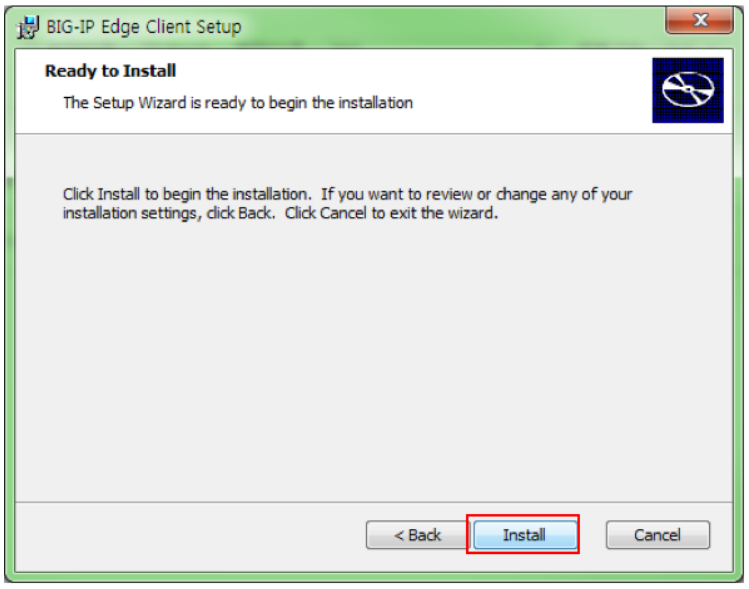
Windows 사용자용 Agent 와 MAC 사용자용 Agent 가 구분되어 있습니다.

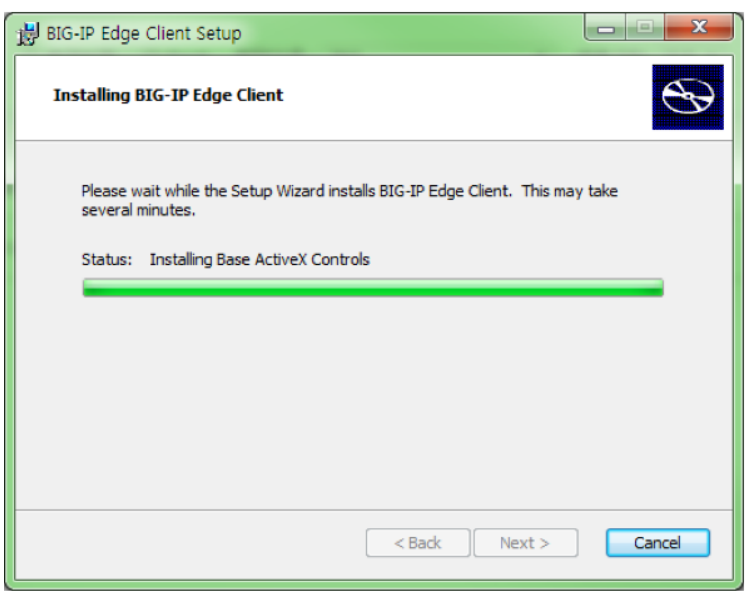
Step 2. Agent 설치

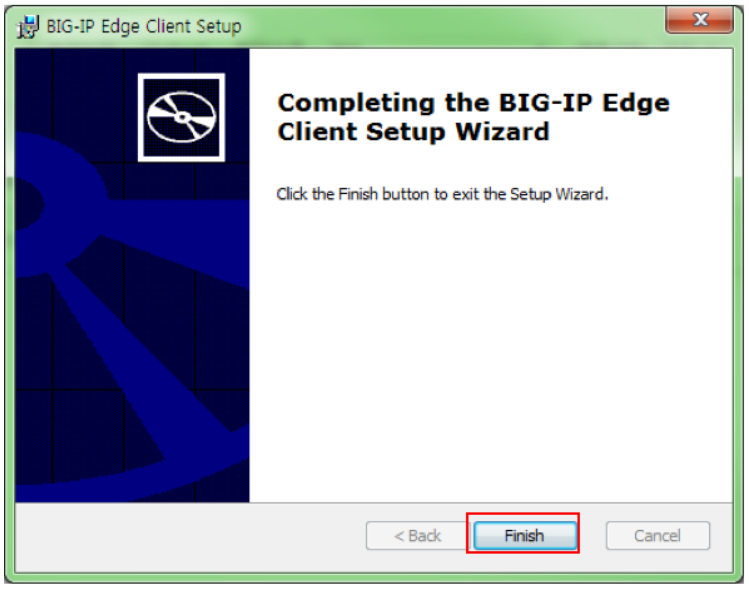
② 다운로드한 Agent 를 설치합니다.

설치는 다음 그림과 같은 순서로 진행합니다.


BIG-IP Edge Client Setup
Welcome to the BIG-IP Edge Client Setup Wizard
The Setup Wizard will install BIG-IP Edge Client on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
< Back
Next >
Cancel

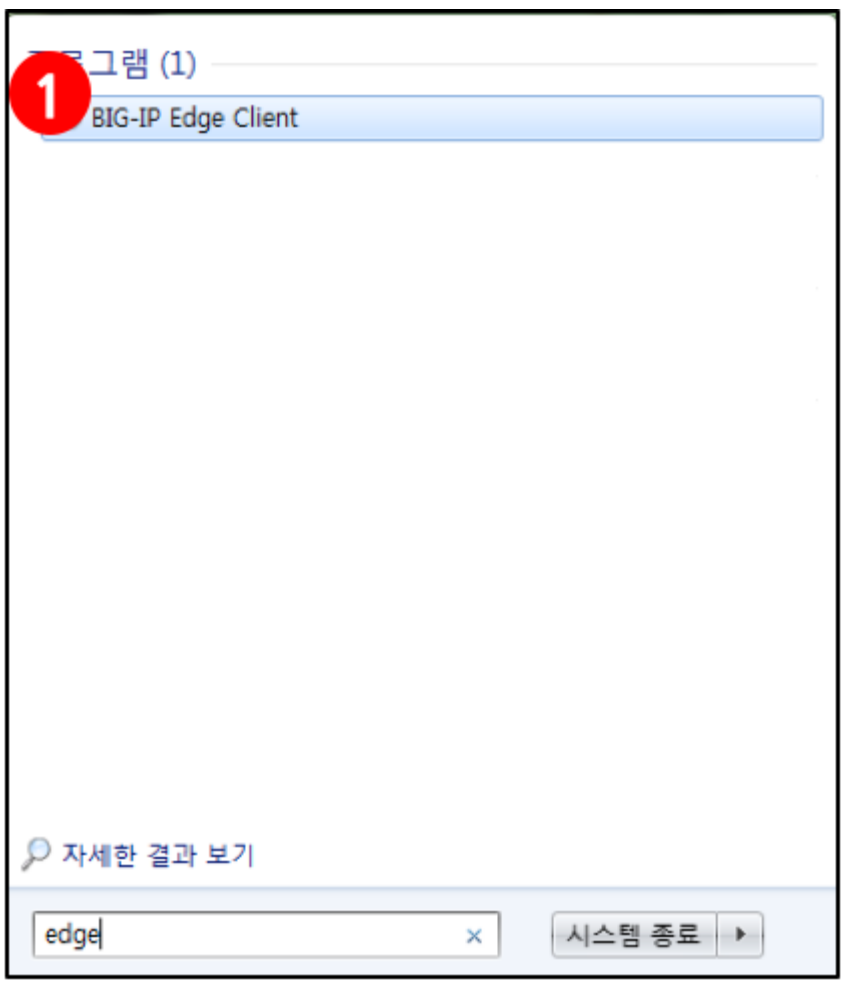

BIG-IP Edge Client Setup
Ready to Install
The Setup Wizard is ready to begin the installation
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
< Back
Install
Cancel


BIG-IP Edge Client Setup
Installing BIG-IP Edge Client
Please wait while the Setup Wizard installs BIG-IP Edge Client. This may take several minutes.
Status: Installing Base ActiveX Controls
< Back
Next >
Cancel


BIG-IP Edge Client Setup
Completing the BIG-IP Edge Client Setup Wizard
Click the Finish button to exit the Setup Wizard.
< Back
Finish
Cancel

SSL VPN Agent 접속

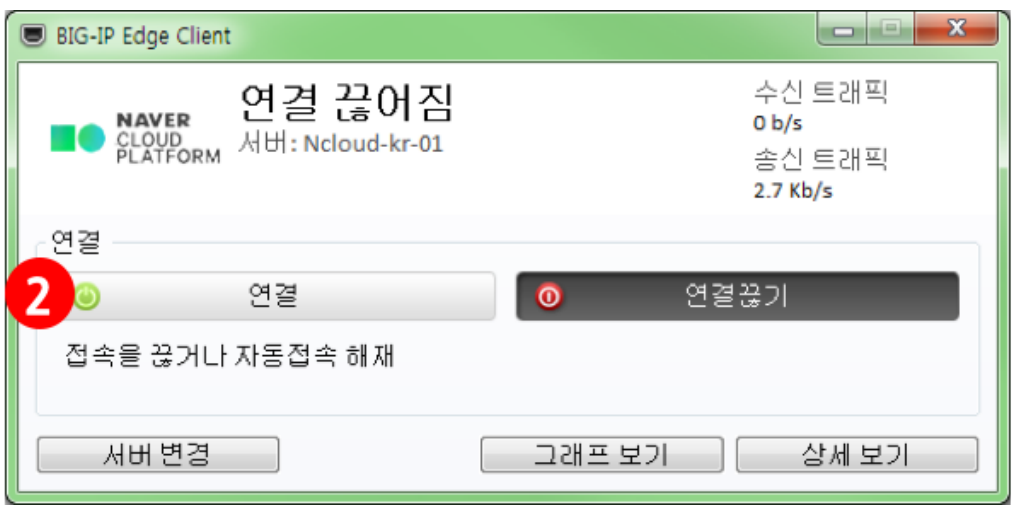
Step 1. Agent 실행



① 설치한 Agent(BIG-IP Edge Client)를 실행합니다.

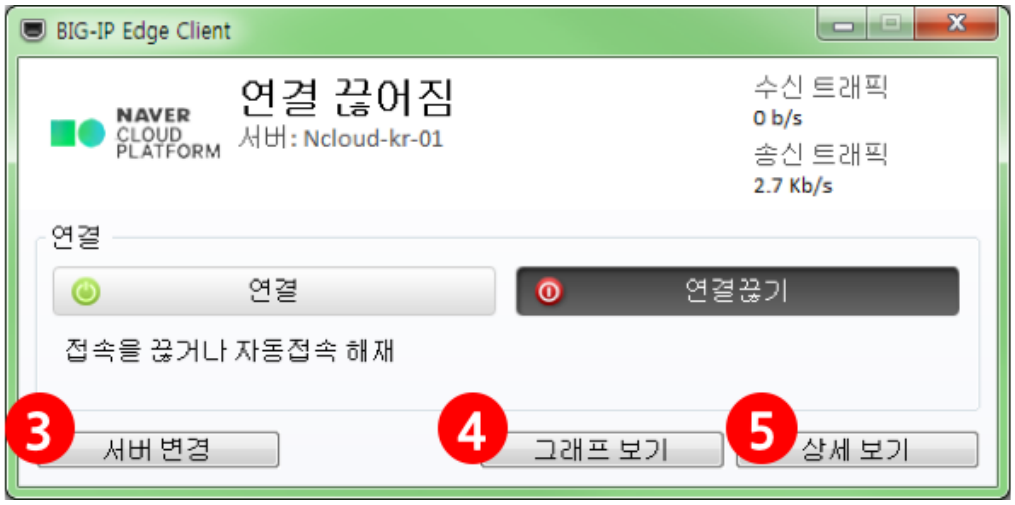
설치 시와 마찬가지로, 타 VPN 연결이 활성화되어 있는 상태에서 Agent 실행은 권장하지 않습니다. 충돌의 가능성이 있습니다.

Step 2. 접속



② **연결**을 클릭하여 접속합니다.

Step 2-1. 옵션

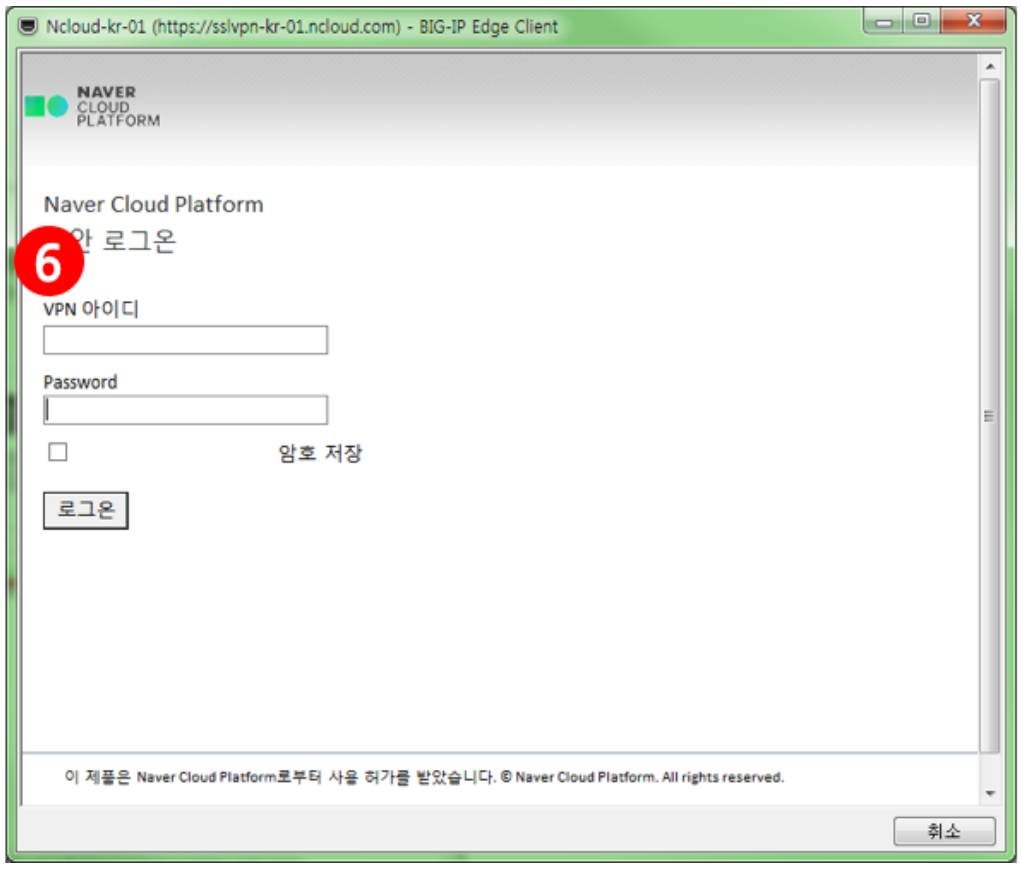


③ 서버 변경: 사용자가 Big-IP 를 이용한 다른 SSL VPN 서비스를 사용하는 경우 이 버튼을 클릭하여 접속 경로를 변경할 수 있습니다.

④ 그래프 보기/숨기기: 트래픽 사용량을 볼 수 있습니다. 인증 후에도 열람 가능합니다.

⑤ 상세 보기: 해당 접속 경로의 세부 정보를 볼 수 있습니다. 인증 후에도 열람 가능합니다.

Step 3. 인증



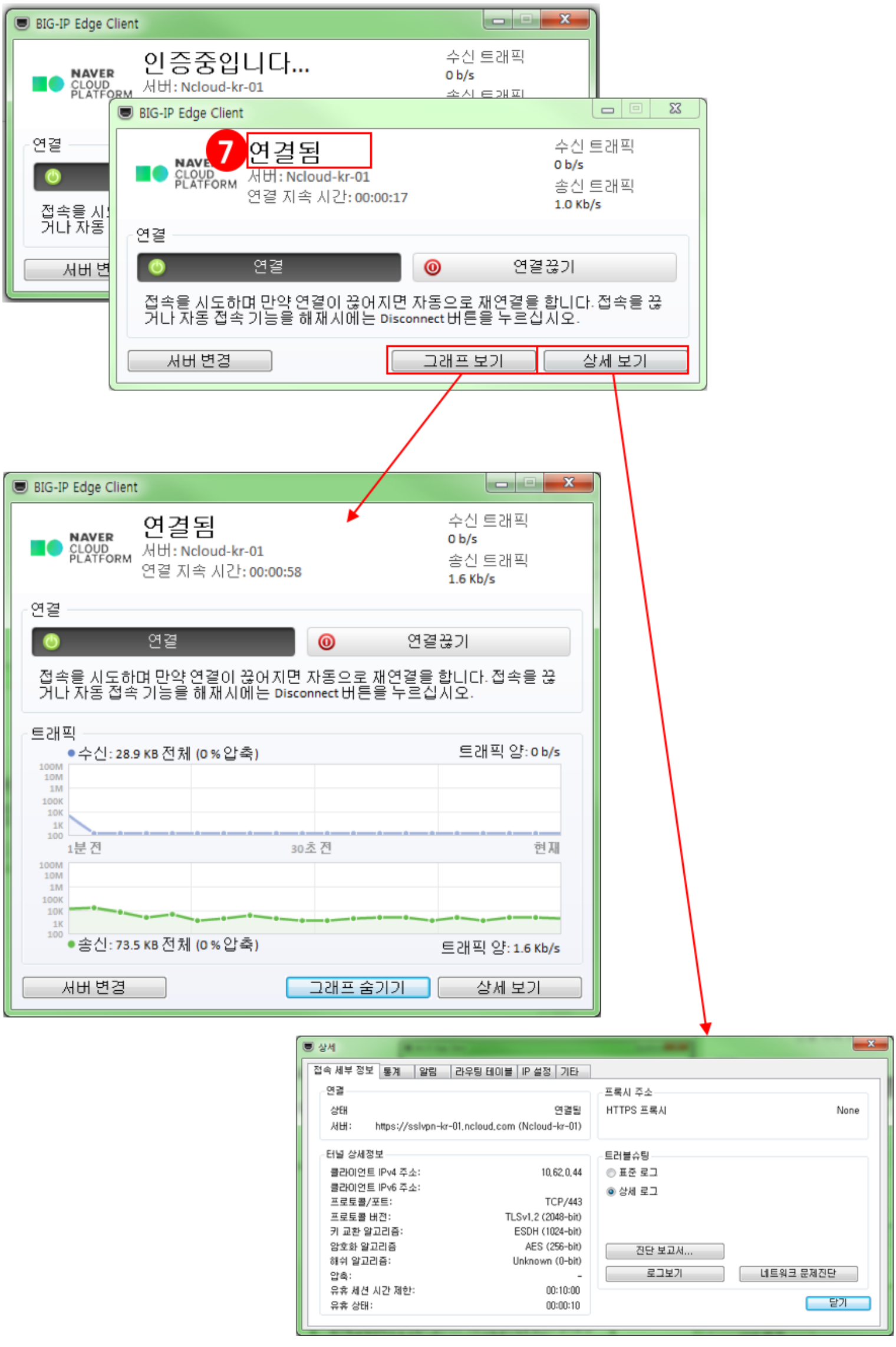
⑥ ID 와 비밀번호를 입력해 인증받습니다.

Step 3-1. 이차인증

인증방식으로 이차인증을 선택한 경우에 해당합니다.

ID 와 비밀번호를 입력하면 OTP 입력 창이 나타납니다. 잠시 기다린 후에 휴대전화번호 및 이메일로 전송된 OTP 를 입력합니다.

Step 4. 완료



⑦ 인증에 성공하면 접속이 완료됩니다.

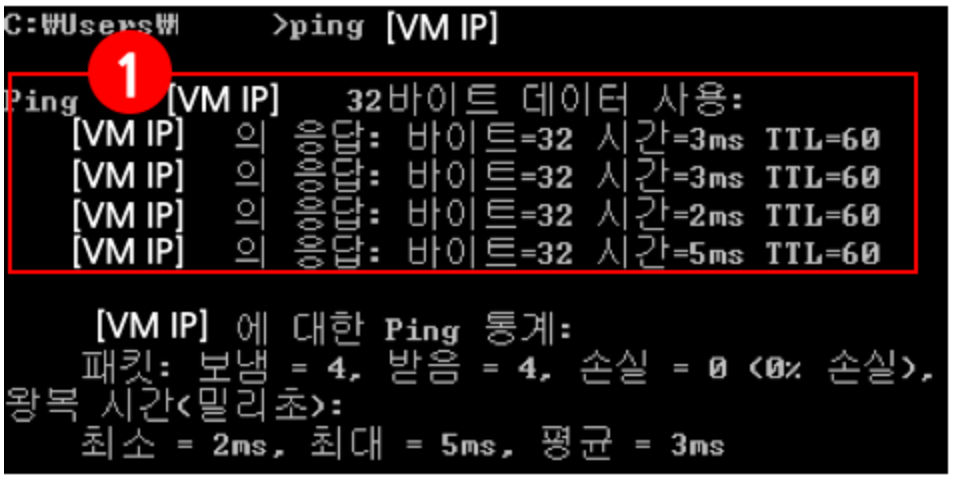
그래프 보기, 상세 보기 등을 클릭하면 더 자세한 정보를 확인할 수 있습니다.

SSL VPN Agent 접속 확인

네트워크 확인

콘솔 창을 실행합니다

- Windows 는 실행 창에서 `cmd` 입력
- macOS 는 콘솔 app 실행



① 현재 사용자의 IP 정보를 확인합니다.

- Windows 는 `ipconfig` 실행
- macOS 는 `ifconfig` 실행

② 사용자가 SSL VPN 생성 시 받은 IP pool 에 포함된 IP 를 할당받았다면 정상적으로 접속이 완료된 것입니다.

ACG 에 SSL VPN ip pool 에 대한 규칙을 등록했다면 `ping`, `ssh` 등의 명령을 통해 해당 VM 과의 통신을 확인할 수 있습니다.

참고 사항

① SSL VPN 은 모든 글로벌 리전 서버로의 접속을 제공합니다.

- 한국 리전에서 SSL VPN 상품 가입 후 글로벌 리전 서버로 접속

② SSL VPN Agent 설치 및 접속 시 주의 사항

- SSL VPN 은 로그인 시뿐만 아니라 Agent 설치 시에도 네트워크 접속을 필요로 합니다.
- 원활한 Agent 설치 및 로그인을 위해 반드시 방화벽 혹은 NAC 등에서 `sslvpn-kr-01.ncloud.com:443` 아웃바운드 트래픽이 허용되어 있는지 확인해 주세요.

연관 정보 바로가기

- 서버 생성 가이드
- ACG 사용 가이드
- 글로벌 리전 사용 가이드