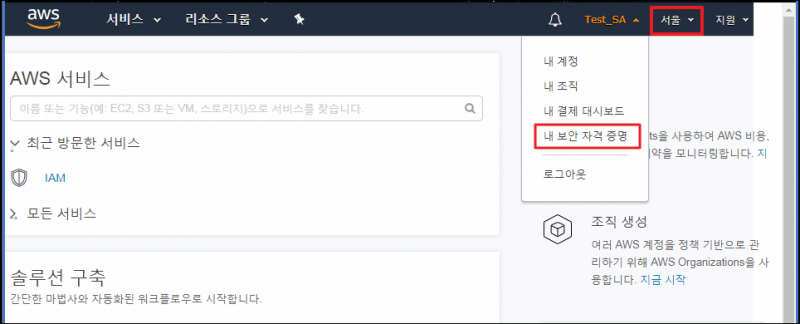
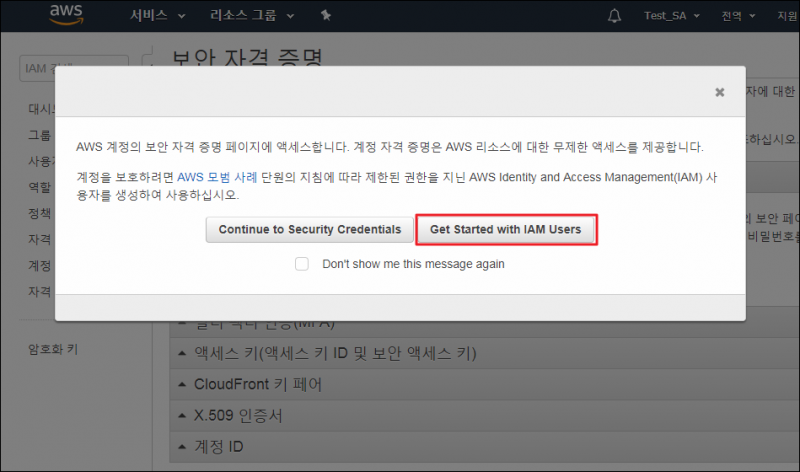
실습 IAM

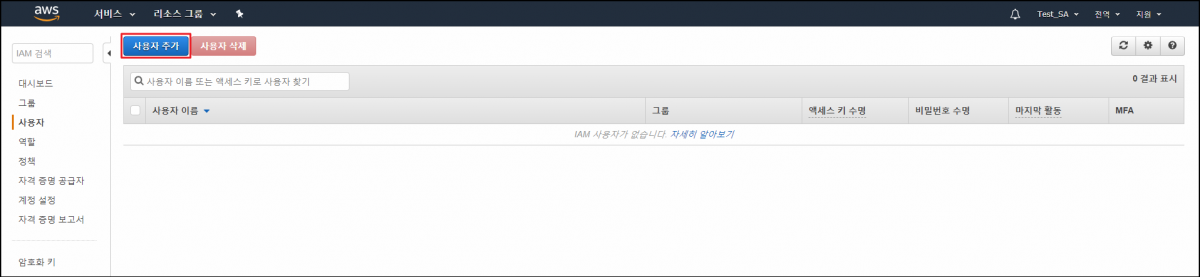
IAM 유저를 생성해보겠습니다.



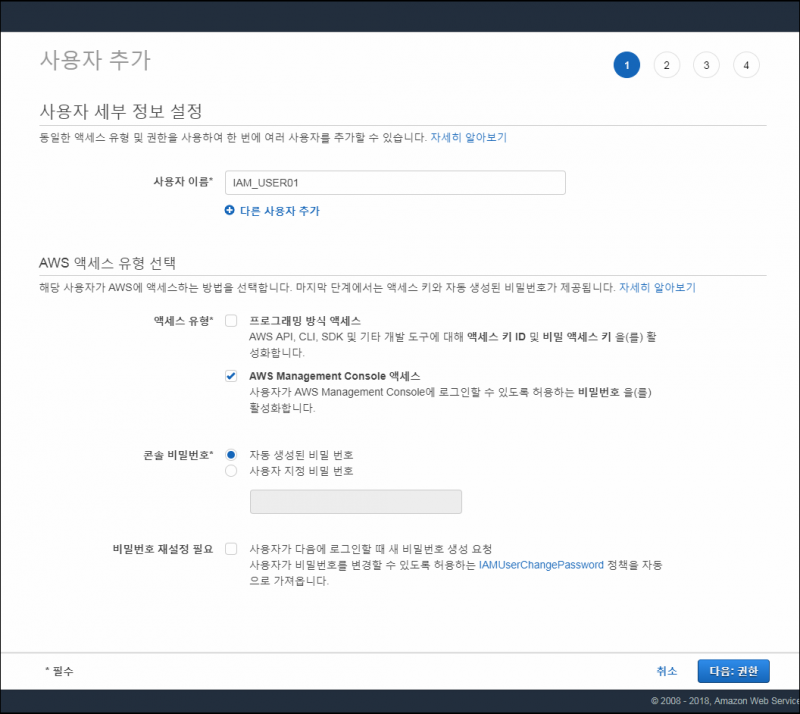
1. 내 계정을 클릭한 뒤 드롭다운에서 **[내 보안 자격 증명]**을 클릭합니다. 리전은 서울로 선택합니다. 앞으로 모든 작업은 서울 리전에서 진행하겠습니다.



2. 다음의 팝업창이 나타납니다. **[Get started with IAM Users]**를 클릭합니다. 또는 AWS Management 콘솔에서 **[서비스] -> [IAM]**으로 접속합니다.



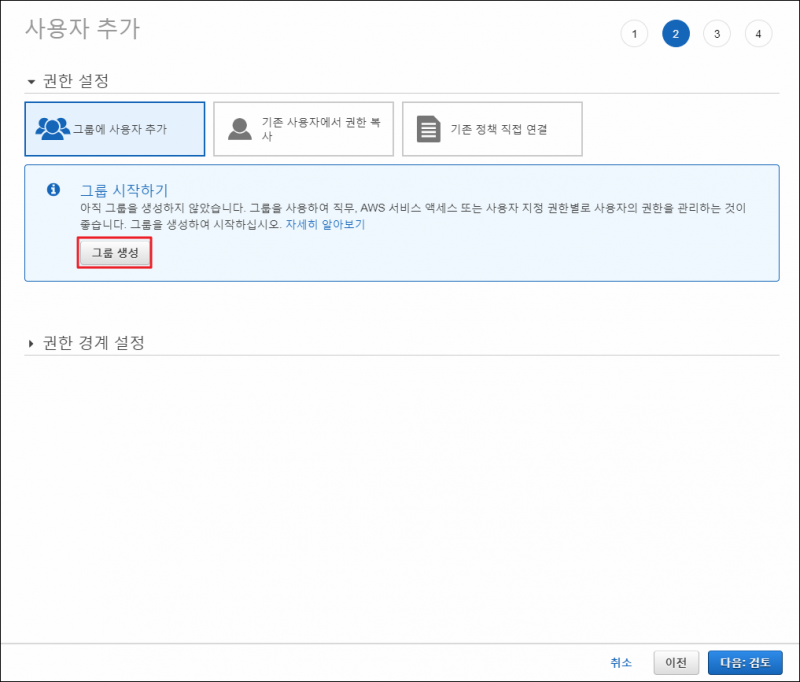
3. 사용자 탭에서 **[사용자 추가]** 를 클릭합니다.



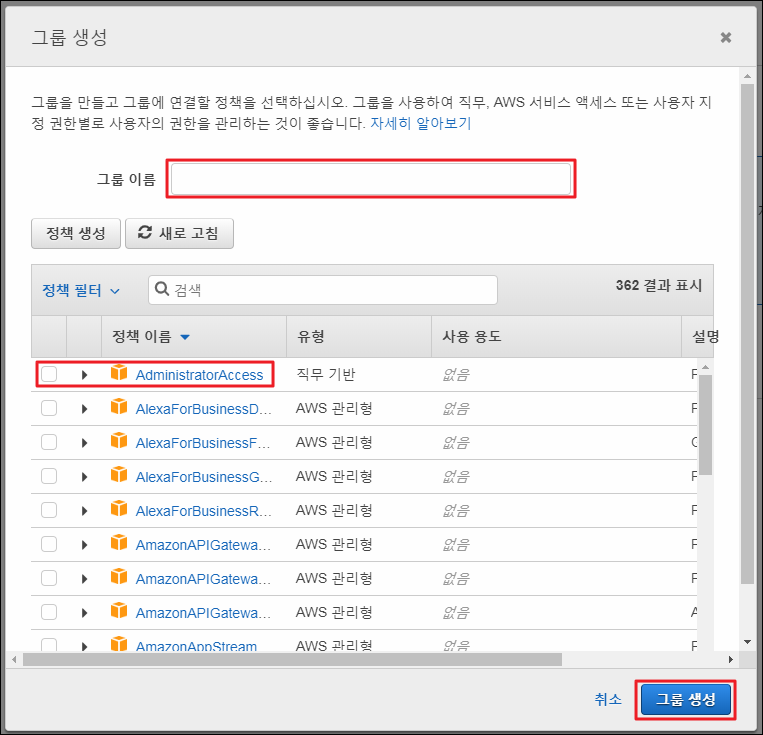
4. 신규 사용자의 이름을 원하는 대로 입력합니다. 이것은 **AWS에 로그인할 때 사용하는 이름**입니다. 하나 이상의 사용자를 동시에 추가하려면, 추가하는 각 사용자에 대해 **[다른 사용자 추가]**를 선택한 후 사용자 이름을 입력합니다. 한 번에 최대 10명까지 사용자를 추가할 수 있습니다.

사용자 이름에는 최대 64개의 알파벳, 숫자 및 더하기(+), 등호(=), 쉼표(,), 마침표(.), 앳(@), 그리고 하이픈(-) 조합을 사용할 수 있습니다. 이름은 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어 “TESTUSER”와 “testuser”라는 두 사용자를 만들 수는 없습니다.

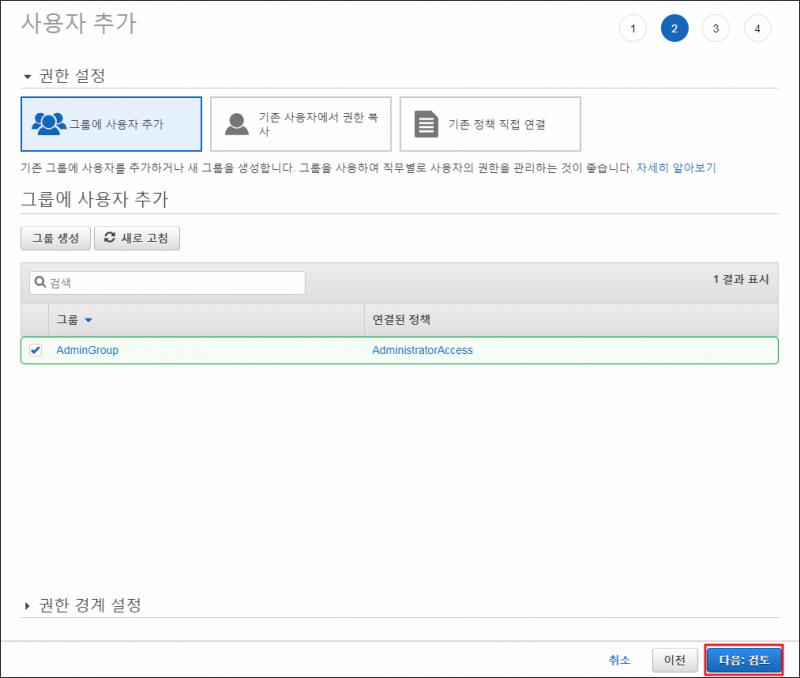
액세스 유형은 **AWS Management Console 액세스**, 콘솔 비밀번호는 **자동 생성**되도록 체크하고 **[다음]**을 클릭합니다.



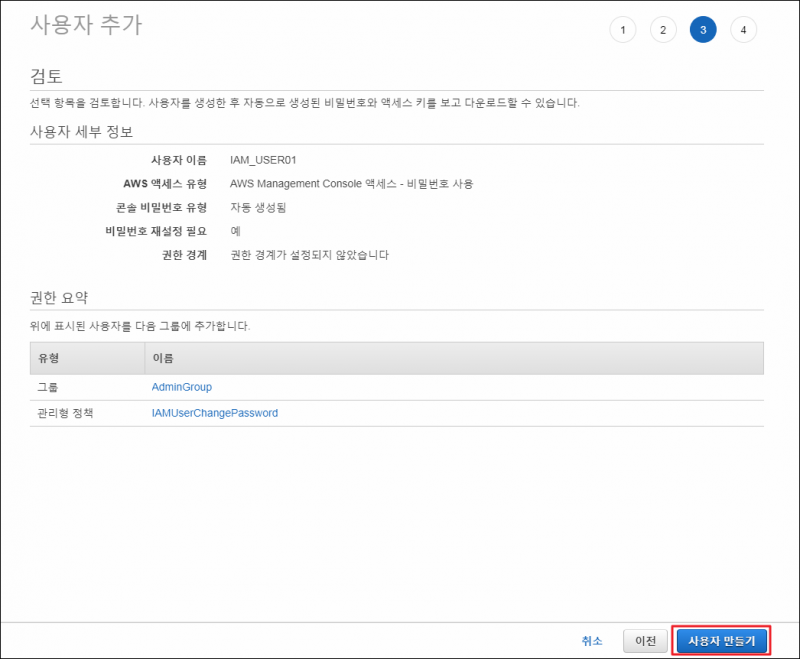
5. 권한 설정에서 그룹을 생성할 수 있습니다. 그룹에 권한을 설정하고 유저를 추가하면, 일괄적으로 관리할 수 있어 편리합니다. 유저에게서 권한을 제거하고 싶을 때는 그룹에서 사용자를 제거하면 됩니다. **[그룹 생성]**을 클릭합니다.



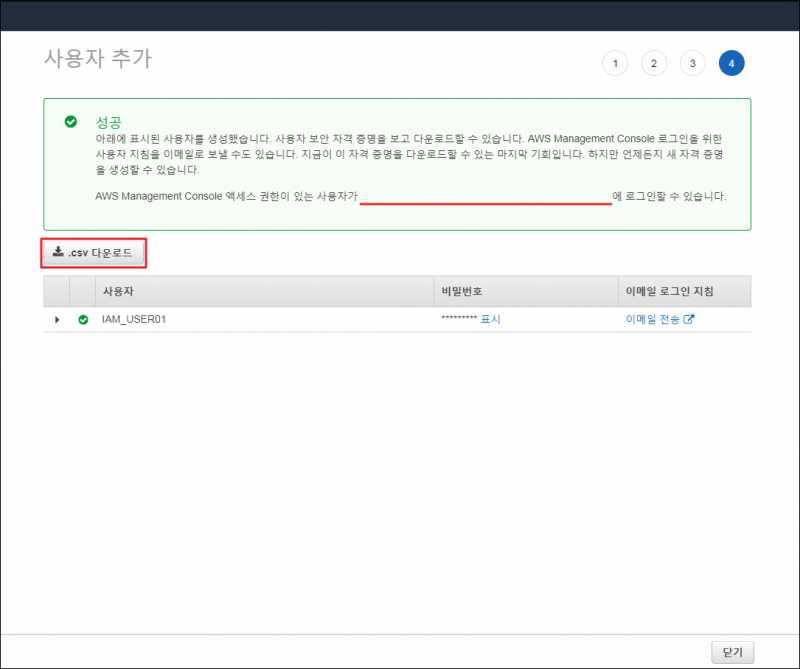
6. 그룹 이름을 만들고 ‘AdministratorAccess’를 체크합니다. 관리자 권한을 해당 그룹에 부여하는 것입니다. **[그룹 생성]**을 클릭합니다.



7. 이제 생성된 관리자 그룹에 사용자를 추가하겠습니다. **[다음: 검토]**를 클릭합니다.



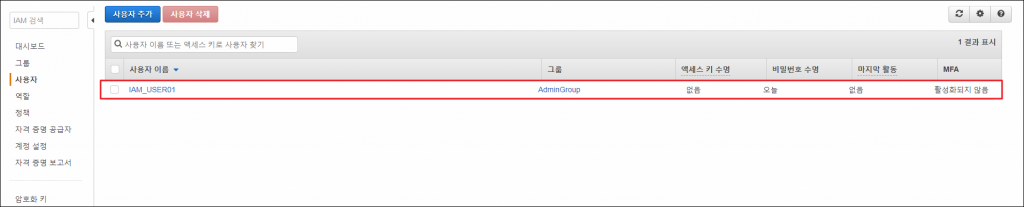
8. 사용자 세부 정보와 그룹이름을 확인하고 **[사용자 만들기]**를 클릭합니다.



9. 밑줄 친 위치에는 사용자의 콘솔 액세스 주소를 알려줍니다. 해당 주소를 통해 IAM 유저로 로그인 할 수 있습니다. 사용자의 액세스 키(액세스 키 ID와 보안 액세스 키)를 보려면 보고 싶은 각 암호와 액세스 키 옆에 있는 표시를 선택합니다. 액세스 키를 저장하려면 **[**.csv 다운로드]를 선택한 후 안전한 위치에 파일을 저장합니다.

**중요**

보안 액세스 키는 이 때만 확인 및 다운로드가 가능하기 때문에 사용자에게 AWS API를 사용하도록 하려면 이 정보를 제공해야 합니다. 사용자의 새 액세스 키 ID와 보안 액세스 키를 안전한 장소에 보관하십시오. 이 단계가 지난 후에는 보안 키에 다시 액세스할 수 없습니다.

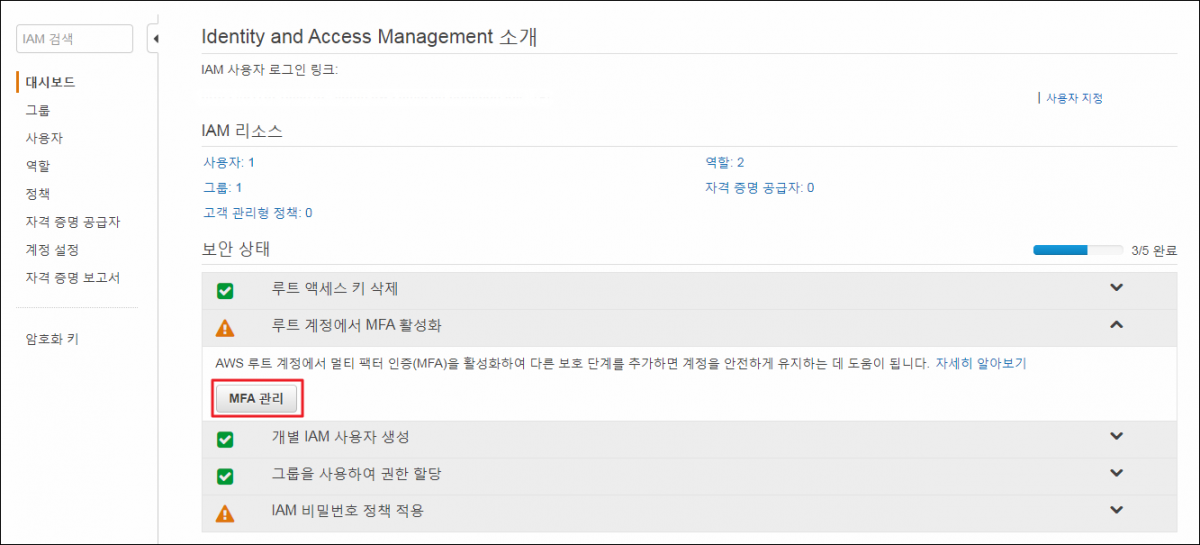


10. IAM\_USER01 사용자가 생성된 것을 볼 수 있습니다. 앞으로는 이 IAM 유저로 로그인하여 네트워크를 구성할 수 있고, 루트 계정은 안전하게 보관할 수 있습니다.

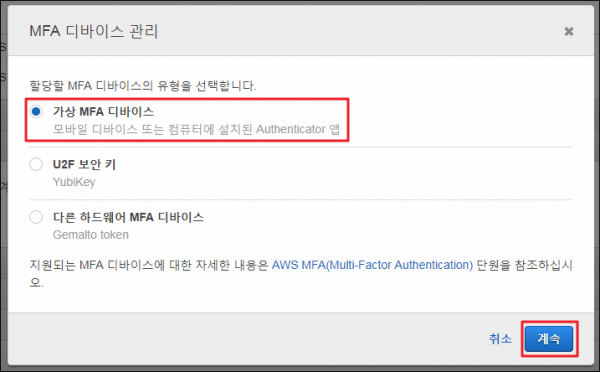
실습 2 루트 계정에 MFA를 활성화

AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 간단하며 효과적인 수단입니다. AWS 계정 및 해당 계정에 속하는 개별 IAM 사용자에 대해 AWS MFA를 활성화할 수 있습니다. 루트 계정에는 MFA를 구성하여 AWS 리소스를 보호하는 것이 좋습니다. 사용자가 AWS 웹사이트나 서비스에 액세스할 때 승인된 인증 디바이스 또는 SMS(문자 서비스) 문자 메시지의 고유한 인증 코드를 입력해야 하기 때문에 MFA는 보안을 더 강화합니다.

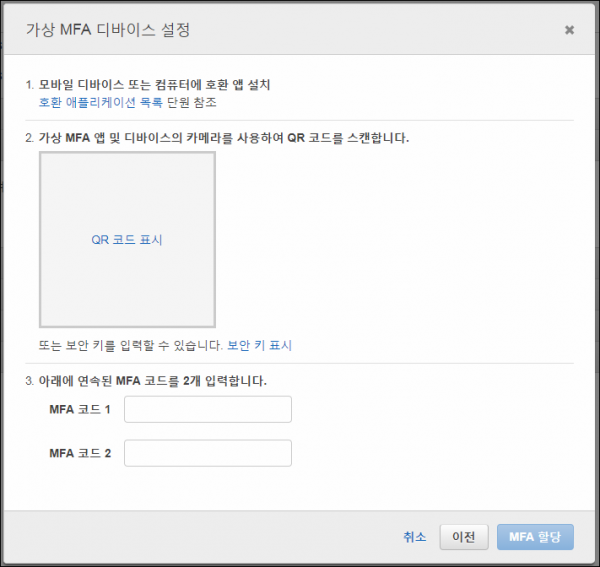
MFA는 보안 토큰 기반과 SMS 문자 메시지 기반 방식이 있으나, AWS는 2019년 2월 1일부터 SMS 기반 MFA 지원을 중단되었습니다. 실습에서는 보안 토큰 기반의 가상 MFA 어플리케이션(Google Authenticator)을 사용하겠습니다.

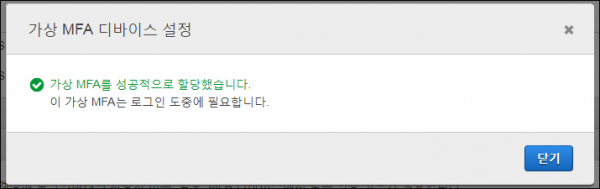
11.  IAM 콘솔에 접속합니다. 대시보드에서 **[루트 계정에서 MFA 활성화] -> [MFA 관리]**를 클릭합니다.

**12. [멀티 팩터 인증(MFA)] -> [MFA 활성화]**를 클릭합니다.

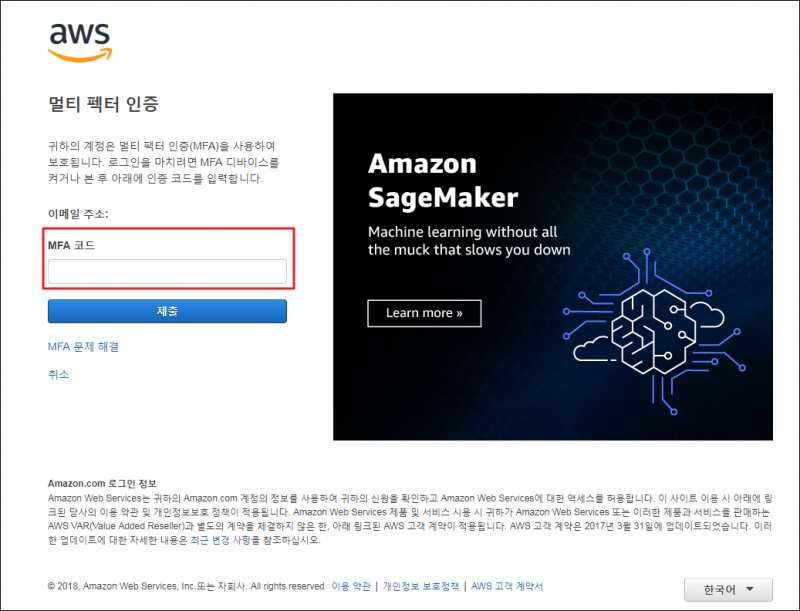


13. 가상 MFA 디바이스를 체크하고 **[계속]**을 클릭합니다.

14. 스마트폰에서 **[Google OTP]**를 설치하고 **[바코드 스캔]**을 이용하여 QR코드를 스캔하면 MFA 코드가 생성됩니다. 연속된 MFA코드 2개를 입력하고 **[MFA 할당]**을 클릭합니다.



15. 위와 같은 창이 생기면 성공적으로 MFA가 할당된 것입니다. 이제 루트 계정으로 로그인을 할 때는 MFA 인증을 추가로 거쳐야만 로그인할 수 있습니다.

16. 루트 계정으로 로그인 시 MFA 코드를 입력하라는 화면이 뜹니다.  Google OTP에서 해당 MFA 코드를 입력하면 로그인할 수 있습니다.