Add a permission의

AWS 로그인

AWS 로그인: Add a permission의

Table of Contents

AWS 로그인이란 무엇입니까?

이 설명서는 사용자 유형에 따라 Amazon Web Services (AWS)에 로그인할 수 있는 다양한 방법을 이해하는 데 도움을 줍니다. 사용자 유형과 액세스하려는 AWS 리소스에 따라 로그인하는 방법에 대한 자세한 내용은 다음 자습서 중 하나를 참조하세요.

- 에 로그인 AWS Management Console
- AWS 액세스 포털에 로그인
- 페더레이션 ID로 로그인
- 를 통해 로그인 AWS Command Line Interface
- 를 사용하여 로그인 AWS Builder ID

에 로그인하는 데 문제가 있는 경우 섹션을 AWS 계정참조하세요AWS 계정 로그인 문제 해결. 에 대한 도움말은 단원을 AWS Builder ID 참조하십시오AWS Builder ID 문제 해결. 를 생성하시겠습니까 AWS 계정? 가입합니다 AWS. 에 가입하면 사용자 또는 조직에 도움이 AWS 되는 방법에 대한 자세한 내용은 문의처를 참조하세요.

주제

- 용어
- AWS 로그인을 위한 리전 가용성
- 로그인 이벤트 로깅
- 사용자 유형 결정
- 로그인 URL 확인
- 허용 목록에 추가할 도메인
- AWS 계정 관리자를 위한 보안 모범 사례

용어

Amazon Web Services(AWS)는 일반적인 용어를 사용하여 로그인 프로세스를 설명합니다. 이러한 용어를 숙지하는 것이 좋습니다.

관리자

AWS 계정 관리자 또는 IAM 관리자라고도 합니다. 일반적으로 정보기술(IT) 직원인 관리자는 AWS 계정을 감독하는 개인입니다. 관리자는 소속 조직의 다른 구성원보다 AWS 계정 에 대해 더 높은 수준의 권한을 가집니다. 관리자는에 대한 설정을 설정하고 구현합니다 AWS 계정. 또한 IAM 또는 IAM Identity Center 사용자도 생성합니다. 관리자는 이러한 사용자에게 액세스 보안 인증과 AWS에 로그인할 수 있는 로그인 URL을 제공합니다.

Account

표준에는 AWS 리소스와 해당 리소스에 액세스할 수 있는 자격 증명이 모두 AWS 계정 포함됩니다. 계정은 계정 소유자의 이메일 주소 및 암호와 연결됩니다.

보안 인증 정보

액세스 보안 인증 또는 보안 인증 정보라고도 합니다. 인증 및 권한 부여에서 시스템은 보안 인증을 사용하여 호출하는 사용자와 요청된 액세스를 허용할지 여부를 식별합니다. 자격 증명은 사용자가 로그인하고 AWS 리소스에 액세스하기 위해 AWS 에 제공하는 정보입니다. 인간 사용자의 보안 인증에는 이메일 주소, 사용자 이름, 사용자 정의 암호, 계정 ID 또는 별칭, 확인 코드, 일회용 다중 인증(MFA) 코드가 포함될 수 있습니다. 프로그래밍 방식 액세스의 경우 액세스 키를 사용할 수도 있습니다. 가능한 경우 단기 액세스 키를 사용하는 것이 좋습니다.

보안 인증에 대한 자세한 내용은 AWS 보안 인증 정보를 참조하십시오.

> **Note**
>
> 사용자가 제출해야 하는 보안 인증의 유형은 사용자 유형에 따라 다릅니다.

기업 보안 인증

사용자가 회사 네트워크 및 리소스에 액세스할 때 제공하는 보안 인증 정보. 회사 관리자는 회사 네트워크 및 리소스에 액세스하는 AWS 계정 데 사용하는 것과 동일한 자격 증명을 사용하도록를 설정할 수 있습니다. 이러한 보안 인증 정보는 관리자 또는 지원 센터 직원이 제공합니다.

프로필

AWS Builder ID에 가입하면 프로필을 생성합니다. 프로필에는 귀하가 제공한 연락처 정보와 다중 인증(MFA) 디바이스 및 활성 세션을 관리하는 기능이 포함됩니다. 또한 개인정보 보호 및 당사가 프로필의

데이터를 처리하는 방법에 대해 자세히 알아볼 수 있습니다. 프로필 및 프로필이 AWS 계정과 관련되는 방식에 대한 자세한 내용은 AWS Builder ID 및 기타 AWS 자격 증명을(를) 참조하십시오.

루트 사용자 보안 인증 정보

루트 사용자 보안 인증은 AWS 계정을 생성하는 데 사용된 이메일 주소 및 암호입니다. 추가로 보안을 강화하기 위해 루트 사용자 보안 인증에 MFA를 추가하는 것이 좋습니다. 루트 사용자 보안 인증은 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한을 제공합니다. 루트 사용자에 대한 자세한 내용은 루트 사용자 섹션을 참조하세요.

User

사용자는 제품에 대한 AWS API 호출을 수행하거나 AWS 리소스에 액세스할 수 있는 권한이 있는 사람 또는 애플리케이션입니다. 각 사용자는 다른 사용자와 공유되지 않는 고유한 보안 인증 정보 세트를 가집니다. 이러한 보안 인증은 AWS 계정에 대한 보안 인증 정보와 별개입니다. 자세한 내용은 사용자 유형 결정 단원을 참조하십시오.

확인 코드

확인 코드는 로그인 프로세스 중에 다중 인증(MFA)을 사용하여 사용자의 신원을 확인합니다. 확인 코드의 전달 방법은 다양합니다. 이는 문자 메시지나 이메일을 통해 전송될 수 있습니다. 자세한 내용은 관리자에게 문의하세요.

AWS 로그인을 위한 리전 가용성

AWS 로그인은 일반적으로 사용되는 여러에서 사용할 수 있습니다 AWS 리전. 이러한 가용성을 통해 AWS 서비스 및 비즈니스 애플리케이션에 더 쉽게 액세스할 수 있습니다. 로그인이 지원하는 리전의 전체 목록은 AWS 로그인 엔드포인트 및 할당량을 참조하십시오.

로그인 이벤트 로깅

CloudTrail은에서 자동으로 활성화 AWS 계정 되며 활동이 발생할 때 이벤트를 기록합니다. 다음 리소스는 로그인 이벤트 로깅 및 모니터링에 대해 자세히 알아보는 데 도움이 될 수 있습니다.

- CloudTrail 로그는에 로그인을 시도합니다 AWS Management Console. 모든 IAM 사용자, 루트 사용자 및 페더레이션 사용자 로그인 이벤트는 CloudTrail 로그 파일에 레코드를 생성합니다. 자세한 내용은 AWS CloudTrail 사용자 가이드의 AWS Management Console 로그인 이벤트를 참조하세요.

- 리전 엔드포인트를 사용하여에 로그인하는 경우 AWS Management Console CloudTrail은 엔드포인트에 적합한 리전에 `ConsoleLogin` 이벤트를 기록합니다. AWS 로그인 엔드포인트에 대한 자세한 내용은 AWS 일반 참조 안내서의 AWS 로그인 엔드포인트 및 할당량을 참조하세요.
- CloudTrail이 IAM Identity Center의 로그인 이벤트를 기록하는 방법에 대한 자세한 내용은 IAM Identity Center 사용 설명서의 Understanding IAM Identity Center sign-in events를 참조하세요.
- CloudTrail이 IAM에서 다양한 사용자 자격 증명 정보를 로깅하는 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 를 사용하여 IAM 및 AWS STS API 호출 로깅 AWS CloudTrail을 참조하세요.

AWS 로그인은 네트워크 위치 및 보안 주체 자격 증명을 기반으로 콘솔 액세스를 제한할 수 있는 리소스 기반 정책 및 리소스 제어 정책을 지원합니다. 루트 사용자의 경우 암호 프롬프트가 나타나기 전에 네트워크 위치가 검증됩니다. 모든 보안 주체 유형에 대해 정책은 사전 인증 및 사후 인증 시 평가됩니다. 자세한 내용은 리소스 기반 정책 및 리소스 제어 정책을 사용하여 콘솔 액세스 제어 단원을 참조하십시오.

사용자 유형 결정

로그인 방법은 사용자 유형에 따라 다릅니다 AWS . 귀하는 AWS 계정 을 루트 사용자, IAM 사용자, IAM Identity Center의 사용자 또는 페더레이션 ID로 관리할 수 있습니다. AWS Builder ID 프로파일을 사용하여 특정 AWS 서비스 및 도구에 액세스할 수 있습니다. 다양한 사용자 유형이 아래에 나열되어 있습니다.

주제

- 루트 사용자
- IAM 사용자
- IAM Identity Center 사용자
- 페더레이션 ID
- AWS Builder ID 사용자

루트 사용자

계정 소유자 또는 계정 루트 사용자라고도 합니다. 루트 사용자는의 모든 AWS 서비스 및 리소스에 완전히 액세스할 수 있습니다 AWS 계정. 를 처음 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명은 AWS 계정 루트 사용자입니다. 계정을 생성할 때 사용한 이메일 주소와 암호를 입력하여 루트 사용자로 로그인

할 수 있습니다. 루트 사용자는 AWS Management Console로 로그인합니다. 로그인 방법에 대한 단계별 지침은 루트 사용자 AWS Management Console 로에 로그인 섹션을 참조하십시오.

> **Important**
>
> 를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

루트 사용자를 포함하는 다양한 IAM 자격 증명에 대한 자세한 내용은 IAM 자격 증명(사용자, 그룹 및 역할)을 참조하세요.

IAM 사용자

IAM 사용자는 AWS에서 생성하는 엔터티입니다. 이 사용자는 특정 사용자 지정 권한을 보유한 AWS 계정 내의 자격 증명입니다. IAM 사용자 보안 인증은 AWS Management Console에 로그인하는 데 사용되는 이름과 암호로 구성됩니다. 로그인 방법에 대한 단계별 지침은 IAM 사용자 AWS Management Console 로에 로그인 섹션을 참조하십시오.

IAM 사용자를 포함하는 다양한 IAM 자격 증명에 대한 자세한 내용은 IAM 자격 증명(사용자, 그룹 및 역할)을 참조하세요.

IAM Identity Center 사용자

IAM Identity Center 사용자는의 멤버이며 액세스 포털을 통해 여러 AWS 계정 및 애플리케이션에 대한 AWS 액세스 권한을 부여받을 AWS Organizations 수 있습니다. 소속 회사에서 Active Directory 또는 다른 ID 제공업체를 IAM Identity Center와 통합한 경우, IAM Identity Center의 사용자는 소속 기업 보안 인증을 사용하여 로그인할 수 있습니다. IAM Identity Center는 관리자가 사용자를 생성할 수 있는 ID 제공업체일 수도 있습니다. 자격 증명 공급자에 관계없이 IAM Identity Center의 사용자는 조직의 특정 로그인 URL인 AWS 액세스 포털을 사용하여 로그인합니다. IAM Identity Center 사용자는 AWS Management Console URL을 통해 로그인할 수 없습니다.

IAM Identity Center의 인간 사용자는 다음 중 하나에서 AWS 액세스 포털 URL을 가져올 수 있습니다.

- 관리자 또는 헬프데스크 직원이 보낸 메시지
- IAM Identity Center 가입 초대가 AWS 포함된의 이메일

> **Tip**
>
> IAM Identity Center 서비스에서 보내는 모든 이메일은 no-reply@signin.aws 또는 no-reply@login.awsapps.com 주소에서 발송됩니다. 이러한 발신자 이메일 주소의 이메일은 수신하고 정크 또는 스팸으로 처리하지 않도록 이메일 시스템을 구성하는 것이 좋습니다.

로그인 방법에 대한 단계별 지침은 AWS 액세스 포털에 로그인 섹션을 참조하십시오.

> **Note**
>
> 나중에 액세스할 수 있도록 AWS 액세스 포털에 대한 소속 조직의 특정 로그인 URL을 북마크에 추가하는 것이 좋습니다.

IAM Identity Center에 대한 자세한 내용은 IAM Identity Center란 무엇인가요?를 참조하세요.

페더레이션 ID

대신에, 페더레이션 ID는 Login with Amazon, Facebook, Google 또는 다른 OpenID Connect(OIDC) 호환ID 제공업체(IdP)등의 널리 알려진 외부 ID 제공업체(IdP)를 사용해 사용자가 로그인할 수 있습니다. 웹 자격 증명 페더레이션을 사용하면 인증 토큰을 받은 다음 해당 토큰을의 리소스를 사용할 권한이 있는 IAM 역할에 매핑 AWS 되는의 임시 보안 자격 증명과 교환할 수 있습니다 AWS 계정. AWS Management Console 또는 AWS 액세스 포털로 로그인 하지 않습니다. 대신 사용 중인 외부 ID에 따라 로그인 방법이 결정됩니다.

자세한 내용은 페더레이션 ID로 로그인 단원을 참조하십시오.

AWS Builder ID 사용자

AWS Builder ID 사용자는 액세스하려는 AWS 서비스 또는 도구에 특별히 로그인합니다. AWS Builder ID 사용자는 이미 있거나 생성하려는 모든 AWS 계정 를 보완합니다. AWS Builder ID는 사용자를 개인으로 나타내며, 이를 사용하여 없이 AWS 서비스 및 도구에 액세스할 수 있습니다 AWS 계정. 또한 정보를 열람하고 업데이트할 수 있는 프로필도 보유하게 됩니다. 자세한 내용은 를 사용하여 로그인 AWS Builder ID 단원을 참조하십시오.

AWS Builder ID는 AWS 전문가로부터 배우고 온라인으로 클라우드 기술을 구축할 수 있는 온라인 학습 센터인 AWS Skill Builder 구독과는 별개입니다. AWS Skill Builder에 대한 자세한 내용은 AWS Skill Builder를 참조하세요.

로그인 URL 확인

다음 URLs 중 하나를 사용하여 사용자의 종류에 AWS 따라에 액세스 AWS 합니다. 자세한 내용은 사용자 유형 결정 단원을 참조하십시오.

주제

- AWS 계정 루트 사용자 로그인 URL
- AWS 액세스 포털
- IAM 사용자 로그인 URL
- 페더레이션 ID URL
- AWS Builder ID URL

AWS 계정 루트 사용자 로그인 URL

루트 사용자는 AWS 로그인 페이지에서 AWS Management Console 에 액세스합니다https://console.aws.amazon.com/ .

이 로그인 페이지에는 IAM 사용자로 로그인하는 옵션도 있습니다.

AWS 액세스 포털

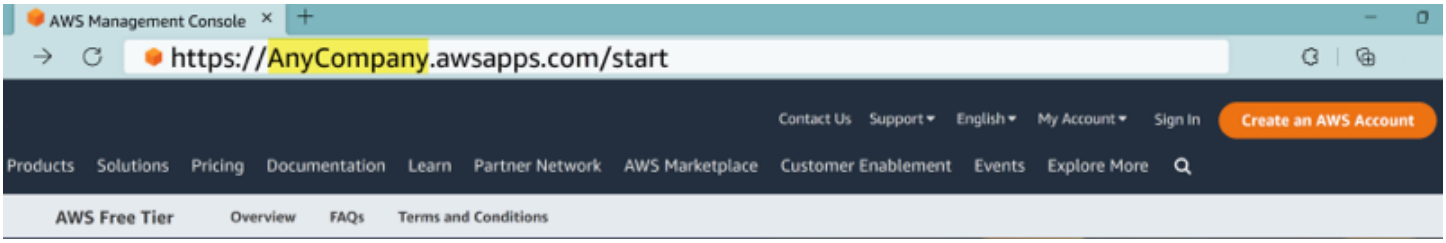
AWS 액세스 포털은 IAM Identity Center의 사용자가 로그인하고 계정에 액세스할 수 있는 특정 로그인 URL입니다. 관리자가 IAM Identity Center에서 사용자를 생성할 때 관리자는 사용자가 IAM Identity Center에 가입하라는 이메일 초대를 받을지 아니면 일회용 암호와 AWS 액세스 포털 URL이 포함된 관리자 또는 헬프데스크 직원의 메시지를 받을지 선택합니다. 특정 로그인 URL의 형식은 다음 예시와 같습니다.

```
https://d-xxxxxxxxxx.awsapps.com/start
```

또는

```
https://your_subdomain.awsapps.com/start
```

특정 로그인 URL은 관리자가 이를 사용자 지정할 수 있으므로 다양합니다. 특정 로그인 URL은 문자 D로 시작하여 그 뒤에 10개의 무작위 숫자와 문자가 올 수 있습니다. 로그인 URL에도 하위 도메인을 사용할 수 있으며, 여기에는 다음 예시와 같이 소속 회사 이름이 포함될 수 있습니다.



> **Note**
>
> 나중에 액세스할 수 있도록 AWS 액세스 포털의 특정 로그인 URL을 북마크하는 것이 좋습니다.

AWS 액세스 포털에 대한 자세한 내용은 AWS 액세스 포털 사용을 참조하세요.

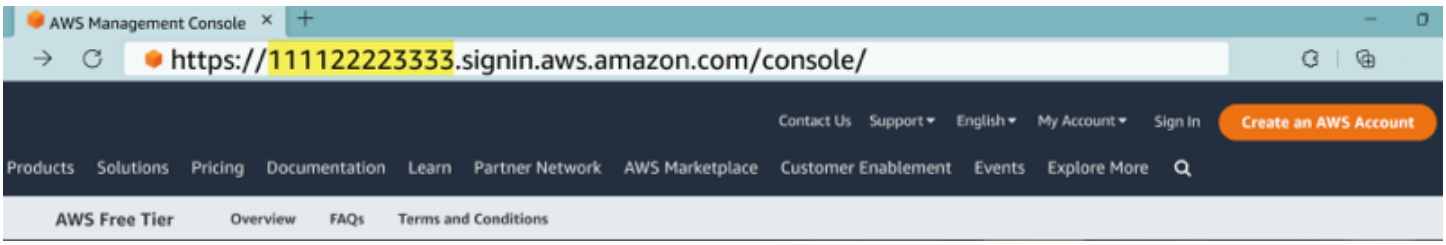
IAM 사용자 로그인 URL

IAM 사용자는 특정 IAM 사용자 로그인 URL을 AWS Management Console 사용하여에 액세스할 수 있습니다. IAM 사용자 로그인 URL은 AWS 계정 ID 또는 별칭과 `signin.aws.amazon.com/console`

IAM 사용자 로그인 URL의 예시는 다음과 같습니다.

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

계정 ID가 111122223333인 경우 로그인 URL은 다음과 같습니다.



IAM 사용자 로그인 URL AWS 계정 을 사용하여에 액세스하는 데 문제가 있는 경우 의 복원력 AWS Identity and Access Management에서 자세한 내용을 참조하세요.

페더레이션 ID URL

페더레이션 ID의 로그인 URL은 다양합니다. 외부 ID 또는 외부 ID 제공업체(idP)에서 페더레이션 ID의 로그인 URL을 결정합니다. 외부 자격 증명은 Windows Active Directory, Login with Amazon,

Facebook, 또는 Google일 수 있습니다. 페더레이션 ID로 로그인하는 방법에 대한 자세한 내용은 소속 관리자에게 문의하세요.

페더레이션 ID에 대한 자세한 내용은 웹 ID 페더레이션 정보를 참조하세요.

AWS Builder ID URL

AWS Builder ID 프로파일의 URL은 입니다https://profile.aws.amazon.com/. AWS Builder ID를 사용하는 경우 로그인 URL은 액세스하려는 서비스에 따라 달라집니다. 예를 들어, Amazon CodeCatalyst에 로그인하려면 https://codecatalyst.aws/login(으)로 이동하십시오.

허용 목록에 추가할 도메인

차세대 방화벽(NGFW) 또는 보안 웹 게이트웨이(SWG)와 같은 웹 콘텐츠 필터링 솔루션을 사용하여 특정 AWS 도메인 또는 URL 엔드포인트에 대한 액세스를 필터링하는 경우 웹 콘텐츠 필터링 솔루션 허용 목록에 다음 도메인 또는 URL 엔드포인트를 추가해야 합니다.

AWS 허용 목록에 도메인 로그인

사용자 또는 조직이 IP 또는 도메인 필터링을 구현하는 경우 AWS Management Console을(를) 사용하려면 도메인을 허용 목록에 추가해야 합니다. AWS Management Console에 액세스하려는 네트워크에서 다음 도메인에 액세스할 수 있어야 합니다.

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

AWS 허용 목록에 대한 로그인 관리 도메인

AWS CLI를 사용하여 콘솔 액세스 제어를 구성하는 경우 AWS 로그인 컨트롤 플레인 엔드포인트를 허용 목록에 추가해야 합니다. 이 엔드포인트는 정책 관리를 처리하며 이전 섹션의 콘솔 로그인 도메인과 다릅니다.

- signin.*[Region]*.api.aws

*[##]*을 호출 중인 AWS 리전으로 바꿉니다. 모든 상용 리전에서 사용할 수 있습니다. 예시: `signin.us-east-1.api.aws`.

AWS 액세스 포털 허용 목록에 대한 도메인

차세대 방화벽(NGFW) 또는 보안 웹 게이트웨이(SWG)와 같은 웹 콘텐츠 필터링 솔루션을 사용하여 특정 AWS 도메인 또는 URL 엔드포인트에 대한 액세스를 필터링하는 경우 웹 콘텐츠 필터링 솔루션 허용 목록에 다음 도메인 또는 URL 엔드포인트를 추가해야 합니다. 이렇게 하면에 액세스할 수 있습니다 AWS 액세스 포털.

다음 목록은 웹 콘텐츠 필터링 솔루션 허용 목록에 추가할 IPv4 및 듀얼 스택 도메인과 URL 엔드포인트를 제공합니다. 듀얼 스택 엔드포인트에 대한 자세한 내용은 IAM Identity Center 사용 설명서의에 대한 액세스를 허용하도록 방화벽 및 게이트웨이 업데이트를 참조하세요 AWS 액세스 포털.

IPv4 허용 목록

- *[Directory ID or alias]*.awsapps.com
- *[IAM Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com

듀얼 스택 허용 목록

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws

- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

AWS Builder ID 허용 목록에 도메인 추가

사용자 또는 조직이 IP 또는 도메인 필터링을 구현하는 경우 AWS Builder ID를 생성 및 사용하려면 도메인을 허용 목록에 추가해야 합니다. AWS Builder ID에 액세스하려는 네트워크에서 다음 도메인에 액세스할 수 있어야 합니다.

- view.awsapps.com/start
- *.portal.*.app.aws
- *.aws.dev
- *.api.aws
- *.uis.awsstatic.com
- *.console.aws.a2z.com
- oidc.*.amazonaws.com
- oidc.*.api.aws
- *.sso.amazonaws.com
- *.sso.*.amazonaws.com
- *.sso-portal.*.amazonaws.com
- sso.*.api.aws
- *.signin.aws
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

- `profile.aws.amazon.com`

AWS 계정 관리자를 위한 보안 모범 사례

새를 생성한 계정 관리자인 경우 사용자가 로그인할 때 AWS 보안 모범 사례를 따를 수 있도록 다음 단계를 AWS 계정수행하는 것이 좋습니다.

1. 아직 활성화하지 않은 경우 루트 사용자로 로그인하여 멀티 팩터 인증(MFA)을 활성화하고 IAM Identity Center에서 AWS 관리 사용자를 생성합니다. 그다음 루트 보안 인증을 보호하고 이를 일상적인 업무에 사용하지 마세요.
2. AWS 계정 관리자로 로그인하고 다음 자격 증명을 설정합니다.
   - 다른 인간 사용자를 위해 최소 권한 사용자를 생성하세요.
   - 워크로드용 임시 보안 인증을 설정합니다.
   - 장기 보안 인증이 필요한 사용 사례의 경우에만 액세스 키를 생성합니다.
3. 권한을 추가하여 해당 ID에 액세스 권한을 부여하세요. AWS 관리형 정책을 시작하고 최소 권한으로 이동할 수 있습니다.
   - AWS IAM Identity Center(AWS Single Sign-On 후속) 사용자에게 권한 세트를 추가합니다.
   - 워크로드에 사용되는 IAM 역할에 ID 기반 정책을 추가합니다.
   - 장기 보안 인증이 필요한 사용 사례의 경우에 IAM 사용자를 위한 ID 기반 정책을 추가합니다.
   - IAM 사용자에 대한 자세한 내용은 IAM의 보안 모범 사례를 참조하세요.
4. 에 로그인 AWS Management Console에 대한 정보를 저장하고 공유하세요. 이 정보는 생성한 ID 유형에 따라 다릅니다.
5. 중요한 계정 및 보안 관련 알림을 받을 수 있도록 루트 사용자 이메일 주소와 기본 계정 연락처 전화번호를 최신 상태로 유지하십시오.
   - AWS 계정 루트 사용자의 계정 이름, 이메일 주소 또는 암호를 수정하십시오.
   - 기본 계정 연락처에 액세스하거나 이를 업데이트하세요.
6. IAM의 보안 모범 사례를 검토하여 추가 ID 및 액세스 관리 모범 사례에 대해 알아보십시오.
7. 네트워크 기반 액세스 제어 구현: 로그인 리소스 기반 정책 또는 리소스 제어 정책(RCPs)을 사용하여 콘솔 로그인을 승인된 IP 주소 범위 또는 VPCs. 콘솔 프라이빗 액세스를 사용하는 환경의 경우 엔드포인트를 통해 액세스할 수 있는 계정을 제어하도록 VPC 엔드포인트 정책을 구성합니다(콘솔 프라이빗 액세스 참조). 로그인 리소스 기반 정책, RCPs 및 VPC 엔드포인트 정책은 서로 다른 적용 지점에서 계층화된 네트워크 제어를 제공합니다. 루트 사용자의 경우 로그인 정책은 권한

없는 네트워크의 액세스 시도에 대해 자격 증명 페이지를 완전히 차단합니다. 계정 잠금을 방지하기 위해 복구 액세스를 위해 제외된 보안 주체를 구성하는 것이 AWS 좋지만 이는 선택 사항입니다. 자세한 내용은 리소스 기반 정책 및 리소스 제어 정책을 사용하여 콘솔 액세스 제어 단원을 참조하십시오.

에 로그인 AWS Management Console

기본 로그인 URL(https://console.aws.amazon.com/) AWS Management Console 에서에 AWS 로그인할 때 루트 사용자 또는 IAM 사용자 중에서 사용자 유형을 선택해야 합니다. 어떤 유형의 사용자인지 잘 모르겠으면 사용자 유형 결정 섹션을 참조하세요.

루트 사용자는 무제한 계정 액세스 권한을 가지며 AWS 계정을 생성한 사람과 연관이 있습니다. 그런 다음 루트 사용자는 IAM 사용자, AWS IAM Identity Center의 사용자와 같은 다른 유형의 사용자를 생성하고 액세스 보안 인증을 할당합니다.

IAM 사용자는 특정 사용자 지정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자가 로그인하면 기본 로그인 URL `https://account_alias_or_id.signin.aws.amazon.com/console/` 대신 등 AWS 계정 또는 별칭이 포함된 AWS 로그인 URL을 사용할 수 있습니다`https://console.aws.amazon.com/` .

의 단일 브라우저에서 최대 5개의 서로 다른 자격 증명에 동시에 로그인할 수 있습니다 AWS Management Console. 이들은 서로 다른 계정 또는 동일한 계정의 루트 사용자, IAM 사용자 또는 페더레이션 역할의 조합일 수 있습니다. 자세한 내용은 AWS Management Console 시작 안내서의 Signing in to multiple accounts를 참조하세요.

자습서

- 루트 사용자 AWS Management Console 로에 로그인
- IAM 사용자 AWS Management Console 로에 로그인

어떤 유형의 사용자인지 잘 모르겠으면 사용자 유형 결정 섹션을 참조하세요.

자습서

- 루트 사용자 AWS Management Console 로에 로그인
- IAM 사용자 AWS Management Console 로에 로그인

루트 사용자 AWS Management Console 로에 로그인

를 처음 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다.

> **Important**
>
> 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증 정보가 필요한 작업을 참조하세요.

루트 사용자로 로그인하기

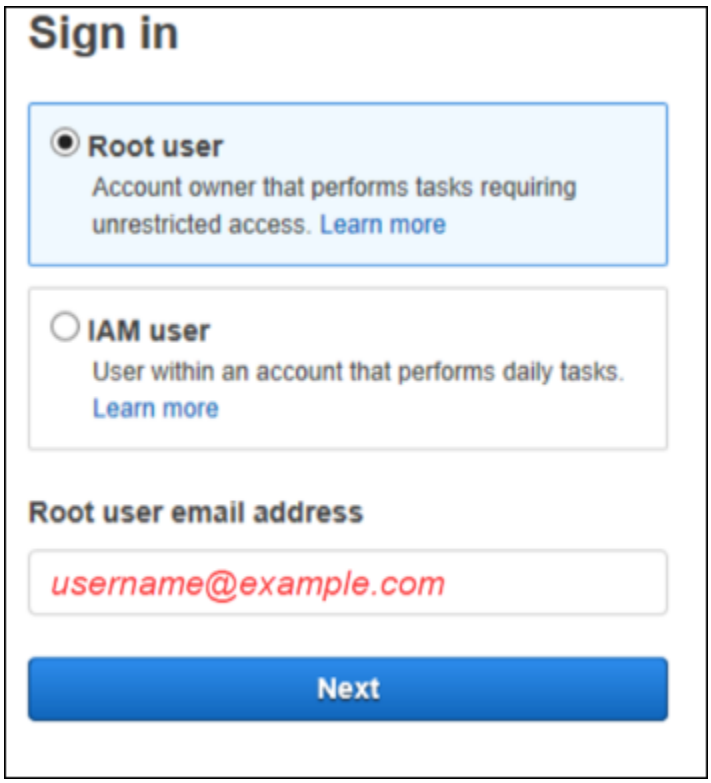
AWS Management Console에 이미 다른 자격 증명으로 로그인된 상태에서도 루트 사용자로 로그인할 수 있습니다. 자세한 내용은 AWS Management Console 시작 안내서의 Signing in to multiple accounts를 참조하세요.

AWS 계정 를 사용하여 관리되는 에는 루트 사용자 자격 증명이 없을 AWS Organizations 수 있으며, 멤버 계정에서 루트 사용자 작업을 수행하려면 관리자에게 문의해야 합니다. 루트 사용자로 로그인할 수 없는 경우 AWS 계정 로그인 문제 해결 섹션을 참조하세요.

1. AWS Management Console 에서를 엽니다https://console.aws.amazon.com/.

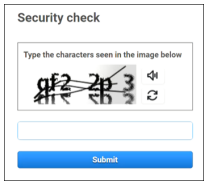
   > **Note**
   >
   > 이전에 이 브라우저를 사용하여 IAM 사용자로 로그인한 경우, 브라우저에 IAM 사용자 로그인 페이지가 대신 표시될 수 있습니다. 루트 사용자 이메일을 사용하여 로그인을 선택합니다.

2. 루트 사용자를 선택합니다.



3. 루트 사용자 이메일 주소에 루트 사용자와 연결된 이메일 주소를 입력합니다. 그다음 Next를 선택합니다.
4. 보안 검사를 완료하라는 메시지가 표시되면, 표시된 문자를 입력하여 계속하십시오. 보안 검사를 완료할 수 없는 경우 오디오를 듣거나 보안 검사를 새로 고쳐 새 문자 세트를 받으십시오.

> **Tip**
>
> 표시되거나 들리는 영숫자를 공백 없이 순서대로 입력합니다.



5. 암호를 입력합니다.

6. MFA로 인증하십시오. MFA는 루트 사용자에게 기본적으로 강제 적용됩니다. 독립형 계정과 멤버 계정의 루트 사용자의 경우, MFA를 수동으로 활성화해야 하며, 이는 강력히 권장됩니다. 자세한 내용은 AWS Identity and Access Management 사용자 가이드의 AWS 계정 루트 사용자를 위한 다중 인증을 참조하세요.

> **Tip**
>
> 보안 모범 사례로 무단 사용을 방지하려면 AWS 조직의 멤버 계정에서 모든 루트 사용자 자격 증명을 제거하는 것이 좋습니다. 이 옵션을 선택하는 경우, 멤버 계정은 루트 사용자로 로그인하거나, 암호 복구를 수행하거나, MFA를 설정할 수 없습니다. 이 경우, 관리 계정 관리자만이 멤버 계정에서 루트 사용자 자격 증명을 필요로 하는 작업을 수행할 수 있습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 멤버 계정에 대한 루트 액세스 중앙 관리를 참조하세요.

7. 로그인을 선택합니다. 가 AWS Management Console 나타납니다.

인증 후 콘솔 홈 페이지가 AWS Management Console 열립니다.

추가 정보

AWS 계정 루트 사용자에 대한 자세한 내용은 다음 리소스를 참조하세요.

- 루트 사용자에 대한 개요는 AWS 계정 루트 사용자를 참조하십시오.
- 루트 사용자 사용에 대한 자세한 내용은 AWS 계정 루트 사용자 사용을 참조하세요.

- 루트 사용자 암호 재설정 방법에 대한 단계별 지침은 에 대한 루트 사용자 암호를 잊어버렸습니다. AWS 계정 섹션을 참조하세요.

IAM 사용자 AWS Management Console 로에 로그인

IAM 사용자는 AWS 리소스와 상호 작용할 권한이 AWS 계정 있는 내에서 생성된 자격 증명입니다. IAM 사용자는 계정 ID 또는 별칭, 사용자 이름, 암호를 사용하여 로그인합니다. IAM 사용자 이름은 소속 관리자가 설정합니다. IAM 사용자 이름은 *Zhang*과 같은 친숙한 이름이거나 *zhang@example.com*과 같은 이메일 주소일 수 있습니다. IAM 사용자 이름에는 공백을 포함할 수 없지만 대문자와 소문자, 숫자, 기호 + = , . @ _ -는 포함할 수 있습니다.

> **Tip**
>
> IAM 사용자가 다중 인증(MFA)을 활성화한 경우, 인증 디바이스에 대한 액세스 권한이 있어야 합니다. 자세한 내용은 IAM 로그인 페이지에서 MFA 디바이스 사용하기를 참조하세요.

IAM 사용자로 로그인하기

AWS Management Console에 이미 다른 자격 증명으로 로그인된 상태에서도 IAM 사용자로 로그인할 수 있습니다. 자세한 내용은 AWS Management Console 시작 안내서의 Signing in to multiple accounts를 참조하세요.

1. AWS Management Console 에서를 엽니다https://console.aws.amazon.com/.
2. 기본 로그인 페이지가 표시됩니다. 계정 ID(12자리) 또는 별칭, IAM 사용자 이름, 그리고 암호를 입력하세요.

   > **Note**
   >
   > 이전에 현재 브라우저에서 IAM 사용자로 로그인한 적이 있거나 계정 로그인 URL을 사용 중인 경우, 계정 ID 또는 별칭을 입력할 필요가 없을 수 있습니다.

3. 로그인을 선택합니다.
4. IAM 사용자에 대해 MFA가 활성화된 경우 인증자를 사용하여 자격 증명을 확인해야 AWS 합니다. 자세한 내용은 AWS에서 다중 인증(MFA) 사용을 참조하세요.

인증 후 콘솔 홈 페이지가 AWS Management Console 열립니다.

추가 정보

IAM 사용자에 대한 자세한 내용은 다음 리소스를 참조하세요.

- IAM에 대한 개요는 ID 및 액세스 관리란 무엇입니까?를 참조하십시오.
- AWS 계정 IDs 대한 자세한 내용은 AWS 계정 ID 및 해당 별칭을 참조하세요.
- IAM 사용자 암호 재설정 방법에 대한 단계별 지침은 에 대한 IAM 사용자 암호를 잊어버렸습니다. AWS 계정 섹션을 참조하세요.

리소스 기반 정책 및 리소스 제어 정책을 사용하여 콘솔 액세스 제어

> **Important**
>
> 콘솔 로그인 액세스는 기본적으로 활성화됩니다. AWS 로그인은 처음에 무제한 콘솔 액세스를 허용합니다. 제한을 추가하려면 계정 또는 조직에 대한 콘솔 권한 부여 구성을 활성화합니다. 생성하는 리소스 권한 문은 콘솔 권한 부여를 활성화할 때까지 영향을 주지 않습니다. 리소스 정책을 사용하여 콘솔 액세스 제어 시작하기을(를) 참조하세요.

AWS 로그인은 AWS 로그인에 대한 액세스를 제어하는 리소스 기반 정책 및 리소스 제어 정책(RCPs)을 지원합니다. 이러한 정책을 사용하여 인증 전, 중, 후에 AWS Management Console 액세스 전반에 걸쳐 사용자 자격 증명 및 네트워크 위치를 확인합니다. 루트 사용자의 경우 이러한 정책은 자격 증명 수집이 시작되기 전에 네트워크 위치와 사용자 자격 증명을 검증합니다. 보안 인증은 액세스가 예상 네트워크에서 시작된 경우에만 입력할 수 있습니다.

AWS 로그인 리소스 기반 정책:

- 개별 AWS 계정에 적용합니다.
- 계정 관리자가 네트워크 파라미터 및 보안 주체 자격 증명을 기반으로 콘솔 액세스를 제한하도록 합니다.

리소스 제어 정책(RCPs):

- AWS Organizations를 통해 조직 전체에 적용합니다.
- 모든 멤버 계정에 중앙 집중식 거버넌스를 제공합니다.

두 정책 유형 모두 인증 전에 액세스를 확인합니다. 이렇게 하면 보안 주체가 예상치 못한 네트워크에서 로그인 페이지에 액세스하지 못하게 됩니다.

이러한 정책은 계속 적용되는 IAM 자격 증명 기반 정책을 대체하지 않습니다.

> **Note**
>
> 조직 수준 구성 및 관리를 포함한 리소스 제어 정책에 대한 전체 설명서는 AWS Organizations 사용 설명서의 리소스 제어 정책을 참조하세요. 이 섹션에서는 주로 AWS 로그인 리소스 기반 정책에 중점을 둡니다.

AWS 로그인 리소스 기반 정책 및 RCPs 다음 인증 방법에 적용됩니다.

- AWS Management Console - 콘솔 로그인 페이지를 사용하여 직접 로그인합니다.
- AWS IAM Identity Center - IAM Identity Center를 사용한 콘솔 로그인.
- 페더레이션 자격 증명 공급자 - SAML 또는 OIDC 페더레이션을 통해 로그인합니다.
- AWS 로그인과 통합된 애플리케이션 - Amazon Connect, Amazon QuickSight, AWS Health Dashboard, Amazon AppStream, Amazon Lightsail, AWS IQ.

이러한 제어는 액세스 키(AWS SDKs 또는 SigV4로 서명된 API 호출)를 사용한 프로그래밍 방식 액세스에는 적용되지 않습니다.

AWS 로그인이 리소스 기반 정책을 평가하는 방법

AWS 로그인은 콘솔 액세스 중 인증 전(인증 전 단계)과 인증 성공 후(인증 후 단계)의 두 지점에서 해당 리소스 기반 정책 또는 리소스 제어 정책(RCPs)을 평가합니다. 각 평가는 정책에 정의된 조건 키를 확인합니다. 사용 가능한 키는 단계와 작업에 따라 다릅니다. 자세한 내용은 지원되는 조건 키을 참조하세요.

> **Note**
>
> 루트 사용자 로그인의 경우 암호 프롬프트가 나타나기 전에 예기치 않은 네트워크의 액세스 시도가 차단됩니다. 이렇게 하면 예상치 못한 네트워크에서 자격 증명이 제출되지 않습니다.

인증 후 평가는 보안 주체의 자격 증명 기반 정책도 고려합니다. 관련 로그인 작업을 거부하는 IAM 정책은 네트워크 조건이 충족되더라도 콘솔 세션이 부여되지 않도록 할 수 있습니다.

지원되는 작업

AWS 로그인 리소스 정책(리소스 기반 정책 및 RCPs)은 다음 작업을 지원합니다.

`signin:Authenticate`

이는 로그인 요청이 수신될 때 평가 전용(호출할 수 없음) 작업입니다. 이는 사전 인증 검사이며 보안 주체가 로그인 페이지에 자격 증명을 입력하거나(루트 사용자, IAM 사용자) 자격 증명 공급자 또는 AWS STS(연동 사용자, 역할)의 자격 증명을 사용하여 콘솔 로그인을 시작할 때 발생합니다.

지원되는 조건 키: `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, `aws:VpcSourceIp`, `aws:RequestedRegion`, `signin:PrincipalArn`.

사용자의 자격 증명이 아직 확인되지 않았으므로이 작업에는 보안 주체 기반 전역 조건 키(`aws:PrincipalArn`, `aws:PrincipalAccount`)를 사용할 수 없습니다.

`signin:AuthorizeOAuth2Access`

OAuth 권한 부여 코드 생성에 사용됩니다. 인증에 성공하면 시스템이 OAuth 권한 부여 코드를 생성할 때이 작업이 트리거됩니다. 이때 사용자는 인증되고 보안 주체 기반 조건 키를 사용할 수 있습니다.

지원되는 조건 키: `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, `aws:VpcSourceIp`, `aws:RequestedRegion`, `aws:PrincipalArn`, `aws:PrincipalAccount`.

`signin:CreateOAuth2Token`

이 인증 후 작업은 OAuth 토큰 생성 및 교환에 사용됩니다. 이 작업은 액세스 토큰에 대한 권한 부여 코드를 사용하거나, 토큰을 새로 고치거나, 토큰 교환 작업을 수행할 때 트리거됩니다. 이 단계에서는 보안 주체 기반 조건 키를 사용할 수 있습니다.

지원되는 조건 키: `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, `aws:VpcSourceIp`, `aws:RequestedRegion`, `aws:PrincipalArn`, `aws:PrincipalAccount`.

Important

AWS 로그인 정책(리소스 기반 정책 또는 RCPs)`signin:Authenticate`을 생성할 때 정책 전반의 세 가지 작업, 즉 사전 인증 문`signin:AuthorizeOAuth2Access`과 사후 인증 문`signin:CreateOAuth2Token`을 모두 다룹니다. 콘솔 로그인은 세 작업을 순차적으로 모두 통과하는 OAuth 2.0을 사용합니다. 정책에서 작업을 생략하면 해당 단계가 보호되지 않습니다. `signin:CreateAccount`를 포함한 VPC 엔드포인트 정책 작업은 AWS Management Console 프라이빗 액세스를 참조하세요.

지원되는 조건 키

AWS 로그인은 리소스 기반 정책 및 리소스 제어 정책(RCPs)에서 다음과 같은 조건 키를 지원합니다. 다음 키를 사용하여 네트워크 위치 및 보안 주체 자격 증명을 기반으로 콘솔 액세스를 제어합니다.

- 네트워크 기반(모든 작업): `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, `aws:VpcSourceIp`, `aws:RequestedRegion`.
- 자격 증명 기반(인증 후 작업): `aws:PrincipalArn`, `aws:PrincipalAccount`.
- 서비스별(사전 인증만 해당): `signin:PrincipalArn`.

자세한 사용 규칙, 연산자 호환성, 조합 제한 및 작업별 가용성 매트릭스는 섹션을 참조하세요AWS 로그인 조건 키 참조.

리소스 정책을 사용하여 콘솔 액세스 제어 시작하기

사전 조건

- AWS CLI 설치 및 구성됨.
- 적절한 IAM 권한(참조AWS 관리형 정책: AWSSignInResourcePolicyManagement).
- 식별된 네트워크 경계(IP 범위, VPCs 또는 VPC 엔드포인트).
- 액세스를 유지할 지정된 제외 보안 주체(권장하지만 선택 사항).
- 네트워크에서 송신 필터링을 사용하는 경우 AWS 로그인 컨트롤 플레인 엔드포인트를 허용 목록에 추가합니다(참조AWS 허용 목록에 대한 로그인 관리 도메인).

> **Important**
>
> 프로덕션 환경에서 콘솔 인증을 활성화하기 전에는 긴급 복구 액세스를 유지하도록 하나 이상의 제외된 보안 주체를 구성하는 것이 AWS 좋습니다. 명시적으로 제외되지 않는 한 루트 사용자를 포함한 모든 보안 주체는 정책의 적용을 받습니다. 제외된 보안 주체는 선택 사항이지만 네트워크 조건이 예기치 않게 변경되면 보안 주체를 생략하면 계정 잠금 위험이 증가합니다.

AWS 로그인 정책의 모든 쓰기 작업에 `--region us-east-1` 대해를 지정합니다.는이 리전에서 전역적으로 정책을 AWS 복제합니다. 읽기 작업은 모든 리전을 대상으로 할 수 있습니다.

1단계: 리소스 권한 문 생성

액세스 제어를 정의하는 권한 문을 생성합니다. 모든 쓰기 작업에는가 필요합니다`--region us-east-1`(AWS 로그인 서비스는이 리전에서만 정책 변경을 수락함). 나머지 파라미터(`--source-vpc`, `--source-ip`, `--requested-region`, `--excluded-principal`)는 정책의 조건을 정의합니다. 예를 들어,는 us-west-2 리전 로그인 엔드포인트에 로그인을 제한하는 조건을 `--requested-region us-west-2` 추가합니다.

예 - 회사 VPC에 대한 액세스 제한:

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
  --client-token unique-request-id-12345 \
  --region us-east-1
```

예 - 특정 IP 범위에 대한 액세스를 제한합니다.

```
aws signin put-resource-permission-statement \
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> `--excluded-principal` 파라미터는 네트워크 제한을 우회하는 제외된 보안 주체를 지정하여 네트워크 조건이 변경될 경우 긴급 액세스를 유지합니다.

2단계: 콘솔 권한 부여 구성 활성화

다음 단계에서는 계정 또는 조직의 콘솔 로그인 프로세스에 대한 정책 적용을 활성화합니다. 리소스 권한 문은 언제든지 생성할 수 있지만 콘솔 권한 부여가 활성화될 때까지 평가되지 않습니다.

> **Warning**
>
> 콘솔 권한 부여를 활성화하면 네트워크 조건이 잘못 구성되거나 기존 서비스 제어 정책(SCP) 또는 리소스 제어 정책(RCP)이 AWS 로그인 작업을 거부하는 경

우 보안 주체가 잠길 수 있습니다. 콘솔 인증을 활성화하기 전에 권한 문이 올바른지 확인하고 , 또는 `signin:Authenticate`를 거부하는 SCP 또는 RCP를 제거`signin:AuthorizeOAuth2Access`하거나 조정합니다`signin:CreateOAuth2Token`.

독립 실행형 계정의 경우:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

AWS Organizations 경우:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
  --region us-east-1
```

구성을 확인합니다.

```
aws signin get-console-authorization-configuration \
  --target-id <your-target-id> \
  --region <your-region>
```

콘솔 권한 부여 구성을 삭제합니다.

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

3단계: 정책 확인

모든 권한 설명을 나열합니다.

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

전체 통합 정책을 검색합니다.

```
aws signin get-resource-policy \
  --region <your-region>
```

get-resource-policy 명령은 모든 권한 문으로 구성된 전체 리소스 기반 정책을 반환합니다. 콘솔 액세스를 테스트하기 전에이 정책을 검토하여 의도한 액세스 제어를 반영하는지 확인합니다.

리전별 가용성

콘솔 권한 부여 APIs 모든 AWS 상용 리전에서 사용할 수 있습니다. 운영하는 모든 리전에서 이러한 APIs 호출할 수 있습니다.

> **Important**
>
> us-east-1 리전에서 쓰기 작업(put-console-authorization-configuration, put-resource-permission-statement, delete-console-authorization-configuration, delete-resource-permission-statement)을 수행해야 합니다. 에서 생성된 정책은 전역적으로 us-east-1 자동으로 복제됩니다. 읽기 작업(get-console-authorization-configuration, list-resource-permission-statements, get-resource-policy)은 모든 리전에서 수행할 수 있습니다.

정책 구조 이해

AWS 로그인 정책에는 콘솔 로그인 흐름의 다양한 단계를 보호하는 두 개의 문이 포함되어 있습니다.

- 사전 인증 문(작업: **signin:Authenticate**): 인증이 완료되기 전에 로그인 요청이 수신될 때 평가됩니다. 보안 주체의 자격 증명aws:PrincipalArn이 확인되지 않았기 때문에이 단계에서는 전역 키를 사용할 수 없습니다. 이 단계에서signin:PrincipalArn는 네트워크 제한에서 특정 보안 주체를 제외할 수 있습니다. 이 단계에서는 네트워크 기반 조건 키를 평가할 수 있습니다.
- 인증 후 문(작업: **signin:AuthorizeOAuth2Access**, **signin:CreateOAuth2Token**): OAuth 토큰 교환 중에 인증 후 평가됩니다. aws:PrincipalArn를 사용하여 특정 보안 주체를 제외합니다. 이 단계에서는 모든 네트워크 기반 및 자격 증명 기반 조건 키를 평가할 수 있습니다.

콘솔 로그인은 세 작업을 순차적으로 모두 통과하는 OAuth 2.0을 사용하기 때문에 두 명령문이 모두 필요합니다. 문이 하나뿐인 정책은 다른 단계는 보호되지 않습니다. signin:PrincipalArn는 루트 사용자, IAM 사용자 및 역할 보안 주체 유형을 지원합니다.는 모든 보안 주체 유형(루트 사용자, IAM 사용자, 페더레이션 사용자, 역할)을 aws:PrincipalArn 지원합니다.

정책 예시

예제 1: 네트워크 경계 및 제외된 보안 주체가 있는 RCP

다음 리소스 제어 정책(RCP)은 조직 내 모든 계정의 회사 네트워크 외부에서 AWS Management Console 로그인하는 것을 거부합니다. 지정된 제외 보안 주체는 긴급 액세스에서 제외됩니다. VPC IDs는 리전 내에서만 고유하므로 정책에는 VPC 기반 액세스를 예상 리전에 고정시키는 세 번째 문이 포함됩니다.

`EnforceNetworkPerimeterPreAuth` 문은 `signin:PrincipalArn`를 사용하여 사전 인증 단계에서 제외된 보안 주체를 제외합니다. `EnforceNetworkPerimeterPostAuth` 문은 `aws:PrincipalArn`를 사용하여 인증 후 제외된 보안 주체를 제외합니다. `EnforceSourceVPCRegion` 문은 요청 리전이 VPC 리전과 일치하는지 확인하여 지정된 VPC의 예상 리전에 대한 액세스를 제한합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
```

```
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
        }
      }
    }
  ]
}
```

이 정책은 다음과 같습니다.

- 요청이 회사 IP 범위 또는 회사 VPC에서 시작되지 않는 한 로그인 페이지에 대한 액세스를 거부합니다. 제외된 루트 계정 및 IAM 사용자는 `signin:PrincipalArn` (사전 인증)을 통해 제외됩니다.
- 기업 IP 범위 또는 VPC가 아닌 한 OAuth 토큰 교환을 거부합니다. 제외된 루트 계정, IAM 사용자 및 역할은 `aws:PrincipalArn` (인증 후 글로벌 키)를 통해 제외됩니다.
- 요청이 지정된 VPC에서 왔지만 리전이 일치하지 않는 경우 액세스가 거부됩니다. AWS VPC IDs는 리전 내에서 고유하며 동일한 VPC ID가 다른 리전에 존재할 수 있습니다.
- RCP로 구성된 경우 AWS 조직 전체에 전역적으로 적용됩니다.

예제 2: 제외된 보안 주체가 있는 IP 기반 액세스에 대한 리소스 기반 정책

다음 리소스 기반 정책은 지정된 IP 범위 외부에서 요청하는 모든 보안 주체에 대한 콘솔 액세스를 거부하며 제외된 보안 주체는 제외됩니다. 정책에는 서비스별 `signin:PrincipalArn` 키를 사용하는 사전 인증 문과 전역 `aws:PrincipalArn` 키를 사용하는 사후 인증 문이라는 두 가지 문이 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
```

```
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

이 정책은 다음과 같습니다.

- IP 범위에서 연결하지 않는 한 모든 보안 주체에 대한 액세스를 거부합니다<my-corporate-cidr>.
- (사전 인증) 및 signin:PrincipalArn (사aws:PrincipalArn후 인증)를 사용하여 네트워크 제한에서 제외된 보안 주체를 제외합니다.
- 리소스 기반 정책이 구성된 특정 계정에만 적용됩니다(로 식별됨<my-aws-account-id>).

모범 사례

긴급 복구 액세스를 위해 제외된 보안 주체 구성

AWS 에서는 프로덕션 환경에서 콘솔 권한 부여 정책을 적용하기 전에 제외된 사용자를 하나 이상 구성할 것을 권장합니다. 사전 인증 단계에서 signin:PrincipalArn 조건 키는 루트 사용자, IAM 사용자 및 역할 보안 주체를 제외합니다. 인증 후 단계에서 aws:PrincipalArn 조건 키는 모든 보안 주체 유형(루트 사용자, IAM 사용자, 페더레이션 사용자, 역할)을 제외합니다.

제외된 보안 주체는 선택 사항이지만 생략하면 네트워크 조건이 예기치 않게 변경되거나 정책이 잘못 구성된 경우 계정 잠금 위험이 증가합니다.

권장 제외-보안 주체 구성 단계:

1. 제외된 IAM 역할(예: BreakGlassRole)을 생성합니다.

2. 제외된 역할의 경우 역할 신뢰 정책에 MFA가 필요합니다.
3. 제외된 자격 증명에 긴급 복구에 필요한 최소 권한만 부여합니다.
4. 사전 인증(`signin:PrincipalArn`) 및 사후 인증(`aws:PrincipalArn`) 정책 설명 모두에 제외된 보안 주체 ARN을 포함합니다.
5. 복구 절차를 문서화하고 외부에 안전하게 저장합니다 AWS.
6. 제외된 보안 주체 액세스를 주기적으로 테스트하여 필요할 때 작동하는지 확인합니다.

복구 액세스 경로 유지

위에서 설명한 제외된 보안 주체 외에도 콘솔 권한 부여 정책이 예기치 않게 로그인을 차단하는 경우 대체 액세스 방법을 사용할 수 있는지 확인합니다.

- 역할 기반 프로그래밍 방식 액세스: 콘솔 권한 부여 정책은 대화형 콘솔 로그인에만 적용됩니다. SigV4로 서명된 API 요청에는 적용되지 않습니다. 프로그래밍 방식 액세스(예: 기존 액세스 키, 교차 계정 역할)가 있는 경우 이를 사용하여 제한 정책을 호출`signin:DeleteConsoleAuthorizationConfiguration`하고 제거합니다. 자격 증명에는 `signin:DeleteConsoleAuthorizationConfiguration` 권한(`AWSSignInResourcePolicyManagement`관리형 정책에 포함됨)이 포함되어야 합니다.는 장기 IAM 사용자 액세스 키에 대한 임시 자격 증명을 AWS 권장합니다. 멤버 계정의 경우 관리 계정 관리자는 멤버 계정(`aws sts assume-role`)`OrganizationAccountAccessRole`에서를 수임하여 이러한 임시 자격 증명을 얻을 수 있습니다.
- AWS 지원 복구: 루트 사용자 계정 이메일 및 전화번호를 최신 상태로 유지합니다. excluded-principal 및 프로그래밍 방식 액세스를 모두 사용할 수 없는 경우 AWS Support는 자격 증명 확인 후 복구 포털 링크를 제공할 수 있습니다. 전체 복구 프로세스는 콘솔 권한 부여를 활성화한 후 계정이 잠겼습니다. 섹션을 참조하세요.

프로덕션 배포 전 테스트

AWS 에서는 정책이 계정에 미치는 영향을 철저히 테스트하지 않고 조직의 루트에 제한적인 RCPs를 연결하지 않을 것을 권장합니다. 대신 계정을 한 번에 하나씩 또는 최소한 작은 숫자로 이동할 수 있는 OU를 생성하여 실수로 사용자를 키 계정에서 잠그지 않도록 합니다.

테스트 워크플로:

1. 기본 네트워크 제한을 사용하여 단일 권한 문을 생성합니다.
2. 비프로덕션 계정에서 콘솔 권한 부여를 활성화합니다.

3. 허용된 네트워크와 거부된 네트워크 모두에서 콘솔 액세스를 테스트합니다.
4. Amazon CloudTrail 로그를 검토하여 정책 평가 동작을 확인합니다.
5. 제외된 보안 주체를 사용하여 액세스를 테스트합니다.
6. 추가 네트워크 및 계정으로 점진적으로 확장합니다.
7. 프로덕션 계정에 적용하기 전에 모니터링합니다.

defense-in-depth를 사용한 설계

광범위한 보안 전략 내에서 AWS 로그인 리소스 기반 정책 및 리소스 제어 정책을 하나의 계층으로 사용합니다. AWS 로그인 정책은 네트워크 위치 및 보안 주체 자격 증명에 따라 콘솔 액세스를 제한합니다. 다른 정책 유형과 결합하여 포괄적인 액세스 제어를 생성합니다.

- AWS 로그인 정책(리소스 기반 정책 및 RCPs): 인증 전, 중, 후에 네트워크 위치 및 보안 주체 자격 증명을 기반으로 콘솔 액세스를 제한합니다.
- IAM 정책: 로그인 후 사용자가 수행할 수 있는 작업을 제어합니다.
- 서비스 제어 정책(SCPs): 모든 보안 주체에 조직 전체의 권한 가드레일을 적용합니다.
- VPC 엔드포인트 정책: VPC 엔드포인트를 통해 액세스할 수 있는 서비스 및 계정을 제어합니다.

지속적으로 모니터링 및 감사

AWS CloudTrail 는 모든 AWS 로그인 정책 평가 및 구성 변경을 자동으로 기록합니다. 최대 90일 동안 CloudTrail 이벤트 기록에서 이러한 이벤트를 봅니다. 보존 기간을 늘리려면 추적을 생성하여 Amazon S3에 이벤트를 전송합니다(추적 생성 참조). 실시간 알림의 경우 AWS 로그인 이벤트와 일치하는 Amazon EventBridge 규칙을 생성하거나, 지표 필터 기반 경보를 위해 CloudWatch Logs 로그 그룹에 전달하도록 추적을 구성하거나, 기존 SIEM 솔루션에 이벤트를 전달합니다.

사용 사례

네트워크 경계 적용

기업 VPCs. 사용자가 신뢰할 수 있는 네트워크 위치에서만 로그인할 수 있도록 개별 계정에 대한 리소스 기반 정책 또는 조직 전체의 적용을 위한 리소스 제어 정책(RCPs)을 사용하여 퍼블릭 또는 신뢰할 수 없는 네트워크에서의 무단 액세스를 방지합니다.

예제 시나리오: 회사가 회사 네트워크 또는 승인된 AWS VPCs에서 시작하려면 모든 콘솔 액세스가 필요합니다. 단일 계정에 대한 리소스 기반 정책 또는 조직 전체의 RCP를 구성하여 긴급 관리자의 긴급 복구 액세스를 유지하면서 다른 모든 네트워크의 액세스를 거부합니다.

규정 준수 요구 사항

네트워크 기반 액세스 제어에 대한 규제 요구 사항을 충족합니다. 많은 규정 준수 프레임워크에서는 조직이 네트워크 위치에 따라 민감한 시스템에 대한 액세스를 제한해야 합니다. AWS 로그인 정책은 이러한 요구 사항 준수를 입증하는 감사 가능하고 시행 가능한 제어를 제공합니다.

예제 시나리오: 금융 서비스 회사는 승인된 네트워크에서만 콘솔에 액세스해야 하는 규정을 준수해야 합니다. RCPs 사용하여 조직 전체의 네트워크 제한을 적용하고 규정 준수의 증거로 AWS CloudTrail 로그를 유지합니다.

다중 계정 거버넌스

AWS Organizations에서 일관된 콘솔 액세스 정책을 구현합니다. RCPs 사용하여 모든 멤버 계정에 표준 네트워크 제한을 적용하여 개별 계정 수준 구성 없이 일관된 보안 태세를 보장합니다.

예제 시나리오: AWS 계정이 100개 이상인 기업은 RCPs 사용하여 조직 내 VPC 엔드포인트에서 모든 콘솔 액세스를 시작하도록 요구하는 정책을 적용하여 모든 계정에서 일관된 네트워크 제어를 확인합니다.

타사 액세스 제어

특정 네트워크의 파트너 또는 계약자에게 임시 콘솔 액세스 권한을 부여합니다. 조직은 전반적인 보안 태세를 손상시키지 않고 외부 당사자에 대한 시간 제한, 네트워크 제한 콘솔 액세스를 생성할 수 있습니다.

예제 시나리오: 회사가 컨설팅 회사 임시 콘솔 액세스 권한을 부여해야 합니다. 이들은 컨설팅 회사의 알려진 IP 범위에서만, 그리고 컨설턴트에게 할당된 IAM 역할에 대해서만 액세스를 허용하는 리소스 기반 정책을 생성합니다.

콘솔 액세스를 특정 보안 주체로 제한

네트워크 위치에 관계없이 정의된 보안 주체 집합만에 로그인 AWS Management Console하고 다른 모든 보안 주체를 거부하도록 허용합니다. 이는 VPC 엔드포인트를 사용하지 않고 자격 증명 기반 콘솔 제한을 원하는 고객에게 유용합니다. 콘솔 로그인이 거부된 보안 주체는 프로그래밍 방식 액세스를 유지합니다. AWS 로그인 정책은 콘솔 로그인만 게이트하고 제외된 보안 주체만 로그인할 수 있습니다.

예제 시나리오: 회사가 관리자만 콘솔을 사용하기를 원합니다. 관리자 보안 주체 ARNs을 제외한 모든 보안 주체에 대한 콘솔 로그인을 거부하는 RCP를 구성합니다. 유효한 자격 증명이 있는

Amazon EC2 인스턴스 역할은 프로그래밍 방식으로 권한을 유지하더라도 제외된 보안 주체가 아니므로 콘솔에 로그인할 수 없습니다. 이를 통해 콘솔 로그인에 사용되는 인스턴스 역할 자격 증명의 일반적인 사례를 해결할 수 있습니다.

콘솔 액세스 제어 문제 해결

로그인 리소스 기반 정책의 네트워크 조건으로 인해 로그인할 수 없음

AWS 로그인 정책에 의해 액세스가 거부되면 다음 오류 메시지 중 하나가 표시될 수 있습니다.

- “인증 정보가 잘못되었습니다. 다시 시도하세요.” (리소스 기반 정책에 의한 사전 인증 거부)
- “인증 실패 잘못된 요청”(RDP의 사전 인증 거부)
- “인증 실패:이 계정에 액세스하려면 다른 네트워크에서 로그인하거나 관리자에게 자세한 내용을 문의하세요.”(인증 후 거부)

이러한 오류가 표시되고 액세스가 허용되어야 한다고 생각되면 AWS 관리자에게 문의하십시오. `errorMessage` "리소스 기반 정책으로 인해 권한 부여가 거부됨" 또는 "리소스 제어 정책으로 인해 권한 부여가 거부됨"이 포함된 `ConsoleLogin` 이벤트에 대한 CloudTrail 로그를 검토하여 액세스를 거부한 정책 설명을 식별할 수 있습니다.

가능한 원인:

- 소스 IP 주소가 허용된 CIDR 범위에 있지 않습니다.
- 필수 VPC 또는 VPC 엔드포인트에 연결되어 있지 않습니다.
- 정책의 예상 리전과 일치하지 않는 리전 로그인 엔드포인트에 액세스하고 있습니다.
- 보안 주체 ARN이 정책의 제외된 보안 주체에 올바르게 나열되지 않습니다.
- 정책이 최근에 업데이트되었으며 변경 사항이 아직 전역적으로 복제되지 않았습니다.

해결 방법:

- 회사 네트워크 또는 VPN에 연결되어 있는지 확인합니다.
- VPC 엔드포인트 기반 제한이 구성된 경우 올바른 VPC 엔드포인트를 통해에 액세스하고 있는지 확인합니다.
- AWS 관리자에게 문의하여 정책 구성을 확인하고 권한이 부여된 네트워크를 확인합니다.

- 제외된 보안 주체로 구성된 경우 제외된 보안 주체 목록에서 보안 주체 ARN이 올바르게 구성되었는지 확인합니다.
- 최근에 정책이 변경된 경우 글로벌 복제가 완료될 때까지 몇 분 정도 기다립니다.

이 문제를 진단하는 관리자의 경우:

- 정책 평가 이벤트에 대한 AWS CloudTrail 로그를 검토하여 액세스를 거부한 정책 설명을 식별합니다.
- `aws signin get-resource-policy`를 사용하여 현재 정책 구성을 검토합니다.
- 사용자의 네트워크 위치가 정책의 조건과 일치하는지 확인합니다.
- 사용자가 네트워크 제한에서 제외되어야 하는 경우 제외된 보안 주체가 올바르게 구성되었는지 확인합니다.

콘솔 권한 부여를 활성화한 후 계정이 잠겼습니다.

콘솔 인증을 구성했고 계정에 더 이상 액세스할 수 없는 경우 정책을 적용하기 전에 제외된 보안 주체를 구성하지 않았을 수 있습니다.

계정 유형 및 사용 가능한 자격 증명에 따라 액세스를 다시 획득할 수 있는 여러 경로가 있습니다.

옵션 1: 프로그래밍 방식 액세스 사용(AWS CLI 또는 SDK)

콘솔 권한 부여 정책은 대화형 콘솔 로그인에만 적용됩니다. SigV4로 서명된 API 요청에는 적용되지 않습니다. 프로그래밍 방식 액세스(예: 기존 액세스 키, 교차 계정 역할)가 있는 경우 이를 사용하여 제한 정책을 호출`signin:DeleteConsoleAuthorizationConfiguration`하고 제거합니다. 사용하는 자격 증명에는를 호출할 수 있는 권한이 있어야 합니다`signin:DeleteConsoleAuthorizationConfiguration`. `AWSSignInResourcePolicyManagement` 관리형 정책에는이 permission. AWS recommds가 장기 IAM 사용자 액세스 키에 대한 임시 자격 증명을 포함합니다. 멤버 계정의 경우 관리 계정 관리자는 멤버 계정`OrganizationAccountAccessRole`에서를 수임하여 임시 자격 증명을 얻을 수 있습니다. 이 역할은 조직에 가입하도록 초대된 계정에서 자동으로 생성되지 않습니다.

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

또는 특정 권한 설명을 삭제합니다.

```
# First, list statements to get the statement ID
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

옵션 2: AWS Support에 문의

프로그래밍 방식 액세스 권한이 없고 계정 액세스OrganizationAccountAccessRole에를 사용할 수 없는 경우 AWS Support에 문의하여 잠금 복구 프로세스를 시작합니다.

복구 프로세스는 다음과 같이 작동합니다.

1. 위의 옵션을 사용하여 문제를 해결할 수 없는 경우 지원 센터에서 AWS 지원 사례를 엽니다. AWS Support는 계정을 검사하기 전에 자격 증명을 확인합니다. 확인 방법에는 루트 사용자 계정 이메일 주소 확인, 전화 확인 통화 응답 또는 계정 보안 질문에 대한 답변이 포함될 수 있습니다.
2. AWS 지원은 콘솔 액세스 문제가 리소스 기반 정책 잠금으로 인해 발생했음을 확인합니다.
3. AWS Support는 복구 포털 링크를 공유합니다. 이 링크를 사용하여 `signin:DeleteConsoleAuthorizationConfiguration` 권한이 있는 계정의 IAM 보안 주체로 로그인합니다. 이 권한을 통해 보안 주체는 잠금을 유발하는 콘솔 권한 부여 구성을 삭제할 수 있습니다.

> **Important**
>
> 복구 포털은 모든 리소스 권한 문을 포함하여 계정에 대한 전체 콘솔 권한 부여 구성을 제거합니다. 복구 포털은 AWS 로그인 리소스 기반 정책의 재구성을 허용하지 않습니다.

복구 포털 링크는 AWS Support에서 공유한 후 72시간 후에 만료됩니다. 해당 기간 내에 복구를 완료하지 않으면 AWS Support에 문의하여 프로세스를 다시 시작하세요.

액세스 권한을 다시 획득한 후:

- 적절하게 구성된 제외된 보안 주체를 포함하도록 리소스 권한 설명을 검토하고 업데이트합니다.
- 콘솔 인증을 다시 활성화하기 전에 예상 네트워크에서 콘솔 액세스를 테스트합니다.

- 나중에 참조할 수 있도록 복구 절차를 문서화합니다.

변경 사항이 매번 즉시 표시되는 것은 아닙니다

정책 변경은 전역적으로 복제되지만 복제에는 몇 분 정도 걸릴 수 있습니다.

해결 방법:

- 정책을 변경한 후 글로벌 복제가 완료될 때까지 몇 분 정도 기다립니다.
- `get-resource-policy` 명령을 사용하여 변경 사항을 확인합니다.

```
aws signin get-resource-policy --region <your-region>
```

- AWS CloudTrail 로그에서 정책 평가 이벤트를 확인하여 새 정책이 평가되고 있는지 확인합니다.
- 작업에 올바른 리전을 사용하고 있는지 확인합니다(쓰기 작업은를 사용해야 함`us-east-1`).
- VPC 엔드포인트 기반 조건을 사용하는 경우 VPC 엔드포인트 정책도 올바르게 구성되어 있는지 확인합니다.

일반적인 정책 복제 문제:

- 캐시된 로그인 페이지: 브라우저가 로그인 페이지를 캐시할 수 있습니다. 브라우저 캐시를 지우거나 incognito 창을 사용하여 정책 변경을 테스트합니다.
- 충돌하는 문: 여러 권한 문이 있는 경우 서로 충돌하지 않는지 확인합니다. `get-resource-policy`를 사용하여 통합 정책을 검토합니다.
- VPC 엔드포인트 정책: AWS 로그인 정책은 VPC 엔드포인트 정책과 함께 작동합니다. 둘 다 원하는 액세스를 허용해야 합니다.

AWS 로그인 조건 키 참조

이 페이지에는 AWS 로그인 리소스 기반 정책 및 리소스 제어 정책(RCPs)에서 사용할 수 있는 조건 키가 나열되며 각 키가 적용되는 평가 단계와 작업이 표시됩니다. `signin:PrincipalArn` 만 AWS 로그인에만 해당되며 다른는 AWS 전역 조건 키입니다. 전역 키 정의는 AWS 전역 조건 컨텍스트 키를 참조하세요.

서비스 승인 참조의 작업 및 조건 키의 전체 목록은 AWS 로그인에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

네트워크 기반 조건 키

이러한 조건 키는 요청이 시작되는 위치를 확인합니다. AWS 로그인은 리소스 기반 정책과 RCPs 모두에서 모든 AWS 로그인 작업(`signin:Authenticate`, 및 `signin:AuthorizeOAuth2Accesssignin:CreateOAuth2Token`)에 대해 요청을 평가합니다.

네트워크 기반 조건 키

조건 키	연산자	설명	사용 규칙
`aws:SourceIp`	`IpAddress` , `NotIpAddress`	퍼블릭 IP 주소 또는 CIDR 범위	요청이 VPC 엔드포인트를 사용하는 경우 존재하지 않습니다. 동일한 문에서 VPC 기반 조건과 결합할 때 `IfExists` 연산자를 사용합니다.
`aws:SourceVpc`	`StringEquals` , `StringNotEquals`	VPC ID(`vpc-xxxxxxxx`)	요청이 VPC 엔드포인트를 사용하는 경우에만 표시됩니다. 리전 간 VPC ID 충돌`aws:RequestedRegion` 을 방지하려면와 함께 사용합니다.
`aws:SourceVpce`	`StringEquals` , `StringNotEquals`	VPC 엔드포인트 ID(`vpce-xxxxxxxx`)	요청이 VPC 엔드포인트를 사용하는 경우에만 표시됩니다.

조건 키	연산자	설명	사용 규칙
aws:VpcSourceIp	IpAddress , NotIpAddress	VPC 내 프라이빗 IP	항상 aws:SourceVpc 또는 aws:VpcSourceIp 조건 키와 함께 aws:SourceVpce 조건 키를 사용합니다.
aws:RequestedRegion	StringEquals , StringNotEquals	대상 AWS 리전 코드	리전 간 VPC ID 충돌을 방지하기 aws:SourceVpc 위해를 사용할 때 권장됩니다. 여러 리전을 지정할 수 있습니다.

> **Important**
>
> 단일 요청에는 aws:SourceIp (퍼블릭 네트워크) 또는 aws:SourceVpc (VPC 엔드포인트)가 포함되며 둘 다 포함되지 않습니다. 두 경로를 모두 포함하는 거부 정책을 작성할 때는 IfExists 연산자(예: NotIpAddressIfExists)를 사용하거나 별도의 문을 생성합니다.

자격 증명 기반 조건 키

이러한 조건 키는 누가 요청을 하는지 확인합니다. 보안 주체 자격 증명이 설정된 인증 후 작업(signin:AuthorizeOAuth2Access 및 signin:CreateOAuth2Token)에만 사용할 수 있습니다.

자격 증명 기반 조건 키

조건 키	연산자	설명	예제
aws:PrincipalArn	ArnEquals , ArnLike, ArnNotEquals , StringEquals , StringLike	인증된 IAM 보안 주체의 ARN	arn:aws:iam::123456789012:user/alice , arn:aws:iam::123456789012:role/Admin

조건 키	연산자	설명	예제
aws:PrincipalAccount	StringEquals , StringNotEquals	AWS 보안 주체의 계정 ID	123456789012

서비스별 조건 키: signin:PrincipalArn

다음 조건 키는 AWS 로그인에만 적용되며 글로벌 AWS 키가 아닙니다. 사전 인증 평가 중에만 사용할 수 있습니다. 인증을 완료하기 전에 로그인을 시작하는 보안 주체를 식별하는 signin:PrincipalArn 데 사용합니다. 이는와 동일한 사전 인증aws:PrincipalArn이며 인증 후까지 사용할 수 없습니다.

연산자

ARN 연산자(ArnEquals, ArnLike, ArnNotEquals, ArnNotLike) 및 문자열 연산자(StringEquals, StringLike).

가용성

AWS 로그인에는 사전 인증 단계(signin:Authenticate작업) 동안 요청 컨텍스트에이 키가 포함됩니다. 인증 후 작업(signin:AuthorizeOAuth2Access 및)에는 사용할 수 없습니다signin:CreateOAuth2Token.

데이터 유형

ARN. 문자열 연산자 대신 ARN 연산자를 사용합니다.

값 유형

단일 값입니다.

지원 버전:

리소스 기반 정책 및 RCPs

ARN 연산자를 사용하여 값을 비교합니다. 다음 보안 주체 유형을 지정할 수 있습니다.

- AWS 계정 루트 사용자(arn:aws:iam::123456789012:root)
- IAM 사용자(arn:aws:iam::123456789012:user/*user-name*)
- IAM 역할(arn:aws:iam::123456789012:role/*role-name*)

사용 사례: 네트워크 제한에서 제외된 보안 주체 자격 증명을 제외하여 다른 모든 액세스 시도에 대해 네트워크 제어를 적용하면서 잠금을 방지합니다.

예 - 루트 사용자를 제외한 무단 네트워크에서의 사전 인증 액세스를 거부합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
```

```
}
```

이 정책은 계정 루트 사용자를 제외하고 203.0.113.0/24 IP 범위 외부에서의 콘솔 액세스를 거부합니다. 사전 인증 문은 인증을 완료하기 전에 signin:PrincipalArn를 사용하여 루트 사용자를 제외합니다. 인증 후 문은 OAuth 토큰 교환 중에 aws:PrincipalArn를 사용하여 인증 후 동일한 보안 주체를 제외합니다. 정책 예시을(를) 참조하세요.

작업별 조건 키 가용성

작업별 조건 키 가용성

조건 키	로그인:인증	로그인:AuthorizeOAuth2Access	로그인:CreateOAuth2Token
aws:SourceIp	예	예	예
aws:SourceVpc	예	예	예
aws:SourceVpce	예	예	예
aws:VpcSourceIp	예	예	예
aws:RequestedRegion	예	예	예
aws:PrincipalArn	–	예	예
aws:PrincipalAccount	–	예	예
signin:PrincipalArn	예	–	–

> **Note**
>
> signin:CreateAccount 작업은 콘솔 프라이빗 액세스에 대한 VPC 엔드포인트 정책에서만 사용되며 리소스 기반 정책 또는 RCPs에는 사용할 수 없습니다. 서비스별 조건 키는 연결되지 않습니다. 콘솔 프라이빗 액세스를 참조하세요.

관련 정보

- 리소스 기반 정책 및 리소스 제어 정책을 사용하여 콘솔 액세스 제어
- AWS Management Console 프라이빗 액세스
- AWS 전역 조건 컨텍스트 키
- AWS 로그인에 사용되는 작업, 리소스 및 조건 키

AWS 액세스 포털에 로그인

IAM Identity Center의 사용자는의 멤버입니다 AWS Organizations. IAM Identity Center의 사용자는 특정 로그인 URL로 액세스 포털에 로그인하여 여러 AWS 계정 및 비즈니스 애플리케이션에 AWS 액세스할 수 있습니다. 로그인 URL에 대한 자세한 내용은 AWS 액세스 포털 섹션을 참조하십시오.

IAM Identity Center에서 사용자 AWS 계정 로에 로그인하기 전에 다음과 같은 필수 정보를 수집합니다.

- 기업 사용자 이름
- 기업 암호
- 특정 로그인 URL

> **Note**
>
> 로그인한 후 AWS 액세스 포털 세션은 8시간 동안 유효합니다. 8시간 후에는 다시 로그인해야 합니다.

AWS 액세스 포털에 로그인하려면

1. 브라우저 창에서 `https://your_subdomain.awsapps.com/start` 또는 듀얼 스택 URL 형식과 같이 이메일을 통해 제공된 로그인 URL을 붙여 넣습니다`https://[IAM Identity Center instance ID].portal.[Region].app.aws`. 그런 다음 Enter 키를 누릅니다.
2. 기업 보안 인증(예: 사용자 이름 및 암호)을 사용하여 로그인합니다.

   > **Note**
   >
   > 소속 관리자가 이메일로 일회용 암호(OTP)를 보내왔고 이번이 처음 로그인인 경우 해당 암호를 입력하십시오. 로그인 후에는 향후 로그인에 사용할 새 암호를 만들어야 합니다.

3. 확인 코드를 입력하라는 요청이 있으면 이메일에서 확인 코드를 확인하세요. 그런 다음 해당 코드를 복사하여 로그인 페이지에 붙여넣습니다.

> **Note**
>
> 확인 코드는 보통 이메일로 전송되지만 전달 방법은 다를 수 있습니다. 아직 이메일로 이를 받지 못했다면 관리자에게 확인 코드에 대한 세부 정보를 확인하세요.

4. IAM Identity Center의 사용자에 대해 MFA를 활성화한 경우, MFA를 사용하여 인증합니다.
5. 인증 후 포털에 표시되는 AWS 계정 모든 및 애플리케이션에 액세스할 수 있습니다.

   a. 에 로그인하려면 AWS Management Console 계정 탭을 선택하고 관리할 개별 계정을 선택합니다.

      사용자의 역할이 표시됩니다. 계정의 역할 이름을 선택하여 AWS Management Console을 엽니다. 액세스 키를 선택하여 명령줄 또는 프로그래밍 방식의 액세스에 대한 자격 증명을 가져옵니다.

   b. 애플리케이션 탭을 선택하여 사용 가능한 애플리케이션을 표시하고 액세스하려는 애플리케이션의 아이콘을 선택합니다.

IAM Identity Center 사용자로 로그인하면 세션이라고 하는 일정 기간 동안 리소스에 액세스할 수 있는 보안 인증이 제공됩니다. 기본적으로 사용자는 8시간 동안 AWS 계정 에 로그인할 수 있습니다. IAM Identity Center 관리자는 최소 15분에서 최대 90일까지 다른 기간을 지정할 수 있습니다. 세션이 종료된 후 다시 로그인할 수 있습니다.

추가 정보

IAM Identity Center의 사용자에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- IAM Identity Center에 대한 개요는 IAM Identity Center란 무엇인가요?를 참조하세요.
- AWS 액세스 포털에 대한 자세한 내용은 AWS 액세스 포털 사용을 참조하세요.
- IAM Identity Center 세션에 대한 자세한 내용은 사용자 인증을 참조하십시오.
- IAM Identity Center 사용자 암호 재설정 방법에 대한 단계별 지침은 에 대한 IAM Identity Center 암호를 잊어버렸습니다. AWS 계정 섹션을 참조하세요.
- 사용자 또는 조직에서 IP 또는 도메인 필터링을 구현하는 경우 AWS 액세스 포털을 생성하고 사용하려면 도메인을 허용 목록에 추가해야 할 수 있습니다. IAM Identity Center는 IPv4 및 듀얼 스택 엔드포인트를 모두 지원합니다. 네트워크에서 IPv6를 사용하는 경우 듀얼 스택 엔드포인트 도메인을 사용합니다. 도메인 허용 목록에 대한 자세한 내용은 허용 목록에 추가할 도메인 섹션을 참조하세요.

를 통해 로그인 AWS Command Line Interface

가를 AWS CLI 인증하는 방법을 설정해야 합니다 AWS. 워크플로 및 보안 요구 사항에 가장 적합한 방법을 선택합니다.

- 콘솔 자격 증명으로 로그인(권장) 루트, IAM 사용자 또는 IAM과의 페더레이션을 AWS 계정 액세스에 사용하는 경우.
- IAM Identity Center 자격 증명으로 로그인 AWS 계정 액세스에 Identity Center를 사용하는 경우.

콘솔 자격 증명으로 로그인(권장)

이 인증 방법을 사용하면에서 콘솔 자격 증명을 사용할 수 AWS CLI있으므로 계정 설정 후 몇 분 내에 AWS 프로그래밍 방식으로를 쉽게 시작할 수 있습니다. AWS CLI, AWS SDKs AWS Tools for PowerShell.

사전 조건

- 를 설치합니다 AWS CLI. 자세한 내용은 Installing or updating to the latest version of the AWS CLI를 참조하세요. `aws login` 명령을 사용하려면 최소 2.32.0 버전이 필요합니다.
- 루트 사용자, IAM 사용자 또는 IAM과의 페더레이션 AWS Management Console 을 통해에 로그인할 수 있는 액세스 권한. IAM Identity Center를 사용하는 경우 대신 IAM Identity Center 자격 증명으로 로그인로 이동합니다.
- IAM 자격 증명에 적절한 권한이 있는지 확인합니다. SignInLocalDevelopmentAccess 관리형 정책을 IAM 사용자, 역할 또는 그룹에 연결합니다. 루트 사용자로 로그인하는 경우 추가 권한이 필요하지 않습니다.

콘솔 자격 증명으로 로그인하려면

1. 다음 명령을 실행하여 브라우저 기반 인증 프로세스를 시작합니다.

   ```
   $ aws login
   ```

   `aws login` 명령은 다음과 같은 몇 가지 선택적 파라미터를 지원합니다.

   - `aws login --remote` - 디바이스가 브라우저를 지원하지 않는 경우 디바이스 간 인증

> **Note**
>
> 동일 디바이스(`aws login`) 및 교차 디바이스(`aws login --remote`) 인증에 대한 액세스를 제어할 수 있습니다. 관련 IAM 정책에서 다음 리소스 ARN을 사용합니다.
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost` - `aws login`을 사용한 동일 디바이스 인증에 이 ARN을 사용합니다.
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote` - `aws login --remote`를 사용한 교차 디바이스 인증에 이 ARN을 사용합니다.

- `aws login --profile profile-name` - 특정 프로필로 인증하려면
- `aws login --region region` - 특정 리전에서 인증하려면

2. 터미널의 프롬프트를 따릅니다. 명령은 기본 브라우저를 자동으로 열고 인증 프로세스를 안내합니다. 인증에 성공하면 AWS CLI 세션은 최대 12시간 동안 유효합니다.
3. 세션을 종료하려면 다음을 사용합니다.

```
$ aws logout
```

를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우 AWS에서 PowerShell용 AWS 도구 인증을 참조 AWS Tools for PowerShell하세요. AWS SDKs 사용하는 경우 AWS SDKs 및 액세스를 참조하세요.

IAM Identity Center 자격 증명으로 로그인

AWS 액세스 포털을 사용하면 IAM Identity Center 사용자가를 쉽게 선택하고에 대한 임시 보안 자격 증명을 AWS 계정 얻을 수 있습니다 AWS CLI. 이러한 자격 증명을 가져오는 방법에 대한 자세한 내용은 의 리전 가용성 AWS Builder ID 섹션을 참조하세요. IAM Identity Center로 사용자를 인증하도록를 AWS CLI 직접 구성할 수도 있습니다.

IAM Identity Center 자격 증명으로 로그인하려면

1. 사전 필수 단계를 완료했는지 확인합니다.
2. 처음 로그인하는 경우 `aws configure sso`마법사를 사용하여 프로필을 설정하십시오.
3. 프로필을 구성한 후 다음 명령을 실행한 다음 터미널의 프롬프트를 따릅니다.

```
$ aws sso login --profile my-profile
```

추가 정보

명령줄을 사용한 로그인에 대한 자세한 내용은 다음 리소스를 참조하세요.

- 콘솔 자격 증명을 사용하여 AWS 로컬 개발을 위해 로그인하는 방법에 대한 자세한 내용은 AWS CLI의 인증 및 액세스 자격 증명을 참조하세요.
- AWS CLI 로그인 프로세스에 대한 자세한 내용은에 대한 단기 자격 증명으로 인증을 참조하세요 AWS CLI.
- IAM Identity Center 구성에 대한 자세한 내용은 IAM Identity Center를 사용하도록 구성을 참조 AWS CLI 하세요.

페더레이션 ID로 로그인

페더레이션 자격 증명은 외부 자격 증명으로 보안 AWS 계정 리소스에 액세스할 수 있는 사용자입니다. 외부 자격 증명은 회사 자격 증명 스토어(예: LDAP 또는 Windows Active Directory) 또는 제3자(예: Amazon, Facebook 또는 Google을 통한 로그인)에서 가져올 수 있습니다. 페더레이션 자격 증명은 AWS Management Console 또는 AWS 액세스 포털로 로그인하지 않습니다. 사용 중인 외부 ID 유형에 따라 페더레이션 ID의 로그인 방식이 결정됩니다.

관리자는 `https://signin.aws.amazon.com/federation`을(를) 포함하는 사용자 지정 URL을 만들어야 합니다. 자세한 내용은 AWS Management Console에 대한 사용자 정의 ID 브로커 액세스 사용을 참조하세요.

> **Note**
>
> 관리자가 페더레이션 ID를 생성합니다. 페더레이션 ID로 로그인하는 방법에 대한 자세한 내용은 소속 관리자에게 문의하세요.

페더레이션 ID에 대한 자세한 내용은 웹 ID 페더레이션 정보를 참조하세요.

를 사용하여 로그인 AWS Builder ID

AWS Builder ID 는 Amazon CodeCatalyst, Amazon Q Developer 및 AWS 교육 Certification을 비롯한 일부 도구 및 서비스에 대한 액세스를 제공하는 개인 프로필입니다.는 사용자를 개인으로 AWS Builder ID 나타내며 기존 AWS 계정에 있을 수 있는 자격 증명 및 데이터와 독립적입니다. 다른 개인 프로필과 마찬가지로는 개인, 교육 및 경력 목표를 진행하면서 함께 AWS Builder ID 남아 있습니다.

는 이미 소유하거나 생성하려는 모든 AWS 계정 를 AWS Builder ID 보완합니다. 는 사용자가 생성하는 AWS 리소스의 컨테이너 AWS 계정 역할을 하고 해당 리소스에 대한 보안 경계를 제공하지만는 사용자를 개인으로 AWS Builder ID 나타냅니다. 자세한 내용은 AWS Builder ID 및 기타 AWS 자격 증명 단원을 참조하십시오.

AWS Builder ID 는 무료입니다. 에서 사용하는 AWS 리소스에 대해서만 비용을 지불합니다 AWS 계정. 요금에 대한 자세한 내용은 AWS 요금 부분을 참조하세요.

사용자 또는 조직이 IP 또는 도메인 필터링을 구현하는 경우 AWS Builder ID를 생성 및 사용하려면 도메인을 허용 목록에 추가해야 합니다. 도메인 허용 목록에 대한 자세한 내용은 허용 목록에 추가할 도메인 섹션을 참조하세요.

> **Note**
>
> AWS Builder ID는 AWS 전문가로부터 배우고 온라인으로 클라우드 기술을 구축할 수 있는 온라인 학습 센터인 AWS Skill Builder 구독과는 별개입니다. AWS Skill Builder에 대한 자세한 내용은 AWS Skill Builder를 참조하세요.

주제

- AWS Builder ID 다중 인증(MFA) 관리
- 의 개인 정보 보호 및 데이터 AWS Builder ID
- AWS Builder ID 및 기타 AWS 자격 증명

로 로그인하려면 AWS Builder ID

1. 액세스하려는 AWS 도구 또는 서비스의 AWS Builder ID 프로필 또는 로그인 페이지로 이동합니다. 예를 들어, Amazon CodeCatalyst에 로그인하려면 https://codecatalyst.aws로 이동합니다.
2. 에 로그인하는 방법 선택 AWS Builder ID
   - 기존에 계정이 있습니다
   - Google 계정이 있음
   - Apple 계정이 있음
   - GitHub 계정이 있음
   - Amazon 계정이 있음

기존에 계정이 있습니다

1. 기존 계정의 경우를 생성하는 데 사용한 이메일을 입력하고 로그인을 AWS Builder ID 선택합니다.
2. 를 생성하는 데 사용한 이메일을 입력하고 로그인을 AWS Builder ID 선택합니다.
3. AWS Builder ID페이지에 로그인에서 암호를 입력합니다.
4. (선택) 나중에 추가 확인을 요구하는 메시지 없이 이 디바이스에서 로그인 하려면, 이는신뢰할 수 있는 디바이스 옆의 상자를 선택합니다.
5. 계속을 선택합니다.
6. 추가 확인 필요 페이지가 표시되면, 브라우저의 지침에 따라 필수 코드나 보안 키를 제공하십시오.

> **Note**
>
> 보안을 위해 로그인 브라우저, 위치 및 디바이스를 분석합니다. 이 디바이스를 신뢰하도록 요청하면 로그인할 때마다 다중 인증(MFA) 코드를 제공하지 않아도 됩니다. 자세한 내용은 신뢰할 수 있는 디바이스 단원을 참조하십시오.

Google 계정이 있음

Google 계정이 이미와 연결되어 있는 경우 다른 이메일 주소를 사용하여 애플리케이션에 로그인해야 AWS Builder ID합니다. 자세한 내용은 Google로 로그인할 수 없습니다 단원을 참조하십시오.

1. Google 계정을 사용하여 로그인하려면 Google로 계속을 AWS Builder ID선택합니다.
2. Google로 로그인 페이지에서 로그인할 Google 계정의 정보를 입력합니다.
3. 계속을 선택하여 AWS 애플리케이션 홈페이지를 로드합니다.

Apple 계정이 있음

Apple 계정이 이미와 연결되어 있는 경우 다른 이메일 주소를 사용하여 애플리케이션에 로그인해야 AWS Builder ID합니다. 자세한 내용은 Apple로 로그인할 수 없음 단원을 참조하십시오.

1. Apple 계정을 사용하여 로그인하려면 Apple 계속을 AWS Builder ID선택합니다.
2. Apple로 로그인 페이지에서 Apple 계정이 로그인할 정보를 입력합니다.
3. 계속을 선택하여 AWS 애플리케이션 홈페이지를 로드합니다.

GitHub 계정이 있음

GitHub 계정이 이미와 연결되어 있는 경우 다른 이메일 주소를 사용하여 애플리케이션에 로그인 AWS Builder ID해야 합니다. 자세한 내용은 GitHub로 로그인할 수 없음 단원을 참조하십시오.

1. GitHub 계정을 사용하여 로그인하려면 GitHub 계속을 AWS Builder ID선택합니다.
2. GitHub로 로그인 페이지에서 로그인할 GitHub 계정의 정보를 입력합니다.
3. 계속을 선택하여 AWS 애플리케이션 홈페이지를 로드합니다.

Amazon 계정이 있음

Amazon 계정이 이미와 연결되어 있는 AWS Builder ID경우 다른 이메일 주소를 사용하여 애플리케이션에 로그인해야 합니다. 자세한 내용은 Amazon으로 로그인할 수 없음 단원을 참조하십시오.

1. Amazon 계정을 사용하여 로그인하려면 Amazon 계속을 AWS Builder ID선택합니다.
2. Amazon으로 로그인 페이지에서 로그인할 Amazon 계정의 정보를 입력합니다.
3. 계속을 선택하여 AWS 애플리케이션 홈페이지를 로드합니다.

의 리전 가용성 AWS Builder ID

AWS Builder ID 는 다음에서 사용할 수 있습니다 AWS 리전. 를 사용하는 애플리케이션은 다른 리전에서 작동할 AWS Builder ID 수 있습니다.

이름	코드
미국 동부(버지니아 북부)	us-east-1

생성 AWS Builder ID

를 사용하는 AWS 도구 및 서비스 중 하나에 가입할 AWS Builder ID 때를 생성합니다. AWS 도구 또는 서비스에 대한 가입 프로세스의 일환으로 이메일 주소, 이름 및 암호로 가입합니다.

암호는 다음 요구 사항을 준수해야 합니다.

- 암호는 대/소문자를 구분합니다.
- 암호 길이는 8~64자여야 합니다.
- 암호는 각각의 다음 네 가지 범주의 문자를 최소 1자씩 포함해야 합니다.
  - 소문자(a~z)
  - 대문자(A-Z)
  - 숫자(0-9)
  - 영숫자 외의 특수 문자(~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- 최근 사용한 세 개의 암호는 다시 사용할 수 없습니다.
- 제3자로부터 유출된 데이터 세트를 통해 공개적으로 알려진 암호는 사용할 수 없습니다.

> **Note**
>
> 를 사용하는 도구 및 서비스는 필요할 AWS Builder ID 때를 생성하고 사용하도록 AWS Builder ID 지시합니다.

를 생성하려면 AWS Builder ID

1. 액세스하려는 AWS 도구 또는 서비스의 AWS Builder ID 프로필 또는 가입 페이지로 이동합니다. 예를 들어, Amazon CodeCatalyst에 로그인하려면 https://codecatalyst.aws로 이동합니다.
2. 생성 방법 선택 AWS Builder ID
   - Google 계정을 사용하려면 Google 계속을 선택하고 프롬프트에 따라 가입 프로세스를 완료합니다. 이렇게 하면 아래 3~8단계를 건너뜁니다. 9단계로 이동합니다.
   - Apple 계정을 사용하려면 Apple 계속을 선택하고 프롬프트에 따라 가입 프로세스를 완료합니다. 이렇게 하면 아래 3~8단계를 건너뜁니다. 9단계로 이동합니다.

     > **Note**
     >
     > Apple로 로그인에 대해 iCloud+ "내 이메일 숨기기" 기능을 활성화하도록 선택하면 실제 이메일 주소 대신 Apple 계정에 지정된 내 이메일 숨기기 주소로 AWS Builder ID가 생성됩니다. 이 이메일 주소는 변경할 수 없지만 이름과 성은 계속 편집할 수 있습니다. 에 로그인해야 하는 경우 내 이메일 숨기기 주소를 사용해야 AWS Builder ID합니다. AWS Builder ID 는 내 이메일 숨기기 주소를 사용하여 이메일 통신을 전송합니다. 자세한 내용은 Sign in with Apple에서 내 이메일 숨기기를 사용하는 방법을 참조하세요.

   - GitHub 계정을 사용하려면 GitHub 계속을 선택하고 프롬프트에 따라 가입 프로세스를 완료합니다. 이렇게 하면 아래 3~8단계를 건너뜁니다. 9단계로 이동합니다.
   - Amazon 계정을 사용하려면 Amazon 계속을 선택하고 프롬프트에 따라 가입 프로세스를 완료합니다. 이렇게 하면 아래 3~8단계를 건너뜁니다. 9단계로 이동합니다.
   - 이메일 및 암호로 계정을 생성하려면 다음 단계를 계속 진행합니다.
3. 생성 AWS Builder ID 페이지에서 귀하의 이메일 주소를 입력합니다. 개인 이메일을 사용하는 것이 좋습니다.
4. 다음을 선택합니다.
5. 귀하의 성함을 입력하고 다음를 선택합니다.
6. 이메일 확인 페이지에서 이메일 주소로 전송된 확인 코드를 입력합니다. 확인를 선택합니다. 이메일 공급자에 따라 이메일 수신에 몇 분 정도 걸릴 수도 있습니다. 스팸 및 정크 폴더에서 해당 코드를 확인하세요. 5분 AWS 후에도의 이메일이 표시되지 않으면 코드 재전송을 선택합니다.
7. 이메일을 확인한 후 암호 선택 페이지에서 암호를 입력하고 이메일을 확인합니다.
8. Captcha가 추가 보안으로 표시되는 경우, 표시되는 문자를 입력하십시오.
9. 생성(Create) AWS Builder ID을 선택합니다.

신뢰할 수 있는 디바이스

로그인 페이지에서 이는신뢰할 수 있는 디바이스 옵션을 선택하면, 향후 해당 디바이스에서 해당 웹 브라우저를 통한 모든 로그인이 승인된 것으로 간주됩니다. 즉, 신뢰할 수 있는 디바이스에서 MFA 코드를 제공할 필요가 없습니다. 하지만 브라우저, 쿠키 또는 IP 주소가 변경될 경우 추가 확인을 위해 MFA 코드를 사용해야 할 수도 있습니다.

AWS 를 사용하는 도구 및 서비스 AWS Builder ID

로 로그인하여 다음 AWS 도구 및 서비스에 AWS Builder ID 액세스할 수 있습니다. 요금에 대해 제공되는 기능 또는 이점에 액세스하려면가 필요합니다 AWS 계정.

기본적으로를 사용하여 AWS 도구 또는 서비스에 로그인하면 세션 기간이 30일 동안 지속됩니다. 단 AWS Builder ID, 세션 기간이 90일인 Amazon Q Developer는 예외입니다. 세션이 종료된 후 다시 로그인해야 합니다.

AWS 클라우드 커뮤니티

Community.aws는에서 액세스할 수 있는 AWS 빌더 커뮤니티의 플랫폼입니다 AWS Builder ID. 교육 콘텐츠를 검색하고, 개인적인 생각과 프로젝트를 공유하며, 다른 사람의 게시물에 댓글을 달고, 좋아하는 빌더를 팔로우할 수 있는 곳입니다.

Amazon CodeCatalyst

Amazon CodeCatalyst 사용을 시작할 AWS Builder ID 때를 생성하고 문제, 코드 커밋 및 풀 요청과 같은 활동과 연결할 별칭을 선택합니다. 소속 팀이 다음 프로젝트를 성공적으로 구축하는 데 필요한 도구, 인프라 및 환경을 모두 갖춘 Amazon CodeCatalyst 스페이스로 다른 사람들을 초대하십시오. 클라우드 AWS 계정 에 새 프로젝트를 배포하려면이 필요합니다.

AWS Migration Hub

를 사용하여 AWS Migration Hub (Migration Hub)에 액세스합니다 AWS Builder ID. Migration Hub는 기존 서버를 검색하고, 마이그레이션을 계획하며, 각 애플리케이션 마이그레이션의 상태를 추적할 수 있는 단일 위치를 제공합니다.

Amazon Q Developer

Amazon Q Developer는 AWS 애플리케이션을 이해, 구축, 확장 및 운영하는 데 도움이 되는 생성형 AI 기반 대화형 어시스턴트입니다. 자세한 내용은 Amazon Q Developer 사용 설명서의 What is Amazon Q Developer?를 참조하세요.

AWS re:Post

AWS re:Post는 AWS 서비스를 사용하여 혁신의 속도를 높이고 운영 효율성을 개선할 수 있도록 전문적인 기술 지침을 제공합니다. AWS 계정 또는 신용 카드 없이 re:Post에서 로 로그인 AWS Builder ID 하고 커뮤니티에 가입할 수 있습니다.

AWS 시작

AWS Builder ID 를 사용하여 AWS 학습 콘텐츠, 도구, 리소스 및 지원을 사용하여 스타트업을 확장할 수 있는 Startups에 가입합니다 AWS.

AWS 교육 및 인증

를 사용하여 AWS 교육 및 인증 AWS Builder ID 에 액세스하여 AWS Skill Builder로 AWS 클라우드 기술을 구축하고, AWS 전문가로부터 배우고, 업계에서 인정받는 자격 증명을 사용하여 클라우드 전문 지식을 검증할 수 있습니다.

Kiro

Kiro는 사양 기반 개발을 통해 프로토타입에서 프로덕션으로 전환하는 데 도움이 되는 에이전트 IDE입니다. 간단한 작업부터 복잡한 작업까지 Kiro는 고객과 협력하여 프롬프트를 세부 사양으로 변환한 다음 작동 코드, 문서 및 테스트로 변환합니다. Kiro를 사용하면 빌드하는 것이 정확히 원하는 것이며 팀과 공유할 준비가 된 것입니다. Kiro의 에이전트는 까다로운 문제를 해결하고 설명서 생성 및 단위 테스트와 같은 작업을 자동화하는 데 도움이 됩니다. Kiro를 사용하면 모든 단계에서 운전자의 좌석에 있는 동안 프로토타입을 넘어 빌드할 수 있습니다.

웹사이트 등록 포털(WRP)

를 AWS 마케팅 웹 사이트의 영구 고객 자격 증명 및 등록 프로필 AWS Builder ID 로 사용할 수 있습니다. 새 웨비나에 등록하고 그동안 등록했거나 참석한 모든 웨비나를 보려면 My webinars를 참조하십시오.

AWS Builder ID 프로필 편집

프로필 정보는 언제든지 변경할 수 있습니다. 를 생성하는 데 사용한 이메일 주소 및 이름과 별명을 편집할 수 AWS Builder ID있습니다. Google 또는 Apple과 같은 소셜 로그인을 사용하는 경우 이름과 별명만 편집할 수 있습니다.

이름은 도구 및 서비스에서 다른 사람과 교류할 때 귀하를 지칭하는 방식입니다. 닉네임은 별명 AWS, 친구 및 긴밀히 협력하는 다른 사람들이 어떻게 알려지길 원하는지 나타냅니다.

> **Note**
>
> 를 사용하는 도구 및 서비스는 필요할 AWS Builder ID 때를 생성하고 사용하도록 AWS Builder ID 지시합니다.

프로필 정보 편집하기

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 내 세부 정보를 선택합니다.
3. 내 세부 정보 페이지에서 프로필 옆의 편집 버튼을 선택합니다.
4. 프로필 편집 페이지에서 이름과 별명을 원하는 대로 변경합니다.
5. 변경 사항 저장을 선택합니다. 페이지 상단에 프로필을 업데이트했음을 알리는 녹색 확인 메시지가 나타납니다.

> **Note**
>
> 다른 로그인 파트너 중 하나에서 이름과 별명을 변경하더라도, 해당 설정은 귀하의 AWS Builder ID에서는 업데이트되지 않습니다.

연락처 정보를 편집하려면

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 내 세부 정보를 선택합니다.
3. 내 세부 정보 페이지에서 연락처 정보 옆의 편집 버튼을 선택합니다.
4. 연락처 정보 편집 페이지에서 이메일 주소를 변경합니다.
5. 이메일 확인을 선택합니다. 대화 상자가 나타납니다.
6. 이메일 확인 대화 상자에서 이메일로 코드를 받은 후 확인 코드에 해당 코드를 입력합니다. 확인를 선택합니다.

AWS Builder ID 암호 변경

암호는 다음 요구 사항을 준수해야 합니다.

- 암호는 대/소문자를 구분합니다.
- 암호 길이는 8~64자여야 합니다.
- 암호는 각각의 다음 네 가지 범주의 문자를 최소 1자씩 포함해야 합니다.
  - 소문자(a~z)
  - 대문자(A-Z)
  - 숫자(0-9)
  - 영숫자 외의 특수 문자(~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 최근 사용한 세 개의 암호는 다시 사용할 수 없습니다.

> **Note**
>
> Google 또는 Apple과 같은 소셜 로그인을 사용하는 AWS Builder ID 계정에서는 암호 변경을 사용할 수 없습니다. 소셜 로그인을 사용하여 로그인한 경우 소셜 로그인 계정을 통해 암호를 관리합니다. 소셜 로그인의 암호를 변경하려면:
>
> - Google 계정의 경우 (Google) 암호 변경 또는 재설정을 참조하세요.
> - Apple 계정의 경우 Apple 계정 암호 변경을 참조하세요.
> - GitHub 계정의 경우 GitHub 액세스 자격 증명 업데이트를 참조하세요.
> - Amazon 계정의 경우 Amazon 암호를 변경하는 방법을 참조하세요.

AWS Builder ID 암호를 변경하려면

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 보안을 선택합니다.
3. 보안 페이지에서 암호 변경를 선택합니다. 그러면 새 페이지로 이동합니다.
4. 암호를 다시 입력하세요 페이지에서 암호 아래에 현재 암호를 입력합니다. 그다음 로그인을 선택합니다.
5. 암호 변경 페이지에서 새 암호 아래에 사용하려는 새 암호를 입력합니다. 그런 다음 암호 확인 아래에 사용하려는 새 암호를 다시 입력합니다.
6. 암호 변경를 선택합니다. AWS Builder ID 프로필로 리디렉션됩니다.

에 대한 모든 활성 세션 삭제 AWS Builder ID

디바이스에 로그인됨 아래에 현재 로그인한 모든 디바이스를 볼 수 있습니다. 디바이스가 인식되지 않는 경우, 보안 모범 사례로, 먼저 암호를 변경하고 그다음 모든 곳에서 로그아웃하십시오. AWS Builder ID의 보안 페이지에서 모든 활성 세션을 삭제하여 모든 디바이스에서 로그아웃할 수 있습니다.

> **Note**
>
> AWS Builder ID 는 IDE에서 Amazon Q Developer에 대한 90일 확장 세션을 지원합니다. 각 새 IDE 로그인에 대해 두 개의 세션 항목을 볼 수 있습니다. IDE에서 로그아웃하면 더 이상 유효하지 않더라도 로그인된 디바이스에 나열된 IDE 세션을 계속 볼 수 있습니다. 이 세션은 90일이 만료되면 사라집니다.

모든 활성 세션 삭제하기

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 보안을 선택합니다.
3. 보안 페이지에서 모든 활성 세션 삭제을 선택합니다.
4. 모든 세션 삭제 대화 상자에서 모두 삭제을 입력합니다. 모든 세션을 삭제하면 다른 브라우저를 AWS Builder ID포함하여를 사용하여 로그인했을 수 있는 모든 디바이스에서 로그아웃합니다. 그런 다음 모든 세션 삭제을 선택합니다.

> **Note**
>
> Google 또는 Apple과 같은 소셜 로그인 계정을 사용하는 경우 활성 AWS Builder ID 세션을 삭제해도 소셜 로그인 계정에서 로그아웃되지 않습니다.

삭제 AWS Builder ID

다음 절차에서는 AWS Builder ID 계정을 삭제하는 방법을 설명합니다.

> **Warning**
>
> 를 삭제 AWS Builder ID 하면 다음과 같은 결과가 발생합니다.

- 액세스 손실 - 더 이상를 통해 이전에 액세스한 AWS 도구 및 서비스에 액세스할 수 없습니다 AWS Builder ID. AWS Builder ID 는 보유한 AWS 계정과 별개이며를 삭제 AWS Builder ID 해도 AWS 계정이 해지되지 않습니다.
- 콘텐츠 삭제 - 와만 연결된 나머지 콘텐츠 AWS Builder ID 는 삭제되며 더 이상를 사용하여 애플리케이션에서 콘텐츠에 액세스하거나 콘텐츠를 복구할 수 없습니다 AWS Builder ID.
- 개인 정보 삭제 -의 생성 및 관리와 관련하여 제공한 모든 개인 정보는 AWS Builder ID 삭제됩니다. 단, 삭제 요청의 기록 또는 사용자를 식별하지 않는 형식의 데이터와 같이에서 요구하거나 허용하는 대로 개인 정보를 보존할 AWS 수 있습니다.

  AWS 개인 정보 보호 고지에서 사용자 정보를 처리하는 방법에 대해 자세히 알아볼 수 있습니다. AWS AWS 커뮤니케이션 기본 설정 센터를 방문하여 커뮤니케이션 기본 설정을 업데이트하거나 구독을 취소할 수 있습니다.
- 소셜 로그인 계정은 변경되지 않음 - Google 또는 Apple과 같은 소셜 로그인을 사용하는 경우를 삭제해도 소셜 로그인 계정과 관련된 어떤 것도 삭제되지 AWS Builder ID 않습니다. 해당 계정을 삭제하는 방법을 알아보려면 소셜 로그인 공급자의 설명서를 참조하세요. 소셜 로그인 계정에서 AWS Builder ID 연결을 삭제해도 AWS Builder ID 계정이 삭제되지는 않지만 더 이상 AWS Builder ID 프로필에 액세스할 수 없습니다.

를 삭제하려면 AWS Builder ID

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 개인 정보 보호 및 데이터를 선택합니다.
3. 개인 정보 보호 및 데이터 페이지에서 삭제 중 AWS Builder ID 아래에서 삭제 AWS Builder ID을 선택합니다.
4. 각 고지 사항 옆의 확인란을 선택하여 계속할 준비가 되었음을 확인합니다.
5. 삭제 AWS Builder ID를 선택합니다.

AWS Builder ID 다중 인증(MFA) 관리

다중 인증(MFA)은 보안을 강화하는 간단하고 효과적인 메커니즘입니다. 첫 번째 요소인 암호는 기억해야 하는 비밀이며 지식 요소라고도 합니다. 다른 요소로는 보유 요소(보안 키 등 귀하가 보유하는 것) 또는 고유 요소(생체인식 스캔 등 귀하에 대한 것)가 있습니다. AWS Builder ID을(를) 위한 추가 레이어를 추가하도록 MFA를 설정하는 것이 좋습니다.

내장된 인증자를 등록하고 물리적으로 안전한 위치에 보관하는 보안 키를 등록할 수 있습니다. 내장된 인증자를 사용할 수 없는 경우 등록된 보안 키를 사용할 수 있습니다. 인증 애플리케이션의 경우, 해당 앱에서 클라우드 백업 또는 동기화 기능을 활성화할 수도 있습니다. 이렇게 하면 MFA 디바이스가 분실되거나 파손된 경우에도 프로필에 대한 액세스 권한을 잃지 않도록 할 수 있습니다.

중요 사항

- 여러 개의 MFA 디바이스를 등록하는 것이 좋습니다. 등록된 모든 MFA 디바이스에 대한 액세스 권한을 상실한 경우에는 AWS Builder ID을(를) 복구할 수 없습니다.
- 등록된 MFA 디바이스를 정기적으로 검토하여 최신 상태이고 작동하는지 확인하는 것이 좋습니다. 또한 이러한 디바이스를 사용하지 않을 때는 물리적으로 안전한 장소에 보관해야 합니다.
- Google로 계속을 사용하여 계정을 생성한 경우 Google 계정을 통해 다중 인증을 활성화할 수 있습니다. 자세한 내용은 2-Step 확인 켜기를 참조하세요.
- Apple에서 계속을 사용하여 계정을 생성한 경우 Apple 계정에서 다중 인증이 이미 활성화되어 있을 수 있습니다. 그렇지 않은 경우 활성화 방법에 대한 자세한 내용은 Apple 계정에 대한 2단계 인증을 참조하세요.
- GitHub로 계속을 사용하여 계정을 생성한 경우 GitHub 계정을 통해 다중 인증을 활성화할 수 있습니다. 자세한 내용은 (GitHub) 2단계 인증 구성을 참조하세요.
- Amazon에서 계속을 사용하여 계정을 생성한 경우 Amazon 계정을 통해 다중 인증을 활성화할 수 있습니다. 자세한 내용은 2단계 확인이란 무엇입니까?를 참조하세요.

에 사용 가능한 MFA 유형 AWS Builder ID

AWS Builder ID 는 다음과 같은 다중 인증(MFA) 디바이스 유형을 지원합니다.

FIDO2 인증자

FIDO2는 CTAP2 및 WebAuthn을 포함하는 표준이며, 공개 키 암호화를 기반으로 합니다. FIDO 보안 인증은 AWS와 같이 해당 보안 인증이 생성된 웹사이트에 고유한 것이므로 피싱 방지 기능이 있습니다.

AWS 는 FIDO 인증자에 대해 가장 일반적인 두 가지 폼 팩터인 내장 인증자와 보안 키를 지원합니다. 가장 일반적인 유형의 FIDO 인증자에 대한 자세한 내용은 아래를 참조하세요.

주제

- 내장된 인증자

- 보안 키
- 암호 관리자, 패스키 공급자, 기타 FIDO 인증자

내장된 인증자

MacBook의 TouchID 또는 Windows Hello 호환 카메라와 같이 일부 디바이스에는 내장된 인증자가 있습니다. 디바이스가 WebAuthn을 비롯한 FIDO 프로토콜과 호환되는 경우, 지문이나 얼굴을 2차 요소로 사용할 수 있습니다. 자세한 내용은 FIDO 인증을 참조하세요.

보안 키

FIDO2와 호환되는 외부 USB, BLE 또는 NFC 연결 보안 키를 구입할 수 있습니다. MFA 디바이스에 대한 메시지가 표시되면 해당 키의 센서를 누릅니다. YubiKey 또는 Feitian은 호환되는 디바이스를 만듭니다. 호환되는 모든 보안 키 목록은 FIDO 인증 제품을 참조하십시오.

암호 관리자, 패스키 공급자, 기타 FIDO 인증자

여러 제3자 공급자는 모바일 애플리케이션에서 암호 관리자, FIDO 모드가 있는 스마트 카드 및 기타 폼 팩터의 기능으로 FIDO 인증을 지원합니다. 이러한 FIDO 호환 디바이스는 IAM Identity Center에서도 작동할 수 있지만, MFA에 이 옵션을 활성화하기 전에 FIDO 인증자를 직접 테스트해 보는 것이 좋습니다.

> **Note**
>
> 일부 FIDO 인증자는 패스키라고 하는 검색 가능한 FIDO 보안 인증을 생성할 수 있습니다. 패스키는 이를 생성한 디바이스에 바인딩되거나, 클라우드에 동기화되거나 백업될 수 있습니다. 예를 들어, 지원되는 Macbook에서 Apple Touch ID를 사용하여 패스키를 등록한 다음, 로그인 시 화면에 표시되는 메시지에 따라 iCloud에 있는 패스키를 사용하여 Google Chrome을 사용하는 Windows 노트북에서 어떠한 사이트에 로그인할 수 있습니다. 동기화 가능한 패스키를 지원하는 디바이스 및 운영 체제와 브라우저 간의 현재 패스키 상호 운용성에 대한 자세한 내용은 FIDO Alliance And World Wide Web Consortium(W3C)에서 관리하는 리소스인 passkeys.dev에서 디바이스 지원을 참조하십시오.

인증 애플리케이션

인증 앱은 일회용 암호(OTP) 기반 제3자 인증자입니다. 모바일 디바이스 또는 태블릿에 설치된 인증 애플리케이션을 승인된 MFA 디바이스로 사용할 수 있습니다. 제3자 인증 애플리케이션은 6자리 인증

코드를 생성할 수 있는 표준 기반 시간 기반 일회용 암호(TOTP) 알고리즘인 RFC 6238과 호환되어야 합니다.

MFA에 대한 메시지가 표시되면 제공된 입력 상자에 인증 앱에서 보낸 유효한 코드를 입력해야 합니다. 사용자에게 할당된 각 MFA 디바이스는 고유해야 합니다. 특정 사용자에 대해 두 개의 인증 앱을 등록할 수 있습니다.

다음과 같은 잘 알려진 제3자 인증 앱 중에서 선택할 수 있습니다. 그러나 모든 TOTP 준수 애플리케이션은 AWS Builder ID MFA에서 작동합니다.

운영 체제	테스트를 거친 인증 앱
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

AWS Builder ID MFA 디바이스 등록

> **Note**
>
> MFA 가입 이후, 로그아웃한 다음 동일한 디바이스에 다시 로그인하면 신뢰할 수 있는 디바이스에서 MFA에 대한 메시지가 표시되지 않을 수 있습니다.

인증 앱을 사용하여 MFA 디바이스 등록하기

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 보안을 선택합니다.
3. 보안 페이지에서 디바이스 등록를 선택합니다.
4. MFA 디바이스 등록 페이지에서 Authenticator 앱을 선택합니다.
5. AWS Builder ID 는 QR 코드 그래픽을 포함한 구성 정보를 작동하고 표시합니다. 이 그래픽은 QR 코드를 지원하지 않는 인증 앱에서 수동 입력할 수 있는 '보안 구성 키'를 표시한 것입니다.
6. 인증 앱을 엽니다. 앱 목록은 인증 애플리케이션 섹션을 참조하세요.

인증 앱이 다수의 MFA 디바이스 또는 계정을 지원하는 경우 새로운 MFA 디바이스 또는 계정을 생성하는 옵션을 선택합니다.

7. MFA 앱의 QR 코드 지원 여부를 결정한 후 인증 관리자 앱 설정 페이지에서 다음 중 한 가지를 실행합니다.

   1. QR 코드 표시를 선택한 다음 해당 앱을 사용하여 QR 코드를 스캔합니다. 예를 들어, 카메라 모양의 아이콘을 선택하거나 코드 스캔와 비슷한 옵션을 선택합니다. 그런 다음 디바이스의 카메라를 사용하여 해당 코드를 스캔합니다.
   2. Show Secret key를 선택한 다음 MFA 앱에 해당 비밀 키를 입력합니다.

   작업을 마치면 인증 앱이 일회용 암호를 생성하여 표시합니다.

8. Authenticator 코드 상자에 현재 인증 앱에 표시되는 일회용 암호를 입력합니다. Assign MFA(MFA 할당)을 선택합니다.

   > **Important**
   >
   > 코드를 생성한 후 즉시 요청을 제출하세요. 코드를 생성한 다음 요청을 제출하기 위해 너무 오래 기다리면 MFA 디바이스가와 성공적으로 연결 AWS Builder ID되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화할 수 있습니다. 자세한 내용은 인증 앱으로 등록하거나 로그인하려고 시도하면 '예상치 못한 오류가 발생했습니다'라는 메시지가 나타납니다. 단원을 참조하십시오.

9. 디바이스에 친숙한 이름을 지정하려면 이름 바꾸기를 AWS Builder ID선택합니다. 이 이름은 이 디바이스를 등록한 다른 디바이스와 구별하는 데 도움이 됩니다.

이제 MFA 디바이스를 사용할 준비가 되었습니다 AWS Builder ID.

보안 키를 AWS Builder ID MFA 디바이스로 등록

보안 키를 사용하여 MFA 디바이스 등록하기

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 보안을 선택합니다.
3. 보안 페이지에서 디바이스 등록를 선택합니다.
4. MFA 디바이스 등록 페이지에서 보안 키를 선택합니다.

5. 보안 키가 활성화되어 있는지 확인하십시오. 별도의 물리적 보안 키를 사용하는 경우 이를 컴퓨터에 연결하세요.
6. 화면에 표시되는 지시 사항을 따릅니다. 운영 체제 및 브라우저에 따라 환경이 달라집니다.
7. 디바이스에 친숙한 이름을 지정하려면 이름 바꾸기를 AWS Builder ID선택합니다. 이 이름은 이 디바이스를 등록한 다른 디바이스와 구별하는 데 도움이 됩니다.

이제 MFA 디바이스를 사용할 준비가 되었습니다 AWS Builder ID.

AWS Builder ID MFA 디바이스 이름 바꾸기

MFA 디바이스의 이름을 변경하기

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 보안을 선택합니다. 이 페이지로 이동하면 이름 바꾸기이 회색으로 표시됩니다.
3. 변경할 MFA 디바이스를 선택합니다. 이렇게 하면 이름 바꾸기을 선택할 수 있습니다. 대화 상자가 나타납니다.
4. 표시되는 메시지에서 MFA 디바이스 이름에 새 이름을 입력하고 이름 바꾸기을 선택합니다. 이름이 변경된 디바이스는 다중 인증(MFA) 디바이스 아래에 표시됩니다.

MFA 디바이스 삭제

활성 MFA 디바이스를 두 개 이상 유지하는 것이 좋습니다. 디바이스를 제거하기 전에 교체 MFA 디바이스를 등록하는 방법에 대해 AWS Builder ID MFA 디바이스 등록을(를) 참조하십시오. 에 대한 멀티 팩터 인증을 비활성화하려면 프로필에서 등록된 모든 MFA 디바이스를 AWS Builder ID제거합니다.

MFA 디바이스 삭제하기

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 보안을 선택합니다.
3. 삭제하려는 MFA 디바이스를 선택하고 삭제을 선택합니다.
4. MFA 디바이스 삭제? 모달에서 지시사항에 따라 디바이스를 삭제하십시오.
5. 삭제을 선택합니다.

삭제된 디바이스는 더 이상 다중 인증(MFA) 디바이스 아래에 표시되지 않습니다.

의 개인 정보 보호 및 데이터 AWS Builder ID

AWS 개인정보 취급방침에서는 개인 데이터를 처리하는 방법이 간략하게 설명됩니다. AWS Builder ID 프로필을 삭제하는 방법에 대한 자세한 내용은 섹션을 참조하세요삭제 AWS Builder ID.

AWS Builder ID 데이터 요청

및 로 액세스한 AWS 애플리케이션 및 서비스와 관련된 개인 정보를 요청 AWS Builder ID 하고 볼 수 있습니다 AWS Builder ID. 다른 AWS 웹 사이트, 애플리케이션, 제품, 서비스, 이벤트 및 경험과 관련하여 제공되는 개인 정보를 포함하여 데이터 주체 권리를 행사하는 방법에 대한 자세한 내용은 섹션을 참조하세요https://aws.amazon.com/privacy.

데이터 요청

1. 에서 AWS Builder ID 프로필에 로그인합니다https://profile.aws.amazon.com.
2. 내 AWS Builder ID 데이터를 선택합니다.
3. 내 AWS Builder ID 데이터 페이지의 삭제 AWS Builder ID에서 데이터 요청을 선택합니다.
4. 요청이 접수되었다는 녹색 확인 메시지가 페이지 상단에 표시되며, 30일 이내에 해당 요청을 완료할 것입니다.
5. 요청이 처리되었다는 이메일을 받으면 AWS Builder ID 프로필의 개인 정보 보호 및 데이터 페이지로 다시 이동하십시오. 새로 사용할 수 있는 데이터를 가진 ZIP 아카이브 다운로드 버튼을 선택하십시오.

   데이터 요청이 보류 중인 동안에는 AWS Builder ID을(를) 삭제할 수 없습니다.

AWS Builder ID 및 기타 AWS 자격 증명

AWS Builder ID 는 AWS 계정 또는 로그인 자격 증명과 별개입니다. AWS Builder ID 와의 루트 사용자 이메일에 동일한 이메일을 사용할 수 있습니다 AWS 계정.

AWS Builder ID:

- 를 사용하는 도구 및 서비스에 액세스할 수 있습니다 AWS Builder ID.
- AWS 계정 또는 애플리케이션에서 지정한 정책 및 구성과 같은 기존 보안 제어에는 영향을 주지 않습니다.
- 기존 루트, IAM Identity Center 또는 IAM 사용자, 보안 인증 또는 계정을 대체하지 않습니다.

- AWS Management Console, AWS CLI, AWS SDKs 또는 AWS 도구 키트에 액세스하기 위한 AWS IAM 자격 증명을 가져올 수 없습니다.

AWS 계정 는 연락처 및 결제 정보가 포함된 리소스 컨테이너입니다. S3, EC2 또는 Lambda와 같은 청구 및 측정 AWS 서비스를 운영할 보안 경계를 설정합니다. 계정 소유자는 AWS 계정 에서에 로그인할 수 있습니다 AWS Management Console. 자세한 내용은 AWS Management Console에 로그인을 참조하세요.

가 기존 IAM Identity Center 자격 증명과 AWS Builder ID 연결되는 방법

해당 ID를 소유한 개인으로서 귀하는 AWS Builder ID을(를) 관리합니다. 이는 학교나 직장 등 다른 조직에 대해 가지고 있을 수 있는 다른 어떤 ID와도 관련이 없습니다. IAM Identity Center의 직원 자격 증명을 사용하여 작업 자신을 표현하고를 사용하여 프라이빗 자신을 표현 AWS Builder ID 할 수 있습니다. 이러한 ID는 독립적으로 작동합니다.

AWS IAM Identity Center(AWS Single Sign-On 후속)의 사용자는 기업 IT 또는 클라우드 관리자 또는 Okta, Ping 또는 Azure와 같은 조직의 ID 제공업체 관리자가 관리합니다. IAM Identity Center의 사용자는 AWS Organizations에서 여러 계정 전반의 리소스에 액세스할 수 있습니다.

다중 AWS Builder ID 프로필

각 ID가 고유한 이메일 주소를 사용하는 AWS Builder ID 한 두 개 이상을 생성할 수 있습니다. 그러나 둘 이상을 사용하면 어떤 용도로 사용 AWS Builder ID 했는지 기억하기 어려울 AWS Builder ID 수 있습니다. 가능하면 AWS 도구 및 서비스의 AWS Builder ID 모든 활동에 단일를 사용하는 것이 좋습니다.

에서 로그아웃 AWS

에서 로그아웃하는 방법은 사용자 유형에 AWS 계정 따라 다릅니다 AWS . 계정 루트 사용자, IAM 사용자, IAM Identity Center의 사용자, 페더레이션 ID 또는 AWS Builder ID 사용자일 수 있습니다. 어떤 유형의 사용자인지 잘 모르겠으면 사용자 유형 결정 섹션을 참조하세요.

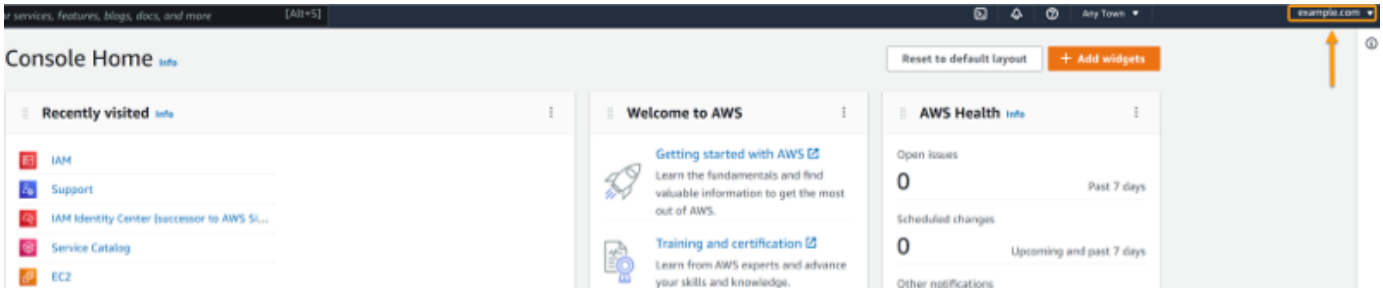
주제

- 에서 로그아웃 AWS Management Console
- AWS 액세스 포털에서 로그아웃
- AWS Builder ID에서 로그아웃

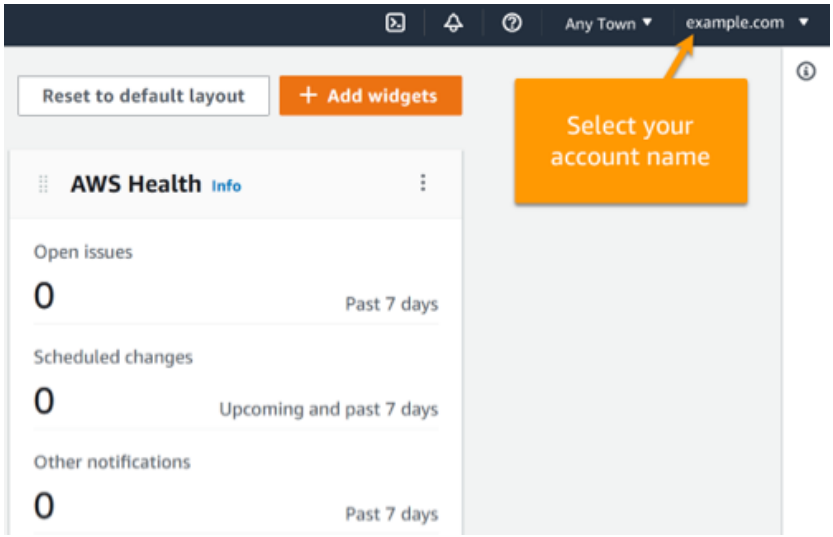
에서 로그아웃 AWS Management Console

에서 로그아웃하려면 AWS Management Console

1. 에 로그인하면 다음 이미지에 표시된 것과 유사한 페이지에 AWS Management Console도착합니다. 계정 이름 또는 IAM 사용자 이름이 오른쪽 상단 모서리에 표시됩니다.



2. 상단 오른쪽 모서리에 있는 탐색 모음에서 사용자 이름을 선택합니다.



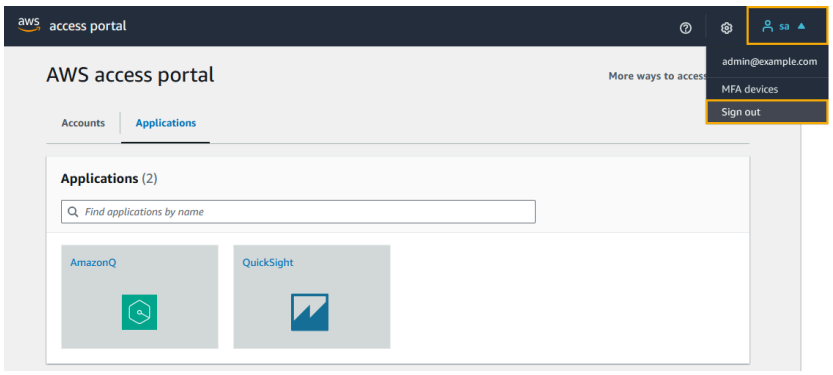
3. 로그아웃 옵션을 선택합니다. 로그인된 계정 수에 따라 버튼 옵션이 달라집니다.
   - 하나의 계정에만 로그인한 경우 로그아웃을 선택합니다.
   - 모든 세션에서 로그아웃을 선택하여 모든 자격 증명에서 동시에 로그아웃합니다.
   - 현재 세션에서 로그아웃을 선택하여 선택한 자격 증명에서 로그아웃합니다.
4. AWS Management Console 웹 페이지로 돌아갑니다.

여러 계정에 로그인하는 방법에 대한 자세한 내용은 AWS Management Console 시작하기 안내서의 여러 계정에 로그인하기를 참조하세요.

AWS 액세스 포털에서 로그아웃

AWS 액세스 포털에서 로그아웃하려면

1. 상단 오른쪽 모서리에 있는 탐색 모음에서 사용자 이름을 선택합니다.
2. 다음 이미지에 표시된 대로 로그아웃을 선택합니다.



3. 성공적으로 로그아웃하면 이제 AWS 액세스 포털 로그인 페이지가 표시됩니다.

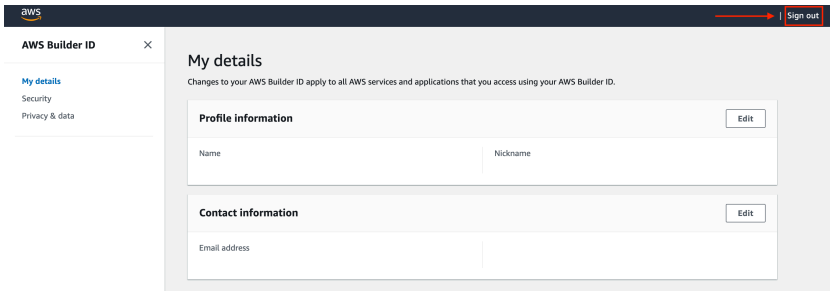
외부 ID 제공업체(IdP)를 ID 소스로 사용하는 경우 로그아웃해도 자격 증명의 활성 세션이 종료되지 않습니다. AWS 액세스 포털로 다시 이동하면, 자격 증명을 제공하지 않고도 자동으로 로그인될 수 있습니다.

AWS Builder ID에서 로그아웃

AWS Builder ID를 사용하여 액세스한 AWS 서비스에서 로그아웃하려면 서비스에서 로그아웃해야 합니다. AWS Builder ID 프로파일에서 로그아웃하려면 다음 절차를 참조하세요.

AWS Builder ID 프로파일에서 로그아웃하려면

1. 에서 AWS Builder ID 프로필에 로그인https://profile.aws.amazon.com/하면 내 세부 정보에 도착합니다.
2. AWS Builder ID 프로필 페이지의 오른쪽 상단에서 로그아웃을 선택합니다.



3. AWS Builder ID 프로필이 더 이상 표시되지 않으면 로그아웃된 것입니다.

AWS 계정 로그인 문제 해결

여기의 정보를 사용하여 로그인 및 기타 AWS 계정 문제를 해결할 수 있습니다. 에 로그인하는 방법에 대한 step-by-step 지침은 섹션을 AWS 계정참조하세요에 로그인 AWS Management Console.

로그인 문제를 해결하는 데 도움이 되는 문제 해결 주제가 없는 경우 다음 양식을 작성하여 지원 로 사례를 생성할 수 있습니다. 저는 고객이며 결제 또는 계정 지원을 찾고 있습니다. AWS 보안 모범 사례로 지원 는 로그인한 계정 AWS 계정 이외의 다른 계정의 세부 정보를 논의할 수 없습니다. 또한 AWS Support는 어떤 이유로든 계정과 연결된 보안 인증을 변경할 수 없습니다.

> **Note**
>
> 지원 는 지원 담당자에게 문의하기 위한 직통 전화번호를 게시하지 않습니다.

로그인 문제 해결에 대한 자세한 내용은에 로그인하거나에 액세스하는 데 문제가 있는 경우 어떻게 해야 하나요 AWS 계정?를 참조하세요. Amazon.com에 로그인하는 데 문제가 있는 경우 이 페이지 대신 Amazon 고객 서비스를 참조하세요.

주제

- 자격 AWS Management Console 증명이 작동하지 않음
- 루트 사용자의 경우 암호 재설정이 필요함
- 내의 이메일에 액세스할 수 없음 AWS 계정
- 내 MFA 디바이스가 분실되거나 작동 중단됨
- AWS Management Console 로그인 페이지에 액세스할 수 없음
- 로그인 리소스 기반 정책의 네트워크 조건으로 인해 로그인할 수 없음
- 콘솔 권한 부여를 활성화한 후 계정이 잠겼습니다.
- 정책 변경 사항이 적용되지 않음
- AWS 계정 ID 또는 별칭을 찾으려면 어떻게 해야 합니까?
- 내 계정 확인 코드가 필요함
- 에 대한 루트 사용자 암호를 잊어버렸습니다. AWS 계정
- 에 대한 IAM 사용자 암호를 잊어버렸습니다. AWS 계정
- 내에 대한 연동 자격 증명 암호를 잊어버렸습니다. AWS 계정
- 기존에 로그인할 수 AWS 계정 없으며 동일한 이메일 주소로 새 AWS 계정 를 생성할 수 없습니다.

- 일시 중지된를 다시 활성화해야 합니다. AWS 계정
- 로그인 문제를 위해 지원 에 문의해야 합니다.
- 결제 문제에 AWS Billing 대해에 문의해야 합니다.
- 소매 주문에 대해 질문이 있음
- 내를 관리하는 데 도움이 필요합니다. AWS 계정
- AWS 액세스 포털 자격 증명이 작동하지 않음
- 에 대한 IAM Identity Center 암호를 잊어버렸습니다. AWS 계정
- IAM Identity Center 콘솔에 로그인하려고 할 때 'It's not you, it's us'라는 오류 발생

자격 AWS Management Console 증명이 작동하지 않음

사용자 이름과 암호는 기억하지만 보안 인증이 작동하지 않는 경우, 페이지를 잘못 찾은 것일 수 있습니다. 다른 페이지에서 로그인해 보세요.

루트 사용자 로그인 페이지

- 를 생성하거나 소유하고 루트 사용자 자격 증명이 필요한 작업을 AWS 계정 수행하는 경우에 계정 이메일 주소를 입력합니다AWS Management Console. 루트 사용자에 액세스하는 방법을 알아보려면 루트 사용자로 로그인하기 섹션을 참조하세요. 루트 사용자 암호를 잊어버린 경우 재설정할 수 있습니다. 자세한 정보는 에 대한 루트 사용자 암호를 잊어버렸습니다. AWS 계정을 참조하세요. 루트 사용자 이메일 주소를 잊어버린 경우 이메일 받은 편지함에서 AWS에서 보낸 이메일을 확인하십시오.
- 루트 사용자 계정에 로그인하려 했으나 나의 루트 사용자 계정에는 암호 복구가 비활성화되어 있으며, 루트 사용자 자격 증명이 없습니다.'라는 오류가 발생한 경우 루트 사용자로 로그인하거나 계정의 루트 사용자에 대한 암호 복구를 수행할 수 없습니다.를 사용하여 관리되는 AWS 멤버 계정에는 루트 사용자 암호, 액세스 키, 서명 인증서 또는 활성 다중 인증(MFA)이 없을 AWS Organizations 수 있습니다.

  루트 사용자 작업은 관리 계정이나 IAM에 대한 위임된 관리자만이 멤버 계정에서 수행할 수 있습니다. 루트 사용자 자격 증명이 필요한 태스크를 수행해야 하는 경우 관리자에게 문의하세요. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 멤버 계정에 대한 루트 액세스 중앙 관리를 참조하세요.

IAM 사용자 로그인 페이지

- 사용자 또는 다른 사용자가 내에서 IAM 사용자를 생성한 경우 로그인하려면 해당 AWS 계정 ID 또는 별칭을 알아야 AWS 계정합니다. AWS Management Console에 계정 ID 또는 별칭, 사용자 이름, 암호를 입력합니다. IAM 사용자 로그인 페이지에 액세스하는 방법을 알아보려면 IAM 사용자로 로그인하기 섹션을 참조하세요. IAM 사용자 암호를 잊어버린 경우, IAM 사용자 암호 재설정에 대한 정보는 에 대한 IAM 사용자 암호를 잊어버렸습니다. AWS 계정을(를) 참조하세요. 계정 번호를 잊어버린 경우 이메일, 브라우저 즐겨찾기 또는 브라우저 기록에서 `signin.aws.amazon.com/`을(를) 포함하는 URL을 검색하세요. 계정 ID 또는 별칭은 URL의 `"account="` 텍스트를 따릅니다. 계정 ID 또는 별칭을 찾을 수 없는 경우 administrator. 지원 cant help you recover this information. 로그인하기 전까지는 계정 ID 또는 별칭을 볼 수 없습니다.

루트 사용자의 경우 암호 재설정이 필요함

계정 보호를 위해 AWS Management Console에 로그인하려고 하면 다음 메시지가 표시될 수 있습니다.

암호 재설정이 필요합니다. 보안을 고려하여 암호를 재설정해야 합니다. 계정을 안전하게 유지하려면 아래에서 암호 분실을 선택하고 암호를 재설정해야 합니다.

이 메시지 외에도는 계정과 연결된 이메일을 통해 잠재적 문제를 식별할 때도 AWS 알려줍니다. 이 이메일에는 암호 재설정이 필요한 이유가 포함되어 있습니다. 예를 들어,에 대한 비정상적인 로그인 활동을 식별하거나와 연결된 AWS 계정 자격 증명을 온라인으로 AWS 계정 공개적으로 사용할 수 있습니다.

루트 사용자 자격 증명을 안전하게 유지하도록 암호를 업데이트합니다. 루트 사용자 암호를 재설정하는 방법을 알아보려면 내 AWS 계정의 루트 사용자 암호를 잊음을 참조하세요.

내의 이메일에 액세스할 수 없음 AWS 계정

를 생성할 때 이메일 주소와 암호를 AWS 계정제공합니다. AWS 계정 루트 사용자의 자격 증명입니다. 와 연결된 이메일 주소가 확실하지 않은 경우 AWS 계정를 여는 데 사용되었을 수 있는 조직의 이메일 주소로 @signin.aws 또는 @verify.signin.aws로 끝나는 저장된 서신을 찾습니다 AWS 계정. 소속 팀, 조직 또는 가족의 다른 구성원에게 물어보세요. 아는 사람이 해당 계정을 만들었다면 액세스 권한을 얻도록 도와줄 수 있습니다.

이메일 주소를 알고 있지만 더 이상 이메일에 액세스할 수 없는 경우 먼저 다음 옵션 중 하나를 사용하여 이메일에 대한 액세스를 복구해 보세요.

- 이메일 주소의 도메인을 소유한 경우 삭제된 이메일 주소를 복원할 수 있습니다. 또는 더 이상 메일 서버에 존재하지 않는 이메일 주소로 보낸 메시지를 모두 포착하고 다른 이메일 주소로 리디렉션하는 이메일 계정에 대한 catch-all을 설정할 수 있습니다.
- 계정의 이메일 주소가 회사 이메일 시스템에 속한 경우라면 IT 시스템 관리자에게 문의하는 것이 좋습니다. 시스템 관리자가 이메일 주소에 대한 액세스 권한을 다시 받을 수 있도록 도와 줄 것입니다.

여전히에 로그인할 수 없는 경우에 문의하여 대체 지원 옵션을 찾을 AWS 계정수 있습니다 지원.

내 MFA 디바이스가 분실되거나 작동 중단됨

MFA 디바이스를 분실했거나, 손상되었거나, 작동하지 않는 경우, MFA 인증 요청을 보내도 일회용 암호(OTP)를 받지 못합니다.

IAM 사용자

동일한 IAM 사용자에게 등록된 다른 MFA 디바이스를 사용하여 로그인할 수 있습니다.

작동하지 않는 MFA 디바이스를 비활성화하려면 IAM 사용자는 관리자에게 연락해야 합니다. 이러한 사용자는 관리자의 도움 없이는 MFA 디바이스를 복구할 수 없습니다. 관리자는 일반적으로 조직의 다른 구성원 AWS 계정 보다에 대한 더 높은 수준의 권한을 가진 정보 기술(IT) 직원입니다. 이 개인은 귀하의 계정을 만들었고 사용자에게 로그인할 수 있는 액세스 보안 인증을 제공합니다.

루트 사용자

루트 사용자에 대한 액세스 권한을 복구하려면, 동일한 루트 사용자에게 등록된 다른 MFA 디바이스를 사용하여 로그인해야 합니다. 그런 다음, MFA 디바이스를 복구하거나 업데이트할 수 있는 다음 옵션들을 검토하십시오.

- MFA 디바이스 복구에 대한 단계별 지침은 MFA 디바이스 분실 또는 작동 중단 시 어떻게 해야 하나요?를 참조하십시오.
- MFA 디바이스의 전화번호를 업데이트하는 방법에 대한 단계별 지침은 분실한 MFA 디바이스를 재설정하기 위해 전화번호를 업데이트하려면 어떻게 해야 하나요?를 참조하십시오.
- MFA 디바이스를 활성화하는 step-by-step 지침은 에서 사용자를 위한 MFA 디바이스 활성화 AWS를 참조하세요.
- MFA 디바이스를 복구할 수 없는 경우 지원에 문의하세요.

> **Note**
>
> IAM 사용자는 관리자에게 문의하여 MFA 디바이스에 대한 지원을 받아야 합니다.는 MFA 디바이스 문제에 대해 IAM 사용자를 지원할 지원 수 없습니다.

AWS Management Console 로그인 페이지에 액세스할 수 없음

로그인 페이지가 표시되지 않는 경우, 도메인이 방화벽에 의해 차단되었을 수 있습니다. 네트워크 관리자에게 문의하여 사용자 유형과 로그인 방법에 따라 웹 콘텐츠 필터링 솔루션 허용 목록에 다음 도메인 또는 URL 엔드포인트를 추가하세요.

루트 사용자 및 IAM 사용자	*.signin.aws.amazon.com
Amazon.com 계정 로그인	www.amazon.com
IAM Identity Center 사용자 및 자사 애플리케이션 로그인	• *.awsapps.com (http://awsapps.com/) • *.signin.aws

로그인 리소스 기반 정책의 네트워크 조건으로 인해 로그인할 수 없음

다음 오류 메시지 중 하나가 표시되면 로그인 리소스 기반 정책 또는 리소스 제어 정책(RCP)이 네트워크 위치에 따라 액세스를 제한할 수 있습니다.

- “인증 정보가 잘못되었습니다. 다시 시도하세요.”
- “인증 실패 잘못된 요청”
- “인증 실패:이 계정에 액세스하려면 다른 네트워크에서 로그인하거나 관리자에게 자세한 내용을 문의하세요.”

자세한 문제 해결 단계는 관리자에게 문의하거나 로그인 리소스 기반 정책의 네트워크 조건으로 인해 로그인할 수 없음 섹션을 참조하세요.

콘솔 권한 부여를 활성화한 후 계정이 잠겼습니다.

콘솔 인증을 구성했고 계정에 더 이상 액세스할 수 없는 경우 정책을 적용하기 전에 제외된 보안 주체 또는 긴급 복구 액세스를 구성하지 않았을 수 있습니다. AWS CLI 셀프 서비스, `OrganizationAccountAccessRole`및 AWS 지원 옵션을 포함한 해결 단계는 섹션을 참조하세요콘솔 권한 부여를 활성화한 후 계정이 잠겼습니다..

정책 변경 사항이 적용되지 않음

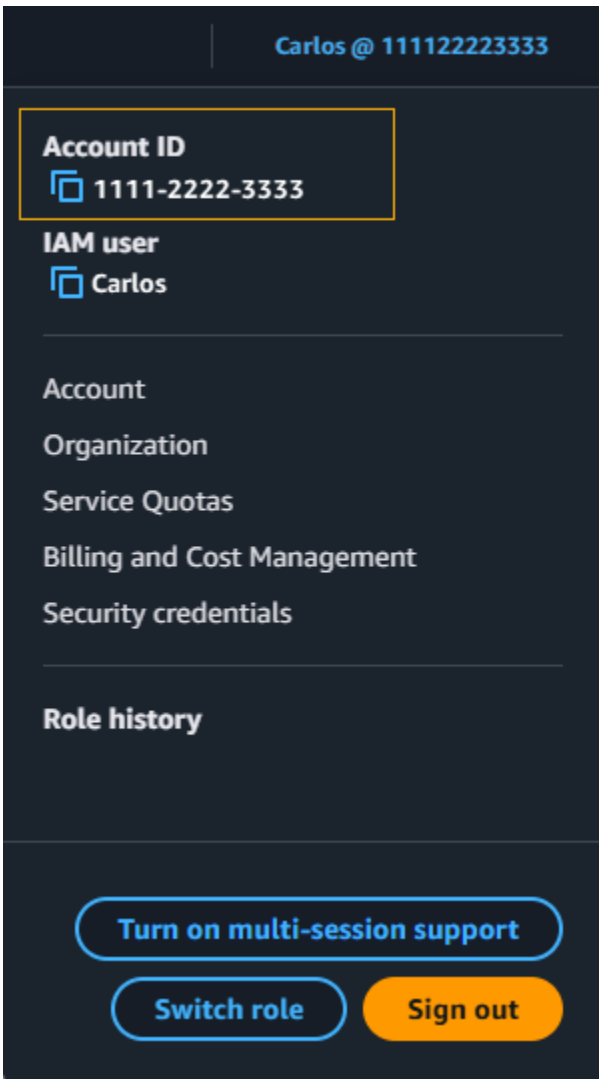
콘솔 권한 부여 구성 및 리소스 권한 문에 대한 변경 사항은 전역적으로 복제되며 적용되는 데 몇 분 정도 걸릴 수 있습니다. 대기 후 변경 사항이 표시되지 않는 경우 문제 해결 단계는 변경 사항이 매번 즉시 표시되는 것은 아닙니다 섹션을 참조하세요.

AWS 계정 ID 또는 별칭을 찾으려면 어떻게 해야 합니까?

IAM 사용자인 경우 로그인하지 않았으면 관리자에게 AWS 계정 ID 또는 별칭을 요청하세요. 관리자는 일반적으로 조직의 다른 구성원 AWS 계정 보다에 대한 더 높은 수준의 권한을 가진 정보 기술(IT) 직원입니다. 이 개인은 귀하의 계정을 만들었고 사용자에게 로그인할 수 있는 액세스 보안 인증을 제공합니다.

에 액세스할 수 있는 IAM 사용자인 경우 로그인 URL에서 AWS Management Console계정 ID를 찾을 수 있습니다. 관리자가 보낸 이메일에서 로그인 URL을 확인하세요. 계정 ID는 로그인 URL의 처음 12자리입니다. 예를 들어 다음 URL에서 `https://`*`111122223333`*`.signin.aws.amazon.com/console` AWS 계정 ID는 111122223333입니다.

에 로그인한 후 해당 리전 옆의 탐색 모음에서 계정 정보를 찾을 AWS Management Console수 있습니다. 예를 들어 다음 스크린샷에서 IAM 사용자 Carlos의는 AWS 계정 1111-2222-3333입니다.



AWS 계정 ID 및 별칭과 ID 및 별칭을 찾는 방법에 대한 자세한 내용은 AWS 계정 ID 및 별칭을 참조하세요.

내 계정 확인 코드가 필요함

계정 이메일 주소와 암호를 제공한 경우 AWS 경우에 따라 일회성 확인 코드를 제공해야 합니다. 확인 코드를 검색하려면와 연결된 이메일에서 Amazon Web Services의 AWS 계정 메시지를 확인합니다. 해당 이메일 주소는 @signin.aws 또는 @verify.signin.aws로 끝납니다. 메시지의 지침을 따릅니다. 계정으로 메시지가 오지 않았으면 스팸 및 정크 폴더를 확인합니다. 그 이메일에 더 이상 액세스할 수 없는 경우에는 내의 이메일에 액세스할 수 없음 AWS 계정 섹션을 참조하세요.

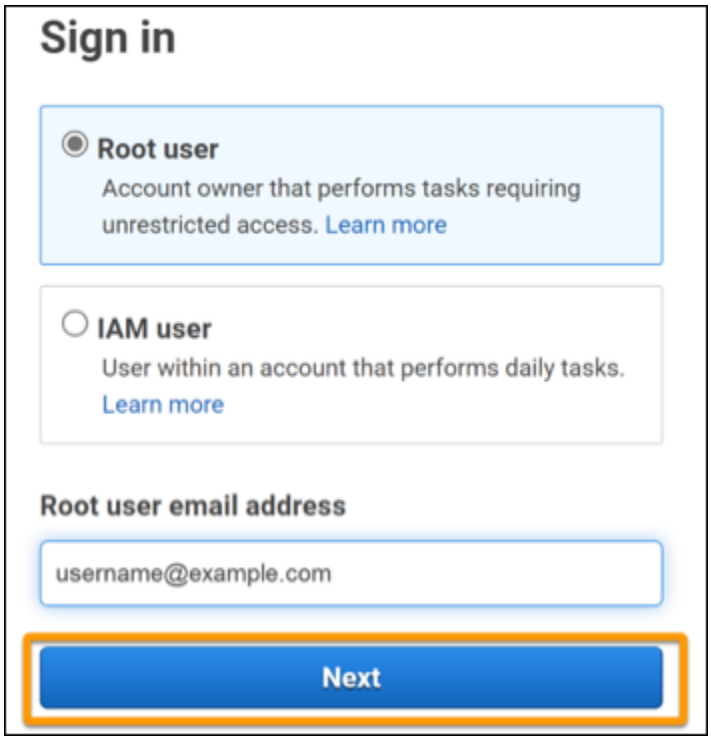
에 대한 루트 사용자 암호를 잊어버렸습니다. AWS 계정

루트 사용자이고 암호를 분실했거나 잊어버린 경우에서 "암호 찾기" 링크를 선택하여 암호를 재설정 AWS 계정할 수 있습니다 AWS Management Console. AWS 계정의 이메일 주소를 알고 있어야 하며 이메일 계정에 액세스할 수 있어야 합니다. 암호 복구 프로세스 중에 암호를 재설정할 수 있는 링크가 이메일로 전송됩니다. 링크는를 생성하는 데 사용한 이메일 주소로 전송됩니다 AWS 계정.

AWS Organizations를 사용하여 생성한 계정의 암호를 재설정하려면 루트 사용자로 멤버 계정 액세스를 참조하세요.

루트 사용자 암호 재설정하기

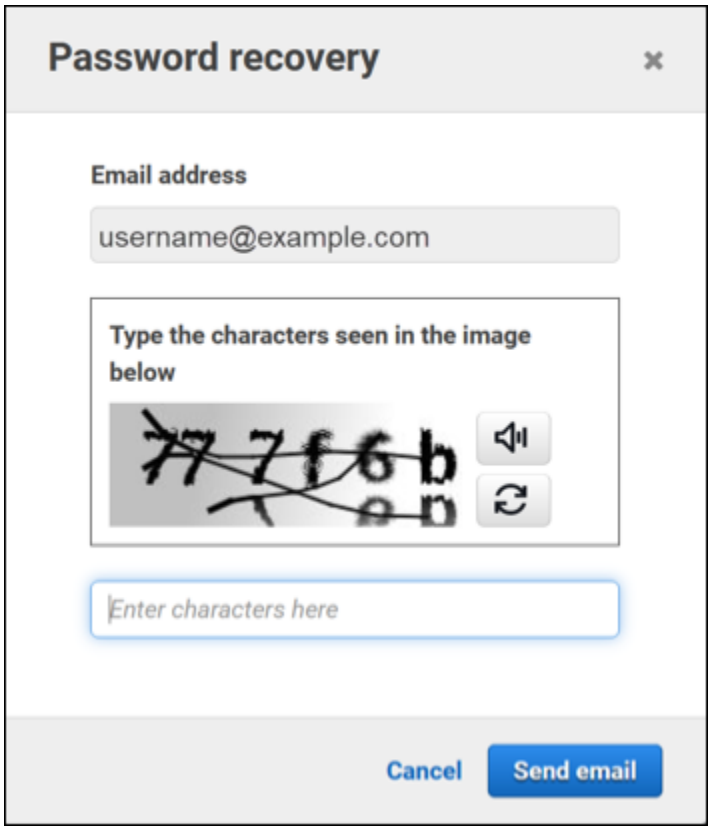
1. AWS 이메일 주소를 사용하여 AWS 관리 콘솔에 루트 사용자로 로그인을 시작합니다. 그리고 다음을 선택합니다.



> **Note**
>
> AWS Management Console에 IAM 사용자 보안 인증을 사용하여 로그인한 경우, 로그아웃해야 루트 사용자 암호를 재설정할 수 있습니다. 해당 계정의 IAM 사용자 로그인 페이지가 표시되면, 페이지 하단에 있는 루트 계정 자격 증명을 사용한 로그인(Sign-in using root account credentials)을 선택합니다. 필요한 경우 계정 이메일 주소를 입력하고 다음을 선택하여 Root user sign in(루트 사용자 로그인) 페이지에 액세스합니다.

2. Forgot Password?를 선택합니다.

3. 암호 복구 단계를 완료하세요. 보안 검사를 완료할 수 없는 경우 오디오를 듣거나 보안 검사를 새로 고쳐 새 문자 세트를 받으십시오. 암호 복구 페이지의 예시는 다음 이미지에 나와 있습니다.

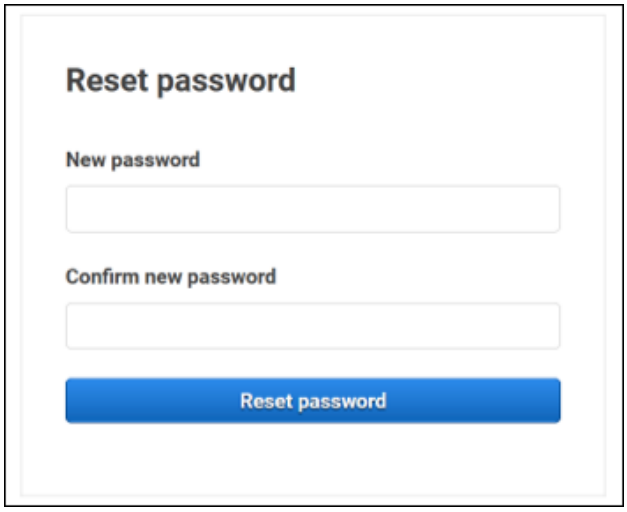


4. 암호 복구 단계를 완료하면 AWS 계정과 연결된 이메일 주소로 추가 지침이 전송되었다는 메시지가 나타납니다.

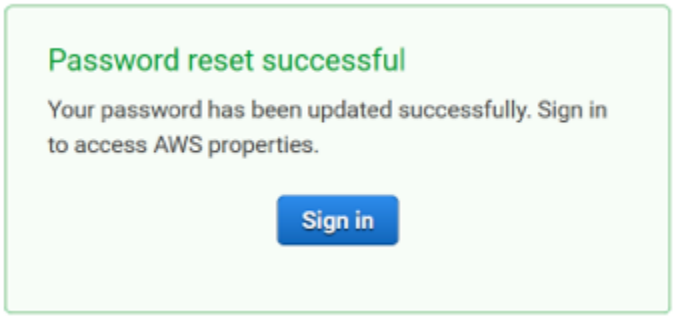
   암호를 재설정할 수 있는 링크가 포함된 이메일이 AWS 계정의 생성에 사용된 이메일로 전송됩니다.

> **Note**
>
> 해당 이메일은 @signin.aws 또는 @verify.signin.aws로 끝나는 주소에서 전송됩니다.

5. AWS 이메일에 제공된 링크를 선택하여 AWS 루트 사용자 암호를 재설정합니다.
6. 해당 링크를 클릭하면 새 루트 사용자 암호를 만들 수 있는 새 웹 페이지로 이동합니다.



암호 재설정이 성공했다는 확인 메시지가 나타납니다. 성공적인 암호 재설정은 다음 이미지와 같이 표시됩니다.

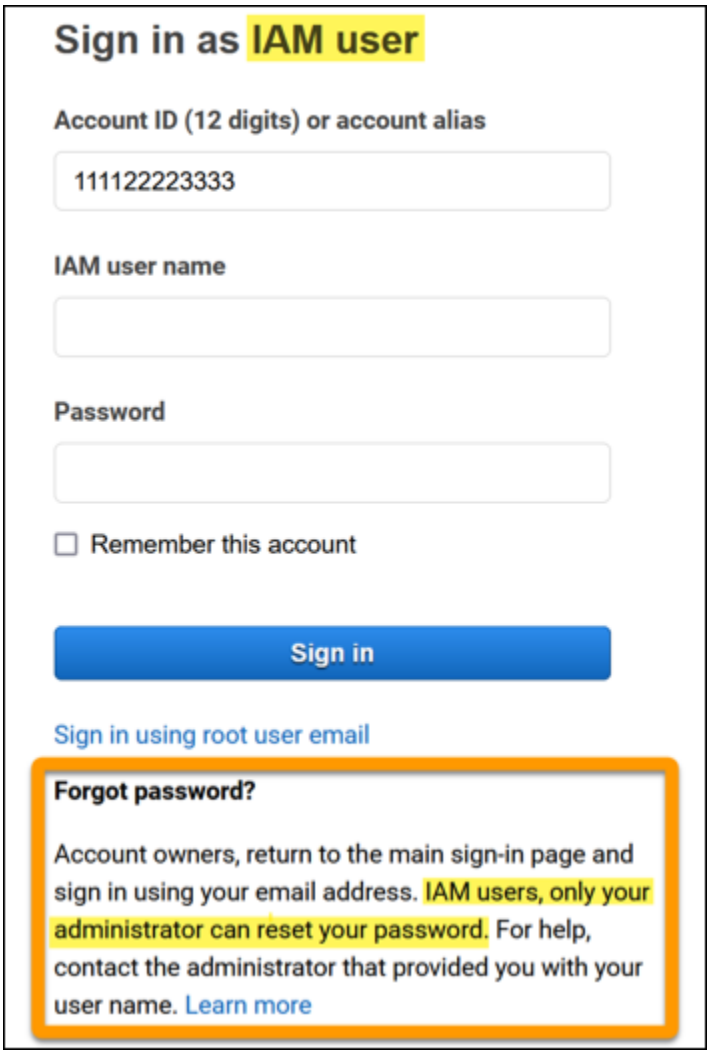


루트 사용자 암호 재설정에 대한 자세한 내용은 분실하거나 잊어버린 AWS 암호를 복구하려면 어떻게 해야 하나요?를 참조하세요.

에 대한 IAM 사용자 암호를 잊어버렸습니다. AWS 계정

IAM 사용자 암호를 변경하려면 해당 권한이 있어야 합니다. IAM 사용자 암호 재설정에 대한 자세한 내용은 IAM 사용자가 자신의 암호를 변경하는 방법을 참조하십시오.

암호를 재설정할 권한이 없는 경우, IAM 관리자만 IAM 사용자 암호를 재설정할 수 있습니다. IAM 사용자는 IAM 관리자에게 문의하여 암호를 재설정해야 합니다. 관리자는 일반적으로 조직의 다른 구성원 AWS 계정 보다에 대한 더 높은 수준의 권한을 가진 정보 기술(IT) 직원입니다. 이 개인은 귀하의 계정을 만들었고 사용자에게 로그인할 수 있는 액세스 보안 인증을 제공합니다.



보안을 위해 지원 는 자격 증명을 보거나 제공하거나 변경할 수 있는 액세스 권한이 없습니다.

IAM 사용자 암호 재설정에 대한 자세한 내용은 분실하거나 잊어버린 AWS 암호를 복구하려면 어떻게 해야 하나요?를 참조하세요.

관리자가 암호를 관리하는 방법에 대해 알아보려면 IAM 사용자 암호 관리하기를 참조하세요.

내에 대한 연동 자격 증명 암호를 잊어버렸습니다. AWS 계정

페더레이션 자격 증명은 외부 자격 증명 AWS 계정 으로에 액세스하기 위해 로그인합니다. 사용 중인 외부 ID 유형에 따라 페더레이션 ID의 로그인 방식이 결정됩니다. 관리자가 페더레이션 ID를 생성합니

다. 암호를 재설정하는 방법에 대한 자세한 내용은 관리자에게 문의하세요. 관리자는 일반적으로 조직의 다른 구성원 AWS 계정 보다에 대한 더 높은 수준의 권한을 가진 정보 기술(IT) 직원입니다. 이 개인은 귀하의 계정을 만들었고 사용자에게 로그인할 수 있는 액세스 보안 인증을 제공합니다.

기존에 로그인할 수 AWS 계정 없으며 동일한 이메일 주소로 새 AWS 계정 를 생성할 수 없습니다.

하나의 이메일 주소는 하나의 AWS 계정 루트 사용자에만 연결할 수 있습니다. 루트 사용자 계정을 닫은 후 90일 이상 닫은 경우 계정을 다시 열거나이 계정과 연결된 이메일 주소를 AWS 계정 사용하여 새를 생성할 수 없습니다.

이 문제를 해결하려면 새 계정을 등록할 때 평소 사용하는 이메일 주소 뒤에 더하기 기호(+)를 추가하는 하위 주소 지정을 사용할 수 있습니다. 더하기 기호(+) 뒤에는 대문자나 소문자, 숫자 또는 기타 SMTP(Simple Mail Transfer Protocol) 지원 문자가 올 수 있습니다. 예를 들어, 평소 사용하는 이메일이 `email@yourcompany.com`인 경우 `email+1@yourcompany.com` 또는 `email+tag@yourcompany.com`을(를) 사용할 수 있습니다. 이 주소는 평소 사용하는 이메일 주소와 동일한 수신함에 연결되어 있더라도 새 주소로 간주됩니다. 새 계정을 등록하기 전에 추가된 이메일 주소로 테스트 이메일을 보내 이메일 공급자가 하위 주소 지정을 지원하는지 확인하는 것이 좋습니다.

일시 중지된를 다시 활성화해야 합니다. AWS 계정

AWS 계정 가 일시 중지되어 복원하려는 경우 일시 중지된를 다시 활성화하려면 어떻게 해야 합니까 AWS 계정?를 참조하세요.

로그인 문제를 위해 지원 에 문의해야 합니다.

모든 것을 시도한 경우 결제 및 계정 지원 요청을 완료 지원 하여에서 도움을 받을 수 있습니다.

결제 문제에 AWS Billing 대해에 문의해야 합니다.

에 로그인할 수 없고 AWS Billing 결제 문제로에 문의 AWS 계정 하려는 경우 결제 및 계정 지원 요청을 통해 그렇게 할 수 있습니다. 요금 및 결제 방법을 AWS 결제 및 비용 관리포함하여에 대한 자세한 내용은 도움 받기를 AWS Billing 참조하세요.

소매 주문에 대해 질문이 있음

www.amazon.com 계정에 문제가 있거나 소매 주문에 대한 질문이 있는 경우, 지원 옵션 및 문의하기를 참조하십시오.

내를 관리하는 데 도움이 필요합니다. AWS 계정

의 신용 카드 변경 AWS 계정, 사기 행위 보고 또는 해지에 도움이 필요한 경우 AWS 계정의 다른 문제 해결을 AWS 계정 참조하세요.

AWS 액세스 포털 자격 증명이 작동하지 않음

AWS 액세스 포털에 로그인할 수 없는 경우 이전에에 액세스한 방법을 기억해 보십시오 AWS.

암호를 사용했는지 전혀 기억나지 않는 경우

자격 AWS 증명을 사용하지 AWS 않고 이전에에 액세스했을 수 있습니다. 이는 IAM Identity Center를 통한 엔터프라이즈 Single Sign-On에서 흔히 발생합니다. AWS 이렇게 하면 자격 증명을 입력하지 않고도 회사 자격 증명을 사용하여 AWS 계정 또는 애플리케이션에 액세스할 수 있습니다.

- AWS 액세스 포털 - 관리자가 외부의 자격 증명을 사용하여 AWS 에 액세스하도록 허용하는 경우 포털의 URL이 AWS필요합니다. 이메일, 브라우저 즐겨찾기 또는 브라우저 기록에서 `awsapps.com/start` 또는 `signin.aws/platform/login`을 포함하는 URL을 확인하세요.

  예를 들어 사용자 지정 URL에는 `https://d-1234567890.awsapps.com/start`와 같은 ID 또는 도메인이 포함될 수 있습니다. 포털 링크를 찾을 수 없는 경우 관리자에게 문의하십시오.이 정보를 복구하는 데 도움을 줄 지원 수 없습니다.

사용자 이름과 암호는 기억하지만 보안 인증이 작동하지 않는 경우, 페이지를 잘못 찾은 것일 수 있습니다. 웹 브라우저의 URL을 확인하십시오. https://signin.aws.amazon.com/인 경우 페더레이션 사용자 또는 IAM Identity Center 사용자는 보안 인증을 사용하여 로그인할 수 없습니다.

- AWS 액세스 포털 - 관리자가에 대한 AWS IAM Identity Center(AWS Single Sign-On 후속) 자격 증명 소스를 설정한 경우 조직의 AWS 액세스 포털에서 사용자 이름과 암호를 사용하여 로그인해야 AWS합니다. 포털의 URL을 찾으려면 이메일, 보안 암호 저장소, 브라우저 즐겨찾기 또는 브라우저 기록에서 `awsapps.com/start` 또는 `signin.aws/platform/login`을(를) 포함하는 URL을 확인하세요. 예를 들어 사용자 지정 URL에는 다음과 같은 ID 또는 도메인이 포함될 수 있습니다. 포털

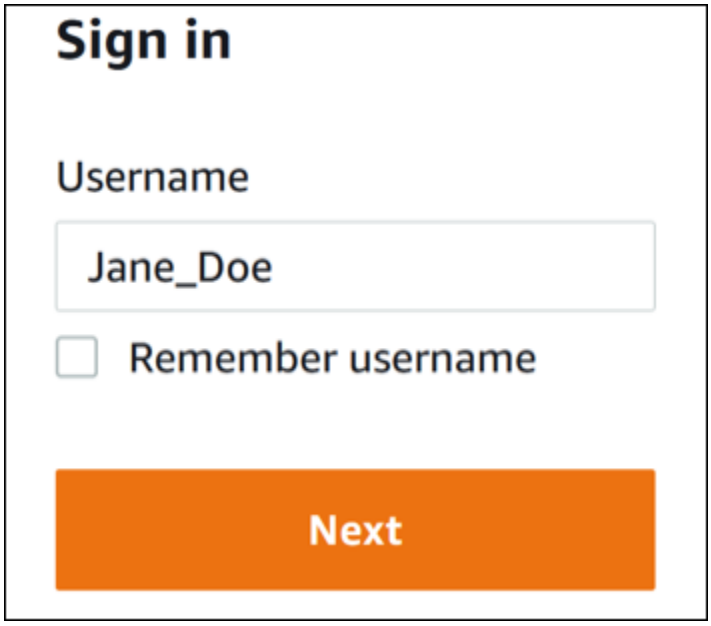
링크를 찾을 수 없는 `https://d-1234567890.awsapps.com/start.` 경우 administrator. 지원 cant help you recover this information.

에 대한 IAM Identity Center 암호를 잊어버렸습니다. AWS 계정

IAM Identity Center인 경우 AWS 계정의 암호를 분실했거나 잊어버렸으면 암호를 재설정할 수 있습니다. IAM Identity Center의 계정에 사용되는 이메일 주소를 알고 있어야 하며 해당 계정에 액세스할 수 있어야 합니다. 암호 재설정 링크가 AWS 계정 이메일로 전송됩니다.

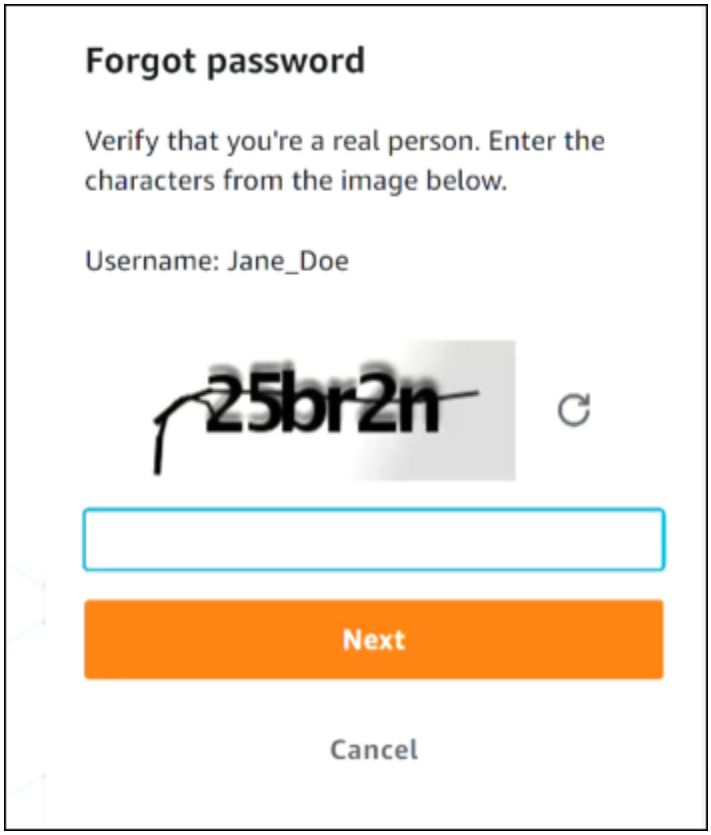
IAM Identity Center의 사용자 암호를 재설정하기

1. AWS 액세스 포털 URL 링크를 사용하고 사용자 이름을 입력합니다. 그리고 다음을 선택합니다.

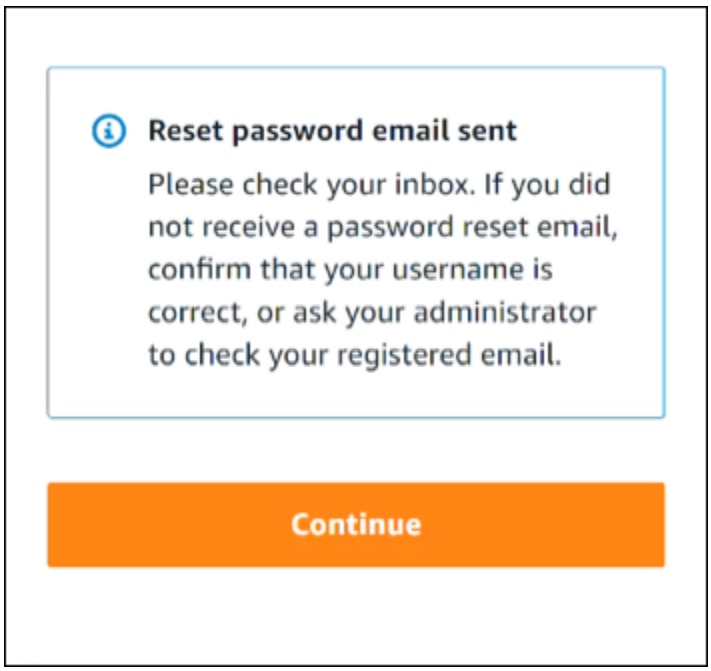


2. 다음 이미지에 표시된 대로 비밀번호 분실를 선택합니다.

3. 암호 복구 단계를 완료하세요.



4. 암호 복구 단계를 완료하면 암호를 재설정하는 데 사용할 수 있는 이메일 메시지를 받았다는 확인 메시지가 다음과 같이 표시됩니다.



암호 재설정 링크가 포함된 이메일이 IAM Identity Center 사용자 계정과 연결된 이메일로 전송됩니다. AWS 이메일에 제공된 링크를 선택하여 암호를 재설정합니다. 이 링크를 클릭하면 새 암호를 생성할 수 있는 새 웹 페이지로 이동합니다. 새 암호를 생성하면 암호 재설정이 성공했다는 확인 메시지가 표시됩니다.

암호를 재설정하라는 이메일을 받지 못한 경우, 관리자에게 IAM Identity Center의 사용자로 등록한 이메일을 확인해 달라고 요청하십시오.

IAM Identity Center 콘솔에 로그인하려고 할 때 'It's not you, it's us'라는 오류 발생

이 오류는 IAM Identity Center 인스턴스 또는 자격 증명 소스로 사용 중인 외부 ID 제공업체(idP)에 설정 문제가 있음을 나타냅니다. 다음을 확인하는 것이 좋습니다.

- 로그인에 사용하는 디바이스의 날짜 및 시간 설정을 확인합니다. 날짜와 시간을 자동으로 설정하는 것이 좋습니다. 사용할 수 없는 경우 날짜와 시간을 알려진 Network Time Protocol(NTP) 서버에 동기화하는 것이 좋습니다.
- IAM Identity Center에 업로드된 IdP 인증서가 ID 제공업체가 제공한 것과 동일한지 확인합니다. 설정으로 이동하여 IAM Identity Center 콘솔에서 인증서를 확인할 수 있습니다. 자격 증명 소스 탭의 작업 아래에서 인증 관리를 선택합니다. 새 인증서를 가져와야 할 수 있습니다.

- IdP SAML 메타데이터 파일에서 NameID 형식이 `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`인지 확인합니다.
- AD Connector를 사용하는 경우 서비스 계정의 자격 증명이 올바르고 만료되지 않았는지 확인합니다. 자세한 내용은 에서 AD Connector 서비스 계정 자격 증명 업데이트를 참조하세요 Directory Service.

AWS Builder ID 문제 해결

여기에 있는 정보를 사용하면 AWS Builder ID와(과) 관련된 문제를 해결하는 데 도움이 될 수 있습니다.

주제

내 이메일이 이미 사용 중입니다.

입력한 이메일이 이미 사용 중이고 자신의 것으로 인식하는 경우 이미 AWS Builder ID에 가입했을 수 있습니다. 해당 이메일 주소를 사용하여 로그인해 보세요. 암호가 기억나지 않는 경우 암호를 잊어버렸습니다을(를) 참조하십시오.

이메일 인증을 완료할 수 없습니다

AWS Builder ID에 가입했지만 확인 이메일을 받지 못한 경우 다음 문제 해결 작업을 완료합니다.

1. 스팸, 정크, 삭제된 항목 폴더를 확인하세요.

   > **Note**
   >
   > 이 확인 이메일은 no-reply@signin.aws 또는 no-reply@login.awsapps.com 주소에서 발송됩니다. 이러한 발신자 이메일 주소에서 오는 이메일을 수신하고 이를 정크 또는 스팸으로 처리하지 않도록 메일 시스템을 구성하는 것이 좋습니다.

2. Resend code를 선택하고 받은 편지함을 새로 고친 다음 스팸, 정크, 삭제된 항목 폴더를 다시 확인하세요.
3. 그래도 확인 이메일이 보이지 않으면 AWS Builder ID 이메일 주소에 오타가 있는지 다시 확인하세요. 이메일 주소를 잘못 입력한 경우, 보유 중인 이메일 주소로 다시 가입하세요.

Google로 로그인할 수 없습니다

Google 계정과 이메일 주소가 동일한 기존 AWS Builder ID 프로필이 있는 경우 AWS Builder ID 암호를 사용하여 계정에 로그인합니다. 암호가 기억나지 않는 경우 암호를 잊어버렸습니다을(를) 참조하십시오.

Google 암호로 로그인하는 데 도움이 필요하면 Google로 로그인할 수 없습니다를 참조하세요.

Apple로 로그인할 수 없음

Apple 계정과 이메일 주소가 동일한 기존 AWS Builder ID 프로필이 있는 경우 AWS Builder ID 암호를 사용하여 계정에 로그인합니다. 암호가 기억나지 않는 경우 암호를 잊어버렸습니다을(를) 참조하십시오.

Apple 암호로 로그인하는 데 도움이 필요하면 Apple 계정에 로그인할 수 없는 경우 단원을 참조하십시오.

GitHub로 로그인할 수 없음

GitHub 계정과 이메일 주소가 동일한 기존 AWS Builder ID 프로필이 있는 경우 AWS Builder ID 암호를 사용하여 계정에 로그인합니다. 암호가 기억나지 않는 경우 암호를 잊어버렸습니다을(를) 참조하십시오.

GitHub 암호로 로그인하는 데 도움이 필요하면 로그인할 수 없음 - GitHub 지원을 참조하세요.

Amazon으로 로그인할 수 없음

Amazon 계정과 이메일 주소가 동일한 기존 AWS Builder ID 프로필이 있는 경우 AWS Builder ID 암호를 사용하여 계정에 로그인합니다. 암호가 기억나지 않는 경우 암호를 잊어버렸습니다을(를) 참조하십시오.

Amazon 암호로 로그인하는 방법에 대한 도움말은 로그인 도움말을 참조하세요.

Google에서 계속을 AWS Builder ID 사용하여에 가입하려고 할 때 로그인 오류가 발생했습니다.

즉, Google 계정과 동일한 이메일 주소를 AWS Builder ID 사용하는가 있거나 Google 계정과 연결된 이메일 주소가 확인되지 않습니다. 어느 경우든 이메일 주소를 입력하고 암호를 제공하여 다시 가입을 시도해 보세요.

Apple에서 계속을 AWS Builder ID 사용하여에 가입하려고 할 때 로그인 오류가 발생했습니다.

즉, Apple 계정과 동일한 이메일 주소를 AWS Builder ID 사용하는 기존가 있거나 Apple Business Manager를 사용하는 회사 또는 Apple School Manager를 사용하는 학교에서 Apple 계정과 연결된 이메일 주소를 확인하거나 관리하지 않습니다. 어느 경우든 이메일 주소를 입력하고 암호를 제공하여 다시 가입을 시도해 보세요.

GitHub에서 계속을 AWS Builder ID 사용하여에 가입하려고 할 때 로그인 오류가 발생했습니다.

즉, GitHub 계정과 동일한 이메일 주소를 AWS Builder ID 사용하는가 있거나 GitHub 계정과 연결된 이메일 주소가 확인되지 않습니다. 어느 경우든 이메일 주소를 입력하고 암호를 제공하여 다시 가입을 시도해 보세요.

Amazon에서 계속을 AWS Builder ID 사용하여에 가입하려고 할 때 로그인 오류가 발생했습니다.

즉, Amazon 계정과 동일한 이메일 주소를 AWS Builder ID 사용하는가 있거나 Amazon 계정과 연결된 이메일 주소가 확인되지 않습니다. 어느 경우든 이메일 주소를 입력하고 암호를 제공하여 다시 가입을 시도해 보세요.

내 로 로그인하려고 할 때 'It's not you, it's us'라는 오류가 표시됩니다. AWS Builder ID

로그인하려고 할 때 이 오류 메시지를 받는 경우, 로컬 설정이나 이메일 주소에 문제가 있을 수 있습니다

- 로그인에 사용하는 디바이스의 날짜 및 시간 설정을 확인합니다. 날짜와 시간을 자동으로 설정하는 것이 좋습니다. 사용할 수 없는 경우 날짜와 시간을 알려진 Network Time Protocol(NTP) 서버에 동기화하는 것이 좋습니다.
- 이메일 주소에 형식 오류가 없는지 검토합니다. 다음과 같은 문제가 발생하면 AWS Builder ID을(를) 사용하여 로그인하려고 할 때 오류가 반환됩니다.
  - 이메일 주소의 공백
  - 이메일 주소의 슬래시(/)
  - 이메일 주소의 두 마침표(.)
  - 이메일 주소에 앰퍼샌드(@) 2개
  - 이메일 주소 끝에 있는 쉼표(,)
  - 이메일 주소 끝에 있는 대괄호(])

암호를 잊어버렸습니다

잊어버린 암호 재설정하기

1. AWS Builder ID로 로그인 페이지에서 이메일 주소에 AWS Builder ID를 생성하는 데 사용한 이메일을 입력합니다. 다음을 선택합니다.
2. Forgot Password?를 선택합니다. 암호를 재설정할 수 있는 AWS Builder ID와 연결된 이메일 주소로 링크를 보냅니다.
3. 이 이메일의 지침을 따르십시오.

새 암호를 설정할 수 없습니다

보안을 위해 암호를 설정하거나 변경할 때마다 다음 요구 사항을 준수해야 합니다.

- 암호는 대/소문자를 구분합니다.
- 암호 길이는 8~64자여야 합니다.
- 암호는 각각의 다음 네 가지 범주의 문자를 최소 1자씩 포함해야 합니다.
  - 소문자(a~z)
  - 대문자(A-Z)
  - 숫자(0-9)
  - 영숫자가 아닌 문자(~!@#$%^management portal*_-+=`|\(){}[]:;'"<>,.?/)
- 최근 사용한 세 개의 암호는 다시 사용할 수 없습니다.
- 제3자로부터 유출된 데이터 세트를 통해 공개적으로 알려진 암호는 사용할 수 없습니다.

암호가 작동하지 않습니다

암호를 기억하지만 AWS Builder ID로 로그인할 때 암호가 작동하지 않는 경우 다음을 확인하세요.

- Caps Lock이 꺼져 있습니다.
- 이전 암호를 사용하지 않습니다.
- 에 대한 암호가 아닌 AWS Builder ID 암호를 사용하고 있습니다 AWS 계정.

암호가 최신이고 올바르게 입력되었는지 확인했지만 여전히 작동하지 않는 경우, 암호를 잊어버렸습니다의 지침에 따라 암호를 재설정하세요.

암호가 작동하지 않아 AWS Builder ID 이메일 주소로 전송된 이메일에 더 이상 액세스할 수 없습니다.

그래도 AWS Builder ID에 로그인할 수 있는 경우 프로필 페이지를 사용하여 AWS Builder ID 이메일을 새 이메일 주소로 업데이트합니다. 이메일 확인을 완료하면에 로그인하여 새 이메일 주소로 커뮤니케이션을 AWS 받을 수 있습니다.

회사나 학교 이메일 주소를 사용하다가 해당 회사나 학교를 그만둔 후 해당 주소로 전송된 이메일을 받을 수 없는 경우, 해당 이메일 시스템의 관리자에게 문의하세요. 해당 회사나 학교에서 해당 이메일을 새 주소로 전달하거나, 임시 액세스 권한을 부여하거나, 해당 사서함의 콘텐츠를 공유할 수 있습니다.

MFA를 활성화할 수 없습니다.

MFA를 활성화하려면 AWS Builder ID 다중 인증(MFA) 관리의 단계에 따라 프로필에 MFA 디바이스를 하나 이상 추가하십시오.

인증 앱을 MFA 디바이스로 추가할 수 없습니다

새 MFA 디바이스를 추가할 수 없는 경우, 해당 애플리케이션에 등록할 수 있는 MFA 디바이스 수량 한도에 도달했을 수 있습니다. 사용하지 않는 MFA 디바이스를 제거하거나 다른 인증 앱을 사용해 보십시오.

MFA 디바이스를 제거할 수 없습니다

MFA를 비활성화하려면 MFA 디바이스 삭제의 단계에 따라 MFA 디바이스 제거를 진행하세요. 하지만 MFA를 활성화된 상태로 유지하려면 기존 MFA 디바이스 삭제를 시도하기 전에 다른 MFA 디바이스를 추가해야 합니다. MFA 디바이스 추가에 대한 자세한 내용은 AWS Builder ID 다중 인증(MFA) 관리 섹션을 참조하세요.

인증 앱으로 등록하거나 로그인하려고 시도하면 '예상치 못한 오류가 발생했습니다'라는 메시지가 나타납니다.

AWS Builder ID가 코드 기반 인증 앱과 함께 사용하는 것과 같은 시간 기반 일회용 암호(TOTP) 시스템은 클라이언트와 서버 간의 시간 동기화에 의존합니다. 인증 앱이 설치된 디바이스가 신뢰할 수 있는 시간 출처와 올바르게 동기화되었는지 확인하거나, NIST 또는 기타 지역/리전별 등가물과 같은 신뢰할 수 있는 출처와 일치하도록 디바이스의 시간을 수동으로 설정하세요.

AWS Builder ID에 로그인하려고 할 때 'It's not you, it'라는 메시지가 표시됩니다.

로그인에 사용하는 디바이스의 날짜 및 시간 설정을 확인합니다. 날짜와 시간을 자동으로 설정할 것을 권장합니다. 사용할 수 없는 경우 날짜와 시간을 알려진 Network Time Protocol(NTP) 서버에 동기화하는 것이 좋습니다.

로그아웃을 해도 완전히 로그아웃되지 않습니다.

시스템은 즉시 로그아웃하도록 설계되어 있지만 완전 로그아웃에는 최대 1시간이 걸릴 수 있습니다.

> **Note**
>
> Google 또는 Apple과 같은 소셜 로그인 계정을 사용하는 경우 활성 AWS Builder ID 세션을 삭제해도 소셜 로그인 계정에서 로그아웃되지 않습니다.

여전히 문제해결 방법을 찾고 있습니다

지원 피드백 양식을 작성할 수 있습니다. 요청 정보 섹션의 지원 방법에서 AWS Builder ID를 사용하고 있음을 포함시킵니다. 문제를 가장 효율적으로 해결할 수 있도록 최대한 자세하게 설명해 주세요.

AWS 에 대한 관리형 정책 AWS 로그인

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonManagedSignUpServicePolicy

이 `AmazonManagedSignUpServicePolicy` 정책은 AWS 계정 가입 프로세스를 완료하는 데 필요한 권한을 부여합니다.

사용자, 그룹 및 역할에 `AmazonManagedSignUpServicePolicy`를 연결할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- 고객 확인 - 고객 확인 세부 정보와 적격성 상태를 생성, 검색 및 업데이트하는 것을 허용하며, 확인 문서를 위한 업로드 URL 생성을 포함합니다.

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 추가 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 AmazonManagedSignUpServicePolicy을(를) 참조하세요.

AWS 관리형 정책: ApplicationProvisioningPolicy

ApplicationProvisioningPolicy 정책은 IAM 역할 및 정책 관리, SSO 구성, ID 스토어 운영을 포함하여 애플리케이션 프로비저닝 및 ID 관리 작업에 필요한 포괄적인 권한을 부여합니다.

사용자, 그룹 및 역할에 `ApplicationProvisioningPolicy`를 연결할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- IAM 관리 - 역할 및 정책 생성, 업데이트, 삭제, 역할 첨부 관리, 서비스 연결 역할 생성 등을 포함한 포괄적인 IAM 작업을 허용합니다.
- AWS 기반 연구 및 엔지니어링 스튜디오 - AWS 기반 연구 및 엔지니어링 스튜디오 리소스에 대한 모든 작업을 허용합니다.
- 역할 전달 - IAM 역할을 다른 서비스로 전달할 수 있습니다.
- IAM Identity Center- IAM Identity Center 인스턴스, 애플리케이션, 할당, 권한 부여 및 인증 방법을 관리할 수 있습니다.
- ID 스토어 - ID 스토어에서 사용자 및 그룹 정보를 읽을 수 있습니다.
- IAM Identity Center OAuth - IAM Identity Center OAuth를 통해 IAM 세션을 인증할 수 있습니다.
- 사용자 프로필 및 디렉터리 - 외부 ID 제공업체 설정을 포함하여 IAM Identity Center 커넥터, 사용자 프로필 및 디렉터리 구성을 관리할 수 있습니다.
- 사용자 구독 - 사용자 구독을 나열할 수 있습니다.

정책의 최신 버전 JSON 정책 문서를 포함하여 더 자세한 내용을 보려면 AWS 관리형 정책 참조 안내서의 ApplicationProvisioningPolicy를 참조하세요.

AWS 관리형 정책: SignInLocalDevelopmentAccess

이 `SignInLocalDevelopmentAccess` 정책은 콘솔 자격 증명을 AWS 사용하여에 프로그래밍 방식으로 액세스할 수 있는 권한을 부여합니다.

사용자, 그룹 및 역할에 `SignInLocalDevelopmentAccess`를 연결할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- OAuth2 액세스 권한 부여 - 브라우저를 통해 인증하고 자격 증명 교환을 위한 OAuth 2.0 권한 부여 코드를 가져올 수 있는 권한을 부여합니다.
- OAuth2 토큰 생성 - 개발자 도구 및 애플리케이션에서 AWS 서비스에 액세스하는 데 사용할 수 있는 OAuth 2.0 액세스 토큰 및 새로 고침 토큰에 대한 권한 부여 코드를 교환할 수 있는 권한을 부여합니다.

> **Note**
>
> 이 AWS 관리형 정책을 추가하면 동일한 디바이스 인증과 교차 디바이스 인증 모두에 대한 권한이 부여됩니다. 이 정책은 다음 리소스에 대한 작업을 승인합니다.
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost` -를 사용한 동일 디바이스 인증에 사용됩니다`aws login`.
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote` -를 사용한 디바이스 간 인증에 사용됩니다`aws login --remote`.
>
> 인증 방법 중 하나에 대한 액세스를 제어하려면 자체 관리형 정책 또는 서비스 제어 정책(SCP)을 생성할 수 있습니다. 이러한 리소스 ARNs 사용하여 콘솔 자격 증명을 사용하여 AWS에 대한 프로그래밍 방식 액세스를 허용하거나 거부합니다.

자세한 내용은 콘솔 자격 증명으로 로그인(권장) 단원을 참조하십시오. 최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 안내서의 SignInLocalDevelopmentAccess를 참조하세요.

AWS 관리형 정책: AWSSignInResourcePolicyManagement

이 `AWSSignInResourcePolicyManagement` 정책은 AWS 로그인에 대한 콘솔 권한 부여 구성 및 리소스 권한 설명을 관리할 수 있는 권한을 부여합니다.

사용자, 그룹 및 역할에 `AWSSignInResourcePolicyManagement`를 연결할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `signin:PutConsoleAuthorizationConfiguration` - 콘솔 권한 부여 설정을 생성하거나 업데이트합니다.
- `signin:GetConsoleAuthorizationConfiguration` - 현재 콘솔 권한 부여 구성을 검색합니다.
- `signin:DeleteConsoleAuthorizationConfiguration` - 콘솔 권한 부여 구성을 제거합니다.
- `signin:PutResourcePermissionStatement` - 리소스 권한 문을 생성하거나 업데이트합니다.
- `signin:DeleteResourcePermissionStatement` - 리소스 권한 문을 제거합니다.

- `signin:ListResourcePermissionStatements` - 계정에 대한 리소스 권한 설명을 나열합니다.
- `signin:GetResourcePolicy` - 통합 리소스 기반 정책을 검색합니다.

다음은 정책 JSON입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
                "signin:PutResourcePermissionStatement",
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

이 정책을 AWS 로그인에 대한 리소스 기반 정책을 관리하는 IAM 보안 주체(사용자 또는 역할)에 연결합니다. 여기에는 네트워크 기반 액세스 제어를 구성하는 보안 관리자, 콘솔 액세스 정책을 감사해야 하는 규정 준수 책임자, 긴급 복구 액세스 구성을 관리하는 운영 팀이 포함됩니다.

> **Important**
>
> 이 정책은 콘솔 권한 부여 제어에 대한 관리 액세스 권한을 부여합니다. 이 정책을 할당할 때 최소 권한 원칙을 적용합니다. IAM 조건을 사용하여 이러한 권한을 사용할 수 있는 시기와 방법을 추가로 제한하는 것이 좋습니다.

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 안내서의 AWSSignInResourcePolicyManagement를 참조하세요.

AWS 로그인 AWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS 로그인 이후부터의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS 로그인 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AWSSignInResourcePolicyManagement – 새 정책	AWS 로그인에 대한 콘솔 권한 부여 구성 및 리소스 권한 설명을 관리할 수 있는 권한을 부여하는 새로운 AWS 관리형 정책이 추가되었습니다.	2026년 6월 10일
SignInLocalDevelopmentAccess – 새 정책	기존 콘솔 자격 증명을 AWS 사용하여에 프로그래밍 방식으로 액세스할 수 있는 권한을 부여하는 새로운 AWS 관리형 정책이 추가되었습니다.	2025년 11월 19일
ApplicationProvisioningPolicy – 새 정책	IAM 역할 및 정책 관리, IAM Identity Center 구성, Identity Store 작업을 포함하여 애플리케이션 프로비저닝 및 자격 증명 관리 작업에 대한 포괄적인 권한을 부여하는 새로운 AWS 관리형 정책을 추가했습니다.	2025년 9월 30일
AmazonManagedSignUpServicePolicy – 새 정책	고객 확인 및 결제 설정 작업을 포함하여 AWS 계정 가입 프로세스에 필요한 권한을 부여하는 새로운 AWS 관리형 정책이 추가되었습니다.	2025년 9월 30일
AWS 로그인 에서 변경 내용 추적 시작	AWS 로그인 가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2025년 9월 30일

문서 이력

다음 표에서는 AWS 로그인 설명서에 추가된 중요 사항에 대해 설명합니다. 사용자로부터 받은 의견을 수렴하기 위해 설명서가 자주 업데이트됩니다.

- 최신 주요 설명서 업데이트: 2026년 6월 10일

변경 사항	설명	날짜
로그인 리소스 기반 정책 및 리소스 제어 정책 지원	로그인 리소스 기반 정책 및 리소스 제어 정책(RCPs), 새 조건 키 참조, `AWSSignInResourcePolicyManagement` 관리형 정책 및 관련 문제 해결을 사용하여 AWS Management Console 액세스를 제어하는 설명서를 추가했습니다.	2026년 6월 10일
GitHub 및 Amazon을 사용한 로그인 지원	AWS 로그인 는 이제 GitHub로 로그인 및 Amazon으로 로그인을 지원하므로 GitHub 또는 Amazon 계정을 AWS Builder ID 사용하여를 생성할 수 있습니다.	2026년 3월 10일
Sign in with Apple 지원	AWS 로그인 는 이제 Sign in with Apple을 지원하므로 문제 해결 AWS Builder ID 에 추가된 Apple Account. AWS Builder ID topics 업데이트 및 새 문제 해결 주제를 AWS Builder ID 사용하여를 생성할 수 있습니다.	2026년 2월 5일
새로운 관리형 정책	AWS 로그인 에서 새로운 관리형 정책을 릴리스했습니다.는	2025년 11월 19일

	기존 콘솔 자격 증명을 AWS 사용하여에 프로그래밍 방식으로 액세스할 수 있는 권한을 `SignInLocalDevelopmentAccess` 부여합니다. 자세한 내용은 AWS 로그인 AWS 관리형 정책에 대한 업데이트를 참조하세요.	
Google로 로그인 지원	AWS 로그인 는 이제 Google로 로그인을 지원하므로 문제 해결에 추가된 Google Account. AWS Builder ID topics 업데이트 및 새 문제 해결 주제를 AWS Builder ID 사용하여를 생성할 수 있습니다. AWS Builder ID	2025년 9월 30일
새 관리형 정책	AWS 로그인 는 두 개의 새로운 관리형 정책을 릴리스했습니다. `AmazonManagedSignUpServicePolicy` 는 AWS 계정 가입 프로세스를 완료하는 데 필요한 권한을 부여합니다. `ApplicationProvisioningPolicy` 는 애플리케이션 프로비저닝 및 자격 증명 관리 작업에 대한 포괄적인 권한을 부여합니다. 자세한 내용은 AWS 로그인AWS 관리형 정책 업데이트를 참조하세요.	2025년 9월 30일
문제 해결 주제 업데이트됨	AWS Builder ID 및에 로그인하기 위한 새로운 문제 해결 주제가 추가되었습니다 AWS Management Console.	2024년 2월 27일

구성에 대한 여러 주제 업데이트됨	사용자 유형 업데이트, 사용자 유형 확인 제거 및 사용자 유형에 콘텐츠 통합, 에 로그인하는 방법 AWS	2023년 5월 15일
여러 주제 및 상단 배너 업데이트됨	사용자 유형, 사용자 유형 결정, 로그인 방법 AWS, AWS 로그인이란 무엇입니까?가 업데이트되었습니다. 루트 사용자 및 IAM 사용자 로그인 절차도 업데이트됨.	2023년 3월 3일
AWS Management Console 로그인에 대한 소개 단락 업데이트	사용자 유형 결정은 페이지 상단으로 이동하고, 계정 루트 사용자에 있는 메모는 제거됨.	2023년 2월 27일
추가됨 AWS Builder ID	AWS 로그인 사용 설명서에 AWS Builder ID 주제를 추가하고 기존 주제에 콘텐츠를 통합했습니다.	2023년 1월 31일
구성 업데이트	고객 피드백을 바탕으로 로그인 방법에 대해 더 명확하게 설명하도록 TOC가 업데이트됨. 로그인 튜토리얼이 업데이트됨. 용어 및 사용자 유형 결정이 업데이트됨. IAM 사용자 및 루트 사용자와 같은 용어를 정의할 수 있도록 교차 연결이 개선됨.	2022년 12월 22일
새 안내서	AWS 로그인 사용 설명서의 첫 번째 릴리스입니다.	2022년 8월 31일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.