aws

사용 설명서

Amazon One

Amazon One: 사용 설명서

Table of Contents

Amazon One Enterprise란 무엇인가요?

Amazon One Enterprise는 배지, PINs 또는 암호를 사용하지 않고도 직원에게 건물 및 엔터프라이즈 자산에 대한 보안 액세스를 제공하는 새로운 사이트 기반 인증 서비스입니다.

주제

Amazon One 디바이스

Amazon One 디바이스는 엔터프라이즈 액세스 제어를 위한 안전한 야자수 기반 자격 증명 서비스인 Amazon One Enterprise용으로 설계되었습니다. 다음 디바이스 사양에 유의하세요.

- 사용자 입력 - 팜 생체 인식, QR 코드 일치
- 호스트 인터페이스 - Wi-Fi(2.4GHz 및 5GHz), 이더넷, USB Type-A 2개, USB Type-B 1개
- 사용자 피드백 - 5.5” 터치스크린, 조명, 스피커, 헤드폰
- 물리적 액세스 제어 프로토콜 - OSDP 및 Wiegand
- 전원 공급 - POE, 제공된 DC 어댑터에 대한 110/220VAC 입력 AC, 15V에서 30W
- 보안 - 변조 스위치
- 차원(HxWxD mm) — 86 x 85 x 256

Amazon One Enterprise 콘솔

Amazon One Enterprise에는 다음과 같은 방법으로 사용할 수 있는 콘솔이 포함되어 있습니다.

- IT 또는 시설 관리자는 Amazon One Enterprise를 사용하여 사이트를 생성하고 관리합니다. 사이트는 Amazon One Enterprise 디바이스 및 사용자 프로필을 모니터링하고 관리하는 동안 팀이 수행하는 작업의 물리적 위치와 유사합니다. IT 또는 시설 관리자 작업에는 다음이 포함됩니다.
  - 물리적 위치에 있는 모든 Amazon One 디바이스 인스턴스를 포함하는 사이트 생성
  - 관리자 사용자를 추가하여 사이트를 관리하고 설치 관리자 사용자를 추가하여 활성화 QR 코드에 액세스

- 관리자는 Amazon One Enterprise를 사용하여 디바이스 인스턴스를 생성하고 Amazon One 디바이스를 관리합니다. 관리 작업에는 다음이 포함됩니다.
  - 사이트에서 디바이스 인스턴스 생성
  - 디바이스 인스턴스에 적용할 구성 템플릿 생성
  - 디바이스 상태 모니터링 및 디바이스 구성 업데이트
  - 사용자 등록 취소

- 설치 관리자는 Amazon One Enterprise를 사용하여 활성화 QR 코드에 액세스하여 디바이스를 활성화합니다. 설치 관리자 작업에는 다음이 포함됩니다.
  - 콘솔에서 활성화 QR 코드에 액세스
  - 활성화할 디바이스 인스턴스에 해당하는 QR 코드 선택
  - Amazon One 디바이스가 설치된 상태에서 선택한 QR 코드 스캔

Amazon One 디바이스 구매

Amazon One Enterprise에 대해 자세히 알아보려면 문의하세요. 그러면 비즈니스 개발 팀원이 연락하여 요금을 포함하여 제안에 대한 자세한 내용을 공유하고 궁금한 사항에 답변해 드릴 것입니다.

Amazon One Enterprise 요금

Amazon One Enterprise 요금에 대해 자세히 알아보려면 문의하세요.

Amazon One 작동 방식

Amazon One은 Amazon One 디바이스를 사용하여 생체 인식으로 사용자를 인증하는 클라우드 기반 생체 인식 서비스입니다. Amazon One 디바이스는 문의를 통해 주문할 수 있습니다.

Amazon One 디바이스를 설치한 후 Amazon One 콘솔 및 인증 애플리케이션의 AWS 계정에 디바이스를 활성화하고 등록할 수 있습니다. 등록된 사용자 생체인식 프로필을 볼 수 있습니다. 필요한 경우 등록을 취소하고 생체 인식 데이터를 삭제할 수 있습니다.

Amazon One Console은 디바이스 추적 및 월별 청구서 보기와 같은 운영 활동을 관리하기 위한 중앙 집중식 허브 역할을 합니다. 사용자는 현장의 지도 등록 스테이션에서 자신의 팔목을 스캔하여 등록할 수 있습니다. 등록이 완료되면 사용자는 Amazon One 지원 디바이스 위로 팔목을 가져가 보안 위치에 원활하게 들어오거나 나갈 수 있습니다.

주제

Amazon One 워크플로

다음은 Amazon One의 기본 워크플로를 자세히 설명합니다.

1. 문의를 통해 Amazon One 디바이스를 구매하고 설치합니다.
2. 디바이스를 설치한 후 Amazon One을 활성화합니다.
3. Amazon One 계정에 로그인합니다.
4. 사용자 등록 및 입력 디바이스를 구성합니다.
5. 직원 야자수를 등록합니다.
6. 관리 및 모니터링 기능을 사용하여 디바이스 상태를 보장하고, 구성을 최신 상태로 유지하고, 포괄적인 감독을 위해 사용자 등록을 추적합니다.

Amazon One 주요 용어

다음은 Amazon One의 주요 용어입니다.

- 사이트 - 고객이 Amazon One 디바이스를 설치하는 고객 관리형 물리적 건물입니다. 사이트는 Amazon One 디바이스의 시설, 네트워킹 및 전원 요구 사항을 충족해야 합니다.

- 디바이스 - 인증을 위한 Amazon One 양자 스캔 생체 인식 디바이스입니다.
- 디바이스 인스턴스 - 구성이 있는 디바이스의 논리적 표현입니다. 디바이스 인스턴스를 사용하면 이전에 설정한 구성 및 이름을 자동으로 상속하면서 Amazon One 디바이스를 교체할 수 있습니다. 디바이스 인스턴스에는 사용자 정의 이름(액세스 제어 소프트웨어와 공유된 이름 지정 규칙)과 통신 구성 세트가 있습니다. 디바이스 인스턴스에는 세 가지 기본 상태가 있습니다.
  - 구성 필요
  - 활성화 준비 완료
  - 활성
- 구성 템플릿 - 디바이스 인스턴스에 적용되는 모든 구성 세트입니다.

Amazon One 콘솔 설정

이 장에서는 Amazon One 콘솔을 시작하기 위한 기본 단계를 설명합니다.

사이트, 디바이스 인스턴스 및 구성 템플릿 설정 - 다음 단계에 따라 Amazon One 디바이스를 보관할 물리적 위치를 추가하기 위한 프레임워크를 생성한 다음 Amazon One Enterprise 콘솔을 사용하여 이를 구성하고 관리합니다. 사이트, 디바이스 인스턴스 및 구성 템플릿 수에 따라이 프로세스를 가끔 또는 한 번만 사용합니다.

주제

AWS 계정에 가입합니다

AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성하십시오.

AWS 계정에 등록하려면

1. https://portal.aws.amazon.com/billing/signup를 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 수 있는 권한이 있습니다. 보안 모범 사례로 사용자에게 관리 액세스 권한을 할당하고 루트 사용자만 사용하여 루트 사용자 액세스가 필요한 작업을 수행합니다.

AWS에서는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 로 이동하여 내 계정을 https://aws.amazon.com/ 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

AWS 계정에 가입한 후 AWS 계정 루트 사용자를 보호하고, AWS IAM Identity Center를 활성화하고, 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

주제

AWS 계정 보안

이제 Amazon One 계정에 로그인했으므로 계정을 보호합니다.

AWS 계정 루트 사용자를 보호하려면

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 AWS Management Console에 로그인합니다.
2. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
3. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔)를 참조하세요.

관리 액세스 권한이 있는 사용자 생성

이제 Amazon One 계정을 보호했으므로 관리 액세스 권한이 있는 사용자를 생성합니다.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center 활성화를 참조하세요.

2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스 구성을 참조하세요.

관리자로 로그인

이제 관리자 액세스 권한이 있는 사용자를 생성했으므로 관리자로 로그인합니다.

관리자 액세스 권한이 있는 사용자로 로그인하려면

- IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용하여 IAM Identity Center 사용자로 로그인합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS Sign-in 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

이제 관리자로 로그인했으므로 추가 사용자에게 액세스 권한을 할당할 수 있습니다.

추가 사용자에게 액세스 권한을 할당하려면

- 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

  지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

Amazon One 사용자 추가

관리자 사용자 외에도 관리자 권한이 없는 사용자를 추가할 수 있습니다. 예를 들어 이러한 사용자는 Amazon One 디바이스 활성화 QR 코드를 검색하여 Amazon One 디바이스를 활성화하기 위해서만 Amazon One 콘솔에 액세스하는 설치 관리자일 수 있습니다.

Amazon One 사용자를 추가하려면

1. 사용 AWS AWS 로그인 설명서의에 로그인하는 방법에 설명된 대로 사용자 유형에 적합한 로그인 절차를 따릅니다.
2. 탐색 창에서 사용자를 선택한 다음 사용자 추가를 선택합니다.

3. 사용자 세부 정보 지정 페이지의 사용자 세부 정보 아래에 있는 사용자 이름에 새 사용자의 이름을 입력합니다. 이것은 AWS에 로그인할 때 사용하는 이름입니다.

> **Note**
>
> 의 IAM 리소스 수와 크기는 AWS 계정 제한됩니다. 자세한 내용은 IAM 및 AWS STS 할당량을 참조하세요. 사용자 이름은 최대 64자의 문자, 숫자 및 더하기(+), 등호(=), 쉼표(,), 마침표(.), at 기호(@), 밑줄(_), 하이픈(-) 문자의 조합일 수 있습니다. 이름은 계정 내에서 고유해야 합니다. 대/소문자를 구분하지 않습니다. 예를 들어 "TESTUSER"와 "testuser"라는 두 사용자를 만들 수는 없습니다. 사용자 이름이 정책에서 또는 ARN의 일부로 사용되는 경우 이름은 대소문자를 구분합니다. 콘솔에서 고객에게 사용자 이름이 표시되는 경우(예: 로그인 프로세스 중) 사용자 이름은 대소문자를 구분하지 않습니다.

4. 콘솔 액세스 권한을 제공하려는지 여부를 묻는 메시지가 표시됩니다. 에 대한 사용자 액세스 권한 제공 – AWS Management Console 선택 사항을 선택합니다.
5. IAM 사용자를 생성하려면 선택합니다.
6. 콘솔 암호의 경우 다음 중 하나를 선택합니다.

   - 자동 생성된 암호 - 사용자에게 계정 암호 정책을 충족하는 임의로 생성된 암호가 제공됩니다. 암호 검색 페이지에 이르면 암호를 보거나 다운로드할 수 있습니다.
   - 사용자 지정 암호 - 필드에 입력한 암호가 사용자에게 할당됩니다.

7. (선택 사항) 사용자가 처음 로그인할 때 암호를 변경해야 하도록 하려면 기본적으로 다음 로그인 시 새 암호를 생성해야 합니다(권장).

> **Note**
>
> 관리자가 사용자 자신의 비밀번호 변경 허용 계정 암호 정책 설정을 활성화한 경우 이 확인란은 아무 작업도 수행하지 않습니다. 그렇지 않은 경우에는 새 사용자에게 `IAMUserChangePassword`라는 AWS 관리형 정책이 자동으로 연결됩니다. 이 정책은 사용자에게 자신의 암호를 변경할 수 있는 권한을 부여합니다.

8. 다음을 선택합니다.
9. 권한 설정 페이지에서 정책을 직접 연결을 선택합니다.
10. 사용자에게 연결할 정책을 선택합니다.

    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess 관리형 정책은 Amazon One Enterprise 콘솔에서만 활성화 QR 코드에 대한 사용자 액세스를 제공합니다. 이 정책은 Amazon One 디바이스를 설치하기 위해 타사를 고용하는 기업에 적합합니다.

11. 다음을 선택합니다.
12. (선택 사항) 검토 및 생성 페이지의 태그에서 새 태그 추가를 선택하여 태그를 키 값 페어로 연결해 메타데이터를 사용자에게 추가합니다. IAM에서 태그를 사용하는 방법에 대한 자세한 내용은 IAM 리소스 태깅을 참조하세요.
13. 이 시점까지의 모든 선택을 검토합니다. 계속 진행할 준비가 되었으면 사용자 생성을 선택합니다.
14. 비밀번호 검색 페이지에서 사용자에게 할당된 비밀번호를 가져옵니다.
    - 암호 옆에 있는 보기를 선택하여 사용자 암호를 보고 수동으로 기록할 수 있습니다.
    - .csv 다운로드를 선택하여 사용자의 로그인 자격 증명을 안전한 위치에 저장할 수 있는 .csv 파일로 다운로드합니다.
15. 이메일 로그인 지침을 선택합니다. 사용자 지정하여 사용자에게 보낼 수 있는 초안과 함께 로컬 메일 클라이언트가 열립니다. 이메일 템플릿에는 각 사용자에 대한 다음과 같은 세부 정보가 포함되어 있습니다.
    - 사용자 이름
    - 계정 로그인 페이지의 URL. 다음 예제를 사용하여 올바른 계정 ID 번호 또는 계정 별칭을 대체합니다.

```
https://AWS-account-ID or alias.signin.aws.amazon.com/console
```

> **Important**
>
> 생성된 이메일에는 사용자 암호가 포함되어 있지 않습니다. 조직의 보안 지침을 준수하는 방식으로 사용자에게 암호를 제공해야 합니다.

사이트 생성

이제에 로그인했으므로 Amazon One 콘솔을 사용하여 사이트를 생성할 AWS Management Console 수 있습니다.

> **Important**
>
> Amazon One은 미국 동부(버지니아 북부) 리전에서만 사용할 수 있습니다.

사이트 생성

1. https://console.aws.amazon.com/one-enterprise Amazon One 콘솔을 엽니다.
2. 개요로 이동을 선택합니다.
3. 탐색 창에서 사이트를 선택합니다.
4. 사이트 생성을 선택합니다.
5. 사이트 정보의 사이트 이름에 사이트 이름을 입력합니다.
6. 물리적 주소에 Amazon One 디바이스를 설치할 사이트의 주소를 입력합니다.
7. (선택 사항) 사이트에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 사이트를 생성하기 전에이 태그를 제거하려면 제거를 선택합니다.
8. 사이트 생성을 선택하여 사이트를 생성합니다.

디바이스 인스턴스 생성

이제 AWS Management Console에서 사이트를 생성했으므로 Amazon One 콘솔을 사용하여 디바이스 인스턴스를 생성할 수 있습니다.

디바이스 인스턴스를 생성하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다. 비활성화된 인스턴스 탭에 있는지 확인합니다.
3. 인스턴스 세부 정보의 사이트 드롭다운에서 사이트를 선택하거나 사이트 생성 버튼을 선택하여 새 사이트를 생성합니다.
4. 각 개별 디바이스 인스턴스 이름을 수동으로 입력합니다.

5. (선택 사항) 디바이스 인스턴스에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 디바이스 인스턴스를 생성하기 전에이 태그를 제거하려면 제거를 선택합니다.
6. 인스턴스 생성을 선택하여 디바이스 인스턴스를 생성합니다.

> **Note**
>
> 참고: 디바이스 인스턴스를 구성해야 설치가 가능합니다.

구성 템플릿 생성

이제 디바이스 인스턴스를 생성했으므로 Amazon One 콘솔을 사용하여 구성 템플릿을 생성할 수 있습니다.

구성 템플릿을 만들려면

1. https://console.aws.amazon.com/one-enterprise Amazon One 콘솔을 엽니다.
2. 탐색 창에서 구성 템플릿을 선택합니다.
3. 템플릿 생성을 선택합니다.
4. 템플릿 정보의 템플릿 이름에 구성 템플릿의 이름을 입력합니다.
5. 디바이스 구성에서 작업 모드를 선택합니다.

   To configure Enrollment operating mode

   1. (선택 사항) Wifi 구성에서 Wifi 자격 증명을 제공합니다.
   2. (선택 사항) 사이트에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 사이트를 생성하기 전에이 태그를 제거하려면 제거를 선택합니다.
   3. 구성을 선택합니다.

   To configure Entry operating mode

   1. 제어판 설정에서 Amazon One 디바이스가 제어판과 통신할 수 있도록 통신 설정을 제공합니다.
   2. 배지 형식 설정에서 회사 배지 형식의 레이아웃을 지정하는 구성 설정을 제공합니다.
   3. (선택 사항) Wifi 구성에서 Wifi 자격 증명을 제공합니다.

4. (선택 사항) 사이트에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 사이트를 생성하기 전에이 태그를 제거하려면 제거를 선택합니다.
5. 구성을 선택합니다.

> **Important**
>
> 보안 액세스를 위해 Amazon One의 전체 기능을 활성화하려면 하나 이상의 등록 디바이스와 하나의 입력 디바이스를 구성해야 합니다.

활성화를 위한 디바이스 인스턴스 구성

디바이스 인스턴스를 생성한 후 이전에 생성한 구성 템플릿으로 디바이스 인스턴스를 구성하거나(참조구성 템플릿 생성) 구성을 수동으로 추가할 수 있습니다.

활성화를 위해 디바이스 인스턴스를 구성하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다. 비활성화된 인스턴스 탭에 있는지 확인합니다.
3. 구성할 인스턴스를 하나 이상 선택합니다.
4. 구성을 선택합니다.
5. 디바이스 구성에서 다음 두 가지 입력 방법 중 하나를 선택합니다.

   a. 템플릿 사용 옵션의 드롭다운에서 템플릿을 선택합니다. 가져온이 구성 정보를 검토하거나 변경합니다.

      템플릿 생성 옵션은 섹션을 참조하세요구성 템플릿 생성.

   b. 수동 입력 옵션에서 작동 모드를 선택합니다.

      To configure Enrollment operating mode

      a. (선택 사항) Wifi 구성에서 Wifi 자격 증명을 제공합니다.

      b. (선택 사항) 사이트에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 사이트를 생성하기 전에이 태그를 제거하려면 제거를 선택합니다.

      c. 구성을 선택합니다.

To configure Entry operating mode

a. 제어판 설정에서 Amazon One 디바이스가 제어판과 통신할 수 있도록 통신 설정을 제공합니다.
b. 배지 형식 설정에서 회사 배지 형식의 레이아웃을 지정하는 구성 설정을 제공합니다.
c. (선택 사항) Wifi 구성에서 Wifi 자격 증명을 제공합니다.
d. (선택 사항) 사이트에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 사이트를 생성하기 전에이 태그를 제거하려면 제거를 선택합니다.
e. 구성을 선택합니다.

6. 비활성화된 인스턴스 테이블에서 인스턴스 상태에가 표시되어야 합니다 

.
7. 활성화 QR 코드를 활성화에 사용할 수 있는지 확인합니다. 탐색 창에서 활성화 QR 코드를 선택합니다.
8. 사이트 선택 드롭다운 목록에서 사이트를 선택합니다.
9. 사이트 정보에서 사이트 주소를 확인합니다.
10. 활성화 QR 코드에서 각 디바이스 인스턴스에는 해당 QR 코드가 있습니다. QR 코드 가져오기를 선택하여 활성화 QR 코드를 표시합니다.

> **Important**
>
> 보안 액세스를 위해 Amazon One의 전체 기능을 활성화하려면 하나 이상의 등록 디바이스와 하나의 입력 디바이스를 구성해야 합니다.

Amazon One 설치 및 활성화

Amazon One 콘솔을 성공적으로 설정한 후 다음 단계에서는 사이트에 Amazon One 디바이스를 설치하고 제대로 활성화되었는지 확인합니다. 이 프로세스에는 디바이스를 지정된 영역에 물리적으로 배치, 네트워크에 연결, 원활한 사용자 식별 및 트랜잭션 기능을 지원하는 활성화 프로세스 완료가 포함됩니다. 활성화되면 Amazon One 디바이스가 고객 또는 직원에게 안전하고 터치 없는 환경을 제공할 준비가 됩니다.

> **Note**
>
> 이 섹션에서는 설치에 중점을 두고 모바일 브라우저를 사용하여 AWS Management Console에 액세스하여 디바이스 정품 인증 QR 코드를 가져옵니다.

주제

요구 사항 이해

Amazon One 디바이스는 제어가 가능한 문이 있는 모든 기업 또는 비즈니스 위치에 설치할 수 있습니다.

제어판 요구 사항

Amazon One 디바이스는 대부분의 표준 액세스 제어판에 리더로 연결할 수 있습니다. Amazon One 디바이스는 다음 프로토콜을 지원합니다.

- OSDP(v1 및 v2)
- Wiegand

네트워크 요구 사항

정상 작동하려면 Amazon One 디바이스를 항상 인터넷에 연결해야 합니다. 유선 이더넷 또는 Wi-Fi를 통해 인터넷 연결을 제공할 수 있습니다. 최소 필수 대역폭은 10Mbps입니다.

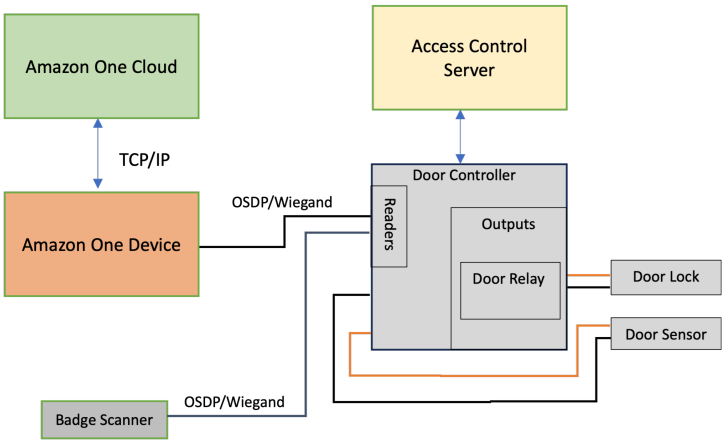
전원 요구 사항

Amazon One 디바이스는 다음 두 가지 방법 중 하나로 전원을 공급할 수 있습니다.

- 상자에 제공된 120V 전원 어댑터를 사용합니다.
- PoE+ 지원 디바이스를 사용합니다.

설치 개념 이해

빌딩 액세스를 올바르게 보호하려면 다음 블록 다이어그램에 설명된 대로 일반적인 액세스 제어 환경의 일부로 디바이스를 설치하는 것이 좋습니다.



액세스 제어 환경은 일반적으로 다음과 같은 구성 요소로 구성됩니다.

- Amazon One 디바이스: 건물의 보안 영역에 액세스하려는 개인을 식별하기 위해 생체인식 인증을 수행하는 휴대폰 인식 디바이스입니다.
- 액세스 제어 서버:이 구성 요소는 일반적으로 보안 영역에 대한 사용자의 액세스 권한을 제어합니다. 영역에 액세스할 수 있는 개인의 배지 IDs는이 서버에 저장됩니다. 이 서버는 관련 IDs에 캐싱합니다.
- 도어 컨트롤러:
  - Amazon One 디바이스는 OSDP 인터페이스를 통해 도어 컨트롤러 서버에 연결합니다.
  - Wiegand 인터페이스가 필요한 경우 COTS OSDP-to-Wiegand 변환기를 사용할 수 있습니다.

- 인증에 성공하면 Amazon One 디바이스가 사용자의 배지 ID를 도어 컨트롤러로 보냅니다.
- 도어 컨트롤러는 결정으로 응답합니다. 그러면 Amazon One 디바이스가 액세스 권한 부여됨 또는 액세스 거부됨 메시지를 표시할 수 있습니다.

- 배지 스캐너: 배지 스캐너는 일반적으로 배지를 스캔하고 배지 번호를 액세스 제어 서버로 전송하는 데 사용됩니다. Amazon One을 사용하면 배지 스캐너가 Amazon One 디바이스에 연결되어 사용자가 배지를 스캔할 수 있으며, 이를 통해 사용자는 자신의 팔목 프로필과 연결할 수 있습니다.

Amazon One Pedestal 설치

Amazon One Pedestal은 사용자에게 원활하고 터치 없는 경험을 제공하도록 설계된 Amazon One 식별 및 트랜잭션 시스템의 주요 구성 요소입니다. 이 디바이스는 안전한 생체인식 인증을 제공합니다. 이를 다양한 위치에 통합하여 원활한 액세스 또는 결제 솔루션을 제공할 수 있습니다.

이 섹션에서는 위치 요구 사항과 Amazon One Pedestal 설치를 위한 step-by-step 지침을 제공합니다. 적절한 준비 및 설치는 시스템이 안전하고 효율적으로 작동하여 사용자에게 원활하고 신뢰할 수 있는 환경을 제공하는 데 중요합니다.

Amazon One Pedestal 설치를 위한 사전 조건 및 준비

설치를 시작하기 전에 안전하고 효과적인 설정을 위해 다음 조건이 충족되는지 확인합니다.

- 전원 요구 사항: POE+(Power over Ethernet)를 사용하여 디바이스에 전원을 공급하는 경우 Cat6 케이블이 이미 설치되어 있고 POE+ 인젝터 또는 스위치를 사용할 수 있는지 확인합니다. 또는 AC 전원(120V)을 사용하는 경우 액세스 가능한 AC 콘센트가 받침대에서 20피트 이내에 있는지 확인합니다.

- 물리적 설정: 안정적이고 안전한 받침대 설치를 위해 바닥이 평평하고 깔끔하며 잔해가 없어야 합니다.
- 받침대 위치: 출입문, 차선 또는 액세스 포인트를 차단하지 않는 위치에 받침대를 설치하여 영역 주위를 쉽게 이동할 수 있습니다.
- 케이블 관리: 어수선하지 않고 정상적인 사용 중에 발생할 수 있는 손상을 방지하기 위해 모든 초과 케이블을 받침대 내부에 라우팅하고 보호합니다.

이러한 사전 조건이 확인되면 설치 프로세스를 진행할 수 있습니다.

Amazon One Pedestal을 설치하려면

1. 패키징에서 Amazon One Pedestal을 제거합니다.
2. M4 변조 방지 나사 두 개를 모두 풀어 도어를 제거합니다.
3. 전원 케이블을 연결합니다.
4. pedestal base plate의 구멍을 통해 케이블을 라우팅합니다.
5. 받침대 내부에 여분의 전원 케이블을 감습니다.
6. 이더넷 케이블(Cat5E 이상)을 받침대의 하단 판을 통해 라우팅하고 이더넷 포트에 연결합니다.
7. 페디스털 베이스에서 2인치 위에 있는 이더넷 케이블에 페라이트 루프를 설치합니다.
8. RS485 직렬 케이블을 액세스 제어판(또는 배지 리더)에서 1피트 초과 길이의 받침대로 공급합니다.
9. 페디스털 베이스에서 2인치 위에 있는 RS485 케이블에 페라이트 루프를 설치합니다.
10. 콘센트에 전원을 연결하고 Amazon One 디바이스가 켜져 있는지 확인합니다.
11. 문을 받침대에 다시 연결하고 M4 변조 방지 나사 2개를 다시 묶어 고정합니다.

Amazon One 디바이스를 설치한 후 디바이스를 활성화할 준비가 되었습니다.

벽면 장착 가능 Amazon One 디바이스 설치

벽 장착 가능 Amazon One 디바이스는 다양한 환경의 사용자에게 원활하고 터치 없는 경험을 제공하도록 설계된 다목적 소형 생체 인식 식별 시스템입니다. 안전한 액세스 또는 결제를 위해 고급 휴대폰 인식 기술을 사용하므로 소매 공간, 사무실 입구 등과 같은 트래픽이 많은 위치에 적합합니다.

이 섹션에서는 최적의 성능과 보안을 보장하기 위해 벽면 장착 가능한 Amazon One 디바이스를 설치하는 데 필요한 위치 요구 사항과 자세한 단계를 간략하게 설명합니다.

벽면 장착 가능 Amazon One 디바이스 설치를 위한 사전 조건 및 준비

설치를 시작하기 전에 디바이스가 효과적으로 작동하고 스페이스 내에 올바르게 설정되도록 다음 조건이 충족되는지 확인합니다.

- 실내 전용: 벽 장착 가능 Amazon One 디바이스는 실내 전용이므로 적절한 환경에 설치되어야 합니다.
- 벽 요구 사항: 디바이스의 적절한 정렬 및 기능을 보장하려면 벽이 수평이어야 합니다.
- 탑재 높이: 벽면 탑재 상단은 설치 후 지면에서 44~46인치 이내로 배치하여 사용자가 쉽게 액세스할 수 있도록 해야 합니다.
- 케이블 관리: 모든 초과 케이블이 벽 마운트 뒤에 배치되고 손상이나 잡동사니를 방지하기 위해 안전하게 고정되어 있는지 확인합니다.
- Power Over Ethernet(PoE++): Power Over Ethernet(PoE++)을 사용하는 경우 IEEE 802.3bt(유형 3) 클래스 6 PoE++ 스위치(엔드 스팬) 또는 인젝터(중간 기간)를 사용할 수 있는지 확인합니다. PoE++ 소스는 나열되거나 인증되어야 하며 IEC 62368-1 표준을 준수해야 합니다. 중요한 것은 PoE와 동일한 건물 내에 위치해야 한다는 것입니다. AOE 디바이스에는 승인된 PoE++ 소스만 사용합니다.
- 15V DC 전원 입력: 15V DC 전원 입력을 사용하는 경우 Hello Class 2 또는 제한된 전원 공급 장치만 사용해야 합니다. 전원 공급 장치는 안전 및 호환성을 위해 나열되거나 인증되어야 합니다.

필수 도구

- 벽 앵커가 필요한 경우 1/4인치 드라이 월 또는 석조 드릴 비트
- 와이어 스트리퍼
- 파일럿 홀 드릴링을 위한 7/64인치 드릴 비트
- #2 Phillips 드라이버
- 0.5mm x 2mm 플랫헤드 드라이버
- T12 보안 드라이버
- 연필
- 수준

벽 장착 가능 Amazon One 디바이스에 포함됨

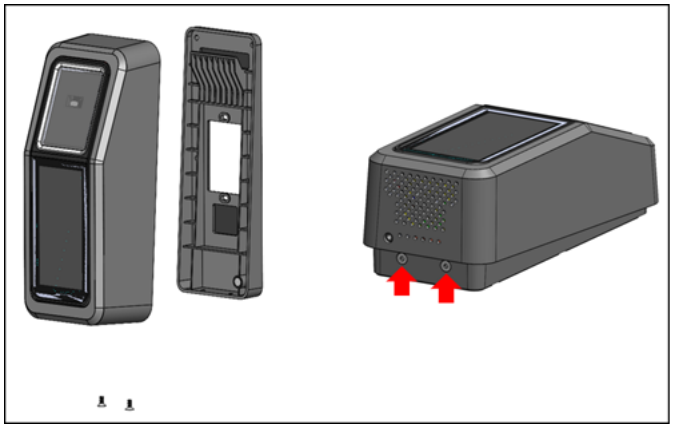
- #8 드라이월 앵커 6개
- 6x #8-32 1in 긴 나사

- #6-32 1in 머신 나사 2개
- 2x 6 위치 터미널 블록 커넥터
- 2" 보안 M4x10 플랫헤드 나사

이러한 사전 조건이 확인되면 설치 단계를 진행하여 벽면 장착 가능한 Amazon One 디바이스를 안전하게 탑재하고 구성할 수 있습니다.

Amazon One 디바이스에 벽 장착 판을 설치하려면

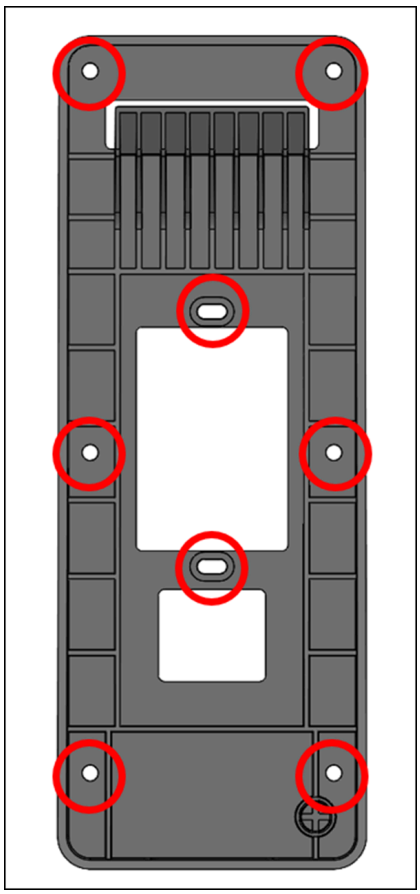
1. 패키징에서 Amazon One 디바이스를 제거합니다.
2. 하단의 두 보안 나사를 제거하여 Amazon One 디바이스에서 탑재 판을 분리합니다.



3. 벽의 원하는 위치에 탑재 판을 배치합니다. 다음 이미지와 같이 브래킷을 템플릿으로 사용하여 외부 6개의 나사 구멍을 표시합니다.

   (선택 사항) 설치 위치에서 단일 갱 박스를 사용할 수 있는 경우 다음을 수행합니다.

   - 장방형 구멍을 통해 포함된 #6-32 기계 나사를 삽입하여 판을 갱 박스에 느슨하게 탑재합니다.
   - 탑재판이 수평인지 확인합니다.
   - 탑재 판을 템플릿으로 사용하여 6개의 나사 위치를 연필로 표시합니다. 장방형 구멍과 #6-32 나사를 탑재판에 대한 추가 지원으로 사용할 수 있습니다. #6-32 나사 위치를 벽판을 장착하는 기본 수단으로 사용하지 마십시오.



4. stucco, drywall, brick 또는 콘크리트 표면에 장착하는 경우 표시된 각 위치에 1/4인치 구멍을 뚫은 다음 앵커가 벽과 같은 높이가 될 때까지 구멍에 눌러 벽 앵커를 설치합니다.

   나무 표면에 장착하는 경우 앵커가 필요하지 않으며 표시된 위치에 7/64인치 파일럿 구멍만 필요합니다.
5. 앵커 위치의 #8 나무 나사를 사용하여 벽판을 벽에 느슨하게 고정합니다.
6. 모든 고정 장치가 제자리에 있으면 탑재판이 수평인지 확인합니다.
7. 나사를 조여 장착 판을 벽에 고정합니다.

벽면 장착 가능 Amazon One 디바이스를 연결하려면

OSDP 및 Weigand 액세스 제어 프로토콜로 Amazon One 디바이스를 구성할 수 있습니다. 설치를 간소화하기 위해 Amazon One 디바이스는 터미널 블록 커넥터(Mfg P/N: Phoenix 연락처 1767694)를 활용합니다. 또한 내부 릴레이 또는 범용 입력 및 출력 연결을 사용하여 외부 디바이스를 직접 제어하도록 Amazon One 디바이스를 구성할 수 있습니다.

1. 애플리케이션에 적합한 연결 구성을 확인하려면 다음 다이어그램 및 연결 표를 참조하세요.

   신호의 자세한 전기 특성은 유선 지침을 참조하세요.

   연결

핀	Connection	설명	사용	
1	GPO	범용 출력	디지털 출력 신호 - 선택 사항	
2	GPI	범용 입력	디지털 입력 신호 - 선택 사항	
3	LED	Wiegand LED	Wiegand LED - 선택 사항	
4	D1	Wiegand D1	Wiegand 데이터 1 - 흰색 와이어	
5	D0	Wiegand D0	Wiegand 데이터 0 - 녹색 와이어	
6	RTN	신호 반환	Wiegand Ground – 검은색 와이어	
7	Com	릴레이 공통	고객 응대 릴레이 공통 - 흰색 와이어	
8	NC	릴레이가 정상적으로 닫힘	고객 응대 릴레이 정상 닫힘 - 주황색 와이어	
9	NO	릴레이 정상 열림	고객 응대 릴레이 정상 열림 - 노란색 와이어	

핀	Connection	설명	사용	
10	RTN	신호 반환	OSDP 반환 - 검은색 와이어	
11	A	RS485_A/D1/클록	OSDP D1 – 흰색 와이어	
12	B	RS485_B/D0/데이터	OSDP D0 – 녹색 와이어	

2. 와이어를 설치할 때 와이어 끝에서 3mm~5mm를 제거합니다.
3. 와이어의 벗긴 끝을 원하는 터미널 위치에 삽입합니다.
4. 플랫헤드 드라이버를 사용하여 터미널 고정 나사를 시계 방향으로 돌려 와이어가 꼭 맞을 때까지 고정합니다. 너무 조이지 마십시오.
5. 고정 후 와이어를 살짝 잡아당겨 고정되었는지 확인합니다.
6. 필요한 연결을 수행한 후 Amazon One 디바이스 터미널 블록의 해당 소켓에 플러그를 삽입합니다.
7. RJ45 잭에 Cat6 이더넷 케이블을 삽입합니다.
8. 벽판의 후크가 디바이스 후면의 구멍으로 미끄러지도록 Amazon One 디바이스를 배치합니다.
9. 디바이스와 탑재판 사이에 케이블이 걸리지 않았는지 확인하고 디바이스가 회전하여 제자리에 장착되도록 합니다.
10. 두 개의 Linux Security M4x10 플랫헤드 나사로 Amazon One 디바이스를 탑재판에 고정합니다.
11. 나사를 손으로 조이세요. 너무 조이지 마세요.

벽면 장착 가능 Amazon One 디바이스를 연결하려면

애플리케이션에 필요한 와이어만 설치합니다.

Wiegand 연결

- 핀 3(LED)에 파란색 와이어를 삽입합니다.
- 흰색 와이어를 핀 4(D1)에 삽입합니다.
- 핀 5(D0)에 녹색 와이어를 삽입합니다.
- 핀 6(RTN)에 검은색 와이어를 삽입합니다.

Wiegand 출력 와이어링

핀	Connection	설명	사용	
3	LED	Wiegand LED	Wiegand LED 입력 - 선택 사항 (5V TTL)	
4	D1	Wiegand D1	Wiegand D1 출력(5V TTL)	
5	D0	Wiegand D0	Wiegand D0 출력(5V TTL)	
6	RTN	신호 반환	Wiegand GND 참조	

디바이스가 줄의 마지막 단위인 경우 RS485 종료 스위치를 “ON”으로 설정합니다. 이 스위치는 라인에서 120옴 저항기 종료를 활성화합니다.

RS485 연결

- 핀 10(RTN)에 검은색 와이어를 삽입합니다.
- 흰색 와이어를 핀 11(A)에 삽입합니다.
- 핀 12(B)에 녹색 와이어를 삽입합니다.

RS485 와이어링

핀	Connection	설명	사용	
10	RTN	신호 반환	Ground(지상)	

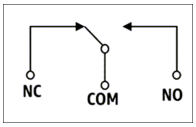
핀	Connection	설명	사용	
11	A	RS485_A/D1/클록	RS485 비 반전 신호	
12	B	RS485_B/D0/데이터	RS485 반전 신호	

릴레이 연결

- 흰색 와이어를 핀 7(COM)에 삽입합니다.
- 핀 8(NC)에 주황색 와이어를 삽입합니다.
- 노란색 와이어를 핀 9(NO)에 삽입합니다.

릴레이 와이어링

핀	Connection	설명	사용	
7	COM	릴레이 공통	고객 응대 릴레이 공통 - 흰색 와이어	
8	NC	릴레이가 정상적으로 닫힘	고객 응대 릴레이 상시 닫힘 - 주황색 와이어	
9	NO	릴레이 정상 열림	고객 응대 릴레이 정상 열림 - 노란색 와이어	



릴레이는 지정된 안전 등급 30VAC/60Mbps, 최대 60W에 따라 작동해야 합니다.

디지털 입력/출력 연결

- 핀 1(GPO)에 파란색 와이어를 삽입합니다.
- 핀 2(GPI)에 파란색 와이어를 삽입합니다.

디지털 입력/출력 와이어링

핀	Connection	설명	사용	
1	GPO	범용 출력	디지털 출력 신호 (5V)	
2	GPI	범용 입력	디지털 입력 신호 (3.6V~5V)	

- 디지털 입력/출력 연결은 나열된 대로 작동해야 합니다.

Amazon One 디바이스를 설치한 후 디바이스를 활성화할 준비가 되었습니다.

보안 액세스를 위한 Amazon One 디바이스 I/O Hub 설치

I/O Hub가 있는 Amazon One 디바이스는 Amazon One Enterprise 시스템의 필수 부분으로, 다양한 환경에 대한 보안을 강화하고 액세스 제어를 간소화하도록 설계되었습니다. 이 디바이스는 생체 인식 양자 인식을 활용하여 사용자에게 안전하고 터치 없는 인증을 제공하므로 사무실 건물, 제한된 진입점 또는 원활한 액세스 관리가 필요한 시설과 같은 고보안 영역에서 사용하기에 적합합니다. I/O Hub는 디바이스와 기존 보안 인프라 간의 브리지 역할을 하므로 도어 잠금, 경보 및 기타 액세스 제어 시스템과 통신할 수 있습니다.

이 섹션에서는 I/O Hub를 사용하여 Amazon One 디바이스를 설치하기 위한 위치 요구 사항과 step-by-step 지침을 제공합니다. 적절한 준비 및 설치는 시스템이 안전하고 효율적으로 작동하여 사용자에게 원활하고 신뢰할 수 있는 환경을 제공하는 데 중요합니다.

I/O Hub를 사용하여 Amazon One Device를 설치하기 위한 사전 조건 및 준비

설치를 시작하기 전에 안전하고 효과적인 설정을 위해 다음 조건을 충족하는지 확인합니다.

- 실내 전용: I/O Hub가 있는 Amazon One 디바이스는 실내 전용으로 설계되었습니다. 적절한 환경에 설치되어 있는지 확인합니다.
- Power Over Ethernet(PoE++): Power Over Ethernet(PoE++)을 사용하는 경우 IEEE 802.3bt(유형 3) 클래스 6 PoE++ 스위치(엔드 스팬) 또는 인젝터(중간 기간)를 사용할 수 있는지 확인합니다. PoE++ 소스는 나열되거나 인증되어야 하며 IEC 62368-1 표준을 준수해야 합니다. 중요한 것은 PoE와 동일한 건물 내에 위치해야 한다는 것입니다. AOE 디바이스에는 승인된 PoE++ 소스만 사용합니다.

- 15V DC 전원 입력: 15V DC 전원 입력을 사용하는 경우 Hello Class 2 또는 승인된 전원 공급 장치만 사용해야 합니다. 전원 공급 장치는 안전을 위해 나열되거나 인증되어야 합니다. 자세한 내용은 아래의 선택적 DC 섹션을 참조하세요.

필수 도구

- 와이어 스트리퍼
- #2 Phillips 드라이버
- 0.5mm x 2mm 플랫헤드 드라이버

I/O Hub가 있는 Amazon One 디바이스에 포함

- 2x 6 위치 터미널 블록 커넥터
- DC 플러그 커넥터
- 72" 전원/데이터 케이블

이러한 사전 조건이 확인되면 설치 프로세스를 진행하여 I/O Hub를 사용하여 Amazon One 디바이스를 안전하고 효율적으로 설정할 수 있습니다. 적절한 준비는 디바이스가 의도한 대로 작동하고 보안 액세스 시스템에 원활하게 통합되도록 보장하는 데 도움이 됩니다.

Amazon One 디바이스의 I/O 허브를 설치하려면

1. 패키징에서 I/O Hub가 있는 Amazon One 디바이스를 제거합니다.
2. 원하는 위치에 I/O 허브를 고정합니다.
3. Amazon One USB 케이블을 I/O 허브 포트에 연결합니다.

4. POE++ 전원의 경우 POE++ 소스의 이더넷 케이블을 I/O 허브 포트에 연결합니다.

   선택 사항: DC 전원의 경우 아래 DC 연결 설치 섹션을 참조하세요.

Amazon One 디바이스의 I/O 허브를 연결하려면

- 드립 루프를 설치하여 실수로 코드를 따라 I/O 허브로 흘러 들어가는 액체를 방지합니다.
- 다음 이미지와 같이 와이어가 손상되거나 스트레스를 받지 않도록 스트레인 완화 고정을 연결합니다.

1. 터미널 블록 플러그를 I/O 허브에 삽입합니다.
2. 터미널 블록 플러그를 통해 애플리케이션에 필요한 와이어만 삽입합니다. 다음 와이어링 테이블 및 다이어그램을 참조하세요.

연결

핀	Connection	설명	사용	
1	RTN	신호 반환	Wiegand 지면 - 검은색 와이어	
2	D1	Wiegand D1	Wiegand Data 1 – 흰색 와이어	
3	D0	Wiegand D0	Wiegand 데이터 0 - 녹색 와이어	
4	LED	Wiegand LED	Wiegand LED - 선택 사항	
5	GPI	범용 입력	디지털 입력 신호 - 선택 사항	

핀	Connection	설명	사용	
6	GPO	범용 출력	디지털 출력 신호 - 선택 사항	
7	B	RS485_B/D0/데이터	OSDP D0 – 녹색 와이어	
8	A	RS485_A/D1/클록	OSDP D1 – 흰색 와이어	
9	RTN	신호 반환	OSDP 반환 - 검은색 와이어	
10	COM	릴레이 공통	고객 응대 릴레이 공통 - 흰색 와이어	
11	NC	릴레이가 정상적으로 닫힘	고객 응대 릴레이 상시 닫힘 - 주황색 와이어	
12	NO	릴레이 정상 열림	고객 응대 릴레이 정상 열림 - 노란색 와이어	

Wiegand 연결

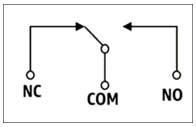
- 핀 1(RTN)에 검은색 와이어를 삽입합니다.
- 흰색 와이어를 핀 2(D1)에 삽입합니다.
- 핀 3(D0)에 녹색 와이어를 삽입합니다.
- 선택 사항: 핀 4(LED)에 녹색 와이어를 삽입합니다.

릴레이 연결

- 흰색 와이어를 핀 10(COM)에 삽입합니다.

- 주황색 와이어를 핀 11(NC)에 삽입합니다.
- 노란색 와이어를 핀 12(NO)에 삽입합니다.

릴레이 다이어그램



릴레이는 지정된 안전 등급 30VAC/60Mbps, 최대 60W에 따라 작동해야 합니다.

RS485 연결

- 핀 7(B)에 녹색 와이어를 삽입합니다.
- 흰색 와이어를 핀 8(A)에 삽입합니다.
- 핀 9(RTN)에 검은색 와이어를 삽입합니다.

디바이스가 줄의 마지막 단위인 경우 RS485 종료 스위치를 “ON”으로 설정합니다. 이 스위치는 라인에서 120옴 저항기 종료를 활성화합니다.

디지털 입력/출력 연결

- 검은색 와이어를 핀 5(GPI)에 삽입합니다.
- 흰색 와이어를 핀 6(GPO)에 삽입합니다.

- 디지털 입력/출력 연결은 나열된 대로 작동해야 합니다.

선택 사항: DC 와이어링 설치

1. 양수(+)의 경우 빨간색 와이어 끝에서 3mm~5mm, 음수(-)의 경우 검은색 와이어 끝에서 벗깁니다.
2. DC 와이어의 벗긴 끝을 DC 플러그에 삽입합니다.

3. 와이어를 제자리에 고정합니다.
4. 유선 DC 플러그를 DC 입력 포트에 삽입합니다.

Amazon One 디바이스를 설치한 후 디바이스를 활성화할 준비가 되었습니다.

Amazon One 디바이스 활성화

Amazon One 디바이스가 설치되고 전원이 켜지면 활성화할 준비가 된 것입니다.

Amazon One 디바이스를 활성화하려면

1. Amazon One 디바이스에서 화면을 탭하여 시작합니다.
2. 이더넷 또는 Wifi를 선택하여 인터넷에 연결합니다.

   디바이스가 인터넷에 연결되자마자 최신 소프트웨어 패키지 다운로드가 시작됩니다.
3. 화면에 소프트웨어 다운로드 완료!가 표시되면 확인을 선택합니다.
4. QR 코드를 선택합니다.

   Amazon One 디바이스 화면에 QR 코드 스캔이 표시됩니다.
5. 활성화 QR 코드를 검색하려면 https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.

   > **Note**
   >
   > Amazon One Enterprise 콘솔에서 활성화 QR 코드에만 액세스할 수 있도록 설치 프로그램에 제한된 권한을 부여하는 것이 좋습니다. Amazon One 사용자 추가을(를) 참조하세요.
6. 탐색 창에서 활성화 QR 코드를 선택합니다.
7. 사이트 선택 드롭다운 목록에서 Amazon One 디바이스가 설치된 사이트를 선택합니다.
8. 사이트 정보에서 사이트 주소를 확인합니다.
9. 활성화 QR 코드에서 활성화하려는 디바이스 인스턴스 이름을 찾고 해당하는 QR 코드 가져오기를 선택하여 QR 코드를 검색합니다.
10. Amazon One 디바이스로 QR 코드를 스캔합니다. QR 코드는 보안을 위해 주기적으로 새로 고쳐지며 QR 코드는 한 번만 사용할 수 있습니다.

11. 사이트 우편번호를 입력하고 올바른 사이트가 표시되는지 확인한 후 설정 확인을 선택합니다.
12. Amazon One 디바이스 화면에 활성화 완료!가 표시되면 디바이스를 사용할 준비가 된 것입니다.

사용자 등록 및 입력

이제 Amazon One 디바이스가 활성화되었으므로 직원은 자신의 팔목을 등록하고 팔목을 인증하여 액세스할 수 있습니다.

주제

엔드포인트 정책 생성

사용자가 입장을 위해 야자수를 인증하려면 먼저 등록 프로세스를 거쳐야 합니다. 보안 담당자는 사용자가 등록하도록 허용하기 전에 항상 사용자의 자격 증명을 확인해야 합니다.

Amazon One 디바이스에 야자수를 등록하려면

1. Amazon One Enterprise 등록 디바이스에서 시작하기를 누릅니다.
2. Amazon One Enterprise 등록 디바이스에 연결된 배지 스캐너로 직원 배지를 스캔합니다.

   배지가 성공적으로 스캔되면 Amazon One 디바이스 화면에 스캔된 배지가 표시됩니다.
3. 이용 약관을 읽은 다음 확인을 누릅니다.
4. 동의 - 팜 생체 정보를 읽고 동의하면 동의함을 누릅니다.
5. 화면의 지침에 따라 등록 프로세스를 완료합니다.

항목에 대한 인증

야자수를 성공적으로 등록하면 Amazon One Enterprise 진입 디바이스에서 야자수로 인증할 준비가 된 것입니다.

Amazon One 디바이스의 진입을 위해 팔목을 인증하려면

- 디바이스 위에 팔목을 올려 놓고 화면의 지침에 따라 팔목을 스캔합니다.

사용자 관리

등록된 사용자 관리 페이지를 사용하여 등록된 사용자를 추적하고 사용자 생체 인식을 삭제할 수 있습니다. 연결된 생체 인식이 삭제된 사용자는 더 이상 인증을 위해 Amazon One 디바이스에 액세스할 수 없습니다.

주제

등록된 사용자 보기

다음 절차에서는 사용자를 등록하는 방법을 자세히 설명합니다.

등록된 사용자를 보려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 등록된 사용자 관리를 선택합니다.
3. 등록된 사용자에서 등록된 모든 사용자와 다음 세부 정보를 확인할 수 있습니다.
    - 배지 ID - 등록 시RFID 배지 리더가 캡처한 배지 식별자 정보입니다.
    - 등록 소스 - 등록에 사용된 Amazon One 디바이스의 세부 정보입니다.
    - 등록 날짜 - 등록 날짜 및 시간입니다.

등록된 사용자 및 생체 인식 삭제

다음 절차에서는 등록된 사용자와 생체 인식을 삭제하는 방법을 자세히 설명합니다.

등록된 사용자 및 해당 생체인식을 삭제하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 등록된 사용자 관리를 선택합니다.
3. 등록된 사용자에서 생체 인식 데이터를 삭제하려는 사용자의 배지 ID를 선택합니다.
4. 생체 인식 삭제를 선택합니다.
5. 삭제를 선택하여 사용자 생체 인식 데이터의 삭제를 확인합니다.

> **Important**
>
> 이 작업을 수행하면 Amazon One Enterprise에서 사용자의 생체 인식이 영구적으로 삭제됩니다. 사용자가 Amazon One Enterprise를 인증에 사용하려면 Amazon One Enterprise 등록 디바이스에 다시 등록해야 합니다. 사용자의 생체 인식을 삭제하면 Amazon One Enterprise에서 배지 ID와 같은 다른 프로필 속성도 영구적으로 삭제됩니다.

Amazon One 디바이스 관리

Amazon One 디바이스가 설치되고 활성화되면 Amazon One Enterprise 콘솔에서 디바이스 상태 보고를 시작합니다. Amazon One Enterprise 콘솔을 사용하여 디바이스 재부팅 또는 구성 업데이트와 같은 디바이스 관리 작업을 수행할 수 있습니다.

주제

Amazon One 디바이스 유지 관리 및 정리

Amazon One 디바이스를 유지 관리하면 최적의 디바이스 운영 환경과 디바이스 환경이 제공됩니다.

Amazon One 디바이스를 청소하기 전에 다음을 확인합니다.

- Amazon One을 활성화하거나 비활성화할 필요는 없지만 디바이스가 전원에 연결되어 있고, 네트워크가 연결되어 있으며, 주변 장치 및 컴패니언 디바이스(해당하는 경우)가 연결되어 있는지 확인합니다.
- 네트워크 연결을 사용할 수 없는 경우 관리자에게 문제를 에스컬레이션합니다(이 경우 Amazon One 디바이스에 오류 화면이 표시됨). 오류 화면이 Amazon One 디바이스에 표시되거나 디바이스 연결 문제가 콘솔에 표시됩니다.
- 권한이 없는 개인이 디바이스를 변조할 수 없도록 디바이스를 물리적으로 보호합니다.
- 매일 Amazon One 디바이스를 시각적으로 검사하여 Amazon One 디바이스에 대한 무단 연결을 확인합니다.
- 디바이스의 눈에 보이는 나사와 케이스를 포함하여 디바이스의 모든 측면을 검사하여 Amazon One 디바이스의 내부 구성 요소/서킷이 노출되는 갭/개방이 없는지 확인합니다.
- 오류 또는 장애가 발생하는 경우 Amazon One 디바이스 화면의 지침을 따르거나 문제 해결 가이드를 참조하여 문제를 해결하세요.

Amazon One 디바이스를 정리하려면

Amazon One 디바이스를 정리하면 지문 및 핸드프린트와 같은 스머지나 표시가 정기적으로 제거됩니다.

> **Note**
>
> 이 가이드에 나열된 것 이외의 다른 청소 제품은 사용하지 마십시오. 권장 청소 일정은 일주일에 한두 번 또는 디바이스에 먼지, 먼지 또는 스머지가 보일 때마다이지만 하루에 한 번 이상은 안 됩니다.

1. Iso™ 알코올(IPA)로 Amazon One 디바이스를 닦습니다. 디바이스의 터치 표면만 정리합니다. Amazon One에서 지시하지 않는 한 광학 창을 만지거나 다른 청소 제품을 사용하지 마세요.
2. 마른 마이크로파이버 의상으로 줄무늬를 닦습니다.
3. 광학 창에서 보이는 모든 흙이나 잔해를 가볍게 털어냅니다(지워서는 안 됨). 광학 윈도우의 청소를 하루에 한 번 이하 및/또는 윈도우가 시각적으로 더러울 때(예: 손가락/손 인화/스머지)로 제한합니다. 디바이스의이 부분은 만지기 위한 것이 아니지만 신규 고객의 실수로 만질 수 있습니다.
4. 해당하는 경우 KIC 스마트 카드 클리너를 사용하여 카드 리더 내부를 정리합니다.
5. 일주일에 한두 번 또는 디바이스에 먼지, 먼지 또는 스머지가 보일 때마다 디바이스를 청소합니다.

사이트 관리

사이트는 디바이스 인스턴스 모음이 설치되고 작동하는 물리적 위치를 나타냅니다. 사이트를 사용하여 동일한 물리적 주소를 공유하는 Amazon One 디바이스를 구성할 수 있습니다.

주제

사이트 이름 변경

다음 절차에서는 디바이스의 사이트 이름을 변경하는 방법을 자세히 설명합니다.

사이트 이름을 변경하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 사이트를 선택합니다.
3. 사이트에서 이름을 편집할 사이트를 선택합니다.
4. 편집을 선택합니다.

5. 사이트 정보에서 원하는 사이트 이름과 사이트 설명(선택 사항)을 입력합니다.
6. 업데이트할 변경 사항 저장을 선택합니다.

사이트 주소 업데이트

다음 절차에서는 디바이스의 사이트 주소를 업데이트하는 방법을 자세히 설명합니다.

사이트 주소를 업데이트하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 사이트를 선택합니다.
3. 사이트에서 주소를 업데이트하려는 사이트를 선택합니다.
4. 디바이스 인스턴스에서 활성화된 인스턴스 수가 0인지 확인합니다.
5. (선택 사항) 활성화된 인스턴스 수가 0이 아닌 경우 섹션을 참조하세요.
6. 편집을 선택합니다.
7. 물리적 주소 아래에 올바른 물리적 주소를 입력합니다.
8. 업데이트할 변경 사항 저장을 선택합니다.

디바이스 인스턴스 관리

디바이스 인스턴스는 구성이 있는 디바이스의 논리적 표현입니다. 디바이스 인스턴스를 사용하면 이전에 설정한 구성 및 이름을 자동으로 상속하면서 Amazon One 디바이스를 교체할 수 있습니다. 디바이스 인스턴스에는 사용자 정의 이름(액세스 제어 소프트웨어와 공유된 이름 지정 규칙)과 통신 구성 세트가 있습니다.

주제

- 디바이스 인스턴스 상태 보기
- Amazon One 디바이스 재부팅
- Amazon One 디바이스 구성 업데이트
- Wi-fi 자격 증명 업데이트
- 디바이스 인스턴스 비활성화

디바이스 인스턴스 상태 보기

다음 절차에서는 디바이스 인스턴스의 상태를 보는 방법을 자세히 설명합니다.

디바이스 인스턴스 상태를 보려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다.
3. 활성화된 인스턴스 아래에 활성화된 Amazon One 디바이스 목록이 표시됩니다.
4. 디바이스 인스턴스 이름을 선택하여 디바이스 인스턴스 세부 정보를 봅니다.

Amazon One 디바이스 재부팅

다음 절차에서는 Amazon One 디바이스를 재부팅하는 방법을 자세히 설명합니다.

Amazon One 디바이스를 재부팅하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다.
3. 활성화된 인스턴스에서 재부팅할 디바이스의 인스턴스 이름을 선택합니다.
4. 재부팅을 선택하여 Amazon One 디바이스를 다시 시작합니다.

Amazon One 디바이스 구성 업데이트

다음 절차에서는 Amazon One 디바이스 구성을 업데이트하는 방법을 자세히 설명합니다.

Amazon One 디바이스 구성을 업데이트하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다.
3. 활성화된 인스턴스에서 업데이트하려는 디바이스의 인스턴스 이름을 선택합니다.
4. 디바이스 구성에서 편집을 선택합니다.

> **Note**
>
> Amazon One 디바이스 모드를 변경하려면 먼저 디바이스 인스턴스를 비활성화한 다음 원하는 디바이스 모드로 구성해야 합니다(참조활성화를 위한 디바이스 인스턴스 구성). 그

런 다음 디바이스 활성화 프로세스를 진행할 수 있습니다(참조Amazon One 디바이스 활성화).

5. 원하는 사항을 변경한 후 디바이스 구성 업데이트를 선택하여 업데이트를 확인합니다.

Wi-fi 자격 증명 업데이트

다음 절차에서는 Wi-Fi 자격 증명을 업데이트하는 방법을 자세히 설명합니다.

Wifi 자격 증명을 업데이트하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다.
3. 활성화된 인스턴스에서 업데이트하려는 디바이스의 인스턴스 이름을 선택합니다.
4. 네트워크에서 편집을 선택합니다.
5. Wi-Fi 구성에서 원하는 대로 변경합니다.
6. 네트워크 업데이트를 선택하여 업데이트를 확인합니다.

디바이스 인스턴스 비활성화

다음 절차에서는 디바이스 인스턴스를 비활성화하는 방법을 자세히 설명합니다.

디바이스 인스턴스를 비활성화하려면

1. https://console.aws.amazon.com/one-enterprise Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스를 선택합니다.
3. 활성화된 인스턴스에서 비활성화하려는 디바이스 인스턴스의 이름을 선택합니다.
4. 디바이스 비활성화를 선택합니다.
5. 비활성화를 확인하려면 메시지 상자에 'deactivate'를 입력하고 디바이스 비활성화를 선택합니다.

보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon One Enterprise에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon One Enterprise를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 Amazon One Enterprise를 구성하는 방법을 보여줍니다. 또한 Amazon One Enterprise 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- Amazon One Enterprise의 데이터 보호
- Amazon One Enterprise의 ID 및 액세스 관리
- Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키
- Amazon One Enterprise에 대한 규정 준수 검증

Amazon One Enterprise의 데이터 보호

AWS 공동 책임 모델 Amazon One Enterprise의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 관한 자세한 내용은 데

이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Amazon One Enterprise 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

저장 데이터의 기본 암호화를 사용하려면

Amazon One Enterprise는 AWS 암호화 키를 사용하여 저장된 민감한 데이터를 보호하기 위해 기본적으로 암호화를 제공합니다.

AWS 소유 키 - Amazon One Enterprise는 기본적으로 이러한 키를 사용하여 민감한 최종 사용자 데이터를 자동으로 암호화합니다. AWS 소유 키를 보거나 관리하거나 사용하거나 사용을 감사할 수 없습니다. 하지만 데이터를 암호화하는 키를 보호하기 위해 어떤 작업을 수행하거나 어떤 프로그램을 변경할

필요가 없습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS 소유 키를 참조하세요.

전송 중 데이터 암호화

Amazon One Enterprise는 전송 계층 보안(TLS)을 사용하여 데이터를 보호하고 서명 버전 4를 사용하여 AWS 서비스에 대한 모든 인바운드 API 요청을 인증합니다. 이 암호화는 기본적으로 활성화되어 있습니다.

Amazon One Enterprise의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 Amazon One Enterprise 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조Amazon One 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(Amazon One Enterprise와 IAM의 작동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(Amazon One Enterprise의 자격 증명 기반 정책 예제 참조)

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증해야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

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.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한

정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Amazon One Enterprise와 IAM의 작동 방식

IAM을 사용하여 Amazon One Enterprise에 대한 액세스를 관리하기 전에 Amazon One Enterprise에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

Amazon One Enterprise에서 사용할 수 있는 IAM 기능

IAM 특성	Amazon One Enterprise 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요

IAM 특성	Amazon One Enterprise 지원
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
엔터티 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

Amazon One Enterprise 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Amazon One Enterprise의 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon One Enterprise의 자격 증명 기반 정책 예제

Amazon One Enterprise 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon One Enterprise의 자격 증명 기반 정책 예제.

Amazon One Enterprise 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

Amazon One Enterprise에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Amazon One Enterprise 작업 목록을 보려면 섹션을 참조하세요Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키.

Amazon One Enterprise의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
one
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [
      "one:action1",
      "one:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "one:Describe*"
```

Amazon One Enterprise 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon One Enterprise의 자격 증명 기반 정책 예제.

Amazon One Enterprise에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Amazon One Enterprise 리소스 유형 및 해당 ARNs 목록을 보고 각 리소스의 ARN을 지정하는 데 사용할 수 있는 작업을 알아보려면 섹션을 참조하세요Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키.

Amazon One Enterprise 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon One Enterprise의 자격 증명 기반 정책 예제.

Amazon One Enterprise에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수

있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Amazon One Enterprise 조건 키 목록을 보고 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 섹션을 참조하세요Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키.

Amazon One Enterprise 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon One Enterprise의 자격 증명 기반 정책 예제.

Amazon One EnterpriseACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon One Enterprise를 사용한 ABAC

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Amazon One Enterprise에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이

AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

Amazon One Enterprise에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Amazon One Enterprise의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Amazon One Enterprise 기능이 중단될 수 있습니다. Amazon One Enterprise가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Amazon One Enterprise의 서비스 연결 역할

서비스 연결 역할 지원: 아니요

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

Amazon One Enterprise의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 Amazon One Enterprise 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 대한 자세한 내용은 서비스 승인 참조의 섹션을 참조하세요. Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키

주제

- 정책 모범 사례
- Amazon One Enterprise 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- Amazon One Enterprise에 대한 읽기 전용 액세스
- Amazon One Enterprise에 대한 전체 액세스 권한
- Amazon One Enterprise Rule API 작업에 지원되는 리소스 수준 권한
- 추가 정보

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 Amazon One Enterprise 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Amazon One Enterprise 콘솔 사용

Amazon One Enterprise 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 Amazon One Enterprise 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 여전히 Amazon One Enterprise 콘솔을 사용할 수 있도록 하려면 Amazon One Enterprise *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

```
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon One Enterprise에 대한 읽기 전용 액세스

다음 예제에서는 Amazon One Enterprise에 읽기 전용 액세스 권한을 `AmazonOneEnterpriseReadOnlyAccess` 부여하는 AWS 관리형 정책을 보여줍니다.

정책 설명에서 `Effect` 요소는 작업 허용 또는 거부 여부를 지정합니다. `Action` 요소는 사용자가 수행할 수 있도록 허용된 특정 작업을 나열합니다. `Resource` 요소는 사용자가 작업을 수행하도록 허용된 AWS 리소스를 나열합니다. Amazon One Enterprise 작업에 대한 액세스를 제어하는 정책의 경우 `Resource` 요소는 항상 "모든 리소스"*를 의미하는 와일드카드인 로 설정됩니다.

서비스가 지원하는 API에 대한 `Action` 요소의 값입니다. 작업 앞에는 Amazon One Enterprise 작업을 참조함을 나타내기 `config:` 위한 작업이 앞에 옵니다. 다음 예제와 같이 * 요소에서 `Action` 와일드카드 문자를 사용할 수 있습니다.

- `"Action": ["one:*DeviceInstanceConfiguration"]`

  이렇게 하면 "DeviceInstance"(`GetDeviceInstanceConfiguration`,)로 끝나는 모든 Amazon One Enterprise 작업이 허용됩니다`CreateDeviceInstanceConfiguration`.

- `"Action": ["one:*"]`

  이렇게 하면 모든 Amazon One Enterprise 작업이 허용되지만 다른 AWS 서비스에 대한 작업은 허용되지 않습니다.
- `"Action": ["*"]`

  이렇게 하면 모든 AWS 작업이 허용됩니다. 이 권한은 계정의 AWS 관리자 역할을 하는 사용자에게 적합합니다.

읽기 전용 정책은 `CreateDeviceInstance`, `UpdateDeviceInstance`및와 같은 작업에 대한 사용자 권한을 부여하지 않습니다`DeleteDeviceInstance`. 이 정책을 사용하는 사용자는 디바이스 인스턴스를 생성하거나, 디바이스 인스턴스를 업데이트하거나, 디바이스 인스턴스를 삭제할 수 없습니다. Amazon One Enterprise 작업 목록은 섹션을 참조하세요Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키.

Amazon One Enterprise에 대한 전체 액세스 권한

다음 예제에서는 Amazon One Enterprise에 대한 전체 액세스 권한을 부여하는 정책을 보여줍니다. 사용자에게 모든 Amazon One Enterprise 작업을 수행할 수 있는 권한을 부여합니다.

> **Important**
>
> 이 정책은 광범위한 권한을 부여합니다. 전체 액세스 권한을 부여하기 전에 최소한의 권한 세트로 시작하여 필요에 따라 추가 권한을 부여하는 것이 좋습니다. 처음부터 권한을 많이 부여한 후 나중에 줄이는 방법보다 이 방법이 더 안전합니다.

Amazon One Enterprise Rule API 작업에 지원되는 리소스 수준 권한

리소스 수준 권한이란 사용자가 작업을 수행할 수 있는 리소스를 지정하는 기능을 말합니다. Amazon One Enterprise는 특정 Amazon One Enterprise 규칙 API 작업에 대한 리소스 수준 권한을 지원합니다. 즉, 특정 Amazon One Enterprise 규칙 작업의 경우 사용자가 해당 작업을 사용할 수 있는 조건을 제어할 수 있습니다. 이러한 조건은 충족되어야 하는 작업이거나 사용자가 사용하도록 허용된 특정 리소스일 수 있습니다.

다음 표에서는 현재 리소스 수준 권한을 지원하는 Amazon One Enterprise 규칙 API 작업에 대해 설명합니다. 또한 각 작업에 지원되는 리소스 및 해당 ARN도 설명합니다. ARN을 지정할 때, 예를 들어, 정확한 리소스 ID를 지정할 수 없거나 지정하길 원치 않는 경우에는 경로에 * 와일드카드를 사용할 수 있습니다.

> **Important**
>
> Amazon One Enterprise 규칙 API 작업이이 표에 나열되지 않은 경우 리소스 수준 권한을 지원하지 않습니다. Amazon One Enterprise 규칙 작업이 리소스 수준 권한을 지원하지 않는 경우 사용자에게 작업을 사용할 수 있는 권한을 부여할 수 있지만 정책 설명의 리소스 요소에 *를 지정해야 합니다.

API 작업	리소스
CreateDeviceInstance	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
GetDeviceInstance	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
UpdateDeviceInstance	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
DeleteDeviceInstance	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
CreateDeviceActivationQrCode	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
DeleteAssociatedDevice	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*

API 작업	리소스
RebootDevice	디바이스 인스턴스 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
CreateDeviceInstanceConfiguration	디바이스 인스턴스 구성 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId* /configuration/*version*
GetDeviceInstanceConfiguration	디바이스 인스턴스 구성 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId* /configuration/*version*
CreateSite	사이트 arn:aws:one:*region:accountID* :site/*siteId*
DeleteSite	사이트 arn:aws:one:*region:accountID* :site/*siteId*
GetSiteAddress	사이트 arn:aws:one:*region:accountID* :site/*siteId*
UpdateSite	사이트 arn:aws:one:*region:accountID* :site/*siteId*
UpdateSiteAddress	사이트 arn:aws:one:*region:accountID* :site/*siteId*
CreateDeviceConfigurationTemplate	디바이스 구성 템플릿 arn:aws:one:*region:accountID* :device-configuration-template/*templateId*

API 작업	리소스
DeleteDeviceConfigurationTemplate	디바이스 구성 템플릿 arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
GetDeviceConfigurationTemplate	디바이스 구성 템플릿 arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
UpdateDeviceConfigurationTemplate	디바이스 구성 템플릿 arn:aws:one:*region:accountID* :device-configuration-template/*templateId*

예를 들어, 특정 사용자에게 특정 규칙에 대해 읽기 액세스를 허용하고 쓰기 액세스를 거부할 수 있습니다.

첫 번째 정책에서는 `GetSite` 지정된 AWS Config 규칙에서와 같은 규칙 읽기 작업을 허용합니다.

두 번째 정책에서는 특정 규칙에 대한 Amazon One Enterprise 규칙 쓰기 작업을 거부합니다.

리소스 수준 권한을 사용하면 Amazon One Enterprise 규칙 API 작업에 대한 특정 작업을 수행하기 위해 읽기 액세스를 허용하고 쓰기 액세스를 거부할 수 있습니다.

추가 정보

IAM 사용자, 그룹, 정책 및 권한 생성에 대해 자세히 알아보려면 IAM 사용 설명서의 첫 IAM 사용자 및 관리자 그룹 생성과 액세스 관리 단원을 참조하세요.

AWS Amazon One Enterprise에 대한 관리형 정책

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 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

AmazonOneEnterpriseFullAccess

이 정책은 모든 Amazon One Enterprise 리소스 및 작업에 대한 액세스를 허용하는 관리 권한을 부여합니다.

one:* 모든 Amazon One Enterprise 작업을 수행할 수 있습니다.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "FullAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:*"
   ],
   "Resource": "*"
  }
 ]
}
```

AmazonOneEnterpriseReadOnlyAccess

이 정책은 모든 Amazon One Enterprise 리소스 및 작업에 읽기 전용 권한을 부여합니다.

one:Get* Amazon One Enterprise 리소스를 가져옵니다.

one:List* Amazon One Enterprise 리소스를 나열합니다.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "ReadOnlyAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:Get*",
    "one:List*"
   ],
   "Resource": "*"
  }
 ]
}
```

AmazonOneEnterpriseInstallerAccess

이 정책은 구성된 모든 디바이스 인스턴스에 대해 활성화 QR 코드를 생성하여 모든 사이트에서 디바이스를 활성화할 수 있는 제한된 읽기 및 쓰기 권한을 부여합니다.

one:CreateDeviceActivationQrCode QR 코드를 생성하여 디바이스를 활성화할 수 있습니다.

one:GetDeviceInstance Amazon One 디바이스 인스턴스에 대한 정보를 가져올 수 있습니다.

one:GetSite Amazon One Enterprise 사이트에 대한 정보를 가져올 수 있습니다.

one:GetSiteAddress Amazon One Enterprise 사이트의 물리적 주소를 가져올 수 있습니다.

one:ListDeviceInstances Amazon One 디바이스 인스턴스를 나열할 수 있습니다.

one:ListSites Amazon One Enterprise 사이트를 나열할 수 있습니다.

JSON

```
{
```

```
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "InstallerAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:CreateDeviceActivationQrCode",
    "one:GetDeviceInstance",
    "one:GetSite",
    "one:GetSiteAddress",
    "one:ListDeviceInstances",
    "one:ListSites"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 관리형 정책에 대한 Amazon One Enterprise 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 수행된 Amazon One Enterprise의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Amazon One Enterprise 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
Amazon One Enterprise에서 AmazonOneMetricPublishAccess 추가	AmazonOneMetricPublishAccess라는 역할 권한 정책은 Amazon One Enterprise가 CloudWatch 네임스페이스 AWS/AmazonOne에서 CloudWatch:PutMetricData를 수행할 수 있도록 허용합니다.	2025년 2월 6일
Amazon One Enterprise에서 변경 사항 추적 시작	Amazon One Enterprise는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2023년 12월 1일

Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키

Amazon One Enterprise(서비스 접두사: one)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

- Amazon One Enterprise에서 정의한 작업
- Amazon One Enterprise에서 정의한 리소스 유형
- Amazon One Enterprise에 사용되는 조건 키

Amazon One Enterprise에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서는 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

작업 테이블의 리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 정책이 적용되는 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 작업에 필요한 리소스가 하나 이상 있는 경우, 호출자에게 해당 리소스와 함께 작업을 사용할 수 있는 권한이 있어야 합니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. IAM 정책의 `Resource` 요소로 리소스 액세스를 제한하는 경우, 각 필수 리소스 유형에 대해 ARN 또는 패턴을 포함해야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 선택적 리소스 유형 중 하나를 사용하도록 선택할 수 있습니다.

작업 테이블의 조건 키 열에는 정책 설명의 `Condition` 요소에서 지정할 수 있는 키가 포함됩니다. 서비스의 리소스와 연결된 조건 키에 대한 자세한 내용은 리소스 유형 테이블의 조건 키 열을 참조하세요.

> **Note**
>
> 리소스 조건 키는 리소스 유형 표에 나열되어 있습니다. 작업에 적용되는 리소스 유형에 대한 링크는 리소스 유형(*필수) 작업 표의 열에서 찾을 수 있습니다. 리소스 유형 테이블의 리소스 유형에는 조건 키 열이 포함되고 이는 작업 표의 작업에 적용되는 리소스 조건 키입니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블을 참조하세요.

작업	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDeviceInstance	디바이스 인스턴스를 생성할 수 있는 권한 부여	쓰기		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	디바이스 인스턴스에 대한 정보를 가져올 수 있는 권한 부여	읽기	device-instance*		
ListDeviceInstances	디바이스 인스턴스를 나열할 수 있는 권한 부여	읽기			
UpdateDeviceInstance	디바이스 인스턴스를 업데이트할 수 있는 권한 부여	쓰기	device-instance*		
DeleteDeviceInstance	디바이스 인스턴스를 삭제할 수 있는 권한 부여	쓰기	device-instance*		
CreateDeviceActivationQrCode	디바이스 인스턴스에서 디바이스를 활성화하는 QR 코드를 생성할 수 있는 권한 부여	쓰기	device-instance*		
DeleteAssociatedDevice	디바이스와 디바이스 인스턴스 간의 연결을 삭제할 수 있는 권한 부여	쓰기	device-instance*		
RebootDevice	디바이스를 재부팅할 수 있는 권한 부여	쓰기	device-instance*		
CreateDeviceInstanceConfiguration	디바이스 인스턴스 구성을 생성할 수 있는 권한 부여	쓰기			

작업	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetDeviceInstanceConfiguration	디바이스 인스턴스 구성에 대한 정보를 가져올 수 있는 권한 부여	읽기	구성*		
CreateSite	사이트를 생성할 수 있는 권한 부여	쓰기		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	디바이스 인스턴스를 삭제할 수 있는 권한 부여	쓰기	사이트*		
GetSite	사이트에 대한 정보를 가져올 수 있는 권한 부여	읽기	사이트*		
ListSites	사이트를 나열할 수 있는 권한 부여	읽기			
GetSiteAddress	사이트 주소에 대한 정보를 가져올 수 있는 권한 부여	읽기	사이트*		
UpdateSite	사이트를 업데이트할 수 있는 권한 부여	쓰기	사이트*		
UpdateSiteAddress	사이트 주소를 업데이트할 수 있는 권한 부여	쓰기	사이트*		
CreateDeviceConfigurationTemplate	디바이스 인스턴스를 생성할 수 있는 권한 부여	쓰기		aws:RequestTag/${TagKey} aws:TagKeys	

작업	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteDeviceConfigurationTemplate	디바이스 구성 템플릿을 삭제할 수 있는 권한 부여	쓰기	device-configuration-template*		
GetDeviceConfigurationTemplate	디바이스 구성 템플릿에 대한 정보를 가져올 수 있는 권한 부여	읽기	device-configuration-template*		
ListDeviceConfigurationTemplates	디바이스 구성 템플릿을 나열할 수 있는 권한 부여	읽기			
UpdateDeviceConfigurationTemplate	디바이스 구성 템플릿을 업데이트할 수 있는 권한 부여	쓰기	device-configuration-template*		
TagResource	리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	device-instance, 사이트, device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	리소스의 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	device-instance, 사이트, device-configuration-template	aws:TagKeys	

작업	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagForResources	리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	읽기			

Amazon One Enterprise에서 정의한 리소스 유형

이 서비스에서 정의하는 리소스 유형은 다음과 같으며, IAM 권한 정책 설명의 Resource 요소에서 사용할 수 있습니다. 작업 테이블의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 조건 키를 정의할 수도 있습니다. 이러한 키는 리소스 유형 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 관한 자세한 내용은 리소스 유형 테이블을 참조하세요.

조건 키	ARN	조건 키
Device Instance	arn:aws:one: *region:accountID* :device-instance/ *deviceInstanceId*	aws:ResourceTag/${TagKey}
Device Instance Configuration	arn:aws:one: *region:accountID* :device-instance/ *deviceInstanceId* /configuration/ *version*	
Site	arn:aws:one: *region:accountID* :site/*siteId*	aws:ResourceTag/${TagKey}
Device Configuration Template	arn:aws:one: *region:accountID* :device-configuration-template/ *templateId*	aws:ResourceTag/${TagKey}

Amazon One Enterprise에 사용되는 조건 키

Amazon One Enterprise는 Condition 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 보다 상세하게 설정할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블을 참조하세요.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 사용 가능한 글로벌 조건 키를 참조하세요.

조건 키	설명	형식
aws:RequestTag/${TagKey}	요청의 태그를 기준으로 액세스를 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	요청의 태그 키를 기준으로 액세스를 필터링합니다.	ArrayOfString

Amazon One Enterprise에 대한 규정 준수 검증

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 범위 내를 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 AWS 보안 설명서를 AWS 서비스참조하세요.

Amazon One Enterprise 모니터링

모니터링은 Amazon One Enterprise 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 Amazon One Enterprise를 모니터링하고, 이상이 있을 때 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 AWS 제공합니다.

- Amazon EventBridge를 사용하여 AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge로 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.
- AWS CloudTrail는 AWS 계정에 의해 또는 계정을 대신하여 수행된 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 호출한 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Amazon EventBridge에서 Amazon One Enterprise 이벤트 모니터링

자체 애플리케이션, software-as-a-service(SaaS) 애플리케이션 및 AWS 서비스의 실시간 데이터 스트림을 제공하는 EventBridge에서 Amazon One Enterprise 이벤트를 모니터링할 수 있습니다. EventBridge는 해당 데이터를 AWS Lambda 및 Amazon Simple Notification Service와 같은 대상으로 라우팅합니다. 이러한 이벤트는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다.

Amazon One Enterprise 이벤트 구독

Amazon One 디바이스 및 사용자 프로필 상태 변경 이벤트는 EventBridge를 사용하여 게시되며 새 규칙을 생성하여 EventBridge 콘솔에서 활성화할 수 있습니다. 이벤트는 순서가 정해져 있지는 않지만 데이터를 사용할 수 있는 타임스탬프가 있습니다. 이벤트는 최상의 노력에 따라 전송됩니다.

Amazon One Enterprise 이벤트를 구독하려면

1. https://console.aws.amazon.com/events/ AWS 콘솔에 로그인합니다.
2. https://console.aws.amazon.com/events/에서 EventBridge 콘솔을 엽니다.
3. 탐색 창의 버스 아래에서 규칙을 선택합니다.
4. 규칙 생성을 선택합니다.

5. 기본 규칙 세부 정보 페이지에서 규칙에 이름을 할당합니다.
6. 이벤트 패턴이 있는 규칙을 선택한 후다음을 선택합니다.
7. 이벤트 패턴 작성 페이지의 이벤트 소스에서 AWS 이벤트 또는 EventBridge 파트너 이벤트가 선택되어 있는지 확인합니다.
8. 샘플 이벤트 유형에서 AWS 이벤트를 선택합니다.
9. 생성 방법에서 사용자 지정 패턴을 선택합니다.
10. 이벤트 패턴 섹션에서 이벤트 소스가 aws:one 및 필수 detail-type인 JSON을 추가합니다.

```
"
source": ["aws.one"],
"detail-type": ["New Successful Enrollment",
"New Successful Un-enrollment",
"Unsuccessful Enrollment",
"Unsuccessful Un-enrollment",
"Successful Recognition",
"Unsuccessful Recognition",
"New Alert(s) Detected",
"Some Alert(s) Cleared"]
}
```

위 목록에서 필수 세부 정보 유형을 선택하고 필요하지 않은 항목을 제거할 수 있습니다.

11. 다음을 선택합니다.
12. 대상 선택(Select target) 페이지에서 Lambda 함수, SQS 대기열 또는 SNS 주제가 포함된 원하는 대상을 선택합니다. 대상 구성에 대한 자세한 내용은 Amazon EventBridge 대상을 참조하세요.

    예를 들어, 누군가가 클럭인하는 시점을 보려면 “성공 인식”을 선택합니다. 그런 다음 이벤트 세부 정보(부록에 나와 있음)를 보고 누가 클럭인했는지 확인합니다.

    워크플로를 완료하려면 외부 API 또는 다른 대상을 실행할 수 있습니다.
13. 선택적으로 태그를 구성할 수 있습니다.
14. 검토 및 생성 페이지에서 규칙 생성을 선택합니다. 규칙 구성에 대한 자세한 내용은 EventBridge 사용 설명서의 EventBridge 규칙을 참조하세요. EventBridge

디바이스 상태 변경 이벤트 유형

디바이스 상태 변경 이벤트는 JSON으로 생성됩니다. 각 이벤트 유형에 대해 규칙에 구성된 대로 선택한 대상에 JSON 블롭이 전송됩니다. 다음 세부 정보 유형을 사용할 수 있습니다.

일부 알림(들) 삭제됨

디바이스가 하나 이상의 상태 확인을 통과했습니다.

새 알림(들) 감지됨

디바이스가 하나 이상의 상태 확인에 실패했습니다.

리소스

디바이스 상태 변경 이벤트가 게시된 deviceInstance arn 목록을 포함합니다.

데이터

clearedAlerts

- deviceInstance가 이전에 실패한 상태 확인을 나타냅니다.
- 알림 유형에 대한 statusCode와 reportedAt 타임스탬프로 구성됩니다.
- 가능한 statusCode 값: NetworkDisconnected, USBDisconnected

currentAlerts

- deviceInstance의 현재 상태를 나타냅니다.
- 알림 유형에 대한 statusCode와 reportedAt 타임스탬프로 구성됩니다.
- 가능한 statusCode 값: NetworkDisconnected, USBDisconnected

newAlerts

- deviceInstance의 새로 실패한 상태 확인을 나타냅니다.
- 알림 유형에 대한 statusCode와 reportedAt 타임스탬프로 구성됩니다.
- 가능한 statusCode 값: NetworkDisconnected, USBDisconnected

currentAlertsCount

- 현재 deviceInstance에서 실패한 상태 확인 수입니다.

assetTagId

- deviceInstance와 연결된 디바이스의 assetTagId입니다.

deviceInstanceName

- 디바이스 상태 이벤트가 게시된 deviceInstance의 이름입니다.

siteName

- deviceInstance가 있는 사이트의 이름입니다.

siteArn

- deviceInstance가 있는 사이트의 Arn입니다.

사용자 프로필 이벤트 유형

사용자 프로필 관련 이벤트 세부 정보 유형은 다음과 같습니다.

새로운 등록 성공

사용자가 성공적으로 등록한 경우.

새로운 등록 취소 성공

사용자가 성공적으로 등록을 취소한 경우.

등록 실패

사용자가 등록에 실패한 경우.

등록 취소 실패

사용자가 등록을 취소하지 못한 경우.

성공적인 인식

사용자가 인증을 위해 바람을 스캔하는 경우.

인식 실패

팔목 스캔 인식에 실패한 경우.

리소스

사용자 프로필 이벤트가 게시된 사용자 프로필 ARN 목록을 포함합니다.

데이터

accountId
- 요청을 시작한 디바이스의 관련 AWS 계정입니다.

requestSource
- 요청을 시작한 디바이스의 deviceInstanceId입니다.

createdTimestamp
- 이벤트가 생성되는 시간입니다.

userStatus
- 사용자의 현재 상태입니다.
- 가능한 값: ACTIVE, DELETED

associatedId
- 배지 ID와 같은 사용자의 연결된 ID입니다.

reason
- 실패한 이벤트에 대해이 값이 표시됩니다. 여기에는 이벤트가 실패한 이유가 포함되어 있습니다.

샘플 이벤트

다음 예제에서는 Amazon One Enterprise에 대한 이벤트를 보여줍니다.

주제
- 디바이스 상태가 정상으로 변경됨
- 디바이스 상태가 심각으로 변경됨
- 디바이스 연결이 온라인으로 변경됨
- 디바이스 연결이 오프라인으로 변경됨

디바이스 상태가 정상으로 변경됨

디바이스가 모든 상태 확인을 통과했습니다.

```
{
        "version": "0",
```

```
        "id": "51e022b4-7ce6-34e0-264b-370948fc1123",
        "detail-type": "Some Alert(s) Cleared",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T19:32:42Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/F5JRte5Jz21Tqx"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "clearedAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:32:42 UTC 2025"
                    }
                ],
                "currentAlerts":
                [],
                "currentAlertsCount": 0,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
      }
```


디바이스 상태가 심각으로 변경됨

디바이스가 하나 이상의 상태 확인에 실패했습니다.


```
{
        "version": "0",
        "id": "07af4893-ef9f-965a-d245-3f0c8bd3c123",
        "detail-type": "New Alert(s) Detected",
        "source": "aws.one",
        "account": "123456789012",
```

```
        "time": "2025-07-17T19:26:58Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "newAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
                    }
                ],
                "currentAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
                    }
                ],
                "currentAlertsCount": 1,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
    }
```


디바이스 연결이 온라인으로 변경됨

이제 디바이스가 인터넷에 연결되었습니다.


```
{
        "version": "0",
        "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
        "detail-type": "Some Alert(s) Cleared",
        "source": "aws.one",
```

```
        "account": "123456789012",
        "time": "2025-07-17T18:28:23Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "clearedAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlerts":
                [],
                "currentAlertsCount": 0,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
      }
```


디바이스 연결이 오프라인으로 변경됨

디바이스가 더 이상 인터넷에 연결되지 않습니다.


```
{
        "version": "0",
        "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
        "detail-type": "New Alert(s) Detected",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T18:28:23Z",
        "region": "us-east-1",
        "resources":
```

```
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "newAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlertsCount": 1,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
      }
```

를 사용하여 Amazon One Enterprise API 호출 로깅 AWS CloudTrail

Amazon One Enterprise는 Amazon One Enterprise에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Amazon One Enterprise에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Amazon One Enterprise 콘솔의 호출과 Amazon One Enterprise API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Amazon One Enterprise에 대한 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. Amazon S3 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Amazon One Enterprise에

수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Amazon One Enterprise 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. Amazon One Enterprise에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Amazon One Enterprise에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Amazon One Enterprise 작업은 CloudTrail에서 로깅되며에 문서화됩니다Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키. 예를 들어 `ListSites`, `RebootDevice`, `DeleteDeviceInstance` 작업을 직접 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Amazon One Enterprise 로그 파일 항목 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 `CreateSite` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예시입니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAKDBGOAT6C2EXAMPLE:J_DOE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_DOE",
        "accountId": "123456789012",
        "accessKeyId": "AKIALAVPULGA71EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAKDBGOAT6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-11T06:28:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-11T07:19:09Z",
    "eventSource": "one.amazonaws.com",
    "eventName": "CreateSite",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "name": "***",
        "description": "***",
        "address": {
            "addressLine1": "***",
```

```
            "addressLine2": "***",
            "addressLine3": "***",
            "city": "EXAMPLE_CITY",
            "postalCode": "12345",
            "countryCode": "EXAMPLE_COUNTRY",
            "stateOrRegion": "EXAMPLE_STATE"
        },
        "clientToken": "abc12d34-567e-8910-1112-12fghi0jk13l"
    },
    "responseElements": {
        "stateOrRegion": "EXAMPLE_STATE",
        "createdAtInMillis": 1697008749263,
        "city": "EXAMPLE_CITY",
        "countryCode": "EXAMPLE_COUNTRY",
        "deviceInstanceCount": 0,
        "postalCode": "12345",
        "name": "***",
        "description": "***",
        "siteId": " abCdefG12hijkL",
        "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkL",
        "tags": "***"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Amazon One 문제 해결

Amazon One Application 또는 Amazon One 디바이스 중 하나에 문제가 있는 경우 다음 제안을 사용하여 문제를 해결합니다. 그런 다음 여전히 문제가 있는 경우 AWS Support에 문의하세요.

주제

- Amazon One 자격 증명 및 액세스 문제 해결
- Amazon One 콘솔 문제 해결
- Amazon One 디바이스 문제 해결

Amazon One 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Amazon One Enterprise 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- Amazon One에서 작업을 수행할 권한이 없음
- 내 외부의 사람이 내 Amazon One 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

Amazon One에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `one:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 one:GetWidget on resource: my-example-widget
```

이 경우, `one:`*`GetWidget`* 작업을 사용하여 *`my-example-widget`* 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Amazon One 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Amazon One Enterprise가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요Amazon One Enterprise와 IAM의 작동 방식.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Amazon One 콘솔 문제 해결

Amazon One Application 또는 Amazon One 디바이스 중 하나에 문제가 있는 경우 다음 제안을 사용하여 문제를 해결합니다. 그런 다음 여전히 문제가 있는 경우 AWS Support에 문의하세요.

주제

사이트를 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공하세요.

- 문제가 지속되면 AWS Support에 문의하십시오.

디바이스 인스턴스를 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공하세요.
- 문제가 지속되면 AWS Support에 문의하십시오.

구성 템플릿을 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공하세요.
- 문제가 지속되면 AWS Support에 문의하십시오.

활성화 QR 코드를 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공하세요.
- 문제가 지속되면 AWS Support에 문의하십시오.

Amazon One 디바이스 문제 해결

Amazon One Console 또는 Amazon One 디바이스 중 하나에 문제가 있는 경우 다음 제안을 사용하여 문제를 해결합니다. 그런 다음 여전히 문제가 있는 경우 AWS Support에 문의하세요.

주제

- 게이트웨이 제한 시간 초과
- 디바이스를 구성할 수 없음
- 오류 메시지 및 오류 코드와 함께 디바이스가 다시 시작됨
- 추가 활동이 없는 디바이스 화면의 Amazon 로고
- 일시적으로 사용할 수 없음
- 문제가 발생했습니다.
- 일시적으로 서비스 중단
- Amazon One 디바이스에 물리적 손상이 있음
- 야자수를 읽을 수 없음
- 팜이 인식되지 않음
- 장기 비활성으로 인해 디바이스가 잠김
- 변조 이벤트로 인해 디바이스가 잠김

빈 화면

이는 디바이스에 전원이 공급되지 않거나 재부팅 중에 멈출 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 디바이스가 재부팅되는 경우 잠시(30초 미만) 기다립니다.
- 디바이스가 비어 있는 동안 조명 링이 깜박이는 경우 최대 30초 동안 기다립니다.
- 전원 코드가 전원 콘센트와 Amazon One 디바이스 후면에 제대로 연결되어 있는지 확인합니다. 또한 코드가 손상되지 않았는지 확인합니다.
- 전원을 확인합니다.
- 모든 케이블이 Amazon One 및 USB 허브에 올바르게 연결되어 있는지 확인합니다.
- 콘솔에서 디바이스를 재부팅합니다.
- 디바이스를 재부팅해도 문제가 해결되지 않으면 전원 공급 장치에서 Amazon One USB 허브를 뽑은 다음 다시 연결합니다.
- 문제가 지속되면 AWS Support에 문의하십시오.

Wi-Fi 또는 네트워크에 연결할 수 없음

이는 디바이스 연결이 끊어질 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- Wi-Fi에 연결된 경우 다른 디바이스를 사용하여 사용 가능한 네트워크에 Wi-Fi가 표시되는지 확인합니다.
- Wi-Fi 라우터가 켜져 있고 범위 내에 있는지 확인합니다.
- 네트워크가 복구되면 디바이스가 다시 연결됩니다.
- 문제가 지속되면 AWS 지원팀에 문의하십시오.

활성 알림으로 디바이스 재부팅

콘솔에서 재부팅을 요청하면 디바이스가 명령을 수신하고 오프라인 상태이거나 네트워크 문제가 발생하더라도 재부팅을 시도할 때까지 작업이 최대 15분 동안 대기합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 재부팅이 완료될 때까지 기다립니다.
- 문제가 지속되면 AWS 지원팀에 문의하십시오.

시스템 오류

이는 내부 오류로 인해 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 화면에서 다시 시작을 선택하여 애플리케이션을 다시 시작합니다.
- 2번 시도한 후 문제가 해결되지 않으면 AWS Support에 문의하십시오.

QR 코드가 인식되지 않음

이는 승인되지 않은 QR 코드 또는 만료된 QR 코드로 인해 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 다시 시도를 선택하여 QR 코드 화면으로 돌아갑니다.
- AWS 콘솔에서 새 QR 코드를 생성한 다음 유효한 QR 코드를 스캔합니다.

QR 코드를 읽을 수 없음

이는 애플리케이션이 QR 코드를 읽을 수 없을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 다시 시도를 선택하여 QR 코드 화면으로 돌아갑니다.
- 문제가 지속되면 활성화 워크플로를 취소하고 다시 시작합니다.

여러 QR 코드가 감지됨

이는 여러 QR 코드가 스캔될 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 다시 시도를 선택하여 QR 코드 화면으로 돌아갑니다.
- 한 번에 하나의 유효한 QR 코드만 스캔합니다.

디바이스 인스턴스가 존재하지 않음

이는 디바이스 인스턴스가 삭제되거나 AWS 콘솔에 존재하지 않을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 다시 시도를 선택하여 QR 코드 화면으로 돌아갑니다.
- AWS 콘솔에서 올바른 디바이스 인스턴스를 확인합니다. 디바이스 인스턴스가 누락된 경우 관리자에게 문의하세요.
- 해당 디바이스 인스턴스에 대한 새 QR 코드를 생성한 다음 새 QR 코드를 스캔합니다.

사이트를 찾을 수 없음

이는 사이트가 삭제되거나 AWS 콘솔에 존재하지 않을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- AWS 콘솔에서 사이트 정보를 확인합니다. 사이트가 없는 경우 관리자에게 문의하세요.

우편 번호가 일치하지 않습니다.

이는 디바이스에 대해 구성된 것과 다른 우편번호를 입력할 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 다시 시도를 선택하여 우편 번호 화면으로 돌아갑니다.
- 올바른 사이트 우편번호가 있는지 확인합니다.
- 문제가 지속되면 관리자에게 문의하여 AWS 콘솔에서 사이트 ZIP 코드를 확인하세요.

게이트웨이 제한 시간 초과

이는 지정된 시간 내에 게이트웨이의 응답이 없을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 재시작을 선택하여 애플리케이션을 다시 시작합니다.
- 두 번 시도한 후 문제가 해결되지 않으면 AWS Support에 문의하십시오.

디바이스를 구성할 수 없음

이는 작업이 디바이스 디스크에 구성을 저장하지 못한 경우에 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 재시작을 선택하여 애플리케이션을 다시 시작합니다.
- 두 번 시도한 후 문제가 해결되지 않으면 AWS Support에 문의하십시오.

오류 메시지 및 오류 코드와 함께 디바이스가 다시 시작됨

이 문제를 해결하려면 다음을 수행합니다.

- 재시작을 선택하고 디바이스가 복구되도록 합니다.
- 디바이스가 복구되지 않으면 전원 공급 장치에서 USB 허브를 뽑았다가 다시 연결합니다.
- 문제가 지속되면 AWS Support에 문의하십시오.

추가 활동이 없는 디바이스 화면의 Amazon 로고

이 문제를 해결하려면 다음을 수행합니다.

- 디바이스가 재부팅되는 경우 잠시(30초 미만) 기다립니다.
- 전원 공급 장치에서 USB 허브를 뽑았다가 다시 연결합니다.
- 문제가 지속되면 AWS Support에 문의하십시오.

일시적으로 사용할 수 없음

이 문제를 해결하려면 다음을 수행합니다.

- 호스트 디바이스/시스템과의 USB 연결이 안전한지 확인합니다.
- USB 허브로 연결되는 모든 케이블을 분리하고 다시 연결합니다.
- 문제가 지속되면 AWS Support에 문의하십시오.

문제가 발생했습니다.

이는 내부 오류가 있을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

1. 디바이스를 종료합니다.
2. 전원 공급 장치에서 분리합니다.
3. 30초 동안 기다립니다.
4. 디바이스를 전원에 다시 연결합니다.
5. 디바이스의 전원을 켭니다.
6. 문제가 지속되면 AWS Support에 문의하십시오.

일시적으로 서비스 중단

이는 Amazon One에서 디바이스를 서비스 중단 상태로 이동했을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- AWS Support에 연락하십시오.

Amazon One 디바이스에 물리적 손상이 있음

이 문제를 해결하려면 다음을 수행합니다.

- 다음 단계는 AWS Support에 문의하고 발생한 일, 발생한 시간, 발생한 이유와 같은 세부 정보를 최대한 많이 제공하세요.

야자수를 읽을 수 없음

이 문제를 해결하려면 다음을 수행합니다.

- Amazon One 디바이스에 줄무늬와 스머지가 없는지 다시 확인합니다.
- 고객의 팔목에 붕대, 소매 및 심각한 먼지/오일과 같은 오클루전이 없는지 확인합니다.
- 문제가 지속되고 디바이스가 아무것도 읽지 않는 경우 AWS Support에 문의하세요.

팜이 인식되지 않음

이 문제를 해결하려면 다음을 수행합니다.

- 고객이 다른 휴대폰을 사용해 보도록 합니다.
- 고객이 이미 등록되어 있는지 확인합니다. 그렇지 않은 경우 온라인 또는 디바이스에 등록하도록 합니다.
- 문제가 지속되고 디바이스가 아무것도 읽지 않는 경우 AWS Support에 문의하세요.

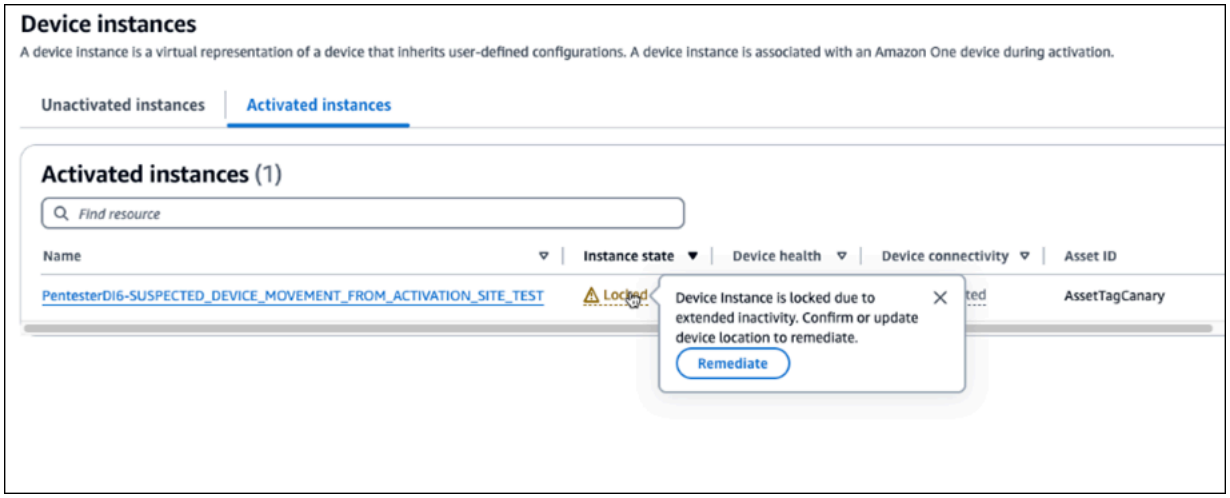
장기 비활성으로 인해 디바이스가 잠김

디바이스가 활성화 사이트에서 이동한 것으로 의심되면 사용자를 잠급니다. 이는 디바이스가 최대 120시간의 오프라인 시간을 초과할 때 발생합니다.

다음을 수행하여 디바이스를 잠금 해제합니다.

1. AWS 콘솔에 로그인하고 디바이스 인스턴스를 선택합니다.
2. 페이지 상단의 오류 배너에서 문제 해결을 선택합니다.

   선택 사항: 활성화된 인스턴스에서 잠김을 선택하고 수정을 선택합니다.



3. 디바이스가 여전히 원래 활성화 사이트에 있는 경우 예를 선택합니다. 디바이스는이 사이트에 있습니다.
4. 디바이스가 다른 사이트에 있는 경우 아니요, 디바이스가 다른 사이트에 있는 경우를 선택합니다. 아니요를 선택하면 디바이스가 비활성화됩니다. 새 사이트에서 디바이스를 활성화합니다.

변조 이벤트로 인해 디바이스가 잠김

보안상의 이유로 변조 이벤트가 발생할 경우 Amazon One 디바이스가 잠깁니다.

이 문제를 해결하려면 다음을 수행합니다.

- AWS Support에 연락하십시오.

Amazon One Enterprise 사용 설명서의 문서 기록

다음 표에서는 Amazon One Enterprise의 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
업데이트	서비스 연결 역할 섹션 추가	2025년 2월 4일
업데이트	추가됨: 시나리오 기반 콘텐츠	2024년 10월 10일
업데이트	주제 추가: Amazon One Enterprise 콘솔 문제 해결	2024년 10월 10일
업데이트	주제 추가: Amazon One Enterprise 디바이스 문제 해결	2024년 10월 10일
업데이트	추가된 장: Amazon One Enterprise 설정	2024년 10월 10일
업데이트	주제 추가: Amazon One Enterprise 디바이스 유지 관리 및 정리	2024년 10월 10일
업데이트	재구성된 콘텐츠	2024년 10월 10일
업데이트	주제 추가: 보안 액세스를 위한 Amazon One Enterprise 디바이스 I/O Hub 설치	2024년 8월 14일
업데이트	주제 추가: 벽면 장착 가능한 Amazon One Enterprise 디바이스 설치	2024년 6월 5일
최초 릴리스	Amazon One Enterprise 사용 설명서의 최초 릴리스	2023년 11월 27일

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