aws

사용자 가이드

Amazon One Enterprise

Amazon One Enterprise: 사용자 가이드

Table of Contents

아마존 원 엔터프라이즈란 무엇입니까?

Amazon One Enterprise는 직원이 배지나 암호를 사용하지 않고도 건물과 기업 자산에 안전하게 액세스할 수 있도록 하는 새로운 팜 기반 인증 서비스입니다. PINs

주제

아마존 원 디바이스

Amazon One 디바이스는 엔터프라이즈 액세스 제어를 위한 안전한 팜 기반 ID 서비스인 Amazon One Enterprise용으로 설계되었습니다. 다음 디바이스 사양을 참고하십시오.

- 사용자 입력 — 팜 생체인식, QR 코드 매칭
- 호스트 인터페이스 — Wi-Fi (2.4 GHz 및 5GHz), 이더넷, A형 2개, USB B형 1개 USB
- 사용자 피드백 — 5.5인치 터치스크린, 라이트링, 스피커, 헤드폰
- 물리적 액세스 제어 프로토콜 — 및 Wiegand OSDP
- 전원 공급 장치 —POE, 110/220 VAC 입력 AC-DC 어댑터 제공, 30W @ 15V
- 보안 — 탬퍼 스위치
- 크기 (HxWxD 밀리미터) — 86 x 85 x 256

아마존 원 엔터프라이즈 콘솔

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

- IT 또는 시설 관리자는 Amazon One Enterprise를 사용하여 사이트를 만들고 관리합니다. 이 사이트는 팀이 Amazon One Enterprise 디바이스 및 사용자 프로필을 모니터링하고 관리하면서 수행하는 작업을 수행할 수 있는 물리적 위치와 비슷합니다. IT 또는 시설 관리자 작업에는 다음이 포함됩니다.
  - 물리적 위치에 있는 모든 Amazon One 디바이스 인스턴스를 포함하는 사이트 생성
  - 사이트를 관리할 관리자 사용자와 활성화 QR 코드에 액세스할 설치 사용자 추가
- 관리자는 Amazon One Enterprise를 사용하여 디바이스 인스턴스를 생성하고 Amazon One 디바이스를 관리합니다. 관리 작업에는 다음이 포함됩니다.
  - 사이트에서 기기 인스턴스 만들기

  - 장치 인스턴스에 적용할 구성 템플릿 만들기
  - 장치 상태 모니터링 및 장치 구성 업데이트
  - 사용자 등록 취소

- 설치자는 Amazon One Enterprise를 사용하여 활성화 QR 코드에 액세스하여 디바이스를 활성화합니다. 설치 작업에는 다음이 포함됩니다.
  - 콘솔에서 활성화 QR 코드에 액세스하기
  - 활성화할 장치 인스턴스에 해당하는 QR 코드 선택
  - Amazon One 디바이스가 설치된 상태에서 선택한 QR 코드를 스캔합니다.

아마존 원 디바이스 구매

Amazon One Enterprise에 대해 자세히 알아보려면 당사로 문의해 주십시오. 그러면 비즈니스 개발 팀 원이 연락하여 가격을 비롯한 당사 제품에 대한 자세한 내용을 공유하고 궁금한 사항에 답변해 드립니다.

아마존 원 엔터프라이즈 요금

Amazon One Enterprise 요금에 대해 자세히 알아보려면 당사에 문의하십시오.

Amazon One Enterprise 작동 방식

Amazon One Enterprise는 Amazon One 디바이스를 사용하여 사용자의 손바닥 생체 인식으로 사용자를 인증하는 클라우드 기반 생체 인식 서비스입니다. 당사에 문의하여 Amazon One 디바이스를 주문할 수 있으며에서 Amazon One Enterprise 보안 액세스 서비스에 가입할 수 있습니다 AWS Management Console.

Amazon One Enterprise를 설치한 후 Amazon One Enterprise 콘솔 및 인증 애플리케이션에서 디바이스를 활성화하고 AWS 계정 에 등록할 수 있습니다. 등록된 직원의 생체인식 프로필을 보고 필요한 경우 등록을 취소할 수 있습니다. 직원이 회사를 떠나거나 배지를 분실하면 생체 인식 데이터를 쉽게 삭제할 수 있습니다.

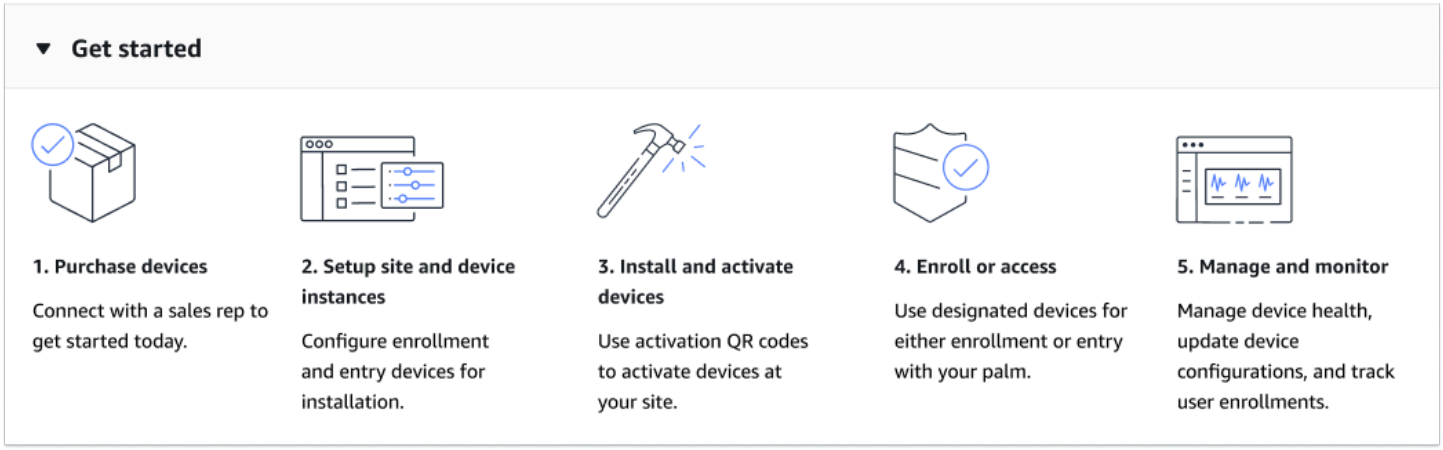
Amazon One Enterprise 콘솔은 설치된 디바이스 추적 및 월별 청구서 보기와 같은 운영 활동을 관리하기 위한 중앙 집중식 허브 역할을 합니다. 직원은 현장의 감독 등록 스테이션에서 배지와 손바닥을 스캔하여 등록할 수 있습니다. 등록이 완료되면 직원은 Amazon One 디바이스 위로 손바닥을 가져가 보안 위치를 원활하게 출입할 수 있습니다.

주제

- Amazon One Enterprise 워크플로
- Amazon One Enterprise 키 용어

Amazon One Enterprise 워크플로

다음 다이어그램은 Amazon One Enterprise의 기본 워크플로를 보여줍니다.



1. 당사에 문의하여 Amazon One 디바이스를 구매합니다.
2. 사이트 및 디바이스 인스턴스를 생성하고, 등록을 구성하고, 설치를 위해 디바이스를 입력합니다.

3. 설치 후 디바이스 인스턴스와 관련된 보안 QR 코드를 스캔하여 Amazon One 디바이스를 활성화합니다.
4. 직원에게 손바닥을 등록한 다음 손바닥으로 인증하여 액세스하도록 요청합니다.
5. 관리 및 모니터링 기능을 활용합니다. 디바이스 상태를 확인하고, 구성을 최신 상태로 유지하고, 포괄적인 감독을 위해 사용자 등록을 추적합니다.

Amazon One Enterprise 키 용어

다음은 Amazon One Enterprise의 주요 용어입니다.

- 사이트 - 고객이 Amazon One Enterprise 디바이스를 설치하는 고객 관리형 물리적 건물입니다. 사이트는 Amazon One Enterprise 디바이스의 시설, 네트워킹 및 전원 요구 사항을 충족해야 합니다.
- 디바이스 - 인증을 위해 생체 인식 디바이스를 스캔하는 Amazon One Enterprise 야자수입니다.
- 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 집합입니다.

Amazon One Enterprise 설정

이 장에서는 Amazon One Enterprise를 시작하기 위한 기본 단계를 설명합니다.

사이트, 디바이스 인스턴스 및 구성 템플릿 설정 - 다음 단계에 따라 Amazon One 디바이스를 수용할 물리적 위치를 추가하기 위한 프레임워크를 생성한 다음 Amazon One Enterprise 콘솔을 사용하여 해당 위치를 구성하고 관리합니다. 사이트, 디바이스 인스턴스 및 구성 템플릿의 수에 따라 이 프로세스는 가끔만 또는 한 번만 사용합니다.

주제

AWS 계정에 가입

AWS 계정이 없는 경우 다음 단계를 완료하여 계정을 생성합니다.

AWS 계정에 가입하려면

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 사용자는 계정의 모든 AWS 서비스 및 리소스에 액세스할 수 있습니다. 보안 모범 사례로 사용자에게 관리 액세스 권한을 할당하고 루트 사용자 액세스가 필요한 작업을 수행하는 데 루트 사용자만 사용합니다.

AWS 는 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 활성화한 다음 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

주제

AWS 계정 보안

이제 Amazon One Enterprise 계정에 로그인했으므로 계정을 보호하세요.

AWS 계정 루트 사용자를 보호하려면

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

   루트 사용자를 사용하여 로그인하는 방법에 대한 자세한 내용은 로그인 사용 설명서의 루트 사용자로 AWS 로그인을 참조하세요.
3. 루트 사용자에 대해 다중 인증(MFA)을 켭니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

이제 Amazon One Enterprise 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 전송URL된 로그인을 사용하여 IAM Identity Center 사용자로 로그인합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 방법에 대한 자세한 내용은 로그인 사용 설명서의 AWS 액세스 포털에 AWS 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 Enterprise 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 Enterprise 콘솔에 액세스하는 설치 관리자일 수 있습니다.

Amazon One Enterprise 사용자를 추가하려면

1. AWS AWS 로그인 사용 설명서의 에 로그인하는 방법에 설명된 대로 사용자 유형에 적합한 로그인 절차를 따릅니다.
2. 탐색 창에서 사용자 를 선택한 다음 사용자 추가 를 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 할당량 섹션을 참조하세요. 사용자 이름은 최대 64자의 문자, 숫자 및 더하기(+), 같음(=), 쉼표(,), 마침표(.), 시그니쳐(@), 밑줄(_), 하이픈(-) 문자를 조합하여 사용할 수 있습니다. 이름은 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어 TESTUSER 및 테스트 사용자 라는 두 사용자를 생성할 수 없습니다. 정책에서 또는 의 일부로 사용자 이름을 사용하는 경우 ARN이름은 대/소문자를 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 사항 을 선택합니다.
5. IAM 사용자를 생성하려는 경우 를 선택합니다.
6. 콘솔 암호의 경우 다음 중 하나를 선택합니다.

   - 자동 생성된 암호 - 사용자에게 계정 암호 정책 을 충족하는 무작위로 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. 에서 태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 지정을 IAM참조하세요. IAM
13. 이 시점까지 수행한 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 보안 인증을 안전한 위치에 저장할 수 있는 .csv 파일로 다운로드합니다.
15. 이메일 로그인 지침을 선택합니다. 로컬 메일 클라이언트는 사용자 지정을 거쳐 사용자에게 발송할 수 있는 초안 형태로 열립니다. 이메일 템플릿에는 각 사용자에 대한 다음과 같은 세부 정보가 포함되어 있습니다.
    - 사용자 이름
    - URL 계정 로그인 페이지로 이동합니다. 다음 예를 사용하여 정확한 계정 ID 번호 또는 계정 별칭으로 대치합니다.

```
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

이제 에 로그인했으므로 Amazon One Enterprise 콘솔을 사용하여 사이트를 생성할 AWS Management Console수 있습니다.

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

사이트를 생성하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/one-enterprise 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 개요로 이동을 선택합니다.
3. 탐색 창에서 사이트를 선택합니다.
4. 사이트 생성을 선택합니다.
5. 사이트 정보 의 사이트 이름 에 사이트의 이름을 입력합니다.
6. 물리적 주소 에서 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 전에 이 태그를 제거하려면 제거를 선택합니다.
8. 사이트 생성을 선택하여 사이트를 생성합니다.

디바이스 인스턴스 생성

이제 AWS 관리 콘솔에서 사이트를 생성했으므로 Amazon One Enterprise 콘솔을 사용하여 디바이스 인스턴스를 생성할 수 있습니다.

디바이스 인스턴스를 생성하려면

1. https://console.aws.amazon.com/one-enterprise에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스 를 선택합니다. 비활성화된 인스턴스 탭에 있는지 확인합니다.
3. 인스턴스 세부 정보 에서 사이트 드롭다운에서 사이트를 선택하거나 사이트 생성 버튼을 선택하여 새 사이트를 생성합니다.
4. 각 개별 디바이스 인스턴스 이름 을 수동으로 입력합니다.

5. (선택 사항) 디바이스 인스턴스에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 디바이스 인스턴스를 생성하기 전에 이 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 Enterprise 콘솔을 사용하여 구성 템플릿을 생성할 수 있습니다.

구성 템플릿을 생성하려면

1. https://console.aws.amazon.com/one-enterprise에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 구성 템플릿 을 선택합니다.
3. 템플릿 생성을 선택합니다.
4. 템플릿 정보 의 템플릿 이름 에 구성 템플릿의 이름을 입력합니다.
5. 디바이스 구성에서 작업 모드 를 선택합니다.

   To configure Enrollment operating mode

   1. (선택 사항) Wifi 구성에서 Wifi 보안 인증 정보 를 제공합니다.
   2. (선택 사항) 사이트에 태그를 추가하려면 태그 아래에 키-값 페어를 입력한 다음 새 태그 추가를 선택합니다. 사이트를 생성하기 전에 이 태그를 제거하려면 제거를 선택합니다.
   3. 구성을 선택합니다.

   To configure Entry operating mode

   1. 제어판 설정 에서 Amazon One 디바이스가 제어판과 통신할 수 있도록 통신 설정을 제공합니다.
   2. 배지 형식 설정 에서 회사 배지 형식의 레이아웃을 지정하는 구성 설정을 제공합니다.
   3. (선택 사항) Wifi 구성 에서 Wifi 보안 인증 정보 를 제공합니다.

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

> **Important**
>
> 보안 액세스를 위해 Amazon One Enterprise의 전체 기능을 활성화하려면 하나 이상의 등록 디바이스와 하나의 항목 디바이스를 구성해야 합니다.

활성화를 위한 디바이스 인스턴스 구성

디바이스 인스턴스가 생성된 후에는 이전에 생성된 구성 템플릿(참조구성 템플릿 생성)으로 디바이스 인스턴스를 구성하거나 구성을 수동으로 추가할 수 있습니다.

활성화를 위해 디바이스 인스턴스를 구성하려면

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

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

      템플릿 생성 옵션은 섹션을 참조하세요구성 템플릿 생성.

   b. 수동 입력 옵션에서 작동 모드 를 선택합니다.

      To configure Enrollment operating mode

      a. (선택 사항) Wifi 구성 에서 Wifi 자격 증명 을 제공합니다.

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

      c. 구성을 선택합니다.

To configure Entry operating mode

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

6. 비활성화된 인스턴스 테이블 아래에 인스턴스 상태가 를 표시해야 합니다 

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

> **Important**
>
> 보안 액세스를 위해 Amazon One Enterprise의 전체 기능을 활성화하려면 하나 이상의 등록 디바이스와 하나의 항목 디바이스를 구성해야 합니다.

Amazon One 설치 및 활성화

Amazon One Enterprise 콘솔을 설정한 후 다음 단계는 사이트에 Amazon One Enterprise 디바이스를 설치한 다음 활성화하는 것입니다.

> **Note**
>
> 이 섹션에서는 설치에 중점을 두고 모바일 브라우저를 사용하여 에 액세스 AWS Management Console 하여 디바이스 활성화 QR 코드를 가져옵니다.

주제

요구 사항 이해

Amazon One 디바이스는 전기적으로 제어할 수 있는 문이 있는 모든 기업 또는 비즈니스 위치에 설치할 수 있습니다.

제어판 요구 사항

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

- OSDP (v1 및 v2)
- Wiegand

네트워크 요구 사항

Amazon One 디바이스는 정상 작동을 위해 항상 인터넷에 연결해야 합니다. 인터넷 연결은 유선 이더넷 또는 Wi-Fi를 통해 제공할 수 있습니다. 최소 필수 대역폭은 10Mbps입니다.

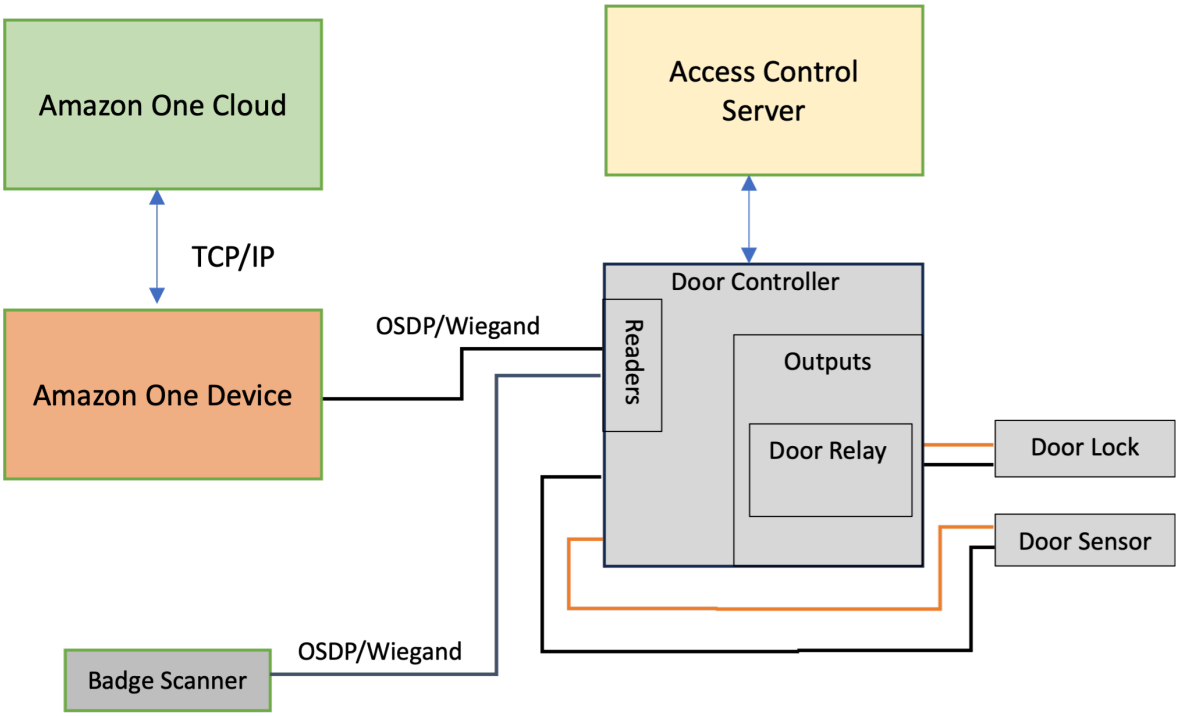
전원 요구 사항

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

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

설치 개념 이해

건물 액세스를 적절하게 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 손바닥 인식 디바이스입니다.

- 액세스 제어 서버: 이 구성 요소는 일반적으로 보안 영역에 대한 사용자의 액세스 권한을 제어합니다. 영역에 액세스할 수 있는 IDs 개인의 배지는 일반적으로 이 서버에 저장됩니다. 이 서버는 적절한 문 컨트롤러IDs와 관련된 를 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 디바이스는 사용자의 배지 ID를 도어 컨트롤러로 전송합니다.
  - 도어 컨트롤러는 결정에 응답하며, 그러면 Amazon One 디바이스가 액세스 권한 부여됨 또는 액세스 거부됨 메시지를 표시할 수 있습니다.
- 배지 스캐너: 배지 스캐너는 일반적으로 RFID 배지를 스캔하고 배지 번호를 Access Control Server로 전송하는 데 사용됩니다. Amazon One Enterprise를 사용하면 배지 스캐너가 등록 Amazon One 디바이스에 연결되어 직원의 배지를 스캔하고 손바닥 프로파일과 연결할 수 있습니다.

Amazon One Enterprise 받침대 설치

이 섹션에서는 Amazon One Enterprise 받침대를 설치하는 데 필요한 위치 요구 사항과 단계를 간략하게 설명합니다.

설치를 시작하기 전에 다음 사전 조건이 충족되는지 확인합니다.

- POE+를 사용하여 디바이스에 전원을 공급하는 경우 Cat6 케이블이 배치되어 있고 POE+ 인젝터 또는 스위치를 사용할 수 있는지 확인합니다.
- AC 전원(120V) 소스를 사용하는 경우 AOE 받침대에서 20피트 이내에 AC 콘센트를 사용할 수 있어야 합니다.
- 바닥은 평평하고 깨끗해야 합니다.
- 받침대가 문이나 차선을 막아서는 안 됩니다.
- 모든 초과 케이블은 받침대 내부에 보관하고 고정해야 합니다.

Amazon One 디바이스 받침대를 설치하려면

1. 패키징에서 Amazon One Enterprise 받침대를 제거합니다.
2. 두 M4 부정조작 방지 나사를 모두 풀어 도어를 제거합니다.
3. 전원 케이블을 연결합니다. 받침대 베이스 플레이트의 구멍을 통해 케이블을 배선합니다.
4. 받침대 내부에 여분의 전원 케이블을 감습니다.
5. 이더넷 케이블(Cat5E 이상)을 받침대의 하단 플레이트를 통해 라우팅하고 이더넷 포트에 연결합니다.
6. 이더넷 케이블(Cat5E 이상)을 받침대의 하단 플레이트를 통해 라우팅하고 이더넷 포트에 연결합니다.
7. 페디스탈 베이스 위 2인치에 이더넷 케이블에 페라이트 루프를 설치합니다.
8. RS485 직렬 케이블을 액세스 제어판(또는 배지 리더)에서 받침대로 1피트 초과 길이로 공급합니다.
9. 페디스탈 바닥에서 2인치 위에 있는 RS485 케이블에 페라이트 루프를 설치합니다.
10. 콘센트에 전원을 연결하고 Amazon One 디바이스가 켜져 있는지 확인합니다.
11. 도어를 받침대에 다시 연결하고 M4 변조 방지 나사 2개를 다시 조여 고정합니다.

벽면 장착형 Amazon One 디바이스 설치

이 섹션에서는 벽 장착형 Amazon One 디바이스를 설치하는 데 필요한 위치 요구 사항과 단계를 자세히 설명합니다.

설치를 시작하기 전에 다음을 확인합니다.

- 벽면 탑재형 Amazon One 디바이스는 실내 전용입니다.
- 벽은 수평입니다.
- 벽면 마운트의 상단은 탑재 후 지면에서 44~46'보다 크지 않아야 합니다.
- 모든 초과 케이블은 벽걸이 마운트 뒤에 있고 고정되어 있습니다.
- Power Over Ethernet(PoE ++)의 경우:

  802.3bt(유형 3) 클래스 IEEE 6 POE++ 스위치(엔드 스팬) 또는 인젝터(미드스팬)를 사용할 수 있는지 확인합니다. 이 스위치는 등록 또는 인증되었으며 IEC 62368-1을 준수합니다.

  승인된 PoE ++ 소스에서만 AOE를 사용합니다.

PoE ++ 소스는 동일한 건물 내에 있어야 합니다.

- 15V DC 전원 입력의 경우 NEC 클래스 2 또는 등록되거나 인증된 제한된 전원 공급 장치와 함께 Amazon One 디바이스만 사용해야 합니다.

필수 도구:

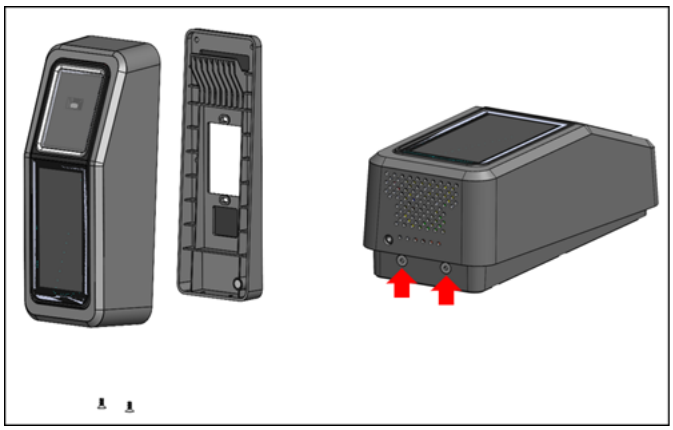
- 벽 앵커가 필요한 경우 1/4” 건식 벽 또는 석조 드릴 비트
- 와이어 스트리퍼
- 파일럿 홀 드릴링을 위한 7/64인치 드릴 비트
- #2 Phillips 드라이버
- 0.5mm x 2mm 일자 드라이버
- T12 보안 Torx 드라이버
- 연필
- 수준

벽면 탑재형 Amazon One 디바이스에 포함됨:

- 6x #8 드라이월 앵커
- 6x #8-32 1인치 긴 나사
- #6-32 1in 기계 나사 2개
- 2x 6 위치 터미널 블록 커넥터
- Torx Security M4x10 플랫헤드 나사 2개

Amazon One 디바이스에 벽 장착 플레이트를 설치하려면

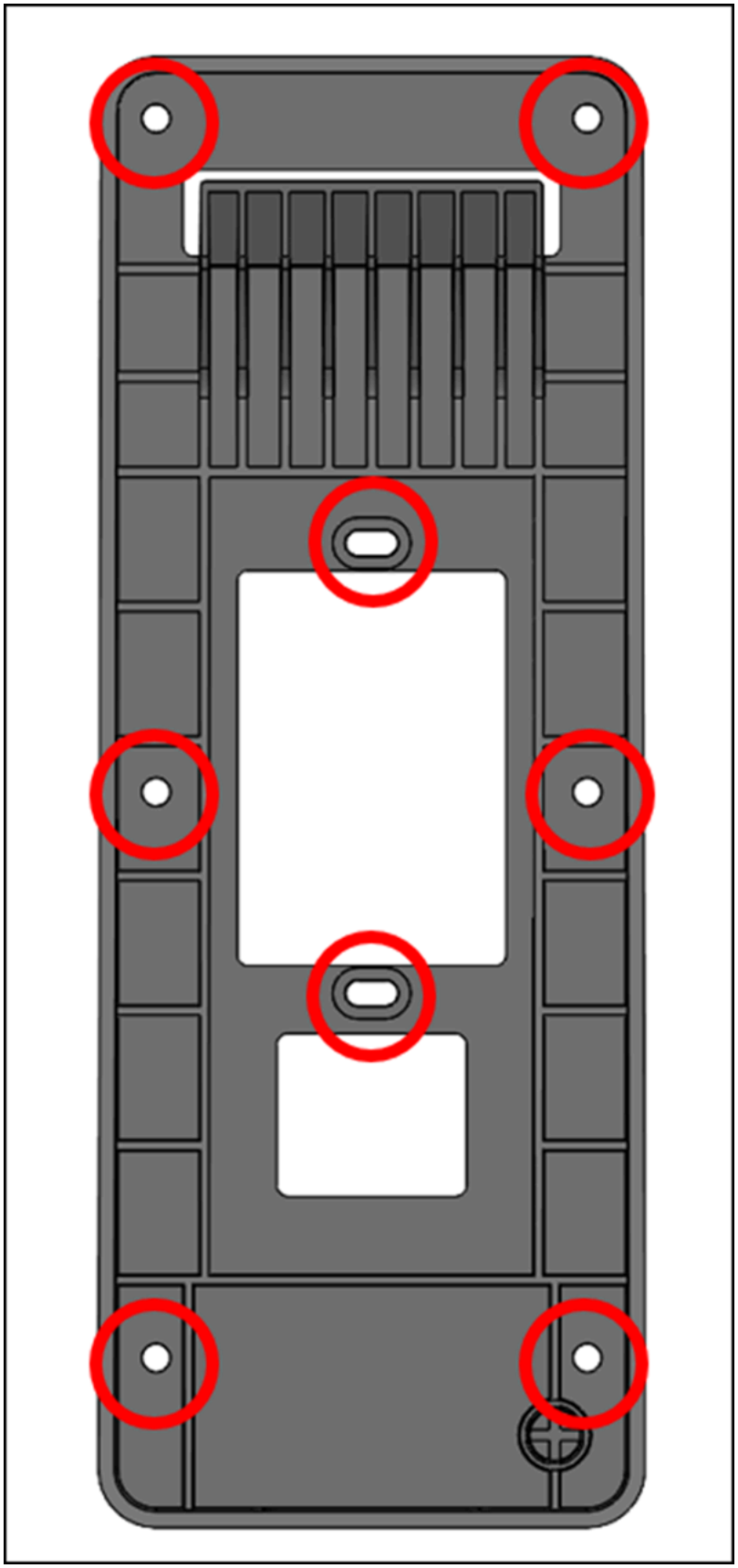
1. 패키징에서 Amazon One 디바이스를 제거합니다.
2. 두 개의 하단 Torx 보안 나사를 제거하여 Amazon One 디바이스에서 탑재 플레이트를 분리합니다.



3. 원하는 위치의 벽에 장착 플레이트를 배치합니다. 브래킷을 템플릿으로 사용하여 다음 이미지와 같이 외부 6개의 나사 구멍을 표시합니다.

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

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



4. 스터코, 드라이월, 벽돌 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 탑재하는 경우 앵커는 필요하지 않으며 표시된 위치에는 7/64” 파일럿 구멍만 필요합니다.

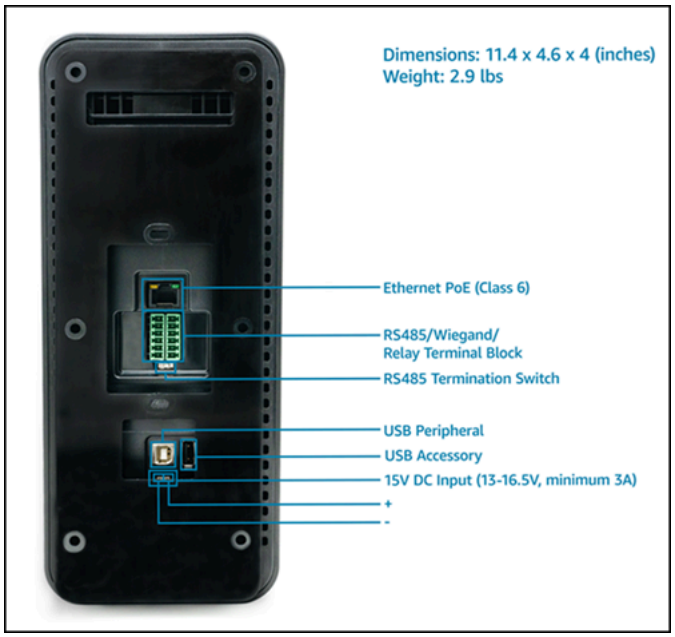
5. 앵커 위치의 #8 나무 나사를 사용하여 벽판을 벽에 느슨하게 고정합니다.
6. 모든 체결구가 제자리에 배치된 후 장착 플레이트가 수평인지 확인합니다.
7. 나사를 조여 장착 플레이트를 벽에 고정합니다.

벽면 탑재형 Amazon One 디바이스를 연결하려면

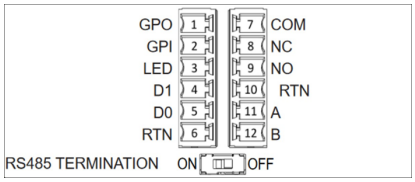
OSDP 및 Weigand 액세스 제어 프로토콜을 사용하여 Amazon One 디바이스를 구성할 수 있습니다. 설치를 간소화하기 위해 Amazon One 디바이스는 터미널 블록 커넥터(Mfg P/N: Phoenix Contact 1767694)를 사용합니다. 또한 내부 릴레이 또는 범용 입력 및 출력 연결을 사용하여 외부 디바이스를 직접 제어하도록 Amazon One 디바이스를 구성하는 옵션도 있습니다.

1. 애플리케이션에 적합한 배선 구성을 확인하려면 다음 다이어그램 및 연결 테이블을 참조하세요.

   신호의 자세한 전기적 특성은 배선 지침을 참조하세요.



   연결



핀	연결	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 커먼	접점 릴레이 커먼 - 흰색 와이어	
8	NC	릴레이 정상 닫힘	접점 릴레이 상시 닫힘 - 주황색 와이어	
9	NO	릴레이 정상 열림	접점 릴레이 상시 열림 - 노란색 와이어	
10	RTN	신호 반환	OSDP 반환 - 검은색 와이어	

핀	연결	설명	사용	
11	A	RS485_A/D1/시계	OSDP D1 - 흰색 와이어	
12	B	RS485_B/D0/데이터	OSDP D0 - 녹색 와이어	

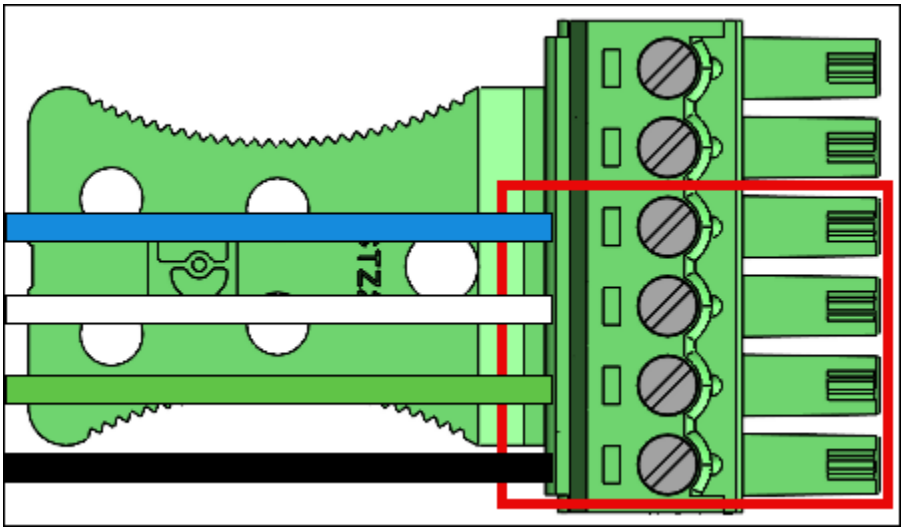
2. 와이어를 설치할 때 와이어 끝에서 3mm~5mm를 벗겨냅니다.
3. 와이어의 벗겨진 끝을 원하는 터미널 위치에 삽입합니다.
4. 일자 드라이버를 사용하여 단자 고정 나사를 시계 방향으로 돌려 와이어가 꼭 맞을 때까지 고정합니다. 너무 조이지 마세요.
5. 고정 후 와이어를 살짝 잡아당겨 고정되었는지 확인합니다.
6. 필요한 연결을 수행한 후 Amazon One 디바이스 터미널 블록의 해당 소켓에 플러그를 삽입합니다.
7. Cat6 이더넷 케이블을 RJ45잭에 삽입합니다.
8. 벽판의 후크가 디바이스 후면의 개구부로 미끄러지도록 Amazon One 디바이스를 배치합니다.
9. 케이블이 디바이스와 탑재판 사이에 걸리지 않도록 하고 디바이스가 피벗되어 제자리에 고정되도록 합니다.
10. 두 개의 Torx Security M4x10 플랫헤드 나사를 사용하여 Amazon One 디바이스를 탑재판에 고정합니다.
11. 나사를 손으로 조입니다. 너무 조이지 마세요.

벽면 장착형 Amazon One 디바이스를 연결하려면

애플리케이션에 필요한 와이어만 설치합니다.

Wiegand 연결

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



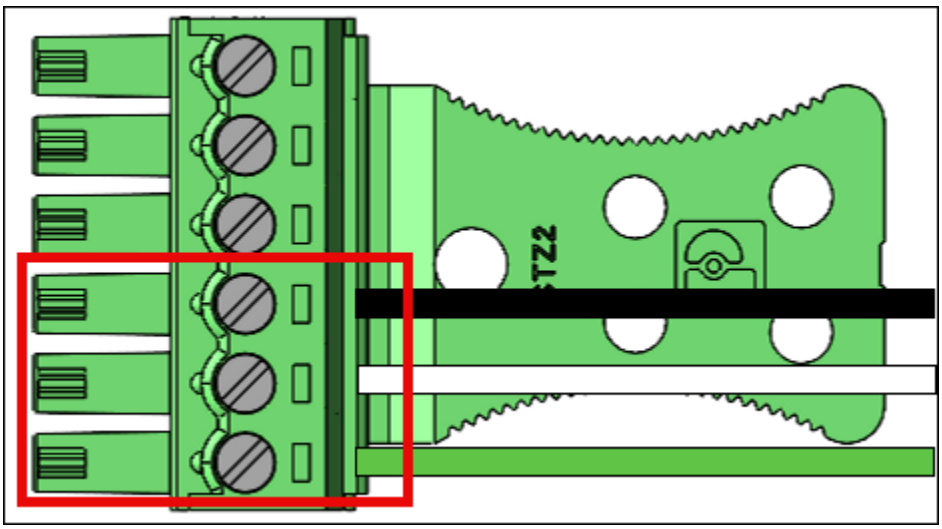
Wiegand 출력 배선

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

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

RS485 연결

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

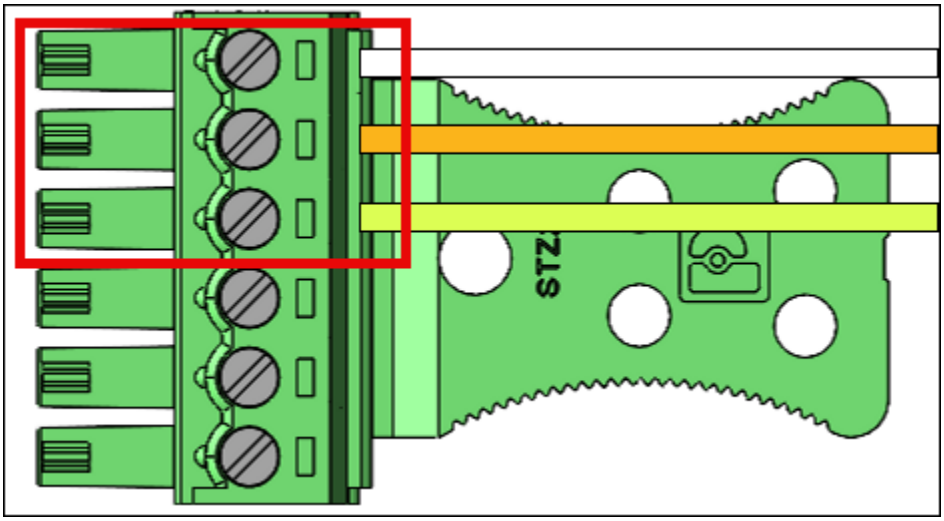


RS485 배선

핀	연결	설명	사용	
10	RTN	신호 반환	Ground(지상)	
11	A	RS485_A/D1/시계	RS485 비역전 신호	
12	B	RS485_B/D0/데이터	RS485 신호 반전	

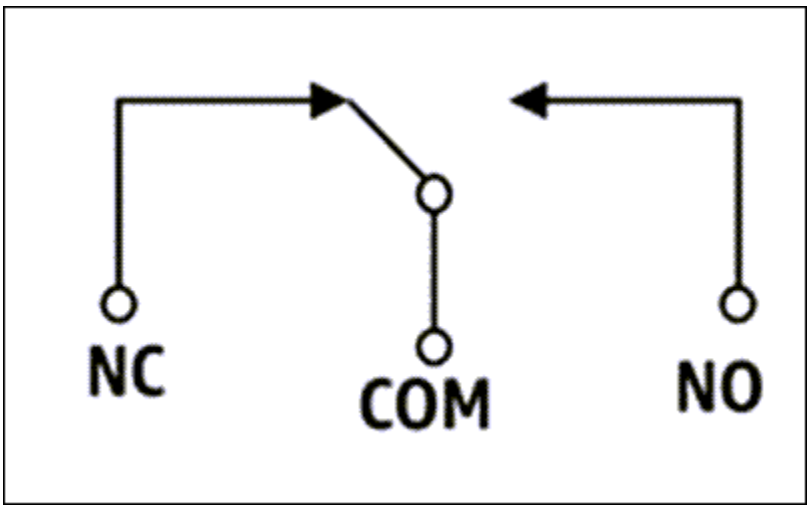
릴레이 연결

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



릴레이 배선

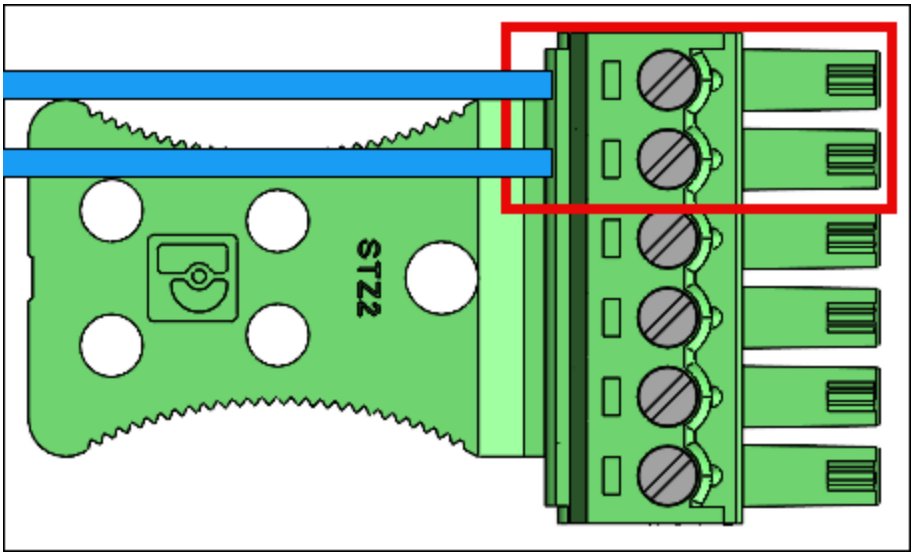
핀	연결	설명	사용	
7	COM	릴레이 커먼	접점 릴레이 커먼 - 흰색 와이어	
8	NC	릴레이 정상 닫힘	접점 릴레이 상시 닫힘 - 주황색 와이어	
9	NO	릴레이 정상 열림	접점 릴레이 상시 열림 - 노란색 와이어	



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

디지털 입력/출력 연결

- 핀 1()에 파란색 와이어를 삽입합니다GPO.
- 핀 2()에 파란색 와이어를 삽입합니다GPI.



핀	연결	설명	사용	
1	GPO	범용 출력	디지털 출력 신호 (5V)	

핀	연결	설명	사용	
2	GPI	범용 입력	디지털 입력 신호 (3.6V – 5V)	

- 디지털 입력/출력 연결은 나열된 대로 작동해야 합니다.

Amazon One 디바이스를 활성화Amazon One 디바이스 활성화하려면 섹션을 참조하세요.

보안 액세스를 위한 Amazon One 디바이스 I/O Hub 설치

이 섹션에서는 I/O Hub를 사용하여 Amazon One Enterprise(AOE) 디바이스를 설치하는 데 필요한 위치 요구 사항과 단계를 자세히 설명합니다.

설치를 시작하기 전에 다음을 확인합니다.

- I/O Hub가 있는 Amazon One 디바이스는 실내 전용입니다.
- Power Over Ethernet(PoE ++)의 경우:

  IEEE 802.3bt(유형 3) 클래스 6 POE++ 스위치(엔드 스팬) 또는 인젝터(미드스팬)를 사용할 수 있는지 확인합니다. 이 스위치는 등록 또는 인증되었으며 IEC 62368-1을 준수합니다.

  승인된 PoE ++ 소스가 있는 Amazon One 디바이스만 사용합니다.

  PoE ++ 소스는 동일한 건물 내에 있어야 합니다.

- 15V DC 전원 입력의 경우, 나열되거나 인증된 NEC Class 2 또는 전원 제한 승인 전원 공급 장치와 함께 Amazon One 디바이스만 사용해야 합니다. 아래의 선택적 DC 섹션을 참조하세요.

필수 도구:

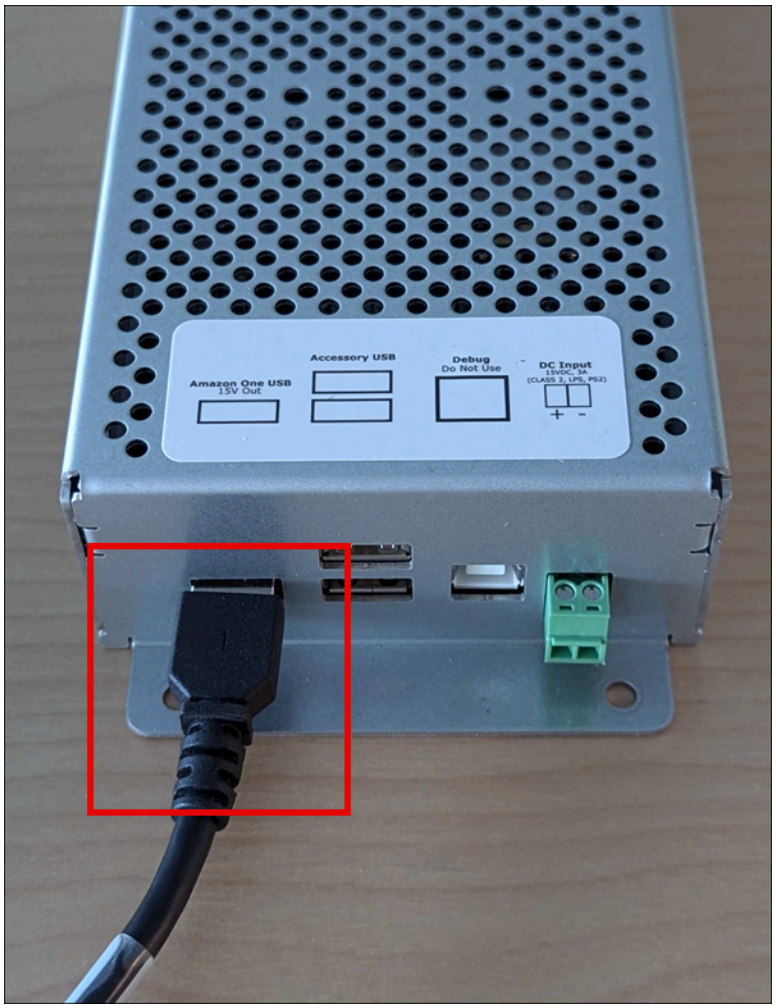
- 와이어 스트리퍼
- #2 Phillips 드라이버
- 0.5mm x 2mm 일자 드라이버

I/O Hub가 있는 Amazon One 디바이스에 포함됨:

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

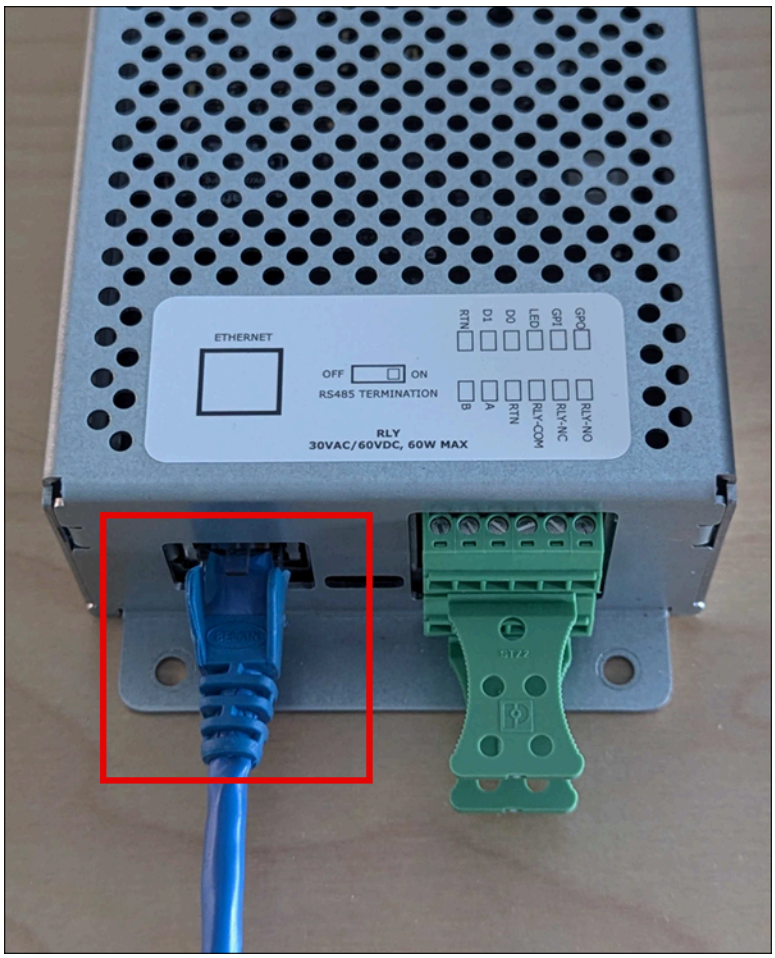
Amazon One 디바이스의 I/O 허브를 설치하려면

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



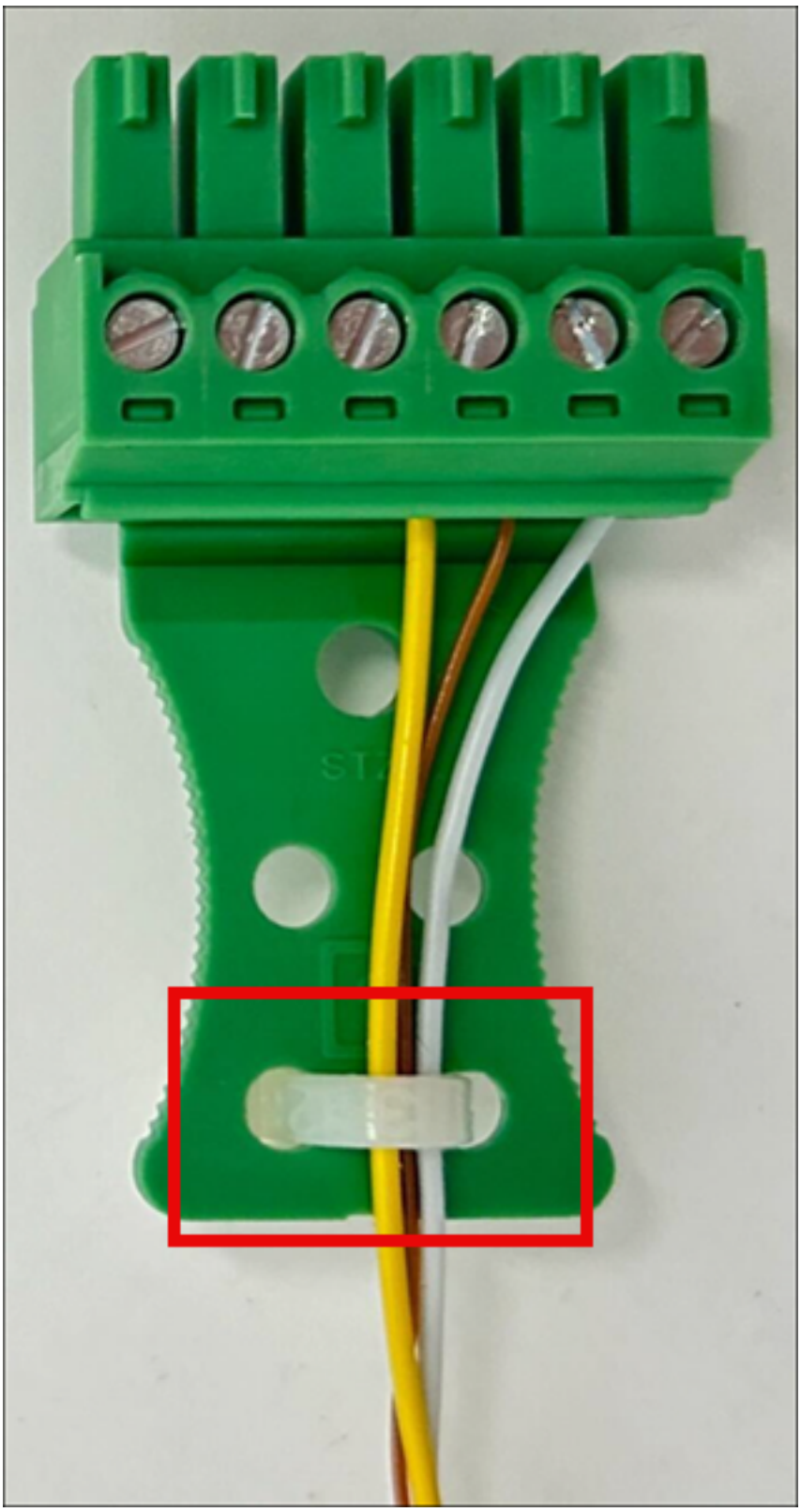
4. POE++ 전원의 경우 POE++ 소스의 이더넷 케이블을 I/O 허브 포트에 연결합니다.

   선택 사항: DC 전원의 경우 아래의 DC 배선 설치 섹션을 참조하세요.



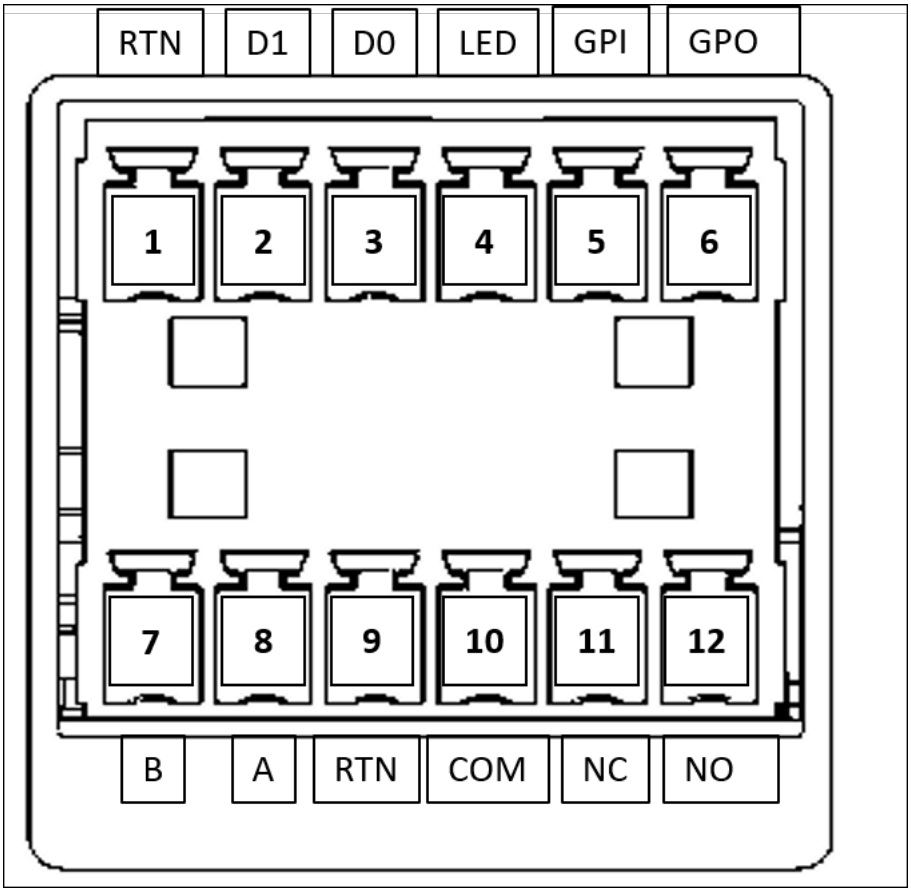
Amazon One 디바이스의 I/O 허브를 연결하려면

- 드립 루프를 설치하여 액체가 실수로 코드를 통해 I/O 허브로 흘러 들어가지 않도록 합니다.
- 다음 이미지와 같이 스트레인 릴리프 클램프를 연결하여 와이어가 손상되거나 스트레스를 받지 않도록 보호합니다.



1. 터미널 블록 플러그를 통해 애플리케이션에 필요한 와이어만 삽입합니다. 다음 배선 표 및 다이어그램을 참조하세요.

2. 터미널 블록 플러그를 I/O 허브에 삽입합니다.

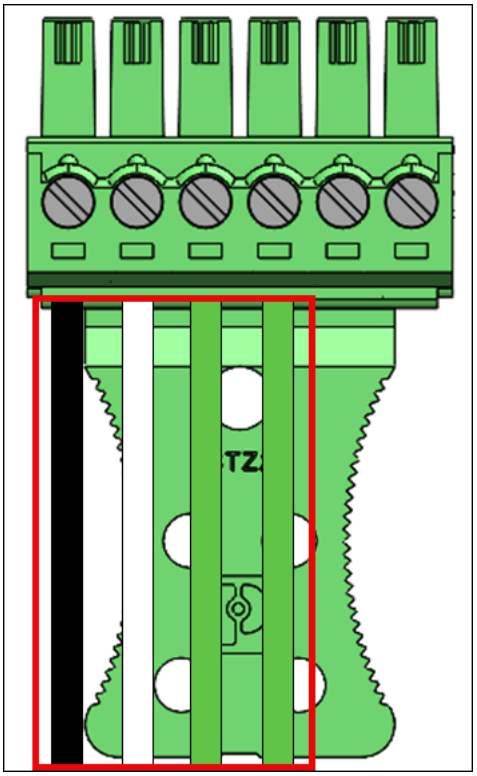


핀	연결	설명	사용	
1	RTN	신호 반환	Wiegand 접지 - 검은색 와이어	
2	D1	Wiegand D1	Wiegand Data 1 - 흰색 와이어	
3	D0	Wiegand D0	Wiegand 데이터 0 - 녹색 와이어	
4	LED	Wiegand LED	Wiegand LED - 선택 사항	

핀	연결	설명	사용	
5	GPI	범용 입력	디지털 입력 신호 - 선택 사항	
6	GPO	범용 출력	디지털 출력 신호 - 선택 사항	
7	B	RS485_B/D0/데이터	OSDP D0 - 녹색 와이어	
8	A	RS485_A/D1/시계	OSDP D1 - 흰색 와이어	
9	RTN	신호 반환	OSDP 반환 - 검은색 와이어	
10	COM	릴레이 커먼	접점 릴레이 커먼 - 흰색 와이어	
11	NC	릴레이 정상 닫힘	접점 릴레이 상시 닫힘 - 주황색 와이어	
12	NO	릴레이 정상 열림	접점 릴레이 정상 열림 - 노란색 와이어	

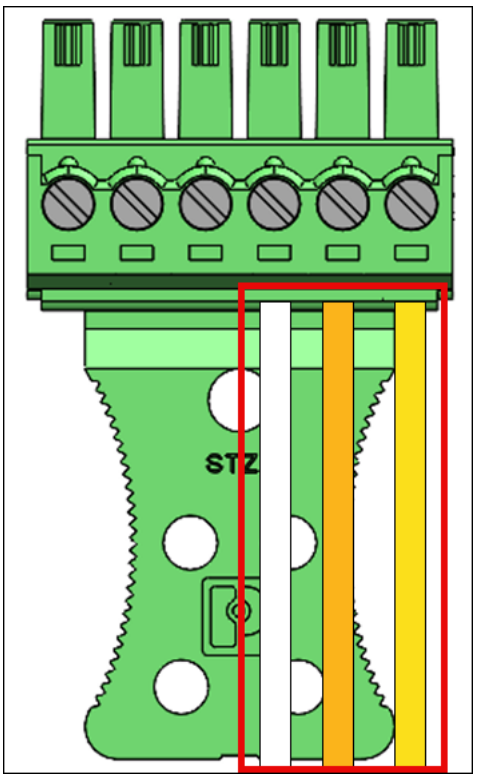
Wiegand 연결

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

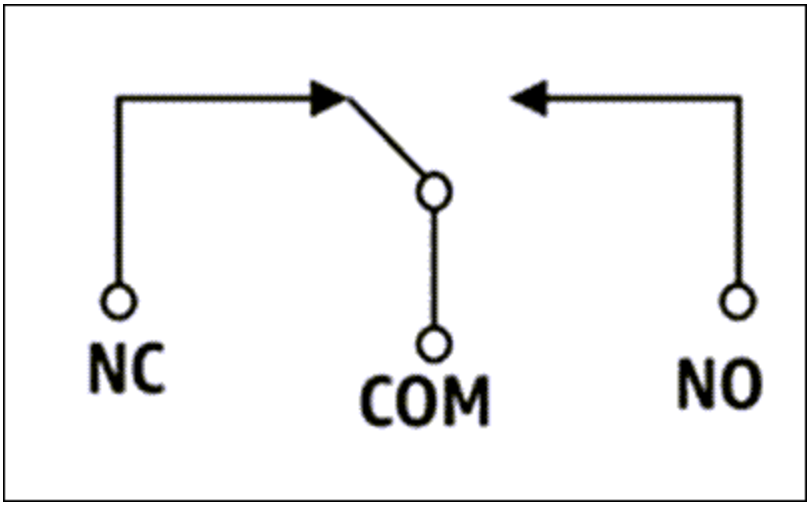


릴레이 연결

- 흰색 와이어를 핀 10()에 삽입합니다COM.
- 핀 11(NC)에 주황색 와이어를 삽입합니다.
- 노란색 와이어를 핀 12(NO)에 삽입합니다.



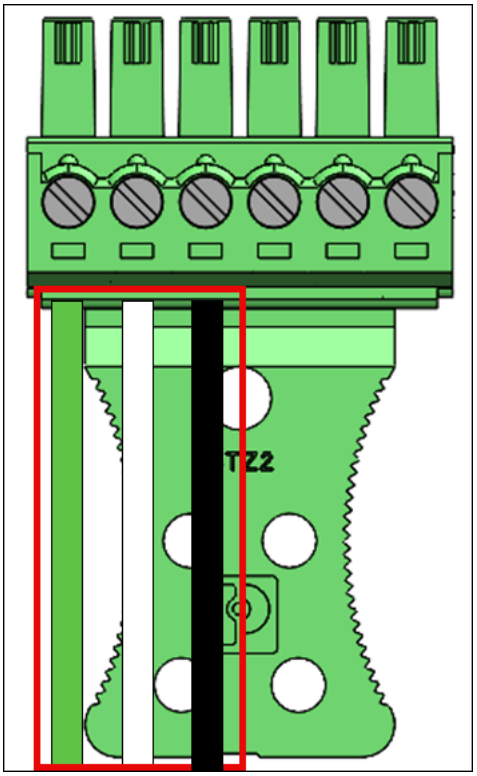
릴레이 다이어그램



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

RS485 연결

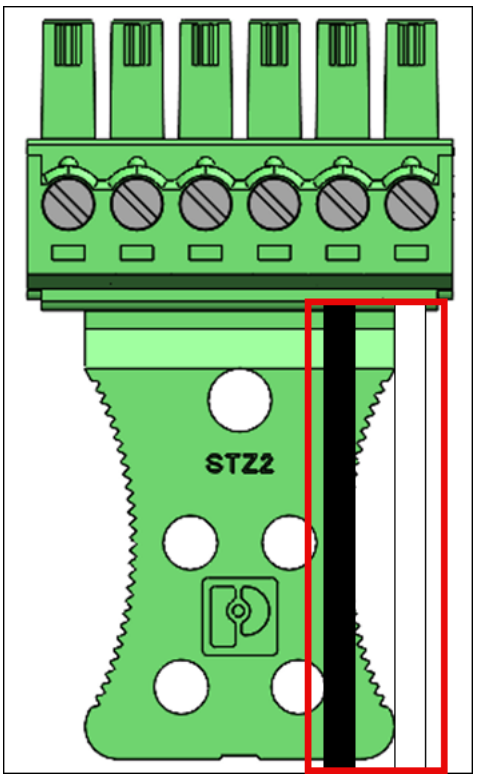
- 핀 7(B)에 녹색 와이어를 삽입합니다.
- 흰색 와이어를 핀 8(A)에 삽입합니다.
- 핀 9()에 검은색 와이어를 삽입합니다RTN.



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

디지털 입력/출력 연결

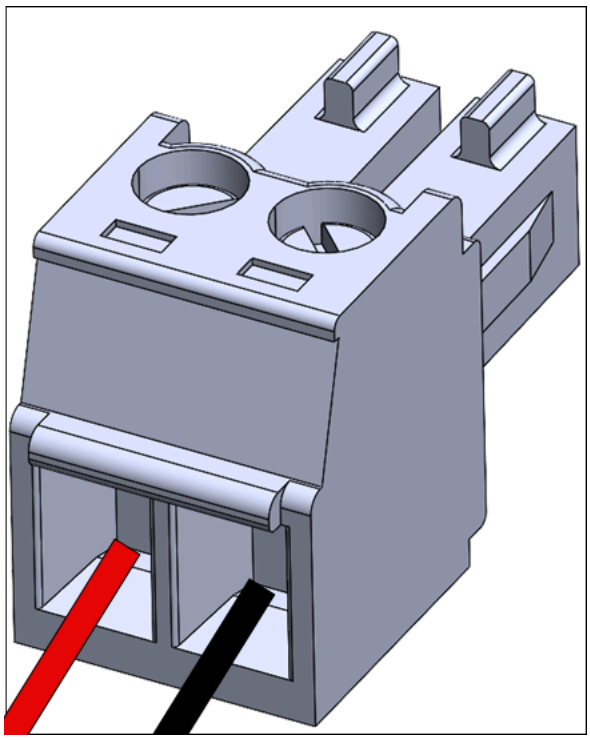
- 핀 5()에 검은색 와이어를 삽입합니다GPI.
- 흰색 와이어를 핀 6()에 삽입합니다GPO.



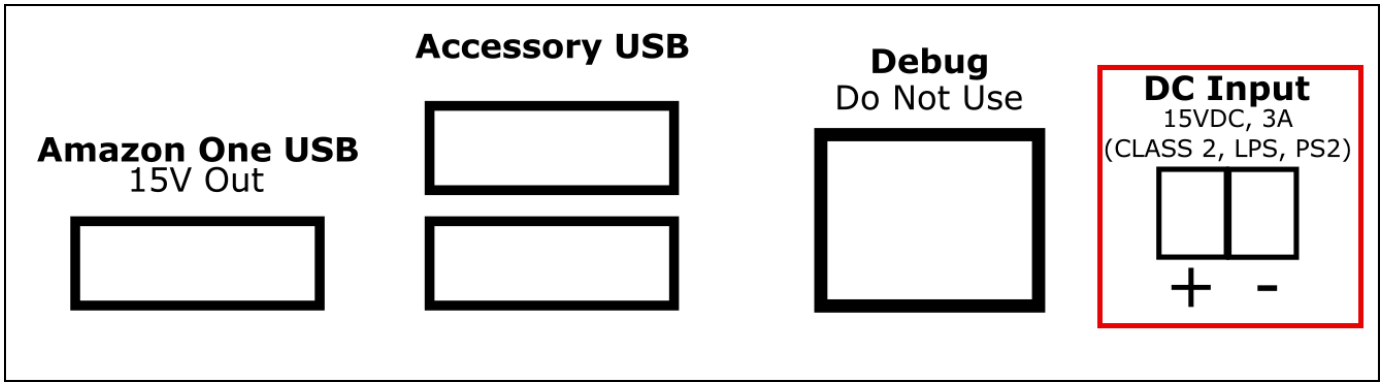
- 디지털 입력/출력 연결은 나열된 대로 작동해야 합니다.

선택 사항: DC 배선 설치

1. 빨간색 와이어의 끝에서 3mm~5mm를 벗기면 양수(+)가 되고 검은색 와이어의 끝이 음수(-)가 됩니다.
2. DC 와이어의 벗겨진 끝을 DC 플러그에 삽입합니다.



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



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 연결되면 즉시 최신 소프트웨어 패키지 다운로드가 시작됩니다.

3. 화면에 소프트웨어 다운로드 완료!가 표시되면 확인을 선택합니다.
4. QR 코드 를 선택합니다.

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

   > **Note**
   >
   > Amazon One Enterprise 콘솔에서 활성화 QR 코드에만 액세스할 수 있도록 설치자에게 제한된 권한을 부여하는 것이 좋습니다. Amazon One Enterprise 사용자 추가을 참조하세요.
6. 탐색 창에서 활성화 QR 코드 를 선택합니다.
7. 사이트 선택 드롭다운 목록에서 Amazon One 디바이스가 설치된 사이트를 선택합니다.
8. 사이트 정보 에서 사이트 주소를 확인합니다.
9. 활성화 QR 코드 에서 활성화하려는 디바이스 인스턴스 이름을 찾은 다음 해당 QR 코드 가져오기를 선택하여 QR 코드를 검색합니다.
10. Amazon One 디바이스로 QR 코드를 스캔합니다. QR 코드는 보안을 위해 주기적으로 새로 고쳐지므로 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 손바닥 등록을 시작하고 손바닥을 인증하여 액세스 권한을 얻을 수 있습니다.

주제

엔드포인트 정책 생성

사용자가 입장을 위해 손바닥을 인증하려면 먼저 등록 프로세스를 거쳐야 합니다. 보안 담당자는 사용자가 등록하도록 허용하기 전에 항상 사용자의 신원을 확인해야 합니다.

Amazon One 디바이스에 손바닥을 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. 사용 약관 을 읽은 다음 확인을 누릅니다.
4. 동의 - Palm 생체 정보를 읽고 동의하면 동의함을 누릅니다.
5. 화면의 지침에 따라 등록 프로세스를 완료합니다.

항목 인증

손바닥을 성공적으로 등록하면 Amazon One Enterprise 입력 디바이스에서 손바닥으로 인증할 준비가 된 것입니다.

Amazon One 디바이스의 진입을 위해 손바닥을 인증하려면

- 디바이스 위에 손바닥을 올려 놓고 화면의 지침에 따라 손바닥을 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 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 등록된 사용자 관리 를 선택합니다.
3. 등록된 사용자 에서 등록된 모든 사용자와 다음 세부 정보를 확인할 수 있습니다.
    - 배지 ID - 등록 시 배지 리더가 캡처한 RFID 배지 식별자 정보입니다.
    - 등록 소스 - 등록에 사용된 Amazon One 디바이스의 세부 정보입니다.
    - 등록 날짜 - 등록 날짜 및 시간입니다.

등록된 사용자 및 해당 생체 인식 삭제

다음 절차에서는 등록된 사용자와 해당 생체인식을 삭제하는 방법을 자세히 설명합니다.

등록된 사용자 및 해당 생체인식을 삭제하려면

1. https://console.aws.amazon.com/one-enterprise 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 등록된 사용자 관리 를 선택합니다.
3. 등록된 사용자 에서 손바닥 생체인식 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 손바닥 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 디바이스를 설치하고 활성화한 후 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 청소

Amazon One 디바이스를 유지 관리하면 최적의 디바이스 운영 환경과 디바이스 경험을 얻을 수 있습니다.

Amazon One 디바이스를 청소하기 전에 다음을 확인하세요.

- Amazon One을 활성화하거나 비활성화할 필요는 없지만 디바이스가 전원에 연결되고 네트워크 연결이 되어 있으며 모든 주변 및 동반 디바이스(해당하는 경우)가 연결되어 있는지 확인합니다.
- 네트워크 연결을 사용할 수 없는 경우(이 경우 Amazon One 디바이스에 오류 화면이 표시됨), Amazon One 디바이스에 오류 화면이 표시되거나 콘솔에 디바이스 연결 문제가 표시되는 경우 관리자에게 문제를 에스컬레이션합니다.
- 권한이 없는 개인이 디바이스를 조작할 수 없도록 디바이스를 물리적으로 보호합니다.
- Amazon One 디바이스에 대한 무단 연결을 확인하여 매일 Amazon One 디바이스를 시각적으로 검사합니다.
- Amazon One 디바이스의 내부 구성 요소/회로가 노출되는 간격/개방이 없는지 확인하기 위해 디바이스의 눈에 보이는 나사와 케이스를 포함하여 디바이스의 모든 면에 변조 징후가 있는지 검사합니다.
- 오류 또는 장애가 발생하는 경우 Amazon One 디바이스 화면의 지침을 따르거나 문제 해결 안내서를 참조하여 문제를 해결하세요.

Amazon One 디바이스를 청소하려면

Amazon One 디바이스를 청소하면 지문 및 손자국과 같은 스머지 또는 마크가 정기적으로 제거됩니다.

> **Note**
>
> 이 가이드에 나열된 것 이외의 다른 세척 제품은 사용하지 마십시오. 권장 청소 일정은 일주일에 1~2회 또는 디바이스에 먼지, 먼지 또는 얼룩이 보일 때마다입니다. 단, 하루에 한 번 이상은 안 됩니다.

1. Amazon One 디바이스를 이소프로필 알코올(IPA) Wipes로 닦습니다. 디바이스의 터치 표면만 청소합니다. Amazon One에서 지시하지 않는 한 광학 창을 만지거나 다른 청소 제품을 사용하지 마세요.
2. 마른 극세사 천으로 줄무늬를 닦습니다.
3. 광학 창에서 눈에 보이는 먼지나 파편을 가볍게 더스트합니다(닦지 마세요). 광학 윈도우의 청소를 하루에 한 번 이하로 제한합니다 and/or when the window is visually dirty (e.g., finger/hand prints/smudges). 디바이스의 이 부분은 만지기 위한 것이 아니지만 새 고객이 실수로 만질 수 있습니다.
4. 해당하는 경우 KIC 스마트 카드 클리너를 사용하여 카드 리더 내부를 청소합니다.
5. 일주일에 한두 번 디바이스를 청소하거나 디바이스에 먼지, 먼지 또는 얼룩이 보일 때마다 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 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 사이트 를 선택합니다.
3. 사이트 에서 이름을 편집하려는 사이트를 선택합니다.
4. 편집을 선택합니다.
5. 사이트 정보에서 원하는 사이트 이름과 사이트 설명을 입력합니다(선택 사항).
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-enterprise에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 사이트 를 선택합니다.
3. 사이트 에서 주소를 업데이트하려는 사이트를 선택합니다.
4. 디바이스 인스턴스 에서 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 명명 규칙)과 통신 구성 세트가 있습니다.

주제

- 디바이스 인스턴스 상태 보기
- Amazon One 디바이스 재부팅

- Amazon One 디바이스 구성 업데이트
- Wi-Fi 보안 인증 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 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스 를 선택합니다.
3. 활성화된 인스턴스 아래에 활성화된 Amazon One 디바이스 목록이 표시됩니다.
4. 디바이스 인스턴스 세부 정보를 보려면 디바이스 인스턴스 이름을 선택합니다.

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 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스 를 선택합니다.
3. 활성화된 인스턴스 에서 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 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스 를 선택합니다.
3. 활성화된 인스턴스 에서 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). 그런 다음 디바이스 활성화 프로세스를 진행할 수 있습니다(참조Amazon One 디바이스 활성화).

5. 원하는 변경을 수행한 후 디바이스 구성 업데이트를 선택하여 업데이트를 확인합니다.

Wi-Fi 보안 인증 업데이트

다음 절차에서는 Wi-Fi 보안 인증 정보를 업데이트하는 방법을 자세히 설명합니다.

Wifi 자격 증명을 업데이트하려면

1. https://console.aws.amazon.com/one-enterprise에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스 를 선택합니다.
3. 활성화된 인스턴스 에서 업데이트하려는 디바이스의 인스턴스 이름을 선택합니다.
4. 네트워크 에서 편집 을 선택합니다.
5. Wi-Fi 구성에서 원하는 내용을 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 에서 Amazon One Enterprise 콘솔을 엽니다.
2. 탐색 창에서 디바이스 인스턴스 를 선택합니다.
3. 활성화된 인스턴스 에서 비활성화하려는 디바이스 인스턴스의 이름을 선택합니다.
4. 디바이스 비활성화를 선택합니다.
5. 비활성화를 확인하려면 메시지 상자에 '비활성화'를 입력하고 디바이스 비활성화 를 선택합니다.

보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 가장 보안에 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 - 에서 AWS 서비스를 실행하는 인프라를 보호할 AWS 책임이 있습니다 AWS 클라우드. AWS 또한 는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 규정 준수 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon One Enterprise에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 AWS 프로그램의 범위 내 서비스 규정 준수 프로그램의 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 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 방법도 알아봅니다.

주제

- Amazon One Enterprise의 데이터 보호
- Amazon One Enterprise의 자격 증명 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 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 개인 정보 보호에 대한 자세한 내용은 데이터 개인 정보 보호

를 FAQ참조하세요. 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 ()를 사용하여 개별 사용자를 설정하는 것이 좋습니다IAM. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 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 사용하세요.
- 명령줄 인터페이스 또는를 AWS 통해 FIPS에 액세스할 때 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 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 CLI또는 API를 사용하여 작업하는 경우가 포함됩니다 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에를 제공하는 경우 해당 서버에 URL 대한 요청을 검증URL하기 위해에 자격 증명 정보를 포함하지 않는 것이 좋습니다.

저장 데이터의 기본 암호화를 사용하려면

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

AWS 소유 키 - Amazon One Enterprise는 기본적으로 이러한 키를 사용하여 민감한 최종 사용자 데이터를 자동으로 암호화합니다. 사용자는 AWS 소유 키를 보거나 관리 또는 사용할 수 없으며 해당 키의 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 자격 증명 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 사용하도록 인증(로그인) 및 권한 부여(권한 부여)를 받을 수 있는 사용자를 제어합니다. IAM는 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

사용 방법 AWS Identity and Access Management (IAM)은 Amazon One Enterprise에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Amazon One Enterprise 서비스를 사용하여 작업을 수행하는 경우 관리자는 필요한 자격 증명과 권한을 제공합니다. 더 많은 Amazon One Enterprise 기능을 사용하여 작업을 수행하려면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Amazon One Enterprise의 기능에 액세스할 수 없는 경우 섹션을 참조하세요Amazon One Enterprise 자격 증명 및 액세스 문제 해결.

서비스 관리자 - 회사에서 Amazon One Enterprise 리소스를 책임지고 있는 경우 Amazon One Enterprise에 대한 전체 액세스 권한이 있을 수 있습니다. 서비스 사용자가 액세스해야 하는 Amazon

One Enterprise 기능과 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Amazon One EnterpriseIAM에서를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요Amazon One Enterprise의 작동 방식 IAM.

IAM 관리자 - IAM 관리자인 경우 Amazon One Enterprise에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. 에서 사용할 수 있는 Amazon One Enterprise 자격 증명 기반 정책의 예를 보려면 섹션을 IAM참조하세요Amazon One Enterprise의 자격 증명 기반 정책 예제.

ID를 통한 인증

인증은 자격 증명 AWS 으로에 로그인하는 방법입니다. 로 AWS 계정 루트 사용자, IAM 사용자로 또는 IAM 역할을 수임하여 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인하는 경우 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정한 상태입니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 대한 서명 버전 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화하도록 AWS 권장합니다. 자세한 내용은 사용 설명서의 다중 인증 및 사용 설명서AWS 의 다중 인증 IAM 섹션을 참조하세요IAM. AWS IAM Identity Center

AWS 계정 루트 사용자

를 생성할 때 먼저 계정의 모든 AWS 서비스 및 리소스에 대한 전체 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 테 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수

있는 태스크를 수행하는 데 사용하십시오. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 연동을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명이 액세스하면 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보안 인증 정보를 사용하는 것이 좋습니다. 그러나 IAM 사용자와 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 라는 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 자격 증명만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 이 역할은 IAM 사용자와 비슷하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 역할(콘솔)로 전

환할 AWS Management Console수 있습니다. IAM 또는 AWS API 작업을 호출하거나 사용자 지정를 AWS CLI 사용하여 역할을 수임할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 자격 증명이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자(페더레이션)에 대한 역할 생성을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를의 역할과 상호 연관시킵니다IAM. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대해 다른 권한을 일시적으로 수임할 수 있습니다.
- 크로스 계정 액세스 – IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 AWS 서비스 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는 직접 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행할 때 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다.는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 FAS 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신하는 경우에만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정, 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 에 권한을 위임할 역할 생성을 AWS 서비스 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에

표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며, EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있도록 합니다. 자세한 내용은 IAM 사용 설명서EC2의 IAM 역할 사용을 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 실행하기 위한 방법과 상관없이 작업을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console, AWS CLI또는에서 역할 정보를 가져올 수 있습니다 AWS API.

ID 기반 정책

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 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 설명서의 고객 관리형 정책을 사용하여 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는

독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 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 또는이 포함될 수 있습니다 AWS 서비스.

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

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 AmazonVPC은를 지원하는 서비스의 예입니다ACLs. 에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 ACLs참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM 개체(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔티티의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) -의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책 SCPs입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 모든 계정에 적용할 수 있습니다. 는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을

SCP 제한합니다 AWS 계정 루트 사용자. 조직 및에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 SCPs참조하세요.

- 리소스 제어 정책(RCPs) - 소유한 각 리소스에 연결된 JSON 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 IAM 정책RCPs입니다. 는 멤버 계정의 리소스에 대한 권한을 RCP 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. 를 AWS 서비스 지원하는 목록을 RCPs포함하여 조직 및에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 RCPs참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

Amazon One Enterprise의 작동 방식 IAM

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

IAM Amazon One Enterprise와 함께 사용할 수 있는 기능

IAM 기능	Amazon One Enterprise 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예

IAM 기능	Amazon One Enterprise 지원
ACLs	아니요
ABAC (정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

Amazon One Enterprise 및 기타 AWS 서비스가 대부분의 IAM 기능을 어떻게 사용하는지 전체적으로 알아보려면 IAM 사용 설명서의 AWS 에서 작업하는 서비스를 IAM 참조하세요.

Amazon One Enterprise의 자격 증명 기반 정책

ID 기반 정책 지원: 예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 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 설명서의 고객 관리형 정책을 사용하여 사용자 지정 IAM 권한 정의를 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. 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 문서입니다. 리소스 기반 정책의 예는 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.

크로스 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 교차 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념합니다. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 개체(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.

Amazon One Enterprise에 대한 정책 작업

정책 작업 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 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. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함합니다.

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 다음과 같이 쉼표로 구분합니다.

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

```
      "one:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe(이)라는 단어로 시작하는 모든 작업은 다음을 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 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 객체를 지정합니다. 문에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 가장 좋은 방법은 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정하는 것입니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Amazon One Enterprise 리소스 유형 및 해당의 목록을 보고 각 리소스ARN의를 지정하는 데 사용할 수 있는 작업을 ARNs알아보려면 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 Enterprise의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 문이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 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.

ACLs Amazon One Enterprise의

지원: ACLs 아니요

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

ABAC Amazon One Enterprise 사용

지원ABAC(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. 엔터티 및 리소스에 태그를 지정하는 것은의 첫 번째 단계입니다ABAC. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로워지는 상황에 도움이 됩니다.

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.

에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여로 권한 정의를 ABAC참조하세요. 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어 사용(ABAC)을 ABAC참조하세요.

Amazon One Enterprise에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인할 때 작동하지 AWS 서비스 않는 경우도 있습니다. 임시 자격 증명으로 AWS 서비스 작업하는 것을 포함하여 자세한 내용은 IAM 사용 설명서의 AWS 서비스 로 작업하는 IAM 섹션을 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS API. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 동적으로 임시 자격 증명을 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 내용은 의 임시 보안 자격 증명을 IAM참조하세요.

Amazon One Enterprise에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션 지원(FAS): 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다.는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 FAS 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신하는 경우에만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.

Amazon One Enterprise의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정, 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 에 권한을 위임할 역할 생성을 AWS 서비스 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 링크 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 표시 AWS 계정 되며 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 서비스 단원을 참조하세요. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Amazon One Enterprise의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 Amazon One Enterprise 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는를 사용하여 작업을 수행할 수 없습니다 AWS API. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

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

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

주제

정책 모범 사례

자격 증명 기반 정책은 계정에서 Amazon One Enterprise 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- 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 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 관한AWS 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 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 정책 조건을 작성하여를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다SSL. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer를 사용한 정책 검증을 참조하세요.

- 멀티 팩터 인증 필요(MFA) -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해를 AWS 계정캡니다. API 작업을 호출할 MFA 때를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 를 사용한 보안 API 액세스를 MFA 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 권한을 통해의 Amazon One Enterprise 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 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 에만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다 AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스하도록 허용합니다.

사용자와 역할이 여전히 Amazon One Enterprise 콘솔을 사용할 수 있도록 하려면 Amazon One Enterprise *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책을 엔터티에 연결합니다. 자세한 내용은 IAM사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함되어 있습니다 AWS API.

```
{
    "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 부여하는 AWS 관리`AmazonOneEnterpriseReadOnlyAccess`형 정책을 보여줍니다.

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

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.

Action 요소의 값은 서비스가 지원하는 APIs에 해당합니다. Amazon One Enterprise 작업을 참조함을 나타내기 config: 위해 작업 앞에가 표시됩니다. 다음 예제와 같이 * 요소에서 Action 와일드카드 문자를 사용할 수 있습니다.

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

  이렇게 하면 “DeviceInstance”(GetDeviceInstanceConfiguration,)로 끝나는 모든 Amazon One Enterprise 작업이 허용됩니다CreateDeviceInstanceConfiguration.

- "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 사용자에게 CreateDeviceInstance, UpdateDeviceInstance및와 같은 작업에 대한 권한을 부여하지 않습니다DeleteDeviceInstance. 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

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.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "one:*"
            ],
            "Resource": "*"
        },
    ]
}
```

Amazon One Enterprise 규칙 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 작업을 설명합니다. 또한 각 작업에 대해 지원되는 리소스와에 ARNs 대해서도 설명합니다. 를 지정할 때 경로에 * 와일드카드를 사용할 ARN수 있습니다. 예를 들어 정확한 리소스를 지정할 수 없거나 지정하지 않으려는 경우입니다IDs.

> **Important**
>
> Amazon One Enterprise 규칙 API 작업이이 테이블에 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

API 작업	리소스
	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*
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*

API 작업	리소스
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*
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.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "one:GetSite",
                    "one:GetSiteAddress"
                ],
                "Resource": [
                    "arn:aws:one:region:accountID:site/siteId"
                ]
            }
        ]
    }
```

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "one:DeleteSite",
                "one:UpdateSiteAddress"
               ],
            "Resource": "arn:aws:one:region:accountID:site/siteId"
           }
      ]
   }
```

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

추가 정보

IAM 사용자, 그룹, 정책 및 권한 생성에 대한 자세한 내용은 IAM 사용 설명서의 첫 번째 IAM 사용자 및 관리자 그룹 생성 및 액세스 관리를 참조하세요.

AWS Amazon One 엔터프라이즈에 대한 관리형 정책

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

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

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

자세한 내용은 IAM사용 설명서의 AWS 관리형 정책을 참조하십시오.

AmazonOneEnterpriseFullAccess

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

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

```
{
```

```
 "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 엔터프라이즈 리소스를 가져옵니다.

`one:List*`Amazon One 엔터프라이즈 리소스를 나열합니다.

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

AmazonOneEnterpriseInstallerAccess

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

`one:CreateDeviceActivationQrCode`QR 코드를 생성하여 장치를 활성화할 수 있습니다.

one:GetDeviceInstanceAmazon One 디바이스 인스턴스에 대한 정보를 가져올 수 있습니다.

one:GetSiteAmazon One 엔터프라이즈 사이트에 대한 정보를 가져올 수 있습니다.

one:GetSiteAddressAmazon One 엔터프라이즈 사이트의 실제 주소를 가져올 수 있습니다.

one:ListDeviceInstancesAmazon One 디바이스 인스턴스를 나열할 수 있습니다.

one:ListSitesAmazon One 엔터프라이즈 사이트를 나열할 수 있습니다.

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

Amazon One 엔터프라이즈, AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 이루어진 Amazon One Enterprise의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Amazon One 엔터프라이즈 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
Amazon One Enterprise는 변경 사항 추적을 시작했습니다	Amazon One Enterprise는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2023년 12월 1일

Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키

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

주제

Amazon One Enterprise에서 정의한 작업

정책 설명의 `Action` 요소에 다음 작업을 지정할 수 있습니다. IAM 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용할 때는 일반적으로 이름이 같은 API 작업이나 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. 열에 리소스 유형이 포함된 경우 해당 작업이 포함된 명령문에 해당 ARN 유형의 리소스를 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. IAM정책의 `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	기기 인스턴스 생성 권한 부여	쓰기		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	디바이스 인스턴스에 대한 정보를 가져올 수 있는 권한 부여	읽기	기기 인스턴스*		
ListDeviceInstances	디바이스 인스턴스를 나열할 수 있는 권한 부여	읽기			
UpdateDeviceInstance	디바이스 인스턴스 업데이트 권한 부여	쓰기	기기 인스턴스*		
DeleteDeviceInstance	디바이스 인스턴스 삭제 권한 부여	쓰기	디바이스 인스턴스*		
CreateDeviceActivationQrCode	기기 인스턴스에서 기기를 활성화하기 위한 QR 코드 생성 권한 부여	쓰기	기기 인스턴스*		
DeleteAssociatedDevice	기기와 기기 인스턴스 간 연결을 삭제할 수 있는 권한 부여	쓰기	디바이스 인스턴스*		
RebootDevice	기기 재부팅 권한 부여	쓰기	디바이스 인스턴스*		
CreateDeviceInstan	디바이스 인스턴스 구성을 생성할 수 있는 권한 부여	쓰기			

작업	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ceConfiguration					
GetDeviceInstanceConfiguration	디바이스 인스턴스 구성에 대한 정보를 가져올 수 있는 권한을 부여합니다.	읽기	구성*		
CreateSite	사이트 생성 권한 부여	쓰기		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	디바이스 인스턴스 삭제 권한 부여	쓰기	사이트*		
GetSite	사이트에 대한 정보를 얻을 수 있는 권한 부여	읽기	사이트*		
ListSites	사이트 목록 표시 권한 부여	읽기			
GetSiteAddress	사이트 주소에 대한 정보를 얻을 수 있는 권한 부여	읽기	사이트*		
UpdateSite	사이트 업데이트 권한 부여	쓰기	사이트*		
UpdateSiteAddress	사이트 주소 업데이트 권한 부여	쓰기	사이트*		
CreateDeviceConfigurationTemplate	디바이스 인스턴스 생성 권한 부여	쓰기		aws:RequestTag/${TagKey} aws:TagKeys	

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

다음 리소스 유형은 이 서비스에 의해 정의되며 IAM 권한 정책 설명의 Resource 요소에 사용될 수 있습니다. 작업 테이블의 각 작업에서 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.

리소스 유형	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 IAM 정책 Condition 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	유형
aws:RequestTag/${TagKey}	요청의 태그를 기준으로 액세스를 필터링합니다.	String
aws:ResourceTag/${TagKey}	리소스와 연결된 태그를 기준으로 액세스를 필터링합니다.	String
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 규정 준수 프로그램 AWS 서비스 범위규정 준수 프로그램 범위 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 에서 보고서 다운로드 AWS Artifact에서 .

를 사용할 때 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 -이 백서에서는 기업이 HIPAA AWS 를 사용하여 적격 애플리케이션을 생성하는 방법을 설명합니다.

> **Note**
>
> 모두 HIPAA 자격이 AWS 서비스 있는 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하세요.

- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(), 결제카드 산업보안표준위원회(NIST), PCI국제표준화

기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 이를 AWS 서비스 통해 내 보안 상태를 포괄적으로 볼 수 있습니다 AWS. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty – 의심스러운 활동 및 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정워크로드DSS, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다.는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 GuardDuty 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험 및 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

Amazon One Enterprise 모니터링

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

- Amazon EventBridge은 AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 응답하는 데 사용할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge 에 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서 섹션을 참조하세요.
- AWS CloudTrail 는 AWS 계정에서 직접 또는 계정을 대신하여 수행된 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전달합니다. 라는 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시점을 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Amazon에서 Amazon One Enterprise 이벤트 모니터링 EventBridge

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

Amazon One Enterprise 이벤트 구독

Amazon One 디바이스 및 사용자 프로필 상태 변경 이벤트는 를 사용하여 게시되며 EventBridge새 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. 에서 EventBridge 콘솔을 엽니다https://console.aws.amazon.com/events/.
2. 탐색 창의 버스에서 규칙 을 선택합니다.
3. Create rule을 선택합니다.

4. 기본 규칙 세부 정보 페이지에서 규칙에 이름을 할당하고 이벤트 패턴이 있는 규칙을 선택한 다음 다음을 선택합니다.
5. 이벤트 패턴 빌드 페이지의 이벤트 소스에서 AWS 이벤트 또는 EventBridge 파트너 이벤트가 선택되었는지 확인합니다.
6. 샘플 이벤트 유형에서 내 이벤트 유형 입력을 선택합니다.
7. 에서 복사하여 붙여넣습니다샘플 이벤트.
8. 생성 방법 에서 사용자 지정 패턴 을 선택합니다. 이벤트 패턴 섹션에서 이벤트 소스JSON가 `aws:one`이고 필수 세부 정보 유형이 인 를 추가한 다음 다음을 선택합니다.
9. 대상(들) 선택 페이지에서 Lambda 함수, SQS 대기열 또는 SNS 주제가 포함된 원하는 대상을 선택합니다. 대상 구성에 대한 자세한 내용은 Amazon EventBridge 대상 을 참조하세요.
10. 선택적으로 태그를 구성할 수 있습니다.
11. 검토 및 생성 페이지에서 규칙 생성을 선택합니다. 규칙 구성에 대한 자세한 내용은 EventBridge 사용 설명서의 EventBridge 규칙을 참조하세요.

디바이스 상태 변경 이벤트 유형

디바이스 상태 변경 이벤트는 에서 생성됩니다JSON. 각 이벤트 유형에 대해 규칙에 구성된 대로 선택한 대상으로 JSON blob이 전송됩니다. 다음 세부 정보 유형을 사용할 수 있습니다.

디바이스 상태 상태가 정상으로 변경됨

디바이스가 모든 상태 확인을 통과했습니다.

디바이스 상태 상태가 위험으로 변경됨

디바이스가 하나 이상의 상태 확인에 실패했습니다.

디바이스 연결이 오프라인으로 변경됨

디바이스가 인터넷에 연결되어 있지 않습니다.

디바이스 연결이 온라인으로 변경됨

디바이스가 인터넷에 연결되어 있습니다.

resources

Device Status Change 이벤트가 게시된 deviceInstance arn 목록을 포함합니다.

metadata

siteName

- 이 있는 사이트의 이름 deviceInstance 입니다.

siteArn

- 이 있는 사이트의 Arn deviceInstance 입니다.

data

currentConnectivity

- deviceInstance 가 인터넷에 연결되었는지 또는 인터넷에서 연결 해제되었는지 여부를 나타냅니다.
- 가능한 값: CONNECTED, DISCONNECTED

previousConnectivity

- 이벤트 전에 가 인터넷에 연결되었는지 또는 인터넷에서 연결 해제 deviceInstance 되었는지 여부를 나타냅니다.
- 가능한 값: CONNECTED, DISCONNECTED

currentHealthStatus

- 이 모든 상태 확인을 통과 deviceInstance 했는지 여부를 나타냅니다.
- 가능한 값: HEALTHY, CRITICAL

previousHealthStatus

- 가 마지막으로 검사했을 때 모든 상태 검사를 deviceInstance 통과했는지 여부를 나타냅니다.
- 가능한 값: HEALTHY, CRITICAL

assetTagId

- 와 연결된 디바이스 assetTagId 의 . deviceInstance

deviceInstanceName

- 디바이스 상태 이벤트 deviceInstance 가 게시된 의 이름입니다.

사용자 프로필 이벤트 유형

사용자 프로필 관련 이벤트 세부 정보 유형은 다음과 같습니다.

새 등록 성공

사용자가 성공적으로 등록한 경우.

새로운 등록 취소 성공

사용자가 성공적으로 등록을 취소한 경우.

등록 실패

사용자가 등록하지 못한 경우.

등록 취소 실패

사용자가 등록을 취소하지 못한 경우.

성공적인 인식

사용자가 인증을 위해 손바닥을 스캔하는 경우.

인식 실패

손바닥 스캔 인식에 실패한 경우.

resources

사용자 프로필 이벤트가 게시된 사용자 프로필 arn의 목록을 포함합니다.

data

accountId

- 요청을 시작한 디바이스의 관련 AWS 계정입니다.

requestSource

- 요청을 시작한 디바이스 deviceInstanceId 의 입니다.

createdTimestamp

- 이벤트가 생성되는 시간입니다.

userStatus

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

associatedId

- 배지 ID와 같은 사용자의 연결된 ID입니다.

reason

- 이 값은 실패한 이벤트에 대해 표시됩니다. 여기에는 이벤트가 실패한 이유가 포함되어 있습니다.

샘플 이벤트

다음 예제에서는 Amazon One Enterprise에 대한 이벤트를 보여줍니다.

주제

디바이스 상태 상태가 정상으로 변경됨

디바이스가 모든 상태를 전달했고 디바이스 인스턴스 상태 상태가 CRITICAL 상태 HEALTHY 상태에서 로 변경되었습니다.


```
{
    "version": "0",
    "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
    "detail-type": "Device Health Status Changed To Healthy",
    "source": "aws.one",
    "account": "123456789012",
    "time": "2022-10-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
    "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "HEALTHY",
      "previousHealthStatus": "CRITICAL",
```

```
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

디바이스 상태 상태가 위험으로 변경됨

디바이스가 하나 이상의 상태 확인에 실패했고 디바이스 인스턴스 상태 상태가 CRITICAL에서 로 변경되었습니다HEALTHY.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Health Status Changed To Critical",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "CRITICAL",
      "previousHealthStatus": "HEALTHY",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

디바이스 연결이 온라인으로 변경됨

디바이스가 인터넷에 연결되고 디바이스 인스턴스의 연결 상태가 CONNECTED에서 로 변경되었습니다DISCONNECTED.

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

```
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Online",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "CONNECTED",
      "previousConnectivity": "DISCONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

디바이스 연결이 오프라인으로 변경됨

디바이스가 인터넷에 연결되어 있지 않으며 디바이스 인스턴스의 연결 상태가 DISCONNECTED에서로 변경되었습니다CONNECTED.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
```

```
      "currentConnectivity": "DISCONNECTED",
      "previousConnectivity": "CONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

새로 등록 성공

사용자가 성공적으로 등록되었을 때의 이벤트입니다.

```
{
    "version": "0",
    "id": "aebc9c86-f20e-75db-caaa-63bf14926f59",
    "detail-type": "New Successful Enrollment",
    "source": "aws.one",
    "account": "679792848029",
    "time": "2023-11-22T02:55:17Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:one:us-east-1:679792848029:user"
    ],
    "detail": {
        "version": "1.0.0",
        "data": {
            "accountId": "679792848029",
            "enrollmentSource": "QfUuUnFqs5accJ",
            "createdTimestamp": "2023-11-22T02:55:17Z",
            "userStatus": "ACTIVE",
            "associatedIds": "[{\"associatedIdType\":\"badge\",\"associatedIdValue\":
\"1111358294500\"}]",
        }
    }
}
```

를 사용하여 Amazon One Enterprise API 통화 로깅 AWS CloudTrail

Amazon One Enterprise는 Amazon One Enterprise에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail Amazon One

Enterprise에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Amazon One Enterprise 콘솔에서의 통화와 Amazon One Enterprise API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 Amazon One Enterprise용 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Amazon One Enterprise에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

아마존 원 엔터프라이즈 정보 CloudTrail

CloudTrail 계정을 생성할 AWS 계정 때 활성화됩니다. Amazon One Enterprise에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 내 사이트에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

Amazon One Enterprise의 이벤트를 AWS 계정포함하여 귀하의 이벤트에 대한 지속적인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 다음에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Amazon One Enterprise 작업은 에 의해 CloudTrail 기록되고 문서화됩니다. Amazon One Enterprise에 사용되는 작업, 리소스 및 조건 키 예를 들어`ListSites`, 에 대한 호출 `RebootDevice` 및 `DeleteDeviceInstance` 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 보안 인증을 사용하여 요청이 생성되었는지 여부.

- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity요소를 참조하십시오.

Amazon One 엔터프라이즈 로그 파일 항목의 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateSite` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
    "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 Enterprise 문제 해결

Amazon One 디바이스 또는 Amazon One 디바이스 중 하나에 문제가 있는 경우 다음 제안을 사용하여 문제를 해결합니다. 그래도 문제가 지속되면 AWS Support에 문의하세요.

주제

Amazon One Enterprise 자격 증명 및 액세스 문제 해결

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

주제

Amazon One Enterprise에서 작업을 수행할 권한이 없음

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `one:`*`GetWidget`* 권한이 없는 경우에 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 문의하십시오. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Amazon One Enterprise 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(ACLs)을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Amazon One Enterprise가 이러한 기능을 지원하는지 알아보려면 섹션을 참조하세요Amazon One Enterprise의 작동 방식 IAM.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유 AWS 계정 한 다른의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 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.
- 교차 계정 액세스를 위한 역할 및 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.

Amazon One 콘솔 문제 해결

Amazon One 콘솔 또는 Amazon One 디바이스 중 하나에 문제가 있는 경우 다음 제안을 사용하여 문제를 해결합니다. 그래도 문제가 지속되면 AWS Support에 문의하세요.

주제

- 사이트를 생성할 수 없음
- 디바이스 인스턴스를 생성할 수 없음
- 구성 템플릿을 생성할 수 없습니다.
- 활성화 QR 코드를 생성할 수 없음

사이트를 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공합니다.

- 문제가 지속되면 AWS Support에 문의하세요.

디바이스 인스턴스를 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공합니다.
- 문제가 지속되면 AWS Support에 문의하세요.

구성 템플릿을 생성할 수 없습니다.

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공합니다.
- 문제가 지속되면 AWS Support에 문의하세요.

활성화 QR 코드를 생성할 수 없음

- Amazon One Console 관리자에게 문의하여 액세스 권한을 제공합니다.
- 문제가 지속되면 AWS Support에 문의하세요.

Amazon One 디바이스 문제 해결

Amazon One 콘솔 또는 Amazon One 디바이스 중 하나에 문제가 있는 경우 다음 제안을 사용하여 문제를 해결합니다. 그래도 문제가 지속되면 AWS Support에 문의하세요.

주제

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 뒷면에 단단히 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 허브의 플러그를 뽑은 다음 다시 연결합니다.
- 문제가 지속되면 AWS Support에 문의하세요.

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.

시스템 오류

내부 오류로 인해 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

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

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 유효한 QR 코드 하나만 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 문의하십시오.
- 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 문의하십시오.

ZIP 코드가 일치하지 않음

이는 디바이스에 대해 구성된 코드와 다른 ZIP 코드를 입력할 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- 다시 시도를 선택하여 ZIP 코드 화면으로 돌아갑니다.
- 올바른 사이트 ZIP 코드가 있는지 확인합니다.
- 문제가 지속되면 관리자에게 문의하여 AWS 콘솔에서 사이트 ZIP 코드를 확인합니다.

게이트웨이 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 허브의 플러그를 뽑고 다시 연결합니다.
- 문제가 지속되면 AWS Support에 문의하세요.

추가 활동이 없는 디바이스 화면의 Amazon 로고

이 문제를 해결하려면 다음을 수행합니다.

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

일시적으로 사용할 수 없음

이 문제를 해결하려면 다음을 수행합니다.

- 호스트 디바이스/시스템과의 USB 연결이 안전한지 확인합니다.
- USB 허브로 들어가는 모든 케이블을 분리하고 다시 연결합니다.

- 문제가 지속되면 AWS Support에 문의하세요.

디바이스 잠김

보안상의 이유로 변조 이벤트가 발생할 경우 Amazon One 디바이스가 잠깁니다.

이 문제를 해결하려면 다음을 수행합니다.

- AWS Support에 문의하십시오.

종료 시 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 문의하세요.

일시적으로 서비스 중단

이는 Amazon One에서 디바이스를 서비스 중단 상태로 이동했을 때 발생합니다.

이 문제를 해결하려면 다음을 수행합니다.

- AWS Support에 문의하십시오.

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 줄무늬 및 스머지가 없는지 다시 확인합니다.
- 고객의 손바닥에 붕대, 소매, 심각한 먼지/오일과 같은 오클루전이 없는지 확인합니다.
- 문제가 지속되고 디바이스가 어떠한 야자수도 읽지 않는 경우 AWS Support에 문의하세요.

Palm이 인식되지 않음

이 문제를 해결하려면 다음을 수행합니다.

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

장기 비활성으로 인해 디바이스가 잠김

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

다음을 수행하여 디바이스를 잠금 해제합니다.

1. 페이지 상단의 오류 배너에서 수정을 선택합니다.
2. 디바이스가 여전히 활성화 사이트에 있는 경우 예를 선택하고 디바이스가이 사이트에 있는 경우를 선택합니다.
3. 디바이스가 다른 사이트에 있는 경우 아니요를 선택하면 디바이스가 다른 사이트에 있는 것입니다. 아니요를 선택하면 디바이스가 비활성화됩니다. 새 사이트에서 디바이스를 활성화합니다.

Amazon One Enterprise 사용 설명서의 문서 기록

다음 표에서는 Amazon One Enterprise의 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
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	장: Amazon One Enterprise 설정 추가	2024년 10월 10일
업데이트	주제 추가: Amazon One Enterprise 디바이스 유지 관리 및 청소	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: 벽 장착형 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.