Benutzerhandbuch

Amazon One

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon One: Benutzerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon One Enterprise? ... 1
Amazon One-Gerät ... 1
Amazon One Enterprise-Konsole ... 2
Kauf von Amazon One-Geräten ... 3
Preise für Amazon One Enterprise ... 3
So funktioniert Amazon One ... 4
Amazon One-Arbeitsablauf ... 4
Wichtige Begriffe von Amazon One ... 5
Einrichtung der Amazon One-Konsole ... 6
Registrieren Sie sich für ein AWS-Konto. ... 6
Erstellen eines Benutzers mit Administratorzugriff ... 7
Sicherung Ihres AWS-Kontos ... 7
Einen Benutzer mit Administratorzugriff erstellen ... 8
Als Administrator anmelden ... 8
Zugriff weiteren Benutzern zuweisen ... 8
Amazon One-Benutzer hinzufügen ... 9
Erstellen einer Seite ... 12
Geräteinstanzen erstellen ... 12
Erstellen Sie eine Konfigurationsvorlage ... 13
Konfigurieren Sie eine Geräte-Instance für die Aktivierung ... 14
Amazon One installieren und aktivieren ... 17
Anforderungen verstehen ... 17
Unterstützte Standards ... 17
Netzwerkanforderung ... 18
Leistungsbedarf ... 18
Installationskonzepte verstehen ... 18
Installation von Amazon One Pedestal ... 19
Installation des an der Wand montierbaren Amazon One-Geräts ... 21
Amazon One Device I/O Hub für sicheren Zugriff installieren ... 33
Amazon One-Gerät aktivieren ... 44
Benutzer registrieren und eingeben ... 46
Eine Endpunktrichtlinie erstellen ... 46
Authentifizierung für die Einreise ... 46
Verwalten von Benutzern ... 48

Eingeschriebene Benutzer anzeigen ... 48
Löschen registrierter Benutzer und ihrer biometrischen Daten ... 48
Amazon One-Geräte verwalten ... 50
Wartung und Reinigung von Amazon One-Geräten ... 50
Um das Amazon One-Gerät zu reinigen ... 51
Verwaltung der Website ... 51
Der Name der Website wird geändert ... 52
Die Adresse der Website wird aktualisiert ... 52
Verwaltung von Geräteinstanzen ... 53
Status der Geräteinstanz anzeigen ... 53
Ein Amazon One-Gerät neu starten ... 53
Aktualisierung der Amazon One-Gerätekonfigurationen ... 54
Aktualisierung der Wi-Fi-Anmeldeinformationen ... 54
Geräteinstanzen deaktivieren ... 55
Sicherheit ... 56
Datenschutz ... 56
Um die Standardverschlüsselung von Daten im Ruhezustand zu verwenden ... 58
Verschlüsseln von Daten während der Übertragung. ... 58
Identity and Access Management ... 58
Zielgruppe ... 59
Authentifizierung mit Identitäten ... 59
Verwalten des Zugriffs mit Richtlinien ... 63
So arbeitet Amazon One Enterprise mit IAM ... 66
Beispiele für identitätsbasierte Richtlinien ... 74
AWS verwaltete Richtlinien ... 83
Aktionen, Ressourcen und Bedingungsschlüssel ... 87
Aktionen ... 87
Ressourcentypen ... 92
Bedingungsschlüssel ... 92
Compliance-Validierung ... 93
Überwachen ... 95
Überwachung von Ereignissen ... 95
Abonnieren Sie Amazon One Enterprise-Veranstaltungen ... 95
Ereignistypen zur Änderung des Gerätestatus ... 97
Ereignistypen für Benutzerprofile ... 98
Beispielereignisse ... 100

Der Status des Geräts wurde auf „Gesund“ geändert ... 100
Der Gesundheitsstatus des Geräts wurde auf Kritisch geändert ... 101
Die Gerätekonnektivität wurde auf „Online“ geändert ... 101
Die Gerätekonnektivität wurde auf offline geändert ... 102
CloudTrail protokolliert ... 103
Informationen zu Amazon One Enterprise in CloudTrail ... 103
Grundlegendes zu Amazon One Enterprise-Protokolldateieinträgen ... 104
Fehlerbehebung ... 107
Fehlerbehebung für -Identität und -Zugriff ... 107
Ich bin nicht berechtigt, eine Aktion in Amazon One durchzuführen ... 107
Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon One-Ressourcen ermöglichen ... 108
Fehlerbehebung bei der Amazon One Console ... 108
Ich kann keine Site erstellen ... 109
Ich kann keine Geräte-Instance erstellen ... 109
Ich kann keine Konfigurationsvorlage erstellen ... 109
Ich kann keinen Aktivierungs-QR-Code erstellen ... 109
Fehlerbehebung beim Amazon One-Gerät ... 109
Leerer Bildschirm ... 110
Ich kann keine Verbindung zu WLAN oder Netzwerk herstellen ... 111
Ein Gerät mit aktiven Warnmeldungen neu starten ... 111
Systemfehler ... 111
Der QR-Code wird nicht erkannt ... 112
Der QR-Code kann nicht gelesen werden ... 112
Es wurden mehrere QR-Codes erkannt ... 112
Die Geräteinstanz ist nicht vorhanden ... 112
Die Seite wurde nicht gefunden ... 113
Die Postleitzahl stimmt nicht überein ... 113
Gateway hat das Zeitlimit überschritten ... 113
Ich kann das Gerät nicht konfigurieren ... 113
Das Gerät wurde mit Fehlermeldung und Fehlercode neu gestartet ... 114
Amazon-Logo auf dem Gerätebildschirm ohne weitere Aktivität ... 114
Vorübergehend nicht verfügbar ... 114
Bei uns ist etwas schief gelaufen ... 114
Vorübergehend außer Betrieb ... 115
Das Amazon One-Gerät ist physisch beschädigt ... 115

Palm kann nicht gelesen werden 115
Palm wurde nicht erkannt 115
Das Gerät wurde aufgrund längerer Inaktivität gesperrt 116
Das Gerät wurde aufgrund eines Manipulationsereignisses gesperrt 117
Dokumentverlauf 118
..... cxx

Was ist Amazon One Enterprise?

Amazon One Enterprise ist ein neuer Palm-basierter Authentifizierungsservice, der Mitarbeitern sicheren Zugang zu Gebäuden und Unternehmensressourcen bietet, ohne dass Ausweise oder Passcodes verwendet werden müssen. PINs

Themen

- Amazon One-Gerät
- Amazon One Enterprise-Konsole
- Kauf von Amazon One-Geräten
- Preise für Amazon One Enterprise

Amazon One-Gerät

Das Amazon One-Gerät wurde für Amazon One Enterprise entwickelt, einen sicheren, palmenbasierten Identitätsdienst für die Zugriffskontrolle von Unternehmen. Beachten Sie die folgenden Gerätespezifikationen:

- Benutzereingaben — Palm Biometrics, QR-Code-Abgleich
- Host-Schnittstelle — Wi-Fi (2.4 GHz und 5 GHz), Ethernet, 2 x USB Typ A, 1 x USB Typ B
- Benutzerfeedback — 5,5-Zoll-Touchscreen, Lightring, Lautsprecher, Kopfhörer
- Protokoll für die physische Zugangskontrolle — OSDP und Wiegand
- Stromversorgung — POE, AC/DC-Adapter mit 110/220 VAC-Eingang im Lieferumfang enthalten, 30 W bei 15 V
- Sicherheit — Manipulationsschalter
- Abmessung (HxWxD mm) — 86 x 85 x 256

Amazon One Enterprise-Konsole

Amazon One Enterprise umfasst eine Konsole, die auf folgende Weise verwendet werden kann:

- Ein IT- oder Facility Manager verwendet Amazon One Enterprise, um eine Site zu erstellen und zu verwalten. Die Site ähnelt einem physischen Standort für die Aufgaben, die das Team bei der Überwachung und Verwaltung von Amazon One Enterprise-Geräten und Benutzerprofilen ausführt. Zu den Aufgaben des IT- oder Facility-Managers gehören:
  - Erstellen einer Site, die alle Amazon One-Geräte-Instances an einem physischen Standort enthält
  - Hinzufügen eines Admin-Benutzers zur Verwaltung der Site und eines Installer-Benutzers für den Zugriff auf Aktivierungs-QR-Codes

- Ein Administrator verwendet Amazon One Enterprise, um Geräte-Instances zu erstellen und Amazon One-Geräte zu verwalten. Zu den Aufgaben des Administrators gehören:
  - Eine Geräteinstanz unter einer Site erstellen
  - Erstellen einer Konfigurationsvorlage, die auf eine Geräteinstanz angewendet werden soll
  - Überwachung des Gerätezustands und Aktualisierung der Gerätekonfigurationen
  - Benutzerregistrierungen stornieren
- Ein Installateur verwendet Amazon One Enterprise, um auf Aktivierungs-QR-Codes zuzugreifen und Geräte zu aktivieren. Zu den Aufgaben des Installateurs gehören:
  - Zugreifen auf einen Aktivierungs-QR-Code auf der Konsole
  - Auswahl eines QR-Codes, der der zu aktivierenden Geräteinstanz entspricht
  - Scannen des ausgewählten QR-Codes bei installiertem Amazon One-Gerät

Kauf von Amazon One-Geräten

Kontaktieren Sie uns, um mehr über Amazon One Enterprise zu erfahren. Ein Mitglied des Business Development-Teams wird sich mit Ihnen in Verbindung setzen, um Ihnen weitere Informationen zu unserem Angebot, einschließlich der Preise, mitzuteilen und alle Ihre Fragen zu beantworten.

Preise für Amazon One Enterprise

Kontaktieren Sie uns, um mehr über die Preise von Amazon One Enterprise zu erfahren.

So funktioniert Amazon One

Amazon One ist ein Cloud-basierter biometrischer Dienst, der ein Amazon One-Gerät verwendet, um einen Benutzer anhand seiner Handflächenbiometrie zu authentifizieren. Sie können Amazon One-Geräte bestellen, indem Sie uns kontaktieren.

Nach der Installation des Amazon One-Geräts können Sie Ihre Geräte mit Ihrem AWS-Konto auf der Amazon One Console und der Authentifizierungsanwendung aktivieren und registrieren. Sie können die biometrischen Profile registrierter Benutzer einsehen. Bei Bedarf können Sie ihre Registrierung stornieren und ihre biometrischen Daten löschen.

Die Amazon One Console dient als zentraler Knotenpunkt für die Verwaltung betrieblicher Aktivitäten wie die Verfolgung von Geräten und die Anzeige monatlicher Rechnungen. Benutzer können sich registrieren, indem sie ihre Handflächen an überwachten Registrierungsstationen vor Ort scannen. Nach der Registrierung können Benutzer sichere Standorte problemlos betreten oder verlassen, indem sie ihre Handfläche über ein Amazon One-fähiges Gerät bewegen.

Themen

- Amazon One-Arbeitsablauf
- Wichtige Begriffe von Amazon One

Amazon One-Arbeitsablauf

Im Folgenden wird der grundlegende Arbeitsablauf von Amazon One beschrieben:

1. Kaufen und installieren Sie die Amazon One-Geräte, indem Sie uns kontaktieren.
2. Aktivieren Sie Amazon One nach der Installation des Geräts.
3. Melden Sie sich bei Ihrem Amazon One-Konto an.
4. Konfigurieren Sie Benutzerregistrierungs- und Eingabegeräte.
5. Registrieren Sie die Handflächen Ihrer Mitarbeiter.
6. Verwenden Sie Verwaltungs- und Überwachungsfunktionen, um den Zustand der Geräte sicherzustellen, Konfigurationen auf dem neuesten Stand zu halten und Benutzeranmeldungen nachzuverfolgen, um einen umfassenden Überblick zu erhalten.

Wichtige Begriffe von Amazon One

Dies sind die wichtigsten Begriffe für Amazon One:

- Standort — Der Kunde verwaltete physische Gebäude, in denen der Kunde Amazon One-Geräte installiert. Ein Standort muss die Anlagen-, Netzwerk- und Stromversorgungsanforderungen für Ihre Amazon One-Geräte erfüllen.
- Gerät — Ein biometrisches Handflächenscanning-Gerät von Amazon One zur Authentifizierung.
- Geräteinstanz — Eine logische Darstellung eines Geräts mit Konfigurationen. Die Verwendung von Geräte-Instances ermöglicht den Austausch von Amazon One-Geräten, wobei die zuvor festgelegten Konfigurationen und Namen automatisch übernommen werden. Eine Geräte-Instance hat einen benutzerdefinierten Namen (gemeinsame Benennungskonvention mit Ihrer Zugriffskontrollsoftware) und eine Reihe von Kommunikationskonfigurationen. Geräteinstanzen haben drei Hauptstatus:
  - Benötigt Konfiguration
  - Bereit für die Aktivierung
  - Aktiv
- Konfigurationsvorlage — Ein umfassender Satz von Konfigurationen, die auf eine Geräteinstanz angewendet werden.

Einrichtung der Amazon One-Konsole

In diesem Kapitel werden die grundlegenden Schritte für den Einstieg in die Amazon One-Konsole erläutert.

Einrichtung einer Site, Geräte-Instances und Konfigurationsvorlagen — Gehen Sie wie folgt vor, um ein Framework für das Hinzufügen eines physischen Standorts für Ihre Amazon One-Geräte zu erstellen und diese anschließend mithilfe der Amazon One Enterprise-Konsole zu konfigurieren und zu verwalten. Sie werden diesen Prozess nur gelegentlich oder sogar nur einmal verwenden, abhängig von der Anzahl der Standorte, Geräte-Instances und Ihren Konfigurationsvorlagen.

Themen

- Registrieren Sie sich für ein AWS-Konto.
- Erstellen eines Benutzers mit Administratorzugriff
- Amazon One-Benutzer hinzufügen
- Erstellen einer Seite
- Geräteinstanzen erstellen
- Erstellen Sie eine Konfigurationsvorlage
- Konfigurieren Sie eine Geräte-Instance für die Aktivierung

Registrieren Sie sich für ein AWS-Konto.

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos durch.

Registrieren Sie sich für ein AWS-Konto wie folgt:

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für ein AWS-Konto registrieren, wird ein Root-Benutzer für das AWS-Konto erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und -Ressourcen des Kontos. Aus

Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Registrierung abgeschlossen ist. Unter Mein Konto können Sie jederzeit Ihre aktuellen Kontoaktivitäten einsehen https://aws.amazon.com/ und Ihr Konto verwalten

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für ein AWS-Konto angemeldet haben, sichern Sie den Root-Benutzer Ihres AWS-Kontos, aktivieren Sie AWS IAM Identity Center und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Themen

- Sicherung Ihres AWS-Kontos
- Einen Benutzer mit Administratorzugriff erstellen
- Als Administrator anmelden
- Zugriff weiteren Benutzern zuweisen

Sicherung Ihres AWS-Kontos

Nachdem Sie sich bei Ihrem Amazon One-Konto angemeldet haben, sichern Sie Ihr Konto.

Um den Root-Benutzer Ihres AWS-Kontos zu sichern

1. Melden Sie sich als Kontoinhaber bei der AWS-Managementkonsole an, indem Sie Root-Benutzer auswählen und die E-Mail-Adresse Ihres AWS-Kontos eingeben.
2. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Als Root-Benutzer anmelden im AWS-Anmelde-Benutzerhandbuch.
3. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen dazu finden Sie unter Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Kontos (Konsole) im IAM-Benutzerhandbuch.

Einen Benutzer mit Administratorzugriff erstellen

Nachdem Sie Ihr Amazon One-Konto gesichert haben, erstellen Sie einen Benutzer mit Administratorzugriff.

So erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Enabling AWS IAM Identity Center im AWS IAM Identity Center-Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung des IAM Identity Center-Verzeichnisses als Identitätsquelle finden Sie unter Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren im AWS IAM Identity Center-Benutzerhandbuch.

Als Administrator anmelden

Nachdem Sie einen Benutzer mit Administratorzugriff erstellt haben, melden Sie sich als Administrator an.

Um sich als Benutzer mit Administratorzugriff anzumelden

- Melden Sie sich mit Ihrem IAM Identity Center-Benutzer an und verwenden Sie dabei die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM Identity Center-Benutzer erstellt haben.

  Hilfestellung zur Anmeldung mit einem IAM-Identity-Center-Benutzer finden Sie unter Anmelden beim AWS-Zugangsportal im Benutzerhandbuch zur AWS-Anmeldung.

Zugriff weiteren Benutzern zuweisen

Nachdem Sie sich als Administrator angemeldet haben, können Sie weiteren Benutzern Zugriff zuweisen.

Um weiteren Benutzern Zugriff zuzuweisen

- Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

  Anweisungen finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center-Benutzerhandbuch.

Amazon One-Benutzer hinzufügen

Neben Administratorbenutzern können Sie auch Benutzer hinzufügen, denen Administratorrechte fehlen. Bei diesen Benutzern kann es sich beispielsweise um Installateure handeln, die nur auf die Amazon One-Konsole zugreifen, um QR-Codes zur Geräteaktivierung für die Aktivierung von Amazon One-Geräten abzurufen.

So fügen Sie einen Amazon One-Benutzer hinzu

1. Folgen Sie dem für Ihren Benutzertyp geeigneten Anmeldeverfahren, wie unter So melden Sie sich an AWS im AWS-Anmeldung Benutzerhandbuch beschrieben.
2. Wählen Sie im Navigationsbereich Benutzer und dann Benutzer hinzufügen aus.
3. Geben Sie auf der Seite Specify user details (Benutzerdetails angeben) unter User details (Benutzerdetails) in das Feld User name (Benutzername) den Namen für den neuen Benutzer ein. Dies ist der Anmeldename für AWS.

   > **Note**
   >
   > Die Anzahl und Größe der IAM-Ressourcen in einem AWS-Konto sind begrenzt. Weitere Informationen finden Sie unter IAM- und AWS STS STS-Kontingente. Benutzernamen können eine Kombination aus bis zu 64 Buchstaben, Ziffern und den folgenden Zeichen sein: Plus (+), Gleichheit (=), Komma (,), Punkt (.), At-Zeichen (@), Unterstrich (_) und Bindestrich (-). Namen müssen innerhalb eines Kontos eindeutig sein. Es wird hierbei nicht zwischen Groß- und Kleinschreibung unterschieden. So können Sie beispielsweise keine zwei Gruppen mit Namen TESTBENUTZER und testbenutzer erstellen. Wenn ein Benutzername in einer Richtlinie oder als Teil eines ARN verwendet wird, ist die Groß-/Kleinschreibung des Namens zu beachten. Wenn Kunden in der Konsole ein Benutzername angezeigt wird, beispielsweise während des Anmeldevorgangs, wird die Groß-/Kleinschreibung des Benutzernamens nicht beachtet.

4. Sie werden gefragt, ob Sie einer Person Zugriff auf die Konsole gewähren. Wählen Sie Benutzerzugriff auf bereitstellen aus — optional. AWS Management Console
5. Wählen Sie Ich möchte einen IAM-Benutzer erstellen aus.
6. Wählen Sie für Console password (Konsolenpasswort) eine der nachstehenden Optionen aus:
   - Automatisch generiertes Passwort — Der Benutzer erhält ein zufällig generiertes Passwort, das den Passwortrichtlinien für das Konto entspricht. Sie können das Passwort auf der Seite Retrieve passwort (Passwort abrufen) ansehen oder herunterladen.
   - Benutzerdefiniertes Passwort — Dem Benutzer wird das Passwort zugewiesen, das Sie in das Feld eingeben.
7. (Optional) Standardmäßig ist die Option Benutzer müssen bei der nächsten Anmeldung ein neues Passwort erstellen (empfohlen) ausgewählt, um sicherzustellen, dass der Benutzer sein Passwort bei der ersten Anmeldung ändern muss.

   > **Note**
   >
   > Wenn ein Administrator die Kontopasswortrichtlinie Allow users to change their own password (Benutzer dürfen ihr eigenes Kennwort ändern) aktiviert hat, bewirkt dieses Kontrollkästchen nichts. Andernfalls wird automatisch eine verwaltete AWS -Richtlinie mit dem Namen `IAMUserChangePassword` an die neuen Benutzer angehängt. Die Richtlinie gewährt ihnen die Erlaubnis, ihre eigenen Passwörter zu ändern.

8. Klicken Sie auf Weiter.
9. Wählen Sie auf der Seite Berechtigungen festlegen die Option Richtlinien direkt anhängen aus.
10. Wählen Sie die Richtlinien aus, die Sie dem Benutzer zuordnen möchten.
    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

    > **Note**
    >
    > AmazonOneEnterpriseInstallerAccess Die verwaltete Richtlinie gewährt Benutzern nur in der Amazon One Enterprise-Konsole Zugriff auf Aktivierungs-QR-Codes. Diese Richtlinie ist ideal für Unternehmen, die einen Drittanbieter mit der Installation von Amazon One-Geräten beauftragen.

11. Klicken Sie auf Weiter.
12. (Optional) Auf der Seite Review and create (Überprüfen und erstellen) wählen Sie unter Tags (Tags) die Option Add new tag (Neues Tag hinzufügen), um dem Benutzer Metadaten hinzuzufügen, indem Sie Tags als Schlüssel-Wert-Paare anhängen. Weitere Informationen dazu, wie Sie verwenden können von Tags mit IAM finden Sie unter Tagging von Amazon RDSIAM-Ressourcen.
13. Überprüfen Sie alle Entscheidungen, die Sie bis zu diesem Zeitpunkt getroffen haben. Wenn Sie bereit sind, fortzufahren, wählen Sie Create user (Benutzer erstellen) aus.
14. Rufen Sie auf der Seite Retrieve password (Passwort abrufen) das dem Benutzer zugewiesene Passwort ab:
    - Wählen Sie neben dem Passwort die Option Show (Anzeigen) aus, um das Passwort des Benutzers anzuzeigen, sodass Sie es manuell aufzeichnen können.
    - Wählen Sie „.csv herunterladen“, um die Anmeldeinformationen des Benutzers als CSV-Datei herunterzuladen, die Sie an einem sicheren Ort speichern können.
15. Wählen Sie Email sign-in instructions (E-Mail-Anmeldeanweisungen) aus. Dadurch wird Ihr lokaler E-Mail-Client aufgerufen und sie können den E-Mail-Entwurf anpassen und an den Benutzer senden. Die E-Mail-Vorlage enthält die folgenden Details für jeden Benutzer:
    - Benutzername
    - URL der Anmelde-Website des Kontos. Verwenden Sie das folgende Beispiel und ersetzen Sie dabei die richtige Konto-ID-Nummer oder den Konto-Alias:

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

> **Important**
>
> Das Passwort des Benutzers ist nicht in der generierten E-Mail enthalten. Sie müssen dem Benutzer das Passwort in einer Form zukommen lassen, die den Sicherheitsrichtlinien Ihres Unternehmens entspricht.

Erstellen einer Seite

Nachdem Sie sich bei angemeldet haben AWS Management Console, können Sie die Amazon One-Konsole verwenden, um Ihre Website zu erstellen.

> **Important**
>
> Amazon One ist nur in der Region USA Ost (Nord-Virginia) verfügbar.

So erstellen Sie einen Standort:

1. Öffnen Sie die Amazon One-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie Gehe zur Übersicht.
3. Wählen Sie im Navigationsbereich Standorte aus.
4. Wählen Sie Websites erstellen aus.
5. Geben Sie unter Site-Informationen für Sitename einen Namen für die Site ein.
6. Geben Sie unter Physische Adresse die Adresse des Standorts ein, an dem Ihre Amazon One-Geräte installiert werden.
7. (Optional) Um der Site ein Tag hinzuzufügen, geben Sie unter Tags ein Schlüssel-Wert-Paar ein und wählen Sie dann Neues Tag hinzufügen aus. Um dieses Tag vor dem Erstellen der Website zu entfernen, wählen Sie Entfernen.
8. Wählen Sie Site erstellen, um die Site zu erstellen.

Geräteinstanzen erstellen

Nachdem Sie in der AWS-Managementkonsole eine Site erstellt haben, können Sie die Amazon One-Konsole verwenden, um Geräte-Instances zu erstellen.

Um eine Geräte-Instance zu erstellen

1. Öffnen Sie die Amazon One-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich Geräte-Instances aus. Vergewissern Sie sich, dass Sie sich auf der Registerkarte „Unaktivierte Instanzen“ befinden.
3. Wählen Sie unter Instanzdetails eine Site aus dem Drop-down-Menü Site aus oder erstellen Sie eine neue Site, indem Sie auf die Schaltfläche Site erstellen klicken.

4. Geben Sie den Namen jeder einzelnen Geräteinstanz manuell ein.
5. (Optional) Um der Geräteinstanz ein Tag hinzuzufügen, geben Sie unter Tags ein Schlüssel-Wert-Paar ein und wählen Sie dann Neues Tag hinzufügen aus. Um dieses Tag zu entfernen, bevor Sie die Geräteinstanz erstellen, wählen Sie Entfernen.
6. Wählen Sie Instanzen erstellen, um die Geräteinstanzen zu erstellen.

> **Note**
>
> Hinweis: Geräteinstanzen müssen konfiguriert werden, bevor die Installation erfolgen kann.

Erstellen Sie eine Konfigurationsvorlage

Nachdem Sie Geräte-Instances erstellt haben, können Sie die Amazon One-Konsole verwenden, um eine Konfigurationsvorlage zu erstellen.

Um eine Konfigurationsvorlage zu erstellen

1. Öffnen Sie die Amazon One-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Konfigurationsvorlagen aus.
3. Wählen Sie Create template (Vorlage erstellen) aus.
4. Geben Sie unter Vorlageninformationen für Vorlagenname einen Namen für die Konfigurationsvorlage ein.
5. Wählen Sie unter Gerätekonfigurationen einen Betriebsmodus aus.

   To configure Enrollment operating mode

   1. (Optional) Geben Sie unter WLAN-Konfiguration Ihre WLAN-Anmeldeinformationen ein.
   2. (Optional) Um der Site ein Tag hinzuzufügen, geben Sie unter Tags ein Schlüssel-Wert-Paar ein und wählen Sie dann Neues Tag hinzufügen aus. Um dieses Tag vor dem Erstellen der Website zu entfernen, wählen Sie Entfernen.
   3. Wählen Sie Konfigurieren aus.

To configure Entry operating mode

1. Geben Sie unter Systemsteuerungseinstellungen die Kommunikationseinstellungen für Amazon One-Geräte an, um mit Ihrem Control Panel zu kommunizieren.
2. Geben Sie unter Einstellungen für das Ausweisformat die Konfigurationseinstellungen ein, die das Layout Ihres Firmenausweisformats festlegen.
3. (Optional) Geben Sie unter WLAN-Konfiguration Ihre WLAN-Anmeldeinformationen ein.
4. (Optional) Um der Site ein Tag hinzuzufügen, geben Sie unter Tags ein Schlüssel-Wert-Paar ein und wählen Sie dann Neues Tag hinzufügen aus. Um dieses Tag vor dem Erstellen der Website zu entfernen, wählen Sie Entfernen.
5. Wählen Sie Konfigurieren aus.

> **Important**
>
> Sie müssen mindestens ein Registrierungsgerät und ein Eingabegerät konfigurieren, um alle Funktionen von Amazon One für den sicheren Zugriff nutzen zu können.

Konfigurieren Sie eine Geräte-Instance für die Aktivierung

Nachdem eine Geräte-Instance erstellt wurde, konfigurieren Sie die Geräte-Instance mit einer zuvor erstellten Konfigurationsvorlage (siheErstellen Sie eine Konfigurationsvorlage), oder Sie können Konfigurationen manuell hinzufügen.

Um eine Geräteinstanz für die Aktivierung zu konfigurieren

1. Öffnen Sie die Amazon One-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich Device Instances aus. Vergewissern Sie sich, dass Sie sich auf der Registerkarte „Unaktivierte Instanzen“ befinden.
3. Wählen Sie eine oder mehrere Instanzen zur Konfiguration aus.
4. Wählen Sie Konfigurieren aus.
5. Wählen Sie unter Gerätekonfigurationen eine der beiden Eingabemethoden aus:

a. Wählen Sie für die Option Vorlage verwenden eine Vorlage aus der Dropdownliste aus. Überprüfen Sie diese importierten Konfigurationsinformationen oder nehmen Sie Änderungen daran vor.

   Informationen zur Option Vorlage erstellen finden Sie unterErstellen Sie eine Konfigurationsvorlage.

b. Wählen Sie für die Option Manuelle Eingabe einen Betriebsmodus aus.

   To configure Enrollment operating mode

   a. (Optional) Geben Sie unter WLAN-Konfiguration einen WLAN-Berechtigungsnachweis ein.
   b. (Optional) Um der Site ein Tag hinzuzufügen, geben Sie unter Tags ein Schlüssel-Wert-Paar ein und wählen Sie dann Neues Tag hinzufügen aus. Um dieses Tag vor dem Erstellen der Website zu entfernen, wählen Sie Entfernen.
   c. Wählen Sie Konfigurieren aus.

   To configure Entry operating mode

   a. Geben Sie unter Systemsteuerungseinstellungen die Kommunikationseinstellungen für Amazon One-Geräte an, um mit Ihrem Control Panel zu kommunizieren.
   b. Geben Sie unter Einstellungen für das Ausweisformat die Konfigurationseinstellungen ein, die das Layout Ihres Firmenausweisformats festlegen.
   c. (Optional) Geben Sie unter WLAN-Konfiguration einen WLAN-Berechtigungsnachweis ein.
   d. (Optional) Um der Site ein Tag hinzuzufügen, geben Sie unter Tags ein Schlüssel-Wert-Paar ein und wählen Sie dann Neues Tag hinzufügen aus. Um dieses Tag vor dem Erstellen der Website zu entfernen, wählen Sie Entfernen.
   e. Wählen Sie Konfigurieren aus.

6. In der Tabelle Unaktivierte Instanzen sollte der Instanzstatus angezeigt

   werden.

7. Stellen Sie sicher, dass Aktivierungs-QR-Codes für die Aktivierung verfügbar sind. Wählen Sie im Navigationsbereich die Option Aktivierungs-QR-Code aus.
8. Wählen Sie aus der Dropdownliste Site auswählen eine Site aus.
9. Überprüfen Sie unter Standortinformationen die Site-Adresse.
10. Unter Aktivierungs-QR-Codes hat jede Geräteinstanz einen entsprechenden QR-Code. Wählen Sie QR-Code abrufen, um die Aktivierungs-QR-Codes anzuzeigen.

> **Important**
>
> Sie müssen mindestens ein Registrierungsgerät und ein Eingabegerät konfigurieren, um alle Funktionen von Amazon One für den sicheren Zugriff nutzen zu können.

Amazon One installieren und aktivieren

Nachdem Sie Ihre Amazon One-Konsole erfolgreich eingerichtet haben, müssen Sie als Nächstes Amazon One-Geräte an Ihrem Standort installieren und sicherstellen, dass sie ordnungsgemäß aktiviert sind. Dieser Prozess umfasst die physische Platzierung der Geräte in bestimmten Bereichen, die Verbindung mit Ihrem Netzwerk und den Abschluss des Aktivierungsprozesses, um eine nahtlose Benutzeridentifikation und Transaktionsfunktionen zu ermöglichen. Nach der Aktivierung sind Ihre Amazon One-Geräte bereit, Ihren Kunden oder Mitarbeitern ein sicheres, berührungsloses Erlebnis zu bieten.

> **Note**
>
> Dieser Abschnitt konzentriert sich auf die Installation und verwendet einen mobilen Browser, um QR-Codes AWS Management Console zur Geräteaktivierung abzurufen.

Themen

- Anforderungen verstehen
- Installationskonzepte verstehen
- Installation von Amazon One Pedestal
- Installation des an der Wand montierbaren Amazon One-Geräts
- Amazon One Device I/O Hub für sicheren Zugriff installieren
- Amazon One-Gerät aktivieren

Anforderungen verstehen

Ein Amazon One-Gerät kann an jedem Unternehmens- oder Geschäftsstandort installiert werden, dessen Türen elektrisch gesteuert werden können.

Anforderung an das Bedienfeld

Amazon One-Geräte können als Lesegerät an die meisten Standard-Zutrittskontrollfelder angeschlossen werden. Amazon One-Geräte unterstützen die folgenden Protokolle:

- OSDP (v1 und v2)

- Wiegand

Netzwerkanforderung

Amazon One-Geräte müssen für den normalen Betrieb immer mit dem Internet verbunden sein. Die Internetverbindung kann entweder über kabelgebundenes Ethernet oder WLAN bereitgestellt werden. Die erforderliche Mindestbandbreite beträgt 10 Mbit/s.

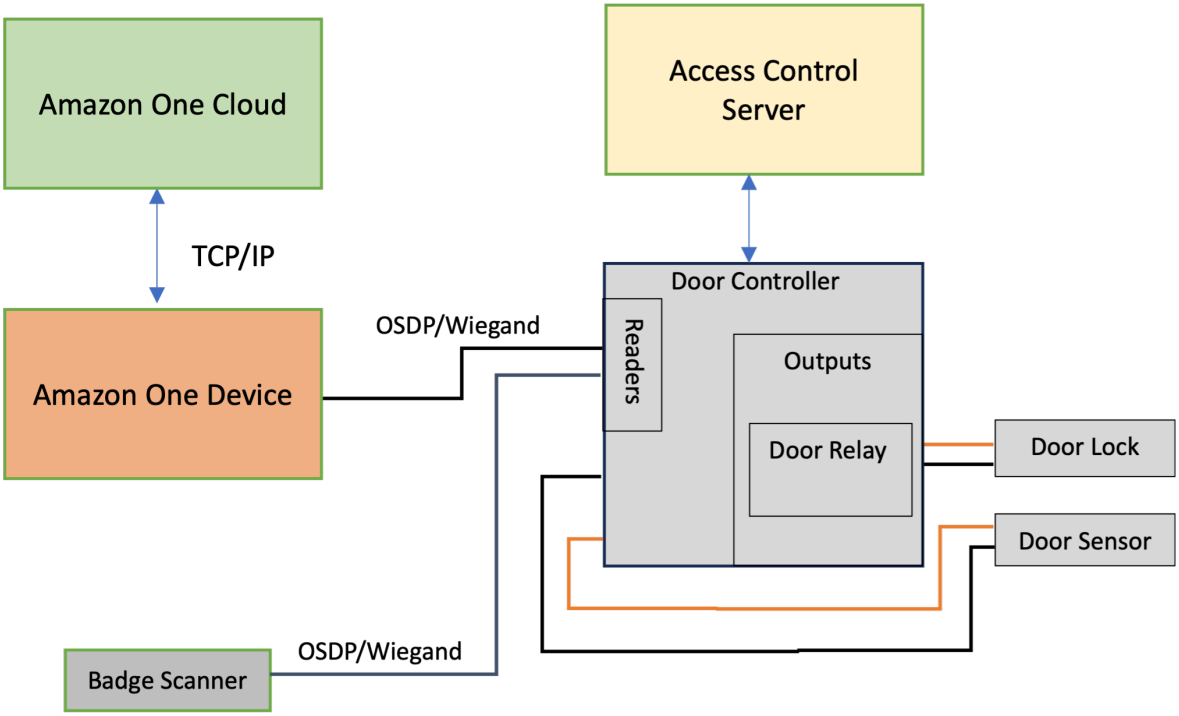
Leistungsbedarf

Amazon One-Geräte können auf zwei Arten mit Strom versorgt werden:

- Mithilfe des im Lieferumfang enthaltenen 120-V-Netzadapters.
- Durch die Verwendung eines PoE+-fähigen Geräts.

Installationskonzepte verstehen

Um den Gebäudezugang ordnungsgemäß zu sichern, empfiehlt Amazon One, das Gerät als Teil einer typischen Zutrittskontrollumgebung zu installieren, wie im folgenden Blockdiagramm beschrieben.



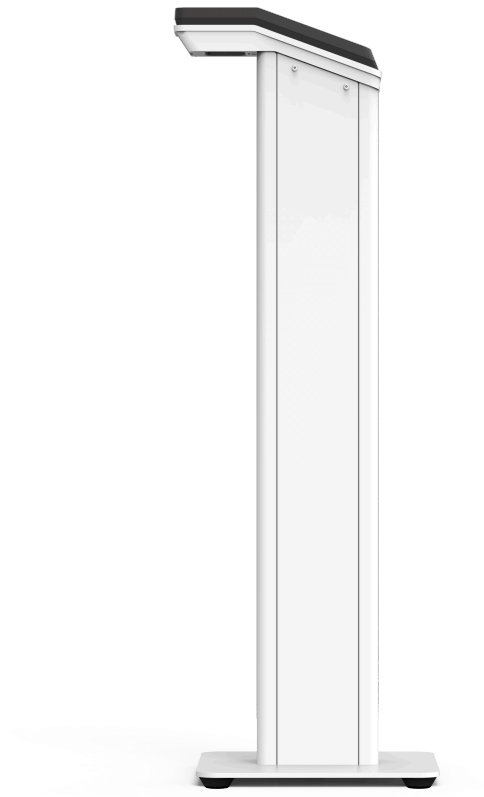
Eine Zutrittskontrollumgebung besteht in der Regel aus den folgenden Komponenten:

- Amazon One-Gerät: Dies ist das Handflächenerkennungsgerät, das eine biometrische Authentifizierung durchführt, um die Person zu identifizieren, die versucht, Zugang zu einem sicheren Bereich des Gebäudes zu erhalten.
- Zugriffskontrollserver: Diese Komponente steuert in der Regel die Zugriffsrechte der Benutzer auf den sicheren Bereich. Die IDs Ausweise von Personen, die Zugang zu dem Bereich haben, werden auf diesem Server gespeichert. Dieser Server zwischenspeichert die für IDs die entsprechenden Türsteuerungen relevanten.
- Türcontroller:
  - Ein Amazon One-Gerät stellt über eine OSDP-Schnittstelle eine Verbindung zum Türsteuerungsserver her.
  - Wenn eine Wiegand-Schnittstelle erforderlich ist, kann ein OSDP-to-Wiegand COTS-Konverter verwendet werden.
  - Nach erfolgreicher Authentifizierung sendet das Amazon One-Gerät die Badge-ID des Benutzers an die Türsteuerung.
  - Die Türsteuerung reagiert mit einer Entscheidung, sodass das Amazon One-Gerät entweder die Meldung „Zugriff gewährt“ oder „Zugriff verweigert“ anzeigen kann.
- Ausweisscanner: Ein Ausweisscanner wird normalerweise verwendet, um RFID-Ausweise zu scannen und die Ausweisnummer an den Zutrittskontrollserver zu senden. Bei Amazon One stellt ein Ausweisscanner eine Verbindung zum Amazon One-Gerät her, sodass Benutzer ihre Ausweise scannen können, wodurch sie ihren Handflächenprofilen zugeordnet werden.

Installation von Amazon One Pedestal

Das Amazon One Pedestal ist eine Schlüsselkomponente des Identifikations- und Transaktionssystems von Amazon One, das darauf ausgelegt ist, Benutzern ein nahtloses, berührungsloses Erlebnis zu bieten. Dieses Gerät verfügt über eine sichere biometrische Authentifizierung. Sie können es an verschiedenen Standorten integrieren, um reibungslose Zugangs- oder Zahlungslösungen bereitzustellen.

Dieser Abschnitt enthält die Standortanforderungen und step-by-step Anweisungen für die Installation von Amazon One Pedestal. Die richtige Vorbereitung und Installation sind entscheidend, um sicherzustellen, dass das System sicher und effizient funktioniert und den Benutzern ein reibungsloses und zuverlässiges Erlebnis bietet.



Voraussetzungen und Vorbereitung für die Installation des Amazon One Pedestal

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass die folgenden Bedingungen für eine sichere und effektive Einrichtung erfüllt sind:

- Stromanforderungen: Wenn Sie POE+ (Power over Ethernet) zur Stromversorgung des Geräts verwenden, stellen Sie sicher, dass die Cat6-Kabel bereits installiert sind und ein POE+-Injektor oder -Switch zur Verwendung verfügbar ist. Wenn Wechselstrom (120 V) verwendet wird, stellen Sie alternativ sicher, dass sich eine zugängliche Netzsteckdose in einem Umkreis von 20 Fuß vom Standfuß befindet.
- Physischer Aufbau: Der Boden muss eben, sauber und frei von jeglichem Schmutz sein, um eine stabile und sichere Installation auf dem Standfuß zu gewährleisten.

- Standort des Sockels: Stellen Sie den Standfuß so auf, dass er keine Türen, Gassen oder Zugänge blockiert, sodass er sich leicht im Raum bewegen kann.
- Kabelmanagement: Verlegen und sichern Sie alle überschüssigen Kabel innerhalb des Sockels, um Unordnung zu vermeiden und mögliche Schäden bei normalem Gebrauch zu vermeiden.

Sobald diese Voraussetzungen bestätigt wurden, können Sie mit dem Installationsvorgang fortfahren.

So installieren Sie Amazon One Pedestal

1. Nehmen Sie den Amazon One Pedestal aus der Verpackung.
2. Entfernen Sie die Tür, indem Sie beide manipulationssicheren M4-Schrauben lösen.
3. Stecken Sie das Netzkabel ein.
4. Führen Sie das Kabel durch das Loch in der Sockelgrundplatte.
5. Wickeln Sie überschüssiges Stromkabel im Inneren des Sockels auf.
6. Führen Sie das Ethernet-Kabel (Cat5E oder besser) durch die Bodenplatte des Sockels und stecken Sie es in den Ethernet-Anschluss.
7. Installieren Sie eine Ferritschleife am Ethernet-Kabel 2 Zoll über der Basis des Sockels.
8. Führen Sie das RS485 serielle Kabel vom Zutrittskontrollpanel (oder dem Ausweislesegerät) mit einer Überlänge von 1 Fuß zum Podest.
9. Am RS485 Kabel 2 Zoll über dem Standfuß des Sockels eine Ferritschlaufe anbringen.
10. Stecken Sie die Stromversorgung in die Steckdose und vergewissern Sie sich, dass das Amazon One-Gerät eingeschaltet ist.
11. Befestigen Sie die Tür wieder am Sockel und schrauben Sie die beiden M4-Schrauben zur Sicherung wieder fest.

Nach der Installation Ihres Amazon One-Geräts können Sie das Gerät aktivieren.

Installation des an der Wand montierbaren Amazon One-Geräts

Das an der Wand montierbare Amazon One-Gerät ist ein vielseitiges, kompaktes biometrisches Identifikationssystem, das Benutzern in verschiedenen Umgebungen ein nahtloses, berührungsloses Erlebnis bietet. Es verwendet fortschrittliche Handflächenerkennungstechnologie für sicheren Zugang oder Bezahlung und ist somit ideal für stark frequentierte Standorte wie Einzelhandelsflächen, Büroeingänge und mehr.

In diesem Abschnitt werden die erforderlichen Standortanforderungen und die detaillierten Schritte zur Installation des an der Wand montierten Amazon One-Geräts beschrieben, um optimale Leistung und Sicherheit zu gewährleisten.

Voraussetzungen und Vorbereitung für die Installation des an der Wand montierbaren Amazon One-Geräts

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, um sicherzustellen, dass das Gerät effektiv funktioniert und ordnungsgemäß in Ihrem Raum aufgestellt ist:

- Nur zur Verwendung in Innenräumen: Das an der Wand montierbare Amazon One-Gerät ist nur für den Gebrauch in Innenräumen vorgesehen. Stellen Sie daher sicher, dass es in einer geeigneten Umgebung installiert wird.
- Anforderungen an die Wand: Die Wand muss eben sein, um eine korrekte Ausrichtung und Funktionalität des Geräts zu gewährleisten.
- Montagehöhe: Die Oberseite der Wandhalterung sollte nach der Installation nicht höher als 44-46 Zoll über dem Boden positioniert werden, um den Benutzern den Zugang zu erleichtern.
- Kabelmanagement: Stellen Sie sicher, dass alle überschüssigen Kabel hinter der Wandhalterung verlegt und sicher befestigt sind, um Beschädigungen oder Unordnung zu vermeiden.
- Power Over Ethernet (PoE++): Wenn Sie Power Over Ethernet (PoE++) verwenden, stellen Sie sicher, dass ein IEEE 802.3bt (Typ 3) PoE++-Switch (End Span) oder Injector (Midspan) der Klasse 6 verfügbar ist. Die PoE++-Quelle muss aufgeführt oder zertifiziert sein und den IEC 62368-1-Standards entsprechen. Wichtig ist, dass sich die PoE++-Quelle im selben Gebäude wie das Gerät befinden muss. Verwenden Sie nur eine zugelassene PoE++-Quelle mit dem AOE-Gerät.
- 15-V-DC-Stromeingang: Wenn Sie einen 15-V-DC-Stromeingang verwenden, stellen Sie sicher, dass nur ein Netzteil der NEC-Klasse 2 oder ein zugelassenes Netzteil mit begrenzter Leistung verwendet wird. Das Netzteil muss aus Sicherheits- und Kompatibilitätsgründen aufgeführt oder zertifiziert sein.

Erforderliche Werkzeuge

- 1/4-Zoll-Bohrer für Trockenbau oder Mauerwerk, falls Wandanker erforderlich sind
- Abisoliergerät
- 7/64-Zoll-Bohrer zum Bohren von Pilotlöchern

- #2 Kreuzschlitzschraubendreher
- 0,5 mm x 2 mm Schlitzschraubendreher
- Sicherer T12-Torx-Treiber
- Bleistift
- Level

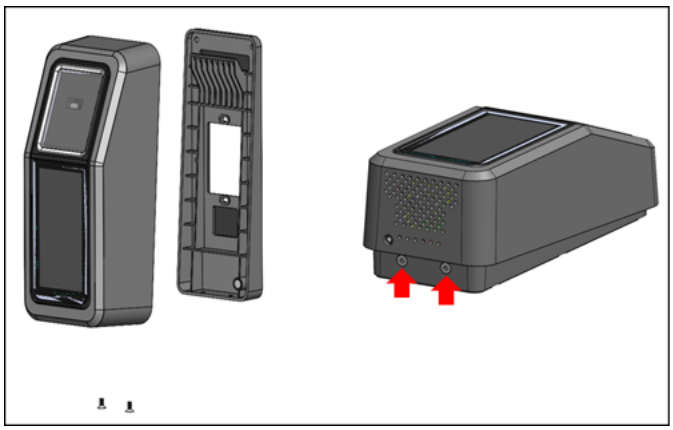
Im Lieferumfang des an der Wand montierbaren Amazon One-Geräts enthalten

- 6 x #8 Trockenbauanker
- 6 x #8 -32 1-Zoll-lange Schrauben
- 2 x #6 -32 1-Zoll-Maschinenschrauben
- 2 x Klemmenblockstecker mit 6 Positionen
- 2 Torx-Sicherheits-Flachkopfschrauben M4x10

Sobald diese Voraussetzungen bestätigt sind, können Sie mit den Installationsschritten fortfahren, um das an der Wand montierbare Amazon One-Gerät sicher zu montieren und zu konfigurieren.

So installieren Sie die Wandmontageplatte für Ihr Amazon One-Gerät

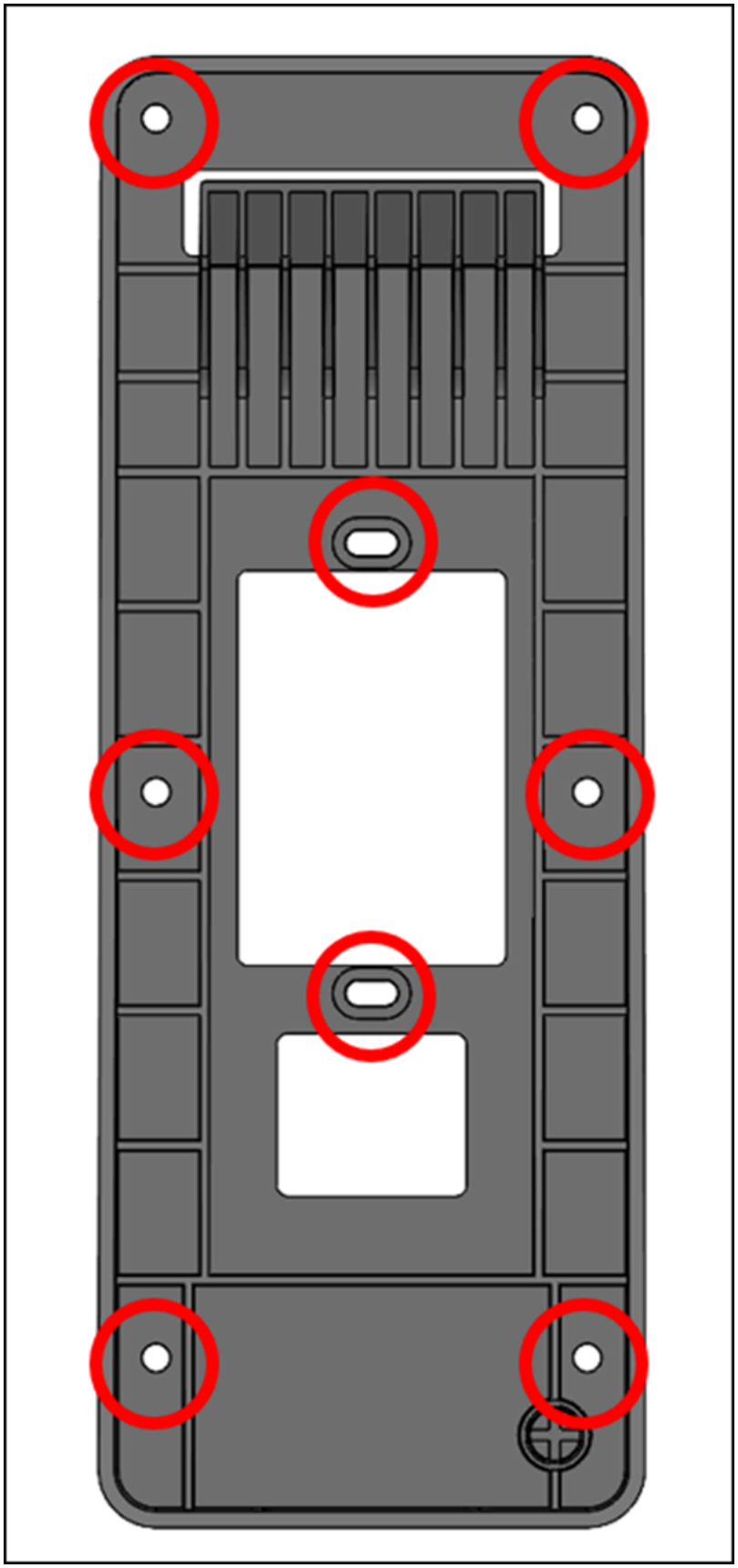
1. Nehmen Sie Ihr Amazon One-Gerät aus der Verpackung.
2. Trennen Sie die Montageplatte von Ihrem Amazon One-Gerät, indem Sie die beiden unteren Torx-Sicherheitsschrauben entfernen.



3. Positionieren Sie die Montageplatte an der gewünschten Stelle an der Wand. Verwenden Sie die Halterung als Schablone, um die äußeren sechs Schraubenlöcher zu markieren, wie in der folgenden Abbildung gezeigt.

(Optional) Wenn in der Einbauposition eine Einzelbox verfügbar ist, gehen Sie wie folgt vor:

- Befestigen Sie die Platte lose an der Sammelbox, indem Sie die mitgelieferten Maschinenschrauben #6 -32 durch die Langlöcher stecken.
- Stellen Sie sicher, dass die Montageplatte waagerecht ist.
- Verwenden Sie die Montageplatte als Schablone, um die sechs Schraubenpositionen mit einem Bleistift zu markieren. Sie können die Langlöcher und die Schraube #6 -32 als zusätzliche Stütze für die Montageplatte verwenden. Verwenden Sie die Schraubenpositionen #6 -32 nicht als primäres Mittel zur Befestigung der Wandplatte.



4. Bei der Montage in Stuck-, Trockenbau-, Ziegel- oder Betonoberflächen bohren Sie an jeder markierten Stelle 1/4-Zoll-Löcher und bringen Sie dann Wandanker an, indem Sie sie in das Loch drücken, bis der Dübel bündig mit der Wand abschließt.

   Bei der Montage auf einer Holzoberfläche sind die Dübel nicht erforderlich und an den markierten Stellen sind nur 7/64-Zoll-Vorlöcher erforderlich.
5. Befestigen Sie die Wandplatte mit den #8 -Holzschrauben an den Ankerpositionen locker an der Wand.
6. Nachdem alle Befestigungselemente angebracht sind, stellen Sie sicher, dass die Montageplatte waagerecht ist.
7. Ziehen Sie die Schrauben fest, um die Montageplatte an der Wand zu befestigen.

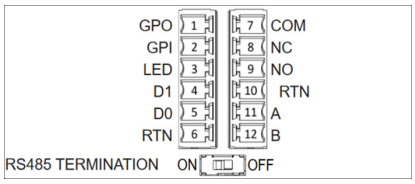
Um Ihr an der Wand montierbares Amazon One-Gerät anzuschließen

Sie können Amazon One-Geräte mit den Protokollen OSDP und Weigand Access Control konfigurieren. Um die Installation zu vereinfachen, verwendet das Amazon One-Gerät Klemmenblockanschlüsse (Mfg P/N: Phoenix Contact 1767694). Sie haben auch die Möglichkeit, das Amazon One-Gerät so zu konfigurieren, dass externe Geräte direkt über das interne Relais oder die Allzweck-Eingangs- und Ausgangsanschlüsse gesteuert werden.

1. Anhand des folgenden Diagramms und der Verbindungstabelle können Sie die passende Verkabelungskonfiguration für Ihre Anwendung ermitteln.

   Einzelheiten zu den elektrischen Eigenschaften der Signale finden Sie in der Verkabelungsanleitung.

   Verbindungen



Pin	Verbindung	Beschreibung	Verwenden Sie	
1	GEHEN	Ausgabe für allgemeine Zwecke	Digitales Ausgangssignal — optional	

Pin	Verbindung	Beschreibung	Verwenden Sie
2	GPI	Eingabe für allgemeine Zwecke	Digitales Eingangssignal — optional
3	GEFÜHRT	Wiegand LED	Wiegand LED — fakultativ
4	D1	Wiegand D1	Wiegand Data 1 — Weißer Draht
5	D0	Wiegand D0	Wiegand Data 0 — Grünes Kabel
6	RTN	Signalrückkehr	Wiegand Ground — Schwarzer Draht
7	Com	Relay üblich	Kontaktrelais allgemein — weißer Draht
8	NC	Das Relais ist normalerweise geschlossen	Kontaktrelais normalerweise geschlossen — orangefarbenes Kabel
9	NO	Das Relais ist normalerweise geöffnet	Das Kontaktre lais ist normal geöffnet — gelber Draht

Pin	Verbindung	Beschreibung	Verwenden Sie
10	RTN	Signalrückkehr	OSDP-Rück kehr — Schwarzer Draht
11	A	RS485_A/D1/ Uhr	OSDP D1 — Weißes Kabel
12	B	RS485_B/D0/ Daten	OSDP D0 — Grünes Kabel

2. Ziehen Sie bei der Installation eines Kabels 3 mm bis 5 mm vom Ende des Kabels ab.
3. Stecken Sie das abisolierte Ende des Kabels in die gewünschte Klemmenposition.
4. Drehen Sie die Klemmenbefestigungsschraube mit einem Schlitzschraubendreher im Uhrzeigersinn, um das Kabel festzuklemmen, bis es fest sitzt. Nicht zu fest anziehen.
5. Ziehen Sie nach dem Befestigen vorsichtig am Draht, um sicherzustellen, dass er sitzt.
6. Nachdem Sie die erforderlichen Verbindungen hergestellt haben, stecken Sie den Stecker in die entsprechende Buchse Ihres Amazon One-Geräteklemmenblocks.
7. Stecken Sie das Cat6-Ethernet-Kabel in die Buchse. RJ45
8. Stellen Sie das Amazon One-Gerät so auf, dass der Haken an der Wandplatte in die Öffnung auf der Rückseite des Geräts gleitet.
9. Stellen Sie sicher, dass sich die Kabel nicht zwischen dem Gerät und der Montageplatte verfangen, und lassen Sie das Gerät schwenken und in die richtige Position bringen.
10. Befestigen Sie Ihr Amazon One-Gerät mit zwei Torx Security M4x10-Flachkopfschrauben an der Montageplatte.
11. Ziehen Sie die Schrauben von Hand fest. Nicht zu fest anziehen.

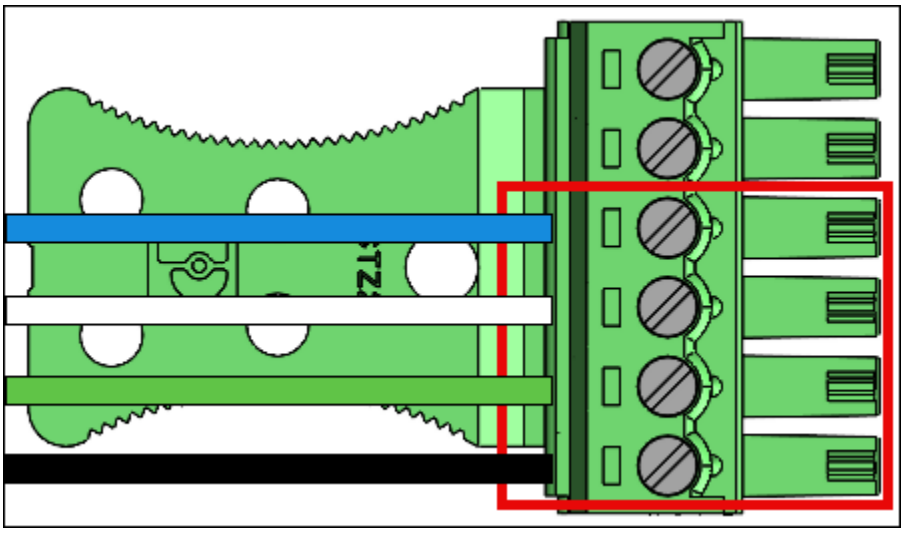
So verkabeln Sie Ihr an der Wand montierbares Amazon One-Gerät

Installieren Sie nur die für Ihre Anwendung erforderlichen Kabel.

Wiegand-Verbindungen

- Stecken Sie das blaue Kabel in Pin 3 (LED).

- Stecken Sie das weiße Kabel in Pin 4 (D1).
- Stecken Sie das grüne Kabel in Pin 5 (D0).
- Stecken Sie das schwarze Kabel in Pin 6 (RTN).



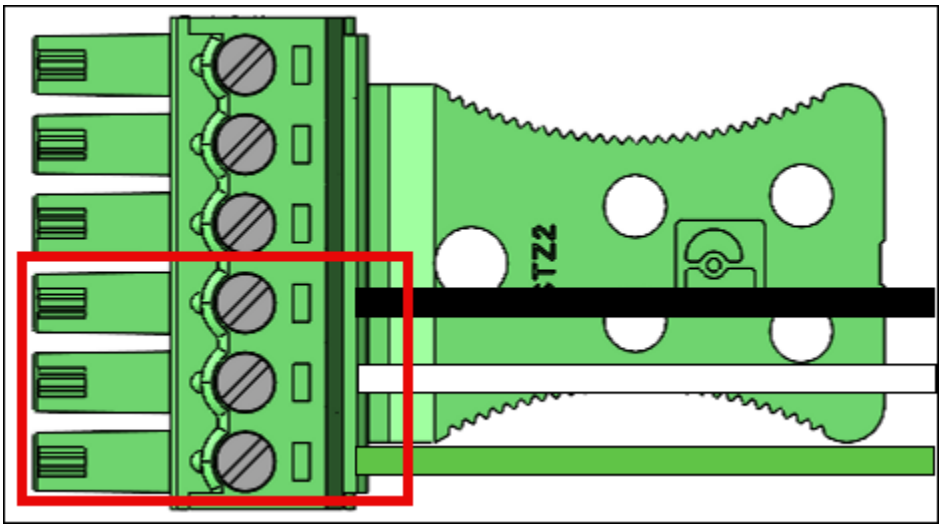
Wiegand-Ausgangsverkabelung

Pin	Verbindung	Beschreibung	Verwenden Sie
3	GEFÜHRT	Wiegand LED	Wiegand LED-Eingang — optional (5 V TTL)
4	D1	Wiegand D1	Wiegand D1-Ausgang (5 V TTL)
5	D0	Wiegand D0	Wiegand D0-Ausgang (5 V TTL)
6	RTN	Signalrückkehr	Referenz Wiegand GND

Schalten Sie den RS485 Abschlussschalter auf „ON“, wenn das Gerät das letzte Gerät in der Leitung ist. Dieser Schalter aktiviert den 120-Ohm-Widerstandsanschluss an der Leitung.

RS485 Verbindungen

- Stecken Sie das schwarze Kabel in Pin 10 (RTN).
- Stecken Sie das weiße Kabel in Pin 11 (A).
- Stecken Sie das grüne Kabel in Pin 12 (B).



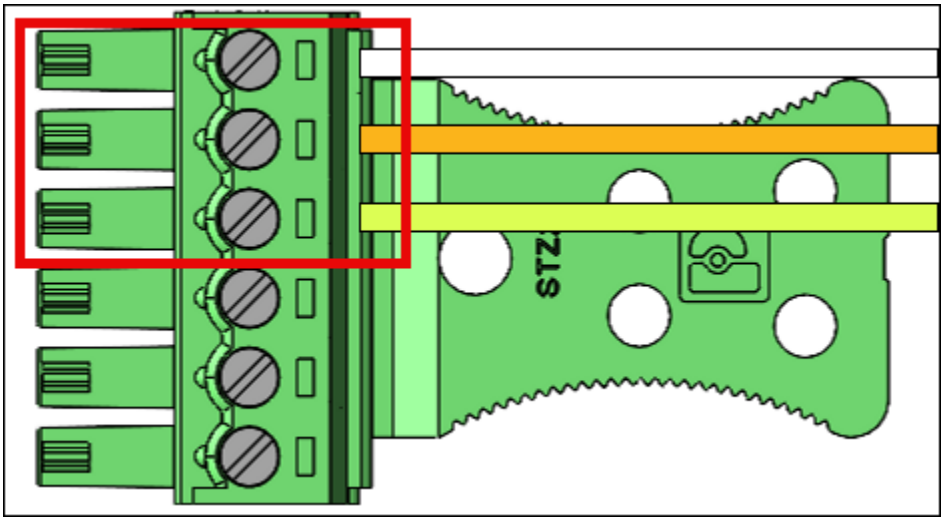
RS485 Verkabelung

Pin	Verbindung	Beschreibung	Verwenden Sie
10	RTN	Signalrückkehr	Ground (Boden)
11	A	RS485_A/D1/Uhr	RS485 nichtinvertierendes Signal
12	B	RS485_B/D0/Daten	RS485 invertierendes Signal

Relaisverbindungen

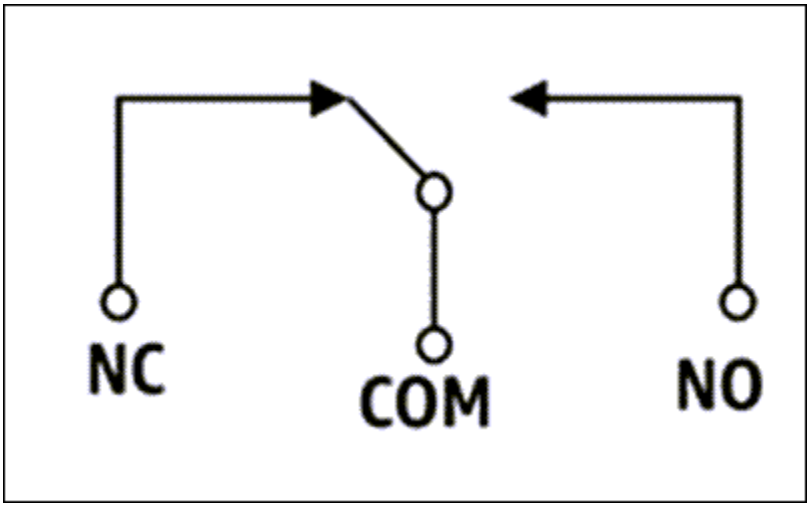
- Stecken Sie das weiße Kabel in Pin 7 (COM).
- Stecken Sie das orangefarbene Kabel in Pin 8 (NC).

- Stecken Sie das gelbe Kabel in Pin 9 (NO).



Verkabelung des Relais

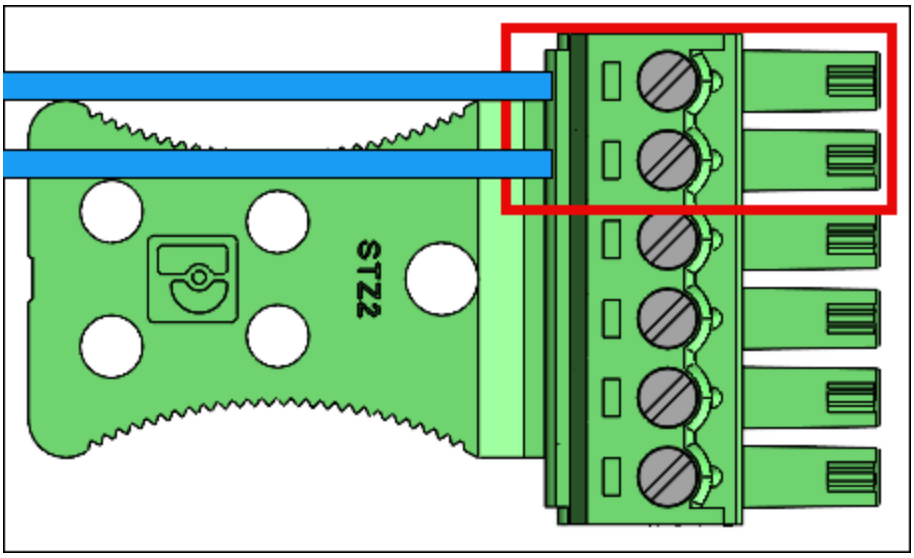
Pin	Verbindung	Beschreibung	Verwenden Sie
7	COM	Gemeinsames Relais	Kontaktrelais Common — Weißer Draht
8	NC	Das Relais ist normalerweise geschlossen	Kontaktrelais normalerweise geschlossen — orangefarbenes Kabel
9	NO	Das Relais ist normalerweise geöffnet	Das Kontaktre lais ist normal geöffnet — gelber Draht



Das Relais sollte gemäß den angegebenen Sicherheitsklassen 30 VAC/60 VDC, max. 60 W betrieben werden.

Digitale Eingangs-/Ausgangsanschlüsse

- Stecken Sie das blaue Kabel in Pin 1 (GPO).
- Stecken Sie das blaue Kabel in Pin 2 (GPI).



Digitale Eingangs-/Ausgangsverkabelung

Pin	Verbindung	Beschreibung	Verwenden Sie	
1	GEH	Ausgabe für allgemeine Zwecke	Digitales Ausgangssignal (5 V)	
2	GPI	Eingabe für allgemeine Zwecke	Digitales Eingangssignal (3,6 V — 5 V)	

- Die digitalen Eingangs-/Ausgangsanschlüsse sollten wie angegeben betrieben werden.

Nach der Installation Ihres Amazon One-Geräts können Sie das Gerät aktivieren.

Amazon One Device I/O Hub für sicheren Zugriff installieren

Das Amazon One-Gerät mit I/O Hub ist ein integraler Bestandteil des Amazon One Enterprise-Systems, das darauf ausgelegt ist, die Sicherheit zu erhöhen und die Zugriffskontrolle für eine Vielzahl von Umgebungen zu optimieren. Das Gerät nutzt die biometrische Handflächenerkennung, um Benutzern eine sichere, berührungslose Authentifizierung zu ermöglichen. Dadurch eignet es sich ideal für den Einsatz in Hochsicherheitsbereichen wie Bürogebäuden, eingeschränkten Zugangspunkten oder Einrichtungen, die eine nahtlose Zugangsverwaltung erfordern. Der I/O Hub fungiert als Brücke zwischen dem Gerät und Ihrer vorhandenen Sicherheitsinfrastruktur und ermöglicht die Kommunikation mit Türschlössern, Alarmanlagen und anderen Zutrittskontrollsystemen.

Dieser Abschnitt enthält die Standortanforderungen und step-by-step Anweisungen für die Installation des Amazon One-Geräts mit I/O Hub. Die richtige Vorbereitung und Installation sind entscheidend, um sicherzustellen, dass das System sicher und effizient funktioniert und den Benutzern ein reibungsloses und zuverlässiges Erlebnis bietet.

Voraussetzungen und Vorbereitung für die Installation des Amazon One-Geräts mit I/O Hub

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, um eine sichere und effektive Einrichtung zu gewährleisten:

- Nur für den Gebrauch in Innenräumen: Das Amazon One-Gerät mit I/O Hub ist nur für den Gebrauch in Innenräumen konzipiert. Stellen Sie sicher, dass es in einer geeigneten Umgebung installiert ist.
- Power Over Ethernet (PoE++): Wenn Sie Power Over Ethernet (PoE++) verwenden, stellen Sie sicher, dass ein IEEE 802.3bt (Typ 3) PoE++-Switch (End Span) oder Injector (Midspan) der Klasse 6 verfügbar ist. Die PoE++-Quelle muss aufgeführt oder zertifiziert sein und den IEC 62368-1-Standards entsprechen. Wichtig ist, dass sich die PoE++-Quelle im selben Gebäude wie das Gerät befinden muss. Verwenden Sie nur eine zugelassene PoE++-Quelle mit dem AOE-Gerät.

- 15-V-DC-Stromeingang: Wenn Sie einen 15-V-DC-Stromeingang verwenden, stellen Sie sicher, dass nur ein Netzteil der NEC-Klasse 2 oder ein zugelassenes Netzteil mit begrenzter Leistung verwendet wird. Das Netzteil muss aus Sicherheitsgründen aufgeführt oder zertifiziert sein. Weitere Informationen finden Sie im Abschnitt Optionale Gleichstromversorgung weiter unten.

Erforderliche Tools

- Abisoliergerät
- #2 Kreuzschlitzschraubendreher
- 0,5 mm x 2 mm Schlitzschraubendreher

Im Amazon One-Gerät mit I/O Hub enthalten

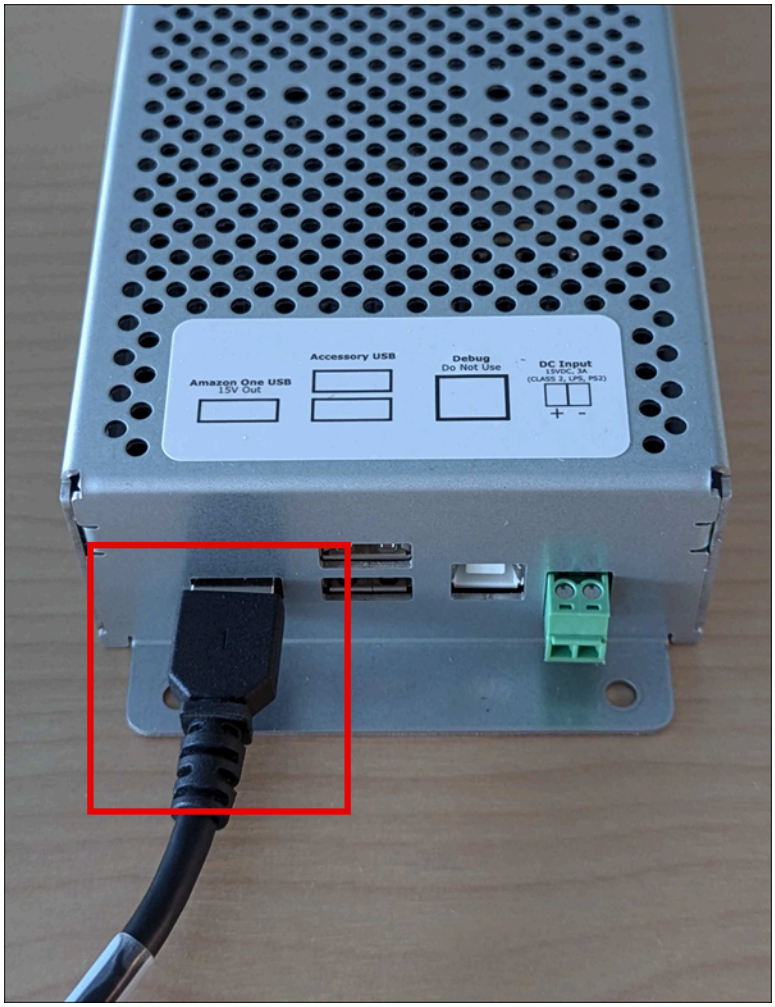
- 2 x Klemmenblockstecker mit 6 Positionen
- DC-Steckverbinder
- 72-Zoll-Strom-/Datenkabel

Sobald diese Voraussetzungen bestätigt sind, können Sie mit dem Installationsvorgang fortfahren und so eine sichere und effiziente Einrichtung Ihres Amazon One-Geräts mit I/O Hub sicherstellen. Durch die richtige Vorbereitung wird sichergestellt, dass das Gerät wie vorgesehen funktioniert und sich problemlos in Ihr sicheres Zugangssystem integrieren lässt.

Um den I/O-Hub für Ihr Amazon One-Gerät zu installieren

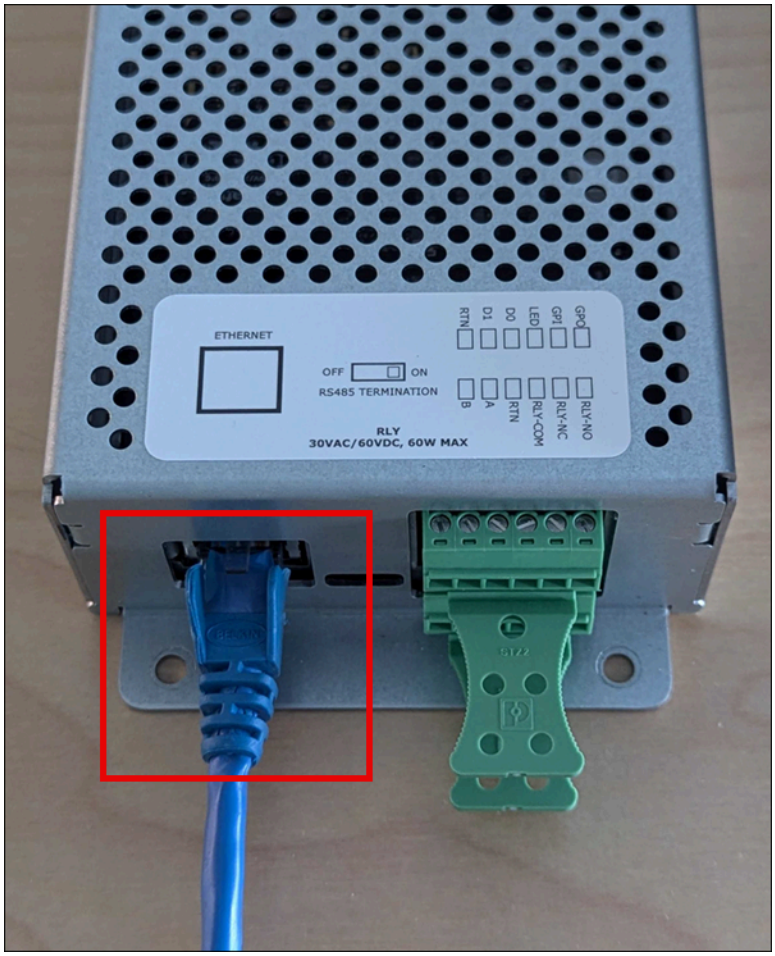
1. Nehmen Sie Ihr Amazon One-Gerät mit I/O Hub aus der Verpackung.

2. Sichern Sie den I/O-Hub am gewünschten Ort.
3. Stecken Sie das Amazon One USB-Kabel in den I/O-Hub-Anschluss.



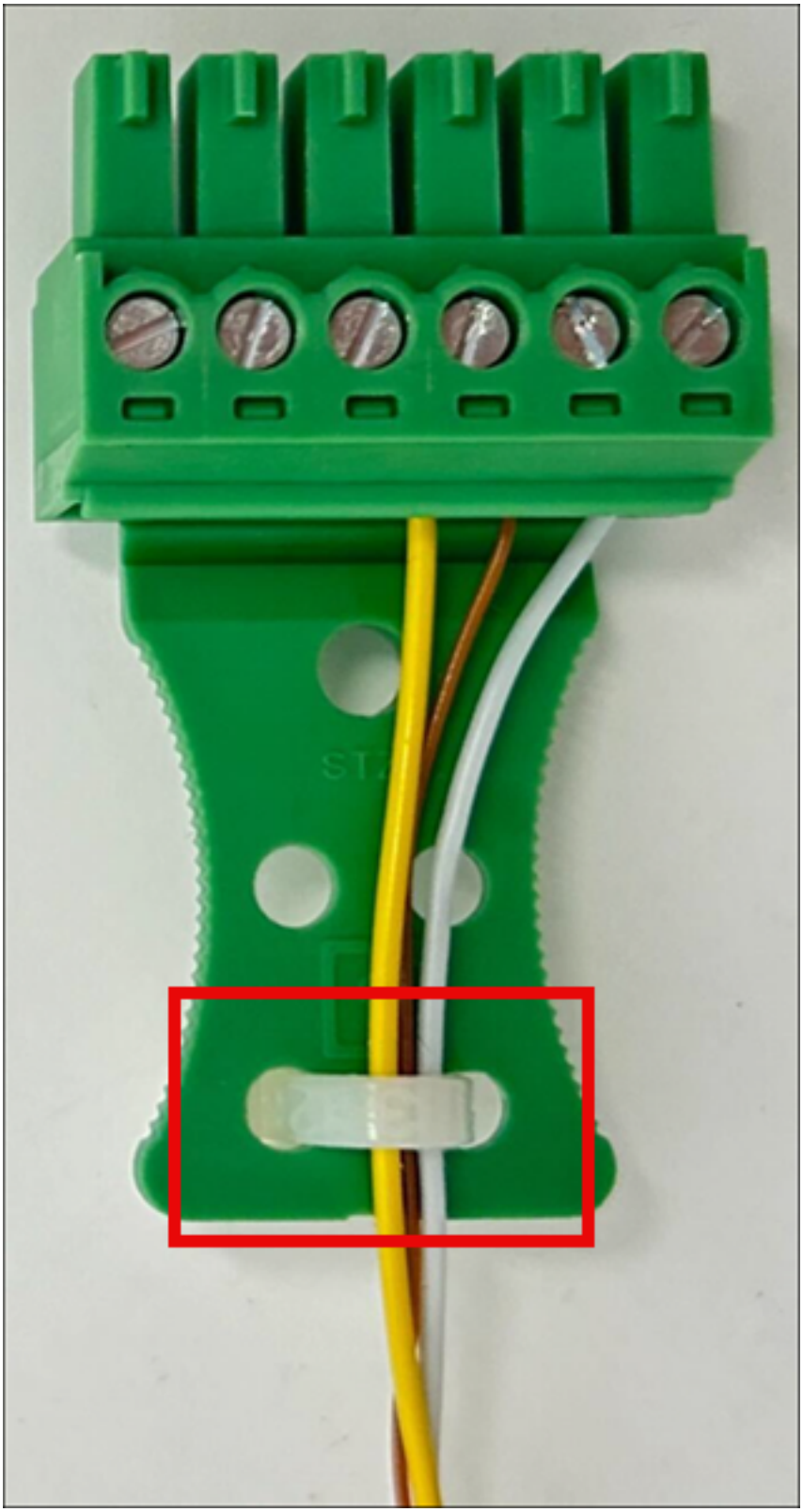
4. Um POE++ mit Strom zu versorgen, stecken Sie das Ethernet-Kabel von der POE++-Quelle in den I/O-Hub-Anschluss.

   Optional: Informationen zur Gleichstromversorgung finden Sie im Abschnitt zur Installation der DC-Verkabelung weiter unten.



So verkabeln Sie den I/O-Hub für Ihr Amazon One-Gerät

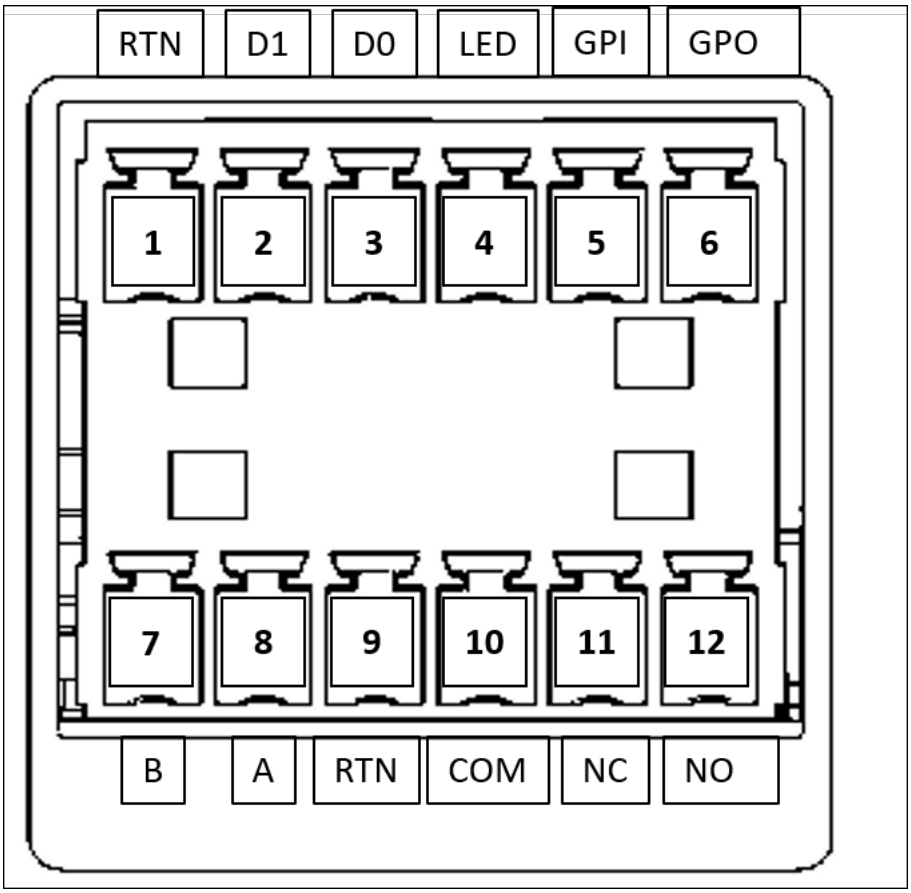
- Installieren Sie eine Tropfschleife, um zu verhindern, dass Flüssigkeiten versehentlich über das Kabel in den I/O-Hub laufen.
- Bringen Sie eine Zugentlastungsklemme an, um die Kabel vor Beschädigung oder stress zu schützen, wie in der folgenden Abbildung gezeigt.



1. Stecken Sie die Stecker der Klemmenleiste in den I/O-Hub.

2. Stecken Sie nur die für Ihre Anwendung erforderlichen Kabel in die Klemmenblockstecker. Beachten Sie die folgende Verkabelungstabelle und die folgenden Diagramme.

Verbindungen

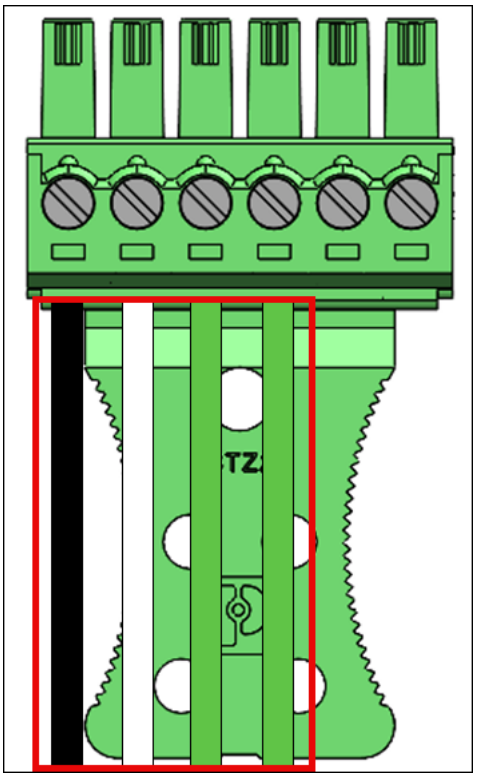


Pin	Verbindung	Beschreibung	Verwenden Sie
1	RTN	Signalrückkehr	Wiegand Ground — Schwarzer Draht
2	D1	Wiegand D1	Wiegand Data 1 — Weißer Draht
3	D0	Wiegand D0	Wiegand Data 0 — Grünes Kabel

Pin	Verbindung	Beschreibung	Verwenden Sie
4	GEFÜHRT	Wiegand LED	Wiegand LED — fakultativ
5	GPI	Eingabe für allgemeine Zwecke	Digitales Eingangssignal — optional
6	GEH	Ausgabe für allgemeine Zwecke	Digitales Ausgangssignal — optional
7	B	RS485_B/D0/ Daten	OSDP D0 — Grünes Kabel
8	A	RS485_A/D1/Uhr	OSDP D1 — Weißes Kabel
9	RTN	Signalrückkehr	OSDP-Rückkehr — Schwarzer Draht
10	COM	Relay Common	Kontaktrelais allgemein — Weißer Draht
11	NC	Das Relais ist normalerweise geschlossen	Kontaktrelais normalerweise geschlossen — orangefarbenes Kabel
12	NO	Das Relais ist normalerweise geöffnet	Das Kontaktre lais ist normal geöffnet — gelber Draht

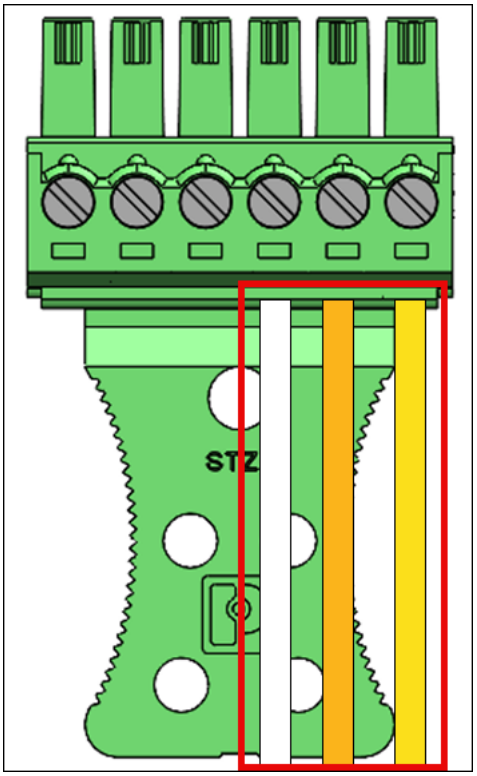
Wiegand-Verbindungen

- Stecken Sie das schwarze Kabel in Pin 1 (RTN).
- Stecken Sie das weiße Kabel in Pin 2 (D1).
- Stecken Sie das grüne Kabel in Pin 3 (D0).
- Optional: Stecken Sie das grüne Kabel in Pin 4 (LED).

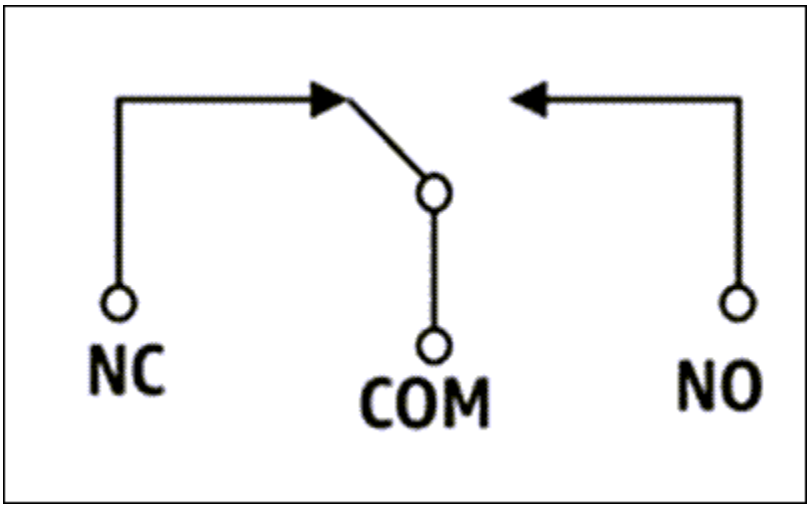


Relaisverbindungen

- Stecken Sie das weiße Kabel in Pin 10 (COM).
- Stecken Sie das orangefarbene Kabel in Pin 11 (NC).
- Stecken Sie das gelbe Kabel in Pin 12 (NO).



Relaisdiagramm

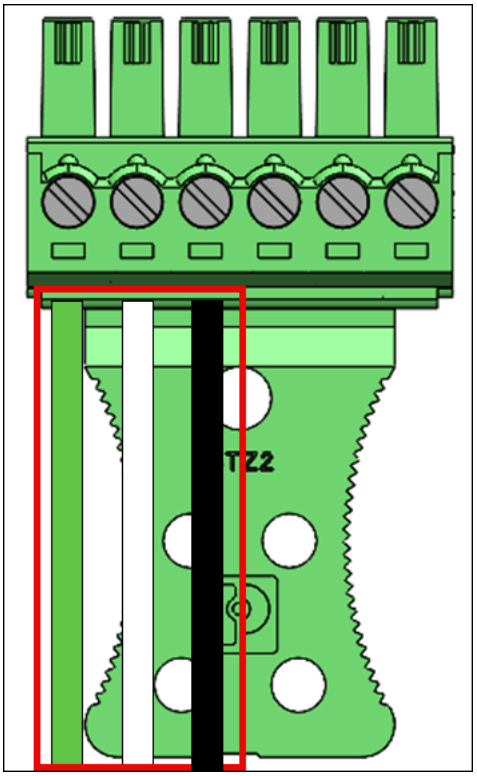


Das Relais sollte gemäß den angegebenen Sicherheitsklassen 30 VAC/60 VDC, max. 60 W betrieben werden.

RS485 Verbindungen

- Stecken Sie das grüne Kabel in Pin 7 (B).
- Stecken Sie das weiße Kabel in Pin 8 (A).

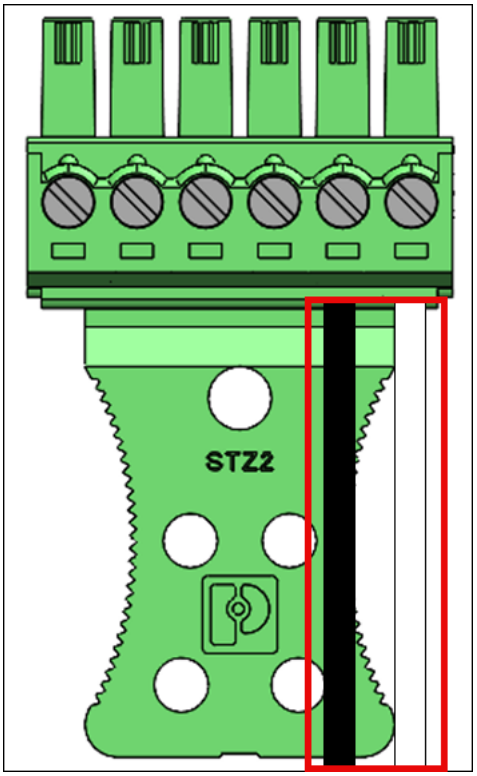
- Stecken Sie das schwarze Kabel in Pin 9 (RTN).



Schalten Sie den RS485 Abschlussschalter auf „ON“, wenn das Gerät das letzte Gerät in der Leitung ist. Dieser Schalter aktiviert den 120-Ohm-Widerstandsanschluss an der Leitung.

Digitale Eingangs-/Ausgangsanschlüsse

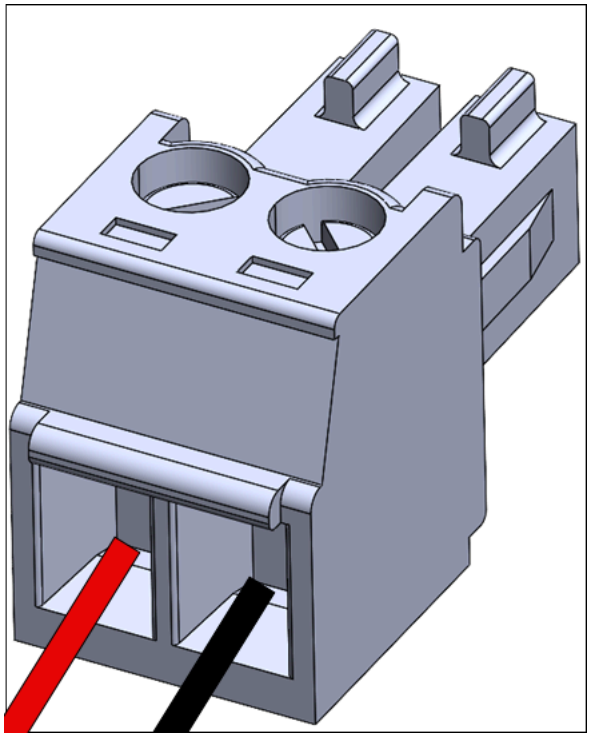
- Stecken Sie das schwarze Kabel in Pin 5 (GPI).
- Stecken Sie das weiße Kabel in Pin 6 (GPO).



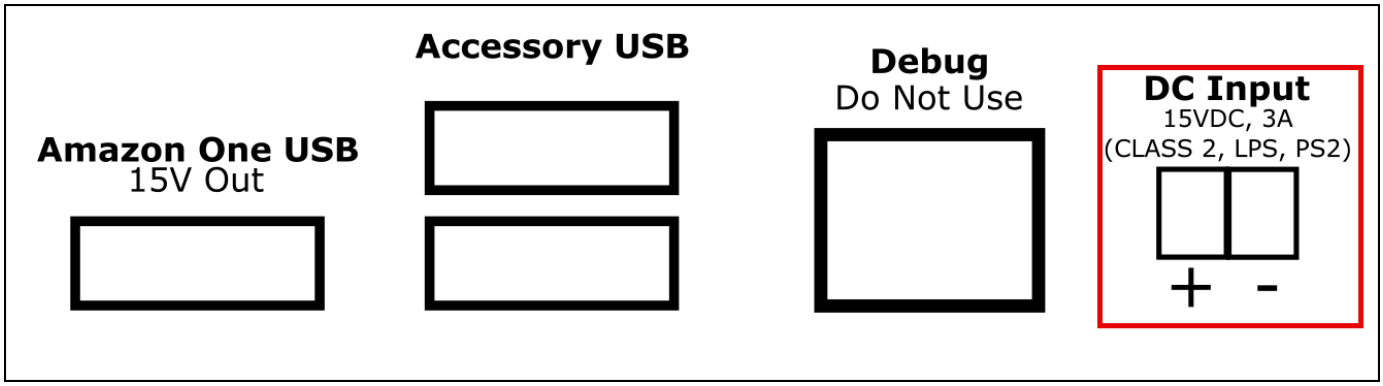
- Die digitalen Eingangs-/Ausgangsanschlüsse sollten wie angegeben betrieben werden.

Optional: Zur Installation der Gleichstromverkabelung

1. Ziehen Sie 3 mm bis 5 mm vom Ende eines roten Kabels für Plus (+) und eines schwarzen Kabels für Minus (-) ab.
2. Stecken Sie das abisolierte Ende des DC-Kabels in den DC-Stecker.



3. Schrauben Sie den Draht in die richtige Position.
4. Stecken Sie den verdrahteten DC-Stecker in den DC-Eingangsanschluss.



Nach der Installation Ihres Amazon One-Geräts können Sie das Gerät aktivieren.

Amazon One-Gerät aktivieren

Wenn Ihr Amazon One-Gerät installiert und eingeschaltet ist, können Sie es aktivieren.

Um Ihr Amazon One-Gerät zu aktivieren

1. Tippen Sie auf dem Amazon One-Gerät auf den Bildschirm, um loszulegen.

2. Wählen Sie Ethernet oder WLAN, um eine Verbindung zum Internet herzustellen.

   Sobald das Gerät mit dem Internet verbunden ist, beginnt es mit dem Herunterladen des neuesten Softwarepakets.
3. Wenn auf dem Bildschirm angezeigt wird, dass der Software-Download abgeschlossen ist! , wählen Sie OK.
4. Wählen Sie QR-Code aus.

   Auf dem Bildschirm des Amazon One-Geräts wird der QR-Code scannen angezeigt.
5. Um den Aktivierungs-QR-Code abzurufen, öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.

   > **Note**
   >
   > Wir empfehlen Ihnen dringend, Ihren Installateuren eingeschränkte Berechtigungen zu gewähren, sodass sie nur Zugriff auf die Aktivierungs-QR-Codes in Ihrer Amazon One Enterprise-Konsole haben. Siehe Amazon One-Benutzer hinzufügen.
6. Wählen Sie im Navigationsbereich die Option Aktivierungs-QR-Codes aus.
7. Wählen Sie aus der Drop-down-Liste „Standort auswählen“ den Standort aus, an dem das Amazon One-Gerät installiert ist.
8. Bestätigen Sie unter Standortinformationen die Seitenadresse.
9. Suchen Sie unter Aktivierungs-QR-Codes nach dem Namen der Geräteinstanz, die Sie aktivieren, und wählen Sie den entsprechenden QR-Code abrufen aus, um den QR-Code abzurufen.
10. Scannen Sie den QR-Code mit dem Amazon One-Gerät. Beachten Sie, dass der QR-Code aus Sicherheitsgründen regelmäßig aktualisiert wird. Sie dürfen einen QR-Code nur einmal verwenden.
11. Geben Sie die Postleitzahl der Website ein und wählen Sie Einstellungen bestätigen aus, nachdem Sie überprüft haben, ob die richtige Website angezeigt wird.
12. Wenn auf dem Bildschirm des Amazon One-Geräts die Aktivierung abgeschlossen angezeigt wird! , das Gerät ist einsatzbereit.

Benutzer registrieren und eingeben

Jetzt, da Ihr Amazon One-Gerät aktiviert ist, können Ihre Mitarbeiter damit beginnen, ihre Handflächen zu registrieren und ihre Handflächen zu authentifizieren, um Zugriff zu erhalten.

Themen

- Eine Endpunktrichtlinie erstellen
- Authentifizierung für die Einreise

Eine Endpunktrichtlinie erstellen

Bevor Benutzer ihre Handflächen für den Zugriff authentifizieren können, müssen sie den Registrierungsprozess durchlaufen. Sicherheitspersonal sollte immer die Identität des Benutzers überprüfen, bevor es dem Benutzer erlaubt, sich zu registrieren.

Um Ihre Palms auf einem Amazon One-Gerät zu registrieren

1. Drücken Sie auf dem Amazon One Enterprise-Registrierungsgerät auf Erste Schritte.
2. Scannen Sie einen Mitarbeiterausweis mit dem Ausweisscanner, der mit Ihrem Amazon One Enterprise-Registrierungsgerät verbunden ist.

   Wenn das Badge erfolgreich gescannt wurde, wird auf dem Bildschirm des Amazon One-Geräts angezeigt, dass Badge gescannt wurde.
3. Lesen Sie sich die Nutzungsbedingungen durch und drücken Sie dann auf OK.
4. Lesen Sie sich „Einwilligung — Ihre biometrischen Daten von Palm“ durch und klicken Sie auf „Ich stimme zu“, wenn Sie damit einverstanden sind.
5. Folgen Sie den Anweisungen auf dem Bildschirm, um den Registrierungsprozess abzuschließen.

Authentifizierung für die Einreise

Nachdem Sie Ihre Palms erfolgreich registriert haben, können Sie sich mit Ihrem Palm auf Ihrem Amazon One Enterprise-Eingabegerät authentifizieren.

Um Ihre Handfläche für die Eingabe auf einem Amazon One-Gerät zu authentifizieren

- Bewegen Sie Ihre Handfläche auf das Gerät und folgen Sie den Anweisungen auf dem Bildschirm, um Ihre Handfläche zu scannen.

Verwalten von Benutzern

Sie können die Verwaltungsseite für registrierte Benutzer verwenden, um den Überblick über die registrierten Benutzer zu behalten und die biometrischen Daten der Benutzer zu löschen. Ein Benutzer, dessen zugehörige biometrische Daten gelöscht wurden, hat keinen Zugriff mehr auf Amazon One-Geräte zur Authentifizierung.

Themen

- Eingeschriebene Benutzer anzeigen
- Löschen registrierter Benutzer und ihrer biometrischen Daten

Eingeschriebene Benutzer anzeigen

Das folgende Verfahren beschreibt, wie Sie Benutzer registrieren.

Um registrierte Benutzer anzuzeigen

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Enrolled user management aus.
3. Unter Registrierte Benutzer finden Sie alle registrierten Benutzer und die folgenden Details:
   - Badge-ID — Informationen zur Badge-ID, die bei der Registrierung von einem RFID-Ausweislesegerät erfasst wurden.
   - Registrierungsquelle — Details des Amazon One-Geräts, das für die Registrierung verwendet wurde.
   - Anmeldedatum — Datum und Uhrzeit der Registrierung.

Löschen registrierter Benutzer und ihrer biometrischen Daten

Das folgende Verfahren beschreibt, wie registrierte Benutzer und ihre biometrischen Daten gelöscht werden.

Um registrierte Benutzer und ihre biometrischen Daten zu löschen

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Enrolled user management aus.
3. Wählen Sie unter Registrierte Benutzer die Badge-ID des Benutzers aus, dessen biometrische Handflächendaten Sie löschen möchten.
4. Wählen Sie „Biometrie löschen“.
5. Wählen Sie Löschen, um das Löschen der biometrischen Benutzerdaten zu bestätigen.

> **Important**
>
> Diese Aktion führt zur dauerhaften Löschung der biometrischen Daten der Handfläche eines Benutzers aus Amazon One Enterprise. Der Benutzer muss sich erneut mit einem Amazon One Enterprise-Registrierungsgerät registrieren, um Amazon One Enterprise für die Authentifizierung verwenden zu können. Durch das Löschen der biometrischen Daten eines Benutzers werden auch andere Profilattribute wie die Badge-ID aus Amazon One Enterprise dauerhaft gelöscht.

Amazon One-Geräte verwalten

Nachdem Ihr Amazon One-Gerät installiert und aktiviert wurde, beginnt es mit der Meldung des Gerätezustands auf der Amazon One Enterprise-Konsole. Sie können die Amazon One Enterprise-Konsole verwenden, um Geräteverwaltungsaufgaben wie das Neustarten von Geräten oder das Aktualisieren von Konfigurationen durchzuführen.

Themen

- Wartung und Reinigung von Amazon One-Geräten
- Verwaltung der Website
- Verwaltung von Geräteinstanzen

Wartung und Reinigung von Amazon One-Geräten

Die Wartung Ihres Amazon One-Geräts bietet die optimale Betriebsumgebung und das optimale Geräteerlebnis.

Stellen Sie vor der Reinigung des Amazon One-Geräts Folgendes sicher:

- Sie müssen Amazon One zwar nicht aktivieren oder deaktivieren, stellen Sie jedoch sicher, dass die Geräte an die Stromversorgung angeschlossen sind, über eine Netzwerkverbindung verfügen und alle Peripherie- und Begleitgeräte (falls zutreffend) angeschlossen sind.
- Eskalieren Sie Probleme an Ihren Administrator, wenn die Netzwerkverbindung nicht verfügbar ist (in diesem Fall wird auf dem Amazon One-Gerät ein Fehlerbildschirm angezeigt), auf dem Amazon One-Gerät ein Fehlerbildschirm angezeigt wird oder ein Problem mit der Geräteverbindung auf der Konsole angezeigt wird.
- Schützen Sie Geräte physisch, sodass Unbefugte sie nicht manipulieren können.
- Überprüfen Sie Amazon One-Geräte täglich visuell und überprüfen Sie, ob unbefugte Verbindungen zu Amazon One-Geräten bestehen.
- Untersuchen Sie alle Seiten des Geräts auf Anzeichen von Manipulation, einschließlich sichtbarer Schrauben am Gerät und am Gehäuse, um sicherzustellen, dass keine Lücken/Öffnungen vorhanden sind, durch die die internen Komponenten/Schaltkreise des Amazon One-Geräts freigelegt werden können.
- Folgen Sie im Falle von Fehlern oder Ausfällen den Anweisungen auf dem Bildschirm des Amazon One-Geräts oder lesen Sie die Anleitung zur Fehlerbehebung, um Probleme zu beheben.

Um das Amazon One-Gerät zu reinigen

Wenn Sie Ihr Amazon One-Gerät regelmäßig reinigen, werden Flecken oder Spuren wie Finger- und Handabdrücke entfernt.

> **Note**
>
> Verwenden Sie keine anderen als die in diesem Handbuch aufgeführten Reinigungsmittel. Der empfohlene Reinigungsplan ist ein- oder zweimal pro Woche oder immer dann, wenn Schmutz, Staub oder Flecken auf dem Gerät sichtbar sind, jedoch niemals öfter als einmal täglich.

1. Wischen Sie das Amazon One-Gerät mit Reinigungstüchern für Isopropylalkohol (IPA) ab. Reinigen Sie nur die Berührungsoberfläche des Geräts. Berühren Sie das optische Fenster nicht und verwenden Sie kein anderes Reinigungsmittel, es sei denn, Sie werden von Amazon One dazu aufgefordert.
2. Wischen Sie alle Streifen mit einem trockenen Mikrofasertuch ab.
3. Sichtbaren Schmutz oder Ablagerungen leicht vom optischen Fenster abstauben (nicht abwischen). Beschränken Sie die Reinigung des optischen Fensters auf höchstens einmal täglichand/or when the window is visually dirty (e.g., finger/hand prints/smudges). Dieser Teil des Geräts darf nicht berührt werden, es kann jedoch zu versehentlichen Berührungen durch neue Kunden kommen.
4. Verwenden Sie gegebenenfalls einen KIC Smartcard-Cleaner, um das Innere eines Kartenlesegeräts zu reinigen.
5. Reinigen Sie das Gerät ein- oder zweimal pro Woche oder immer dann, wenn Schmutz, Staub oder Flecken auf dem Gerät sichtbar sind.

Verwaltung der Website

Eine Site stellt einen physischen Standort dar, an dem eine Reihe von Geräteinstanzen installiert sind und betrieben werden. Sie können Websites verwenden, um Amazon One-Geräte zu organisieren, die dieselbe physische Adresse verwenden.

Themen

- Der Name der Website wird geändert

- Die Adresse der Website wird aktualisiert

Der Name der Website wird geändert

Das folgende Verfahren beschreibt, wie Sie den Site-Namen für Ihr Gerät ändern können.

Um den Site-Namen zu ändern

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich Site aus.
3. Wählen Sie unter Websites die Site aus, für die Sie den Namen bearbeiten möchten.
4. Wählen Sie Edit (Bearbeiten) aus.
5. Geben Sie unter Site-Informationen den gewünschten Site-Namen und die Site-Beschreibung ein (optional).
6. Wählen Sie Zu aktualisierende Änderungen speichern aus.

Die Adresse der Website wird aktualisiert

Das folgende Verfahren beschreibt, wie Sie die Seitenadresse für Ihr Gerät aktualisieren.

Um die Site-Adresse zu aktualisieren

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich Site aus.
3. Wählen Sie unter Websites die Site aus, für die Sie die Adresse aktualisieren möchten.
4. Stellen Sie unter Geräteinstanzen sicher, dass die Anzahl der aktivierten Instanzen 0 ist.
5. (Optional) Wenn die Anzahl der aktivierten Instanzen nicht 0 ist, finden Sie weitere Informationen unter
6. Wählen Sie Edit (Bearbeiten) aus.
7. Geben Sie unter Physikalische Adresse die richtige physische Adresse ein.
8. Wählen Sie Zu aktualisierende Änderungen speichern aus.

Verwaltung von Geräteinstanzen

Eine Geräteinstanz ist eine logische Darstellung eines Geräts mit Konfigurationen. Die Verwendung von Geräte-Instances ermöglicht den Austausch von Amazon One-Geräten, wobei die zuvor festgelegten Konfigurationen und Namen automatisch übernommen werden. Eine Geräte-Instance hat einen benutzerdefinierten Namen (gemeinsame Benennungskonvention mit Ihrer Zugriffskontrollsoftware) und eine Reihe von Kommunikationskonfigurationen.

Themen

- Status der Geräteinstanz anzeigen
- Ein Amazon One-Gerät neu starten
- Aktualisierung der Amazon One-Gerätekonfigurationen
- Aktualisierung der Wi-Fi-Anmeldeinformationen
- Geräteinstanzen deaktivieren

Status der Geräteinstanz anzeigen

Das folgende Verfahren beschreibt, wie Sie den Status Ihrer Geräteinstanz anzeigen können.

Um den Status der Geräteinstanz anzuzeigen

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Geräteinstanz aus.
3. Unter Aktivierte Instances sehen Sie eine Liste der aktivierten Amazon One-Geräte.
4. Wählen Sie einen Geräte-Instanznamen, um die Details der Geräteinstanz anzuzeigen.

Ein Amazon One-Gerät neu starten

Das folgende Verfahren beschreibt, wie Sie Ihr Amazon One-Gerät neu starten.

Um ein Amazon One-Gerät neu zu starten

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.

2. Wählen Sie im Navigationsbereich die Option Geräteinstanz aus.
3. Wählen Sie unter Aktivierte Instanzen den Instanznamen des Geräts aus, das Sie neu starten möchten.
4. Wählen Sie Reboot, um das Amazon One-Gerät neu zu starten.

Aktualisierung der Amazon One-Gerätekonfigurationen

Das folgende Verfahren beschreibt, wie Sie Amazon One-Gerätekonfigurationen aktualisieren.

So aktualisieren Sie Amazon One-Gerätekonfigurationen

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Geräteinstanz aus.
3. Wählen Sie unter Aktivierte Instanzen den Instanznamen des Geräts aus, das Sie aktualisieren möchten.
4. Wählen Sie unter Gerätekonfigurationen die Option Bearbeiten aus.

> **Note**
>
> Um den Amazon One-Gerätemodus zu ändern, müssen Sie zuerst die Geräteinstanz deaktivieren und sie dann mit dem gewünschten Gerätemodus konfigurieren (siehe Konfigurieren Sie eine Geräte-Instance für die Aktivierung). Anschließend können Sie den Geräteaktivierungsprozess durchführen (siehe Amazon One-Gerät aktivieren).

5. Nachdem Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Gerätekonfigurationen aktualisieren, um das Update zu bestätigen.

Aktualisierung der Wi-Fi-Anmeldeinformationen

Das folgende Verfahren beschreibt, wie Sie Wi-Fi-Anmeldeinformationen aktualisieren.

Um WLAN-Anmeldeinformationen zu aktualisieren

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Geräteinstanz aus.

3. Wählen Sie unter Aktivierte Instanzen den Instanznamen des Geräts aus, das Sie aktualisieren möchten.
4. Wählen Sie unter Netzwerk die Option Bearbeiten aus.
5. Nehmen Sie unter Wi-Fi-Konfigurationen die gewünschten Änderungen vor.
6. Wählen Sie Netzwerk aktualisieren, um das Update zu bestätigen.

Geräteinstanzen deaktivieren

Das folgende Verfahren beschreibt, wie Geräteinstanzen deaktiviert werden.

Um Geräteinstanzen zu deaktivieren

1. Öffnen Sie die Amazon One Enterprise-Konsole unter https://console.aws.amazon.com/one-enterprise.
2. Wählen Sie im Navigationsbereich die Option Geräteinstanz aus.
3. Wählen Sie unter Aktivierte Instanzen den Namen der Geräteinstanz aus, die Sie deaktivieren möchten.
4. Wählen Sie Gerät deaktivieren.
5. Um die Deaktivierung zu bestätigen, geben Sie „Deaktivieren“ in das Nachrichtenfeld ein und wählen Sie Gerät deaktivieren.

Sicherheit

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon One Enterprise gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung von Amazon One Enterprise anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon One Enterprise konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Amazon One Enterprise-Ressourcen überwachen und sichern können.

Themen

- Datenschutz in Amazon One Enterprise
- Identitäts- und Zugriffsmanagement für Amazon One Enterprise
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise
- Konformitätsvalidierung für Amazon One Enterprise

Datenschutz in Amazon One Enterprise

Das AWS Modell der mit gilt für den Datenschutz in Amazon One Enterprise. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der

alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon One Enterprise oder einem anderen Unternehmen AWS-Services über die Konsole AWS CLI, API oder arbeiten AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Um die Standardverschlüsselung von Daten im Ruhezustand zu verwenden

Amazon One Enterprise bietet standardmäßig Verschlüsselung, um sensible Daten im Ruhezustand mithilfe von AWS-Verschlüsselungsschlüsseln zu schützen.

AWS-eigene Schlüssel — Amazon One Enterprise verwendet diese Schlüssel standardmäßig, um sensible Endbenutzerdaten automatisch zu verschlüsseln. Sie können AWS-eigene Schlüssel nicht anzeigen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme zum Schutz der Schlüssel ändern, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie unter AWS-eigene Schlüssel im AWS Key Management Service Developer Guide.

Verschlüsseln von Daten während der Übertragung.

Amazon One Enterprise verwendet Transport Layer Security (TLS) zur Sicherung von Daten und Signature Version 4 zur Authentifizierung aller eingehenden API-Anfragen an AWS-Services. Diese Verschlüsselung ist standardmäßig aktiviert.

Identitäts- und Zugriffsmanagement für Amazon One Enterprise

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon One Enterprise-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So arbeitet Amazon One Enterprise mit IAM
- Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise
- AWS verwaltete Richtlinien für Amazon One Enterprise

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon One Enterprise ausführen.

Servicebenutzer — Wenn Sie den Amazon One Enterprise-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Amazon One Enterprise-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in Amazon One Enterprise nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Amazon One-Identität und -Zugriff.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für Amazon One Enterprise-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon One Enterprise. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon One Enterprise Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon One Enterprise nutzen kann, finden Sie unterSo arbeitet Amazon One Enterprise mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon One Enterprise zu verwalten. Beispiele für identitätsbasierte Amazon One Enterprise-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen

Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem

beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe einen Namen geben IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management

Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen

mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein

bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten

ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So arbeitet Amazon One Enterprise mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon One Enterprise zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Amazon One Enterprise verfügbar sind.

IAM-Funktionen, die Sie mit Amazon One Enterprise verwenden können

IAM-Feature	Unterstützung für Amazon One Enterprise
Identitätsbasierte Richtlinien	Ja

IAM-Feature	Unterstützung für Amazon One Enterprise
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie Amazon One Enterprise und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Services, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Amazon One Enterprise

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer

identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Beispiele für identitätsbasierte Richtlinien von Amazon One Enterprise finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Ressourcenbasierte Richtlinien innerhalb von Amazon One Enterprise

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für Amazon One Enterprise

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Amazon One Enterprise-Aktionen finden Sie unterAktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise.

Richtlinienaktionen in Amazon One Enterprise verwenden das folgende Präfix vor der Aktion:

```
one
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

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

Beispiele für identitätsbasierte Richtlinien von Amazon One Enterprise finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Richtlinienressourcen für Amazon One Enterprise

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Amazon One Enterprise-Ressourcentypen und ihrer Ressourcen sowie Informationen darüber ARNs, mit welchen Aktionen Sie den ARN der einzelnen Ressourcen angeben können, finden Sie unterAktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise.

Beispiele für identitätsbasierte Richtlinien von Amazon One Enterprise finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Schlüssel für Richtlinienbedingungen für Amazon One Enterprise

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation

aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Amazon One Enterprise-Bedingungsschlüssel und Informationen darüber, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unterAktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise.

Beispiele für identitätsbasierte Richtlinien von Amazon One Enterprise finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

ACLs bei Amazon One Enterprise

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Amazon One Enterprise

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Amazon One Enterprise verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Hauptberechtigungen für Amazon One Enterprise

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion

in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Amazon One Enterprise

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Amazon One Enterprise beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon One Enterprise Sie dazu anleitet.

Servicebezogene Rollen für Amazon One Enterprise

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon One Enterprise-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon One Enterprise definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie Aktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Amazon One Enterprise-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Nur-Lese-Zugriff auf Amazon One Enterprise
- Voller Zugriff auf Amazon One Enterprise
- Unterstützte Berechtigungen auf Ressourcenebene für Amazon One Enterprise Rule API-Aktionen
- Zusätzliche Informationen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon One Enterprise-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst

Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon One Enterprise-Konsole

Um auf die Amazon One Enterprise-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon One Enterprise-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen weiterhin die Amazon One Enterprise-Konsole verwenden können, fügen Sie den Entitäten auch die Amazon One Enterprise `ConsoleAccess` - oder `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "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": "*"
        }
    ]
}
```

Nur-Lese-Zugriff auf Amazon One Enterprise

Das folgende Beispiel zeigt eine AWS verwaltete Richtlinie, `AmazonOneEnterpriseReadOnlyAccess` die Amazon One Enterprise schreibgeschützten Zugriff gewährt.

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

In den Richtlinienanweisungen gibt das Element `Effect` an, ob die Aktionen zugelassen oder verweigert werden. Das Element `Action` listet die spezifischen Aktionen auf, die der Benutzer ausführen darf. Das Element `Resource` listet die AWS -Ressourcen auf, für die der Benutzer diese Aktionen ausführen darf. Bei Richtlinien, die den Zugriff auf Amazon One Enterprise-Aktionen

steuern, ist das `Resource` Element immer auf gesetzt`*`, ein Platzhalter, der „alle Ressourcen“ bedeutet.

Die Werte im `Action` Element entsprechen denen, die von den APIs Diensten unterstützt werden. Den Aktionen ist ein Hinweis vorangestelltconfig:, dass sie sich auf Amazon One Enterprise-Aktionen beziehen. Sie können das Platzhalterzeichen `*` im Element `Action` beispielsweise wie folgt verwenden:

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

  Dies ermöglicht alle Amazon One Enterprise-Aktionen, die mit "DeviceInstance" (`GetDeviceInstanceConfiguration`,`CreateDeviceInstanceConfiguration`) enden.
- `"Action": ["one:*"]`

  Dies ermöglicht alle Amazon One Enterprise-Aktionen, jedoch keine Aktionen für andere AWS Dienste.
- `"Action": ["*"]`

  Dies ermöglicht alle AWS Aktionen. Diese Berechtigung ist für einen Benutzer geeignet, der als AWS Administrator für Ihr Konto fungiert.

Die Richtlinie „Nur Lesen“ gewährt Benutzern keine Berechtigungen für Aktionen wie `CreateDeviceInstanceUpdateDeviceInstance`, und. `DeleteDeviceInstance` Benutzer mit dieser Richtlinie dürfen keine Geräteinstanz erstellen, eine Geräteinstanz aktualisieren oder eine Geräteinstanz löschen. Eine Liste der Amazon One Enterprise-Aktionen finden Sie unterAktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise.

Voller Zugriff auf Amazon One Enterprise

Das folgende Beispiel zeigt eine Richtlinie, die vollen Zugriff auf Amazon One Enterprise gewährt. Es gewährt Benutzern die Erlaubnis, alle Amazon One Enterprise-Aktionen durchzuführen.

> **Important**
>
> Diese Richtlinie gewährt umfassende Berechtigungen. Bevor Sie Vollzugriff gewähren, sollten Sie gegebenenfalls mit einem Mindestsatz von Berechtigungen beginnen und zusätzliche

Berechtigungen nach Bedarf gewähren. Diese Methode ist besser, als anfangs zu weit gefasste Berechtigungen zu gewähren und dann später zu versuchen, sie zu begrenzen.

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

Unterstützte Berechtigungen auf Ressourcenebene für Amazon One Enterprise Rule API-Aktionen

Berechtigungen auf Ressourcenebene bedeutet, dass Sie angeben können, für welche Ressourcen die Benutzer Aktionen ausführen dürfen. Amazon One Enterprise unterstützt Berechtigungen auf Ressourcenebene für bestimmte Amazon One Enterprise-Regel-API-Aktionen. Das bedeutet, dass Sie für bestimmte Amazon One Enterprise-Regelaktionen die Bedingungen kontrollieren können, unter denen Benutzer diese Aktionen verwenden dürfen. Diese Bedingungen können Aktionen sein, die erfüllt sein müssen, oder bestimmte Ressourcen, die von den Benutzern verwendet werden dürfen.

In der folgenden Tabelle werden die API-Aktionen für Amazon One Enterprise-Regeln beschrieben, die derzeit Berechtigungen auf Ressourcenebene unterstützen. Außerdem werden die unterstützten Ressourcen und ihre ARNs für jede Aktion benötigten Ressourcen beschrieben. Wenn Sie einen ARN angeben, können Sie den Platzhalter * in Ihren Pfaden verwenden, z. B. wenn Sie die genaue Ressource IDs nicht angeben können oder wollen.

> **Important**
>
> Wenn eine Amazon One Enterprise-Regel-API-Aktion in dieser Tabelle nicht aufgeführt ist, unterstützt sie keine Berechtigungen auf Ressourcenebene. Wenn eine Amazon One Enterprise-Regelaktion keine Berechtigungen auf Ressourcenebene unterstützt, können Sie

Benutzern Berechtigungen zur Verwendung der Aktion gewähren. Sie müssen jedoch ein Sternchen für das Ressourcenelement in Ihrer Richtlinienerklärung angeben.

API-Aktion	Ressourcen
CreateDeviceInstance	Geräte-Instance arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
GetDeviceInstance	Geräte-Instanz arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
UpdateDeviceInstance	Geräte-Instanz arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteDeviceInstance	Geräte-Instanz arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceActivationQrCode	Geräte-Instanz arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteAssociatedDevice	Geräte-Instanz arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
RebootDevice	Geräte-Instanz arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*

API-Aktion	Ressourcen
CreateDeviceInstanceConfiguration	Konfiguration der Geräteinstanz arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
GetDeviceInstanceConfiguration	Konfiguration der Geräteinstanz arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
CreateSite	Site arn:aws:one ::site/ *region:accountID siteId*
DeleteSite	Site arn:aws:one ::site/ *region:accountID siteId*
GetSiteAddress	Site arn:aws:one ::site/ *region:accountID siteId*
UpdateSite	Site arn:aws:one ::site/ *region:accountID siteId*
UpdateSiteAddress	Site arn:aws:one ::site/ *region:accountID siteId*
CreateDeviceConfigurationTemplate	Vorlage für die Gerätekonfiguration arn:aws:one::/*region:accountID* device-configuration-template*templateId*
DeleteDeviceConfigurationTemplate	Vorlage für die Gerätekonfiguration arn:aws:one::/*region:accountID* device-configuration-template*templateId*

API-Aktion	Ressourcen
GetDeviceConfigurationTemplate	Vorlage für die Gerätekonfiguration arn:aws:one::/*region:accountID* device-configuration-template*templateId*
UpdateDeviceConfigurationTemplate	Vorlage für die Gerätekonfiguration arn:aws:one::/*region:accountID* device-configuration-template*templateId*

Angenommen, Sie möchten bestimmten Benutzern den Lesezugriff auf bestimmte Regeln erteilen und den Schreibzugriff verweigern.

In der ersten Richtlinie erlauben Sie der AWS Config Regel Leseaktionen, z. B. `GetSite` für die angegebenen Regeln.

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

In der zweiten Richtlinie verweigern Sie der Amazon One Enterprise-Regel Schreibaktionen für die spezifische Regel.

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

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

Mit Berechtigungen auf Ressourcenebene können Sie Lesezugriff gewähren und Schreibzugriff verweigern, um bestimmte Aktionen für Amazon One Enterprise Rule API-Aktionen auszuführen.

Zusätzliche Informationen

Weitere Informationen zum Erstellen von IAM-Benutzern, Gruppen, Richtlinien und Berechtigungen finden Sie unter Erstellen Ihrer ersten IAM-Benutzer- und -Administratorgruppe und Zugriffsverwaltung im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für Amazon One Enterprise

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AmazonOneEnterpriseFullAccess

Diese Richtlinie gewährt Administratorberechtigungen, die den Zugriff auf alle Ressourcen und Abläufe von Amazon One Enterprise ermöglichen.

`one:*`Ermöglicht es Ihnen, alle Amazon One Enterprise-Aktionen durchzuführen.

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

AmazonOneEnterpriseReadOnlyAccess

Diese Richtlinie gewährt allen Amazon One Enterprise-Ressourcen und -Vorgängen nur Leseberechtigungen.

`one:Get*`Ruft die Amazon One Enterprise-Ressourcen ab.

`one:List*`Listet die Amazon One Enterprise-Ressourcen auf.

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

AmazonOneEnterpriseInstallerAccess

Diese Richtlinie gewährt eingeschränkte Lese- und Schreibberechtigungen, mit denen Sie einen Aktivierungs-QR-Code für jede konfigurierte Geräteinstanz erstellen können, um das Gerät an einem beliebigen Standort zu aktivieren.

`one:CreateDeviceActivationQrCode`Ermöglicht es Ihnen, einen QR-Code zur Aktivierung des Geräts zu erstellen.

`one:GetDeviceInstance`Ermöglicht das Abrufen von Informationen zu einer Amazon One-Geräteinstanz.

`one:GetSite`Ermöglicht das Abrufen von Informationen zu einer Amazon One Enterprise-Site.

`one:GetSiteAddress`Ermöglicht das Abrufen der physischen Adresse einer Amazon One Enterprise-Site.

`one:ListDeviceInstances`Ermöglicht es Ihnen, die Amazon One-Geräteinstanzen aufzulisten.

`one:ListSites`Lassen Sie sich die Amazon One Enterprise-Websites auflisten.

```
{
 "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 Enterprise-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon One Enterprise an, die seit Beginn der Nachverfolgung dieser Änderungen durch diesen Service vorgenommen wurden. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Amazon One Enterprise Document-Verlaufsseite.

Änderung	Beschreibung	Datum
Amazon One Enterprise hinzugefügt AmazonOne MetricPublishAccess	Die genannte Rollenberechtigungsrichtlinie AmazonOneMetricPublishAccess ermöglicht es Amazon One Enterprise, Folgendes auszuführen CloudWatch: PutMetricData im CloudWatch Namespace AmazonOne AWS/.	6. Februar 2025
Amazon One Enterprise hat mit der Nachverfolgung von Änderungen begonnen	Amazon One Enterprise hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	1. Dezember 2023

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise

Amazon One Enterprise (Servicepräfix: `one`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Themen

- Von Amazon One Enterprise definierte Aktionen
- Von Amazon One Enterprise definierte Ressourcentypen
- Bedingungsschlüssel für Amazon One Enterprise

Von Amazon One Enterprise definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeviceInstance	Erteilen Sie die Erlaubnis, eine Geräteinstanz zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	Erteilen Sie die Erlaubnis, Informationen zur Geräteinstanz abzurufen	Lesen	Geräte-Instanz*		
ListDeviceInstances	Erteilen Sie die Erlaubnis, Geräteinstanzen aufzulisten	Lesen			
UpdateDeviceInstance	Erteilen Sie die Erlaubnis, die Geräteinstanz zu aktualisieren	Schreiben	Geräte-Instanz*		
DeleteDeviceInstance	Erteilen Sie die Erlaubnis zum Löschen der Geräteinstanz	Schreiben	Geräte-Instanz*		
CreateDeviceActivationQrCode	Erteilen Sie die Erlaubnis, einen QR-Code zur Aktivieru	Schreiben	Geräte-Instanz*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	ng eines Geräts auf einer Geräteinstanz zu erstellen				
DeleteAssociatedDevice	Erteilen Sie die Erlaubnis, die Verknüpfung zwischen Gerät und Geräteinstanz zu löschen	Schreiben	Geräte-Instanz*		
RebootDevice	Erteilen Sie die Erlaubnis, das Gerät neu zu starten	Schreiben	Geräte-Instanz*		
CreateDeviceInstanceConfiguration	Erteilen Sie die Erlaubnis, eine Geräteinstanzkonfiguration zu erstellen	Schreiben			
GetDeviceInstanceConfiguration	Erteilen Sie die Erlaubnis, Informationen zur Konfiguration der Geräteinstanz abzurufen	Lesen	Konfiguration*		
CreateSite	Erteilen Sie die Erlaubnis, eine Site zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	Erteilen Sie die Erlaubnis zum Löschen der Geräteinstanz	Schreiben	Webseiten*		
GetSite	Erteilen Sie die Erlaubnis, Informationen über die Website zu erhalten	Lesen	Webseiten*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSites	Erteilen Sie die Erlaubnis, Websites aufzulisten	Lesen			
GetSiteAddress	Erteilen Sie die Erlaubnis, Informationen zur Adresse der Website abzurufen	Lesen	Webseiten *		
UpdateSite	Erteilen Sie die Erlaubnis, die Website zu aktualisieren	Schreiben	Webseiten *		
UpdateSiteAddress	Erteilen Sie die Erlaubnis, die Adresse der Website zu aktualisieren	Schreiben	Webseiten *		
CreateDeviceConfigurationTemplate	Erteilen Sie die Erlaubnis, eine Geräteinstanz zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	Erteilen Sie die Erlaubnis zum Löschen der Gerätekonfigurationsvorlage	Schreiben	device-configuration-template*		
GetDeviceConfigurationTemplate	Erteilen Sie die Erlaubnis, Informationen zur Gerätekonfigurationsvorlage abzurufen	Lesen	device-configuration-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDeviceConfigurationTemplates	Erteilen Sie die Erlaubnis, Gerätekonfigurationsvorlagen aufzulisten	Lesen			
UpdateDeviceConfigurationTemplate	Erteilen Sie die Erlaubnis, die Gerätekonfigurationsvorlage zu aktualisieren	Schreiben	device-configuration-template*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Tagging	Geräteinstanz, Standort, device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	Geräteinstanz, Standort, device-configuration-template	aws:TagKeys	
ListTagForResources	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			

Von Amazon One Enterprise definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
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}

Bedingungsschlüssel für Amazon One Enterprise

Amazon One Enterprise definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tags aus der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	String
aws:TagKeys	Filtert den Zugriff nach Tag-Schlüsseln aus der Anforderung	ArrayOfString

Konformitätsvalidierung für Amazon One Enterprise

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den

Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.

- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Überwachung von Amazon One Enterprise

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon One Enterprise und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Amazon One Enterprise zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse im AWS Rahmen von Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachung von Amazon One Enterprise-Ereignissen in Amazon EventBridge

Sie können Amazon One Enterprise-Ereignisse überwachen EventBridge, das einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, software-as-a-service (SaaS-) Anwendungen und AWS Diensten bereitstellt. EventBridgeleitet diese Daten an Ziele wie AWS Lambda Amazon Simple Notification Service weiter. Diese Ereignisse liefern einen Strom von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit.

Abonnieren Sie Amazon One Enterprise-Veranstaltungen

Ereignisse zur Änderung des Geräte- und Benutzerprofilstatus von Amazon One werden mithilfe von Amazon One veröffentlicht und können in der EventBridge Konsole aktiviert werden EventBridge, indem eine neue Regel erstellt wird. Ereignisse werden in keiner bestimmten Reihenfolge angeboten, besitzen jedoch einen Zeitstempel, der Ihnen die Datennutzung ermöglicht. Ereignisse werden auf bestmögliche Weise ausgegeben.

Um Amazon One Enterprise-Veranstaltungen zu abonnieren

1. Melden Sie sich bei Ihrer AWS-Konsole an unter https://console.aws.amazon.com/events/.
2. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.
3. Wählen Sie im Navigationsbereich unter Busse die Option Regeln aus.
4. Wählen Sie Regel erstellen aus.
5. Weisen Sie der Regel auf der Detailseite der Standardregel einen Namen zu.
6. Wählen Sie Rule with an event pattern 8Regel mit einem Ereignismuster) und dann Next (Weiter) aus.
7. Vergewissern Sie sich, dass auf der Seite Ereignismuster erstellen unter Ereignisquelle die Option AWS Ereignisse oder EventBridge Partnerereignisse ausgewählt ist.
8. Wählen Sie unter Beispiel-Ereignistyp die Option AWS-Ereignisse aus.
9. Wählen Sie als Erstellungsmethode die Option Benutzerdefiniertes Muster aus.
10. Fügen Sie im Abschnitt Ereignismuster eine JSON-Datei mit der Ereignisquelle `aws:one` und dem erforderlichen Detailtyp hinzu:

```
"
source": ["aws.one"],
"detail-type": ["New Successful Enrollment",
"New Successful Un-enrollment",
"Unsuccessful Enrollment",
"Unsuccessful Un-enrollment",
"Successful Recognition",
"Unsuccessful Recognition"]
}
```

    Sie können den erforderlichen Detailtyp aus der obigen Liste auswählen und die nicht erforderlichen Daten entfernen.

11. Wählen Sie Weiter.
12. Wählen Sie auf der Seite Ziel (e) auswählen ein Ziel Ihrer Wahl aus, das eine Lambda-Funktion, eine SQS-Warteschlange oder ein SNS-Thema enthält. Informationen zur Konfiguration von Zielen finden Sie unter EventBridge Amazon-Ziele.

Um beispielsweise zu sehen, wann sich jemand angemeldet hat, wählen Sie „Erfolgreiche Anerkennung“. Schauen Sie sich dann die Veranstaltungsdetails (im Anhang) an, um zu sehen, wer sich angemeldet hat.

Um Ihren Workflow abzuschließen, können Sie eine externe API oder ein anderes Ziel ausführen.

13. Optional können Sie Tags konfigurieren.
14. Wählen Sie auf der Seite Überprüfen und erstellen die Option Regel erstellen aus. Weitere Informationen zur Konfiguration von Regeln finden Sie unter EventBridgeRegeln im EventBridge Benutzerhandbuch.

Ereignistypen zur Änderung des Gerätestatus

Ereignisse zur Änderung des Gerätestatus werden in JSON generiert. Für jeden Ereignistyp wird ein JSON-Blob entsprechend Ihrer Regelkonfigurierung an das Ziel Ihrer Wahl gesendet. Die folgenden Detailtypen sind verfügbar:

Der Status des Geräts wurde auf „Gesund“ geändert

Das Gerät hat alle Zustandsprüfungen bestanden.

Der Status Health Geräts wurde auf Kritisch geändert

Das Gerät hat eine oder mehrere Integritätsprüfungen nicht bestanden.

Die Gerätekonnektivität wurde auf Offline geändert

Das Gerät ist nicht mit dem Internet verbunden.

Die Gerätekonnektivität wurde auf Online geändert

Das Gerät ist mit dem Internet verbunden.

Ressourcen

Enthält die Liste der DeviceInstance-Arn, für die das Ereignis Device Status Change veröffentlicht wurde.

Metadaten

Name der Website

- Name der Site, auf der die DeviceInstance vorhanden ist.

SiteN

- Arn für die Site, auf der die DeviceInstance vorhanden ist.

data

Aktuelle Konnektivität

- Stellt dar, ob die DeviceInstance mit dem Internet verbunden oder getrennt ist.
- Mögliche Werte: CONNECTED, DISCONNECTED

Frühere Konnektivität

- Stellt dar, ob die DeviceInstance vor dem Ereignis mit dem Internet verbunden oder vom Internet getrennt war.
- Mögliche Werte: CONNECTED, DISCONNECTED

currentHealthStatus

- Stellt dar, ob die DeviceInstance alle Integritätsprüfungen bestanden hat.
- Mögliche Werte: HEALTHY, CRITICAL

previousHealthStatus

- Gibt an, ob die DeviceInstance bei der letzten Überprüfung alle Integritätsprüfungen bestanden hat.
- Mögliche Werte: HEALTHY, CRITICAL

assetTagId

- Das Gerät, das assetTagId der DeviceInstance zugeordnet ist.

deviceInstanceName

- Der Name der DeviceInstance, für die das Gerätestatus-Ereignis veröffentlicht wurde.

Ereignistypen für Benutzerprofile

Es gibt folgende Typen von Ereignisdetails im Zusammenhang mit Benutzerprofilen:

Neue erfolgreiche Registrierung

Wenn sich ein Benutzer erfolgreich registriert hat.

Neue erfolgreiche Abmeldung

Wenn sich ein Benutzer erfolgreich abgemeldet hat.

Fehlgeschlagene Registrierung

Wenn sich ein Benutzer nicht registrieren konnte.

Abmeldung erfolglos

Wenn ein Benutzer die Registrierung nicht abmelden konnte.

Erfolgreiche Anerkennung

Wenn ein Benutzer Palm erfolgreich zur Authentifizierung scannt.

Erfolglose Anerkennung

Wenn die Erkennung eines Handflächenscans fehlschlug.

Ressourcen

Enthält die Liste der Benutzerprofil-ARN, für die das Benutzerprofilereignis veröffentlicht wurde.

data

accountId

- Das relevante AWS Konto für das Gerät, das die Anfrage initiiert hat.

Quelle der Anfrage

- Dies ist das deviceInstanceId des Geräts, das die Anfrage initiiert hat.

Erstellter Zeitstempel

- Die Uhrzeit der Erstellung des Ereignisses.

Benutzerstatus

- Der aktuelle Status des Benutzers.
- Mögliche Werte: ACTIVE, DELETED

Assoziierte ID

- Die zugehörige ID des Benutzers, zum Beispiel die Badge-ID.

Grund

- Dieser Wert wird für erfolglose Ereignisse angezeigt. Er enthält den Grund, warum das Ereignis nicht erfolgreich war.

Beispielereignisse

Die folgenden Beispiele zeigen Ereignisse für Amazon One Enterprise.

Themen

- Der Status des Geräts wurde auf „Gesund“ geändert
- Der Gesundheitsstatus des Geräts wurde auf Kritisch geändert
- Die Gerätekonnektivität wurde auf „Online“ geändert
- Die Gerätekonnektivität wurde auf offline geändert

Der Status des Geräts wurde auf „Gesund“ geändert

Das Gerät hat alle Integritätsstufen bestanden und der Integritätsstatus der Geräteinstanz wurde von KRITISCH auf GESUND geändert.

```
{
    "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"
    }
```

```
  }
}
```

Der Gesundheitsstatus des Geräts wurde auf Kritisch geändert

Das Gerät hat eine oder mehrere Integritätsprüfungen nicht bestanden, und der Systemstatus der Geräteinstanz wurde von HEALTHY auf KRITISCH geändert.

```
{
  "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"
    }
  }
}
```

Die Gerätekonnektivität wurde auf „Online“ geändert

Das Gerät ist mit dem Internet verbunden und der Konnektivitätsstatus der Geräteinstanz wurde von DISCONNECTED auf CONNECTED geändert.

```
{
  "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"
    }
  }
}
```

Die Gerätekonnektivität wurde auf offline geändert

Das Gerät ist nicht mit dem Internet verbunden und der Konnektivitätsstatus der Geräteinstanz wurde von CONNECTED in DISCONNECTED geändert.

```
{
  "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"
    }
  }
}
```

Protokollieren von Amazon One Enterprise API-Aufrufen mit AWS CloudTrail

Amazon One Enterprise ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon One Enterprise ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Amazon One Enterprise als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon One Enterprise-Konsole und Code-Aufrufe an die Amazon One Enterprise API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon One Enterprise. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Amazon One Enterprise gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu Amazon One Enterprise in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in Amazon One Enterprise auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Amazon One Enterprise, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Amazon One Enterprise-Aktionen werden von protokolliert CloudTrail und sind dokumentiert in derAktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise. Beispielsweise generieren Aufrufe von `RebootDevice` und `DeleteDeviceInstance` Aktionen Einträge in den CloudTrail Protokolldateien. `ListSites`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu Amazon One Enterprise-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateSite` Aktion demonstriert.

```
{
    "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"
}
```

Problembehebung bei Amazon One

Wenn Sie Probleme mit der Amazon One-Anwendung oder einem Ihrer Amazon One-Geräte haben, verwenden Sie diese Vorschläge, um das Problem zu beheben. Wenn Sie dann immer noch Probleme haben, wenden Sie sich an den AWS-Support.

Themen

- Fehlerbehebung bei Amazon One-Identität und -Zugriff
- Fehlerbehebung bei der Amazon One Console
- Fehlerbehebung beim Amazon One-Gerät

Fehlerbehebung bei Amazon One-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon One Enterprise und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon One durchzuführen
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon One-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Amazon One durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `one:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `one:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon One-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon One Enterprise diese Funktionen unterstützt, finden Sie unterSo arbeitet Amazon One Enterprise mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Fehlerbehebung bei der Amazon One Console

Wenn Sie Probleme mit der Amazon One-Anwendung oder einem Ihrer Amazon One-Geräte haben, verwenden Sie diese Vorschläge, um das Problem zu beheben. Wenn Sie dann immer noch Probleme haben, wenden Sie sich an den AWS-Support.

Themen

- Ich kann keine Site erstellen

- Ich kann keine Geräte-Instance erstellen
- Ich kann keine Konfigurationsvorlage erstellen
- Ich kann keinen Aktivierungs-QR-Code erstellen

Ich kann keine Site erstellen

- Wenden Sie sich an Ihren Amazon One Console-Administrator, um Ihnen Zugriff zu gewähren.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Ich kann keine Geräte-Instance erstellen

- Wenden Sie sich an Ihren Amazon One Console-Administrator, um Ihnen Zugriff zu gewähren.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Ich kann keine Konfigurationsvorlage erstellen

- Wenden Sie sich an Ihren Amazon One Console-Administrator, um Ihnen Zugriff zu gewähren.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Ich kann keinen Aktivierungs-QR-Code erstellen

- Wenden Sie sich an Ihren Amazon One Console-Administrator, um Ihnen Zugriff zu gewähren.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Fehlerbehebung beim Amazon One-Gerät

Wenn Sie Probleme mit der Amazon One Console oder einem Ihrer Amazon One-Geräte haben, verwenden Sie diese Vorschläge, um das Problem zu beheben. Wenn Sie dann immer noch Probleme haben, wenden Sie sich an den AWS-Support.

Themen

- Leerer Bildschirm
- Ich kann keine Verbindung zu WLAN oder Netzwerk herstellen

- Ein Gerät mit aktiven Warnmeldungen neu starten
- Systemfehler
- Der QR-Code wird nicht erkannt
- Der QR-Code kann nicht gelesen werden
- Es wurden mehrere QR-Codes erkannt
- Die Geräteinstanz ist nicht vorhanden
- Die Seite wurde nicht gefunden
- Die Postleitzahl stimmt nicht überein
- Gateway hat das Zeitlimit überschritten
- Ich kann das Gerät nicht konfigurieren
- Das Gerät wurde mit Fehlermeldung und Fehlercode neu gestartet
- Amazon-Logo auf dem Gerätebildschirm ohne weitere Aktivität
- Vorübergehend nicht verfügbar
- Bei uns ist etwas schief gelaufen
- Vorübergehend außer Betrieb
- Das Amazon One-Gerät ist physisch beschädigt
- Palm kann nicht gelesen werden
- Palm wurde nicht erkannt
- Das Gerät wurde aufgrund längerer Inaktivität gesperrt
- Das Gerät wurde aufgrund eines Manipulationsereignisses gesperrt

Leerer Bildschirm

Dies tritt auf, wenn das Gerät nicht mit Strom versorgt wird oder beim Neustart hängen bleibt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Warten Sie einige Augenblicke (weniger als 30 Sekunden), falls das Gerät neu gestartet wird.
- Wenn der Lichtring pulsiert, während das Gerät leer ist, warten Sie bis zu 30 Sekunden.
- Prüfen Sie, ob das Netzkabel sowohl an der Steckdose als auch fest an der Rückseite des Amazon One-Geräts angeschlossen ist. Stellen Sie außerdem sicher, dass das Kabel nicht beschädigt ist.
- Überprüfen Sie die Stromquelle.

- Vergewissern Sie sich, dass alle Kabel ordnungsgemäß an den Amazon One und den USB-Hub angeschlossen sind.
- Starten Sie das Gerät von der Konsole aus neu.
- Wenn das Problem durch einen Neustart des Geräts nicht behoben wird, trennen Sie den Amazon One USB-Hub von der Stromversorgung und schließen Sie ihn dann wieder an.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Ich kann keine Verbindung zu WLAN oder Netzwerk herstellen

Dies tritt auf, wenn das Gerät die Konnektivität verliert.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wenn Sie mit WLAN verbunden sind, überprüfen Sie mit einem anderen Gerät, ob das WLAN in den verfügbaren Netzwerken angezeigt wird.
- Prüfen Sie, ob der Wi-Fi-Router eingeschaltet ist und sich in Reichweite befindet.
- Das Gerät stellt die Verbindung wieder her, sobald das Netzwerk wiederhergestellt ist.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS-Support.

Ein Gerät mit aktiven Warnmeldungen neu starten

Wenn ein Neustart von der Konsole aus angefordert wird, wartet der Vorgang bis zu 15 Minuten, bis das Gerät den Befehl empfängt und versucht, neu zu starten, auch wenn es offline ist oder Netzwerkprobleme auftreten.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Warten Sie, bis der Neustart abgeschlossen ist.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS-Support.

Systemfehler

Dies ist auf einen internen Fehler zurückzuführen.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie auf dem Bildschirm die Option Neu starten, um die Anwendung neu zu starten.

- Wenn das Problem nach zwei Versuchen nicht behoben ist, wenden Sie sich an den AWS-Support.

Der QR-Code wird nicht erkannt

Dies ist auf einen nicht autorisierten oder abgelaufenen QR-Code zurückzuführen.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Erneut versuchen, um zum QR-Code-Bildschirm zurückzukehren.
- Erstellen Sie einen neuen QR-Code auf der AWS-Konsole und scannen Sie dann den gültigen QR-Code.

Der QR-Code kann nicht gelesen werden

Dies tritt auf, wenn die Anwendung den QR-Code nicht lesen kann.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Erneut versuchen, um zum QR-Code-Bildschirm zurückzukehren.
- Wenn das Problem weiterhin besteht, brechen Sie den Aktivierungs-Workflow ab und starten Sie ihn neu.

Es wurden mehrere QR-Codes erkannt

Dies tritt auf, wenn mehrere QR-Codes gescannt werden.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Erneut versuchen, um zum QR-Code-Bildschirm zurückzukehren.
- Scannen Sie jeweils nur einen gültigen QR-Code.

Die Geräteinstanz ist nicht vorhanden

Dies tritt auf, wenn die Geräteinstanz gelöscht wird oder in der AWS-Konsole nicht vorhanden ist.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Erneut versuchen, um zum QR-Code-Bildschirm zurückzukehren.

- Suchen Sie in der AWS-Konsole nach der richtigen Geräteinstanz. Wenn die Geräteinstanz fehlt, wenden Sie sich an Ihren Administrator.
- Erstellen Sie einen neuen QR-Code für diese Geräteinstanz und scannen Sie dann den neuen QR-Code.

Die Seite wurde nicht gefunden

Dies tritt auf, wenn die Site gelöscht wird oder in der AWS-Konsole nicht vorhanden ist.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Informationen zur Website finden Sie in der AWS-Konsole. Wenn die Site nicht existiert, wenden Sie sich an Ihren Administrator.

Die Postleitzahl stimmt nicht überein

Dies tritt auf, wenn Sie eine andere Postleitzahl als die für das Gerät konfigurierte eingeben.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Erneut versuchen, um zum Bildschirm mit der Postleitzahl zurückzukehren.
- Prüfen Sie, ob Sie die richtige Postleitzahl für die Website angegeben haben.
- Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren Administrator, um die Postleitzahl der Site in der AWS-Konsole zu überprüfen.

Gateway hat das Zeitlimit überschritten

Dies tritt auf, wenn innerhalb einer bestimmten Zeit keine Antwort vom Gateway eingeht.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Neu starten, um die Anwendung neu zu starten.
- Wenn das Problem nach zwei Versuchen nicht behoben ist, wenden Sie sich an den AWS-Support.

Ich kann das Gerät nicht konfigurieren

Dies tritt auf, wenn der Vorgang die Konfiguration nicht auf der Gerätefestplatte speichern konnte.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie Neu starten, um die Anwendung neu zu starten.
- Wenn das Problem nach zwei Versuchen nicht behoben ist, wenden Sie sich an den AWS-Support.

Das Gerät wurde mit Fehlermeldung und Fehlercode neu gestartet

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wählen Sie „Neu starten“ und lassen Sie das Gerät wiederherstellen.
- Wenn das Gerät nicht wiederhergestellt werden kann, trennen Sie den USB-Hub von der Stromversorgung und schließen Sie ihn erneut an.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Amazon-Logo auf dem Gerätebildschirm ohne weitere Aktivität

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Warten Sie einige Augenblicke (weniger als 30 Sekunden), falls das Gerät neu gestartet wird.
- Trennen Sie den USB-Hub von der Stromversorgung und schließen Sie ihn erneut an.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Vorübergehend nicht verfügbar

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Stellen Sie sicher, dass die USB-Verbindungen mit dem Hostgerät/System sicher sind.
- Trennen Sie alle Kabel, die in den USB-Hub führen, und schließen Sie sie wieder an.
- Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Bei uns ist etwas schief gelaufen

Dies tritt auf, wenn ein interner Fehler vorliegt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Fahren Sie das Gerät herunter.
2. Trennen Sie das Gerät von der Stromversorgung.
3. Warte 30 Sekunden.
4. Schließen Sie das Gerät wieder an die Stromquelle an.
5. Schalten Sie das Gerät ein.
6. Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Vorübergehend außer Betrieb

Dies tritt auf, wenn das Gerät von Amazon One außer Betrieb genommen wurde.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Kontaktieren Sie den AWS Support.

Das Amazon One-Gerät ist physisch beschädigt

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Wenden Sie sich für die nächsten Schritte an den AWS-Support und geben Sie so viele Details wie möglich an, z. B. was passiert ist, wann es passiert ist und warum es passiert ist.

Palm kann nicht gelesen werden

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Vergewissern Sie sich, dass das Amazon One-Gerät frei von Streifen und Flecken ist.
- Stellen Sie sicher, dass die Handfläche des Kunden frei von Verschlüssen wie Bandagen, Ärmeln und starkem Schmutz/Öl ist.
- Wenn das Problem weiterhin besteht und das Gerät keine Handfläche liest, wenden Sie sich an den AWS-Support.

Palm wurde nicht erkannt

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Lassen Sie den Kunden versuchen, seine andere Handfläche zu verwenden.
- Stellen Sie sicher, dass der Kunde bereits registriert ist. Falls nicht, bitten Sie ihn, sich online oder auf dem Gerät zu registrieren.
- Wenn das Problem weiterhin besteht und das Gerät keinen Handkontakt erkennt, wenden Sie sich an den AWS-Support.

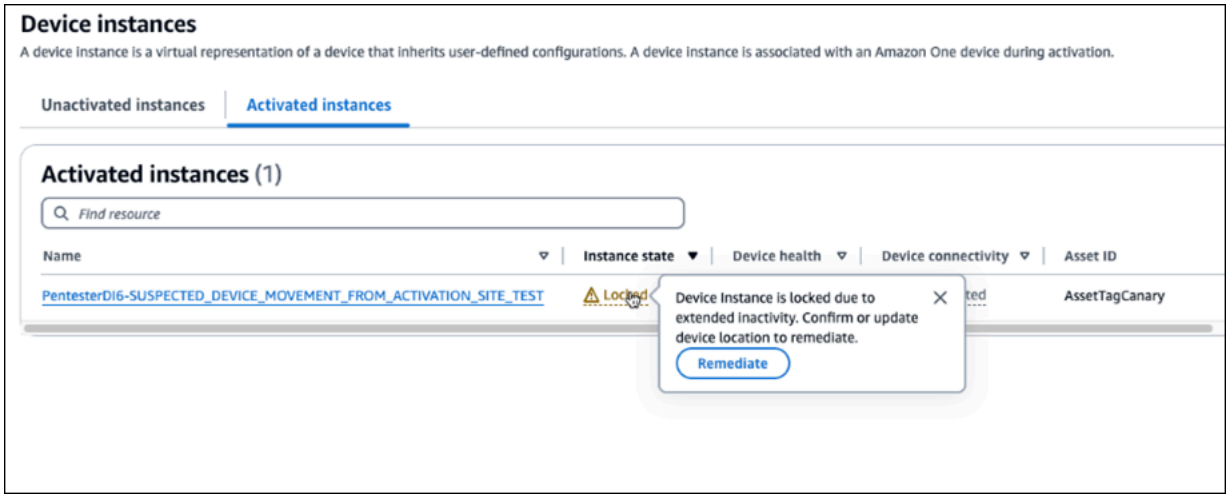
Das Gerät wurde aufgrund längerer Inaktivität gesperrt

Wenn das Gerät vermutet, dass es von der Aktivierungsseite entfernt wurde, werden Benutzer gesperrt. Dies tritt auf, wenn das Gerät die maximale Offline-Zeit von 120 Stunden überschreitet.

Gehen Sie wie folgt vor, um das Gerät zu entsperren:

1. Melden Sie sich bei Ihrer AWS-Konsole an und wählen Sie die Geräteinstanz aus.
2. Wählen Sie im Fehlerbanner oben auf der Seite die Option Remediate aus.

   Optional: Wählen Sie unter Aktivierte Instanzen die Option Gesperrt und dann Korrigieren aus.



3. Wenn sich das Gerät immer noch an der ursprünglichen Aktivierungsstelle befindet, wählen Sie Ja, das Gerät befindet sich an diesem Standort.
4. Wenn sich das Gerät an einem anderen Standort befindet, wählen Sie Nein, das Gerät befindet sich an einem anderen Standort. Wenn Sie Nein wählen, wird das Gerät deaktiviert. Aktivieren Sie das Gerät am neuen Standort.

Das Gerät wurde aufgrund eines Manipulationsereignisses gesperrt

Aus Sicherheitsgründen wird das Amazon One-Gerät im Falle eines Manipulationsereignisses gesperrt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Kontaktieren Sie den AWS Support.

Dokumentenverlauf für das Amazon One Enterprise-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon One Enterprise beschrieben.

Änderung	Beschreibung	Datum
Aktualisieren	Abschnitt mit serviceverknüpften Rollen hinzugefügt	4. Februar 2025
Aktualisieren	Hinzugefügt: Szenariogesteuerter Inhalt	10. Oktober 2024
Aktualisieren	Thema hinzugefügt: Fehlerbehebung bei der Amazon One Enterprise-Konsole	10. Oktober 2024
Aktualisieren	Thema hinzugefügt: Fehlerbehebung beim Amazon One Enterprise-Gerät	10. Oktober 2024
Aktualisieren	Kapitel hinzugefügt: Amazon One Enterprise einrichten	10. Oktober 2024
Aktualisieren	Thema hinzugefügt: Wartung und Reinigung von Amazon One Enterprise-Geräten	10. Oktober 2024
Aktualisieren	Inhalt neu organisiert	10. Oktober 2024
Aktualisieren	Thema hinzugefügt: Installation von Amazon One Enterprise Device I/O Hub für sicheren Zugriff	14. August 2024
Aktualisieren	Thema hinzugefügt: Installation eines an der Wand	5. Juni 2024

	montierbaren Amazon One Enterprise-Geräts	
Erstversion	Erste Version des Amazon One Enterprise User Guide	8. November 2023

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.