aws

Benutzerhandbuch

Amazon One Enterprise

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon One Enterprise: Benutzerhandbuch

Copyright © 2024 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?

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

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 5GHz), Ethernet, 2 x Typ A, 1 x USB Typ B USB
- Benutzerfeedback — 5,5-Zoll-Touchscreen, Lightring, Lautsprecher, Kopfhörer
- Physical Access Control Protocol — OSDP und Wiegand
- Stromversorgung —POE, AC/DC-Adapter mit VAC 110/220-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

Amazon One-Geräte kaufen

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 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 Enterprise

Amazon One Enterprise ist ein Cloud-basierter biometrischer Dienst, der ein Amazon One-Gerät verwendet, um einen Benutzer mithilfe seiner Handflächenbiometrie zu authentifizieren. Sie können Amazon One-Geräte bestellen, indem Sie uns kontaktieren, und Sie können sich für den Amazon One Enterprise Secure Access Service anmelden, indem Sie den AWS Management Console.

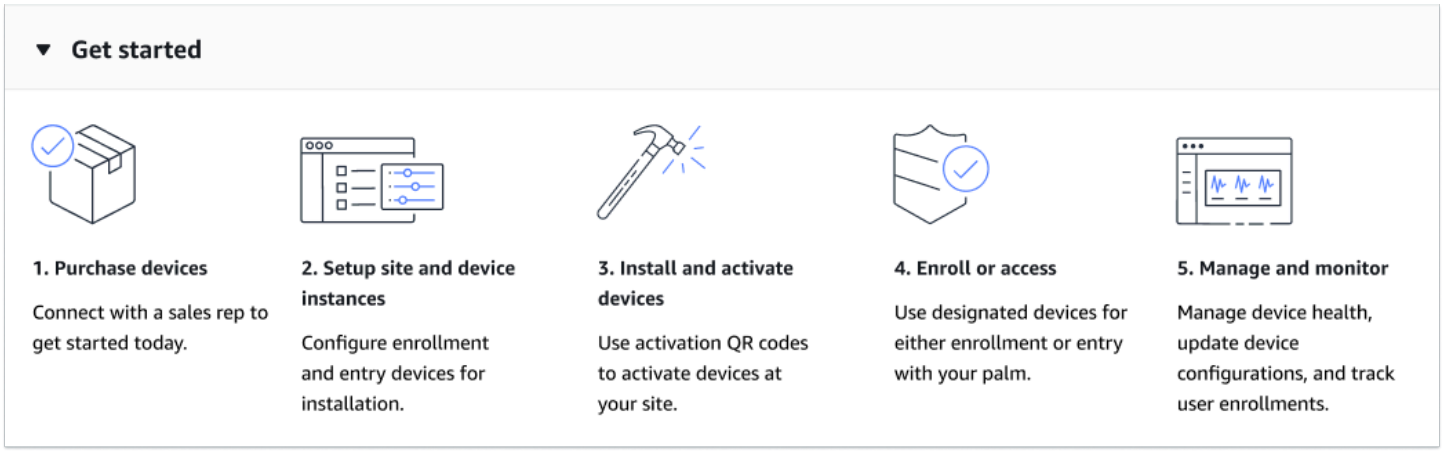
Nach der Installation von Amazon One Enterprise können Sie Geräte aktivieren und sie bei Ihrem AWS-Konto auf der Amazon One Enterprise Console registrieren und die Authentifizierungsanwendung verwenden. Sie können auch das biometrische Profil eines registrierten Mitarbeiters einsehen und die Registrierung eines Mitarbeiters stornieren. Wenn Mitarbeiter Ihr Unternehmen verlassen oder ihren Ausweis verlieren, können Sie ihre biometrischen Daten ganz einfach löschen. Die Amazon One Enterprise Console dient auch als zentraler Ort für die Verwaltung betrieblicher Aktivitäten, wie z. B. die Nachverfolgung installierter Geräte und die Anzeige monatlicher Rechnungen.

Mitarbeiter können sich registrieren, indem sie ihre Ausweise und Handflächen an überwachten Registrierungsstationen vor Ort scannen. Nachdem Mitarbeiter registriert sind, können sie einfach ihre Handfläche über ein Amazon One-Gerät bewegen, um einen sicheren Standort zu betreten oder zu verlassen.

Themen

Amazon One Enterprise-Arbeitsablauf

Das folgende Diagramm zeigt den grundlegenden Arbeitsablauf von Amazon One Enterprise.



1. Kaufen Sie ein Amazon One-Gerät, indem Sie uns kontaktieren.
2. Erstellen Sie Websites und Geräteinstanzen und konfigurieren Sie Registrierungs- und Eingabegeräte für die Installation.
3. Aktivieren Sie nach der Installation Amazon One-Geräte, indem Sie einen sicheren QR-Code scannen, der für die Geräteinstanz spezifisch ist.
4. Bitten Sie die Mitarbeiter, ihre Handflächen zu registrieren und sich dann mit ihren Handflächen zu authentifizieren, um Zugang zu erhalten.
5. Nutzen Sie Verwaltungs- und Überwachungsfunktionen: Stellen Sie den Zustand der Geräte sicher, halten Sie die Konfigurationen auf dem neuesten Stand und verfolgen Sie Benutzeranmeldungen, um einen umfassenden Überblick zu erhalten.

Wichtige Begriffe von Amazon One Enterprise

Dies sind die wichtigsten Begriffe für Amazon One Enterprise:

- Standort — Der Kunde verwaltete physische Gebäude, in denen der Kunde Amazon One Enterprise-Geräte installiert. Ein Standort muss die Anlagen-, Netzwerk- und Stromversorgungsanforderungen für Ihre Amazon One Enterprise-Geräte erfüllen.
- Gerät — Ein biometrisches Handflächenscanner-Gerät von Amazon One Enterprise 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.

Erste Schritte

In diesem Kapitel werden die grundlegenden Schritte für den Einstieg in Amazon One Enterprise erklärt:

1. 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 zu konfigurieren und zu verwalten. Die Schritte verwenden die Amazon One Enterprise-Konsole. Sie werden diesen Vorgang nur gelegentlich oder sogar nur einmal verwenden, abhängig von der Anzahl der Standorte, Geräte-Instances und Konfigurationsvorlagen, für die Sie sich entscheiden.
2. Geräte installieren und aktivieren — Gehen Sie zu Beginn Ihrer Einrichtung wie folgt vor. Für die Geräteaktivierung müssen Installateure über ein Mobiltelefon auf die Amazon One Enterprise-Konsole zugreifen, um Aktivierungs-QR-Codes abzurufen.
3. Geräte- und Benutzerverwaltung — Folgen Sie diesen Schritten für den täglichen Gebrauch der Amazon One Enterprise-Konsole. Sie können diese Schritte verwenden, um den Zustand der Geräte zu überwachen, Kennzahlen zur Benutzerinteraktion zu verstehen und Geräte zu konfigurieren.

Um mehr über Amazon One Enterprise zu erfahren, können Sie die Produktdetailseite von Amazon One Enterprise besuchen.

Themen

Amazon One Enterprise einrichten

Der erste Schritt bei der Nutzung von Amazon One Enterprise besteht darin, Ihre Site, Geräte-Instances und Konfigurationsvorlagen mithilfe der Amazon One Enterprise-Konsole einzurichten.

Themen

Schritt 1: Erstellen Sie ein Konto und einen Admin-Benutzer

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
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 eine anmelden AWS-Konto, ein Root-Benutzer des AWS-Kontoswird erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen im Konto. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich an bei der AWS Management Consoleals Kontoinhaber wählen Sie Root-Benutzer und geben Sie Ihren AWS-Konto E-Mail-Adresse. 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-Anmeldung Benutzerleitfaden.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren Sie ein virtuelles MFA Gerät für AWS-Konto Root-Benutzer (Konsole) im IAMBenutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center in der AWS IAM Identity Center Benutzerleitfaden.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Für ein Tutorial zur Verwendung des IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis in der AWS IAM Identity Center Benutzerleitfaden.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM Identity Center-Benutzer anzumelden, verwenden Sie die Anmeldung, URL die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM Identity Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie unter Anmelden bei AWS Zugriffsportal im AWS-Anmeldung Benutzerleitfaden.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie unter Einen Berechtigungssatz erstellen in der AWS IAM Identity Center Benutzerleitfaden.

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

   Anweisungen finden Sie unter Gruppen hinzufügen in der AWS IAM Identity Center Benutzerleitfaden.

Schritt 2: Amazon One Enterprise-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 Enterprise-Konsole zugreifen, um QR-Codes zur Geräteaktivierung zur Aktivierung von Amazon One-Geräten abzurufen.

So fügen Sie einen Amazon One Enterprise-Benutzer hinzu

1. Folgen Sie dem für Ihren Benutzertyp geeigneten Anmeldeverfahren, wie unter So melden Sie sich an AWS in der AWS-Anmeldung Benutzerleitfaden.
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 ihr Anmeldename für AWS.

   > **Note**
   >
   > Die Anzahl und Größe der IAM Ressourcen in einem AWS-Konto sind begrenzt. Weitere Informationen finden Sie unter IAMund AWS STS Kontingente. Benutzernamen können eine Kombination aus bis zu 64 Buchstaben, Ziffern und den folgenden Zeichen sein: Pluszeichen (+), Gleichheitszeichen (=), Komma (,), Punkt (.), At-Zeichen (@), Unterstrich (_) und Bindestrich (-). Namen müssen innerhalb eines Kontos eindeutig sein. Es wird hierbei nicht zwischen Groß- und Kleinschreibung unterschieden. Sie können beispielsweise nicht zwei Benutzer namens TESTUSERund testuser erstellen. Wenn ein Benutzername in einer Richtlinie oder als Teil einer verwendet wirdARN, unterscheidet der Name zwischen Groß- und Kleinschreibung. 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 gewähren auf — AWS Management Console optional.
5. Wählen Sie Ich möchte einen IAM Benutzer erstellen.
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 ein angehängt AWS verwaltete Richtlinie `IAMUserChangePassword`, die nach den neuen Benutzern benannt ist. 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 zur Verwendung von Tags in finden Sie IAM unter IAMRessourcen zum Taggen.
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
    - URLzur Anmeldeseite für das Konto. 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.

Schritt 3: Erstellen Sie eine Site

Jetzt, da Sie sich bei der angemeldet haben AWS Management Console, können Sie die Amazon One Enterprise-Konsole verwenden, um Ihre Site zu erstellen.

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

So erstellen Sie einen Standort:

1. Öffnen Sie die Amazon One Enterprise-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.

Schritt 4: Geräteinstanzen erstellen

Um eine Geräte-Instance zu erstellen

1. Öffnen Sie die Amazon One Enterprise-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 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.

Schritt 5: Erstellen Sie eine Konfigurationsvorlage

Um eine Konfigurationsvorlage zu erstellen

1. Öffnen Sie die Amazon One Enterprise-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 Enterprise für den sicheren Zugriff nutzen zu können.

Schritt 6: Konfigurieren Sie eine Geräte-Instance für die Aktivierung

Nachdem eine Geräte-Instance erstellt wurde, konfigurieren Sie die Geräte-Instance mit einer zuvor erstellten Konfigurationsvorlage (sieheSchritt 5: Erstellen Sie eine Konfigurationsvorlage), oder Sie können Konfigurationen manuell hinzufügen.

Um eine Geräteinstanz für die Aktivierung zu konfigurieren

1. Öffnen Sie die Amazon One Enterprise-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 unterSchritt 5: Erstellen 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. Bestätigen 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 Enterprise für den sicheren Zugriff nutzen zu können.

Amazon One installieren und aktivieren

Nachdem Ihre Amazon One Enterprise-Konsole eingerichtet wurde, bestehen die nächsten Schritte darin, Amazon One Enterprise-Geräte auf Ihrer Site zu installieren und sie anschließend zu aktivieren.

> **Note**
>
> Dieser Abschnitt konzentriert sich auf die Installation und verwendet einen mobilen Browser für den Zugriff AWS Management Console um QR-Codes zur Geräteaktivierung zu erhalten.

Themen

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.

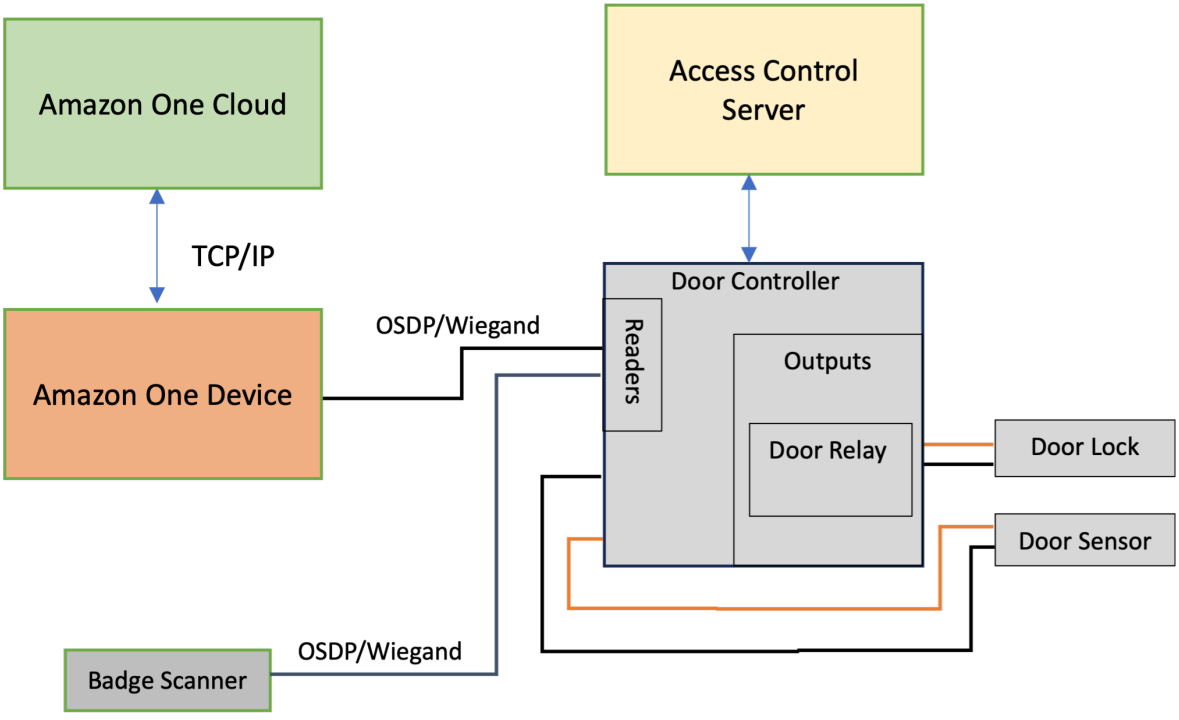
Leistungsbedarf

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 Enterprise, das Gerät als Teil einer typischen Zutrittskontrollumgebung zu installieren, wie im folgenden Blockdiagramm beschrieben.



Eine Zugriffskontrollumgebung 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.
- Access Control Server: Diese Komponente steuert in der Regel die Zugriffsrechte von Benutzern auf den sicheren Bereich. Die IDs Ausweise von Personen, die Zugang zu dem Bereich haben, werden normalerweise auf diesem Server gespeichert. Auf diesem Server werden die für die jeweiligen Türsteuerungen relevanten IDs Daten zwischengespeichert.
- Türcontroller:
  - Ein Amazon One-Gerät stellt über eine OSDP Schnittstelle eine Verbindung zum Door Controller-Server her.
  - Wenn eine Wiegand-Schnittstelle erforderlich ist, kann ein COTS OSDP Wiegand-Konverter verwendet werden.
  - Nach erfolgreicher Authentifizierung sendet das Amazon One-Gerät die Badge-ID des Benutzers an den Door Controller.
  - Die Türsteuerung reagiert mit einer Entscheidung, die es dem Amazon One-Gerät dann ermöglicht, entweder die Meldung „Zugriff gewährt“ oder „Zugriff verweigert“ anzuzeigen.
- Ausweisscanner: Ein Ausweisscanner wird normalerweise verwendet, um RFID Ausweise zu scannen und die Ausweisnummer an den Access Control Server zu senden. Bei Amazon One Enterprise ist ein Ausweisscanner mit dem Amazon One-Gerät für die Registrierung verbunden, sodass Ausweise von Mitarbeitern gescannt und ihren Handflächenprofilen zugeordnet werden können.

Installation von Amazon One Enterprise Pedestal

In diesem Abschnitt werden die Standortanforderungen und die Schritte beschrieben, die für die Installation eines Amazon One Enterprise-Podests erforderlich sind.

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Wenn Sie POE + zur Stromversorgung des Geräts verwenden, stellen Sie sicher, dass die Cat6-Verkabelung verlegt ist und ein POE +-Injektor oder -Schalter verwendet werden kann.
- Wenn eine Wechselstromquelle (120 V) verwendet wird, sollte eine Netzsteckdose in einem Abstand von 20 Fuß vom Sockel verfügbar sein. AOE
- Der Boden muss eben und sauber sein.
- Der Sockel darf die Tür oder die Gasse nicht blockieren.
- Alle überschüssigen Kabel müssen innerhalb des Sockels aufbewahrt und gesichert werden.

So installieren Sie den Amazon One-Gerätesockel

1. Nehmen Sie den Amazon One Enterprise-Standfuß aus der Verpackung.
2. Entfernen Sie die Tür, indem Sie beide manipulationssicheren M4-Schrauben lösen.
3. Stecken Sie das Netzkabel ein. Führen Sie das Kabel durch das Loch in der Sockelgrundplatte.
4. Wickeln Sie überschüssiges Stromkabel im Inneren des Sockels auf.
5. Führen Sie das Ethernet-Kabel (Cat5E oder besser) durch die Bodenplatte des Sockels und stecken Sie es in den Ethernet-Anschluss.
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. Schließen Sie die Steckdose an 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 erneut fest.

Installation eines an der Wand montierbaren Amazon One-Geräts

In diesem Abschnitt werden die Standortanforderungen und die Schritte beschrieben, die für die Installation Ihres an der Wand montierbaren Amazon One-Geräts erforderlich sind.

Bevor Sie mit der Installation beginnen, stellen Sie Folgendes sicher:

- Das an der Wand montierbare Amazon One-Gerät ist nur für den Gebrauch in Innenräumen bestimmt.
- Die Wand ist eben.
- Die Oberseite der Wandhalterung sollte nach der Montage nicht höher als 44-46 Zoll vom Boden sein.
- Alle überschüssigen Kabel befinden sich hinter der Wandhalterung und sind gesichert.
- Für Power over Ethernet (PoE++):

Stellen Sie sicher, dass ein IEEE 802.3bt-Switch (Typ 3) der Klasse 6 POE ++ (End Span) oder ein Injector (Midspan) zur Verwendung verfügbar ist, der gelistet oder zertifiziert ist und 62368-1 entspricht. IEC

Nur mit einer zugelassenen PoE++-Quelle verwenden. AOE

Die PoE++-Quelle muss sich im selben Gebäude befinden.

- Für eine Eingangsspannung von 15 V Gleichstrom sollten Sie das Amazon One-Gerät nur mit einem Netzteil der NEC Klasse 2 oder einem zugelassenen Netzteil mit begrenzter Leistung verwenden, das aufgeführt oder zertifiziert ist.

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
- T12 Secure Torx-Treiber
- Bleistift
- Level

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

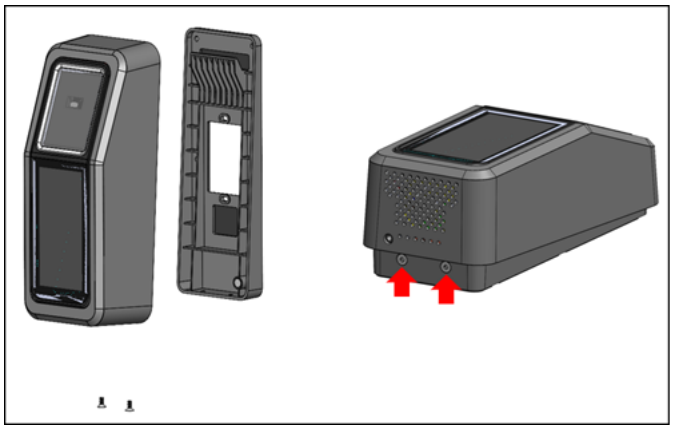
- 6 x #8 Trockenbauanker
- 6 x #8 -32 1-Zoll-lange Schrauben
- 2 x #6 -32 1-Zoll-Maschinenschrauben
- 2 x Klemmenblockstecker mit 6 Positionen
- 2 Torx-Sicherheits-Flachkopfschrauben M4x10

So installieren Sie die Wandmontageplatte für Ihr Amazon One-Gerät

<result>

</result>

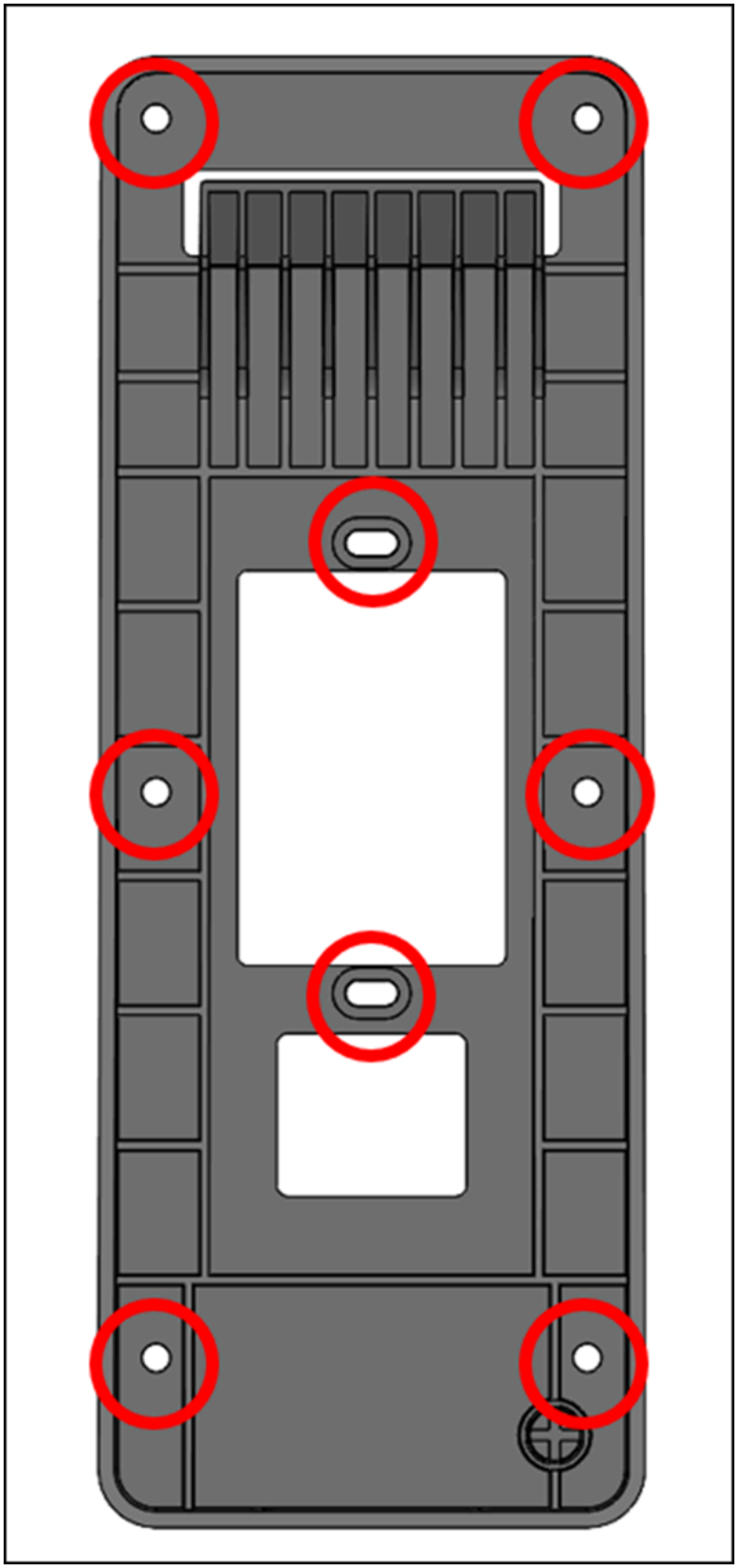
1. Nehmen Sie Ihr Amazon One-Gerät aus der Verpackung.
2. Trennen Sie die Montageplatte von Ihrem Amazon One-Gerät, indem Sie die beiden unteren Torx-Sicherheitsschrauben entfernen.



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.

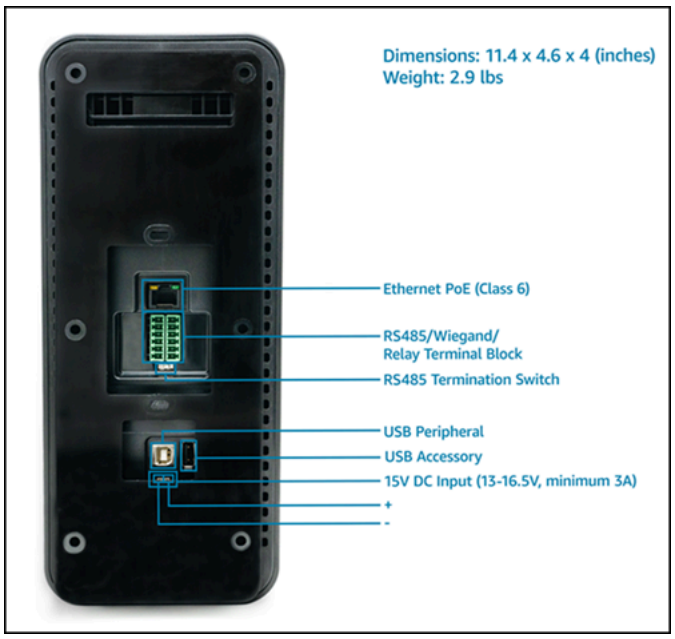
   Bei der Montage auf einer Holzoberfläche sind die Dübel nicht erforderlich und an den markierten Stellen sind nur 7/64-Zoll-Vorlöcher erforderlich.
5. Befestigen Sie die Wandplatte mit den #8 -Holzschrauben an den Ankerpositionen locker an der Wand.
6. Nachdem alle Befestigungselemente angebracht sind,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

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

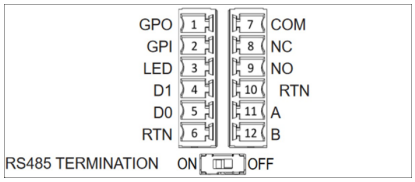
Sie können Amazon One-Geräte mit OSDP und Weigand-Zugriffskontrollprotokollen konfigurieren. Um die Installation zu vereinfachen, verwendet das Amazon One-Gerät Klemmenblockanschlüsse (Mfg P/N: Phoenix Contact 1767694). Sie haben auch die Möglichkeit, das Amazon One-Gerät so zu konfigurieren, dass externe 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.

   Detaillierte elektrische Eigenschaften der Signale finden Sie in den Verkabelungsanweisungen.



Verbindungen



Pin	Verbindung	Beschreibung	Verwenden Sie	
1	GPO	Ausgabe für allgemeine Zwecke	Digitales Ausgangssignal — optional	
2	GPI	Eingang für allgemeine Zwecke	Digitales Eingangssignal — optional	
3	LED	Wiegand LED	Wiegand LED — Fakultativ	
4	D1	Wiegand D1	Wiegand Data 1 — Weißer Draht	

Pin	Verbindung	Beschreibung	Verwenden Sie	
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 Kontaktrelais ist normal geöffnet — gelber Draht	
10	RTN	Signalrückkehr	OSDPRückkehr — Schwarzer Draht	
11	A	RS485_A/D1/ Uhr	OSDPD1 — Weißer Draht	
12	B	RS485_B/D0/ Daten	OSDPD0 — 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.

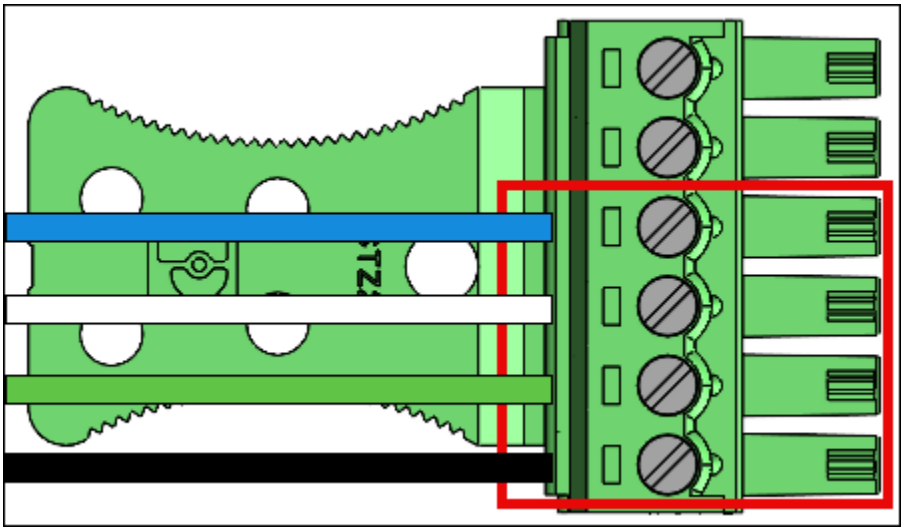
4. Drehen Sie die Klemmenbefestigungsschraube mit einem Schlitzschraubendreher im Uhrzeigersinn, um das Kabel festzuklemmen, bis es fest sitzt. Nicht zu fest anziehen.
5. Ziehen Sie nach dem Befestigen vorsichtig am Draht, um sicherzustellen, dass er sitzt.
6. Nachdem Sie die erforderlichen Verbindungen 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

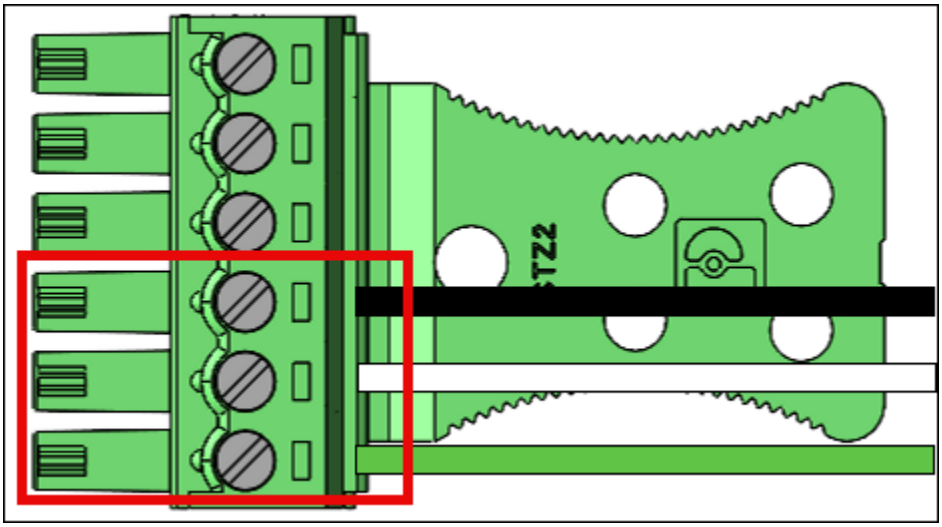
Pin	Verbindung	Beschreibung	Verwenden Sie	
3	LED	Wiegand LED	LEDWiegand-Eingang — optional (5 V) TTL	
4	D1	Wiegand D1	Wiegand D1-Ausgang (5 V) TTL	
5	D0	Wiegand D0	Wiegand D0-Ausgang (5 V) TTL	
6	RTN	Signalrückgabe	Referenz Wiegand GND	

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.

RS485Verbindungen

- 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).

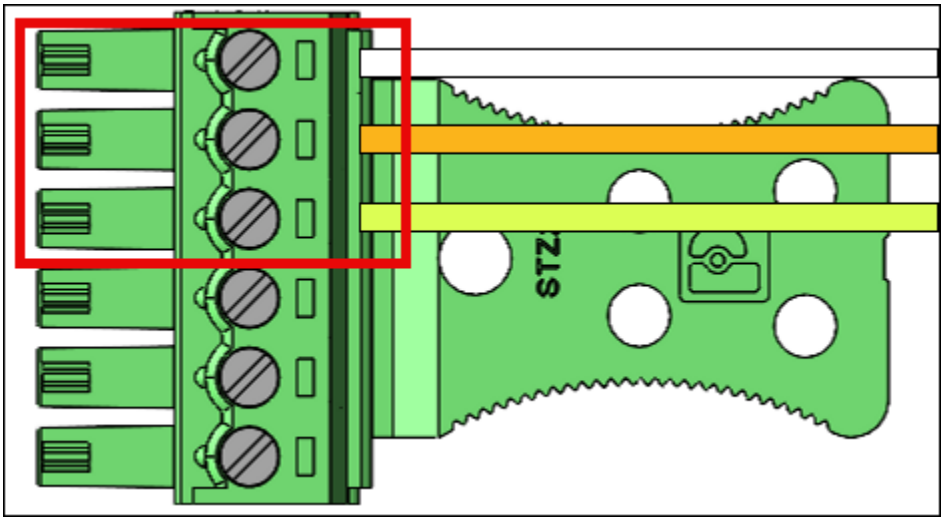


RS485Verkabelung

Pin	Verbindung	Beschreibung	Verwenden Sie	
10	RTN	Signalrückgabe	Ground (Boden)	
11	A	RS485_A/D1/Uhr	RS485nich tinvertierendes Signal	
12	B	RS485_B/D0/ Daten	RS485inve rtierendes Signal	

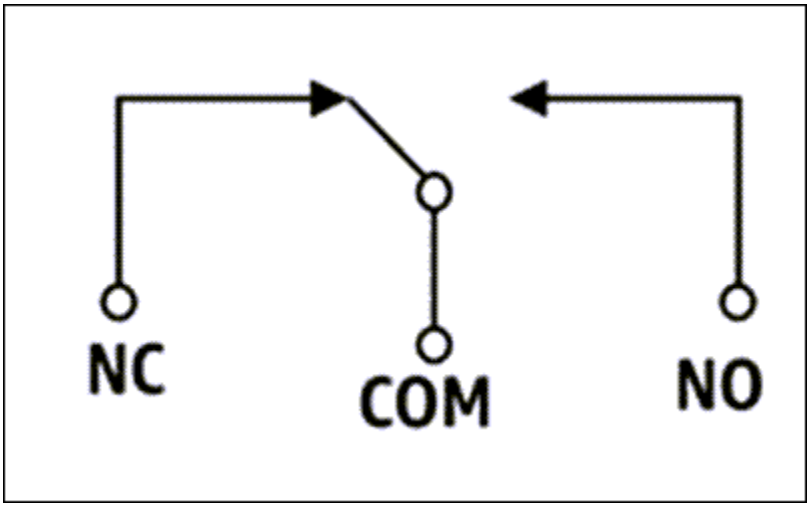
Relaisverbindungen

- 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

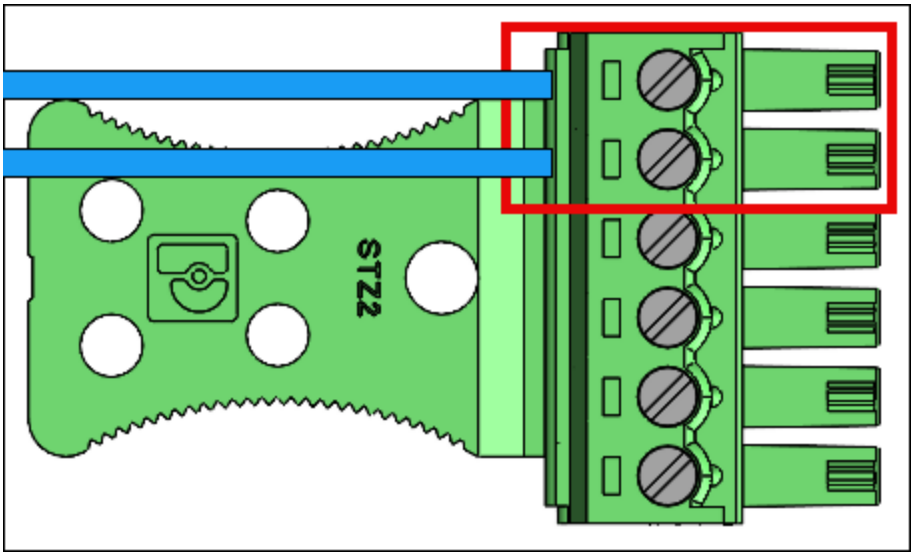
Pin	Verbindung	Beschreibung	Verwenden Sie
7	COM	Relais üblich	Kontaktrelais Common — weißer Draht
8	NC	Das Relais ist normalerweise geschlossen	Kontaktrelais normalerweise geschlossen — orangefarbenes Kabel
9	NO	Das Relais ist normalerweise geöffnet	Das Kontaktrelais ist normal geöffnet — gelber Draht



Das Relais sollte gemäß den angegebenen Sicherheitsklassen 30 VAC /60VDC, 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).



Pin	Verbindung	Beschreibung	Verwenden Sie	
1	GPO	Ausgabe für allgemeine Zwecke	Digitales Ausgangssignal (5 V)	
2	GPI	Allzweck-Eingang	Digitales Eingangssignal (3,6 V — 5 V)	

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

Informationen Amazon One-Gerät aktivieren zur Aktivierung Ihres Amazon One-Geräts finden Sie unter.

Amazon One Device I/O Hub für sicheren Zugriff installieren

In diesem Abschnitt werden die Standortanforderungen und die Schritte beschrieben, die für die Installation Ihres Amazon One Enterprise (AOE) -Geräts mit I/O Hub erforderlich sind.

Bevor Sie mit der Installation beginnen, stellen Sie Folgendes sicher:

- Das Amazon One-Gerät mit I/O Hub ist nur für den Gebrauch in Innenräumen bestimmt.
- Für Power Over Ethernet (PoE++):

  Stellen Sie sicher, dass ein IEEE 802.3bt-Switch (Typ 3) der Klasse 6 POE ++ (End Span) oder ein Injector (Midspan) zur Verwendung verfügbar ist, der gelistet oder zertifiziert ist und 62368-1 entspricht. IEC

  Verwenden Sie nur ein Amazon One-Gerät mit einer zugelassenen PoE++-Quelle.

  Die PoE++-Quelle muss sich im selben Gebäude befinden.

- Für eine Eingangsspannung von 15 V Gleichstrom sollten Sie das Amazon One-Gerät nur mit einem zugelassenen Netzteil der NEC Klasse 2 oder mit begrenzter Leistung verwenden, das aufgeführt oder zertifiziert ist. Weitere Informationen finden Sie im Abschnitt Optionaler Gleichstrom weiter unten.

Erforderliche Tools:

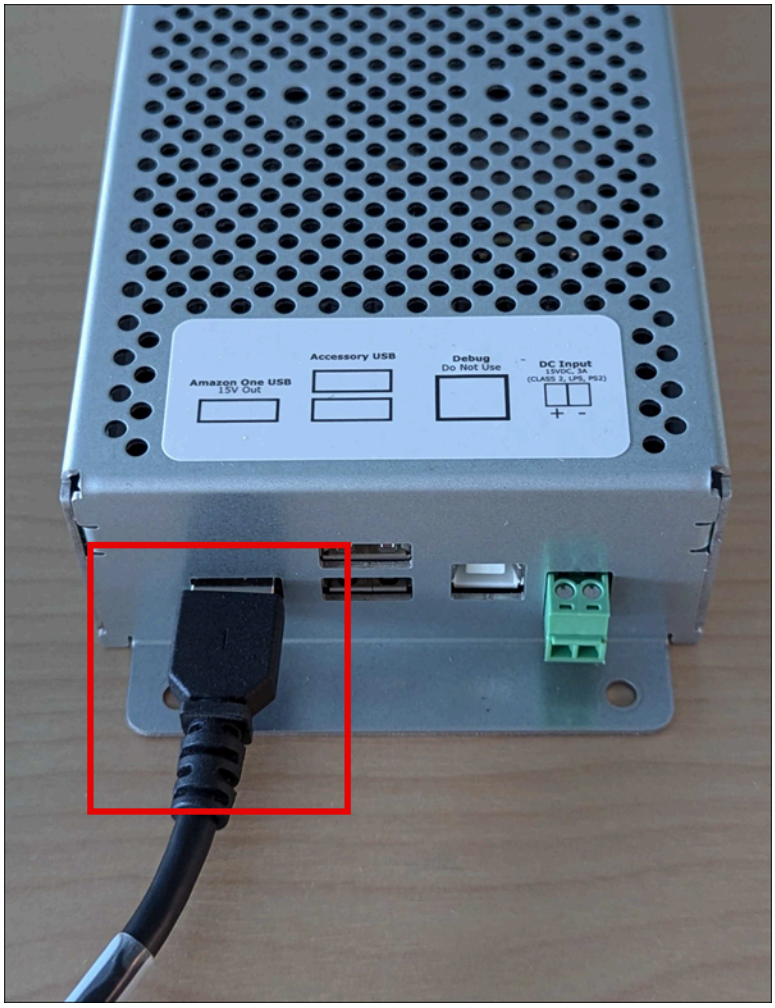
- Abisoliergerät
- #2 Kreuzschlitzschraubendreher
- 0,5 mm x 2 mm Schlitzschraubendreher

Im Lieferumfang des Amazon One-Geräts mit I/O Hub enthalten:

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

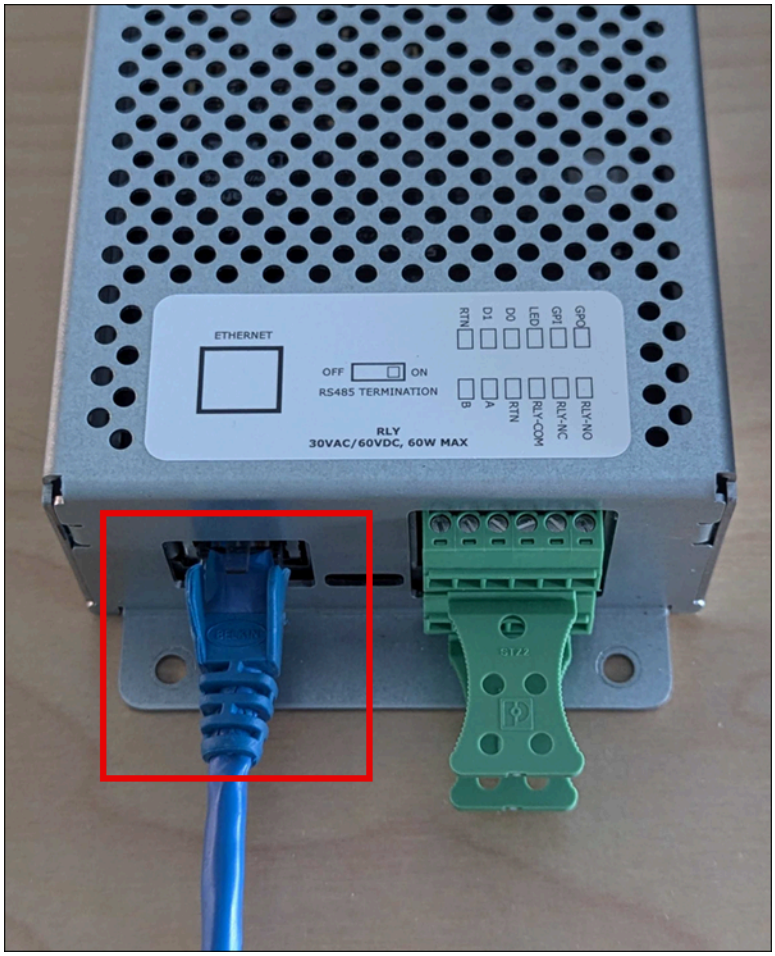
Um den I/O-Hub für Ihr Amazon One-Gerät zu installieren

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 USB One-Kabel in den I/O-Hub-Anschluss.



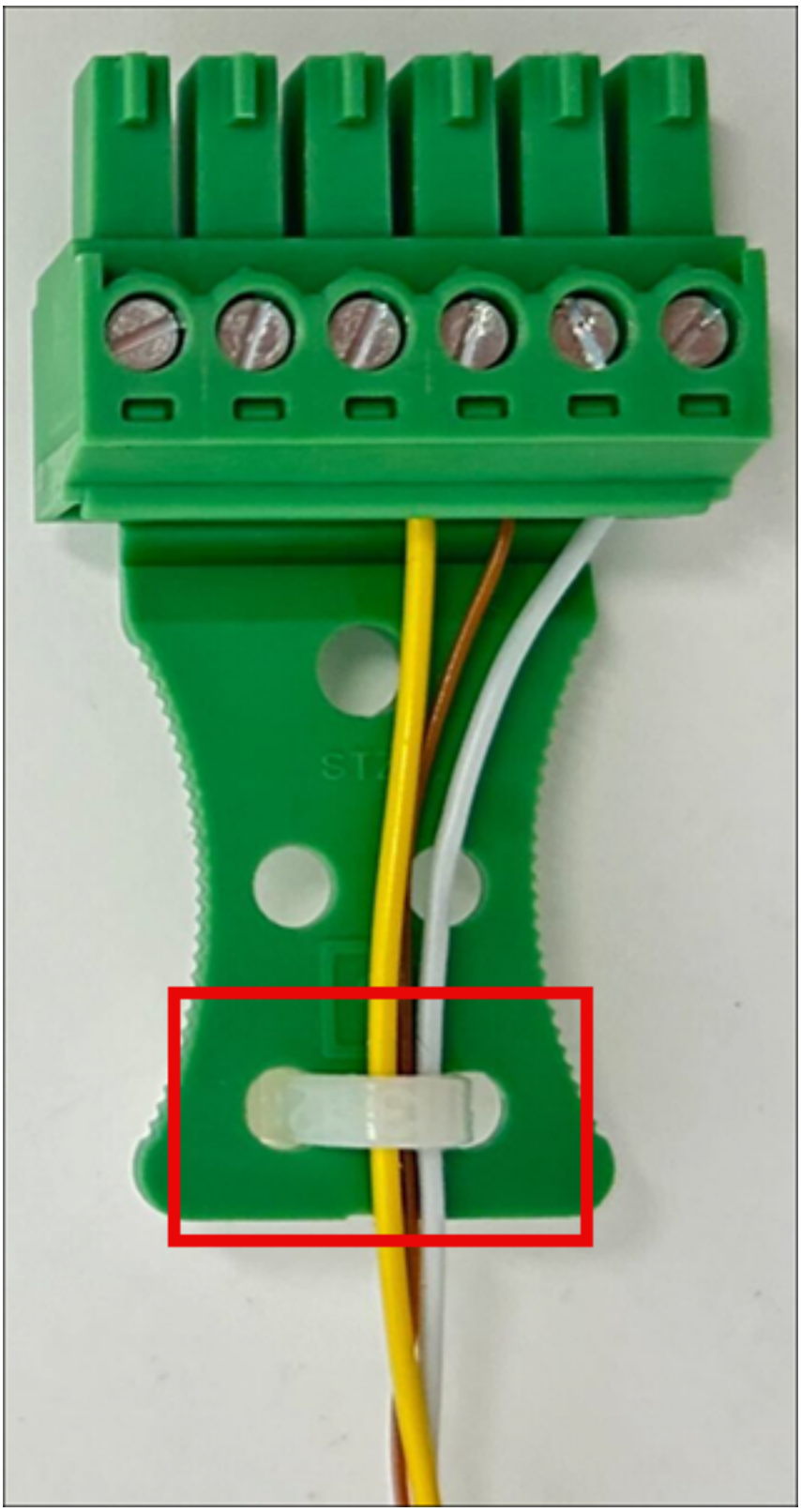
4. Stecken Sie das Ethernet-Kabel von der POE ++-Quelle in den I/O-Hub-Anschluss, um POE ++ mit Strom zu versorgen.

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



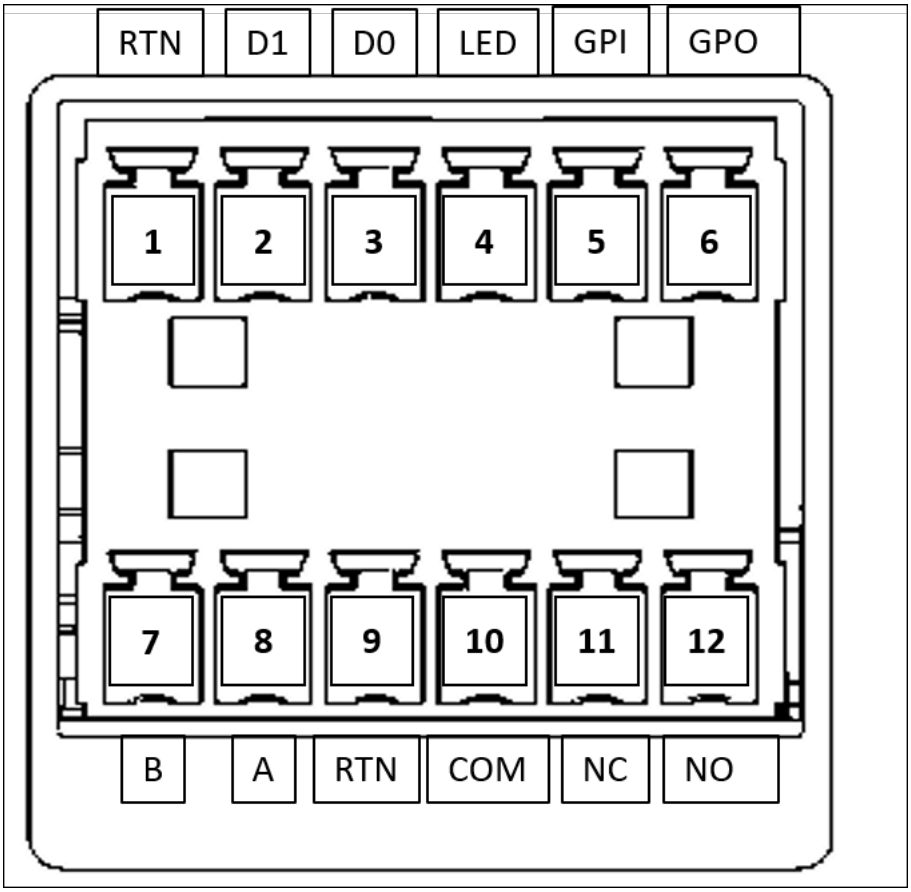
So verkabeln Sie den I/O-Hub für Ihr Amazon One-Gerät

- 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. Führen Sie nur die für Ihre Anwendung erforderlichen Kabel durch die Stecker der Klemmenblöcke. Beachten Sie die folgende Verkabelungstabelle und die folgenden Diagramme.

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



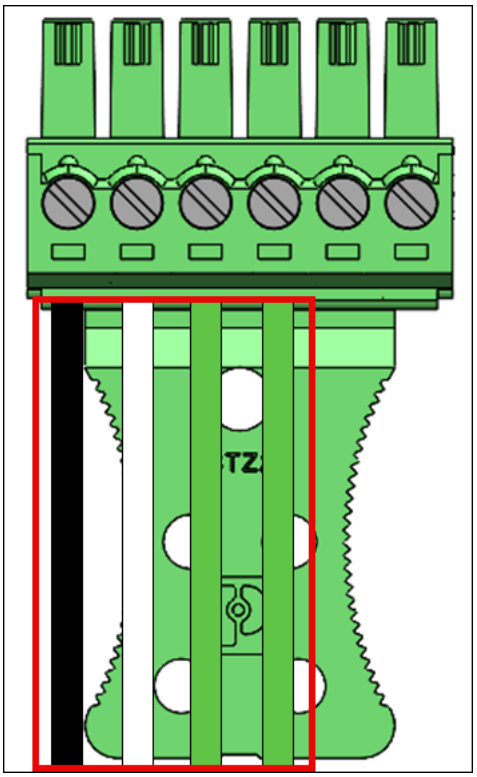
Pin	Verbindung	Beschreibung	Verwenden Sie	
1	RTN	Signalrückgabe	Wiegand Ground — Schwarzer Draht	
2	D1	Wiegand D1	Wiegand Data 1 — Weißer Draht	
3	D0	Wiegand D0	Wiegand Data 0 — Grünes Kabel	
4	LED	Wiegand LED	Wiegand LED — Fakultativ	

Pin	Verbindung	Beschreibung	Verwenden Sie	
5	GPI	Eingabe für allgemeine Zwecke	Digitales Eingangssignal — optional	
6	GPO	Allzweck-Ausgang	Digitales Ausgangssignal — optional	
7	B	RS485_B/D0/ Daten	OSDPD0 — Grünes Kabel	
8	A	RS485_A/D1/Uhr	OSDPD1 — Weißer Draht	
9	RTN	Signalrückkehr	OSDPRückkehr — Schwarzer Draht	
10	COM	Gemeinsames Relais	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

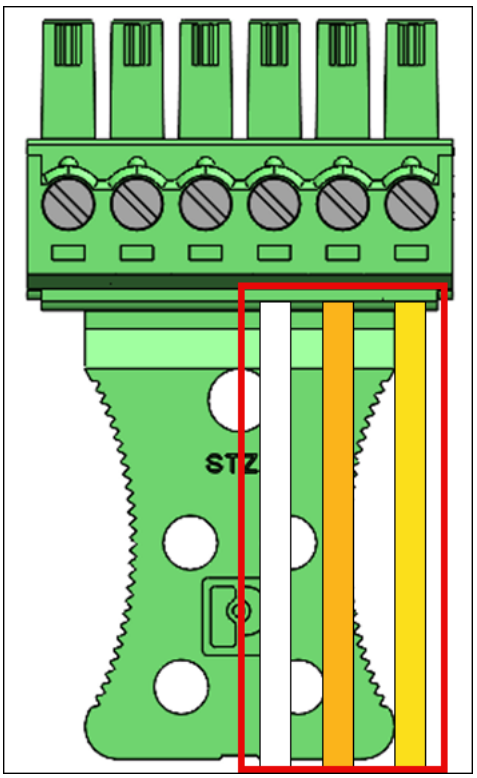
- Stecken Sie das schwarze Kabel in Pin 1 ()RTN.

- 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).

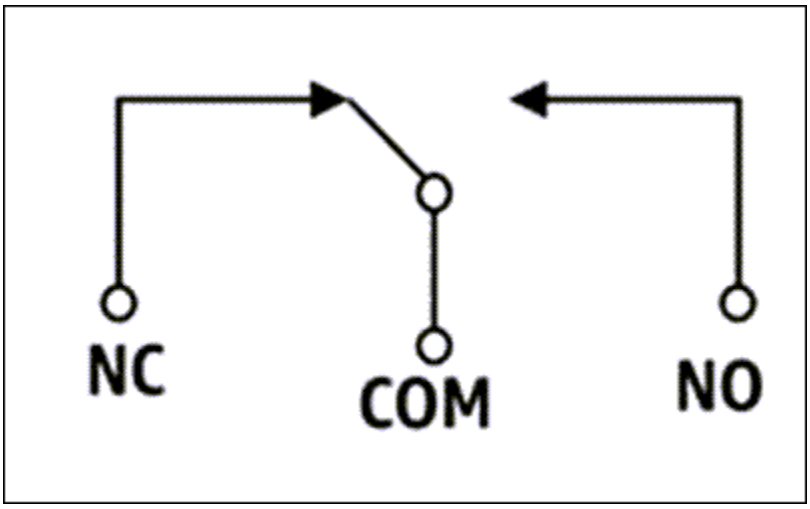


Relaisverbindungen

- 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

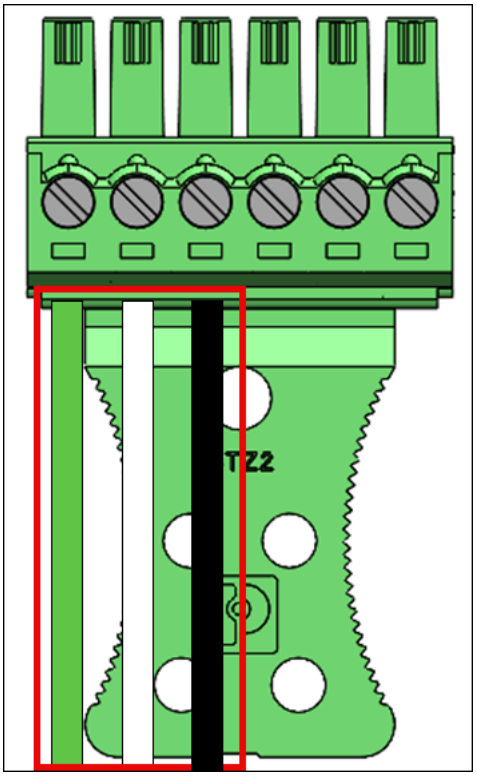


Das Relais sollte gemäß den angegebenen Sicherheitsklassen 30 VAC /60VDC, max. 60 W betrieben werden.

RS485Verbindungen

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

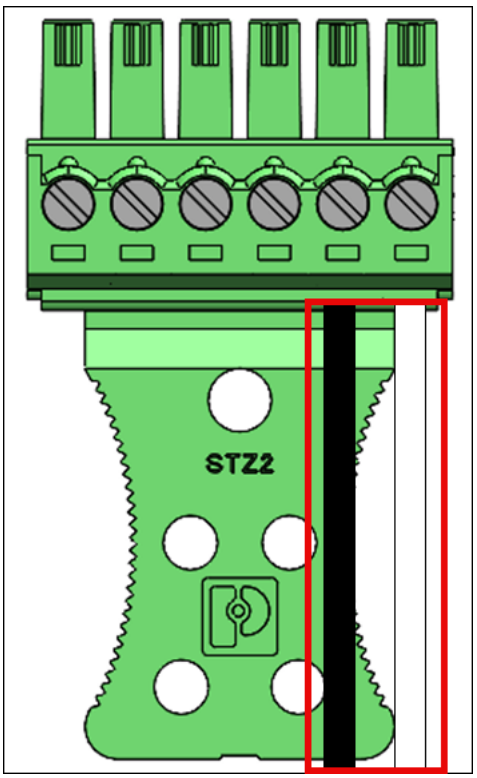
- Stecken Sie das schwarze Kabel in Pin 9 (RTN).



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

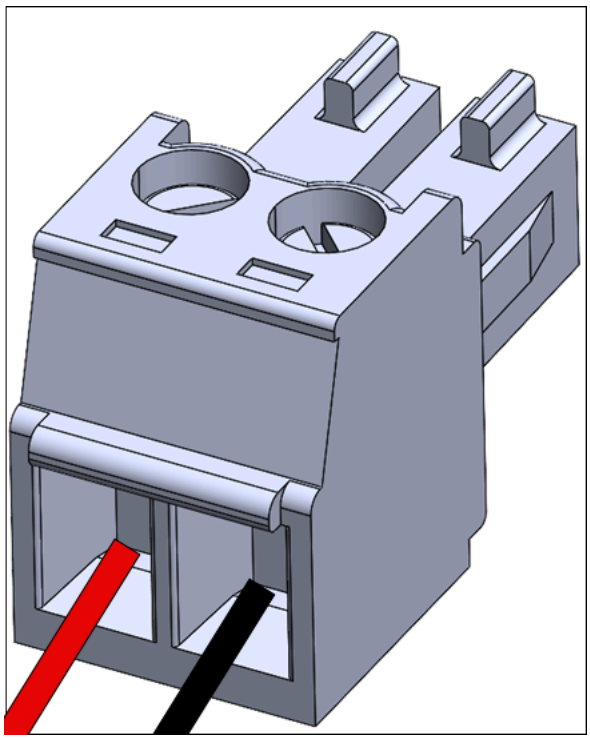
- Stecken Sie das schwarze Kabel in Pin 5 ()GPI.
- Stecken Sie das weiße Kabel in Pin 6 (GPO).



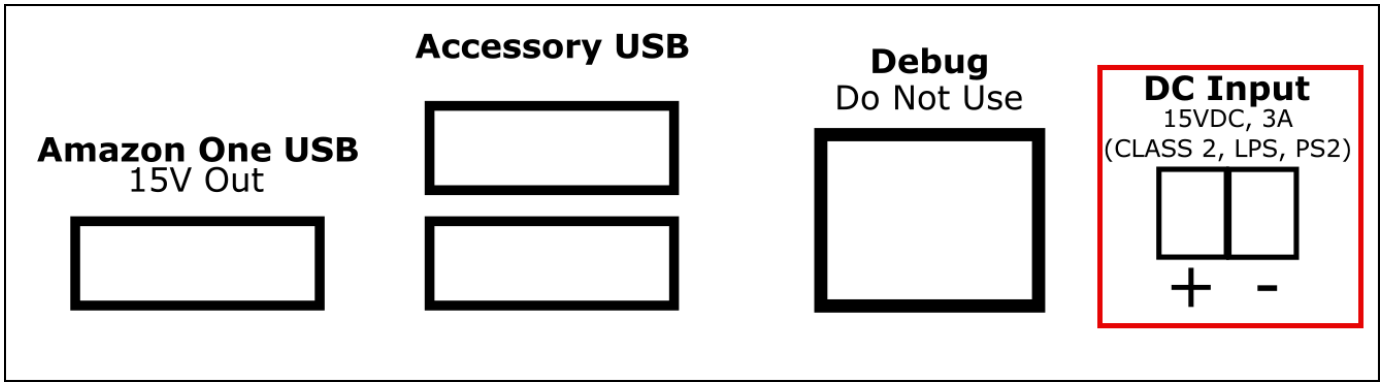
- Die digitalen Eingangs-/Ausgangsanschlüsse sollten wie angegeben betrieben werden.

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.



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 Schritt 2: Amazon One Enterprise-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 Informationen zur Website die Adresse der Website.
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.
11. Wenn auf dem Bildschirm des Amazon One-Geräts die Aktivierung abgeschlossen angezeigt wird! , das Gerät ist einsatzbereit.

Einschreibung und Einreise

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

Registrierung von Benutzern

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.

Authentifizieren Sie sich 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.

Verwaltung registrierter Benutzer

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.

Um registrierte Benutzer einzusehen

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.

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.

Gerätemanagement

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

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.

Um den Namen der Website 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.

Um die Adresse der Website 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 Um Geräteinstanzen zu deaktivieren
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.

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.

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.

Um Amazon One-Gerätekonfigurationen 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 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 (sieheSchritt 6: Konfigurieren Sie eine Geräte-Instance für die Aktivierung). Anschließend können Sie den Geräteaktivierungsprozess durchführen (sieheAmazon One-Gerät aktivieren).

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

Um die 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.

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 in Amazon One Enterprise

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

Das Tool AWS Das Modell Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über

Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Sie sind auch verantwortlich für die Sicherheitskonfiguration und die Verwaltungsaufgaben für AWS-Services die Sie verwenden. Weitere Informationen zum Datenschutz finden Sie in der Datenschutzerklärung FAQ. Informationen zum Datenschutz in Europa finden Sie auf der AWS Modell der geteilten Verantwortung und GDPR Blogbeitrag auf der AWS Blog zum Thema Sicherheit.

Aus Datenschutzgründen empfehlen wir Ihnen, AWS-Konto Anmeldeinformationen und richten Sie einzelne Benutzer ein mit AWS IAM Identity Center or AWS Identity and Access Management (IAM). 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 SieSSL/TLS, um mit zu kommunizieren AWS Ressourcen schätzen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail. Für Informationen zur Verwendung von CloudTrail Spuren zum Erfassen AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerleitfaden.
- 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 FIPS 140-3 validierte kryptografische Module benötigen AWS über eine Befehlszeilenschnittstelle oder einenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten 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 arbeiten AWS-Services mit der KonsoleAPI, AWS CLI, oder 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 einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

Um die Standardverschlüsselung von Daten im Ruhezustand zu verwenden

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

AWSeigene Schlüssel — Amazon One Enterprise verwendet diese Schlüssel standardmäßig, um sensible Endbenutzerdaten automatisch zu verschlüsseln. Sie können AWS eigene Schlüssel nicht einsehen, 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) ist ein AWS-Service das hilft einem Administrator, den Zugriff auf sicher zu kontrollieren AWS Ressourcen schätzen. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon One Enterprise-Ressourcen zu verwenden. IAMist ein AWS-Service das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie benutzt du AWS Identity and Access Management (IAM) unterscheidet sich je nach der Arbeit, 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 Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in Amazon One Enterprise nicht zugreifen können, finden Sie weitere Informationen unterProblembehandlung bei Amazon One Enterprise: 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 Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen Amazon One Enterprise nutzen IAM kann, finden Sie unterSo arbeitet Amazon One Enterprise mit IAM.

IAMAdministrator — 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 verwenden könnenIAM, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon One Enterprise

Authentifizierung mit Identitäten

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

Sie können sich anmelden bei AWS als föderierte Identität mithilfe von Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center) - Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM

Wenn Sie darauf zugreifen AWS Wenn Sie den Verbund verwenden, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der anmelden AWS Management Console oder das AWS Zugangsportal. Weitere Informationen zur Anmeldung bei AWS, siehe So melden Sie sich bei Ihrem an AWS-Konto in der AWS-Anmeldung Benutzerleitfaden.

Wenn Sie darauf zugreifen AWS programmatisch AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie nicht verwenden AWS Tools, Sie müssen Anfragen selbst unterschreiben. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie unter Signieren AWS APIAnfragen im IAMBenutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. Zum Beispiel AWS empfiehlt, 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 Verwendung der Multi-Faktor-Authentifizierung () MFA in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle hat AWS-Services und Ressourcen im Konto. Diese Identität wird als AWS-Konto Root-Benutzer. Der Zugriff erfolgt, 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 und verwenden Sie diese, 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 im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Es hat sich bewährt, menschlichen Benutzern, einschließlich Benutzern, die Administratorzugriff benötigen, vorzuschreiben, für den Zugriff den Verbund mit einem Identitätsanbieter zu verwenden AWS-Services mithilfe temporärer Anmeldeinformationen.

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

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

Für eine zentralisierte Zugriffsverwaltung empfehlen wir die Verwendung AWS IAM Identity Center. 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 und Anwendungen. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? in der AWS IAM Identity Center Benutzerleitfaden.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres AWS-Konto das über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern spezifiziert. 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 eine Gruppe benennen 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 Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität in deinem AWS-Konto das hat spezifische Berechtigungen. Es ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen AWS Management Console indem Sie die Rollen wechseln.

Sie können eine Rolle übernehmen, indem Sie einen anrufen AWS CLI or AWS APIOperation oder mithilfe eines benutzerdefiniertenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- 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 im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 Benutzerleitfaden.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Allerdings mit einigen AWS-Services, Sie können eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services Funktionen in anderen verwenden 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.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen in AWS, Sie gelten als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, die Interaktionen mit anderen erfordert AWS-

Services oder Ressourcen zum Ausfüllen. 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 IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an ein AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen durchzuführen. Mit Diensten verknüpfte Rollen erscheinen in Ihrem AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

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

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff in AWS indem Sie Richtlinien erstellen und diese anhängen AWS Identitäten oder Ressourcen. Eine Richtlinie ist ein Objekt in AWS das, wenn es mit einer Identität oder Ressource verknüpft ist, ihre Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Principal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien sind gespeichert in AWS als JSON Dokumente. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

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 AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services.

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

Zugriffskontrolllisten () ACLs

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

Amazon S3 S3, AWS WAF, und Amazon VPC sind Beispiele für Dienste, die unterstützenACLs. 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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- 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 AWS-Konten den Ihr Unternehmen besitzt. 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. Weitere Informationen

zu Organizations und finden Sie SCPs unter Richtlinien zur Servicesteuerung in der AWS Organizations Benutzerleitfaden.

- 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 im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Um zu erfahren, wie AWS bestimmt, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, siehe Bewertungslogik für Richtlinien im IAMBenutzerhandbuch.

So arbeitet Amazon One Enterprise mit IAM

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

IAMFunktionen, die Sie mit Amazon One Enterprise verwenden können

IAMFunktion	Unterstützung für Amazon One Enterprise
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein

IAMFunktion	Unterstützung für Amazon One Enterprise
ABAC(Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Um einen umfassenden Überblick darüber zu erhalten, wie Amazon One Enterprise und andere AWS Dienste funktionieren mit den meisten IAM Funktionen, siehe AWS Dienste, mit denen IAM im IAMBenutzerhandbuch gearbeitet wird.

Identitätsbasierte Richtlinien für Amazon One Enterprise

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

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 einer Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services.

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal 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 Erlaubnis erteilen, auf die Ressource zuzugreifen. 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 IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Politische Maßnahmen für Amazon One Enterprise

Unterstützt Richtlinienaktionen: Ja

Administratoren können Folgendes verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörigen AWS APIBetrieb. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur Berechtigungen erforderlich sind und für die es keine entsprechende Operation gibt. API 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 Folgendes verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat

sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. 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 darüberARNs, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren 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 verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was 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, AWS wertet sie mithilfe 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. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn

sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Um alle zu sehen AWS globale Bedingungsschlüssel finden Sie unter AWS Kontexttasten für globale Bedingungen im IAMBenutzerhandbuch.

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

ACLsbei Amazon One Enterprise

UnterstütztACLs: Nein

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

ABACmit Amazon One Enterprise

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In AWS, diese Attribute werden Tags genannt. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele Entitäten anhängen AWS Ressourcen schätzen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich 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 finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen mit Amazon One Enterprise verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Etwas AWS-Services funktioniert nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Für zusätzliche Informationen, einschließlich AWS-Services mit temporären Anmeldeinformationen arbeiten, siehe AWS-Services mit denen IAM im IAMBenutzerhandbuch gearbeitet werden kann.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich bei der anmelden AWS Management Console mit einer beliebigen Methode außer einem Benutzernamen und einem Passwort. Zum Beispiel, wenn Sie darauf zugreifen AWS Wenn Sie den Single Sign-On-Link (SSO) Ihres Unternehmens verwenden, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

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

Serviceübergreifende Hauptberechtigungen für Amazon One Enterprise

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen in AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, die Interaktionen mit

anderen erfordert AWS-Services oder Ressourcen zum Ausfüllen. 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 IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an ein 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 dienstbezogene Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen durchzuführen. Mit Diensten verknüpfte Rollen erscheinen in Ihrem AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS Dienste, 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 mit dem ausführen AWS Management Console, AWS Command Line Interface (AWS CLI), oder AWS API. Um Benutzern die Erlaubnis zu

erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

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

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

- Fangen Sie an mit AWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie AWS verwaltete Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie Folgendes definieren AWS vom Kunden verwaltete Richtlinien, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien oder AWS verwaltete Richtlinien für Jobfunktionen im IAMBenutzerhandbuch.

- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über eine bestimmte AWS-Service, wie beispielsweise AWS CloudFormation. Weitere Informationen finden Sie unter IAMJSONRichtlinienelemente: Zustand im IAMBenutzerhandbuch.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer in Ihrem AWS-Konto, schalten Sie MFA für zusätzliche Sicherheit ein. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

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 AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie nicht wie vorgesehen.

Sie müssen Benutzern, die nur Anrufe tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS CLI oder das AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Amazon One Enterprise-Konsole weiterhin verwenden können, hängen Sie auch die Amazon One Enterprise *ConsoleAccess* - oder *ReadOnly* AWS verwaltete Richtlinie für die Entitäten. Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline-Richtlinien und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Nur-Lese-Zugriff auf Amazon One Enterprise

Das folgende Beispiel zeigt eine AWS verwaltete Richtlinie, `AmazonOneEnterpriseReadOnlyAccess` die nur Lesezugriff auf Amazon One Enterprise 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 `Resource` Element listet die AWS Ressourcen, auf denen 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, aber keine Aktionen für andere AWS Dienstleistungen.

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

  Das ermöglicht alles AWS Aktionen. Diese Erlaubnis ist für einen Benutzer geeignet, der als AWS Administrator für Ihr Konto.

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 Actions API

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 API Enterprise-Regelaktionen. 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 Amazon One API Enterprise-Regelaktionen beschrieben, die derzeit Berechtigungen auf Ressourcenebene unterstützen. Außerdem werden die unterstützten Ressourcen und ihre ARNs für jede Aktion benötigten Ressourcen beschrieben. Wenn Sie eine angebenARN, 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 API Enterprise-Regelaktion 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 für das Ressourcenelement Ihrer Richtlinienerklärung ein Sternchen angeben.

APIAktion	Ressourcen
CreateDeviceInstance	Geräteinstanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*

APIAktion	Ressourcen
GetDeviceInstance	Geräte-Instanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*
UpdateDeviceInstance	Geräte-Instanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*
DeleteDeviceInstance	Geräte-Instanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*
CreateDeviceActivationQrCode	Geräte-Instanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*
DeleteAssociatedDevice	Geräte-Instanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*
RebootDevice	Geräte-Instanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId*
CreateDeviceInstanceConfiguration	Konfiguration der Geräteinstanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId* /konfiguration/*version*
GetDeviceInstanceConfiguration	Konfiguration der Geräteinstanz arn:aws:one:*region:accountID* :Geräte-Instanz/*deviceInstanceId* /konfiguration/*version*

APIAktion	Ressourcen
CreateSite	Site arn:aws:one:*region:accountID* :seite/*siteId*
DeleteSite	Site arn:aws:one:*region:accountID* :seite/*siteId*
GetSiteAddress	Site arn:aws:one:*region:accountID* :seite/*siteId*
UpdateSite	Site arn:aws:one:*region:accountID* :seite/*siteId*
UpdateSiteAddress	Site arn:aws:one:*region:accountID* :seite/*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*
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 AWS Config Aktionen zum Lesen von Regeln, `GetSite` z. B. 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 API Enterprise-Regelaktionen auszuführen.

Zusätzliche Informationen

Weitere Informationen zum Erstellen von IAM Benutzern, Gruppen, Richtlinien und Berechtigungen finden Sie im Benutzerhandbuch unter Creating Your First IAM User and Administrators Group and Access Management. IAM

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 dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, 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 für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete 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 im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

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 die Erstellung eines QR-Codes zur Aktivierung des Geräts.

`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 hat begonnen, Änderungen nachzuverfolgen	Amazon One Enterprise hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	1. Dezember 2023

Problembehandlung bei Amazon One Enterprise: 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 auftreten könnenIAM.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon One Enterprise durchzuführen
- Ich möchte Leute außerhalb meines AWS-Konto um auf meine Amazon One Enterprise-Ressourcen zuzugreifen

Ich bin nicht berechtigt, eine Aktion in Amazon One Enterprise 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 `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `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 AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Leute außerhalb meines AWS-Konto um auf meine Amazon One Enterprise-Ressourcen zuzugreifen

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.
- Um zu erfahren, wie Sie Zugriff auf Ihre Ressourcen in allen Bereichen gewähren können AWS-Konten die Ihnen gehören, finden Sie unter Gewähren des Zugriffs für einen IAM Benutzer in einem anderen AWS-Konto die Sie besitzen, finden Sie im IAMBenutzerhandbuch.
- Um zu erfahren, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, siehe Zugriff gewähren auf AWS-Konten Eigentum Dritter im IAMBenutzerhandbuch.
- Informationen zur Bereitstellung des Zugriffs über einen Identitätsverbund finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise

Amazon One Enterprise (Servicepräfix:one) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur 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 `Action` Element einer IAM Grundsatzerklärung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, gewähren oder verweigern Sie normalerweise den Zugriff auf den API Vorgang oder 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 in ARN einer Anweisung mit dieser Aktion einen Ressourcentyp 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 `Resource` Element in einer IAM Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp ein ARN Oder-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 Berechtigung zum Erstellen einer Geräteinstanz	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 Aktivierung eines Geräts auf einer Geräteinstanz zu erstellen	Schreiben	Geräte-Instanz*		
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*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeviceInstanceConfiguration	Erteilen Sie die Berechtigung zum Erstellen der Geräteinstanzkonfiguration	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*		
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*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
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*		
ListDeviceConfigurationTemplates	Erteilen Sie die Erlaubnis, Gerätekonfigurationsvorlagen aufzulisten	Lesen			
UpdateDeviceConfigurationTemplate	Erteilen Sie die Erlaubnis, die Gerätekonfigurationsvorlage zu aktualisieren	Schreiben	device-configuration-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
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 Dienst definiert und können als `Resource` Element von IAM Berechtigungsrichtlinien verwendet werden. Jede Aktion in der Tabelle „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 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

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach Tag-Schlüsseln aus der Anforderung	ArrayOfString

Konformitätsprüfung 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:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

> **Note**
>
> Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- 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 für 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)) zusammengefasst.

- 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. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- 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 zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- 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.

Protokollierung und Überwachung 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 Anrufe 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 Anrufe 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.

Amazon One Enterprise-Veranstaltungen abonnieren

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. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich unter Busse die Option Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Weisen Sie der Regel auf der Detailseite der Standardregel einen Namen zu, wählen Sie Regel mit einem Ereignismuster aus, und klicken Sie dann auf Weiter.
5. Vergewissern Sie sich, dass auf der Seite Ereignismuster erstellen unter Ereignisquelle die Option AWS Ereignisse oder EventBridge Partnerereignisse ausgewählt ist.
6. Wählen Sie unter Ereignistyp die Option Eigenen Ereignistyp eingeben aus.
7. Kopieren und fügen Sie aus einem derBeispielereignisse.
8. Wählen Sie als Erstellungsmethode die Option Benutzerdefiniertes Muster aus. Fügen Sie im Abschnitt Ereignismuster ein Ereignis JSON mit der Ereignisquelle als **`aws:one`** und dem erforderlichen Detailtyp hinzu, und wählen Sie dann Weiter aus.
9. 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.
10. Optional können Sie Tags konfigurieren.
11. 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 generiertJSON. Für jeden Ereignistyp wird ein JSON Blob an das Ziel Ihrer Wahl gesendet, wie in der Regel konfiguriert. 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 ARNs, für die das Ereignis „Änderung des Gerätestatus“ veröffentlicht wurde.

Metadaten

siteName

- Name der Site, auf der der vorhanden deviceInstance ist.

siteArn

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

data

currentConnectivity

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

previousConnectivity

- Gibt an, ob vor dem Ereignis eine Verbindung zum Internet hergestellt oder getrennt deviceInstance wurde.
- Mögliche Werte:CONNECTED, DISCONNECTED

currentHealthStatus

- Stellt dar, ob der alle Zustandsprüfungen bestanden deviceInstance hat.
- Mögliche Werte:HEALTHY, CRITICAL

previousHealthStatus

- Gibt an, ob bei der letzten Überprüfung alle Integritätsprüfungen deviceInstance bestanden wurden.
- Mögliche Werte:HEALTHY, CRITICAL

assetTagId

- Das assetTagId des Geräts, das mit dem verknüpft istdeviceInstance.

deviceInstanceName

- Der Name des Geräts, deviceInstance für das 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.

Erfolglose 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.

requestSource

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

createdTimestamp

- Die Uhrzeit, zu der das Ereignis erstellt wurde.

userStatus

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

associatedId

- 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

Das Gerät hat alle Integritätswerte bestanden und der Integritätsstatus der Geräteinstanz wurde HEALTHY von „CRITICALIntegritätsstatus“ 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 Zustand des Geräts wurde auf Kritisch geändert

Das Gerät hat eine oder mehrere Integritätsprüfungen nicht bestanden, und der Systemstatus der Geräteinstanz wurde auf CRITICAL von geändertHEALTHY.

```
{
  "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 auf CONNECTED von geändertDISCONNECTED.

```
{
  "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 auf DISCONNECTED von geändertCONNECTED.

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

Neue erfolgreiche Registrierung

Ein Ereignis, bei dem sich ein Benutzer erfolgreich registriert hat.

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

```
        }
    }
}
```

Protokollieren von Amazon One API Enterprise-Anrufen 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 Anrufe für Amazon One Enterprise als Ereignisse. Zu den erfassten Anrufen gehören Anrufe von der Amazon One Enterprise-Konsole und Code-Aufrufe an den Amazon One API Enterprise-Betrieb. 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 dem 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 SNS Amazon-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 in der dokumentiertAktionen, 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 im CloudTrail userIdentityElement.

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"
}
```

Dokumentenverlauf für das Amazon One Enterprise-Benutzerhandbuch

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

Änderung	Beschreibung	Datum
Aktualisieren	Neues Thema hinzugefügt: Installation von Amazon One Device I/O Hub für sicheren Zugriff Amazon One Enterprise User Guide	14. August 2024
Aktualisieren	Neues Thema hinzugefügt: Installation eines an der Wand montierbaren Amazon One-Geräts Amazon One Enterprise User Guide	5. Juni 2024
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.