aws

ユーザーガイド

Amazon One Enterprise

Amazon One Enterprise: ユーザーガイド

Table of Contents

Amazon One Enterprise とは

Amazon One Enterprise は、バッジ、、PINsまたはパスコードを使用せずに、建物や企業資産への安全なアクセスを従業員に提供する新しいアクルードベースの認証サービスです。

トピック

Amazon One デバイス

Amazon One デバイスは、エンタープライズアクセスコントロールのための安全で、証明書ベースのアイデンティティサービスである Amazon One Enterprise 向けに設計されています。次のデバイス仕様に注意してください。

- ユーザー入力 — ヤシ生体認証、QR コードマッチング
- ホストインターフェイス — Wi-Fi (2.4 GHzおよび 5 GHz) 、イーサネット、2x USB Type-A、1 USB Type-B
- ユーザーフィードバック — 5.5 インチタッチスクリーン、照明、スピーカー、ヘッドフォン
- 物理アクセスコントロールプロトコル — OSDPおよび Wiegand
- 電源 — POE、110/220 VAC入力 AC から DC アダプター付属、30W @ 15V
- セキュリティ — 改ざんスイッチ
- ディメンション (HxWxD mm) — 86 x 85 x 256

Amazon One Enterprise コンソール

Amazon One Enterprise には、次の方法で使用できるコンソールが含まれています。

- IT マネージャーまたは施設マネージャーは、Amazon One Enterprise を使用してサイトを作成および管理します。このサイトは、Amazon One Enterprise デバイスとユーザープロファイルのモニタリングと管理中にチームが実行するタスクの物理的な場所のようになります。IT または施設マネージャーのタスクには以下が含まれます。
  - すべての Amazon One デバイスインスタンスを物理的な場所に格納するサイトの作成
  - サイトを管理する管理者ユーザーとアクティベーション QR コードにアクセスするためのインストーラユーザーの追加

- 管理者は Amazon One Enterprise を使用してデバイスインスタンスを作成し、Amazon One デバイスを管理します。管理タスクには以下が含まれます。

  - サイトの下にデバイスインスタンスを作成する
  - デバイスインスタンスに適用する設定テンプレートの作成
  - デバイスの状態のモニタリングとデバイス設定の更新
  - ユーザー登録のキャンセル

- インストーラは Amazon One Enterprise を使用してアクティベーション QR コードにアクセスし、デバイスをアクティブ化します。インストーラタスクには以下が含まれます。
  - コンソールでのアクティベーション QR コードへのアクセス
  - アクティブ化するデバイスインスタンスに対応する QR コードの選択
  - Amazon One デバイスがインストールされた状態で選択した QR コードをスキャンする

Amazon One デバイスの購入

Amazon One Enterprise の詳細については、お問い合わせください。ビジネス開発チームのメンバーから連絡があり、料金など、当社のサービスに関する詳細を共有し、ご質問があれば回答いたします。

Amazon One Enterprise の料金

Amazon One Enterprise の料金の詳細については、お問い合わせください。

Amazon One Enterprise の仕組み

Amazon One Enterprise は、Amazon One デバイスを使用してユーザーを認証するクラウドベースの生体認証サービスです。Amazon One デバイスを注文するには にお問い合わせいただき、Amazon One Enterprise セキュアアクセスサービスにサインアップするには を使用します AWS Management Console。

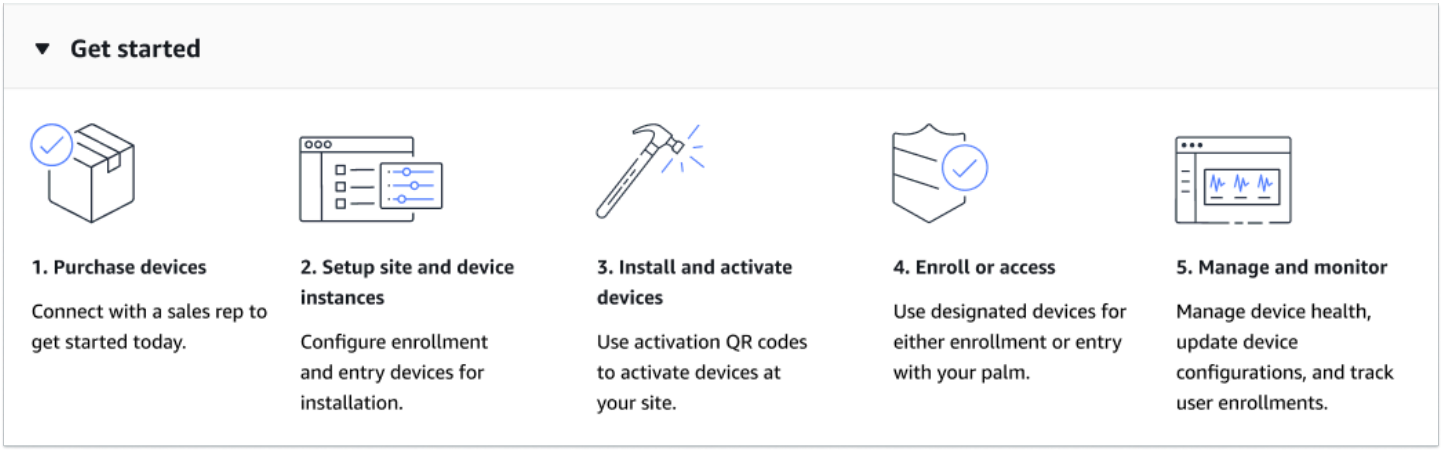
Amazon One Enterprise をインストールしたら、デバイスをアクティブ化して Amazon One Enterprise コンソール AWS アカウント の に登録し、認証アプリケーションを使用できます。登録された従業員の生体認証プロファイルを表示したり、従業員の登録をキャンセルしたりすることもできます。従業員が退職したりバッジを紛失したりすると、生体認証データを簡単に削除できます。Amazon One Enterprise Console は、インストールされたデバイスの追跡や月額請求の表示などの運用アクティビティを管理するための一元的な場所としても機能します。

従業員は、オンサイトの教師あり登録ステーションでバッジと家具をスキャンしてサインアップできます。従業員が登録されたら、Amazon One デバイスにカーソルを合わせるだけで、安全な場所に出入りできます。

トピック

Amazon One Enterprise ワークフロー

次の図は、Amazon One Enterprise の基本的なワークフローを示しています。



1. Amazon One デバイスを購入するには、 にお問い合わせください。

2. サイトとデバイスインスタンスを作成し、インストール用の登録デバイスとエントリデバイスを設定します。
3. インストール後、デバイスインスタンスに固有の安全な QR コードをスキャンして Amazon One デバイスをアクティブ化します。
4. 従業員に、各自の身分証明を登録し、その身分証明で認証してアクセス権を取得するように依頼します。
5. 管理およびモニタリング機能を活用する: デバイスの正常性を確保し、設定を最新の状態に保ち、ユーザー登録を追跡して包括的な監視を行います。

Amazon One Enterprise の主要用語

Amazon One Enterprise の主な用語は次のとおりです。

- サイト — お客様が Amazon One Enterprise デバイスをインストールするカスタマー管理の物理的な建物。サイトは、Amazon One Enterprise デバイスの施設、ネットワーク、および電源の要件を満たしている必要があります。
- デバイス - 認証用の Amazon One Enterprise スキャプションスキャン生体認証デバイス。
- デバイスインスタンス — 設定を持つデバイスの論理表現。デバイスインスタンスを使用すると、以前に設定した設定と名前を自動的に継承しながら、Amazon One デバイスをスワップできます。デバイスインスタンスには、ユーザー定義の名前 (アクセスコントロールソフトウェアとの共有命名規則) と一連の通信設定があります。デバイスインスタンスには 3 つの主要な状態があります。
  - 設定が必要
  - アクティベーション準備完了
  - [アクティブ]
- 設定テンプレート — デバイスインスタンスに適用されるすべての設定セット。

使用開始

この章では、Amazon One Enterprise の使用を開始するための基本的な手順について説明します。

1. サイト、デバイスインスタンス、および設定テンプレートのセットアップ — 以下の手順に従って、Amazon One デバイスを格納する物理的な場所を追加するためのフレームワークを作成し、それらを設定および管理します。この手順では、Amazon One Enterprise コンソールを使用します。このプロセスは、選択したサイト、デバイスインスタンス、および設定テンプレートの数に応じて、ときどき、または 1 回だけ使用します。
2. デバイスのインストールとアクティブ化 — セットアップの開始時に以下の手順に従います。デバイスのアクティベーションでは、インストーラが携帯電話から Amazon One Enterprise コンソールにアクセスしてアクティベーション QR コードを取得する必要があります。
3. デバイスとユーザー管理 — Amazon One Enterprise コンソールを毎日使用するには、次の手順に従います。これらのステップを使用して、デバイスのヘルスをモニタリングし、ユーザーエンゲージメントメトリクスを理解し、デバイスを設定できます。

Amazon One Enterprise の詳細については、「Amazon One Enterprise 製品の詳細」ページを参照してください。

トピック

Amazon One Enterprise のセットアップ

Amazon One Enterprise を使用する最初のステップは、Amazon One Enterprise コンソールを使用してサイト、デバイスインスタンス、および設定テンプレートを設定することです。

トピック

ステップ 1: アカウントと管理者ユーザーを作成する

にサインアップする AWS アカウント

をお持ちでない場合 AWS アカウントで、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/サインアップ を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップするとき AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーはすべての にアクセスできます AWS のサービス アカウントの および リソース。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ に移動し、マイアカウント を選択すると、いつでも現在のアカウントアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップした後 AWS アカウント、 をセキュリティで保護する AWS アカウントのルートユーザー、有効化 AWS IAM Identity Center、および日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. にサインインします。AWS Management Console ルートユーザーを選択し、 AWS アカウント E メールアドレス。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、「」の「ルートユーザーとしてサインインする」を参照してください。 AWS サインイン ユーザーガイド 。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「 の仮想MFAデバイスの有効化」を参照してください。 AWS アカウントIAM ユーザーガイドのルートユーザー (コンソール) 。

管理アクセスを持つユーザーを作成する

1. IAM Identity Center を有効にします。

   手順については、「 の有効化」を参照してください。 AWS IAM Identity Center ()AWS IAM Identity Center ユーザーガイド 。

2. IAM Identity Center で、ユーザーに管理アクセス権を付与します。

   の使用に関するチュートリアル IAM アイデンティティセンターディレクトリ ID ソースとして、「デフォルトを使用してユーザーアクセスを設定する」を参照してください。 IAM アイデンティティセンターディレクトリ ()AWS IAM Identity Center ユーザーガイド 。

管理アクセス権を持つユーザーとしてサインインする

- IAM Identity Center ユーザーでサインインするには、IAMIdentity Center ユーザーの作成時に E メールアドレスにURL送信されたサインインを使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 へのサインイン」を参照してください。 AWS の アクセスポータル AWS サインイン ユーザーガイド 。

追加のユーザーにアクセス権を割り当てる

1. IAM Identity Center で、最小特権のアクセス許可を適用するベストプラクティスに従うアクセス許可セットを作成します。

   手順については、「」の「アクセス許可セットの作成」を参照してください。 AWS IAM Identity Center ユーザーガイド 。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「」の「グループの追加」を参照してください。 AWS IAM Identity Center ユーザーガイド 。

ステップ 2: Amazon One Enterprise ユーザーを追加する

管理者ユーザーに加えて、管理者権限のないユーザーも追加できます。例えば、これらのユーザーは、Amazon One Enterprise コンソールにアクセスするインストーラであり、Amazon One デバイスをアクティブ化するためのデバイスアクティベーション QR コードを取得するだけです。

Amazon One Enterprise ユーザーを追加するには

1. 「 へのサインイン方法」の説明に従って、ユーザータイプに適したサインイン手順に従ってください。 AWS の AWS サインイン ユーザーガイド 。
2. ナビゲーションペインで、ユーザー を選択し、ユーザーの追加 を選択します。
3. [ユーザーの詳細を指定] ページの [ユーザーの詳細] の [ユーザー名] に、新しいユーザーの名前を入力します。これは のサインイン名です。 AWS.

   > **Note**
   >
   > 内のIAMリソースの数とサイズ AWS アカウント には制限があります。詳細については、IAM「」およびAWSSTS「 クォータ」を参照してください。ユーザー名は、最大 64 文字、数字、および次の文字の組み合わせにすることができます。プラス (+)、等号 (=)、カンマ (,)、ピリオド (.)、アットマーク (@)、アンダースコア (_)、ハイフン (-)。名前はアカウント内で一意である必要があります。大文字と小文字は区別されません。例えば、 TESTUSERと testuser という名前の 2 つのユーザーを作成することはできません。ポリシーまたは の一部としてユーザー名を使用する場合ARN、名前では大文字と小文字が区別されます。サインイン中など、コンソールにユーザー名が表示される場合、大文字と小文字は区別されません。

4. 個人にコンソールアクセスを提供しているかどうかを尋ねられます。「 へのユーザーアクセスを提供する」を選択します – AWS Management Console オプション 。
5. IAM ユーザー を作成するを選択します。
6. [コンソールのパスワード] で、以下のいずれかを選択します。

- 自動生成されたパスワード – ユーザーには、アカウントパスワードポリシー を満たすランダムに生成されたパスワードが与えられます。[パスワードの取得] ページに到達すると、パスワードを表示またはダウンロードできます。
- カスタムパスワード – ユーザーには、 フィールドに入力したパスワードが割り当てられます。

7. (オプション) デフォルトでは、ユーザーは次回のサインイン時に新しいパスワードを作成する必要があります (推奨) 。これにより、ユーザーは初回サインイン時にパスワードを変更する必要があります。

> **Note**
>
> 管理者が「[ユーザーにパスワードの変更を許可] のアカウントのパスワードポリシー設定」を有効にしている場合、このチェックボックスには何の効果もありません。それ以外の場合は、自動的に がアタッチされます。 AWS 新しいユーザーに という名前の `IAMUserChangePassword` マネージドポリシー。ポリシーは、ユーザーに対して、各自のパスワードを変更するためのアクセス許可を付与します。

8. [次へ] を選択します。
9. 許可を設定 ページで、ポリシーを直接アタッチする を選択します。
10. ユーザーにアタッチするポリシーを選択します。

- AmazonOneEnterpriseReadOnlyAccess
- AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess 管理ポリシーは、Amazon One Enterprise コンソールでのみアクティベーション QR コードへのユーザーアクセスを提供します。このポリシーは、Amazon One デバイスをインストールするためにサードパーティーを雇用する企業に最適です。

11. [次へ] を選択します。
12. (オプション) [レビューと作成] ページの [タグ] で [新しいタグを追加] を選択し、ユーザーにキーと値のペアとしてタグをアタッチし、メタデータを追加します。でのタグの使用の詳細についてはIAM、「 IAMリソースのタグ付け」を参照してください。

13. この時点で行ったすべての選択肢を確認します。続行する準備ができたら、[ユーザーの作成] を選択します。
14. [パスワードの取得] ページで、ユーザーに割り当てられたパスワードを取得します。
    - パスワードの横にある [表示] を選択すると、ユーザーのパスワードが表示され、手動で記録できます。
    - Download .csv を選択して、ユーザーのサインイン認証情報を安全な場所に保存できる .csv ファイルとしてダウンロードします。
15. [メールのサインイン方法] を選択します。ローカルメールクライアントに下書きが表示され、カスタマイズしてユーザーに送信できます。メールのテンプレートには、各ユーザーの以下の詳細が含まれています。
    - [ユーザーネーム]
    - URL アカウントサインインページに移動します。次の例を使用して、適切なアカウント ID またはアカウントエイリアスと置き換えます。

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

> **Important**
>
> ユーザーのパスワードは、生成されたメールには記載されていません。パスワードは、組織のセキュリティガイドラインに従った方法でユーザーに提供する必要があります。

ステップ 3: サイトを作成する

にサインインしたので AWS Management Consoleでは、Amazon One Enterprise コンソールを使用してサイトを作成できます。

> **Important**
>
> Amazon One Enterprise は、米国東部 (バージニア北部) リージョンでのみ利用できます。

サイトを作成するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. 「概要に移動」を選択します。
3. ナビゲーションペインで、[サイト] を選択します。
4. サイトの作成 を選択します。
5. サイト情報 のサイト名 にサイトの名前を入力します。
6. 「住所」に、Amazon One デバイスをインストールするサイトの住所を入力します。
7. (オプション) サイトにタグを追加するには、タグ の下にキーと値のペアを入力し、新しいタグを追加 を選択します。サイトを作成する前にこのタグを削除するには、 の削除を選択します。
8. サイトの作成を選択してサイトを作成します。

ステップ 4: デバイスインスタンスを作成する

デバイスインスタンスを作成するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。非アクティブ化されたインスタンスタブが表示されていることを確認します。
3. 「インスタンスの詳細」で、サイトドロップダウンからサイトを選択するか、「サイトの作成」ボタンを選択して新しいサイトを作成します。
4. 個々のデバイスインスタンス名 を手動で入力します。
5. (オプション) デバイスインスタンスにタグを追加するには、タグ の下にキーと値のペアを入力し、新しいタグ を追加 を選択します。デバイスインスタンスを作成する前にこのタグを削除するには、「 の削除」を選択します。
6. インスタンスの作成 を選択して、デバイスインスタンスを作成します。

> **Note**
>
> 注: デバイスインスタンスは、インストールを実行する前に設定する必要があります。

ステップ 5: 設定テンプレートを作成する

設定テンプレートを作成するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、設定テンプレート を選択します。
3. [テンプレートを作成] をクリックします。
4. 「テンプレート情報」の「テンプレート名」に、設定テンプレートの名前を入力します。
5. デバイス設定 で、オペレーションモード を選択します。

   To configure Enrollment operating mode

   1. (オプション) Wifi 設定 で、Wifi 認証情報 を指定します。
   2. (オプション) サイトにタグを追加するには、タグ の下にキーと値のペアを入力し、新しいタグ を追加 を選択します。サイトを作成する前にこのタグを削除するには、 の削除を選択します。
   3. [設定] を選択します。

   To configure Entry operating mode

   1. コントロールパネル設定 で、コントロールパネルと通信するための Amazon One デバイスの通信設定を指定します。
   2. バッジ形式設定 で、会社のバッジ形式のレイアウトを指定する構成設定を指定します。
   3. (オプション) Wifi 設定 で、Wifi 認証情報 を指定します。
   4. (オプション) サイトにタグを追加するには、タグ の下にキーと値のペアを入力し、新しいタグを追加 を選択します。サイトを作成する前にこのタグを削除するには、 の削除を選択します。
   5. [設定] を選択します。

> **Important**
>
> Amazon One Enterprise の全機能を有効にして安全なアクセスを実現するには、少なくとも 1 つの登録デバイスと 1 つのエントリデバイスを設定する必要があります。

ステップ 6: アクティベーション用にデバイスインスタンスを設定する

デバイスインスタンスを作成したら、以前に作成した設定テンプレートを使用してデバイスインスタンスを設定するか (「」を参照ステップ 5: 設定テンプレートを作成する)、手動で設定を追加できます。

デバイスインスタンスをアクティベーション用に設定するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。非アクティブ化されたインスタンスタブが表示されていることを確認します。
3. 設定するインスタンスを 1 つ以上選択します。
4. [設定] を選択します。
5. 「デバイス設定」で、次の 2 つの入力方法のいずれかを選択します。

   a. テンプレートの使用オプションで、ドロップダウンからテンプレートを選択します。このインポートされた設定情報を確認または変更します。

      テンプレートの作成オプションについては、「」を参照してくださいステップ 5: 設定テンプレートを作成する。

   b. 手動入力オプションで、操作モード を選択します。

      To configure Enrollment operating mode

      a. (オプション) Wifi 設定 で、Wifi 認証情報 を指定します。
      b. (オプション) サイトにタグを追加するには、タグ の下にキーと値のペアを入力し、新しいタグ を追加 を選択します。サイトを作成する前にこのタグを削除するには、 の削除を選択します。
      c. [設定] を選択します。

      To configure Entry operating mode

      a. コントロールパネル設定 で、コントロールパネルと通信するための Amazon One デバイスの通信設定を指定します。
      b. バッジ形式設定 で、会社のバッジ形式のレイアウトを指定する構成設定を指定します。

c. (オプション) Wifi 設定 で、Wifi 認証情報 を指定します。

d. (オプション) サイトにタグを追加するには、タグ の下にキーと値のペアを入力し、新しいタグを追加 を選択します。サイトを作成する前にこのタグを削除するには、 の削除を選択します。

e. [設定] を選択します。

6. 非アクティブ化されたインスタンステーブルで、インスタンスの状態は と表示されます 

。

7. アクティベーション QR コードがアクティベーションに使用できることを確認します。ナビゲーションペインで、アクティベーション QR コード を選択します。

8. サイトの選択ドロップダウンリストから、サイト を選択します。

9. サイト情報 で、サイトアドレスを検証します。

10. アクティベーション QR コード では、各デバイスインスタンスには対応する QR コードがあります。QR コードを取得 を選択して、アクティベーション QR コードを表示します。

> **Important**
>
> Amazon One Enterprise の全機能を有効にして安全なアクセスを実現するには、少なくとも 1 つの登録デバイスと 1 つのエントリデバイスを設定する必要があります。

Amazon One のインストールとアクティブ化

Amazon One Enterprise コンソールを設定したら、次のステップとして Amazon One Enterprise デバイスをサイトにインストールし、アクティブ化します。

> **Note**
>
> このセクションでは、インストールに焦点を当て、モバイルブラウザを使用して にアクセスします。 AWS Management Console デバイスアクティベーション QR コードを取得するには、 を使用します。

トピック

要件を理解する

Amazon One デバイスは、建物を閉鎖できるドアがある会社または会社の任意の場所にインストールできます。

コントロールパネルの要件

Amazon One デバイスは、ほとんどの標準アクセスコントロールパネルにリーダーとして接続できます。Amazon One デバイスは、次のプロトコルをサポートしています。

- OSDP (v1 および v2)
- Wiegand

ネットワーク要件

Amazon One デバイスは、通常のオペレーションで常にインターネットに接続する必要があります。インターネット接続は、有線イーサネットまたは Wi-Fi のいずれかで提供できます。必要な最小帯域幅は 10 Mbps です。

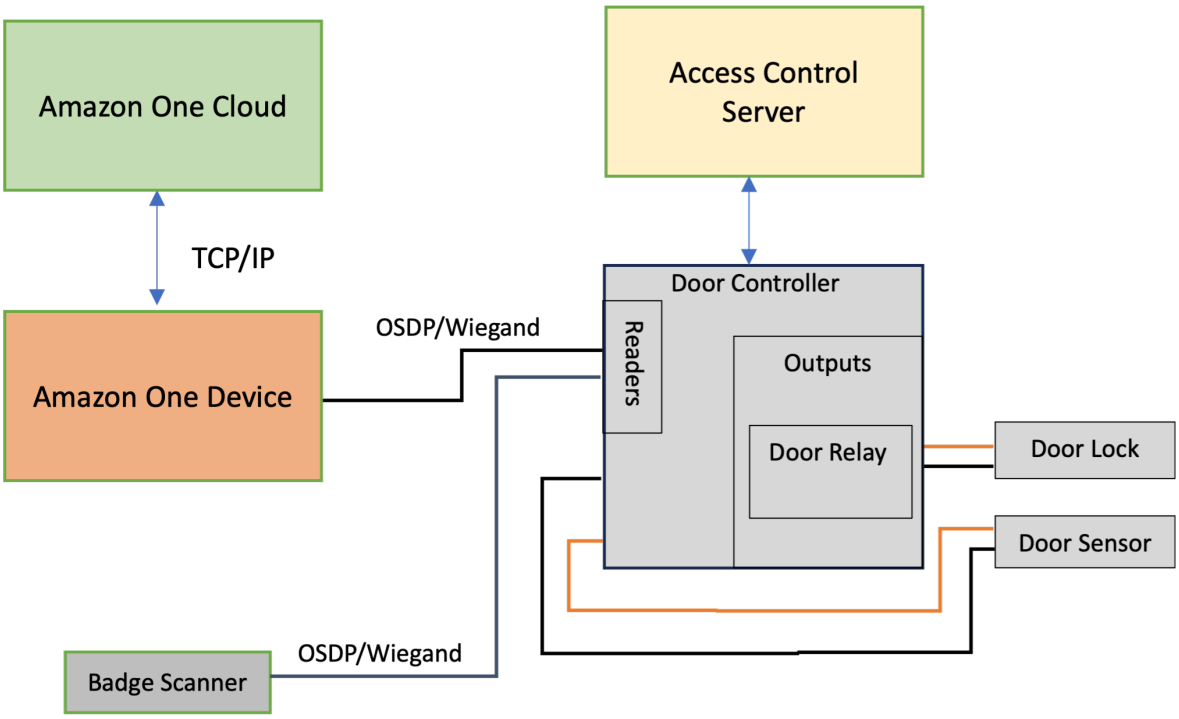
電力要件

Amazon One デバイスは、次の 2 つの方法のいずれかで電源を供給できます。

- ボックスで提供されている 120V 電源アダプターを使用します。
- PoE + 対応デバイスを使用する。

インストールの概念を理解する

構築アクセスを適切に保護するために、Amazon One Enterprise では、次のブロック図に示すように、一般的なアクセスコントロール環境の一部としてデバイスをインストールすることをお勧めします。



アクセスコントロール環境は通常、次のコンポーネントで構成されます。

- Amazon One デバイス: これは、建物の安全なエリアにアクセスしようとしている個人を特定するために生体認証を実行する、舌上認識デバイスです。
- アクセスコントロールサーバー: このコンポーネントは通常、ユーザーのセキュアエリアへのアクセス権限を制御します。通常IDs、エリアにアクセスできる個人のバッジは、このサーバーに保存されます。このサーバーは、適切なドアコントローラーIDsに関連する をキャッシュします。
- ドアコントローラー :
  - Amazon One デバイスは、 OSDPインターフェイスを介してドアコントローラーサーバーに接続します。
  - Wiegand インターフェイスが必要な場合は、 OSDPから Wiegand COTS へのコンバーターを使用できます。
  - 認証が成功すると、Amazon One デバイスはユーザーのバッジ ID を ドアコントローラーに送信します。
  - ドアコントローラーは決定を返信し、Amazon One デバイスがアクセス許可またはアクセス拒否メッセージを表示できるようにします。
- バッジスキャナー: バッジスキャナーは通常、RFIDバッジをスキャンしてバッジ番号を Access Control Server に送信するために使用されます。Amazon One Enterprise では、バッジスキャナーが登録 Amazon One デバイスに接続され、従業員のバッジをスキャンして、そのプロフィールに関連付けることができます。

Amazon One Enterprise ペデスタルのインストール

このセクションでは、Amazon One Enterprise ペデスタルのインストールに必要な場所の要件と手順の概要を説明します。

インストールを開始する前に、以下の前提条件を満たしていることを確認してください。

- POE+ を使用してデバイスに電力を供給する場合は、Cat6 ケーブルが配置され、POE+ インジェクターまたはスイッチが使用可能であることを確認します。
- AC 電源 (120V) ソースを使用している場合、AC コンセントはペデスタルから 20 AOE フィート以内に使用可能である必要があります。
- 床は水平でクリーンである必要があります。

- 台座はドアや車線をブロックしてはいけません。
- 余分なケーブルはすべて台座内に保管し、固定する必要があります。

Amazon One デバイスペデスタルをインストールするには

1. パッケージから Amazon One Enterprise ペデスタルを削除します。
2. 両方の M4 改ざん防止ネジをネジで外して、ドアを取り外します。
3. 電源ケーブルを接続します。ケーブルを台座ベースプレートの穴に通します。
4. ペデスタル内に余分な電源ケーブルを巻き付けます。
5. イーサネットケーブル (Cat5E 以上) を台座の下部プレートに通し、イーサネットポートに接続します。
6. イーサネットケーブル (Cat5E 以上) を台座の下部プレートに通し、イーサネットポートに接続します。
7. イーサネットケーブルのフェライトループを、台座のベースから 2 インチ上に取り付けます。
8. アクセスコントロールパネル (またはバッジリーダー) からペデスタルにRS485シリアルケーブルをフィードします。長さは 1 ft 超過します。
9. 台座のベースから 2 インチ上のRS485ケーブルにフェライトループを設置します。
10. 電源をコンセントに接続し、Amazon One デバイスがオンになっていることを確認します。
11. ドアを台座に再取り付けし、2 つの M4 改ざん防止ネジを再度ネジで固定します。

ウォールマウント可能な Amazon One デバイスのインストール

このセクションでは、ウォールマウント可能な Amazon One デバイスのインストールに必要な場所の要件と手順について詳しく説明します。

インストールを開始する前に、以下を確認してください。

- 壁面取り付け可能な Amazon One デバイスは、室内専用です。
- 壁は水平です。
- 壁面マウントの上部は、取り付け後に地面から 44～46" 以下にする必要があります。
- 余分なケーブルはすべて壁面取り付けの背後にあり、固定されています。
- Power over Ethernet (PoE++):

IEEE 802.3bt (タイプ 3) クラス 6 POE++ スイッチ (エンドスパン) またはインジェクター (ミッドスパン) IEC が使用可能であることを確認してください。このスイッチは、リスト化または認定されており、62368-1 に準拠しています。

AOE 承認された PoEソースでのみ使用してください。

++ PoE ソースは同じ建物内に配置する必要があります。

- DC 15V の電源入力では、NECクラス 2 または制限付きの承認済み電源がリストまたは認定されている Amazon One デバイスのみを使用する必要があります。

必要なツール：

- 壁アンカーが必要な場合は、1/4 インチドライウォールまたはメイソンドリルビット
- ワイヤストリッパー
- パイロットホールをドリルするための 7/64 インチドリルビット
- #2 プラスドライバー
- 0.5mm x 2mm マイナスドライバー
- T12 Secure Torx ドライバー
- 鉛筆
- レベル

ウォールマウント可能な Amazon One デバイスに含まれています。

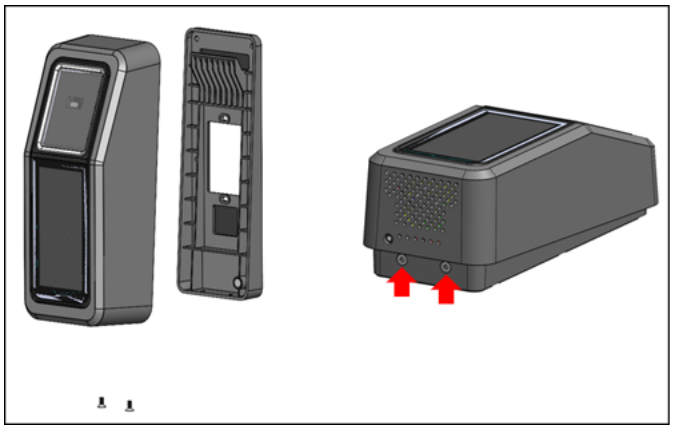
- 6x #8 ドライウォールアンカー
- #8-32 1 インチ長ネジ 6 本
- 2x #6-32 1in マシンネジ
- 2x 6 ポジションターミナルブロックコネクタ
- 2 トルクスセキュリティ M4x10 マイナスネジ

Amazon One デバイスの壁面取り付けプレートをインストールするには

<result>

</result>

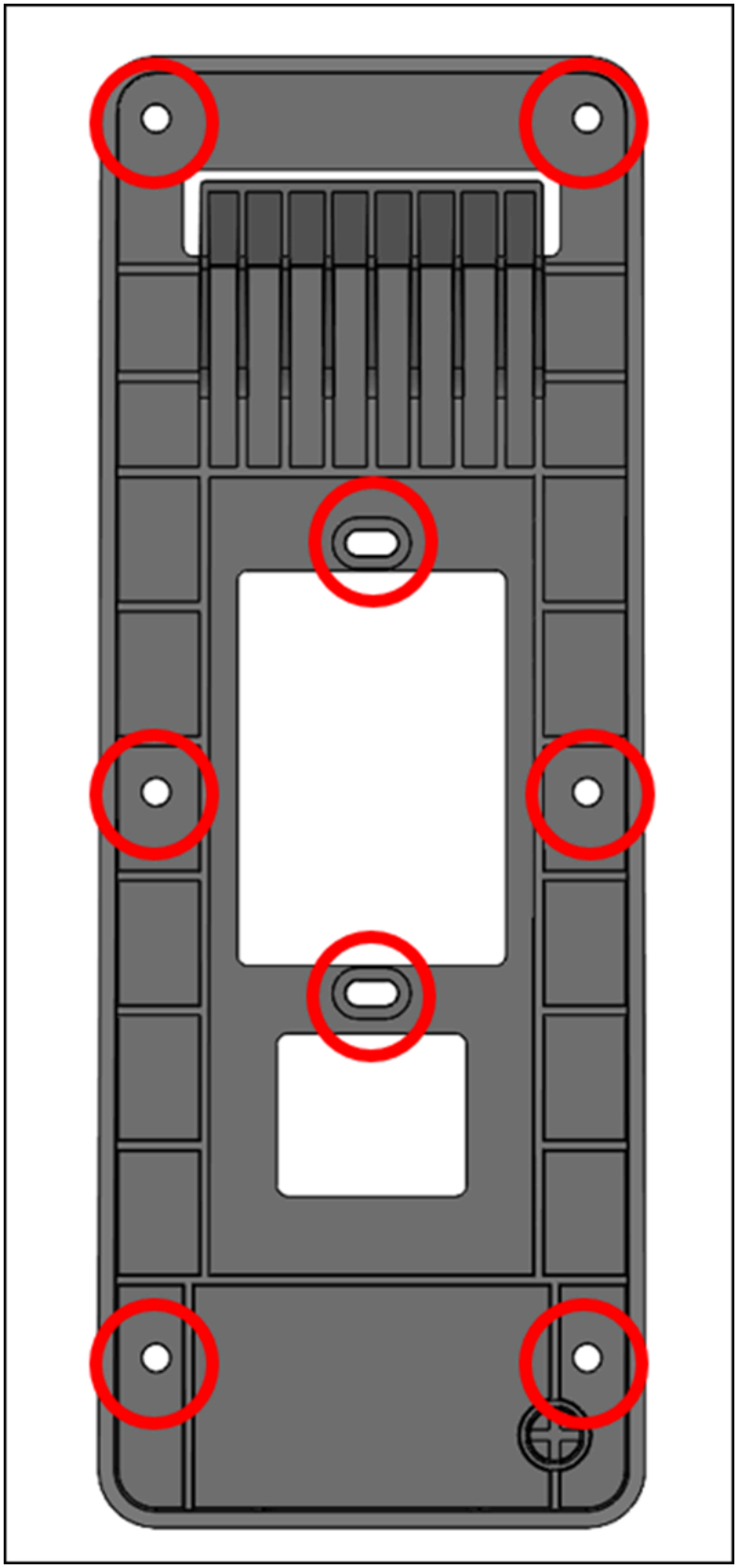
1. Amazon One デバイスをパッケージから削除します。
2. 下部の 2 つの Torx セキュリティネジを取り外して、Amazon One デバイスからマウントプレートを分離します。



3. 取り付けプレートを壁面を希望の位置に配置します。次の図に示すように、ブラケットをテンプレートとして使用して、外側の 6 つのネジ穴をマークします。

   (オプション) インストール位置に 1 つのギャングボックスがある場合は、以下を実行します。

   - 付属の #6-32 機械ネジを楕円穴に挿入して、プレートをギャングボックスに緩く取り付けます。
   - マウントプレートが水平であることを確認します。
   - マウントプレートをテンプレートとして使用して、6 つのネジの位置を鉛筆でマークします。取り付けプレートの追加サポートとして、長方形の穴と #6-32 ネジを使用できます。壁板を取り付ける主な手段として、#6-32 ネジの位置を使用しないでください。



4. スタッコ、ドライウォール、レンガ、またはコンクリートの表面に取り付ける場合は、マークされた各場所に 1/4 インチホールをドリルで開け、アンカーが壁と面一になるまで穴に押し込んで壁アンカーを設置します。

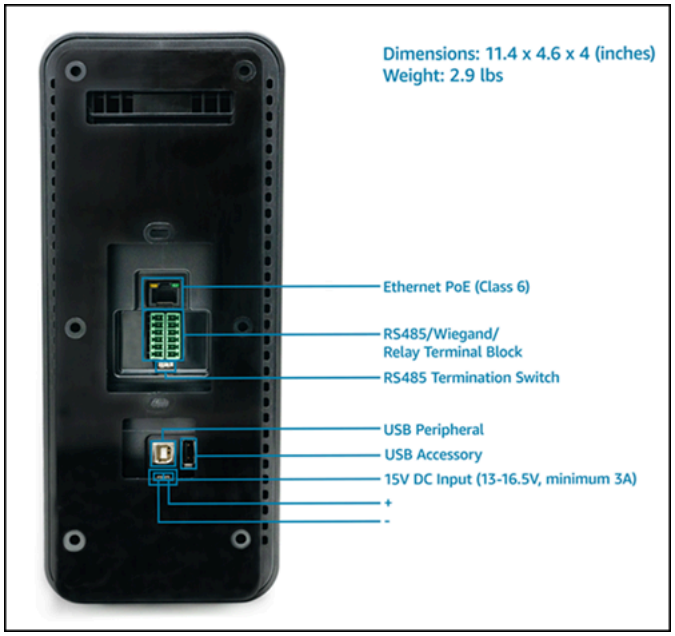
   床面に取り付ける場合、アンカーは必要ではなく、マークされた場所に 7/64 インチパイロットホールのみが必要です。
5. アンカーポジションの #8 木ネジを使用して、壁板を壁に緩く固定します。
6. ブラシがすべて揃ったら、マウントプレートが水平であることを確認します。
7. ネジを締めて、取り付けプレートを壁に固定します。

ウォールマウント可能な Amazon One デバイスを接続するには

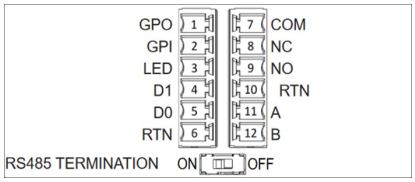
OSDP および Weigand アクセスコントロールプロトコルを使用して Amazon One デバイスを設定できます。インストールを簡素化するために、Amazon One デバイスはターミナルブロックコネクタを使用します (製造 P/N: Phoenix Contact 1767694)。また、内部リレーまたは汎用入出力接続を使用して、外部デバイスを直接制御するように Amazon One デバイスを設定するオプションもあります。

1. アプリケーションに適したワイヤリング設定を確認するには、次の図と接続表を参照してください。

   信号の詳細な電気特性については、「ワイヤリング手順」を参照してください。



   接続



ピン	Connection	説明	使用アイテム
1	GPO	汎用出力	デジタル出力信号 - オプション
2	GPI	汎用入力	デジタル入力信号 — オプション
3	LED	Wiegand LED	Wiegand LED – オプション
4	D1	Wiegand D1	Wiegand データ 1 – ホワイトワイヤ
5	D0	Wiegand D0	Wiegand データ 0 – グリーンワイヤ
6	RTN	シグナルリターン	Wiegand Ground – 黒線
7	通信	リレー共通	問い合わせリレー共通 — 白線
8	NC	リレーが正常に閉じられている	コンタクトリレーが通常閉じている — オレンジ色のワイヤ

ピン	Connection	説明	使用アイテム
9	いいえ	リレーは通常開	コンタクトリレーが正常に開いている — 黄色のワイヤ
10	RTN	シグナルリターン	OSDP return – 黒線
11	A	RS485_A/D1/クロック	OSDP D1 – 白線
12	B	RS485_B/D0/データ	OSDP D0 – 緑色のワイヤ

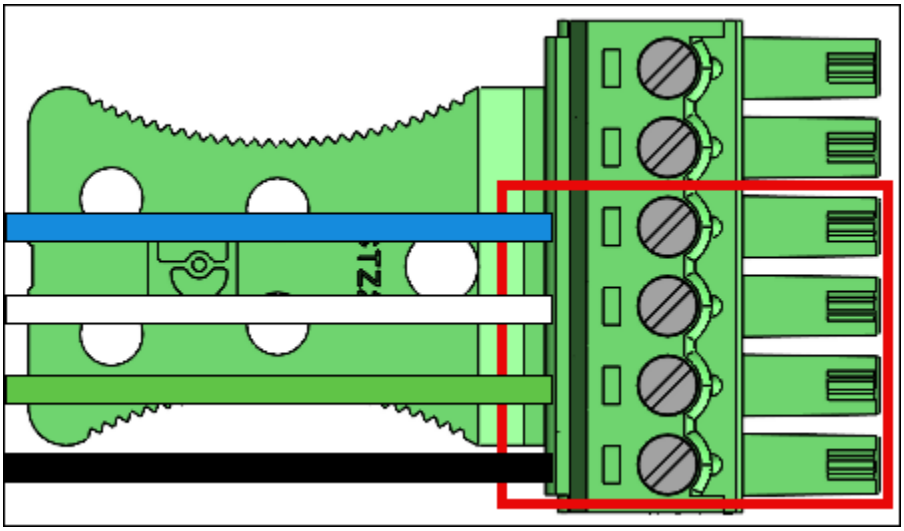
2. ワイヤを取り付けるときは、ワイヤの端から 3～5 mm 取り外します。
3. ワイヤのストライピングされた端を目的のターミナル位置に挿入します。
4. マイナスドライバーを使用して、ターミナル保持ネジを時計回りに回して、ワイヤが固定されるまでワイヤに固定します。きつすぎないでください。
5. 引き締め後、ワイヤーの引き込みをめがね、ワイヤーが固定されていることを確認します。
6. 必要な接続を行ったら、Amazon One デバイスターミナルブロックの対応するソケットにプラグを挿入します。
7. Cat6 イーサネットケーブルをRJ45ジャックに挿入します。
8. Amazon One デバイスを配置して、壁板のフックがデバイスの背面の開口部にスライドするようにします。
9. ケーブルがデバイスとマウントプレートの間に挟まれていないことを確認し、デバイスをピボットして所定の位置に固定します。
10. 2 本の Torx Security M4x10 マイナスネジを使用して、Amazon One デバイスをマウントプレートに固定します。
11. ネジを手締めします。きつすぎないでください。

ウォールマウント可能な Amazon One デバイスをワイヤリングするには

アプリケーションに必要なワイヤのみをインストールします。

Wiegand 接続

- 青いワイヤをピン 3 () に挿入しますLED。
- ピン 4 (D1) に白いワイヤを挿入します。
- 緑色のワイヤをピン 5 (D0) に挿入します。
- 黒いワイヤをピン 6 () に挿入しますRTN。



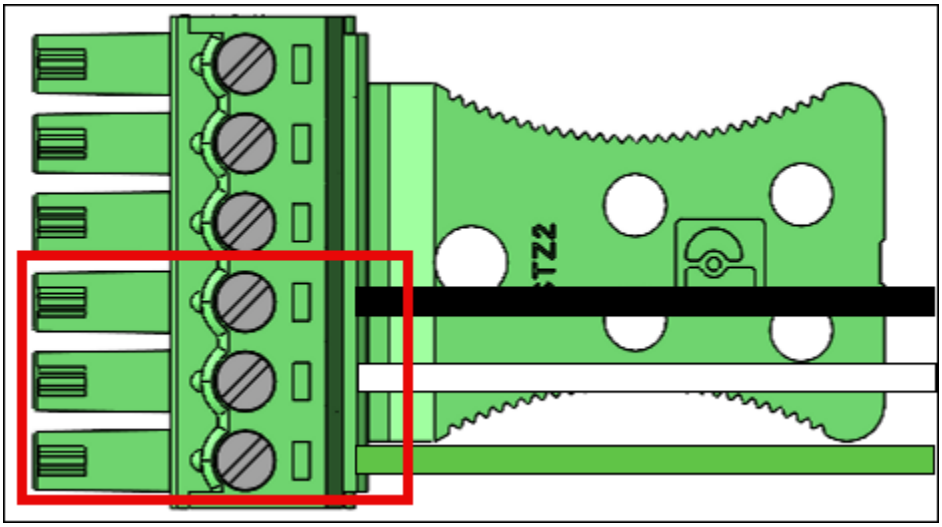
Wiegand 出力のワイヤリング

ピン	Connection	説明	使用アイテム	
3	LED	Wiegand LED	Wiegand LED入力 – オプション (5V TTL)	
4	D1	Wiegand D1	Wiegand D1 出力 (5V TTL)	
5	D0	Wiegand D0	Wiegand D0 出力 (5V TTL)	
6	RTN	シグナルリターン	Wiegand GNDリファレンス	

デバイスがライン上の最後の単位である場合は、RS485終了スイッチを「オン」にします。このスイッチは、 ラインで 120 オームの抵抗終了を有効にします。

RS485 接続

- 黒いワイヤをピン 10 () に挿入しますRTN。
- ピン 11 (A) に白いワイヤを挿入します。
- 緑色のワイヤをピン 12 (B) に挿入します。

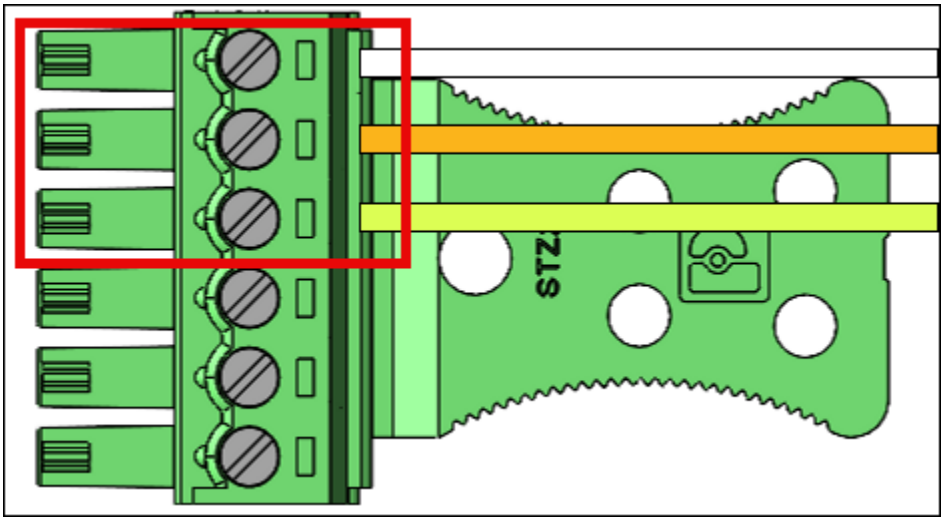


RS485 ワイヤリング

ピン	Connection	説明	使用アイテム	
10	RTN	シグナルリターン	地上	
11	A	RS485_A/D1/クロック	RS485 非反転信号	
12	B	RS485_B/D0/データ	RS485 信号の反転	

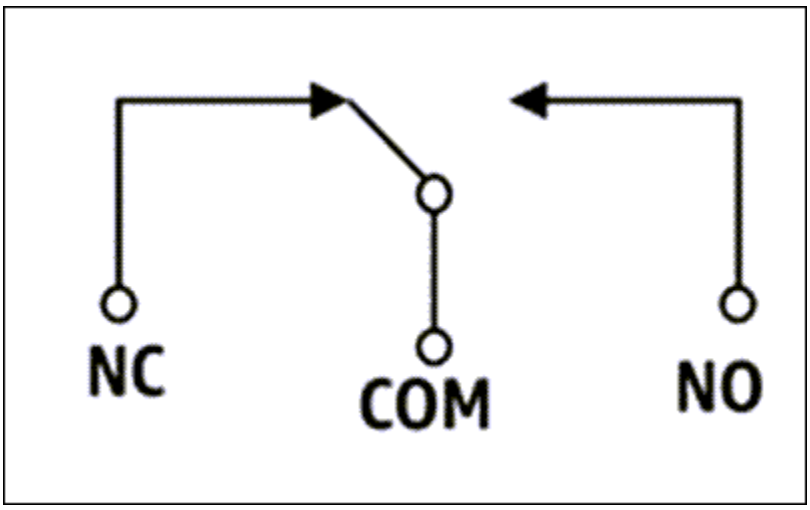
リレー接続

- ピン 7 () に白いワイヤを挿入しますCOM。
- オレンジ色のワイヤをピン 8 (NC) に挿入します。
- 黄色のワイヤをピン 9 (NO) に挿入します。



リレーのワイヤリング

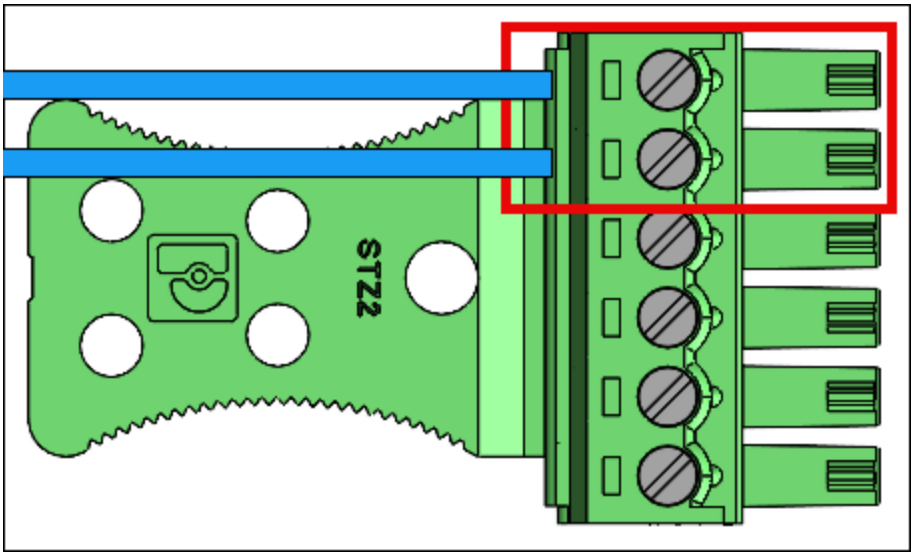
ピン	Connection	説明	使用アイテム
7	COM	リレー共通	問い合わせリレー共通 — ホワイトワイヤ
8	NC	リレーが正常に閉じられている	コンタクトリレーが通常閉じている — オレンジ色のワイヤ
9	いいえ	リレーは通常開	コンタクトリレーが正常に開いている — 黄色のワイヤ



リレーは、指定された安全評価 30VAC/60VDC、最大 60W に従って動作する必要があります。

デジタル入出力接続

- 青いワイヤをピン 1 () に挿入しますGPO。
- 青いワイヤをピン 2 () に挿入しますGPI。



ピン	Connection	説明	使用アイテム	
1	GPO	汎用出力	デジタル出力信号 (5V)	

ピン	Connection	説明	使用アイテム	
2	GPI	汎用入力	デジタル入力信号 (3.6V ~ 5V)	

- デジタル入出力接続は、リストされているとおりに動作する必要があります。

Amazon One デバイスをアクティブ化Amazon One Device のアクティブ化するには、「」を参照してください。

安全なアクセスのための Amazon One デバイス I/O Hub のインストール

このセクションでは、I/O Hub で Amazon One Enterprise (AOE) デバイスをインストールするために必要な場所の要件と手順について詳しく説明します。

インストールを開始する前に、以下を確認してください。

- I/O Hub を備えた Amazon One デバイスは、室内専用です。
- Power over Ethernet (PoE++):

  IEEE 802.3bt (タイプ 3) クラス 6 POE++ スイッチ (エンドスパン) またはインジェクター (ミッドスパン) IEC が使用可能であることを確認してください。このスイッチは、リスト化または認定されており、62368-1 に準拠しています。

  Amazon One デバイスは、承認された PoEソースでのみ使用してください。

  ++ PoE ソースは同じ建物内に配置する必要があります。

- DC 15V の電源入力では、NECクラス 2 の Amazon One デバイス、またはリスト化または認定されている電力制限付きの承認済み電源のみを使用する必要があります。以下のオプションの DC セクションを参照してください。

必要なツール：

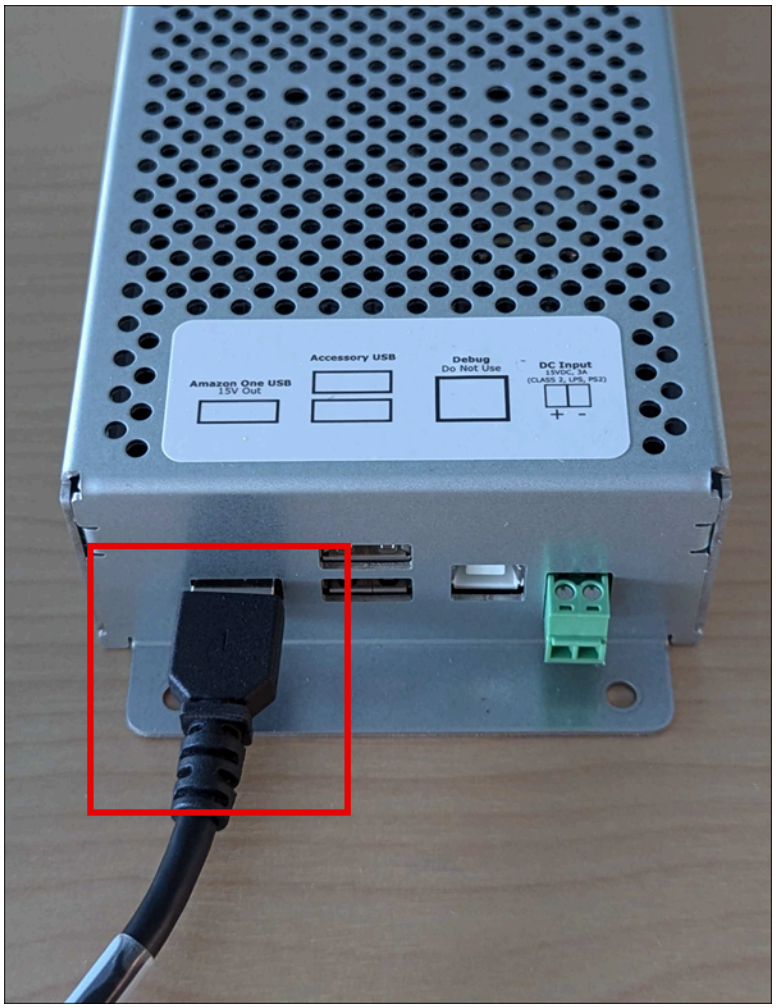
- ワイヤストリッパー
- #2 プラスドライバー
- 0.5mm x 2mm マイナスドライバー

I/O Hub を備えた Amazon One デバイスに含まれています。

- 2x 6 ポジションターミナルブロックコネクタ
- DC プラグコネクタ
- 72「電源ケーブル/データケーブル」

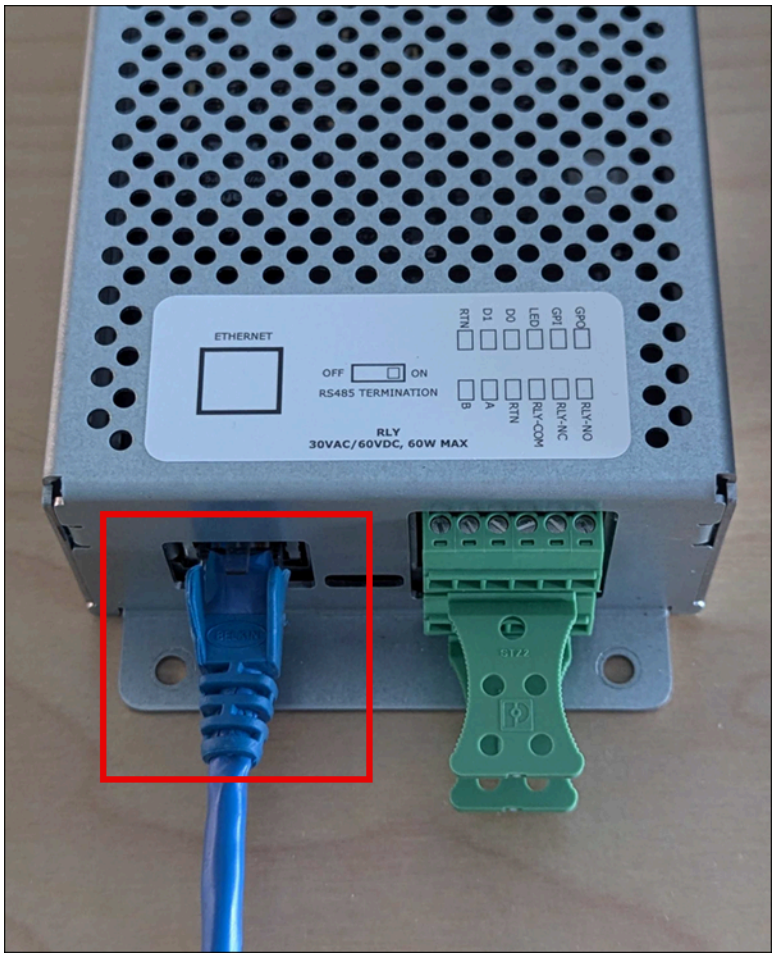
Amazon One デバイスの I/O ハブをインストールするには

1. I/O Hub を備えた Amazon One デバイスをパッケージから削除します。
2. I/O ハブを希望の場所に固定します。
3. Amazon One ケーブルを I/O ハブポートUSBに接続します。



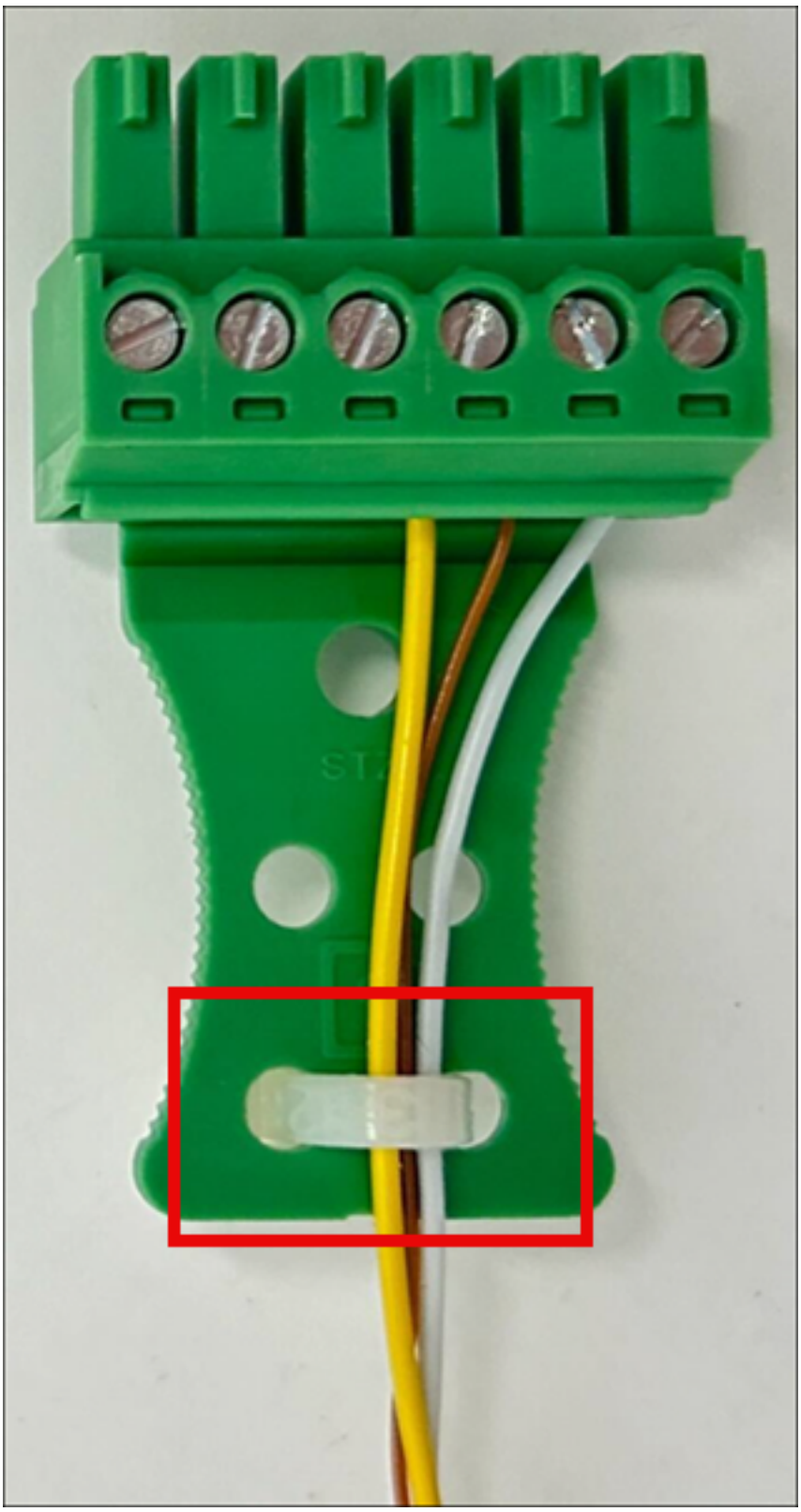
4. POE++ 電源の場合は、POE++ ソースから I/O ハブポートにイーサネットケーブルを接続します。

オプション: DC 電源については、以下の「DC 接続のインストール」セクションを参照してください。



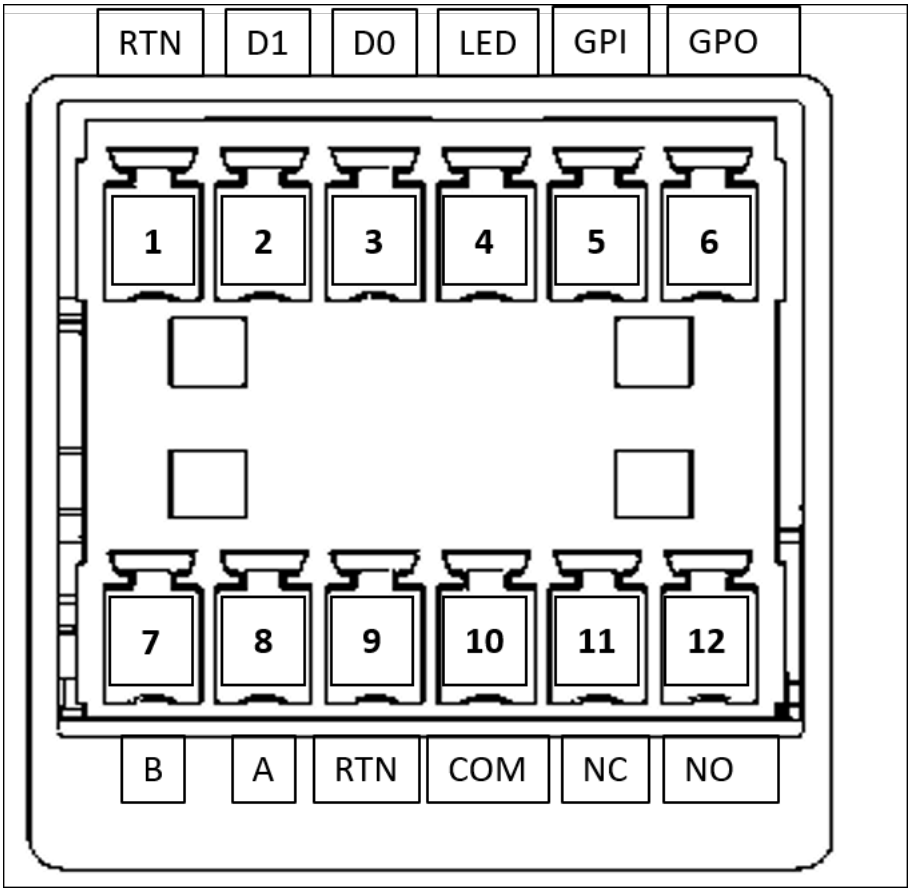
Amazon One デバイスの I/O ハブをワイヤリングするには

- 跳ね返りループを設置して、誤って水がコードから I/O ハブに流れ込まないようにします。
- 次の図に示すように、ストレインドレプリケーションクランプをアタッチして、ワイヤを損傷やストレスから保護します。



1. ターミナルブロックプラグを介して、アプリケーションに必要なワイヤのみを挿入します。次のワイヤリングテーブルと図を参照してください。

2. ターミナルブロックプラグを I/O ハブに挿入します。

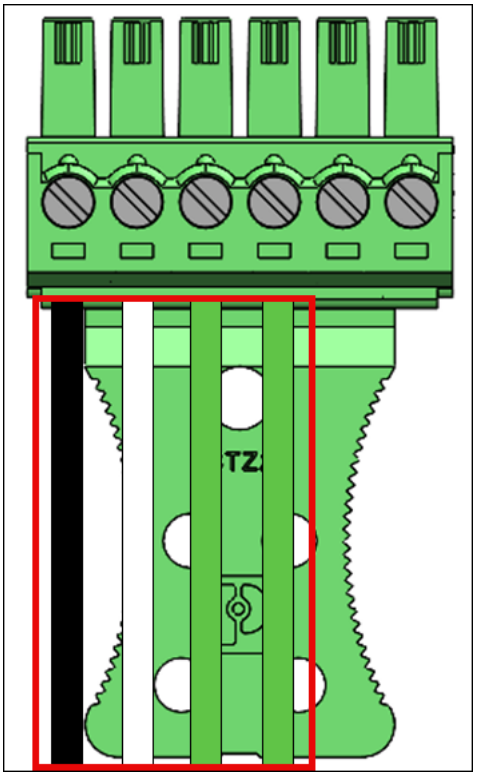


ピン	Connection	説明	使用アイテム	
1	RTN	シグナルリターン	Wiegand Ground – 黒線	
2	D1	Wiegand D1	Wiegand データ 1 – ホワイトワイヤ	
3	D0	Wiegand D0	Wiegand データ 0 – グリーンワイヤ	
4	LED	Wiegand LED	Wiegand LED – オプション	

ピン	Connection	説明	使用アイテム
5	GPI	汎用入力	デジタル入力信号 — オプション
6	GPO	汎用出力	デジタル出力信号 - オプション
7	B	RS485_B/D0/データ	OSDP D0 – 緑色のワイヤ
8	A	RS485_A/D1/クロック	OSDP D1 – 白線
9	RTN	シグナルリターン	OSDP return – 黒線
10	COM	リレー共通	コンタクトリレー共通 — 白線
11	NC	リレーは通常閉じている	コンタクトリレーは通常閉じている — オレンジ色のワイヤ
12	いいえ	リレーは通常開	コンタクトリレーが正常に開いている — 黄色のワイヤ

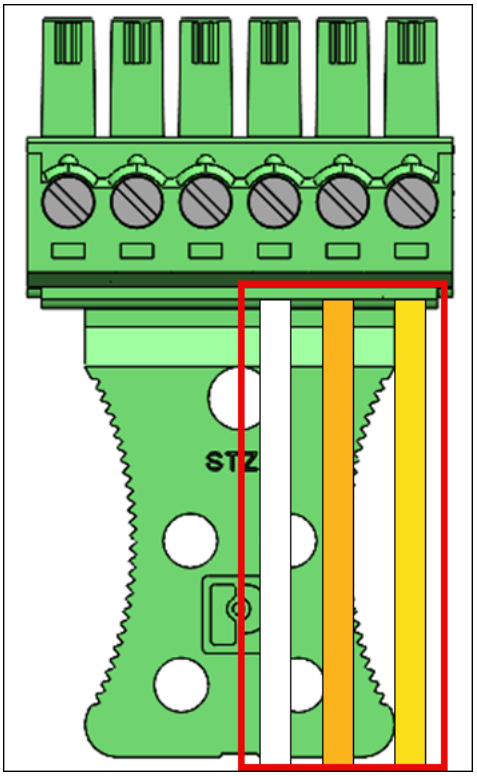
Wiegand 接続

- 黒いワイヤをピン 1 () に挿入しますRTN。
- ピン 2 (D1) に白いワイヤを挿入します。
- 緑色のワイヤをピン 3 (D0) に挿入します。
- オプション: 緑色のワイヤをピン 4 () に挿入しますLED。

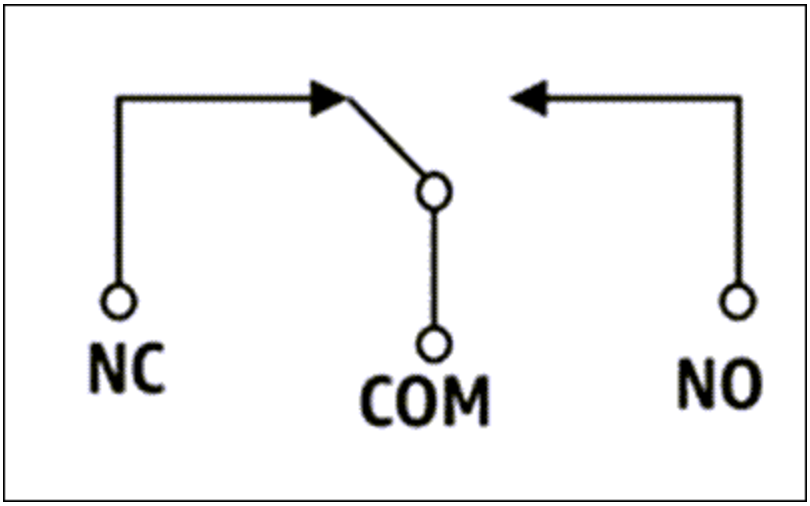


リレー接続

- 白いワイヤをピン 10 () に挿入しますCOM。
- オレンジ色のワイヤをピン 11 (NC) に挿入します。
- 黄色のワイヤをピン 12 (NO) に挿入します。



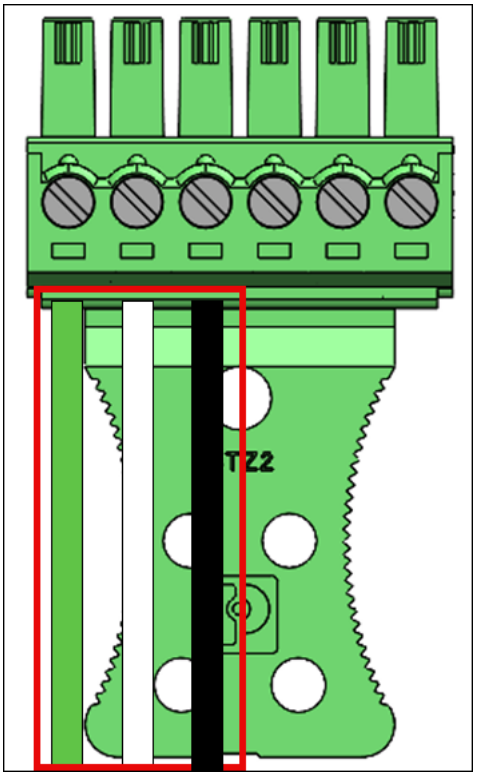
リレー図



リレーは、指定された安全評価 30VAC/60VDC、最大 60W に従って動作する必要があります。

RS485 接続

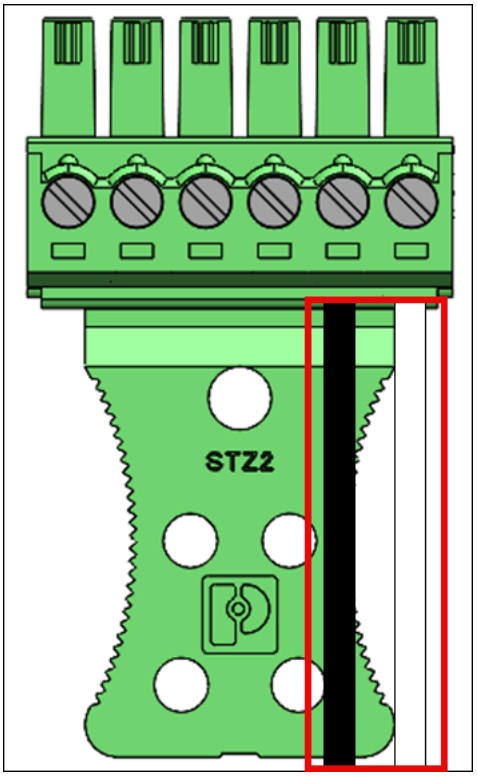
- 緑色のワイヤをピン 7 (B) に挿入します。
- ピン 8 (A) に白いワイヤを挿入します。
- 黒いワイヤをピン 9 () に挿入しますRTN。



デバイスが行の最後の単位である場合は、RS485終了スイッチを「オン」にします。このスイッチは、 ラインで 120 オームの抵抗終了を有効にします。

デジタル入出力接続

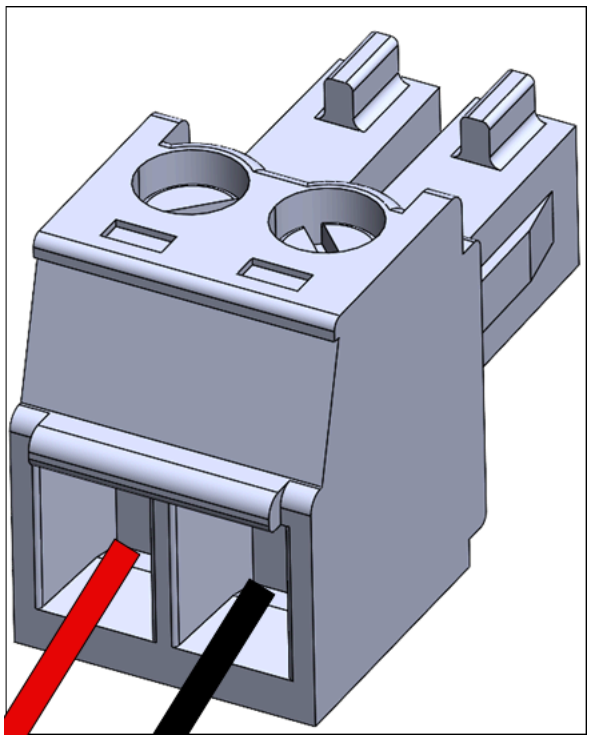
- 黒いワイヤをピン 5 () に挿入しますGPI。
- 白いワイヤをピン 6 () に挿入しますGPO。



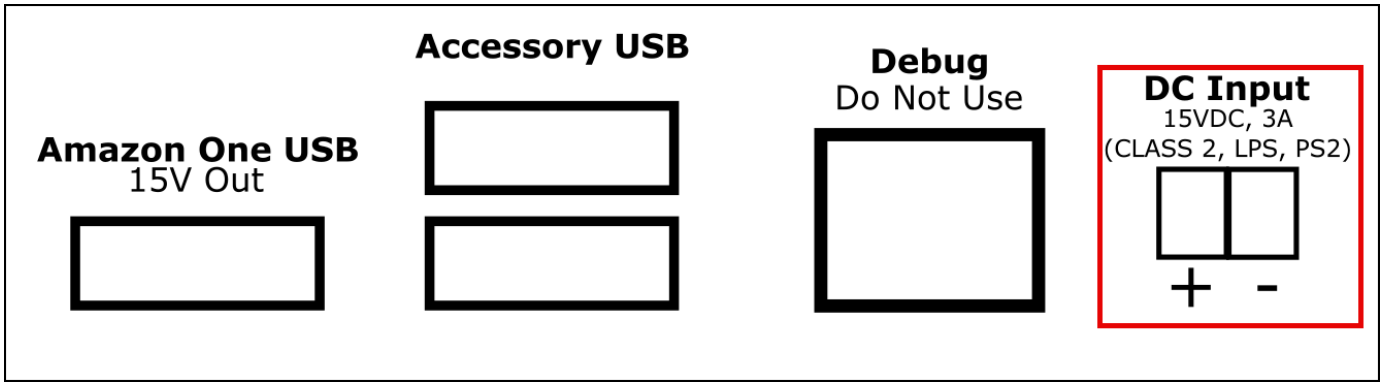
- デジタル入出力接続は、リストされているとおりに動作する必要があります。

オプション: DC ワイヤリングをインストールするには

1. 正の (+) の場合は赤色のワイヤの端から 3mm ~ 5mm、負の (-) の場合は黒のワイヤを取り除きます。
2. DC ワイヤのストライピングされた端を DC プラグに挿入します。



3. ワイヤを所定の位置に固定します。
4. 有線 DC プラグを DC 入力ポートに挿入します。



Amazon One Device のアクティブ化

Amazon One デバイスをインストールして電源を入れると、アクティブ化する準備が整います。

Amazon One デバイスをアクティブ化するには

1. Amazon One デバイスで、画面をタップして開始します。
2. インターネットに接続するには、イーサネットまたは Wifi を選択します。

デバイスがインターネットに接続するとすぐに、最新のソフトウェアパッケージのダウンロードが開始されます。

3. 画面にソフトウェアのダウンロードが完了したことが表示されたら、OK を選択します。
4. QR コード を選択します。

   Amazon One デバイス画面には、スキャン QR コード が表示されます。
5. アクティベーション QR コードを取得するには、https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。

   > **Note**
   >
   > Amazon One Enterprise コンソールでアクティベーション QR コードにのみアクセスできるように、インストーラーに限定的なアクセス許可を付与することを強くお勧めします。「ステップ 2: Amazon One Enterprise ユーザーを追加する」を参照してください。
6. ナビゲーションペインで、アクティベーション QR コード を選択します。
7. サイトの選択ドロップダウンリストから、Amazon One デバイスがインストールされているサイトを選択します。
8. サイト情報 で、サイトアドレスを確認します。
9. アクティベーション QR コード で、アクティブ化するデバイスインスタンス名を探し、対応する QR コードを取得 を選択して QR コードを取得します。
10. Amazon One デバイスで QR コードをスキャンします。
11. Amazon One デバイスの画面にアクティベーション完了と表示されると、デバイスは使用可能になります。

登録とエントリ

Amazon One デバイスがアクティブ化されたので、従業員は自分の紋章の登録を開始し、紋章を認証してアクセスできるようになります。

トピック

- ユーザー登録
- エントリの認証

ユーザー登録

ユーザーがエントリのアタッチを認証する前に、登録プロセスを実行する必要があります。セキュリティ担当者は、ユーザーの登録を許可する前に、常にユーザーの ID を確認する必要があります。

Amazon One デバイスで録音を登録するには

1. Amazon One Enterprise 登録デバイスで、開始方法 を押します。
2. Amazon One Enterprise 登録デバイスに接続されているバッジスキャナーで従業員バッジをスキャンします。

   バッジが正常にスキャンされると、Amazon One デバイス画面には、スキャンされたバッジが表示されます。
3. 利用規約を読み、OK を押します。
4. 「同意」を読む - お客様のヤシの生体認証情報「」を参照し、同意する場合は「同意」を押します。
5. 画面の指示に従って登録プロセスを完了します。

エントリの認証

アプライドを正常に登録したら、Amazon One Enterprise エントリデバイスでアプライドを使用して認証する準備が整います。

Amazon One デバイスでエントリのアプライドを認証するには

- デバイスの上部にカーソルを置き、画面の指示に従ってアプライドをスキャンします。

登録されたユーザー管理

登録済みユーザー管理ページを使用して、登録済みユーザーを追跡し、ユーザーの生体認証を削除できます。関連付けられた生体認証が削除されたユーザーは、認証のために Amazon One デバイスにアクセスできなくなります。

登録済みユーザーを表示するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。

2. ナビゲーションペインで、登録済みユーザー管理 を選択します。
3. 登録済みユーザー には、登録済みユーザーと以下の詳細がすべて表示されます。
   - バッジ ID — 登録時にバッジリーダーによってキャプチャされたRFIDバッジ識別子情報。
   - 登録ソース — 登録に使用された Amazon One デバイスの詳細。
   - 登録日 — 登録日時。

登録されたユーザーとその生体認証を削除するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、登録済みユーザー管理 を選択します。
3. 登録済みユーザー で、登録済み生体認証データを削除するユーザーのバッジ ID を選択します。
4. 生体認証 の削除 を選択します。
5. 削除 を選択して、ユーザーの生体認証データの削除を確認します。

> **Important**
>
> このアクションにより、Amazon One Enterprise からユーザーの生体認証が永続的に削除されます。認証に Amazon One Enterprise を使用するには、ユーザーは Amazon One Enterprise 登録デバイスに再度登録する必要があります。ユーザーの生体認証を削除すると、バッジ ID などの他のプロファイル属性も Amazon One Enterprise から完全に削除されます。

デバイスの管理

Amazon One デバイスをインストールしてアクティブ化すると、Amazon One Enterprise コンソールでデバイスの状態の報告が開始されます。Amazon One Enterprise コンソールを使用して、デバイスの再起動や設定の更新などのデバイス管理タスクを実行できます。

トピック

サイト管理

サイトは、一連のデバイスインスタンスがインストールされ、運用されている物理的な場所を表します。サイトを使用して、同じ住所を共有する Amazon One デバイスを整理できます。

サイト名を変更するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、サイト を選択します。
3. サイト で、名前を編集するサイトを選択します。
4. [編集] を選択します。
5. サイト情報に、目的のサイト名とサイトの説明を入力します (オプション)。
6. 更新する変更の保存を選択します。

サイトアドレスを更新するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、サイト を選択します。
3. サイト で、アドレスを更新するサイトを選択します。
4. デバイスインスタンス で、アクティブ化されたインスタンスの数が 0 であることを確認します。
5. (オプション) アクティブ化されたインスタンスの数が 0 でない場合は、「」を参照してください。 デバイスインスタンスを無効にするには
6. [編集] を選択します。
7. 「住所」に正しい住所を入力します。
8. 更新する変更の保存を選択します。

デバイスインスタンス管理

デバイスインスタンスは、設定を持つデバイスの論理表現です。デバイスインスタンスを使用すると、以前に設定した設定と名前を自動的に継承しながら、Amazon One デバイスをスワップできま

す。デバイスインスタンスには、ユーザー定義の名前 (アクセスコントロールソフトウェアとの共有命名規則) と一連の通信設定があります。

デバイスインスタンスのステータスを表示するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。
3. アクティブ化されたインスタンス の下に、アクティブ化された Amazon One デバイスのリストが表示されます。
4. デバイスインスタンス名を選択すると、デバイスインスタンスの詳細が表示されます。

Amazon One デバイスを再起動するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。
3. アクティブ化されたインスタンス で、再起動するデバイスのインスタンス名を選択します。
4. 再起動 を選択して Amazon One デバイスを再起動します。

Amazon One デバイス設定を更新するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。
3. アクティブ化されたインスタンス で、更新するデバイスのインスタンス名を選択します。
4. デバイス設定 で、編集 を選択します。

> **Note**
>
> Amazon One デバイスモードを変更するには、まずデバイスインスタンスを非アクティブ化してから、目的のデバイスモードで設定する必要があります (「」を参照ステップ 6: アクティベーション用にデバイスインスタンスを設定する)。その後、デバイスのアクティベーションプロセスを実行できます (「」を参照Amazon One Device のアクティブ化)。

5. 必要な変更を加えたら、デバイス設定の更新を選択して更新を確認します。

Wifi 認証情報を更新するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。
3. アクティブ化されたインスタンス で、更新するデバイスのインスタンス名を選択します。
4. ネットワーク で、編集 を選択します。
5. Wi-Fi 設定 で、必要な変更を加えます。
6. ネットワークの更新 を選択して、更新を確認します。

デバイスインスタンスを無効にするには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、デバイスインスタンス を選択します。
3. アクティブ化されたインスタンス で、非アクティブ化するデバイスインスタンスの名前を選択します。
4. デバイス を非アクティブ化 を選択します。
5. 非アクティブ化を確認するには、メッセージボックスに「非アクティブ化」と入力し、「デバイスの非アクティブ化」を選択します。

Amazon One Enterprise のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。また、 は、お客様が安全に使用できるサービス AWS も提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。Amazon One Enterprise に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon One Enterprise を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように Amazon One Enterprise を設定する方法について説明します。また、Amazon One Enterprise リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- Amazon One Enterprise でのデータ保護
- Amazon One Enterprise の Identity and Access Management
- Amazon One Enterprise のアクション、リソース、および条件キー
- Amazon One Enterprise のコンプライアンス検証

Amazon One Enterprise でのデータ保護

- AWS 責任共有モデル、Amazon One Enterprise でのデータ保護に適用されます。このモデルで説明されているように、 AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。 AWS クラウド。 お客様は、このインフラストラクチャでホストされているコン

テンツの制御を維持する責任があります。また、 のセキュリティ設定と管理タスクについても責任を負います。 AWS のサービス 使用する 。データプライバシーの詳細については、「データプライバシーFAQ」を参照してください。欧州でのデータ保護の詳細については、「」を参照してください。 AWS の責任共有モデルとGDPRブログ記事 AWS セキュリティブログ 。

データ保護の目的で、 を保護することをお勧めします。 AWS アカウント 認証情報と を使用して個々のユーザーをセットアップする AWS IAM Identity Center または AWS Identity and Access Management （ IAM ）。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1TLS.2 が必要で、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定する AWS CloudTrail。 CloudTrail 証跡を使用してキャプチャする方法については、「」を参照してください。 AWS アクティビティ、「」の「証 CloudTrail 跡の使用」を参照してください。 AWS CloudTrail ユーザーガイド。
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス.
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- アクセス時に FIPS 140-3 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。使用可能なFIPSエンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、Amazon One Enterprise またはその他の を使用する場合も同様です。 AWS のサービス コンソール、API、 AWS CLI、または AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

保管中のデータのデフォルトの暗号化を使用するには

Amazon One Enterprise は、デフォルトで暗号化を提供し、AWS暗号化キーを使用して保管中の機密データを保護します。

AWS 所有キー — Amazon One Enterprise は、デフォルトでこれらのキーを使用して、機密性の高いエンドユーザーデータを自動的に暗号化します。AWS 所有キーを表示、管理、使用したり、その使用を監査したりすることはできません。ただし、データを暗号化するキーを保護するためのアクションの実施やプログラムの変更を行う必要はありません。詳細については、「 Key Management Service デベロッパーガイド」の「 AWS所有AWSキー」を参照してください。

転送中のデータの暗号化

Amazon One Enterprise は、Transport Layer Security (TLS) を使用してデータを保護し、署名バージョン 4 を使用して AWSサービスへのすべてのインバウンドAPIリクエストを認証します。この暗号化はデフォルトで有効になっています。

Amazon One Enterprise の Identity and Access Management

AWS Identity and Access Management （ IAM) は AWS のサービス 管理者が へのアクセスを安全に制御するのに役立ちます。 AWS リソースの使用料金を見積もることができます。IAM 管理者は、誰を認証 (サインイン) し、誰に Amazon One Enterprise リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は AWS のサービス 追加料金なしで使用できます。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon One Enterprise と の連携方法 IAM
- Amazon One Enterprise のアイデンティティベースのポリシーの例
- AWS Amazon One Enterprise の マネージドポリシー
- Amazon One Enterprise のアイデンティティとアクセスのトラブルシューティング

対象者

の使用方法 AWS Identity and Access Management （ IAM) は、Amazon One Enterprise で行う作業によって異なります。

サービスユーザー - Amazon One Enterprise サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの Amazon One Enterprise 機能を使用

して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Amazon One Enterprise の機能にアクセスできない場合は、「」を参照してくださいAmazon One Enterprise のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の Amazon One Enterprise リソースを担当している場合は、通常、Amazon One Enterprise へのフルアクセスがあります。サービスユーザーがどの Amazon One Enterprise 機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、の基本概念を理解してくださいIAM。会社で Amazon One Enterprise IAMを使用する方法の詳細については、「」を参照してくださいAmazon One Enterprise と の連携方法 IAM。

IAM 管理者 – IAM管理者は、Amazon One Enterprise へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。で使用できる Amazon One Enterprise アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証は、 にサインインする方法です。 AWS ID 認証情報を使用する。認証されている必要があります (にサインインします AWSとしての) AWS アカウントのルートユーザー、 IAM ユーザーとして、または IAMロールを引き受ける方法。

にサインインできます。 AWS ID ソースを通じて提供される認証情報を使用して、フェデレーティッド ID として を指定します。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。にアクセスする場合 AWS フェデレーションを使用すると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 にサインインできます。 AWS Management Console または AWS アクセスポータル。へのサインインの詳細については、「」を参照してください。 AWS「 にサインインする方法」を参照してください。 AWS アカウント ()AWS サインイン ユーザーガイド 。

アクセスする場合 AWS プログラムにより、 AWS は、 認証情報を使用してリクエストに暗号で署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) を提供します。を使用しない場合 AWS ツール、リクエストには自分で署名する必要があります。推奨される方法を使用してリクエストに自分で署名する方法の詳細については、「署名」を参照してください。AWS API IAMユーザーガイドの リクエスト。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 などです AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「」の「多要素認証」を参照してください。 AWS IAM Identity Center ユーザーガイドと での多要素認証 (MFA) の使用 AWS「」(IAM ユーザーガイド) を参照してください。

AWS アカウント ルートユーザー

を作成する場合 AWS アカウントでは、すべての への完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。 AWS のサービス アカウントの および リソース。この ID は と呼ばれます。 AWS アカウント root ユーザー と には、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「 IAMユーザーガイド」の「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して にアクセスすることを要求します。 AWS のサービス 一時的な認証情報を使用する。

フェデレーティッド ID は、エンタープライズユーザーディレクトリのユーザー、ウェブ ID プロバイダー、 AWS Directory Service、Identity Center ディレクトリ、または にアクセスする任意のユーザー AWS のサービス ID ソースを通じて提供される認証情報を使用する。フェデレーティッド ID アクセスの場合 AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

一元的なアクセス管理を行うには、 を使用することをお勧めします。 AWS IAM Identity Center。 Identity Center でユーザーとグループを作成するか、独自の IAM ID ソース内のユーザーとグループのセットに接続して同期し、すべての で使用できます。 AWS アカウント および アプリケーション。IAM Identity Center の詳細については、「」のIAM「Identity Center とは」を参照してください。 AWS IAM Identity Center ユーザーガイド 。

IAM ユーザーとグループ

IAM ユーザーは 内のアイデンティティです。 AWS アカウント 1 人のユーザーまたはアプリケーションに対して特定のアクセス許可を持つ 。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧

めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「 ユーザーガイド」の「長期的な認証情報を必要とするユースケースでアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、 という名前のグループIAMAdminsを作成し、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールではなく) ユーザーを作成する場合IAM」を参照してください。

IAM ロール

IAM ロールは 内のアイデンティティです。 AWS アカウント 特定のアクセス許可を持つ 。これは IAM ユーザーと似ていますが、特定のユーザーに関連付けられていません。で一時的に IAMロールを引き受けることができます。 AWS Management Console ロールを切り替えます。を呼び出すことでロールを引き受けることができます。 AWS CLI または AWS API オペレーション、またはカスタム の使用URL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「」の「アクセス許可セット」を参照してください。 AWS IAM Identity Center ユーザーガイド 。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。

- クロスアカウントアクセス – IAMロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、 AWS のサービスでは、ポリシーをリソースに直接アタッチできます (ロールをプロキシとして使用する代わりに) 。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。
- クロスサービスアクセス – 一部 AWS のサービス 他の の機能を使用する AWS のサービス。 例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を使用します。 AWS のサービス、 リクエストとの組み合わせ AWS のサービス ダウンストリームサービスにリクエストを行う 。FAS リクエストは、サービスが他の とのやり取りを必要とするリクエストを受け取った場合にのみ行われます。 AWS のサービス または完了するリソース。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 にアクセス許可を委任するロールの作成」を参照してください。 AWS のサービス「」(IAM ユーザーガイド) を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です。 AWS のサービス。 このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールが に表示されます。 AWS アカウント と は サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 を作成しているアプリケーションの一時的な認証情報を管理できます。 AWS CLI または AWS API リクエスト。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。を割り当てるには AWS EC2 インスタンスにロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行

されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、「 ユーザーガイド」の「 (ユーザーではなく) IAMロールを作成する場合IAM」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスをコントロールする AWS ポリシーを作成して にアタッチする AWS ID またはリソース。ポリシーは のオブジェクトです。 AWS アイデンティティまたはリソースに関連付けられている場合、そのアクセス許可を定義します。 AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは に保存されます。 AWS JSON ドキュメントとして。JSON ポリシードキュメントの構造と内容の詳細については、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 からロール情報を取得できます。 AWS Management Console、 AWS CLI、または AWS API.

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれてい

ます。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです。 AWS アカウント。 管理ポリシーには以下が含まれます。 AWS 管理ポリシーとカスタマー管理ポリシー。管理ポリシーとインラインポリシーのどちらかを選択する方法については、IAM ユーザーガイドの「管理ポリシーとインラインポリシーの選択」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービス.

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。は使用できません AWS リソースベースのポリシーIAMの からの マネージドポリシー。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、 AWS WAF、、および Amazon VPCは、 をサポートする のサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境

界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」の「 IAMエンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) — SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定するJSONポリシーです。 AWS Organizations. AWS Organizations は、複数の をグループ化して一元管理するためのサービスです。 AWS アカウント お客様のビジネスが所有する 。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します。 AWS アカウントのルートユーザー。 Organizations と の詳細についてはSCPs、「」の「サービスコントロールポリシー」を参照してください。 AWS Organizations ユーザーガイド。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「 ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。方法を学ぶには AWS は、複数のポリシータイプが関与する場合にリクエストを許可するかどうかを決定します。「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

Amazon One Enterprise と の連携方法 IAM

IAM を使用して Amazon One Enterprise へのアクセスを管理する前に、Amazon One Enterprise で使用できるIAM機能を確認してください。

IAM Amazon One Enterprise で使用できる の機能

IAM 機能	Amazon One Enterprise のサポート
アイデンティティベースのポリシー	あり

IAM 機能	Amazon One Enterprise のサポート
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	あり
ACLs	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	なし

Amazon One Enterprise とその他の の概要を把握するには AWS サービスはほとんどのIAM機能で動作します。「」を参照してください。 AWS ユーザーガイドIAMの「 と連携する IAM のサービス」。

Amazon One Enterprise のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」を参照してください。

Amazon One Enterprise のアイデンティティベースのポリシーの例

Amazon One Enterprise アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

Amazon One Enterprise 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロール信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービス.

クロスアカウントアクセスを有効にするには、リソースベースのポリシーのプリンシパルとして、アカウント全体または別のアカウントのIAMエンティティを指定できます。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントのIAM管理者は、リソースにアクセスするためのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

Amazon One Enterprise のポリシーアクション

ポリシーアクションのサポート: あり

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action`要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションは通常、関連付けられている と同じ名前です。 AWS API

オペレーション。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Amazon One Enterprise アクションのリストを確認するには、「」を参照してくださいAmazon One Enterprise のアクション、リソース、および条件キー。

Amazon One Enterprise のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
one
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

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

Amazon One Enterprise アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

Amazon One Enterprise のポリシーリソース

ポリシーリソースのサポート: あり

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

Amazon One Enterprise リソースタイプとその のリスト、ARNsおよび各リソースARNの を指定するために使用できるアクションについては、「」を参照してくださいAmazon One Enterprise のアクション、リソース、および条件キー。

Amazon One Enterprise アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

Amazon One Enterprise のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

ステートメントで複数のCondition要素を指定するか、単一のCondition要素で複数のキーを指定する場合は、 AWS は論理ANDオペレーションを使用してそれらを評価します。1 つの条件キーに複数の値を指定する場合は、 AWS は論理ORオペレーションを使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、リソースにIAMユーザー名でタグ付けされている場合にのみ、リソースへのアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべてを表示するには AWS グローバル条件キー、「」を参照してください。 AWSIAM ユーザーガイドの グローバル条件コンテキストキー。

Amazon One Enterprise の条件キーのリストと、条件キーを使用できるアクションとリソースについては、「」を参照してくださいAmazon One Enterprise のアクション、リソース、および条件キー。

Amazon One Enterprise アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

ACLs Amazon One Enterprise の

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

ABAC Amazon One Enterprise を使用する

サポート ABAC (ポリシー内のタグ): はい

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。In AWSでは、これらの属性はタグ と呼ばれます。IAM エンティティ (ユーザーまたはロール) と多くの にタグをアタッチできます。 AWS リソースの使用料金を見積もることができます。エンティティとリソースのタグ付けは、 の最初のステップですABAC。次に、プリンシパルのタグが、アクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細についてはABAC、「 IAMユーザーガイド」の「 とはABAC」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」を参照してください。

Amazon One Enterprise での一時的な認証情報の使用

一時的な認証情報のサポート: あり

ある程度 AWS のサービス 一時的な認証情報を使用してサインインすると、 は機能しません。以下を含む追加情報 AWS のサービス 一時的な認証情報の使用については、「」を参照してください。AWS のサービス ユーザーガイドの IAMで動作する IAM 。

にサインインする場合、一時的な認証情報を使用している AWS Management Console ユーザー名とパスワード以外の方法を使用する。例えば、 にアクセスする場合 AWS 会社のシングルサインオン (SSO) リンクを使用すると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

を使用して、一時的な認証情報を手動で作成できます。 AWS CLI または AWS API。その後、これらの一時的な認証情報を使用して にアクセスできます。 AWS. AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

Amazon One Enterprise のクロスサービスプリンシパル許可

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を使用します。 AWS のサービス、 リクエストとの組み合わせ AWS のサービス ダウンストリームサービスにリクエストを行う 。FAS リクエストは、サービスが他の とのやり取りを必要とするリクエストを受け取った場合にのみ行われます。 AWS のサービス または完了するリソース。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Amazon One Enterprise のサービスロール

サービスロールのサポート: なし

サービスロールは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 にアクセス許可を委任するロールの作成」を参照してください。 AWS のサービス「」(IAM ユーザーガイド) を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、Amazon One Enterprise の機能が破損する可能性があります。Amazon One Enterprise が指示する場合以外は、サービスロールを編集しないでください。

Amazon One Enterprise のサービスにリンクされたロール

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です。 AWS のサービス。 このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールが に表示されます。 AWS アカウント と は サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「」を参照してください。AWS と連携する のサービスIAM。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

Amazon One Enterprise のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには Amazon One Enterprise リソースを作成または変更するアクセス許可はありません。また、 を使用してタスクを実行することはできません。 AWS Management Console, AWS Command Line Interface (AWS CLI) 、または AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

各リソースタイプの の形式など、Amazon One Enterprise で定義されるアクションとリソースタイプの詳細については、Amazon One Enterprise のアクション、リソース、および条件キー「サービス認証リファレンスARNs」の「」を参照してください。

トピック

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Amazon One Enterprise リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションでは、 のコストが発生する可能性があります。 AWS アカウント。 アイデンティティベースのポリシーを作成または編集するときは、以下のガイドラインと推奨事項に従ってください。

- の使用を開始する AWS 管理ポリシーと最小特権のアクセス許可への移行 – ユーザーとワークロードへのアクセス許可の付与を開始するには、 を使用します。 AWS 多くの一般的なユースケースにアクセス許可を付与する マネージドポリシー。これらは で利用できます。 AWS アカウント。を定義してアクセス許可をさらに減らすことをお勧めします。 AWS ユースケースに固有の カスタマー管理ポリシー。詳細については、「」を参照してくださいAWS マネージドポリシーまたはAWS ユーザーガイドの ジョブ機能の IAM マネージドポリシー。
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを を使用して送信する必要があることを指定できますSSL。特定の を通じてサービスアクションが使用されている場合、条件を使用してサービスアクションへのアクセスを許可することもできます。 AWS のサービスまたは AWS CloudFormation。 詳細については、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」を参照してください。
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能

的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。

- 多要素認証を要求する (MFA) — でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合 AWS アカウントのセキュリティを強化するMFAには、 をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細については、「 IAMユーザーガイド」のMFA「 で保護されたAPIアクセスの設定」を参照してください。

のベストプラクティスの詳細についてはIAM、「 ユーザーガイド」の「 のセキュリティのベストプラクティスIAMIAM」を参照してください。

Amazon One Enterprise コンソールの使用

Amazon One Enterprise コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の Amazon One Enterprise リソースの詳細を一覧表示および表示できます。 AWS アカウント。 最小限必要なアクセス許可よりも制限されたアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。AWS CLI または AWS API。代わりに、実行しようとしているAPIオペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーとロールが引き続き Amazon One Enterprise コンソールを使用できるようにするには、Amazon One Enterprise *ConsoleAccess*または *ReadOnly* AWS エンティティへの マネージドポリシー。詳細については、「 ユーザーガイド」の「ユーザーへのアクセス許可の追加IAM」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。 AWS CLI または AWS API.

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

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

Amazon One Enterprise への読み取り専用アクセス

次の例は、 AWS Amazon One Enterprise への読み取り専用アクセスAmazonOneEnterpriseReadOnlyAccessを許可する マネージドポリシー。

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

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

このポリシーステートメントの Effect 要素で、アクションが許可されるか拒否されるかを指定します。Action 要素には、ユーザーによる実行を許可する特定のアクションを指定します。Resource 要素には、 AWS ユーザーがこれらのアクションを実行できる リソース。Amazon One Enterprise アクションへのアクセスを制御するポリシーの場合、 Resource要素は常に「すべてのリソース」を意味するワイルドカード *に設定されます。

Action 要素の値は、サービスがサポートAPIsする に対応します。アクションの前に が付きconfig:、Amazon One Enterprise アクションを参照していることを示します。次の例に示すように、* ワイルドカード文字を Action 要素で使用できます。

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

  これにより、DeviceInstance「」 (GetDeviceInstanceConfiguration、) で終わるすべての Amazon One Enterprise アクションが許可されますCreateDeviceInstanceConfiguration。

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

  これにより、すべての Amazon One Enterprise アクションが許可されますが、他の のアクションは許可されません。 AWS サービス。

- "Action": ["*"]

  これにより、すべての AWS アクション。このアクセス許可は、 として機能するユーザーに適しています。 AWS アカウントの 管理者。

読み取り専用ポリシーは、、CreateDeviceInstance、 UpdateDeviceInstanceなどのアクションに対するアクセス許可をユーザーに付与しませんDeleteDeviceInstance。このポリシーを持つユーザーは、デバイスインスタンスの作成、デバイスインスタンスの更新、デバイスインスタンスの削除を行うことはできません。Amazon One Enterprise アクションのリストについては、「」を参照してくださいAmazon One Enterprise のアクション、リソース、および条件キー。

Amazon One Enterprise へのフルアクセス

次の例は、Amazon One Enterprise へのフルアクセスを許可するポリシーを示しています。これにより、すべての Amazon One Enterprise アクションを実行するアクセス許可がユーザーに付与されます。

> **Important**
>
> このポリシーによって、広範なアクセスが許可されます。フルアクセスを付与する前にまず最小限のアクセス許可から開始し、必要に応じて追加のアクセス許可を付与することを検討してください。この方法は、寛容なアクセス許可から開始して、後でそれを厳しくするよりも安全です。

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

Amazon One Enterprise ルールAPIアクションでサポートされるリソースレベルのアクセス許可

リソースレベルのアクセス許可とは、ユーザーがアクションを実行できるリソースを指定できる機能を意味します。Amazon One Enterprise は、特定の Amazon One Enterprise ルールAPIアクションのリソースレベルのアクセス許可をサポートします。つまり、特定の Amazon One Enterprise ルールアクションでは、ユーザーがそれらのアクションを使用できる条件を制御できます。これらの条件には、アクションの要件や、ユーザーが使用できる特定のリソースなどがあります。

次の表に、現在リソースレベルのアクセス許可をサポートしている Amazon One Enterprise ルールAPIアクションを示します。また、各アクションARNsでサポートされているリソースと についても説明します。を指定する場合ARN、パスに * ワイルドカードを使用できます。例えば、正確なリソース を指定できない、または指定しない場合は、 ですIDs。

> **Important**
>
> Amazon One Enterprise ルールAPIアクションがこの表に表示されていない場合、リソースレベルのアクセス許可はサポートされていません。Amazon One Enterprise ルールアクションがリソースレベルのアクセス許可をサポートしていない場合は、アクションを使用するアクセス許可をユーザーに付与できますが、ポリシーステートメントのリソース要素に * を指定する必要があります。

API アクション	リソース
CreateDeviceInstance	デバイスインスタンス arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
GetDeviceInstance	デバイスインスタンス arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
UpdateDeviceInstance	デバイスインスタンス arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
DeleteDeviceInstance	デバイスインスタンス arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
CreateDeviceActivationQrCode	デバイスインスタンス arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
DeleteAssociatedDevice	デバイスインスタンス

API アクション	リソース
	arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
RebootDevice	デバイスインスタンス arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId*
CreateDeviceInstanceConfiguration	デバイスインスタンスの設定 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId* /configuration/*version*
GetDeviceInstanceConfiguration	デバイスインスタンスの設定 arn:aws:one:*region:accountID* :device-instance/*deviceInstanceId* /configuration/*version*
CreateSite	サイト arn:aws:one:*region:accountID* :site/*siteId*
DeleteSite	サイト arn:aws:one:*region:accountID* :site/*siteId*
GetSiteAddress	サイト arn:aws:one:*region:accountID* :site/*siteId*
UpdateSite	サイト arn:aws:one:*region:accountID* :site/*siteId*
UpdateSiteAddress	サイト arn:aws:one:*region:accountID* :site/*siteId*

API アクション	リソース
CreateDeviceConfigurationTemplate	デバイス設定テンプレート arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
DeleteDeviceConfigurationTemplate	デバイス設定テンプレート arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
GetDeviceConfigurationTemplate	デバイス設定テンプレート arn:aws:one:*region:accountID* :device-configuration-template/*templateId*
UpdateDeviceConfigurationTemplate	デバイス設定テンプレート arn:aws:one:*region:accountID* :device-configuration-template/*templateId*

例えば、特定のルールで特定のユーザーに読み取りアクセスを許可して、書き込みアクセスを拒否するとします。

最初のポリシーでは、 AWS Config ルールは、指定されたルールGetSiteに対する などのアクションを読み込みます。

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

```
            }
        ]
    }
```

2 番目のポリシーでは、特定のルールに対する Amazon One Enterprise ルールの書き込みアクションを拒否します。

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

リソースレベルのアクセス許可を使用すると、読み取りアクセスを許可し、書き込みアクセスを拒否して、Amazon One Enterprise ルールアクションに対して特定のAPIアクションを実行できます。

追加情報

IAM ユーザー、グループ、ポリシー、アクセス許可の作成の詳細については、 IAMユーザーガイドの「最初のIAMユーザーと管理者のグループの作成」および「アクセス管理」を参照してください。

AWS Amazon One Enterprise の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 AWS のサービス は、新しい AWS が起動されたとき、または既存のサービスで新しいAPIオペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「 ユーザーガイド」の「 AWS 管理ポリシーIAM」を参照してください。

AmazonOneEnterpriseFullAccess

このポリシーは、すべての Amazon One Enterprise リソースとオペレーションへのアクセスを許可する管理アクセス許可を付与します。

one:* すべての Amazon One Enterprise アクションを実行できます。

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

AmazonOneEnterpriseReadOnlyAccess

このポリシーは、すべての Amazon One Enterprise リソースとオペレーションに読み取り専用アクセス許可を付与します。

one:Get* Amazon One Enterprise リソースを取得します。

one:List* Amazon One Enterprise リソースを一覧表示します。

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

AmazonOneEnterpriseInstallerAccess

このポリシーは、設定されたデバイスインスタンスのアクティベーション QR コードを作成して、任意のサイトでデバイスをアクティブ化できる、制限付きの読み取りおよび書き込みアクセス許可を付与します。

one:CreateDeviceActivationQrCode QR コードを作成してデバイスをアクティブ化できます。

one:GetDeviceInstance Amazon One デバイスインスタンスに関する情報を取得できます。

one:GetSite Amazon One Enterprise サイトに関する情報を取得できます。

one:GetSiteAddress Amazon One Enterprise サイトの住所を取得できます。

one:ListDeviceInstances Amazon One デバイスインスタンスを一覧表示できます。

one:ListSites Amazon One Enterprise サイトを一覧表示できます。

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

```
    "Effect": "Allow",
    "Action": [
     "one:CreateDeviceActivationQrCode",
     "one:GetDeviceInstance",
     "one:GetSite",
     "one:GetSiteAddress",
     "one:ListDeviceInstances",
     "one:ListSites"
    ],
    "Resource": "*"
   }
  ]
}
```

AWS マネージドポリシーに対する Amazon One Enterprise の更新

Amazon One Enterprise の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始してから行われた分について表示します。このページの変更に関する自動通知については、Amazon One Enterprise Document の履歴ページのRSSフィードをサブスクライブしてください。

変更	説明	日付
Amazon One Enterprise が変更の追跡を開始しました	Amazon One Enterprise が AWS マネージドポリシーの変更の追跡を開始しました。	2023 年 12 月 1 日

Amazon One Enterprise のアイデンティティとアクセスのトラブルシューティング

以下の情報は、Amazon One Enterprise および の使用時に発生する可能性がある一般的な問題の診断と修復に役立ちますIAM。

トピック

- Amazon One Enterprise でアクションを実行する権限がない
- 自分の 以外のユーザーに許可したい AWS アカウント Amazon One Enterprise リソースにアクセスする

Amazon One Enterprise でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のone:*GetWidget*アクセス許可がない場合に発生します。

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

この場合、one:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 にお問い合わせください。 AWS 管理者。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに許可したい AWS アカウント Amazon One Enterprise リソースにアクセスする

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- Amazon One Enterprise がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAmazon One Enterprise と の連携方法 IAM。
- 全体で リソースへのアクセスを提供する方法を学ぶには AWS アカウント 所有している 。「別のIAMユーザーへのアクセスを提供する」を参照してください。 AWS アカウント ユーザーガイドで所有している IAM 。
- リソースへのアクセスをサードパーティーに提供する方法を学ぶには AWS アカウント、「 へのアクセスの提供」を参照してください。 AWS アカウント ユーザーガイドの「第三者が所有していますIAM」。
- ID フェデレーションを通じてアクセスを提供する方法については、 IAMユーザーガイドの「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション)」を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

Amazon One Enterprise のアクション、リソース、および条件キー

Amazon One Enterprise (サービスプレフィックス: one) では、 アクセスIAM許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

トピック

- Amazon One Enterprise で定義されるアクション
- Amazon One Enterprise で定義されるリソースタイプ
- Amazon One Enterprise の条件キー

Amazon One Enterprise で定義されるアクション

IAM ポリシーステートメントの Action要素で次のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合、通常、同じ名前のAPIオペレーションまたはCLIコマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれている場合は、ARNそのアクションを含むステートメントでそのタイプの を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource要素を使用してリソースアクセスを制限する場合は、必要なリソースタイプごとに ARNまたは パターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDeviceInstance	デバイスインスタンスを作成するアクセス許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	デバイスインスタンスに関する情報を取得する許可を付与	読み取り	デバイスインスタンス*		
ListDeviceInstances	デバイスインスタンスを一覧表示するアクセス許可を付与する	読み取り			
UpdateDeviceInstance	デバイスインスタンスを更新するアクセス許可を付与する	書き込み	デバイスインスタンス*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDeviceInstance	デバイスインスタンスを削除するアクセス許可を付与する	書き込み	デバイスインスタンス*		
CreateDeviceActivationQrCode	デバイスインスタンスでデバイスをアクティブ化するための QR コードを作成するアクセス許可を付与します	書き込み	デバイスインスタンス*		
DeleteAssociatedDevice	デバイスとデバイスインスタンス間の関連付けを削除する許可を付与	書き込み	デバイスインスタンス*		
RebootDevice	デバイスを再起動するアクセス許可を付与する	書き込み	デバイスインスタンス*		
CreateDeviceInstanceConfiguration	デバイスインスタンス設定を作成するアクセス許可を付与する	書き込み			
GetDeviceInstanceConfiguration	デバイスインスタンス設定に関する情報を取得する許可を付与	読み取り	設定*		
CreateSite	サイトを作成するアクセス許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	デバイスインスタンスを削除するアクセス許可を付与する	書き込み	サイト*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSite	サイトに関する情報を取得する許可を付与	読み取り	サイト*		
ListSites	サイトを一覧表示するアクセス許可を付与する	読み取り			
GetSiteAddress	サイトアドレスに関する情報を取得する許可を付与	読み取り	サイト*		
UpdateSite	サイトを更新するアクセス許可を付与する	書き込み	サイト*		
UpdateSiteAddress	サイトアドレスを更新する許可を付与	書き込み	サイト*		
CreateDeviceConfigurationTemplate	デバイスインスタンスを作成するアクセス許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	デバイス設定テンプレートを削除する許可を付与	書き込み	device-configuration-template*		
GetDeviceConfigurationTemplate	デバイス設定テンプレートに関する情報を取得する許可を付与	読み取り	device-configuration-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDeviceConfigurationTemplates	デバイス設定テンプレートを一覧表示する許可を付与	読み取り			
UpdateDeviceConfigurationTemplate	デバイス設定テンプレートを更新する許可を付与	書き込み	device-configuration-template*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	デバイスインスタンス、サイト、device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	デバイスインスタンス、サイト、device-configuration-template	aws:TagKeys	
ListTagForResources	リソースのタグを一覧表示する許可を付与	読み取り			

Amazon One Enterprise で定義されるリソースタイプ

次のリソースタイプは、このサービスによって定義され、IAMアクセス許可ポリシーステートメントの Resource要素で使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Device Instance	arn:aws:one: *region:accountID* :device-instance/ *deviceInstanceId*	aws:ResourceTag/${TagKey}
Device Instance Configuration	arn:aws:one: *region:accountID* :device-instance/ *deviceInstanceId* /configuration/ *version*	
Site	arn:aws:one: *region:accountID* :site/*siteId*	aws:ResourceTag/${TagKey}
Device Configuration Template	arn:aws:one: *region:accountID* :device-configuration-template/ *templateId*	aws:ResourceTag/${TagKey}

Amazon One Enterprise の条件キー

Amazon One Enterprise では、 IAMポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを確認するには、「使用できるグローバル条件キー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストからのタグに基づいてアクセスをフィルタリング	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストからのタグキーに基づいてアクセスをフィルタリング	ArrayOfString

Amazon One Enterprise のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスHIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべての AWS のサービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST) 、Payment Card Industry Security Standards Council ()、PCI国際標準化機構 (ISO) など) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことでDSS、 PCI などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon One Enterprise のログ記録とモニタリング

モニタリングは、Amazon One Enterprise およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS は、Amazon One Enterprise をモニタリングし、問題が発生した場合は報告し、必要に応じて自動アクションを実行するための以下のモニタリングツールを提供します。

- Amazon EventBridge を使用すると、 AWS サービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。 AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、「Amazon ユーザーガイド EventBridge 」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われたAPI呼び出しおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しが発生した日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

Amazon での Amazon One Enterprise イベントのモニタリング EventBridge

で Amazon One Enterprise イベントをモニタリングできます。これにより EventBridge、独自のアプリケーション、 software-as-a-service (SaaS) アプリケーション、および AWS サービスからリアルタイムのデータのストリームが配信されます。 EventBridge は、そのデータを AWS Lambda や Amazon Simple Notification Service などのターゲットにルーティングします。これらのイベントは、 AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。

Amazon One Enterprise イベントをサブスクライブする

Amazon One デバイスおよびユーザープロファイルのステータス変更イベントは、 を使用して発行され EventBridge、新しいルールを作成することで EventBridge コンソールで有効にできます。イベントは順序付けされていませんが、データの使用に役立つタイムスタンプがあります。イベントは、ベストエフォートベースで出力されます。

Amazon One Enterprise イベントをサブスクライブするには

1. で EventBridge コンソールを開きますhttps://console.aws.amazon.com/events/。
2. ナビゲーションペインのバス で、ルール を選択します。
3. [Create rule (ルールの作成)] を選択します。
4. [Default rule detail] (デフォルトルール詳細) ページで、ルールに名前を割り当て、[Rule with an event pattern] (イベントパターンを持つルール) を選択し、[Next] (次へ) を選択します。
5. ビルドイベントパターンページのイベントソース で、AWS イベントまたは EventBridge パートナーイベントが選択されていることを確認します。
6. サンプルイベントタイプ で、「自分の を入力」を選択します。
7. のいずれかからコピーして貼り付けますイベント例。
8. 作成方法 で、カスタムパターン を選択します。「イベントパターン」セクションJSONで、イベントソースを `aws:one`として、必要な詳細タイプを持つ を追加し、次へ を選択します。
9. ターゲットの選択ページで、Lambda 関数、SQSキュー、またはSNSトピックを含む任意のターゲットを選択します。ターゲットの設定の詳細については、「Amazon EventBridge ターゲット」を参照してください。
10. 必要に応じて、タグを設定できます。
11. [Review and create] (確認して作成) ページで、[Create rule] (ルールの作成) を選択します。ルールの設定の詳細については、「 ユーザーガイド」の「 EventBridgeルール EventBridge 」を参照してください。

デバイスステータス変更イベントタイプ

デバイスステータス変更イベントは で生成されますJSON。イベントタイプごとに、ルールで設定されているように、選択したターゲットに JSON BLOB が送信されます。次の詳細タイプを使用できます。

デバイスのヘルスステータスが正常に変更されました

デバイスはすべてのヘルスチェックに合格しました。

デバイスヘルスステータスが「Critical」に変更されました

デバイスが 1 つ以上のヘルスチェックに失敗しました。

デバイス接続がオフラインに変更されました

デバイスがインターネットに接続されていません。

デバイス接続がオンラインに変更されました

デバイスがインターネットに接続されている。

resources

Device Status Change イベントが発行された deviceInstance arn のリストが含まれます。

metadata

siteName

- deviceInstance が存在するサイトの名前。

siteArn

- deviceInstance が存在するサイトの Arn。

データ

currentConnectivity

- deviceInstance がインターネットに接続されているか切断されているかを表します。
- 指定できる値: CONNECTED、 DISCONNECTED

previousConnectivity

- イベントの前に がインターネットに接続されていたか、インターネットから切断 deviceInstance されていたかを表します。
- 指定できる値: CONNECTED、 DISCONNECTED

currentHealthStatus

- deviceInstance がすべてのヘルスチェックに合格したかどうかを表します。
- 指定できる値: HEALTHY、 CRITICAL

previousHealthStatus

- が最後にチェックしたときにすべてのヘルスチェックに deviceInstance 合格したかどうかを表します。
- 指定できる値: HEALTHY、 CRITICAL

assetTagId

- に関連付けられている assetTagId デバイスの deviceInstance。

deviceInstanceName

- Device Status Event が公開された deviceInstance の名前。

ユーザープロファイルイベントタイプ

ユーザープロファイル関連のイベントの詳細タイプは次のとおりです。

新しい正常な登録

ユーザーが正常に登録されたとき。

新しい正常な登録解除

ユーザーが正常に登録解除されたとき。

登録失敗

ユーザーが登録に失敗したとき。

登録解除失敗

ユーザーが登録解除に失敗したとき。

正常な認識

ユーザーが認証のために跳ね返りを正常にスキャンしたとき。

失敗した認識

蝶形スキャンの認識が失敗した場合。

resources

ユーザープロファイルイベントが公開されたユーザープロファイル arn のリストが含まれます。

データ

accountId

- リクエストを開始したデバイスの関連 AWS アカウント。

requestSource

- これは、リクエストを開始した deviceInstanceId デバイスの です。

createdTimestamp

- イベントの作成時刻。

userStatus

- ユーザーの現在のステータス。
- 指定できる値: ACTIVE、 DELETED

associatedId

- バッジ ID など、ユーザーの関連付けられた ID。

理由

- この値は、失敗したイベントに表示されます。これには、イベントが失敗した理由が含まれます。

イベント例

次の例は、Amazon One Enterprise のイベントを示しています。

トピック

- デバイスのヘルスステータスが正常に変更されました
- デバイスのヘルスステータスが重大に変更されました
- デバイス接続がオンラインに変更されました
- デバイス接続がオフラインに変更されました
- 新規登録成功

デバイスのヘルスステータスが正常に変更されました

デバイスはすべてのヘルスを渡し、デバイスインスタンスのヘルスステータスがCRITICALヘルスステータスHEALTHYから に変更されました。

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

デバイスのヘルスステータスが重大に変更されました

デバイスが 1 つ以上のヘルスチェックに失敗し、デバイスインスタンスのヘルスステータスが CRITICALから に変更されましたHEALTHY。

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

デバイス接続がオンラインに変更されました

デバイスがインターネットに接続され、デバイスインスタンスの接続ステータスが CONNECTEDから に変更されましたDISCONNECTED。

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

デバイス接続がオフラインに変更されました

デバイスがインターネットに接続されておらず、デバイスインスタンスの接続ステータスが DISCONNECTEDから に変更されましたCONNECTED。

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

新規登録成功

ユーザーが正常に登録されたときのイベント。

```
{
    "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\"}]",
        }
    }
}
```

を使用した Amazon One Enterprise APIコールのログ記録 AWS CloudTrail

Amazon One Enterprise は AWS CloudTrail、Amazon One Enterprise のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。 は、Amazon One Enterprise のすべてのAPI呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、Amazon One Enterprise コンソールからの呼び出しと、Amazon One Enterprise APIオペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Amazon One Enterprise の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。 Amazon S3 証跡を設定しない場合でも、CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。で収集された情報を使用して CloudTrail、Amazon One Enterprise に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

の Amazon One Enterprise 情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。Amazon One Enterprise でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。 で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴 で CloudTrail イベントを表示する」を参照してください。

Amazon One Enterprise のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- CloudTrail がサポートするサービスと統合
- の Amazon SNS通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての Amazon One Enterprise アクションは によってログに記録 CloudTrail され、 に文書化されますAmazon One Enterprise のアクション、リソース、および条件キー。例えば、、、DeleteDeviceInstanceアクションを呼び出すRebootDeviceとListSites、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが root または AWS Identity and Access Management （ IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity「」要素を参照してください。

Amazon One Enterprise ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリックAPIコールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 CreateSiteアクションを示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAKDBGOAT6C2EXAMPLE:J_DOE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_DOE",
        "accountId": "123456789012",
        "accessKeyId": "AKIALAVPULGA71EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAKDBGOAT6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
```

```
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-11T06:28:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-11T07:19:09Z",
    "eventSource": "one.amazonaws.com",
    "eventName": "CreateSite",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "name": "***",
        "description": "***",
        "address": {
            "addressLine1": "***",
            "addressLine2": "***",
            "addressLine3": "***",
            "city": "EXAMPLE_CITY",
            "postalCode": "12345",
            "countryCode": "EXAMPLE_COUNTRY",
            "stateOrRegion": "EXAMPLE_STATE"
        },
        "clientToken": "abc12d34-567e-8910-1112-12fghi0jk13l"
    },
    "responseElements": {
        "stateOrRegion": "EXAMPLE_STATE",
        "createdAtInMillis": 1697008749263,
        "city": "EXAMPLE_CITY",
        "countryCode": "EXAMPLE_COUNTRY",
        "deviceInstanceCount": 0,
        "postalCode": "12345",
        "name": "***",
        "description": "***",
        "siteId": " abCdefG12hijkL",
        "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkL",
        "tags": "***"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
```

```
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Amazon One Enterprise ユーザーガイドのドキュメント履歴

次の表に、Amazon One Enterprise のドキュメントリリースを示します。

変更	説明	日付
更新	新しいトピックの追加: Amazon One Enterprise ユーザーガイドへの安全なアクセスのための Amazon One Device I/O Hub のインストール	2024 年 8 月 14 日
更新	新しいトピックの追加: 壁面マウント可能な Amazon One デバイス Amazon One Enterprise ユーザーガイドのインストール	2024 年 6 月 5 日
初回リリース	Amazon One Enterprise ユーザーガイドの初回リリース	2023 年 11 月 27 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。