aws

ユーザーガイド

Amazon One

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

Amazon One: ユーザーガイド

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

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Amazon One Enterprise とは 1
Amazon One デバイス 1
Amazon One Enterprise コンソール 2
Amazon One デバイスの購入 3
Amazon One Enterprise の料金 3
Amazon One の仕組み 4
Amazon One ワークフロー 4
Amazon One の主要な用語 4
Amazon One コンソールのセットアップ 6
AWS アカウントのサインアップ 6
管理アクセスを持つユーザーを作成する 7
AWS アカウントの保護 7
管理アクセス権を持つユーザーの作成 7
管理者としてサインインする 8
追加ユーザーへのアクセスの割り当て 8
Amazon One ユーザーを追加する 9
サイトの作成 11
デバイスインスタンスを作成する 12
設定テンプレートを作成する 12
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 13
Amazon One のインストールとアクティブ化 16
要件について 16
サポートされている標準 16
ネットワーク要件 17
電力要件 17
インストールの概念を理解する 17
Amazon One Pedestal のインストール 18
ウォールマウント可能な Amazon One デバイスのインストール 20
安全なアクセスのための Amazon One Device I/O Hub のインストール 31
Amazon One デバイスのアクティブ化 42
ユーザーの登録と入力 44
エンドポイントポリシーの作成 44
エントリの認証 44
ユーザーの管理 45

登録済みユーザーの表示 45
登録済みユーザーとその生体認証の削除 45
Amazon One デバイスの管理 47
Amazon One デバイスのメンテナンスとクリーニング 47
Amazon One デバイスをクリーンアップするには 48
サイト管理 48
サイト名の変更 49
サイトアドレスの更新 49
デバイスインスタンス管理 50
デバイスインスタンスのステータスの表示 50
Amazon One デバイスの再起動 50
Amazon One デバイス設定の更新 51
Wi-Fi 認証情報の更新 51
デバイスインスタンスの非アクティブ化 52
セキュリティ 53
データ保護 53
保管中のデータのデフォルトの暗号化を使用するには 54
転送中のデータの暗号化 55
Identity and Access Management 55
対象者 55
アイデンティティを使用した認証 56
ポリシーを使用したアクセスの管理 60
Amazon One Enterprise と IAM の連携方法 62
アイデンティティベースのポリシーの例 69
AWS マネージドポリシー 78
アクション、リソース、および条件キー 82
アクション 82
リソースタイプ 86
条件キー 87
コンプライアンス検証 88
モニタリング 90
イベントのモニタリング 90
Amazon One Enterprise イベントをサブスクライブする 90
デバイスステータス変更イベントタイプ 92
ユーザープロファイルイベントタイプ 93
イベント例 95

デバイスのヘルスステータスが正常に変更されました 95
デバイスのヘルスステータスがクリティカルに変更されました 96
デバイス接続がオンラインに変更されました 96
デバイス接続がオフラインに変更されました 97
CloudTrail ログ 98
CloudTrail の Amazon One Enterprise 情報 98
Amazon One Enterprise ログファイルエントリについて 99
トラブルシューティング 102
ID とアクセスのトラブルシューティング 102
Amazon One でアクションを実行する権限がありません 102
自分の 以外のユーザーに Amazon One リソース AWS アカウント へのアクセスを許可したい 103
Amazon One コンソールのトラブルシューティング 103
サイトを作成できない 104
デバイスインスタンスを作成できません 104
設定テンプレートを作成できません 104
アクティベーション QR コードを作成できない 104
Amazon One デバイスのトラブルシューティング 104
空白画面 105
Wi-Fi またはネットワークに接続できない 106
アクティブなアラートでデバイスを再起動する 106
システムエラー 106
QR コードが認識されない 107
QR コードを読み取れない 107
複数の QR コードが検出されました 107
デバイスインスタンスが存在しません 107
サイトが見つかりません 108
郵便番号が一致しません 108
ゲートウェイがタイムアウトしました 108
デバイスを設定できない 108
デバイスがエラーメッセージとエラーコードで再起動しました 109
デバイス画面上の Amazon ロゴ。それ以上のアクティビティはありません。 109
一時的に使用不可 109
問題が発生しました 109
一時的なサービス停止 110
Amazon One デバイスに物理的な損傷がある 110

アダルトを読み取れない 110
手掌が認識されない 110
非アクティブが長引いたためデバイスがロックされました 111
改ざんイベントによりデバイスがロックされました 111
ドキュメント履歴 113
..... cxv

Amazon One Enterprise とは

Amazon One Enterprise は、バッジ、PINs、パスコードを使用せずに、建物やエンタープライズアセットへの安全なアクセスを従業員に許可する、新しい冪定ベースの認証サービスです。

トピック

- Amazon One デバイス
- Amazon One Enterprise コンソール
- Amazon One デバイスの購入
- Amazon One Enterprise の料金

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、冪等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 — 手津生体認証、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 と Wiegand
- 電源 — POE、AC から DC への 110/220 VAC 入力、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 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。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なものです。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。
  - 物理的な場所にすべての Amazon One デバイスインスタンスを含むサイトの作成
  - 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。管理者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 の仕組み

Amazon One はクラウドベースの生体認証サービスで、Amazon One デバイスを使用して、ユーザーの生体認証をアタッチします。Amazon One デバイスを注文するには、お問い合わせください。

Amazon One デバイスをインストールしたら、Amazon One コンソールと認証アプリケーションでデバイスをアクティブ化して AWS アカウントに登録できます。登録されたユーザーの生体認証プロファイルを表示できます。必要に応じて、登録をキャンセルし、生体認証データを削除できます。

Amazon One Console は、デバイスの追跡や月別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ハブとして機能します。ユーザーは、オンサイトの教師あり登録ステーションで手掌をスキャンして登録できます。登録すると、ユーザーは Amazon One 対応デバイスの上にアタッチすることで、安全な場所にシームレスに出入りできます。

トピック

- Amazon One ワークフロー
- Amazon One の主要な用語

Amazon One ワークフロー

Amazon One の基本的なワークフローを以下に示します。

1. Amazon One デバイスを購入してインストールするには、お問い合わせください。
2. デバイスをインストールしたら、Amazon One をアクティブ化します。
3. Amazon One アカウントにサインインします。
4. ユーザー登録デバイスとエントリデバイスを設定します。
5. 従業員の手榴弾を登録します。
6. 管理およびモニタリング機能を使用して、デバイスの正常性を確保し、設定を最新の状態に保ち、包括的な監視のためにユーザー登録を追跡します。

Amazon One の主要な用語

Amazon One の主な用語は次のとおりです。

- サイト — 顧客が Amazon One デバイスをインストールするカスタマーマネージドの物理的な建物。サイトは、Amazon One デバイスの施設、ネットワーク、電源の要件を満たす必要があります。
- デバイス — 認証用の Amazon One のアクリ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設定の包括的なセット。

Amazon One コンソールのセットアップ

この章では、Amazon One コンソール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。

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、Amazon One Enterprise コンソールを使用して設定および管理します。このプロセスは、サイト数、デバイスインスタンス、設定テンプレートに応じて、たまに、または 1 回だけ使用します。

トピック

- AWS アカウントのサインアップ
- 管理アクセスを持つユーザーを作成する
- Amazon One ユーザーを追加する
- サイトの作成
- デバイスインスタンスを作成する
- 設定テンプレートを作成する
- 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

AWS アカウントのサインアップ

AWS アカウントをお持ちでない場合は、以下の手順に従ってアカウントを作成してください。

サインアップして AWS アカウントを作成するには

1. https://portal.aws.amazon.com/billing/signup 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。

   AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS サービスとリソースへのアクセス権があります。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を必要とするタスクを実行する

AWS のサインアップ処理が完了すると、ユーザーに確認メールが送信されます。にアクセスして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https://aws.amazon.com/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

AWS アカウントにサインアップしたら、AWS アカウントのルートユーザーを保護し、AWS IAM Identity Center を有効にして、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。

トピック

- AWS アカウントの保護
- 管理アクセス権を持つユーザーの作成
- 管理者としてサインインする
- 追加ユーザーへのアクセスの割り当て

AWS アカウントの保護

Amazon One アカウントにサインインしたので、アカウントを保護します。

AWS アカウントのルートユーザーを保護するには

1. ルートユーザーを選択し、AWS アカウントの E メールアドレスを入力して、AWS マネジメントコンソールにアカウント所有者としてサインインします。
2. 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、AWS サインインユーザーガイドの「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。
3. 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、「IAM ユーザーガイド」の「AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセス権を持つユーザーの作成

Amazon One アカウントをセキュリティで保護したら、管理者アクセス権を持つユーザーを作成します。

管理アクセスを持つユーザーを作成するには

1. IAM アイデンティティセンターを有効にします。

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

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   IAM Identity Center ディレクトリを ID ソースとして使用する方法のチュートリアルについては、AWS IAM Identity Center ユーザーガイドの「デフォルトの IAM Identity Center ディレクトリ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。

管理者としてサインインする

管理者アクセス権を持つユーザーを作成したので、管理者としてサインインします。

管理者アクセス権を持つユーザーとしてサインインするには

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

  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、「AWS サインイン ユーザーガイド」の「AWS アクセスポータルにサインインする」を参照してください。

追加ユーザーへのアクセスの割り当て

管理者としてサインインしたので、追加のユーザーにアクセスを割り当てることができます。

追加のユーザーにアクセスを割り当てるには

- 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、AWS IAM Identity Center ユーザーガイドの「グループの追加」を参照してください。

Amazon One 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 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 コードを取得する場合のみです。

Amazon One ユーザーを追加するには

1. 「 AWS サインイン ユーザーガイド」の「 にサインインする方法」の説明に従って AWS 、ユーザータイプに適したサインイン手順に従います。
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、 AWSのサインイン名です。

   > **Note**
   >
   > 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 と AWS STS のクォータ」を参照してください。ユーザー名は、最大 64 文字の英字、数字、およびプラス記号 (+)、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 (-) の組み合わせにすることができます。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 というユーザーと testuser というユーザーを作成することはできません。ユーザー名をポリシーまたは ARN の一部として使用する場合、名前の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。選択 へのユーザーアクセスを提供する – 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、アカウントの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、`IAMUserChangePassword` という名前の AWS マネージドポリシーが自動的に新しいユーザーにアタッチされます。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] を選択してください。
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] を選択してください。
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。IAM でのタグの使用の詳細については、「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。

    - ユーザー名
    - アカウントのサインインページへの URL。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。

サイトの作成

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

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

サイトを作成するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One 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. サイト情報で、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、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。

デバイスインスタンスを作成する

AWS マネジメントコンソールでサイトを作成したので、Amazon One コンソールを使用してデバイスインスタンスを作成できます。

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 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、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。

設定テンプレートを作成する

デバイスインスタンスを作成したら、Amazon One コンソールを使用して設定テンプレートを作成できます。

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 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、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、削除を選択します。
5. [設定] を選択します。

> **Important**
>
> 安全なアクセスのために Amazon One の全機能を有効にするには、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。

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 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、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、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、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のテーブルで、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対応する QR コードがあります。QR コードの取得 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**
>
> 安全なアクセスのために Amazon One の全機能を有効にするには、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 コンソールを正常にセットアップしたら、次のステップとして、Amazon One デバイスをサイトにインストールし、デバイスが適切にアクティブ化されていることを確認します。このプロセスには、デバイスを指定されたエリアに物理的に配置し、ネットワークに接続し、アクティベーションプロセスを完了してシームレスなユーザー識別とトランザクション機能を有効にすることが含まれます。アクティブ化すると、Amazon One デバイスは、顧客または従業員に安全でタッチレスなエクスペリエンスを提供する準備が整います。

> **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 AWS Management Console 、デバイスのアクティベーション QR コードを取得します。

トピック

- 要件について
- インストールの概念を理解する
- Amazon One Pedestal のインストール
- ウォールマウント可能な Amazon One デバイスのインストール
- 安全なアクセスのための Amazon One Device I/O Hub のインストール
- Amazon One デバイスのアクティブ化

要件について

Amazon One デバイスは、ドアが隠れて管理できる任意の企業またはビジネス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 で提供できます。必要な最小帯域幅は 10 Mbps です。

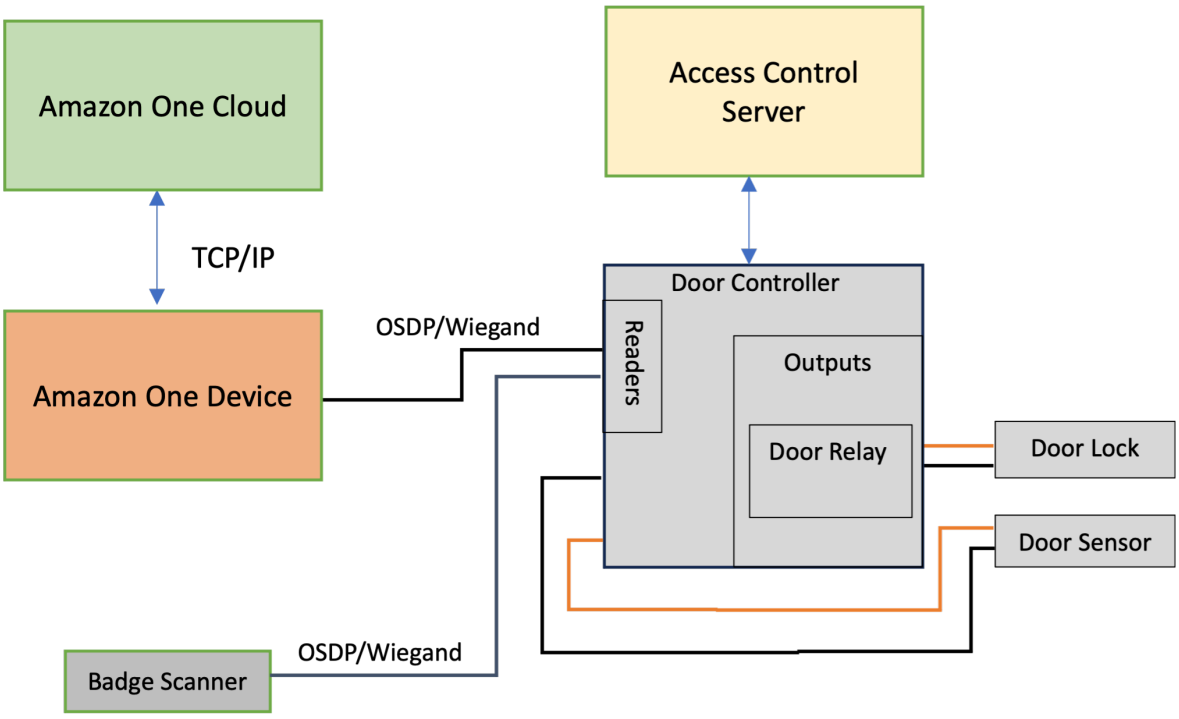
電力要件

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。

- 同梱されている 120V 電源アダプタを使用します。
- 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 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識別するために生体認証を実行する、改良認識デバイスです。
- 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、ユーザーの安全なエリアへのアクセス権限を制御します。エリアにアクセスできる個人のバッジ IDs は、このサーバーに保存されます。このサーバーは、関連する IDs を適切なドアコントローラーにキャッシュします。
- 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、COTS OSDP-to-Wiegandコンバーターを使用できます。
  - 認証に成功すると、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で応答し、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、バッジをスキャンしてバッジ番号をアクセスコントロールサーバーに送信するために使用されます。Amazon One では、バッジスキャナーが Amazon One デバイスに接続され、ユーザーはバッジをスキャンして、それらをプロフィールに関連付けます。

Amazon One Pedestal のインストール

Amazon One Pedestal は、Amazon One 識別およびトランザクションシステムの主要なコンポーネントであり、ユーザーにシームレスでタッチレスなエクスペリエンスを提供するように設計されています。このデバイスは、安全な生体認証を備えています。さまざまな場所に統合して、スムーズなアクセスまたは支払いソリューションを提供できます。

このセクションでは、Amazon One Pedestal をインストールするための場所の要件とstep-by-stepについて説明します。適切な準備とインストールは、システムが安全かつ効率的に動作し、ユーザーにスムーズで信頼性の高いエクスペリエンスを提供する上で重要です。

Amazon One Pedestal のインストールの前提条件と準備

インストールを開始する前に、安全で安全で効果的なセットアップのために、次の条件が満たされていることを確認してください。

- 電力要件: POE+ (Power over Ethernet) を使用してデバイスに電力を供給する場合は、Cat6 ケーブルがすでにインストールされており、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。または、AC 電源 (120V) を使用している場合は、アクセス可能な AC コンセントが台座から 20 フィート以内にあることを確認してください。
- 物理的なセットアップ: 安定した安全な台座を設置するには、床が水平で、クリーンで、ごみがない必要があります。

- 台座の場所: ドア、車線、アクセスポイントがブロックされない場所に台座を設置し、エリア内を簡単に移動できるようにします。
- ケーブル管理: 余分なケーブルをすべて台座内にルーティングして固定し、乱雑さを防ぎ、通常の使用中に潜在的な損傷を防ぎます。

これらの前提条件を確認したら、インストールプロセスを続行できます。

Amazon One Pedestal をインストールするには

1. パッケージから Amazon One Pedestal を削除します。
2. 両方の M4 改ざん防止ネジを取り外して、ドアを取り外します。
3. 電源ケーブルを接続します。
4. ケーブルを台座ベースプレートの穴に通します。
5. 余分な電源ケーブルを台座内に巻き付けます。
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に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. RS485 シリアルケーブルをアクセスコントロールパネル (またはバッジリーダー) から台座にフィードします。長さは 1 フィート超過します。
9. フェライトループを、台座のベースから 2 インチ上の RS485 ケーブルにインストールします。
10. コンセントに電源を接続し、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 不正開封防止ネジを再ネジで固定します。

Amazon One デバイスをインストールしたら、デバイスをアクティブ化する準備が整います。

ウォールマウント可能な Amazon One デバイスのインストール

ウォールマウント可能な Amazon One デバイスは、さまざまな環境のユーザーにシームレスでタッチレスなエクスペリエンスを提供するように設計された、汎用的でコンパクトな生体認証識別システムです。アドバンスト・アコグナイザー・レコグナイザー・テクノロジーを使用して安全なアクセスや支払いを実現し、小売スペースやオフィスの入口などの交通量の多い場所に理想的です。

このセクションでは、最適なパフォーマンスとセキュリティを確保するために、壁面マウント可能な Amazon One 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詳細な手順について説明します。

壁面マウント可能な Amazon One デバイスのインストールの前提条件と準備

インストールを開始する前に、デバイスが効果的に動作し、スペース内で適切に設定されていることを確認するために、次の条件が満たされていることを確認してください。

- 屋内使用のみ: 壁面マウント可能な Amazon One デバイスは屋内使用のみを目的としているため、適切な環境にインストールされていることを確認してください。
- 壁の要件: デバイスを適切に配置して機能させるには、壁が水平である必要があります。
- マウントの高さ: 壁面マウントの上部は、ユーザーがアクセスしやすいように、設置後に地面から 44～46 インチ以内に配置する必要があります。
- ケーブル管理: 余分なケーブルはすべて壁面マウントの背後でルーティングされ、損傷や乱雑さを防ぐために安全に固定されていることを確認します。
- Power Over Ethernet (PoE++): Power Over Ethernet (PoE++) を使用している場合は、IEEE 802.3bt (タイプ 3) クラス 6 の 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) が使用可能であることを確認します。PoE++ ソースはリスト化または認定され、IEC 62368-1 標準に準拠している必要があります。重要な点として、PoE++ ソースはデバイスと同じ建物内に配置する必要があります。AOE デバイスでは、承認された PoE++ ソースのみを使用してください。
- DC 15V 電源入力: DC 15V 電源入力を使用している場合は、必ず ™ クラス 2 または電力制限付き承認済み電源のみを使用してください。電源は、安全性と互換性についてリスト化または認定されている必要があります。

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
- 0.5 mm x 2 mm フラットヘッドドライバー
- T12 Secure Torx ドライバー
- 鉛筆
- レベル

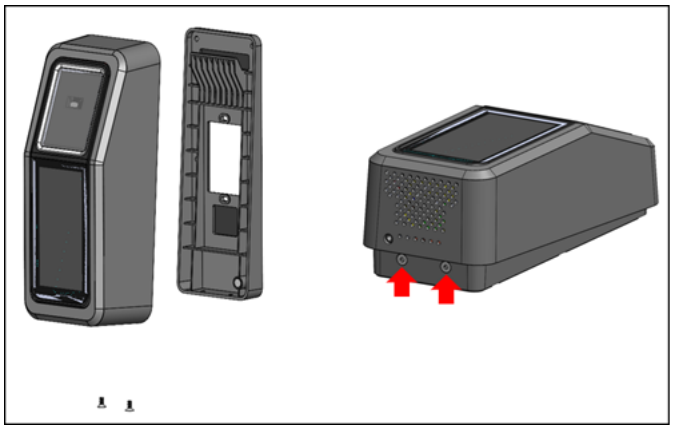
壁面マウント可能な Amazon One デバイスに付属

- 6x #8 ドライウォールアンカー
- 6x #8-32 1in ロングネジ
- 2x #6-32 1in マシンねじ
- 2x 6 ポジションターミナルブロックコネクタ
- 2 Torx Security M4x10 フラットヘッドネジ

これらの前提条件が確認されたら、インストール手順を進めて、壁面マウント可能な Amazon One デバイスを安全にマウントして設定できます。

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

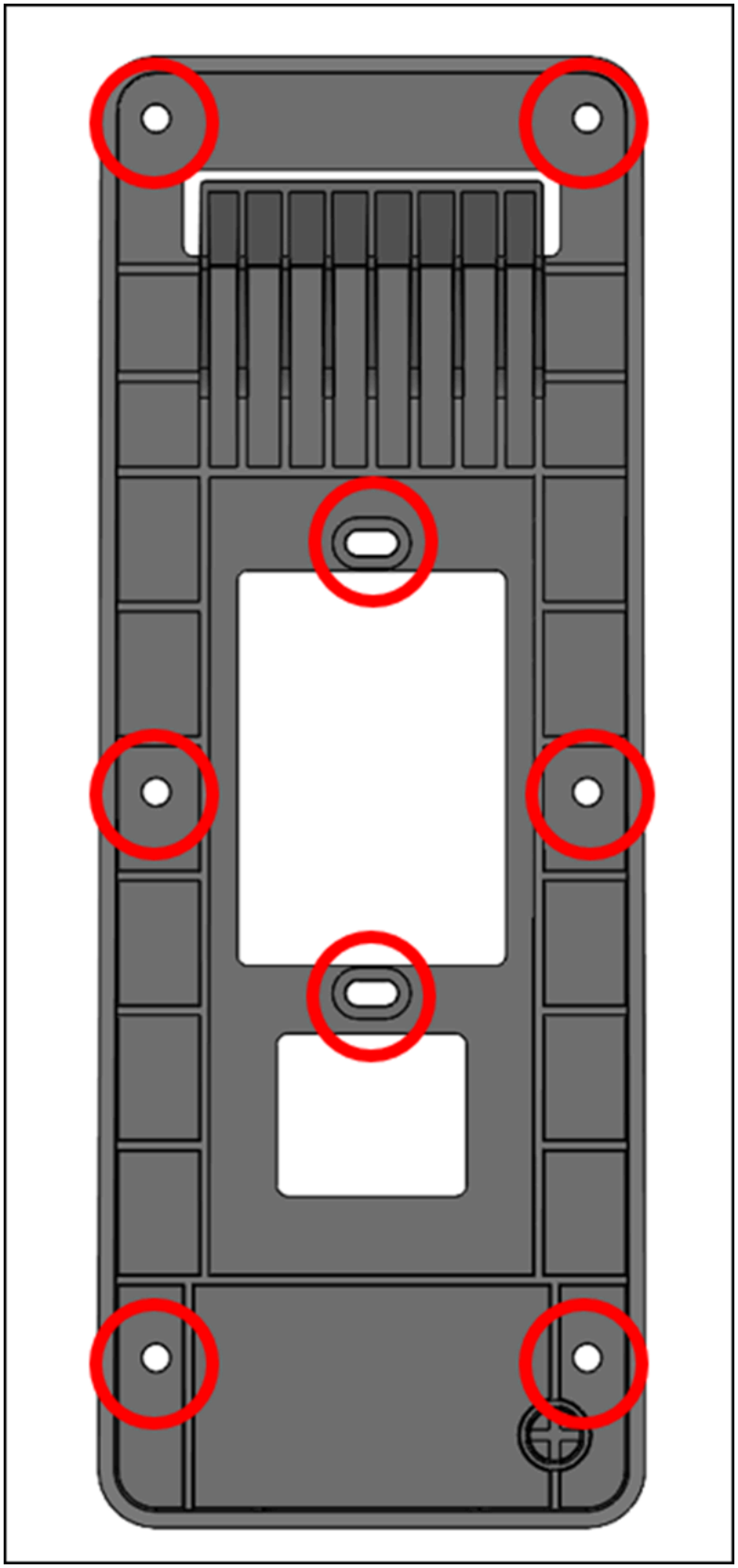
1. Amazon One デバイスをパッケージから削除します。
2. 下部の 2 つの Torx セキュリティネジを取り外して、マウントプレートを Amazon One デバイスから分離します。



3. マウントプレートを壁面の目的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 機械ネジをオブロングホールに挿入して、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。マウントプレートの追加サポートとして、オブロングホールと #6-32 ネジを使用できます。#6-32 ネジの位置を壁板を取り付ける主な手段として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マウントする場合は、マークされた各場所に 1/4 インチ穴をドリルし、アンカーが壁とフラッシュされるまで穴に押して壁アンカーを設置します。

   木構造表面に取り付ける場合、アンカーは必須ではなく、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. アンカー位置の #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、マウントプレートを壁に固定します。

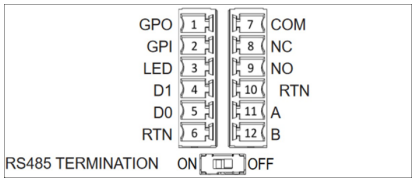
ウォールマウント可能な Amazon One デバイスを接続するには

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 (Mfg P/N: Phoenix Contact 1767694) を使用します。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決定するには、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	接続	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	

ピン	接続	説明	使用アイテム
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 – 緑のワイヤ
6	RTN	シグナルリターン	Wiegand Ground – 黒線
7	コム	リレー共通	コンタクトリレー共通 – ホワイトワイヤ
8	NC	リレーは通常閉じています	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
9	いいえ	リレーは通常開いている	コンタクトリレーは通常開いている – 黄色のワイヤ
10	RTN	シグナルリターン	OSDP リターン – ブラックワイヤ
11	A	RS485_A/D1/クロック	OSDP D1 – ホワイトワイヤ
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、ワイヤの終端から 3 ~ 5 mm 取り外します。

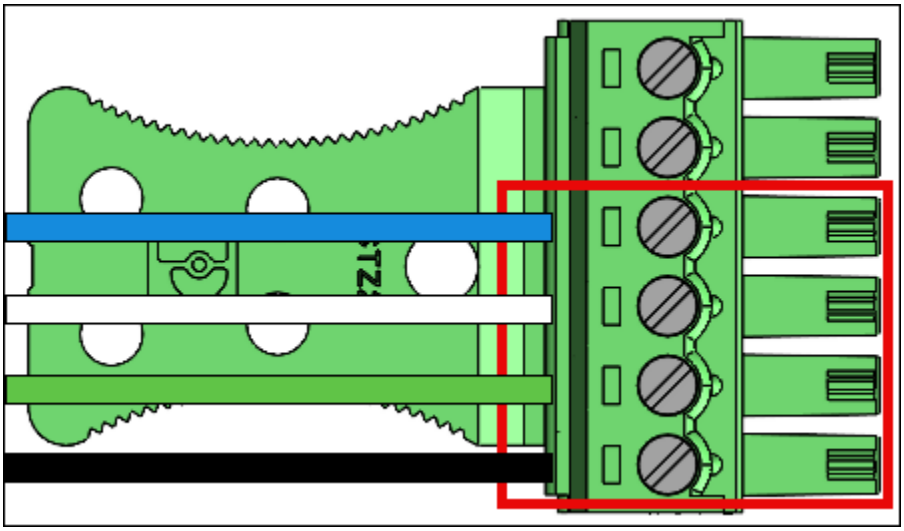
3. ワイヤのストライピングされた端を目的の終端位置に挿入します。
4. マイナスドライバーを使用して、ターミナル保持ネジを時計回りに回し、ワイヤーが固定されるまで固定します。きつくしすぎないでください。
5. 着地後、着地を確認するためにワイヤーのゲージを引いてください。
6. 必要な接続を行ったら、Amazon One デバイスターミナルブロックの対応するソケットにプラグを挿入します。
7. Cat6 イーサネットケーブルを RJ45 ジャックに挿入します。
8. Amazon One デバイスを配置して、壁板のフックがデバイスの背面の開きにスライドするようにします。
9. ケーブルがデバ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、デバイスのピボットと固定を所定の位置にします。
10. 2 つの Torx Security M4x10 フラットヘッドネジを使用して、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。きつくしすぎないでください。

壁面マウント可能な 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 (LED) に挿入します。
- 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 (RTN) に挿入します。



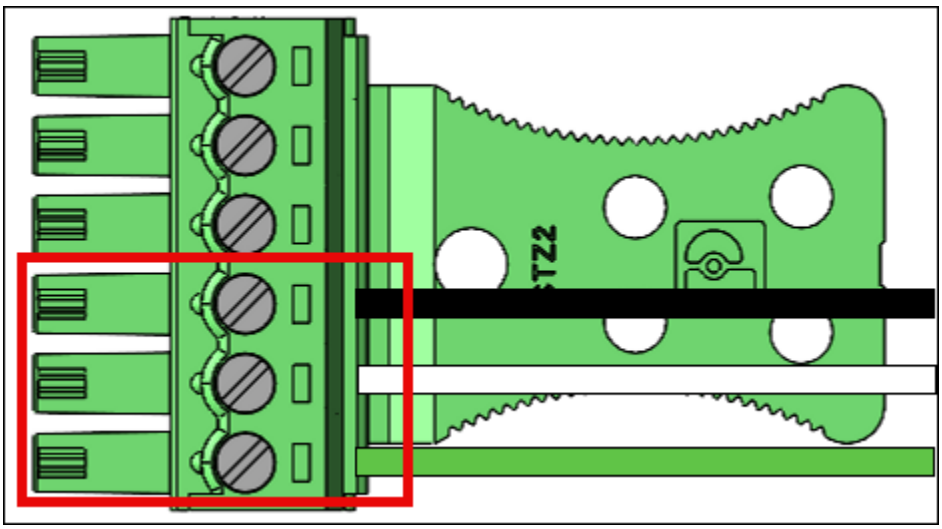
Wiegand 出力ワイヤリング

ピン	接続	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ユニットである場合は、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 オームの抵抗終端を有効にします。

RS485 接続

- 黒線をピン 10 (RTN) に挿入します。
- 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。

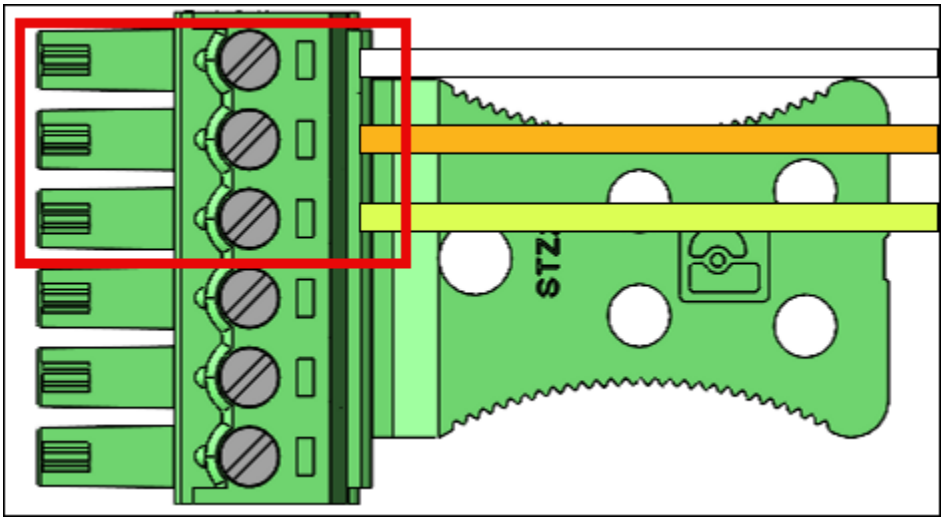


RS485 ワイヤリング

ピン	接続	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 反転信号

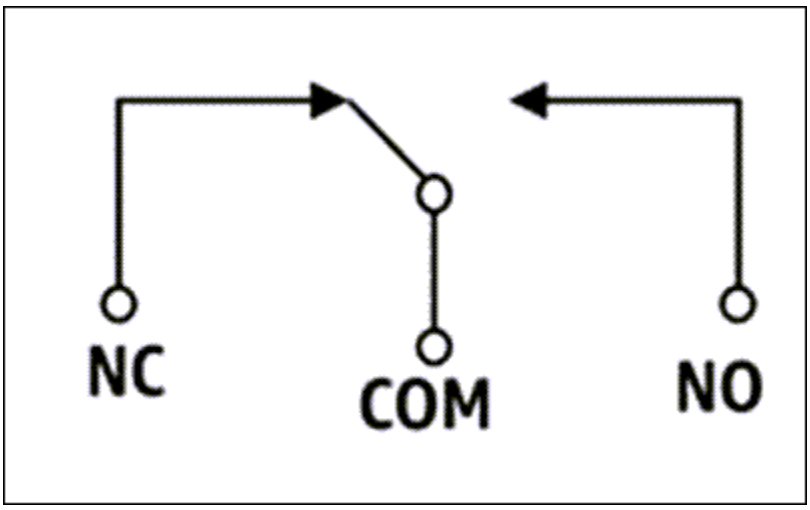
リレー接続

- ピン 7 (COM) に白いワイヤを挿入します。
- 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。



リレーワイヤリング

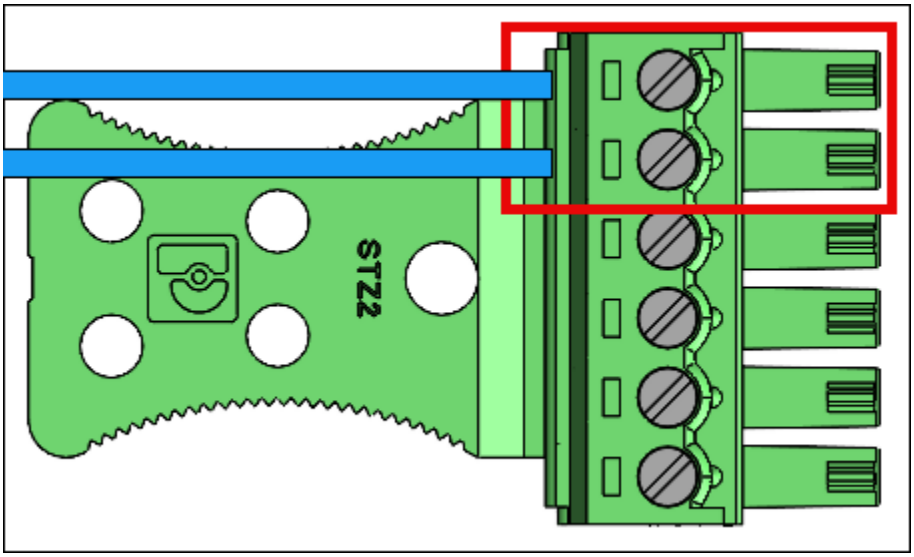
ピン	接続	説明	使用アイテム
7	COM	リレー共通	コンタクトリレー共通 – ホワイトワイヤ
8	NC	リレーは通常閉じています	コンタクトリレーは通常閉じている – オレンジ色のワイヤ
9	いいえ	リレーは通常開いている	コンタクトリレーは通常開いている – 黄色のワイヤ



リレーは、指定された安全評価 30VAC/60™、最大 60W に従って操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 (GPO) に挿入します。
- 青いワイヤをピン 2 (GPI) に挿入します。



デジタル入出力のワイヤリング

ピン	接続	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	接続	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、リストされているように操作する必要があります。

Amazon One デバイスをインストールしたら、デバイスをアクティブ化する準備が整います。

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

I/O Hub を備えた Amazon One デバイスは、Amazon One Enterprise システムの不可欠な部分であり、さまざまな環境のセキュリティを強化し、アクセスコントロールを合理化するように設計されています。このデバイスは、生体認証による送達認識を活用して、ユーザーに安全でタッチレスな認証を提供するため、オフィスビル、制限された入口、シームレスなアクセス管理を必要とする施設などのセキュリティの高いエリアでの使用に最適です。I/O Hub は、デバイスと既存のセキュリティインフラストラクチャ間のブリッジとして機能し、ドアロック、アラーム、その他のアクセスコントロールシステムとの通信を可能にします。

このセクションでは、I/O Hub で Amazon One デバイスをインストールするための場所の要件と step-by-stepについて説明します。適切な準備とインストールは、システムが安全かつ効率的に動作し、ユーザーにスムーズで信頼性の高いエクスペリエンスを提供する上で重要です。

I/O Hub で Amazon One Device をインストールするための前提条件と準備

インストールを開始する前に、以下の条件が満たされていることを確認し、安全で安全で効果的なセットアップを行います。

- 屋内使用のみ: I/O Hub を備えた Amazon One デバイスは、屋内使用専用に設計されています。適切な環境にインストールされていることを確認します。
- Power Over Ethernet (PoE++): Power Over Ethernet (PoE++) を使用している場合は、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) が使用可能であることを確認します。PoE++ ソースはリスト化または認定され、IEC 62368-1 標準に準拠している必要があります。重要な点として、PoE++ ソースはデバイスと同じ建物内に配置する必要があります。AOE デバイスでは、承認された PoE++ ソースのみを使用してください。

- DC 15V 電源入力: DC 15V 電源入力を使用している場合は、必ず "" クラス 2 または電源制限付きの承認済み電源のみを使用してください。電源は、安全性についてリスト化または認定されている必要があります。詳細については、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
- 0.5 mm x 2 mm フラットヘッドドライバー

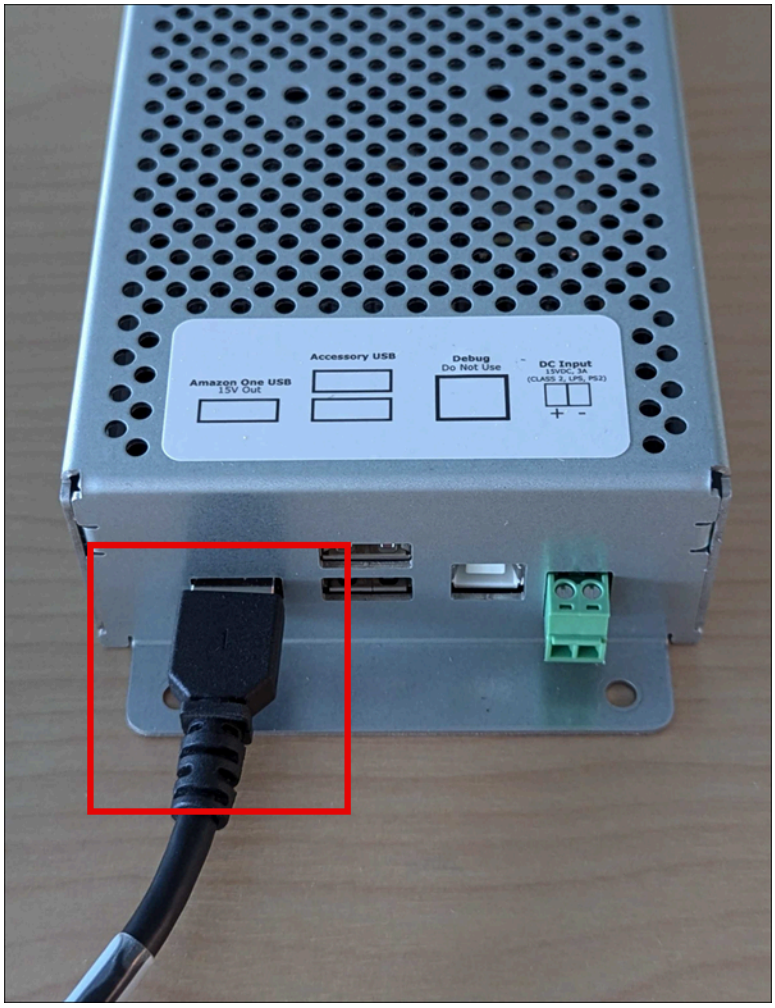
I/O Hub を備えた Amazon One デバイスに含まれている

- 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 インチ電源ケーブル/データケーブル

これらの前提条件が確認されたら、インストールプロセスを進め、I/O Hub を使用して Amazon One デバイスを安全かつ効率的にセットアップできます。適切な準備を行うことで、デバイスが意図したとおりに機能し、安全なアクセスシステムにスムーズに統合されます。

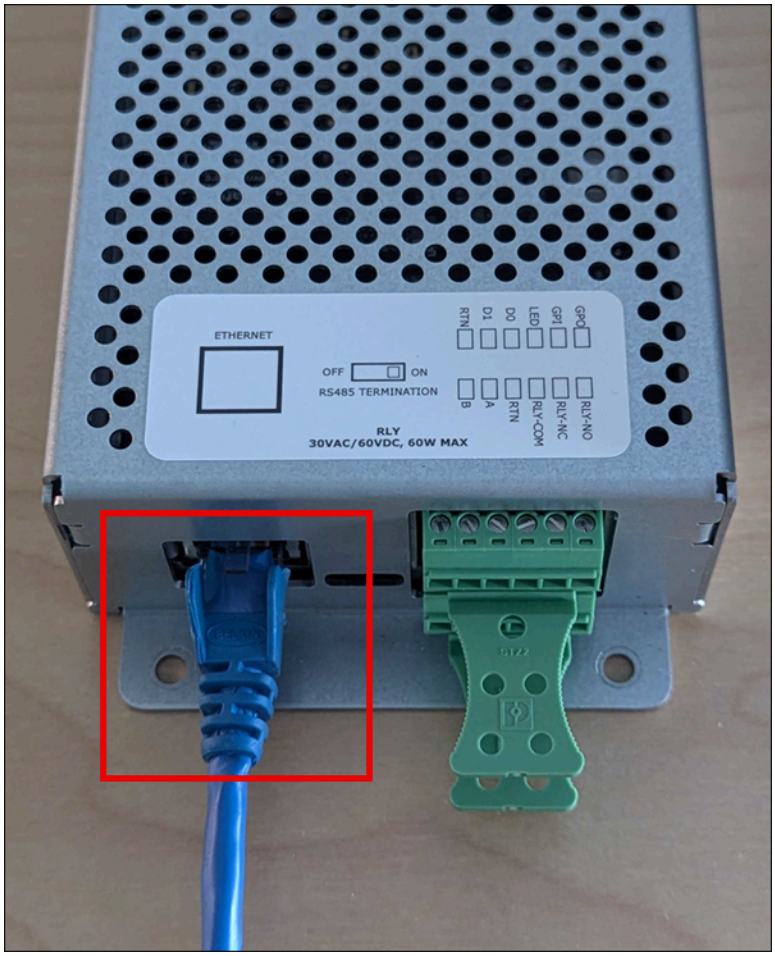
Amazon One デバイスの I/O ハブをインストールするには

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 ハブを目的の場所に固定します。
3. Amazon One USB ケーブルを I/O ハブポートに接続します。



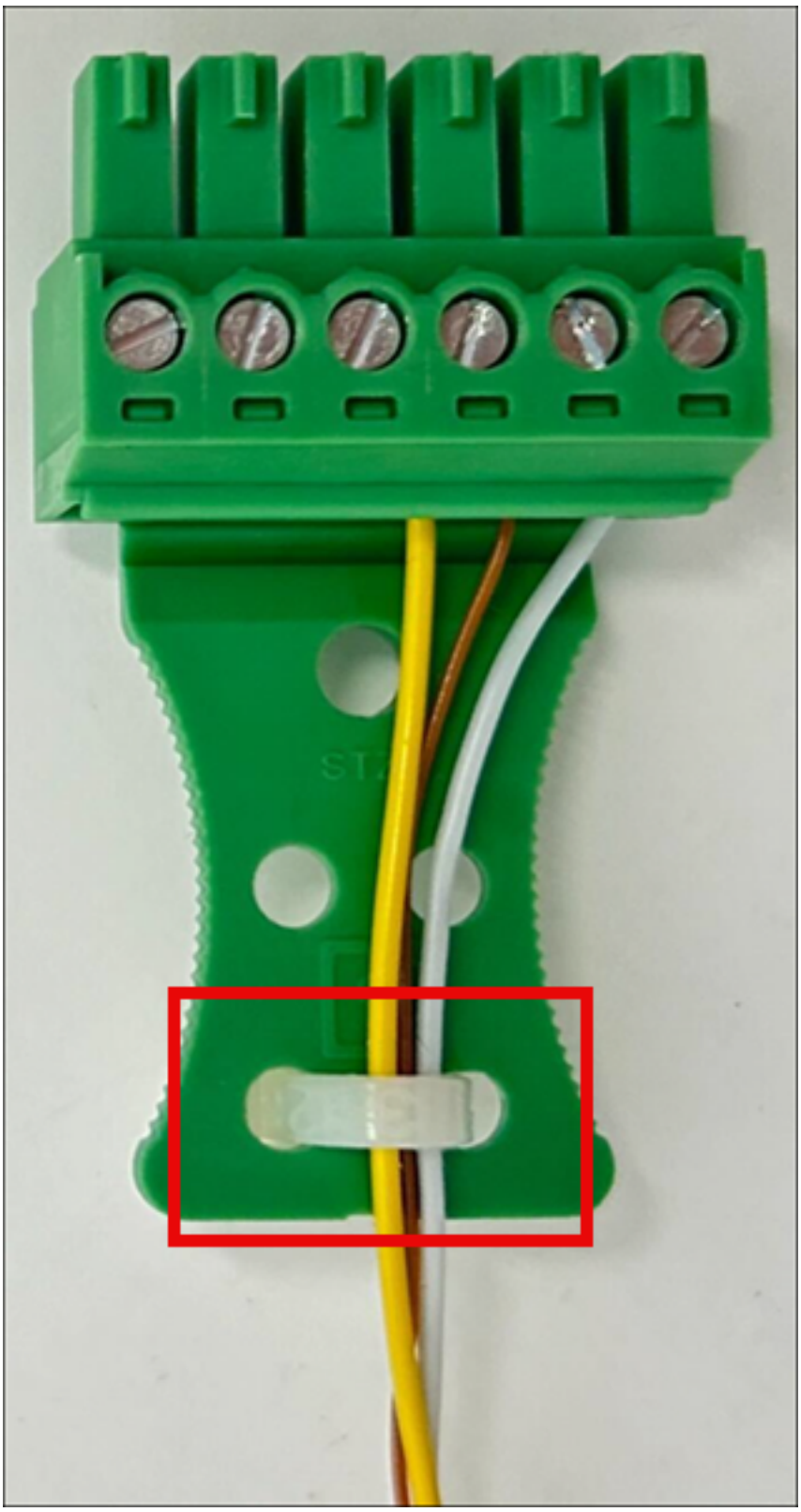
4. POE++ 電源の場合は、イーサネットケーブルを POE++ ソースから I/O ハブポートに接続します。

   オプション: DC 電源の場合は、以下の DC ワイヤリング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

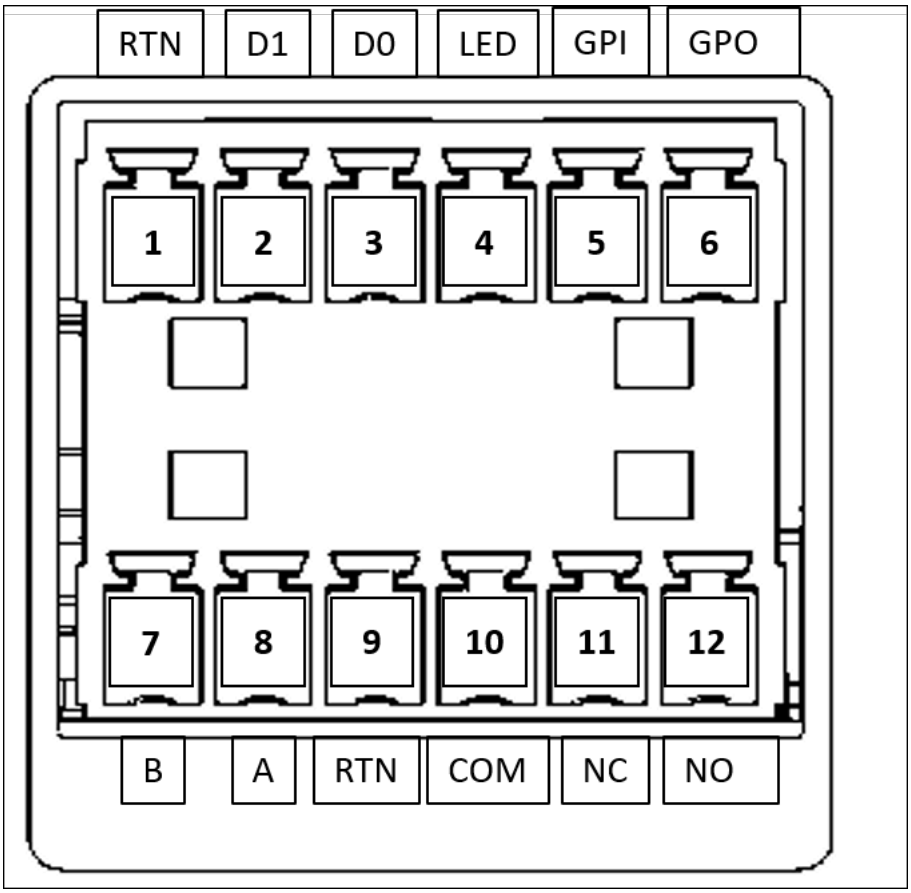
- 誤ってコードを下りて I/O ハブに流れる水を避けるために、跳ね返りループを設置します。
- 次の図に示すように、ワイヤーを損傷やストレスから保護するために、ストレインドリムーブクランプをアタッチします。



1. ターミナルブロックプラグを I/O ハブに挿入します。

2. 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。次の連結表と図を参照してください。

接続



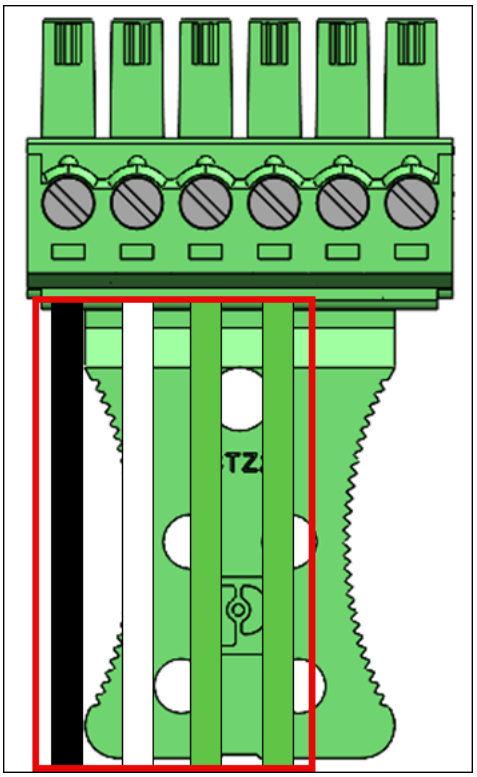
ピン	接続	説明	使用アイテム	
1	RTN	シグナルリターン	Wiegand Ground – ブラックワイヤ	
2	D1	Wiegand D1	Wiegand データ 1 – ホワイトワイヤ	
3	D0	Wiegand D0	Wiegand データ 0 – 緑のワイヤ	

ピン	接続	説明	使用アイテム
4	LED	Wiegand LED	Wiegand LED – オプション
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 – ホワイトワイヤ
9	RTN	シグナルリターン	OSDP リターン – ブラックワイヤ
10	COM	リレー共通	コンタクトリレー共通 – ホワイトワイヤ
11	NC	リレーは通常閉じています	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	リレーの通常開	コンタクトリレーは通常開いている – 黄色のワイヤ

Wiegand 接続

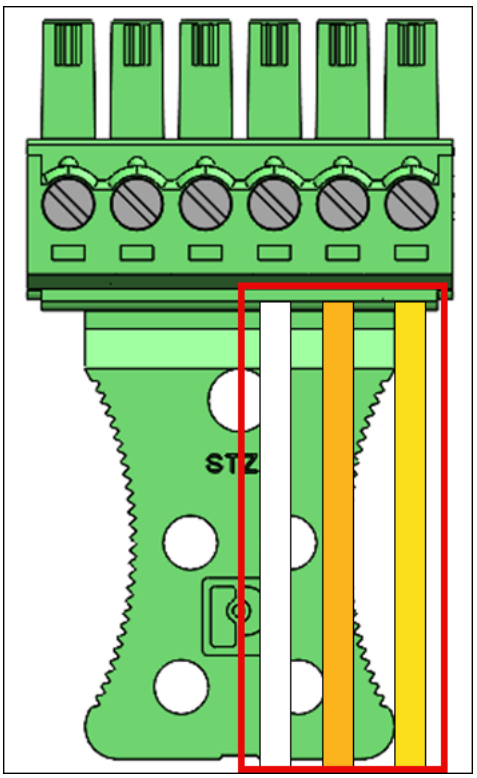
- 黒いワイヤをピン 1 (RTN) に挿入します。

- 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 (LED) に挿入します。

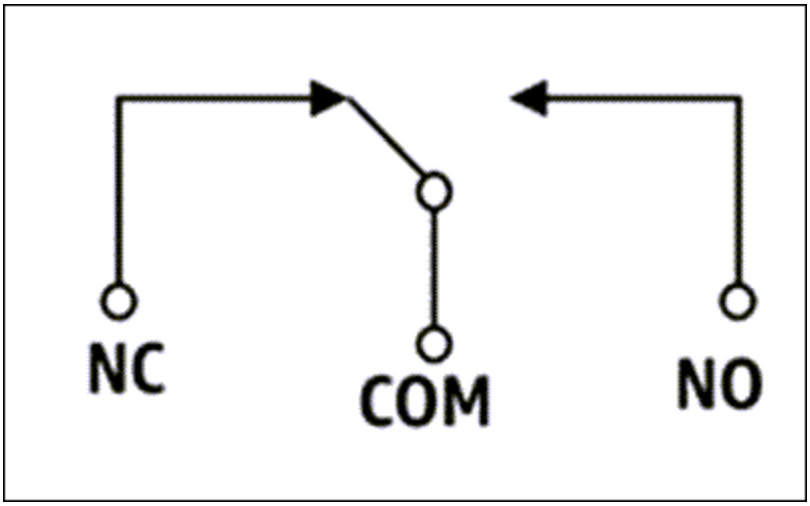


リレー接続

- ピン 10 (COM) に白いワイヤを挿入します。
- 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。



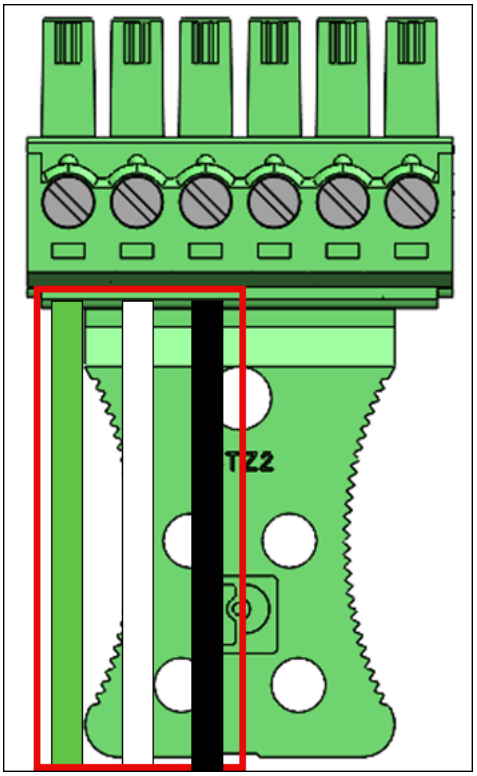
リレー図



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

RS485 接続

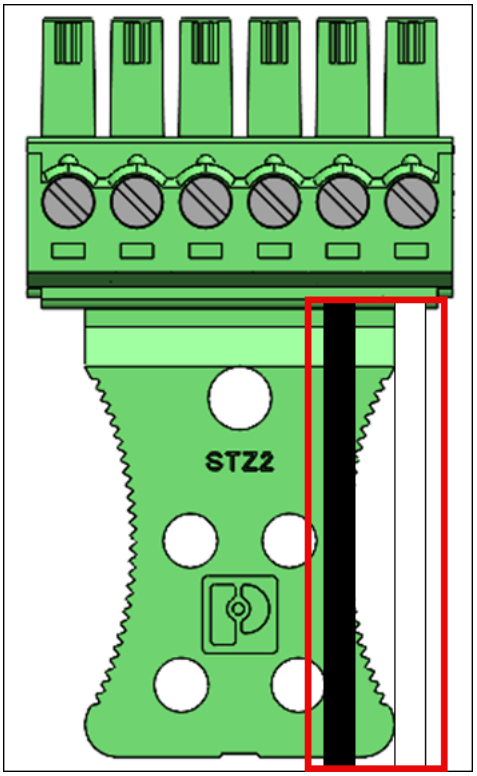
- 緑色のワイヤをピン 7 (B) に挿入します。
- ピン 8 (A) に白いワイヤを挿入します。
- 黒いワイヤをピン 9 (RTN) に挿入します。



デバイスがライン上の最後のユニットである場合は、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 オームの抵抗終端を有効にします。

デジタル入出力接続

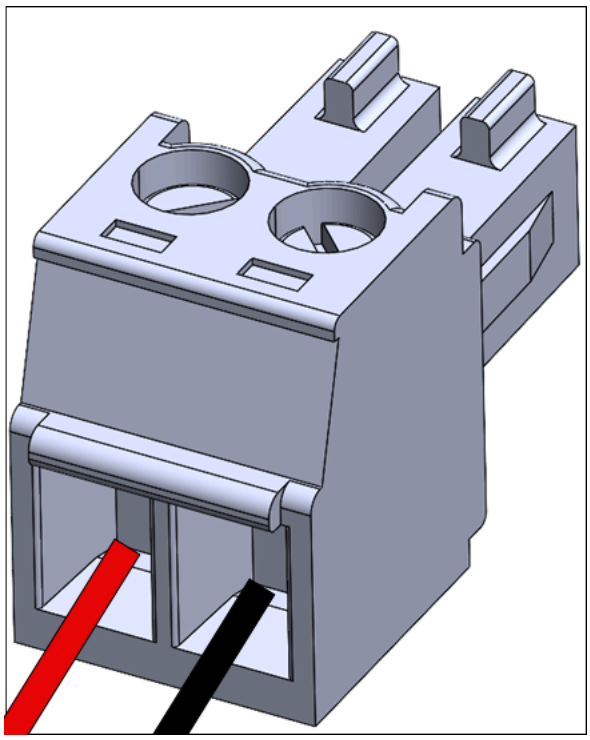
- 黒線をピン 5 (GPI) に挿入します。
- ピン 6 (GPO) に白いワイヤを挿入します。



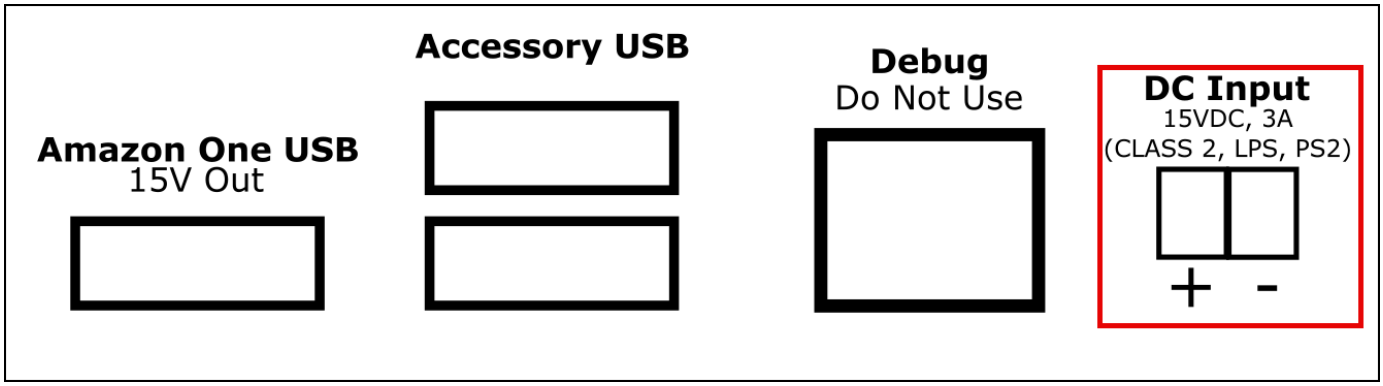
- デジタル入出力接続は、リストされているとおりに動作する必要があります。

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 3 mm ~ 5 mm、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ねじ込みます。
4. 有線 DC プラグを DC 入力ポートに挿入します。



Amazon One デバイスをインストールしたら、デバイスをアクティブ化する準備が整います。

Amazon One デバイスのアクティブ化

Amazon One デバイスがインストールされ、電源が入ると、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ました！と表示されたら、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。「Amazon One 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 Get QR コードを選択して 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。QR コードはセキュリティのために定期的に更新されるため、QR コードは 1 回しか使用できません。
11. サイトの郵便番号を入力し、正しいサイトが表示されたことを確認してから設定の確認を選択します。
12. 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。

ユーザーの登録と入力

Amazon One デバイスがアクティブ化されたので、従業員は自分の代理人を登録し、代理人を認証してアクセスできるようになります。

トピック

- エンドポイントポリシーの作成
- エントリの認証

エンドポイントポリシーの作成

ユーザーが入室用を認証する前に、登録プロセスを経る必要があります。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 デバイスにモニターリングを登録するには

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を使用して、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 デバイスの画面にバッジがスキャンされたと表示されます。
3. 利用規約を読み、OK キーを押します。
4. 同意をお読みください - お客様の住所の生体認証情報をお読みになり、同意する場合は「同意する」とお押しください。
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

本番登録が完了したら、Amazon One Enterprise エントリデバイスで本番登録を使用して認証する準備が整います。

Amazon One デバイスへのエントリについて詞を認証するには

- デバイスの上部にカーソルを置き、画面の指示に従って舌をスキャンします。

ユーザーの管理

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たり、ユーザーの生体認証を削除したりできます。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。

トピック

- 登録済みユーザーの表示
- 登録済みユーザーとその生体認証の削除

登録済みユーザーの表示

次の手順では、ユーザーを登録する方法について詳しく説明します。

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. 登録されたユーザーには、登録されたすべてのユーザーと以下の詳細が表示されます。
    - 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。

登録済みユーザーとその生体認証の削除

次の手順では、登録されたユーザーとその生体認証を削除する方法について詳しく説明します。

登録済み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. 登録されたユーザーで、登録された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. メトリクス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完全に削除されます。ユーザーが Amazon One Enterprise を認証に使用できるようにするには、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。

Amazon One 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

- Amazon One デバイスのメンテナンスとクリーニング
- サイト管理
- デバイスインスタンス管理

Amazon One デバイスのメンテナンスとクリーニング

Amazon One デバイスを維持すると、最適なデバイス運用環境とデバイスエクスペリエンスが提供されます。

Amazon One デバイスをクリーニングする前に、以下を確認してください。

- Amazon One を有効または無効にする必要はありませんが、デバイスが電源に接続され、ネットワーク接続があり、周辺機器およびコンパニオンデバイス (該当する場合) が接続されていることを確認してください。
- ネットワーク接続が利用できない場合 (エラー画面が Amazon One デバイスに表示される場合) 、エラー画面が Amazon One デバイスに表示されるか、デバイス接続の問題がコンソールに表示される場合は、問題を管理者にエスカレーションします。
- 権限のない個人が改ざんできないように、デバイスを物理的に保護します。
- Amazon One デバイスを毎日視覚的に検査し、Amazon One デバイスへの不正な接続がないか確認します。
- デバイスの目に見えるネジや大文字と小文字など、改ざんの兆候がないかデバイスのすべての側面を検査し、いずれかの Amazon One デバイスの内部コンポーネント/ネジが露出するギャップ/開きがないことを確認します。
- エラーや障害が発生した場合は、Amazon One デバイス画面の指示に従うか、トラブルシューティングガイドを参照して問題を修正してください。

Amazon One デバイスをクリーンアップするには

Amazon One デバイスを定期的にクリーニングすると、フィンガープリントやハンドプリントなどのスマッジやマークが削除されます。

> **Note**
>
> このガイドに記載されている以外のクリーニング製品を使用しないでください。推奨されるクリーニングスケジュールは、1 週間に 1 回または 2 回、またはデバイスに土、ほこり、またはスマッジが表示されるたびにですが、1 日に 1 回以上は表示されません。

1. Iso™ Carbon (IPA) Wipes を使用して Amazon One デバイスをワイプします。デバイスのタッチサーフェスのみをクリーニングします。Amazon One からの指示がない限り、光学ウィンドウにタッチしたり、他のクリーニング製品を使用したりしないでください。
2. しわは、ドライなマイクロボイスクロスでふき取ってください。
3. 光学ウィンドウから目に見える土やゴミを軽く埃 (ワイプしないでください) します。光学ウィンドウのクリーニングは、1 日に 1 回、および/またはウィンドウが視覚的にダーティ (指/手の印刷/しみなど) である場合に制限します。デバイスのこの部分は、触れることを意図していませんが、新しい顧客から不注意で触れる可能性があります。
4. 該当する場合は、KIC スマートカードクリーナーを使用してカードリーダーの内側をクリーニングします。
5. デバイスを週に 1 ~ 2 回、またはデバイスにゴミ、ほこり、またはしみが見られるたびにクリーニングします。

サイト管理

サイトは、デバイスインスタンスのコレクション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。

トピック

- サイト名の変更
- サイトアドレスの更新

サイト名の変更

次の手順では、デバイスのサイト名を変更する方法について詳しく説明します。

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。

サイトアドレスの更新

次の手順では、デバイスのサイトアドレスを更新する方法について詳しく説明します。

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。
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。

トピック

- デバイスインスタンスのステータスの表示
- Amazon One デバイスの再起動
- Amazon One デバイス設定の更新
- Wi-Fi 認証情報の更新
- デバイスインスタンスの非アクティブ化

デバイスインスタンスのステータスの表示

次の手順では、デバイスインスタンスのステータスを表示する方法について詳しく説明します。

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して、デバイスインスタンスの詳細を表示します。

Amazon One デバイスの再起動

次の手順では、Amazon One デバイスを再起動する方法について詳しく説明します。

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. Amazon One デバイスを再起動するには、再起動を選択します。

Amazon One デバイス設定の更新

次の手順では、Amazon One デバイス設定を更新する方法について詳しく説明します。

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)。次に、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 デバイスのアクティブ化)。

5. 必要な変更を行ったら、デバイス設定の更新を選択して更新を確認します。

Wi-Fi 認証情報の更新

次の手順では、Wi-Fi 認証情報を更新する方法について詳しく説明します。

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の非アクティブ化

次の手順では、デバイスインスタンスを非アクティブ化する方法について詳しく説明します。

デバイスインスタンスを非アクティブ化するには

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. デバイスを無効にするを選択します。
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。

セキュリティ

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、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 とお客様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があります AWS クラウド。 AWS また、 は、お客様が安全に使用できるサービスも提供します。AWS コンプライアンス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、ユーザーは、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 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

Amazon One Enterprise でのデータ保護には、 AWS 責任共有モデルが適用されます。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。ユーザーは、このインフラストラクチャでホストされるコンテンツ

に対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。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に関するよくある質問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、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。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 AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 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します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理された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。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な 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を、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含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Amazon One Enterprise AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL 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 が所有するキーを表示、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、AWS Key Management Service デベロッパーガイドの「AWS 所有キー」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 の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、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。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、追加料金なしで AWS のサービス 使用できる です。

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 IAM の連携方法
- 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

対象者

AWS Identity and Access Management (IAM) の使用方法は、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 – ジョブを実行するために Amazon One Enterprise サービスを使用する場合、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すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。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 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。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で Amazon One Enterprise で 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 IAM の連携方法。

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。IAM 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、「」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

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM アイデンティティセンター) ユーザー、会社のシングルサインオン認証、Google または Facebook 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場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して にアクセスすると、間接的 AWS にロールを引き受けます。

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

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

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、 では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用する AWS ことを

お勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 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。この ID は AWS アカウント ルートユーザーと呼ばれ、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「ルートユーザー認証情報が必要なタスク」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が、一時的な認証情報 AWS のサービス を使用して にアクセスするために ID プロバイダーとのフェデレーションを使用することを要求します。

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、ウェブ ID プロバイダー、、AWS Directory Serviceアイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするすべてのユーザーです。フェデレーティッド ID が にアクセスすると 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。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の 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 AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに特定のアクセス許可 AWS アカウントを持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、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 ユーザーでの長期的な認証情報が必要な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、「IAM 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のためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団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、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

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、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次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については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで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、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサー

ビス、 (ロールをプロキシとして使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。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アクションを実行すると AWS、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と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストをリクエストする を組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。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、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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。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は に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンク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 EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、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、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」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

でアクセスを制御するには AWS 、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、そのアクセス許可を定義します。 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 AWS 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 JSON ドキュメント AWS として に保存されます。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、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、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方法を問わず、アクションの許可を定義します。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、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

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ポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれ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いずれかを選択する」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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 を含めることができます 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。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL 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は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、「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ています。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ポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限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、ビジネスが所

有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。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 (SCP) を一部またはすべてのアカウントに適用できます。SCP 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を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- 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、「IAM ユーザーガイド」の「セッションポリシー」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。複数のポリシータイプが関係する場合に がリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

Amazon One Enterprise と IAM の連携方法

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 機能について学びます。

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

Amazon One Enterprise およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」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

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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、許可または拒否するアクションとリソース、およびアクションを許可または拒否す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学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」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 のアイデンティティベースのポリシーの例については、「」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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 を含めることができます 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、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。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、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」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 JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。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` 要素にはポリシー内の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が記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない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アクセス許可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 のアイデンティティベースのポリシーの例については、「」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 JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。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。

Resource JSON ポリシー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 ARNs「」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 のアイデンティティベースのポリシーの例については、「」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 JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。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して、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。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子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と、 は論理ORオペレーションを使用して条件 AWS 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 IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」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ています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

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 のアイデンティティベースのポリシーの例については、「」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 ACLs

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL 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は使用しません。

Amazon One Enterprise での ABAC

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (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。ではAWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、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した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM 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」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

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する機能などの詳細については、AWS のサービス「IAM ユーザーガイド」の「IAM と連携する」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、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。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。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 AWS することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」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 (FAS) のサポート: あり

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と AWS、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と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストをリクエストする を組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。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

サービスロールとは、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、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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。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は に表示され AWS アカウント 、 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、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされた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、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM 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、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARNs「」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

トピック

- ポリシーに関するベストプラクティス
- Amazon One Enterprise コンソールの使用
- 自分の権限の表示をユーザーに許可する
- Amazon One Enterprise への読み取り専用アクセス
- Amazon One Enterprise へのフルアクセス
- Amazon One Enterprise Rule API アクションでサポートされているリソースレベルのアクセス許可
- 追加情報

ポリシーに関する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を実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、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AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な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 を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで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、アクションや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 SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用される場合に AWS のサービス、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 CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」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、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – 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は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、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 を使用した安全な API アクセス」を参照してください。

IAM で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 IAM でのセキュリティのベストプラクティス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。最小限必要な許可よりも制限が厳しい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。

AWS CLI または AWS API 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。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が許可されます。

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、エンティティに Amazon One Enterprise *ConsoleAccess* または *ReadOnly* AWS マネージドポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」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、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、

または AWS CLI または AWS API 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。

```
{
    "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、Amazon One Enterprise への読み取り専用アクセスを許可する AWS マネージドポリシーである `AmazonOneEnterpriseReadOnlyAccess` を示しています。

```
{
  "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、それらのアクションをユーザーが実行する対象の AWS リソースを指定します。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 に設定されます。これは*「すべてのリソース」を意味するワイルドカードです。

Action 要素の値は、サービスがサポートする API に対応しています。アクションは、Amazon One Enterprise アクションを参照していることを示すconfig:ために が先頭に付けられます。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、Amazon One Enterprise のすべてのアクションが許可されますが、他の AWS サービスのアクションは許可されません。
- "Action": ["*"]

  これにより、すべての AWS アクションが許可されます。このアクセス許可は、アカウントの AWS 管理者として動作するユーザーに適しています。

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 Rule API アクションでサポートされてい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。

次の表は、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 アクションを示しています。各アクションでサポートされるリソースとその ARN についても説明しています。ARN の指定時、正確なリソース ID を指定できない (したくない) 場合などに、パスに * ワイルドカードを使用できます。

> **Important**
>
> Amazon One Enterprise ルール API アクションがこのテーブルにリストされていない場合、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

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

API アクション	リソース
UpdateSiteAddress	サイト arn:aws:one:*region:accountID* :site/*siteId*
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、指定した AWS Config ルール`GetSite`で などの読み取りアクションをルールに許可します。

```
{
        "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、Amazon One Enterprise ルール API アクションに対して特定のアクションを実行するための読み取りアクセスを許可し、書き込みアクセスを拒否できます。

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。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可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) に影響します。 AWS は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API オペレーションが利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「IAM ユーザーガイド」の「AWS マネージドポリシー」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への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 デバイスをアクティブ化するための QR コードを作成できます。

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

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 Amazon One Enterprise の AWS マネージドポリシーの更新に関する詳細を表示します。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 履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
Amazon One Enterprise に AmazonOneMetricPublishAccess を追加	AmazonOneMetricPublishAccess という名前のロール許可ポリシーにより、Amazon One Enterprise は CloudWatch 名前空間 AWS/AmazonOne で CloudWatch:PutMetricData を実行できます。	2025 年 2 月 6 日

変更	説明	日付
Amazon One Enterprise が変更の追跡を開始	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、IAM アクセス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、アクション、および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` エレメントでは、以下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は、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る場合、そのアクションを含むステートメントでそのタイプの ARN 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` 要素で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許可を付与	読み取り			
UpdateDeviceInstance	デバイスインスタンスを更新する許可を付与	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許可を付与	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 QR コードを作成する許可を付与	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許可を付与	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許可を付与	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	Tagging	device-instance、site、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	Tagging	device-instance、site、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

以下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` エレメントで使用できます。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 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/${TagKey}	リクエストからのタグに基づいてアクセスをフィルタリング	String
aws:ResourceTag/${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	String

条件キー	説明	[Type] (タイプ)
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AWS のサービス プログラムによる対象範囲内コンプライアンス」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「 Compliance ProgramsAssurance」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、「Downloading AWS Artifact reports 」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。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービス が HIPAA に対応しているわけではありません。
- 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、お客様の業界と場所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。このガイドは、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) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 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 、セキュリティ状態を包括的に把握できます 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一覧については、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 – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、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 を使用すると、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、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- 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、およびパフォーマンスを維持する上で重要な部分です。 は、Amazon One Enterprise をモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するために、以下のモニタリングツール AWS 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 EventBridge ユーザーガイド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 コール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。が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、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

Amazon EventBridge 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。EventBridge は、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を提供します。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 EventBridge を使用して発行され、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. https://console.aws.amazon.com/events/ で AWS コンソールにログインします。
2. https://console.aws.amazon.com/events/ で EventBridge コンソールを開きます。
3. ナビゲーションペインの [バス] で、[ルール] を選択します。
4. ルールの作成を選択します。
5. デフォルトルールの詳細ページで、ルールに名前を割り当てます。
6. [Rule with an event pattern] (イベントパターンを持つルール) を選択してから、[Next] (次へ) を選択します。
7. [イベントパターンを構築] 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。
8. サンプルイベントタイプで、AWS イベントを選択します。
9. 作成方法 で、カスタムパターンを選択します。
10. 「イベントパターン」セクションで、イベントソースを `aws:one`とし、必要な詳細タイプを持つ JSON を追加します。

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

    上記のリストから必要な詳細タイプを選択し、不要なものを削除できます。
11. [Next (次へ)] を選択します。
12. Select target (s) 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。

    例えば、誰かがいつクロックインしたかを表示するには、「Successful Recognition」を選択します。次に、イベントの詳細 (付録を参照) を見て、誰がクロックインしたかを確認します。

ワークフローを完了するには、外部 API または別のターゲットを実行します。

13. 必要に応じて、タグを設定できます。
14. [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、EventBridge ユーザーガイド」の「EventBridge ルール」を参照してください。 EventBridge

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 JSON で生成されます。イベントタイプごとに、ルールで設定されているように、JSON ブロブが、選択したターゲットに送信されます。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。

デバイスの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。

リソース

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どうかを表します。
- 指定できる値: CONNECTED、DISCONNECTED

previousConnectivity

- イベント前に deviceInstance がインターネットに接続されていたか切断されたかを表します。
- 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

- deviceInstance が最後にチェックされたときに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

assetTagId

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

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。

新規登録解除成功

ユーザーが正常に登録解除された場合。

失敗した登録

ユーザーが登録に失敗したとき。

失敗した登録解除

ユーザーが登録解除に失敗したとき。

認識の成功

ユーザーが認証のために舌を正常にスキャンしたとき。

失敗した認識

凸状スキャンの認識に失敗したとき。

リソース

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デバイスの deviceInstanceId です。

createdTimestamp

- イベントが作成された時刻。

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クリティカルに変更されました
- 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

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に合格し、デバイスインスタンスのヘルスステータスは重大ヘルスステータスから HEALTHY 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クリティカルに変更されました

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 HEALTHY から CRITICAL に変更されました。

```
{
  "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 DISCONNECTED から CONNECTED に変更されました。

```
{
  "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 CONNECTED から DISCONNECTED に変更されました。

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

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。CloudTrail は、Amazon One Enterprise のすべての API コールをイベントとしてキャプチャします。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 S3バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。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。CloudTrail で収集された情報を使用して、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。

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

CloudTrail の Amazon One Enterprise 情報

アカウントを作成する AWS アカウント と、 で CloudTrail 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イベント履歴の他の AWS サービスイベントとともに CloudTrail 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、 CloudTrail イベント履歴でのイベントの表示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。追跡により、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 がサポートされているサービスと統合」

- 「CloudTrail の Amazon SNS 通知の設定」
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

すべての Amazon One Enterprise アクションは CloudTrail によってログに記録され、 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、`ListSites`、`RebootDevice`、`DeleteDeviceInstance` の各アクションを呼び出すと、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。

- リクエストがルートまたは 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 エレメント」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

「トレイル」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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、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の情報を含みます。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。

以下の例は、`CreateSite` アクションを示す CloudTrail ログエントリです。

```
{
    "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 のトラブルシューティング

Amazon One Application または Amazon One デバイスのいずれかに問題がある場合は、以下の提案を使用して問題のトラブルシューティングを行います。その後、それでも問題が解決しない場合は、AWS サポートにお問い合わせください。

トピック

- Amazon One 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
- Amazon One コンソールのトラブルシューティング
- Amazon One デバイスのトラブルシューティング

Amazon One 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 と IAM 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正に役立ちます。

トピック

- Amazon One でアクションを実行する権限がありません
- 自分の 以外のユーザーに Amazon One リソース AWS アカウント へのアクセスを許可したい

Amazon One でアクションを実行する権限がありません

アクションを実行する権限がないというエラーが表示された場合は、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。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なone:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
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、 AWS 管理者にお問い合わせください。サインイン資格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 Amazon One リソース AWS アカウント へのアクセスを許可したい

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 (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

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 IAM の連携方法。
- 所有 AWS アカウント している のリソースへの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「所有 AWS アカウント している別の 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。
- 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については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介し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「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Amazon One コンソールのトラブルシューティング

Amazon One Application または Amazon One デバイスのいずれかに問題がある場合は、以下の提案を使用して問題のトラブルシューティングを行います。その後、それでも問題が解決しない場合は、AWS サポートにお問い合わせください。

トピック

- サイトを作成できない
- デバイスインスタンスを作成できません

- 設定テンプレートを作成できません
- アクティベーション QR コードを作成できない

サイトを作成できない

- Amazon One Console 管理者に連絡して、アクセス権を付与してください。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

デバイスインスタンスを作成できません

- Amazon One Console 管理者に連絡して、アクセス権を付与してください。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

設定テンプレートを作成できません

- Amazon One Console 管理者に連絡して、アクセス権を付与してください。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

アクティベーション QR コードを作成できない

- Amazon One Console 管理者に連絡して、アクセス権を付与してください。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

Amazon One デバイスのトラブルシューティング

Amazon One コンソールまたは Amazon One デバイスのいずれかに問題がある場合は、次の提案を使用して問題のトラブルシューティングを行います。その後、それでも問題が解決しない場合は、AWS サポートにお問い合わせください。

トピック

- 空白画面
- Wi-Fi またはネットワークに接続できない
- アクティブなアラートでデバイスを再起動する

- システムエラー
- QR コードが認識されない
- QR コードを読み取れない
- 複数の QR コードが検出されました
- デバイスインスタンスが存在しません
- サイトが見つかりません
- 郵便番号が一致しません
- ゲートウェイがタイムアウトしました
- デバイスを設定できない
- デバイスがエラーメッセージとエラーコードで再起動しました
- デバイス画面上の Amazon ロゴ。それ以上のアクティビティはありません。
- 一時的に使用不可
- 問題が発生しました
- 一時的なサービス停止
- Amazon One デバイスに物理的な損傷がある
- アダルトを読み取れない
- 手掌が認識されない
- 非アクティブが長引いたためデバイスがロックされました
- 改ざんイベントによりデバイスがロックされました

空白画面

これは、デバイスに電源がない場合、または再起動中に停止した場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- デバイスを再起動する場合は、しばらく (30 秒未満) 待ちます。
- デバイスが空白のときにライトリングが点滅している場合は、最大 30 秒待ちます。
- 電源コードが、Amazon One デバイスの背面だけでなく、電源にもしっかりと接続されているかどうかを確認します。また、コードに損傷がないことを確認します。
- 電源を確認します。

- すべてのケーブルが Amazon One と USB ハブに正しく接続されていることを確認します。
- コンソールからデバイスを再起動します。
- デバイスを再起動しても問題が解決しない場合は、Amazon One USB ハブを電源から取り外してから、再度差し込みます。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

Wi-Fi またはネットワークに接続できない

これは、デバイスが接続を失ったときに発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- Wi-Fi に接続されている場合は、別のデバイスを使用して、Wi-Fi が利用可能なネットワークに表示されるかどうかを確認します。
- Wi-Fi ルーターがオンになっており、範囲内にあるかどうかを確認します。
- ネットワークが復旧すると、デバイスは再接続します。
- 問題が解決しない場合は、AWS サポートにお問い合わせください。

アクティブなアラートでデバイスを再起動する

コンソールから再起動がリクエストされると、オフラインまたはネットワークの問題に直面していても、 オペレーションはデバイスがコマンドを受信して再起動を試みるまで最大 15 分待ちます。

この問題のトラブルシューティングを行うには、以下を実行します。

- 再起動が完了するまで待ちます。
- 問題が解決しない場合は、AWS サポートにお問い合わせください。

システムエラー

これは内部エラーが原因で発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- 画面で再起動を選択して、アプリケーションを再起動します。
- 2 回試行しても問題が解決しない場合は、AWS サポートにお問い合わせください。

QR コードが認識されない

これは、不正な QR コードまたは期限切れの QR コードが原因で発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- もう一度試して、QR コード画面に戻ります。
- AWS コンソールで新しい QR コードを作成し、有効な QR コードをスキャンします。

QR コードを読み取れない

これは、アプリケーションが QR コードを読み取れない場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- もう一度試して、QR コード画面に戻ります。
- 問題が解決しない場合は、アクティベーションワークフローをキャンセルして再起動します。

複数の QR コードが検出されました

これは、複数の QR コードがスキャンされた場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- もう一度試して、QR コード画面に戻ります。
- 一度にスキャンできる有効な QR コードは 1 つだけです。

デバイスインスタンスが存在しません

これは、デバイスインスタンスが削除されるか、AWS コンソールに存在しない場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- もう一度試して、QR コード画面に戻ります。
- AWS コンソールで正しいデバイスインスタンスを確認します。デバイスインスタンスが見つからない場合は、管理者にお問い合わせください。
- そのデバイスインスタンスの新しい QR コードを作成し、新しい QR コードをスキャンします。

サイトが見つかりません

これは、サイトが削除されるか、AWS コンソールに存在しない場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- AWS コンソールでサイト情報を確認します。サイトが存在しない場合は、管理者にお問い合わせください。

郵便番号が一致しません

これは、デバイスに設定された郵便番号とは異なる郵便番号を入力した場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- もう一度試して、郵便番号画面に戻ります。
- 正しいサイトの ZIP コードがあるかどうかを確認します。
- 問題が解決しない場合は、管理者に連絡して、AWS コンソールでサイトの ZIP コードを確認してください。

ゲートウェイがタイムアウトしました

これは、指定した時間内にゲートウェイからの応答がない場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- 再起動を選択してアプリケーションを再起動します。
- 2 回試行しても問題が解決しない場合は、AWS サポートにお問い合わせください。

デバイスを設定できない

これは、オペレーションがデバイスディスクに設定を保存できなかった場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- 再起動を選択してアプリケーションを再起動します。
- 2 回試行しても問題が解決しない場合は、AWS サポートにお問い合わせください。

デバイスがエラーメッセージとエラーコードで再起動しました

この問題のトラブルシューティングを行うには、以下を実行します。

- 再起動 を選択し、デバイスを回復させます。
- デバイスが回復しない場合は、USB ハブを電源から取り外して再接続します。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

デバイス画面上の Amazon ロゴ。それ以上のアクティビティはありません。

この問題のトラブルシューティングを行うには、以下を実行します。

- デバイスを再起動する場合は、しばらく (30 秒未満) 待ちます。
- 電源から USB ハブを取り外し、再接続します。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

一時的に使用不可

この問題のトラブルシューティングを行うには、以下を実行します。

- ホストデバイス/システムとの USB 接続が安全であることを確認します。
- USB ハブに入るすべてのケーブルを切断して再接続します。
- 問題が解決しない場合は、AWS Support までお問い合わせください。

問題が発生しました

これは、内部エラーがある場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

1. デバイスをシャットダウンします。
2. 電源から切断します。
3. 30 秒待ちます。

4. デバイスを電源に差し込みます。
5. デバイスの電源をオンにします。
6. 問題が解決しない場合は、AWS Support までお問い合わせください。

一時的なサービス停止

これは、デバイスが Amazon One によってサービスから移動された場合に発生します。

この問題のトラブルシューティングを行うには、以下を実行します。

- AWS サポートにお問い合わせください。

Amazon One デバイスに物理的な損傷がある

この問題のトラブルシューティングを行うには、以下を実行します。

- 次のステップについては、AWS サポートに連絡し、発生した内容、発生した日時、発生した理由など、できるだけ多くの詳細を提供します。

アダルトを読み取れない

この問題のトラブルシューティングを行うには、以下を実行します。

- Amazon One デバイスに線や汚れがないことを再度確認します。
- お客様のアロップルに包帯、アロップル、および大量の土や土壌などの遮蔽物がないことを確認します。
- 問題が解決せず、デバイスが潮汐を読み取らない場合は、AWS サポートにお問い合わせください。

手掌が認識されない

この問題のトラブルシューティングを行うには、以下を実行します。

- お客様に、他の のシボを試してもらいます。
- 顧客が既に登録されていることを確認します。そうでない場合は、オンラインまたはデバイスで登録してもらいます。

- 問題が解決せず、デバイスが挨拶の問い合わせを読み取らない場合は、AWS サポートにお問い合わせください。

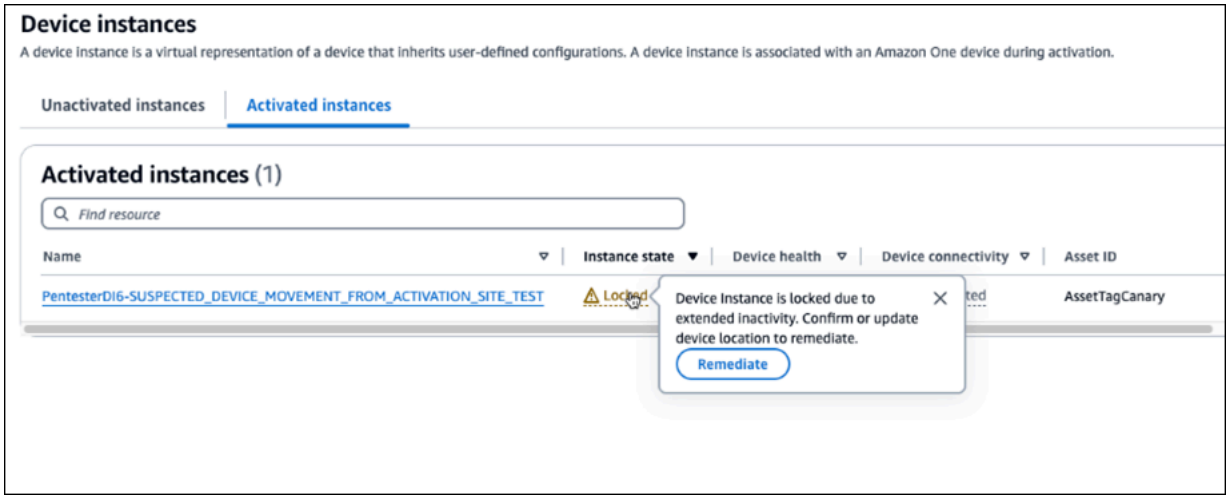
非アクティブが長引いたためデバイスがロックされました

デバイスがアクティベーションサイトから移動されたと疑うと、ユーザーはロックアウトされます。これは、デバイスが最大 120 時間のオフライン時間を超えた場合に発生します。

デバイスのロックを解除するには、以下を実行します。

1. AWS コンソールにログインし、デバイスインスタンスを選択します。
2. ページ上部のエラーバナーから、修正を選択します。

   オプション: アクティブ化されたインスタンスから、ロック済みを選択し、修復を選択します。



3. デバイスが元のアクティベーションサイトにまだある場合は、はい、デバイスはこのサイトにありますを選択します。
4. デバイスが別のサイトにある場合は、いいえを選択します。デバイスは別のサイトにあります。No を選択すると、デバイスは非アクティブ化されます。新しいサイトでデバイスをアクティブ化します。

改ざんイベントによりデバイスがロックされました

セキュリティ上の理由から、改ざんイベントが発生した場合、Amazon One デバイスはロックされます。

この問題のトラブルシューティングを行うには、以下を実行します。

- AWS サポートにお問い合わせください。

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	サービスにリンクされたロールセクションを追加	2025 年 2 月 4 日
更新	追加: シナリオ駆動型コンテンツ	2024 年 10 月 10 日
更新	トピックの追加: Amazon One Enterprise コンソールのトラブルシューティング	2024 年 10 月 10 日
更新	トピックの追加: Amazon One Enterprise デバイスのトラブルシューティング	2024 年 10 月 10 日
更新	章を追加: Amazon One Enterprise のセットアップ	2024 年 10 月 10 日
更新	トピックの追加: Amazon One Enterprise デバイスのメンテナンスとクリーニング	2024 年 10 月 10 日
更新	再編成されたコンテンツ	2024 年 10 月 10 日
更新	トピックの追加: 安全なアクセスのための Amazon One Enterprise デバイス I/O ハブのインストール	2024 年 8 月 14 日
更新	追加されたトピック: 壁面マウント可能な Amazon One Enterprise デバイスのインストール	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。