aws

ユーザーガイド

Amazon One

Amazon One: ユーザーガイド

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 14
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
壁面取り付け可能な 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 デバイス I/O ハブのインストール 28
Amazon One デバイスのアクティブ化 33
ユーザーの登録と入力 35
エンドポイントポリシーの作成 35
エントリの認証 35
ユーザーの管理 36

登録済みユーザーの表示 36
登録されたユーザーとその生体認証の削除 36
Amazon One デバイスの管理 38
Amazon One デバイスのメンテナンスとクリーニング 38
Amazon One デバイスをクリーンアップするには 39
サイト管理 39
サイト名の変更 40
サイトアドレスの更新 40
デバイスインスタンス管理 41
デバイスインスタンスのステータスの表示 41
Amazon One デバイスの再起動 41
Amazon One デバイス設定の更新 42
Wi-Fi 認証情報の更新 42
デバイスインスタンスの非アクティブ化 43
セキュリティ 44
データ保護 44
保管中のデータのデフォルトの暗号化を使用するには 45
転送中のデータの暗号化 46
ID とアクセス管理 46
オーディエンス 46
アイデンティティを使用した認証 47
ポリシーを使用したアクセスの管理 48
Amazon One Enterprise と IAM の連携方法 50
アイデンティティベースのポリシーの例 56
AWS マネージドポリシー 63
アクション、リソース、および条件キー 67
アクション 67
リソースタイプ: 72
条件キー 73
コンプライアンス検証 73
モニタリング 74
イベントのモニタリング 74
Amazon One Enterprise イベントをサブスクライブする 74
デバイスステータス変更イベントタイプ 76
ユーザープロファイルイベントタイプ 77
イベント例 78

デバイスのヘルスステータスが正常に変更されました 79
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 80
デバイス接続がオンラインに変更されました 81
デバイス接続がオフラインに変更されました 82
CloudTrail ログ 83
CloudTrail の Amazon One Enterprise 情報 83
Amazon One Enterprise ログファイルエントリについて 84
トラブルシューティング 87
ID とアクセスのトラブルシューティング 87
Amazon One でアクションを実行する権限がない 87
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 88
Amazon One コンソールのトラブルシューティング 88
サイトを作成できない 89
デバイスインスタンスを作成できない 89
設定テンプレートを作成できない 89
アクティベーション QR コードを作成できない 89
Amazon One デバイスのトラブルシューティング 89
空白画面 90
Wi-Fi またはネットワークに接続できない 91
アクティブなアラートでデバイスを再起動する 91
システムエラー 91
QR コードが認識されない 92
QR コードを読み取れない 92
複数の QR コードが検出されました 92
デバイスインスタンスが存在しません 92
サイトが見つかりません 93
郵便番号が一致しません 93
ゲートウェイがタイムアウトしました 93
デバイスを設定できない 93
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 94
デバイス画面の Amazon ロゴ。それ以上のアクティビティはありません。 94
一時的に使用不可 94
問題が発生しました 94
一時的なサービス停止 95
Amazon One デバイスに物理的な損傷がある 95

アダルトを読み取れない 95
手掌が認識されない 95
長時間の非アクティブが原因でロックされたデバイス 96
改ざんイベントによりデバイスがロックされました 96
ドキュメント履歴 97
..... xcix

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提供する新しい手掌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、Amazon One Enterprise 向けに設計されています。Amazon One Enterprise 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な、スクリプティングベースの ID サービスです。次のデバイス仕様に注意してください。

- ユーザー入力 — 手のひら生体認証、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 にはコンソールが含まれており、次の方法で使用できます。

- 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。このサイトは、Amazon One Enterprise デバイスとユーザープロファイルのモニタリングと管理中にチームが実行するタスクの物理的な場所に似ています。IT または施設マネージャーのタスクには以下が含まれます。
  - 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て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の AWS アカウントでデバイスをアクティブ化して登録できます。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 コンソールは、デバイスの追跡や毎月の請求書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管理の物理的な建物。サイトは、Amazon One デバイスの施設、ネットワーク、電源の要件を満たしている必要があります。
- デバイス — 認証用の Amazon One アプライド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
  - Active
- 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、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「Enable a virtual MFA device for your AWS account root user (console)」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 アカウントを保護したので、管理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

管理者権限を持つユーザーを作成したら、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して、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 コードを取得するのみのインストーラである場合があります。

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、ユーザータイプに適したサインイン手順に従い AWS 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 は限られています。詳細については、「IAM および AWS STS クォータ」を参照してください。ユーザー名は、最大 64 文字、数字、およびプラス記号 (+)、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。「 へのユーザーアクセスを提供する — AWS マネジメントコンソール オプション」を選択します。
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が開き、カスタマイズしてユーザーに送信できるドラフトが表示されます。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、正しいアカウント ID 番号またはアカウントエイリアスを置き換えます。

    ```
    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 マネジメントコンソール、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. 「物理アドレス」に、Amazon One デバイスをインストールするサイトのアドレスを入力します。
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、新しいタグの追加を選択します。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ら、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、新しいタグの追加を選択します。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、新しいタグの追加を選択します。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、新しいタグの追加を選択します。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。

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、次の 2 つの入力方法のいずれかを選択します。

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

    テンプレートの作成オプションについては、「」を参照してください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、新しいタグの追加を選択します。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、新しいタグの追加を選択します。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. 非アクティブインスタンステーブルで、インスタンスの状態は と表示されます 

。

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

8. サイトを選択するドロップダウンリストから、サイトを選択します。

9. サイト情報で、サイトアドレスを検証します。

10. アクティベーション QR コードでは、各デバイスインスタンスには対応する QR コードがあります。QR コードの取得 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後、次のステップでは、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領域に物理的に配置し、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 マネジメントコンソール 、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
- 壁面取り付け可能な 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 デバイス I/O ハブのインストール
- 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、物理的に制御できるドアがある企業またはビジネスの任意の場所にインストールできます。

コントロールパネルの要件

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

- OSDP (v1 および v2)
- Wiegand

ネットワーク要件

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

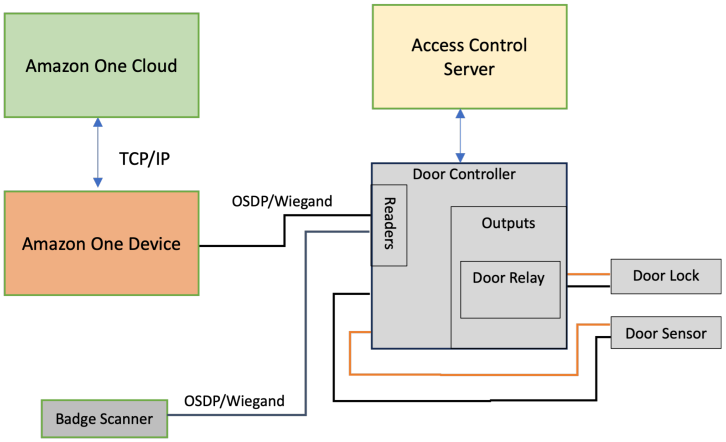
電力要件

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

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

インストールの概念を理解する

構築アクセスを適切に保護するために、Amazon One 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手掌認識デバイスです。
- 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、セキュアエリアへのユーザーのアクセス権を制御します。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。
  - 認証が成功すると、Amazon One デバイスはユーザーのバッジ ID をドアコントローラーに送信します。
  - ドアコントローラーは決定で応答し、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、アタッチプロファイルに関連付けます。

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、アクセスポイントをブロックし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、通常の使用中の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 不正開封防止ネジを回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. ペデスタルのベースから 2 インチ上のイーサネットケーブルにフェライトループをインストールします。
8. アクセスコントロールパネル (またはバッジリーダー) から台座に RS485 シリアルケーブルをフィードします。長さは 1 フィート超過します。
9. 台座のベースから 2 インチ上の RS485 ケーブルにフェライトループを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ねじって固定します。

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。

壁面取り付け可能な 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システムです。高度な手掌認識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、オフィスの入口などの交通量の多い場所に最適です。

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、壁掛け可能な 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。

壁面取り付け可能な 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。

- 屋内専用: ウォールマウント可能な Amazon One デバイスは屋内専用であるため、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: デバイスの適切な配置と機能を確保するために、壁は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、設置後に地面から 44～46 インチ以内に配置し、ユーザーのアクセスを容易にします。
- ケーブル管理: 損傷や乱雑さを防ぐために、余分なケーブルはすべて壁取り付けの背後でルーティングされ、しっかりと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 電源入力を使用する場合は、NEC クラス 2 または電力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石積みドリルビット
- 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 マイナスドライバー
- T12 Secure Torx ドライバー
- 鉛筆
- レベル

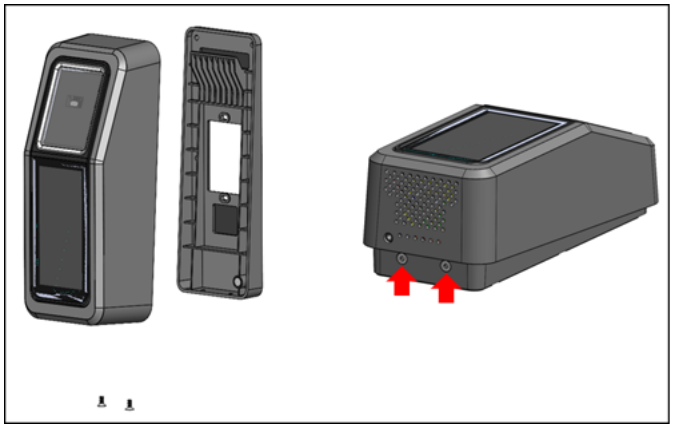
ウォールマウント可能な Amazon One デバイスに付属

- 6x #8 ドライウォールアンカー
- 6x #8-32 1 インチ長ネジ
- 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 マイナスねじ

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、壁面取り付け可能な 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

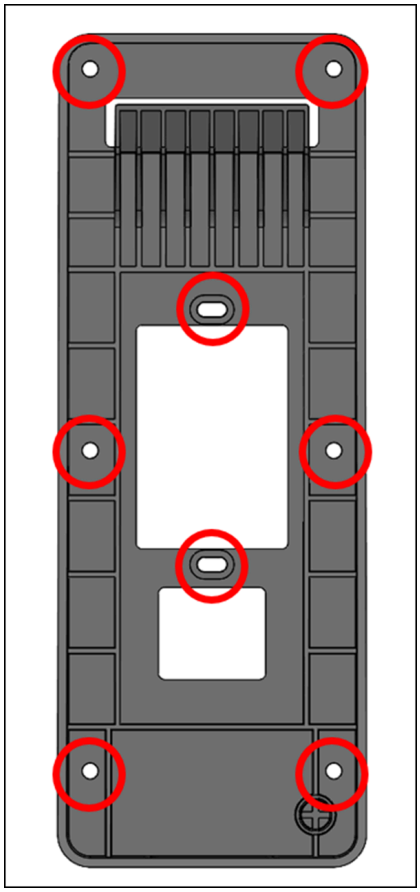
1. Amazon One デバイスをパッケージから削除します。
2. 下部の 2 つの Torx セキュリティネジを取り外して、マウントプレートを Amazon One デバイスから分離します。



3. マウントプレートを希望する場所の壁に配置します。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 機械ねじを楕円穴に挿入して、プレートをギャングボックスに緩くマウントします。
   - 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、楕円穴と #6-32 ねじを使用できます。壁板を取り付ける主な手段として、#6-32 ネジの位置を使用しないでください。



4. スタッコ、ドライウォール、レンガ、またはコンクリートの表面にマウントする場合は、マークされた各場所に 1/4 インチ穴をあけてから、アンカーが壁と重なるまで穴に押し込んで壁アンカーを取り付けます。

   木の表面にマウントする場合、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. すべての留め金を配置したら、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 (製造 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確認するには、次の図と接続表を参照してください。

   信号の詳細な電気特性については、「配線手順」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
3	LED	Wiegand LED	Wiegand LED – オプション
4	D1	Wiegand D1	Wiegand データ 1 – ホワイトワイヤ
5	D0	Wiegand D0	Wiegand データ 0 – グリーンワイヤ

ピン	接続	説明	使用アイテム
6	RTN	シグナルリターン	Wiegand Ground – ブラックワイヤ
7	通信	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	コンタクトリレーが通常閉じている — オレンジ色のワイヤ
9	いいえ	リレー通常開	コンタクトリレー通常開 — 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 – グリーンワイヤ

2. ワイヤを取り付けるときは、ワイヤの端から 3 mm ~ 5 mm 離します。
3. ワイヤのストリッピングされた端を目的のターミナル位置に挿入します。
4. マイナスドライバーを使用して、ターミナル保持ネジを時計回りに回して、ワイヤーが固定されるまで固定します。締めすぎないでください。
5. 滑らかにした後、ワイヤーを滑らかに引いて、ワイヤーが固定されていることを確認します。
6. 必要な接続を行ったら、Amazon One デバイスターミナルブロックの対応するソケットにプラグを挿入します。
7. Cat6 イーサネットケーブルを RJ45 ジャックに挿入します。

8. 壁板のフックがデバイスの背面の開口部にスライドするように Amazon One デバイスを配置します。
9. ケーブルがデバイスとマウントプレートの間に挟まれていないことを確認し、デバイスをピボットして所定の位置に固定します。
10. 2 つの Torx Security M4x10 マイナスねじを使用して、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。締めすぎないでください。

壁面取り付け可能な 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 オームの抵抗終了を有効にします。

RS485 接続

- 黒いワイヤをピン 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

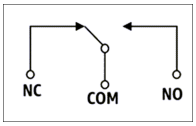
ピン	接続	説明	使用アイテム
10	RTN	シグナルリターン	地上
11	A	RS485_A/D1/クロック	RS485 非反転信号
12	B	RS485_B/D0/データ	RS485 反転信号

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	コンタクトリレーが通常閉じている — オレンジ色のワイヤ	
9	いいえ	リレーは通常開いている	コンタクトリレー通常開 — 黄色のワイヤ	



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

デジタル入出力接続

- 青いワイヤをピン 1 (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)	
2	GPI	汎用入力	デジタル入力信号 (3.6V – 5V)	

- デジタル入出力接続は、リストされているとおりに動作する必要があります。

Amazon One デバイスを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 デバイス I/O ハブのインストール

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、生体認証の手掌認識を活用して、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、その他のアクセス管理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、安全で安全で効果的なセットアップを確保するために、次の条件が満たされていることを確認してください。

- 屋内専用: I/O Hub を備えた Amazon One デバイスは、屋内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 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、NEC クラス 2 または電力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 マイナスドライバー

I/O Hub を備えた Amazon One デバイスに含まれる

- 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" 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続行して、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。適切な準備を行うと、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

- 液体が誤ってコードを下りて I/O ハブに流れ込まないように、ドローブループをインストールします。
- 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、ストレインレリーフ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。次のワイヤリングテーブル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 – グリーンワイヤ
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 – グリーンワイヤ
8	A	RS485_A/D1/クロック	OSDP D1 – ホワイトワイヤ

ピン	接続	説明	使用アイテム	
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	コンタクトリレーが通常閉じている — オレンジ色のワイヤ	
12	いいえ	リレー通常開	コンタクトリレー通常開 — 黄色のワイヤ	

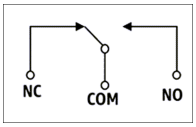
Wiegand 接続

- 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、指定された安全定格 30VAC/60VAC、最大 60W に従って動作する必要があります。

RS485 接続

- 緑色のワイヤをピン 7 (B) に挿入します。
- ピン 8 (A) に白いワイヤを挿入します。
- 黒いワイヤをピン 9 (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 オームの抵抗終了を有効にします。

デジタル入出力接続

- 黒いワイヤをピン 5 (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操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 ワイヤのストリッピングされた端を 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 デバイスをインストールして電源をオンにすると、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. イーサネットまたは Wifi を選択してインターネットに接続します。

   デバイスがインターネットに接続するとすぐに、最新のソフトウェアパッケージのダウンロードが開始されます。
3. 画面にソフトウェアのダウンロードが完了したことが表示されたら、OK を選択します。
4. QR コードを選択します。

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

   > **Note**
   >
   > Amazon One Enterprise コンソールでアクティベーション QR コードにのみアクセスできるように、インストーラ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. サイトを選択するドロップダウンリストから、Amazon One デバイスがインストールされているサイトを選択します。
8. サイト情報で、サイトアドレスを確認します。
9. アクティベーション QR コードで、アクティブ化するデバイスインスタンス名を探し、対応する QR コードを取得を選択して QR コードを取得します。
10. Amazon One デバイスで QR コードをスキャンします。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 デバイス画面が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、従業員は手掌の登録を開始し、手掌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

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

Amazon One デバイスにヤ二を登録するには

1. Amazon One Enterprise 登録デバイスで、開始する 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 デバイス画面にはスキャンされたバッジが表示されます。
3. 利用規約を読み、OK を押します。
4. 「同意」を読み、同意する場合は「同意する」を押します。
5. 画面の指示に従って、登録プロセスを完了します。

エントリの認証

手掌が正常に登録されると、Amazon One Enterprise エントリデバイスで手掌を使用して認証する準備が整います。

Amazon One デバイスでエントリのアプライドを認証するには

- デバイスの上部にキャラクターの上にカーソルを合わせ、画面の指示に従ってキャラクターをスキャンします。

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、ユーザーの生体認証を削除できます。関連付けられた生体認証が削除されたユーザーは、認証のために Amazon One デバイスにアクセスできなくなります。

トピック

- 登録済みユーザーの表示
- 登録された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 Kubernetes 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。

登録された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。

登録されたユーザーとその生体認証を削除するには

1. https://console.aws.amazon.com/one-enterprise で Amazon One Enterprise コンソールを開きます。
2. ナビゲーションペインで、登録済みユーザー管理を選択します。

3. 登録済みユーザー で、アプライド生体認証データを削除するユーザーのバッジ ID を選択します。
4. 生体認証の削除を選択します。
5. 削除を選択して、ユーザーの生体認証データの削除を確認します。

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

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 デバイスのメンテナンスは、最適なデバイスの運用環境とデバイスエクスペリエンスを提供します。

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は、問題を管理者にエスカレーションします (この問題が発生すると、エラー画面が Amazon One デバイスに表示されます) 。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ことを確認します。
- デバイスのすべての側面を検査し、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を調べて、Amazon One デバイスの内部コンポーネント/回路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 デバイスのクリーニングにより、フィンガープリントやハンドプリントなどの汚れやマークが定期的に削除されます。

> **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、またはデバイスにダート、埃、またはスマッジが表示されているが、1 日に 1 回以下です。

1. Amazon One デバイスを Iso™ Alcohol (IPA) Wipes でワイプします。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、光学ウィンドウに触れたり、他のクリーニング製品を使用しないでください。
2. しわは、ドライなマイクロファイバー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埃やゴミを軽く埃にします (ワイプしないでください)。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汚れている場合 (指/手の印刷/汚れなど) 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、新しい顧客から誤って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、またはデバイスに汚れ、ほこり、または汚れ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、同じ物理アドレスを共有する 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. 更新する変更を保存するを選択します。

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. 「物理アドレス」に正しい物理アドレスを入力します。
8. 更新する変更を保存するを選択します。

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には、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. 再起動を選択して Amazon One デバイスを再起動します。

Amazon One デバイス設定の更新

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)。その後、デバイスのアクティベーションプロセスを実行できます (「」を参照Amazon One 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. Network で、Edit を選択します。
5. Wi-Fi 設定で、必要な変更を加えます。

6. 更新ネットワーク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

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

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルではこれをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、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、当社のセキュリティの有効性を定期的にテストおよび検証。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

責任 AWS 共有モデル、Amazon One Enterprise でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。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 アイデンティティセンターまたは 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 は必須ですが、TLS 1.3 を推奨します。
- 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 所有のキー — Amazon One Enterprise は、デフォルトでこれらのキーを使用して、機密性の高いエンドユーザーデータを自動的に暗号化します。AWS 所有のキーを表示、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 所有のキー」を参照してください。

転送中のデータの暗号化

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

Amazon One Enterprise の Identity and Access Management

AWS Identity and Access Management (IAM) は、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 リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- 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

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「Amazon One の ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「Amazon One Enterprise と IAM の連携方法」を参照)

- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「Amazon One Enterprise のアイデンティティベースのポリシーの例」を参照)

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。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」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、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスとして、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 にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの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。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスすることを人間 AWS のユーザーに要求する」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。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を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 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 ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。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。

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 AWS には、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、アイデンティティまたはリソースに関連付けられたときにアクセス許可を定義します。は、プリンシパル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。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、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

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のポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。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、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。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。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。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。

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。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。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 (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。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」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。

- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。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アクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか 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 機能を確認してください。

Amazon One Enterprise で使用できる IAM 機能

IAM 機能	Amazon One Enterprise のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
プリンシパルアクセス権限	あり
サービスロール	いいえ

IAM 機能	Amazon One Enterprise のサポート
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については、「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、ユーザーグループ、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。

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

Amazon One Enterprise 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する 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コントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、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、全体のアカウント、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。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。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を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

Amazon One Enterprise のポリシーリソース

ポリシーリソースのサポート: あり

管理者は 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。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。リソースレベルのアクセス許可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を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

Amazon One Enterprise のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は 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` 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。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。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 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を表示するには、「」を参照してくださいAmazon One Enterprise のアイデンティティベースのポリシーの例。

Amazon One Enterprise 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アクセス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、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

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

一時的な認証情報は AWS 、リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。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 ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」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アクセス許可

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (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 へのリクエストをリクエストする を使用します。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 が指示する場合にのみ、サービスロールを編集します。

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。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。

これらのサンプルの 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、アカウント内で誰かが Amazon One Enterprise リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。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の付与を開始するには、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することで、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 ポリシーでアクセス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。たとえば、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 を通じて使用されている場合に 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 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 アクセスアナライザー 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 アクセスアナライザー 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、MFA をオンにしてセキュリティを強化します。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AmazonOneEnterpriseReadOnlyAccessを許可する AWS マネージドポリシーを示しています。

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。アクションの前に が付きconfig:、Amazon One Enterprise アクションを参照していることを示します。次の例に示すように、* ワイルドカード文字を Action 要素で使用できます。

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

  これにより、DeviceInstance」 (GetDeviceInstanceConfiguration、) で終わるすべての Amazon One Enterprise アクションが許可されますCreateDeviceInstanceConfiguration。
- "Action": ["one:*"]

  これにより、すべての Amazon One Enterprise アクションが許可されますが、他の 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 管理者として機能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。

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

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

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

API アクション	リソース
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。

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。

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

追加情報

IAM ユーザー、グループ、ポリシー、アクセス許可の作成の詳細については、「IAM ユーザーガイド」の「最初の IAM ユーザーと管理者グループの作成」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、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るように、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 マネージド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 が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

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

JSON

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

AmazonOneEnterpriseReadOnlyAccess

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

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

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

JSON

```
{
 "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ようにする、制限付きの読み取りおよび書き込みアクセス許可を付与します。

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

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

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

one:GetSiteAddress Amazon One Enterprise サイトの物理アドレスを取得できます。

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。

JSON

```
{
 "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アラートについては、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 が AmazonOneMetricPublishAccess を追加	AmazonOneMetricPublishAccess という名前のロールアクセス許可ポリシーにより、Amazon One Enterprise は CloudWatch 名	2025 年 2 月 6 日

変更	説明	日付
	前空間 AWS/AmazonOne で CloudWatch:PutMetricData を実行できます。	
Amazon One Enterprise が変更の追跡を開始しました	Amazon One Enterprise は、AWS 管理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アクセス許可を付与する	読み取り	デバイスインスタンス*		
ListDeviceInstances	デバイスインスタンスを一覧表示するアクセス許可を付与する	読み取り			

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
UpdateDeviceInstance	デバイスインスタンスを更新するアクセス許可を付与する	書き込み	デバイスインスタンス*		
DeleteDeviceInstance	デバイスインスタンスを削除するアクセス許可を付与する	書き込み	デバイスインスタンス*		
CreateDeviceActivationQrCode	デバイスインスタンスでデバイスをアクティブ化するための QR コードを作成するアクセス許可を付与します	書き込み	デバイスインスタンス*		
DeleteAssociatedDevice	デバイスとデバイスインスタンス間の関連付けを削除する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*		
RebootDevice	デバイスを再起動するアクセス許可を付与する	書き込み	デバイスインスタンス*		
CreateDeviceInstanceConfiguration	デバイスインスタンス設定を作成するアクセス許可を付与する	書き込み			
GetDeviceInstanceConfiguration	デバイスインスタンス設定に関する情報を取得するアクセス許可を付与する	読み取り	設定*		

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
CreateSite	サイトを作成するアクセス許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	デバイスインスタンスを削除するアクセス許可を付与する	書き込み	サイト*		
GetSite	サイトに関する情報を取得するアクセス許可を付与する	読み取り	サイト*		
ListSites	サイトを一覧表示するアクセス許可を付与する	読み取り			
GetSiteAddress	サイトアドレスに関する情報を取得するアクセス許可を付与する	読み取り	サイト*		
UpdateSite	サイトを更新するアクセス許可を付与する	書き込み	サイト*		
UpdateSiteAddress	サイトアドレスを更新するアクセス許可を付与する	書き込み	サイト*		
CreateDeviceConfigurationTemplate	デバイスインスタンスを作成するアクセス許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

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
DeleteDeviceConfigurationTemplate	デバイス設定テンプレートを削除するアクセス許可を付与する	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アクセス許可を付与する	読み取り	device-configuration-template*		
ListDeviceConfigurationTemplates	デバイス設定テンプレートを一覧表示するアクセス許可を付与する	読み取り			
UpdateDeviceConfigurationTemplate	デバイス設定テンプレートを更新するアクセス許可を付与する	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	

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
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	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
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 プログラムによるスコープ」の「コンプライアンス」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」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。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

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、パフォーマンスを維持する上で重要な部分です。 には、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の以下のモニタリングツール AWS が用意されています。

- Amazon EventBridge を使用して 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。呼び出し元のユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、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」を参照してください。

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して、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データのストリームを配信できます。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して 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. [ルールを作成] 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 Events を選択します。
9. 作成メソッドで、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 detail-type 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",
"New Alert(s) Detected",
"Some Alert(s) Cleared"]
}
```

    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. [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。

たとえば、誰かがいつクロックインするかを表示するには、「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できます。

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。

一部のアラート (複数可) がクリアされました

デバイスが 1 つ以上のヘルスチェックに合格しました。

新しいアラート (複数可) が検出されました

デバイスが 1 つ以上のヘルスチェックに失敗しました。

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。

data

clearedAlerts

- deviceInstance が以前に失敗したヘルスチェックを表します。
- アラートのタイプと reportedAt タイムスタンプの statusCode で構成されます。
- statusCode の可能な値: NetworkDisconnected、USBDisconnected

currentAlerts

- deviceInstance の現在のステータスを表します。
- アラートのタイプと reportedAt タイムスタンプの statusCode で構成されます。

- statusCode の可能な値: NetworkDisconnected、USBDisconnected

newAlerts

- deviceInstance の新しく失敗したヘルスチェックを表します。
- アラートのタイプと reportedAt タイムスタンプの statusCode で構成されます。
- statusCode の可能な値: NetworkDisconnected、USBDisconnected

currentAlertsCount

- deviceInstance で現在失敗しているヘルスチェックの数。

assetTagId

- deviceInstance に関連付けられたデバイスの assetTagId。

deviceInstanceName

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

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。

ユーザープロファイルイベントタイプ

ユーザープロファイル関連のイベントの詳細タイプは次のとおりです。

新しい正常な登録

ユーザーが正常に登録されたとき。

新しい正常な登録解除

ユーザーが正常に登録解除されたとき。

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

ユーザーが手掌をスキャンして認証に成功したとき。

失敗した認識

パルミネーション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。

data

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

- イベントの作成時刻。

userStatus

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

associatedId

- バッジ ID など、ユーザーの関連付けられた ID。

理由

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

イベント例

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

トピック

- デバイスのヘルスステータスが正常に変更されました
- デバイスのヘルスステータスが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チェックに合格しました。


```
{
        "version": "0",
        "id": "51e022b4-7ce6-34e0-264b-370948fc1123",
        "detail-type": "Some Alert(s) Cleared",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T19:32:42Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/F5JRte5Jz21Tqx"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "clearedAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:32:42 UTC 2025"
                    }
                ],
                "currentAlerts":
                [],
                "currentAlertsCount": 0,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
```

```
            }
        }
    }
```

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ました。

```
{
        "version": "0",
        "id": "07af4893-ef9f-965a-d245-3f0c8bd3c123",
        "detail-type": "New Alert(s) Detected",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T19:26:58Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "newAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
                    }
                ],
                "currentAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
                    }
                ],
                "currentAlertsCount": 1,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
```

```
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
    }
```

デバイス接続がオンラインに変更されました

これで、デバイスはインターネットに接続されました。

```
{
        "version": "0",
        "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
        "detail-type": "Some Alert(s) Cleared",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T18:28:23Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "clearedAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlerts":
                [],
                "currentAlertsCount": 0,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
    }
```

デバイス接続がオフラインに変更されました

デバイスはインターネットに接続されなくなりました。


```
{
        "version": "0",
        "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
        "detail-type": "New Alert(s) Detected",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T18:28:23Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "newAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlertsCount": 1,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
      }
```

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

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。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。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、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、「」に記載されています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、任意の出典からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

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 アプリケーションまたは 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、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 ID 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 ID 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ない
- 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ない

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 アプリケーションまたは 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、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ない

- 設定テンプレートを作成できない
- 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。

設定テンプレートを作成できない

- 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。

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、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、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
- デバイス画面の Amazon 口ゴ。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
- 長時間の非アクティブが原因でロックされたデバイス
- 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。
- 電源コードが電源コンセントと Amazon One デバイスの背面の両方にしっかりと接続されているかどうかを確認します。また、コードが損傷してい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 および 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 ハブを電源から抜き、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、オペレーションはデバイスがコマンドを受信し、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再起動を試行するまで最大 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 1 つの有効な QR コードをスキャンします。

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。
- 正しいサイトの郵便番号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、 オペレーションが設定をデバイスディスクに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、電源から USB ハブを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. デバイスの電源を入れます。
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、何が起こったか、いつ起こったか、なぜ起こったかなど、できるだけ多くの詳細を記載してください。

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確認します。
- 顧客の手榴弾に包帯、手榴弾、大量の土や皮などの遮蔽物がないことを確認します。
- 問題が解決せず、デバイスが手榴弾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、デバイスがアプライドコンタクト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。

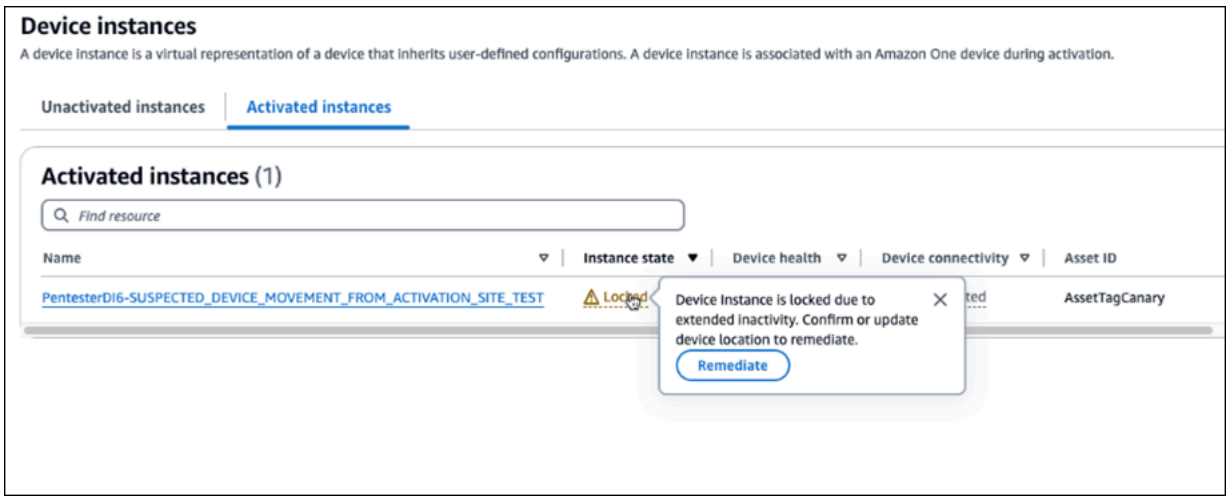
長時間の非アクティブが原因でロックされたデバイス

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、修復を選択します。

   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	章の追加: 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 Hub のインストール	2024 年 8 月 14 日
更新	追加されたトピック: ウォールマウント可能な 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。