ユーザーガイド

AWS サインイン

AWS サインイン: ユーザーガイド

Table of Contents

AWS サインインとは

このガイドは、ユーザーのタイプに応じて、Amazon Web Services (AWS) にサインインするさまざまな方法を理解するのに役立ちます。ユーザータイプとアクセスする AWS リソースに基づいてサインインする方法の詳細については、次のいずれかのチュートリアルを参照してください。

- にサインインする AWS マネジメントコンソール
- AWS アクセスポータルにサインインする
- フェデレーティッドアイデンティティとしてのサインイン
- を使用してサインインする AWS Command Line Interface
- でサインインする AWS ビルダー ID

へのサインインに問題がある場合は AWS アカウント、「」を参照してくださいサインインに関する問題 AWS アカウント のトラブルシューティング。のヘルプについては、 AWS ビルダー ID 「」を参照してくださいAWS Builder ID の問題のトラブルシューティング。を作成する AWS アカウント 場合 にサインアップします AWS。へのサインアップ AWS がユーザーまたは組織にどのように役立つかの詳細については、「お問い合わせ」を参照してください。

トピック

- 用語
- AWS サインインのリージョンの可用性
- サインインイベントのログ記録
- ユーザータイプを決定する
- サインイン URL を決定する
- 許可リストに追加するドメイン
- AWS アカウント 管理者向けのセキュリティのベストプラクティス

用語

Amazon Web Services (AWS) では、一般的な用語を使用してサインインプロセスを説明しています。これらの用語を読んで理解することをお勧めします。

管理者

AWS アカウント 管理者または IAM 管理者とも呼ばれます。管理者 (通常は情報技術 (IT) 担当者) は、 AWS アカウントを監督するユーザーです。管理者は、組織の他のメンバーよりも AWS アカウント に対して高いレベルの権限を持っています。管理者は、 の設定を確立して実装します AWS アカウント。また、IAM または IAM アイデンティティセンターのユーザーを作成します。管理者はこれらのユーザーにアクセス認証情報と AWSにサインイン用のサインイン URL を提供します。

アカウント

標準 AWS アカウント には、 AWS リソースと、それらのリソースにアクセスできる ID の両方が含まれます。アカウントは、アカウント所有者の E メールアドレスとパスワードに関連付けられます。

認証情報

アクセス認証情報またはセキュリティ認証情報とも呼ばれます。認証および認可を実行する際にシステムは、誰が呼び出しをしているかを特定し、リクエストされたアクセスを許可するかどうかを決定するために認証情報を使用します。認証情報は、ユーザーがサインインして AWS リソースにアクセス AWS するために に提供する情報です。人間のユーザーの認証情報には、メールアドレス、ユーザー名、ユーザー定義のパスワード、アカウント ID またはエイリアス、検証コード、および単回使用の多要素認証 (MFA) コードが含まれます。プログラムによるアクセスには、アクセスキーを使用することもできます。可能な場合は、短期のアクセスキーの使用をお勧めします。

認証情報の詳細については、「AWS セキュリティ認証情報」を参照してください。

> **Note**
>
> ユーザーが送信しなければならない認証情報の種類は、ユーザータイプによって異なります。

企業認証情報

ユーザーが企業ネットワークやリソースにアクセスする際に提供する認証情報。社内管理者は、社内ネットワークとリソースへのアクセスに使用するのと同じ認証情報 AWS アカウント を使用するように を設定できます。これらの認証情報は、管理者またはヘルプデスクの従業員から提供されます。

プロファイル

Builder ID AWS にサインアップすると、プロファイルが作成されます。プロファイルには、指定した連絡先情報、多要素認証 (MFA) デバイスとアクティブなセッションを管理する機能が含まれます。また、プライバシーやデータの取り扱い方法については、プロフィールをご覧ください。プロフィールとそれがどのように AWS アカウントと関連しているかについての詳細は、「AWS ビルダー ID およびその他の AWS 認証情報」を参照してください。

ルートユーザーの認証情報

ルートユーザーの認証情報は、 AWS アカウントの作成に使用したメールアドレスとパスワードです。セキュリティを強化するために、ルートユーザーの認証情報に MFA を追加することを強くお勧めします。ルートユーザー認証情報は、アカウント内の全ての AWS サービスとリソースへの完全なアクセス権を提供します。 ルートユーザー の詳細については、「ルートユーザー」を参照してください。

ユーザー

ユーザーは、製品への API コール AWS や AWS リソースへのアクセス権限を持つユーザーまたはアプリケーションです。各ユーザーには、他のユーザーと共有されない一連の固有のセキュリティ認証情報があります。これらの認証情報は、 AWS アカウントのセキュリティ認証情報とは異なります。詳細については、「ユーザータイプを決定する」を参照してください。

検証コード

認証コードは、多要素認証 (MFA) を使用してサインインプロセス中にユーザーアイデンティティを確認します。認証コードの配信方法はさまざまです。テキストメッセージまたは E メールで送信できます。詳細については、管理者に確認してください。

AWS サインインのリージョンの可用性

AWS サインインは、一般的に使用されるいくつかの で使用できます AWS リージョン。この可用性により、 AWS サービスやビジネスアプリケーションに簡単にアクセスできます。サインインがサポートするリージョンの完全なリストについては、「AWS サインインエンドポイントとクォータ」を参照してください。

サインインイベントのログ記録

CloudTrail は で自動的に有効 AWS アカウント になり、アクティビティが発生したときにイベントを記録します。以下のリソースは、サインインイベントのログ記録とモニタリングの詳細を学習するのに役立ちます。

- CloudTrail ログは へのサインインを試みます AWS マネジメントコンソール。すべての IAM ユーザー、ルートユーザー、フェデレーションユーザーのサインインイベントは、CloudTrail ログファイルに記録を生成します。詳細については、「AWS CloudTrail ユーザーガイド」の「AWS マネジメントコンソール サインインイベント」を参照してください。
- リージョンエンドポイントを使用して にサインインすると AWS マネジメントコンソール、CloudTrail はエンドポイントの適切なリージョンに`ConsoleLogin`イベントを記録します。AWS サインインエンドポイントの詳細については、 AWS 全般のリファレンスガイドAWS の「サインインエンドポイントとクォータ」を参照してください。
- CloudTrail が IAM Identity Center のサインインイベントを記録する方法の詳細については、「IAM Identity Center ユーザーガイド」の「IAM Identity Center サインインイベントを理解する」を参照してください。
- CloudTrail が IAM でさまざまなユーザー ID 情報をログに記録する方法の詳細については、AWS Identity and Access Management 「 ユーザーガイド」の「 を使用した IAM および AWS STS API 呼び出しのログ記録 AWS CloudTrail」を参照してください。

AWS サインインは、ネットワークの場所とプリンシパル ID に基づいてコンソールアクセスを制限できるリソースベースのポリシーとリソースコントロールポリシーをサポートしています。ルートユーザーの場合、パスワードプロンプトが表示される前にネットワークの場所が検証されます。すべてのプリンシパルタイプについて、ポリシーは認証前と認証後に評価されます。詳細については、「リソースベースのポリシーとリソースコントロールポリシーによるコンソールアクセスの制御」を参照してください。

ユーザータイプを決定する

サインイン方法は、ユーザーの種類によって異なります AWS 。 AWS アカウント は、ルートユーザー、IAM ユーザー、IAM アイデンティティセンターでのユーザー、またはフェデレーティッドアイデンティティとして管理できます。 AWS Builder ID プロファイルを使用して、特定の AWS サービスやツールにアクセスできます。さまざまなユーザータイプを以下に示します。

トピック

- ルートユーザー
- IAM ユーザー
- IAM アイデンティセンター
- フェデレーテッドアイデンティティ
- AWS Builder ID ユーザー

ルートユーザー

アカウントオーナーまたはアカウントルートユーザーとも呼ばれます。ルートユーザーとして、 のすべての AWS サービスとリソースへの完全なアクセス権があります AWS アカウント。を初めて作成するときは AWS アカウント、アカウント内のすべての AWS サービスとリソースへの完全なアクセス権を持つ単一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 アカウントのルートユーザーです。アカウントの作成に使用したメールアドレスとパスワードを使用して、ルートユーザーとしてサインインできます。ルートユーザーは AWS マネジメントコンソール の方法でサインインします。サインインの手順については、「ルートユーザー AWS マネジメントコンソール として にサインインする」を参照してください。

> **Important**
>
> を作成するときは AWS アカウント、まず、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 ルート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。

ルート・ユーザを含む IAM アイデンティティの詳細については、「IAM アイデンティ (ユーザー、ユーザーグループ、ロール)」を参照してください。

IAM ユーザー

IAM ユーザーは、 AWSで作成したエンティティです。このユーザーは、特定のカスタムアクセス権限を持つ AWS アカウント 内のアイデンティティです。 IAM ユーザー認証情報は、AWS マネジメントコンソール へのサインインに使用される名前とパスワードで構成されます。サインインの手順については、「IAM ユーザー AWS マネジメントコンソール として にサインインする」を参照してください。

IAM ユーザを含むIAM アイデンティティの詳細については、「IAM アイデンティ (ユーザー、ユーザーグループ、ロール)」を参照してください。

IAM アイデンティティセンター

IAM Identity Center ユーザーは のメンバーであり AWS Organizations 、 AWS アクセスポータルを通じて複数の AWS アカウント およびアプリケーションへのアクセスを許可できます。会社が アクティブディレクトリ または別のアイデンティティプロバイダーを IAM アイデンティティセンターと統合している場合、IAM アイデンティティセンターのユーザーは会社の認証情報を使用してサインインできます。IAM アイデンティティセンターは、管理者がユーザーを作成できるアイデンティティプロバイダーにもなります。ID プロバイダーに関係なく、IAM Identity Center のユーザーは、組織の特定のサインイン URL である AWS アクセスポータルを使用してサインインします。IAM アイデンティティセンターのユーザーが AWS マネジメントコンソール の URL からサインインできない。

IAM Identity Center のヒューマンユーザーは、次のいずれかから AWS アクセスポータル URL を取得できます。

- 管理者またはヘルプデスクの従業員からのメッセージ
- IAM Identity Center への招待 AWS を含む からの E メール

> **Tip**
>
> IAM アイデンティティセンターのサービスによって送信されるすべての E メールは、no-reply@signin.aws または no-reply@login.awsapps.com のアドレスから送信されます。これらの送信者メールアドレスからのメールを受け入れ、迷惑メールやスパムとして処理しないように、メールシステムを設定することをお勧めします。

サインインの手順については、「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。

> **Note**
>
> AWS アクセスポータルには組織の特定のサインイン URL をブックマークして、後でアクセスできるようにすることをお勧めします。

IAM Identity Center の詳細については、「IAM アイデンティティセンターとは」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

フェデレーティッド ID は、よく知られている外部 ID プロバイダー (IdP) (例: Login with Amazon、Facebook、Google などの OpenID Connect (OIDC) 互換の IdP) を使用してサインインすることができるユーザーです。ウェブ ID フェデレーションを使用すると、認証トークンを受け取り、そのトークンを の一時的なセキュリティ認証情報と交換できます。 AWS そのトークンは、 のリソースを使用するアクセス許可を持つ IAM ロールにマッピングされます AWS アカウント。 AWS マネジメントコンソール または AWS アクセスポータルではサインインしません。代わりに、使用している外部アイデンティティによってサインイン方法が決まります。

詳細については、「フェデレーティッドアイデンティティとしてのサインイン」を参照してください。

AWS Builder ID ユーザー

AWS Builder ID ユーザーとして、アクセスする AWS サービスまたはツールに特にサインインします。 AWS Builder ID ユーザーは、既に持ってい AWS アカウント るもの、または作成するものを補完します。 AWS Builder ID はユーザーを表し、 を使用せずに AWS サービスやツールにアクセスするために使用できます AWS アカウント。また、情報を確認したり更新したりできるプロフィールもあります。詳細については、「でサインインする AWS ビルダー ID」を参照してください。

AWS Builder ID AWS は、 AWS エキスパートから学び、オンラインでクラウドスキルを構築できるオンライン学習センターである Skill Builder サブスクリプションとは異なります。 AWS スキルビルダーの詳細については、AWS 「スキルビルダー」を参照してください。

サインイン URL を決定する

ユーザーの種類 AWS に応じて、次のいずれかURLs を使用して にアクセスします AWS 。詳細については、「ユーザータイプを決定する」を参照してください。

トピック

- AWS アカウント ルートユーザーのサインイン URL
- AWS アクセスポータル
- IAM ユーザーのサインイン URL
- フェデレーティッドアイデンティティ URL

- AWS ビルダー ID URL

AWS アカウント ルートユーザーのサインイン URL

ルートユーザーは、 AWS サインインページ AWS マネジメントコンソール から にアクセスしますhttps://console.aws.amazon.com/ 。

このサインインページには、IAM ユーザーとしてサインインするオプションもあります。

AWS アクセスポータル

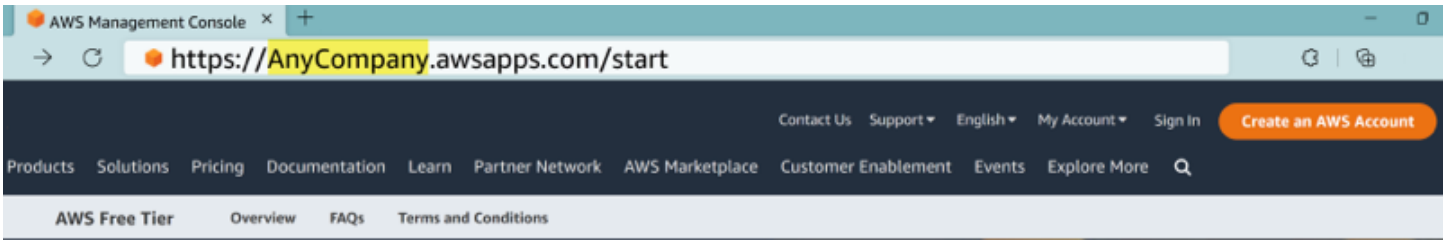
AWS アクセスポータルは、IAM Identity Center のユーザーがサインインしてアカウントにアクセスするための特定のサインイン URL です。管理者が IAM アイデンティティセンターでユーザーを作成すると、管理者は、ユーザーが IAM アイデンティティセンターへの招待メールを受信するか、管理者またはヘルプデスクの従業員からワンタイムパスワードと AWS アクセスポータル URL を含むメッセージを受信するかを選択します。特定のサインイン URL の形式は、次の例のようになります。

```
https://d-xxxxxxxxxx.awsapps.com/start
```

または

```
https://your_subdomain.awsapps.com/start
```

特定のサインイン URL は、管理者がカスタマイズできるため異なります。特定のサインイン URL は D で始まり、その後に 10 個のランダムな数字と文字が続く場合があります。次の例のように、サインイン URL にサブドメインを使用して会社名を含めることもできます。



> **Note**
>
> アクセス AWS ポータルの特定のサインイン URL をブックマークして、後でアクセスできるようにすることをお勧めします。

AWS アクセスポータルの詳細については、AWS 「 アクセスポータルの使用」を参照してください。

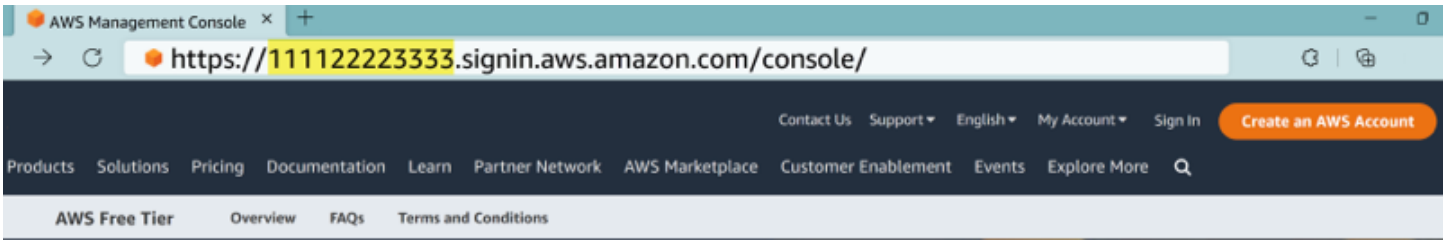
IAM ユーザーのサインイン URL

IAM ユーザーは、特定の IAM ユーザーのサインイン URL AWS マネジメントコンソール を使用してにアクセスできます。IAM ユーザーのサインイン URL は、 AWS アカウント ID またはエイリアスと `signin.aws.amazon.com/console`

IAM ユーザーのサインイン URL の例：

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

アカウント ID が 111122223333 の場合、サインイン URL は次のようになります。



IAM ユーザーのサインイン URL AWS アカウント を使用して にアクセスする際に問題が発生した場合は、「 の耐障害性 AWS Identity and Access Management」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 URL

フェデレーティッドアイデンティティのサインイン URL はさまざまです。外部アイデンティティまたは外部 ID プロバイダー (IdP) は、フェデレーティッドアイデンティティのサインイン URL を決定します。外部アイデンティティは、Windows アクティブディレクトリ、Login with Amazon、Facebook、または Google のいずれかです。フェデレーション ID としてサインインする方法の詳細については、管理者にお問い合わせください。

フェデレーティッドアイデンティティの詳細については、「ウェブ ID フェデレーションについて」を参照してください

AWS ビルダー ID URL

AWS Builder ID プロファイルの URL は ですhttps://profile.aws.amazon.com/。 AWS Builder ID を使用する場合、サインイン URL はアクセスするサービスによって異なります。たとえば、Amazon CodeCatalyst にサインインするには、「https://codecatalyst.aws/login」を参照してください。

許可リストに追加するドメイン

次世代ファイアウォール (NGFW) や Secure Web Gateway (SWG) などのウェブコンテンツフィルタリングソリューションを使用して特定の AWS ドメインまたは URL エンドポイントへのアクセスをフィルタリングする場合は、ウェブコンテンツフィルタリングソリューションの許可リストに次のドメインまたは URL エンドポイントを追加する必要があります。

AWS 許可リストへのドメインのサインイン

お客様またはお客様の組織が IP またはドメインフィルタリングを実装する場合、ドメインを許可リストに登録して、 AWS マネジメントコンソールを使用する必要があります。次のドメインは、AWS マネジメントコンソールへのアクセスを試みるネットワークでアクセス可能である必要があります。

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

AWS 許可リストへのサインイン管理ドメイン

AWS CLI を使用してコンソールのアクセスコントロールを設定する場合は、 AWS サインインコントロールプレーンエンドポイントを許可リストに登録する必要があります。このエンドポイントはポリシー管理を処理し、前のセクションのコンソールサインインドメインとは異なります。

- signin.*[Region]*.api.aws

  [#####] を呼び出している AWS リージョンに置き換えます。すべての商用の リージョンで使用できます。例えば、signin.us-east-1.api.aws などです。

AWS アクセスポータル 許可リストのドメイン

次世代ファイアウォール (NGFW) や Secure Web Gateway (SWG) などのウェブコンテンツフィルタリングソリューションを使用して特定の AWS ドメインまたは URL エンドポイントへのアクセスをフィルタリングする場合は、ウェブコンテンツフィルタリングソリューションの許可リストに次の

ドメインまたは URL エンドポイントを追加する必要があります。これにより、 にアクセスできます AWS アクセスポータル。

次のリストは、ウェブコンテンツフィルタリングソリューションの許可リストに追加する IPv4 およびデュアルスタックのドメインと URL エンドポイントを示しています。デュアルスタックエンドポイントの詳細については、IAM Identity Center ユーザーガイドの「ファイアウォールとゲートウェイを更新して へのアクセスを許可する AWS アクセスポータル」を参照してください。

IPv4 許可リスト

- *[Directory ID or alias]*.awsapps.com
- *[IAM Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com

デュアルスタック許可リスト

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net

- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

AWS ビルダー ID 許可リストのドメイン

お客様またはお客様の組織が IP またはドメインフィルタリングを実装する場合、ドメインを許可リストに登録して、 AWS ビルダー IDを作成して使用する必要があります。以下のドメインは、 AWS ビルダー IDへのアクセスを試みるネットワークでアクセス可能である必要があります。

- view.awsapps.com/start
- *.portal.*.app.aws
- *.aws.dev
- *.api.aws
- *.uis.awsstatic.com
- *.console.aws.a2z.com
- oidc.*.amazonaws.com
- oidc.*.api.aws
- *.sso.amazonaws.com
- *.sso.*.amazonaws.com
- *.sso-portal.*.amazonaws.com
- sso.*.api.aws
- *.signin.aws
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- profile.aws.amazon.com

AWS アカウント 管理者向けのセキュリティのベストプラクティス

新しい を作成したアカウント管理者の場合は AWS アカウント、ユーザーがサインインするときに AWS セキュリティのベストプラクティスに従うことができるように、次の手順を実行することをお勧めします。

1. ルートユーザーとしてサインインして多要素認証 (MFA) を有効にし、まだ作成していない場合は IAM アイデンティティセンターでAWS 管理ユーザーを作成します。それから、ルートの認証情報を保護し、日常的な作業には使わないようにしましょう。
2. AWS アカウント 管理者としてサインインし、次の ID を設定します。
   - 他のユーザーのために最小特権ユーザーを作成します。
   - ワークロード用の一時認証情報を設定する。
   - アクセスキーは、長期的な認証情報を必要とするユースケースのためにのみ作成してください。
3. これらのアイデンティティへのアクセスを許可する権限を追加します。AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行できます。
   - IAM AWS アイデンティティセンター (AWS シングルサインオンの後継) ユーザーにアクセス許可セットを追加します。
   - ワークロードに使用する IAM ロールにアイデンティティベースのポリシーを追加します。
   - 長期的な認証情報を必要とするユースケースのために IAM ユーザー向けのアイデンティティベースのポリシーを追加します。
   - IAM ユーザーの詳細については、IAM 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。
4. にサインインする AWS マネジメントコンソール に関する情報を保存して共有する。この情報は、作成したアイデンティティのタイプによって異なります。
5. アカウントやセキュリティに関する重要な通知を受け取れるように、ルートユーザーのメールアドレスとプライマリアカウントの連絡先電話番号は常に最新の状態にしておいてください。
   - AWS アカウントのルートユーザーのアカウント名、E メールアドレス、パスワードの変更。
   - プライマリアカウント連絡先のアクセスまたは更新
6. アイデンティティとアクセス管理のその他のベストプラクティスについては、「IAM のセキュリティのベストプラクティス」をご覧ください。
7. ネットワークベースのアクセスコントロールを実装する: サインインリソースベースのポリシーまたはリソースコントロールポリシー (RCPs) を使用して、コンソールのサインインを承認された IP アドレス範囲または VPCs。コンソールプライベートアクセスを使用する環境では、VPC エンドポイントポリシーを設定して、エンドポイント経由でアクセスできるアカウントを制御します (「コンソールプライベートアクセス」を参照)。サインインリソースベースのポリシー、RCPs、VPC エンドポイントポリシーを組み合わせて、さまざまな適用ポイントでレイヤードネットワークコントロールを提供します。ルートユーザーの場合、サインインポリシー

は、不正なネットワークからのアクセス試行時に認証情報ページを完全にブロックします。アカウントロックアウトを防ぐために、除外されたプリンシパルをリカバリアクセス用に設定 AWS することをお勧めしますが、これはオプションです。詳細については、「リソースベースのポリシーとリソースコントロールポリシーによるコンソールアクセスの制御」を参照してください。

にサインインする AWS マネジメントコンソール

メインサインイン URL (https://console.aws.amazon.com/) AWS マネジメントコンソール から に AWS サインインするときは、ルートユーザーまたは IAM ユーザーのいずれかのユーザータイプを選択する必要があります。自分がどのようなユーザーか明確でない場合は、「ユーザータイプを決定する」を参照してください。

ルートユーザーは無制限にアカウントにアクセスでき、 AWS アカウントの作成者と関連付けられています。次に、ルートユーザーは IAM ユーザーや AWS IAM アイデンティティセンターのユーザーなどの他のタイプのユーザーを作成し、アクセス認証情報を割り当てます。

IAM ユーザーは、特定のカスタムアクセス許可 AWS アカウント を持つ 内の ID です。IAM ユーザーがサインインすると、メインサインイン URL `https://account_alias_or_id.signin.aws.amazon.com/console/`の代わりに、AWS アカウント または エイリアスを含む AWS サインイン URL を使用できますhttps://console.aws.amazon.com/ 。

では、1 つのブラウザで最大 5 つの異なる ID に同時にサインインできます AWS マネジメントコンソール。これらは、異なるアカウントまたは同じアカウントのルートユーザー、IAM ユーザー、またはフェデレーションロールの組み合わせです。詳細については、「AWS マネジメントコンソール 入門ガイド」の「複数の入門ガイドアカウントへのサインイン」を参照してください。

チュートリアル

- ルートユーザー AWS マネジメントコンソール として にサインインする
- IAM ユーザー AWS マネジメントコンソール として にサインインする

自分がどのようなユーザーか明確でない場合は、「ユーザータイプを決定する」を参照してください。

チュートリアル

- ルートユーザー AWS マネジメントコンソール として にサインインする
- IAM ユーザー AWS マネジメントコンソール として にサインインする

ルートユーザー AWS マネジメントコンソール として にサインインする

を初めて作成するときは 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。

> **Important**
>
> 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。ルートユーザー資格情報は保護し、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「ルートユーザー資格情報が必要なタスク」を参照してください。

ルートユーザーとしてサインインする

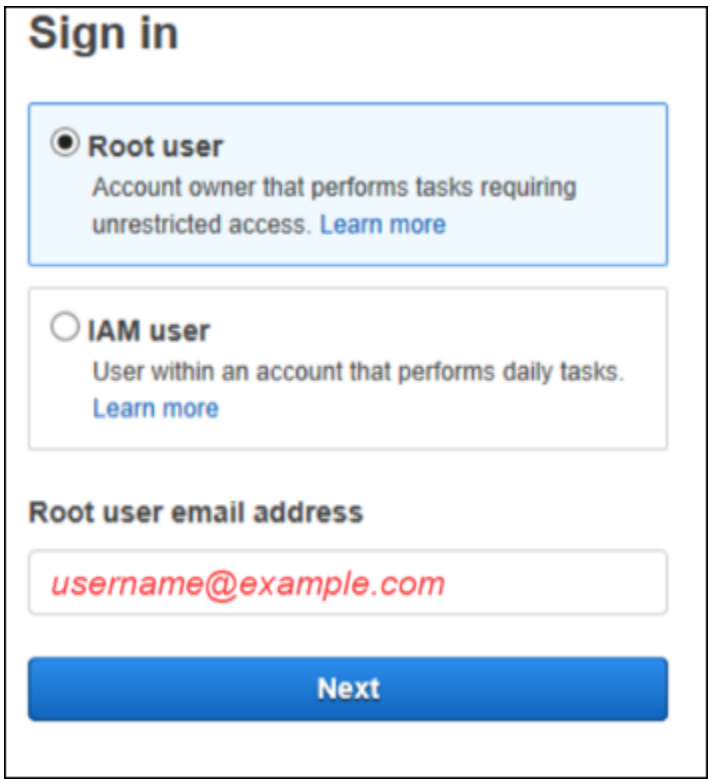
AWS マネジメントコンソールで別の ID に既にサインインしているときに、ルートユーザーとしてサインインできます。詳細については、「AWS マネジメントコンソール 入門ガイド」の「複数の入門ガイドアカウントへのサインイン」を参照してください。

AWS アカウント を使用した 管理にはルートユーザー認証情報がない AWS Organizations 可能性があるため、 管理者に連絡してメンバーアカウントでルートユーザーアクションを実行する必要があります。ルートユーザーとしてサインインできない場合は、「サインインに関する問題 AWS アカウント のトラブルシューティング」を参照してください。

1. AWS マネジメントコンソール で を開きますhttps://console.aws.amazon.com/。

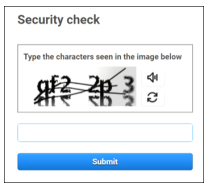
   > **Note**
   >
   > 以前にこのブラウザを使用して IAM ユーザーとしてサインインしたことがある場合は、代わりに IAM ユーザーのサインインページが表示される場合があります。[ルートユーザーの E メールを使用してサインイン] を選択します。

2. [ルートユーザー] を選択します。



3. [ルートユーザーの E メールアドレス]に、ルートユーザーに関連付けられている E メールアドレスを入力します。[次へ]を選択します。
4. セキュリティチェックを完了するように求められたら、表示された文字を入力して続行します。セキュリティチェックを完了できない場合は、音声を聞くか、新しい文字セットのセキュリティチェックを更新してみてください。

> **Tip**
>
> 表示される (または聞こえる) 英数字を、スペースを入れずに順番に入力します。



5. パスワードを入力します。

6. MFA で認証します。MFA は、デフォルトでルートユーザーに強制されます。スタンドアロンアカウントとメンバーアカウントのルートユーザーの場合、MFA を手動で有効にする必要があり、これを強くお勧めします。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS アカウント ルートユーザーの多要素認証」を参照してください。

> **Tip**
>
> セキュリティのベストプラクティスとして、不正使用を防ぐために、 AWS 組織のメンバーアカウントからすべてのルートユーザー認証情報を削除することをお勧めします。このオプションを選択した場合、メンバーアカウントはルートユーザーとしてサインインしたり、パスワード復旧を実行したり、MFA を設定したりすることはできません。この場合、管理アカウント管理者のみが、メンバーアカウントのルートユーザー認証情報を必要とするタスクを実行できます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「メンバーアカウントのルートアクセスを一元管理する」を参照してください。

7. [サインイン] を選択します。 AWS マネジメントコンソール が表示されます。

認証後、 AWS マネジメントコンソール コンソールのホームページが開きます。

追加情報

AWS アカウント ルートユーザーに関する詳細情報が必要な場合は、次のリソースを参照してください。

- ルートユーザーの概要については、「AWS アカウント ルートユーザー」を参照してください。
- ルートユーザーの使用の詳細については、AWS アカウント「ルートユーザーの使用」を参照してください。
- ルートユーザーのパスワードをリセットする手順については、「のルートユーザーパスワードを忘れました AWS アカウント」を参照してください。

IAM ユーザー AWS マネジメントコンソール として にサインインする

IAM ユーザーは、 AWS リソースを操作するアクセス許可 AWS アカウント を持つ 内で作成された ID です。IAM ユーザーは、アカウント ID またはエイリアス、ユーザー名、パスワードを使ってサインインします。IAM ユーザー名は管理者によって設定されます。IAM ユーザー名は、*Zhang* などのわかりやすい名前でも、*zhang@example.com* などの E メールアドレスでもかまいません。IAM ユーザー名にスペースを含めることはできませんが、大文字、小文字、数字、+ = , . @ _ - などの記号を使用できます。

> **Tip**
>
> IAM ユーザーが多要素認証 (MFA) を有効にしている場合は、認証デバイスへのアクセス権が必要です。詳細については、「IAM サインインページで MFA デバイスを使用する」を参照してください。

IAM ユーザーとしてサインインするには

AWS マネジメントコンソールで別の ID に既にサインインしている場合は、IAM ユーザーとしてサインインできます。詳細については、「AWS マネジメントコンソール 入門ガイド」の「複数の入門ガイドアカウントへのサインイン」を参照してください。

1. AWS マネジメントコンソール で を開きますhttps://console.aws.amazon.com/。
2. メインサインインページが表示されます。アカウント ID (12 桁) またはエイリアス、IAM ユーザー名、パスワードを入力します。

> **Note**
>
> 現在のブラウザで IAM ユーザーとして以前にサインインしたことがある場合、またはアカウントのサインイン URL を使用している場合は、アカウント ID やエイリアスを入力する必要がない場合があります。

3. [サインイン] を選択します。
4. IAM ユーザーに対して MFA が有効になっている場合、 は認証ツールで ID を確認 AWS する必要があります。詳細については、「AWSで多要素認証 (MFA) を使用する」を参照してください。

認証後、 AWS マネジメントコンソール コンソールのホームページが開きます。

追加情報

IAM ユーザーの詳細については、以下のリソースを参照してください。

- IAM の概要については、「アイデンティティとアクセス管理とは」を参照してください。
- AWS アカウント IDs「 AWS アカウント ID とそのエイリアス」を参照してください。
- IAM ユーザーパスワードをリセットする方法の手順については、「の IAM ユーザーパスワードを忘れた AWS アカウント」を参照してください。

リソースベースのポリシーとリソースコントロールポリシーによるコンソールアクセスの制御

> **Important**
>
> コンソールのサインインアクセスはデフォルトで有効になっています。 AWS サインインでは、最初は無制限のコンソールアクセスが許可されます。制限を追加するには、アカウントまたは組織のコンソール認可設定を有効にします。作成したリソース許可ステートメントは、コンソール認可を有効にするまで効果がありません。「リソースポリシーを使用したコンソールアクセスコントロールの開始方法」を参照してください。

AWS サインインは、 AWS サインインへのアクセスを制御するためのリソースベースのポリシーとリソースコントロールポリシー (RCPs) をサポートします。これらのポリシーを使用して、認証前、認証中、認証後の AWS マネジメントコンソール アクセス全体でユーザー ID とネットワークの場所を検証します。ルートユーザーの場合、これらのポリシーは、認証情報収集を開始する前にネットワークの場所とユーザー ID を検証します。認証情報は、アクセスが予想されるネットワークから発信された場合にのみ入力できます。

AWS サインインリソースベースのポリシー:

- を個々の AWS アカウントに適用します。
- アカウント管理者が、ネットワークパラメータとプリンシパル ID に基づいてコンソールへのアクセスを制限できるようにします。

リソースコントロールポリシー (RCPs):

- AWS Organizations を通じて組織全体に適用します。
- すべてのメンバーアカウントを一元管理します。

どちらのポリシータイプも、認証前にアクセスを検証します。これにより、プリンシパルが予期しないネットワークからサインインページにアクセスできなくなります。

これらのポリシーは、引き続き適用される IAM アイデンティティベースのポリシーを置き換えるものではありません。

> **Note**
>
> 組織レベルの設定と管理を含むリソースコントロールポリシーの完全なドキュメントについては、AWS Organizations ユーザーガイドの「リソースコントロールポリシー」を参照してください。このセクションでは、主に AWS サインインリソースベースのポリシーに焦点を当てます。

AWS サインインリソースベースのポリシーと RCPsは、次の認証方法に適用されます。

- AWS マネジメントコンソール – コンソールのログインページを使用した直接サインイン。
- AWS IAM アイデンティティセンター – IAM アイデンティティセンターを使用したコンソールサインイン。
- フェデレーティッド ID プロバイダー – SAML または OIDC フェデレーションを使用してサインインします。
- AWS サインインと統合されたアプリケーション – Amazon Connect、Amazon QuickSight、 AWS Health Dashboard、Amazon AppStream、Amazon Lightsail、AWS IQ。

これらのコントロールは、アクセスキー (AWS SDKsまたは SigV4 で署名された API コール) を使用したプログラムによるアクセスには適用されません。

AWS サインインがリソースベースのポリシーを評価する方法

AWS サインインは、認証前 (認証前フェーズ) と認証成功後 (認証後フェーズ) の 2 つの時点で、該当するリソースベースのポリシーまたはリソースコントロールポリシー (RCPs) を評価します。各評価は、ポリシーで定義されている条件キーをチェックします。使用できるキーは、フェーズとアクションによって異なります。詳細については、「サポートされている条件キー」を参照してください。

> **Note**
>
> ルートユーザーのサインインの場合、パスワードプロンプトが表示される前に、予期しないネットワークからのアクセス試行がブロックされます。これにより、予期しないネットワークからの認証情報の送信が防止されます。

認証後、評価ではプリンシパルのアイデンティティベースのポリシーも考慮されます。関連するサインインアクションを拒否する IAM ポリシーは、ネットワーク条件が満たされた場合でも、コンソールセッションの付与を妨げる可能性があります。

サポートされているアクション

AWS サインインリソースポリシー (リソースベースのポリシーと RCPs) では、次のアクションがサポートされています。

`signin:Authenticate`

これは、サインインリクエストが受信されたときに評価される評価専用 (呼び出し不可) アクションです。これは認証前チェックであり、プリンシパルがサインインページ (ルートユーザー、IAM ユーザー) に認証情報を入力するか、ID プロバイダーまたは AWS STS (フェデレーティッドユーザー、ロール) の認証情報を使用してコンソールサインインを開始すると発生します。

サポートされている条件キー:
`aws:SourceIp`、`aws:SourceVpc`、、`aws:SourceVpce`、`aws:VpcSourceIpaws:RequestedRegi`

ユーザーの ID がまだ確認されていないため、プリンシパルベースのグローバル条件キー (`aws:PrincipalArn`、`aws:PrincipalAccount`) はこのアクションでは使用できません。

`signin:AuthorizeOAuth2Access`

OAuth 認可コードの生成に使用されます。認証が成功すると、システムが OAuth 認可コードを生成すると、このアクションがトリガーされます。この時点で、ユーザーは認証され、プリンシパルベースの条件キーを使用できます。

サポートされている条件キー:
`aws:SourceIp`、`aws:SourceVpc`、、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:RequestedRe`

`signin:CreateOAuth2Token`

この認証後アクションは、OAuth トークンの作成と交換に使用されます。このアクションは、アクセストークンの認可コードの引き換え、トークンの更新、トークン交換オペレーションの実行時にトリガーされます。このフェーズでは、プリンシパルベースの条件キーを使用できます。

サポートされている条件キー:
`aws:SourceIp`、`aws:SourceVpc`、、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:RequestedRe`

> **Important**
>
> AWS サインインポリシー (リソースベースのポリシーまたは RCPs) を作成するときは、認証前ステートメント`signin:AuthorizeOAuth2Access`と認証`signin:CreateOAuth2Token`後ステートメント`signin:Authenticate`の 3 つのアクションすべてをポリシー全体でカバーします。コンソールのサインインでは、OAuth 2.0 を使用します。OAuth 2.0 は、3 つのアクションすべてを順番に流れます。ポリシーが アクションを省略した場合、対応するフェーズは保護されません。を含む VPC エンドポイントポリシーアクションについては`signin:CreateAccount`、「AWS マネジメントコンソールのプライベートアクセス」を参照してください。

サポートされている条件キー

AWS サインインは、リソースベースのポリシーとリソースコントロールポリシー (RCPs) で次の条件キーをサポートします。これらのキーを使用して、ネットワークの場所とプリンシパル ID に基づいてコンソールへのアクセスを制御します。

- ネットワークベース (すべてのアクション): `aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:RequestedRegic`
- ID ベース (認証後アクション): `aws:PrincipalArn`、`aws:PrincipalAccount`。
- サービス固有 (事前認証のみ): `signin:PrincipalArn`。

詳細な使用ルール、オペレータの互換性、組み合わせの制限、アクション別の可用性マトリックスについては、「」を参照してくださいAWS サインイン条件キーリファレンス。

リソースポリシーを使用したコンソールアクセスコントロールの開始方法

前提条件

- AWS CLI がインストールされ、設定されています。
- 適切な IAM アクセス許可 (「」を参照AWS マネージドポリシー: AWSSignInResourcePolicyManagement)。
- 識別されたネットワーク境界 (IP 範囲、VPCs、または VPC エンドポイント) 。
- アクセスを保持するために指定された除外されたプリンシパル (推奨されますが、オプション) 。

- ネットワークで出力フィルタリングを使用している場合は、 AWS サインインコントロールプレーンエンドポイントを許可リストに登録します (「」を参照AWS 許可リストへのサインイン管理ドメイン)。

> **Important**
>
> 本番環境でコンソール認可を有効にする前に、緊急復旧アクセスを維持するために、少なくとも 1 つの除外されたプリンシパルを設定する AWS ことをお勧めします。ルートユーザーを含むすべてのプリンシパルは、明示的に除外されない限り、ポリシーの対象となります。除外されたプリンシパルはオプションですが、除外すると、ネットワーク条件が予期せず変化した場合にアカウントがロックアウトされるリスクが高まります。

AWS サインインポリシーのすべての書き込みオペレーション`--region us-east-1`に を指定します。 はこのリージョンからグローバルにポリシーを AWS レプリケートします。読み取りオペレーションは任意のリージョンをターゲットにできます。

ステップ 1: リソースアクセス許可ステートメントを作成する

アクセスコントロールを定義するアクセス許可ステートメントを作成します。すべての書き込みオペレーションには が必要です `--region us-east-1` (AWS サインインサービスは、このリージョンでのみポリシーの変更を受け入れます) 。残りのパラメータ (`--source-vpc`、`--source-ip`、`--requested-region`、`--excluded-principal`) は、ポリシーの条件を定義します。たとえば、 は、us-west-2 リージョンのサインインエンドポイントへのサインインを制限する条件`--requested-region us-west-2`を追加します。

例 – 企業 VPC へのアクセスを制限する:

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
  --client-token unique-request-id-12345 \
  --region us-east-1
```

例 – 特定の IP 範囲へのアクセスを制限します。

```
aws signin put-resource-permission-statement \
```

```
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> `--excluded-principal` パラメータは、ネットワーク制限をバイパスする除外されたプリンシパルを指定し、ネットワーク条件が変化しても緊急アクセスを維持します。

ステップ 2: コンソール認可設定を有効にする

次の手順では、アカウントまたは組織のコンソールサインインプロセスのポリシーの適用を有効にします。リソース許可ステートメントはいつでも作成できますが、コンソール認可が有効になるまで評価されません。

> **Warning**
>
> コンソール認可を有効にすると、ネットワーク条件が正しく設定されていない場合、または既存のサービスコントロールポリシー (SCP) またはリソースコントロールポリシー (RCP) が AWS サインインアクションを拒否した場合、プリンシパルがロックアウトされる可能性があります。コンソール認可を有効にする前に、アクセス許可ステートメントが正しいことを確認し、`signin:Authenticate`、、または を拒否する SCP または RCP を削除`signin:AuthorizeOAuth2Access`または調整します`signin:CreateOAuth2Token`。

スタンドアロンアカウントの場合:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

AWS Organizations の場合:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
  --region us-east-1
```

設定の検証:

```
aws signin get-console-authorization-configuration \
  --target-id <your-target-id> \
  --region <your-region>
```

コンソール認可設定を削除します。

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

ステップ 3: ポリシーを検証する

すべてのアクセス許可ステートメントを一覧表示します。

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

完全な統合ポリシーを取得します。

```
aws signin get-resource-policy \
  --region <your-region>
```

`get-resource-policy` コマンドは、すべてのアクセス許可ステートメントで構成される完全なリソースベースのポリシーを返します。コンソールアクセスをテストする前に、このポリシーを確認して、意図したアクセスコントロールを反映していることを確認します。

リージョン別の可用性

コンソール認可 APIsは、すべての AWS 商用リージョンで使用できます。これらの APIs は、運用している任意のリージョンから呼び出すことができます。

> **Important**
>
> 書き込みオペレーション (`put-console-authorization-configuration`、`put-resource-permission-statement`、`delete-console-authorization-configuration`、`delete-resource-permission-statement`) は、 `us-east-1`リージョンで実行する必要があります。で作成されたポリシー`us-east-1`は、グローバルに自動的にレプリケートされます。読み取りオペレーション (`get-console-authorization-`

configuration、list-resource-permission-statements、get-resource-policy) は任意のリージョンから実行できます。

ポリシー構造を理解する

AWS サインインポリシーには、コンソールのサインインフローのさまざまなフェーズを保護する 2 つのステートメントが含まれています。

- 認証前ステートメント (アクション: **signin:Authenticate**): サインインリクエストが受信されたときに、認証が完了する前に評価されます。プリンシパルの ID aws:PrincipalArnが未確認であるため、グローバルキーはこのフェーズでは使用できません。このフェーズsignin:PrincipalArnでは、特定のプリンシパルをネットワーク制限から除外できます。ネットワークベースの条件キーは、このフェーズで評価できます。
- 認証後ステートメント (アクション: **signin:AuthorizeOAuth2Access**、**signin:CreateOAuth2Token**): 認証後、OAuth トークン交換中に評価されます。特定のプリンシパルを除外aws:PrincipalArnするために使用します。このフェーズでは、すべてのネットワークベースおよびアイデンティティベースの条件キーを評価できます。

コンソールのサインインでは OAuth 2.0 が使用されるため、両方のステートメントが必要です。OAuth 2.0 は 3 つのアクションすべてを順番に流れます。ステートメントが 1 つしかないポリシーでは、他のフェーズは保護されません。 signin:PrincipalArnはルートユーザー、IAM ユーザー、ロールのプリンシパルタイプをサポートします。 はすべてのプリンシパルタイプ (ルートユーザー、IAM ユーザー、フェデレーティッドユーザー、ロール) aws:PrincipalArnをサポートします。

ポリシーの例

例 1: ネットワーク境界と除外されたプリンシパルを持つ RCP

次のリソースコントロールポリシー (RCP) は、組織内のすべてのアカウントで、企業ネットワークの外部からの AWS マネジメントコンソール サインインを拒否します。指定された除外されたプリンシパルは緊急アクセスの対象外です。VPC IDs はリージョン内でのみ一意であるため、ポリシーには、予想されるリージョンへの VPC ベースのアクセスをピン留めする 3 番目のステートメントが含まれます。

EnforceNetworkPerimeterPreAuth ステートメントは、 signin:PrincipalArnを使用して、事前認証フェーズ中に除外されたプリンシパルを除外します。EnforceNetworkPerimeterPostAuth ステートメントは を使用してaws:PrincipalArn、認証後に除外されたプリンシパルを除外します。EnforceSourceVPCRegion ステートメントは、リクエストリージョンが VPC リージョンと一致することを確認し、指定された VPC の予想されるリージョンへのアクセスを制限します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
```

```
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
        }
      }
    }
  ]
}
```

このポリシー:

- リクエストが企業 IP 範囲または企業 VPC から発信されない限り、サインインページへのアクセスを拒否します。除外されたルートアカウントと IAM ユーザーは、 `signin:PrincipalArn` (事前認証) によって除外されます。

- 企業の IP 範囲または VPC からの場合を除き、OAuth トークン交換を拒否します。除外されたルートアカウント、IAM ユーザー、ロールは、 aws:PrincipalArn (認証後グローバルキー) を介して除外されます。
- リクエストが指定された VPC から送信され、リージョンが一致しない場合、アクセスは拒否されます。 AWS VPC IDsはリージョン内で一意であり、同じ VPC ID は異なるリージョンに存在する可能性があります。
- RCP として設定されている場合、AWS Organization 全体にグローバルに適用されます。

例 2: 除外されたプリンシパルを持つ IP ベースのアクセスのリソースベースのポリシー

次のリソースベースのポリシーは、指定された IP 範囲外からリクエストを行うすべてのプリンシパルへのコンソールアクセスを拒否します。除外されたプリンシパルは除外されます。このポリシーには、サービス固有のsignin:PrincipalArnキーを使用する認証前ステートメントと、グローバルaws:PrincipalArnキーを使用する認証後ステートメントの 2 つのステートメントが含まれています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
```

```
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

このポリシー:

- IP 範囲 から接続しない限り、すべてのプリンシパルへのアクセスを拒否します<my-corporate-cidr>。
- (事前認証) と signin:PrincipalArn (事後認証) を使用して、除外されたプリンシパルをネットワーク制限から除外aws:PrincipalArnします。
- リソースベースのポリシーが設定されている (によって識別される) 特定のアカウントにのみ適用されます<my-aws-account-id>。

ベストプラクティス

緊急復旧アクセスのために除外されたプリンシパルを設定する

AWS では、本番環境でコンソール認可ポリシーを適用する前に、少なくとも 1 人の除外ユーザーを設定することをお勧めします。認証前段階では、signin:PrincipalArn条件キーはルートユーザー、IAM ユーザー、ロールプリンシパルを除外します。認証後段階では、aws:PrincipalArn条件キーはすべてのプリンシパルタイプ (ルートユーザー、IAM ユーザー、フェデレーティッドユーザー、ロール) を除外します。

除外されたプリンシパルはオプションですが、除外すると、ネットワーク条件が予期せず変化したり、ポリシーの設定が間違っていたりした場合に、アカウントがロックアウトされるリスクが高まります。

推奨される除外プリンシパル設定ステップ:

1. 除外された IAM ロールを作成します (例: `BreakGlassRole`)。
2. 除外されたロールの場合、ロールの信頼ポリシーに MFA が必要です。
3. 緊急復旧に必要な最小限のアクセス許可のみを、除外された ID に付与します。
4. 認証前 (`signin:PrincipalArn`) ポリシーステートメントと認証後 (`aws:PrincipalArn`) ポリシーステートメントの両方に、除外されたプリンシパル ARN を含めます。
5. 復旧手順を文書化し、 の外部に安全に保存します AWS。
6. 除外されたプリンシパルアクセスを定期的にテストして、必要に応じて機能することを確認します。

復旧アクセスパスを維持する

上記の除外されたプリンシパルに加えて、コンソール認可ポリシーが予期せずサインインをブロックした場合に、代替のアクセス方法が利用可能であることを確認します。

- ロールベースのプログラムによるアクセス: コンソール認可ポリシーは、インタラクティブコンソールのサインインにのみ適用されます。SigV4 で署名された API リクエストには適用されません。プログラムによるアクセス (既存のアクセスキー、クロスアカウントロールなど) がある場合は、それを使用して を呼び出し`signin:DeleteConsoleAuthorizationConfiguration`、制限ポリシーを削除します。認証情報には アクセス`signin:DeleteConsoleAuthorizationConfiguration`許可を含める必要があります (`AWSSignInResourcePolicyManagement`管理ポリシーに含まれています) 。 は、長期的な IAM ユーザーアクセスキーよりも一時的な認証情報 AWS を推奨します。メンバーアカウントの場合、管理アカウント管理者はメンバーアカウント (`aws sts assume-role`) `OrganizationAccountAccessRole` で引き受けて、これらの一時的な認証情報を取得できます。
- AWS サポートリカバリ: ルートユーザーアカウントの E メールと電話番号を最新の状態に保ちます。除外されたプリンシパルアクセスとプログラムによるアクセスの両方が利用できない場合、AWS サポートは ID 検証後に復旧ポータルリンクを提供できます。完全な復旧プロセスコンソール認可を有効にした後、アカウントからロックアウトされているについては、「」を参照してください。

本番デプロイ前のテスト

AWS では、ポリシーがアカウントに与える影響を徹底的にテストすることなく、制限付き RCPs を組織のルートにアタッチしないことをお勧めします。代わりに、一度に 1 つずつ、または少なくとも少数でアカウントを移動できる OU を作成して、キーアカウントからユーザーを誤ってロックしないようにします。

テストワークフロー:

1. プライマリネットワークの制限を使用して 1 つのアクセス許可ステートメントを作成します。
2. 非本番稼働用アカウントでコンソール認可を有効にします。
3. 許可されたネットワークと拒否されたネットワークの両方からのコンソールアクセスをテストします。
4. Amazon CloudTrail ログを確認して、ポリシー評価の動作を確認します。
5. 除外されたプリンシパルを使用してアクセスをテストします。
6. 追加のネットワークとアカウントに徐々に拡張します。
7. 本番稼働用アカウントを強制する前にモニタリングします。

defense-in-depthを使用した設計

AWS サインインリソースベースのポリシーとリソースコントロールポリシーを、より広範なセキュリティ戦略内の 1 つのレイヤーとして使用します。 AWS サインインポリシーは、ネットワークの場所とプリンシパル ID に基づいてコンソールへのアクセスを制限します。これらを他のポリシータイプと組み合わせて、包括的なアクセスコントロールを作成します。

- AWS サインインポリシー (リソースベースのポリシーと RCPs): 認証前、認証中、認証後のネットワークの場所とプリンシパルアイデンティティに基づいてコンソールへのアクセスを制限します。
- IAM ポリシー: サインイン後にユーザーが実行できるアクションを制御します。
- サービスコントロールポリシー (SCPs): 組織全体のアクセス許可ガードレールをすべてのプリンシパルに適用します。
- VPC エンドポイントポリシー: VPC エンドポイントを介してアクセスできるサービスとアカウントを制御します。

継続的なモニタリングと監査

AWS CloudTrail は、すべての AWS サインインポリシーの評価と設定変更を自動的に記録します。これらのイベントを CloudTrail イベント履歴で最大 90 日間表示します。保持期間を長くするには、証跡を作成して Amazon S3 にイベントを配信します (「証跡の作成」を参照)。リアルタイムアラートの場合は、 AWS サインインイベントに一致する Amazon EventBridge ルールを作成するか、メトリクスフィルターベースのアラームの CloudWatch Logs ロググループに配信するように証跡を設定するか、既存の SIEM ソリューションにイベントを転送します。

ユースケース

ネットワーク境界の適用

社内 VPCs。個々のアカウントにはリソースベースのポリシーを使用し、組織全体の強制にはリソースコントロールポリシー (RCPs) を使用して、ユーザーが信頼できるネットワークロケーションからのみサインインできるようにし、パブリックネットワークまたは信頼されていないネットワークからの不正アクセスを防止します。

シナリオ例: 企業は、自社のネットワークまたは承認された AWS VPCs からすべてのコンソールにアクセスする必要があります。緊急管理者の緊急復旧アクセスを維持しながら、他のすべてのネットワークからのアクセスを拒否する 1 つのアカウントまたは組織全体の RCP にリソースベースのポリシーを設定します。

コンプライアンス要件

ネットワークベースのアクセスコントロールの規制要件を満たします。多くのコンプライアンスフレームワークでは、組織はネットワークの場所に基づいて機密システムへのアクセスを制限する必要があります。 AWS サインインポリシーは、これらの要件への準拠を示す監査可能で強制可能なコントロールを提供します。

シナリオ例: 金融サービス企業は、承認されたネットワークからのコンソールアクセスのみを要求する規制に準拠する必要があります。RCPsのネットワーク制限を適用し、コンプライアンスの証拠として AWS CloudTrail ログを維持します。

マルチアカウントガバナンス

AWS Organizations 全体で一貫したコンソールアクセスポリシーを実装します。RCPsを使用して、すべてのメンバーアカウントに標準のネットワーク制限を適用し、個々のアカウントレベルの設定を必要とせずに一貫したセキュリティ体制を確保します。

シナリオ例: 100 以上の AWS アカウントを持つ企業はRCPs を使用して、すべてのコンソールアクセスが組織内の VPC エンドポイントから発信されることを要求するポリシーを適用し、すべてのアカウントで一貫したネットワークコントロールを確認します。

サードパーティーのアクセスコントロール

特定のネットワークからパートナーまたは請負業者に一時的なコンソールアクセスを付与します。組織は、全体的なセキュリティ体制を損なうことなく、外部関係者の時間制限付きネットワーク制限付きコンソールアクセスを作成できます。

シナリオ例: 企業はコンサルティング会社に一時的なコンソールアクセスを許可する必要があります。コンサルティング会社の既知の IP 範囲からのみ、およびコンサルタントに割り当てられた IAM ロールに対してのみアクセスを許可するリソースベースのポリシーを作成します。

コンソールへのアクセスを特定のプリンシパルに制限する

ネットワークの場所に関係なく AWS マネジメントコンソール、定義された一連のプリンシパルのみに へのサインインを許可し、他のすべてのプリンシパルを拒否します。これは、VPC エンドポイントを使用しておらず、アイデンティティベースのコンソールの制限が必要なお客様に役立ちます。コンソールへのサインインが拒否されたプリンシパルは、プログラムによるアクセスを保持します。 AWS サインインポリシーはコンソールへのサインインのみをゲートし、除外したプリンシパルのみがサインインできます。

シナリオ例: ある会社では、管理者のみが コンソールを使用できるようにしています。これらは、管理者プリンシパル ARNsを設定します。有効な認証情報を持つ Amazon EC2 インスタンスロールは、プログラムによるアクセス許可を保持していても、除外されたプリンシパルではないため、コンソールにサインインできません。これは、コンソールのサインインに使用されるインスタンスロール認証情報の一般的なケースに対処します。

コンソールのアクセスコントロールのトラブルシューティング

サインインリソースベースのポリシーのネットワーク条件によりサインインできない

AWS サインインポリシーによってアクセスが拒否されると、次のいずれかのエラーメッセージが表示されることがあります。

- 「認証情報が正しくありません。もう一度試してください。」 (リソースベースのポリシーによる事前認証の拒否)
- 「認証に失敗しました 無効なリクエスト」 (RCP による事前認証拒否)

- 「認証に失敗しました: このアカウントにアクセスするには、別のネットワークからサインインするか、管理者に連絡して詳細を確認してください」(認証後拒否)

これらのエラーのいずれかが表示され、アクセスを許可する必要があると思われる場合は、 AWS 管理者にお問い合わせください。CloudTrail ログで、`errorMessage`「リソースベースのポリシーにより承認が拒否されました」または「リソースコントロールポリシーにより承認が拒否されました」の`ConsoleLogin`イベントを確認し、どのポリシーステートメントがアクセスを拒否したかを特定できます。

考えられる原因:

- ソース IP アドレスが許可された CIDR 範囲内にありません。
- 必要な VPC または VPC エンドポイントに接続されていません。
- ポリシーで想定されるリージョンと一致しないリージョンのサインインエンドポイントにアクセスしています。
- プリンシパル ARN がポリシーの除外されたプリンシパルに正しくリストされていません。
- ポリシーは最近更新され、変更はまだグローバルにレプリケートされていません。

解決策:

- 社内ネットワークまたは VPN に接続していることを確認します。
- VPC エンドポイントベースの制限が設定されている場合は、正しい VPC エンドポイントを介してにアクセスしていることを確認します。
- AWS 管理者に連絡してポリシー設定を確認し、どのネットワークが承認されているかを確認してください。
- 除外されたプリンシパルとして設定されている場合は、除外されたプリンシパルリストでプリンシパル ARN が正しく設定されていることを確認します。
- ポリシーが最近変更された場合は、グローバルレプリケーションが完了するまで数分待ちます。

管理者がこの問題の診断を行う場合:

- ポリシー評価イベントの AWS CloudTrail ログを確認して、アクセスを拒否したポリシーステートメントを特定します。
- `aws signin get-resource-policy` を使用して、現在のポリシー設定を確認します。
- ユーザーのネットワークロケーションがポリシーの条件と一致していることを確認します。

- ユーザーをネットワーク制限から除外する必要がある場合は、除外されたプリンシパルが正しく設定されていることを確認します。

コンソール認可を有効にした後、アカウントからロックアウトされている

コンソール認可を設定し、アカウントにアクセスできなくなった場合、ポリシーを適用する前に除外されたプリンシパルを設定していない可能性があります。

アカウントタイプと使用可能な認証情報に応じて、アクセスを回復するためのパスが複数あります。

オプション 1: プログラムによるアクセスを使用する (AWS CLI または SDK)

コンソール認可ポリシーは、インタラクティブコンソールのサインインにのみ適用されます。SigV4 で署名された API リクエストには適用されません。プログラムによるアクセス (既存のアクセスキー、クロスアカウントロールなど) がある場合は、それを使用して を呼び出しsignin:DeleteConsoleAuthorizationConfiguration、制限ポリシーを削除します。使用する認証情報には、 を呼び出すアクセス許可が必要ですsignin:DeleteConsoleAuthorizationConfiguration。AWSSignInResourcePolicyManagemen管理ポリシーには、この permission. AWS recommends temporary credentials over long-term IAM user access keys が含まれています。メンバーアカウントの場合、管理アカウント管理者はメンバーアカウントOrganizationAccountAccessRoleで引き受けて一時的な認証情報を取得できます。このロールは、組織に招待されたアカウントでは自動的に作成されません。

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

または、特定のアクセス許可ステートメントを削除します。

```
# First, list statements to get the statement ID
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

オプション 2: AWS サポートに問い合わせる

プログラムによるアクセスがなく、アカウントアクセスOrganizationAccountAccessRoleに を使用できない場合は、 AWS サポートに連絡してロックアウト復旧プロセスを開始してください。

復旧プロセスは次のように機能します。

1. 上記のオプションを使用して問題を解決できない場合は、 サポートセンターで AWS サポートケースを開きます。 AWS サポートは、アカウントを調べる前に ID を検証します。検証方法には、ルートユーザーアカウントの E メールアドレスの確認、電話検証コールへの応答、アカウントのセキュリティ質問への応答などがあります。
2. AWS サポートは、コンソールアクセスの問題がリソースベースのポリシーのロックアウトによって引き起こされることを確認します。
3. AWS サポートは復旧ポータルリンクを共有します。このリンクを使用して、 アクセスsignin:DeleteConsoleAuthorizationConfiguration許可を持つアカウントの IAM プリンシパルでサインインします。このアクセス許可により、プリンシパルはロックアウトの原因となるコンソール認可設定を削除できます。

> **Important**
>
> リカバリポータルは、すべてのリソース許可ステートメントを含む、アカウントのコンソール認可設定全体を削除します。リカバリポータルでは、 AWS サインインリソースベースのポリシーの再設定は許可されません。

復旧ポータルリンクは、 AWS サポートが共有してから 72 時間後に期限切れになります。その期間内に復旧を完了しない場合は、 AWS サポートに連絡してプロセスを再起動してください。

アクセスを回復した後:

- リソース許可ステートメントを確認して更新し、適切に設定された除外されたプリンシパルを含めます。
- コンソール認可を再度有効にする前に、予想されるネットワークからのコンソールアクセスをテストします。
- 今後の参照用に復旧手順を文書化します。

行った変更がすぐに表示されないことがある

ポリシーの変更はグローバルにレプリケートされますが、レプリケーションには数分かかる場合があります。

解決策:

- グローバルレプリケーションが完了するまで、ポリシーを変更してから数分待ちます。
- get-resource-policy コマンドを使用して変更を確認します。

```
aws signin get-resource-policy --region <your-region>
```

- ポリシー評価イベントの AWS CloudTrail ログをチェックして、新しいポリシーが評価されていることを確認します。
- オペレーションに正しいリージョンを使用していることを確認します (書き込みオペレーションでは を使用する必要がありますus-east-1)。
- VPC エンドポイントベースの条件を使用する場合は、VPC エンドポイントポリシーも正しく設定されていることを確認します。

一般的なポリシーレプリケーションの問題:

- キャッシュされたサインインページ: ブラウザはサインインページをキャッシュする場合があります。ブラウザキャッシュをクリアするか、シークレットウィンドウを使用してポリシーの変更をテストします。
- 競合するステートメント: 複数のアクセス許可ステートメントがある場合は、相互に競合していないことを確認します。get-resource-policy 統合ポリシーを確認するには、 を使用します。
- VPC エンドポイントポリシー: AWS サインインポリシーは、VPC エンドポイントポリシーと連動します。どちらも必要なアクセスを許可する必要があります。

AWS サインイン条件キーリファレンス

このページでは、 AWS サインインリソースベースのポリシーとリソースコントロールポリシー (RCPs) で使用できる条件キーを一覧表示し、各キーが適用される評価フェーズとアクションを示します。 AWS サインインにのみ固有`signin:PrincipalArn`であり、その他は AWS グローバル条件キーです。グローバルキーの定義については、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。

サービス認可リファレンスのアクションと条件キーの完全なリストについては、AWS 「サインインのアクション、リソース、および条件キー」を参照してください。

ネットワークベースの条件キー

これらの条件キーは、リクエストの送信元をチェックします。 AWS Sign-In は、リソースベースのポリシーと RCPs の両方で、すべての AWS サインインアクション (`signin:Authenticate`、`signin:AuthorizeOAuth2Access`、`signin:CreateOAuth2Token`) についてそれらを評価します。

ネットワークベースの条件キー

条件キー	オペレータ	説明	使用ルール
`aws:SourceIp`	`IpAddress` , `NotIpAddress`	パブリック IP アドレスまたは CIDR 範囲	リクエストが VPC エンドポイントを使用する場合には存在しません。同じステートメントで VPC ベースの条件と組み合わせる場合は、 `IfExists` 演算子を使用します。
`aws:SourceVpc`	`StringEquals` , `StringNotEquals`	VPC ID (`vpc-xxxxxxxx`)	リクエストが VPC エンドポイントを使用している場合にのみ存在します。と `aws:RequestedRegion` を使用して、クロスリージョン VPC ID の衝突を防止します。

条件キー	オペレータ	説明	使用ルール
aws:SourceVpce	StringEquals , StringNotEquals	VPC エンドポイント ID (vpce-xxxxxxxx)	リクエストが VPC エンドポイントを使用している場合にのみ存在します。
aws:VpcSourceIp	IpAddress , NotIpAddress	VPC 内のプライベート IP	aws:VpcSourceIp 条件キーは必ず aws:SourceVpc または aws:SourceVpce 条件キーとともに使用してください。
aws:RequestedRegion	StringEquals , StringNotEquals	ターゲット AWS リージョンコード	クロスリージョン VPC ID の衝突を防ぐために を使用する場合aws:SourceVpc に推奨されます。複数のリージョンを指定できます。

> **Important**
>
> 1 つのリクエストにはaws:SourceIp、両方ではなく、 (パブリックネットワーク) またはaws:SourceVpc (VPC エンドポイント) が含まれます。両方のパスを対象とする拒否なしポリシーを記述する場合は、IfExists演算子 (などNotIpAddressIfExists) を使用するか、個別のステートメントを作成します。

ID ベースの条件キー

これらの条件キーは、リクエストを行っているユーザーをチェックします。これらは、プリンシパル ID が確立された認証後アクション (signin:AuthorizeOAuth2Access および signin:CreateOAuth2Token) でのみ使用できます。

ID ベースの条件キー

条件キー	オペレータ	説明	例
aws:PrincipalArn	ArnEquals , ArnLike, ArnNotEquals , StringEquals , StringLike	認証された IAM プリンシパルの ARN	arn:aws:iam::123456789012:user/alice , arn:aws:iam::123456789012:role/Admin
aws:PrincipalAccount	StringEquals , StringNotEquals	AWS プリンシパルのアカウント ID	123456789012

サービス固有の条件キー: signin:PrincipalArn

次の条件キーは AWS サインインに固有であり、グローバル AWS キーではありません。これは、認証前評価中にのみ使用できます。を使用してsignin:PrincipalArn、認証が完了する前にサインインを開始するプリンシパルを識別します。これは と同等の事前認証でありaws:PrincipalArn、認証後までは使用できません。

オペレータ

ARN 演算子 (ArnEquals、ArnLike、ArnNotEquals、ArnNotLike) と文字列演算子 (StringEquals、StringLike)。

可用性

AWS サインインには、事前認証フェーズ (signin:Authenticateアクション) 中のリクエストコンテキストにこのキーが含まれます。認証後のアクション (signin:AuthorizeOAuth2Access および) では使用できませんsignin:CreateOAuth2Token。

データ型

ARN。文字列演算子ではなく ARN 演算子を使用します。

値の型

単一値。

以下でサポート

リソースベースのポリシーと RCPs。

ARN 演算子を使用して値を比較します。次のプリンシパルタイプを指定できます。

- AWS アカウント ルートユーザー (arn:aws:iam::123456789012:root)
- IAM ユーザー (arn:aws:iam::123456789012:user/*user-name*)
- IAM ロール (arn:aws:iam::123456789012:role/*role-name*)

ユースケース: 除外されたプリンシパル ID をネットワーク制限から除外し、他のすべてのアクセス試行に対してネットワークコントロールを適用しながらロックアウトを防止します。

例 – ルートユーザーを除き、不正なネットワークからの事前認証アクセスを拒否します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Effect": "Deny",
```

```
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

このポリシーは、アカウントのルートユーザーを除き、203.0.113.0/24IP 範囲外からのコンソールアクセスを拒否します。認証前ステートメントは、認証が完了する前に signin:PrincipalArn を使用してルートユーザーを除外します。認証後ステートメントはaws:PrincipalArn、OAuth トークン交換中に、認証後に を使用して同じプリンシパルを除外します。「ポリシーの例」を参照してください。

アクション別の条件キーの可用性

アクション別の条件キーの可用性

条件キー	サインイン：認証	signin:AuthorizeOAuth2Access	signin:CreateOAuth2Token
aws:SourceIp	はい	はい	はい
aws:SourceVpc	はい	はい	はい
aws:SourceVpce	はい	はい	はい
aws:VpcSourceIp	はい	はい	はい
aws:RequestedRegion	はい	はい	はい

条件キー	サインイン：認証	signin:AuthorizeOAuth2Access	signin:CreateOAuth2Token
aws:PrincipalArn	–	はい	はい
aws:PrincipalAccount	–	はい	はい
signin:PrincipalArn	はい	–	–

> **Note**
>
> signin:CreateAccount アクションはコンソールプライベートアクセスの VPC エンドポイントポリシーでのみ使用され、リソースベースのポリシーまたは RCPsでは使用できません。サービス固有の条件キーは関連付けられていません。コンソールのプライベートアクセスを参照してください。

関連情報

- リソースベースのポリシーとリソースコントロールポリシーによるコンソールアクセスの制御
- AWS マネジメントコンソール プライベートアクセス
- AWS グローバル条件コンテキストキー
- AWS サインインのアクション、リソース、および条件キー

AWS アクセスポータルにサインインする

IAM Identity Center のユーザーは のメンバーです AWS Organizations。IAM Identity Center のユーザーは、特定のサインイン URL を使用して AWS アクセスポータルにサインインすることで、複数の AWS アカウント およびビジネスアプリケーションにアクセスできます。特定のサインイン URL の詳細については、「AWS アクセスポータル」を参照してください 。

IAM Identity Center のユーザー AWS アカウント として にサインインする前に、以下の必須情報を収集します。

- 企業ユーザー名
- 企業パスワード
- 特定のサインイン URL

> **Note**
>
> サインインすると、 AWS アクセスポータルセッションは 8 時間有効です。8 時間後に再度サインインする必要があります。

AWS アクセスポータルにサインインするには

1. ブラウザウィンドウで、 `https://your_subdomain.awsapps.com/start`やデュアルスタック URL 形式 など、E メールで提供されたサインイン URL を貼り付けます`https://[IAM Identity Center instance ID].portal.[Region].app.aws`。次に、エンター キーを押します。
2. 企業認証情報 (ユーザー名とパスワードなど) を使ってサインインします。

> **Note**
>
> 管理者から E メールでワンタイムパスワード (OTP) が送信され、初めてサインインする場合は、そのパスワードを入力します。サインインしたら、今後のサインイン用に新しいパスワードを作成する必要があります。

3. 認証コードの入力を求められた場合は、E メールを確認してください。次に、コードをコピーしてサインインページに貼り付けてください。

> **Note**
>
> 認証コードは通常、E メールで送信されますが、配信方法が異なる場合があります。E メールで認証コードを受け取っていない場合は、管理者に認証コードの詳細を確認してください。

4. IAM アイデンティティセンターでユーザーの MFA が有効になっている場合は、それを使用して認証します。
5. 認証後、ポータルに表示される任意の AWS アカウント およびアプリケーションにアクセスできます。

   a. にサインインするには、 AWS マネジメントコンソール 「アカウント」タブを選択し、管理する個々のアカウントを選択します。

      ユーザーのロールが表示されます。アカウントのロール名を選択して AWS マネジメントコンソールを開きます。アクセスキーを選択して、コマンドラインまたはプログラムによるアクセスの認証情報を取得します。

   b. [アプリケーション] タブを選択して使用可能なアプリケーションを表示し、アクセスするアプリケーションのアイコンを選択します。

IAM アイデンティティセンターにユーザーとしてサインインすると、セッションと呼ばれる一定の期間、リソースにアクセスするための認証情報が提供されます。デフォルトでは、ユーザーが AWS アカウント にサインインできる時間は 8 時間です。IAM Identity Center 管理者は、最小 15 分から最大 90 日までの期間を指定できます。セッションが終了した後は、再びサインインできます。

追加情報

IAM アイデンティティセンターのユーザーについての情報は、以下のリソースを参照してください。

- IAM アイデンティティセンターの概要については、「IAM アイデンティティセンターとは」を参照してください。
- AWS アクセスポータルの詳細については、AWS 「 アクセスポータルの使用」を参照してください。

- IAM アイデンティティセンターのセッションの詳細については、「ユーザー認証」を参照してください。
- IAM アイデンティティセンターのユーザーパスワードをリセットする手順については、「の IAM Identity Center パスワードを忘れました AWS アカウント」を参照してください。
- お客様またはお客様の組織が IP またはドメインフィルタリングを実装している場合、 AWS アクセスポータルを作成および使用するドメインを許可リストに登録する必要がある場合があります。IAM Identity Center は、IPv4 エンドポイントとデュアルスタックエンドポイントの両方をサポートしています。ネットワークで IPv6 を使用している場合は、デュアルスタックのエンドポイントドメインを使用します。ドメインの許可リストの詳細については、許可リストに追加するドメイン を参照してください。

を使用してサインインする AWS Command Line Interface

による AWS CLI 認証方法を確立する必要があります AWS。ワークフローとセキュリティ要件に最適な方法を選択します。

- コンソール認証情報を使用してログインする (推奨) AWS アカウントアクセスに root、IAM ユーザー、または IAM とのフェデレーションを使用する場合。
- IAM Identity Center 認証情報を使用してログインする AWS アカウントアクセスに Identity Center を使用する場合。

コンソール認証情報を使用してログインする (推奨)

この認証方法では、 でコンソール認証情報を使用できるため AWS CLI、アカウントのセットアップから数分以内に AWS プログラムで を簡単に開始できます。、 AWS SDKs AWS CLI、 などのローカル開発ツール間でシームレスに動作する一時的な認証情報を取得できます AWS Tools for PowerShell。

前提条件

- をインストールします AWS CLI。詳細については、「AWS CLIの最新バージョンのインストールまたは更新」を参照してください。`aws login` コマンドを使用するには、2.32.0 以降のバージョンが必要です。
- ルートユーザー、IAM ユーザー AWS マネジメントコンソール 、または IAM とのフェデレーションを通じて にサインインするためのアクセス。IAM Identity Center を使用する場合は、代わりに「IAM Identity Center 認証情報を使用してログインする」を参照してください。
- IAM ID に適切なアクセス許可があることを確認します。SignInLocalDevelopmentAccess 管理ポリシーを IAM ユーザー、ロール、またはグループにアタッチします。ルートユーザーとしてサインインする場合、追加のアクセス許可は必要ありません。

コンソール認証情報を使用してログインするには

1. 次のコマンドを実行して、ブラウザベースの認証プロセスを開始します。

   ```
   $ aws login
   ```

   `aws login` コマンドは、いくつかのオプションパラメータをサポートしています。

- `aws login --remote` - デバイスがブラウザをサポートしていない場合のクロスデバイス認証用

> **Note**
>
> 同一デバイス (`aws login`) 認証およびデバイス間 (`aws login --remote`) 認証へのアクセスを制御できます。関連する IAM ポリシーで次のリソース ARN を使用します。
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost` – この ARN は、`aws login` による同一デバイス認証に使用します。
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote` – この ARN は、`aws login --remote` によるデバイス間認証に使用します。

- `aws login --profile profile-name` - 特定のプロファイルで認証するには
- `aws login --region region` - 特定のリージョンで認証するには

2. ターミナルのプロンプトに従います。コマンドによってデフォルトのブラウザが自動的に開き、認証プロセスが案内されます。認証に成功すると、 AWS CLI セッションは最大 12 時間有効です。
3. セッションを終了するには、以下を使用します。

```
$ aws logout
```

を使用してプログラムで AWS サービスにアクセスする場合は AWS Tools for PowerShell、「AWS Tools for PowerShell with AWS」を参照してください。 AWS SDKs「AWS SDKs」を参照してください。

IAM Identity Center 認証情報を使用してログインする

AWS アクセスポータルを使用すると、IAM Identity Center ユーザーは を選択し AWS アカウント 、の一時的なセキュリティ認証情報を簡単に取得できます AWS CLI。これらの認証情報を取得する方法の詳細については、「のリージョンの可用性 AWS ビルダー ID」を参照してください。IAM Identity Center でユーザーを認証するように AWS CLI を直接設定することもできます。

IAM Identity Center 認証情報を使用してログインするには

1. 前提条件を満たしていることを確認してください。
2. 初めてサインインする場合は、aws configure sso ウィザードを使用してプロファイルを設定してください。
3. プロファイルを設定したら、次のコマンドを実行し、ターミナルのプロンプトに従います。

```
$ aws sso login --profile my-profile
```

追加情報

コマンドラインを使用したサインインの詳細については、次のリソースを参照してください。

- コンソール認証情報を使用して AWS ローカル開発にログインする方法の詳細については、「AWS CLI の認証とアクセス認証情報」を参照してください。
- AWS CLI サインインプロセスの詳細については、「 の短期認証情報による認証 AWS CLI」を参照してください。
- IAM Identity Center の設定の詳細については、「IAM Identity Center を使用する AWS CLI ように を設定する」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としてのサインイン

フェデレーティッドアイデンティティは、外部 ID を持つ安全な AWS アカウント リソースにアクセスできるユーザーです。外部認証は、企業の ID ストア (LDAP や Windows の Active Directory など) またはサードパーティー (Login with Amazon、Facebook、または Google でのログインなど) から取得できます。フェデレーティッド ID は、 AWS マネジメントコンソール または AWS アクセスポータルでサインインしません。使用する外部アイデンティティのタイプによって、フェデレーション ID のサインイン方法が決まります。

管理者は、`https://signin.aws.amazon.com/federation` を含むカスタム URL を作成する必要があります。詳細については、「AWS マネジメントコンソールへのカスタムアイデンティティブローカーアクセスの有効化」を参照してください。

> **Note**
>
> 管理者はフェデレーション ID を作成します。フェデレーション ID としてサインインする方法の詳細については、管理者にお問い合わせください。

フェデレーティッドアイデンティティの詳細については、「ウェブ ID フェデレーションについて」を参照してください

でサインインする AWS ビルダー ID

AWS ビルダー ID は、Amazon CodeCatalyst、Amazon Q Developer、および AWS トレーニング Certification などの一部のツールやサービスへのアクセスを提供する個人プロファイルです。 はユーザーを個人として AWS ビルダー ID 表し、既存の AWS アカウントにある認証情報やデータから独立しています。他の個人プロファイルと同様に、 は、個人、教育、キャリアの目標を進めるにつれて、お客様と共に AWS ビルダー ID 残ります。

は、すでに所有 AWS アカウント している、または作成する可能性のあるものを AWS ビルダー ID 補完します。は、作成した AWS リソースのコンテナ AWS アカウント として機能し、それらのリソースのセキュリティ境界を提供しますが、 はユーザーを個人として AWS ビルダー ID 表します。詳細については、「AWS ビルダー ID およびその他の AWS 認証情報」を参照してください。

AWS ビルダー ID は無料です。で消費する AWS リソースに対してのみ料金が発生します AWS アカウント。料金の詳細については、「AWS 料金表」を参照してください。

お客様またはお客様の組織が IP またはドメインフィルタリングを実装する場合、ドメインを許可リストに登録して、 AWS ビルダー IDを作成して使用する必要があります。ドメインの許可リストの詳細については、許可リストに追加するドメイン を参照してください。

> **Note**
>
> AWS Builder ID AWS は、 AWS エキスパートから学び、クラウドスキルをオンラインで構築できるオンライン学習センターである Skill Builder サブスクリプションとは異なります。AWS Skill Builder の詳細については、「AWS Skill Builder」を参照してください。

トピック

- を削除する AWS ビルダー ID
- AWS ビルダー ID 多要素認証 (MFA) の管理
- のプライバシーとデータ AWS ビルダー ID
- AWS ビルダー ID およびその他の AWS 認証情報

でサインインするには AWS ビルダー ID

1. アクセスする AWS ツールまたはサービスのAWS ビルダー ID プロファイルまたはサインインページに移動します。例えば、Amazon CodeCatalyst にサインインするには、https://codecatalyst.aws にアクセスします。
2. にサインインする方法を選択する AWS ビルダー ID
   - 既存のアカウントがある場合
   - Google アカウントを持っている
   - Apple アカウントを持っている
   - GitHub アカウントを持っている
   - Amazon アカウントを持っている

既存のアカウントがある場合

1. 既存のアカウントの場合は、 の作成に使用した E メールを入力し AWS ビルダー ID 、サインインを選択します。
2. の作成に使用した E メールを入力し AWS ビルダー ID 、サインインを選択します。
3. [AWS ビルダー IDでサインイン] ページで、[パスワード] を入力します。
4. (オプション) このデバイスから今後のサインインしたときに追加の確認を求められないようにするには、[信頼できるデバイスです]の横にあるボックスをチェックします。
5. [続行] をクリックしてください。
6. [追加認証が必要] ページが表示された場合は、ブラウザの指示に従って必要なコードまたはセキュリティキーを入力してください。

> **Note**
>
> セキュリティのため、ログインブラウザ、場所、デバイスを分析します。このデバイスを信頼していると報告した場合、サインインするたびに多要素認証 (MFA) コードを入力する必要はありません。詳細については、「信頼されたデバイス」を参照してください。

Google アカウントを持っている

Google アカウントが既に に関連付けられている場合は AWS ビルダー ID、別の E メールアドレスを使用してアプリケーションにサインインする必要があります。詳細については、「Google でサインインできない」を参照してください。

1. Google アカウントを使用して にサインインするには AWS ビルダー ID、Google で続行を選択します。
2. Google でサインイン ページで、Google アカウントがサインインするための情報を入力します。
3. 続行を選択して AWS アプリケーションのホームページをロードします。

Apple アカウントを持っている

Apple アカウントが既に に関連付けられている場合は AWS ビルダー ID、別の E メールアドレスを使用してアプリケーションにサインインする必要があります。詳細については、「Apple でサインインできない」を参照してください。

1. Apple アカウントを使用して にサインインするには AWS ビルダー ID、「Apple で続行」を選択します。
2. 「Apple でサインイン」ページで、Apple アカウントがサインインする情報を入力します。
3. 「続行」を選択して AWS アプリケーションのホームページをロードします。

GitHub アカウントを持っている

GitHub アカウントが既に に関連付けられている場合は AWS ビルダー ID、別の E メールアドレスを使用してアプリケーションにサインインする必要があります。詳細については、「GitHub でサインインできない」を参照してください。

1. GitHub アカウントを使用して にサインインするには AWS ビルダー ID、GitHub で続行」を選択します。
2. GitHub でサインインページで、サインインする GitHub アカウントの情報を入力します。
3. 続行を選択して AWS アプリケーションのホームページをロードします。

Amazon アカウントを持っている

Amazon アカウントが既に に関連付けられている場合は AWS ビルダー ID、別の E メールアドレスを使用してアプリケーションにサインインする必要があります。詳細については、「Amazon でサインインできない」を参照してください。

1. Amazon アカウントを使用して にサインインするには AWS ビルダー ID、「Amazon で続行」を選択します。
2. Amazon でサインイン ページで、Amazon アカウントがサインインするための情報を入力します。
3. 続行を選択して AWS アプリケーションのホームページをロードします。

のリージョンの可用性 AWS ビルダー ID

AWS ビルダー ID は以下の で利用できます AWS リージョン。を使用するアプリケーションは AWS ビルダー ID 、他のリージョンで動作する可能性があります。

名前	コード
米国東部 (バージニア北部)	us–east–1

を作成する AWS ビルダー ID

を使用する AWS ツールやサービスのいずれかにサインアップ AWS ビルダー ID するときに、 を作成します。 AWS ツールまたはサービスのサインアッププロセスの一環として、E メールアドレス、名前、パスワードでサインアップします。

パスワードは以下の条件を満たす必要があります。

- パスワードでは、大文字と小文字が区別されます。

- パスワードの長さは8文字から64文字の間でなければなりません。
- パスワードには、次の 4 つカテゴリから少なくとも 1 文字を含める必要があります。
  - 小文字 a～z
  - 大文字 A～Z
  - 数字 (0～9)
  - 英数字以外の文字 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 最後の3つのパスワードは再使用できません。
- 第三者から漏洩したデータセットを通じて公に知られているパスワードは使用できません。

> **Note**
>
> を使用するツールとサービスは AWS ビルダー ID 、 AWS ビルダー ID 必要に応じて を作成して使用します。

を作成するには AWS ビルダー ID

1. アクセスする AWS ツールまたはサービスのAWS ビルダー ID プロファイルまたはサインアップページに移動します。例えば、Amazon CodeCatalyst にサインインするには、https://codecatalyst.aws にアクセスします。
2. の作成方法を選択する AWS ビルダー ID
   - Google アカウントを使用するには、Google で続行を選択し、プロンプトに従ってサインアッププロセスを完了します。これにより、以下のステップ 3～8 を省略します。ステップ 9 に進みます。
   - Apple アカウントを使用するには、「Apple で続行」を選択し、プロンプトに従ってサインアッププロセスを完了します。これにより、以下のステップ 3～8 を省略します。ステップ 9 に進みます。

     > **Note**
     >
     > Sign in with Apple で iCloud+ の「E メールの非表示」機能を有効にすると、 AWS ビルダー ID は実際の E メールアドレスではなく、Apple アカウントで指定された E メールアドレスの非表示で作成されます。この E メールアドレスを変更することはできませんが、姓名は編集可能です。にサインインする必要がある場合は AWS ビルダー ID、E メールアドレスの非表示を使用する必要があります。 AWS ビル

ダー ID は E メール通信の送信に E メールアドレスの非表示を使用します。詳細については、「Apple でサインインして E メールを非表示にする」を参照してください。

- GitHub アカウントを使用するには、GitHub で続行を選択し、プロンプトに従ってサインアッププロセスを完了します。これにより、以下のステップ 3～8 を省略します。ステップ 9 に進みます。
- Amazon アカウントを使用するには、「Amazon で続行」を選択し、プロンプトに従ってサインアッププロセスを完了します。これにより、以下のステップ 3～8 を省略します。ステップ 9 に進みます。
- E メールとパスワードを使用してアカウントを作成するには、次のステップに進みます。

3. [AWS ビルダー IDを作成] ページで、[メールアドレス] を入力します。個人用の E メールを使用することをお勧めします。
4. 次へをクリックします。
5. [お名前]を入力し、[次へ]を選択します。
6. E メール確認ページで、E メールアドレスに送信された確認コードを入力します。確認を選択します。E メールプロバイダーによっては、E メールの受信まで数分かかる場合があります。スパムフォルダと迷惑メールフォルダにコードがないか確認してください。5 分 AWS 経っても からの E メールが表示されない場合は、コードの再送信を選択します。
7. お客様のEメールを確認した後、パスワードの選択ページで、パスワード とパスワードの確認を入力してください。
8. セキュリティ強化として キャプチャが表示される場合は、表示されている文字を入力してください。
9. [作成] AWS ビルダー ID を選択します。

信頼されたデバイス

サインインページで This is a trusted device(これは信頼できるデバイスです) というオプションを選択すると、そのデバイスのそのウェブブラウザからの今後のすべてのサインインを承認されたものとみなします。つまり、信頼できるデバイスには MFA コードを入力する必要がないということです。ただし、ブラウザ、Cookie、または IP アドレスが変更された場合は、MFA コードを使用して追加の認証を行う必要がある場合があります。

AWS を使用するツールとサービス AWS ビルダー ID

を使用してサインイン AWS ビルダー ID すると、次の AWS ツールやサービスにアクセスできます。料金で提供される機能や利点にアクセスするには、 が必要です AWS アカウント。

デフォルトでは、 を使用して AWS ツールまたはサービスにサインインすると AWS ビルダー ID、セッション期間は 90 日間のセッション期間を持つ Amazon Q Developer を除き、30 日間続きます。セッションが終了すると、再びサインインする必要があります。

AWS クラウドコミュニティ

Community.aws は、 と AWS ビルダーコミュニティがアクセスできるプラットフォームです AWS ビルダー ID。ここでは、教育コンテンツの検索、個人的な考えやプロジェクトの共有、他のユーザーの投稿へのコメント、お気に入りのビルダーの参照を行うことができます。

Amazon CodeCatalyst

Amazon CodeCatalyst の使用を開始する AWS ビルダー ID ときに を作成し、問題、コードコミット、プルリクエストなどのアクティビティに関連付けられるエイリアスを選択します。チームが次のプロジェクトを成功させるために必要なツール、インフラストラクチャ、環境が揃っている Amazon CodeCatalyst スペースに他の人を招待できます。新しいプロジェクトをクラウドにデプロイ AWS アカウント するには、 が必要です。

AWS Migration Hub

を使用して AWS Migration Hub (Migration Hub) にアクセスします AWS ビルダー ID。Migration Hub を使用すると、1 か所で既存のサーバーを検出し、移行を計画して、各アプリケーションの移行ステータスを追跡できます。

Amazon Q Developer

Amazon Q Developer は、生成 AI を活用した会話アシスタントであり、 AWS アプリケーションの理解、構築、拡張、運用に役立ちます。詳細については、「Amazon Q Developer ユーザーガイド」の「Amazon Q Developer とは」を参照してください。

AWS re:Post

AWS re:Post は専門的な技術ガイダンスを提供するため、 AWS サービスを使用してより迅速にイノベーションを起こし、運用効率を向上させることができます。でサインイン AWS ビルダー ID し、 AWS アカウント または クレジットカードなしで re:Post でコミュニティに参加できます。

AWS スタートアップ

AWS ビルダー ID を使用してAWS スタートアップに参加し、学習コンテンツ、ツール、リソース、サポートを使用してスタートアップを成長させることができます AWS。

AWS トレーニング および 認定

を使用して AWS ビルダー ID 、AWS Skill Builder で AWS クラウド スキルを構築し、 AWS エキスパートから学び、業界で認められている認証情報を使用してクラウドの専門知識を検証できる AWS トレーニング および 認定にアクセスできます。

Kiro

Kiro は、仕様駆動型開発を使用してプロトタイプから本番稼働に移行するのに役立つエージェント IDE です。Kiro は、シンプルなタスクから複雑なタスクまで、プロンプトを詳細な仕様へ、そして作業コード、ドキュメント、テストに変換します。Kiro では、構築する内容がまさに目的であり、チームと共有する準備が整います。Kiro のエージェントは、困難な問題を解決し、ドキュメントやユニットテストの生成などのタスクを自動化するのに役立ちます。Kiro を使用すると、プロトタイプを超えた開発を行いながら、あらゆる工程で主導権を握ることができます。

ウェブサイト登録ポータル (WRP)

をAWS マーケティングウェブサイトの永続的な顧客 ID および登録プロファイル AWS ビルダー ID として使用できます。新しいウェビナーに登録したり、登録または参加したすべてのウェビナーを視聴したりするには、「マイウェビナー」を参照してください。

AWS ビルダー ID プロファイルを編集する

プロファイルの情報はいつでも変更できます。の作成に使用した E メールアドレスと名前 AWS ビルダー ID、およびニックネームを編集できます。Google や Apple などのソーシャルログインを使用する場合、名前とニックネームのみが編集可能です。

[名前] は、他の人と交流するときに、ツールやサービスでどのように呼ばれるかを表します。ニックネームは、密接に協力する人 AWS、友人、その他の人々にどのように知られたいかを示します。

> **Note**
>
> を使用するツールとサービスは AWS ビルダー ID 、 AWS ビルダー ID 必要に応じて を作成して使用します。

プロファイル情報を編集するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. 個人情報を選択します。
3. 個人情報ページで、プロファイルの隣にある 編集を選択します。
4. プロフィールの編集ページで、名前と ニックネームに必要な変更を加えます。
5. 変更の保存をクリックします。プロファイルの更新が完了したことを知らせる緑色の確認メッセージが表示されます。

> **Note**
>
> 他のサインインパートナーのいずれかで名前とニックネームを変更しても、 AWS ビルダー IDの設定には反映されません。

連絡先情報を編集するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. 個人情報を選択します。
3. 個人情報ページで、連絡先情報の横にある 編集ボタンを選択します。
4. 連絡先情報の編集 ページで、メールアドレスを変更します。
5. [メールを確認] を選択します。ダイアログボックスが表示されます。
6. E メールでコードを受け取ったら、[E メールの確認] ダイアログボックスの [認証コード] にそのコードを入力します。確認を選択します。

AWS ビルダー ID パスワードを変更する

パスワードは以下の条件を満たす必要があります。

- パスワードでは、大文字と小文字が区別されます。
- パスワードの長さは8文字から64文字の間でなければなりません。
- パスワードには、次の 4 つカテゴリから少なくとも 1 文字を含める必要があります。
  - 小文字 a～z
  - 大文字 A～Z

- 数字 (0〜9)
- 英数字以外の文字 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

- 最後の3つのパスワードは再使用できません。

> **Note**
>
> パスワードの変更は、Google や Apple などのソーシャルログインを使用する AWS ビルダー ID アカウントでは使用できません。ソーシャルログインを使用してサインインした場合は、ソーシャルログインアカウントを使用してパスワードを管理します。ソーシャルログインのパスワードを変更するには:
>
> - Google アカウントについては、「(Google) パスワードの変更またはリセット」を参照してください。
> - Apple アカウントについては、「Apple アカウントのパスワードを変更する」を参照してください。
> - GitHub アカウントについては、GitHub アクセス認証情報の更新」を参照してください。
> - Amazon アカウントについては、「Amazon パスワードの変更方法」を参照してください。

AWS ビルダー ID パスワードを変更するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. セキュリティを選択します。
3. セキュリティ ページで、パスワードの変更を選択します。これにより、新しいページに移動します。
4. パスワードの再入力ページの パスワードに、現在のパスワードを入力します。次に [サインイン] を選択します。
5. [パスワードの変更] ページの [新しいパスワード] で、使用したい新しいパスワードを入力します。次に、[パスワードの確認] に、使用したい新しいパスワードを再入力します。
6. その後、[パスワードの変更] をクリックします。 AWS ビルダー ID プロフィールにリダイレクトされます。

のすべてのアクティブなセッションを削除する AWS ビルダー ID

[ログイン中のデバイス] には、現在ログインしているすべてのデバイスを表示できます。デバイスがわからない場合は、セキュリティ上のベストプラクティスとして、まずパスワードを変更してから、すべてのデバイスからサインアウトしてください。 AWS ビルダー IDビルダー ID の [セキュリティ] ページでは、アクティブなセッションをすべて削除することで、すべてのデバイスからサインアウトできます。

> **Note**
>
> AWS ビルダー ID は、IDE で Amazon Q Developer の 90 日間の延長セッションをサポートします。新しい IDE サインインごとに、2 つのセッションエントリを表示できます。IDE からサインアウトすると、有効ではなくなった IDE セッションも [サインインしたデバイス] に引き続き表示されます。これらのセッションは、90 日間の期限が切れると表示されなくなります。

すべてのアクティブなセッションを削除するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. セキュリティを選択します。
3. セキュリティ ページで、すべてのアクティブなセッションを削除 を選択します。
4. [すべてのセッションを削除] ダイアログボックスで、全て削除と入力します。すべてのセッションを削除することで、さまざまなブラウザなど AWS ビルダー ID、 を使用してサインインしたすべてのデバイスからサインアウトできます。次に [すべてのセッションを削除] を選択します。

> **Note**
>
> Google や Apple などのソーシャルログインアカウントを使用する場合、アクティブな AWS ビルダー ID セッションを削除しても、ソーシャルログインアカウントからログアウトされることはありません。

を削除する AWS ビルダー ID

次の手順では、 AWS ビルダー ID アカウントを削除する方法について説明します。

Warning

を削除すると AWS ビルダー ID 、次のようになります。

- アクセスの喪失 – を通じて以前にアクセスした AWS ツールやサービスにアクセスできなくなります AWS ビルダー ID。 AWS ビルダー ID は所有している AWS アカウントとは別のものであり、 を削除しても AWS アカウント AWS ビルダー ID は閉鎖されません。
- コンテンツの削除 – にのみ関連付けられている残りのコンテンツ AWS ビルダー ID は削除され、 を使用してアプリケーションからコンテンツにアクセスまたは復元できなくなります AWS ビルダー ID。
- 個人情報の削除 – の作成と管理に関連して提供した個人情報 AWS ビルダー ID は削除されます。ただし、削除リクエストの記録や個人を特定できない形式のデータなど、法律で要求または許可されている個人情報は保持 AWS される場合があります。

  AWS がお客様の情報を処理する方法の詳細については、AWS プライバシー通知を参照してください。AWS Communications Preferences Center にアクセスして、 AWS 通信設定を更新したり、サブスクリプションを解除したりできます。
- ソーシャルログインアカウントは変更されません – Google や Apple などのソーシャルログインを使用している場合、 を削除 AWS ビルダー ID しても、ソーシャルログインアカウントに関連するものは削除されません。これらのアカウントを削除する方法については、ソーシャルログインプロバイダーのドキュメントを参照してください。ソーシャルログインアカウントから AWS ビルダー ID 接続を削除しても AWS ビルダー ID アカウントは削除されませんが、 AWS ビルダー ID プロファイルにアクセスできなくなります。

を削除するには AWS ビルダー ID

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. プライバシーとデータを選択します。
3. [プライバシーとデータ] ページで、[削除 AWS ビルダー ID] の下に[削除 AWS ビルダー ID] を選択します。
4. 各免責事項の横にあるチェックボックスを選択し、続行する準備ができていることを確認します。
5. [Delete] AWS ビルダー ID (削除) をクリックします。

AWS ビルダー ID 多要素認証 (MFA) の管理

多要素認証 (MFA) は、セキュリティを強化するためのシンプルで効果的なメカニズムです。1 つ目の要因であるパスワードは、ユーザーが記憶する秘密であり、知識要因とも呼ばれます。その他の要因としては、所有要因 (セキュリティキーなど、ユーザーが持っているもの) や継承要因 (生体認証スキャンなど、ユーザー自身のもの) があります。 AWS ビルダー IDにレイヤーを追加するように MFA を設定することを強くお勧めします。

組み込みの認証アプリケーションを登録し、物理的に安全な場所に保管するセキュリティキーも登録することができます。組み込みの認証ソフトを使用できない場合は、登録済みのセキュリティキーを使用できます。認証アプリケーションについては、それらのアプリでクラウドバックアップまたは同期機能を有効にすることもできます。これにより、MFA デバイスを紛失または破損した場合に、プロファイルにアクセスできなくなることを防ぐことができます。

重要ポイント

- 複数の MFA デバイスを登録することをお勧めします。登録されているすべての MFA デバイスにアクセスできなくなると、 AWS ビルダー IDの復元ができなくなります。
- 登録した MFA デバイスを定期的に見直して、最新で機能していることを確認することをお勧めします。また、これらのデバイスは、使用しないときは物理的に安全な場所に保管してください。
- [Google で続行] を使用してアカウントを作成した場合は、Google アカウントを通じて多要素認証を有効にできます。詳細については、「2 段階認証を有効にする」を参照してください。
- Continue with Apple を使用してアカウントを作成した場合、Apple アカウントで多要素認証が既に有効になっている可能性があります。そうでない場合は、有効にする方法の詳細については、「Apple アカウントの 2 要素認証」を参照してください。
- Continue with GitHub を使用してアカウントを作成した場合は、GitHub アカウントを通じて多要素認証を有効にできます。詳細については、「Configuring (GitHub) two-factor authentication」を参照してください。
- Continue with Amazon を使用してアカウントを作成した場合は、Amazon アカウントを通じて多要素認証を有効にできます。詳細については、「2 ステップ検証とは」を参照してください。

で使用できる MFA タイプ AWS ビルダー ID

AWS ビルダー ID は、次の多要素認証 (MFA) デバイスタイプをサポートしています。

FIDO2 認証機能

FIDO2 は CTAP2 と WebAuthn を含む標準であり、パブリックキー暗号に基づいています。FIDO 認証情報は、認証情報が作成された Web サイト (AWSなど) 固有のものであるため、フィッシング詐欺に対して強固です。

AWS は、FIDO 認証の最も一般的なフォームファクタとして、組み込み認証とセキュリティキーの 2 つをサポートしています。FIDO 認証機能の最も一般的なタイプの詳細については、以下を参照してください。

トピック

- 組み込みの認証機能
- セキュリティキー
- パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証システム

組み込みの認証機能

MacBook の TouchID や、Windows Hello 対応のカメラなどの一部デバイスはビルトイン認証システムを装備しています。お使いのデバイスが WebAuthn を含む FIDO プロトコルと互換性がある場合は、指紋や顔を第二の要素として使用できます。詳細については、FIDO 認証 を参照してください。

セキュリティキー

FIDO2 対応の外付け USB、BLE、または NFC 接続のセキュリティキーを購入できます。MFA デバイスの入力を求められたら、キーのセンサーをタップします。YubiKey または Feitian は互換性のあるデバイスを製造しています。互換性のあるすべてのセキュリティキーのリストについては、FIDO 認定製品をご覧ください。

パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証システム

複数のサードパーティプロバイダーが、パスワードマネージャー、FIDO モードのスマートカード、その他のフォームの要素の機能として、モバイルアプリケーションの FIDO 認証をサポートしています。これらの FIDO 互換デバイスは IAM Identity Center で動作しますが、このオプションを MFA で有効にする前に FIDO 認証機能をご自身でテストすることをお勧めします。

> **Note**
>
> FIDO 認証機能の中には、パスキーと呼ばれる検出可能な FIDO 認証情報を作成できるものもあります。パスキーは、パスキーを作成したデバイスにバインドされている場合もあれ

ば、同期可能でクラウドにバックアップされている場合もあります。例えば、サポートされている Macbook で Apple Touch ID を使ってパスキーを登録し、ログイン時に画面に表示される指示に従って iCloud のパスキーで Google Chrome を使って Windows ラップトップからサイトにログインできます。どのデバイスが同期可能なパスキーをサポートしていると、オペレーティングシステムとブラウザ間の現在のパスキーの相互運用性をサポートしているの詳細は、FIDO アライアンスとワールドワイドウェブコンソーシアム (W3C) が管理するリソースである passkeys.dev の「デバイスサポート」を参照してください。

認証アプリケーション

認証アプリケーションは、ワンタイムパスワード (OTP) ベースのサードパーティー認証機能を備えています。モバイルデバイスやタブレットにインストールされた認証アプリケーションを、許可された MFA デバイスとして使用することができます。サードパーティー認証アプリケーションは、6 桁の認証コードを生成できる標準ベースのタイムベースドワンタイムパスワード (TOTP) アルゴリズムである RFC 6238 に準拠している必要があります。

MFA を求めるプロンプトが表示されたら、認証アプリケーションから有効なコードを入力ボックスに入力する必要があります。ユーザーに割り当てられた各 MFA デバイスは一意であることが必要です。1 人の ユーザーに対して 2 つの認証アプリを登録することができます。

以下の有名なサードパーティの認証アプリケーションから選択できます。ただし、TOTP 準拠のアプリケーションは AWS ビルダー ID MFA で動作します。

オペレーティングシステム	テスト済みの認証アプリ
Android	1Password、Authy、Duo Mobile、Microsoft Authenticator、Google Authenticator
iOS	1Password、Authy、Duo Mobile、Microsoft Authenticator、Google Authenticator

AWS ビルダー ID MFA デバイスを登録する

> **Note**
>
> MFA にサインアップし、サインアウトしてから同じデバイスでサインインすると、信頼できるデバイスでは MFA の入力を求められない場合があります。

認証アプリケーションを使用して MFA デバイスを登録するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. セキュリティを選択します。
3. セキュリティ ページで、デバイスの登録を選択します。
4. MFA デバイスの登録 ページで、認証アプリケーションを選択します。
5. AWS ビルダー ID は、QR コードグラフィックを含む設定情報を操作して表示します。図は、QR コードに対応していない認証アプリケーションでの手動入力に利用できる「シークレット設定キー」を示しています。
6. 認証アプリケーションを開きます。アプリのリストについては、「認証アプリケーション」を参照してください。

   認証アプリケーションが複数の MFA デバイスまたはアカウントをサポートしている場合は、新しい MFA デバイスまたはアカウントを作成するオプションを選択します。
7. MFA アプリケーションが QR コードをサポートしているかどうかを判断し、認証アプリケーションの設定 ページで以下のいずれかの操作を行います。

   1. QR コードの表示を選択し、アプリケーションを使用して QR コードをスキャンします。例えば、カメラアイコンまたは スキャンコード に似たオプションを選択します。次に、デバイスのカメラでコードをスキャンします。
   2. シークレットキーを表示をクリックし、そのシークレットキーを MFA アプリケーションに入力します。

   完了すると、認証アプリケーションがワンタイムパスワードを生成して表示します。
8. 認証システムコードボックスに、現在認証アプリケーションに表示されているワンタイムパスワードを入力します。MFA の割り当てを選択します。

> **Important**
>
> コードを生成したら、即時にリクエストを送信します。コードを生成し、リクエストの送信に時間がかかりすぎると、MFA デバイスは に正常に関連付けられますが AWS ビルダー ID、MFA デバイスは同期されません。これは、タイムベースドワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスの再同期ができます。詳細については、「認証アプリケーションを使用して登録やサインインをしようとすると、「予期しないエラーが発生しました」というメッセージが表示されます」を参照してください。

9. デバイスにわかりやすい名前を付けるには AWS ビルダー ID、名前の変更を選択します。この名前は、このデバイスを登録した他のデバイスと区別するのに役立ちます。

これで、MFA デバイスを で使用する準備ができました AWS ビルダー ID。

セキュリティキーを AWS ビルダー ID MFA デバイスとして登録する

セキュリティキーを使用して MFA デバイスを登録するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. セキュリティを選択します。
3. セキュリティページで、デバイスの登録を選択します。
4. MFA デバイスの登録ページで、セキュリティキーを選択します。
5. セキュリティキーが有効になっていることを確認します。別の物理セキュリティキーを使用する場合は、それをコンピューターに接続します。
6. 画面上の指示に従います。操作性は、オペレーティングシステムとブラウザによって異なります。
7. デバイスにわかりやすい名前を付けるには AWS ビルダー ID、名前の変更を選択します。この名前は、このデバイスを登録した他のデバイスと区別するのに役立ちます。

これで、MFA デバイスを で使用する準備ができました AWS ビルダー ID。

AWS ビルダー ID MFA デバイスの名前を変更する

MFA デバイスの名前を変更するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. セキュリティを選択します。ページに到達すると、名前の変更がグレーアウトされていることがわかります。
3. 変更する MFA デバイスを選択します。これにより、名前の変更を選択できます。そしたら、ダイアログボックスが表示されます。
4. 表示されるプロンプトで、MFA デバイス名に新しい名前を入力し、名前の変更を選択します。名前を変更したデバイスは、多要素認証 (MFA) デバイスに表示されます。

MFA デバイスの削除

2 つ以上の MFA デバイスをアクティブに保つことを推奨します。デバイスを削除する前に、「AWS ビルダー ID MFA デバイスを登録する」を参照して交換用の MFA デバイスを登録してください。の多要素認証を無効にするには AWS ビルダー ID、プロファイルから登録されたすべての MFA デバイスを削除します。

MFA デバイスを削除するには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. セキュリティを選択します。
3. 変更する MFA デバイスを選択したら、削除を選択します。
4. MFA デバイスを削除しますか?モーダルでは、指示に従ってデバイスを削除してください。
5. 削除をクリックします。

削除したデバイスは、[Multi-factor authentication (MFA) devices] (多要素認証 (MFA) デバイス) に表示されなくなります。

のプライバシーとデータ AWS ビルダー ID

「AWS プライバシー通知」には、私たちがお客様の個人データをどのように扱うかが概説されています。 AWS ビルダー ID プロファイルを削除する方法については、「」を参照してくださいを削除する AWS ビルダー ID。

AWS ビルダー ID データをリクエストする

および でアクセスした AWS アプリケーション AWS ビルダー ID とサービスに関連する個人情報は、リクエストして表示できます AWS ビルダー ID。他の AWS ウェブサイト、アプリケーション、製品、サービス、イベント、エクスペリエンスに関連して提供される個人情報など、データサブジェクトの権利を行使する方法の詳細については、「」を参照してくださいhttps://aws.amazon.com/privacy。

個人データをリクエストするには

1. で AWS ビルダー ID プロファイルにサインインしますhttps://profile.aws.amazon.com。
2. AWS ビルダー ID データを選択します。
3. マイ AWS ビルダー ID データページの「 の削除 AWS ビルダー ID」で、「データのリクエスト」を選択します。
4. リクエストが受領され 30 日以内に処理が完了されることを知らせる緑色の確認メッセージがページ上部に表示されます。
5. リクエストが処理されたことを通知するメールを受け取ったら、 AWS ビルダー ID ビルダー ID プロフィールの [プライバシーとデータ] ページに戻ってください。新しく表示された データを含む ZIP アーカイブをダウンロードボタンを選択します。

   データリクエストが保留中の間は、 AWS ビルダー IDを削除することはできません。

AWS ビルダー ID およびその他の AWS 認証情報

AWS ビルダー ID は、 AWS アカウント またはサインイン認証情報とは別のものです。 AWS ビルダー ID と のルートユーザー E メールに同じ E メールを使用できます AWS アカウント。

AWS ビルダー ID:

- が使用するツールやサービスにアクセスできます AWS ビルダー ID。
- AWS アカウント またはアプリケーションで指定したポリシーや設定など、既存のセキュリティコントロールには影響しません。
- 既存のルート、IAM アイデンティティセンター、IAM ユーザー、認証情報、またはアカウントを置き換えません。
- AWS マネジメントコンソール、、 AWS SDKs AWS CLI、または AWS Toolkit AWS にアクセスするための IAM 認証情報を取得できません。

AWS アカウント は、連絡先情報と支払い情報を含むリソースコンテナです。S3, EC2、Lambda などの課金および計測された AWS サービスを運用するセキュリティ境界を確立します。アカウント所有者は、 AWS アカウント で にサインインできます AWS マネジメントコンソール。詳細については、「AWS マネジメントコンソールへのサインイン」を参照してください。

が既存の IAM Identity Center ID とどのように AWS ビルダー ID 関連しているか

アイデンティティを所有する個人は、 AWS ビルダー IDを管理する。学校や職場など、他の組織で持っている他のアイデンティティとは関連がありません。IAM アイデンティティセンターのワークフォース ID を使用して作業自身を表し、 AWS ビルダー ID を使用してプライベート自身を表すことができます。これらの ID は独立して動作します。

IAM アイデンティティセンター (AWS シングルサインオンの後継) AWS のユーザーは、企業の IT 管理者またはクラウド管理者、または Okta、Ping、Azure などの組織の ID プロバイダーの管理者によって管理されます。IAM アイデンティティセンターのユーザーは、 AWS Organizationsの複数のアカウントのリソースにアクセスできます。

複数の AWS ビルダー ID プロファイル

各 ID が一意の E メールアドレスを使用している AWS ビルダー ID 限り、複数の を作成できます。ただし、複数の を使用すると、どの目的でどの を使用した AWS ビルダー ID かを思い出すことが難しくなる AWS ビルダー ID 可能性があります。可能であれば、 AWS ツールやサービスのすべてのアクティビティに 1 AWS ビルダー ID つの を使用することをお勧めします。

からサインアウトする AWS

からサインアウトする方法 AWS アカウント は、ユーザーの種類によって異なります AWS 。アカウントのルートユーザー、IAM ユーザー、IAM Identity Center のユーザー、フェデレーティッド ID、または AWS Builder ID ユーザーを指定できます。自分がどのようなユーザーか明確でない場合は、「ユーザータイプを決定する」を参照してください。

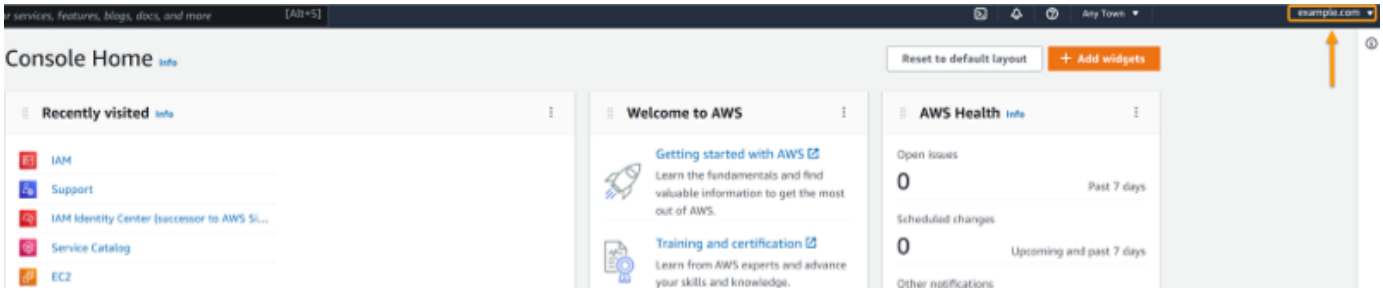
トピック

- からサインアウトする AWS マネジメントコンソール
- AWS アクセスポータルからサインアウトする
- AWS Builder ID からサインアウトする

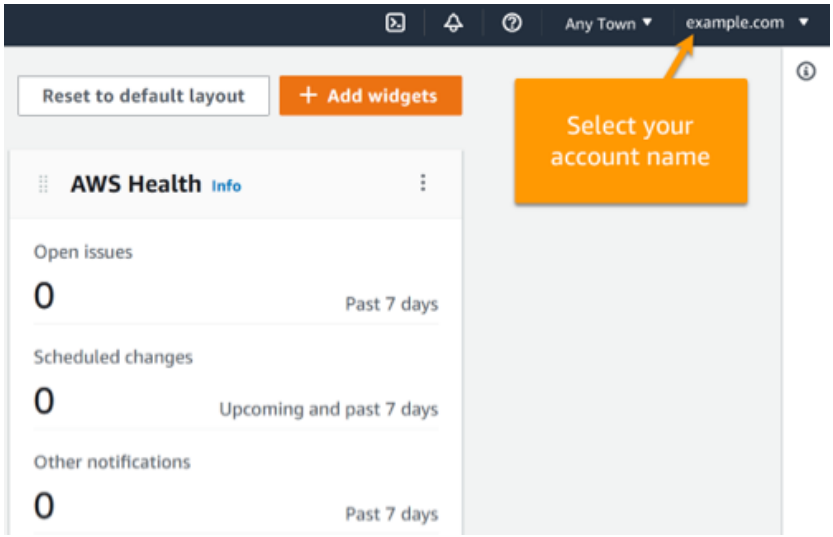
からサインアウトする AWS マネジメントコンソール

からサインアウトするには AWS マネジメントコンソール

1. にサインインすると AWS マネジメントコンソール、次の図に示すようなページが表示されます。右上隅にアカウント名または IAM ユーザー名が表示されます。



2. 右上のナビゲーションバーでユーザー名を選択します。



3. [サインアウト] オプションを選択します。ボタンオプションは、サインインしているアカウントの数によって異なります。

   - 1 つのアカウントにのみサインインしている場合は、[サインアウト] を選択します。
   - [すべてのセッションからサインアウト] を選択して、すべての ID から同時にサインアウトします。
   - [現在のセッションからサインアウト] を選択して、選択した ID からサインアウトします。

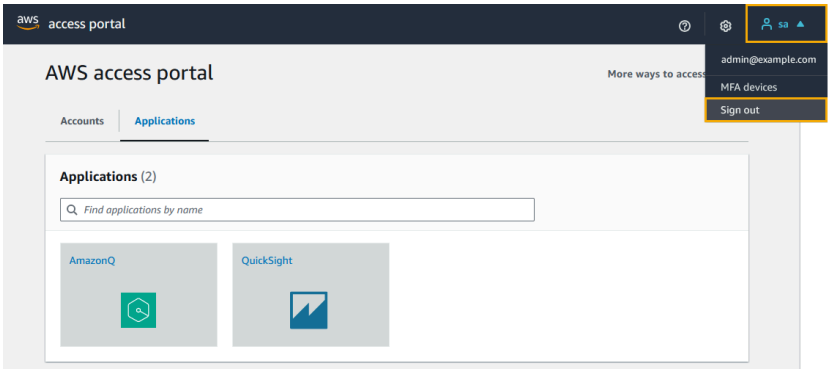
4. AWS マネジメントコンソール ウェブページに戻ります。

複数のアカウントにサインインする方法の詳細については、「AWS マネジメントコンソール 入門ガイド」の「複数のアカウントにサインインする」を参照してください。

AWS アクセスポータルからサインアウトする

AWS アクセスポータルからサインアウトするには

1. 右上のナビゲーションバーでユーザー名を選択します。
2. 次の図に示すように、[サインアウト] を選択します。



3. 正常にサインアウトすると、 AWS アクセスポータルのサインインページが表示されます。

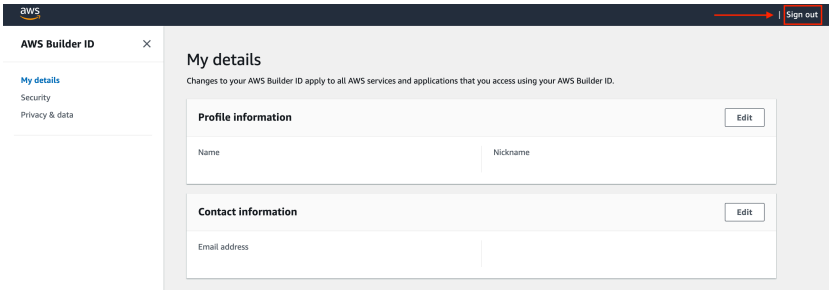
ID ソースとして外部 ID プロバイダー (IdP) を使用する場合、サインアウトしても認証情報のアクティブなセッションは終了しません。 AWS アクセスポータルに戻ると、認証情報を指定せずに自動的にサインインする場合があります。

AWS Builder ID からサインアウトする

AWS Builder ID を使用してアクセスした AWS サービスからサインアウトするには、サービスからサインアウトする必要があります。 AWS Builder ID プロファイルからサインアウトする場合は、次の手順を参照してください。

AWS Builder ID プロファイルからサインアウトするには

1. で AWS Builder ID プロファイルにサインインするとhttps://profile.aws.amazon.com/、詳細が表示されます。
2. AWS Builder ID プロファイルページの右上で、サインアウトを選択します。



3. Builder ID AWS プロファイルが表示されなくなったらサインアウトします。

サインインに関する問題 AWS アカウント のトラブルシューティング

サインインやその他の AWS アカウント 問題のトラブルシューティングには、こちらの情報を参考にしてください。にサインインするstep-by-stepについては AWS アカウント、「」を参照してくださいにサインインする AWS マネジメントコンソール。

サインインの問題に対処するのに役立つトラブルシューティングトピックがない場合は、このフォームに入力 サポート して でケースを作成できます。私は AWS のお客様であり、請求またはアカウントサポートを探しています。セキュリティのベストプラクティスとして、 サポート はサインインしているアカウント AWS アカウント 以外の の詳細を説明できません。また、AWS サポートは、理由の如何を問わず、アカウントに関連付けられている認証情報を変更することもできません。

> **Note**
>
> サポート は、サポート担当者に連絡するための直接電話番号を発行しません。

サインイン問題のトラブルシューティングの詳細については、「 へのサインインまたは へのアクセスに問題がある場合はどうすればよいですか？」を参照してください AWS アカウント。Amazon.com へのサインインに問題がある場合は、「Amazon カスタマーサービス」を参照してください。

トピック

- AWS マネジメントコンソール 認証情報が機能しない
- ルートユーザーのパスワードリセットが必要
- の E メールにアクセスできない AWS アカウント
- MFA デバイスの紛失および故障時の対応
- AWS マネジメントコンソール サインインページにアクセスできない
- サインインリソースベースのポリシーのネットワーク条件によりサインインできない
- コンソール認可を有効にした後、アカウントからロックアウトされている
- ポリシーの変更が有効ではない
- AWS アカウント ID またはエイリアスを見つける方法
- アカウント検証コードが必要

- のルートユーザーパスワードを忘れました AWS アカウント
- の IAM ユーザーパスワードを忘れた AWS アカウント
- のフェデレーション ID パスワードを忘れました AWS アカウント
- 既存の にサインインできず AWS アカウント 、同じ E メールアドレス AWS アカウント で新しいを作成できない
- 中断した を再アクティブ化する必要があります AWS アカウント
- サインインの問題 サポート については、 に連絡する必要があります
- 請求に関する問題 AWS Billing については、 に連絡する必要があります
- 小売注文について質問があります
- の管理にヘルプが必要です AWS アカウント
- AWS アクセスポータルの認証情報が機能しない
- の IAM Identity Center パスワードを忘れました AWS アカウント
- IAM Identity Center コンソールにサインインしようとすると、「It's not you, it's us」というエラーが表示される

AWS マネジメントコンソール 認証情報が機能しない

ユーザー名とパスワードを覚えていても認証情報が使えない場合は、間違ったページに移動している可能性があります。別のページでログインしてみてください。

ルートユーザーのサインインページ

- を作成または所有 AWS アカウント していて、ルートユーザーの認証情報を必要とするタスクを実行している場合は、 にアカウントの E メールアドレスを入力しますAWS マネジメントコンソール。ルートユーザーにアクセスする方法については、ルートユーザーとしてサインインするを参照します。 パスワードを忘れた場合、リセットすることはできません。詳細については「のルートユーザーパスワードを忘れました AWS アカウント」を参照してください。ルートユーザーのメールアドレスを忘れてしまった場合は、 AWSからのメールが届いていないか確認してください。
- ルートユーザーアカウントにサインインしようとして、「ルートユーザーアカウントのパスワード復旧が無効になっています」というエラーが表示された場合は、ルートユーザーの認証情報はありません。ルートユーザーとしてサインインしたり、アカウントのルートユーザーのパスワード復旧を実行したりすることはできません。 を使用して管理される AWS メンバーアカウントには、ルートユーザーのパスワード、アクセスキー、署名証明書、またはアクティブな多要素認証 (MFA) がない AWS Organizations 場合があります。

管理アカウントまたは IAM の委任された管理者のみが、メンバーアカウントでルートユーザーアクションを実行できます。ルートユーザー認証情報を必要とするタスクを実行する必要がある場合は、管理者に問い合わせてください。詳細については、「AWS Identity and Access Management ユーザーガイド」の「メンバーアカウントのルートアクセスを一元管理する」を参照してください。

IAM ユーザーのサインインページ

- 自分または他のユーザーが 内に IAM ユーザーを作成した場合は AWS アカウント、その AWS アカウント ID またはエイリアスを知ってサインインする必要があります。AWS マネジメントコンソール にアカウント ID またはエイリアス、ユーザー名、パスワードを入力します。IAM ユーザーのサインインページにアクセスする方法については、「IAM ユーザーとしてサインインするには」を参照してください。IAM ユーザーパスワードを忘れた場合は、IAM ユーザーパスワードのリセットについて、「の IAM ユーザーパスワードを忘れた AWS アカウント」を参照してください。アカウント番号を忘れた場合は、メール、ブラウザーのお気に入り、またはブラウザーの履歴で、`signin.aws.amazon.com/` を含む URL を検索してください。アカウント ID またはエイリアスは、URL の `"account="` テキストの後に続きます。アカウント ID またはエイリアスが見つからない場合は、administrator にお問い合わせください。この情報 サポート を復旧することはできません。アカウントIDまたはエイリアスは、サインインするまで表示されません。

ルートユーザーのパスワードリセットが必要

アカウントを保護するために、 AWS マネジメントコンソールにサインインしようとすると、次のメッセージが表示されることがあります。

パスワードのリセットが必要です。セキュリティの目的でパスワードをリセットする必要があります。アカウントを安全に保つために、以下の [パスワードを忘れた場合] を選択してパスワードをリセットする必要があります。

このメッセージに加えて、 は、お客様のアカウントに関連付けられた E メールを通じて潜在的な問題が特定されたときに AWS も通知します。この E メールには、パスワードのリセットが必要な理由が含まれています。例えば、 AWS アカウント または に関連付けられた認証情報への異常なログインアクティビティを特定すると AWS アカウント 、オンラインで公開されます。

ルートユーザーの認証情報が安全であることを保証するためにパスワードを更新します。ルートユーザーのパスワードをリセットする方法については、「AWS アカウントのルートユーザーパスワードを忘れてしまった」を参照してください。

の E メールにアクセスできない AWS アカウント

を作成するときは AWS アカウント、E メールアドレスとパスワードを指定します。これらは、AWS アカウントのルートユーザーの認証情報です。に関連付けられている E メールアドレスが不明な場合は AWS アカウント、@signin.aws または @verify.signin.aws で終わる、 を開くために使用された可能性のある組織の E メールアドレスに保存されたコレスポンデンスを探します AWS アカウント。チーム、組織、家族の他のメンバーに聞いてみてください。知り合いがアカウントを作成した場合は、その人がアクセスできるように手伝ってくれます。

E メールアドレスがわかっていても、E メールにアクセスできなくなった場合は、まず次のいずれかのオプションを使用して、E メールへのアクセスを回復します。

- E メールアドレスのドメインを所有している場合は、削除した E メールアドレスを復元できます。または、E メールアカウントにキャッチオールを設定することもできます。「キャッチオール」は、メールサーバーに存在しなくなった E メールアドレスに送信されたすべてのメッセージをキャッチし、別のメールアドレスにリダイレクトします。
- アカウントの E メールアドレスが企業 E メールシステムの一部である場合は、IT システム管理者に連絡することをお勧めします。管理者は、E メールへのアクセス許可の回復を支援できる可能性があります。

にまだサインインできない場合は AWS アカウント、 に連絡して代替のサポートオプションを見つけることができます サポート。

MFA デバイスの紛失および故障時の対応

MFA デバイスが紛失、破損、または動作しない場合、MFA 検証リクエストを送信してもワンタイムパスコード (OTP) を受け取ることができません。

IAM ユーザー

同じ IAM ユーザーに登録されている別の MFA デバイスを使用してサインインできます。

IAM ユーザーは、機能していない MFA デバイスを無効にするために管理者に連絡する必要があります。これらのユーザーは、管理者の支援なしに MFA デバイスを復元することはできません。管理者は通常、組織の他のメンバー AWS アカウント よりも高いレベルのアクセス許可を持つ情報技術 (IT) 担当者です。この個人がアカウントを作成し、ユーザーにサインインするためのアクセス認証情報を提供します。

ルートユーザー

ルートユーザーへのアクセスを回復するには、同じルートユーザーに登録されている別の MFA デバイスを使用してサインインする必要があります。それから、次のオプションを確認して MFA デバイスを復旧または更新します。

- MFA デバイスの復旧手順については、「MFA デバイスの紛失および故障時の対応」をご覧ください。
- MFA デバイスの電話番号を更新する手順については、「電話番号を更新して紛失した MFA デバイスをリセットする方法」をご覧ください。
- MFA デバイスをアクティブ化するstep-by-stepについては、「 で MFA デバイスを有効にする AWS」を参照してください。
- MFA デバイスを復旧できない場合は、サポート にお問い合わせください。

> **Note**
>
> IAM ユーザーは、管理者に連絡して MFA デバイスに関するサポートを依頼する必要があります。 サポート は、MFA デバイスの問題で IAM ユーザーをサポートできません。

AWS マネジメントコンソール サインインページにアクセスできない

サインインページが表示されない場合は、ドメインがファイアウォールによってブロックされている可能性があります。ネットワーク管理者に連絡して、ユーザーの種類とサインイン方法に応じて、以下のドメインまたは URL エンドポイントを Web コンテンツフィルターソリューションの許可リストに追加してください。

ルートユーザーと IAM ユーザー	*.signin.aws.amazon.com
Amazon.com アカウントへのサインイン	www.amazon.com
IAM アイデンティティセンターのユーザーとファーストパーティアプリケーションサインイン	• *.awsapps.com (http://awsapps.com/) • *.signin.aws

サインインリソースベースのポリシーのネットワーク条件によりサインインできない

次のいずれかのエラーメッセージが表示される場合、サインインリソースベースのポリシーまたはリソースコントロールポリシー (RCP) が、ネットワークの場所に基づいてアクセスを制限している可能性があります。

- 「認証情報が正しくありません。もう一度試してください。」
- 「認証に失敗しました 無効なリクエスト」
- 「認証に失敗しました: このアカウントにアクセスするには、別のネットワークからサインインするか、管理者にお問い合わせください」

詳細なトラブルシューティング手順サインインリソースベースのポリシーのネットワーク条件によりサインインできないについては、管理者に問い合わせるか、「」を参照してください。

コンソール認可を有効にした後、アカウントからロックアウトされている

コンソール認可を設定し、アカウントにアクセスできなくなった場合、ポリシーを適用する前に除外されたプリンシパルまたは緊急復旧アクセスを設定していない可能性があります。 AWS CLI セルフサービス、OrganizationAccountAccessRole、 AWS サポートオプションなどの解決手順については、「」を参照してくださいコンソール認可を有効にした後、アカウントからロックアウトされている。

ポリシーの変更が有効ではない

コンソール認可設定とリソース許可ステートメントの変更はグローバルにレプリケートされ、有効になるまでに数分かかる場合があります。待機後に変更が表示されない場合は、トラブルシューティングの手順行った変更がすぐに表示されないことがあるについて「」を参照してください。

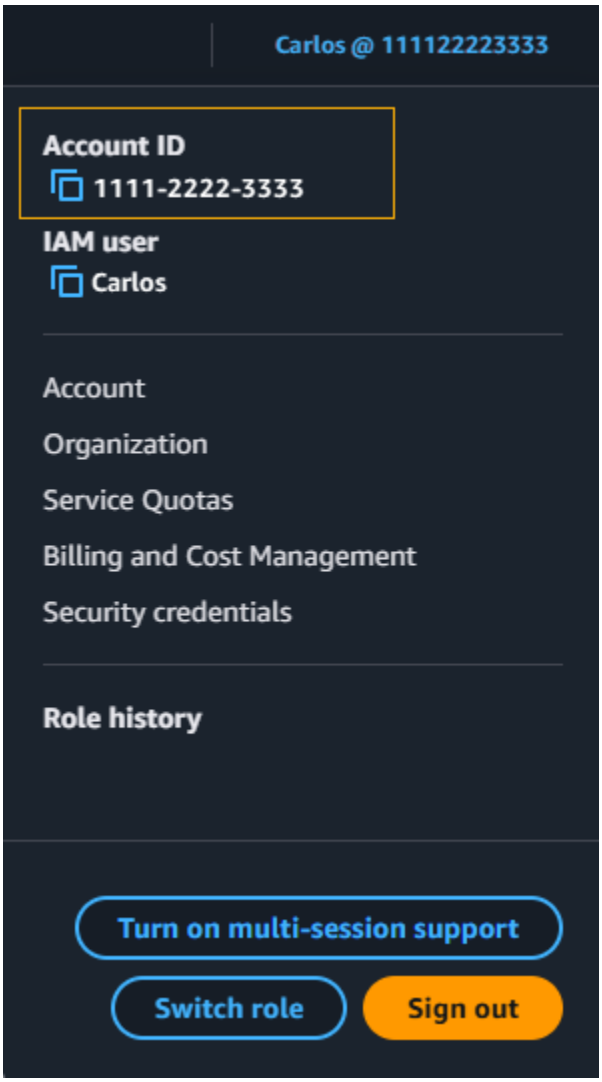
AWS アカウント ID またはエイリアスを見つける方法

IAM ユーザーでサインインしていない場合は、管理者に AWS アカウント の ID またはエイリアスを問い合わせてください。管理者は通常、組織の他のメンバー AWS アカウント よりも高いレベルの

アクセス許可を持つ情報技術 (IT) 担当者です。この個人がアカウントを作成し、ユーザーにサインインするためのアクセス認証情報を提供します。

にアクセスできる IAM ユーザーの場合 AWS マネジメントコンソール、アカウント ID はサインイン URL にあります。管理者からのメールをチェックして、サインイン URL を確認してください。アカウント ID はサインイン URL の最初の 12 桁です。たとえば、次の URL の `https://111122223333.signin.aws.amazon.com/console`では、 AWS アカウント ID は 111122223333 です。

にサインインすると AWS マネジメントコンソール、リージョンの横にあるナビゲーションバーにアカウント情報が表示されます。たとえば、次のスクリーンショットでは、IAM ユーザー Carlos AWS アカウント の は 1111-2222-3333 です。



AWS アカウント ID とエイリアス、およびその検索方法の詳細については、AWS アカウント「ID とそのエイリアス」を参照してください。

アカウント検証コードが必要

アカウントの E メールアドレスとパスワードを指定した場合、 では 1 回限りの検証コードの入力が必要になる AWS ことがあります。検証コードを取得するには、 に関連付けられている E メールをチェックして、Amazon Web Services からの AWS アカウント メッセージを確認します。E メールアドレスは @signin.aws または @verify.signin.aws で終わります。メッセージに記載されている手順に従います。アカウントにメッセージが表示されない場合、スパムや迷惑メールフォルダを確認してください。E メールへのアクセス許可がない場合、「の E メールにアクセスできない AWS アカウント」を参照してください。

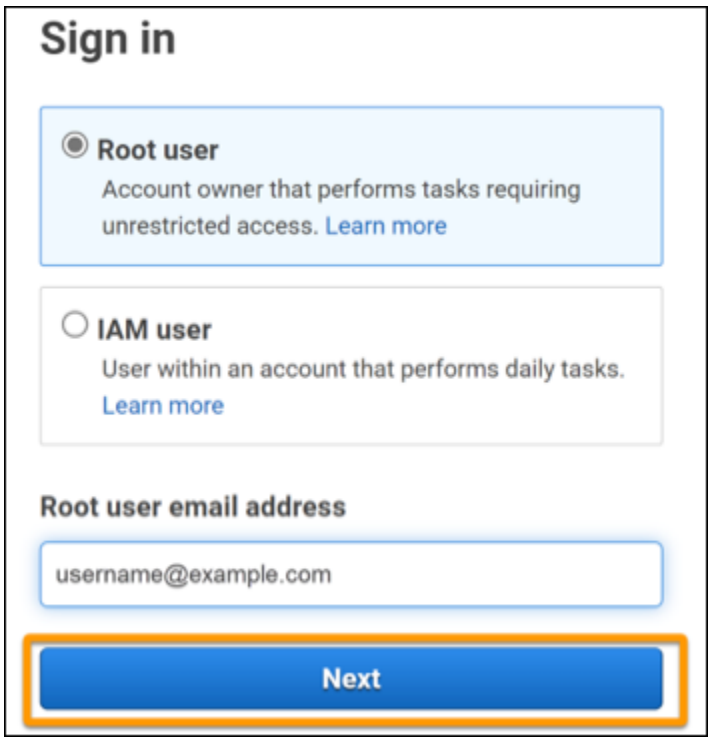
のルートユーザーパスワードを忘れました AWS アカウント

ルートユーザーで、 のパスワードを紛失または忘れた場合は AWS アカウント、 で「パスワードを忘れた場合」リンクを選択してパスワードをリセットできます AWS マネジメントコンソール。AWS アカウントの E メールアドレスを把握し、E メールアカウントにアクセスできる必要があります。パスワード復旧手順中に、パスワードをリセットするためのリンクがメールで送信されます。リンクは、 の作成に使用した E メールアドレスに送信されます AWS アカウント。

AWS Organizations を使用して作成したアカウントのパスワードをリセットするには、「ルートユーザーとしてのメンバーアカウントへのアクセス」を参照してください。

ルートユーザーパスワードをリセットするには

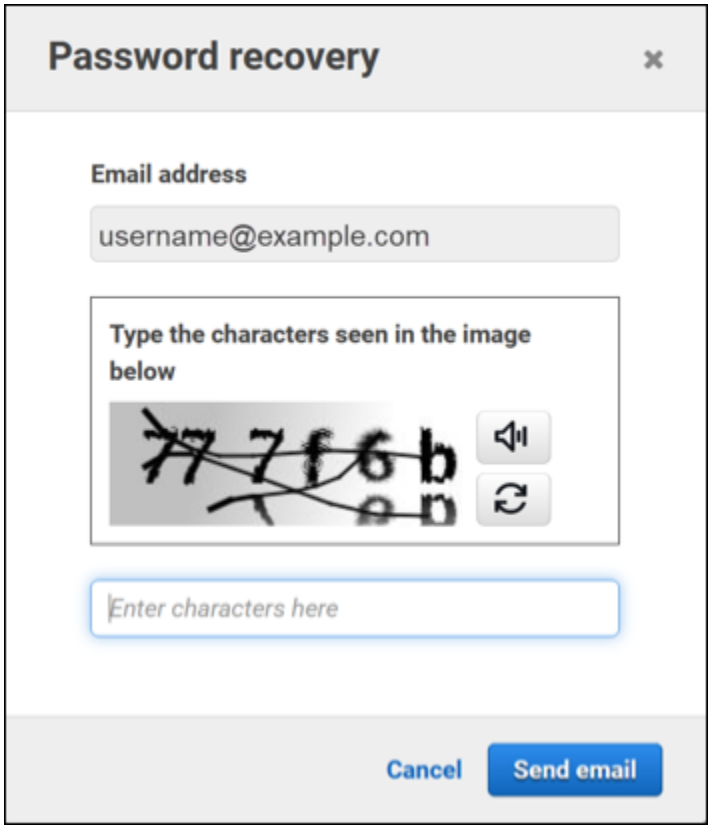
1. AWS E メールアドレスを使用して、ルートユーザーとして AWS マネジメントコンソールへのサインインを開始します。その後、[Next] を選択します。



> **Note**
>
> IAM ユーザー認証情報で AWS マネジメントコンソール にサインインしている場合、ルートユーザーのパスワードをリセットする前にサインアウトする必要があります。アカウント固有の IAM ユーザーのサインインページが表示された場合は、ページの下部付近にある ルートアカウントの認証情報を使用してサインインする を選択します。必要に応じて、アカウントの E メールアドレスを指定し、[次へ] を選択して [ルートuser sign in (ルートユーザーサインイン)] ページにアクセスします。

2. [パスワードを忘れましたか?] を選択します。

3. パスワード復旧手順を完了します。セキュリティチェックを完了できない場合は、音声を聞くか、セキュリティチェックを更新して新しい文字セットが試してください。パスワード復旧ページの例を次の画像に示します。

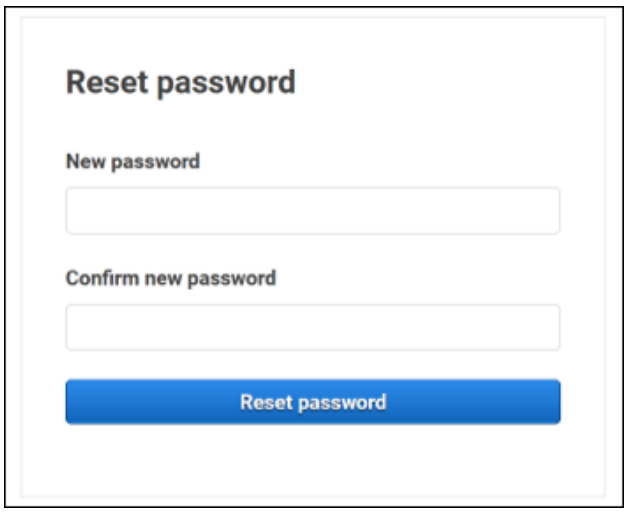


4. パスワード復旧手順を完了すると、 AWS アカウントに関連する E メールアドレスに詳細な手順が送信されたというメッセージを受け取ります。

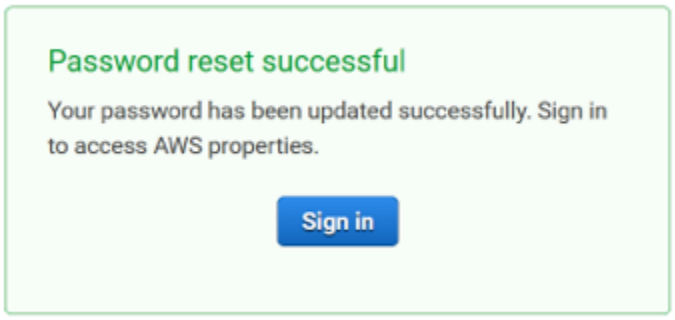
   AWS アカウントの作成に使用した E メールに、パスワードをリセットするためのリンクが送信されます。

   > **Note**
   >
   > E メールは @signin.aws または @verify.signin.aws で終わるアドレスから届きます。

5. E AWS メールに記載されているリンクを選択して、 AWS ルートユーザーのパスワードをリセットします。
6. リンクをクリックすると、新しいルートユーザーパスワードを作成するための新しい Web ページに移動します。



パスワードのリセットが成功したことを示す確認メッセージが届きます。パスワードのリセットが成功したことが次の画像に示します。

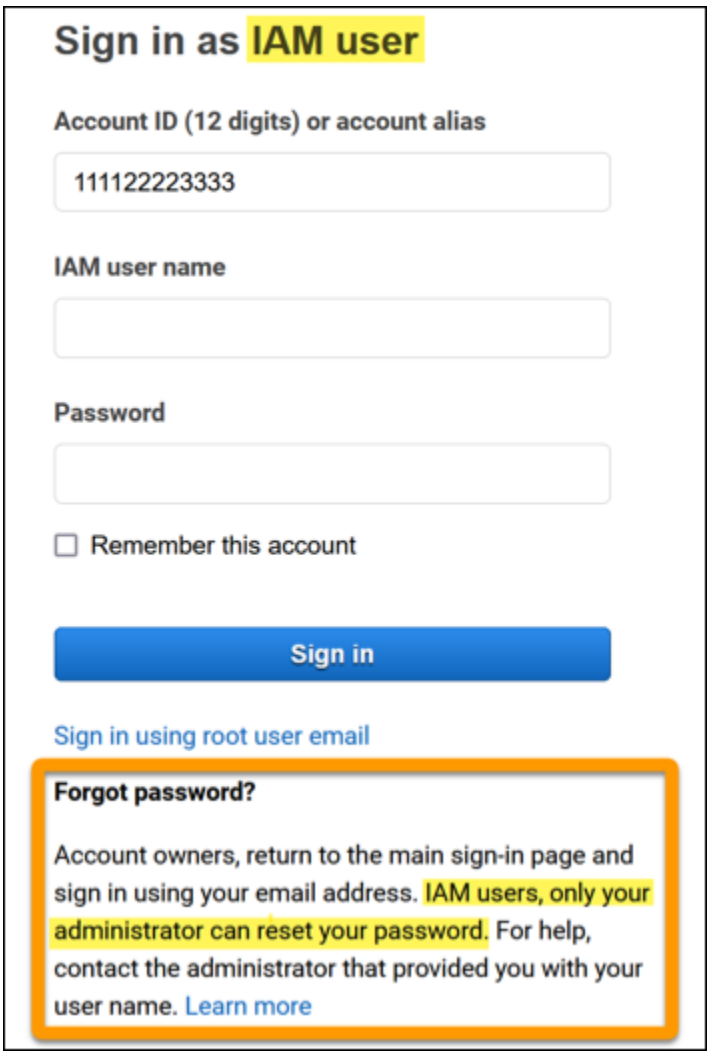


ルートユーザーパスワードのリセットの詳細については、「紛失または忘れた AWS パスワードを復元する方法を教えてください。」を参照してください。

の IAM ユーザーパスワードを忘れた AWS アカウント

IAM ユーザーのパスワードを変更するには、適切な権限が必要です。IAM ユーザーパスワードのリセットの詳細については、「IAM ユーザーが自分のパスワードを変更する方法」を参照してください。

パスワードをリセットする権限がない場合は、IAM 管理者だけが IAM ユーザーパスワードをリセットできます。IAM ユーザーは IAM 管理者に連絡して、パスワードをリセットする必要があります。管理者は通常、組織の他のメンバー AWS アカウント よりも高いレベルのアクセス許可を持つ情報技術 (IT) 担当者です。この個人がアカウントを作成し、ユーザーにサインインするためのアクセス認証情報を提供します。



セキュリティ上の理由から、 サポート には認証情報を表示、提供、または変更するためのアクセス権はありません。

IAM ユーザーパスワードのリセットの詳細については、「紛失または忘れた AWS パスワードを復元するにはどうすればよいですか？」を参照してください。

管理者がパスワードを管理する方法については、「IAM ユーザーのパスワード管理」を参照してください。

のフェデレーション ID パスワードを忘れました AWS アカウント

フェデレーティッド ID は、外部 ID AWS アカウント を使用して にアクセスするためにサインインします。使用する外部 ID のタイプによって、フェデレーション ID のサインイン方法が決まります。管理者はフェデレーション ID を作成します。パスワードをリセットする方法の詳細について

は、管理者に確認してください。管理者は通常、組織の他のメンバー AWS アカウント よりも高いレベルのアクセス許可を持つ情報技術 (IT) 担当者です。この個人がアカウントを作成し、ユーザーにサインインするためのアクセス認証情報を提供します。

既存の にサインインできず AWS アカウント 、同じ E メールアドレス AWS アカウント で新しい を作成できない

1 つの E メールアドレスには 1 つの AWS アカウントのルートユーザーにのみ関連付けることができます。ルートユーザーアカウントを閉鎖し、90 日以上閉鎖されたままである場合、アカウントを再開したり、このアカウントに関連付けられた E メールアドレス AWS アカウント を使用して新しいを作成したりすることはできません。

この問題を解決するには、新しいアカウントにサインアップするときに、通常の E メールアドレスの後にプラス記号 (+) を追加するサブアドレスを使用します。プラス記号 (+) の後には、大文字または小文字、数字、または SMTP (簡易メール転送プロトコル) がサポートするその他の文字を付けることができます。たとえば、普段使っている E メールが `email@yourcompany.com` の場合、`email+1@yourcompany.com` または `email+tag@yourcompany.com` を使用できます。普段使っている E メールアドレスと同じ受信トレイに接続されていても、新しいアドレスと見なされます。新しいアカウントにサインアップする前に、追加した E メールアドレスにテストメールを送信して、メールプロバイダーがサブアドレッシングをサポートしていることを確認することをお勧めします。

中断した を再アクティブ化する必要があります AWS アカウント

AWS アカウント が停止されており、復元する場合は、「停止した を再アクティブ化するにはどうすればよいですか？」を参照してください AWS アカウント。

サインインの問題 サポート については、 に連絡する必要があります

すべてを試した場合は、請求およびアカウントサポートリクエストを完了 サポート することで、 からサポートを受けることができます。

請求に関する問題 AWS Billing については、 に連絡する必要があります

にサインインできず AWS アカウント 、 AWS Billing 請求の問題について に連絡したい場合は、請求およびアカウントサポートリクエストを通じて行うことができます。料金や支払い方法など AWS Billing and Cost Management、 の詳細については、「Getting help with AWS Billing」を参照してください。

小売注文について質問があります

www.amazon.com アカウントに問題がある場合、または小売注文について質問がある場合は、「サポートオプションとお問い合わせ」を参照してください。

の管理にヘルプが必要です AWS アカウント

のクレジットカードの変更 AWS アカウント、不正行為の報告、または の閉鎖についてサポートが必要な場合は AWS アカウント、「 に関するその他の問題のトラブルシューティング AWS アカウント」を参照してください。

AWS アクセスポータルの認証情報が機能しない

AWS アクセスポータルにサインインできない場合は、以前にアクセスした方法を思い出してください AWS。

パスワードを使ったことをまったく覚えていない場合

AWS 認証情報を使用 AWS せずに以前に にアクセスしたことがあるかもしれません。これは、IAM アイデンティティセンター経由のエンタープライズシングルサインオンでは一般的です。 AWS このようにアクセスすると、会社の認証情報を使用して、認証情報を入力せずに AWS アカウントまたはアプリケーションにアクセスすることになります。

- AWS アクセスポータル – 管理者が外部からの認証情報を使用して AWS アクセスすることを許可している場合は AWS、ポータルの URL が必要です。E メール、お気に入りのブラウザ、または `awsapps.com/start` や `signin.aws/platform/login` を含む URL に対するブラウザの履歴を確認してください。

例えば、カスタム URL には ID や https://*d-1234567890*.awsapps.com/start のようなドメインが含まれる場合があります。ポータルリンクが見つからない場合は、管理者にお問い合わせください。この情報の復旧 サポート はサポートされていません。

ユーザー名とパスワードを覚えていても認証情報が使えない場合は、間違ったページに移動している可能性があります。ウェブブラウザで URL を確認してください。https://signin.aws.amazon.com/ の場合、フェデレーティッドユーザーまたは IAM アイデンティティセンターのユーザーは自分の認証情報を使用してサインインできません。

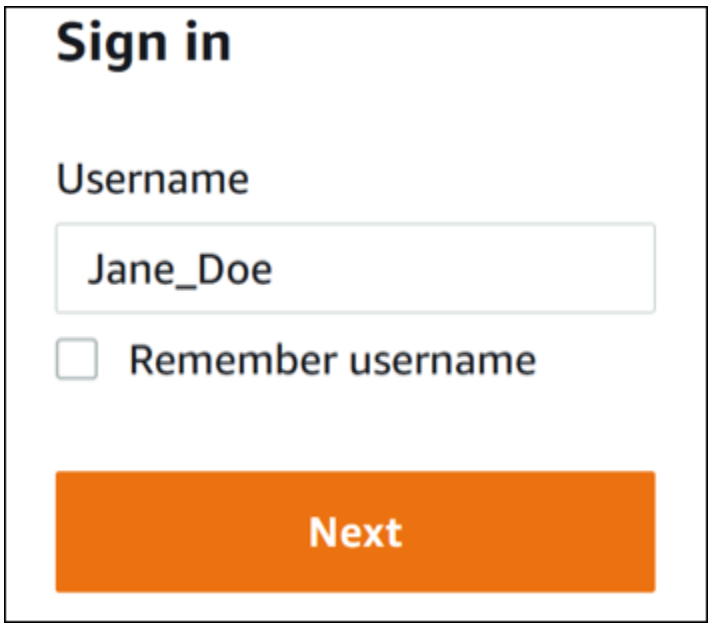
- AWS アクセスポータル – 管理者が AWS IAM アイデンティティセンター (AWS シングルサインオンの後継) の ID ソースをセットアップする場合は AWS、組織の AWS アクセスポータルでユーザー名とパスワードを使用してサインインする必要があります。ポータルの URL を見つけるには、E メール、安全なパスワードストレージ、ブラウザのお気に入り、またはブラウザの履歴で awsapps.com/start または signin.aws/platform/login を含む URL。 例えば、カスタム URL に ID https://*d-1234567890*.awsapps.com/start. や などのドメインが含まれている場合があります。ポータルリンクが見つからない場合は、管理者にお問い合わせください。この情報の復旧には役 サポート に立ちません。

の IAM Identity Center パスワードを忘れました AWS アカウント

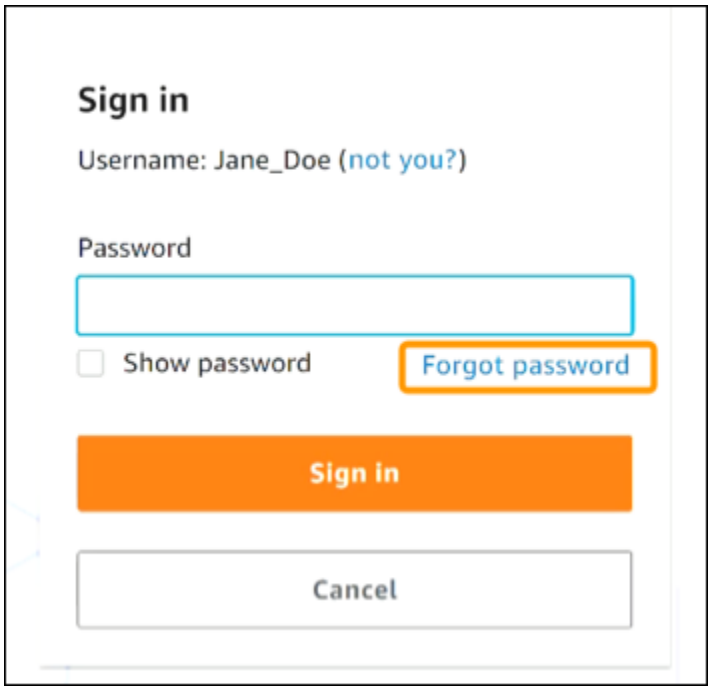
IAM アイデンティティセンターのユーザーで、 AWS アカウントのパスワードを紛失または忘れた場合は、パスワードをリセットできます。IAM アイデンティティセンターのアカウントに使用している E メールアドレスを知っており、アクセス権限を持っている必要があります。パスワードをリセットするためのリンクが AWS アカウント E メールに送信されます。

IAM アイデンティティセンターでユーザーのパスワードをリセットする手順

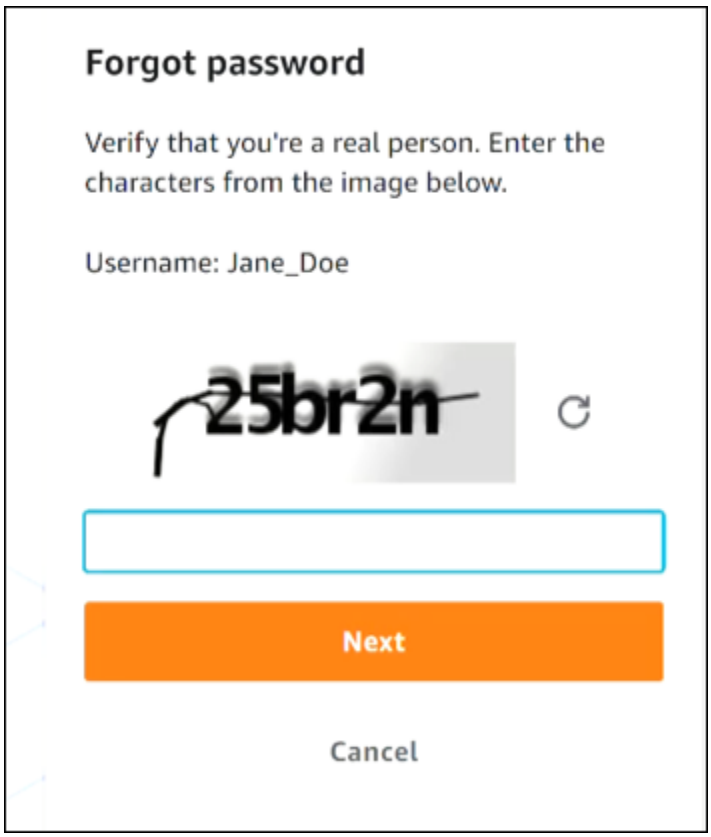
1. AWS アクセスポータルの URL リンクを使用してユーザー名を入力します。その後、[Next] を選択します。



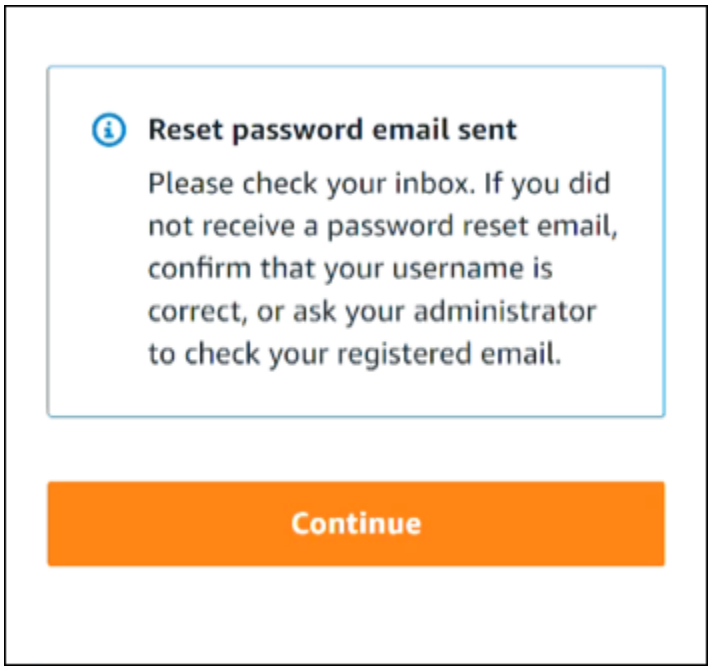
2. 次の画像に示すように、[パスワードを忘れた場合] を選択します。



3. パスワード復旧手順を完了します。



4. パスワード復旧手順を完了すると、パスワードのリセットに使用できる E メールメッセージが送信されたことを確認する以下のメッセージが表示されます。



パスワードをリセットするためのリンクが記載された E メールが、IAM アイデンティティセンターのユーザーアカウントに関連付けられている E メールに送信されます。E AWS メールに記

載されているリンクを選択して、パスワードをリセットします。リンクをクリックすると、新しいパスワードを作成するための新しい Web ページに移動します。新しいパスワードを作成すると、パスワードのリセットが成功したことを示す確認メッセージが表示されます。

パスワードをリセットするためのメールが届かない場合は、管理者に IAM アイデンティティセンターでどの E メールがユーザーに登録されているかを確認するよう依頼してください。

IAM Identity Center コンソールにサインインしようとすると、「It's not you, it's us」というエラーが表示される

このエラーは、IAM Identity Center のインスタンスまたは ID ソースとして使用している外部 ID プロバイダー (IdP) のセットアップの問題があることを示します。次のことを確認することをお勧めします。

- サインインに使用するデバイスの日時設定を確認します。日付と時刻の自動設定を許可することをお勧めします。利用できない場合は、日付と時刻を既知の Network Time Protocol (NTP) サーバーに同期することをお勧めします。
- IAM Identity Center にアップロードされた IdP 証明書が ID プロバイダーから提供された証明書と同じであることを確認します。IAM Identity Center コンソールから証明書を確認するには、[設定] に移動します。[アイデンティティソース] タブの [アクション] で [認証を管理] を選択します。新しい証明書をインポートする必要がある場合があります。
- IdP の SAML メタデータファイルで、NameID 形式が `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` であることを確認します。
- AD Connector を使用している場合は、サービスアカウントの認証情報が正しいこと、および有効期限が切れていないことを確認します。詳細については、「 での AD Connector サービスアカウントの認証情報の更新 Directory Service」を参照してください。

AWS Builder ID の問題のトラブルシューティング

ここに記載する情報を使用すると、 AWS ビルダー ID に関係する問題のトラブルシューティングに役立ちます。

トピック

- AWS Builder ID にサインインしようとすると、「It's not you, it's us」というメッセージが表示されます。
- サインアウトしても完全にサインアウトされない
- まだ問題を解決しようとしています

メールアドレスが既に使われています

入力した E メールが既に使用されており、それを自分の E メールとして認識している場合は、既に AWS Builder ID にサインアップしている可能性があります。そのメールアドレスを使用してサインインしてみてください。パスワードを覚えていない場合、「パスワードを忘れてしまいました」を参照してください。

メールの確認を完了させることができない

AWS Builder ID にサインアップしたが、検証 E メールを受信していない場合は、次のトラブルシューティングタスクを完了します。

1. スパムアイテム、迷惑メールアイテム、削除済みアイテムのフォルダを確認してください。

   > **Note**
   >
   > この検証 E メールは、no-reply@signin.aws または no-reply@login.awsapps.com のアドレスから送信されます。これらの送信者メールアドレスからのメールを受け入れ、迷惑メールやスパムとして処理しないように、メールシステムを設定することをお勧めします。

2. コードを再送信を選択し、受信トレイを更新して、スパムアイテム、迷惑メールアイテム、削除済みアイテムのフォルダをもう一度確認します。
3. それでも検証 E メールが表示されない場合は、 AWS ビルダー ID の E メールアドレスにタイプミスがないかを再確認してください。間違ったメールアドレスを入力した場合は、自分のメールアドレスでもう一度サインアップしてください。

Google でサインインできない

Google アカウントと同じ E メールアドレスを持つ既存の AWS ビルダー ID プロファイルがある場合は、 AWS ビルダー ID パスワードを使用してアカウントにサインインします。パスワードを覚えていない場合、「パスワードを忘れてしまいました」を参照してください。

Google パスワードでサインインする方法については、「Google アカウントにサインインできない」を参照してください。

Apple でサインインできない

Apple アカウントと同じ E メールアドレスを持つ既存の AWS ビルダー ID プロファイルがある場合は、 AWS ビルダー ID パスワードを使用してアカウントにサインインします。パスワードを覚えていない場合、「パスワードを忘れてしまいました」を参照してください。

Apple パスワードでサインインする方法については、「Apple アカウントにサインインできない場合」を参照してください。

GitHub でサインインできない

GitHub アカウントと同じ E メールアドレスを持つ既存の AWS ビルダー ID プロファイルがある場合は、 AWS ビルダー ID パスワードを使用してアカウントにサインインします。パスワードを覚えていない場合、「パスワードを忘れてしまいました」を参照してください。

GitHub パスワードでサインインする方法については、「サインインできない - GitHub サポート」を参照してください。

Amazon でサインインできない

Amazon アカウントと同じ E メールアドレスを持つ既存の AWS ビルダー ID プロファイルがある場合は、 AWS ビルダー ID パスワードを使用してアカウントにサインインします。パスワードを覚えていない場合、「パスワードを忘れてしまいました」を参照してください。

Amazon パスワードでサインインする方法については、「サインインのヘルプ」を参照してください。

Google で続行 AWS ビルダー ID を使用して にサインアップしようとしたときにサインインエラーが表示されました

つまり、Google アカウントと同じ E メールアドレス AWS ビルダー ID を使用する既存の がある か、Google アカウントに関連付けられた E メールアドレスが検証されていないことを意味します。いずれの場合も、E メールアドレスを入力し、パスワードを指定して再度サインアップをお試しください。

Apple で続行 AWS ビルダー ID を使用して にサインアップしようとしたときにサインインエラーが表示されました

つまり、Apple アカウントと同じ E メールアドレス AWS ビルダー ID を使用する既存の がある か、Apple アカウントに関連付けられた E メールアドレスが Apple Business Manager で会社によって検証または管理されていないか、Apple School Manager で学校によって管理されていないことを意味します。いずれの場合も、E メールアドレスを入力し、パスワードを指定して再度サインアップをお試しください。

GitHub で続行 AWS ビルダー ID を使用して にサインアップしようとしたときにサインインエラーが表示されました

つまり、既存の が GitHub アカウントと同じ E メールアドレス AWS ビルダー ID を使用しているか、GitHub アカウントに関連付けられた E メールアドレスが検証されていないことを意味します。いずれの場合も、E メールアドレスを入力し、パスワードを指定して再度サインアップをお試しください。

Amazon で続行 AWS ビルダー ID を使用して にサインアップしようとしたときにサインインエラーが表示されました

つまり、Amazon アカウントと同じ E メールアドレス AWS ビルダー ID を使用する既存の がある か、Amazon アカウントに関連付けられた E メールアドレスが検証されていないことを意味します。いずれの場合も、E メールアドレスを入力し、パスワードを指定して再度サインアップをお試しください。

でサインインしようとすると、「It's not you, it's us」というエラーが表示されます。 AWS ビルダー ID

サインインしようとしたときにこのエラーメッセージが表示された場合は、ローカル設定または E メールアドレスに問題がある可能性があります。

- サインインに使用するデバイスの日時設定を確認します。日付と時刻の自動設定を許可することをお勧めします。利用できない場合は、日付と時刻を既知の Network Time Protocol (NTP) サーバーに同期することをお勧めします。
- E メールアドレスのフォーマットエラーを確認します。次の問題は、 AWS ビルダー IDでサインインしようとすると エラーを返します。
  - E メールアドレスに含まれるスペース
  - E メールアドレスに含まれるスラッシュ (/)
  - E メールアドレスに含まれる 2 つのピリオド (.)
  - E メールアドレスに含まれる 2 つのアンパサンド (@)
  - E メールアドレスの末尾にあるカンマ (,)
  - E メールアドレスの末尾にあるブラケット (])

パスワードを忘れてしまいました

忘れたパスワードをリセットするには

1. AWS ビルダー ID でサインイン ページで、E メールアドレスに AWS ビルダー ID の作成に使用した E メールを入力します。[次へ] を選択します。
2. パスワードを忘れましたか? を選択します。パスワードをリセットできる AWS Builder ID に関連付けられた E メールアドレスへのリンクが送信されます。
3. メールの指示に従います。

新しいパスワードを設定できない

セキュリティ上の理由から、パスワードを設定または変更するときは必ず次の要件に従う必要があります。

- パスワードでは、大文字と小文字が区別されます。

- パスワードの長さは8文字から64文字の間でなければなりません。
- パスワードには、次の 4 つカテゴリから少なくとも 1 文字を含める必要があります。
  - 小文字 a〜z
  - 大文字 A〜Z
  - 数字 0〜9
  - 英数字以外の文字 ~!@#$%^管理ポータル*_-+=`|\{}:;"'<>,.?/
- 最後の 3 つのパスワードは再使用できません。
- 第三者から漏洩したデータセットを通じて公に知られているパスワードは使用できません。

パスワードが機能しません。

パスワードを覚えていても、 AWS Builder ID でサインインするときにパスワードが機能しない場合は、以下を確認してください。

- キャップロックはオフです。
- 古いパスワードは使用していません。
- AWS ビルダー ID パスワードを使用しており、 にパスワードを使用していません AWS アカウント。

パスワードが最新で、正しく入力されていることを確認しても機能しない場合は、パスワードを忘れてしまいました の指示に従ってパスワードをリセットしてください。

パスワードが機能せず、 AWS ビルダー ID の E メールアドレスに送信された E メールにアクセスできなくなる

それでも AWS Builder ID にサインインできる場合は、プロファイルページを使用して AWS Builder ID の E メールを新しい E メールアドレスに更新します。E メールの検証が完了すると、 にサインイン AWS し、新しい E メールアドレスで通信を受信できます。

職場や大学のメールアドレスを使用していて、その後会社や学校を辞め、そのアドレスに送信されたメールを受信できない場合や、 ビルダー ID にサインインできない場合は、そのメールシステムの管理者に連絡してください。メールを新しいアドレスに転送したり、一時的なアクセスを許可したり、メールボックスのコンテンツを共有したりできる場合があります。

MFA を有効にできない

MFA を有効にするには、AWS ビルダー ID 多要素認証 (MFA) の管理 の手順に従って 1 つ以上の MFA デバイスをプロファイルに追加します。

認証アプリケーションを MFA デバイスとして追加できない

別の MFA デバイスを追加できない場合は、そのアプリケーションに登録できる MFA デバイスの上限に達している可能性があります。未使用の MFA デバイスを削除するか、別の認証アプリケーションを使用してみてください。

MFA デバイスを削除できない

MFA を無効にする場合は、MFA デバイスの削除 の手順に従って MFA デバイスを削除してください。ただし、MFA を有効にしておきたい場合は、既存の MFA デバイスを削除する前に、別の MFA デバイスを追加する必要があります。別の MFA デバイスの追加の詳細については、「AWS ビルダー ID 多要素認証 (MFA) の管理」を参照してください。

認証アプリケーションを使用して登録やサインインをしようとすると、「予期しないエラーが発生しました」というメッセージが表示されます

Builder ID AWS がコードベースの認証アプリと組み合わせて使用するものなど、時間ベースのワンタイムパスワード (TOTP) システムは、クライアントとサーバー間の時間同期に依存します。認証アプリケーションをインストールしているデバイスが信頼できるタイムソースに正しく同期されていることを確認するか、またはデバイスの時間を、「NIST」やその他のローカル/地域など、信頼できるソースと一致するように手動で設定してください。

AWS Builder ID にサインインしようとすると、「It's not you, it's us」というメッセージが表示されます。

サインインに使用するデバイスの日付と時刻の設定を確認してください。日付と時刻は自動設定にすることをお勧めします。利用できない場合は、日付と時刻を既知の Network Time Protocol (NTP) サーバーに同期することをお勧めします。

サインアウトしても完全にサインアウトされない

システムはすぐにサインアウトするように設計されていますが、完全にサインアウトするには最大で 1 時間かかる場合があります。

> **Note**
>
> Google や Apple などのソーシャルログインアカウントを使用する場合、アクティブな AWS ビルダー ID セッションを削除しても、ソーシャルログインアカウントからログアウトされることはありません。

まだ問題を解決しようとしています

サポートフィードバックフォームに記入できます。リクエスト情報セクションの「How can we help, include that you're using AWS Builder ID」を参照してください。問題に最大限効率的に対処できるように、できるだけ詳しく説明してください。

AWS の 管理ポリシー AWS サインイン

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 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 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 管理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。

AWS マネージドポリシー: AmazonManagedSignUpServicePolicy

このAmazonManagedSignUpServicePolicyポリシーは、 AWS アカウントサインアッププロセスを完了するために必要なアクセス許可を付与します。

ユーザー、グループおよびロールに AmazonManagedSignUpServicePolicy をアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- 顧客検証 - 検証ドキュメントのアップロード URL の作成など、顧客検証の詳細と適格性ステータスの作成、取得、更新を許可します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AmazonManagedSignUpServicePolicy」を参照してください。

AWS マネージドポリシー: ApplicationProvisioningPolicy

ApplicationProvisioningPolicy ポリシーは、アプリケーションのプロビジョニングおよび ID 管理オペレーションに関する包括的な権限を付与します。これには、IAM ロールとポリシーの管理、SSO 設定、ID ストアオペレーションなどが含まれます。

ユーザー、グループおよびロールに `ApplicationProvisioningPolicy` をアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- IAM 管理 - ロールとポリシーの作成、更新、削除、ロールアタッチメントの管理、サービスにリンクされたロールの作成など、包括的な IAM オペレーションを許可します。
- Research and Engineering Studio on AWS - Research and Engineering Studio on AWS リソースに対するすべてのオペレーションを許可します。
- ロールの受け渡し - IAM ロールを他のサービスに渡すことを許可します。
- IAM アイデンティティセンター - IAM アイデンティティセンターのインスタンス、アプリケーション、割り当て、許可、認証方法の管理を許可します。
- ID ストア - ID ストアからのユーザーおよびグループの情報の読み取りを許可します。
- IAM アイデンティティセンター OAuth - IAM アイデンティティセンター OAuth を介した IAM セッションの認証を許可します。
- ユーザープロファイルとディレクトリ - IAM アイデンティティセンターコネクタ、ユーザープロファイル、外部 ID プロバイダーのセットアップを含むディレクトリ設定を管理できます。
- ユーザーサブスクリプション - ユーザーサブスクリプションのリスト表示を許可します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「ApplicationProvisioningPolicy」を参照してください。

AWS マネージドポリシー: SignInLocalDevelopmentAccess

このSignInLocalDevelopmentAccessポリシーは、コンソール認証情報 AWS を使用して へのプログラムによるアクセス許可を付与します。

ユーザー、グループおよびロールに `SignInLocalDevelopmentAccess` をアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- OAuth2 アクセスの認可 - ブラウザを介して認証し、認証情報交換用の OAuth 2.0 認可コードを取得するアクセス許可を付与します
- OAuth2 トークンの作成 - 開発者ツールやアプリケーションから AWS サービスにアクセスするために使用できる OAuth 2.0 アクセストークンと更新トークンの認可コードを交換するアクセス許可を付与します

> **Note**
>
> この AWS 管理ポリシーを追加すると、同じデバイス認証とクロスデバイス認証の両方のアクセス許可が付与されます。このポリシーは、次のリソースに対するアクションを承認します。
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost` – を使用した同一デバイス認証に使用されます`aws login`。
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote` – を使用したクロスデバイス認証に使用されます`aws login --remote`。
>
> いずれかの認証方法へのアクセスを制御するには、独自の管理ポリシーまたはサービスコントロールポリシー (SCP) を作成できます。これらのリソース ARNs を使用して、コンソール認証情報を使用した AWS へのプログラムによるアクセスを許可または拒否します。

詳細については、「コンソール認証情報を使用してログインする (推奨)」を参照してください。JSON ポリシードキュメントの最新バージョンなど、ポリシーの詳細については、「 AWS マネージドポリシーリファレンスガイド」のSignInLocalDevelopmentAccess」を参照してください。

AWS マネージドポリシー: AWSSignInResourcePolicyManagement

このAWSSignInResourcePolicyManagementポリシーは、 AWS サインインのコンソール認可設定とリソース許可ステートメントを管理するアクセス許可を付与します。

ユーザー、グループおよびロールに AWSSignInResourcePolicyManagement をアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- signin:PutConsoleAuthorizationConfiguration – コンソール認可設定を作成または更新します。
- signin:GetConsoleAuthorizationConfiguration – 現在のコンソール認可設定を取得します。
- signin:DeleteConsoleAuthorizationConfiguration – コンソール認可設定を削除します。
- signin:PutResourcePermissionStatement – リソースアクセス許可ステートメントを作成または更新します。
- signin:DeleteResourcePermissionStatement – リソースアクセス許可ステートメントを削除します。
- signin:ListResourcePermissionStatements – アカウントのリソースアクセス許可ステートメントを一覧表示します。
- signin:GetResourcePolicy – 統合されたリソースベースのポリシーを取得します。

ポリシー JSON は次のとおりです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
                "signin:PutResourcePermissionStatement",
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

このポリシーを AWS 、サインインのリソースベースのポリシーを管理する IAM プリンシパル (ユーザーまたはロール) にアタッチします。これには、ネットワークベースのアクセスコントロールの設定を担当するセキュリティ管理者、コンソールアクセスポリシーを監査する必要があるコンプライアンス担当者、緊急復旧アクセス設定を管理する運用チームが含まれます。

> **Important**
>
> このポリシーは、コンソール認可コントロールへの管理アクセスを許可します。このポリシーを割り当てるときは、最小特権の原則を適用します。IAM 条件を使用して、これらのアクセス許可をいつ、どのように使用できるかをさらに制限することを検討してください。

JSON ポリシードキュメントの最新バージョンなど、ポリシーの詳細については、「 AWS マネージドポリシーリファレンスガイド」のAWSSignInResourcePolicyManagement」を参照してください。

AWS サインイン AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS サインイン してからの AWS の管理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、 AWS サインインドキュメント履歴ページの 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
AWSSignInResourcePolicyManagement – 新しいポリシー	AWS サインインのコンソール認可設定とリソース許可ステートメントを管理するアクセス許可を付与する新しい AWS 管理ポリシーを追加しました。	2026 年 6 月 10 日
SignInLocalDevelopmentAccess – 新しいポリシー	既存のコンソール認証情報 AWS を使用して へのプログラムによるアクセス許可を付与する新しい AWS マネージドポリシーを追加しました。	2025 年 11 月 19 日
ApplicationProvisioningPolicy – 新しいポリシー	IAM ロールとポリシー管理、IAM Identity Center 設	2025 年 9 月 30 日

変更	説明	日付
	定、Identity Store オペレーションなど、アプリケーションのプロビジョニングと ID 管理オペレーションの包括的なアクセス許可を付与する新しい AWS マネージドポリシーを追加しました。	
AmazonManagedSignUpServicePolicy – 新しいポリシー	顧客検証や支払い設定オペレーションなど、 AWS アカウントのサインアッププロセスに必要なアクセス許可を付与する新しい AWS マネージドポリシーを追加しました。	2025 年 9 月 30 日
AWS サインイン が変更の追跡を開始しました	AWS サインイン は、 AWS 管理ポリシーの変更の追跡を開始しました。	2025 年 9 月 30 日

ドキュメント履歴

次の表に、 AWS サインインドキュメントへの重要な追加点を示します。また、お客様からいただいたフィードバックに対応するために、ドキュメントを頻繁に更新しています。

- ドキュメントの最終更新日: 2026 年 6 月 10 日

変更	説明	日付
サインインリソースベースのポリシーとリソースコントロールポリシーのサポート	サインインリソースベースのポリシーとリソースコントロールポリシー (RCPs)、新しい条件キーリファレンス、 `AWSSignInResourcePolicyManagement` 管理ポリシー、および関連するトラブルシューティングを使用して AWS マネジメントコンソール アクセスを制御するためのドキュメントを追加しました。	2026 年 6 月 10 日
GitHub と Amazon でのサインインのサポート	AWS サインイン は、GitHub でサインインと Amazon でサインインをサポートするようになりました。これにより、GitHub または Amazon アカウント AWS ビルダー ID を使用して を作成できます。	2026 年 3 月 10 日
Apple でのサインインのサポート	AWS サインイン で Apple でサインインがサポートされるようになりました。これにより、Apple Account. AWS ビルダー ID topics が更新され、AWS ビルダー ID 問題	2026 年 2 月 5 日

	のトラブルシューティングに追加された新しいトラブルシューティングトピック AWS ビルダー ID を使用して を作成できます。	
新しい 管理ポリシー	AWS サインイン は新しい マネージドポリシーをリリースしました。 は、既存のコンソール認証情報 AWS を使用して へのプログラムによるアクセス許可`SignInLocalDevelopmentAccess` を付与します。詳細については、「AWS サインイン AWS 管理ポリシーの更新」を参照してください。	2025 年 11 月 19 日
Google でのサインインのサポート	AWS サインイン は Google でサインインをサポートするようになりました。これにより、Google Account. AWS ビルダー ID topics が更新され、AWS ビルダー ID 問題のトラブルシューティングに追加された新しいトラブルシューティングトピック AWS ビルダー ID を使用して を作成できます。	2025 年 9 月 30 日

新しいマネージドポリシー	AWS サインイン は、2 つの新しい マネージドポリシー をリリースしました。 は、AWS アカウントサインアッププロセスを完了するために必要なアクセス許可AmazonManagedSignUpServiceP olicy を付与します。 は、アプリケーションのプロビジョニングと ID 管理オペレーションのための包括的なアクセス許可ApplicationProvisioningPolicy を付与します。詳細については、「AWS サインイン AWS 管理ポリシーの更新」を参照してください。	2025 年 9 月 30 日
更新されたトラブルシューティングのトピック	AWS ビルダー ID と にサインインするための新しいトラブルシューティングトピックを追加しました AWS マネジメントコンソール。	2024 年 2 月 27 日
組織に関するいくつかのトピックを更新しました	ユーザータイプの更新、ユーザータイプの決定の削除、そのコンテンツのユーザータイプへの組み込み、 へのサインイン方法 AWS	2023 年 5 月 15 日
いくつかのトピックとトップバナーを更新しました	ユーザータイプ、ユーザータイプの決定、サインイン方法 AWS、AWS サインインとは を更新しました。ルートユーザーと IAM ユーザーのサインイン手順も更新しました。	2023 年 3 月 3 日

AWS マネジメントコンソールサインインの概要の段落を更新しました	ユーザータイプの決定をページ上部に移動し、アカウントルートユーザーにあるメモを削除しました。	2023 年 2 月 27 日
追加済み AWS ビルダー ID	AWS サインインユーザーガイドに AWS ビルダー ID トピックを追加し、コンテンツを既存のトピックに統合しました。	2023 年 1 月 31 日
組織の最新情報	お客様からのフィードバックに基づいて、サインイン方法についてより明確になるように目次を更新しました。サインインチュートリアルを更新しました。用語とユーザータイプの決定を更新しました。IAM ユーザーやルートユーザーなどの用語を定義するためのクロスリンクが改善されました。	2022 年 12 月 22 日
新しいガイド	これは、 AWS 「 サインインユーザーガイド」の最初のリリースです。	2022 年 8 月 31 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。