AWS Single Sign-On

ユーザーガイド

AWS Single Sign-On: ユーザーガイド

Table of Contents

AWS Single Sign-On とは

AWS Single Sign-On は、AWS アカウントおよびクラウドアプリケーションへの SSO アクセスの一元管理を容易にするクラウドベースのシングルサインオン (SSO) サービスです。特に、AWS Organizations 内のすべての AWS アカウントを対象に SSO アクセスとユーザーアクセス許可を管理するうえで役立ちます。AWS SSO はまた、一般的に使用されているサードパーティー SaaS (Software-as-a-Service) や Security Assertion Markup Language (SAML) 2.0 をサポートするカスタムアプリケーションに対するアクセスとアクセス許可を管理するのにも便利です。AWS SSO には、エンドユーザーが自分に割り当てられている AWS アカウント、クラウドアプリケーション、カスタムアプリケーションを一元的に検索したり確認したりできるユーザーポータルが含まれます。

AWS SSO の機能

AWS SSO には次の機能があります。

AWS Organizations との統合

AWS SSO は、他のクラウドネイティブな SSO ソリューションとは異なり、AWS Organizations および AWS API のオペレーションと緊密に統合されます。AWS SSO は AWS Organizations とネイティブに統合され、すべての AWS アカウントを列挙します。アカウントが組織単位 (OU) 内に整理されている場合は、AWS SSO コンソールにも同じように表示されます。この方法により、AWS アカウントのすばやい検出、一般的なアクセス許可セットのデプロイ、およびアクセスの一元管理ができるようになります。

AWS アカウントおよびクラウドアプリケーションへの SSO アクセス

AWS SSO を通じて、すべての AWS アカウント、クラウドアプリケーション、および SAML 2.0 ベースのカスタムアプリケーションにわたって SSO アクセスを容易に管理できるようになります。カスタムスクリプトやサードパーティーのソリューションは必要ありません。–AWS SSO コンソールを使用すると、パーソナライズされたエンドユーザーポータルに対するアクセスを許可したアプリケーションへのワンクリックアクセスを付与するユーザーを、すばやく割り当てることができます。

AWS SSO でユーザーとグループを作成および管理する

サービスを初めて有効にするとき、AWS SSO にデフォルトのディレクトリを作成し ます。このディレクトリを使用して、コンソールで直接ユーザーとグループを管理できます。または、必要に応じて、既存の AWS Managed Microsoft AD ディレクトリに接続して、Windows Server で提供されている標準の Active Directory 管理ツールでユーザーを管理することもできます。AWS SSO でユーザーを管理することを選択した場合、ユーザーの迅速な作成とグループへの整理がすべてコンソール内で簡単に実行できます。

既存の社内認証の活用

AWS SSO は AWS Directory Service を介して Microsoft AD と統合されています。つまり、従業員は社内の Active Directory 認証情報を使用して AWS SSO ユーザーポータルにサインインできます。Active Directory のユーザーに各種アカウントとアプリケーションへのアクセス権を付与するには、ユーザーを適切な Active Directory グループに追加するだけです。たとえば、DevOps グループ SSO アクセス権限を本番環境の AWS アカウントに付与できます。DevOps グループに追加されたユーザーには、これらの AWS アカウントへの SSO アクセスが自動的に付与されます。このオートメーションによって、新規ユーザーをオンボードさせたり、既存のユーザーに新規アカウントとアプリケーションを即座に割り当てたりすることが簡単になります。

一般的に使用されているクラウドアプリケーションとの互換性

AWS SSO では、Salesforce、Box、Office 365 など、一般的に使用されているクラウドアプリケーションをサポートしています。したがって、アプリケーション統合手順を用意することで、こうしたアプリケー

ションに SSO を設定するための時間を短縮できます。これらの手順は、これらの SSO 設定とトラブルシューティングにおいて管理者を支援するガードレールの役割を果たします。管理者は各クラウドアプリケーションの詳細な設定について学習する必要がなくなります。

セットアップと使用状況のモニタリングが簡単

AWS SSO では、可用性の高い SSO サービスをわずか数クリックで有効化できます。追加のインフラストラクチャをデプロイしたり、AWS アカウントを追加で設定することはありません。AWS SSO は高い可用性と安全性を備え、ニーズに合わせて拡張や縮小ができるインフラストラクチャであり、管理するにあたってソフトウェアやハードウェアは必要ありません。AWS SSO は AWS CloudTrail 内のすべてのサインインアクティビティを記録するとともに、SSO アクティビティを一元的にモニタリングおよび監査するための可視性を提供します。

開始方法

この開始方法では、AWS Single Sign-On を有効化してディレクトリに接続し、AWS アカウントに SSO を設定し、最終的にはクラウドアプリケーションに SSO を設定します。必須ではありませんが、コンソールを使用する前に「AWS Single Sign-On の重要な概念の理解 (p. 6)」を確認し、コア機能や用語について理解されておくことをお勧めします。

トピック

AWS SSO の前提条件

AWS SSO をセットアップする前に、次の操作を行う必要があります。

- まず AWS Organizations サービスを設定し、[すべての機能] を有効化します。この設定の詳細については、『AWS Organizations ユーザーガイド』の「組織内のすべての機能の有効化」を参照してください。
- AWS SSO の設定を開始する前に、AWS Organizations のマスターアカウント認証情報を使用してサインインします。AWS SSO の有効化にはこの認証情報が必要です。詳細については、『AWS Organizations ユーザーガイド』の「AWS 組織の作成と管理」を参照してください。組織のメンバーアカウントの認証情報を使用してサインインしている場合は、AWS SSO を設定できません。
- ディレクトリストアを選択して、ユーザーポータルへの SSO アクセスがあるユーザープールを決定します。ユーザーストアにデフォルトの AWS SSO ディレクトリを使用するように選択した場合は、前提条件となるタスクは不要です。AWS SSO を有効にすると、AWS SSO ディレクトリがデフォルトで作成され、すぐに使用できる状態になります。このディレクトリタイプを使用してもコストは発生しません。ユーザーストアの既存の Active Directory に接続する場合は、以下の状態である必要があります。
  - AWS Directory Service に既存の AWS Managed Microsoft AD ディレクトリを設定し、それを組織のマスターアカウント内に配置していること。一度に接続できる AWS Managed Microsoft AD ディレクトリは 1 つのみです。ただし、いつでも別の AWS Managed Microsoft AD ディレクトリに変更、または AWS SSO ディレクトリに戻すことができます。詳細については、『AWS Directory Service Administration Guide』の「AWS Managed Microsoft AD ディレクトリの作成」を参照してください。
  - AWS Managed Microsoft AD ディレクトリが、AWS SSO が利用できる 米国東部 (バージニア北部) (us-east-1) リージョンに存在していること。AWS SSO では、割り当てデータは、ディレクトリと同じリージョンに保存されます。AWS SSO を管理するには、us-east-1 リージョンに所在する必要があります。また、AWS SSO のユーザーポータルでは、接続されたディレクトリと同じアクセス URL が使用されます。

AWS SSOの有効化

AWS SSO コンソールを初めて開くと、その管理を開始するために AWS SSO の有効化を求めるプロンプトが表示されます。すでにこのオプションを選択している場合、このステップは省略できます。選択していない場合、次の手順を使用してその場で有効化します。有効化すると、IAM サービスにリンクされたロールを AWS 組織内の AWS アカウントのいずれかに作成するために必要なアクセス許可が AWS SSO に付与されます。この時点で、サービスにリンクされたロールは作成されません。AWS SSO は後

に、SSO アクセスを AWS アカウントに設定するプロセスの中でこれらのロールを作成します (「AWS アカウントへの SSO の設定 (p. 4)」を参照してください)。

AWS SSO を有効化するには

1. AWS Organizations のマスターアカウント認証情報を使用して AWS マネジメントコンソール にサインインします。
2. AWS SSO コンソールを開きます。
3. [AWS SSO の有効化] を選択します。
4. まだ AWS Organizations, を設定していない場合は、組織を作成するよう要求されます。このプロセスを完了するには、[AWS 組織の作成] を選択します。

ディレクトリを選択する

ディレクトリを選択すると、AWS SSO が、SSO アクセスを必要とするユーザーとグループを検索する場所が決まります。デフォルトでは、迅速かつ簡単なユーザー管理のために AWS SSO ディレクトリを取得します。必要に応じて、AWS Managed Microsoft AD ディレクトリをオンプレミス Active Directory に接続することもできます。

AWS SSO はこのディレクトリ内のユーザーに、パーソナライズされたユーザーポータルが提供されます。ユーザーはそのポータルから複数の AWS アカウントやクラウドアプリケーションを簡単に起動できます。ユーザーは社内認証情報、または AWS SSO で設定した認証情報を使用してポータルにサインインします。サインインすると、事前に許可しているすべてのアプリケーションと AWS アカウントにワンクリックでアクセスできます。

設定するディレクトリタイプによって、以下のトピックのガイダンスを参照してください。

- AWS SSO ディレクトリの管理 (p. 8)
- Microsoft AD ディレクトリへの接続 (p. 11)

サポートされているディレクトリのタイプの詳細については、「ディレクトリの管理 (p. 8)」を参照してください。

AWS アカウントへの SSO の設定

このステップでは、接続されたディレクトリ内のユーザーに対して、AWS 組織の特定の AWS アカウントに提供されている 1 つまたは複数の AWS コンソールへの SSO アクセスを付与できます。結果的に、ユーザーには各自のユーザーポータル内で割り当てられている AWS アカウントのアイコン (「Development」など) のみが表示されます。アイコンをクリックすると、その AWS アカウントで AWS マネジメントコンソール にサインインするときに使用する IAM ロールを選択できます。

AWS アカウントへの SSO アクセスの割り当てを開始するには、「ユーザーアクセスを割り当てる (p. 17)」を参照してください。

クラウドアプリケーションへの SSO の設定

設定するアプリケーションタイプによって、次のいずれかの手順を実行します。

- クラウドアプリケーションを追加して設定する (p. 24)
- カスタム SAML 2.0 アプリケーションを追加して設定する (p. 25)

サポートされているアプリケーションのタイプの詳細については、「アプリケーションへの SSO を管理する (p. 22)」を参照してください。

必要な手順が完了すると、AWS SSO が適切に設定され、サービスプロバイダとの信頼関係が確立されます。ユーザーは、割り当てられたアクセス権限に基づいて各自のユーザーポータル内からこれらのアプリケーションにアクセスできるようになります。

AWS Single Sign-On の重要な概念の理解

SAML フェデレーション、ユーザー認証、IAM アクセス権限に関する重要な概念を理解できれば、AWS Single Sign-On をさらに活用できます。

トピック

SAML フェデレーション

AWS SSO は SAML (セキュリティアサーションマークアップランゲージ) 2.0 を使用して ID フェデレーションをサポートしています。SAML 2.0 は、SAML 認証機関 (ID プロバイダーすなわち IdP) と SAML コンシューマー (サービスプロバイダーすなわち SP) との間でユーザーに関する情報を渡す SAML アサーションを安全に交換するための業界標準です。AWS SSO サービスは、この情報を使用して、AWS SSO ユーザーポータル内でアプリケーションの使用が許可されているユーザーに、フェデレーションシングルサインオン (SSO) を提供します。

AWS SSO は SAML IdP 機能を AWS Managed Microsoft AD または AWS SSO ディレクトリに追加します。それにより、ユーザーは、AWS マネジメントコンソール やサードパーティー製アプリケーション (Office 365、Concur、Salesforce など) を含め、SAML をサポートするサービスへの SSO が可能になります。現時点で AWS SSO は、その他のディレクトリタイプまたは IdP をサポートしていません。

ユーザー認証

ユーザーがユーザー名を使用してユーザーポータルにサインインすると、AWS SSO は、ユーザーの E メールアドレスに関連付けられたディレクトリに基づいて、リクエストを AWS SSO 認証サービスにリダイレクトします。認証されると、AWS アカウントとサードパーティー製 SaaS (Software-as-a-Service) アプリケーションが追加のサインインプロンプトなしでポータルに表示されて、それらへの SSO アクセスが可能になります。つまり、ユーザーは、割り当てられて日常使用しているさまざまな AWS アプリケーションに対して、複数のアカウント認証情報を管理する必要がなくなります。

アクセス権限セット

アクセス許可セットは管理者定義のポリシーの集合であり、特定の AWS アカウントに対するユーザーのアクセス許可が有効かどうかを判断するために、AWS SSO で使用されます。アクセス許可セットには、AWS 管理ポリシー、または AWS SSO に保存されているカスタムポリシーを含めることができます。ポリシーは基本的に、1 つ以上のアクセス権限ステートメントのコンテナとして機能するドキュメントです。これらのステートメントは、さまざまなタスクに対する個々のアクセスコントロール (許可または拒否) を表し、AWS アカウント内でユーザーにどのタスクの実行を許可するかしないかを決定します。

アクセス許可セットは AWS SSO に保存され、AWS アカウントにのみ使用されます。クラウドアプリケーションへのアクセスの管理には使用されません。アクセス許可セットは最終的に、特定の AWS アカ

ウントの IAM ロールとして作成し、信頼ポリシーでユーザーが AWS SSO を介してそのロールを引き受けることを許可します。

ディレクトリの管理

AWS SSO でディレクトリを設定して、ユーザーとグループを保管する場所を指定できます。設定が完了すると、ディレクトリでユーザーまたはグループを検索して、AWS アカウント、クラウドアプリケーション、またはその両方へのシングルサインオンアクセスを付与することができます。

デフォルトでは、AWS SSO により、AWS SSO 内でユーザーとグループの管理に使用できるディレクトリが自動的に提供されます。AWS SSO への保存を選択した場合は、ユーザーとグループを作成し、AWS アカウントとアプリケーションにアクセスのレベルを割り当てます。または、AWS Directory Service を使用して オンプレミスの Active Directory に AWS SSO を接続する (p. 12) か AWS Managed Microsoft AD ディレクトリに AWS SSO を接続する (p. 11)を選択できます。

> Note
>
> AWS SSO は、SAMBA4 ベースの Simple AD を接続先ディレクトリとしてサポートしていません。

トピック

AWS SSO ディレクトリの管理

AWS Single Sign-On では、ユーザーとグループを保存できるデフォルトのディレクトリが利用できます。AWS SSO に保存することを選択した場合、必要なすべての操作は次のとおりです。

1. ユーザーとグループを作成します。
2. ユーザーをメンバーとしてグループに追加します。
3. グループに、AWS アカウントとアプリケーションへの希望するレベルのアクセスを割り当てます。

> Note
>
> AWS SSO ディレクトリで作成するユーザーとグループは、AWS SSO でのみ使用することができます。

AWS Managed Microsoft AD でユーザーを管理する場合は、いつでも AWS SSO ディレクトリの使用を中止し、代わりに、AWS Directory Service を使用して AWS SSO を Microsoft AD に接続できます。詳細については、「Microsoft AD ディレクトリへの接続 (p. 11)」を参照してください。

トピック

ユーザーの追加

次の手順に従って、AWS SSO ディレクトリにユーザーを追加します。

ユーザーを追加するには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[ユーザー] タブを選択し、次に [ユーザーを追加] を選択します。
4. [ユーザーを追加] ページで、以下の必要な情報を入力します。

    a. E メールアドレス
    b. パスワード – ユーザーのパスワードを送信するには、以下の選択肢からいずれかを選択します。

        i. パスワードの設定手順が記載された E メールをユーザーに送信 – このオプションでは、Amazon Web Services からユーザーに自動的に E メールアドレスが送信され、貴社に代わって、AWS SSO ユーザーポータルにアクセスするようにユーザーを招待します。
        ii. ユーザーと共有することができるワンタイムパスワードを生成します – このオプションでは、E メールアドレスから手動でユーザーに送信できる、ユーザーポータルの URL とパスワードの詳細が利用できます。

    c. 名
    d. 姓
    e. 表示名

        Note

        (オプション) AWS SSO で、ユーザーの ID を、ユーザーが使用する必要がある、特定のビジネスアプリケーションにマッピングするのに役立つ、従業員 ID や Office 365 イミュータブル ID などの追加の属性を提供できます。
5. [Next: Groups (次: グループ)] を選択します。
6. ユーザーをメンバーにする 1 つ以上のグループを選択し、[ユーザーを追加] を選択します。

グループの追加

次の手順に従って、AWS SSO ディレクトリにグループを追加します。

グループを追加するには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[グループ] タブを選択し、次に [グループの作成] を選択します。
4. [グループの作成] ダイアログで、[グループの名前] と [説明] を入力します。説明は、グループにどのようなアクセス許可が割り当てられているか (または割り当てられるか) に関する詳細を記載する必要があります。
5. [作成] を選択します。

グループにユーザーを追加

以下の手順に従って、以前に AWS SSO ディレクトリに作成したグループのメンバーとしてユーザーを追加します。

グループのメンバーとしてユーザーを追加するには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[グループ] タブを選択し、次にリストからグループを選択します。

4. グループの [詳細] ページにある [グループメンバー] の下で、[ユーザーの追加] を選択します。
5. [ユーザーをグループに追加] ページで、メンバーとして追加するユーザーを見つけます。それぞれの横にあるチェックボックスをオンにします。
6. [Add user] を選択します。

ユーザーのプロパティの編集

以下の手順に従って、AWS SSO ディレクトリでユーザーのプロパティを編集します。

ユーザーのプロパティを編集するには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[ユーザー] タブを選択し、次に編集するユーザーを選択します。
4. ユーザーの [詳細] ページで、[ユーザーの編集] を選択します。
5. [ユーザーの詳細を編集する] ページで、必要に応じてプロパティを更新し、[変更の保存] を選択します。

   Note

   (オプション) AWS SSO で、ユーザーの ID を、ユーザーが使用する必要がある、特定のビジネスアプリケーションにマッピングするのに役立つ、従業員 ID や Office 365 イミュータブル ID などの追加の属性を変更できます。

ユーザーを無効にする

ユーザーを無効にすると、そのユーザーの詳細の編集、パスワードのリセット、グループへのユーザーの追加、またはそのグループメンバーシップの表示はできません。次の手順に従って、AWS SSO ディレクトリでユーザーを無効にします。

ユーザーを無効にするには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[ユーザー] タブを選択し、次に無効にするユーザーを選択します。
4. [ユーザーを無効化] ダイアログボックスで、[ユーザーを無効化] を選択します。

   Note

   ユーザーを無効にすると、そのユーザーはユーザーポータルにサインインできなくなります。

ユーザーパスワードのリセット

以下の手順に従って、AWS SSO ディレクトリでユーザーのパスワードをリセットします。

ユーザーのパスワードをリセットするには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[ユーザー] タブを選択し、次にパスワードを変更するユーザーを選択します。

4. [パスワードのリセット] ダイアログで、次の選択肢のいずれかを選び、[パスワードのリセット] を選択します。

   a. パスワードのリセット手順が記載された E メールをユーザーに送信します – このオプションでは、Amazon Web Services から、パスワードをリセットする方法について説明する E メールアドレスを自動的にユーザーに送信します。
   b. ワンタイムパスワードを生成し、ユーザーと共有します – このオプションでは、E メールアドレスから手動でユーザーに送信できる、パスワードの詳細が利用できます。

Microsoft AD ディレクトリへの接続

AWS Directory Service を使用して、管理者は AWS Single Sign-On からオンプレミスの Active Directory (AD) または AWS Managed Microsoft AD ディレクトリに接続できます。この Microsoft AD ディレクトリでは、管理者が AWS SSO コンソールを使用してシングルサインオン (SSO) アクセスを割り当てるときに、プル元の ID プールを定義します。会社のディレクトリを AWS SSO に接続すると、管理者は AD ユーザーまたはグループに AWS アカウント、クラウドアプリケーション、またはその両方へのアクセスを許可できます。

AWS Directory Service により、AWS クラウドでホストされているスタンドアロンの AWS Managed Microsoft AD ディレクトリを設定して実行できます。また、AWS Directory Service を使用して AWS リソースを既存のオンプレミスの Microsoft Active Directory に接続することもできます。オンプレミスの Active Directory と連携するように AWS Directory Service を設定するには、最初に、認証をオンプレミスからクラウドに拡張するように信頼関係を設定する必要があります。

> Note
>
> AWS SSO は、SAMBA4 ベースの Simple AD を接続先ディレクトリとしてサポートしていません。

トピック

AWS Managed Microsoft AD ディレクトリに AWS SSO を接続する

AWS Directory Service で管理されている AWS Managed Microsoft AD ディレクトリを AWS SSOに接続するには、以下の手順を実行します。

AWS SSO を AWS Managed Microsoft AD に接続するには

1. AWS SSO コンソールを開きます。

   > Note
   >
   > 次のステップに進む前に、AWS SSO コンソールで、AWS Managed Microsoft AD ディレクトリがあるリージョンのいずれかを使用していることを確認してください。

2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで以下の操作を実行します。

   a. [使用可能なディレクトリ] で、AWS SSO を接続する AWS Managed Microsoft AD ディレクトリを選択します。

b. [User portal URL] (ユーザーポータル URL) に、ユーザーポータルのサインイン URL に使用するプレフィックスを入力します。

4. [Connect directory] (ディレクトリの接続) を選択します。

オンプレミスの Active Directory に AWS SSO を接続する

オンプレミスの Active Directory のユーザーには、AWS アカウントと AWS SSO ユーザーポータルにあるクラウドアプリケーションへの SSO アクセスもあります。そのために、AWS Directory Serviceでは次の 2 つのオプションが利用できます。

- 双方向の信頼関係を作成する – AWS Managed Microsoft AD とオンプレミスの Active Directory との間で作成される双方向の信頼関係により、オンプレミスのユーザーは会社の認証情報を使用してさまざまな AWS サービスおよびビジネスアプリケーションにサインインできます。一方向の信頼は AWS SSO では機能しません。双方向の信頼関係の設定の詳細については、『AWS Directory Service Administration Guide』の「信頼関係を作成する場合」を参照してください。
- AD Connector を作成する – AD Connector は、クラウドに情報をキャッシュすることなく、オンプレミスの Active Directory にディレクトリリクエストをリダイレクトできるディレクトリゲートウェイです。詳細については、『AWS Directory Service Administration Guide』の「ディレクトリに接続する」を参照してください。

  Note

  AWS SSO は SAMBA4 ベースの Simple AD ディレクトリでは機能しません。

属性マッピング

属性マッピングは、AWS SSO に存在する属性タイプを AWS Managed Microsoft AD ディレクトリにある同様の属性にマッピングするために使用されます。AWS SSO は、Microsoft AD ディレクトリからユーザー属性を取得し、AWS SSO ユーザー属性にマッピングします。AWS SSO のこれらのユーザー属性マッピングは、クラウドアプリケーションの SAML アサーションを生成するために使用されます。クラウドアプリケーションによって、正常なシングルサインオンに必要な SAML 属性のリストは異なります。

AWS SSO は、アプリケーションの設定ページの [属性マッピング] タブから一連の属性を事前に取得します。AWS SSO は、これらのユーザー属性を使用して、クラウドアプリケーションに送信される SAML アサーション (SAML 属性) を設定します。次に、これらのユーザー属性が Microsoft AD ディレクトリから取得されます。詳細については、「アプリケーションの属性を AWS SSO の属性にマップする (p. 28)」を参照してください。

AWS SSO は、ディレクトリの設定ページの [属性マッピング] セクションにある一連の属性も管理します。詳細については、「AWS SSO の属性を AWS Managed Microsoft AD ディレクトリの属性にマップする (p. 14)」を参照してください。

サポートされているディレクトリの属性

以下の表では、サポートされている AWS Managed Microsoft AD ディレクトリの属性のうち、AWS SSO のユーザー属性にマップできるものをすべて示しています。

Microsoft AD ディレクトリでサポートされている属性
`${dir:email}`
`${dir:displayname}`

Microsoft AD ディレクトリでサポートされている属性
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

サポートされている Microsoft AD ディレクトリの属性の任意の組み合わせを指定して、AWS SSO の 1 つの属性にマップできます。たとえば、[AWS SSO のユーザー属性] 列の下で `preferredUsername` 属性を選択し、その属性を `${dir:displayname}`、または `${dir:lastname}${dir:firstname }` またはサポートされている任意の 1 つの属性にマップするか、サポートされている属性の任意の組み合わせにマップできます。

サポートされている AWS SSO 属性

以下の表では、サポートされている AWS Managed Microsoft AD ディレクトリの属性のうち、ユーザー属性にマップできる AWS SSO 属性をすべて示しています。後で、アプリケーションの属性マッピングを設定するときに、これらの同じ AWS SSO の属性を、そのアプリケーションで使用されている実際の属性にマップできます。

サポートされている AWS SSO の属性
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:firstName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

デフォルトのマッピング

以下の表に示しているのは、AWS SSO のユーザー属性と AWS Managed Microsoft AD ディレクトリのユーザー属性とのデフォルトのマッピングです。現時点で AWS SSO は、[AWS SSO のユーザー属性] 列の属性のリストのみをサポートしています。

AWS SSO のユーザー属性	Microsoft AD ディレクトリのこの属性へのマップ
`AD_GUID`	`${dir:guid}`
`email`	`${dir:windowsUpn}`
`familyName`	`${dir:lastname}`
`givenName`	`${dir:firstname}`
`middleName`	`${dir:initials}`
`name`	`${dir:displayname}`
`preferredUsername`	`${dir:displayname}`
`subject`	`${dir:windowsUpn}`

必要に応じて、デフォルトのマッピングを変更したり、SAML アサーションに属性を追加したりできます。たとえば、クラウドアプリケーションの `User.Email` SAML 属性にユーザー E メールが必要であり、E メールを Microsoft AD ディレクトリの `windowsUpn` 属性に保存するとします。このマッピングのためには、AWS SSO コンソールで以下の 2 つの場所を変更する必要があります。

1. [ディレクトリ] ページ、[属性マッピング] セクションで、ユーザー属性 **`email`** を **`${dir:windowsUpn}`** 属性 ([Maps to this attribute in your directory (マップされるディレクトリの属性)] 列内) にマップする必要があります。
2. [アプリケーション] ページで一覧からアプリケーションを選択し、[属性マッピング] タブを選択してから、`User.Email` 属性を **`${user:email}`** 属性 ([マップされる AWS SSO の文字列値またはユーザー属性] 列内) にマップする必要があります。

ディレクトリの各属性は ${dir:**`AttributeName`**} 形式で指定する必要があります。たとえば、Microsoft AD ディレクトリの `firstname` 属性は `${dir:firstname}` になります。ディレクトリのすべての属性に実際の値が割り当てられていることが重要です。属性で `${dir:` の後に値がないと、ユーザーのサインイン時に問題が発生します。

AWS SSO の属性を AWS Managed Microsoft AD ディレクトリの属性にマップする

AWS SSO のユーザー属性を Microsoft AD ディレクトリの対応する属性にマップする方法を指定するには、以下の手順を実行します。

AWS SSO の属性をディレクトリの属性にマップするには

1. AWS SSO コンソールを開きます。
2. [接続先ディレクトリ] を選択します。
3. [Attribute mappings] (属性マッピング) で、[Edit attribute mappings] (属性マッピングの編集) を選択します。
4. [属性マッピングの編集] ページで、マップする AWS SSO の属性を見つけ、テキストボックスに値を入力します。たとえば、AWS SSO のユーザー属性 **`email`** を接続先ディレクトリの **`${dir:windowsUpn}`** 属性にマップできます。
5. [Save changes] を選択します。

ディレクトリのタイプの変更

ユーザーの保存場所はいつでも変更することができます。以下の手順を使用して、AWS SSO が提供するディレクトリ (デフォルト) から AWS Managed Microsoft AD ディレクトリに、またはその反対に切り替えます。

ディレクトリのタイプを変更するには

1. AWS SSO コンソールを開きます。
2. [ダッシュボード] から [ディレクトリの管理] を選択します。
3. [ディレクトリ] ページで、[ディレクトリを変更] を選択します。
4. [ディレクトリを変更] ページで、切り替え先のディレクトリを選択し、[次へ] を選択します。Microsoft AD ディレクトリに切り替える場合は、用意されたメニューから利用できるディレクトリを選択する必要があります。

   > **Important**
   >
   > ディレクトリを変更すると、以前に割り当てられたすべてのユーザーの割り当てが削除されます。ディレクトリが正常に変更された後で手動で再適用する必要があります。

5. [Next: Review] を選択します。
6. 免責事項を読み、続行する準備できたら、CONFIRM と入力します。
7. [Finish] を選択します。

AWS アカウントへの SSO を管理する

AWS Single Sign-On は AWS Organizations と統合されているため、管理者は複数の AWS アカウントを選択して、それらのアカウントのユーザーに対して AWS マネジメントコンソール へのシングルサインオン (SSO) アクセスを管理できます。これらの AWS アカウントは、AWS Organizations のマスターアカウントまたはメンバーアカウントのいずれかになります。マスターアカウントは、組織の作成に使用される AWS アカウントのことです。組織に属する残りのアカウントは、メンバーアカウントと呼ばれます。さまざまなアカウントタイプの詳細については、『AWS Organizations ユーザーガイド』の「AWS Organizations の用語と概念」を参照してください。

AWS SSO コンソールからユーザーにアクセスを割り当てたら、アクセス許可セットを使用して、AWS マネジメントコンソール でユーザーに許可する操作をさらに絞り込むことができます。アクセス権限セットの詳細については、「アクセス権限セット (p. 18)」を参照してください。

ユーザーは以下のシンプルなサインインプロセスに従います。

1. ディレクトリ認証情報を使用してユーザーポータルにサインインする。
2. AWS へのフェデレーションアクセスが許可される AWS マネジメントコンソール アカウントの名前を選択する。
3. 複数のアクセス権限セットが割り当てられている場合は、使用する IAM ロールを選択する。

アクセス許可セットは、AWS SSO で一元的にアクセス許可を定義して、すべての AWS アカウントに適用できるようにする方法です。これらのアクセス許可セットは、各 AWS アカウントに IAM ロールとしてプロビジョニングされます。ユーザーポータルは、ユーザーが特定の AWS アカウントの IAMロールの一時認証情報を取得して、AWS CLI への短期アクセスに使用できるようにします。詳細については、「AWS アカウントへの CLI アクセスで使用する IAM ロールの認証情報を取得する方法 (p. 44)」を参照してください。

AWS Organizations で AWS SSO を使用するには、最初に「AWS SSOの有効化 (p. 3)」を実行して、AWS SSO から AWS 組織内の各アカウントに サービスにリンクされたロール (p. 21) を作成できるようにする必要があります。これらのロールは、特定のアカウントに対して「ユーザーアクセスを割り当てる (p. 17)」の手順を実行するまで作成されません。

また、AWS SSO でのカスタム SAML アプリケーションとしてアカウントを設定することで、組織外の AWS アカウントに接続することもできます。このシナリオでは、SSO アクセスを有効にするために必要な IAM ロールと信頼関係をプロビジョンし管理します。方法の詳細については、カスタム SAML 2.0 アプリケーションを追加して設定する (p. 25) を参照してください。

トピック

シングルサインオンアクセス

接続されたディレクトリ内のユーザーに 一般的な職務機能 に基づいて AWS Organizations 組織のマスターまたはメンバー AWS アカウントにアクセス許可を割り当てることができます。または、特定のセ

キュリティ要件を満たすようにカスタムのアクセス許可を使用することもできます。たとえばデータベース管理者には、開発用アカウントでは Amazon RDS に対する広範なアクセス許可を付与しますが、本番稼働用アカウントではそれらのアクセス許可を制限します。AWS SSO によって、AWS アカウントでは必要なすべてのユーザーアクセス許可が自動的に設定されます。

Note

IAM アカウントのルートユーザーまたは AWSSSOMasterAccountAdministrator IAM ポリシーがアタッチされているユーザーのみが、接続されたディレクトリ内のユーザーにマスター AWS アカウントへのアクセス許可を付与することができます。これらの権限を委任する方法の詳細については、「マスターアカウントでユーザーに SSO アクセスを割り当てる権限を委任する (p. 18)」を参照してください。

ユーザーアクセスを割り当てる

接続先ディレクトリのユーザーとグループに SSO アクセスを割り当て、アクセス権限セットによってそれらのユーザーとグループのアクセスレベルを決定するには、以下の手順を実行します。

Note

アクセス権限の管理をシンプルにするために、個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めします。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動するだけで、新しい組織に必要なアクセス権限がそのユーザーに自動的に付与されます。

ユーザーまたはグループにアクセスを割り当てるには

1. AWS SSO コンソールを開きます。

   Note

   次の手順に進む前に、AWS SSO コンソールで、AWS Managed Microsoft AD ディレクトリがある 米国東部 (バージニア北部) (us-east-1) リージョンを使用していることを確認してください。
2. [AWS アカウント] を選択します。
3. [AWS 組織] タブの AWSアカウントのリストで、アクセスを割り当てるアカウントを選択します。
4. AWS アカウントの詳細ページで、[ユーザーの割り当て] を選択します。
5. [ユーザーまたはグループの選択] ページで、ユーザーまたはグループの名前を入力し、[接続先ディレクトリの検索] を選択します。アクセスを割り当てるすべてのアカウントを選択したら、[次へ: アクセス許可セット] を選択します。複数のユーザーまたはグループを指定するには、検索結果に表示される該当するアカウントを選択します。
6. [アクセス許可セットの選択] ページで、ユーザーまたはグループに適用するアクセス許可セットを一覧から選択します。次に、[完了] を選択します。ニーズを満たすアクセス許可が一覧にない場合は、必要に応じて [新しいアクセス許可セットの作成] を選択できます。詳細な手順については、「アクセス権限セットを作成する (p. 19)」を参照してください。
7. [完了] を選択すると、AWS アカウントの設定プロセスが開始されます。

   Note

   この AWS アカウントに SSO アクセスを初めて割り当てた場合は、このプロセスによってアカウントにサービスリンクされたロールが作成されます。詳細については、「AWS SSO のサービスにリンクされたロールの使用 (p. 39)」を参照してください。

   Important

   ユーザーへの割り当てプロセスが完了するまでに数分かかることがあります。プロセスが正常に完了するまでこのページを開いたままにすることが重要です。

ユーザーアクセスを削除する

接続先ディレクトリ内の特定のユーザーまたはグループから AWS アカウントへの SSO アクセスを削除する必要がある場合は、以下の手順を実行します。

AWS アカウントからユーザーアクセスを削除するには

1. AWS SSO コンソールを開きます。
2. [AWS アカウント] を選択します。
3. 一覧で、アクセスを削除するユーザーまたはグループの AWS アカウントを選択します。
4. AWS アカウントの [詳細] ページの [割り当てられたユーザーとグループ] で、一覧からユーザーまたはグループを見つけます。次に、[アクセスの削除] を選択します。
5. [アクセスの削除] ダイアログボックスで、そのユーザーまたはグループの名前を確認します。次に、[アクセスの削除] を選択します。

マスターアカウントでユーザーに SSO アクセスを割り当てる権限を委任する

AWS SSO コンソールを使用して、マスターアカウントへのシングルサインオンアクセスを割り当てるのは特権的アクションです。デフォルトでは、AWS アカウントのルートユーザー、または AWSSSOMasterAccountAdministrator AWS 管理ポリシーがアタッチされているユーザーのみがマスターアカウントに SSO アクセスを割り当てることができます。AWSSSOMasterAccountAdministrator は、AWS Organizations 組織内のマスターアカウントに SSO アクセスの管理を提供します。

ディレクトリ内のユーザーへの SSO アクセスを管理するためにアクセス許可を委任するには、次の手順を実行します。

ディレクトリ内のユーザーへの SSO アクセスを管理するためのアクセス許可を付与するには

1. マスターアカウントのルートユーザーまたはマスターアカウントに IAM 管理者権限を持つ別の IAM ユーザーとして AWS SSO コンソールにサインインします。
2. アクセス権限セットを作成する (p. 19) の手順に従ってアクセス許可セットを作成します。ステップ 5 c まで進んだら、オプションが表示されたら、[Attach AWS managed policies (管理ポリシーをアタッチ)] を選択します。テーブルに表示される IAM ポリシーのリストで、AWSSSOMasterAccountAdministrator AWS 管理ポリシーを選択します。このポリシーは、将来的にこのアクセス許可セットへのアクセスが割り当てられるすべてのユーザーにアクセス許可を付与します。
3. 作成したアクセス許可セットに適切なユーザーを割り当てるには、手順 ユーザーアクセスを割り当てる (p. 17) に従います。
4. 割り当てられたユーザーに以下を通信: ユーザーポータルにサインインし、[AWS アカウント] アイコンを選択するとき、委任したアクセス許可によって認証されるには、適切な IAM ロール名を選択する必要があります。

アクセス権限セット

アクセス権限セットは、ユーザーおよびグループが持つこの AWS アカウントに対するアクセスのレベルを定義します。アクセス許可セットは AWS SSO に保存され、IAM ロールとして AWS アカウントにプロビジョンされます。複数のアクセス権限セットを 1 人のユーザーに割り当てることができます。複数のアクセス権限セットを持つユーザーは、ユーザーポータルへのサインイン時に 1 つのアクセス権限セットを選択する必要があります(ユーザーにはこれらは IAM ロールとして表示されます)。詳細については、「アクセス権限セット (p. 6)」を参照してください。

アクセス権限セットを作成する

作成したカスタムアクセス許可ポリシー、または IAM に存在する事前定義された AWS 管理ポリシー、またはその両方に基づいてアクセス許可セットを作成するには、以下の手順を実行します。

権限セットを作成するには

1. AWS SSO コンソールを開きます。
2. [AWS アカウント] を選択します。
3. [アクセス許可セット] タブを選択します。
4. [アクセス許可セットの作成] を選択します。
5. [新しいアクセス許可セットの作成] ダイアログボックスで、次のいずれかのオプションから選択し、そのオプションの下に表示される指示に従います。

   - 既存の職務機能ポリシーを使用
     1. [職務ポリシーの選択] で、リストからいずれかのデフォルトの IAM 職務ポリシーを選択します。詳細については、「職務に関する AWS 管理ポリシー」を参照してください。
     2. [作成] を選択します。
   - カスタムアクセス権限セットを作成
     1. [カスタムアクセス許可セットの作成] に、AWS SSO でこのアクセス許可セットを識別する名前を入力します。この名前は、ユーザーポータルにアクセスするすべてのユーザーに IAM ロールとしても表示されます。
     2. (オプション) 説明を入力することもできます。この説明は AWS SSO コンソールにのみ表示され、ユーザーポータルではユーザーに表示されません。
     3. [AWS 管理ポリシーのアタッチ] または [カスタムアクセス許可ポリシーの作成] のいずれかを選択します。または、複数のポリシータイプをこのアクセス権限セットにリンクする必要がある場合は、両方を選択します。
     4. [AWS 管理ポリシーのアタッチ] を選択した場合は、[AWS 管理ポリシーのアタッチ] で、リストから最大 10 個の職務関連またはサービス固有の AWS 管理ポリシーを選択します。
     5. [カスタムアクセス許可ポリシーの作成] を選択した場合は、[カスタムアクセス許可ポリシーの作成] で、優先するアクセス許可のあるポリシードキュメントを貼り付けます。AWS SSO タスクの委任に使用するポリシーの例については、「お客様が管理するポリシーの例 (p. 35)」を参照してください。

        アクセスポリシー言語の詳細については、『IAM ユーザーガイド』の「ポリシーの概要」を参照してください。変更を適用する前にこのポリシーの効果をテストするには、IAM Policy Simulator を使用します。
     6. [作成] を選択します。

アクセス権限セットを削除する

1 つ以上のアクセス権限セットを削除して、組織のいずれの AWS アカウントでも使用不可になるようにするには、以下の手順を実行します。

> Note
>
> このアクセス権限セットが割り当てられていたすべてのユーザーおよびグループは、どの AWS アカウントでそのアクセス権限セットが使用されていたかに関係なく、サインインできなくなります。

AWS アカウントからアクセス権限セットを削除するには

1. AWS SSO コンソールを開きます。

2. [AWS アカウント] を選択します。
3. [アクセス許可セット] タブを選択します。
4. 削除するアクセス許可セットを選択してから、[削除] を選択します。
5. [アクセス許可セットの削除] ダイアログボックスで、[削除] を選択します。

セッション期間の設定

アクセス許可の設定ごとに、セッションの有効期間を指定することができ、時間の長さを制御するユーザー AWS アカウントにサインインすることができます。指定された期間が経過すると、AWS によりユーザーがセッションからログアウトされます。AWS アカウントの場合、AWS SSO ではこの設定を使用して、ユーザーのセッションを生成するために使用する IAM ロールの最大のセッション期間を設定します。特定のアクセス許可セットに指定したセッション期間は、AWS マネジメントコンソール と AWS Command Line Interface (CLI) セッションの両方に適用されます。

新しいアクセス許可セットを作成すると、デフォルトのセッションの長さ 1 時間 (秒単位) で設定されます。最短のセッション期間は 1 時間で、最長 12 時間まで設定できます。

> Important
>
> セキュリティのベストプラクティスとして、ロールを実行するために必要な長さを超えるセッション期間を設定しないことをお勧めします。

権限セットが作成された後、更新して、新しいセッションの有効期間を適用できます。AWS アカウントにアクセス許可セットを再適用すると、IAM ロールの最大セッション期間値が更新されます。特定のアクセス許可セットのセッション期間の長さを変更するには、次の手順を実行します。

セッション期間を設定するには

1. AWS SSO コンソールを開きます。
2. [AWS アカウント] を選択します。
3. [アクセス許可セット] タブを選択します。
4. 新しいセッション期間を新しくするアクセス許可セットの名前を選択します。
5. [セッション期間] の横にある [アクセス許可] タブで、[編集] を選択します。
6. [New session duration (新しいセッション期間)] の横にある [Edit session duration (セッション期間の編集)] ページで、新しいセッションの長さの値を選択し、[続行] を選択します。
7. 新しいセッション期間の値を適用するアクセス許可を適用するリストで AWS アカウントを選択し、[Reapply permission set (権限セットの再適用)] を選択します。

IAM ID プロバイダー

AWS アカウントに SSO アクセスを追加すると、AWS SSO によって各 AWS アカウントに IAM ID プロバイダーが作成されます。IAM ID プロバイダーは、アプリケーションと共に IAM アクセスキーのような長期的なセキュリティ認証情報を配布したり組み込んだりする必要がないので、AWS アカウントの安全性の維持に役立ちます。

IAM ID プロバイダーを修復する

ID プロバイダーが削除または変更された場合、その ID プロバイダーを修復するには、以下の手順を実行します。

AWS アカウントの ID プロバイダーを修復するには

1. AWS SSO コンソールを開きます。

2. [AWS アカウント] を選択します。
3. 一覧で、修復する ID プロバイダーに関連付けられている AWS アカウントを選択します。
4. AWS アカウントの詳細ページの [IAM ID プロバイダー] で、[ID プロバイダーの修復] を選択します。

IAM ID プロバイダーを削除する

AWS SSO から IAM ID プロバイダーを削除するには、以下の手順を実行します。

AWS SSO から IAM ID プロバイダーを削除するには

1. AWS SSO マネジメントコンソールを開きます
2. [AWS アカウント] を選択します。
3. 一覧で、削除する IAM ID プロバイダーに関連付けられている AWS アカウントを選択します。
4. AWS アカウントの [詳細] ページの [IAM ID プロバイダー] で、[ID プロバイダーの削除] を選択します。

サービスにリンクされたロール

サービスにリンクされたロールは、定義済みの IAM アクセス許可であり、AWS SSO によりどのユーザーに AWS 組織内の特定の AWS アカウントへの SSO アクセスを委任して行使できるようにするかが定義されています。このサービスでは、サービスにリンクされたロールを組織内のすべての AWS アカウントでプロビジョンすることで、この機能を有効にします。それにより、AWS SSO などの他の AWS サービスがサービス関連のタスクを実行するためにこれらのロールを活用できるようになります。詳細については、「AWS Organizations およびサービスにリンクされたロール」を参照してください。

AWS SSOの有効化 (p. 3) のプロセスの初回実行中、AWS Organizations サービスによって AWS SSO には、AWS アカウントのいずれにも IAM ロールを作成するためのアクセス許可が付与されます。AWS SSO によってこの時点では、いずれの AWS アカウントにもロールは作成されません。サービスにリンクされたロールが AWS アカウントに作成されるのは、AWS SSO コンソールを使用して SSO アクセスを割り当てるアカウントを指定した後でのみです。詳細については、「AWS アカウントへの SSO を管理する (p. 16)」を参照してください。

各 AWS アカウントに作成されるサービスにリンクされたロールの名前は `AWSServiceRoleForSSO` です。詳細については、「AWS SSO のサービスにリンクされたロールの使用 (p. 39)」を参照してください。

アプリケーションへの SSO を管理する

AWS Single Sign-On を使用すると、クラウドアプリケーションへのシングルサインオン (SSO) アクセスをどのユーザーに許可するかを簡単に制御できます。ユーザーは、ディレクトリ認証情報を使用してユーザーポータルにサインインすると、これらのアプリケーションにワンクリックでアクセスできます。

AWS SSO は、AWS SSO とアプリケーションのサービスプロバイダーとの間の信頼関係を介して、これらのアプリケーションと安全にやり取りします。この信頼を作成するには、AWS SSO コンソールを使用してアプリケーションを追加し、AWS SSO とサービスプロバイダーの両方に該当するメタデータでそのアプリケーションを設定します。

アプリケーションが AWS SSO コンソールに正常に追加されたら、アプリケーションに対するアクセス権限がどのユーザーまたはグループに必要かを管理できます。デフォルトでは、アプリケーションを追加するとき、そのアプリケーションにユーザーは割り当てられません。つまり、AWS SSO コンソールで新しく追加したアプリケーションは、それらのアプリケーションにユーザーを割り当てるまで、アクセス可能になりません。AWS SSO は以下のアプリケーションタイプをサポートしています。

- クラウドアプリケーション
- カスタム Security Assertion Markup Language (SAML 2.0) アプリケーション

組織内の特定の AWSアカウントの AWS マネジメントコンソール へのアクセスを従業員に許可することもできます。方法の詳細については、AWS アカウントへの SSO を管理する (p. 16) を参照してください。

以下のセクションでは、サードパーティー製 SaaS (Software-as-a-Service) アプリケーションや、SAML 2.0 で ID フェデレーションをサポートするカスタムアプリケーションへのユーザーアクセスを設定する方法について説明します。

トピック

クラウドアプリケーション

AWS SSO アプリケーション設定ウィザードを使用して、組み込みの SAML インテグレーションを Salesforce、Box、Office 365 など多くの一般的なクラウドアプリケーションに含めることができます。ウィザードから追加できるアプリケーションの完全なリストについては、「サポートされるアプリケーション (p. 23)」を参照してください。

ほとんどのクラウドアプリケーションには、AWS SSO とアプリケーションのサービスプロバイダーとの間の信頼関係を設定する方法に関する詳細な手順が付属しています。これらの手順は、クラウドアプリ

ケーションの設定中と設定後に、それらのアプリケーションの設定ページに表示されます。アプリケーションが設定されたら、そのアプリケーションを必要とするグループまたはユーザーにアクセス権限を割り当てることができます。

サポートされるアプリケーション

AWS SSO には、一般的に使用されている以下のクラウドアプリケーションに対応するサポート機能が組み込まれています。

> Note
>
> AWS サポートエンジニアは、ビジネスおよびエンタープライズサポートプランを利用し、サードパーティー製のソフトウェアを一部の統合タスクで実行しているお客様をサポートできます。サポートされているプラットフォームおよびアプリケーションの最新のリストについては、『AWS サポートの特徴』ページの「サードパーティー製ソフトウェアサポート」を参照してください。

Adobe Creative Cloud	Dropbox	Lucidchart	UserEcho
Aha	DruvaInSync	MangoApps	UserVoice
AnswerHub	EduBrite	NewRelic	Velpic
AppDynamics	Egnyte	Office 365	VictorOps
Assembla	eLeaP	OpsGenie	WeekDone
Atlassian	Engagedly	PagerDuty	WhosOnLocation
BambooHR	Envoy	Panopta	Workplace by Facebook
BenSelect	Evernote	ProdPad	Workstars
Bitglass	Expensify	PurelyHR	xMatters
BMCRemedyforce	EZOfficeInventory	RingCentral	Zendesk
Bonusly	Freshdesk	Salesforce	Zoho
ボックス	FreshService	Samanage	Zoom
BugSnag	Front	ScaleFT	
CakeHR	G Suite	ScreenSteps	
CiscoMeraki	GitHub	ServiceNow	
CiscoUmbrella	GitLab	Slack	
Citrix ShareFile	GoToMeeting	Sli.do	
Clarizen	Grovo	Smartsheet	
ClickTime	Humanity	SnapEngage	
CloudPassage	IdeaScale	SugarCRM	
Convo	Igloo	SumoLogic	
DataDog	JamaSoftware	SurveyMonkey	
Deputy	JFrog Artifactory	Syncplicity	

Deskpro	Jitbit	Tableau	
DigiCert	join.me	TalentLMS	
Dmarcian	Keeper Security	TargetProcess	
Docebo	Klipfolio	TextMagic	
DocuSign	Kudos	ThousandEyes	
Dome9	LiquidFiles	TitanFile	
Domo	LogMeInRescue	Trello	

クラウドアプリケーションを追加して設定する

AWS SSO とクラウドアプリケーションのサービスプロバイダーとの間で SAML の信頼関係を設定する必要がある場合は、以下の手順を実行します。この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーのメタデータエクスチェンジファイルがあることを確認してください。ただし、このファイルがない場合でも、以下の手順を使用してクラウドアプリケーションを手動で設定できます。

クラウドアプリケーションを追加して設定するには

1. AWS SSO コンソールの左側のナビゲーションバーで [アプリケーション] を選択してから、[新しいアプリケーションの追加] を選択します。
2. [アプリケーションの選択] ダイアログボックスで、追加するアプリケーションをリストから選択した後、[追加] を選択します。
3. [<アプリケーション名> の設定] ページの [詳細] で、アプリケーションの表示名を入力します。たとえば、**`Salesforce`** と指定します。
4. [AWS SSO メタデータ] で、以下の操作を行います。

   a. AWS SSO SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。

   b. [AWS SSO 証明書] の横にある [証明書のダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

   Note

   後で、サービスプロバイダーのウェブサイトからクラウドアプリケーションを設定するときに、これらのファイルが必要になります。そのプロバイダーからの手順に従います。
5. [アプリケーションのプロパティ] の下で、[アプリケーション開始 URL]、[リレーステート]、[セッション期間] の追加のプロパティをオプションで指定できます。詳細については、「アプリケーションのプロパティ (p. 25)」を参照してください。
6. [アプリケーションメタデータ] の下で、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。
7. [変更の保存] を選択して設定を保存します。

カスタム SAML 2.0 アプリケーション

AWS SSO アプリケーション設定ウィザードを使用して、Security Assertion Markup Language (SAML) 2.0 を使用する Security Assertion Markup Language(SAML)2.0 を使用した ID フェデレーションを許可するアプリケーションのサポートを追加できます。コンソールでは、アプリケーションセレクタから [カスタ

ム SAML 2.0 アプリケーション] を選択してこれらのアプリケーションを設定します。カスタム SAML アプリケーションを設定する手順のほとんどは、クラウドアプリケーションを設定する手順と同じです。

ただし、アプリケーション用に SAML アサーションを設定する方法を AWS SSO が正しく認識できるように、カスタム SAML アプリケーションの SAML 属性マッピングを追加する必要もあります。アプリケーションを初めて設定するときに、この SAML 属性マッピングを追加できます。また、AWS SSO コンソールからアクセス可能なアプリケーションの詳細ページでも、SAML 属性マッピングを追加できます。

カスタム SAML 2.0 アプリケーションを追加して設定する

AWS SSO とカスタムアプリケーションのサービスプロバイダーとの間で SAML 信頼関係を設定する必要がある場合は、以下の手順を実行します。この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーの証明書とメタデータエクスチェンジファイルがあることを確認してください。

カスタム SAML アプリケーションを追加および設定するには

1. AWS SSO コンソールの左側のナビゲーションペインで、[アプリケーション] を選択します。次に、[新しいアプリケーションの追加] を選択します。
2. [アプリケーションの選択] ダイアログボックスで、[カスタム SAML 2.0 アプリケーション] をリストから選択した後、[アプリケーションの設定] を選択します。
3. [<カスタムアプリケーション名> の設定] ページの [詳細] で、アプリケーションの表示名を入力します。たとえば、**`MyApp`** と指定します。
4. [AWS SSO メタデータ] で、以下の操作を行います。

   a. AWS SSO SAML メタデータファイルの横にある [ダウンロード] をクリックして、ID プロバイダーのメタデータをダウンロードします。

   b. [AWS SSO 証明書] の横にある [証明書のダウンロード] をクリックして、ID プロバイダーの証明書をダウンロードします。

   Note

   後で、サービスプロバイダーのウェブサイトからカスタムアプリケーションを設定するときに、これらのファイルが必要になります。
5. [アプリケーションのプロパティ] の下で、[アプリケーション開始 URL]、[リレーステート]、[セッション期間] の追加のプロパティをオプションで指定できます。詳細については、「アプリケーションのプロパティ (p. 25)」を参照してください。
6. [アプリケーションメタデータ] の下で、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。
7. [変更の保存] を選択して設定を保存します。

アプリケーションのプロパティ

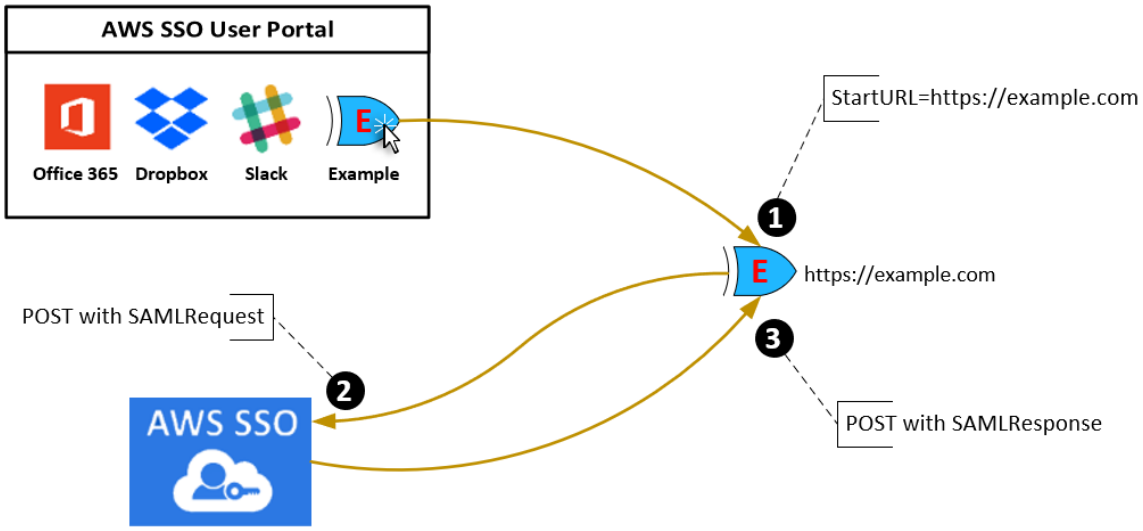
AWS SSO では、以下のアプリケーションのプロパティを追加設定することで、ユーザーエクスペリエンスをカスタマイズできます。

アプリケーション開始 URL

アプリケーション開始 URL を使用して、アプリケーションでフェデレーションプロセスを開始できます。一般的な用途は、サービスプロバイダー (SP) 開始バインディングのみをサポートするアプリケーション用です。

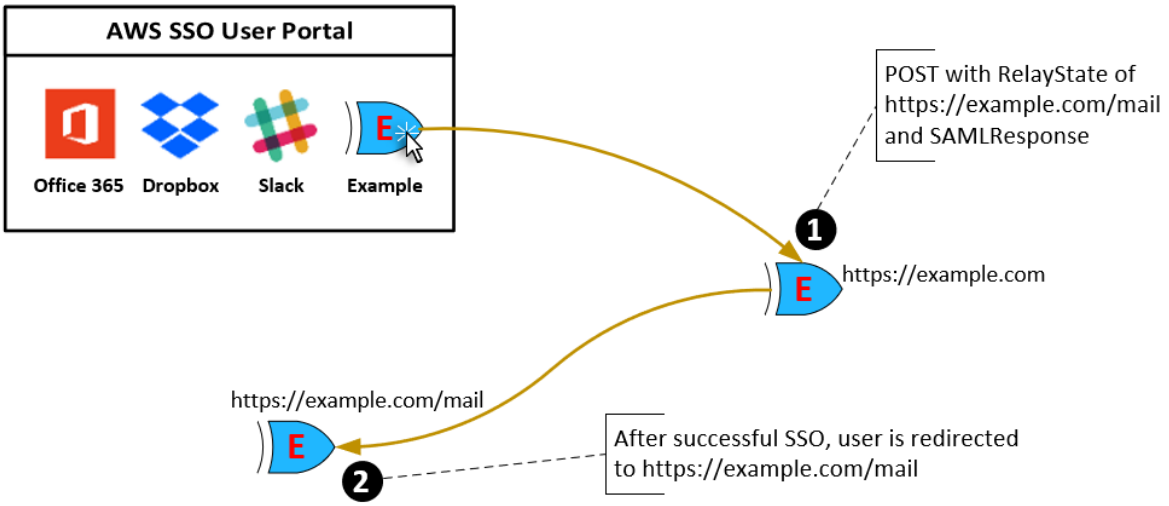
以下のステップと図は、ユーザーがユーザーポータルでアプリケーションを選択したときのアプリケーション開始 URL の認証ワークフローを示しています。

1. ユーザーのブラウザは、アプリケーション開始 URL (この場合は https://example.com) の値を使用して認証リクエストをリダイレクトします。
2. アプリケーションは、`HTML POST` を `SAMLRequest` で AWS SSO に送信します。
3. 次に AWS SSO は、`HTML POST` を `SAMLResponse` でアプリケーションに送り返します。



リレーステート

フェデレーション認証プロセス中に、リレーステートはアプリケーション内でユーザーをリダイレクトします。SAML 2.0 の場合、この値は、変更されずにアプリケーションに渡されます。設定が完了すると、AWS SSO が SAML レスポンスとともにリレーステート値をアプリケーションに送信します。



セッション期間

セッション期間は、アプリケーションのユーザーセッションが有効な時間の長さです。SAML 2.0 では、これは、SAML アサーションの要素、`saml2:SubjectConfirmationData` と `saml2:Conditions` の `NotOnOrAfter` の日付を設定するために使用されます。

セッション期間は次のいずれかの方法でアプリケーションによって解釈されます。

- アプリケーションは、これを使用して SAML アサーションが有効な時間を決定し、ユーザーに許可される時間を決定するときには考慮しません。
- アプリケーションは、これを使用して、ユーザーのセッションに許可される最大時間を決定し、短い期間のユーザーセッションを生成する可能性があります。これは、設定されたセッションの長さよりも短い期間のユーザーセッションのみをアプリケーションがサポートする場合に発生する可能性があります。
- アプリケーションはこれを正確な期間として使用でき、管理者に値の設定を許可しない場合があります。これは、アプリケーションが特定のセッションの長さのみをサポートするときに発生する可能性があります。

セッション期間の使用の詳細については、ご使用のアプリケーションのドキュメントを参照してください。

ユーザーアクセスを割り当てる

クラウドアプリケーションまたはカスタム SAML 2.0 アプリケーションへの SSO アクセスをユーザーに割り当てるには、以下の手順を実行します。

> Note
>
> アクセス権限の管理をシンプルにするためには、個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めしました。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動するだけで、新しい組織に必要なアクセス権限がそのユーザーに自動的に付与されます。

ユーザーまたはグループにアクセスを割り当てるには

1. AWS SSO コンソールを開きます。

   > Note
   >
   > 次の手順に進む前に、AWS SSO コンソールで、AWS Managed Microsoft AD ディレクトリがある 米国東部 (バージニア北部) リージョンを使用していることを確認してください。

2. [Applications (アプリケーション)] を選択します。
3. アプリケーションのリストで、アクセスを割り当てるアプリケーションを選択します。
4. アプリケーションの詳細ページで、[割り当てられたユーザー] タブを選択します。次に、[ユーザーの割り当て] を選択します。
5. [ユーザーの割り当て] ダイアログボックスにユーザー名またはグループ名を入力します。次に、[接続先ディレクトリの検索] を選択します。複数のユーザーまたはグループを指定するには、検索結果に表示される該当するアカウントを選択します。
6. [ユーザーの割り当て] を選択します。

ユーザーアクセスを削除する

クラウドアプリケーションまたはカスタム SAML 2.0 アプリケーションへのユーザーアクセスを削除するには、以下の手順を実行します。

アプリケーションからユーザーアクセスを削除するには

1. AWS SSO コンソールを開きます。

2. [Applications (アプリケーション)] を選択します。
3. アプリケーションのリストで、アクセスを削除するアプリケーションを選択します。
4. アプリケーションの詳細ページで、[割り当てられたユーザー] タブを選択し、削除するユーザーまたはグループを選択してから、[削除] を選択します。
5. [アクセスの削除] ダイアログボックスで、ユーザー名またはグループ名を確認します。次に、[アクセスの削除] を選択します。

アプリケーションの属性を AWS SSO の属性にマップする

一部のサービスプロバイダーでは、ユーザーのサインインに関する追加のデータを渡すためにカスタム SAML アサーションが必要です。その場合は、以下の手順を使用して、アプリケーションのユーザー属性を AWS SSO の対応する属性にマップする方法を指定します。

アプリケーションの属性を AWS SSO の属性にマップするには

1. AWS SSO コンソールを開きます。
2. [Applications (アプリケーション)] を選択します。
3. アプリケーションのリストで、属性をマップするアプリケーションを選択します。
4. アプリケーションの詳細ページで、[属性マッピング] タブを選択します。
5. [新しい属性マッピングの追加] を選択します。
6. 最初のテキストボックスに、アプリケーションの属性を入力します。
7. 2 番目のテキストボックスに、アプリケーションの属性にマップする AWS SSO の属性を入力します。たとえば、アプリケーションの属性 **`Username`** を AWS SSO のユーザー属性 **`email`** にマップできます。AWS SSO で許可されるユーザー属性のリストについては、「属性マッピング (p. 12)」の表を参照してください。
8. この一覧の 3 番目の列で、メニューから属性に該当する形式を選択します。
9. [Save changes] を選択します。

AWS SSO に対する認証とアクセスコントロール

AWS SSO へのアクセスには、リクエストを認証するために AWS によって使用される認証情報が必要です。これらの認証情報には、AWS SSO アプリケーションなどの AWS リソースに対するアクセス許可が必要です。

AWS SSO ユーザーポータルに対する認証は、AWS SSO に接続したディレクトリによって制御されます。ただし、ユーザーポータルからエンドユーザーが利用できる AWS アカウントに対する権限付与は、以下の 2 つの要因によって決まります。

1. AWS SSO コンソールでそれらの AWS アカウントに対するアクセス許可がだれに割り当てられているか。詳細については、「シングルサインオンアクセス (p. 16)」を参照してください。
2. それらの AWS アカウントへの適切なアクセスを許可するために、AWS SSO コンソールでエンドユーザーにどのレベルのアクセス許可が付与されているか。詳細については、「アクセス権限セット (p. 18)」を参照してください。

以下のセクションでは、管理者が AWS SSO コンソールへのアクセスを制御する方法や、AWS SSO コンソールから日常のタスクの管理アクセスを委任する方法について説明します。

認証

AWS には、次のタイプのアイデンティティでアクセスできます。

- AWS アカウントのルートユーザー – AWS アカウントを初めて作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権限を持つシングルサインインアイデンティティで始めます。このアイデンティティは 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のサインインによりアクセスします。強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためだけに ルートユーザー を使用するというベストプラクティスに従います。その後、ルートユーザー認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。
- IAM ユーザー – IAM ユーザーは、特定のカスタム権限 (たとえば、AWS SSO で a directory を作成するアクセス権限) を持つ AWS アカウント内のアイデンティティです。IAM のユーザー名とパスワードを使用して、AWS マネジメントコンソール、AWS ディスカッションフォーラム、AWS Support Center などのセキュリティ保護された AWS ウェブページにサインインできます。

  ユーザー名とパスワードに加えて、各ユーザーのアクセスキーを生成することもできます。いくつかの SDK の 1 つまたは AWS Command Line Interface (CLI) を使ってプログラムで AWS サービスにアクセスするときに、これらのキーを使用できます。SDK と CLI ツールでは、アクセスキーを使用してリクエストが暗号で署名されます。AWS ツールを使用しない場合は、リクエストに自分で署名する必要が

あります。AWS SSO supports では、署名バージョン 4 がサポートされています。これは、インバウンド API リクエストを認証するためのプロトコルです。リクエストの認証の詳細については、『AWS General Reference』の「署名バージョン 4 の署名プロセス」を参照してください。

- IAM ロール – IAM ロールは、特定のアクセス権限を持ち、アカウントで作成できる IAM アイデンティティです。IAM ロールは、AWS で許可/禁止する操作を決めるアクセス権限ポリシーが関連付けられている AWS アイデンティティであるという点で、IAM ユーザーと似ています。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。 IAM ロールと一時的な認証情報は、次の状況で役立ちます。

  - フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブ ID プロバイダーに既存のアイデンティティを使用できます。このようなユーザーはフェデレーティッドユーザーと呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、IAM ユーザーガイドの「フェデレーティッドユーザーとロール」を参照してください。

  - AWS のサービスのアクセス – サービスロールは、サービスがお客様に代わってお客様のアカウントでアクションを実行するために引き受ける IAM ロールです。一部の AWS のサービス環境を設定するときに、サービスが引き受けるロールを定義する必要があります。このサービスロールには、サービスが必要とする AWS のリソースにサービスがアクセスするために必要なすべてのアクセス権限を含める必要があります。サービスロールはサービスによって異なりますが、多くのサービスロールでは、そのサービスの文書化された要件を満たしている限り、アクセス権限を選択することができます。サービスロールは、お客様のアカウント内のみでアクセスを提供します。他のアカウントのサービスへのアクセス権を付与するためにサービスロールを使用することはできません。IAM 内部からロールを作成、修正、削除できます。たとえば、Amazon Redshift がお客様に代わって Amazon S3 バケットにアクセスし、バケットからデータを Amazon Redshift クラスターにロードすることを許可するロールを作成できます。詳細については、IAM ユーザーガイドのAWS サービスにアクセス権限を委任するロールの作成を参照してください。

  - Amazon EC2 で実行中のアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを作成しているアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時認証情報を取得することができます。詳細については、IAM ユーザーガイドの「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用してアクセス権限を付与する」を参照してください。

アクセスコントロール

リクエストを認証するための有効な認証情報があっても、アクセス許可がなければ、AWS SSO リソースの作成やアクセスを行うことはできません。たとえば、AWS SSO 接続先ディレクトリを作成するためのアクセス権限が必要です。

以下のセクションでは、AWS SSO の権限を管理する方法について説明します。最初に概要のセクションを読むことをお勧めします。

- AWS SSO リソースへのアクセス権限の管理の概要 (p. 31)

AWS SSO リソースへのアクセス権限の管理の概要

すべての AWS リソースは AWS アカウントによって所有され、リソースの作成またはアクセスは、アクセス許可のポリシーによって管理されます。アカウント管理者は、IAM ID (ユーザー、グループ、ロール) にアクセス権限ポリシーをアタッチできます。一部のサービス (AWS Lambda など) は、アクセス許可ポリシーをリソースにアタッチすることができます。

> Note
>
> アカウント管理者 (または管理者ユーザー) は、管理者権限を持つユーザーです。詳細については、『IAM ユーザーガイド』の「IAM のベストプラクティス」を参照してください。

アクセス権限を付与する場合、アクセス権限を取得するユーザー、取得するアクセス権限の対象となるリソース、およびそれらのリソースに対して許可される特定のアクションを決定します。

トピック

AWS SSO リソースおよびオペレーション

AWS SSO で、主なリソースはアプリケーションインスタンス、プロファイル、アクセス権限セットです。

リソース所有権について

リソース所有者は、リソースを作成した AWS アカウントです。つまり、リソース所有者は、リソースの作成リクエストを認証するプリンシパルエンティティ (ルートアカウント、IAM ユーザー、または IAM ロール) の AWS アカウントです。以下の例では、このしくみを示しています。

- AWS アカウントのルートユーザーがアプリケーションインスタンスやアクセス許可セットなどの AWS SSO リソースを作成する場合、AWS アカウントはそのリソースの所有者です。
- AWS アカウントに IAM ユーザーを作成し、そのユーザーに AWS SSO リソースを作成するアクセス許可を付与する場合、そのユーザーは AWS SSO リソースを作成できます。ただし、ユーザーが属する AWS アカウントはそのリソースを所有しているとします。
- AWS SSO リソースを作成するためのアクセス許可を持つ AWS アカウントに IAM ロールを作成する場合は、ロールを引き受けることのできるいずれのユーザーも AWS SSO リソースを作成できます。ロールが属する AWS アカウントは AWS SSO リソースを所有しているとします。

リソースへのアクセスの管理

アクセスポリシーでは、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可のポリシーを作成するために使用可能なオプションについて説明します。

Note

このセクションでは、AWS SSO の場合の IAM の使用について説明します。これは、IAM サービスに関する詳細情報を取得できません。完全な IAM ドキュメントについては、IAM ユーザーガイド の「IAM とは」を参照してくださいIAM ポリシー構文の詳細および説明については、『IAM ユーザーガイド』の「AWSIAM ポリシーの参照」を参照してください。

IAM 認証情報にアタッチされているポリシーは、アイデンティティベースのポリシー (IAM ポリシー) と呼ばれます。リソースにアタッチされたポリシーはリソースベースのポリシーと呼ばれます。AWS SSO では、アイデンティティベースのポリシー (IAM ポリシー) のみがサポートされています。

トピック

アイデンティティベースのポリシー (IAM ポリシー)

ポリシーを IAM アイデンティティにアタッチできます。たとえば、次の操作を実行できます。

- アカウントのユーザーまたはグループにアクセス許可ポリシーをアタッチする– アカウント管理者は、特定のユーザーに関連付けられるアクセス許可ポリシーを使用して、そのユーザーに AWS SSO リソース (新しいアプリケーションなど) を追加するためのアクセス許可を付与できます。
- アクセス許可ポリシーをロールにアタッチする (クロスアカウントのアクセス許可を付与する) – アイデンティティベースのアクセス許可ポリシーを IAM ロールにアタッチして、クロスアカウントのアクセス許可を付与することができます。たとえば、アカウント A の管理者は、次のように別の AWS アカウント (たとえば、アカウント B) または AWS サービスにクロスアカウントアクセス許可を付与するロールを作成できます。
  1. アカウント A の管理者は IAM ロールを作成し、そのロールに、アカウント A のリソースに対するアクセス権限を付与するアクセス権限ポリシーをアタッチします。
  2. アカウント A の管理者は、アカウント B をそのロールを引き受けるプリンシパルとして識別するロールに、信頼ポリシーをアタッチします。
  3. アカウント B の管理者は、アカウント B のユーザーにロールを引き受ける権限を委任できるようになります。これにより、アカウント B のユーザーにアカウント A のリソースの作成とアクセスが許可されます。AWS サービスのアクセス許可を付与してロールを引き受けさせたい場合は、信頼ポリシー内のプリンシパルも、AWS サービスのプリンシパルとなることができます。

  IAM を使用したアクセス権限の委任の詳細については、IAM ユーザーガイド の「アクセス管理」を参照してください。

以下のアクセス権限ポリシーは、`List` で始まるすべてのアクションを実行するためのアクセス権限をユーザーに付与します。これらのアクションは、アプリケーションインスタンスやアクセス権限セットなどの AWS SSO リソースに関する情報を表示します。`Resource` 要素内のワイルドカード文字 (*) は、アカウントによって所有されるすべての AWS SSO リソースに対してそれらのアクションが許可されることを示します。

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

AWS SSO でアイデンティティベースのポリシーを使用する方法の詳細については、「AWS SSO でアイデンティティベースのポリシー (IAM ポリシー) を使用する (p. 34)」を参照してください。ユーザー、グループ、ロール、アクセス権限の詳細については、『IAM ユーザーガイド』の「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Amazon S3 などの他のサービスでは、リソースベースのアクセス権限ポリシーもサポートされています。たとえば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス許可を管理できます。AWS SSO はリソースベースのポリシーをサポートしていません。

ポリシー要素の指定 : アクション、効果、リソース、プリンシパル

AWS SSO リソースごとに (「AWS SSO リソースおよびオペレーション (p. 31)」参照)、このサービスは、一連の API オペレーションを定義します。 これらの API オペレーションを実行するためのアクセス許可を付与するために、AWS SSO ではポリシーに一連のアクションを定義できます。API オペレーションを実行する場合には、複数のアクションに対するアクセス権限が必要になることがあります。

以下は、基本的なポリシーの要素です。

- リソース – ポリシーで Amazon Resource Name (ARN) を使用して、ポリシーを適用するリソースを識別します。AWS SSO リソースの場合、IAM ポリシーでは必ずワイルドカード文字 (*) を使用します。詳細については、「AWS SSO リソースおよびオペレーション (p. 31)」を参照してください。
- アクション – アクションのキーワードを使用して、許可または拒否するリソースオペレーションを識別します。たとえば、`sso:DescribePermissionsPolicies` アクセス許可は、AWS SSO `DescribePermissionsPolicies` オペレーションの実行をユーザーに許可します。
- 効果 – ユーザーが特定のアクション—をリクエストする際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に許可していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル – アイデンティティベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、権限 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。AWS SSO では、リソースベースのポリシーはサポートされていません。

IAM ポリシーの構文と説明についての詳細については、『IAM ユーザーガイド』の「AWSIAM ポリシーの参照」を参照してください。

ポリシーでの条件の指定

アクセス権限を付与するとき、アクセスポリシー言語を使用して、ポリシーを有効にするために必要な条件を指定できます。たとえば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、IAM ユーザーガイド の「条件」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。AWS SSO に固有の条件キーはありません。ただし、AWS の条件キーを必要に応じて使用できます。すべての AWS キーのリストについては、『IAM ユーザーガイド』の「使用できるグローバル条件キー」を参照してください。

AWS SSO でアイデンティティベースのポリシー (IAM ポリシー) を使用する

このトピックでは、アカウント管理者が IAM の ID (ユーザー、グループ、ロール) にアタッチできるアクセス権限ポリシーの例を示します。

> Important
>
> 初めに、AWS SSO リソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックを読むことをお勧めします。詳細については、「AWS SSO リソースへのアクセス権限の管理の概要 (p. 31)」を参照してください。

このセクションでは、次のトピックを対象としています。

- AWS SSO コンソールを使用するために必要なアクセス権限 (p. 35)
- での 管理 (事前定義) ポリシー (p. 35)
- お客様が管理するポリシーの例 (p. 35)

以下に示しているのは、アクセス権限ポリシーの例です。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:CreateApplicationInstance",
        "sso:UpdateResponseConfig",
        "sso:UpdateResponseSchemaConfig",
        "sso:UpdateSecurityConfig",
        "sso:UpdateServiceProviderConfig",
        "sso:UpdateApplicationInstanceStatus",
        "sso:UpdateApplicationInstanceDisplay",
        "sso:CreateProfile",
        "sso:SetupTrust"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },

    {
      "Action" : [
        "organizations:xxx",
        "organizations:yyy"
       ],
      "Effect" : "Allow",
      "Resource" : "*"
    },

    {
      "Action" : [
        "ds:AuthorizeApplication"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

ポリシーには以下のものが含まれています。

- 最初のステートメントでは、プロファイルの関連付けを管理する権限をディレクトリ内のユーザーとグループに付与します。すべての AWS SSO リソースを読み取れるアクセス権限も付与します。
- 2 番目のステートメントでは、ディレクトリでユーザーとグループを検索する権限を付与します。プロファイルの関連付けを作成するにはこれが必要になります。

アイデンティティベースのポリシーでアクセス権限を得るプリンシパルを指定していないため、ポリシーでは `Principal` 要素を指定していません。ユーザーにポリシーをアタッチすると、そのユーザーが暗黙のプリンシパルになります。IAM ロールにアクセス権限ポリシーをアタッチすると、ロールの信頼ポリシーで識別されたプリンシパルがアクセス権限を得ることになります。

AWS SSO コンソールを使用するために必要なアクセス権限

AWS SSO コンソールを使用するユーザーには、前述のポリシーに記載されたアクセス権限が必要です。

これらの最小限必要なアクセス権限よりも制限された IAMIAM ポリシーを作成している場合、その IAM ポリシーを使用するユーザーに対してコンソールは意図したとおりには機能しません。

での 管理 (事前定義) ポリシー

AWS は、AWS によって作成され管理されるスタンドアロンの IAM ポリシーが提供する多くの一般的ユースケースに対応します。管理ポリシーは、一般的ユースケースに必要なアクセス権限を付与することで、どの権限が必要なのかをユーザーが調査する必要をなくすることができます。詳細については、『IAM ユーザーガイド』の「AWS 管理ポリシー」を参照してください。

お客様が管理するポリシーの例

このセクションでは、さまざまな AWS SSO アクションのアクセス権限を付与するユーザーポリシー例を示しています。

例

例 1: AWS SSO の設定と有効化をユーザーに許可する

以下のアクセス権限ポリシーでは、AWS SSO コンソールを開いてサービスを有効化できるアクセス権限をユーザーに付与します。そのためには、AWS Organizations のマスターアカウントに付与されるアクセス権限なども必要です。

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

```
         "Effect":"Allow",
         "Action": [
                sso:StartSSO,
                sso:GetSSOStatus
                  ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action": [
                organizations:DescribeAccount,
                organizations:EnableAWSServiceAccess
                  ],
         "Resource":"*"

      }
   ]
}
```

例 2: AWS SSO に接続されたディレクトリの管理をユーザーに許可する

以下のアクセス権限ポリシーでは、接続されたディレクトリを管理するアクセス権限をユーザーに付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:AssociateDirectory,
                sso:DisassociateDirectory,
                sso:ListDirectoryAssociations,
                sso:UpdateDirectoryAssociation
                  ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action": [
                ds:DescribeDirectories
                  ],
         "Resource":"*"
      }
   ]
}
```

例 3: AWS SSO でのアプリケーション管理をユーザーに許可する

以下のアクセス権限ポリシーでは、AWS SSO でアプリケーションインスタンス、プロファイル、証明書を作成および管理できるアクセス権限をユーザーに付与します。

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

```
                sso:ListApplicationTemplates,
                sso:GetApplicationTemplate
                sso:ListApplicationInstances,
                sso:GetApplicationInstance,
                sso:CreateApplicationInstance,
                sso:UpdateApplicationInstanceStatus,
                sso:UpdateApplicationInstanceDisplayData,
                sso:UpdateApplicationInstanceServiceProviderConfiguration,
                sso:UpdateApplicationInstanceResponseConfiguration,
                sso:UpdateApplicationInstanceResponseSchemaConfiguration,
                sso:UpdateApplicationInstanceSecurityConfiguration,
                sso:DeleteApplicationInstance,
                sso:ImportApplicationInstanceServiceProviderMetadata,
                sso:CreateProfile,
                sso:UpdateProfile,
                sso:DeleteProfile,
                sso:GetProfile,
                sso:ListProfiles,
                sso:ListApplicationInstanceCertificates,
                sso:CreateApplicationInstanceCertificate,
                sso:UpdateApplicationInstanceActiveCertificate,
                sso:DeleteApplicationInstanceCertificate
                  ],
         "Resource":"*"
      }
   ]
}
```

例 4: AWS SSO で AWS アカウントのアクセス許可を管理することをユーザーに許可する

以下のアクセス許可ポリシーでは、AWS SSO コンソールで AWS アカウントのアクセス許可セットを作成および管理できるアクセス許可をユーザーに付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationInstances,
                sso:GetApplicationInstance,
                sso:CreateApplicationInstance,
                sso:UpdateApplicationInstanceStatus,
                sso:UpdateApplicationInstanceDisplayData,
                sso:UpdateApplicationInstanceServiceProviderConfiguration,
                sso:UpdateApplicationInstanceResponseConfiguration,
                sso:UpdateApplicationInstanceResponseSchemaConfiguration,
                sso:UpdateApplicationInstanceSecurityConfiguration,
                sso:DeleteApplicationInstance,
                sso:ImportApplicationInstanceServiceProviderMetadata,
                sso:CreateProfile,
                sso:UpdateProfile,
                sso:DeleteProfile,
                sso:GetProfile,
                sso:ListProfiles,
                sso:ListApplicationInstanceCertificates,
                sso:CreateApplicationInstanceCertificate,
                sso:UpdateApplicationInstanceActiveCertificate,
                sso:DeleteApplicationInstanceCertificate,
                sso:CreatePermissionSet,
                sso:GetPermissionSet,
                sso:ListPermissionSets,
```

```
                sso:DeletePermissionSet,
                sso:PutPermissionsPolicy,
                sso:DeletePermissionsPolicy,
                sso:DescribePermissionsPolicies,
                sso:GetTrust,
                sso:CreateTrust,
                sso:UpdateTrust,
                sso:DeleteTrust
                  ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action": [
                organizations:DescribeOrganization
                  ],
         "Resource":"*"
      }
   ]
}
```

例 5: AWS SSO でアプリケーションのアクセスを管理することをユーザーに許可する

以下のアクセス権限ポリシーでは、アプリケーションにアクセスできるメンバーを AWS SSO コンソールで管理できるアクセス権限をユーザーに付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationInstances,
                sso:ListProfileAssociations,
                sso:AssociateProfile,
                sso:DisassociateProfile
                  ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action": [
                ds:DescribeDirectories
                  ],
         "Resource":"*"
      }
   ]
}
```

例 6: AWS SSO とあらかじめ統合されているクラウドアプリケーションの検索をユーザーに許可する

以下のアクセス権限ポリシーでは、AWS SSO とあらかじめ事前されているクラウドアプリケーションを [Add Application] ウィザードを使用して特定できるアクセス権限をユーザーに付与します。

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

```
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationTemplates,
                sso:GetApplicationTemplate
                  ],
         "Resource":"*"
      }
   ]
}
```

例 7: ユーザーに AWS SSO でセキュリティグループの作成と管理を許可する

以下のアクセス許可ポリシーは、AWS SSO コンソールを開いて、AWS SSO がデフォルトで提供するディレクトリでユーザーとグループを追加する許可するアクセス許可をユーザーに付与します。

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

AWS SSO のサービスにリンクされたロールの使用

AWS Single Sign-On は、AWS Identity and Access Management (IAM)サービスにリンクされたロールを使用します。サービスにリンクされたロールは、AWS SSO に直接リンクされた一意のタイプの IAM ロールです。これは AWS SSO によって事前に定義され、そのサービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれます。詳細については、「サービスにリンクされたロール (p. 21)」を参照してください。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、AWS SSO の設定が簡単になります。AWS SSO はこのサービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、AWS SSO のみがそのロールを引き受けます。定義されるアクセス権限には、信頼ポリシーやアクセス権限ポリシーなどがあり、そのアクセス権限ポリシーをその他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携する AWS サービス」を参照の上、[サービスにリンクされたロール] 列が [はい] になっているサービスを検索してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

AWS SSO のサービスにリンクされたロールのアクセス許可

AWS SSO では、サービスにリンクされたロール AWSServiceRoleForSSO を使用して、管理者の代わりに IAM ロール、ポリシー、SAML IdP などの AWS リソースを管理するための AWS SSO アクセス許可を付与します。

AWSServiceRoleForSSO サービスにリンクされたロールは、ロールを引き受ける上で次のサービスを信頼します。

- `AWS SSO`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーでは、AWS SSO はパス「/aws-reserved/sso.amazonaws.com/」にあり、名前のプレフィックスが「AWSReservedSSO_」であるロールで以下のことを実行することができます。

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:ListAttachedRolePolicies`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーでは、AWS SSO は名前のプレフィックスが「AWSSSO_」である SAML プロバイダーで以下のことを実行することができます。

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーでは、AWS SSO はすべての組織で以下のことを実行することができます。

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーでは、AWS SSO はすべての IAM ロール (*) で以下のことを実行することができます。

- `iam:listRoles`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーでは、AWS SSO は「arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO」で以下のことを実行することができます。

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限を設定する必要があります。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールのアクセス許可」を参照してください。

のサービスにリンクされたロールの作成AWS SSO

サービスにリンクされたロールを手動で作成する必要はありません。When a user who is signed in with the AWS organization's master account assigns access to an AWS account for the first time, AWS SSO creates the service-linked role automatically in that AWS account.

> Important
>
> December 7, 2017 以前に AWS SSO サービスを使用していた場合は、サービスにリンクされたロールのサポートが開始された時点で、AWS SSO によって AWSServiceRoleForSSO ロールがアカウントに作成されています。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。

AWS SSO のサービスにリンクされたロールの編集

AWS SSO では、AWSServiceRoleForSSO サービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールの編集」を参照してください。

AWS SSO のサービスにリンクされたロールの削除

AWSServiceRoleForSSO ロールを手動で作成する必要はありません。When an AWS account is removed from an AWS organization, AWS SSO automatically cleans up the resources and deletes the service-linked role from that AWS account.

サービスにリンクされたロールは、IAM コンソール、IAM CLI、または IAM API を使用して手動で削除することもできます。そのためにはまず、サービスにリンクされたロールのリソースをクリーンアップする必要があります。その後で、手動で削除できます。

> Note
>
> リソースを削除する際に、AWS SSO サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

AWSServiceRoleForSSO で使用されている AWS SSO リソースを削除するには

1. AWS アカウントにアクセスするすべてのユーザーとグループについては ユーザーアクセスを削除する (p. 18)。
2. AWS アカウントに関連付けられている アクセス権限セットを削除する (p. 19)。
3. IAM ID プロバイダーを削除する (p. 21) は、AWS SSO と AWS アカウント間の信頼関係を削除します。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

IAM コンソール、IAM CLI、または IAM API を使用して、AWSServiceRoleForSSO サービスにリンクされたロールを削除します。詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールの削除」を参照してください。

ユーザーポータルの使用

ユーザーポータルでは、すべての AWS アカウントとよく使用されるクラウドアプリケーション (Office 365、Concur、Salesforce など) へのシングルサインオンアクセスが可能です。ポータル内から、AWS アカウントまたはアプリケーションのアイコンを選択するだけで、複数のアプリケーションをすばやく起動できます。ポータル内にアイコンがあるということは、お客様の管理者またはヘルプデスク担当者によって AWS アカウントまたはアプリケーションへのアクセスが許可されているということです。つまり、ポータルからこれらのアカウントまたはアプリケーションには、サインインのプロンプトが表示されることなくアクセスできるということです。

以下の状況では、管理者またはヘルプデスク担当者に連絡して追加のアクセスをリクエストしてください。

- アクセスする必要のある AWS アカウントまたはアプリケーションが表示されていない。
- 特定のアカウントまたはアプリケーションへのアクセスが想定したものでない。

トピック

ポータルを使用するためのヒント

日常的に使用しているビジネスツールやアプリケーションと同様に、ユーザーポータルは想定どおりに機能しないことがあります。その場合は、以下のヒントを試してください。

- 場合によっては、サインアウトしてユーザーポータルにサインインしなおす必要があります。この手順は、管理者から最近割り当てられた新しいアプリケーションにアクセスするために必要になります。ただし、すべての新しいアプリケーションは 1 時間ごとに更新されるため、この手順は必須ではありません。
- ユーザーポータルにサインインすると、ポータルに表示されているアプリケーションのアイコンを選択して、そのアプリケーションを開くことができます。アプリケーションを使用し終わったら、アプリケーションを閉じるか、ユーザーポータルからサインアウトします。アプリケーションを閉じると、そのアプリケーションからのみサインアウトされます。ユーザーポータルから開いた他のアプリケーションは開いたままで実行されています。
- 別のユーザーとしてサインインするには、最初にユーザーポータルからサインアウトする必要があります。ポータルからログアウトすると、ブラウザセッションから認証情報が完全に削除されます。

AWS SSO への参加招待を受け入れる方法

ユーザーポータルに初めてサインインする場合は、E メールでアカウントを有効にする方法に関する指示事項を確認します。

アカウントをアクティブ化するには

1. 会社から送られてきたメールに応じて次のいずれかの方法を選択し、ユーザーポータルを使用し始めることができるように、アカウントをアクティブ化します。

   a. AWS Single Sign-On に参加するための招待 という件名の E メールを受信している場合は、開いて [招待を承諾する] を選択すると、[シングルサインオン] ページに移動します。ここでは、ポータルにサインインするたびに使用するパスワードを指定します。パスワードを指定したら、[ユーザーの更新] を選択します。

   b. 貴社の IT サポートまたは IT 管理者から E メールを送信された場合は、アカウントをアクティブ化するために伝えられた指示事項に従います。

2. 新しいパスワードを指定してアカウントを有効にすると、ユーザーポータルにより自動的にサインインされます。されない場合は、次のステップで説明されている指示事項に従って、手動でユーザーポータルにサインインできます。

ユーザーポータルへのサインイン方法

この時点で、管理者またはヘルプデスク担当者から、ユーザーポータルへの特定のサインイン URL が提供されている必要があります。この URL があれば、以下の手順を実行してポータルにサインインできます。

ユーザー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、提供されたサインイン URL を貼り付けます。次に、Enter キーを押します。ポータルへのこのリンクをブックマークに追加して後ですばやくアクセスできるようにすることをお勧めします。
2. 会社の標準のユーザー名とパスワードを使用してサインインします。
3. サインインしたら、ポータルに表示される AWS アカウントとアプリケーションにアクセスできます。そのためには、アイコンを選択するだけです。

ユーザーポータルからのサインアウト方法

ポータルからログアウトすると、認証情報がブラウザセッションから完全に削除されます。

> Note
>
> 別のユーザーとしてサインインする場合は、最初にユーザーポータルからサインアウトする必要があります。

ユーザーポータルからサインアウトするには

- ユーザーポータルで、ポータルの右上隅にある [サインアウト] を選択します。

AWS アカウントまたはアプリケーションの検索方法

アプリケーションまたは AWS アカウントのリストが大きすぎて必要なものが見つからない場合は、[検索] ボックスを使用できます。

ユーザーポータルで AWS アカウントまたはアプリケーションを検索するには

1. ポータルにサインインしている状態で、[検索] ボックスを選択します。

2. アプリケーションの名前を入力します。次に、Enter キーを押します。

パスワードのリセット方法

貴社の方針に応じて、パスワードをリセットする必要がある場合があります。

パスワードをリセットするには

1. ブラウザを開き、ユーザーポータルのサインインページに移動します。
2. [サインイン] ボタンの下で、[パスワードを忘れた場合] を選択します。
3. [ユーザー名] を入力し、提供されたイメージの文字を入力してロボットではないことを確認します。続いて、[パスワードの回復] を選択します。これで、件名 [AWS Directory Service Reset Password Request (AWS Directory Service パスワードリセットリクエスト)] の E メールが送信されます。
4. E メールを受け取ったら、[パスワードのリセット] を選択します。
5. [シングルサインオン] ページで、ポータルの新しいパスワードを指定する必要があります。パスワードを指定して確認したら、[パスワードのリセット] を選択します。

AWS アカウントへの CLI アクセスで使用する IAM ロールの認証情報を取得する方法

AWS CLI を使用して AWS アカウントのリソースに短期間アクセスするための一時セキュリティ認証情報が必要な場合は、ユーザーポータルで以下の手順を実行します。ユーザーポータルを使用すると、簡単に AWS アカウントを選択し、特定のIAM ロールの一時認証情報を簡単に取得できます。その後、すべての必要な認証情報を含む CLI 構文をコピーし、AWS CLI コマンドプロンプトに貼り付けることができます。

デフォルトでは、ユーザーポータルから取得した認証情報は 1 時間有効です。この値は、最大 12 時間に変更することができます。以下の手順を完了したら、一時認証情報が期限切れになるまで、管理者からアクセスを許可された AWS CLI コマンドを実行できます。

> **Note**
>
> 以下の手順を開始する前に、最初に AWS CLI をインストールする必要があります。手順については、「AWS コマンドラインインターフェイスのインストール」を参照してください。

AWS アカウントへの CLI アクセスで使用する IAM ロールの一時認証情報を取得するには

1. ポータルにサインインしている状態で、[AWS アカウント] アイコンを選択してアカウントのリストを展開します。
2. アクセス認証情報を取得する AWS アカウントを選択します。次に、IAM のロール名 (Administrator など) の横にある [Command line or programmatic access] (コマンドラインまたはプログラムによるアクセス) を選択します。
3. [認証情報の取得] ダイアログボックスで、CLI コマンドプロンプトを使用するオペレーティングシステムに応じて、[MacOS and Linux] (MacOS と Linux) または [Windows] を選択します。
4. 一時認証情報の使用方法に応じて、以下の 1 つ以上のオプションを選択します。

   - 選択した AWS アカウントで AWS CLI からコマンドを実行する必要がある場合は、[オプション 1: AWS 環境変数を設定する] で、コマンドを一時停止します。次に、[コピー] を選択します。コマンドを CLI ターミナルウィンドウに貼り付け、Enter キーを押して、必要な環境変数を設定します。
   - 同じ AWS アカウントで複数のコマンドプロンプトからコマンドを実行する必要がある場合は、[オプション 2: AWS 認証情報ファイルにプロファイルを追加する] で、コマンドを一時停止します。次に、[コピー] を選択します。コマンドを AWS 認証情報ファイルに貼り付けて、新しい名前のプ

ロファイルを設定します。詳細については、『AWS CLI ユーザーガイド』の「設定と認証情報ファイル」を参照してください。この方法で認証情報ファイルを変更すると、AWS CLI コマンドの `--profile` オプションでこの認証情報を使用できるようになります。このことは、この同じ認証情報ファイルを使用するすべてのコマンドプロンプトにも当てはまります。

- AWS サービスクライアントから AWS リソースにアクセスする必要がある場合は、[オプション 3: AWS サービスクライアントで個々の値を使用する] で、使用する必要のあるコマンドの横にある [コピー] を選択します。詳細については、『AWS CLI ユーザーガイド』の「AWS STS による一時認証情報の取得」または「アマゾン ウェブ サービスのツール」を参照してください。

5. 認証情報が期限切れになるまで、AWS アカウントで必要に応じて AWS CLI を使用できます。

AWS SSO を使用した AWS CloudTrail API 呼び出しの口グ記録

AWS SSO は、AWS SSO のユーザーやロール、または AWS のサービスによって実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。証跡を作成すると、Amazon S3 バケット、Amazon CloudWatch Logs および Amazon CloudWatch Events への CloudTrail イベントの継続的デリバリーが可能になります。CloudTrail によって収集された情報を使用して、リクエストの作成元の IP アドレス、リクエストの実行者、リクエストの実行日時などの詳細を調べて、AWS SSO に対してどのようなリクエストが行われたかを判断できます。

CloudTrail の詳細については、「AWS CloudTrail User Guide」を参照してください。

CloudTrail 内の AWS SSO 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。AWS SSO でアクティビティが発生すると、そのアクティビティは [Event history] の AWS の他のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

のイベントなど、 アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで作成した証跡がすべての AWS リージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、より詳細な分析と AWS ログで収集されたデータに基づいた行動のためにその他の CloudTrail サービスを設定できます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail でサポートされるサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 「複数のリージョンから CloudTrail ログファイルを受け取る」と「複数のアカウントから CloudTrail ログファイルを受け取る」

AWS アカウントで CloudTrail ログ記録を有効にすると、AWS SSO アクションに対する API コールはログファイルに記録されます。AWS SSO レコードは、AWS の他のサービスのレコードと一緒にログファイルに書き込まれます。CloudTrail は、期間とファイルサイズに基づいて新規ファイルの作成と書き込みのタイミングを決定します。

以下のアクションがサポートされています。

- `AssociateDirectory`
- `AssociateProfile`
- `CreateApplicationInstance`
- `CreateApplicationInstanceCertificate`
- `CreatePermissionSet`
- `CreateProfile`
- `DeleteApplicationInstance`

- DeleteApplicationInstanceCertificate
- DeletePermissionsPolicy
- DeletePermissionSet
- DeleteProfile
- DescribePermissionsPolicies
- DisassociateDirectory
- DisassociateProfile
- GetApplicationInstance
- GetApplicationTemplate
- GetPermissionSet
- GetSSOStatus
- ImportApplicationInstanceServiceProviderMetadata
- ListApplicationInstances
- ListApplicationInstanceCertificates
- ListApplicationTemplates
- ListDirectoryAssociations
- ListPermissionSets
- ListProfileAssociations
- ListProfiles
- PutPermissionsPolicy
- StartSSO
- UpdateApplicationInstanceActiveCertificate
- UpdateApplicationInstanceDisplayData
- UpdateApplicationInstanceServiceProviderConfiguration
- UpdateApplicationInstanceStatus
- UpdateApplicationInstanceResponseConfiguration
- UpdateApplicationInstanceResponseSchemaConfiguration
- UpdateApplicationInstanceSecurityConfiguration
- UpdateDirectoryAssociation
- UpdateProfile

各ログエントリには、誰がリクエストを生成したかに関する情報が含まれます。ログの ID 情報は、リクエストが AWS アカウントのルートユーザーによって行われたか、あるいは IAM ユーザー認証情報を使用して行われたかを確認するのに役立ちます。また、リクエストがロールまたはフェデレーティッドユーザーの一時的なセキュリティ認証情報で行われたか、あるいは別の AWS サービスによって行われたかを知ることもできます。詳細については、「CloudTrail userIdentity 要素」を参照してください。

証跡を作成し、ログファイルを Amazon S3 バケットに必要な期間保存できます。また、Amazon S3 ライフサイクルのルールを定義して、自動的にログファイルをアーカイブまたは削除することもできます。デフォルトでは Amazon S3 のサーバー側の暗号化 (SSE) を使用して、ログファイルが暗号化されます。

ログファイルの配信通知を受けるためには、新しいログファイルの配信時に Amazon SNS 通知が発行されるように CloudTrail を設定します。詳細については、「CloudTrail の Amazon SNS 通知の設定」を参照してください。

また、複数 AWS リージョンと複数の AWS アカウントからの AWS SSO ログファイルを、1 つの Amazon S3 バケットに集約することもできます。詳細は、「CloudTrailログファイルを複数のリージョンから受け取る」と「複数のアカウントから CloudTrail ログファイルを受け取る」を参照してください。

AWS SSO ログファイルエントリの概要

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

以下は、AWS SSO コンソールで発生した管理者 (samadams@example.com) の CloudTrail ログエントリの例です。


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```


以下は、AWS SSO ユーザーポータルで発生したエンドユーザー (bobsmith@example.com) のアクションの CloudTrail ログエントリの例です。


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
```

```
        "eventName":"https://portal.sso.us-east-1.amazonaws.com/instance/appinstances",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"203.0.113.0",
        "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
        "requestParameters":null,
        "responseElements":null,
        "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
        "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
        "eventType":"AwsApiCall",
        "recipientAccountId":"08966example"
      }
   ]
}
```

AWS SSO での制限

以下の表では、AWS SSO での制限について説明します。変更できる制限の詳細については、「AWS サービス制限」を参照してください。

アプリケーションの制限

リソース	デフォルトの制限
サービスプロバイダーの SAML 証明書のファイルサイズ (PEM 形式)	2 KB

AWS アカウントの制限

リソース	デフォルトの制限
AWS SSO のアクセス権限セットの最大数	50
AWS アカウントあたりに許可されるアクセス権限セット数	20
アクセス権限セットあたりの AWS 管理ポリシーの参照数	10
アクセス権限セットあたりのインラインポリシーの数	1
アクセス権限セットあたりのインラインポリシーの最大サイズ	10,000 バイト
AWS アカウントで一度に修復できる IAM ロールの数 *	1
一度に実現できるディレクトリの数	1

* アクセス許可セットは、AWS アカウントに IAM ロールとしてプロビジョニングされます。詳細については、「アクセス権限セット (p. 6)」を参照してください。

接続ディレクトリの制限

リソース	デフォルトの制限
割り当て可能な一意の Active Directory グループの数 *	50

リソース	デフォルトの制限
一度に実現できる接続ディレクトリの数	1

* Active Directory 内のユーザーは複数のディレクトリグループに所属できます。ただし AWS SSO 内では、アプリケーションの使用に関して割り当て可能な Active Directory グループ数は最大 50 です。

AWS SSO ディレクトリの制限

リソース	デフォルトの制限
AWS SSO でサポートされるユーザーの最大数	500
AWS SSO でサポートされるグループの最大数	100

AWS SSO の問題のトラブルシューティング

以下は、AWS SSO コンソールを設定または使用するときに発生する可能性のある問題のトラブルシューティングに役立ちます。

クラウドアプリケーションを正しく設定できません

AWS SSO にあらかじめ統合されているクラウドアプリケーションの各サービスプロバイダーでは詳細な手順書を用意しています。手順書は、AWS SSO コンソール上で該当アプリケーションの [Configuration] タブから確認できます。

問題が、サービスプロバイダーのアプリケーションと AWS SSO の間の信頼関係の設定に関係している場合は、必ず手順書でトラブルシューティングのステップを確認してください。

SAML アサーションのどのデータがサービスプロバイダーに提供されるのか分かりません

ユーザーポータルで次のステップを実行すると、現在サインインしているユーザーに関してアプリケーションのサービスプロバイダーに送信される SAML アサーションのデータを確認できます。この手順では、プロバイダーに送信する前にその内容がブラウザウィンドウに表示されます。

1. ポータルにサインインしている状態で、Shift キーを押しながらアプリケーションを選択します。
2. [You are now in administrator mode] ページの情報を調べます。
3. 情報に問題がなければ、[Send to]<application> を選択してアサーションをサービスプロバイダーに送信し、レスポンスの結果を確認できます。

ドキュメント履歴

以下の表は、AWS Single Sign-On の今回のリリースの内容をまとめたものです。

- ドキュメントの最終更新日: 2018 年 10 月 30 日

update-history-change	update-history-description	update-history-date
AWS アカウントでのセッションの有効期間のサポート	AWS アカウントのセッションの有効期間を設定する方法に関するコンテンツを追加しました。	October 30, 2018
AWS SSO ディレクトリを使用する新しいオプション	AWS SSO ディレクトリを選択するか、既存の AD ディレクトリに接続するためのコンテンツを追加しました。	October 17, 2018
アプリケーションでのリレーステートとセッションの有効期間のサポート	クラウドアプリケーションのリレーステートとセッションの有効期間に関するコンテンツを追加しました。	October 10, 2018
新しいクラウドアプリケーションの追加サポート	アプリケーションカタログに 4me、BambooHR、Bonusly、Citrix ShareFile、ClickTime、Convo、Deputy、Deskpro、Dome9、DruvaInSync、Egnyte および UserEcho を追加しました。	August 3, 2018
マスターアカウントへの SSO アクセスのサポート	マスターアカウントでユーザーに SSO アクセスを委任する方法に関するコンテンツを追加しました。	July 9, 2018
新しいクラウドアプリケーションのサポート	DocuSign、Keeper Security、SugarCRM をアプリケーションカタログに追加しました。	March 16, 2018
CLI アクセスの一時認証情報の取得	AWS CLI コマンドを実行するための一時認証情報を取得する方法に関する情報を追加しました。	February 22, 2018
新規ガイド	これは AWS SSO ユーザーガイドの最初のリリースです。	December 7, 2017

AWS の用語集

最新の AWS の用語については、『AWS General Reference』の「AWS の用語集」を参照してください。