ATLASSIAN

クラウドの ID と アクセス管理に関する アトラシアンのガイド

目次

組織では大小さまざまなデジタル変革が起こり、組織の機能を拡張したり、新たな機会を創出したりしています。

この新しいデジタル環境を最大限活用するコツは、組織内のコラボレーションの円滑化です。的確な意思決定を行うためには、適切な人が適切な情報に、迅速にアクセスできるようにする必要があります。計画を共有し、重要な課題をエスカレーションし、意思決定をドキュメント化して保存し、簡単に見つけられるようにしなければなりません。

こうしたアクティビティ (および生成されるデータ) はすべてクラウドで行われるようになりつつあります。

オンプレミスのソフトウェアはファイアウォールによって保護され、組織ではほんのいくつかの集中管理型アプリケーションのみが使用されていた今までとは異なり、個々のチームが特定のビジネス課題を解決するクラウド ツールを導入するようになりました。また、API を通じて複数のアプリケーションを統合したり、機密性の高い価値のあるデータを複数のソフトウェア ベンダーと共有したりすることも増えました。

これにより、現代における IT 最大の課題が生まれました。日々増加するアプリケーションとエンドポイントでの組織データの保護です。

組織の機密情報をクラウドに移行すると、クラウド アプリとサービスにアクセスできるユーザーを決定するにあたって、今までとは異なる、より強力な制御が必要となります。IT ガバナンスのこの局面、つまりクラウド ID とアクセス管理 (IAM) は、デジタル変革における最大の課題を乗り越えるためのキーとなります。

このガイドでは、企業がクラウドへ移行する際に発生する、以下のような IAM の重要な変化を説明します。

- **クラウド IAM へのアプローチが、どのようにオンプレミス ソリューションやツールからプロセスへと再概念化されたのか**
- **自動化、生産性、セキュリティにおけるクラウド IAM の利点**
- **クラウド IAM の利用を開始する方法と変化の計画を作成する方法**
- **Atlassian クラウド製品とクラウド IAM アプローチを連携させる方法**

クラウド ID とアクセス管理の入門ガイド

クラウド ID とアクセス管理の入門ガイド

クラウド ID とアクセス管理とは

クラウド IAM には、ユーザー ID を管理し、オンプレミスおよびクラウド のアプリケーション両方へのアクセスを制御するためのツールとプロセスが含まれます。最適なクラウド IAM アプローチは、ユーザー ID を管理するための一元的な場所を作成し、それを異なる環境で機能させることです。OS プラットフォーム、認証プロトコル、ロケーション、ベンダーにかかわらず、すべての IT リソースにアクセスできるようにする必要があります。

クラウド ID 管理とオンプレミスの ID 管理の違い

クラウド ID 管理は 20 年前に実現された従来のソリューションを再概念化したものです。当時、ほとんどの IT リソースはオンプレミスであり、ファイアウォールの内側で管理され、1 社のベンダーのシステムとアプリケーションが使用されていました (ほとんどの場合、そのベンダーは Microsoft でした)。これらのシステムは、ほんの数件のアプリケーションを管理するために設計され、数百ものアプリを扱う現在の IT ニーズに応えることができません。

反対に、現在のクラウド ID 管理システムの状況は次のとおりです。

- 異なる種類のシステムを統合する SaaS 製品として提供される。
- 複数の種類のデバイスからアクセスできる。
- ID とアクセス ポリシーを統一できる。
- 変わり続けるアクセス要件に対応できるよう設計されている。

クラウド環境でのユーザー ID の管理は複雑です。新しいクラウド IAM ツールを導入し、従来のオンプレミス システムからの移行パスをマッピングするだけでは済みません。新しいツールのみならず、新しいポリシーを作成し、既存のポリシーをアップデートし、何よりも組織の今後の方向性を見極め、将来的な拡張をサポートできるよう設定する必要があります。

クラウド ID とアクセス管理の利点

- **異なる環境の一元管理**
  クラウドでの ID 管理は、継ぎはぎのようなオンプレミス ID システムおよびツールに取って代わるもので、IT 組織内のリソースが何であれ、シームレスに連携できます。macOS、Linux、AWS、Web アプリケーション、WiFi など、組織は最適だと判断したリソースを使用することができます。
- **ユーザー プロビジョニングを自動化してセキュリティ ポリシーを適用する**
  最新の IAM ソリューションを使用すると、オンプレミス環境とクラウド環境の両方でユーザー アクセス管理を一元化できます。プロビジョニングを自動化して研修プログラムを合理化したり、従業員や請負業者が会社を辞めるときには直ちにアクセスを遮断してセキュリティ ポリシーを維持したりすることができます。
- **コンテキスト アクセス管理を適用する**
  ロケーション、ネットワーク、デバイス制限、リクエストの種類、タイミングなど、ユーザーに割り当てられた役割を上回るリスク要因に基づき、アクセスの動的な意思決定を自動化します。
- **エンドユーザーと IT 部門双方にとっての生産性向上**
  シングル サインオン (SSO) プロバイダー (クラウド IAM アプローチにおける主要なプレイヤーです。これについては後ほど触れます) と連携すると、ユーザーは 1 つのダッシュボードから簡単にすべての企業アプリを見つけ、ログインすることができます。

クラウド IAM の利用を開始する

クラウドに移行し、ID とアクセス管理を一元化する準備ができていたとしても、ID プロバイダー (IdP) ソリューションの選択は、通常のソフトウェア購入ほど素早く決められるものではありません。検索を開始する場合、考慮すべき重要な要因がいくつか存在します。

1. **将来を見据える。**
   成長と拡張という観点から組織が向かう方向性を理解すれば、
   新しい IAM システムは組織の目標をサポートすることができます。

2. **開始する領域について検討する。**
   調査すべきベンダーの優先順位付けに役立ちます。ほとんどの場合、クラウドへの移行を検討している IT 組織は次の 3 つのカテゴリーのいずれかに当てはまります。

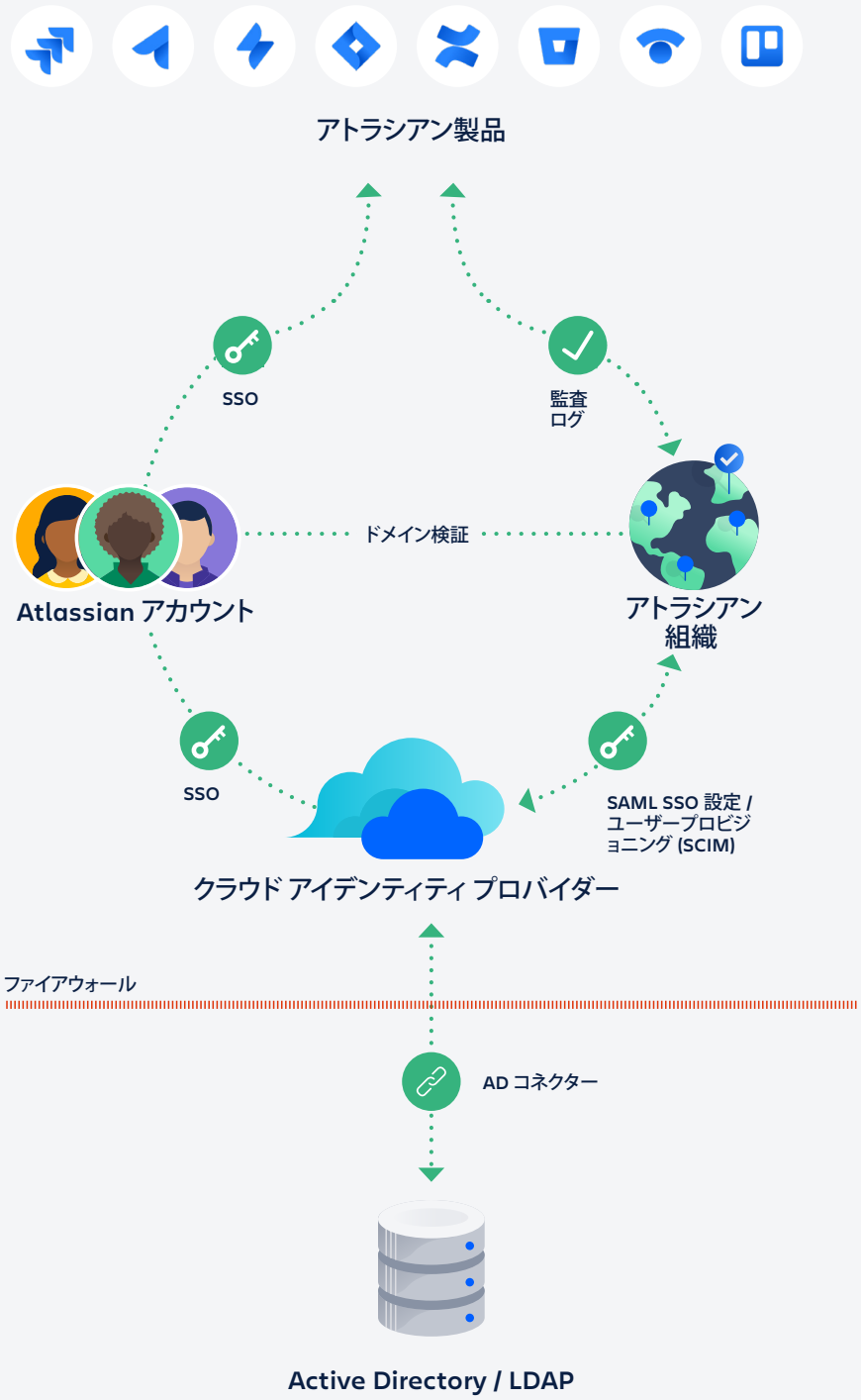
   - 現在オンプレミスで LDAP ディレクトリ システムを使用しており、クラウドに移行したいと考えている。
   - 既存の Microsoft Active Directory (AD) インストールを使用しており、クラウドに移行したいと考えている。理由は異なる環境の管理であることが多い。
   - 現在はユーザー ID 管理のためにユーザー ディレクトリを使用していない。

3. **現在の IT 環境を確認する。**
   インフラストラクチャにおけるすべてのプロトコル、プラットフォーム、ネットワークにシステムとの相互運用性があることを確認する必要があります。

4. **すべてのベンダー アプリと SaaS ツールを確認し、ビジネスにとって重要なものを決定する。**
   優先順位付けされた統合計画の作成を開始するときは特に、アクセス管理する必要があるすべてのアプリケーションを把握します。

> **よいお知らせ**
> 要件と優先順位が明確化されている場合、IAM ベンダー ツールの組み合わせが容易に進む可能性は高くなります。また、IAM プロセスはクラウド化されるため、セキュリティまたはパッチ管理のための新しいハードウェアあるいは内部リソースに大規模な長期投資を行う必要はなくなります。それはクラウドベンダーによって行われるからです。

クラウド IAM 環境を理解する



クラウド ID プロバイダー (IdP) を選択したら、そのプロバイダーがオンプレミスおよびクラウド アプリケーションの全体的な環境にどう適合するのかを理解することが重要です。クラウド ID 環境について考慮すべき要素の一部を次に示します。

- **プロファイル マスターを特定する**
  まず、ユーザーとグループにとって信頼できる唯一の情報源となるアプリケーション、プロファイル マスターを特定します。方法の 1 つは、ユーザーとグループのプロファイル マスターを直接、クラウド IdP に作成すること、もう 1 つの選択肢は、ユーザーとグループのマスターを Workday などの人事情報システムで保持することです。
  - **クラウド IdP をオンプレミス ディレクトリと接続する**
    この図では、オンプレミスの Active Directory または LDAP データベースをプロファイル マスター向けの情報源として定義しました。この場合、クラウド ベースの IdP を、ネットワークでホストされているディレクトリに接続する必要があります。すべての主要なクラウド IdP では、企業ネットワーク内で動作し、クラウド IdP と、信頼できる唯一の情報源である Active Directory または LDAP サーバーのユーザーおよびグループ間の同期を行うエージェントあるいはコネクターを提供しています。オンプレミス システムに Active Directory または LDAP が存在する場合、引き続き ID 管理とオンプレミス アプリケーションへのアクセスにそれを使用できます。
  - **クラウド IdP 経由でクラウド アプリを認証する**
    クラウド内のアプリケーションをクラウド IdP に接続すると、ユーザーは SAML シングル インオン (SSO) などのプロトコルを介して、公開のインターネットからこれらのアプリケーションにアクセスして認証できます。

- **クラウド IdP と SSO 経由で Atlassian アプリケーションへのユーザー アクセスを管理する**
  クラウド IdP は Atlassian アカウントを使用し、SAML SSO を介して Atlassian 組織と IdP 間の SSO 認証を提供することもできます。ユーザーが Atlassian アカウント経由で Jira Software Cloud などの Atlassian アプリケーションにアクセスすると、ログインのために IdP にリダイレクトされます。
- **クラウド IdP を通じて新しい Atlassian ユーザーをプロビジョニングする**
  また、(元々ローカルのオンプレミス Active Directory から同期された) クラウド IdP に存在するユーザーとグループの Atlassian 組織へのプロビジョニングも可能です。これらのグループは ID を同期したまま Atlassian 組織にリンクされたアプリケーションに渡されます。

Atlassian Cloud IAM 戦略を実装する

Atlassian Cloud IAM 戦略を実装する

Atlassian は独自のデジタル変革を経験しました。そのため、組織が移行する際に直面するであろう課題をすべて理解しています。

Atlassian は自社とお客様のために、ベスト プラクティスのフレームワークを設定しました。拡大する組織全体でコラボレーションする際に IT チームが直面する課題を乗り越えるとともに、適切なセキュリティ プロトコルを維持するためのフレームワークです。

このフレームワークでは次を実現するためのガイドラインを設定しました。

一元管理
ユーザー ID 管理を信頼できる唯一の情報源に一元化する。

統合
アプリケーションと主要な ID プロバイダーを統合し、強力なセキュリティと効率性を実現する。

適用
ID プロバイダーがすでに実施済みでない場合、2FA またはパスワード ポリシーを適用する。

監視
ユーザー アクセス、権限、監査ログを定期的に監視する。

信頼できる唯一の情報源に一元化する

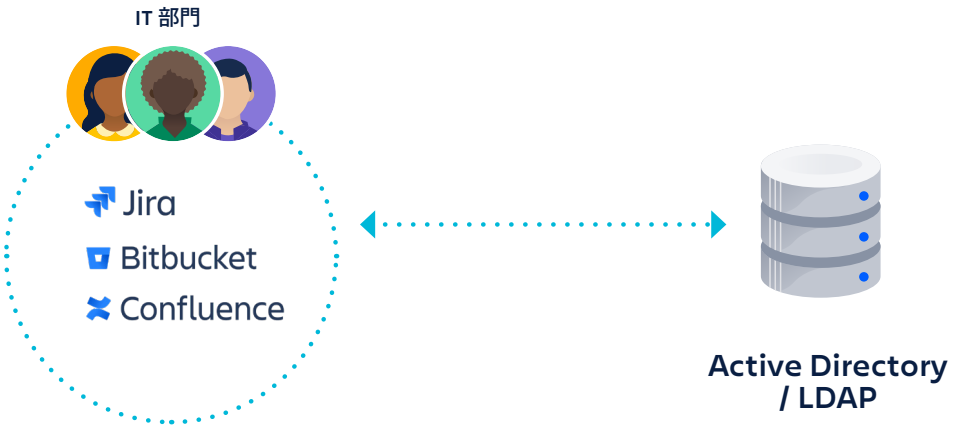
一元管理された ID 管理とアクセスを使用してポリシーを適用し、コストを管理する

Jira Software、Jira Service Management、Confluence、Bitbucket、Trello、Opsgenie など、Atlassian のクラウド製品は、多くの SaaS アプリ同様、通常「ボトムアップ」で導入されます。サブスクリプションは IT 部門で調達されるのではなく、部署ごとに購入され、セキュリティとプライバシーに関する調査プロセスは回避されます。コストを管理しポリシーを適用するため、IT 管理者はこうしたすべてのクラウド アプリケーションを 1 つのシステムで一元管理する必要があります。

Atlassian サーバー環境とクラウド環境: ID とアクセス管理での異なる概念

通常のオンプレミスの Atlassian サーバー環境と Atlassian クラウド環境では ID とアクセスの管理が異なります。アプリケーション間のデータ統合、および ID 管理の概念は、サーバー環境とクラウド環境では異なることに気が付くでしょう。

Atlassian 製品がオンプレミスで使用されている場合、次のような状況が発生します。



製品ごとに IT 部門によって管理されている 1 つの「企業」インスタンスがあり、ユーザー ID 管理において一般的に使用される、企業の Active ディレクトリまたは LDAP ディレクトリにすべてが接続されています。

クラウドでは、同じレベルのガバナンスの実現が難しくなります。複数の部門がクラウド製品で独自のインスタンスを使用している可能性があります。IT 部門は独自の Jira Service Management と Confluence アプリケーションを所有していて、エンジニアリング部門も独自の Jira Software と Bitbucket リポジトリを使用しているかもしれません。

一方、マーケティング部門は Trello を採用していることが判明しました。Slack や Office 365 を使用しているチームも存在します。

誰が何にアクセスしているのでしょうか? 管理されていないアプリケーションが多数存在する場合、すべてを把握することは不可能です。

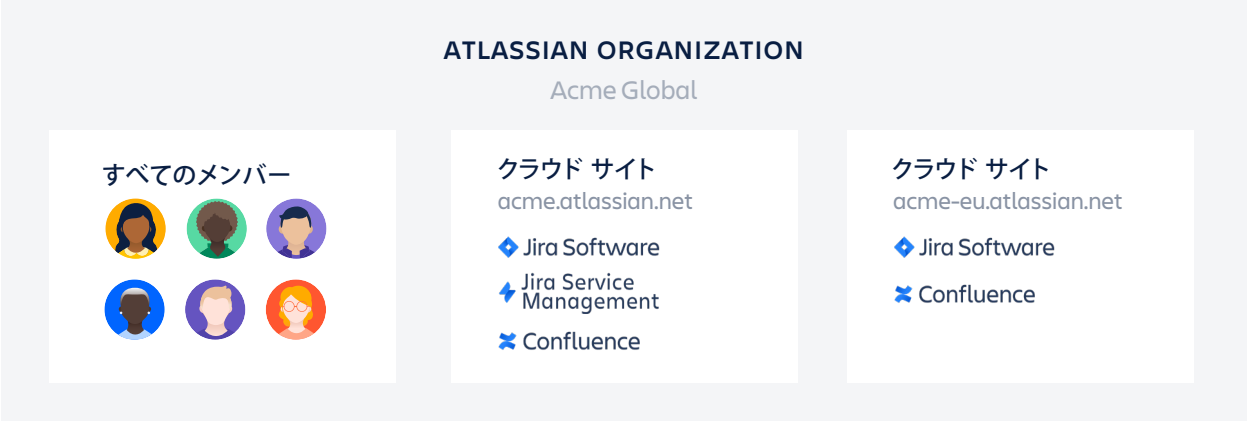
Atlassian クラウド環境では、ユーザーは 1 つのメール アドレスにつき 1 件のアカウントを所有します。各ユーザーは 1 つの企業 ID と 1 つのパスワードを所有しており、Jira Cloud インスタンスであれ、パートナーの Confluence インスタンスであれ、2FA を設定するのは 1 回だけです。つまり、管理者はユーザーごとに 1 件の認証情報を管理するのみで、各ユーザーはすべての Atlassian クラウド製品に 1 つの認証情報でアクセスできるのです。これは関係者の誰にとっても、ID 管理負担の大幅な軽減となります。

組織とドメイン検証で
企業のすべてのユーザーを表示、管理する

Jira と Confluence 製品シリーズで使用されている概念、***「サイト」***をご存知かもしれません。「サイト」を使用すると、異なる製品へのアクセス管理と、サイト全体でのグループおよびその他の設定の共有を行うことができます。Jira または Confluence インスタンスを設定するとき、サイトに名前を付けると、インスタンスへのアクセスに使用できる URL が生成されます。

1 つの組織内で、異なるチームが複数の Atlassian クラウド製品とサイトを使用していることがあります。サンフランシスコのチームは 1 つのサイトで Jira Software を使用し、ニューヨーク オフィスのチームは別のサイトで Jira Service Management を使用しているかもしれません。また、世界各国のエンジニアが独自の Bitbucket アカウントを使用してコードを保存している場合があります。管理者として、サイトや製品にかかわらず、組織全体におけるすべての Atlassian クラウド ユーザーを確認できる単一の場所が必要です。

複数の Atlassian クラウド製品とサイトを 1 か所で管理できるようにするため、Atlassian は Atlassian クラウド製品向けに、***「組織」と呼ばれる新しいグローバル管理レイヤーを作成しました。***



「組織」を使用すると、お客様の会社で使用されている Atlassian クラウド アプリのすべてのユーザーを一元表示することができます。

1 つ以上のサイトが存在する可能性があるため、組織をまとめる新しい宛先、Atlassian 管理者ハブ (**admin.atlassian.com**) を作成しました。

「組織」下では、***ドメイン検証***というプロセスを通じて、組織内の Jira Software、Jira Service Management、Jira Core、Confluence、Bitbucket のクラウド バージョンのすべてのユーザーを管理できます。

ドメインの所有権を検証したら、ドメインのメール アドレスを使用して、Atlassian が把握しているすべてのユーザーの管理を開始できます。これを管理対象アカウントと言います。組織の管理者は、管理対象アカウントのエクスポート、変更、無効化、削除を実行できます。また、管理対象アカウント全体に **Atlassian Access** のセキュリティ ポリシーを適用することもできます。

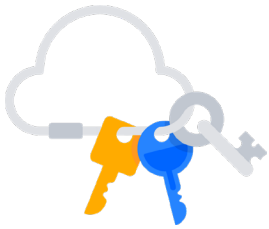
組織内:
クラウド製品向けにユーザー管理を一元化

組織を設定したら、製品とユーザーの管理に役立つツールを見つけることができます。

- **ディレクトリ:** ドメインの検証後に管理できるアカウントのリストが含まれます。また、ユーザー プロビジョニングのために ID プロバイダーと接続する場所でもあります。**詳細を見る**
- **セキュリティ:** **Atlassian Access に登録**すると、より多くの管理およびセキュリティ機能を使用できるようになり、組織を最大限活用できます。**詳細を見る**
- **設定:** 詳細のアップデート、組織管理者としてのユーザーの設定、別のドメインの追加、API キーの作成などを実行できます。**詳細を見る**
- **サイトと製品:** 使用するすべての製品とそのサイトを表示します。ユーザーを登録し、グループおよび製品へのアクセスをアップデートできます。**詳細を見る**

管理者サイトから組織を管理するだけではなく、**組織の REST API** を使用して、組織の詳細情報 (すべてのユーザーとドメインなど) を取得することができます。

AtlassianとIDプロバイダーを統合する



SSOを有効化してエンドユーザー向けのセキュリティを強化し、ログインを簡略化する

ユーザー アカウントを保護するために最も重要なことは、SAML シングル サインオン (SSO) の設定です。すべてのユーザーがログイン時に強力なパスワードと複数の認証基準という要件を満たしていること、SSO プロバイダーを介して承認された場所とデバイスからログインしていることを確認できます。

SSO にクラウド IdP を使用したとき可能になるのは、認証の管理だけではありません。どのデータに誰がアクセスするかも管理できます。Atlassian クラウド製品だけではなくすべての SaaS アプリケーションにおいて、個々のユーザーに権限のレベルを割り当てることができます。

上位のIDプロバイダーへのサポート (随時追加予定)

Atlassian Access へのサブスクリプションを含む Atlassian クラウド製品は、最も一般的な ID プロバイダー 5 社をサポートしています。また、以下に記載されていない任意の ID プロバイダーとのカスタムの SAML 接続の設定も可能です。IdP を使用すると、すべての Atlassian 製品を、管理された認証済みのエンドポイント経由で使用するよう設定できます。これによって、セキュリティ要件の達成に 1 歩近づきます。

BITIUM　Cloud Identity　idaptive

Microsoft Azure　Microsoft Active Directory Federation Services　okta　onelogin

SAML シングル サインオンの利用を開始する

SAML シングル サインオンを Atlassian クラウド製品向けに設定するには、「組織」を作成し、ドメインを検証してから、**Atlassian Access** のトライアルを開始します。その後、手順に従い **SAML シングル サインオン**を設定します。

ユーザー プロビジョニング (SCIM) を使用して ユーザー ライフサイクル管理を自動化する

企業が成長し、システムのユーザーが増えるにつれ、手動から自動のプロビジョニングに移行して、IdP 経由でポリシーに基づくアクセス管理を実行する利点が高まります。これにより IT 部門は各ユーザーに割り当てられた権限を一元表示でき、ユーザー プロビジョニングと無効化を自動化できます。また、アプリケーションにアクセスできるユーザーを決定づけるユーザーまたはグループの属性に基づいて、自動でルールを割り当てることができるようになります。

このユーザー プロビジョニングを円滑化するため、Atlassian では SCIM というプロトコルを使用しています。SCIM では、Okta、Azure AD、Onelogin などの IdP を使用してユーザー ID を管理し、それらの詳細を Atlassian 製品と同期できます。たとえば、Okta で Atlassian アプリケーションをユーザーに割り当てると、Access は自動的に変更を検知し、選択された Jira または Confluence のインスタンスに同期します。

ユーザー プロビジョニングの利点

- **社員のオンボーディングとオフボーディングを自動化する**
  ID プロバイダーと直接同期すると、誰かが入社したときに手動でユーザー アカウントを作成する必要がなくなります。
- **アクセスと権限を管理する**
  Jira プロジェクトへの個人のアクセスと、特定のダッシュボードまたはフィルターを表示する権限を管理できます。また、ID プロバイダーから同期されたグループを使用して、Confluence ページの表示と編集を行うことができます。
- **自動デプロビジョニングでコストを管理する**
  社員が会社を去るときのデプロビジョニング プロセスを自動化することで、不要なサブスクリプション ライセンスの請求を回避することができます。
- **情報流出のリスクを軽減する**
  デプロビジョニングの自動化により、元社員のアクセスは、社員が会社を辞めると同時に自動的に削除されます。

ユーザーとグループを組織に同期する

この図は、ユーザー プロビジョニングの設定後にユーザーとグループが同期される手順を示しています。IdP を組織に接続すると、IdP 内のユーザーとグループが Atlassian クラウド製品に同期されます。

- IdP から組織にユーザーとグループが同期され、プロビジョニングされたユーザーのディレクトリが作成されます。
- 企業のディレクトリは、すべての関連付けられたサイトに同期され、プロビジョニング済みのユーザーとグループにアクセス権を提供します。
- グループは製品に割り当てられ、グループごとのデフォルトの製品アクセス権をユーザーに付与します。

ユーザー プロビジョニングとライフサイクル管理を開始する

Atlassian クラウド製品向けにユーザー プロビジョニングを設定するには、組織を作成し、ドメインを検証してから **Atlassian Access のトライアルを開始**します。その後、これらの手順に従って**ユーザー プロビジョニング**を設定します。

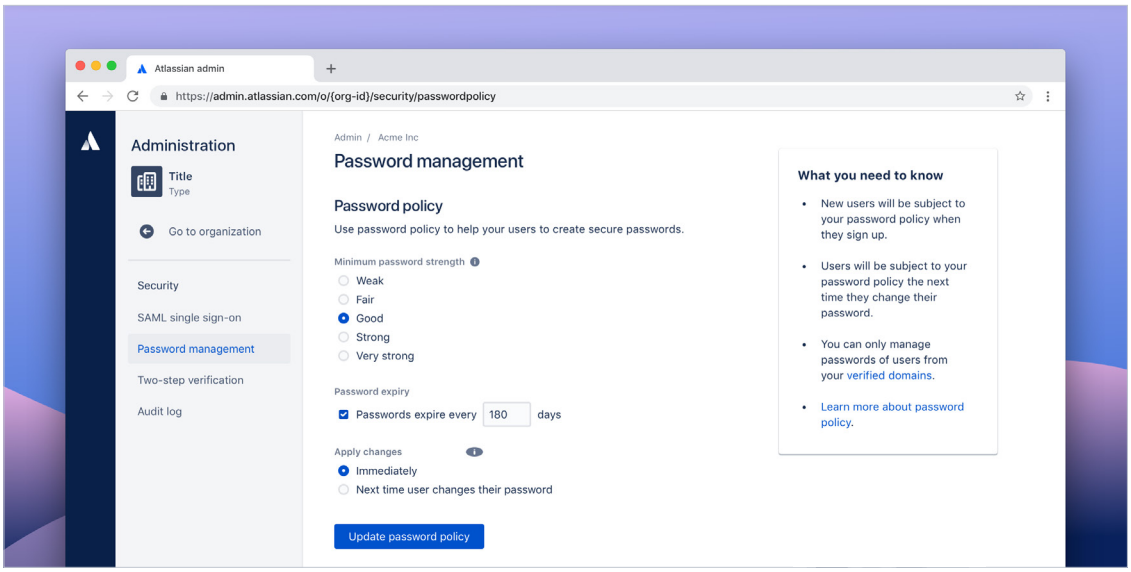
セキュリティ ポリシーを適用する

2 段階認証でアカウントを保護する

主要な ID プロバイダーの多くは 2 段階認証 (2FA) を利用しています。クラウド IdP を使用していない場合は、Atlassian Access を使用して設定を行い、Atlassian 組織でユーザーを管理できます。2 段階認証は、管理されているユーザーの Atlassian アカウントに、ログイン手順をもう 1 段階追加します。ユーザーはログイン時に、パスワードに加えて 6 桁のコードを入力する必要があります。この第 2 のステップが、パスワードが流出したときでもアカウントを保護します。アカウント ログインが保護されていると、組織の製品とリソースも保護されます。

すべてのユーザーに強力なパスワード ポリシーを適用する

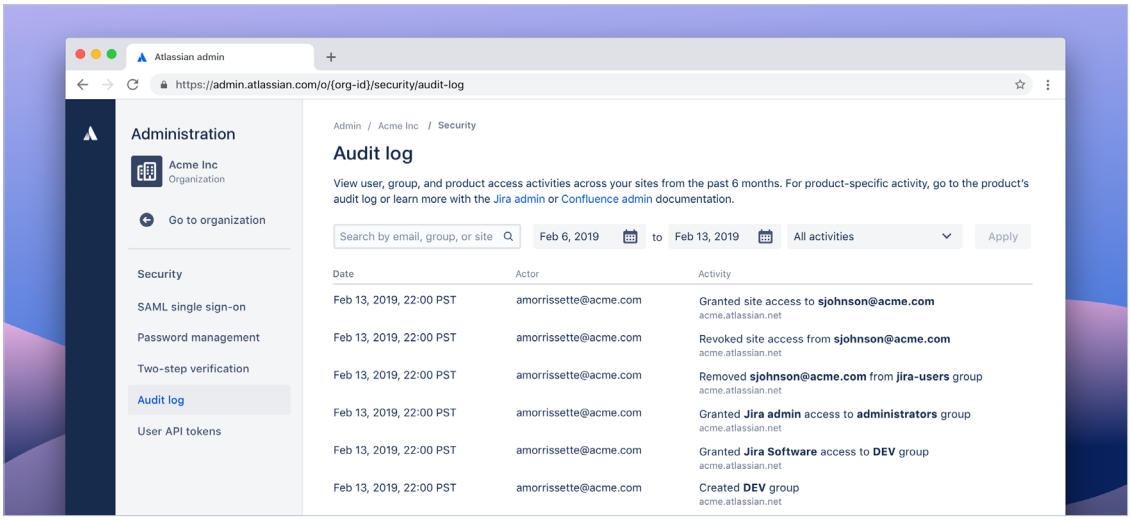
IdP を使用して SSO を有効化していない場合、Atlassian Access はすべてのユーザーへの、より強力なパスワード要件の適用をサポートします。パスワード ポリシーを使用すると、Atlassian クラウド製品にアクセスしているユーザーがパスワードを作成する際、ベスト プラクティスを使用していることが確認されます。これによりセキュリティ侵害のリスクが軽減されます。



アカウントの保護に関するベスト プラクティスの使用を開始する

2 段階認証とパスワード ポリシーを Atlassian クラウド製品全体で適用するには、組織を作成し、ドメインを検証してから **Atlassian Access のトライアルを開始します**。その後、これらの手順に従い、**2 段階認証**と**パスワード ポリシー**を設定できます。

ユーザーの権限とアクティビティを監視する



監査ログを使用してメンバーシップ、アクティビティ、権限を1か所で追跡する

監査ログはさまざまな規制と内部ポリシーへの準拠を確認するための主要な手段です。Atlassian Access を使用すると、組織全体の監査ログを取得し、Jira と Confluence 製品全体におけるユーザーとグループの変更を可視化できます。これらの監査ログは、変更を加えたユーザー、ユーザーとグループのメンバーシップ、これらの異なるグループにアクセスを付与したユーザーなどの詳細を表示します。

また、Atlassian の組織を使用すると、管理者は API トークンへのアクセス権を所有するユーザーを表示できます。これにはトークンの作成者、作成されたトークンの数、トークンへの最終アクセスが含まれます。管理者はトークンを無効化することもできます。

Atlassian 組織でこれらのインサイトを活用すると、データへのアクセス権を持つユーザーの包括的かつドキュメント化されたリストを表示することができ、変更や要件準拠の確認が簡素化されます。

データへのアクセス権を持つユーザーの可視化

Atlassian クラウド製品全体の監査ログを表示するには、組織を作成し、ドメインを検証してから **Atlassian Access のトライアルを開始**します。

Atlassian IAM の実装に向けた次のステップ

1. **作成** 組織の成長目標をまとめた計画を作成し、新しい IAM システムの要件を優先順位付けできるようにします。
2. **調査** IdP と ID およびアクセスの状況を調査し、必要なツールの種類を決定します。
3. **特定** 実装する必要がある新しいポリシーまたはアップデートされたポリシーを特定します。
4. **選択** IAM 計画を完成させるために、IdP と関連するクラウド アプリケーションを選択します。
5. **作成** Atlassian クラウド製品向けの組織を作成し、ドメインを取得します。
6. **登録** Atlassian Access に登録し、セキュリティ ポリシーを適用します。
7. **統合** Atlassian Access と ID プロバイダーを統合し、SSO とユーザー プロビジョニングを実現します。

Atlassian Access による Atlassian クラウド アプリケーションの可視性向上、統合されたユーザーとポリシー管理、セキュリティ強化、ユーザー ライフサイクル管理の簡素化について詳しくご覧になり、**30 日間の無料トライアルを開始してください。**

その他のリソース

ウェビナー: クラウドで Atlassian を保護および拡張する
コラボレーション ツールを使用してチームの能力を向上させ、企業データのセキュリティを強化できます。このウェビナーでは、Atlassian クラウド ID とセキュリティ環境について明確に理解し、セキュリティを強化してユーザー管理のプロセスを合理化させるための主要な戦略を学ぶことができます。

ブログ: クラウド製品向けの 7 つの絶対的なプラクティス
クラウド製品向けにセキュリティのベスト プラクティスを実装することは、グランドマスターを相手にチェスをしているようだと感じるかもしれません。複雑な戦略や今後の計画について、先を読んで把握しておかなければならないと思うでしょう。しかし実際は、小学校 3 年生とチェッカーで対戦しているようなものなのです。

ドキュメント: クラウド セキュリティのベスト プラクティスに従う
これらのベスト プラクティスを使用すると、社内で特に重要な業務を保護するための強力な基盤を構築できます。

ATLASSIAN