ATLASSIAN

Der Atlassian-Leitfaden zu Identitäts- und Zugriffskontrolle in der Cloud

Inhalt

Die digitale Transformation hält in großen wie auch kleinen Unternehmen Einzug, erweitert deren Fähigkeiten und eröffnet völlig neue Möglichkeiten.

Die Vorteile dieser neuen digitalen Welt können jedoch nur voll ausgeschöpft werden, wenn die Zusammenarbeit innerhalb des Unternehmens gefördert wird. Um gute Entscheidungen treffen zu können, müssen die richtigen Mitarbeiter Zugriff auf die richtigen Informationen haben – und zwar schnell. Pläne müssen geteilt, kritische Vorgänge müssen eskaliert und Entscheidungen müssen dokumentiert und gespeichert werden sowie leicht auffindbar sein.

All diese Aktivitäten (und die dabei produzierten Daten) werden zunehmend in die Cloud verlagert.

Früher haben Unternehmen vor Ort Firewall-geschützte Software verwendet und nur eine Handvoll zentral verwalteter Anwendungen genutzt. Heute führen einzelne Teams Cloud-Tools ein, um geschäftliche Probleme gezielt zu lösen. Oft werden mehrere Anwendungen über APIs integriert und dabei wertvolle – manchmal sogar vertrauliche – Daten an mehrere Softwareanbieter gesendet.

Die größte Herausforderung der modernen IT besteht darin, die Unternehmensdaten trotz der steigenden Anzahl von Anwendungen und Endgeräten zu schützen.

Die Verlagerung sensibler Assets Ihres Unternehmens in die Cloud erfordert eine andere – stärkere – Kontrolle darüber, welche Mitarbeiter auf Cloud-Apps und -Services zugreifen können. Dieser Aspekt der IT-Governance – Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) in der Cloud – ist der Schlüssel zur Bewältigung der größten Herausforderung der digitalen Transformation.

Dieser Leitfaden behandelt die wichtigen Änderungen im IAM-Bereich, die der Umstieg der Unternehmen auf die Cloud mit sich bringt, darunter:

- **Die Entwicklung von lokalen Lösungen zu einem neuen Cloud-IAM-Ansatz und von Tools zu Prozessen**
- **Die Vorteile von Cloud-IAM in Bezug auf Automatisierung, Produktivität und Sicherheit**
- **Die ersten Schritte beim Cloud-IAM und Erstellen eines Änderungsplans**
- **Die Nutzung von Atlassian Cloud-Produkten für Ihren Cloud-IAM-Ansatz**

Identitäts- und Zugriffsmanagement in der Cloud: Grundlagen

Identitäts- und Zugriffsmanagement in der Cloud: Grundlagen

Was ist Identitäts- und Zugriffsmanagement in der Cloud?

Cloud-IAM umfasst die Tools und Prozesse zur Verwaltung von Benutzeridentitäten und Kontrolle des Zugriffs auf lokale und Cloud-basierte Anwendungen. Der beste Cloud-IAM-Ansatz bietet einen zentralen Ort für die Verwaltung der Benutzeridentitäten und lässt sich in eine heterogene Arbeitsumgebung integrieren. Der Zugang zu allen IT-Ressourcen sollte stets gewährleistet sein, unabhängig von der Betriebssystemplattform, dem Authentifizierungsprotokoll, dem Standort oder dem Anbieter.

Wie unterscheidet sich das Identitätsmanagement in der Cloud von lokalem Identitätsmanagement?

Das Identitätsmanagement in der Cloud ist ein neuer Ansatz, der sich aus den ursprünglichen, vor zwanzig Jahren eingeführten Lösungen entwickelt hat. Damals wurden die meisten IT-Ressourcen vor Ort hinter der Firewall verwaltet und die Systeme und Anwendungen eines Anbieters (in den meisten Fällen Microsoft) genutzt. Diese Systeme waren für die Verwaltung einiger – und nicht Hunderter – Anwendungen konzipiert. Heute können sie einfach nicht mehr mit den aktuellen Anforderungen an die IT Schritt halten.

Im Gegensatz dazu zeichnen sich die heutigen Systeme für das Identitätsmanagement in der Cloud durch Folgendes aus:

- Angebot als SaaS-Produkte, die sich in verschiedene Arten von Systemen integrieren lassen
- Zugriff von mehreren Gerätetypen aus
- Möglichkeit der Vereinheitlichung Ihrer Identitäts- und Zugriffsrichtlinien
- Fähigkeit zur Anpassung an sich ständig ändernde Zugriffsanforderungen

Bei der Verwaltung von Benutzeridentitäten in einer Cloud-Umgebung ist es jedoch nicht damit getan, neue Cloud-IAM-Tools zu implementieren und anschließend den Migrationspfad von Ihren alten lokalen Systemen zuzuordnen. Sie benötigen nicht nur neue Tools, sondern müssen auch neue Richtlinien erstellen, bestehende Richtlinien aktualisieren und vor allem die weitere Entwicklung Ihres Unternehmens planen, damit Sie anhaltendes Wachstum unterstützen können.

Vorteile des Identitäts- und Zugriffsmanagements in der Cloud

- **Zentralisierte Verwaltung für heterogene Umgebungen**
  Das Identitätsmanagement in der Cloud ersetzt das Patchwork an lokalen Identitätssystemen und Tools und arbeitet nahtlos mit allen Ressourcen in der IT-Abteilung zusammen: macOS, Linux, AWS, Webanwendungen, WLAN – ganz nach den jeweiligen Präferenzen.
- **Automatisierung der Benutzerbereitstellung und Durchsetzung von Sicherheitsrichtlinien**
  Moderne IAM-Lösungen helfen Ihnen, das Benutzerzugriffsmanagement für lokale und Cloud-basierte Umgebungen zu zentralisieren. Sie können die Bereitstellung automatisieren, um das Onboarding zu rationalisieren, und wenn Mitarbeiter und Auftragnehmer das Unternehmen verlassen, können Sie den Zugriff sofort sperren, um die Einhaltung von Sicherheitsrichtlinien zu gewährleisten.
- **Durchsetzung von kontextbezogenem Zugriffsmanagement**
  Automatisieren Sie dynamische Zugriffsentscheidungen basierend auf zugewiesenen Risikofaktoren, die über die zugewiesene Rolle des Benutzers hinausgehen, wie z. B. Standort, Netzwerk, Gerätebeschränkungen, Art der Anfrage und Zeitpunkt.
- **Höhere Produktivität für Endbenutzer und IT**
  Mit einem Single-Sign-On-Anbieter (SSO, ein wichtiger Bestandteil Ihres Cloud-IAM-Ansatzes – mehr dazu später) können Benutzer über ein einziges Dashboard mühelos alle ihre Unternehmens-Apps finden und sich bei ihnen anmelden.

Erste Schritte mit Cloud-IAM

Wenn Sie bereit für den Umstieg auf die Cloud und die Zentralisierung Ihres Identitäts- und Zugriffsmanagements sind, müssen Sie sich für eine Identitätsanbieter-Lösung (IdP) entscheiden. Dies ist jedoch nicht ganz so einfach wie ein gewöhnlicher Softwarekauf. Bei der Suche sind mehrere wichtige Faktoren zu berücksichtigen:

1. **Planen Sie voraus.**
   Wenn Sie wissen, in welche Richtung sich Ihr Unternehmen in Bezug auf Wachstum und Skalierung bewegen muss, können Sie dafür sorgen, dass Ihr neues IAM-System Ihre Ziele unterstützt.

2. **Berücksichtigen Sie Ihre Ausgangsposition.**
   So können Sie potenzielle Anbieter besser priorisieren. In den meisten Fällen fallen IT-Abteilungen, die zur Cloud migrieren möchten, in eine von drei Kategorien:

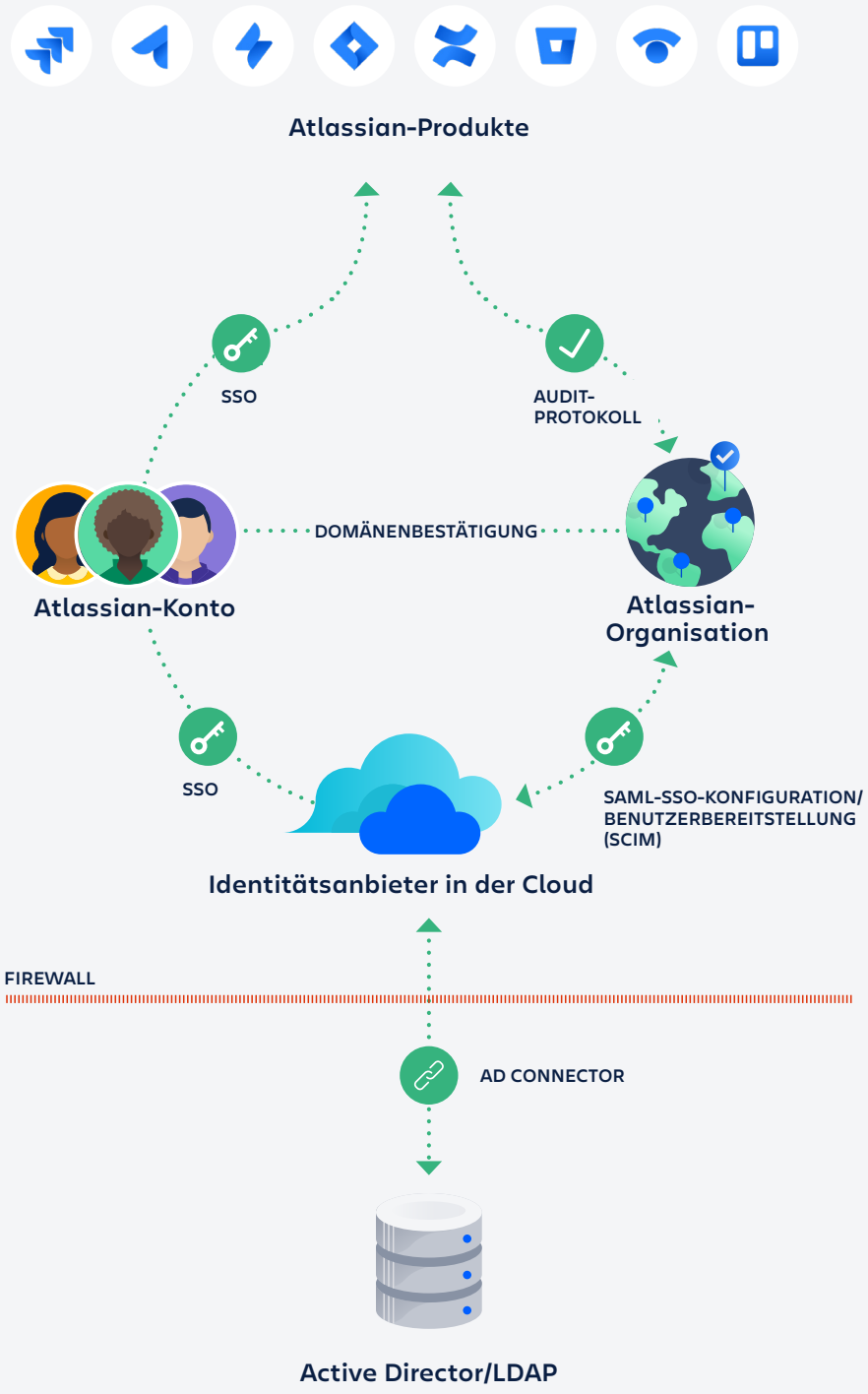
   - Sie nutzen ein lokales LDAP-Verzeichnissystem und möchten in die Cloud wechseln.
   - Sie nutzen eine vorhandene Installation von Microsoft Active Directory (AD) und möchten in die Cloud wechseln, häufig zur Verwaltung einer heterogenen Umgebung.
   - Sie nutzen derzeit überhaupt kein Benutzerverzeichnis, um Benutzeridentitäten zu verwalten.

3. **Machen Sie eine Bestandsaufnahme Ihrer aktuellen IT-Umgebungen.**
   Berücksichtigen Sie alle Protokolle, Plattformen und Netzwerke in Ihrer Infrastruktur, um die Interoperabilität mit Ihren Systemen sicherzustellen.

4. **Erfassen Sie alle Anbieter-Apps und SaaS-Tools und bestimmen Sie, welche davon für das Unternehmen kritisch sind.**
   Ermitteln Sie alle Anwendungen, auf die Sie den Zugriff verwalten müssen, insbesondere wenn Sie mit der Ausarbeitung eines Plans für die Priorisierung von Integrationen beginnen.

> **Gut zu wissen**
> Wenn Sie sich über Ihre Anforderungen und Prioritäten im Klaren sind, haben Sie bessere Aussichten darauf, dass Ihre Suche nach der richtigen Mischung von IAM-Anbieter-Tools reibungslos vorangeht. Da Sie diesen IAM-Prozess in die Cloud bringen, müssen Sie außerdem keine umfangreichen langfristigen Investitionen in neue Hardware oder interne Ressourcen für die Verwaltung der Sicherheit oder von Patches tätigen. Diese Aufgabe erledigen Ihre Cloud-Anbieter für Sie.

Eingehende Kenntnis der Cloud IAM-Umgebung



Sobald Sie Ihren Identitätsanbieter (IdP) für die Cloud ausgewählt haben, ist es wichtig, eine gute Vorstellung davon zu bekommen, wie er in die Gesamtumgebung Ihrer lokalen und cloudbasierten Anwendungen passt. Hier sind einige der Aspekte, die diesbezüglich zu berücksichtigen sind:

- **Identifizierung Ihres Profil-Masters**
  Identifizieren Sie zunächst Ihren Profil-Master – die Anwendung, die als zentrale Informationsquelle für Benutzer und Gruppen dient. Eine Möglichkeit besteht darin, Ihre Benutzer und Gruppen direkt in Ihrem Cloud-IdP als Master festzulegen. Sie können Ihre Benutzer und Gruppen jedoch auch in einem Personalinformationssystem wie Workday als Master speichern.
  - **Verbindung Ihres Cloud-IdP mit Ihrem lokalen Verzeichnis**
    In diesem Diagramm haben wir die Informationsquelle für Profil-Master als lokale Active Directory- oder LDAP-Datenbank definiert. Im vorliegenden Beispiel müssen Sie in der Lage sein, Ihren cloudbasierten IdP mit dem in Ihrem Netzwerk gehosteten Verzeichnisdienst zu verbinden. Alle führenden Cloud-IdPs bieten Agenten oder Konnektoren, die in Ihrem Unternehmensnetzwerk die Synchronisierung zwischen dem Cloud-IdP und den Benutzern und Gruppen in Ihrem Active Directory- oder LDAP-Server ermöglichen – Ihrer zentralen Informationsquelle. Wenn Sie Active Directory oder LDAP in Ihrem lokalen System haben, können Sie dies weiterhin nutzen, um mit Ihren lokalen Anwendungen Identitäten und Zugriffe zu verwalten.
  - **Authentifizierung bei Cloud-Apps über Ihren Cloud-IdP**
    Sie können Anwendungen, die sich in der Cloud befinden, mit Ihrem Cloud-IdP verbinden und Ihre Benutzer können sich über Protokolle wie SAML-Single-Sign-On (SSO) bei diesen Anwendungen aus dem öffentlichen Internet authentifizieren und auf diese zugreifen.
- **Verwaltung des Zugriffs von Benutzern auf Atlassian-Anwendungen über Ihren Cloud-IdP und SSO**
  Ihr Cloud-IdP kann auch mithilfe seines Atlassian-Kontos die SSO-Authentifizierung zwischen Atlassian-Organisationen und dem IdP über SAML-SSO bereitstellen. Wenn Benutzer über ihr Atlassian-Konto auf Atlassian-Anwendungen wie Jira Software Cloud zugreifen, werden sie zur Anmeldung an Ihren IdP weitergeleitet.
- **Bereitstellung neuer Atlassian-Benutzer über Ihren Cloud-IdP**
  Ebenso können Sie Benutzer und Gruppen in Ihrem Cloud-IdP (der ursprünglich von Ihrem lokalen Active Directory synchronisiert wurde) für Ihre Atlassian-Organisation bereitstellen. Dann werden diese Gruppen an die nachgelagerten Anwendungen weitergegeben, die Sie mit Ihrer Atlassian-Organisation verknüpft haben, sodass die Identitäten synchron gehalten werden.

Implementierung Ihrer Atlassian Cloud-IAM-Strategie

Implementierung Ihrer Atlassian Cloud-IAM-Strategie

Wir bei Atlassian haben unsere eigene digitale Transformation durchlaufen. Daher sind wir uns aller möglichen Probleme bewusst, auf die Ihr Unternehmen bei diesem Übergang stoßen kann.

Wir haben ein Best-Practices-Framework eingerichtet, das uns – und unseren Kunden – geholfen hat, einige der Probleme zu bewältigen, mit denen IT-Teams bei der unternehmensweiten Zusammenarbeit im großen Maßstab konfrontiert sind – bei gleichzeitiger Einhaltung aller Sicherheitsprotokolle.

In diesem Framework haben wir Richtlinien erarbeitet, die Sie bei Folgendem unterstützen:

Zentralisierung des Managements von Benutzeridentitäten in einer Informationsquelle

Integration Ihrer Anwendungen mit Ihrem primären Identitätsanbieter für mehr Sicherheit und Effizienz

Durchsetzung von Zwei-Faktor-Authentifizierung und Passwortrichtlinien, falls Sie keinen Identitätsanbieter haben, der das bereits tut

Überwachung des Benutzerzugriffs, der Berechtigungen und der Audit-Protokolle in regelmäßigen Abständen

Schaffung einer zentralen Informationsquelle

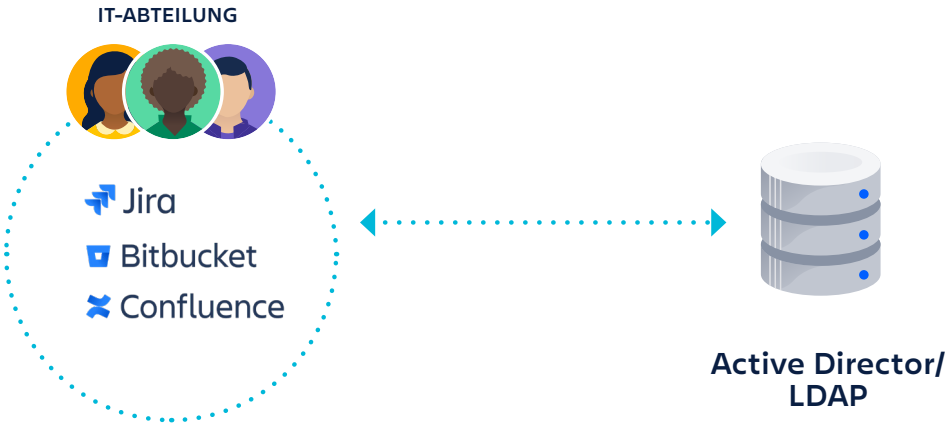
Durchsetzung von Richtlinien und Kontrolle der Kosten durch Identitätsmanagement und Zugriff an einem zentralen Ort

Atlassian Cloud-Produkte wie Jira Software, Jira Service Desk, Confluence, Bitbucket, Trello und Opsgenie werden in der Regel – wie viele andere SaaS-Apps – über einen Bottoms-Up-Ansatz in Unternehmen eingeführt. Abonnements werden von Abteilungen erworben, wobei die IT-Beschaffung – und damit auch Prozesse zur Überprüfung der Sicherheit und des Datenschutzes – umgangen werden. Um Kosten zu kontrollieren und Richtlinien durchzusetzen, müssen IT-Administratoren die Verwaltung all dieser Cloud-Anwendungen in einem System zentralisieren.

Vergleich von Atlassian Server und Cloud: verschiedene Konzepte des Identitäts- und Zugriffsmanagements

Im Folgenden finden Sie einen Vergleich des Identitäts- und Zugriffsmanagements in einer typischen lokalen Atlassian Server-Umgebung und einer Atlassian Cloud-Umgebung. Sie werden feststellen, dass die Datenintegrationen zwischen den Anwendungen in der Serverumgebung anders aussehen als in der Cloudumgebung, und sich das Konzept des Identitätsmanagements ebenfalls unterscheidet.

Bei der lokalen Verwendung von Atlassian-Produkten bietet sich folgendes Bild:



Sie haben für jedes Produkt eine von der IT-Abteilung verwaltete "Unternehmens"-Instanz, die jeweils mit dem Active Directory oder dem LDAP-Verzeichnis Ihres Unternehmens verbunden ist – zwei der gängigsten Hilfsmittel für das Management von Benutzeridentitäten.

Bei einer Cloud-Version ist es schwieriger, den gleichen Grad an Governance zu erreichen. Möglicherweise haben Sie mehrere Abteilungen, die ihre eigenen Instanzen von Cloud-Produkten verwenden. Die IT-Abteilung verfügt gegebenenfalls über ihre eigenen Jira Service Desk- und Confluence-Anwendungen, und das Entwicklerteam hat seine eigene Instanz von Jira Software und ein Bitbucket-Repository.

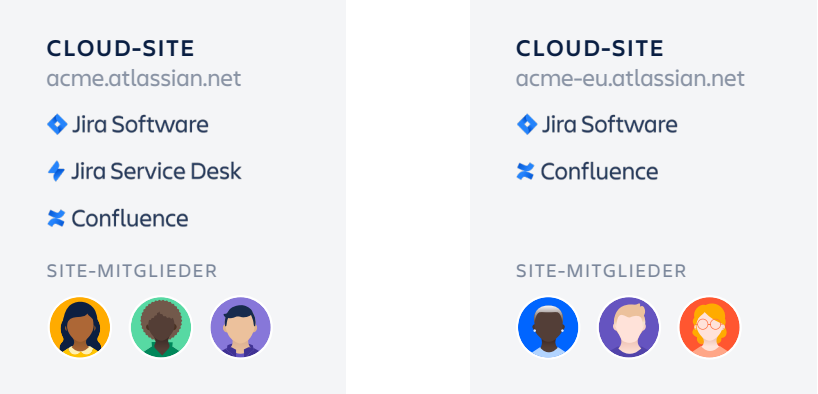
In der Zwischenzeit stellen Sie noch fest, dass die Leute in der Marketingabteilung Trello eingeführt haben. Und dann gab es die ganze Zeit noch die Teams, die Tools wie Slack und Office 365 verwenden.

Wer sind eigentlich all diese Leute und worauf haben sie Zugriff? Bei so vielen nicht verwalteten Anwendungen ist es unmöglich, diese Frage zu beantworten.

Darüber hinaus haben in einer Atlassian Cloud-Umgebung alle Benutzer ein Konto – eines pro E-Mail-Adresse. Jeder Benutzer hat eine Unternehmensidentität und ein Passwort – und muss die Zwei-Faktor-Authentifizierung nur einmal einrichten, sei es für eine Jira Cloud-Instanz oder die Confluence-Instanz eines Partners. Dies bedeutet, dass ein Administrator pro Benutzer nur einen Satz von Anmeldeinformationen verwalten muss und jeder Benutzer mit einem Satz von Anmeldeinformationen auf alle Atlassian Cloud-Produkte zugreifen kann, was das Identitätsmanagement für alle Beteiligten erheblich vereinfacht.

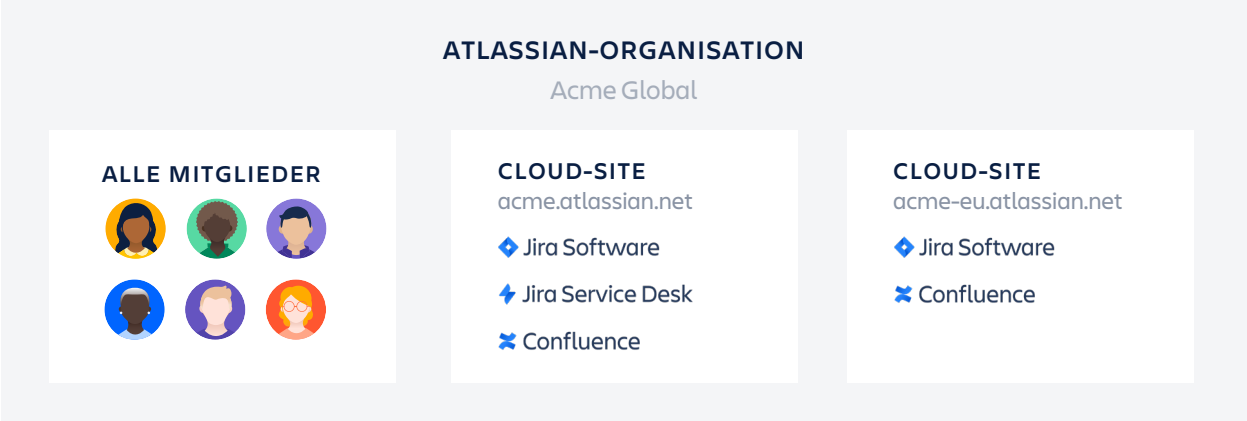
Anzeigen und Verwalten aller Benutzer in Ihrem Unternehmen mithilfe von Organisationen und Domänenbestätigung

Vielleicht haben Sie schon einmal von ***Sites*** gehört, einem Konzept, das wir für die Jira- und Confluence-Produktfamilie nutzen. Es ermöglicht Ihnen, den Zugriff auf die verschiedenen Produkte zu verwalten und Gruppen sowie andere Einstellungen auf der gesamten Site freizugeben. Bei der Einrichtung Ihrer Jira- oder Confluence-Instanz können Sie Ihrer Site einen Namen geben. Dadurch wird eine URL generiert, die Sie für den Zugriff auf Ihre Instanz verwenden.



Verschiedene Teams innerhalb eines Unternehmens könnten mehrere Atlassian Cloud-Produkte und -Sites verwenden. Beispielsweise könnte ein Team in San Francisco Jira Software auf einer Site verwenden, während das Team im New Yorker Büro Jira Service Desk auf einer anderen Site nutzt. Außerdem könnten die auf der ganzen Welt verteilten Entwickler den Code in ihren individuellen Bitbucket-Konten speichern. Als Administrator benötigen Sie einen Ort, an dem Sie unabhängig von Site oder Produkt alle Atlassian Cloud-Benutzer im Unternehmen sehen können.

Um die zentrale Verwaltung mehrerer Atlassian Cloud-Produkte und -Sites zu ermöglichen, haben wir für Atlassian Cloud-Produkte eine neue globale Verwaltungsebene namens ***Organisationen entwickelt.***



Organisationen bieten Ihnen eine zentrale Ansicht aller Benutzer von Atlassian Cloud-Apps, die in Ihrem Unternehmen verwendet werden.

Da Sie möglicherweise über mehr als eine Site verfügen, haben wir außerdem ein neues Ziel namens Atlassian Admin Hub oder **admin.atlassian.com** erstellt, das Organisationen zusammenführt.

Eine Organisation ermöglicht Ihnen, alle Benutzer der Cloud-Versionen von Jira Software, Jira Service Desk, Jira Core, Confluence und Bitbucket Ihres Unternehmens durch einen Prozess namens ***Domänenbestätigung zu verwalten***.

Sobald Sie bestätigt haben, dass eine Domäne Ihnen gehört, können Sie damit beginnen, jeden einzelnen Benutzer mit einer E-Mail-Adresse von Ihrer Atlassian bekannten Domäne zu verwalten. Diese Konten werden als "verwaltete Konten" bezeichnet. Als Organisationsadministrator können Sie diese verwalteten Konten exportieren, ändern, deaktivieren und löschen. Sie haben auch die Möglichkeit, für Ihre verwalteten Konten Sicherheitsrichtlinien von **Atlassian Access** durchzusetzen.

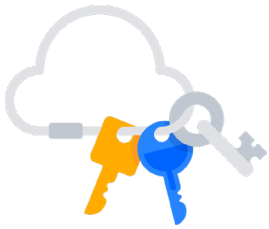
EINBLICK IN ORGANISATIONEN:
ZENTRALISIERTE BENUTZERVERWALTUNG FÜR IHRE CLOUD-PRODUKTE

Wenn Sie Ihre Organisation eingerichtet haben, stehen Ihnen folgende Tools für die Verwaltung von Produkten und Benutzern zur Verfügung:

- **Verzeichnis:** Enthält eine Liste der von Ihnen verwalteten Konten, vorausgesetzt, Sie haben **Ihre Domänen bestätigt**. Hier können Sie auch Ihren Identitätsanbieter für die Benutzerbereitstellung verbinden. **Mehr erfahren**
- **Sicherheit:** **Mit einem Atlassian Access-Abonnement** haben Sie mehr Kontroll- und Sicherheitsfunktionen und können die Vorteile von Organisationen voll ausschöpfen. **Mehr erfahren**
- **Einstellungen:** Hier können Sie Ihre Daten aktualisieren, einen Benutzer zum Organisationsadministrator machen, eine weitere Domäne hinzufügen und einen API-Schlüssel erstellen. **Mehr erfahren**
- **Sites und Produkte:** Ein Überblick über alle von Ihnen verwendeten Produkte und deren Sites, auf denen Sie Benutzer verwalten sowie Gruppen und den Produktzugriff aktualisieren können. **Mehr erfahren**

Zusätzlich zur Verwaltung Ihrer Organisation von der Admin-Site aus können Sie über die **REST-API für Organisationen** Daten zu Ihrer Organisation wie z. B. alle Benutzer und Domänen abrufen.

Integration von Atlassian Access mit Ihrem Identitätsanbieter



Mehr Sicherheit und eine einfachere Anmeldung für Endbenutzer mit SSO

Die wichtigste Maßnahme zum Schutz von Benutzerkonten ist die Einrichtung von SAML-Single-Sign-On oder SSO. Auf diese Weise können Sie sicherstellen, dass sich jeder Benutzer anmeldet und Ihre Anforderungen an sichere Passwörter und mehrere Authentifizierungsstandards erfüllt. Darüber hinaus sorgen Sie dafür, dass die Anmeldung nur von zugelassenen Standorten und Geräten aus erfolgt – alles über Ihren SSO-Anbieter.

Wenn Sie einen Cloud-IdP für SSO nutzen, haben Sie neben der Kontrolle der Authentifizierung noch weitere Möglichkeiten. Sie können auch kontrollieren, wer Zugriff auf welche Daten hat und einzelnen Benutzern Berechtigungsstufen zuweisen – nicht nur für Ihre Atlassian Cloud-Produkte, sondern auch für alle Ihre Saas-Anwendungen.

Unterstützung für führende Identitätsanbieter – weitere folgen demnächst

Atlassian Cloud-Produkte mit einem Abonnement für Atlassian Access unterstützen fünf der gängigsten Identitätsanbieter sowie die Einrichtung einer benutzerdefinierten SAML-Verbindung mit Identitätsanbietern, die unten nicht aufgeführt sind. Mit einem IdP können Sie sicherstellen, dass die Nutzung aller Atlassian-Produkte über einen Authentifizierungsendpunkt erfolgt, den Sie kontrollieren. Damit sind Sie der Erfüllung Ihrer Sicherheitsanforderungen einen Schritt näher.

BITIUM · Cloud Identity · idaptive

Microsoft Azure · Microsoft Active Directory Federation Services · okta · onelogin

ERSTE SCHRITTE MIT SAML-SINGLE-SIGN-ON

Zur Einrichtung von SAML-Single-Sign-On für Atlassian Cloud-Produkte erstellen Sie Ihre Organisation, bestätigen Ihre Domäne und starten dann die Testversion von **Atlassian Access**. Folgen Sie dann diesen Anweisungen zum Einrichten von **SAML-Single-Sign-On**.

Automatisierung des Lifecycle Managements für Benutzer mit Benutzerbereitstellung (SCIM)

Mit dem Wachstum Ihres Unternehmens und der zunehmenden Anzahl an Benutzern in Ihren Systemen ist ein Wechsel von der manuellen Benutzerbereitstellung zum automatisierten, richtliniengesteuerten Zugriffsmanagement über einen IdP empfehlenswert. So erhält die IT einen zentralen Überblick über die Berechtigungen der einzelnen Benutzer und Sie können Benutzer automatisch bereitstellen und deaktivieren sowie basierend auf Benutzer- oder Gruppenattributen automatisch Regeln zuweisen, die bestimmen, wer Zugriff auf welche Anwendungen hat.

Zur Vereinfachung dieser Benutzerbereitstellung nutzen wir das als SCIM bekannte Protokoll. Es ermöglicht Ihnen, Benutzeridentitäten mit einem IdP wie Okta, Azure AD oder Onelogin zu verwalten und diese Daten dann mit Ihren Atlassian-Produkten zu synchronisieren. Wenn Sie beispielsweise einen Benutzer Atlassian-Anwendungen in Okta zuweisen, werden die Änderungen automatisch von Access erkannt und mit den von Ihnen gewählten Jira- oder Confluence-Instanzen synchronisiert.

Vorteile der Benutzerbereitstellung

- **Automatisiertes Onboarding und Offboarding von Mitarbeitern**
  Dank der direkten Synchronisierung mit dem Identitätsanbieter Ihrer Wahl müssen Sie nicht mehr manuell Benutzerkonten erstellen, wenn neue Mitarbeiter eingestellt werden.
- **Verwaltung von Zugriff und Berechtigungen**
  Sie können den Zugriff einzelner Benutzer auf Jira-Projekte und ihre Fähigkeit, bestimmte Dashboards oder Filter anzuzeigen, kontrollieren. Sie können auch Confluence-Seiten mit Gruppen anzeigen und bearbeiten, die von Ihrem Identitätsanbieter synchronisiert wurden.
- **Kostenmanagement mit automatischer Aufhebung der Bereitstellung**
  Mit dem Prozess zur automatischen Aufhebung der Bereitstellung, wenn Mitarbeiter aus dem Unternehmen ausscheiden, wird sichergestellt, dass Ihnen keine Kosten für nicht mehr benötigte Abonnementlizenzen entstehen.
- **Geringeres Risiko von Verstößen gegen die Informationssicherheit**
  Im Zuge der automatischen Aufhebung der Bereitstellung wird Mitarbeitern automatisch der Zugriff entzogen, wenn sie aus dem Unternehmen ausscheiden.

Synchronisieren von Benutzern und Gruppen mit Ihrer Organisation

Dieses Diagramm zeigt, wie Benutzer und Gruppen synchronisiert werden, sobald Sie die Benutzerbereitstellung eingerichtet haben. Nach der Verbindung Ihres IdP mit Ihrer Organisation werden die Benutzer und Gruppen innerhalb des IdP mit Ihren Atlassian Cloud-Produkten synchronisiert.

- Benutzer und Gruppen werden von Ihrem IdP mit Ihrer Organisation synchronisiert. Dabei wird ein Verzeichnis Ihrer bereitgestellten Benutzer erstellt.
- Das Verzeichnis Ihres Unternehmens wird mit allen zugehörigen Sites synchronisiert und ermöglicht so den Zugriff auf Ihre bereitgestellten Benutzer und Gruppen.
- Gruppen werden Produkten zugewiesen und die Benutzer innerhalb einer Gruppe erhalten standardmäßig Zugriff auf die jeweiligen Produkte.

ERSTE SCHRITTE MIT BENUTZERBEREITSTELLUNG UND LIFECYCLE MANAGEMENT

Zur Einrichtung der Benutzerbereitstellung für Atlassian Cloud-Produkte erstellen Sie Ihre Organisation, bestätigen Ihre Domäne und **starten dann die Testversion von Atlassian Access**. Folgen Sie anschließend diesen Anweisungen zum Einrichten der **Benutzerbereitstellung**.

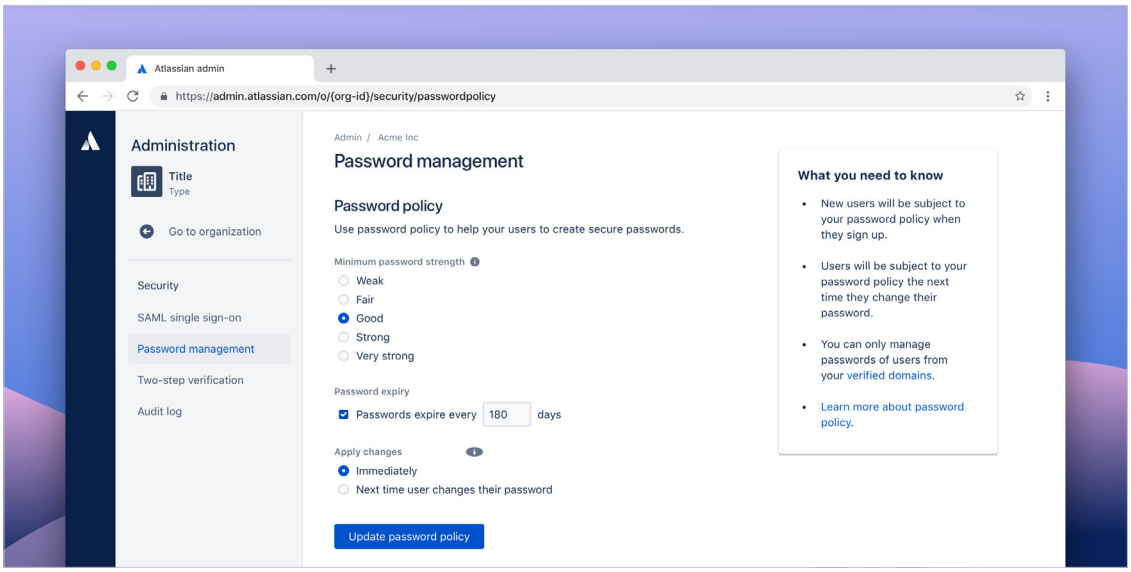
Durchsetzung von Sicherheitsrichtlinien

Schutz Ihres Kontos mit Zwei-Faktor-Authentifizierung

Die meisten großen Identitätsanbieter bieten die Verwaltung der Zwei-Faktor-Authentifizierung (2FA) an. Wenn Sie jedoch keinen Cloud-IdP haben, können Sie diese Funktion mit Atlassian Access einrichten und Benutzer mit einer Atlassian-Organisation verwalten. Mit der Zwei-Faktor-Authentifizierung kommt ein zweiter Anmeldeschritt für die verwalteten Atlassian-Konten der Benutzer hinzu, bei dem zusätzlich zum Passwort ein sechsstelliger Code eingegeben werden muss. Durch den zweiten Schritt bleiben ihre Konten auch dann geschützt, wenn das Passwort kompromittiert ist. Eine sichere Kontoanmeldung verbessert auch die Sicherheit der Produkte und Ressourcen Ihres Unternehmens.

Durchsetzung der Richtlinien für sichere Passwörter bei allen Benutzern

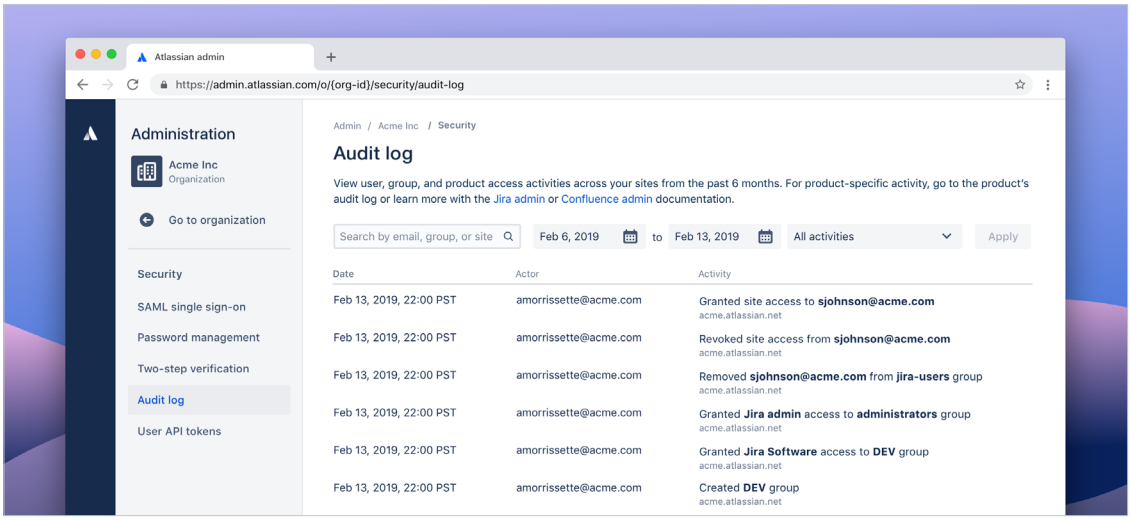
Falls Sie keinen IdP zur Aktivierung von SSO verwenden, kann Atlassian Access Ihnen auch dabei helfen, bei allen Ihren Benutzern strengere Passwortanforderungen durchzusetzen. Passwortrichtlinien sorgen dafür, dass Benutzer, die auf Ihre Atlassian Cloud-Produkte zugreifen, bei der Erstellung von Passwörtern Best Practices anwenden. So wird das Risiko für Sicherheitsverletzungen verringert.



ERSTE SCHRITTE MIT BEST PRACTICES ZUM SCHUTZ IHRER KONTEN

Zur Durchsetzung der Zwei-Faktor-Authentifizierung und Passwortrichtlinien für Ihre Atlassian Cloud-Produkte erstellen Sie Ihre Organisation, bestätigen Ihre Domäne und **starten dann die Testversion von Atlassian Access**. Folgen Sie anschließend diesen Anweisungen zum Einrichten der **verpflichtenden Zwei-Faktor-Authentifizierung** und der **Passwortrichtlinien**.

Überwachung der Berechtigungen und Aktivitäten von Benutzern



Zentrale Verfolgung von Mitgliedschaften, Aktivitäten und Berechtigungen mit Audit-Protokollen

Audit-Protokolle sind ein primäres Mittel für den Nachweis von Compliance mit verschiedenen Vorschriften und internen Richtlinien. Mit Atlassian Access können Sie jetzt organisationsweite Audit-Protokolle abrufen, um einen besseren Überblick über Benutzer- und Gruppenänderungen in Ihren Jira- und Confluence-Produkten zu erhalten. Diese Audit-Protokolle ermöglichen Ihnen das Anzeigen von Details, wie z. B. wer Änderungen vorgenommen hat, Benutzer- und Gruppenmitgliedschaften, wer Zugriff auf diese verschiedenen Gruppen gewährt hat und vieles mehr.

Eine Atlassian-Organisation bietet Administratoren auch Einblick in die Zugriffsberechtigungen für API-Token. Dabei können sie unter anderem sehen, wer das Token erstellt hat, wie viele Token erstellt wurden und wann der letzte Zugriff auf ein Token stattgefunden hat. Administratoren haben auch die Möglichkeit, ein Token zu widerrufen.

Diese Einblicke in Ihre Atlassian-Organisation sorgen dafür, dass Sie umfassend darüber informiert sind, wer Zugriff auf Ihre Daten hat. Die Dokumentation der Aktivitäten vereinfacht darüber hinaus die Untersuchung von Änderungen und den Nachweis der Compliance.

SICHTBARKEIT DER BENUTZER MIT ZUGRIFF AUF IHRE DATEN

Zur Anzeige der Audit-Protokolle für Ihre Atlassian Cloud-Produkte erstellen Sie Ihre Organisation, bestätigen Ihre Domäne und **starten dann die Testversion von Atlassian Access**.

Nächste Schritte zur Implementierung von IAM mit Atlassian

1. **Erstellen** Sie einen Plan für die Wachstumsziele Ihres Unternehmens, damit Sie wissen, welche Anforderungen für Ihr neues IAM-System Priorität haben.
2. **Untersuchen** Sie IdPs und die Identitäts- und Zugriffsanforderungen, um die Arten von Tools zu ermitteln, die Sie benötigen.
3. **Identifizieren** Sie neue oder aktualisierte Richtlinien, die sie implementieren müssen.
4. **Wählen** Sie Ihren IdP und die dazugehörigen Cloud-Anwendungen, um Ihren IAM-Plan abzuschließen.
5. **Erstellen** Sie eine Organisation für Ihre Atlassian Cloud-Produkte und fordern Sie Ihre Domäne an.
6. **Abonnieren** Sie Atlassian Access zur Anwendung von Sicherheitsrichtlinien.
7. **Integrieren** Sie Atlassian Access mit Ihrem Identitätsanbieter für SSO und Benutzerbereitstellung.

Hier erfahren Sie, wie Atlassian Access Ihnen unternehmensweit Einblicke in Ihre Atlassian Cloud-Anwendungen bietet und für ein einheitliches Benutzer- und Richtlinienmanagement, verbesserte Sicherheit und ein vereinfachtes Benutzer-Lifecycle-Management sorgt. **Starten Sie Ihre kostenlose 30-Tage-Testversion.**

ZUSÄTZLICHE RESSOURCEN

Webinar: Schützen und skalieren Sie Atlassian-Produkte in der Cloud
Statten Sie Ihr Team mit Tools für die Zusammenarbeit aus und erhöhen Sie die Sicherheit Ihrer Unternehmensdaten. In diesem Webinar erhalten Sie einen umfassenden Überblick über Identität und Sicherheit in Atlassian Cloud und lernen die wichtigsten Strategien zur Erhöhung der Sicherheit und zur Straffung der Benutzerverwaltungsprozesse kennen.

Blog: 7 nicht verhandelbare Praktiken für Cloud-Produkte
Die Implementierung von Best Practices für die Sicherheit Ihrer Cloud-Produkte fühlt sich möglicherweise so an, als würden Sie eine Partie Schach gegen einen Schachgroßmeister spielen. Sie denken, dass Sie die komplexesten Strategien kennen und zehn Züge im Voraus planen müssen, aber in Wirklichkeit spielen Sie gegen einen drittklassigen Damespieler.

Dokumentation: Best Practices für Sicherheit in der Cloud
Wenden Sie diese Best Practices an, um ein starkes Fundament für die Sicherheit der wichtigsten Daten Ihres Unternehmens zu schaffen.

ATLASSIAN