ATLASSIAN

Le guide Atlassian sur la gestion des identités dans le cloud et la gouvernance des accès

Sommaire

La transformation digitale gagne du terrain dans les organisations de toutes tailles, élargissant leurs capacités et ouvrant la voie à de nouvelles opportunités.

La clé pour tirer pleinement parti de ce nouveau monde numérique ? Faciliter la collaboration au sein d'une organisation. Pour prendre de bonnes décisions, les bonnes personnes doivent être connectées aux bonnes informations, et rapidement. Les plans doivent être partagés, les tickets critiques doivent être remontés, et les décisions doivent être documentées, stockées et facilement trouvables.

De plus en plus, tout ce processus (et les données associées) se déroule dans le cloud.

Contrairement à l'ancien monde où les logiciels sur site étaient derrière un pare-feu et où les organisations ne travaillaient qu'avec une poignée d'apps gérées de manière centralisée, les équipes individuelles adoptent aujourd'hui des outils cloud qui résolvent des problèmes métier spécifiques. Souvent, elles intègrent plusieurs apps via des API et communiquent des données précieuses (et parfois sensibles) à plusieurs fournisseurs de logiciels.

Cela nous amène au plus grand défi de l'informatique moderne : assurer la sécurité des données de votre organisation sur un nombre croissant d'apps et de points de terminaison.

La migration des ressources sensibles de votre organisation vers le cloud nécessite un contrôle différent (et plus strict) sur les employés en mesure d'accéder à ces apps et services cloud. Cet aspect de la gouvernance informatique (et de la gestion des identités et des accès ou IAM) est essentiel pour relever le plus grand défi de la transformation digitale.

Dans ce guide, nous aborderons les changements importants de l'IAM à mesure que les organisations ont migré vers le cloud, notamment :

- **en quoi l'approche d'IAM Cloud a été reconceptualisée des solutions sur site vers le cloud et des outils vers les processus ;**
- **les avantages de l'IAM Cloud en termes d'automatisation, de productivité et de sécurité ;**
- **comment vous lancer avec l'IAM Cloud et élaborer un plan d'action pour le changement ;**
- **comment les produits Atlassian Cloud s'intègrent dans votre approche d'IAM Cloud.**

Gestion des identités et des accès dans le cloud : introduction

Gestion des identités et des accès dans le cloud : introduction

Qu'est-ce que la gestion des identités et des accès dans le cloud ?

La gestion des identités et des accès dans le cloud, ou IAM Cloud, englobe les outils et les processus qui permettent de gérer les identités des utilisateurs et de contrôler les accès aux apps sur site et dans le cloud. La meilleure approche d'IAM Cloud offre un espace centralisé pour gérer les identités des utilisateurs et fonctionne dans des environnements hétérogènes, permettant l'accès à toute ressource informatique, quels que soient la plateforme de système d'exploitation, le protocole d'authentification, l'emplacement ou le fournisseur.

En quoi la gestion des identités dans le cloud diffère-t-elle de la gestion des identités sur site ?

La gestion des identités dans le cloud a été reconceptualisée à partir des solutions originales créées il y a vingt ans. À l'époque, la plupart des ressources informatiques étaient gérées sur site, derrière le pare-feu, à l'aide des systèmes et apps d'un fournisseur unique (le plus souvent, Microsoft). Ces systèmes étaient conçus pour gérer quelques apps, et non des centaines. À présent, ils ne peuvent simplement plus répondre aux exigences informatiques actuelles.

Par comparaison, les systèmes actuels de gestion des identités dans le cloud :

- sont proposés en tant que produits SaaS, qui s'intègrent à différents types de systèmes ;
- sont accessibles à partir de plusieurs types d'appareils ;
- vous permettent d'unifier vos politiques de gestion des identités et des accès ;
- sont conçus pour suivre les exigences d'accès en constante évolution.

Mais la gestion des identités des utilisateurs dans le cloud ne se résume pas à l'implémentation de nouveaux outils d'IAM Cloud et à la cartographie du parcours de migration depuis vos anciens systèmes sur site. Au-delà des nouveaux outils, vous devrez créer de nouvelles politiques, mettre à jour les politiques existantes et, surtout, prévoir l'évolution de votre organisation pour vous assurer que vous êtes prêt à soutenir une croissance continue.

Gestion des identités et des accès dans le cloud : avantages

- **Gestion centralisée pour les environnements hétérogènes**
  La gestion des identités dans le cloud remplace l'approche fragmentée des systèmes et outils sur site, et fonctionne en toute transparence avec toutes les ressources de l'organisation informatique : macOS, Linux, AWS, apps web, Wi-Fi… tout ce que l'organisation considère comme le plus adapté à ses besoins.
- **Provisionnement automatisé des utilisateurs et politiques de sécurité obligatoires**
  Les solutions d'IAM modernes vous permettent de centraliser la gestion des accès utilisateur entre les environnements sur site et cloud. Vous pouvez automatiser le provisionnement pour simplifier l'intégration et, à mesure que les employés et sous-traitants quittent l'entreprise, vous pouvez clôturer leur accès immédiatement, en vous assurant que les politiques de sécurité sont respectées.
- **Gestion obligatoire des accès contextuels**
  Automatisez les décisions d'accès dynamiques en fonction des facteurs de risque assignés au-delà du rôle assigné à l'utilisateur, notamment l'emplacement, le réseau, les restrictions relatives aux appareils, le type de demande et le moment.
- **Productivité accrue pour les utilisateurs finaux ainsi que pour l'équipe informatique**
  Grâce à un fournisseur d'authentification unique ou SSO (qui doit être un élément clé de votre approche d'IAM Cloud, plus d'informations à ce propos ultérieurement), les utilisateurs peuvent facilement trouver toutes leurs apps d'entreprise et s'y connecter à partir d'un tableau de bord unique.

Se lancer avec l'IAM Cloud

Si vous êtes prêt à migrer vers le cloud et à centraliser votre gestion des identités et des accès, le choix d'une solution de fournisseur d'identité (IdP) n'est pas aussi simple que l'achat d'un logiciel lambda. Vous devrez prendre en compte plusieurs facteurs clés lorsque vous vous lancerez dans votre recherche :

1. **Soyez prévoyant.**
   Définissez les objectifs de votre organisation en termes de croissance et d'évolution afin de vous assurer que votre nouveau système IAM vous permettra de les atteindre.

2. **Réfléchissez à votre point de départ.**
   Cela vous aidera à hiérarchiser les fournisseurs potentiels sur lesquels faire des recherches. Dans la plupart des cas, les organisations informatiques qui souhaitent migrer vers le cloud se répartissent en trois catégories :

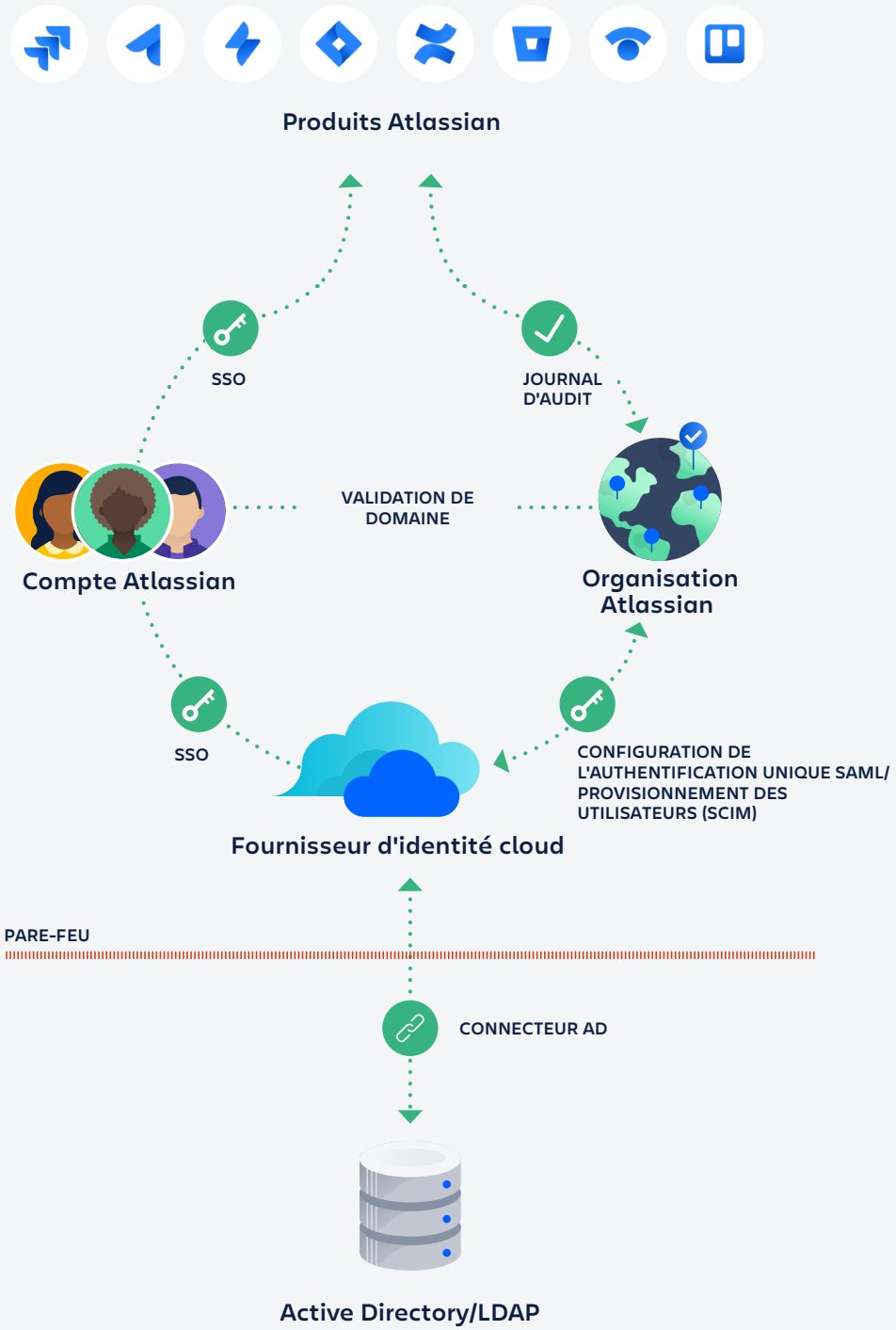
   - Celles qui utilisent actuellement un système d'annuaire LDAP sur site et souhaitent migrer vers le cloud.
   - Celles qui utilisent une installation Microsoft Azure Active Directory (AD) et souhaitent migrer vers le cloud, souvent dans le but de gérer un environnement hétérogène.
   - Celles qui n'utilisent actuellement pas d'annuaire utilisateur pour gérer les identités des utilisateurs.

3. **Faites le point sur vos environnements informatiques actuels.**
   Notez tous les protocoles, toutes les plateformes et tous les réseaux de votre infrastructure de sorte à assurer l'interopérabilité avec vos systèmes.

4. **Répertoriez toutes les apps de fournisseurs ainsi que tous les outils SaaS, et déterminez ceux qui sont essentiels pour l'entreprise.**
   Identifiez toutes les apps pour lesquelles vous devrez gérer les accès, en particulier lorsque vous vous lancerez dans l'élaboration d'un plan d'intégration par ordre de priorité.

> **Bonne nouvelle**
> Lorsque vous avez une vision claire de vos exigences et de vos priorités, votre recherchede la bonne combinaison d'outils de fournisseurs IAM a plus de chances de se dérouler sans encombre. De plus, puisque vous transférez ce processus IAM vers le cloud, vous n'aurez pas besoin d'investir à long terme dans du nouveau matériel ou des ressources internes pour gérer la sécurité ou les correctifs. Ce travail sera effectué pour vous par vos fournisseurs cloud.

Cerner l'environnement IAM Cloud



Une fois que vous avez sélectionné votre fournisseur d'identité (IdP) cloud, il est important de comprendre comment celui-ci s'intègre à l'environnement global de vos apps sur site et cloud. Voici certains éléments à prendre en compte pour cet environnement de gestion des identités dans le cloud :

- **Identifiez votre outil d'administration des profils**
  Tout d'abord, identifiez votre outil d'administration des profils (profile master), l'app qui sera votre source de référence unique pour les utilisateurs et les groupes. Une option consiste à administrer vos utilisateurs et groupes directement dans votre fournisseur d'identité cloud. Une autre option est de les administrer dans votre système d'informations RH, comme Workday.
  - **Connectez votre fournisseur d'identité (IdP) cloud à votre annuaire sur site**
    Dans ce diagramme, nous avons défini la source de référence pour l'administration des profils sur une base de données Active Directory ou LDAP sur site. Dans ce cas, vous devez pouvoir connecter votre fournisseur d'identité cloud à votre service d'annuaire hébergé sur votre réseau. Tous les grands fournisseurs d'identité cloud proposent des agents ou des connecteurs qui fonctionnent au sein de votre réseau d'entreprise pour faciliter la synchronisation entre le fournisseur d'identité cloud et les utilisateurs et groupes de votre annuaire Active Directory ou LDAP, qui est votre source de référence unique. Si vous disposez d'un annuaire Active Directory ou LDAP dans votre système sur site, vous pouvez toujours l'utiliser pour gérer les identités et les accès avec vos apps sur site.
  - **Authentifiez-vous aux apps cloud via votre fournisseur d'identité cloud**
    Vous pouvez connecter vos apps dans le cloud à votre fournisseur d'identité cloud, et vos utilisateurs peuvent accéder à ces apps et s'y authentifier depuis l'Internet public, via des protocoles tels que l'authentification unique (SSO) SAML.
- **Gérez l'accès des utilisateurs aux apps Atlassian via votre fournisseur d'identité cloud et l'authentification unique**
  Votre fournisseur d'identité cloud peut également proposer une authentification SSO entre les organisations Atlassian et lui-même via l'authentification unique SAML à l'aide de leur compte Atlassian. Lorsque les utilisateurs accèdent aux apps Atlassian, comme Jira Software Cloud, via leur compte Atlassian, ils sont redirigés vers votre fournisseur d'identité pour se connecter.
- **Provisionnez de nouveaux utilisateurs Atlassian via votre fournisseur d'identité cloud**
  De même, vous pouvez provisionner les utilisateurs et les groupes qui existent dans votre fournisseur d'identité cloud (qui a été initialement synchronisé à partir de votre annuaire Active Directory sur site local) dans votre organisation Atlassian. Ces groupes sont ensuite transmis en aval aux apps que vous avez liées à votre organisation Atlassian, ce qui permet de maintenir la synchronisation des identités.

Implémenter votre stratégie d'IAM Atlassian Cloud

Implémenter votre stratégie d'IAM Atlassian Cloud

Chez Atlassian, nous avons vécu notre propre transformation digitale, et nous comprenons donc toutes les difficultés que votre organisation peut rencontrer lors de cette transition.

Nous avons créé un framework de bonnes pratiques qui nous a aidés, nous et nos clients, à surmonter certains problèmes auxquels les équipes informatiques sont confrontées dès qu'il est question de collaborer au sein d'une organisation à grande échelle, tout en maintenant tous les protocoles de sécurité adéquats en place.

Dans ce framework, nous avons créé des recommandations qui vous aident à :

Centraliser votre gestion des identités utilisateur dans une source de référence unique.

Intégrer vos apps à votre fournisseur d'identité principal pour une sécurité et une efficacité accrues.

Mettre en place l'authentification à deux facteurs (2FA) obligatoire ou des règles de mot de passe si vous ne disposez pas d'un fournisseur d'identité qui s'en charge pour vous.

Surveiller régulièrement les accès, les autorisations et les journaux d'audit des utilisateurs.

Centraliser les informations pour créer une source de référence unique

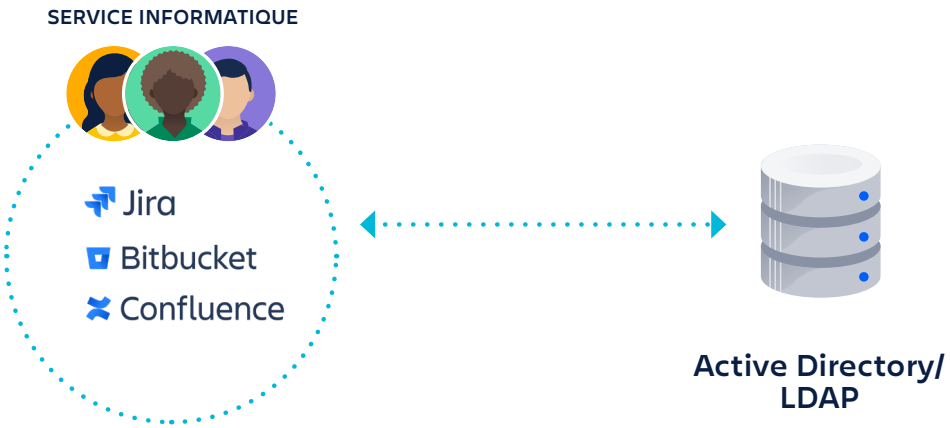
Appliquez des politiques et contrôlez les coûts grâce à la gestion centralisée des identités et des accès

Les produits Atlassian Cloud comme Jira Software, Jira Service Desk, Confluence, Bitbucket, Trello et Opsgenie font généralement l'objet d'une adoption « ascendante » dans les entreprises, à l'instar de nombreuses autres apps SaaS. Les abonnements sont achetés par les services, en contournant les achats informatiques et les processus d'approbation de la sécurité et de la confidentialité. Afin de contrôler les coûts et d'appliquer les politiques, les administrateurs informatiques doivent centraliser la gestion de toutes ces apps cloud en un seul et même système.

Univers Server et Cloud d'Atlassian : différents concepts de gestion des identités et des accès

Voici une comparaison entre ce à quoi ressemble la gestion des identités et des accès dans un environnement Atlassian Server sur site type et dans un environnement Atlassian Cloud. Vous remarquerez que les intégrations de données entre les apps sont différentes dans l'environnement Server et l'environnement Cloud, ainsi que le concept de gestion des identités.

Si les produits Atlassian sont utilisés sur site, l'environnement ressemble à cela :



Vous disposez d'une instance « entreprise » de chaque produit, gérée par le service informatique. Toutes les instances sont connectées à l'annuaire Active Directory ou LDAP de votre entreprise, deux des méthodes de gestion des identités des utilisateurs les plus courantes.

Dans le cloud, atteindre le même niveau de gouvernance peut s'avérer compliqué. Il se peut que plusieurs services utilisent leurs propres instances de produits cloud. Le service informatique peut avoir ses propres apps Jira Service Desk et Confluence, et le service d'ingénierie a sa propre instance de Jira Software ainsi qu'un dépôt Bitbucket.

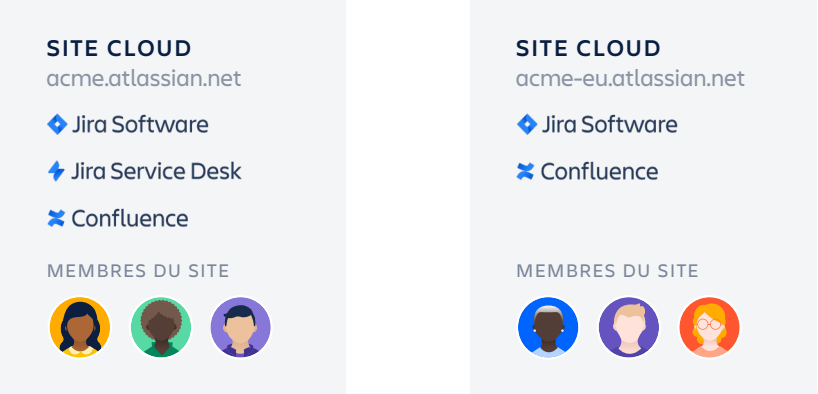
Entre-temps, vous découvrez que les personnes du service marketing ont adopté Trello. Et pendant tout ce temps, certaines de vos équipes utilisent des outils tels que Slack et Office 365.

Qui sont toutes ces personnes et à quoi ont-elles accès ? Lorsque vous avez autant d'apps non gérées en service, il est impossible de savoir.

De plus, dans l'univers Atlassian Cloud, les utilisateurs ont un seul compte par adresse e-mail. Chaque utilisateur dispose d'une identité d'entreprise et d'un mot de passe, et ne doit configurer l'authentification à deux facteurs qu'une seule fois, que ce soit pour une instance Jira Cloud ou pour l'instance Confluence d'un partenaire. Cela signifie qu'un administrateur ne doit gérer qu'un seul ensemble d'identifiants par utilisateur, et que chaque utilisateur peut accéder à tous les produits Atlassian Cloud avec un seul ensemble d'identifiants, ce qui simplifie considérablement la gestion des identités pour toutes les personnes impliquées.

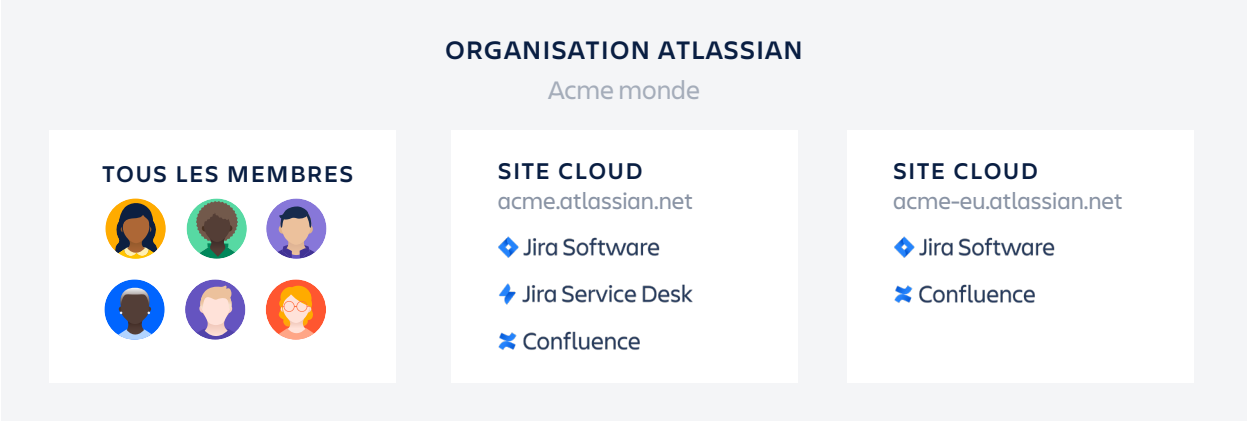
Affichez et gérez tous les utilisateurs au sein de votre entreprise grâce aux organisations et à la validation de domaine

Vous connaissez peut-être les ***sites***, un concept que nous utilisons pour la gamme de produits Jira et Confluence qui vous permet de gérer les accès aux différents produits et de partager des groupes ainsi que d'autres paramètres au sein du site. Lorsque vous configurez votre instance Jira ou Confluence, vous pouvez nommer votre site. L'URL que vous utilisez pour accéder à votre instance est alors générée.



Au sein d'une même organisation, différentes équipes peuvent utiliser plusieurs sites et produits Atlassian Cloud. Une équipe à San Francisco peut utiliser Jira Software sur un site, alors que l'équipe du bureau de New York utilise Jira Service Desk sur un autre. Et les ingénieurs à travers le monde peuvent utiliser leurs comptes Bitbucket individuels pour stocker leur code. En tant qu'administrateur, vous avez besoin d'un espace où voir tous les utilisateurs d'Atlassian Cloud dans votre organisation, quel que soit le site ou le produit.

Pour permettre de gérer plusieurs produits Atlassian Cloud et plusieurs sites en un seul et même endroit, nous avons créé une couche d'administration globale appelée ***organisations.***



Les organisations vous offrent une vue unifiée de tous les utilisateurs d'apps Atlassian Cloud en service dans votre entreprise.

Et puisque vous pouvez avoir plusieurs sites, nous avons créé une plateforme qui rassemble les organisations, appelée le hub d'administration Atlassian, ou **admin.atlassian.com**.

Dans une organisation, vous pouvez gérer tous les utilisateurs de votre organisation sous les versions Cloud de Jira Software, Jira Service Desk, Jira Core, Confluence et Bitbucket via un processus appelé ***validation de domaine***.

Une fois que vous avez confirmé être propriétaire de votre domaine, vous commencerez à gérer chaque utilisateur qui dispose d'une adresse e-mail sur votre domaine et connu d'Atlassian. Nous appelons cela des comptes gérés. En tant qu'administrateur de l'organisation, vous pourrez exporter, modifier, désactiver et supprimer ces comptes gérés. Vous pourrez également appliquer les politiques de sécurité d'**Atlassian Access** sur vos comptes gérés.

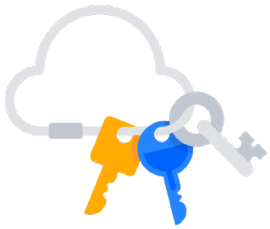
AU SEIN DES ORGANISATIONS :
GESTION CENTRALISÉE DES UTILISATEURS POUR VOS PRODUITS CLOUD

Une fois votre organisation configurée, vous trouverez des outils qui peuvent vous aider à gérer les produits ainsi que les utilisateurs :

- **Annuaire :** inclut une liste des comptes que vous gérez, en supposant que vous avez **validé vos domaines**. C'est également là que vous pouvez connecter votre fournisseur d'identité pour le provisionnement des utilisateurs. **En savoir plus**
- **Sécurité :** bénéficiez de fonctionnalités supplémentaires de contrôle et de sécurité en **vous abonnant à Atlassian Access**. Vous pourrez alors tirer pleinement parti des organisations. **En savoir plus**
- **Paramètres :** actualisez vos informations, désignez un administrateur de l'organisation, ajoutez un autre domaine et créez une clé API. **En savoir plus**
- **Sites et produits :** consultez tous les produits que vous utilisez ainsi que leurs sites. C'est dans cet espace que vous pourrez administrer les utilisateurs et actualiser les groupes ainsi que les accès aux produits. **En savoir plus**

En plus d'administrer votre organisation à partir du site d'administration, vous pouvez utiliser l'**API REST de l'organisation** pour récupérer des informations relatives à votre organisation, telles que tous ses utilisateurs et domaines.

Intégrez Atlassian Access à votre fournisseur d'identité



Activez l'authentification unique (SSO) pour une sécurité accrue et une connexion simplifiée pour les utilisateurs finaux

La mesure la plus importante que vous puissiez prendre pour sécuriser vos comptes utilisateur est de configurer l'authentification unique (ou SSO) SAML. Vous pouvez vous assurer que chaque utilisateur est connecté et respecte vos exigences relatives aux mots de passe forts et à l'authentification multiple. Vous pouvez également vous assurer qu'ils sont connectés depuis des emplacements et appareils approuvés, le tout via votre fournisseur d'authentification unique.

Lorsque vous faites appel à un fournisseur d'identité cloud pour l'authentification unique, vous pouvez aller plus loin que le simple contrôle de l'authentification. Vous pouvez également contrôler qui dispose d'un accès à quelles données. Vous pouvez assigner des niveaux d'autorisation aux utilisateurs individuels, non seulement pour les produits Atlassian Cloud, mais pour toutes vos apps SaaS.

Prenez en charge les principaux fournisseurs d'identité (de nouveaux viendront bientôt s'ajouter à la liste)

Combinés à un abonnement à Atlassian Access, les produits Atlassian Cloud prennent en charge cinq des fournisseurs d'identité les plus courants, ainsi que la configuration d'une connexion SAML personnalisée via n'importe quel fournisseur d'identité non répertorié ci-dessous. Grâce à un fournisseur d'identité, vous pouvez vous assurer que l'utilisation de tous les produits Atlassian passe par un terminal d'authentification que vous contrôlez, ce qui vous permet de faire un pas de plus vers le respect de vos exigences de sécurité.

BITIUM · Cloud Identity · idaptive

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

SE LANCER AVEC L'AUTHENTIFICATION UNIQUE SAML

Pour configurer l'authentification unique SAML pour les produits Atlassian Cloud, créez votre organisation, validez votre domaine, puis démarrez votre essai **Atlassian Access**. Vous pourrez ensuite suivre ces instructions pour configurer l'**authentification unique SAML**.

Automatisez la gestion du cycle de vie des utilisateurs grâce au provisionnement des utilisateurs (SCIM)

À mesure que votre entreprise se développe et que le nombre de personnes dans vos systèmes augmente, il est logique de migrer d'un provisionnement manuel vers une gestion automatisée des accès, qui est axée sur des politiques, via votre fournisseur d'identité. Cela offre à l'équipe informatique une vue centralisée des autorisations assignées à chaque utilisateur, et cela vous permet d'automatiser le provisionnement et le déprovisionnement des utilisateurs, mais aussi d'assigner automatiquement des règles en fonction des attributs de l'utilisateur ou du groupe qui déterminent qui a accès à quelles apps.

Pour simplifier le provisionnement des utilisateurs, nous utilisons un protocole connu sous le nom de SCIM. Il vous permet de gérer les identités des utilisateurs grâce à un fournisseur d'identité tel que Okta, Azure AD ou OneLogin, et de synchroniser ensuite ces informations avec vos produits Atlassian. Par exemple, vous pouvez assigner un utilisateur aux apps Atlassian dans Okta, et Access détectera automatiquement les changements qu'il synchronisera avec les instances Jira ou Confluence de votre choix.

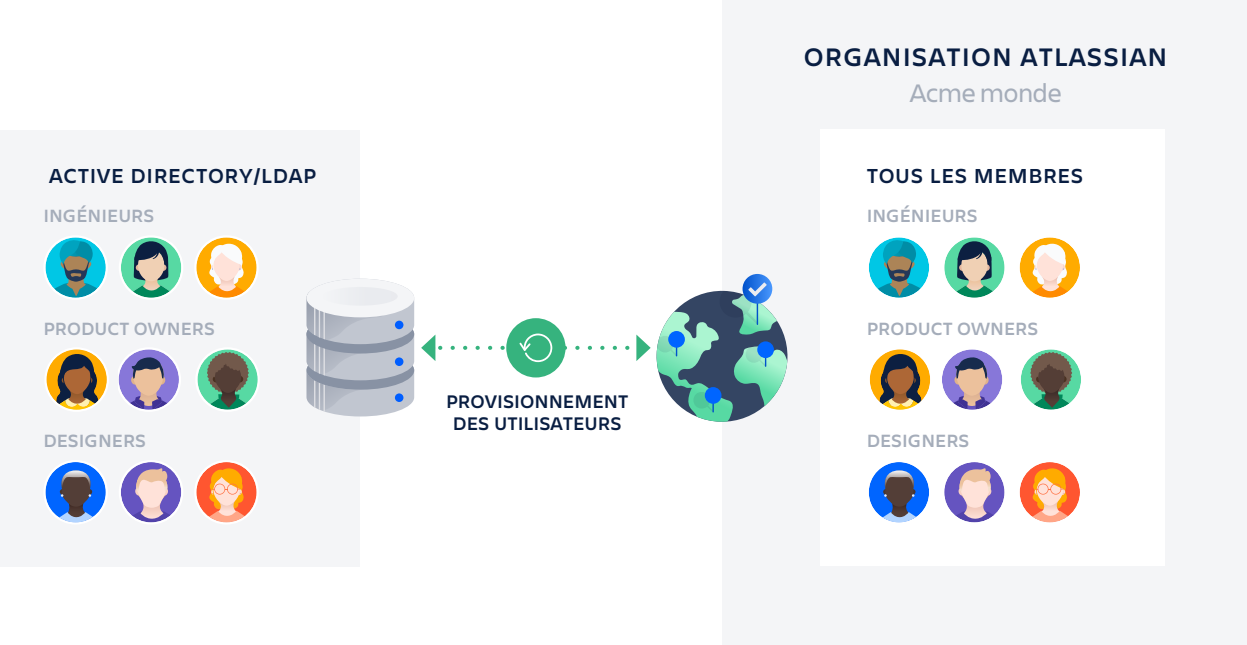
Provisionnement des utilisateurs : avantages

- **Automatisez l'intégration et le départ d'employés**
  Grâce à la synchronisation directe avec votre fournisseur d'identité, vous ne devez plus créer manuellement de comptes utilisateur lorsqu'une personne rejoint l'entreprise.
- **Gérez les accès et les autorisations**
  Vous pouvez contrôler l'accès d'une personne aux projets Jira ainsi que sa capacité à voir certains tableaux de bord ou filtres. Vous pouvez également consulter et modifier des pages Confluence grâce aux groupes synchronisés à partir de votre fournisseur d'identité.
- **Gérez les coûts grâce au déprovisionnement automatique**
  En automatisant le processus de déprovisionnement lorsque des personnes quittent l'entreprise, vous pouvez vous assurer de ne pas être facturé pour des licences dont vous n'avez pas besoin.
- **Réduisez les risques de violation de données**
  Grâce au déprovisionnement automatique, l'accès des anciens employés est automatiquement supprimé lorsqu'ils quittent l'entreprise.

Synchronisez les utilisateurs et les groupes avec votre organisation

Ce diagramme illustre la façon dont les utilisateurs et les groupes se synchronisent une fois que vous avez configuré le provisionnement des utilisateurs. Une fois votre fournisseur d'identité connecté à votre organisation, les utilisateurs et les groupes de votre fournisseur d'identité sont synchronisés avec vos produits Atlassian Cloud.

- Les utilisateurs et les groupes sont synchronisés entre votre fournisseur d'identité et votre organisation, ce qui crée un annuaire de vos utilisateurs provisionnés.
- L'annuaire de votre entreprise se synchronise avec tous les sites associés, ce qui fournit un accès à vos utilisateurs et groupes provisionnés.
- Les groupes sont assignés à des produits, ce qui octroie aux utilisateurs de chaque groupe un accès par défaut aux produits.



SE LANCER AVEC LE PROVISIONNEMENT DES UTILISATEURS ET LA GESTION DU CYCLE DE VIE

Pour configurer le provisionnement des utilisateurs pour les produits Atlassian Cloud, créez votre organisation, validez votre domaine, puis **démarrez votre essai d'Atlassian Access**. Vous pourrez ensuite suivre ces instructions pour configurer le **provisionnement des utilisateurs**.

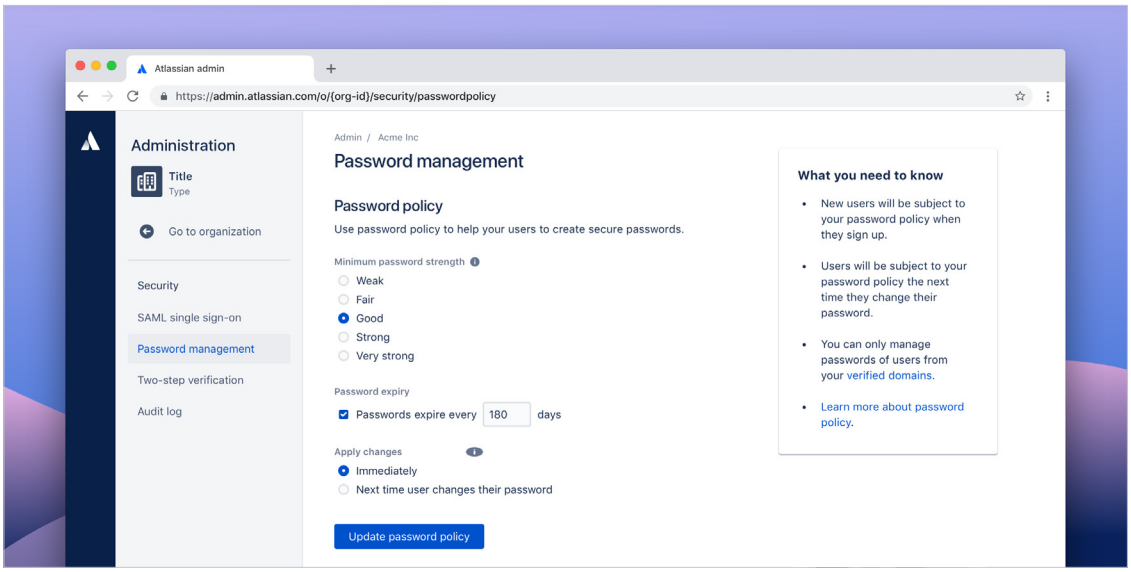
Appliquer les politiques de sécurité

Sécurisez votre compte grâce à la validation en deux étapes

La plupart des fournisseurs d'identité gèrent l'authentification à deux facteurs (2FA). Mais si vous ne disposez pas d'un fournisseur d'identité cloud, vous pouvez utiliser Atlassian Access pour configurer et gérer les utilisateurs d'une organisation Atlassian. La validation en deux étapes ajoute une deuxième étape de connexion pour vos comptes utilisateur Atlassian gérés, qui exige de saisir un code à six chiffres en plus du mot de passe lors de la connexion. La deuxième étape permet de sécuriser leurs comptes, même si le mot de passe est compromis. Lorsque les connexions aux comptes sont sécurisées, les produits et ressources de votre organisation sont plus sûrs.

Appliquez des règles de mot de passe fort pour tous les utilisateurs

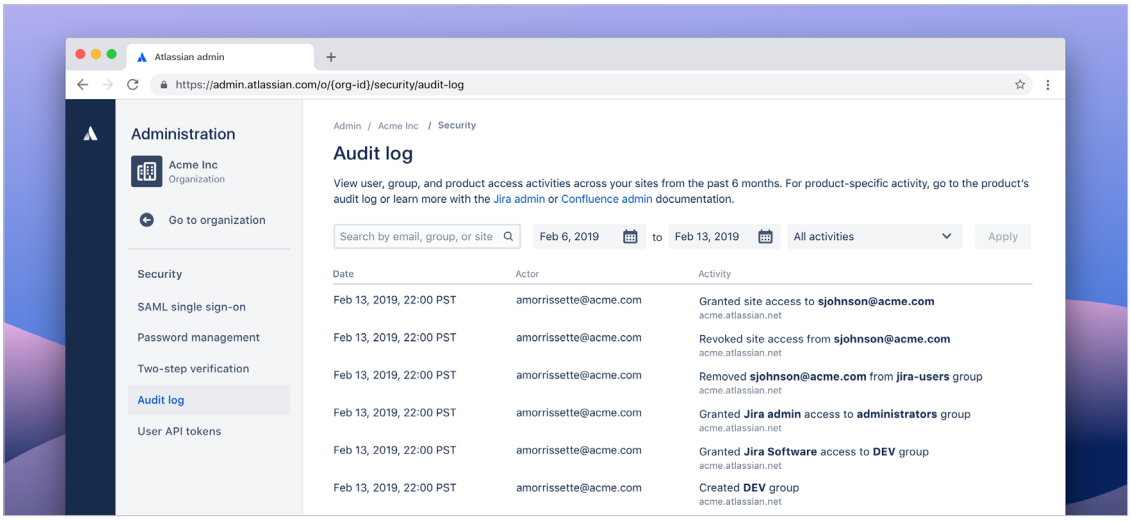
Si vous n'utilisez pas de fournisseur d'identité pour activer l'authentification unique, Atlassian Access peut également vous aider à appliquer des règles de mot de passe plus fort à tous vos utilisateurs. Les règles de mot de passe permettent de s'assurer que les personnes qui accèdent à vos produits Atlassian Cloud appliquent les bonnes pratiques lors de la création de mots de passe. Cela permet de réduire le risque de violations de la sécurité.



SE LANCER AVEC LES BONNES PRATIQUES POUR SÉCURISER VOS COMPTES

Pour appliquer la validation en deux étapes et les règles de mots de passe au sein de vos produits Atlassian Cloud, créez votre organisation, validez votre domaine, puis **démarrez votre essai d'Atlassian Access**. Vous pourrez ensuite suivre ces instructions pour configurer la **validation en deux étapes obligatoire** et les **règles de mots de passe**.

Surveiller les autorisations et activités des utilisateurs



Suivez les adhésions, les activités et les autorisations en un seul et même endroit grâce aux journaux d'audit

Les journaux d'audit sont un moyen essentiel de prouver la conformité à diverses réglementations et politiques internes. Grâce à Atlassian Access, vous pouvez à présent obtenir des journaux d'audit à l'échelle de l'organisation pour une visibilité améliorée sur les changements apportés aux utilisateurs et aux groupes au sein de vos produits Jira et Confluence. Ces journaux d'audit vous permettent de voir des informations, notamment qui a apporté des changements, les utilisateurs et les adhésions aux groupes, qui a demandé l'accès à ces différents groupes, et plus encore.

Grâce à une organisation Atlassian, les administrateurs peuvent également voir qui a accès aux jetons d'API, qui les a créés, le nombre de jetons créés, ainsi que le dernier accès à un jeton. Ils peuvent également révoquer un jeton.

Ces informations étant disponibles dans votre organisation Atlassian, vous disposez d'une vue complète et documentée des personnes qui ont accès à vos données, ce qui peut simplifier les enquêtes sur les changements et aider à prouver la conformité.

OBTENEZ UNE VISIBILITÉ SUR LES PERSONNES QUI ONT ACCÈS À VOS DONNÉES

Pour afficher les journaux d'audit au sein de vos produits Atlassian Cloud, créez votre organisation, validez votre domaine, puis **démarrez votre essai d'Atlassian Access**.

Étapes suivantes pour implémenter l'IAM Atlassian

1. **Élaborez** un plan qui présente les objectifs de croissance de votre organisation, de sorte à pouvoir prioriser les exigences pour votre nouveau système d'IAM.
2. **Examinez** les fournisseurs d'identité ainsi que l'environnement de gestion des identités et des accès, et déterminez les types d'outils dont vous avez besoin.
3. **Identifiez** les nouvelles politiques ou les politiques actualisées que vous devrez implémenter.
4. **Choisissez** votre fournisseur d'identité ainsi que les apps cloud associées pour finaliser votre plan d'IAM.
5. **Créez** une organisation pour vos produits Atlassian Cloud et revendiquez votre domaine.
6. **Abonnez-vous** à Atlassian Access pour appliquer des politiques de sécurité.
7. **Intégrez** Atlassian Access à votre fournisseur d'identité pour l'authentification unique et le provisionnement des utilisateurs.

Découvrez comment Atlassian Access offre une visibilité à l'échelle de l'entreprise sur vos apps Atlassian Cloud, ainsi qu'une gestion unifiée des utilisateurs et des règles, une sécurité accrue, et une gestion simplifiée du cycle de vie des utilisateurs.
Démarrez votre essai gratuit de 30 jours.

RESSOURCES SUPPLÉMENTAIRES

Webinaire : Sécuriser et faire évoluer Atlassian dans le cloud
Offrez à votre équipe des outils collaboratifs, tout en améliorant la sécurité de vos données d'entreprise. Dans ce webinaire, vous cernerez parfaitement l'environnement de gestion de la sécurité et des identités d'Atlassian Cloud, et vous découvrirez des stratégies clés pour renforcer la sécurité et simplifier les processus de gestion des utilisateurs.

Billet de blog : Sept pratiques non négociables pour tout produit cloud
L'implémentation de bonnes pratiques de sécurité pour vos produits cloud peut vous donner l'impression de jouer une partie d'échecs contre un grand maître. Vous pensez devoir connaître les stratégies les plus complexes et planifier dix déplacements à l'avance, mais en réalité, votre adversaire est un enfant de primaire qui joue aux dames.

Documentation : Respectez les bonnes pratiques de sécurité dans le cloud
Utilisez ces bonnes pratiques pour créer une base solide afin de protéger le travail le plus important de votre entreprise.

ATLASSIAN