FICHE TECHNIQUE

Cloud Access Manager

Accès unifié et sécurisé pour répondre à vos enjeux

Avantages

- Accès simple et sécurisé aux applications on-prem et dans le Cloud
- Augmentation de la satisfaction et de la productivité des utilisateurs
- Permettre aux équipes IT de gérer et protéger différentes applications et divers modes d'accès
- Sécurité des accès renforcée avec l'authentification multifacteur
- Économies avec le just-in-time provisioning de Salesforce, Google Apps et Office 365
- Administration simplifiée avec une interface Web basée sur des assistants
- Utilisation de toutes les fonctionnalités offertes par les protocoles OAuth 2.0 et OpenID Connect

Configuration requise

Pour obtenir les détails de la configuration requise, consultez la page oneidentity.com/cloud-access-manager

Il y a quelques années, lorsque tous les utilisateurs et toutes les applications d'une entreprise se trouvaient sur site, le contrôle des accès était simple. Aujourd'hui, les salariés, les partenaires et les clients accèdent aux applications depuis les quatre coins du globe et utilisent des appareils qui ne cessent de se diversifier. Il ne s'agit pas uniquement des applications développées et/ou hébergées en interne, mais aussi des applications basées dans le Cloud telles que Salesforce.com®, Google® Apps™ et Microsoft® Office 365®. Parallèlement, les exigences de sécurité croissent aussi vite, si ce n'est plus rapidement, que les attentes des utilisateurs qui souhaitent bénéficier d'un accès fluide.

C'est donc à l'équipe IT qu'il incombe d'octroyer aux utilisateurs l'accès dont ils ont besoin, lorsqu'ils en ont besoin, tout en veillant à ce que tous les accès soient adaptés, sécurisés et conformes aux stratégies de sécurité. Pour ce faire, il faut réussir à assurer la sécurité et la gestion de tous les accès à la fois, qu'importe le type d'utilisateur, l'emplacement ou le type d'application.

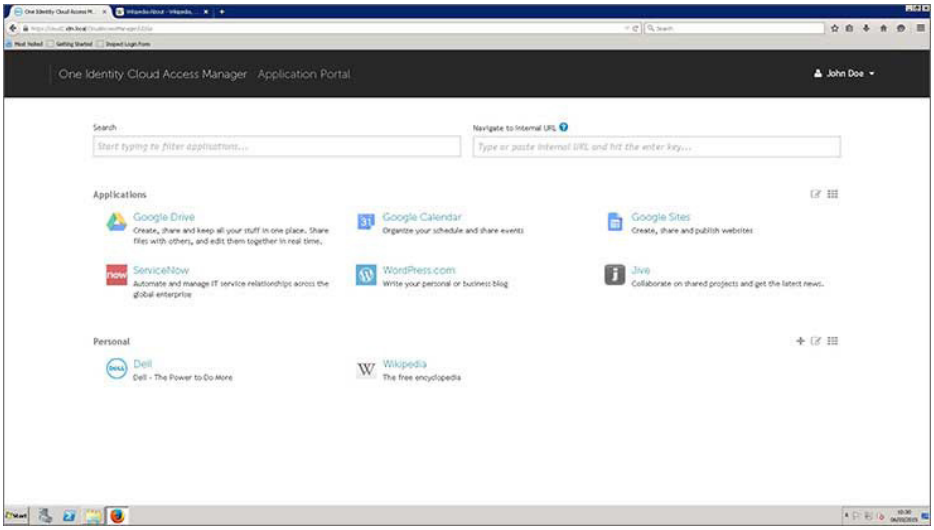
ONE IDENTITY

Avec Cloud Access Manager, de la gamme de produits One Identity, vous pouvez fournir à vos utilisateurs l'accès aux ressources internes, aux applications mobiles personnalisées et aux applications Web basées dans le Cloud dont ils ont besoin depuis un navigateur, tout en améliorant la sécurité et l'efficacité de l'équipe IT. La solution Cloud Access Manager offre des fonctions d'authentification unique (SSO, Single Sign-On), de sécurité contextuelle (ou adaptative), de just-in-time provisioning du Cloud, de fédération, ainsi que d'autorisation et d'audit pour de nombreux types d'applications et scénarios d'accès.

Fonctionnalités

Authentification centralisée, authentification unique et récupération d'attributs

Abandonnez les répertoires dédiés axés sur les applications et échappez à la charge administrative qu'ils représentent en connectant les répertoires et les applications à une plateforme d'authentification centralisée. Désormais, une authentification login + mot de passe permet de créer une session SSO incluant plusieurs applications Web on-prem ou en SaaS ainsi que vos propres applications mobiles via le protocole OpenID Connect. Les technologies permettant d'intégrer les applications sont nombreuses : injection des informations d'identification, HTTP headers, jetons de sécurité SAML (Security Assertion Markup Language), connexion aux médias sociaux conforme au protocole OAuth via Google, Microsoft Live ID, Facebook et Twitter. À l'aide d'un puissant moteur basé sur des règles, la solution Cloud Access Manager peut fournir aux applications protégées des informations complémentaires sur les utilisateurs afin d'affiner le contrôle des accès.



Cloud Access Manager offre une expérience de connexion unifiée pour tout type d'applications : développées en interne, basées sur un navigateur, Web, mobiles basées sur OpenID Connect et SaaS.

Sécurité contextuelle

Identifiez qui accède à quoi, à quel moment et à quel emplacement et mettez en place votre stratégie de sécurité à l'aide du moteur d'analyse de la sécurité (SAE, Security Analytics Engine). Inclus avec Cloud Access Manager, ce moteur collecte des informations à partir de différentes sources pour fournir du contexte et faciliter la prise de décisions relatives aux accès ainsi que leur application. Les informations contextuelles collectées par le moteur SAE portent sur les éléments suivants :

- Navigateur utilisé : analyse de l'historique des navigateurs utilisés afin d'identifier un comportement anormal
- Modèle de géolocalisation : détection des tentatives d'accès à partir d'un emplacement inhabituel
- Emplacement géographique spécifique : blocage des tentatives d'accès à partir de zones géographiques spécifiques connues pour lancer des attaques malveillantes
- Appartenance à un groupe
- Historique des échecs de tentative d'authentification
- Heure : détection des tentatives d'accès qui ne correspondent pas à une utilisation normale
- Liste noire : inventaire des réseaux ou adresses réseau interdits
- Liste blanche : inventaire des réseaux ou adresses réseau approuvés

Authentification multifacteur

La solution Cloud Access Manager prend en charge l'authentification multifacteur comme principale source de connexion et pour l'authentification renforcée imposée par les scores de risque générés par le moteur SAE. Les options disponibles pour l'authentification multifacteur incluent le déploiement sur site de l'outil Defender et le déploiement SaaS de la solution Defender as a Service.

Contrôles d'accès basés sur les politiques de sécurité

Évitez les stratégies de sécurité ponctuelles incohérentes et assurez-vous que les utilisateurs peuvent accéder seulement aux ressources auxquelles ils ont accès en fonction des rôles définis par le département informatique. Les rôles et appartenances aux rôles peuvent être attribués de manière dynamique en fonction de politiques évaluées en temps réel à l'aide de données d'identité existantes. Le contrôle d'accès basé sur des règles peut être appliqué jusqu'aux sous-régions d'une application Web, de manière à implémenter un processus d'autorisation granulaire.

Offrez à vos utilisateurs l'accès aux ressources internes et aux applications Web basées dans le Cloud à l'aide d'une fonction d'authentification unique, tout en améliorant la sécurité et l'efficacité de l'équipe informatique.

Fédération des identités

Garantissez une sécurité cohérente pour différents scénarios d'accès (applications hébergées dans le Cloud, collaboration entre forêts, plateformes hétérogènes, extranets de partenaires) sans que les utilisateurs aient besoin d'une multitude de mots de passe superflus. La solution Cloud Access Manager peut également prendre en charge les ressources SharePoint. Avec la prise en charge de la fédération des rôles Fournisseur d'identités et Fournisseur de services, notre solution permet aux utilisateurs d'accéder plus facilement aux applications Web, indépendamment de l'emplacement des utilisateurs et/ou des applications.

Provisioning des accès au Cloud

Afin de garantir l'authentification unique sur les applications Cloud fédérées telles que Salesforce®, Google Apps ou Office 365, le provisioning des comptes d'utilisateurs doit être effectué au niveau des applications Cloud. La solution Cloud Access Manager contribue à l'amélioration de l'efficacité informatique en offrant à la fois des fonctions de provisioning des accès et d'authentification unique. Le just-in-time provisioning, qui consiste à activer les licences uniquement lorsqu'un accès est réellement utilisé, permet de réaliser des économies.

Accès distant et agrégation de l'espace de travail

Il est possible de personnaliser le portail d'applications Cloud Access Manager afin que les utilisateurs puissent trouver plus facilement toutes les applications dont ils ont besoin pour effectuer leur travail.

En fonction de leur rôle, le portail leur propose un ensemble clair de liens vers les applications qu'ils sont autorisés à utiliser. Le proxy de la solution Cloud Access Manager permet aux utilisateurs d'accéder à toutes les applications via un navigateur Web.

Audit des accès

La solution Cloud Access Manager permet aux professionnels de la sécurité de tirer parti des fonctionnalités d'authentification centralisée et de contrôle d'accès pour réaliser des audits et créer des rapports sur les événements d'accès à des fins de conformité, de répudiation et d'analyse forensique.

Cloud Access Manager prend en charge les types de connexion suivants : HTTP header, protocoles WS-Federation/Trust, jetons SAML, accès par formulaire, accès fédérés en tant que fournisseur d'identités ou de services, ainsi que les protocoles OpenID Connect et OAuth.

À propos de One Identity

La gamme One Identity de solutions de gestion des accès et des identités (IAM) inclut une offre de solutions IAM concrètes de gouvernance des identités, de gestion des accès et de gestion des comptes à privilèges axées sur l'entreprise, modulaires, intégrées et tournées vers l'avenir.

Pour en savoir plus, rendez-vous sur OneIdentity.com

Datasheet-CloudAccessManager-US-KJ-FR-WL-27053

ONE IDENTITY