



FICHE  
TECHNIQUE

# Identity Manager On Demand

Solution fournie par SaaS permettant d'éliminer les risques liés à la gestion des identités et des accès dans l'entreprise

## Avantages

- Administration et gestion des identités complètes fournies à la demande
- Gouvernez l'accès à des ressources locales, Cloud et hybrides, depuis la demande initiale jusqu'à l'exécution, pour les utilisateurs et les données
- Réduisez les risques en vous assurant que les utilisateurs disposent strictement de l'accès dont ils ont besoin
- Répondez aux initiatives d'audit et de conformité par des stratégies d'attestation et de recertification
- Placez les décisions relatives aux accès entre les mains de l'entreprise
- Appuyez-vous sur votre infrastructure et vos investissements existants pour faire évoluer votre système

## Le Cloud sans compromis

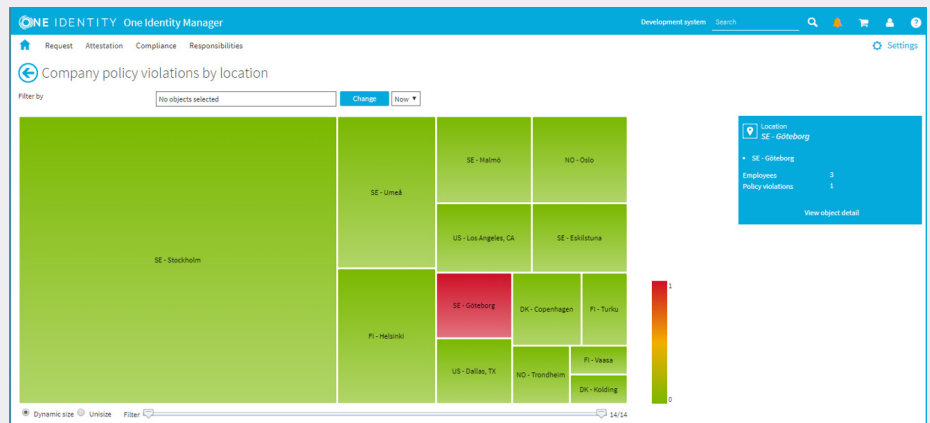
L'administration et la gouvernance des identités (IGA, Identity Governance and Administration) constituent un élément critique de toute organisation moderne et devraient être au cœur de votre stratégie de sécurité. Souvent, la plus grosse interrogation concerne le lieu de déploiement de votre solution d'IGA. Les options SaaS ont toujours eu une fonctionnalité limitée et ne pouvaient répondre aux besoins des utilisateurs, ni s'adapter aux stratégies Cloud ou encore s'intégrer entièrement à un environnement informatique existant. Et si vous pouviez avoir tous les avantages de l'IGA tout en soutenant votre stratégie Cloud ? C'est possible avec One Identity Manager On Demand. Identity Manager On Demand est doté de toute la puissance, l'efficacité et la sécurité de One Identity Manager local, le leader du secteur des solutions d'IGA d'entreprise, mais distribué depuis le Cloud. C'est un Cloud sans compromis.

Désormais, vous pouvez gagner en productivité et restreindre l'accès des utilisateurs aux seules données et applications dont ils ont besoin pour faire leur travail – et rien de plus – par l'intermédiaire d'un modèle SaaS qui ne limite ni les fonctionnalités ni le champ d'application.

Avec Identity Manager On Demand, vous pouvez unifier vos stratégies de sécurité et répondre à vos besoins de gouvernance. Vous pouvez y parvenir tout en améliorant l'agilité de votre entreprise avec une solution IAM à la demande qui est à la fois modulable et extensible.

**LIMITEZ LES RISQUES.  
CONTRÔLEZ LES  
ACCÈS.  
MAÎTRISEZ LES  
IDENTITÉS.  
SÉCURISEZ LES  
DONNÉES.**

Désormais, la gestion des accès et des identités fournie par SaaS peut répondre directement aux besoins métier grâce à la solution One Identity Manager On Demand.



**Figure 1.** La carte thermique de la gouvernance permet une analyse rapide des violations des stratégies en place

## Fonctionnalités

**Cloud sans compromis** – Profitez de tous les avantages d'une solution IGA complète sur un modèle SaaS à la demande, sans renoncer au champ d'application, aux fonctionnalités ni à la sécurité.

**Certification SAP** – Proposez une intégration étroite certifiée SAP et des fonctionnalités précises afin d'exploiter les modèles de sécurité SAP existants, et même de les améliorer.

**Réduction des risques** – Prenez de meilleures décisions en matière de sécurité en associant les stratégies et les informations de sécurité issues de différentes sources afin de réduire votre exposition aux risques et éliminer les silos d'informations.

**Cloud** – Intégrez aisément les systèmes locaux et Cloud dans votre solution de gouvernance des identités à la demande.

**Gouvernance à 360 degrés** – Fournissez aux auditeurs des rapports de gouvernance en temps réel indiquant de façon détaillée quelles sont les ressources présentes dans votre environnement, qui accède aux données et à quel moment, et pourquoi cet accès a été accordé et résilié.

**Provisioning automatisé** – Éliminez les erreurs manuelles en automatisant le provisioning pour tous les systèmes, plateformes ou applications, en local ou dans le Cloud. Étendez le provisioning aux applications d'entreprise telles qu'Exchange Online, SharePoint et Oracle E-Business Suite.

**Accès sécurisé** – Améliorez la sécurité en fournissant aux salariés, fournisseurs, partenaires, clients, étudiants, anciens élèves, membres votants d'une organisation et patients les droits et niveaux d'accès dont ils ont absolument besoin : ni plus, ni moins.

**Conformité immédiate** – Des réglementations externes ? Pas de problème. Les stratégies internes ? Pas de problème. Bénéficiez de la visibilité totale dont vous avez besoin tout en respectant les exigences de tous les autres groupes.

**Portail d'accès en libre-service** – Gagnez du temps en permettant à l'entreprise d'être autonome. Réduisez les efforts fournis par l'équipe d'assistance avec un portail personnalisable façon « panier d'achat ». Les utilisateurs peuvent demander l'accès aux ressources réseau, actifs physiques, groupes et listes de distribution. Ils peuvent également contrôler les autorisations et les droits d'accès pour l'intégralité du cycle de vie des identités tout en utilisant des workflows et des processus d'approbation prédéfinis.

**Gouvernance des accès à privilèges** – Une gouvernance unifiée permet aux utilisateurs de demander, configurer et certifier les accès généraux et à privilèges depuis la même console.

**Tableau de bord pour l'examen des attestations** – Planifiez une attestation de routine ou à la demande et consultez l'état d'un groupe ou d'une liste de distribution à l'aide d'un tableau de bord clair et précis. Vous pouvez ainsi produire des rapports détaillés à des fins de détection ou de mise en application de la conformité.

**Réinitialisation du mot de passe** – Réinitialisez les mots de passe des comptes utilisateur et définissez des préférences de stratégie par utilisateur, conformément aux exigences et aux règles de création de mots de passe en vigueur dans l'entreprise. Vous pouvez instituer plusieurs stratégies de mot de passe granulaires en fonction des rôles utilisateurs.

**Évolution et déploiement selon vos besoins** – Vous pouvez vous appuyer sur votre infrastructure et vos investissements existants pour faire évoluer votre système.

### Certification ISO 27001

One Identity est une succursale de Quest et le leader mondial dans la sécurité des identités. Ses infrastructures et processus dans le Cloud ont reçu la certification ISO/IEC 27001. Il s'agit d'une norme internationale décrivant les bonnes pratiques concernant les systèmes de gestion de la sécurité des informations.

## À propos de One Identity

One Identity, une entité Quest, aide les organisations à mettre en place une stratégie de sécurité axée sur les identités, aussi bien sur site que dans le Cloud ou dans un environnement hybride. Avec notre vaste portefeuille intégré d'offres de gestion des identités, comprenant la gestion des comptes, l'administration et la gouvernance des identités, ainsi que la gestion des accès à privilèges, les organisations peuvent réaliser tout leur potentiel et bénéficier d'une sécurité efficace grâce à une stratégie axée sur les identités, qui assure un accès adéquat à tous les types d'utilisateurs, tous les systèmes et toutes les données. En savoir plus sur le site [OneIdentity.com](https://www.oneidentity.com)

© 2021 One Identity LLC. TOUS DROITS RÉSERVÉS. One Identity et le logo One Identity sont des marques et des marques déposées de One Identity LLC aux États-Unis et dans d'autres pays. Pour obtenir la liste complète des marques déposées One Identity visitez notre site Web [www.oneidentity.com/fr-fr/legal](https://www.oneidentity.com/fr-fr/legal). Toutes les autres marques, marques de service, marques déposées et marques de service déposées appartiennent à leurs propriétaires respectifs.

Datasheet-IDM-OnDemand-PG-FR-WL-64810