





## GARDEZ LE CONTRÔLE DE TOUS LES DROITS D'ACCES DE VOS UTILISATEURS

### PROVISIONING

Le « provisioning » sécurisé – i.e. la mise à disposition immédiate des outils et des ressources nécessaires à vos employés au sein de votre système d'information - simplifie la gestion des identités et des accès dans votre entreprise au quotidien. Un puissant moteur de provisioning fait coïncider les informations utilisateurs provenant des systèmes RH, des annuaires de l'entreprise et des bases de données organisationnelles avec les droits d'accès correspondant dans les applications de votre S. I. (les « systèmes-cibles »). Les droits d'accès approuvés sont automatiquement provisionnés dans les systèmes cibles concernés, peu importe qu'ils aient été générés par des imports de données RH automatisés ou par des processus de validation par workflows.

Les entreprises peuvent ainsi mettre en œuvre des politiques de sécurité cohérentes et homogènes sur l'ensemble des plateformes et des systèmes. Le provisioning automatique permet également de réduire les coûts d'administration et de garantir les bons accès aux bonnes personnes, à tout moment du cycle de vie d'une personne dans l'organisation.

### GOVERNANCE

Grâce aux imports automatisés de données RH, Garancy Identity Manager améliore l'efficacité des processus d'attribution de droits. Il est en effet possible de relier ces imports à des règles de sorte que lors de l'import des données RH, les utilisateurs se voient attribuer automatiquement un package de droits de

« base ». Ainsi, on peut par exemple utiliser des centres de coûts ou des unités d'organisation pour déclencher les règles.

Les fonctionnalités de gouvernance assurent le respect des règles clés de conformité ainsi que la transparence et la traçabilité des autorisations d'accès.

### GESTION DES UTILISATEURS

La gestion des utilisateurs permet à ces derniers de créer des droits manuellement ou en passant par un workflow. Des fonctionnalités de self-service sont également disponibles, comme par exemple la demande de droits ou la réinitialisation de mots de passe. Les demandes d'autorisations réalisées en self-service sont ensuite validées lors d'un processus d'approbation comportant plusieurs étapes.

### GESTION DES RÔLES

La gestion des rôles permet d'implémenter des modèles ou concepts basés sur la hiérarchie de rôles (RBAC). Les responsables (propriétaires) des rôles peuvent être définis directement dans Garancy Identity Manager ou en passant par des workflows.

Garancy Identity Manager supporte le concept de risques. Les rôles peuvent ainsi se voir attribuer un niveau de risque permettant de renforcer l'efficacité et la sécurité des processus d'habilitations. La solution prend également en charge l'attribution des autorisations basée sur les politiques y compris la définition des règles de cumuls toxiques (Segregation of Duties).

FIABLE



Faites confiance à notre rapidité et à notre fiabilité pour gérer vos tâches IAM !

Gestion des accès | Provisioning | Gestion des mots de passe | Self-service utilisateur | Gouvernance | Cycle de vie du rôle | Workflow | Recertification | SoD | Audit de conformité | Access Intelligence | Access Risk Management



## FONCTIONNALITES

### Provisioning

- Intégration flexible des applications grâce à un large choix de connecteurs « out of the box ».
- Synchronisation flexible et hautement extensible ( ? à très haute performance ?) des systèmes cibles à relier.
- Provisioning, consolidation et maintien en cohérence des droits d'accès
- Prise en compte des changements en temps réel.

### Gestion des utilisateurs

- Import automatique des données RH
- Gestion du cycle de vie de l'utilisateur (arrivées, départs et mutations)
- Différenciation entre les différents types d'utilisateurs (salariés internes et externes)
- Administration fine des droits des utilisateurs.

### Gouvernance des accès

- Gestion du cycle de vie des rôles avec les hiérarchies de rôles.
- Attribution automatique de rôles en fonction du profil identifié de l'utilisateur.
- Adoption des règles SOD (séparation des tâches).
- Gestion des habilitations basée sur les rôles, les attributs et sur les directives internes de sécurité informatique.

### Audit et sécurité

- Mise à disposition de listes d'audit pour les droits d'accès dorés
- Historisation des droits d'accès et de leurs changements
- Mise en place d'un référentiel unique et central des habilitations et des politiques de droits d'accès
- Mise à disposition d'un large choix de rapports standards incluant les rapports de conformité

### Expérience utilisateur

- Une interface utilisateur moderne facilitant leur acceptation
- Un GUI simple, intuitif et facile à utiliser.

### Technologie de connecteurs

- Une intégration facile de toutes les applications dans l'infrastructure de sécurité de l'entreprise.
- Support de toutes les versions actuelles des systèmes cibles standards (par exemple SAP, Lotus Notes Microsoft AD ou RACF).
- Mise à disposition d'interfaces standards.
- Connecteur basé sur un framework générique ayant fait ses preuves pour l'intégration des applications développées en interne.



Profitez de la solution IAM la plus large et extensible du marché !

Gestion des accès | Provisioning | Gestion des mots de passe | Self-service utilisateur | Gouvernance | Cycle de vie du rôle | Workflow | Recertification | SoD | Audit de conformité | Access Intelligence | Access Risk Management



## **Beta Systems Software France SARL**

5 avenue de Verdun  
94200 Ivry-sur-Seine  
Tél. : +33 6 76 09 57 78  
info-f@betasystems.com

Partenaire

