

Role Management

EVIDIAN
A Groupe Bull Company



IAM for
business and people

Définissez et faites respecter simplement votre politique de sécurité

Comment mettre en place une politique d'accès efficace pour les applications de l'entreprise et en contrôler son respect ?

La solution Evidian Role Management unifie et simplifie la gestion de vos droits d'accès tout en automatisant le circuit des autorisations.

Comment respecter simplement les nouvelles contraintes légales ?

Vous devez formaliser les procédures d'attribution de droits d'accès – mais surtout les faire respecter... et en convaincre vos auditeurs. Le module Policy Manager est la tour de contrôle de votre politique de sécurité.

Une politique claire

Les droits d'un employé dépendent de son rôle, son organisation, son lieu de travail etc. Ainsi, votre politique d'accès est alignée sur les métiers réels.

Une maintenance aisée

L'ensemble des éléments d'une politique de sécurité est défini par un outil unique. Cela simplifie la documentation et la mise à jour des procédures.

Des audits facilités

De même, les audits sont rapides car effectués à un endroit unique. Vos indicateurs de qualité sont fiables et réguliers.

Votre politique est écrite... mais est-elle appliquée ?

Avec la solution Evidian Role Management, vous vous assurez que vos directives sont réellement mises en place.

Le module Approval Workflow automatise les chaînes de décisions, de l'approbation des droits à la création des comptes. Par quelques clics, les responsables confirment qu'une action a été effectuée.

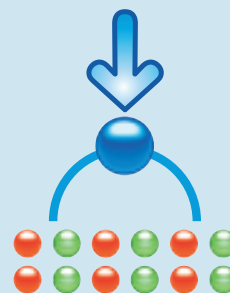
La réconciliation intégrée à Evidian Policy Manager confronte votre politique à la réalité du terrain, de manière régulière et automatique.

Ainsi, utilisateurs et décideurs obéissent naturellement à la politique de sécurité, de façon transparente et grâce à des outils simples.

Comment prendre en compte l'existant ?

Depuis des années, les politiques de sécurité de l'entreprise se sont succédées à travers des procédures variées. Aucun outil ne peut les ignorer, mais comment même connaître les droits existants ?

Le module Policy Manager peut s'appuyer sur la solution Evidian Access Management pour définir la politique de sécurité à partir des accès effectifs et quotidiens des utilisateurs.



ROLE MANAGEMENT

3 raisons d'adopter Evidian Role Management

1 Gérez le cycle de vie complet des droits d'accès

De l'arrivée dans un service au départ de l'entreprise, Evidian Role Management gère les circuits d'autorisation des droits d'accès. Vos utilisateurs sont rapidement productifs.

2 Basez votre politique sur la réalité du terrain

Les droits souhaités sont comparés aux accès et aux comptes applicatifs réels. Votre politique respecte la marche de l'entreprise.

3 Faites respecter votre politique de sécurité

En quelques clics, les managers s'engagent sur leurs décisions. La réconciliation mesure la mise en oeuvre de la politique et l'audit est simple car centralisé.



Evidian Role Management

met en place votre politique de sécurité avec deux modules complémentaires :

► **Policy Manager** permet de définir votre politique de droits d'accès. Avant de déployer une politique, vous la comparez facilement aux comptes et aux accès réels des utilisateurs.

► **Approval Workflow** automatise le circuit d'approbation des droits d'accès. Les décideurs sont informés par e-mail et peuvent approuver ou non les nouveaux droits en quelques clics.

Evidian Policy Manager

A partir d'une seule console, Policy Manager permet de définir et d'appliquer une politique de sécurité des accès à l'échelle de toute l'entreprise.

Un modèle complet

Policy Manager utilise une extension du modèle standard RBAC, prenant en compte la place de l'utilisateur dans l'organisation. Cela limite le nombre des règles nécessaires et simplifie la maintenance et l'évolution de la politique. Toutes les fonctions RBAC comme les rôles, l'héritage et la séparation des tâches sont bien sûr représentées.

Réconciliez votre politique avec les comptes d'utilisateurs

Les comptes déduits de votre politique peuvent être comparés aux comptes existants via *Evidian User Provisioning* ou d'autres solutions de provisionnement. Vous pouvez choisir de mettre à jour l'application cible ou votre politique de sécurité afin de coller au plus près à la réalité du terrain.

Réconciliez votre politique avec le référentiel d'accès SSO de l'entreprise

Policy Manager peut utiliser les informations collectées par *Evidian*

Enterprise SSO pour construire et valider votre modèle. Vous constaterez par exemple qu'un compte est utilisé par plusieurs personnes... ou aucune. L'analyse des écarts permet d'affiner votre politique.

Mise à jour des comptes manuelle ou automatique

Policy Manager peut demander aux administrateurs de créer, modifier ou supprimer des comptes. Ces opérations seront traitées à travers un workflow, ou automatisées par un module de provisionnement, éliminant ainsi la possibilité d'erreur humaine dans la mise à jour des comptes.

Modifiez les comptes sans crainte d'incidents

Des espaces de travail permettent d'évaluer différents scénarios de politiques avant leur application.

A tout moment, vous pouvez mesurer sans danger l'impact d'un changement de politique de sécurité. Quels utilisateurs n'auront plus accès aux applications qu'ils utilisent ? Quels comptes seront modifiés ?

Après vérification, la mise à jour des comptes peut se faire sous le contrôle de Approval Workflow.

Utilisez votre infrastructure existante

Policy Manager utilise nativement vos annuaires d'identités existants. Vos procédures de gestion des utilisateurs restent donc identiques.

Quand un employé est créé ou change de fonction dans l'annuaire de l'entreprise, ses droits sont automatiquement calculés et les procédures nécessaires déclenchées, sans action d'administration.

Une console Web 2.0

La console Policy Manager offre une console d'administration simple basée sur AJAX. Les tâches administratives

peuvent être déléguées au niveau le plus adéquat.

Evidian Approval Workflow

permet aux entreprises de mettre en place des processus de validation fiables, afin d'automatiser la gestion du cycle de vie des utilisateurs.

Entièrement personnalisable, il fonctionne nativement avec Policy Manager.

Approval Workflow fournit :

- un moteur de workflow compatible WfMC,
- une interface graphique simple pour la modélisation des processus de l'entreprise,
- des formulaires Web pour l'interaction avec les utilisateurs.

Un workflow d'approbation automatisé

Une requête (par exemple, la création d'un nouveau compte) est envoyée automatiquement à un décideur chargé de l'approbation des comptes, qui en est informé par e-mail contenant l'adresse URL d'un formulaire de réponse. Le décideur peut alors l'accepter, la rejeter ou la transférer.

Escalade et délégation

Si une requête n'est pas prise en compte après un certain délai, elle peut être « escaladée » vers d'autres décideurs. Par ailleurs, un décideur peut choisir de déléguer sa tâche pendant une période précise à une personne désignée.

Pré-requis

Evidian Role Management s'installe sur un serveur Windows 2003 ou Linux (Q3'2008).

Il s'interface avec les annuaires LDAP V3: Active Directory, ADAM/ADLDS, Sun Java System Directory Server, Novell eDirectory et OpenLDAP.

Pour plus d'information, visitez notre site Web : www.evidian.fr ou contactez nous : srv.evidian-france@evidian.com

Evidian France - rue Jean Jaurès B.P.68 - 78340 Les Clayes sous Bois - France - Tél. +33 (0)1 30 80 37 00 - Fax : +33 (0)1 30 80 37 10

Evidian Role Management est une marque déposée d'Evidian. Toutes les marques citées sont la propriété de leurs propriétaires respectifs.

Evidian se réserve le droit de modifier les caractéristiques de ses produits sans avis préalable.