AM

Access Manager

AUTHORIZATION MANAGEMENT

CENTRALISER ET HARMONISER LA GESTION DE L'ACCÈS

- ☑ gérer l'accès SAP, cloud, Entra ID, SailPoint, AD, etc.
- ☑ assurez la gouvernance grâce à des autorisations basées sur le flux de travail
- ☑ simplifier la provisionnement d'accès via une matrice d'accès intuitive

Les organisations actuelles évoluent dans des environnements informatiques hybrides complexes qui combinent des systèmes SAP sur site, SAP HANA, BW et plusieurs solutions cloud SAP — aux côtés de plateformes tierces telles que Microsoft, SailPoint ou Workday. À mesure que ces environnements s'étendent, les structures d'autorisation deviennent fragmentées et difficiles à gouverner de manière cohérente, nécessitant une approche centralisée et automatisée qui harmonise l'accès entre les systèmes SAP et non-SAP.

Le gestionnaire d'accès (AM) de SUIM propose une solution centralisée de gestion des autorisations en temps réel. Les rôles d'autorisation sont répartis sur l'ensemble du paysage système, couvrant tous les types d'autorisation pertinents — y compris les rôles PFCG, les autorisations SAP HANA, les rôles cloud SAP (par exemple SuccessFactors, SAP BTP, SAP Datasphere, SAP Analytics Cloud), ainsi que les rôles Entra ID, les rôles SailPoint et les groupes Active Directory — permettant une gouvernance d'accès efficace et harmonisée dans des environnements hybrides.

6 FAITS SAILLANTS
DU *ACCESS MANAGER (AM)*

RATIONALISATION DE LA GESTION DES AUTORISATIONS AVEC ACCESS MATIX
AM permet la fourniture d'autorisations entre les systèmes SAP et non-SAP via une matrice d'accès centrale et intuitive. Les attributions peuvent être effectuées via des cases à cocher, inclure des règles dépendant du temps, et être suivies via un journal d'actions complet à des fins d'audit.

REGROUPER DIFFÉRENTS ÉLÉMENTS D'AUTORISATION DANS LES RÔLES D'ENTREPRISE
AM regroupe plusieurs éléments d'autorisation – y compris les rôles SAP, le BI, les autorisations structurelles, les objets de gestion organisationnelle, Active Directory, les autorisations SAP HANA, SAC Teams et les autorisations tierces – en un seul rôle métier, simplifiant les affectations et accordant un accès multi-système en une seule étape.

AUTOMATISER L'ATTRIBUTION DES RÔLES EN FONCTION DES ATTRIBUTS UTILISATEUR
Les rôles sont attribués dynamiquement en fonction des attributs de l'utilisateur tels que le titre de poste, le département ou la fonction, garantissant ainsi que les utilisateurs reçoivent les autorisations appropriées pour leurs tâches tout en maintenant la sécurité et en réduisant les charges administratives.

GÉRER LES DEMANDES D'ACCÈS AVEC LES APPROBATIONS DE FLUX DE TRAVAIL
Le flux de travail en AM guide les demandes d'autorisation à travers des processus d'approbation définis, applique le principe des quatre yeux, vérifie automatiquement les conflits de ségrégation des tâches (SoD) et garantit le respect des règles de licence.

CENTRALISER LA SURVEILLANCE ET LA GESTION DES RÔLES ET PROFILS
Le Quality Cockpit en AM lit et affiche tous les rôles et profils des systèmes cibles, affichant leur statut et leurs attributions d'utilisateurs dans une seule vue. Depuis cette interface centrale, les administrateurs peuvent générer des profils, effectuer des rapprochements utilisateurs ou archiver des rôles, assurant ainsi une gestion d'accès cohérente et efficace sur l'ensemble du paysage.

CHANGEMENTS DE PROCESSUS DE RÔLE ET AUTORISATIONS EN MASSE
Les rôles dérivés et les profils BI sont automatiquement générés à partir des rôles maîtres et des attributs organisationnels tels que les attributions des rôles d'entreprise, de division et d'utilisateur. Cela garantit un accès précis et conforme sans intervention manuelle.

Pour plus d'informations :
www.suim.ch
info@suim.ch

SUIM
SOLUTIONS FOR IDENTITY MANAGEMENT