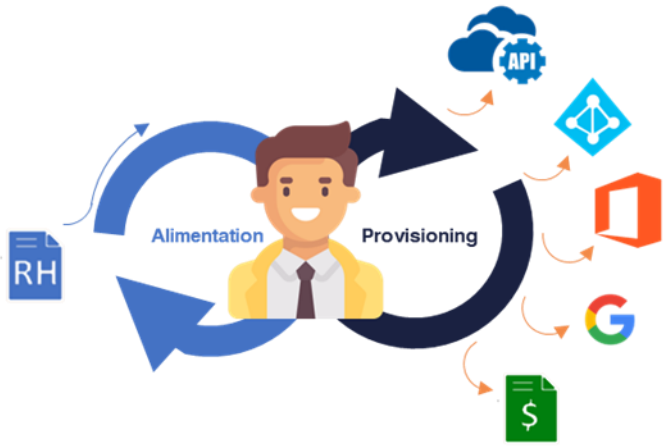
Identity Management
Cloud & On-Premises

Principaux bénéfices

- L'identitovigilance garantit l'unicité des identités et la sécurité du système d'information ;
- L'automatisation des habilitations assure que chaque utilisateur accède uniquement aux ressources auxquelles il est autorisé ;
- Les règles d'accès conforme aux politiques de sécurité garantissent que l'entreprise respecte les réglementations en matière de sécurité et de confidentialité des données ;
- Chaque utilisateur dispose rapidement des accès aux ressources sans interruptions inutiles ou demandes d'accès récurrentes ;
- Les administrateurs gèrent facilement les autorisations d'accès des utilisateurs ou groupes d'utilisateurs ;
- L'attribution automatique des droits réduit les actions d'administration et les coûts opérationnels ;
- Les fonctionnalités avancées de certification des droits et de SoD (Segregation of Duty) renforce la sécurité du SI ;

FairTrust IAM booste votre productivité tout en renforçant la sécurité. Grace à l'approche modulaire, vous bénéficiez rapidement d'avantages concrets.

FairTrust IAM gère le cycle de vie des identités numériques des personnes accédant au système d'information. Ce cycle de vie débute par la création des identités numériques à partir d'informations issues de votre système d'information, comme les bases RH ou référentiel externes.
Pour chaque identité numérique, FairTrust IAM détermine et alloue des droits d'accès au système d'information automatiquement via des règles d'habilitation définie en cohérence avec un modèle de droits, via un processus automatisé (workflow) ou manuellement (affectation discrétionnaire).
Les droits sont automatiquement poussés dans les référentiels de comptes et applications (provisioning), offrant ainsi un contrôle des accès applicatifs et une forte réactivité.
Enfin, chaque identité est clairement définie et présentée dans l'interface FairTrust et toutes les actions, affectations de droits ou changements sont tracés à des fins de contrôle et d'analyse.



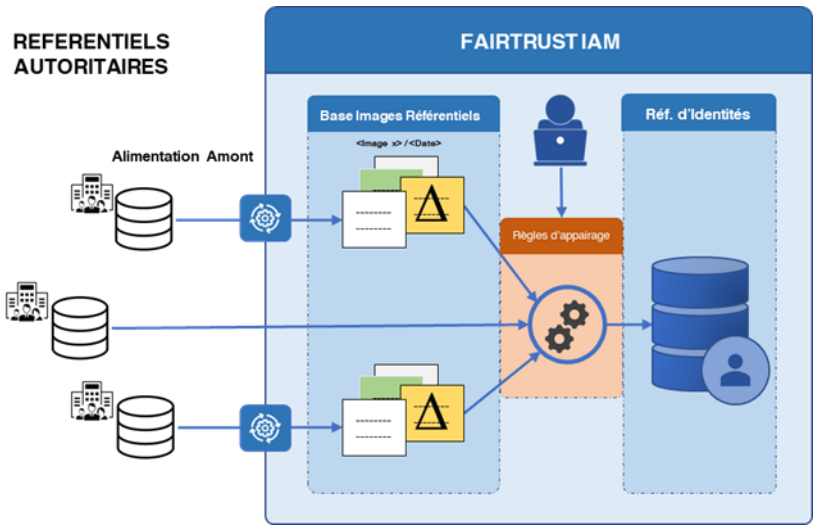
fair trust We help you secure your business

Créez automatiquement les identités

FairTrust intègre plusieurs méthodes d'alimentation des identités :

- La création manuelle d'identité : Les données caractéristiques des personnes sont saisies directement dans l'interface de l'IAM ;
- L'alimentation amont automatisée depuis les référentiels autoritaires : Les agents FairTrust collectent automatiquement les données des référentiels autoritaires et alimentent les attributs d'identités ;

Les mécanismes d'alimentation sont nativement implémentés dans la solution, offrant un maximum de performance et une richesse fonctionnelle. La « base d'images » historise les snapshots successives des référentiels autoritaires et calcul le différentiel entre les dernières images. Seules les données modifiées sont synchronisées avec le référentiel d'identités. En conséquence, un gain de performance significatif des processus d'alimentation.



Centralisez les identités

Clé de voute de la solution d'IAM, le référentiel d'identités centralise les identités numériques des utilisateurs, les règles et les habilitations, les organisations et rapports.

Les identités numériques sont construites à partir d'un ensemble d'attributs adaptés au contexte et métier de l'entreprise. Les attributs sont alimentés lors des « processus d'alimentation » ou calculés à partir d'autres attributs.

Les attributs des personnes sont regroupés par section et présentés dans la fiche d'identité.

Les processus d'appairage réconcilient automatiquement les identités dans une démarche d'identitovigilance (règles d'appairage).

Pour plus d'informations sur les fonctionnalité d'identitovigilance, téléchargez notre « Guide Produit - FairTrust IAM »

Définitions et termes

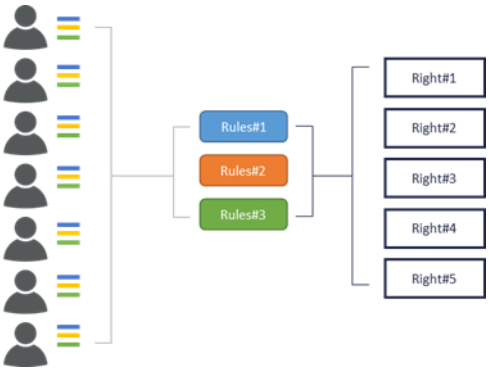
- Identité numérique : prolongement de l' « identité légale », elle est définie par un ensemble d'éléments invariables comme le nom, le prénom, la date de naissance…
- « Attributs » désignent les informations caractérisant une identité numérique : Par exemple « Attribut Nom », « Attribut Prénom », « Attribut Grade »…
- Référentiels autoritaires désignent les sources de données, considérées comme fiable, utilisées pour attribuer des valeurs aux attributs.
- Référentiel d'identités est la base centrale de la solution FairTrust IAM. Il stocke et gère l'ensemble des objets : Attributs, Organisations, Contrats, Rôles, Cartes, Droits d'accès (habilitations)…
- Alimentation amont est l'ensemble des mécanismes et processus permettant d'affecter des valeurs aux attributs des identités numériques.
- Les « agents FairTrust » réalisent les échanges de données entre l'IAM FairTrust et les référentiels autoritaires dans les processus d'alimentation ou les référentiels de comptes lors du provisioning.
- Les « Bases d'images de référentiel » stockent et historisent les images (snapshots) des référentiels autoritaires et référentiels de comptes.

Bénéficiez de la richesse du modèle de droits OrBAC

FairTrust IAM détermine les accès aux ressources du SI pour chaque utilisateur, en fonction de qui il est, de ses affectations, rôles, responsabilités et besoins.

Le modèle OrBAC permet de gérer efficacement les habilitations des utilisateurs en se basant sur les organisations des entreprises et les caractéristiques des individus. Ce modèle offre une gestion avancée des habilitations.

L'ajout, la modification ou la suppression d'une règle d'habilitation n'impacte pas les autres règles existantes. En conséquence, vous faites évoluer votre système FairTrust IAM en manière incrémentale, au rythme de l'évolution de votre SI.



Définitions et termes

- Le « modèle de droits », également appelé modèle d'autorisation, établit les règles et les contrôles permettant de déterminer les droits d'accès de chaque identité au sein du système d'information.
- Les habilitations désignent les autorisations ou permissions accordées aux utilisateurs pour l'accès aux ressources du système d'information.
- Les « applications » représentent les ressources du système d'information dont l'accès est piloté au travers des mécanismes de l'IAM.
- Les Référentiels de comptes ou bases de comptes (account repository) base contrôlent l'ensemble des droits d'accès des utilisateurs à une ou plusieurs applications.
- Les « droits d'accès » à une application désignent les autorisations accordées à un utilisateur pour accéder à une application donnée.
- Les « Bases d'images de référentiel » stocke les images (snapshots) des référentiels autoritaires et référentiels de comptes.

Pilotez les droits d'accès par des règles

Les règles d'habilitation automatisent la création, suppression et/ou modification des permissions accordées à un utilisateur en fonction de certaines conditions. Elles offrent plusieurs avantages :

- L'attribution est rapide et sans action manuelle, réduisant les couts de gestion ;
- Les règles sont auditables et définies en conformité avec les réglementations et politiques de sécurité en vigueur ;
- Exécutés régulièrement, elles assurent que les utilisateurs possèdent uniquement les permissions nécessaires, au bon moment, pour effectuer leurs taches ;
- Elles réduisent les risques d'erreurs humaines et peuvent être mise à jour pour répondre à l'évolution des besoins et l'organisation de l'entreprise ;

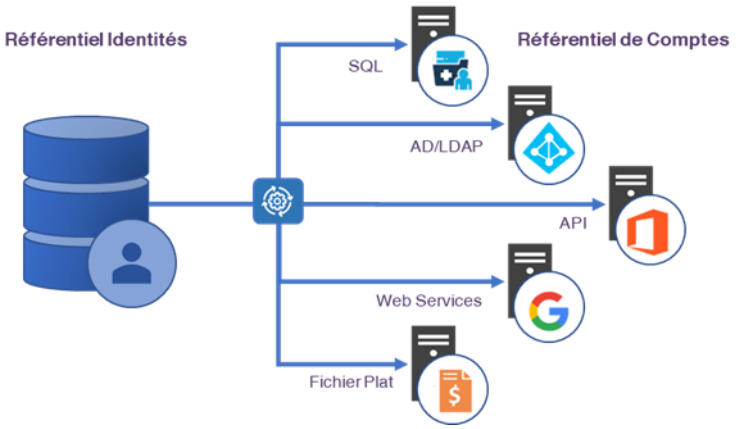
Gardez un contrôle manuel

L'affectation discrétionnaire est limitée aux opérateurs autorisés qui décident d'attribuer des habilitations en fonction de critères qu'ils jugent pertinents. Cette méthode répond aux cas d'usage où il est difficile d'établir des règles strictes, ou lorsque le droit concerne un nombre restreint d'utilisateur.

L'affectation discrétionnaire est réalisée directement dans la console FairTrust Center.

Automatisez la création des comptes utilisateurs

FairTrust IAM automatise la création des comptes et des droits dans l'ensemble des applications et référentiels de comptes, en fonction des habilitations utilisateurs.



Le provisioning est spécifique à chaque référentiel de comptes. Il regroupe les mécanismes de création / modification / suppression des comptes dans les référentiels. FairTrust IAM supporte nativement le provisioning vers :

- Fichier plat : Par exemple fichier CSV ;
- Web Service : Service mis à disposition par l'application cible, permettant l'échange d'informations et la création des comptes et droits.
- LDAP : protocole d'échange avec les services d'annuaire ;
- ADSI : format de synchronisation avec votre annuaire Active Directory ;
- SQL : Langage permettant l'échange d'information avec les référentiels utilisant une base de données SQL pour la gestion des comptes et droits utilisateurs ;
- Custom : Interface de programmation mise à disposition par le référentiel cible pour l'échange d'informations et la création des comptes et droits ;

Les données d'authentification sont directement provisionnées dans le référentiel FairTrust SSO. En conséquence, l'utilisateur est directement opérationnel. Ses droits sont provisionnés dans l'application et son authentification est automatisée par FairTrust SSO.

Contrôle et historisation des comptes

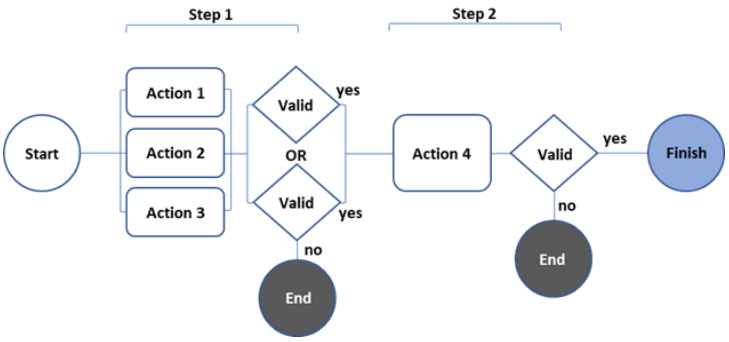
La « base d'images des référentiels » conserve une image des référentiels de comptes. En conséquence, l'IAM détecte les modifications réalisées sans passer par la solution de gestion d'identité. Ces modifications sont soit supprimées du référentiel, soit converties en droits manuels.
De plus, FairTrust offre une représentation de l'évolution des comptes utilisable dans un processus d'analyse.

Dynamisez les flux - Workflows

Les workflows modélisent les processus décisionnels en étapes séquentielles ou parallèles et automatisent certaines taches :

- Workflows de validation : Ils automatisent les circuits de validation et les demandes approbations;
- Workflows d'information : Ils automatisent le partage d'informations entre plusieurs cibles, par exemple, d'un mail d'information sur la création ou la suppression d'une identité ou un changement d'habilitation.

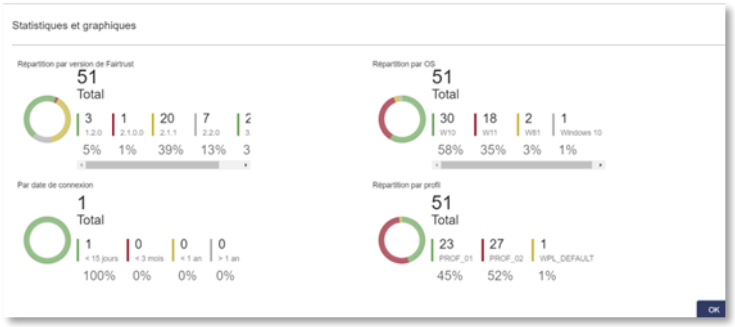
Les workflows sont lancés manuellement par les utilisateurs autorisés, programmés à une date précise ou exécutés automatiquement à partir de déclencheurs, exemple le changement d'état d'un attribut.



Restez informé en permanence

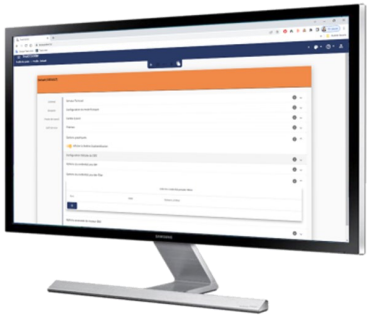
L'ensemble des opérations d'administrations et des actions de l'utilisateurs est tracé. Les rapports d'audits permettent de rechercher des événements. Les audits sont exportables vers des solutions tierces.
Les audits générés sur le poste de travail sont envoyés au serveur d'administration central. Si le serveur n'est pas disponible, les audits sont stockés dans un cache sur le poste de travail, en attendant que le serveur soit de nouveau disponible.

En standard la solution FairTrust IAM propose un ensemble de rapports fournissant un suivi graphique d'indicateurs de la solution.



Console d'administration

Les interfaces FairTrust IAM sont conçues pour d'optimiser l'expérience utilisateur et l'accessibilité aux données et aux fonctionnalités de configuration, d'administration et d'exploitation.



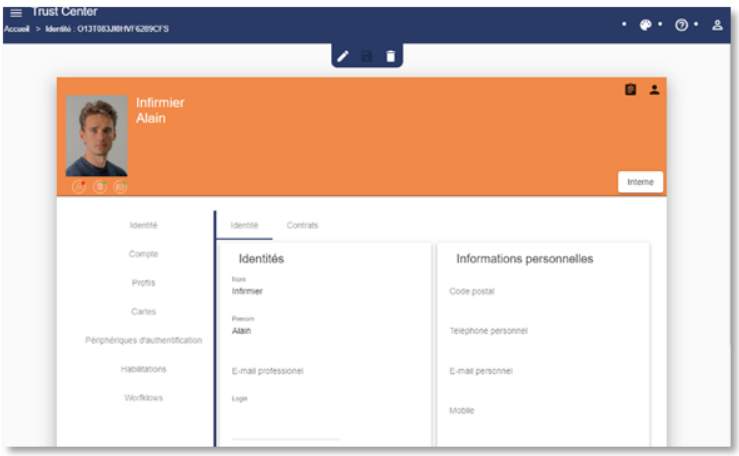
Le moteur de recherche

Le moteur de recherche de personne est la première interface présentée aux utilisateurs. Il permet de retrouver une identité en fonction de plusieurs critères basés sur des attributs. En cliquant sur une personne, vous accédez à sa fiche d'identité.

Fiche d'identité

La fiche d'identité est une « vue » sur le référentiel d'identités présentant les informations spécifiques à une personne en fonction du profil de l'utilisateur, notamment :

- Ses comptes ;
- Ses systèmes d'authentification ;
- Ses workflows ;
- Ses contrats ;
- Ses informations personnelles ;
- ...



Pour plus d'informations téléchargez notre « Guide Produit - FairTrust IAM »

FAIRTRUST s.a.s.

9 Allée du Bois Louët

35235 Rennes

Tel. +33 2 30 96 07 47

www.fairtrust.com

A propos de FairTrust

FairTrust est éditeur de solutions de cybersécurité. Nous croyons que toutes les entreprises ont droit à la meilleure sécurité quelles que soient leurs tailles ou leur métier. Nous contribuons au renforcement de la sécurité des systèmes d'information des entreprises dans tous les secteurs d'activités. Basé sur le principe de l'IAM, nous intervenons sur l'authentification forte des utilisateurs, la gestion du cycle de vie des mots de passe, la gestion des identités et des habilitations.