



CHECKLIST DE PRÉPARATION

Préparer une gestion des accès OneLogin sans angle mort

Utilisez cette checklist avant de déployer ou d'évaluer OneLogin pour vos accès professionnels. Elle aide à relier les besoins métiers, les règles de sécurité et le fonctionnement concret des applications.

Au sommaire

- 1 Le rôle de OneLogin en un coup d'œil
- 2 1. Cartographier les accès à centraliser
- 3 2. Structurer l'identité et les droits
- 4 3. Configurer un parcours de connexion cohérent
- 5 Repères : ne pas confondre les fonctions
- 6 4. Valider l'offre et l'exploitation

Le rôle de OneLogin en un coup d'œil

OneLogin est une plateforme cloud de gestion des identités et des accès (IAM).

Elle centralise l'accès aux applications professionnelles depuis un portail.

L'authentification unique (SSO) limite les nouvelles saisies d'identifiants pour les services compatibles.

Les groupes, rôles et règles d'accès déterminent les applications visibles et autorisées pour chaque utilisateur.

LE PARCOURS DE CONNEXION ONELOGIN

Un accès sécurisé, simple et unifié à toutes vos applications

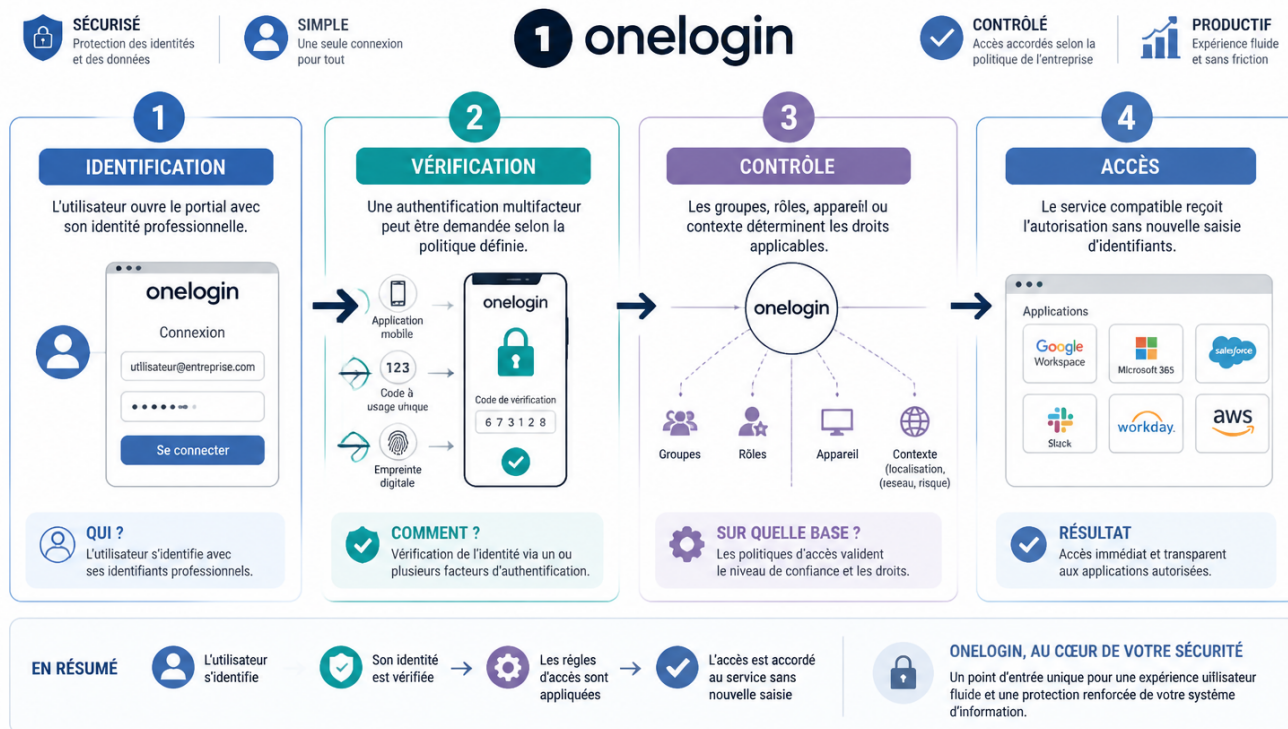


SCHÉMA Du compte professionnel à l'application autorisée : identification, vérification, contrôle et accès.

1. Cartographier les accès à centraliser

Lister les applications professionnelles concernées

Distinguer les services critiques des outils secondaires.

- Vérifier la compatibilité de chaque application avec les protocoles nécessaires**
Le SSO dépend de la compatibilité du service.
- Identifier les populations d'utilisateurs**
Collaborateurs, équipes, administrateurs et autres profils à encadrer.
- Repérer les accès à privilèges ou particulièrement sensibles**
Ils demandent des règles et contrôles adaptés.

2. Structurer l'identité et les droits

- Vérifier la fiabilité de l'annuaire d'entreprise**
Les comptes et informations utilisateur doivent rester à jour.
- Définir les groupes métier utiles**
Ils servent à attribuer les accès de manière cohérente.
- Clarifier les rôles et les droits associés**
Le SSO ne définit pas seul les autorisations métier.
- Prévoir le traitement des changements de poste**
Une évolution de rôle doit entraîner une mise à jour contrôlée des accès.
- Formaliser la suppression ou le retrait des droits lors d'un départ**
Réduire le risque de comptes ou d'accès oubliés.

3. Configurer un parcours de connexion cohérent

- Définir l'identité professionnelle utilisée pour accéder au portail**
Le portail devient le point de connexion central.
- Choisir les règles d'authentification multifacteur**
Son efficacité dépend des méthodes activées et de leur configuration.
- Déterminer les critères de contrôle d'accès**
Rôle, équipe, application, appareil utilisé ou contexte de connexion.
- Tester le parcours utilisateur complet**
Identification, vérification, contrôle puis accès à l'application autorisée.

Repères : ne pas confondre les fonctions

Notion	Ce qu'elle apporte	Point de vigilance
Authentification unique (SSO)	Accès à plusieurs services compatibles après une connexion initiale.	Elle ne définit pas à elle seule les droits métier.
Gestion des identités	Organisation des comptes, groupes, rôles et données utilisateur.	Elle suppose un annuaire fiable et des règles maintenues à jour.
Gestionnaire de mots de passe	Conservation ou génération d'identifiants selon la fonction.	Il ne remplace pas une politique globale de contrôle des droits.

4. Valider l'offre et l'exploitation

- ☐ **Contrôler les intégrations réellement nécessaires**
Commencer par les applications critiques.
- ☐ **Vérifier les fonctions incluses dans l'offre envisagée**
Les capacités peuvent varier selon l'offre et le périmètre retenus.
- ☐ **Définir qui administre les règles et les droits**
Le pilotage central doit avoir des responsabilités claires.
- ☐ **Préparer des procédures de secours**
Prévoir les situations où le parcours habituel de connexion ne peut pas être suivi.
- ☐ **Prévoir une revue régulière des comptes et des accès**
Les droits doivent rester alignés avec la situation réelle des utilisateurs.

! Point de vigilance

Centraliser les connexions ne suffit pas : la valeur de la gestion des accès dépend de la qualité de l'annuaire, des règles d'attribution des droits, des méthodes multifacteur activées et des procédures prévues en cas d'incident.

Les fonctions disponibles et les intégrations prises en charge dépendent de l'offre souscrite, de la configuration retenue et des applications concernées.