∞drive suite

Guide d'administration

Gestion des accès

Avertissement

Liste de diffusion

Société	Rôle
Groupe Oodrive	Collaborateurs et clients du Groupe Oodrive

Sommaire

1. Prendre en main la configuration de votre espace

Sommaire

En tant que titulaire d'un compte Oodrive avec des droits d'administration, vous avez été nommé comme responsable d'un ou de plusieurs modules d'administration de l'espace de travail de votre société.

Ainsi, vous êtes chargé de paramétrer un certain nombre d'options concernant le comportement des applications mises au service des collaborateurs de votre organisation.

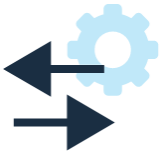
Plusieurs modules d'administration peuvent être à votre disposition dans le portail de la suite Oodrive, en fonction de la répartition de ces responsabilités au sein de votre société.

Certains modules d'administration sont commun à toutes les solutions Oodrive et permettent de configurer et superviser votre espace de travail dans son ensemble :

Modules d'administration communs	
Gestion des accès 	• paramétrage de l'accès et de l'authentification à l'espace de travail Accéder à la documentation
Gestion des utilisateurs 	• gestion des utilisateurs de l'espace de travail Accéder à la documentation
Gestion de la personnalisation graphique 	• paramétrage des noms, des logos et des couleurs de l'espace de travail Accéder à la documentation
Suivi des activités 	• suivi des activités de l'ensemble des utilisateurs sur l'espace de travail Accéder à la documentation

Modules d'administration communs	
Administration des textes légaux 	• gestion des textes légaux et de leur approbation par les utilisateurs de l'espace de travail Accéder à la documentation

D'autres modules d'administration sont spécifiques à une solution précise. Ces modules vous permettent de paramétrer chaque application selon les besoins de votre organisation :

Modules d'administration spécifiques	
Administration des partages 	• module spécifique aux solutions Oodrive Work_share et Oodrive Work • paramétrage des options des applications de partage et de collaboration • suivi des activités des utilisateurs Accéder à la documentation
Administration de Work 	• module spécifique à la solution Oodrive Work • gestion des espaces d'équipe Accéder à la documentation
Gestion des sauvegardes 	• module spécifique à la solution Oodrive Save • paramétrage des jeux et des politiques de sauvegarde de votre parc d'utilisateurs Accéder à la documentation
Administration de Oodrive Media 	• module spécifique à la solution Oodrive Media • configuration de l'application Médiathèque Accéder à la documentation

Modules d'administration spécifiques	
Administration de Oodrive Meet 	• module spécifique à la solution Oodrive Meet • configuration des options de réunion Accéder à la documentation

Un guide d'administration est disponible pour chacun de ces modules, afin de vous accompagner dans la configuration de votre espace de travail en fonction de votre rôle.

À noter : Les modules d'administration auxquels vous avez accès ou non dépendent de la configuration définie par le support Oodrive et son point de contact privilégié au sein de votre société.

1.1. Compatibilité

Les solutions Oodrive fonctionnent sur différents systèmes d'exploitation et navigateurs. Voici la liste des versions compatibles :

Systèmes d'exploitation

- **Windows**

  Systèmes d'exploitation couverts par le support standard Microsoft (Cf. cycle de vie de Windows : http://windows.microsoft.com/en-us/windows/lifecycle)

- **MacOs et iOS**

  Versions majeures n et n-1 (en cours et précédente)

- **Android**

  Versions majeures n et n-1 (en cours et précédente)

Navigateurs Internet

- **Microsoft Edge, Google Chrome et Mozilla Firefox**

  Versions majeures n et n-1 (en cours et précédente)

- **Safari**

  Version majeure la plus récente disponible sur un système d'exploitation Apple compatible

Autres logiciels

- **JRE (pour les applets)**

  JRE (et JDK) supportés par Oracle sur leurs systèmes d'exploitation respectifs

- **Microsoft Outlook**

  Versions couvertes par le support standard Microsoft

1.2. Se connecter à votre espace

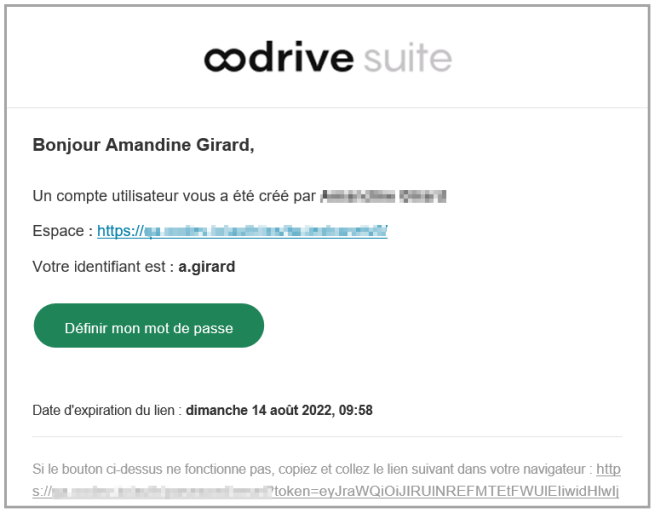
Il existe deux manières de vous connecter à votre espace :

- avec vos identifiants Oodrive
- avec vos identifiants d'entreprise

Le ou les modes de connexion disponibles sur votre espace dépendent de la configuration effectuée dans le module Gestion des accès.

Connectez-vous avec vos identifiants Oodrive

1. Récupérez l'identifiant qui vous a été communiqué par e-mail lors de la création de votre compte et cliquez sur le bouton **Définir mon mot de passe**.



2. Vous serez redirigé vers une page de votre navigateur vous demandant de définir un mot de passe et de le confirmer avant de cliquer sur le bouton **Valider**.

3. Cliquez sur le bouton **Se connecter** pour accéder à la page de connexion.

   Remarque : Si le champ de connexion avec identifiants Oodrive n'est pas visible, cliquez sur **Connectez-vous avec vos identifiants** pour l'afficher.

4. Saisissez votre identifiant et cliquez sur **Suivant**.

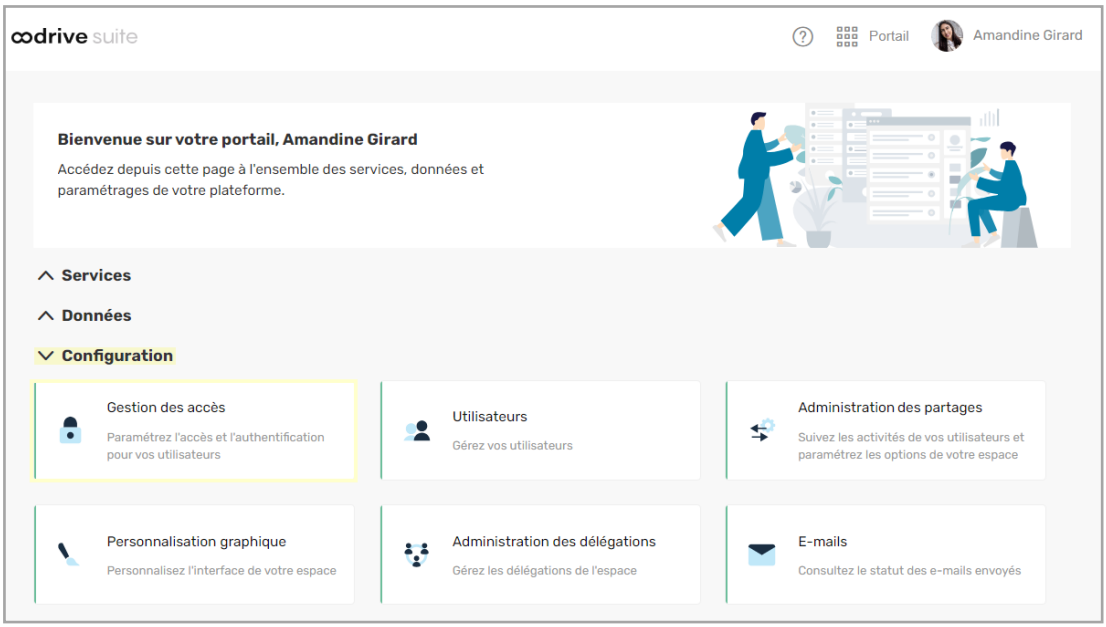
5. Saisissez le mot de passe que vous venez de définir puis cliquez sur **Se connecter**.

   Attention : Suite à 5 tentatives de connexion échouées, un code de sécurité vous sera automatiquement envoyé par e-mail. Ce code sera ainsi requis en complément de votre mot de passe.

   En cas d'oubli de votre mot de passe, cliquez sur **Mot de passe oublié**.

   Si la double authentification a déjà été paramétrée sur votre espace, vous serez également convié à saisir le code reçu sur votre appareil mobile.

6. Ensuite, vous accéderez au portail de la suite Oodrive, où se trouve l'ensemble des applications et des modules de configuration auxquels vous avez accès.



Pour revenir au portail à tout moment, cliquez sur 

dans le coin supérieur droit de la page, puis sélectionnez **Portail**.

À noter : Pour des raisons de sécurité, vous êtes automatiquement déconnecté de votre session au bout de 30 minutes d'inactivité (ou au bout de 4 heures si la fonctionnalité de discussion d'Oodrive Work est activée). Vous pouvez prolonger votre session en cliquant sur **Continuer à naviguer** lorsque que l'avertissement de déconnexion s'affiche à l'écran.

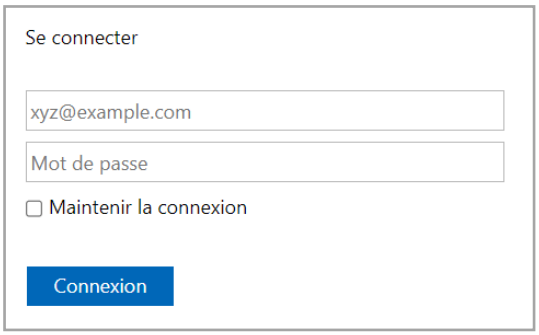
Déconnectez-vous à tout moment en cliquant sur votre nom dans le coin supérieur droit de la page, puis cliquez sur le bouton **Déconnexion**.

Connectez-vous avec vos identifiants d'entreprise

1. Cliquez sur le bouton **Se connecter avec SSO**.

   Si ce bouton n'est pas disponible, cliquez sur le lien **Connectez- vous avec l'authentification unique d'entreprise (SSO)**.

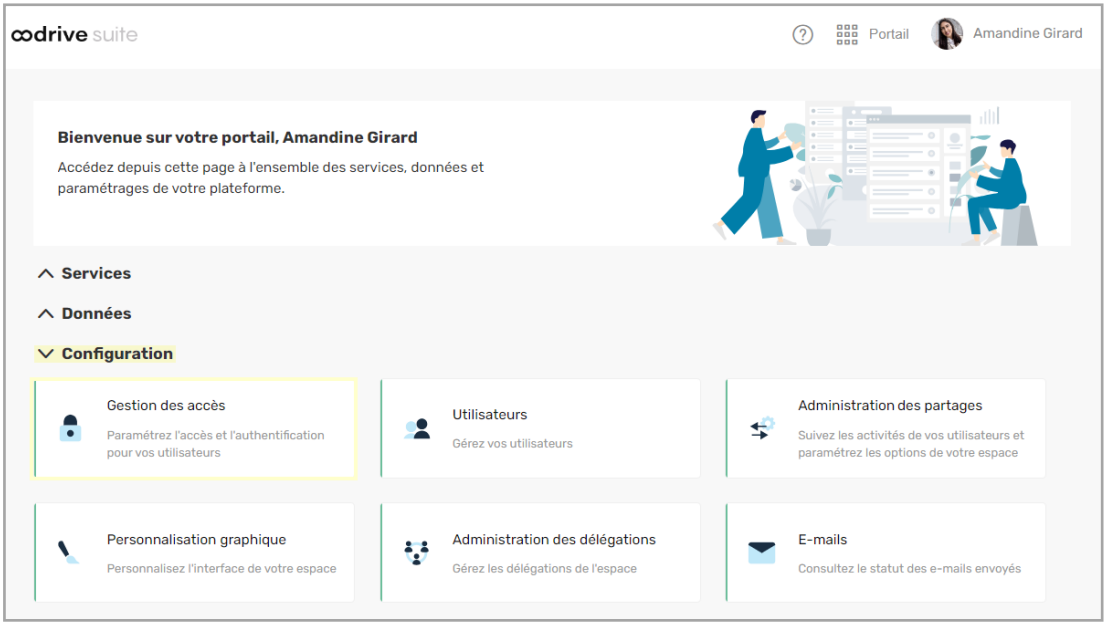
2. Saisissez vos identifiants d'entreprise et cliquez sur **Connexion**.



Si vous avez oublié le mot de passe associé à votre identifiant d'entreprise, veuillez contacter l'administrateur IT de votre société.

Si la double authentification a déjà été paramétrée sur votre espace, vous serez également convié à saisir le code reçu sur votre appareil mobile.

3. Ensuite, vous accéderez au portail de la suite Oodrive, où se trouve l'ensemble des applications et des modules de configuration auxquels vous avez accès.



Pour revenir au portail à tout moment, cliquez sur 

dans le coin supérieur droit de la page, puis sélectionnez **Portail**.

À noter : Pour des raisons de sécurité, vous êtes automatiquement déconnecté de votre session au bout de 30 minutes d'inactivité (ou au bout de 4 heures si la fonctionnalité de discussion d'Oodrive Work est activée). Vous pouvez prolonger votre session en cliquant sur **Continuer à naviguer** lorsque que l'avertissement de déconnexion s'affiche à l'écran.

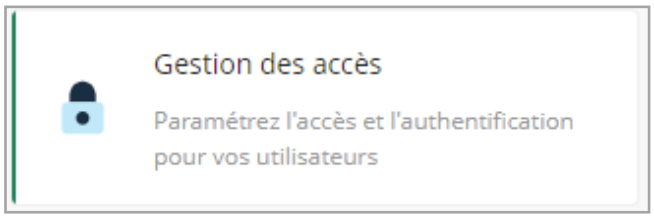
Déconnectez-vous à tout moment en cliquant sur votre nom dans le coin supérieur droit de la page, puis cliquez sur le bouton **Déconnexion**.

1.3. Vue d'ensemble du module de gestion des accès

En tant qu'utilisateur titulaire des droits d'administration, vous assurez ainsi la mise en place des paramètres de sécurité adaptés et conformes aux exigences de votre organisation.

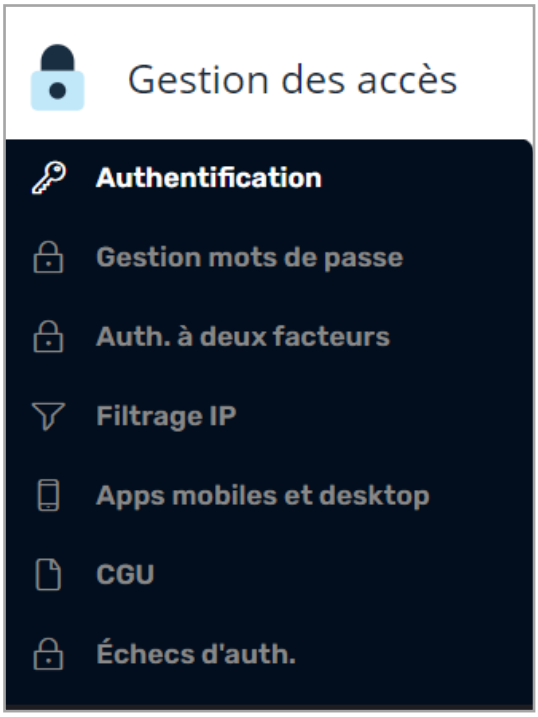
Les paramètres relatifs à l'authentification des utilisateurs se configurent dans le module de gestion des accès qui se compose des contrôles d'accès suivants :

- le protocole d'authentification (LDAP, SAML, Kerberos)
- le niveau de complexité des mots de passe
- l'authentification à deux facteurs
- le filtrage d'adresse IP
- l'accès par application mobile
- les conditions générales d'utilisation (CGU)
- les tentatives d'authentification



1.4. Parcourir le module de gestion des accès

Accédez rapidement à l'ensemble des rubriques du module de gestion des accès depuis le panneau de navigation situé sur le côté gauche de la page.



2. Configurer un protocole d'authentification externe

Sommaire

Avant que vos collaborateurs ne commencent à se servir des applications de l'espace de travail, vous pouvez choisir de mettre en place un protocole d'authentification externe correspondant aux configurations requises par la politique de sécurité de votre société.

Quatre protocoles d'authentification externes sont à votre disposition :

Les protocoles d'authentification disponibles	
Lightweight Directory Access Protocol (LDAP)	Optimal pour les sociétés cherchant à automatiser l'administration des comptes grâce à la mutualisation des données de l'annuaire d'entreprise.
Security Assertion Markup Language (SAML)	Idéal pour les sociétés qui préfèrent une authentification par single sign-on (SSO) afin que ses utilisateurs puissent se connecter directement par leurs identifiants d'entreprise. Ce protocole d'authentification est préconisé pour sa simplicité et son niveau de sécurité élevé.
Kerberos	Une bonne mesure de sécurité pour les sociétés qui souhaitent gérer l'authentification par un protocole de chiffrement symétrique.
Open ID Connect	Idéal pour les sociétés qui souhaitent déléguer l'authentification de leurs collaborateurs à un fournisseur d'identité de confiance.

Veuillez noter : Vous pouvez imposer l'authentification via un protocole d'authentification externe à l'ensemble des utilisateurs de votre espace ou bien l'utiliser en parallèle de l'authentification avec identifiants de connexion oodrive.

2.1. Lightweight Directory Access Protocol (LDAP)

Le protocole LDAP est un moyen de faire le provisioning des comptes. Lorsqu'il est activé, Oodrive Suite interroge l'annuaire de votre société pour vérifier l'identifiant et le mot de passe entrés par l'utilisateur. Si ceux-ci sont corrects, l'utilisateur se connecte ; il est rejeté dans le cas contraire.

Préalablement à cette configuration, nous vous invitons à contacter le Support Oodrive afin de procéder à l'ouverture des flux et permettre la communication entre votre annuaire LDAP et nos services.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Authentification**.

2. Cliquez sur le menu déroulant, puis sélectionnez **LDAP**.

3. Si vous voulez appliquer ce mode d'authentification à tous les utilisateurs de votre espace, sans exception, cochez **Forcer ce type d'authentification**.

   Remarque : Vous ne devez pas cocher cette option si vous avez prévu d'activer l'authentification sans mot de passe sur votre espace.

4. Cliquez sur le bouton **Appliquer**, puis cliquez sur le bouton **Nouvelle configuration**.

5. Indiquez le **nom de la configuration** et le **type d'utilisateur** (utilisateur ou contact) pour lequel vous souhaitez configurer le protocole LDAP.

6. Renseignez les champs de la section **Connexion** et cliquez sur **Test** pour vérifier que la connexion s'établit correctement.

   En cas d'erreur, vérifiez que :

   - l'information du champs **Hôte** (votre IP ou nom de domaine) a bien été communiquée aux équipes Oodrive,
   - l'IP publique d'Oodrive est bien autorisée à se connecter à votre annuaire LDAP.

7. Renseignez les champs de la sections **Configuration** pour indiquer quels utilisateurs de votre annuaire LDAP doivent être provisionnés sur votre espace de travail Oodrive.

8. Renseignez les champs de la section **Attributs** pour permettre le provisionnement automatique des comptes à partir des informations de votre annuaire LDAP. Tous les champs marqués d'une étoile rouge sont requis.

   Attention : Les champs ci-dessous ne doivent pas être confondus, veillez à les renseigner avec soin.

   - **Identifiant** : identifiant devant figurer sur la fiche utilisateur dans votre espace de travail Oodrive
   - **Login LDAP** : élément permettant à l'utilisateur de s'identifier auprès de LDAP depuis la page de connexion de votre espace de travail (par exemple : adresse e-mail, numéro de téléphone, nom d'usage...)
   - **Identifiant LDAP** : clé unique utilisée pour identifier le compte utilisateur LDAP dans l'annuaire. Cette valeur ne doit pas être modifiée car elle permet de relier le compte Oodrive de l'utilisateur à son compte LDAP.

9. Cliquez sur le bouton **Test configuration** afin de tester la connexion LDAP et de vérifier que cette dernière fonctionne correctement.

   Une fenêtre affiche les comptes qui seront créés grâce à votre configuration, ainsi que les informations qui rempliront leur fiche utilisateur.

10. Cliquez sur le bouton **Créer** pour finaliser votre configuration.

11. Une fois votre configuration créée, cliquez sur le bouton **Synchroniser** pour effectuer le provisionnement des utilisateurs à partir de votre annuaire LDAP.

Vous pourrez retrouver les utilisateurs provisionnés via LDAP dans le module d'administration Utilisateurs.

Revenez à la rubrique **Authentification** pour modifier ce protocole d'authentification à tout moment.

2.2. Security Assertion Markup Language (SAML)

Le SSO (Single Sign-On ou authentification unique) par SAML permet à un utilisateur d'accéder à plusieurs applications par ses identifiants d'entreprise.

Si l'utilisateur est déjà authentifié à son IDP (Identity Provider) lors de la demande de connexion, il accédera directement à la solution sans avoir besoin de ressaisir ses identifiants.

En revanche, si l'utilisateur ne s'est pas encore authentifié, il sera redirigé vers son IDP pour qu'il puisse s'authentifier rapidement et se connecter à son espace de travail.

La procédure qui suit permet de configurer le SSO par SAML pour l'IDP Active Directory Federation Services (AD FS) connecté à un répertoire d'utilisateurs LDAP.

Étape 1 : Définir le type d'authentification

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Authentification**.

2. Cliquez sur le menu déroulant, puis sélectionnez **SAML**.

3. Si vous voulez appliquer ce mode d'authentification à tous les utilisateurs de votre espace, sans exception, cochez **Forcer ce type d'authentification**.

   Attention : Vous ne devez pas cocher cette option si vous avez prévu d'activer l'authentification sans mot de passe sur votre espace.

4. Cliquez sur le bouton **Appliquer** pour valider votre choix.

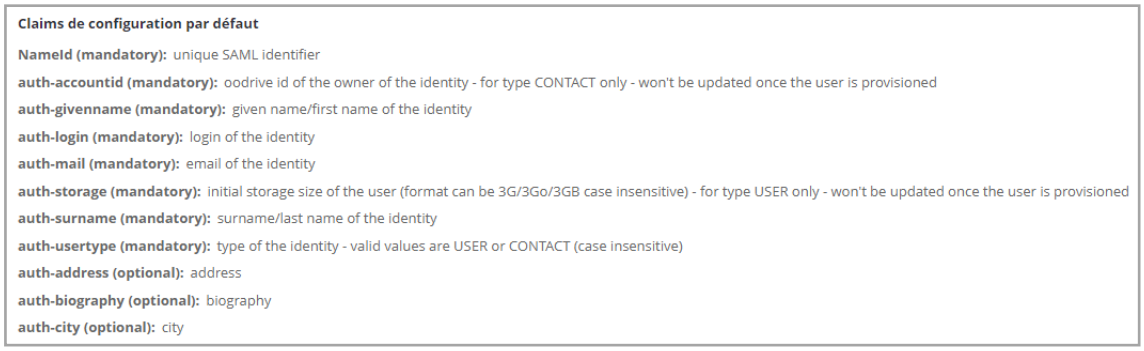
Étape 2 : Effectuer la transmission des fichiers de métadonnées

Afin d'établir une relation de confiance entre les deux entités et leur permettre de communiquer, la plateforme Oodrive et votre IDP doivent chacun disposer du fichier de métadonnées de l'autre.

Transmettre votre fichier de métadonnées à Oodrive

1. Depuis la rubrique **Authentification**, cliquez sur le bouton **Parcourir** pour chercher et sélectionner votre fichier de métadonnées au format XML, à l'aide de l'explorateur de fichiers de votre poste.

   À noter : Afin d'assurer la bonne configuration des claims de configuration, veuillez consulter les définitions qui se trouvent en bas la page avant de sélectionner le fichier de métadonnées.



2. Saisissez un nom du fichier pour le serveur de stockage en réseau, puis cliquez sur le bouton **Importer**.

Télécharger le fichier de métadonnées Oodrive

1. Dans la section **Configuration du serveur SAML Oodrive**, cliquez sur le lien **Télécharger le fichier metadata Oodrive**.

2. Enregistrer le fichier **spring_saml_metadata.xml** à l'aide de l'explorateur de fichiers de votre poste.

Ce fichier de métadonnées vous permettra d'enregistrer Oodrive comme partie de confiance auprès de votre IDP.

Étape 3 : Configurer la partie de confiance sur le serveur AD FS

1. Sur le serveur AD FS, ouvrez **Gestion AD FS**.

2. Déployez le dossier **Relations de confiance**.

3. Effectuez un clic droit sur le dossier **Approbation des parties de confiance**, et sélectionnez **Ajouter une approbation de partie de confiance**.

   Vous accédez à l'assistant de configuration d'une partie de confiance.

4. Cliquez sur **Démarrer** pour commencer la configuration.

5. À l'étape **Sélectionner une source de données**, cochez **Importer des données d'une partie de confiance à partir d'un fichier**.

6. À l'aide de l'explorateur de fichiers, sélectionnez le fichier **spring_saml_metadata.xml** que vous avez téléchargé dans le module **Gestion des accès**.

7. Cliquez sur **Suivant**.

8. À l'étape **Spécifier le nom complet**, renseignez **Oodrive** comme nom de la partie de confiance.

9. Cliquez sur le bouton **Suivant** jusqu'à atteindre la dernière étape, puis cliquez sur le bouton **Fermer**.

Étape 4 : Configurer les règles de revendication

Une fois la partie de confiance créée, vous accédez automatiquement à la fenêtre d'édition des règles de revendication.

Remarque : Si la fenêtre d'édition des règles de revendication ne s'ouvre pas automatiquement, effectuez un clic droit sur la partie de confiance que vous venez de créer et cliquez sur **Modifier les règles de revendication**.

La configuration des règles de revendication va rendre possible la communication entre l'IDP et la plateforme Oodrive.

Établir la correspondance entre les variables

Cette étape consiste à faire correspondre entre elles les variables utilisées par chaque entité afin de garantir la viabilité des échanges de données.

1. Cliquez sur le bouton **Ajouter une règle**.

2. Dans la liste déroulante **Modèle de règle de revendication**, sélectionnez **Envoyer les attributs LDAP en tant que revendications**, puis cliquez sur **Suivant**.

3. Dans le champ **Nom de la règle de revendication**, saisissez **AD-Rules**.

4. Dans la liste déroulante **Magasin d'attributs**, sélectionnez **Active Directory**.

5. Dans la grille **Mappage des attributs LDAP aux types de revendications sortantes**, faites les associations suivantes :

Attribut LDAP	Type de revendication sortante
SAM-Account-Name	Name ID
E-Mail-Addresses	auth-login
Company	auth-company
E-Mail-Addresses	auth-mail
Given-Name	auth-givenname
Surname	auth-surname

   Remarque : Pour effectuer les associations optionnelles, veuillez consulter les définitions qui se trouvent dans la rubrique **Authentification** du module de Gestion des accès, sous **Claims de configuration par défaut**.

6. Cliquez sur **Terminer**.

Configurer le type d'utilisateur par défaut

Lorsque vos collaborateurs se connectent pour la première fois à l'espace de travail avec leurs identifiants LDAP, un compte leur est automatiquement créé. Cette étape permet d'indiquer à la plateforme Oodrive de leur créer des comptes de type Utilisateur ou Contact.

1. Cliquez sur le bouton **Ajouter une règle**.

2. Dans la liste déroulante **Modèle de règle de revendication**, sélectionnez **Envoyer les revendications en utilisant une règle personnalisée**, puis cliquez sur **Suivant**.

3. Dans le champ **Nom de la règle de revendication**, saisissez **auth-usertype**.

4. Dans le champ **Règle personnalisée**, renseignez l'une des règles suivantes :
    - Pour créer des comptes de type Utilisateur : **=> issue(Type = "auth-usertype", Value = "USER")**
    - Pour créer des comptes de type Contact : **=> issue(Type = "auth-usertype", Value = "CONTACT")**

5. Cliquez sur **Terminer**.

Configurer le stockage par défaut

L'espace de stockage alloué à un Utilisateur ne peut en aucun cas être nul. Cette étape consiste à configurer l'espace de stockage par défaut alloué aux collaborateurs à la création de leur compte.

1. Cliquez sur le bouton **Ajouter une règle**.

2. Dans la liste déroulante **Modèle de règle de revendication**, sélectionnez Envoyer les revendications en utilisant une règle personnalisée, puis cliquez sur **Suivant**.

3. Dans le champ **Nom de la règle de revendication**, saisissez **auth-storage**.

4. Dans le champ **Règle personnalisée**, renseignez la règle suivante : **=> issue(Type = "auth-storage", Value = "5G") ;**

    Veuillez noter : Cette règle permet de configurer un stockage par défaut de 5 Go. Le responsable de provisioning pourra modifier cette valeur ultérieurement depuis le module de **Gestion des utilisateurs**.

5. Cliquez sur **Terminer**.

Une fois que vous avez terminé de configurer les trois règles de revendication, cliquez sur **OK**.

Vous avez terminé la configuration du SSO par SAML. Vos utilisateurs peuvent désormais accéder à leur espace de travail grâce à leurs identifiants d'entreprise.

Suspendre le provisionnement automatique des comptes

Si vous souhaitez garder la main sur le provisionnement des utilisateurs de votre espace et gérer la création des comptes utilisateurs de façon manuelle, vous avez la possibilité de désactiver le provisionnement automatique des comptes.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Authentification**.

2. Cliquez sur le menu déroulant, puis sélectionnez **SAML**.

3. Rendez-vous dans la section **Liste des fichiers metadatas sur le NAS** et cliquez sur l'icône de crayon à droite de votre fichier de métadonnées.

4. Dans la fenêtre **Modifier le mapping des champs**, rendez-vous dans la section **Création Auto** et cochez **Non**.

5. Cliquez sur **Enregistrer**.

Revenez dans ce menu à tout moment pour réactiver le provisionnement automatique des comptes.

2.3. Kerberos (Active Directory)

Le SSO (Single Sign-On ou authentification unique) par Kerberos permet de gérer l'authentification par un protocole de chiffrement symétrique. Le service principal de Kerberos est une identité unique à laquelle Kerberos peut fournir des tickets de connexion. Cela signifie que chaque utilisateur doit être associé à un service unique afin de configurer ce type de protocole d'authentification.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Authentification**.

2. Cliquez sur le menu déroulant, puis sélectionnez **Kerberos**.

3. Si vous voulez appliquer ce mode d'authentification à tous les utilisateurs de l'espace, sans exception, cochez **Forcer ce type d'authentification**.

   Attention : Vous ne devez pas cocher cette option si vous avez prévu d'activer l'authentification sans mot de passe sur votre espace.

4. Cliquez sur le bouton **Appliquer**, puis cliquez sur le bouton **Parcourir** pour chercher et sélectionner un fichier keytab de votre arborescence de fichiers.

5. Répétez jusqu'à ce que vous ayez importé tous les fichiers keytab sur le serveur de stockage en réseau.

6. Saisissez le nom du service principal, puis cliquez sur le bouton Importer.

Revenez à la rubrique **Authentification** pour modifier ce protocole d'authentification à tout moment.

2.4. OpenID Connect

L'authentification par OpenID Connect permet à la plateforme Oodrive de vérifier l'identité d'un utilisateur en se basant sur l'identification fournie par un serveur d'authentification externe comme Github, Google, Okta, ou tout autre service compatible.

Afin de sécuriser et contrôler au mieux les accès à votre espace, seuls les fournisseurs d'identité que vous aurez préalablement enregistrés depuis le module de Gestion des accès pourront être utilisés pour accéder à votre espace via OpenID Connect.

Veuillez noter : Les services externes que vous configurez permettent uniquement d'authentifier un collaborateur et n'ont aucunement accès aux données stockées sur votre espace.

Pour se connecter à votre espace de travail via OpenID Connect, le collaborateur devra suivre les étapes ci-dessous.

Étape 1 : Accès à la page de connexion de l'espace

L'utilisateur se rend sur la page de connexion de votre espace de travail, puis clique sur le bouton Suivant qui se trouve sous « Veuillez vous connecter avec vos identifiants de connexion d'entreprise ».

Étape 2 : Sélection du service

L'utilisateur sélectionne le service par lequel il souhaite se connecter, parmi ceux que vous avez configuré.

Attention : Il est déconseillé de sélectionner l'un des services préconfigurés (Google, Github, Okta) lorsque vous effectuez la configuration d'OpenID Connect, car tous les utilisateurs disposant d'un compte auprès de cet acteur pourront accéder à votre espace, sans restrictions particulières.

Étape 3 : Connexion au service

L'utilisateur est redirigé sur le processus de connexion habituel du service sélectionné.

Une fois la connexion établie, la plateforme Oodrive récupère automatiquement le nom, prénom et adresse e-mail de l'utilisateur et lui crée un compte sur votre espace de travail.

Étape 4 : Accès à l'espace de travail

L'utilisateur accède à votre espace de travail via le compte qui vient de lui être créé.

Configurer OpenID Connect

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Authentification**.

2. Cliquez sur le menu déroulant, puis sélectionnez **OpenID Connect**.

3. Si vous voulez appliquer ce mode d'authentification à tous les utilisateurs de votre espace, sans exception, cochez **Forcer ce type d'authentification**.

   Attention : Vous ne devez pas cocher cette option si vous avez prévu d'activer l'authentification sans mot de passe sur votre espace.

4. Cliquez sur le bouton **Appliquer**, puis cliquez sur **Nouvelle configuration** pour configurer un nouveau fournisseur d'identité.

5. Renseigner le **Nom de la configuration**, puis sélectionnez **Autre** dans la liste déroulante **Fournisseur d'identité**.

   Attention : Il est déconseillé de configurer OpenID Connect avec l'un des services préconfigurés (Google, Github, Okta). Nous vous recommandons plutôt de configurer vous-même ces services en sélectionnant l'option **Autre**, afin que seuls vos employés puissent accéder à votre espace.

6. Renseignez les champs de la section **Connexion**. Tous les champs du formulaire sont requis.

7. Lorsque vous avez terminé, cliquez sur le bouton **Créer**.

8. Cliquez sur le fournisseur d'identité que vous venez d'ajouter et copiez le lien situé dans la section **Lien à transmettre au fournisseur d'authentification OpenID**.

   Vous devez transmettre ce lien à votre fournisseur d'identité pour finaliser la configuration d'OpenID Connect.

Revenez à la rubrique **Authentification** pour modifier cette option à tout moment.

3. Gérer la complexité des mots de passe

Sommaire

Pour renforcer la robustesse du mot de passe des utilisateurs de votre espace et améliorer le niveau de sécurité de vos données, vous pouvez exiger l'utilisation d'un mot de passe d'une certaine longueur, composé d'une combinaison spécifique de caractères (des lettres, des chiffres, et/ou des caractères spéciaux) de votre choix.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Gestion mots de passe**.

2. Définissez les caractéristiques suivantes du mot de passe des utilisateurs :

    - la taille minimum (16 caractères par défaut) ;
    - le nombre minimum de lettres et de chiffres (1 lettre et 1 chiffre par défaut) ;
    - l'utilisation des caractères spéciaux (option désactivée par défaut).

3. Si vous souhaitez être notifié en cas d'échec de connexion d'un utilisateur, cochez l'option **M'avertir par e-mail en cas d'échec de connexion**.

    Un e-mail vous sera envoyé au bout de cinq échecs consécutifs.

4. Par défaut, le mot de passe des utilisateurs expirera tous les trois mois.

    - Pour désactiver l'expiration automatique du mot de passe, décochez l'option **Activer l'expiration des mots de passe**.
    - Pour prolonger le délai d'expiration des mots de passe à 6 ou 12 mois, cochez **après 6 mois** ou **après 12 mois**.

5. Cliquez sur le bouton **Enregistrer** en bas de la page pour confirmer votre sélection.

4. Configurer les options d'authentification

Sommaire

Le module de Gestion des accès vous permet de configurer au choix l'**authentification à deux facteurs** ou bien l'**authentification sans mot de passe**.

Présentation des options d'authentification		
	Authentification sans mot de passe	**Authentification à deux facteurs**
Description	Une connexion à l'espace de travail à l'aide d'un appareil mobile ou d'une clé de sécurité Yubikey, sans mot de passe	Une étape d'authentification supplémentaire au simple mot de passe
Compatibilité avec un protocole externe		
LDAP		●
SAML		●
Kerberos		●
Modes d'authentification disponibles		
Code de sécurité SMS	●	●
Code de sécurité éphémère	●	●
Clé de sécurité	●	●

Remarque : L'autorisation d'une option d'authentification sur votre espace vous laisse la possibilité de personnaliser la configuration sur chaque fiche utilisateur. En revanche, l'imposition d'une option d'authentification la rendra obligatoire pour l'ensemble des utilisateurs de votre espace.

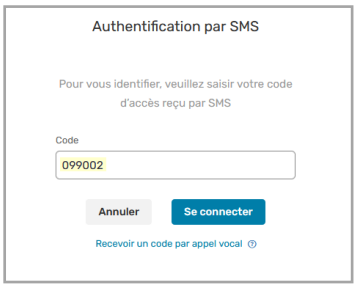
4.1. Présentation générale des options d'authentification

Le code de sécurité SMS

Le code SMS permet à l'utilisateur de réceptionner un code de sécurité par réseau mobile sur son téléphone portable, sans besoin d'une connexion internet. Si le code n'est pas bien reçu par SMS, l'utilisateur peut demander à le recevoir par appel vocal depuis la page de saisie du code SMS.

Réception du code

Saisie du code



Suite à 5 échecs consécutifs d'authentification par code de sécurité SMS, un utilisateur verra son compte bloqué. Il pourra le débloquer en sollicitant l'intervention d'un Administrateur ou bien en réussissant une connexion avec un nouveau code de sécurité reçu par email.

À noter : Le code de sécurité par SMS est un module supplémentaire qui est uniquement disponible si activé au préalable pour votre espace.

Le code de sécurité éphémère

Ce type de code de sécurité est compatible avec toute application d'authentification qui génère des codes de sécurité (ex: Oodrive Authenticator, Google Authenticator, Microsoft Authenticator, etc.).

Nous vous recommandons l'application Oodrive Authenticator, développée spécialement pour permettre à vos utilisateurs de s'authentifier à Oodrive via code éphémère.

Génération du code éphémère

Saisie du code éphémère

Pour se servir de ce mode d'authentification lors de sa première connexion, l'utilisateur devra suivre les étapes ci-dessous.

Étape 1 : Installation sur smartphone

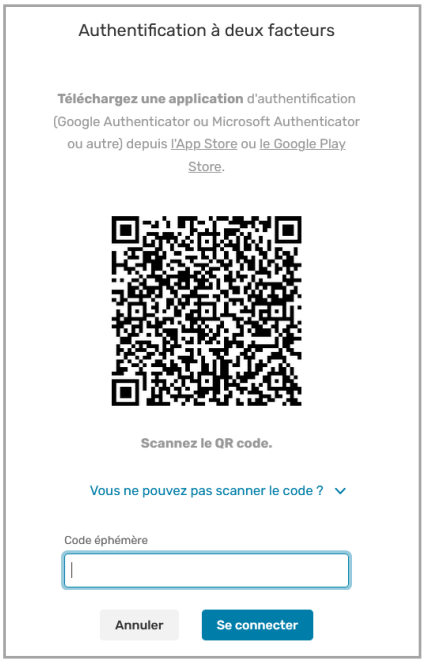
Téléchargement et installation de l'application d'authentification de son choix sur appareil mobile.

Étape 2 : Connexion à l'espace de travail via navigateur web

L'utilisateur se rend sur la page de connexion de son espace de travail et se connecte à l'aide de ses identifiants Oodrive ou de ses identifiants d'entreprise.

Étape 3 : Association de l'application d'authentification à l'espace de travail

Lors du premier usage, l'utilisateur accédera à la page d'authentification à deux facteurs ci-dessous :



À l'aide de l'application d'authentification téléchargée au préalable sur smartphone ou tablette, l'utilisateur pourra scanner le QR code qui se présente sur cette page afin d'associer l'application d'authentification mobile avec son espace de travail.

Lors des prochaines connexions, après avoir saisi ses identifiants, l'utilisateur accédera directement à la page de double authentification pour renseigner le code éphémère généré par son application d'authentification.

Suite à 5 échecs consécutifs d'authentification par code éphémère, un utilisateur verra son compte bloqué. Il pourra le débloquer en sollicitant l'intervention d'un Administrateur ou bien en réussissant une connexion avec un nouveau code de sécurité reçu par email.

Remarque : En cas de perte ou de changement d'appareil mobile, veuillez contacter le responsable de provisioning de votre espace.

La clé de sécurité Yubikey

L'authentification par clé de sécurité est disponible uniquement pour les navigateurs suivants :

- Google Chrome version 67
- Mozilla Firefox version 60
- Microsoft EdgeHTML 18

Lors de sa première connexion avec ce mode d'authentification, l'utilisateur devra suivre les étapes ci-dessous.

Étape 1 : Connexion à l'espace de travail via navigateur web

L'utilisateur se rend sur la page de connexion de son espace de travail et se connecte à l'aide de ses identifiants Oodrive ou de ses identifiants d'entreprise.

Étape 2 : Insertion de la clé de sécurité

L'utilisateur est invité par son navigateur à insérer sa clé de sécurité dans l'ordinateur.

Étape 3 : Saisie du code PIN

Lors du premier usage de la clé de sécurité, l'utilisateur est invité par son navigateur à définir un code PIN. Pour cela, il doit saisir son nouveau code PIN, puis le confirmer.

Lors des connexions suivantes, l'utilisateur devra simplement insérer sa clé de sécurité et renseigner le code PIN préalablement défini.

Étape 4 : Appui sur la clé de sécurité

L'utilisateur touche sa clé de sécurité pour compléter l'authentification. Il accède alors à son espace de travail.

À noter : L'authentification par clé de sécurité est un module supplémentaire qui est uniquement disponible si activé au préalable pour votre espace.

4.2. Configurer l'authentification à deux facteurs

L'authentification à deux facteurs vous permet de renforcer la sécurité de votre espace en rajoutant une étape d'authentification supplémentaire au simple mot de passe.

Vous pouvez configurer l'authentification à deux facteurs de deux manières :

- **Autoriser** l'activation d'un second facteur, afin de laisser au responsable de provisioning de votre espace le choix d'activer *ou non* la double authentification pour un utilisateur.
- **Imposer** l'usage de la double authentification à tous les utilisateurs de votre espace, auquel cas le responsable de provisioning devra obligatoirement sélectionner un mode de double authentification pour chaque utilisateur.

Autoriser l'activation d'un second facteur

Si vous autorisez l'authentification à deux facteurs, le responsable de provisioning de votre espace aura la possibilité d'activer ou non la double authentification pour chaque utilisateur.

1. Dans le module **Gestion des accès**, cliquez sur **Auth. à deux facteurs**.
2. Cochez l'option **Activer l'authentification à deux facteurs**.
3. Sélectionnez **Autoriser la sélection d'un deuxième facteur d'authentification**.
4. Cochez le ou les modes d'authentification que vous voulez rendre disponible au responsable du provisioning (**SMS**, **Code éphémère** et/ou **Clé de sécurité**).
5. Cliquez sur le bouton **Enregistrer** en bas de la page.

Revenez à la rubrique **Auth. à deux facteurs** pour modifier ou désactiver l'authentification à deux facteurs.

Imposer le second facteur à tous les utilisateurs

Si vous imposez l'authentification à deux facteurs, le responsable du provisioning de votre espace devra obligatoirement attribuer un mode de double authentification pour chaque nouvel utilisateur.

Attention : Pour les anciens utilisateurs (créés avant l'imposition du second facteur), le second facteur ne sera pas activé tant que le responsable du provisioning n'aura pas mis à jour leur fiche utilisateur.

1. Dans le module **Gestion des accès**, cliquez sur **Auth. à deux facteurs**.
2. Cochez l'option **Activer l'authentification à deux facteurs**.
3. Sélectionnez **Imposer l'authentification à deux facteurs**.

4. Cochez le ou les modes d'authentification que vous voulez rendre disponible au responsable du provisioning (**SMS**, **Code éphémère** et/ou **Clé de sécurité**).

   Attention : Si vous forcez la clé de sécurité ou le code SMS comme unique mode d'authentification, les utilisateurs qui ne disposent pas d'une Yubikey ou pour lesquels il manque les bons numéros téléphone n'auront pas la possibilité de se connecter à leur espace de travail.

5. Cliquez sur le bouton **Enregistrer** en bas de la page.

Revenez à la rubrique **Auth. à deux facteurs** pour modifier ou désactiver l'authentification à deux facteurs.

4.3. Configurer l'authentification sans mot de passe

L'authentification sans mot de passe permet à vos utilisateurs de se connecter directement à leur espace à l'aide de leur appareil mobile ou de leur clé de sécurité Yubiley, sans avoir à renseigner de mot de passe.

Veuillez noter : Il est impossible d'utiliser l'authentification sans mot de passe pour un utilisateur créé via un protocole d'authentification externe.

Vous pouvez configurer l'authentification sans mot de passe de deux manières :

- **Autoriser** l'authentification sans mot de passe, afin de laisser au responsable de provisioning de votre espace le choix de l'activer ou non pour un utilisateur.
- **Imposer** l'usage de l'authentification sans mot de passe à tous les utilisateurs de votre espace, auquel cas le responsable de provisioning devra sélectionner un mode d'authentification pour chaque utilisateur.

Autoriser l'authentification sans mot de passe

Si vous autorisez l'authentification sans mot de passe, le responsable de provisioning de votre espace aura la possibilité de l'activer ou non pour chaque utilisateur.

1. Dans le module **Gestion des accès**, cliquez sur **Auth. à deux facteurs**.

2. Cochez l'option **Activer l'authentification à deux facteurs**.

3. Sélectionnez **Autoriser la sélection d'un deuxième facteur d'authentification**.

4. Cochez le ou les modes d'authentification que vous voulez rendre disponible au responsable du provisioning (**SMS**, **Code éphémère** et/ou **Clé de sécurité**).

5. Cochez l'option **Sans mot de passe**.

6. Cliquez sur le bouton **Enregistrer** en bas de la page.

Revenez à la rubrique **Auth. à deux facteurs** pour modifier ou désactiver l'authentification sans mot de passe.

Imposer l'authentification sans mot de passe

Si vous imposez l'authentification sans mot de passe, le responsable de provisioning de votre espace devra choisir un mode d'authentification pour chaque utilisateur.

Attention : Pour les utilisateurs (créés avant l'imposition du second facteur), l'authentification sans mot de passe ne sera pas activée tant que le responsable du provisioning n'aura pas mis à jour leur fiche utilisateur.

1. Dans le module **Gestion des accès**, cliquez sur **Auth. à deux facteurs**.
2. Cochez l'option **Activer l'authentification à deux facteurs**.
3. Sélectionnez **Imposer l'authentification à deux facteurs**.
4. Cochez le ou les modes d'authentification que vous voulez rendre disponible au responsable du provisioning (**SMS**, **Code éphémère** et/ou **Clé de sécurité**).

   Attention : Si vous forcez la **clé de sécurité** ou le **code SMS** comme unique mode d'authentification, les utilisateurs qui ne disposent pas d'une Yubikey ou pour lesquels il manque les bons numéros téléphone n'auront pas la possibilité de se connecter à leur espace de travail .
5. Cochez l'option **Sans mot de passe**.
6. Cliquez sur le bouton **Enregistrer** en bas de la page.

Revenez à la rubrique **Auth. à deux facteurs** pour modifier ou désactiver l'authentification sans mot de passe.

5. Configurer le filtrage d'adresse IP

Sommaire

Afin de mettre en place un niveau de sécurité supplémentaire, vous pouvez bloquer ou autoriser l'accès de certains postes à votre espace. En filtrant l'accès par adresse IP, vous limiterez directement les postes et appareils mobiles qui pourront se connecter aux applications de l'espace de travail.

5.1. Activer le filtrage d'adresse IP

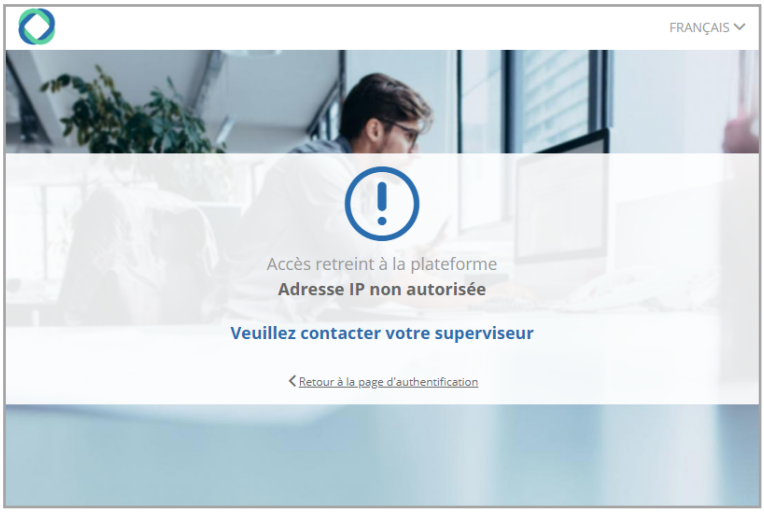
1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Filtrage IP**.
2. Cochez l'option **Activer le filtrage d'adresse IP**.
3. Sélectionnez la manière dont vous voulez filtrer les adresses IP :
   - **en autorisant** (le filtrage par inclusion) ou,
   - **en interdisant** (le filtrage par exclusion).

   Veuillez noter : Il n'est pas possible de mettre en place le filtrage par inclusion et exclusion à la fois.
4. Saisissez une adresse IP dans le champ fourni, puis cliquez sur Ajouter.

   Remarque : Vous avez également la possibilité de renseigner des plages d'adresses IP.
5. En bas de la page, cliquez sur **Enregistrer**.
6. Répétez les étapes 4 et 5 pour ajouter d'autres adresses IP.

L'activation du filtrage d'adresse IP s'appliquera lors de la prochaine connexion d'un utilisateur sur l'adresse IP filtrée.

Message d'adresse IP non autorisée



5.2. Désactiver le filtrage d'adresse IP

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Filtrage IP**.
2. Décochez l'option **Activer le filtrage d'adresse IP**.
3. En bas de la page, cliquez sur **Enregistrer**.

Vos filtres resteront disponibles la prochaine fois que vous activez cette option.

5.3. Supprimer un filtre d'adresse IP

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Filtrage IP**.
2. Ensuite, dans la liste d'adresses autorisée ou non autorisée, cliquez sur la petite corbeille à droite de l'adresse IP à supprimer.

   Astuce : Si vous sectionnez la mauvaise adresse IP par erreur, cliquez sur le bouton **Réinitialiser** en bas de la page pour annuler l'action.
3. Cliquez sur **Enregistrer** pour effectuer la modification.

6. Gérer l'accès aux applications mobiles et de bureau

Sommaire

6.1. Applications mobiles

Par défaut, les utilisateurs peuvent se connecter à l'espace de travail de votre société depuis smartphone et tablette par les applications mobiles d'oodrive (notamment, BoardNox, oodrive_meeting, Oodrive mobile et oodrive_share). Cependant, si vous préférez ne pas autoriser les utilisateurs à se servir des applications mobiles, vous pouvez modifier cette option.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Apps mobiles et desktop**.

2. Dans la section **Applications mobiles**, cochez **Non** pour désactiver l'accès aux applications mobiles.

3. En bas de la page, cliquez sur **Enregistrer**.

Lors des prochaines tentatives de connexion à votre espace de travail sous application mobile, l'utilisateur recevra un message d'interdiction :

Vous pouvez réactiver l'accès aux applications mobiles à tout moment.

À noter : La désactivation de l'accès aux applications mobiles n'empêchera pas pour autant l'accès à l'espace de travail via le navigateur web d'un appareil mobile.

Pour interdire l'accès par appareil mobile, il est recommandé d'activer le filtrage d'adresses IP pour tous les appareils sur lesquels vos utilisateurs sont susceptibles à se connecter. Vous pouvez également inclure un paragraphe sur le sujet dans vos conditions générales d'utilisation.

6.2. Applications de bureau

Plusieurs applications de bureau sont disponibles sur votre espace de travail afin de permettre aux utilisateurs de gérer et partager leurs documents plus facilement au quotidien (EasyTransfer, WebSynchro, Plugin Outlook). Cependant, si vous préférez ne pas autoriser les utilisateurs à se servir des applications de bureau, vous pouvez choisir de les désactiver.

1. Dans le module **Apps mobiles et desktop**, cliquez sur la rubrique **Apps mobiles et desktop**.

2. Dans la section **Applications desktop**, cochez **Non** pour désactiver l'accès aux applications de bureau.

3. En bas de la page, cliquez sur **Enregistrer**.

Les utilisateurs ne seront désormais plus en mesure d'accéder à votre espace de travail avec une application de bureau.

Vous pouvez réactiver l'accès aux applications de bureau à tout moment.

7. Afficher des conditions générales d'utilisation (CGU)

Sommaire

Veuillez noter : Le nouveau module **Administration des textes légaux** est désormais disponible pour une gestion plus avancée des CGU et autres textes légaux.

Une fois que vous aurez configuré un premier texte dans le module **Administration des textes légaux**, la rubrique **CGU** du module **Gestion des accès** sera désactivée.

Si vous avez des conditions générales d'utilisation (CGU) à communiquer aux collaborateurs de votre espace avant qu'ils y accèdent, vous pouvez activer cette option. Suite à toute modification des CGU, vous aurez la possibilité de les afficher à nouveau aux utilisateurs de votre espace.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **CGU**.

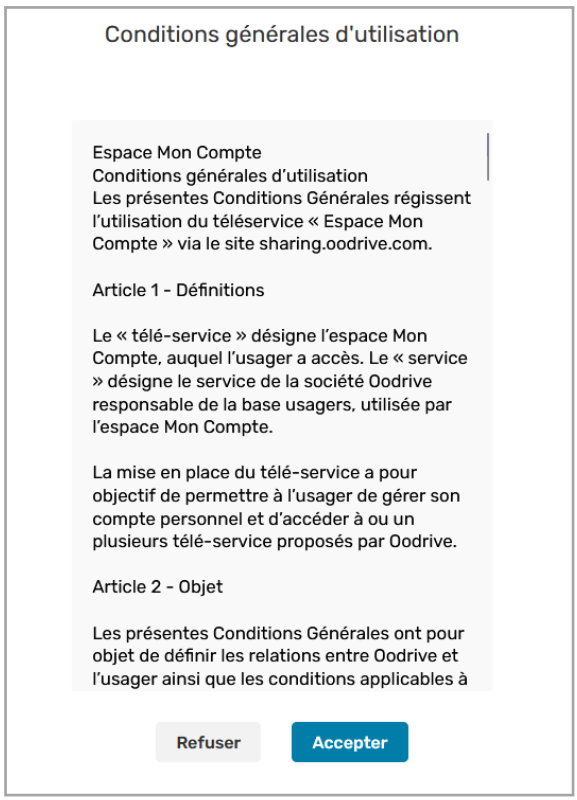
2. Cliquez sur **Oui**.

3. Saisissez ou collez le texte des conditions générales d'utilisation à faire apparaître sur les écrans des utilisateurs suite à leur première connexion à l'espace de travail.

4. Choisissez la fréquence d'affichage des CGU :
   - à la première connexion, ou
   - à chaque connexion.

5. Cliquez sur le bouton **Enregistrer** en bas à gauche de la page pour sauvegarder vos changements et activer l'affichage des CGU.

La prochaine fois qu'un utilisateur se connectera à l'espace de travail, il sera demandé d'accepter les CGU avant de pouvoir y accéder.



Pour réactualiser les conditions générales d'utilisation :

1. Dans la zone de saisie, modifiez les CGU.
2. Cliquez sur le bouton **Enregistrer** pour sauvegarder vos modifications.
3. Dans le coin supérieur droit de la page, cliquez sur le bouton **Réinitialiser l'acceptation** pour afficher à nouveau la page des CGU à tout utilisateur de votre espace.
4. Cliquez sur le bouton **Réinitialiser** pour confirmer.

8. Superviser les tentatives d'authentification

Sommaire

La rubrique **Échecs d'auth**. vous permet de consulter les tentatives de connexion à votre espace qui se sont soldées par un échec.

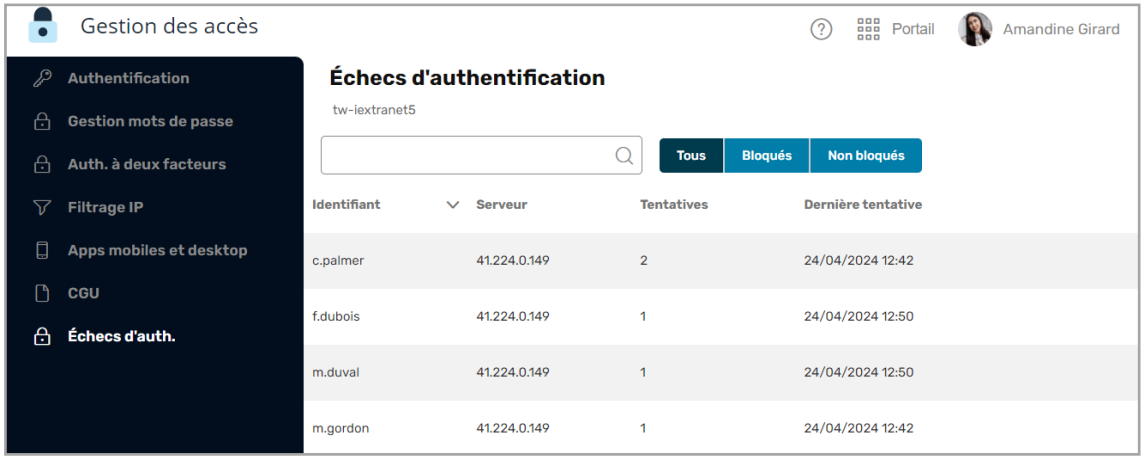
Ces tentatives en échec peuvent être le résultat d'un filtrage par adresse IP ou d'un oubli de mot de passe de la part de vos utilisateurs, mais elles peuvent également vous aider à identifier une éventuelle activité suspecte sur votre espace.

Par mesure de sécurité, la plateforme Oodrive bloque automatiquement le compte d'un utilisateur après 5 tentatives de connexion en échec. En tant qu'Administrateur vous avez la possibilité d'intervenir pour débloquer le compte d'un utilisateur de votre espace.

8.1. Consulter les tentatives de connexion en échec

1. Dans le module **Gestion des accès**, cliquez sur la rubrique Échecs d'auth.

2. Vous visualisez l'ensemble des tentatives de connexion en échec et leurs caractéristiques :
   - Identifiant du compte,
   - Adresse IP,
   - Nombre de tentatives en échec pour le couple compte/adresse IP.



Remarque : Lorsque la connexion est réussie pour un couple compte/adresse IP, il disparaît de la liste des échecs d'authentification et le nombre de tentatives en échec est réinitialisé.

3. Vous pouvez filtrer la liste par statut de compte, en cliquant sur le bouton **Bloqués** ou **Non bloqués**.

8.2. Débloquer un compte

Lorsqu'un compte est bloqué, l'utilisateur sera invité à saisir, en complément de son mot de passe, un code de sécurité reçu par e-mail pour débloquer son compte. Vous avez également la possibilité, en tant qu'administrateur, de débloquer un compte directement depuis le module de Gestion des accès.

1. Dans le module **Gestion des accès**, cliquez sur la rubrique **Echecs d'auth**.

2. Cliquez sur le bouton **Bloqués** pour accéder à la liste des comptes bloqués.

3. Identifiez le compte que vous souhaitez débloquer et cliquez sur le bouton **Débloquer** associé.

4. Cliquez sur **Débloquer** pour confirmer votre choix.

   L'utilisateur pourra alors se reconnecter normalement, sans avoir à saisir de code de sécurité.

   Veuillez noter :

   - Si un utilisateur a bloqué son compte car il a oublié son mot de passe, le responsable de provisioning peut le réinitialiser depuis le module Utilisateurs. L'utilisateur recevra alors un e-mail lui permettant de définir un nouveau mot de passe.
   - Si un utilisateur a bloqué son compte après 5 échecs consécutifs d'authentification par code de sécurité, il a la possibilité de le débloquer lui-même en renseignant un nouveau code de sécurité reçu par email. En cas de perte ou de changement d'appareil mobile, le responsable de provisioning pourra modifier le second facteur d'authentification depuis le module Utilisateurs.

Lorsque vous débloquez un compte, il disparaît de la liste des échecs d'authentification et le nombre de tentatives en échec est réinitialisé.


∞drive