∞drive suite

Administrator Guide

Access management

Terms of use

Distribution list

Company	Role
Oodrive Group	Oodrive Group colleagues and customers

Contents

1. Getting started configuring your workspace 5

1.1. Compatibility 8

Operating systems 8

Web browsers 8

Other software 8

1.2. Log in to your workspace 9

Log in with your Oodrive login credentials 9

Log in with your company login credentials 11

1.3. Overview of the Access Management module 12

1.4. Browse the Access Management module 13

2. Configuring an external authentication protocol 14

2.1. Lightweight Directory Access Protocol (LDAP) 14

2.2. Security Assertion Markup Language (SAML) 16

Step 1: Define the authentication type 16

Step 2: Exchange metadata files 16

Step 3: Configure the relying party trust on your AD FS server 17

Step 4: Configure the claim rules 18

Disable automatic account provisioning 20

2.3. Kerberos (Active Directory) 21

2.4. OpenID Connect 21

Configuring OpenID Connect 22

3. Managing password complexity 24

4. Configuring authentication options 25

4.1. General presentation of the authentication options 26

SMS security code 26

TOTP security code 26

Yubikey security key 28

4.2. Configuring two-factor authentication 28

Allow activation of a second authentication factor 29

Require a second authentication factor for all users 29

4.3. Configuring passwordless authentication 30

Allow passwordless authentication 30
Require passwordless authentication 31
5. Configuring IP address filtering 32
5.1. Enable IP address filtering 32
5.2. Disable IP address filtering 33
5.3. Remove the IP address filter 33
6. Managing access to mobile and desktop applications 34
6.1. Mobile applications 34
6.2. Desktop applications 35
7. Displaying terms of service (TOS) 36
8. Monitoring authentication attempts 38
8.1. View failed login attempts 38
8.2. Unlock an account 39

1. Getting started configuring your workspace

Summary

As an Oodrive account holder with administrative rights, you have been made administrator of one or more administration modules on your company's workspace.

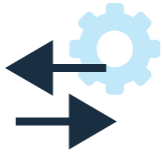
As a result, you are responsible for configuring a certain number of options relating to the behavior of applications offered to your organization's employees.

Several administration modules may be available to you in the Oodrive Suite portal, depending on how these responsibilities have been assigned within your company.

Some administration modules are shared between all Oodrive solutions and allow you to configure and monitor your workspace as a whole :

Shared administration modules	
Access Management 	• Configuration of workspace access and authentication Access documentation
User Management 	• Management of workspace users Access documentation
Custom Graphics Management 	• Configuration of the workspace name, logos and colors Access documentation
Activity Tracking 	• Activity tracking for all workspace users Access documentation
Administration of Legal Notices 	• Management of legal notices and approval by workspace users Access documentation

Other administration modules are dedicated to a specific solution. These modules allow you to configure each application according to the needs of your organization :

Solution-specific administration modules	
Sharing Administration 	• Module dedicated to Oodrive Work_share and Oodrive Work • Configuration of options for sharing and collaboration applications • Monitoring of user activities Access documentation
Work Administration 	• Module dedicated to Oodrive Work • Teamspace management Access documentation
Backup Management 	• Module dedicated to Oodrive Save • Configuration of savesets and backup policies for your user base Access documentation
Oodrive Media Administration 	• Module dedicated to Oodrive Media • Configuration of the Media Library application Access documentation
Oodrive Meet Administration 	• Module dedicated to Oodrive Meet • Configuration of meeting options Access documentation

An administrator guide is available for each of these modules in order to assist you in configuring your workspace, depending on your role.

Please note: Only Oodrive technical support can be responsible for assigning and modifying administration rights. As a result, the administration modules to which you have access depend on the configuration defined by Oodrive support and its main point of contact within your company.

1.1. Compatibility

Oodrive solutions run on different operating systems and browsers. You will find the list of compatible versions below:

Operating systems

- **Windows**

  Operating systems covered by Microsoft standard support (Cf. Windows lifecycle: http://windows.microsoft. com/en-us/windows/lifecycle)

- **MacOs et iOS**

  Major versions n and n-1 (current and previous)

- **Android**

  Major versions n and n-1 (current and previous)

Web browsers

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

  Major versions n and n-1 (current and previous)

- **Safari**

  Latest major version available on a compatible Apple operating system

Other software

- **JRE (for applets)**

  JRE (and JDK) supported by Oracle on their respective operating systems

- **Microsoft Outlook**

  Versions covered by Microsoft standard support

1.2. Log in to your workspace

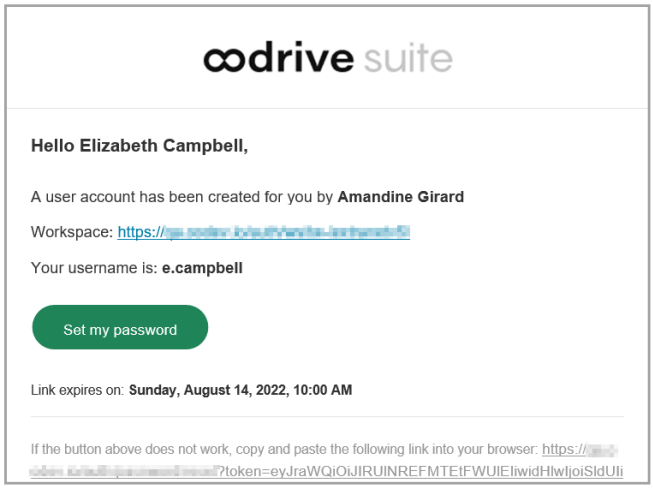
There are two ways to log in to your workspace:

- using your Oodrive login credentials
- using your company login credentials

The login options available on your workspace depend on your Access Management module settings.

Log in with your Oodrive login credentials

1. Retrieve the username emailed to you when your account was created and click **Set my password**.



2. You will be redirected to a browser page asking you to set a password and confirm it before clicking **Validate**.

3. Click **Log in** to access the login page.

   Please note: If the Oodrive login field is not displayed, click **Log in using your login credentials** to access it.

4. Enter your username and click **Next**.

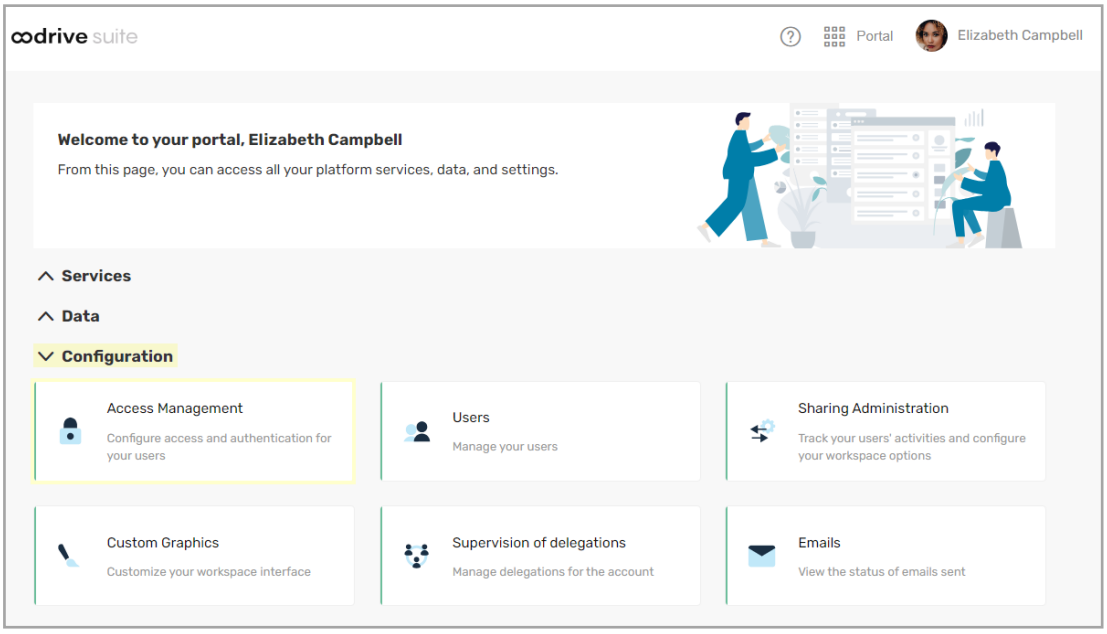
5. Enter the password you have just specified, then click **Log in**.

   Careful: After 5 failed login attempts, a security code will automatically be sent via email. This code will be required in addition to your password.

   If you have forgotten your password, click **Forgot your password?**

   If two-factor authentication has already been configured on your workspace, you will also be asked to enter the code received on your mobile device.

6. Next, you will access the Oodrive Suite portal, where you will find all the applications and configuration modules to which you have access.



To return to the portal at any time, click on 

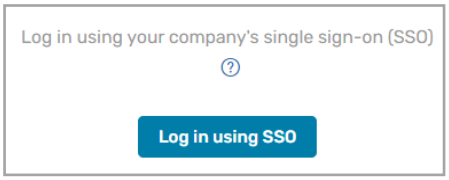
in the upper-right corner of the page, then select **Portal**.

Please note: As a security measure, you will be automatically logged out of your session after 30 minutes of inactivity (or after 4 hours if the Oodrive Work discussion feature is enabled). You can extend your session by clicking **Continue to browse** when the logout warning appears on the screen.

Log out at any time by clicking on your name in the upper-right corner of the page, then on **Logout**.

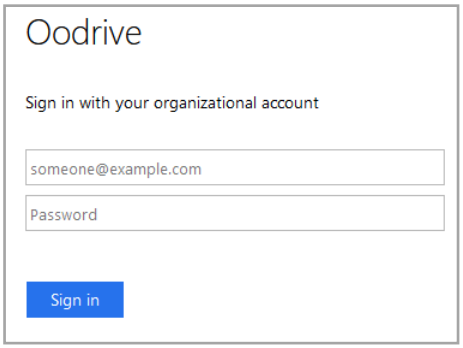
Log in with your company login credentials

1. Click the **Log in using SSO** button.



If the button is not available, click **Log in using your company's single sign-on (SSO)**

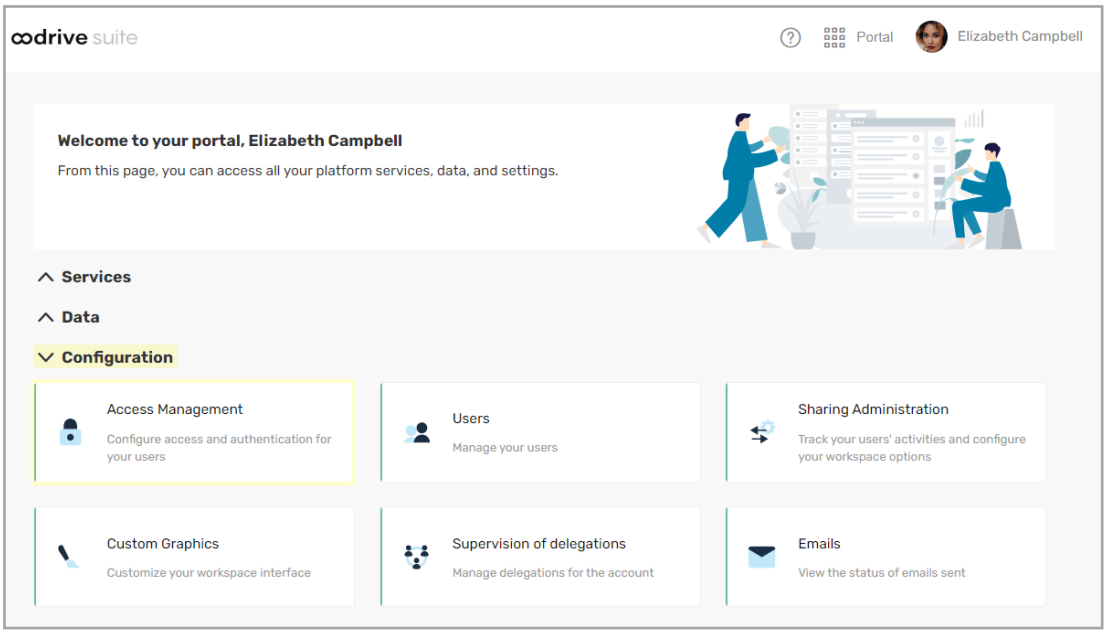
2. Enter your company login credentials and click **Log in**.



If you have forgotten the password associated with your company username, please contact your company's IT administrator.

If two-factor authentication has already been configured on your workspace, you will also be asked to enter the code received on your mobile device.

3. Next, you will access the Oodrive Suite portal where you will find all the applications and configuration modules to which you have access.



To return to the portal at any time, click on 

in the upper-right corner of the page, then select **Portal**.

Please note: As a security measure, you will be automatically logged out of your session after 30 minutes of inactivity (or after 4 hours if the Oodrive Work discussion feature is enabled). You can extend your session by clicking **Continue to browse** when the logout warning appears on the screen.

Log out at any time by clicking on your name in the upper-right corner of the page, then on **Logout**.

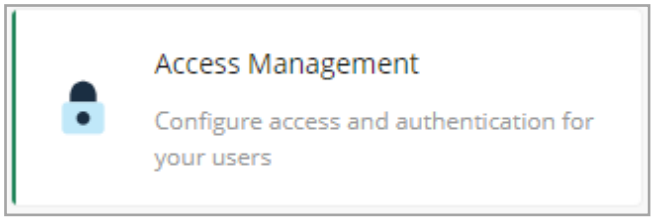
1.3. Overview of the Access Management module

As a user with administrative rights, you are responsible for implementing security settings that are compliant with your company's requirements.

User authentication settings are configured in the Access Management module, which consists of the following access controls:

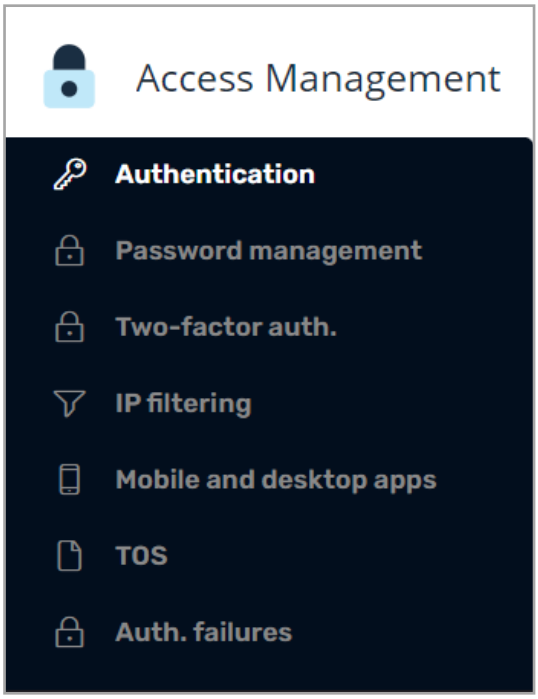
- Authentication protocol (LDAP, SAML, Kerberos)
- Password complexity
- Two-factor authentication
- IP address filtering
- Mobile application access

- Terms of Service (TOS)
- Authentication attempts



1.4. Browse the Access Management module

In the navigation panel on the left side of the page, you can quickly access all of the Access Management module sections.



2. Configuring an external authentication protocol

Summary

Before employees start using the workspace applications, you can choose to set up an external authentication protocol that meets the security settings required by your company.

Four external authentication protocols are available to you:

Available authentication protocols	
Lightweight Directory Access Protocol (LDAP)	Optimal for companies looking to automate the administration of accounts through the use of corporate directory data.
Security Assertion Markup Language (SAML)	Ideal for companies preferring single sign-on (SSO) authentication so that users can log in directly using their business credentials. This authentication protocol is recommended for its simplicity and high level of security.
Kerberos	A good security measure for companies seeking to manage authentication via a symmetric encryption protocol.
Open ID Connect	Ideal for companies seeking to delegate authentication of their employees to a trusted identity provider.

Please note: You can either require authentication via an external authentication protocol or you can allow for its use alongside oodrive credentials.

2.1. Lightweight Directory Access Protocol (LDAP)

The LDAP protocol is a way to perform account provisioning. When activated, the Oodrive platform queries your company directory to check the user name and password entered by the user. If correct, the user logs in, otherwise the login attempt is denied.

Before you proceed with this configuration, we invite you to contact the Oodrive Support Team in order to set up the necessary network firewall rules and allow communication between your LDAP directory and our services.

1. In the **Access Management** module, click on the **Authentication** section.

2. Click on the drop-down menu, then select **LDAP**.

3. If you would like to apply this authentication mode to all workspace users, without exception, check **Require this authentication type**.

   Note: Do not check this option if you plan to enable passwordless authentication on your workspace.

4. Click **Apply**, then click **New configuration**.

5. Indicate a **Configuration name** and the **User type** (user or contact) for which you would like to configure the LDAP protocol.

6. Complete the fields in the **Connection** section, then click **Test** to verify whether the connection can be established.

   In case of an error, check that:

   - You have already provided the information in the **Host** field (your IP adress or domain name) to the Oodrive Support Team
   - Oodrive's public IP is allowed to access your LDAP directory

7. Complete the fields in the **Configuration** section to indicate which users from your LDAP directory should be provisioned in your Oodrive workspace.

8. Complete the fields in the **Attributes** section to set up the automatic provisioning of accounts based on information from your LDAP directory. All fields with a red asterisk are required.

   Careful: The following fields must not be confused. Please use the information provided below to fill them in properly.

   - **Username** : username displayed on the user sheet in your Oodrive workspace
   - **LDAP login** : information allowing users to authenticate to LDAP from the login page of your workspace (E.g. email address, phone number, username...)
   - **LDAP ID** : unique key used to identify a user account in the LDAP directory. This value should not be changed because it links a user's Oodrive account to their LDAP account

9. Click the button **Configuration test** to test the LDAP connection and verify that it works properly.

10. Click **Create** to save your configuration.

11. Once the configuration is complete, click **Synchronize** to proceed with the provisioning of accounts from your LDAP directory.

You can find the accounts provisioned via LDAP in the Utilisateurs administration module.

Return to the **Authentication** section to modify this authentication protocol at any time.

2.2. Security Assertion Markup Language (SAML)

SSO (Single Sign-On or SSO) via SAML allows a user to access multiple applications using their company login credentials.

If the user is already authenticated in the IDP (Identity Provider) when making the login request, they will directly access the solution without needing to re-enter their login credentials.

If, on the other hand, the user is not yet authenticated, they will be redirected to their IDP so they can quickly authenticate and log in to their workspace.

The following procedure will help you configure SAML SSO for the Active Directory Federation Services (AD FS) IDP connected to an LDAP user directory.

Step 1: Define the authentication type

1. In the **Access Management** module, click on the **Authentication** section.
2. Click on the drop-down menu, then select **SAML**.
3. If you would like to apply this authentication mode to all workspace users, without exception, check **Require this authentication type**.

   Note: Do not check this option if you plan to enable passwordless authentication on your workspace.
4. Click **Apply** to confirm your choice.

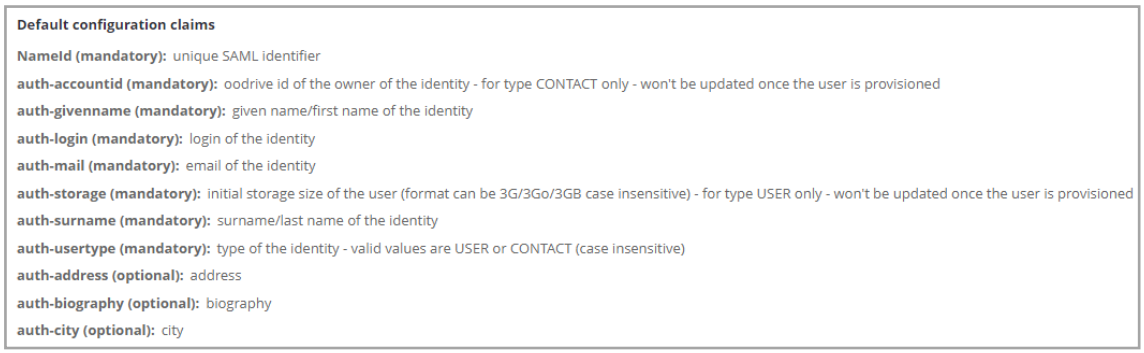
Step 2: Exchange metadata files

In order to establish a relationship of trust between the two entities, and make communication possible, the Oodrive platform and your IDP need to have access to each other's metadata files.

Transfer your metadata file to Oodrive

1. In the **Authentication** section, click **Browse** to search and select your metadata file in XML format, from your computer's file explorer.

   Note: In order to ensure the proper configuration of the configuration claims, please see the definitions found along the bottom of the page before selecting the metadata file.



2. Enter a file name for the network storage server, then click **Import**.

Download Oodrive's metadata file

1. In the **Oodrive SAML server configuration** section, click **Download Oodrive metadata file**.

2. Use your computer's file manager to save the file **spring_saml_metadata.xml**.

This metadata file will allow you to register Oodrive as a trusted party with your IDP.

Step 3: Configure the relying party trust on your AD FS server

1. On the AD FS server, open **AD FS Management**.

2. Expand the **Trust Relationships** folder.

3. Right-click the **Relying Party Trust** folder and select **Add Relying Party Trust**.

   You are accessing the configuration wizard of a relying party trust.

4. Click **Start** to begin the configuration process.

5. At the **Select Data Source** step, select **Import data about the relying party from a file**.

6. Use your file manager to select the file **spring_ saml_ metadata.xml**, which you downloaded in the **Access Management** module.

7. Click **Next**.

8. At the **Specify display name** step, enter **Oodrive** as the relying party trust's display name.

9. Click **Next** until you reach the last step, then click **Close**.

Step 4: Configure the claim rules

Once you finish configuring the relying party trust, you automatically access the claim rules edition window.

Note: If the claim rules edition window does not open automatically, right click the relying party trust you just created and click **Edit Claim Rules**.

Configuring the claim rules will enable communication between the Oodrive platform and your IDP.

Establish correspondence between variables

This step consists in linking the variables of each entity to their counterpart in order to ensure the viability of data exchange.

1. Click **Add Rule**.

2. In the **Claim rule template** drop-down menu, select **Send LDAP Attributes as Claims**, then click **Next**.

3. In the **Claim rule name** field, enter **AD-Rules**.

4. In the **Attribute Store** drop-down menu, select **Active Directory**.

5. In the **Mapping of LDAP attributes to outgoing claim types** table, make the following associations:

LDAP Attribute	Outgoing Claim Type
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

   Note: To make optional associations, please refer to definitions found in the **Authentication** section of the Access Management module, under **Default configuration claims**.

6. Click **Finish**.

Set up the default user type

When your colleagues log in to the workspace for the first time with their LDAP credentials, an account is automatically created for them. This step shows you how to set up platform User or Contact accounts for them.

1. Click **Add Rule**.

2. In the **Claim rule template** drop-down menu, select **Send Claims Using Custom Rule**, then click **Next**.

3. In the **Claim rule name** field, enter **auth-usertype**.

4. In the **Custom rule** field, enter one of the following rules:
   - To create User accounts: **=> issue(Type = "auth-usertype", Value = "USER")**
   - To create Contact accounts: **=> issue (Type = "auth- usertype", Value = "CONTACT")**

5. Click **Finish**.

Set up the default storage

The storage space allocated to a User can never be void. This step consists in setting up the default storage allocated to colleagues when their account is created.

1. Click **Add Rule**.
2. In the **Claim rule template** drop-down menu, select **Send Claims Using Custom Rule**, then click **Next**.
3. In the **Claim rule name** field, enter **auth-storage**.
4. In the **Custom rule** field, enter the following rule: **=> issue(Type = "auth-storage", Value = "5G") ;**

   Please note: This rule sets up a default storage value of 5 GB. Your provisioning manager can later change this value in the **User management** module.
5. Click **Finish**.

Once you finish configuring the three claim rules, click **OK**.

You have finished configuring the SAML SSO. Your users can now access their workspace with their company login credentials.

Disable automatic account provisioning

If you want to keep control over the provisioning of your workspace user, and manage the creation of user accounts manually, you can disable automatic account provisioning.

1. In the **Access management** module, click on the **Authentication** section.
2. Click on the drop-down menu and select **SAML**.
3. Go to the **List of metadata files on the NAS** section and click on the pencil icon to the right of your metadata file.
4. In the **Edit field mapping** window, go to the **Auto Creation** section and select **No**.
5. Click **Save**.

Return to this section at any time to re-enable automatic account provisioning.

2.3. Kerberos (Active Directory)

SSO (Single Sign-On or SSO) via Kerberos allows for managing authentication using a symmetric encryption protocol. Kerberos provides session specific authentication tickets. This means that each user must be associated with a single service in order for this type of authentication protocol to be configured.

1. In the **Access Management** module, click on the **Authentication** section.
2. Click on the drop-down menu, then select **Kerberos**.
3. If you would like to apply this authentication mode to all workspace users, without exception, check **Require this authentication type**.

   Note: Do not check this option if you plan to enable passwordless authentication on your workspace.
4. Click **Apply**, then click **Browse** to search and select your keytab file in XML format, from the file explorer.
5. Repeat until you have imported all the keytab files on the network storage server.
6. Enter the name of the main service, then click **Import**.

Return to the **Authentication** section to modify this option at any time.

2.4. OpenID Connect

Authentication via OpenID Connect allows the Oodrive platform to verify a user's identity using the authentication provided by an external authorization server such as Github, Google, Okta, or any other compatible service.

In order to secure and control access to your workspace, only the identity providers that you have previously registered in the Access Management module can be used to access your workspace via OpenID Connect.

Please note: Configuring an external service only enables the authentication of employees and does not in any case enable access to the data stored on your workspace.

To log in to your workspace using OpenID Connect, users must follow the steps below.

Step 1: Access the workspace login page

The user goes to the workspace login page, then clicks **Next** located under “Please login using your company credentials”.

Step 2: Select a service

The user selects the service they want to use to log in, among those you have configured.

Careful: It is not recommended to select one of the pre-configured services (Google, Github, Okta) when configuring OpenID Connect, as all users who have an account with this service will be able to access your workspace, without any particular restrictions in place.

Step 3: Log in to the service

The user is redirected to the standard login process of the selected service.

Once logged in, the Oodrive platform automatically retrieves the last name, first name and email address of the user and creates a new account for them on your workspace.

Step 4: Access the workspace

The user accesses your workspace with the account that was just created for them.

Configuring OpenID Connect

1. In the **Access Management** module, click on the **Authentication** section.
2. Click on the drop-down menu and select **OpenID Connect**.
3. If you would like to apply this authentication mode to all workspace users, without exception, check **Require this authentication type**.

   Note: Do not check this option if you plan to enable passwordless authentication on your workspace.
4. Click **Apply**, then **New configuration** to configure a new identity provider.

5. Enter the **Configuration name**, then select **Other** in the **Identity provider** drop-down list.

   Careful: It is not recommended to select one of the pre-configured services (Google, Github, Okta) when configuring OpenID Connect. We advise that you configure these services yourself by selecting **Other**, so that only your employees may access your workspace.

6. Complete the fields in the **Connection** section. All fields in the form are required.

7. When you have finished, click **Create**.

8. Click on the identity provider you have just configured and copy the link in the **Link to be sent to OpenID authentication provider** section.

   You need to share this link with your identity provider in order to complete the configuration of OpenID Connect.

Return to the **Authentication** section to modify this option at any time.

3. Managing password complexity

Summary

To increase the robustness of workspace user passwords and better secure your data, you can require the use of passwords of a specific length and character combination of your choice (letters, numbers, and/or special characters).

1. In the **Access Management** module, click on the **Password management** section.
2. Define the following user password characteristics:
   - minimum length (16 characters by default)
   - minimum number of letters and numbers (1 letter and 1 number by default)
   - use of special characters (disabled by default)
3. If you would like to be notified in the event of user login failure, enable the option **Alert me by email in the event of a failed login**.

   An e-mail will be sent to you after five consecutive failures.
4. By default, user passwords expire every three months.
   - To disable password expiration, deselect the option **Enable password expiration**.
   - To extend the time period before password expiration to 6 or 12 months, select **after 6 months** or **after 12 months**.
5. Click **Save** along the bottom of the page to confirm your selection.

4. Configuring authentication options

Summary

The Access Management module allows you to configure either **two-factor authentication** or **passwordless authentication**.

Overview of the authentication options		
	Passwordless authentication	**Two-factor authentication**
Description	Authentication with a mobile device or a Yubikey security key, without need for a password	An extra authentication step in addition to a simple password
External protocol compatibility		
LDAP		●
SAML		●
Kerberos		●
Available authentication modes		
SMS security code	●	●
TOTP security code	●	●
Security key	●	●

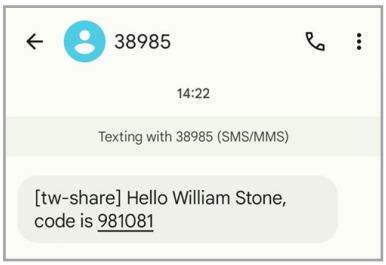
Please note: Allowing an authentication option on your workspace gives you the possibility to personalize the configuration of each user file. On the other hand, requiring the use of an authentication option will make this option mandatory for all workspace users.

4.1. General presentation of the authentication options

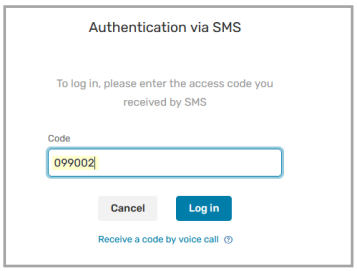
SMS security code

The SMS code allows the user to receive a security code via cell phone mobile network, without needing an internet connection. If the code is not properly received via SMS, the user can ask to receive a phone call from the entry page for the SMS code.

Receiving the code



Entering the code



If authentication via SMS security code fails five times in a row, the account will be locked. Users can unlock their account by requesting intervention from an Administrator or by successfully logging in with a new security code sent via email.

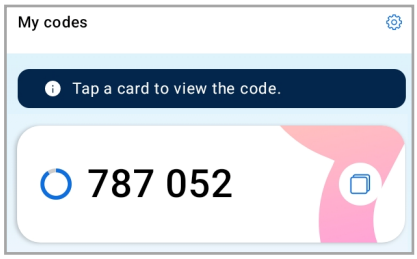
Note: The SMS security code is an add-on module, which is only available if activated for your workspace beforehand.

TOTP security code

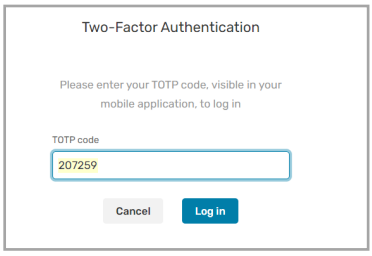
The TOTP security code (Time-based One-time password) is compatible with any authentication app that generates security codes (e.g. Oodrive Authenticator, Google Authenticator, Microsoft Authenticator, etc.).

We recommend the Oodrive Authenticator application, specially developed to enable your users to authenticate to Oodrive via TOTP security code.

Generating the TOTP code



Entering the TOTP code



To use this authentication mode after first logging in, the user must follow the steps below.

Step 1: Download to smartphone

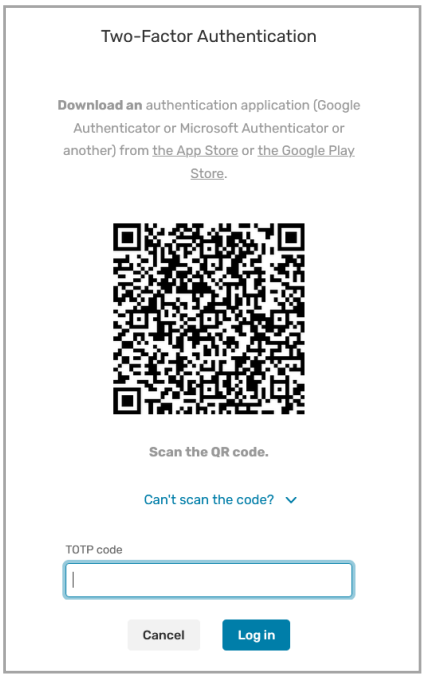
The user downloads the authentication app of their choice to the mobile device.

Step 2: Log in to the workspace via web browser

The user goes to the workspace login page and logs in using their company credentials or their Oodrive credentials

Step 3: Associate the authentication app with the workspace

When using for the first time, the user will be directed to the two-factor authentication page below:



Using the authentication app previously downloaded via smartphone or tablet, the user will be able to scan the QR code displaying on this page to set up the mobile authentication app with the workspace.

The next time the user signs in, after entering their login credentials, they will be able to directly access the two-factor authentication page to enter the temporary code generated by their authentication app.

If authentication via TOTP fails five times in a row, the account will be locked. Users can unlock their account by requesting intervention from an Administrator or by successfully logging in with a new security code sent via email.

Note: If a user loses or changes their mobile device, please contact your workspace provisioning manager.

Yubikey security key

Authentication via security key is only available on the following browsers:

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

When first logging in with this authentication mode, the user must follow the steps below.

Step 1: Log in to the workspace via web browser

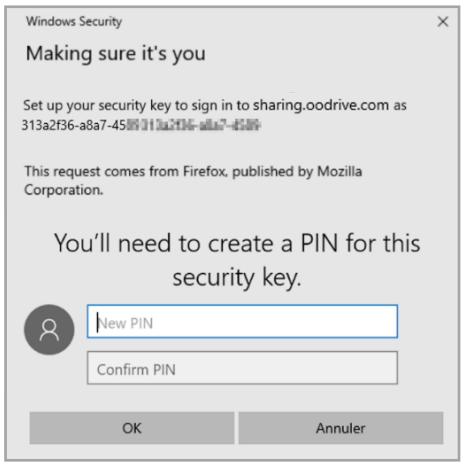
The user goes to the workspace login page and logs in using their company credentials or their Oodrive credentials.

Step 2: Insert the security key

The user is prompted by the browser to insert their security key into the computer.

Step 3: Enter the PIN code

When using their security key for the first time, the user will be prompted to create a PIN code. To do this, they must enter a new PIN code, then confirm it.



Next time they log in, the user will simply need to insert their key and enter the PIN code they just created.

Step 4: Touch the security key

The user touches their key to complete the authentication process. The user then accesses the workspace.

Note: Authentication via security key is an add-on module, which is only available if activated for your workspace beforehand.

4.2. Configuring two-factor authentication

Two-factor authentication allows you to enhance the security of your platform by adding an extra authentication step in addition to a simple password.

There are two ways to configure two-factor authentication:

- **Allow** activation of a second factor, so that the provisioning manager of your workspace may choose whether *or not* to activate two-factor authentication for a user.
- **Require** the use of two-factor authentication for all workspace users, in which case the provisioning manager will be required to select a dual authentication mode for each user.

Allow activation of a second authentication factor

If you allow two-factor authentication, the provisioning manager of your workspace may choose whether to activate it for a user.

1. In the **Access Management** module, click on the **Two-Factor Auth.** section.
2. Select the **Enable two-factor authentication** option.
3. Select **Authorize the selection of a second authentication factor**.
4. Select the authentication mode(s) that you would like to make available to the provisioning manager (**SMS**, **TOTP Code** and/or **Security Key**).
5. Click **Save** along the bottom of the page.

Return to the **Two Factor Auth.** section to modify or disable two-factor authentication.

Require a second authentication factor for all users

If you require the use of two-factor authentication, the provisioning manager of your workspace must select a dual authentication mode for each new user.

Careful: For older user accounts (created before a second factor was required), the second factor will not be activated until the provisioning manager updates their user file.

1. In the **Access Management** module, click on the **Two-Factor Auth.** section.
2. Select the **Enable two-factor authentication** option.
3. Select **Require two-factor authentication**.

4. Select the authentication mode(s) that you would like to make available to the provisioning manager (**SMS**, **TOTP Code** and/or **Security Key**).

   Careful: If the security key or the SMS code is required as the only authentication mode, user accounts without access to a Yubikey device or without accurate, up-to-date mobile phone numbers will not be able to log in to their workspace .

5. Click **Save** along the bottom of the page.

Return to the **Two Factor Auth.** section to modify or disable two-factor authentication.

4.3. Configuring passwordless authentication

Passwordless authentication allows workspace users to log in using their mobile device or their Yubikey security key, without having to provide their password.

Note: Users created through an external authentication protocol can't use passwordless authentication.

There are two ways to configure passwordless authentication:

- **Allow** passwordless authentication, so that the provisioning manager of your workspace may choose whether or not to activate passwordless authentication for a user.
- **Require** passwordless authentication for all workspace users, in which case the provisioning manager will be required to select an authentication mode for each user.

Allow passwordless authentication

If you allow passwordless authentication, the provisioning manager of your workspace may choose whether to activate it for a user.

1. In the **Access Management** module, click on the Two-Factor Auth. section.
2. Select the **Enable two-factor authentication** option.
3. Select **Authorize the selection of a second authentication factor**.
4. Select the authentication mode(s) that you would like to make available to the provisioning manager (**SMS**, **TOTP Code** and/or **Security Key**).
5. Select the **Passwordless option**.
6. Click **Save** along the bottom of the page.

Return to the **Two Factor Auth.** section to modify or disable passwordless authentication.

Require passwordless authentication

If you require the use of passwordless authentication, the provisioning manager of your workspace must select an authentication mode for each new user.

Careful: For older user accounts (created before a second factor was required), passwordless authentication will not be activated until the provisioning manager updates their user file.

1. In the **Access Management** module, click on the **Two-Factor Auth.** section.
2. Select the **Enable two-factor authentication** option.
3. Select **Require two-factor authentication**.
4. Select the authentication mode(s) that you would like to make available to the provisioning manager (**SMS**, **TOTP Code** and/or **Security Key**).

   Careful: If the security key or the SMS code is required as the only authentication mode, user accounts without access to a Yubikey device or without accurate, up-to-date mobile phone numbers will not be able to log in to their workspace.
5. Select the **Passwordless** option.
6. Click **Save** along the bottom of the page.

Return to the **Two Factor Auth.** section to modify or disable two-factor authentication.

5. Configuring IP address filtering

Summary

In order to increase workspace security, you can block or allow access from certain computers. By filtering access by IP address, you can directly limit the workstations and mobile devices able to log into workspace applications.

5.1. Enable IP address filtering

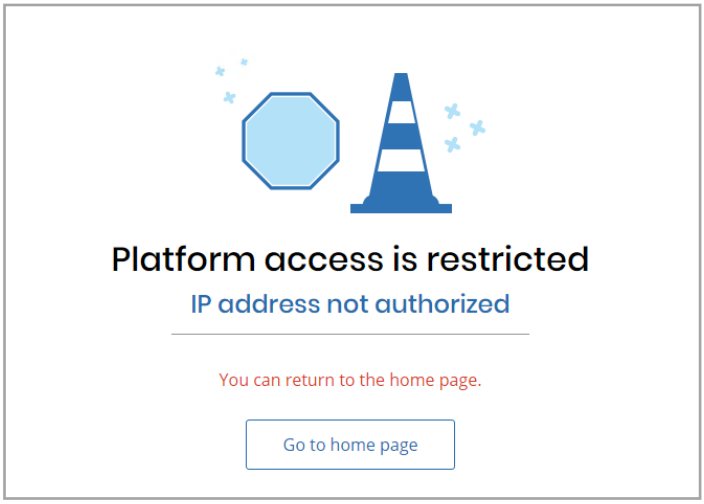
1. In the **Access Management** module, click on the **IP filtering** section.
2. Select the **Enable IP address filtering** option.
3. Choose how you would like to filter IP addresses:
   - **by authorizing** (white listing) or
   - **by prohibiting** (black listing)

   Please note: You cannot apply white lists and black lists simultaneously.
4. Enter an IP address in the field provided, then click **Add**.

   Note: You also have the option to enter IP ranges.
5. Along the bottom of the page, click **Save**.
6. Repeat steps 4 and 5 to add additional IP addresses.

IP address filtering will apply the next time users on filtered IP addresses attempt to log in.

Unauthorized IP address message



5.2. Disable IP address filtering

1. In the **Access Management** module, click on the **IP filtering** section.
2. Unselect the **Enable IP address filtering** option.
3. Along the bottom of the page, click **Save**.

Your filters will be remain available the next time you enable this option.

5.3. Remove the IP address filter

1. In the **Access Management** module, click on the **IP filtering** section.
2. Next, in the list of authorized or unauthorized addresses, click on the recycle bin icon located to the right of the IP address.

   Tip: If you select an IP address by mistake, click **Reset** along the bottom of the page to undo the action.
3. Click **Save** to apply your changes.

6. Managing access to mobile and desktop applications

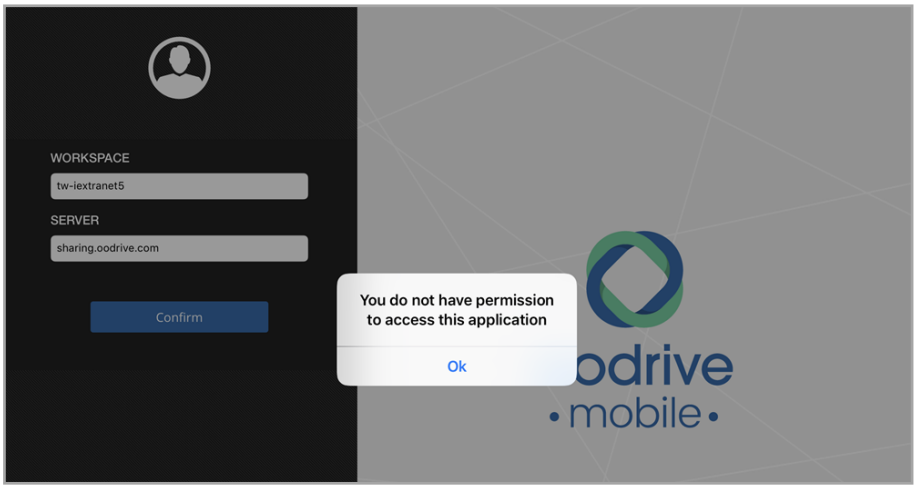
Summary

6.1. Mobile applications

By default, users can log into your company workspace on their smartphone or tablet from oodrive mobile applications (including, BoardNox, oodrive_meeting, Oodrive Mobile and oodrive_share). However, if you would rather prevent the use of mobile applications, you can change this option.

1. In the **Access Management** module, click on the **Mobile and desktop apps** section.
2. In the **Mobile applications** section, select **No** to disable access to mobile applications.
3. Along the bottom of the page, click **Save**.

The next time a user tries to log in to your workspace on a mobile application, they will receive an accessed refused message:



You can re-enable access to mobile applications at any time.

Note: Disabling access to mobile applications will not, however, prevent access to the workspace via web browser on mobile devices.

To prohibit platform access via mobile device, it is recommended that you enable IP address filtering for all mobile devices from which users are likely to log in. You can also include a paragraph on the subject in your terms of service.

6.2. Desktop applications

Several desktop applications are available on your workspace to help users share and manage files more easily (EasyTransfer, WebSynchro, Plugin Outlook). However, if you would rather prevent the use of desktop applications, you can disable these applications.

1. In the **Access Management** module, click on the **Mobile and desktop apps** section.
2. In the **Desktop applications** section, select **No** to disable access to desktop applications.
3. Along the bottom of the page, click **Save**.

Users will no longer be able to access your workspace using desktop applications.

You can re-enable access to desktop applications at any time.

7. Displaying terms of service (TOS)

Summary

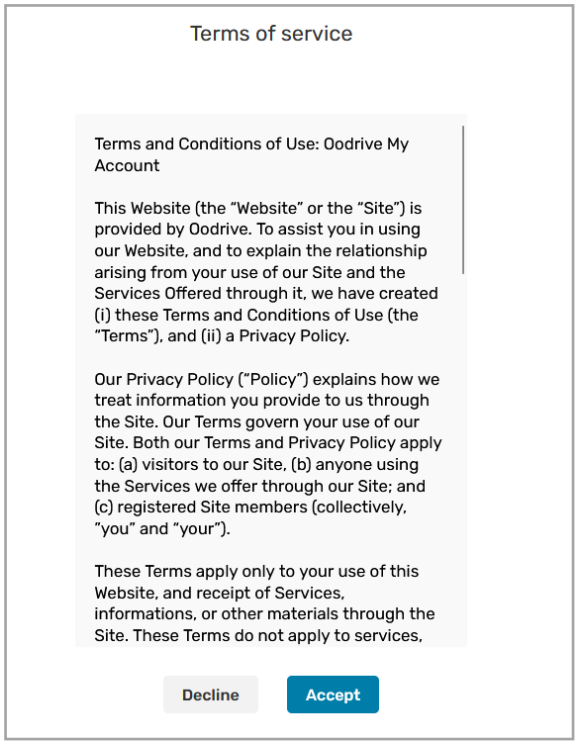
Please note: A new module, **Administration of Legal Notices**, is now available for more advanced management of TOS and other legal notices.

Once you have configured your first notice in the **Administration of Legal Notices** module, the **TOS** section in the **Access management** module will be deactivated.

If you have general terms of service (TOS) to communicate to employees on the workspace before they access it, you can enable this option. After making any changes to the terms of service, you will have the option to re-display the TOS to workspace users.

1. In the **Access Management** module, click on the **TOS** section.
2. Click **Yes**.
3. Enter or paste the content of the terms of service to display to users after they first log in to your workspace.
4. Choose the frequency with which you would like to display the TOS to users:
   - at first log in
   - at every log in
5. Click **Save** along the bottom of the page to save your changes and enable the display of the TOS.

The next time a user logs into your workspace, they will be asked to accept the TOS being able to access the platform.



To update the terms of service:

1. In the text box, modify the TOS.
2. Click **Save** to apply your changes.
3. In the upper-right corner of the page, click **Reset acceptance** to display the updated TOS page to workspace users.
4. Click **Reset** to confirm.

8. Monitoring authentication attempts

Summary

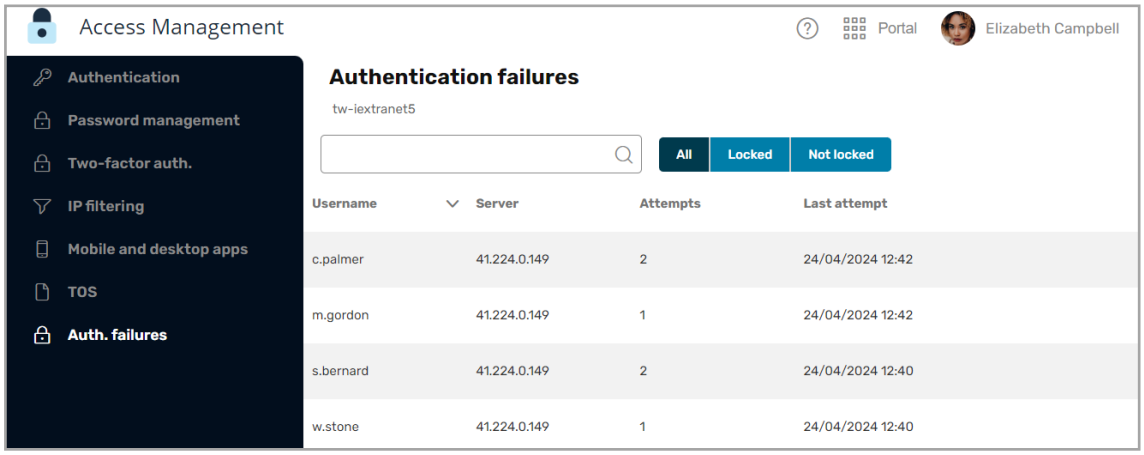
The **Auth. failures** section allows you to view the list of failed login attempts on the workspace.

These failed attempts may be the result of IP address filtering or users forgetting their passwords, but they can also help you identify potential suspicious activity on your workspace.

As a security measure, the Oodrive platform automatically locks user accounts after 5 failed login attempts. As an Administrator, you can intervene to unlock the account of workspace users.

8.1. View failed login attempts

1. In the Access Management module, click on the Auth. failures section.
2. You view all failed login attempts and their information:
    - Account username,
    - IP address,
    - Number of failed attempts for the username/IP address combination.



Note: When authentication is successful for a username/IP address combination, it disappears from the authentication failures list, and the number of failed attempts is reset.

3. You can sort the list by account status, by clicking Locked or Not locked.

8.2. Unlock an account

When an account is locked, the user will be required to enter a security code sent by email, in addition to their password, to unlock their account. As an Administrator, you also have the option to unlock an account directly from the Access Management module.

1. In the **Access Management** module, click on the **Auth. failures** section.
2. Click **Locked** to access the list of locked accounts.
3. Find the account you want to unlock and click its **Unlock** button.
4. Click **Unlock** to confirm.

   The user is now able to log in as usual, without having to enter a security code.

   Please note:

   - If a user has locked their account because they forgot their password, the provisioning manager can reset it in the Users module. The user will then receive an email allowing them to create a new password.
   - If a user has locked their account after failing to enter the correct security code 5 times in a row, they can unlock their account by entering a new security code sent via email. In case of loss or replacement of the mobile device used for authentication, the provisioning manager can modify the second factor of authentication in the Users module.

Once you unlock an account, it is removed from the authentication failures list, and the number of failed attempts is reset.


∞drive