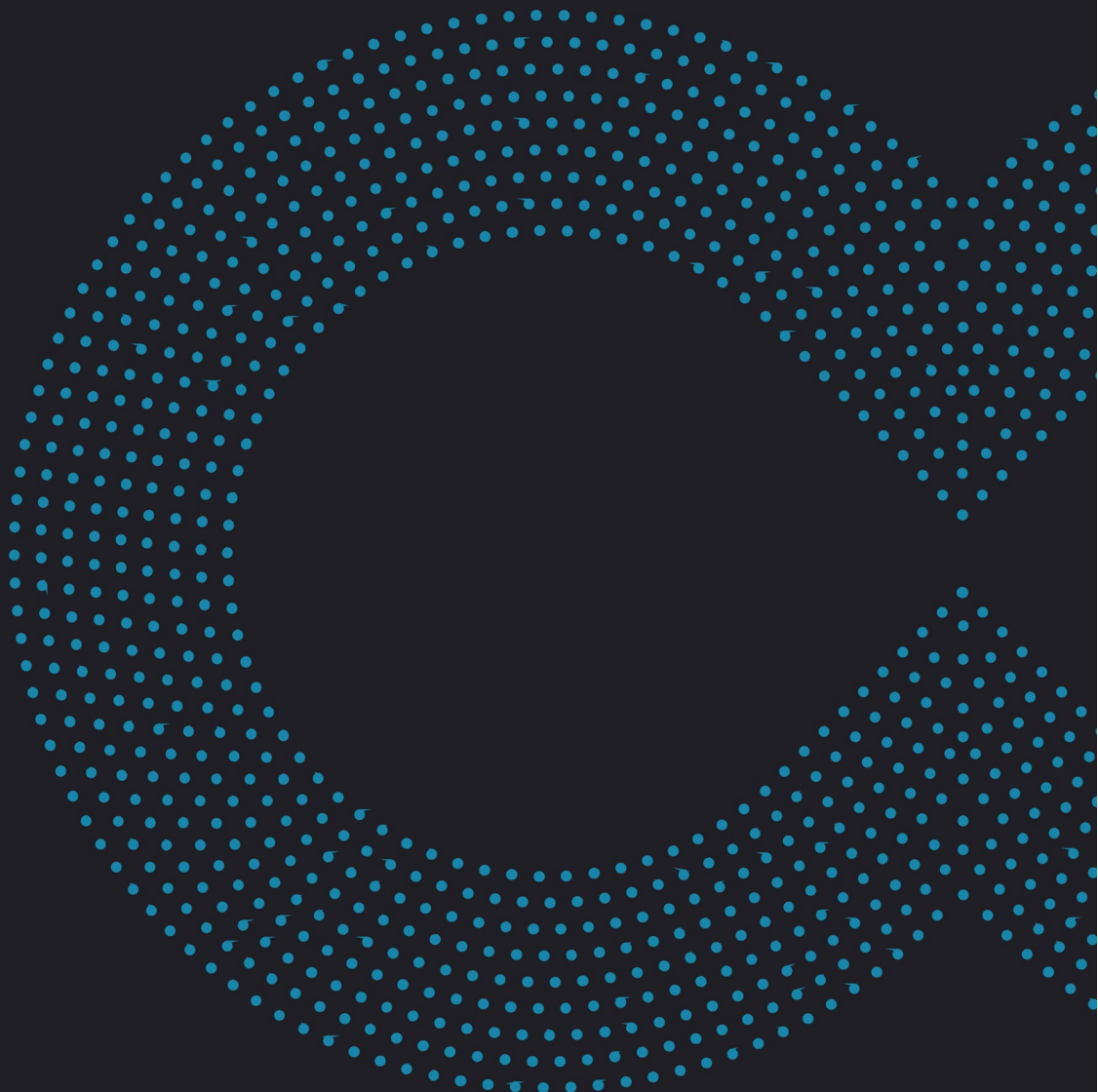
drive work

Administrator Guide

Sharing Administration



oodrive work

Terms of use

Without prejudice to any rights reserved and unless expressly authorized, no part of this document may be reproduced, recorded or introduced into a consultation system, or sent in any format or by any means whatsoever without the written permission of the OODRIVE GROUP.

Any requests for permission to reproduce or obtain further copies of this document should be sent to the OODRIVE GROUP.

Distribution list

Company	Role
Oodrive Group	Oodrive Group colleagues and customers

oodrive work

Contents

1. Getting started configuring your workspace

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

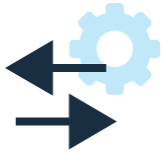
As a result, you are responsible for configuring a certain number of options relating to the behavior of applications offered to your organization's employees.

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

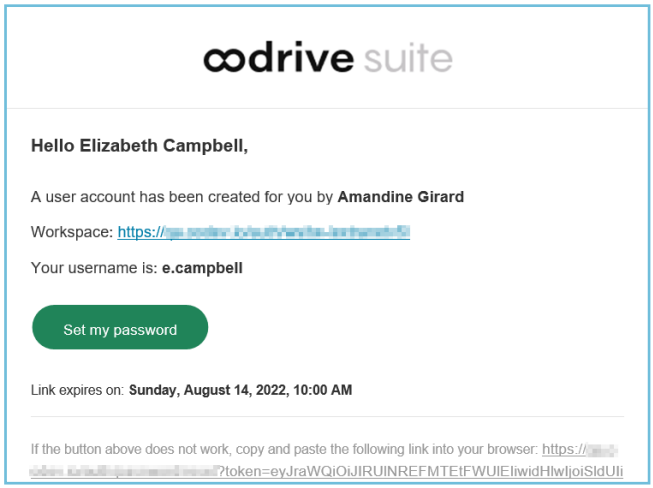
There are two ways to log in to your workspace:

- 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**.

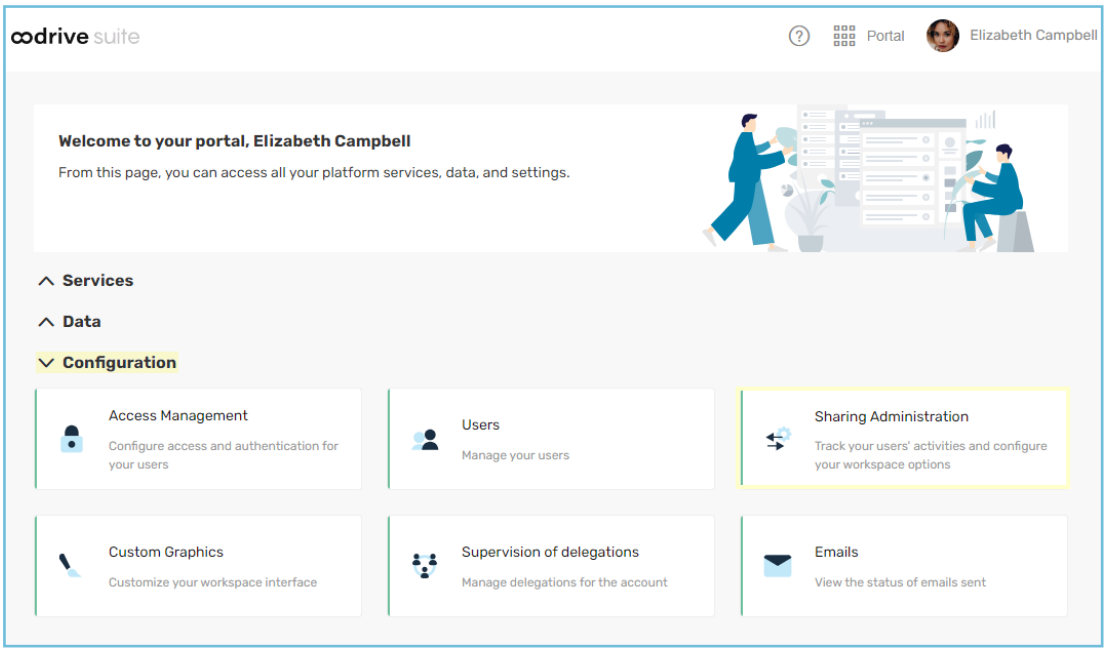
5. Enter the password you have just specified, then click **Log in**.

   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 

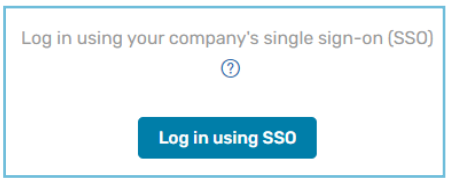
in the upper-right corner of the page, then select **Portal**.

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**.

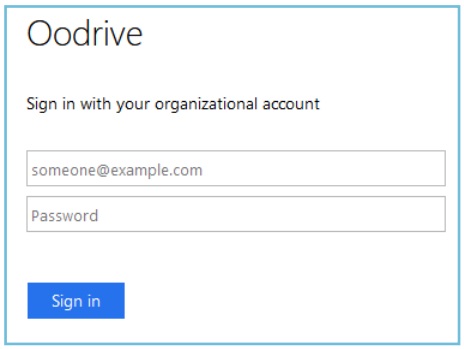
Log in with your company login credentials

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)**

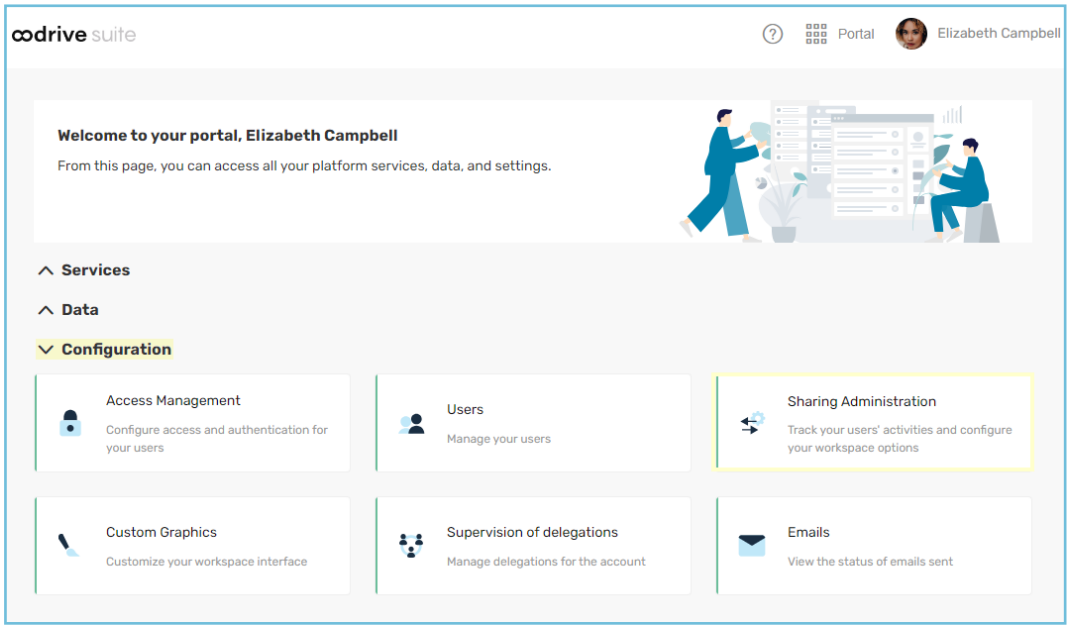
2. Enter your company login credentials and click **Log in**.



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**.

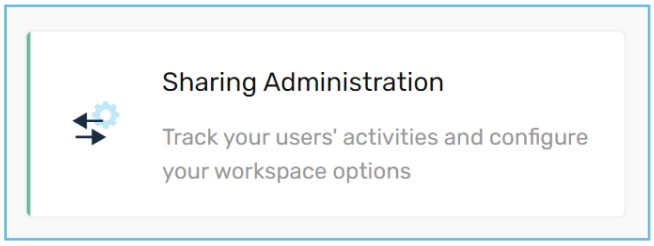
Please note: As a security measure, you will be automatically logged out of your session after 30 minutes of inactivity (or after 4 hours if the Oodrive Work discussion feature is enabled). You can extend your session by clicking **Continue to browse** when the logout warning appears on the screen.

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 Sharing Administration module

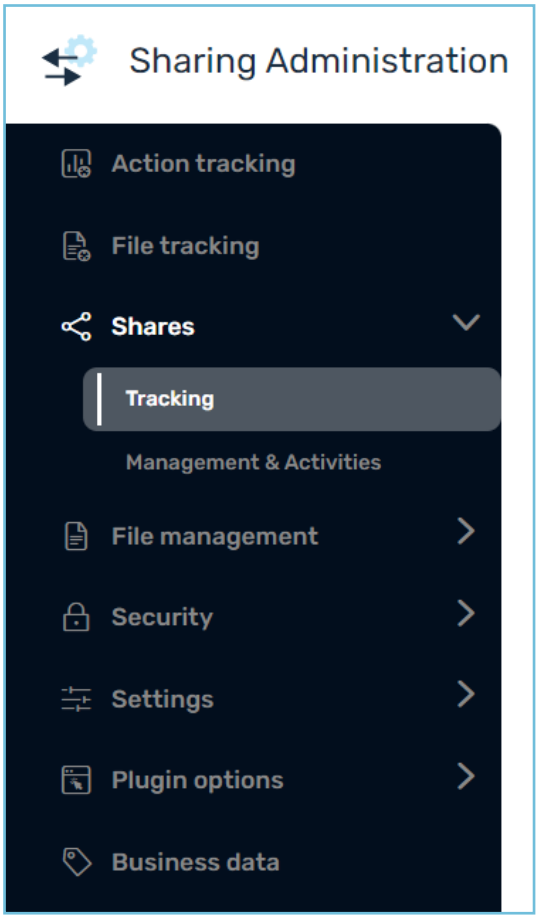
As a user with administrative rights, you are responsible for configuring advanced options for the platform, monitoring platform activity and managing shared files.

Configure	Monitor	Manage
• Configure settings for your platform applications regarding files, sharing, security and plugins. • Allow for certain options to be modified by Users.	• Track general platform activities, file activities, and share activities • Generate instant reports • Schedule and modify reports	• Track the creation of new shares • Perform platform file lifecycle management : activate, deactivate and permanently delete shares created by Users



1.4. Browse the Sharing Administration module

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



2. Platform activity monitoring

Track activities performed on the platform by Users, Contacts and Anonymous Contacts (without a login) in the **Action tracking**, **File tracking** and **Share tracking** sections. From here, you can monitor the following activities across your platform, and create and schedule reports regarding these activities:

Action tracking	File tracking	Share Tracking

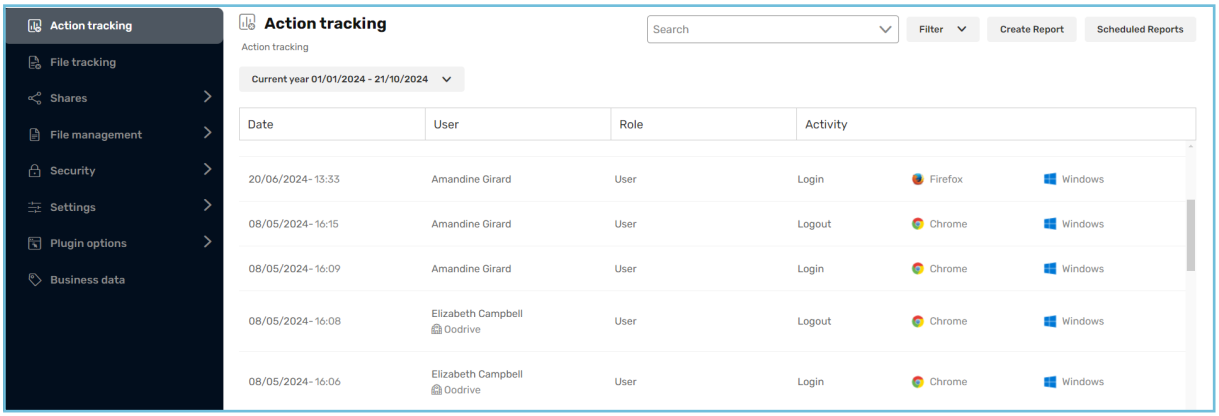
Monitor general platform activities:
• Account login/logout
• Contact creation/ modification/deletion
• Workspace option modifications
• Clear recycle bin
	Monitor file activities:
	• Upload/download
	• Create/delete
	• View/rename/modify
	• Copy/move
	• Lock/unlock
	• Restore
		Monitor shared file activities:
		• File sharing (via link, email, read-only, drop folder, collaborative folder)
		• Custom website templates
		  • Create
		  • Modify
		  • Delete

2.1. Action tracking

Track activities performed by platform Users, Contacts and Anonymous Contacts (without a login) in the Action tracking section. From here, you can monitor the following general activities on the platform:

- Account login/logout
- Contact creation/modification/deletion
- Workspace option modifications
- Recycle bin purging

You can also create and schedule reports regarding these activities.



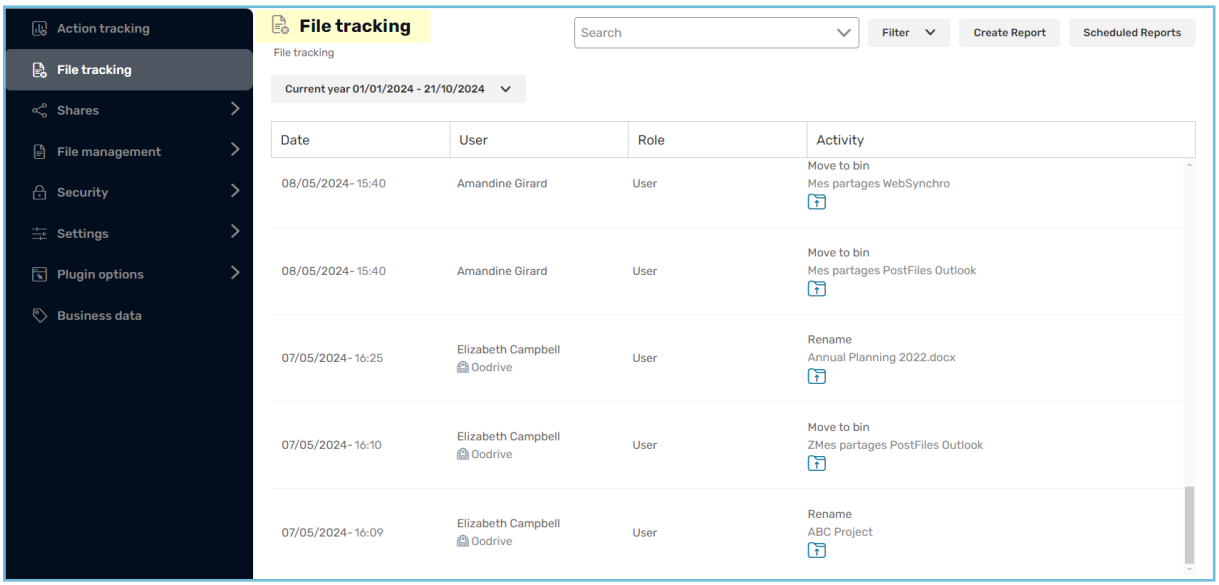
2.2. File tracking

Track file specific activities performed by Users, Contacts and Anonymous Contacts (without a login) in the **File tracking** section. From here, you can monitor the following file activities on your workspace:

- Upload/download
- Create/delete
- View/rename/modify
- Copy/move
- Lock/unlock
- Restore

You can also create and schedule reports regarding these activities.

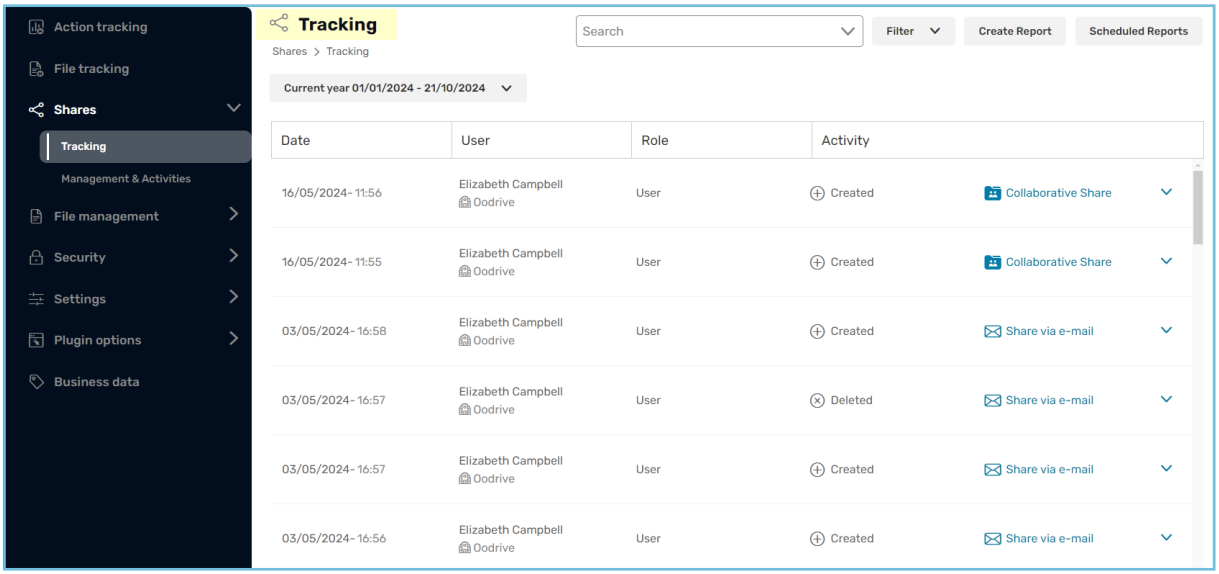
Please note: For help managing and monitoring shared files, please refer to the **Share tracking** and **Managing shared files** section of this user guide.



2.3. Share tracking

Track actions relating to shared files, and custom site templates used to share files by Users, Contacts and Anonymous Contacts (without a login). From here, you can monitor and generate reports regarding the following activities on your workspace:

- **File sharing (via link, email, read-only, drop folder, collaborative folder)**
  - Share
  - Update
  - Remove content
- **Custom share templates**
  - Create
  - Modify
  - Delete

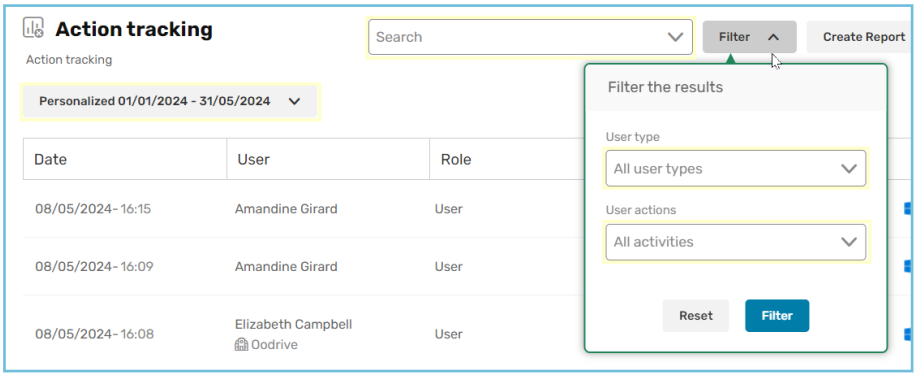


2.4. Search & filter

Search the tracking activity to view platform user and/or company-specific activities using the search bar in the upper-right corner of each tracking section.

For more advanced searches, use the **Filter** drop-down menu to filter by **user account type** and/or **activity**.

You can also apply an additional filter by date (personalized, current year, last week, last month, last year).



To return to the section tracking view, clear the search bar and click on the **Reset** button in the **Filter** menu.

2.5. Generate an instant report

You can generate instant tracking reports regarding user platform activity from any of the three tracking sections (**Action tracking**, **File tracking**, **Share tracking**) depending on the focus of your report. Filter tracking data to zero in on the most relevant platform activities before generating your report in CSV, XLS or XLSX file formats.

1. Go to the tracking section for which you would like to generate a report (**Action tracking**, **File tracking** or **Share tracking**).

2. Use the search bar and filter options to focus your report on the specific activity (user type, activity, date range). By default, general tracking activity view is filtered by the current calendar year.

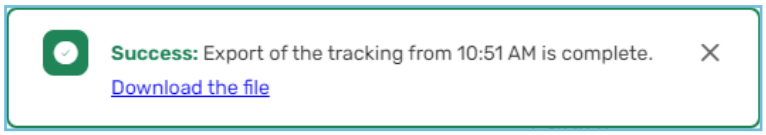
3. In the upper-right corner of the page, click **Create Report**.

4. Select **Generate a report**.

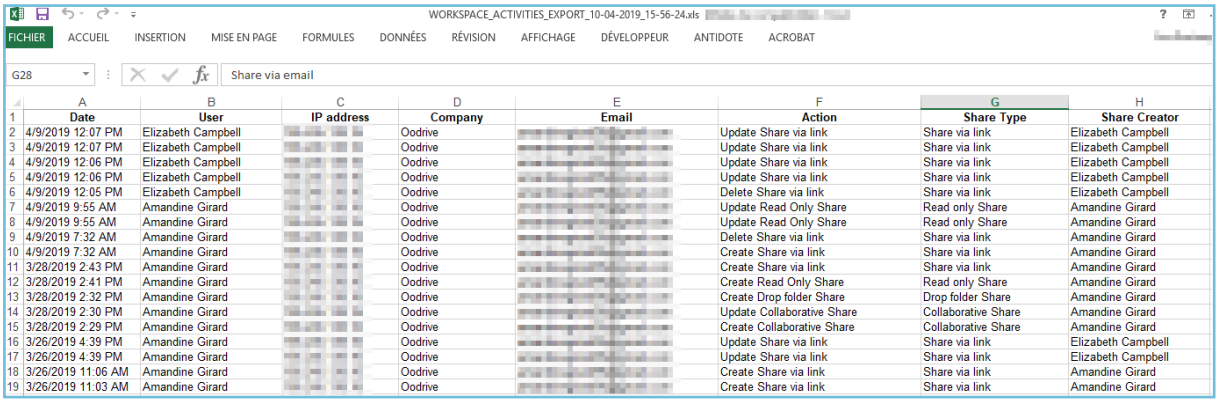
5. Click on the drop-down menu and select the report file type that you would like to generate (CSV, XLS or XLSX).

6. Click **Export**.

7. In the confirmation message, click **Download the file**.



8. In your web browser, a **Workspace_Activities_Export** file will download. Click on the downloaded file to open.



WORKSPACE_ACTIVITIES_EXPORT_10-04-2019_15-56-24.xls

FICHIER ACCUEIL INSERTION MISE EN PAGE FORMULES DONNÉES RÉVISION AFFICHAGE DÉVELOPPEUR ANTIDOTE ACROBAT

G28 | Share via email

	A	B	C	D	E	F	G	H
1	Date	User	IP address	Company	Email	Action	Share Type	Share Creator
2	4/9/2019 12:07 PM	Elizabeth Campbell		Oodrive		Update Share via link	Share via link	Elizabeth Campbell
3	4/9/2019 12:07 PM	Elizabeth Campbell		Oodrive		Update Share via link	Share via link	Elizabeth Campbell
4	4/9/2019 12:06 PM	Elizabeth Campbell		Oodrive		Update Share via link	Share via link	Elizabeth Campbell
5	4/9/2019 12:06 PM	Elizabeth Campbell		Oodrive		Update Share via link	Share via link	Elizabeth Campbell
6	4/9/2019 12:05 PM	Elizabeth Campbell		Oodrive		Delete Share via link	Share via link	Elizabeth Campbell
7	4/9/2019 9:55 AM	Amandine Girard		Oodrive		Update Read Only Share	Read only Share	Amandine Girard
8	4/9/2019 9:55 AM	Amandine Girard		Oodrive		Update Read Only Share	Read only Share	Amandine Girard
9	4/9/2019 7:32 AM	Amandine Girard		Oodrive		Delete Share via link	Share via link	Amandine Girard
10	4/9/2019 7:32 AM	Amandine Girard		Oodrive		Create Share via link	Share via link	Amandine Girard
11	3/28/2019 2:43 PM	Amandine Girard		Oodrive		Create Share via link	Share via link	Amandine Girard
12	3/28/2019 2:41 PM	Amandine Girard		Oodrive		Create Read Only Share	Read only Share	Amandine Girard
13	3/28/2019 2:32 PM	Amandine Girard		Oodrive		Create Drop folder Share	Drop folder Share	Amandine Girard
14	3/28/2019 2:30 PM	Amandine Girard		Oodrive		Update Collaborative Share	Collaborative Share	Amandine Girard
15	3/28/2019 2:29 PM	Amandine Girard		Oodrive		Create Collaborative Share	Collaborative Share	Amandine Girard
16	3/26/2019 4:39 PM	Amandine Girard		Oodrive		Update Share via link	Share via link	Elizabeth Campbell
17	3/26/2019 4:39 PM	Amandine Girard		Oodrive		Update Share via link	Share via link	Elizabeth Campbell
18	3/26/2019 11:06 AM	Amandine Girard		Oodrive		Create Share via link	Share via link	Amandine Girard
19	3/26/2019 11:03 AM	Amandine Girard		Oodrive		Create Share via link	Share via link	Amandine Girard

2.6. Schedule a report

Automate the report generation process on a daily, weekly, and/or monthly basis. This can be done in any of the three tracking sections (Action tracking, File tracking, Share tracking), depending on the focus of your report. You can then further filter tracking data to only include the most salient platform tracking data.

Once a scheduled report has been auto-generated, the designated recipient(s) will automatically receive an email containing a download link to the new report.

1. Go to the tracking section for which you would like to generate a report (**Action tracking**, **File tracking** or **Share tracking**).

2. Use the search bar and filter options to focus your report on the specific activity (user type, activity, date range). By default, general tracking activity view is filtered by the current calendar year.

3. In the upper-right corner of the page, click **Create Report**.

4. Under **Schedule a recurring report**, click on the drop-down menu and select the file type of the report that you would like to schedule (CSV, XLS or XLSX).

5. Under **Scope**, to schedule a report based on the filters currently applied, leave the **Current filters** option selected.

   To schedule a report including all activities tracked within the given tracking section, select **All activities**.

6. Select the period of time to include in the scheduled report (**Since yesterday**, **last week** or **last month**).

7. Select the frequency with which you would like to auto generate the report (**Daily**, **weekly**, **monthly**).

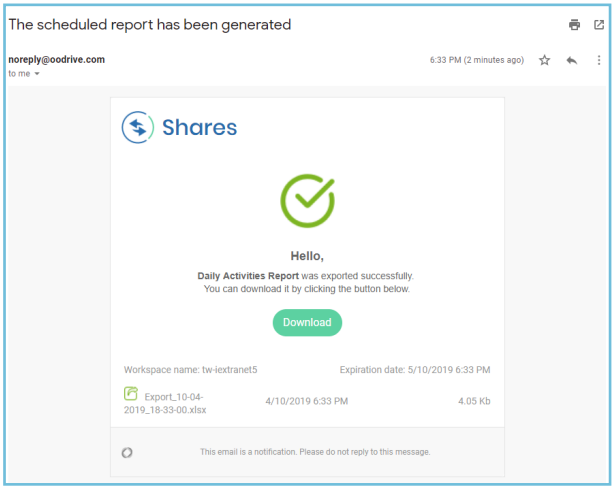
8. Enter a **Report name**. This will appear, along with any additional reports scheduled, in the **Scheduled Reports** view.

9. In the **Email address for notifications** field, enter the name of the user who should be notified via email once the report has been generated at the scheduled date and time. As you type, a list of available users appears for you to select.

10. Click **Create**.

A confirmation message will appear confirming that the report has been successfully planned.

Below is an example of the email notification received following a scheduled report. The new report can be downloaded locally by clicking on **Download**.



2.7. Modify a scheduled report

Scheduled reports are located in the three tracking sections of the application (**Action tracking**, **File tracking** and **Share tracking**). Click on the **Scheduled Reports** button in each of those sections to:

- Make changes to reports
- Temporarily disable or re-enable reports
- Permanently delete reports

Modify an existing scheduled report

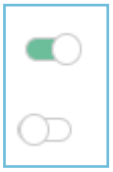
1. Go to the tracking section for the report that you would like to modify (**Action tracking**, **File tracking** or **Share tracking**).
2. In the upper-right corner of the page, click **Scheduled Reports**.
3. In the **Scheduled Reports** side bar on the right side of the page, identify the report that you would like to modify.

   A search bar is available in this section to help you find the report that you are looking for.
4. Next to the report, click the **Edit** icon.
5. Update the form and click **Update export** to save your changes.

Disable or re-enable a scheduled report

1. Go to the tracking section for the report that you would like to modify (**Action tracking**, **File tracking** or **Share tracking**).
2. In the upper-right corner of the page, click **Scheduled Reports**.
3. In the **Scheduled Reports** side bar on the right side of the page, identify the report that you would like to disable or re-enable.

   A search bar is available in this section to help you find the report that you are looking for.
4. Next to the report, click on the toggle switch.



A green screen toggle switch indicates that the report is enabled.

A white screen toggle switch indicates that the report is disabled.

Delete a scheduled report

1. Go to the tracking section for the report that you would like to modify **(Action tracking**, **File tracking** or **Share tracking**).

2. In the upper-right corner of the page, click **Scheduled Report**s.

3. In the **Scheduled Reports** side bar on the right side of the page, identify the report that you would like to delete.

   A search bar is available in this section to help you find the report that you are looking for.

4. Next to the report, click the **Delete** icon.

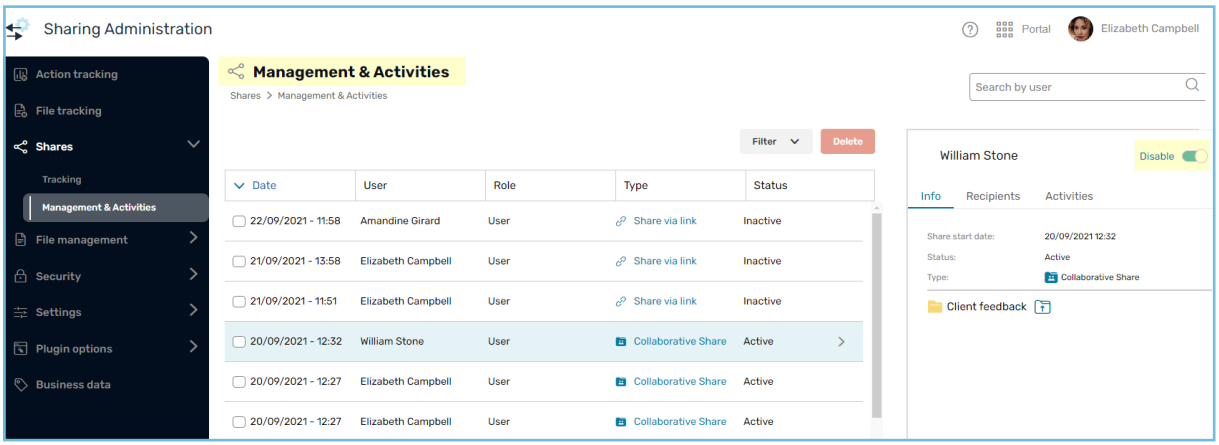
5. Click **Confirm** to permanently delete the scheduled report.

3. Share management & activities

Monitor and manage files shared by users in **Shares > Management & Activities**. From here, you can intervene at any time to maintain control over any workspace files that have been shared, whether via link, email, read-only, drop folder, or collaborative folder.

Manage shared files by performing the following actions:

- Reactivate shared files
- Deactivate shared files
- Delete shared files



3.1. Activate & deactivate shares

You have the option to intervene on the behalf of workspace users to activate or deactivate their shares, regardless of the share type (link, email, read-only, drop folder, collaborative folder). Deactivating a share renders it temporarily inaccessible until you, or the share creator, reactivate it.

1. In the navigation panel along the left side of the page, click the **Shares** section and select **Management & Activities**.

2. Click on the share that you would like to activate or deactivate from the list.

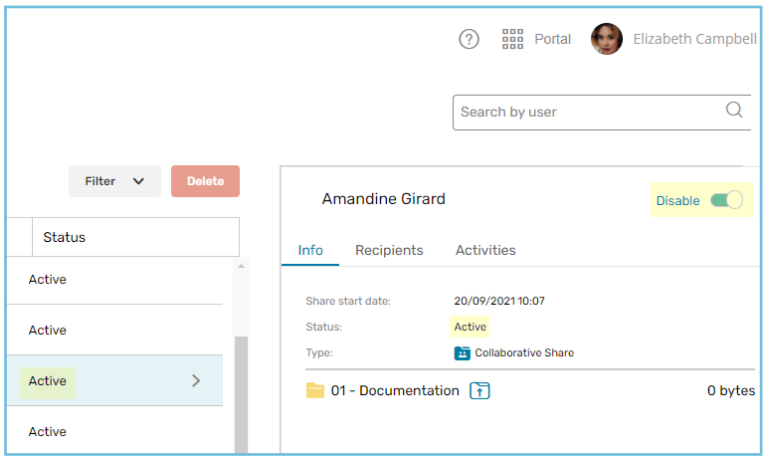
   Use the search bar and/or the filters to help find the specific share that you would like to manage.

3. In the side panel along the right side of the page, you can verify the details of the share in each available tab:

Info	Recipients	Activities
Start date, status, type location, size	User and Contacts with whom the files have been shared	Monitoring details regarding actions performed by each share recipient

4. To activate or deactivate the share, click on the toggle switch located in the upper-right corner of the side panel.

   The color green indicates that the share is currently active. The status of the share will immediately update in the side panel, as well as in the tracking view. In the example below, the share has been **activated**:



Return to this section at any time to make changes.

3.2. Delete shares

You can delete shares created by workspace users regardless of the share type (link, email, read-only, drop folder, collaborative folder). Deleting a share will not only render it inaccessible to those with whom it was previously shared, but it will also permanently remove it from the share creator's **Manage sharing** section.

Please note: After deleting a share, the original unshared files will remain available to the share creator.

1. In the navigation panel along the left side of the page, click the Shares section and select **Management & Activities**.

2. Select the share(s) that you would like to permanently delete.

   Use the search bar and/or the filters to help find the specific share that you would like to delete.

3. To delete, click on **Delete** in the upper-right corner of the page, then click **Confirm**.

4. File management

Manage workspace files and configure the following options:

- **Automatic deletion of files**

  Automatically delete obsolete files from your company's workspace.

- **Authorized/prohibited file types**

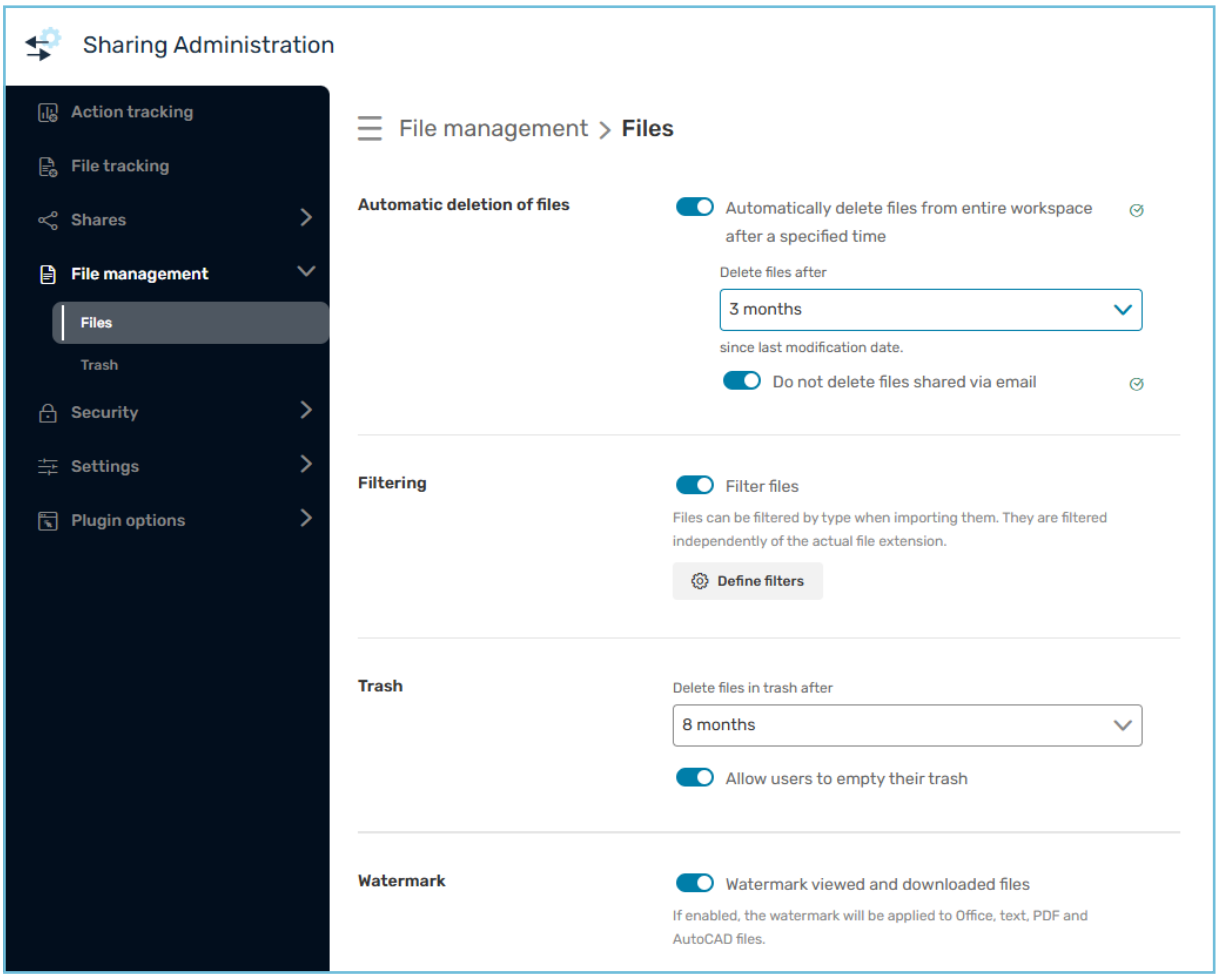
  Restrict permitted file types to control the types of files that can be uploaded to your company's workspace.

- **Trash**

  Manage the trash retention settings and perform file restoration to restore workspace files that have been accidentally deleted.

- **Watermark**

  Watermark all files viewed and downloaded from the workspace to enhance data protection and deter unauthorized distribution.



4.1. Automatic deletion of files

You can automatically delete obsolete files from your workspace. To do this, you need to define a time period after which an unused file should be deleted. This time period is reset each time the file is modified.

Deleted files are moved to the trash. They can then be restored until the trash is emptied.

IMPORTANT: Automatic deletion affects all files in your workspace, regardless of who owns them.

1. In the navigation panel along the left side of the page, select the **File management** section.

2. Enable or disable the **Automatically delete files from entire workspace after a specified time** option.

3. If you have enabled the automatic deletion option, select the time period after which unmodified files will be deleted (from 1 day to 3 years).

4. To prevent automatic deletion of documents still being shared, you can enable the **Do not delete files shared via email** option.

   IMPORTANT: if The **Do not delete files shared via email** option is enabled:

   - Files shared via email will not be automatically deleted from your workspace, unless the user has chosen to enable the **Delete files when the share is over** option.
   - Files shared via email or via link remain available to recipients, even if the original has been deleted from your workspace.

5. Click **Save**.

Return to this section at any time to make changes.

4.2. File types

If you would like to limit the permitted file types that can be uploaded to your company's workspace, this can be done by including or excluding specific file categories and file types e.g.: archive (ar, arj, bz2), audio (wave, mp3, real audio), document (html, MS Office, PDF), executable (exe, class, pl), image (jpeg, tiff, png) and video files (avi, mov, wmv).

1. In the navigation panel along the left side of the page, select the **File management** section.

2. In the **Filtering** section, enable the **Filter files** setting, then click **Define filters**.

3. To filter by exclusion, select **Do not allow file types**.

   To filter by inclusion, select **Allow only these file types**.

4. Next, select the applicable file types.

   To select an entire file category, select any of the following file types: archive, audio, document, executable, image and video file types.

   To select specific file extensions, click on the arrow to the left of the file category and choose the file extensions to exclude/include.

5. Click **Save**.

Return to this section at any time to make changes.

4.3. Watermark workspace documents

Please note: This feature is disabled by default. If you would like to enable it for your workspace, please contact Oodrive Support.

You can apply a watermark to files viewed or downloaded from the workspace. This will enhance data protection and deter unauthorized distribution.

Once enabled, all files in the workspace will be watermarked.

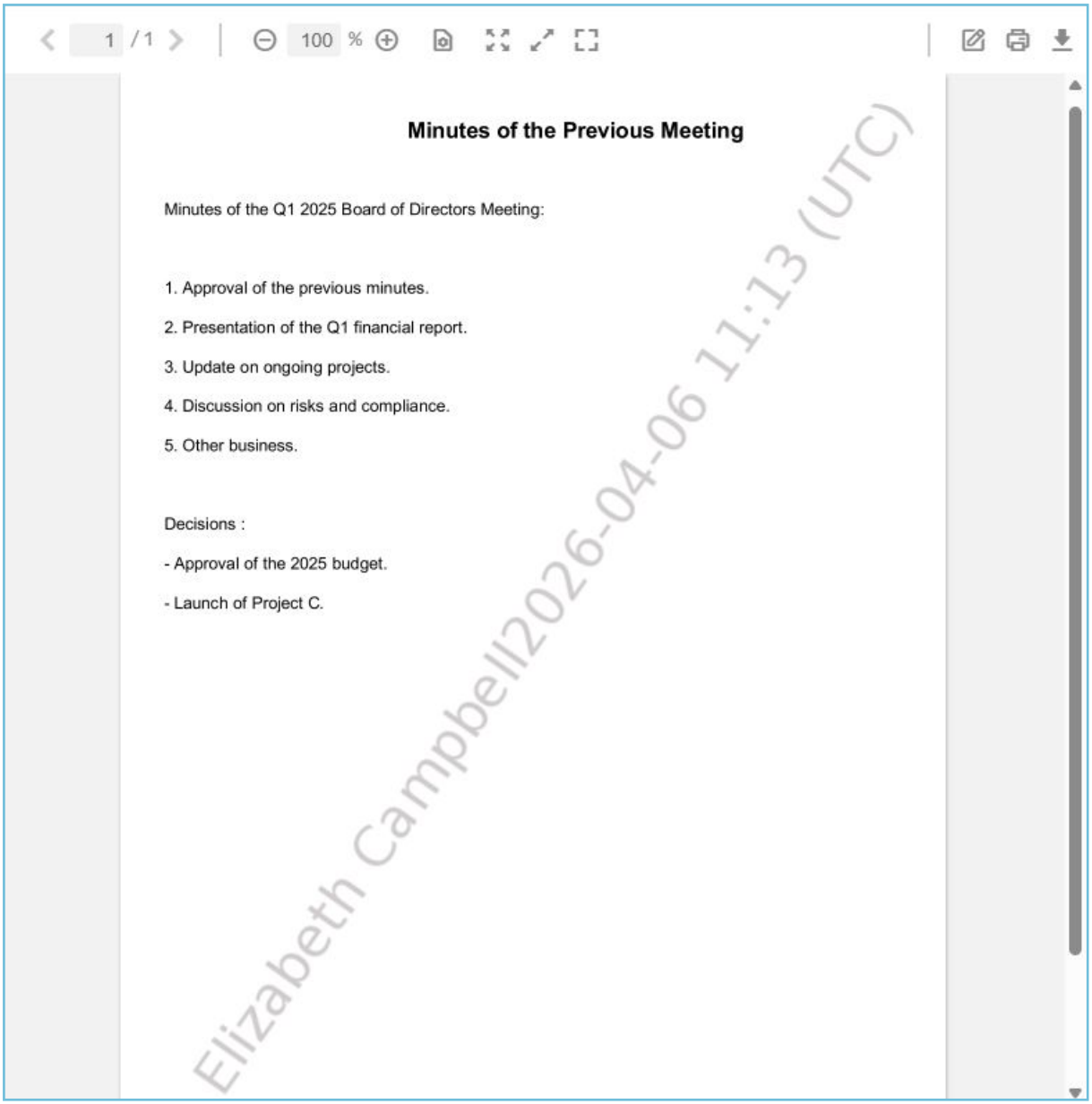
The dynamic watermark is timestamped and displays the following information:

Source	Information displayed
My space / teamspace	Name of the user viewing or downloading the file
Collaborative share	
Share via email (registered contact)	
Share via email (email address only)	Email address of the recipient viewing or downloading the file
Share via link	Name of the share owner, date and time the link was created

To watermark all the files on your workspace :

1. In the navigation panel along the left side of the page, select the **File management** section.
2. Enable the **Watermark viewed and downloaded files** option.
3. Click **Save**.

A watermark is now applied to all files viewed and downloaded from the workspace.



Return to this section to disable compulsory workspace-wide watermarking.

4.4. Trash

Manage the trash retention settings for your workspace and perform file restoration for users to restore files before they are permanently deleted.

Trash retention

1. In the navigation panel along the left side of the page, select the **File management** section.

2. Click the **Delete files in trash after** drop-down menu and select the time period before permanently deleting files in the trash (from 1 day to 3 years).

3. Enable or disable the **Allow users to empty their trash** setting, depending on whether you want to allow or prevent this action.

4. Click **Save**.

Return to this section at any time to make changes.

Permanent deletion

1. In the navigation panel along the left side of the page, select **File management**, then select **Trash**.

2. From the **Trash** section, you can view the following details regarding each deleted item:
   - File name
   - Original location
   - Owner
   - Date deleted
   - File size

3. To permanently delete individual files, select the file(s) that you would like to remove in the **File name** column and click **Delete selection**, then click **Confirm**.

   To permanently delete all files in the trash, click **Empty trash** in the upper-right corner of the page, then click **Confirm**.

5. Platform security management

Enable additional security features to better protect workspace files and data accessed on the platform and via Oodrive mobile applications.

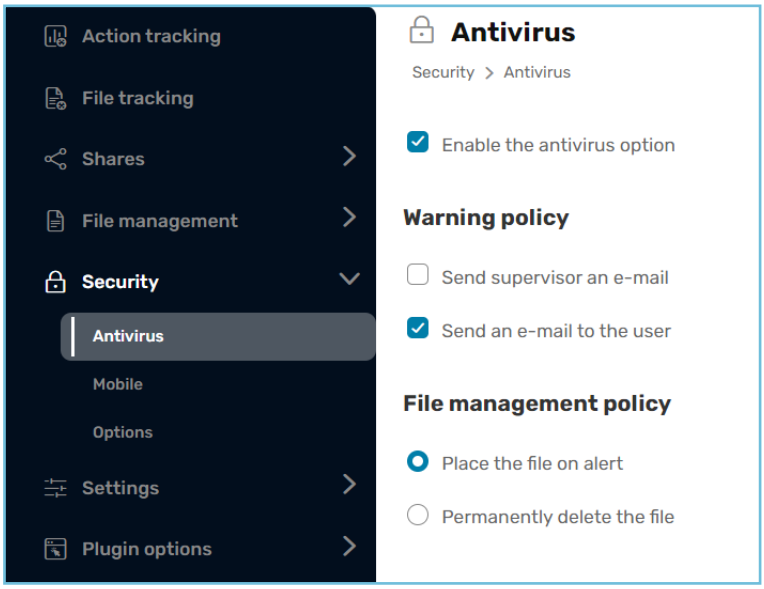
By default, the platform antivirus is activated to place corrupted files on alert and notify the file owner of any detected issues. However, you can modify this antivirus policy so that corrupted files are automatically deleted from your company's workspace.

For users accessing your workspace via Oodrive mobile applications, you also have the option to configure mobile device security options such as:

- Security code
- Biometric authentication
- Data removal
- Third-party apps
- Mobile data networks
- Automatic disconnection

If necessary, you can choose to suspend the downloading of desktop and mobile applications.

You can also enable automatic data removal so that cached data and files synched for viewing offline are automatically removed from the device each time the user logs out of the application.



5.1. Antivirus

The platform provides anti-virus protection that scans your workspace data to detect and contain eventual threats. Configure the antivirus options to notify key personnel of infected, corrupted or potentially malicious files. You can also choose how to manage those files, either by placing them on alert, or permanently deleting them for your company's workspace.

Warning policy

1. In the navigation panel along the left side of the page, select the **Security** section.
2. To notify workspace administrators select **Send supervisor an email**.

   To notify the file owner, select **Send an email to the user**.
3. Enter the email address for the notification to be sent to.
4. Click **Save**.

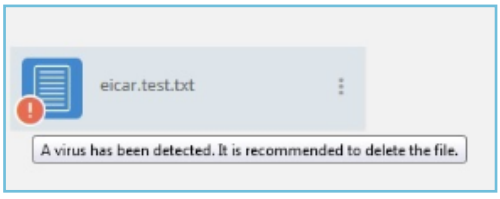
Return to this section at any time to make changes.

File management policy

By default, infected, corrupted or potentially malicious files detected by the antivirus with will be placed on alert. However, if you prefer, you can enable an option to automatically delete files flagged by the antivirus.

1. In the navigation panel along the left side of the page, select the Security section.
2. To notify workspace administrators select **Permanently delete the file**.
3. Click **Save**.

Below is an example of a file that has been flagged after a virus was detected:



Return to this section at any time to make changes.

5.2. Mobile security

Set up mobile security options for users connecting to Oodrive mobile applications. The following options are available for:

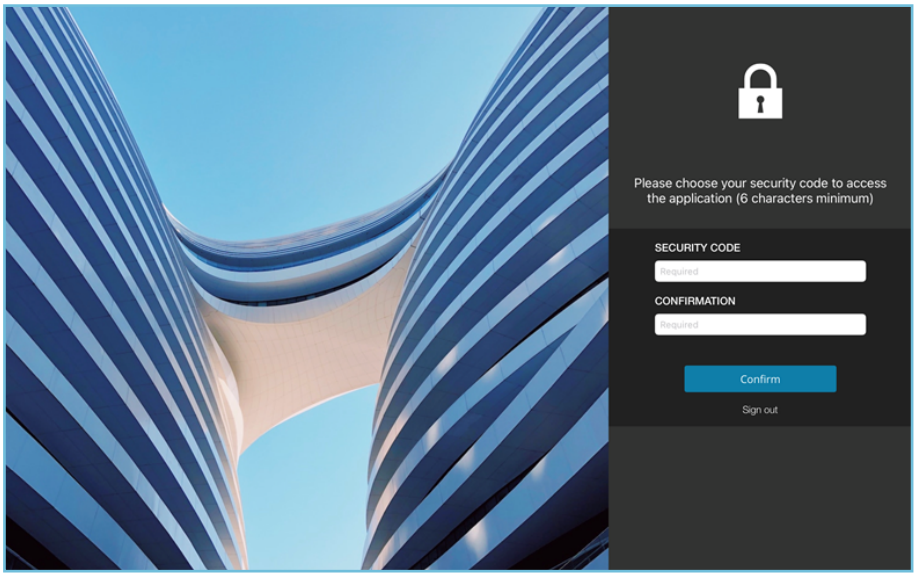
- Security code
- Biometric authentication
- Data removal in the case of failed login attempts
- Third-party apps
- Mobile data use

- Data removal
- Automatic disconnection

Security code

Enable the security code option to add an additional layer of security to Oodrive mobile applications. Once enabled, users with be required to enter their login and security code before being able to access the application.

Below, an Oodrive Mobile user is prompted to set a security code.



1. In the navigation panel along the left side of the page, select the **Security** section, then select **Mobile**.

2. In the **Security code** section, select **Force use of a security code**.

3. Require a minimum number of characters (at least 4) by selecting the **Specify minimum length for security code** option and clicking on the plus symbol.

4. Use the **Validity of security code** drop-down list to select the time period after which a new security code must be defined.

5. Click **Save**.

Return to this section at any time to make changes.

Biometric authentication

You have the option to allow users to replace their security code with fingerprint ID or facial recognition on mobile devices offering these features. Once enabled, users will be prompted to configure biometric authentication in their device settings.

Please note: This feature is not available for the following mobile applications:

- Oodrive Mobile for iOS
- Oodrive_share for iOS

1. In the navigation panel along the left side of the page, select the **Security** section, then select **Mobile**.
2. In the **Security code** section, select **Allow use of biometric authentication**.
3. Click **Save**.

Return to this section at any time to make changes.

Data removal in case of failed login attempts

Protect user data on mobile devices by enabling data removal in case of failed login attempts. When the application detects an important number of failed login attempts, this option deletes cached information, as well as files synchronized offline.

1. In the navigation panel along the left side of the page, select **Security** and then select **Mobile**.
2. In the **Security code** section, select **Erase data in the event of failed attempts**.
3. Click **Save**.

Return to this section at any time to make changes.

Mobile Notifications

You can enable push notifications for users of the mobile applications. Once enabled, users will be notified of the latest activities related to the collaborative shares they have created or received.

1. In the navigation panel along the left side of the page, select **Security** and then select **Mobile**.
2. In the **Options** section at the bottom of the page, select **Enable push notifications**.
3. Click **Save**.

Please note: Users can enable or disable notifications for each collaborative share individually, without any impact on the activity summary.

Return to this section at any time to make changes.

Third-party apps

For security reasons, you may prefer to block the use of third-party apps by users accessing files on Oodrive mobile applications. Once enabled, users trying to access files in the application will only be able to do so via Oodrive specific application features.

1. In the navigation panel along the left side of the page, select **Security** and then select **Mobile**.
2. In the **Options** section at the bottom of the page, select **Block third-party applications**.
3. Click **Save**.

Return to this section at any time to make changes.

Mobile data network use

You have the option to restrict the use of Oodrive mobile applications to company-specific Wi-Fi networks by blocking the use of mobile data. Once you enable this option, users will only be able to access Oodrive applications offline when connected to a mobile data network.

To restrict the Wi-Fi networks to which users can connect, you or your IT security administrator must enable IP address filtering in the Authentication module.

1. In the navigation panel along the left side of the page, select **Security** and then select **Mobile**.
2. In the **Options** section at the bottom of the page, select **Prevent the use of mobile data**.
3. Click **Save**.

Return to this section at any time to make changes.

Data removal upon logout

Add an additional layer of security to protect user data on mobile devices by enabling the data removal option. Doing so will delete the application cache and login information, as well as files synchronized offline in between user sessions once the user logs out of the application.

1. In the navigation panel along the left side of the page, select **Security** and then select **Mobile**.
2. In the **Options** section at the bottom of the page, select **Delete data upon logout**.
3. Click **Save**.

Return to this section at any time to make changes.

Automatic disconnection

For security reasons, you can set a time after which users must provide their password again to keep using the application

1. In the navigation panel along the left side of the page, select **Security** and then select **Mobile**.

2. In the **Options** section at the bottom of the page, click the **Automatic logout after** drop down list.

3. Select the time period after which the user must provide their password (unlimited or between 5 minutes and 48 hours).

4. Click **Save**.

Return to this section at any time to make changes.

5.3. Options

As an Administrator, you have control over the availability of desktop and mobile applications on your platform. You can choose to suspend downloading of these applications at any time. In this case, the applications download menu will no longer be accessible to your colleagues.

1. In the navigation panel along the left side of the page, select **Security** and then **Options**.

2. Select or deselect the option(s) of you choice to enable or disable the downloading of desktop or mobile applications.

3. Click **Save**.

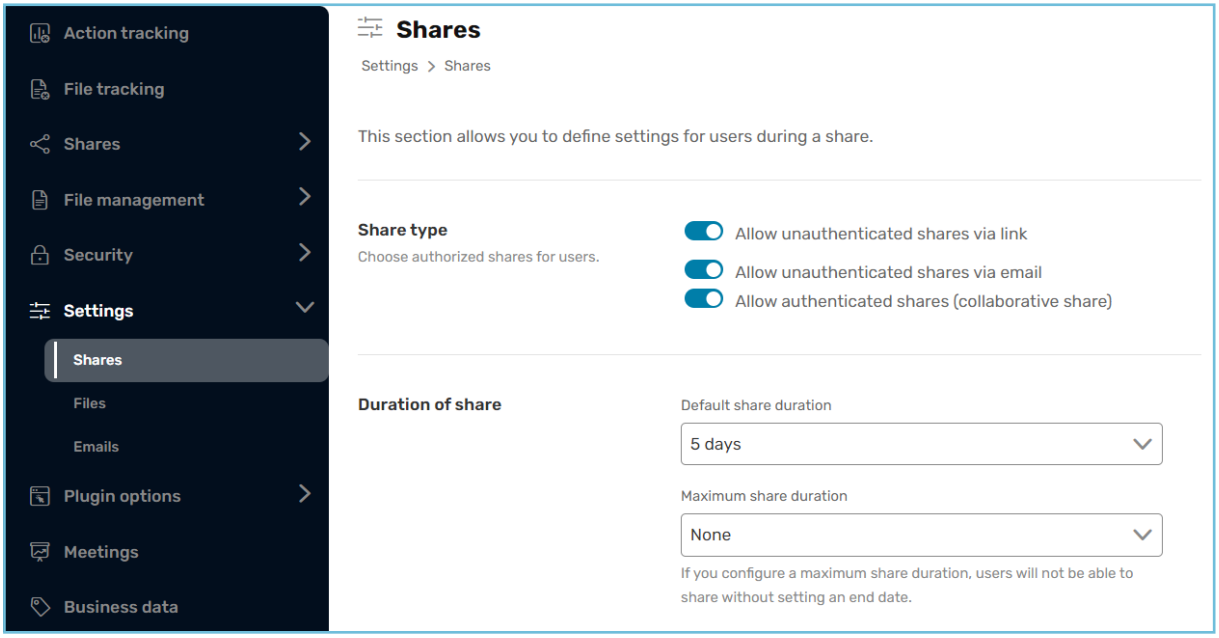
Return to this section at any time to make changes.

6. Settings management

As an Administrator, you have the ability to configure sharing, e-mail and file options on your workspace in order to customize its features and adapt it to fit its intended use within your organization.

Maintain greater control over workspace files and shares by configuring the following options:

- Authorized share types
- Duration of share
- Password protection
- Dynamic watermark
- Personalization of sharing emails
- Memos
- Number of file versions
- Sender email address (notifications)



6.1. Share settings

Authorized share types

By default, all types of sharing are enabled on your workspace.

As an administrator, you can choose which share types are allowed on your workspace, depending on your business needs and your organization's security policy.

You can:

- Allow / forbid sharing via link.
- Allow / forbid sharing via email and drop box.
- Allow / forbid collaborative sharing.

For example, if you wish to restrict use of the workspace to internal collaboration, you can restrict sharing exclusively to collaborative folders, accessible only to users with an account on that workspace.

This prevents any external distribution via hypertext link, e-mail or attachment (PostFiles plugin).

Conversely, if you want your workspace to be used for file transfer only, you can disable collaborative sharing and authorize sharing via link or e-mail.

Note: For more details on the different share types, please consult this sharing comparative document.

Allow / forbid sharing via link

1. In the navigation panel along the left side of the page, select **Settings**, then **Shares**.
2. Enable or disable the **Allow unauthenticated shares via link** toggle switch.
3. Click **Save** twice, then click **Confirm** to confirm your choice.

   If you choose to disable sharing via link, existing shares will be deactivated and the feature will no longer appear on your workspace.

Go back to **Share type** to enable or disable sharing via link in your workspace.

Allow / forbid sharing via email

1. In the navigation panel along the left side of the page, select **Settings**, then **Shares**.
2. Enable or disable the **Allow unauthenticated shares via email** toggle switch.
3. Click **Save** twice, then click **Confirm** to confirm your choice.

   If you choose to disable sharing via email, existing shares will be deactivated and the feature will no longer appear on your workspace. This includes drop boxes.

Go back to **Share type** to enable or disable sharing via email in your workspace.

Allow / forbid collaborative sharing

1. In the navigation panel along the left side of the page, select **Settings** then **Shares**.
2. Disable the **Allow authenticated shares (collaborative share)** toggle switch.
3. Click **Save** twice, then click **Confirm** to confirm your choice.

   If you choose to disable collaborative sharing, existing shares will be deactivated and the feature will no longer appear on your workspace.

Go back to **Share type** to enable or disable collaborative sharing in your workspace.

Duration of share

Manage the lifecycle of files shared via email from your company workspace or from your personal inbox using the PostFiles plugin:

- The **default share duration**, allows you to define a default end-date value for files shared from your company workspace. However, it should be noted that this value will only be applied if the sender chooses to apply the end-date option when sharing the files/folders.
- The **maximum share duration**, allows you to restrict the maximum amount of time for which files may be made available when shared from your company workspace.

1. In the navigation panel along the left side of the page, select the **Settings** section.
2. In the **Duration of share** section, click the **Default share duration** drop-down menu to set the default file availability period (from 1 day to 3 years).
3. If you want to enforce a limit on the availability of shares, click the **Maximum share duration** drop-down menu to set the maximum file availability period (from 1 day to 3 years).
4. Click **Save**.

Return to this section at any time to make changes.

End-of-share alert

By default, users who define a share end-date can choose to receive an end-of-share alert. When enabled, the sender of the share receives an email notification 48 hours before the share expires, and can modify the share-end date if an extension is needed.

1. In the navigation panel along the left side of the page, select **Settings**.

2. To manage the end-of-share alert settings, go to the **Duration of share** section and click the **End of share alert** drop-down menu.

3. Select a default behavior for the end-of-share alert:

   - **Disabled, modifiable by user**
   - **Disabled, non modifiable by user**
   - **Enabled, modifiable by user**
   - **Enabled, non modifiable by user**

   If you allow users to modify this setting, they will be able to choose whether to enable the end-of-share alert.

4. Click **Save**.

Return to this section at any time to make changes.

Password protection

Add an additional layer of security to shared files by activating password protection on your workspace.

By default, users will be able to deactivate password protection on a file by file basis. However, if you would like, you can change this setting to require the use of a password to access all shared files.

There are two password protection options:

- **One-time password (OTP)**

  Available for sharing via email only, this password is generated and sent by the platform automatically when a recipient tries to access the share. It can only be used once and expires after 30 minutes.

- **Personalized password**

  Available for sharing via link or email, this password is defined by the owner of the share. It is the same for all recipients and can be used more than once.

1. In the navigation panel along the left side of the page, select **Settings** then **Shares**.

2. To manage the password protection settings, go to the **APccess torotect share** section and click the drop-down menu corresponding to the option you'd like to enable :
   - **Protection via OTP (one-time password)**
   - **Protection by personalized password**

3. Select a default behavior for the password protection option:
   - **Disabled, modifiable by user**
   - **Disabled, non modifiable by user**
   - **Enabled, modifiable by user**
   - **Enabled, non modifiable by user**

   If you allow users to modify this setting, they will be able to choose whether to enable password protection.

4. Repeat these steps if you'd like to configure a second password protection option.

5. Click **Save** to activate this option on your workspace.

Return to this section at any time to make changes.

Restriction of access permissions

Maintain better control over collaborative shares by defining which access permissions you want to make available to workspace users.

The **Share permissions** section allows you to define the highest access permissions level that users can assign to recipients of their collaborative shares.

1. In the navigation panel along the left side of the page, select **Settings** then **Shares**.

2. To define which access permissions may be assigned to a share recipient, go to the **Share permissions** section and drag the cursor to the highest access permission level you want to make available to users:

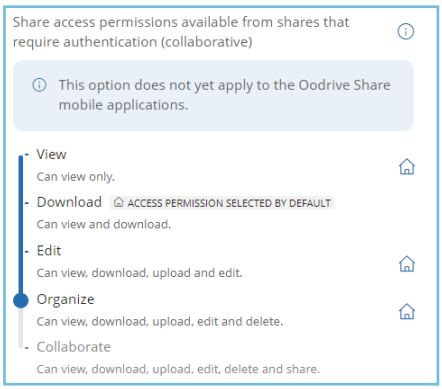
Access permissions	Actions available to share recipient
View	view only.
Download	view and download.

Access permissions	Actions available to share recipient
Edit	view, download, upload and edit.
Organize	view, download, upload, edit and delete.
Collaborate	view, download, upload, edit, delete and share.

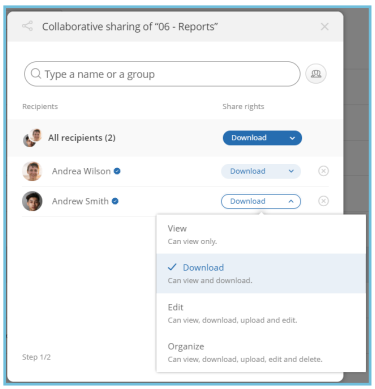
3. To define which access permission is selected by default when creating collaborative shares, click the icon next to that permission.

4. Click **Save**.

Only the access permissions selected in the **Share permissions** section will be displayed when workspace users create collaborative shares.



Restriction of access permissions in the Sharing Administration module



Available access permissions when creating a collaborative share

Please note: The restriction of share access permissions has no impact on existing collaborative shares, unless the owner attempts to modify the share. In this case, the owner will be required to select a new access permission from the list of available options.

Return to this section at any time to make changes.

Delete files when share ends

By default, users can enable a setting that will delete files shared via e-mail once the share expires. When enabled, shared files will be automatically deleted from the workspace at the end-of-share date. However, the deleted files can still be found in their owner's trash.

1. In the navigation panel along the left side of the page, select **Settings**.

2. To manage the automatic deletion settings, go to the **Shared files** section and click the **Automatic deletion of files when share expires** drop-down menu.

3. Select a default behavior for the automatic deletion of files:

   - **Disabled, modifiable by user**
   - **Disabled, non modifiable by user**
   - **Enabled, modifiable by user**
   - **Enabled, non modifiable by user**

   If you allow users to modify this setting, they will be able to choose whether to enable automatic deletion of files when a share expires.

4. Click **Save**.

Return to this section at any time to make changes.

Dynamic watermark

Enable the dynamic watermark option to better protect shared workspace files. When enabled, this option automatically transforms shared Microsoft Office, TXT and AutoCAD files into dynamically watermarked PDFs.

As a result, once the share is received and viewed/printed/downloaded, every page of the document will include the share recipient's name and the date of the share. However, when a file is shared via link, the link creator's information is displayed instead of the recipient's.

Please note: When using this option with the PostFiles plugin, all email attachments will be automatically transformed into PDF files when shared, regardless of the actual format of the file (s) attached. The dynamic watermark does not apply to video or image file formats.

1. In the navigation panel along the left side of the page, select **Settings** then **Share options**.

2. Define the share types for which you want to enable the dynamic watermark by selecting the corresponding option:

   - **Add a watermark to files shared via email or link**
   - **Add watermark to collaborative shares**

   To allow the user to modify this setting, select **Allow the user to change this option**.

To prevent the user from modifying this setting, deselect the option **Allow the user to change this option**.

3. Click **Save** to activate on your workspace.

Below is an example of a document visualized with the dynamic watermark option applied:

Return to this section at any time to make changes.

Personalization of email content

This option, which is enabled by default, allows workspace users to personalize the content of sharing emails.

You can disable/re-enable this option at any time in the share options.

1. In the navigation panel along the left side of the page, select **Settings** and then **Shares**.

2. Enable or disable the **Allow personalization of e-mail content** setting to allow or prevent personalization of sharing emails.

3. Click **Save**.

Return to this section at any time to make changes.

6.2. File settings

Memos

This option allows platform users to create memos on files and folders they own, or which were made available to them through sharing.

Users can create memos for various purposes, for example:

- Adding personal annotations to their own files and folders
- Collaborating on a remote project without marking documents with annotations
- Collaborating on documents for which they do not have modification rights
- Participating in a digitized validation process

Please note: The owner of each file can delete memos added by their colleagues.

1. In the navigation panel along the left side of the page, select **Settings** and then **Files**.
2. Select **Enable memos**.
3. If you want to enable the option to tag other users, select **Authorize users to tag other users** and click **Enable**.

   Users will be able to tag colleagues in memos to draw their attention to a message. Email notifications are automatically sent to the tagged users.
4. Click **Save** to activate on your workspace.

Return to this section at any time to disable these options.

If you disable memos, memos created by users will no longer be accessible on the workspace, but they will be kept in memory and restored if the option is re-enabled at a later date.

Maximum number of versions allowed

The collaboration application automatically generates a new version each time a file is edited on the platform. By default, the platform keeps the ten latest versions of a file, so that users may retrieve an earlier version if needed.

As an Administrator, you can define the maximum number of versions to keep for workspace files.

Careful: If you enter a number of versions that is less than the previous setting, all additional versions will be permanently lost.

1. In the navigation panel along the left side of the page, select **Settings**, then **Files**.
2. Enter the number of versions to keep in the **Maximum number of file versions** field.
3. Click **Save** to update the maximum number of versions allowed on your workspace.

Return to this section at any time to make changes.

6.3. Email settings

When collaborating within the Oodrive solution, users will automatically receive email notifications about shared files and platform activities.

By default, these notifications are sent from the address “notifications@oodrive.com”. The sender name, however, depends on the type of notification:

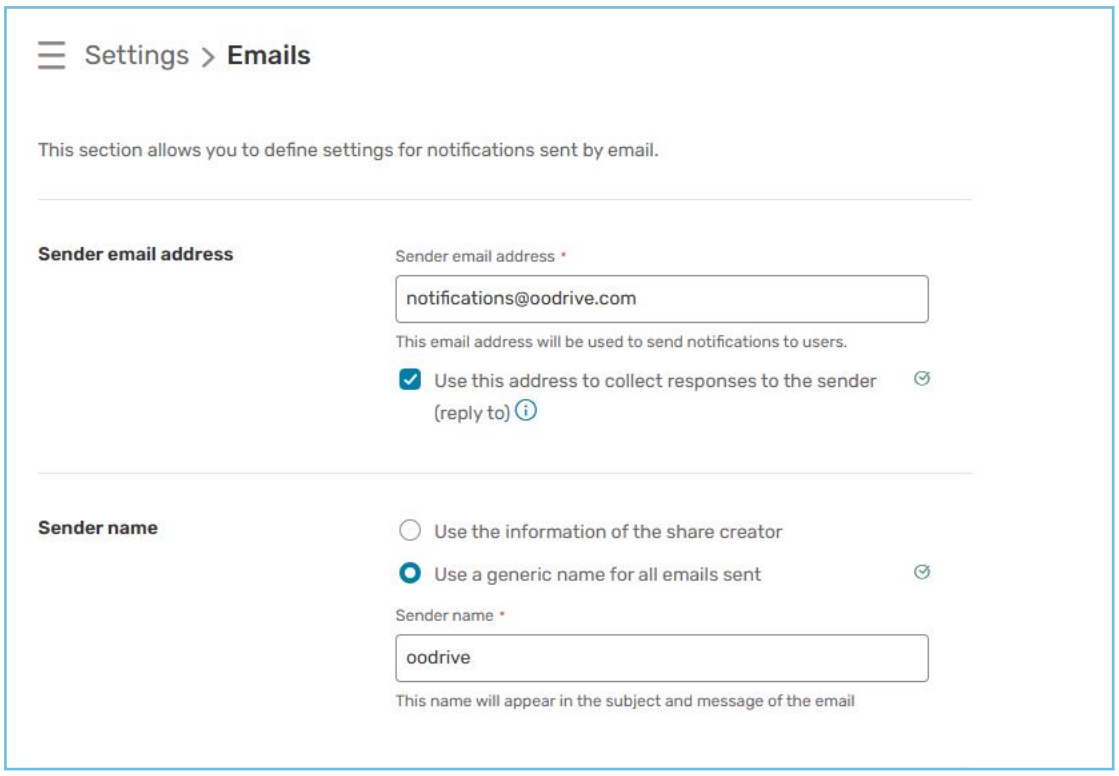
- “Notification” for general platform activity notifications
- The first and last name of the user who created an account or a share

As an administrator, you have the option to customize both the sender address and the sender name.

Configure the sender email address

You can set up a generic sender address for the notifications sent by the platform. You can also choose to use this address to centralize responses from recipients.

1. In the navigation panel along the left side of the page, select **Settings** and then **Emails**.
2. Go to the **Sender email address** section and enter a new sender email address in the field provided.



3. If you want recipients' replies to be redirected to this mailbox, check the box **Use this address to collect responses to the sender (reply to)**.

4. Click **Save**.

Modify the sender emails at any time by returning to the **Emails** section and saving your changes.

Set up a generic sender name

By default, when a user creates an account or a share (collaborative, via drop box, or via email), their name appears as the sender in the notification emails sent to recipients.

However, it is possible to configure a generic sender name that will replace the personal information of the user who performed the action.

1. In the navigation panel along the left side of the page, select **Settings** and then **Emails**.

2. Go to the **Sender name** section and select **Use a generic name for all emails sent**.

3. Enter the generic name you would like to use in the field and click **Save**.

   This name will appear in the email subject line and message body.

7. Plugin management

Two components are available to manage attachments via the Outlook email client.

- The **Oodrive Work** add-in, compatible with the most recent version of the Outlook client and available for Web, Windows and Mac environments.
- The **PostFiles** plugin, compatible with older versions of the Outlook client and available for Windows only.

These components take over from the standard attachment system and generate a secure sharing link, with all the security and tracking options specific to the Oodrive Work solution.

7.1. Deployment

Deploy Oodrive Workadd-in

Oodrive puts at your disposal a manifest file in XML format. This manifest contains all the information needed to integrate the add-in into Outlook (such as the service URL, required permissions and the add-in's user interface).

Two versions are available depending on the options you wish to make available:

- **Standard configuration:** users can choose whether or not to use the Work add-in to send attachments, at their own discretion.

  The standard configuration offers the following features:

  - Generation of a sharing link in the email
  - Automatic addition of attachments (configurable file size for triggering)
  - Limit on the number of downloads
  - Choice of sharing duration and automatic file deletion at the end of sharing period
  - Add watermark to shared files
  - Add password for access to shared files
  - Choice of language for the sharing link

  Download the manifest in standard configuration.
- **Advanced configuration:** the administrator can configure additional options specific to the Outlook add-in in the **Share Administration** module.

  The advanced configuration offers the following features:

  - All the features of the standard configuration
  - The workspace administrator can make the use of the Oodrive Work add-in mandatory

- Activity summary on sent shares
- One-time password (OTP) protection for sent shares

Download the manifest in advanced configuration..

Requirements : Download one of the two manifests provided by Oodrive to proceed with deployment.

The Office 365 administrator must:

1. Sign in to the Microsoft 365 Admin Center.
2. Import the XML manifest file via add-ins management (either in the Exchange Admin Center, or directly via the "Integrated apps" section).
3. Choose the deployment method (to all users, to specific groups or to certain users).
4. Define whether the add-in is mandatory or optional.
5. Validate deployment so that the add-in is automatically available in Outlook for all targeted users.

For more information about the deployment of add-ins in Microsoft, please refer to: Deploy add-ins in the Microsoft 365 admin center.

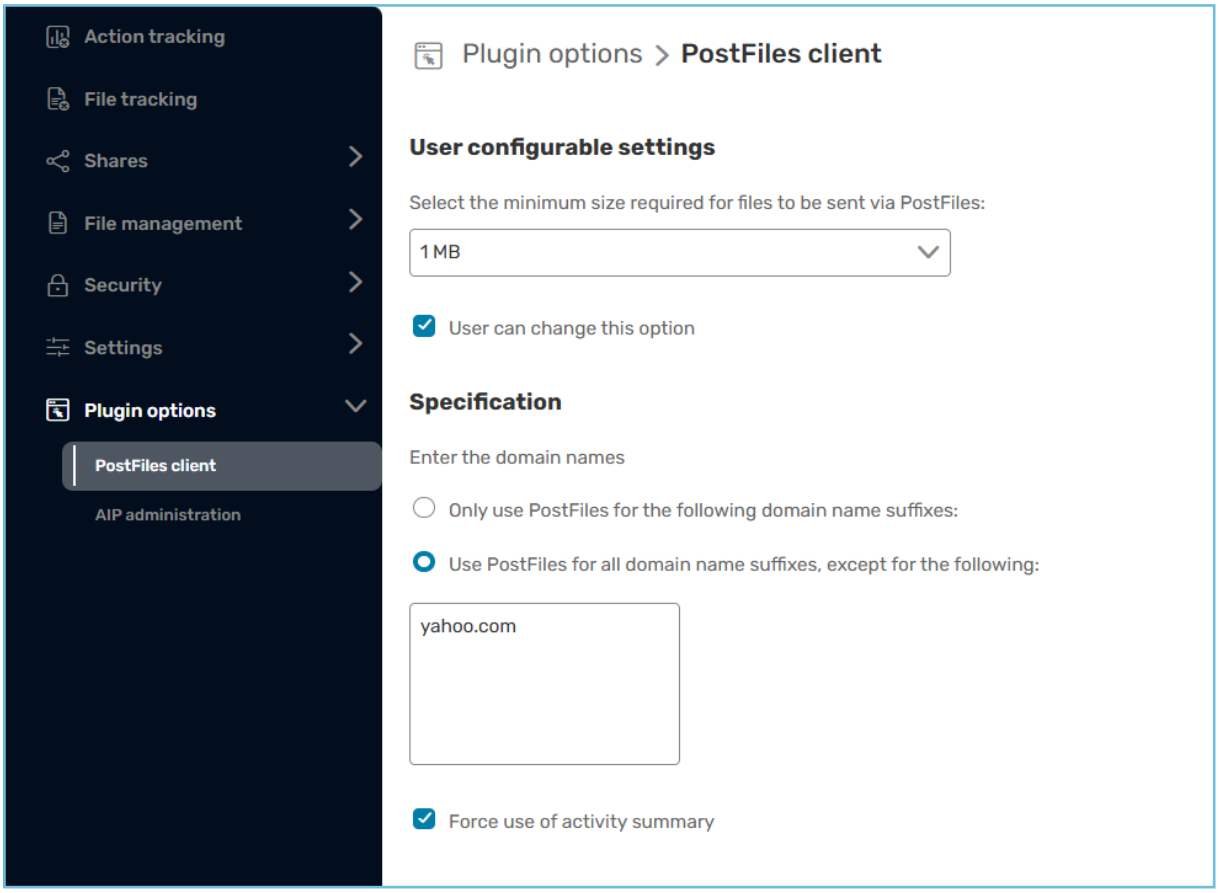
Deploy PostFiles plugin

For more information about the deployment of the PostFiles plugin, please refer to the dedicated guide: PostFiles Outlook Administration.

7.2. Configure plug-in options

You can configure the following advanced options for the **PostFiles plug-in** and Oodrive Work add-in in the **PostFiles client** section:

- Define the minimum file size required for attachments to be sent via the plugin
- Require or prevent the use of the plugin for certain email domains (cannot be changed by the user)
- Require activation of the activity summary when using the plugin



Minimum file size

Careful: This option is available for the Work add-in only if you have deployed the manifest in advanced configuration.

Set the minimum file size required for attachments to be sent via the PostFiles plugin or Work add-in.

By default, users will be allowed to modify these options based on their personal preferences. However, if you would like, you can prevent individual users from modifying these settings.

1. In the navigation panel along the left side of the page, select the **Plugin options** section.
2. In the **User configurable settings**, go to **Select the minimum size required for files to be sent via PostFiles** and click on the drop-down menu.
3. Select a file size (100 KB to 20 MB).

   If you select **Unlimited**, the plugin/add-in will be used to send email attachments regardless of the file size.

4. To allow the user to modify this setting, leave the option **User can change this option** selected.

   To prevent the user from modifying this setting, deselect the option **User can change this option** selected.

5. Click **Save** to apply your changes.

Return to this section at any time to make changes.

Email domains

Please note: This option is currently only available for the PostFiles plug-in.

Require or prevent the use of the PostFiles plugin for certain email domains. Doing so will ensure, for example, that the PostFiles plugin is always used or is never used when collaborating with specific external partners.

1. In the navigation panel along the left side of the page, select the **Plugin options** section.

2. In the **PostFiles client** section, go to the **Specification** section.

3. Select how you would like to configure the use of the PostFiles plugin via domain names:

   - **Require** the use of the PostFiles plugin: **Only use PostFiles for the following domain name suffixes**
   - **Prevent** the use of the PostFiles plugin: **Use PostFiles for all domain name suffixes, except for the following**

   Please note: You cannot use both methods simultaneously.

4. Enter an email address domain name in the field provided (e.g., google.com, hotmail.com, etc.) and click **Add**. Repeat the process to add others.

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

Remove email domains at any time by clicking on the recycle bin to the right of the email domain you would like to remove, then click **Save**.

Activity summary

Careful: The **Force use of activity summary** option is available for the Work add-in only if you have deployed the manifest in advanced configuration.

By default, plugin users can choose whether to receive reports informing them of activities performed by sharing recipients.

However, if you would like, you can enforce the use of reports for all plugin users. Users can still choose how often they want to receive these reports.

1. In the navigation panel along the left side of the page, select the **Plugin options** section.
2. In the **Specification** section, select the **Force use of activity summary** option.
3. Click **Save** to apply your changes.

Return to this section at any time to disable this option.

7.3. AIP Administration

The **AIP Administration** section allows you to configure confidentiality labels for attachments to be sent via the PostFiles plug-in and the Work add-in. You also can enforce the use of the add-in based on MPIP labels to secure attachments.

For more information, please refer to the following guides:

- Administrator Guide Microsoft AIP for PostFiles Outlook.
- Administrator Guide Microsoft MPIP for Work for Outlook.


∞drive