

Policies and configuration

For institutional (branded) instances, several policies can be set as well as additional configuration. In this page the possibilities are listed.

Institute's (technical) contact persons can send specific requests regarding these policies and configuration options via our [service desk](#).

Contents

- [Policies](#)
- [Contact and online resources](#)
- [General configuration](#)
- [Sharing configuration](#)
 - [Public links](#)
 - [Shares](#)

Policies

Name	Description	Values	Default
Account types	The types of accounts that can be created to authenticate a user. To enable SURFconext logins, your institute's ICT department needs to approve Research Drive to connect to your institute's identity provider.	<ul style="list-style-type: none">• SURFconext & local• Local only	SURFconext & local
Federated login	Federated login with SURFconext with or without attributes . An attribute (e.g. researcher, employee) can be connected to the login. Only users with the specified attribute can login with their institutional account.	<ul style="list-style-type: none">• SURFconext• SURFconext with attributes	SURFconext
Two-factor authentication	Allow the use of two-factor authentication for all institutional users using SURFsecureID . For guest accounts: option for 2FA in user settings of individual account cannot be technically enforced, but should be part of (RDM) policy	<ul style="list-style-type: none">• Enabled• Disabled	DISABLED
Retention period (trashbin)	The period a file or folder is residing in the trash bin (and can be restored) before it is permanently removed from the system.	<ul style="list-style-type: none">• 30 days• 90 days• Longer	30 days
Retention period (versions)	The period a file or folder is residing in the versions (and can be restored) before it is permanently removed from the system. Note that retention logic is in place.	<ul style="list-style-type: none">• 14 days• 30 days• Longer	14 days
External storage	Allow connections to external storage providers or systems such as Google Drive, Dropbox, Amazon S3, SURFdrive, etc. Specific providers can be enabled or disabled.	<ul style="list-style-type: none">• Enabled• Disabled	DISABLED
Jupyter Notebook	Allow users to run their own Jupyter notebooks and store them in one of the folders in Research Drive.	<ul style="list-style-type: none">• Enabled• Disabled	ENABLED
Collaborative editing	Allow users to collaboratively work in documents simultaneously using OnlyOffice. This includes Word-like, PowerPoint-like and Excel-like documents.	<ul style="list-style-type: none">• Enabled• Disabled	ENABLED
Password policy (general)	Set the policies for the password for local user accounts and public links	<ul style="list-style-type: none">• Enforce <i>n</i> lowercase, uppercase letters, numbers and/or special characters, enforce a minimum and /or maximum length	10 character minimum

Password policy (users)	Set additional password policies for local user accounts Note: this does <i>not</i> apply to your institutional password policy and thus users that login via SURFconext	<ul style="list-style-type: none"> Last n passwords should not be used Force users to change their password on first login 	No policies set
Password policy (public links)	Set additional password policies for public links	<ul style="list-style-type: none"> n days maximum until link expires if password is set n days maximum until link expires if password is not set 	No policies set

Contact and online resources

Name	Description	Values	Default
Helpdesk contact	The contact point for helpdesk-related questions and issues specific for the institute (email address)	Your institute's helpdesk email address	
Wiki URL	The URL of the wiki where additional and user documentation can be found specific for the institute	Your institute's wiki URL	
Terms of Use URL	The URL of the terms of use of the instance defined by the institute	Your institute's terms of use URL	
Privacy policy URL	The URL of the privacy policy that applies to the instance defined by the institute	Your institute's privacy policy URL	

Greyed-out items are coming soon.

General configuration

It is possible to set specific configuration value for elements within Research Drive, like sharing options. This can be useful to limit sharing of sensitive data or increase security during authentication.






Option	Description	Values	Default
External storage types	Define the allowed external storage services and protocols to be applied by a user	<ul style="list-style-type: none"> Amazon S3 Dropbox Google Drive OneDrive ownCloud SFTP WebDAV 	None
Allow sharing of external storage folders	Allow a user to share the folders that are obtained from an external storage service	<ul style="list-style-type: none"> Enabled Disabled 	ENABLED
Offer client downloads on first login	Show OwnCloud client download options on first login	<ul style="list-style-type: none"> Enabled Disabled 	ENABLED

Sharing configuration

Sharing is an important feature of Research Drive. By default many sharing options are enabled to offer flexibility and usability, but if required some aspects can be turned off for security reasons or institutional policies.




Public links

Public links can be used to quickly share data from your instance with people that do not have a user account or specific access to the data.

Option	Description	Values	Default
Allow public links	Allow sharing of files and folders using a public link	<ul style="list-style-type: none">• Enabled• Disabled	
Enforce public link passwords	Enforce the use of passwords for public links A distinction can be made between links that are read-only or allow uploads or edits to files and folders.	<ul style="list-style-type: none">• Enabled• Disabled	
Public link expiration	Enforce automatic expiration of public links	Either or both: <ul style="list-style-type: none">• n days until link expires if password is set• n days until link expires if password is not set	No policies set
Allow emailing public links	Allow a user to send a public link directly via email in the Research Drive instance	<ul style="list-style-type: none">• Enabled• Disabled	
Allow sharing via social media	Allow sharing public links directly via social media	<ul style="list-style-type: none">• Enabled• Disabled	
Allow file drop functionality	Allow a public link to provide a file drop zone where users can upload files without seeing other user's uploads	<ul style="list-style-type: none">• Enabled• Disabled	

Shares

Shares are used to share files or folders with users that are known in your instance or with [other ownCloud-based instances](#) such as SURFdrive or another institute's Research Drive.

Option	Description	Values	Default
Automatically accept local shares	Automatically accept new shares coming from your own instance without an accept notification	<ul style="list-style-type: none">• Enabled• Disabled	
Allow resharing	Allow repeated sharing of files and folders that have been shared with a user	<ul style="list-style-type: none">• Enabled• Disabled	
Allow sharing with groups	Allow sharing of files and folders with a group (instead of only with a specific user)	<ul style="list-style-type: none">• Enabled• Disabled	

<ul style="list-style-type: none"> • Restrict to users in own groups 	Restrict users to only share with users in groups they are a member of	<ul style="list-style-type: none"> • Enabled • Disabled 	DISABLED
<ul style="list-style-type: none"> • Restrict to own groups 	Restrict users to only share with groups they are a member of	<ul style="list-style-type: none"> • Enabled • Disabled 	DISABLED
Allow mail notification for shares	Allow users to send mail notification for shared files to other users	<ul style="list-style-type: none"> • Enabled • Disabled 	ENABLED
Allow user name auto-completion in share dialog	<p>Always show a list of user names based on the characters typed in the share dialog.</p> <p>If this is disabled the full user name needs to be entered before an option becomes visible</p>	<ul style="list-style-type: none"> • Enabled • Disabled 	ENABLED
Federated sharing creation	Allow sharing of files and folders to users of other instances (e.g. SURFdrive or another institute's Research Drive instance)	<ul style="list-style-type: none"> • Enabled • Disabled 	ENABLED
Federated sharing acceptance	Allow receiving shares of files and folders from users of other instances (e.g. SURFdrive or another institute's Research Drive instance)	<ul style="list-style-type: none"> • Enabled • Disabled 	ENABLED