Administration Help

Fabasoft Private Cloud

Contents

1 Introduction

The Fabasoft Private Cloud lets you create a digital business network for your company based on relationships of trust – for secure cross-company, transnational collaboration in the cloud.

2 Organization

In the Fabasoft Private Cloud you act as organization. Via the organization you can carry out all the relevant administrative tasks. The management tasks include, for example, the administration of members the assignment of service packages and defining the authentication settings.

Your organization is automatically placed on "Home", if you are owner or administrator of the organization.

Click the organization to open the organization dashboard. In the tools area you can directly execute frequently needed actions. The content area provides an overview of the organization.

Note:

- Owners have access to all Teamrooms of the organization and thus can view all the data. Administrators can manage the organization but cannot access the Teamrooms of the organization. Chapter 3 "Organization Roles" describes how to change the roles.

3 Organization Roles

Via the following organization roles, you can define users who are responsible for managing the organization:

- Owner and Co-Owners
  The owner and co-owners can manage the organization, have access to all Teamrooms of the organization and thus can view all the data.
  A new owner can only be entitled by the current owner. Co-owners can be defined by the owner and other co-owners.

- Main Owner
  If a main owner is defined, only this user will receive the automatically generated e-mail messages concerning the organization. The user is also listed as contact in case of missing permissions.
  The *Main Owner* field is only visible if at least one co-owner is defined.

- Compliance Manager
  Due to legal regulations, it may be necessary to anonymize users. When a user's membership is terminated, compliance managers are notified by e-mail. The compliance managers can immediately anonymize the user, identify all links to the user or define a reminder for a specific point in time.

- Main Administrator and Administrators
  The main administrator and the administrators can manage the organization but have no access to the Teamrooms of the organization. The main administrator can be chosen from the administrators. If a main administrator is defined, only this administrator receives automatically generated messages that concern the organization. Otherwise all administrators receive these messages.
  Administrators and the main administrator can be defined by the owner, co-owners.
  The *Main Administrator* field is only visible if at least two administrators are defined.

- Support Team
The support team handles the organization-internal management of support requests and can be defined differently in the respective context (app, Teamroom) if necessary.

To define organization roles, perform the following steps:

1. In the dashboard of the organization click *Advanced Settings.*
2. Click the "Define Organization Roles" action.
3. Define the desired organization roles.
4. Click "Save".

Note: Organization roles (except *Owner*) can also be assigned to users who are not members of the organization.

4 Organization Members

To allow users to access the Fabasoft Private Cloud, they have to be added as organization members to the organization.

The administration of members, external members, teams, organizational units and external organizations follows a uniform scheme. This allows you to quickly find your way around all areas of membership administration.

Lists in the Membership Administration

- Lists provide an easy way to perform operations on multiple users simultaneously.
- You can cut, copy or paste users and thus efficiently define the organizational structures. For example, you can use `Ctrl + X` to remove the selected users from a team.
- The properties of users, organizational units, external organizations or teams can also be changed efficiently using column editing (`F2` key or `Ctrl + C` and `Ctrl + V`).

Determining the Main Organization

If a user is a member of multiple organizations, the main organization is determined as follows:

1. The user is a member of the organization and the organization's e-mail domain matches the user's email domain.
2. The user is a member of the organization.
3. The user is an external member of the organization.
4. The user is a member of the trial organization and the e-mail domain of the trial organization matches the e-mail domain of the user.
5. The user is a member of the trial organization.
6. The user is an external member of the trial organization.

4.1 Import Members

Via the CSV import also many members can be created comfortably.

1. In the dashboard of the organization click *Membership*, to open the membership administration.
2. Click the "Import Members" action.

3. Enter the path to the CSV file in the *Content* field.
   Note: Click the "Download CSV Template" button to retrieve a template that describes the necessary data structure.

4. Click "Start Import".

5. After the import has finished, click "Next".

The imported members are stored in the members list. In case of a re-import existing members are updated. The unique identification of the members is carried out via the e-mail address.

The "Invite Members to the Organization" action can be used to send an invitation e-mail to the imported members (see chapter 4.3 "Invite Members").

Data structure of the CSV file

CSV Column	Description
EMail	Log-in E-Mail Address (unique; required) **Note:** Used as key if `objexternalkey` does not contain a value.
CN	Common Name (is necessary for the log-in with client certificates and has to correspond with the CN of the client certificate of the particular user)
PinPhone	Phone Number the SMS PIN Is Sent to (if not defined, the log-in e-mail address is used)
PinEMail	E-Mail Address the E-Mail PIN Is Sent to (if not defined, the log-in e-mail address is used)
PinRadiusID	RADIUS Server User Identification (if RADIUS is used, the user identification corresponding to your server configuration can be defined here)
PinOrder	Dispatch Type for Two-Factor Authentication • `MPO_SMSFIRST` (SMS) • `MPO_EMAILFIRST` (E-Mail) • `MPO_RADIUSFIRST` (Use RADIUS Server)
samlemail	E-Mail Address for Active Directory / SAML 2.0
FirstName	First Name (required)
MiddleInitial	Middle Initial
Surname	Surname (required)
Title	Title
PostTitle	Post Title

Sex	Sex (possible values: `SEX_FEMALE`, `SEX_MALE`, `SEX_DIVERSE`)
Salutation	Salutation
Birthday	Birthday (format: `yyyy-mm-dd`)
Street	Addresses (Street)
PostOfficeBox	Addresses (Post Office Box)
ZipCode	Addresses (ZIP Code)
City	Addresses (City)
State	Addresses (State)
Country	Addresses (Country)
Phone	Telephone Numbers (Business)
Fax	Telephone Numbers (Fax)
Mobile	Telephone Numbers (Mobile)
PrivatePhone	Telephone Numbers (Private)
Function	Function in the Organization
TeamKey	Import ID (of the team; if no team with the import ID is found a new one is created, otherwise the name is updated if applicable)
TeamName	Name (of the team)
AdminTeamKey	Team Administrator (possible values: *Import IDs* of the teams to be administrated separated by „|")
Website	Website
Language	Language (spelling corresponding to the language e.g. Español; the possible values can be found in the CSV template or in the „Basic Settings" under *Language*; alternatively language identifiers according to ISO 639-1 can be used)
Edition	Edition (possible values: *Fabasoft Cloud ID* or reference of the edition)
Apps	Apps (possible values: *Fabasoft Cloud ID* or full reference of apps separated by „|")

`InvalidAuthMethods`	Deactivated Authentication Methods (possible value: `AuthenticationMethodUsernamePassword`)
`MainLocation`	Default Data Location (possible values: `at`, `de`, `ch`; not available in the Fabasoft Private Cloud)
`InvitationSent`	Invited (possible values: `true`, `false`)
`ManageHome`	Manage Home (possible values: `true`, `false`)
`CreateTeamrooms`	Create Teamrooms – All Data Locations (possible values: `true`, `false`)
`CreateTeamrooms-LocationAustria`	Create Teamrooms – Data Location Austria (possible values: `true`, `false`; not available in the Fabasoft Private Cloud)
`CreateTeamrooms-LocationGermany`	Create Teamrooms – Data Location Germany (possible values: `true`, `false`; not available in the Fabasoft Private Cloud)
`CreateTeamrooms-LocationSwitzerland`	Create Teamrooms – Data Location Switzerland (possible values: `true`, `false`; not available in the Fabasoft Private Cloud)
`TransferTeamrooms`	Transfer Teamrooms (possible values: `true`, `false`)
`grpolicysearchaudit`	Use Search Folders for Audit Logs (possible values: `true`, `false`)
`grpolicyaddmembers`	Add Members to the Organization (possible values: `true`, `false`)
`grpolicyremovemembers`	Remove Members From the Organization (possible values: `true`, `false`)
`grorgstructmanagers`	Manage Organizational Structure (possible values: `true`, `false`)
`grorgunitmanagers`	Manage Teams (possible values: `true`, `false`)
`grpolicyaddexternal`	Add External Members to the Organization (possible values: `true`, `false`)
`grextorgmanagers`	Manage External Organizations (possible values: `true`, `false`)
`grpolicyopenonlineex`	Edit Office Documents in Microsoft Office Online (possible values: `true`, `false`)

`grpolicyreadonworkspace`	Open or Download Content on the Device (possible values: `true`, `false`)
`ImageName`	Photo (name of the image that should be assigned)
`ImageTeamrooms`	*Fabasoft Cloud ID* of the Teamroom that contains the images
`objexternalkey`	Unique ID **Note:** Used as key if a value is present (thus allowing you to update the e-mail address that is otherwise used as key).
`OverrideKeys`	CSV columns of properties to be overwritten separated by commas (otherwise empty values are ignored and values are added in list properties) For addresses, telephone numbers and organization policies following keys must be used for the related CSV columns: `address`, `telephone`, `policies` (for addresses, telephone numbers the following applies: overwriting is carried out within the corresponding type, e.g. Fax; for policies the following applies: empty cell is equivalent to `false`)

Note: To add several addresses or assign members to several teams, more lines with the same e-mail address (`EMail`) can be specified.

4.2 Add Members

In addition to the CSV import, members can also be created and managed individually.

1. In the dashboard of the organization, click *Membership* to open the membership administration.
2. Click the "Add Members" action.
3. In the *Users* field, enter the e-mail address of the user.
4. In the drop-down menu, click an existing user to add the user as a member. If no user with the entered e-mail address exists, click "Invite new user" to create a new user.
5. To add additional members repeat step 3 and 4.
6. If applicable, select the teams or organizational units to which the users should be assigned.
7. Click the "Add" button.
8. Assign an edition and apps to users without an edition and click "Assign". This step is omitted, if all specified users already have an edition.
9. Click "Invite" to send each member an e-mail with a link to the initial setting of the password. Click "Invite Later" to send the invitation later (see chapter 4.3 "Invite Members").

The added members can be further processed via the "Properties" context menu command.

4.3 Invite Members

If you have performed a CSV import or manually added users who have not yet been invited, you can send an invitation via the "Invite Members to the Organization" action.

To invite members, perform the following steps:

1. In the organization, click the "Invite Members to the Organization" action. The action is only available if members are present who have to be invited.
2. Define the recipients. For easy selection of recipients, the following recipient groups can be selected: not invited members, not registered members and members with open confirmation.
3. The fields *Subject* and *Message* are prefilled. Take any necessary adjustments.
4. Click "Invite".

An e-mail with a link to the initial setting of the password is sent to the members.

Note:

*   Members can also be invited to organizational units, teams and external organizations.
*   The e-mail standard text can be defined in the properties of the organization ("E-Mail Invitations" tab).

4.4 State Information

To check the state information of users, navigate in the organization in the membership administration. The state information is shown as columns by default.

*   *State*
    Users can be the owner, member or external member of the organization. If the state must be confirmed by the user and the confirmation is still pending, the "Confirmation Required" state is displayed.
*   *Invited*
    Shows whether the user has been invited by e-mail. The value can also be manually changed to "Yes", if the user should no longer to be considered in the "Invite Members" dialog, for example.
*   *Registered*
    Shows whether the user is registered and can therefore log into the Fabasoft Cloud.

Note: Users who rejected an invitation or have been excluded from the organization are displayed in the membership administration under "Exclusions".

4.5 Change Membership

External members can be converted to members and vice versa.

To change the membership, perform the following steps:

1. In the dashboard of the organization, click *Membership*.
2. Navigate to the desired member or external member.
3. In the context menu of the member or external member, click "Change Membership".
4. If applicable, select external organizations, teams or organizational units to which the user should be assigned to and click the "Change Membership" button.

5. If a member has administrative rights in the organization, you must confirm the loss of the rights.

Changing a membership removes a member from all teams and organizational units and removes an external member from all external organizations.

4.6 Exclude Members

Members who have been excluded from an organization are also removed from all positions, teams and Teamrooms. When excluding a member, a successor can be defined. This successor is entered in the positions, teams and Teamrooms that the user has been excluded from.

To exclude a member from an organization, perform the following steps:

1. Navigate to the desired member.
2. In the context menu of the member, click "Exclude Member".
3. Define whether the member is to be informed by e-mail and the user is to be deactivated. If necessary, specify a successor.
   o The user can only be deactivated, if the user is managed by your organization. If the user is not a member of any other organization, the user is always deactivated.
   o Only members can be selected as successors of members. Members and external members can be selected as successors of external members.
4. Click "Exclude Member" to confirm the exclusion.

Excluded members are displayed in the organization in the membership administration under "Exclusions". Here you can also view the processing state of the exclusion.

Processing State:

- In Progress
  The exclusion is processed using a background task. If an error occurs, this process is repeated up to five times. If the fifth attempt is also unsuccessful, the processing state is changed to "Manual" and the organization administrators receive an e-mail with the option to manually handle the unhandled Teamrooms and revoke access rights.

- Finished
  The exclusion was successfully carried out.

- Manual
  The exclusion could not be carried out completely automatically. The organization administrators will receive an e-mail with the option to manually handle the unhandled Teamrooms and revoke access rights.

Note:

- Users who have full control in the organization's Teamrooms and are members of this organization will be notified by e-mail. If the excluded user is the last user with „Full Control" in a Teamroom and no successor has been defined, the owner of the organization becomes the user with "Full Control" of the Teamroom.

- Activities in the member's worklist are automatically assigned to the successor.

- If a successor is defined when terminating the membership of a user with special organizational roles (e.g. co-owner), the successor is not entered in the organizational roles.

- The removal of the user from the Teamroom and the adding of the successor to the Teamroom may take some time.
- When terminating a membership in external organizations, organizational units or teams, those with full control in the Teamroom are also informed by e-mail, if the Teamroom is restricted to the affected external organization, organizational unit or team.
- For Teamrooms of other organizations the following applies:
  - If the user's membership in his or her main organization is terminated, users with full control in Teamrooms of other organizations will also be informed about the exclusion and, if applicable, about the successor. The access rights can be manually adjusted by a user with full control.
  - If the user's membership in one of his or her non-main organizations is terminated, only Teamrooms that are restricted to the affected organization are handled.

4.7 Manage Teams

Teams are used for the informal structuring of organization members, external members and members of other organizations. For example, they can be used in Teamrooms to authorize the entire team.

To create a team, perform the following steps:

1. In the dashboard of the organization click *Membership* and then click *Teams*.
2. Click the "Create Team" action.
3. Define a name. In the *Define Team Members* field, you can add users to the team.
4. Click "Create".

Note:

- There are predefined teams per license type that are updated automatically. These can be used in app configurations, for example, as the app roles often correspond to the license types.
- For teams you can define standard Teamrooms (see chapter 8 "Standard Teamrooms").
- Organization administrators can define members who are entitled to manage all teams (organization dashboard > "Advanced Settings" > "Define Policies" > "Actions" tab > *Manage Teams*).
- Organization administrators can define team administrators for individual teams (via the "Define Administrators" action in the respective team). The corresponding teams are placed on "Home" of the team administrators. Team administrators can perform the following actions:
  - add, invite and remove members
  - edit properties of the team
- For teams, the "Notification Settings" tab can be used to define the workflow event settings. The notifications will be sent to the first e-mail address specified in the *E-Mail Addresses* field on the "Address" tab. Thus, not all members of the team are notified anymore, but only the defined e-mail address.

4.8 Define Authentication and Two-Factor Authentication

The log-in can be carried out with username and password or client certificates.

For the two-factor authentication mobile PIN (SMS), e-mail PIN and one-time password via a RADIUS server are provided. Mobile PIN has to be purchased separately.

To change the settings for a user, perform the following steps:

1. Navigate in the desired member and click the "Properties" action.

2. On the "Account" tab, you can define the settings regarding the authentication and second factor.

   o *Primary E-Mail Address*
   The user can log in with this e-mail address. Notifications are also sent to this e-mail address.

   o *Alternate E-Mail Address for Authentication*
   The user can use this e-mail address to log in via username/password, Active Directory or SAML 2.0 (a login server has to be configured in the organization). The e-mail address is only required if it is not the same as the primary e-mail address. Thus, for example, the primary e-mail address can be used for receiving notifications and the alternate e-mail address can be used for the login server.

   o *Common Name (CN)*
   Defines the common name of the corresponding user certificate (certificate authorities have to be defined in the organization).

   o *Mode of Dispatch for Mobile PIN*
   Defines the primary second factor. Depending on the selected factor a phone number, a RADIUS user identification or an e-mail address has to be provided in the following fields. If several fields are filled, the user can select an alternative method when logging in.

   o *Mobile Phone Number for Mobile PIN*
   The PIN is sent to this phone number.

   o *E-Mail Address for Mobile PIN*
   The PIN is sent to this e-mail address.

   o *User ID Used for RADIUS Server*
   Defines the link between the user and the RADIUS server (a RADIUS server has to be configured in the organization).

   o *Deactivated Authentication Methods*
   To prevent the user from logging in using certain authentication methods, the not allowed authentication methods can be defined here. Before disabling authentication methods, make sure you do not lock out the user.

   o *Login Options Acquired From*
   Shows the login options that apply to the user (Active Directory/SAML 2.0, certificate, RADIUS; if available). Login options are determined for external members based on the following evaluation hierarchy (if no settings are available, the next level is considered): primary external organization, "All external members of <cloud organization>" and cloud organization.

3. Click "Next" to save the changes.

Note:

- Only administrators and owners of the primary organization of the user can change the user data. You find the primary organization in the properties of the user on the "User" tab in the *Organization* field.

- The settings can also be defined via the CSV import.

4.9 Show Account Activities of Members

To view the account activities of members, perform the following steps:

1. Navigate to the desired organization, team, external organization or (external) member.
2. Run the "Show Account Activities" or "Advanced" > "Show Account Activities" context menu command.
3. The account activities of the member are displayed and can be downloaded via the "Export Account Activities as CSV File" button.
4. Click "Close".

Note:

- Only members who are managed by you are displayed.
- If a member has never logged in, the columns in the CSV file are filled with "N/A".

4.10 Manage External Members

Employees of suppliers, partner companies or customers can be added as external members to your organization. To simplify the cross-organizational cooperation even further, external organizations are available to combine and manage external members based on their company affiliation.

To manage external members, perform the following steps:

1. In the dashboard of the organization click *Membership*, to open the membership administration.
2. Within *External Members* you can import, add, invite or exclude external members.
3. Within *External Organizations* you can create external organizations to be able to structure external members logically.

Note:

- When importing external members (available CSV columns see chapter 4.1 "Import Members"), the following two additional CSV columns are available in comparison to importing members: `ExtOrganizationKey` (import ID of an external organization) and `ExtOrganizationName` (name of the external organization). In addition, only the organization policies `grpolicyopenonlineex` and `grpolicyreadonworkspace` apply to external members. `AdminTeamKey` is also not available for external members.
- External members consume licenses as members.
- Editions and apps can be assigned to external members as to members.
- External members cannot create Teamrooms that are assigned to the organization.
- Only administrators and owners of the primary organization of the user can change the user data. You find the primary organization in the properties of the user on the "User" tab in the *Organization* field.
- The by default created external organization "All external members" always includes all external members, regardless of whether the members are also assigned to other external organizations.
- Organization administrators can define the primary external organization for an external member ("Organization Membership" tab, *Primary External Organization* field) if the user is a

member of multiple external organizations. If the user is not a member of any external organization, the field is not displayed. When the user is initially added to an external organization, the field is filled automatically.

The settings regarding login options are determined for the external member based on the following evaluation hierarchy (if no settings are available, the next level is considered): primary external organization, "All external members of <cloud organization>" and cloud organization. The administrators of the primary external organization are also authorized to terminate the user's external membership.

- Organization administrators can define members who are entitled to manage all external organizations (Organization dashboard > "Advanced Settings" > "Define Policies" > "Actions" tab > *Manage External Organizations*).

- Organization administrators can define members or external members as administrators for individual external organizations (via the "Define Administrators" action in the respective external organization). The corresponding external organizations are placed on "Home" of the administrators. Administrators can perform the following actions: add, invite and remove external members, terminate external memberships (only if the external organization is the primary external organization of the external member), define certificate and RADIUS settings, edit properties of the external organization.

- For external organizations, on the "Advanced Settings" tab, trusted networks can be specified. For more information, see chapter 9.7 "Define Trusted Networks".

- For external organizations, the "Notification Settings" tab can be used to define the workflow event settings. The notifications will be sent to the first e-mail address specified in the *E-Mail Addresses* field on the "Address" tab. Thus, not all members of the external organization are notified anymore, but only the defined e-mail address.

4.11 Manage the Organizational Structure

The organizational structure is used for the hierarchical mapping of organizational units and positions of your organization. You can find the organizational structure in your organization under "Membership" > "Organizational Structure".

- Organizational Unit
  An organizational unit summarizes one or more positions and can contain subordinate organizational units. The hierarchy of organizational units is defined on the one hand by the tree structure of the organizational structure and on the other hand by the assigned hierarchy levels (e.g. business unit, division, team).

- Position
  Positions are assigned to organizational units and are used to define the jobs in your organization. A concrete user can be assigned to a position.
  There are two types of positions: "Head" and "Staff Member". This information can be used in the workflow for approvals (for example, the leave request for an employee is assigned to the head of the respective organizational unit).

Organizational administrators or users who are entitled via the "Manage Organizational Structure" policy are responsible for maintaining the organizational units and positions (for example, assigning a user to a position).

When you delete organizational units or positions, they are first placed in the wastebasket. There they can be permanently deleted or restored.

4.11.1 Define Hierarchy Levels

If you are in the organizational structure, you can use the "Settings" action to set the hierarchy levels. By default, the following hierarchy levels are predefined:

- Management Board (Level 01)
- Business Unit (Level 02)
- Division (Level 03)
- Team (Level 04)

You can use the "Properties" context menu command to adjust the name and level. You can obtain new hierarchy levels via the "New" background context menu command.

Note: Organizational units can only contain organizational units with a larger level value (for example, organizational units of level 02 can only contain organizational units from level 03).

4.11.2 Create Organizational Units

If you are in the organizational structure, you can create organizational units using the "Create Organizational Unit" action. Navigate in organizational units that have already been created to create subordinate organizational units.

You can set the following values:

- *Name*
  Defines the name of the organizational unit.
- *Staff Unit*
  If an organizational unit is not part of the linear hierarchy, it can be marked as a staff unit.
- *Hierarchy Level*
  Defines the hierarchy level of the organizational unit. Only levels with a higher value than the level defined in the superordinate organizational unit are displayed.
  Note: You can define the available levels in the settings of the organizational structure.
- *Description*
  Defines the description of the organizational unit.
- *Import ID*
  If the organizational structure is externally managed and imported, an import identifier for the organizational unit can be defined. This allows an update of the organizational unit.
- *Members with Role "Head"*
  Defines the heads of the organizational unit.
- *Members with Role "Staff Member"*
  Defines the staff members of the organizational unit.

Note:

- You can use the "Move Organizational Unit" context menu command to move the organizational unit within the organizational structure.
- To convert teams to organizational units, you can use the "Move to Organizational Structure" context menu command.
- For organizational units, the "Notification Settings" tab can be used to define the workflow event settings. The notifications will be sent to the first e-mail address specified in the *E-Mail*

Addresses field on the "Address" tab. Thus, not all members of the organizational unit are notified anymore, but only the defined e-mail address.

4.11.3 Create Positions

If you are in the organizational structure, in an organizational unit, you can use the "Create Position" action to create a position for the respective organizational unit.

You can set the following values:

- *Type*
  Defines whether it is a staff member or a head position.
- *Staff Unit*
  If a position is not part of the linear hierarchy, it can be marked as a staff unit.
- *Organizational Unit*
  The position is assigned to the shown organizational unit.
- *User*
  Defines the employee who is assigned to the position.
- *Primary Position*
  If an employee is assigned to several positions, one position can be marked as primary. The primary position is used for evaluating the supervisor (e.g. in a workflow context).
- *Name*
  Defines the name of the position.

Note:

- You can use the "Move Position" context menu command to move the position within the organizational structure.
- Additional fields are available when using the Fabasoft Personnel File.

4.11.4 Import the Organizational Structure

If you are in the organizational structure, you can use the "Import Organizational Structure" action to import or update the organizational structure using a CSV file. The "Download CSV Template" button can be used to retrieve a template that describes the necessary data structure.

- The *Complete Organizational Structure Matching* option allows you to define whether existing positions and organizational units that do not exist in the CSV file should be deleted.
- The *Only Update Organizational Structure* option (only visible if *Complete Organizational Structure Matching* is disabled) allows you to define whether only existing positions and organizational units are updated. New organizational elements will not be created.

Alternatively, the import can also be carried out via an inbox ("Import Data" action, "Import Organizational Structure" import definition). For a complete structure matching, you must specify a user who will be informed via workflow, if there are organizational elements to be deleted. Deletion only takes place after manual confirmation.

The CSV columns are in general free-text fields of type string. The import ID can be used to update objects. Following CSV columns are available:

CSV Column	Field	Possible Value

Key	Import ID	string
Type	-	string (`OrganizationalUnit`, `OrganizationalPosition`)
ParentKey	-	string (import ID of the superordinate organizational unit; empty on top level)
Name	Name	string
Level	Hierarchy Level	string (import ID of the hierarchy level; only organizational units)
StaffUnit	Staff Unit	string (`TRUE`, `FALSE`; only organizational units)
UnitDescription	Description	string (only organizational units)
PositionType	Type	string (`HeadPos`, `StaffPos`; only positions)
PrimaryPosition	Primary Position	string (`TRUE`, `FALSE`)
User	User	string (import ID or if not defined the e-mail-address of the internal member; only positions)

Note:

- If you change the entry for `ParentKey` or `Level` of an existing organizational element, the organizational element is moved accordingly.
- If the Fabasoft Personnel File is licensed, additional metadata can be imported.

5 License Management

To use the Fabasoft Private Cloud licenses are required. The basis is an edition (e.g. Fabasoft Cloud Superior), which contains depending on the edition corresponding apps. Additionally, special apps (e.g. Scrum Projects) can be purchased and also free apps are available.

Editions and apps can be purchased in the desired number and assigned to members or external members of your organization. The assignment can be carried out automatically, manually or for special apps per configuration.

5.1 Editions and Apps

In the organization's dashboard, click *Licenses* to open the license management. The editions and apps available in your organization are displayed as a list:

- Fabasoft Cloud Professional/Enterprise/Superior (Full Access)
  Allows full access (can be used for members and external members).
  Note: Integrated commenting is not included in Fabasoft Cloud Professional.
- Fabasoft Cloud Professional/Enterprise/Superior (Read Access)
  Allows read access (can be used for members and external members).
- Fabasoft Cloud Enterprise/Superior (Read Access + Comments)
  Allows read access and integrated commenting (can be used for members).
- Fabasoft Cloud Professional/Enterprise/Superior (Access for External Members)
  Allows full access (can be used for external members).
  Note: External members cannot create Teamrooms assigned to the organization, regardless of the license.
- Additional Apps

The *Assignment* column displays the type of assignment:

- "Manually (Default Edition for Members)" and "Manually (Default App)"
  Default editions or apps are automatically assigned to new members. Organizational administrators can also subsequently assign or change the editions or apps.
- Manual
  Manual assigned editions or apps must be explicitly assigned to a member by an organization administrator.
- Configured
  These apps offer various configuration options and roles and are therefore managed using a separate configuration. You cannot change the assignment type.
- Volume-Based
  To use these apps, a volume-based license is required and must be purchased separately.
- Free
  Free apps provide following assignment types:
  - Free (Disabled)
    The app is not available to anyone.
  - Free (Default App)
    The app is automatically assigned to new members.
  - Free (Manually)
    The app must be explicitly assigned by an organization administrator.

You can change the type of assignment using the "Use as Default for Members", "Enable" and "Disable" context menu commands.

Navigate in the edition or app to view the list of licensed members. You can use the "Add Members" action to specify the members who are to have a license. You can use the "Remove License" context menu command to revoke the license.

5.2 Assign Editions and Apps

You can assign editions or apps with manual assignment to individual members.

1. In the dashboard of the organization, click *Members* to open the membership administration.
2. Navigate to the desired member.
3. In the context menu of the member, click "Assign Editions and Apps".

- o *Edition*

  Select the edition that you want to assign to the user.
- o *Manually Assignable Apps*

  Select the apps that you want to assign to the user.

4. Click "Assign".

Note: Select multiple members to make the assignment together.

6 Reports

The following reports are available.

Consistency Check for Documents

The consistency check for documents (virus, hash value and completeness) is performed periodically in order to find improper changes to documents.
By Clicking on "View" the last report is opened. Older reports are available in the *Archive*. The "Open Log File" action allows viewing the log. If inconsistencies occurred, you will find the list of problems in the properties of the report on the "Inconsistencies" tab.

Failed Background Tasks

Background tasks are used to execute actions at a specific point in time. If a background task could not be executed successfully (for example, if the object concerned is locked), the system tries to execute the background task again later. After ten unsuccessful attempts, the background task is suspended and no longer executed automatically. App administrators are informed by e-mail about suspended background tasks in the context of an app. Otherwise, the organization administrators are informed by e-mail.

You can perform the following manual actions for background tasks:

- Define Next Execution (only visible if you have full control on the object)
  Defines a time at which the background task is executed again.
- Send Link
  The background task can be forwarded to a user with appropriate access rights.
- Delete (only visible if you have full control on the object)
  Deletes the background task on the affected object. The task is no longer executed.

Note: The "Failed Background Tasks" widget is only visible, if at least one failed background task is available.

Reports on Unused Teamrooms

The "Create Report" button can be used to identify unused Teamrooms. Teamrooms are considered unused if they were created and last changed before the specified period of time and no access has taken place since that time. The accesses are determined on the basis of the audit log.

With the "Request Teamroom Administrators to Review" action, Teamroom administrators can be requested by e-mail to review the unused Teamrooms and delete old, no longer needed data, if applicable.

Teamroom administrators have the following options via the link in the e-mail:

- "Reviewed" or "All Teamrooms Reviewed" button respectively
  Teamrooms can be marked as "Reviewed". You can specify a date until which the Teamrooms are to be excluded from the reports (one year by default). If the date is removed, the Teamroom will be checked again for the next report.
- "Dissolve" button
  Teamrooms that are no longer needed can be dissolved directly.

7 Advanced Settings

To access the advanced settings, click on *Advanced Settings* in the dashboard of the organization.

7.1 Dashboard

Depending on your edition and licensed apps following areas are available.

Overview

Shows the key information of the organization. By clicking "View" you can navigate to the properties of the organization.

- *Name of the Fabasoft Private Cloud*
  To personalize your installation, you can enter your own name for your private cloud. The name is used in several product strings.
- *E-Mail Address (No Reply)*
  This e-mail address is used for automatic e-mails, such as for sending new events.
- *E-Mail Address (Sender)*
  This e-mail address is used for automatic e-mails that are sent in conjunction with a user account (e.g. Teamroom invitations).

App Configurations

If apps that are based on app configurations are licensed, the corresponding app configurations are displayed here. Navigate in the app configurations widget to create additional app configurations.

Target Domains for "Teamroom Transfer"

Shows domains that can be used as target for transferring or publishing Teamrooms. Navigate in the target domains widget to create additional domains.

OAuth Clients

OAuth clients are needed, for example, for the transfer Teamroom functionality. If you activate a target domain for transferring Teamrooms, an OAuth client is created automatically in the target domain. Navigate in the OAuth client widget, to create OAuth clients manually.

For OAuth clients defined in the organization, you can specify whether the use must be confirmed.

Mindbreeze InSpire Services

Mindbreeze InSpire Services can be used to classify documents automatically. Navigate in the *Mindbreeze InSpire Services* to create additional services. If only one service is available, it is

automatically the default service. If multiple services are available, a service can be set as default service by using the "Set as Default" context menu command. The default service is used if no service has been explicitly defined in the respective context (the fallback does not apply to an app room context).

You can define the following settings:

- *Name*
  The name of the service.

- *Filter Service URL*
  The URL to the Mindbreeze InSpire filter service (e.g.
  `https://mbinspire.example.com:8443/filter/23401`).

- *Tenant*
  The Mindbreeze InSpire prediction service is multi-tenant capable. If a tenant is defined, it will be used in Mindbreeze InSpire.
  Note: In the Mindbreeze Management Center, the *Tenant ID Pattern* property must have the following value: `{{_FSCMINDBREEZE_1_1001_fscmbtenant}}`

- *Project*
  Within a tenant several projects can be managed. If a project is defined, it will be used in Mindbreeze InSpire.
  Note: In the Mindbreeze Management Center, the *Project ID Pattern* property must have the following value: `{{_FSCMINDBREEZE_1_1001_fscmbproject}}`

- *Scope*
  Within a project several scopes can be managed. If a scope is defined, the corresponding model will be used in Mindbreeze InSpire. Otherwise, the default model is used.
  Note: In the Mindbreeze Management Center, the *Scope ID Pattern* property must have the following value: `{{_FSCMINDBREEZE_1_1001_fscmbscope}}`

- *Authentication*
  Defines the authentication type for the filter service.

- *Root and Intermediate Certificate Authorities*
  Defines the root and intermediate certificate authorities for the validation of the SSL server certificates of the filter service.

- *Send Feedback to Mindbreeze InSpire Service*
  Defines whether feedback about the correctness of the classification will be sent to the Mindbreeze InSpire service. This can improve the future classification.

- *Own Mindbreeze InSpire Service for Feedbacks*
  Defines whether the feedback will be sent to a dedicated Mindbreeze InSpire service. If enabled, the data (*Filter Service URL*, *Tenant*, *Project*, *Scope*, *Authentication*) can be specified for the dedicated Mindbreeze InSpire Service.

- *Own Mindbreeze InSpire Service for Training Data*
  Defines whether the training data will be sent to a dedicated Mindbreeze InSpire service. If enabled, the data (*Filter Service URL*, *Tenant*, *Project*, *Scope*, *Authentication*) can be specified for the dedicated Mindbreeze InSpire Service.

- *Software Component Prefixes for the Mapping of Fabasoft Cloud Keys*
  If no full reference is specified in the *Key Mapping* field, the system attempts to determine the property using the software components specified here (e.g. `COOTC@1.1001`).

- *Key Mapping*
  If the keys defined in Mindbreeze InSpire do not correspond to the keys in the Fabasoft Cloud,

a mapping can be defined. As key in the Fabasoft Cloud the reference of the respective property is used (e.g. `COOTC_1_1001_objcategory` for the *Category* property). In the case of user-defined forms the programming name of the property is used as key.
When using short references (e.g. `objcategory`), the corresponding software component must be specified in the *Software Component Prefixes for the Mapping of Fabasoft Cloud Keys* field.

If necessary, contact Mindbreeze InSpire Support to make the specific settings.

Holiday Tables

Holiday tables allow the definition of holidays and time intervals. Holidays are used, for example, in the workflow and time intervals are considered for follow-ups.

By default, holiday tables are available for Austria, Germany and Switzerland. If no specific holiday table is selected in the *Holiday Table* field of app configurations, app rooms or Teamrooms, the default holiday table is used ("Set as Default" context menu command).

A new holiday table can be created using the "Create Holiday Table" action. If applicable, an existing holiday table can also be duplicated.

Holidays can be created using the "Create Holiday" or "Import Holidays" action. When importing, a sample CSV file can be downloaded via the "Download CSV Template" button. Alternatively, the holiday tables provided by the product can also be downloaded as CSV files (properties > *Holidays (CSV File)* field).

Time intervals can be created in the properties of the holiday table in the *Time Intervals* field.

7.2 Define Contact Data

To define the contact data, perform the following steps:

1. In the dashboard of the organization click *Advanced Settings.*
2. Click the "Define Contact Data" action.
3. Enter the desired data.
4. Click "Save".

7.3 Define Logo

You can define a logo, a preview logo, a background image and a header background color for your organization. The logo will be displayed, for example, left above the actions. The preview logo is used when the organization is displayed for instance in a list. The background image is displayed directly on "Home".

To define the logos, perform the following steps:

1. In the dashboard of the organization click *Advanced Settings.*
2. Click the "Define Logo" action.
3. Upload the logos or select already existing logos. If a logo exceeds the maximum display size, it will be automatically displayed smaller.
   Note: The *Logo* is also displayed in the header if no own *Header Logo* has been defined.
4. Upload a background image for the home area.
5. If applicable, specify the background color for the header (as hexadecimal value, e.g.: #FF0000). The colors of the elements of the header are automatically adapted to the background color.

Note: If you select a background color, the background color and the logo are also considered for the login pages. If you select no background color, the top bar is displayed grey because the most logos are designed for a light background.

6. If you enable *Use Logo and Background Color in E-Mails* option, the logo or header logo and the background color are also included in your organization's e-mails sent via the Cloud.

7. If you enable the *Use Logo und Background Color in Support Dialog* option, the logo or header logo and the background color is used in the support dialog for internal support requests.

8. Click "Save".

7.4 Define Policies

You can centrally define policies and default settings for the members of your organization. This is an efficient way to ensure a consistent user experience.

To define the policies, perform the following steps:

1. In the dashboard of the organization, click *Advanced Settings.*

2. Click the "Define Policies" action.

3. Switch to the desired tab and define the policies. Further information can be found in the next chapters.

4. Click "Save".

7.4.1 "Actions" tab

Define which organization members are authorized to execute the following actions:

- *Create Teamrooms*
  Defines the members who are allowed to create Teamrooms.

- *Manage Home*
  Defines the members who are allowed to manage their "Home". Members who are allowed to manage the home area can place or remove objects on their home.

- *Transfer Teamrooms* (Enterprise and higher)
  Defines the members who are allowed to transfer or publish Teamrooms.

- *Edit Forms and Categories*
  Defines the members who are allowed to create, edit and release forms and categories.

- *Edit BPMN Process Diagrams*
  Defines the members who are allowed to create, edit and release BPMN process diagrams.

- *Manage Inbox Rules*
  Defines the members who are allowed to create and edit rules for inboxes.

- *Use Search Folders for Audit Logs* (Enterprise and higher)
  Defines the members who are allowed to see audit logs.

- *Synchronization Mode*
  Defines how the Cloud folder can be used by members to synchronize with the file system ("No Synchronization", "Synchronized Folder", "Synchronized Desktop or Synchronized Folder").
  No synchronization: You can prevent the members can synchronize their data with the file system.
  Synchronized desktop: The members can synchronize their whole "Home".
  Synchronized folder: The data in the synchronized folder of the members is synchronized.

Note:

- These actions are generally not available for external members.
- In the properties of the organization member, you will find the restrictions that apply to this member on the "Policies" tab. If "Executable by all members except" or "Executable by no one except" are defined in the organization, you can also change the settings for the user on this tab. If a policy is defined via a team, the settings cannot be changed at the user.

7.4.2 "Membership Administration" tab

Define settings regarding the membership administration.

- *Add Members to the Organization*
  Defines the members who are allowed to add new members to the organization. Only members whose email address matches one of the organization's email domains can be added.

- *Add External Members to the Organization*
  Defines the members who are allowed to add new external members to the organization.

- *Remove Members from the Organization*
  Defines the members who are allowed to terminate memberships of members.

- *Remove External Members from the Organization*
  Defines the members who are allowed to terminate memberships of external members.

- *Manage Organizational Structure*
  Defines the members who are allowed to manage the organizational structure.

- *Manage External Organizations*
  Defines the members who are allowed to manage external organizations.

- *Manage Teams*
  Defines the members who are allowed to manage teams.

7.4.3 "Content" tab

Define settings regarding the allowed contents.

- *Blocked File Extensions*
  Define a not allowed file extension per line. File with these file extensions cannot be uploaded.

- *Check Blocked File Extensions in ZIP Archives*
  Defines whether file extensions are also checked in ZIP archives.

- *Maximum File Size (in MB)*
  Files can only be uploaded if the file size does not exceed the specified value.

- *Maximum Number of Versions Kept*
  When objects are changed a version is created. Here you can define how many versions are kept at maximum.

- *Signatures With Additional Password Verification (Compliant to FDA 21 CFR Part 11)*
  Allows an additional password prompt when applying a signature that is defined in this policy.

- *Open or Download Content on the Device*
  Can be used to determine for whom the open and download actions are available in the web browser client. In addition, Teamrooms and the assigned objects cannot be duplicated.

For example, you can specify that nobody other than your organization members can use these actions.

- *Open Content via a Network Drive (WebDAV)*
  Defines who is allowed to access your organization's content via a network drive (WebDAV). If access is not allowed, the common WebDAV clients are blocked.

- *Block Downloading of Content via Public Links*
  If enabled, the "Download" button is not displayed for public links throughout the organization. Otherwise, it can be defined for the Teamroom or public link whether the "Download" button is displayed.

- *Allow Push Notifications for Events*
  Defines whether push notifications are sent for events. If the affected object is assigned to another organization, *Allow Push Notifications for Events* must also be enabled in this organization for the push notification to be sent.

- *Allowed Members in Teamrooms*
  By default, users, teams and organizations can be authorized in Teamrooms. You can restrict the allowed members teams and organizations.

7.4.4 "Teamroom" tab

Define the default settings for new Teamrooms of the organization.

- *Access Protection*
  Defines whether only the specified team is allowed to access the Teamroom or whether everyone can read the Teamroom but not search for it.

- *Restrict Shortcuts Within Teamroom*
  Defines which type of shortcuts may be stored in the Teamroom. You can restrict the permitted shortcuts to objects that are assigned to the organization or to objects that are assigned to the Teamroom. In this way, you can prevent, for example, that shortcuts are stored to which the members of the Teamroom do not have access.

- *Restrict the Downloading or Opening of Content on the Device*
  Allows team members to restrict who can open or download content at the device.

- *Roles That Are Allowed to Open or Download Content on the Device*
  Defines which permissions a team member must have in order to open or download content at the device.

- *With Read Access Visible to All Members*
  Defines whether all team members of the team are allowed to see the members with read access. If the setting is disabled, the team members with read access are only visible for members with "Full Control". Note that disabling this setting also restricts other use cases:

  - Only team members with "Full Control" have access to the "Team" action and can start processes.

  - Events can generally be deactivated for team members who are not allowed to see the team. Otherwise, only events will be displayed that do not allow conclusions to be drawn about team members with read access.

  - Team members with read access cannot use annotations, signatures, processes or comment on news feeds.

  - Team members with read access cannot be selected as participants in processes.

  - Team members with read access cannot create public links.

- *Display Notifications for Users Without Rights to View the Team*
  Defines whether events for team members who are not allowed to see the team are generally disabled. Otherwise, only events are displayed that do not allow any conclusions to be drawn about team members with read access.
- *All Team Members May Add Members*
  Defines whether all team members can add users to the team or only team members with "Full Control". Members with change access may grant or revoke change access or read access to other members. Members with read access may grant or revoke read access to other members.
- *Restrict Team Members*
  Defines the organizations, organizational units, teams and external organizations whose members may be added to the Teamroom. If the list does not contain any entries, members can be added without restriction.

7.4.5 "Processes" tab

Define settings regarding processes.

- *Process Administrators*
  A process administrator can monitor and control all processes in the organization.
- *Show Process Statistics for*
  Defines for whom process statistics are displayed. A process administrator can view the statistics for all processes in the organization. A process owner can view the statistics for the processes for which he is responsible.
- *Process Statistics Calculation Interval*
  Defines the interval for calculating the process statistics.
- *Schedule Process Statistics Calculation*
  Defines when the next calculation of process statistics will take place.

7.4.6 "Authentication" tab

Define settings regarding the authentication.

- *Settings for Login Session*
  Defines the settings for the login sessions.
  - *Validity Period*
    Defines the maximum validity period of a login session. You can choose a value between 2 hours and 3 days. The default value is currently 16 hours.
  - *Validity Period in Case of Inactivity*
    Defines the maximum validity period of a login session when the user is inactive. You can choose a value between 15 minutes and 4 hours. The default value is currently 2 hours.
  - *Value for SameSite Attribute of Session Cookie*
    Defines the value of the SameSite attribute of the web browser cookie used for the login session. You can use the "Strict" or "Lax" value to reduce the risk of cross-site request forgery (CSRF). However, these values limit usability and may require users to log in more frequently. The default value is "Lax".
    Note: The integration for Microsoft Teams and the task pane integration for Microsoft Office for the Web can only be used with the "None" value.

- *Trusted Networks*
  Defines IPv4 addresses or address ranges (in CIDR notation, e.g. 198.51.100.0/24) of your trusted networks with which users communicate with the Internet. This allows, for example, extending the logon session binding from one IPv4 address to IPv4 ranges.

- *Authentication Methods That Do Not Require Two-Factor Authentication*
  You can define that single sign-on and certificate authentication methods do not require a second factor. If you disable the second factor, your IT department must take appropriate measures to ensure that the authentication level is still maintained.

- *Permanent Login*
  Defines the users who can use the permanent login.

- *Period of Validity for Permanent Login*
  Defines the maximum time until a new explicit login is required.

- *Permitted Operating Systems for a Permanent Login*
  Defines the operating systems on which permanent login is possible.

- *Certificate Authorities for Computer Certificates for Microsoft Windows, Apple macOS and Ubuntu*
  On devices with Microsoft Windows, Apple macOS or Ubuntu, for security reasons, a permanent login is only possible if the devices can be identified by a computer certificate. This is to prevent users from permanently logging in on devices that are not under your organization's control (such as private or public devices). Specify all certification authorities that issue computer certificates to your organization by uploading the certificates from these certification authorities as a CER file in PEM format.
  If a user wants to perform a permanent login on a device, the system checks whether a computer certificate issued by one of the configured certification authorities can be found on the device. The following certificates are used:
  - Microsoft Windows
    "Local Computer" > "Personal" > "Certificates"
    CN of the certificate: local host name and domain name

  - Apple macOS
    Default keychain
    CN of the certificate: local host name and domain name

  - Ubuntu
    Network authentication certificate (802.1x)
    CN of the certificate: local host name

7.4.7 Default Settings

On the "Basic Settings", "Accessibility", "Notifications", "Workflow" and "Home" tabs, you can define default settings for your members. Additionally, you can define whether the settings are changeable by the members. Via the "Reset to Default Settings" button, you can restore the settings predefined by Fabasoft. You can also define the settings individually in the properties of the members.

Note:

- If the organization from which a user is managed changes, the default settings of the new organization are applied to the user.

- Changes to the default settings only affect new and not existing members.
  The "Apply Organizational Settings" context menu command is available for users, teams,

organizational units, external organizations and organizations in order to take over changed default settings.

7.4.7.1 "Basic Settings" tab

Define the basic settings for your members. Users can find the settings here: "account menu (user name)" > "Basic Settings" > "General" tab.

In the *Allow Users to Change Data Location* field, you can also specify whether users should be able to change the data location. If not, users may only be able to change to the standard data location via the data location menu.

7.4.7.2 "Accessibility" tab

Define the accessibility settings for your members. Users can find the settings here: "account menu (user name)" > "Basic Settings" > "Accessibility" tab.

7.4.7.3 "Notifications" tab

Define the notification settings for your members. Users can find the settings here: "account menu (user name)" > "Advanced Settings" > "Notifications" > "Settings" button > "Settings" tab.

7.4.7.4 "Workflow" tab

Define the workflow settings for your members. Users can find the settings here: "account menu (user name)" > "Advanced Settings" > "Workflow" > "Personal Settings" tab.

7.4.7.5 "Home" tab

Define which items on "Home" should be available to members of the organization.

- *Available Elements on Home*
  Defines which elements are available on Home. Additionally, the size and order of the elements can be defined.
- *Start With*
  Defines an element available on Home that is initially displayed after login.
- *More Elements on Home*
  Defines additional elements that should be available on Home.
- *Show Organization Management for Administrators on Home*
  Define whether the organization management should be shown to administrators of the cloud organization on Home. If you disable this option, administrators can manage only selected settings using the "Settings" action of an app's personal dashboard.

You can define whether members are allowed to manage their home area themselves via the "Manage Home" policy (see chapter 7.4.1 "'Actions' tab').

7.4.8 "Fabasoft Cloud Client" tab

Define the Fabasoft Cloud Client settings.

- *Fabasoft Cloud Client Link in the Software Center*
  Allows organization members to install the Fabasoft Cloud Client via the web client from your

Microsoft Software Center. You can find the corresponding link by navigating to the Fabasoft Cloud Client in the software center and clicking on the "Share" button at the top right.
Note: The link to the Fabasoft Cloud Client in the software center must be updated after each update.

- *Provide Versions From the Software Center Only*
  If the software center is not available on the workstation, the Fabasoft Cloud Client can alternatively be obtained from the cloud installation. To prevent this, the option can be enabled.

7.5 Login Options: Active Directory / SAML 2.0

To enable members or external members of your organization to log in via Active Directory or SAML 2.0, you must configure the appropriate login servers.

Configuration of the Login Server

Follow the steps described in the white paper "Configuration of Single Sign-On":

https://help.cloud.fabasoft.com/index.php?topic=doc/Configuration-of-Single-Sign-On/index.htm

Configuration in the Cloud Organization

To perform the configuration in the cloud organization, proceed as follows:

1. Navigate to the advanced settings of your cloud organization.

2. Click the "Login Options" > "Active Directory / SAML 2.0" action.

3. Select the login method (Active Directory or SAML 2.0) and upload the metadata XML file of your login server.
    Note: If a login server is already configured, click "Add" first.

4. In addition, you can specify whether two-factor authentication is required for the login method and whether users should be automatically created the first time they log in.
    Note: Automatic creation is only possible if the users use the URL for automatic login displayed on the next page.

5. Click "Next".

6. Enter a short name for the login server.

7. Specify the e-mail domains to be associated with this login server.

8. You can make the displayed URL available to your users so that they can log in directly using the login server.

9. Define whether the URL for direct login via the login server should also be used for sent links.

10. Click "Next".

Note:

- Repeat the steps to add additional login servers.

- Existing login servers can also be edited or removed.

- Organization administrators will receive a notification in the welcome screen and by e-mail when the metadata certificate expires within the next two weeks or has expired.

- When a user is automatically created, the user becomes a member if the e-mail domain matches an e-mail domain of the organization. Otherwise, the user becomes an external member.

7.6 Login Options: Certificate

In order that members of your organization can log in via a client certificate, all certificate authorities that are allowed to issue client certificates for your organization, have to be stored in the corresponding field as CER files in PEM format.

Additionally, you have to store the superordinate root and intermediate certificate authorities for the issuing certificate authorities in the corresponding field as CER files in PEM format. Provide for each root, intermediate and issuing certificate authority the corresponding certificate revocation list URLs. You can define whether a two-factor authentication is necessary when using the certificate log-in.

The CN of the certificates and the DN of the issuer must not contain special characters.

To complete the certificate configuration for your organization, you have to add the common name of the corresponding client certificates to the members (see chapter 4.8 "Define Authentication and Two-Factor Authentication").

Note: You can also define certificate settings for external organizations. This way you can provide a client certificate log-in for your external members, too.

7.7 Login Options: RADIUS

In order that your organization members can use a one-time password via a RADIUS server, the settings of the RADIUS server must be defined in your organization. In addition, you have to define the respective *User ID Used for RADIUS Server* for your organization members.

Organization settings

Enter the computer name and the shared secret of the RADIUS server. The connection can be established either via UDP (port 1812) or RadSec (port 2083).

RADIUS server settings

- The IP addresses of the two Fabasoft Private Cloud Nodes must be enabled for communication with the RADIUS server and must be defined in the RADIUS configuration.
- Your RADIUS server has to be accessible via one of the following ports.
  - TCP/2083 (RadSec)
  - UDP/1812

Note: You can also define RADIUS settings for external organizations. This way you can provide a RADIUS log-in for your external members, too.

7.8 Define SMTP Settings

You can define your own SMTP server for e-mails sent via the Fabasoft Cloud. Make sure that the defined SMTP server is officially authorized to send e-mails for the domains of the specified sender e-mail addresses (Sender Policy Framework).

7.9 Define Organization Roles

Via organization roles you can define users who are responsible for managing the organization. For further information about the roles, see chapter 3 "Organization Roles".

7.10 Configure Encryption

In order to be able to encrypt Teamrooms using Fabasoft Secomo, a key server that should be used for encryption has to be defined. Keys created as part of the encryption process will be managed by that key server.

As part of the initial configuration, keys are generated by the key server for your organization. After completion, the encryption functionality will be enabled.

7.11 Configure Digital Signatures

To enable the digital signing of documents with own certificates, you must store the corresponding certificates in your organization ("Advanced Settings" > "Configure Digital Signatures" action). In addition, you can specify which organization members are allowed to sign digitally with the certificates.

In addition to certificates, you can also define stamps. To do this, click the "Add Stamp" button in the *Stamps* field. Assign a name, define the organization members who are allowed to use the stamp and upload an image as stamp.

Note:

- If the use of X.509 certificates is restricted, one of the following usage types ("Key Usage") is required: "Digital Signature" or "Non Repudiation".
- Certificates can be updated using the "Update" context menu command. Organization administrators and owners receive a notification on the welcome screen when the certificate expires within the next two weeks or has expired.
- Certificates can be deleted using the "Delete" context menu command. Deleted certificates can no longer be used for signing, but already signed documents are not affected.

8 Standard Teamrooms

As organization administrator, you can add standard Teamrooms to teams, external organizations, organizational units and to the organization in the organization folder. The standard Teamrooms are displayed in the organization folders of the members who are authorized in the Teamrooms.

To create a standard Teamroom, navigate in the dashboard of the organization in the *Organization Folder* area. Via the "Create Teamroom" action, you can create a new Teamroom and grant access rights in one step.

Note:

- In addition to Teamrooms also inboxes and rooms with user data can be defined as standard Teamroom (e.g. background context menu "New" > *Inbox*).
- The organization folder of teams, external organizations and organizational units can be found in their properties.
- The "Organization Folder" widget is displayed on "Home" if you are authorized to at least one standard Teamroom. You can create additional standard Teamrooms for teams, external organizations, organizational units or for the organization using the "New" action.

9 Additional Management Options

The following additional management options are available.

9.1 Anonymize Users

Due to legal regulations, it may be necessary to anonymize users. Anonymization means that the user is replaced in the organizational context in all shortcuts by a special user provided for anonymization. An example of such a shortcut is the user stored in the *Created by* field of any object.

Anonymization also includes saved versions and audit log entries. Closed documents and documents with a retention period are, however, excluded from anonymization.

Terminating a Membership

When you terminate the membership of a user you are managing, you can choose whether to deactivate the user. Upon deactivation, all personal data except first name, surname and e-mail address will be irrevocably deleted.

Anonymization by a Compliance Manager

The compliance managers are defined via the organizational roles. When a user's membership is terminated, compliance managers are notified by e-mail. The compliance managers can immediately anonymize the user, identify all links to the user or define a reminder for a specific point in time. Since anonymization or identification of the links takes some time, the compliance managers are informed of the outcome by e-mail.

Once the links have been determined, compliance managers can view the links if they have access rights or inform the affected Teamroom administrators to review the links. The "Review" button can be used to mark the Teamrooms as reviewed. Thereby, the Teamroom administrators must define whether they believe that the links can be made anonymous. After all opinions have been collected, the compliance manager can anonymize the user if applicable ("Anonymize User" button).

The anonymization use cases can be carried out at any time for users who are no longer members of the organization using the "Anonymize User" context menu command. The context menu command can also be executed on the organization, in particular to anonymize users who, for example, worked in Teamrooms in the context of the organization but were never members.

Deletion Request by a User

If Fabasoft receives a deletion request from a user, the compliance managers of the organizations concerned are informed about the deletion request and asked anonymize the user.

Deleting the User

Once a user has been completely anonymized in all affected organizations, it is automatically deleted.

9.2 Dissolve All Teamrooms

Caution

> Before executing this use case make sure that you no longer need your data. This step cannot be undone.

As owner or co-owner, you have the option to dissolve all Teamrooms (including app rooms and app configurations) of your organization and irrevocably delete the contained data. In addition, all objects of the organization with the security context "ACL for Objects Without a Teamroom" are deleted.

To perform this use case, you can utilize the "Advanced" > "Dissolve All Teamrooms" context menu command on your organization.

9.3 Show New Events

To ensure traceability in organizational management, the corresponding changes are logged (for example, member added or organizational role assigned). To view the events, navigate to your organization and click the "Show New Events" action.

Via the time travel you can access the versions, which were created due to the changes.

9.4 Show Teamroom Usage

You can get a detailed overview of the users in your organization Teamrooms. The evaluation can be restricted to members of a team, organizational unit, external organization or to a single (external) member.

1. Navigate to the desired organizational element or (external) member.
2. Execute the "Show Teamroom Usage" context menu command.

Note:

- When you execute the context menu command on an organizational element, you first receive an overview of the Teamrooms in which the organizational element has been authorized. The "Show Teamroom Usage for Members" button takes you to the overview of the members of the organizational element.

- Via the "Show Details" context menu command, you get more information about the respective user (e.g. editions and apps of the user). As owner/co-owner, you can additionally see the Teamrooms of the organization in which the user has access rights. You can download the data as a CSV file.

9.5 Permanent Login

With the help of a device binding, a user can remain permanently logged in to the Fabasoft Cloud (see also chapter 7.4.6 ""Authentication" tab"). You can use the "Devices" action of an organization member to log out a permanently logged in device.

9.6 Define Data Protection Settings

To define data protection settings for your organization, perform the following steps:

1. Navigate to your organization.
2. In the context menu of the organization, click "Properties".
3. Switch to the "Data Protection" tab.

4. Enter your data.

  o *First Name* and *Surname*
    Defines the name of the person to be notified if personal data protection is violated.

  o *Notification Address*
    Specifies the postal address or e-mail address for the notification.

  o *URL for Data Protection Information*
    The specified link to your data protection information is displayed in the registration form.

5. Click "Next".

9.7 Define Trusted Networks

Trusted networks are used, for example, in the validation of cookie-based user sessions. During the authentication process, a cookie is issued to identify the user session. This cookie is linked to the user's current device for security reasons. The device is identified by the IPv4 address of the network connection. The user session becomes invalid when the IPv4 address changes. In rare cases it may happen that the IPv4 address changes even though the device remains the same (e.g. if several proxies are involved or the IPv4 address of the device is reassigned). In this case, the user session also becomes invalid and the user must log on again.

However, by defining secure address ranges, a user session remains valid even if the IPv4 address has changed, provided that the new IPv4 address is within the configured range.

To define trusted networks for the organization, perform the following steps:

1. In your organization's dashboard, click *Advanced Settings*.

2. Click the Define Policies" action.

3. Switch to the "Authentication" tab.

4. In the *Trusted Networks* field, enter your IPv4 addresses or address ranges.

5. Click "Next".

Note: For external organizations, trusted networks can be specified on the "Advanced Settings" tab.

9.8 Define a Branding for the Organization

The branding allows you to create personalized Teamrooms. If a branding is defined for an organization, Teamrooms are initialized with this branding. The branding is available if the "Branding" tool is activated.

To create a branding for your organization, perform the following steps:

1. Navigate in your organization.

2. Open the "Branding" tool.

3. Activate the branding if necessary.

4. Click "Edit" below the text.

5. Define a logo, a title and a short description.
   Note: You can format the description via the displayed HTML editor.

6. Click "Save"

Note: Users with full control in a Teamroom can use the "Branding" tool to define a logo, a title and a short formatted description for the respective Teamroom.

9.9 E-Mail Communication

For an overview of all e-mails sent in the course of organizational use cases (invitations, exclusion, etc.), the corresponding e-mails are displayed in the properties of the organization on the "E-Mail Communication" tab.

9.10 Define the Push Notification Service

Push notifications from your Fabasoft Private Cloud can only be delivered via the Fabasoft Cloud. You therefore need an account in the Fabasoft Cloud.

To configure the push notification service, proceed as follows:

Fabasoft Cloud

1. Open the account menu (your user name) and click "Advanced Settings" > "Access for Applications".
2. In the *Passwords for Applications* field, click "New".
3. In the *Valid for* field, select "Push Notification Service".
4. Choose a validity period.
5. Click "Next".

The displayed password is required for the configuration in the Fabasoft Private Cloud.

Fabasoft Private Cloud

1. Navigate to your organization.
2. In the context menu of the organization, click "Properties".
3. Switch to the "Push Notification Service" tab.
4. In the *Use Predefined Service* field, select the data location where you created the password for applications.
5. In the *User* field, type the e-mail address of the cloud user you used to create the password for applications.
6. In the *Password* field, type the generated password for applications.
7. Click "Next".

10 Additional Organizations

As specially authorized administrator of the main organization you can create additional organizations and assign them to your organization members. For these organizations you can specify the number of licenses and the available storage space and you can also carry out further administrative tasks (for this purpose no administrative organization role is required in these organizations).

Depending on whom you define as owner or co-owner, you pass the complete control of the organization to the corresponding users (see chapter 3 "Organization Roles"). In additional organizations no new users can be created.

Note: To define the specially authorized administrators, please contact the Fabasoft Support.

10.1 Create Organization Management

The organization management can be used to create and manage additional organizations.

To create an organization management, perform the following steps:

1. Create a Teamroom and navigate in it.
    Note: The Teamroom has to be assigned to the main organization.

2. Open the context menu in an empty part of the content area and click "New".

3. Select the "Organization Management" entry, enter a name and click "Next".

10.2 Create Organizations

To create an additional organization, perform the following steps:

1. Navigate in the organization management.

2. Click the "Create Organization" action.

3. Define the desired settings.

    o *Name*
       The name of the organization.

    o *Owner*
       The owner of the organization can manage the organization and has access to all Teamrooms of the organization. Only the owner himself can define a new owner.

    o *Co-Owner*
       Co-owners have the same rights as owners but cannot define a new owner.

    o *Licenses*
       Defines how many members with the corresponding license can be added to the organization.

    o *Available Storage Space (in GB)*
       Defines how much storage space can be consumed.

    o *Maximum File Size (in MB)*
       Files can only be uploaded if the file size does not exceed the specified value.

    o *Maximum Number of Versions Kept*
       When objects are changed a version is created. Here you can define how many versions are kept at maximum.

4. Click "Next".

10.3 Manage Organizations

To manage additional organizations, perform the following steps:

1. Navigate in the organization management.

2. On the desired organization execute the "Manage Organization" context menu command.

3. You can change the number of licenses and define storage settings.

4. Click "Save".

As administrator of the main organization you can also carry out all other administrative tasks for the organization. To do so, navigate in the organization and manage the members, the licenses and define advanced settings.

11 Service Desk

The support requests submitted by users can be processed via the service desk.

11.1 Configuring the Service Desk

In "Home" you will find the service desk configuration, which can be used to define the app administrators and app users. App administrators can edit the configuration and app users represent the service desk staff.

Full Control (read-only)

The owner and co-owners of the organization have full access.

Define app administrators

5. In the service desk configuration click the "Authorize Team" action.
6. Click the plus symbol beside the *App Administrator* field.
7. Enter the e-mail address of the desired user and confirm with "Return".

In "Home" of the added app administrators the service desk configuration and the service desk dashboard are stored.

Define app users

1. In the service desk configuration click the "Authorize Team" action.
2. Click the plus symbol beside the *App User* field.
3. Enter the e-mail address of the desired user and confirm with "Return".

In "Home" of the added app users the service desk dashboard is stored. The dashboard allows processing the support requests.

Define settings

1. In the service desk configuration click the "Settings" action.
2. On the "General Settings" tab define the basic service desk configuration.
   - *Automatically Finalize Support Requests*
     If this option is enabled, requests closed by the customer will be automatically finalized without any interaction of a service desk employee.
   - *Sender E-Mail Address*
     For e-mails sent to customers the specified e-mail address is used.
3. Click "Next".

Note: In the properties of the organization, you can enter a URL on the "Data Protection" tab in the *URL for Data Protection Information* field. A link with this URL is inserted in the footer of the support e-mails.

11.2 Using the Service Desk

The service desk dashboard is automatically stored in "Home" of app administrators and app users. The dashboard allows processing the support requests.

The typical course of a support request:

1. The customer submits a request using the support button or the service desk employee creates a request for the customer.
2. The responsible service desk employee is defined.
3. The service desk employee communicates with the customer about the request.
4. After a successful completion the request is closed and finalized.
5. If necessary the request can be reopened.

11.2.1 Service Desk Dashboard

The service desk dashboard is divided into the following areas:

- My Support Requests
  Shows all requests that are assigned to the current service desk employee or no service desk employee.
  - o grey symbol
    The request has the state "Work in Progress" and no service desk employee is assigned.
  - o no symbol
    The request has the state "Work in Progress" and a service desk employee is assigned.
  - o yellow symbol
    The request has the state "Waiting for Customer".
  - o green symbol
    The request has the state "Closed".
- Support Requests in Progress
  Shows all requests with state "Work in Progress" regardless of the service desk employee.
- Recently Processed
  Shows the last hundred requests on which an action was performed.
- Product Changes
  Shows the product changes resulting from the support requests.
- Support Reports
  Shows the generated reports.

In the service desk dashboard, the "Create Support Request" action is available. With this action a service desk employee can create a support request for customers. This is necessary, for example, if the customer submitted the request by phone.

11.2.2 Support Request Actions

On support requests the following actions can be performed. On the one hand the actions are available in the context menu of a request and on the other hand under "Tools" > "Actions" of an opened request.

- Answer
  You can send an answer to the customer that can optionally be marked as solution. The

response is sent automatically via e-mail to the customer. The state changes from "Work in Progress" to "Waiting for Customer".

- Add Remark
You can add a message to a request that can also be sent via e-mail to the customer. The state of the request does not change.

- Set Responsible User
You can assign the request to a dedicated service desk employee.

- Set in Progress
You can change the state of the request from "Waiting for Customer" to "Work in Progress".

- Close Support Request
After a successful completion, you or the customer can set the state of the request to "Closed".
Note: After seven days with the status "Waiting for Customer" and without new communication, a reminder e-mail is sent to the customer. After fourteen days, the support request is automatically closed and an information e-mail is sent to the customer.

- Reopen Support Request
In case of new insights you or the customer can reopen the request.

- Finalize
If it is configured that requests are not automatically finalized, you must do so manually. This gives you the opportunity to review requests closed by customers.

- Properties
You can edit the properties of the request.

- Send
You can send a link to the request by e-mail.

11.2.3 Support Reports

Support reports allow an evaluation of the processed requests within a certain period of time.

To generate a report, perform the following steps:

1. Navigate in the service desk dashboard in the "Support Reports" list.
2. Click the "Create Support Report" action.
3. Enter a name and optionally set a period of time, responsible users and organizations.
4. Click "Next".
5. In the context menu of a report click "Generate Report".

The report is shown.

Note: Using the context menu of the report, you can adjust the defined restrictions or generate the report again.