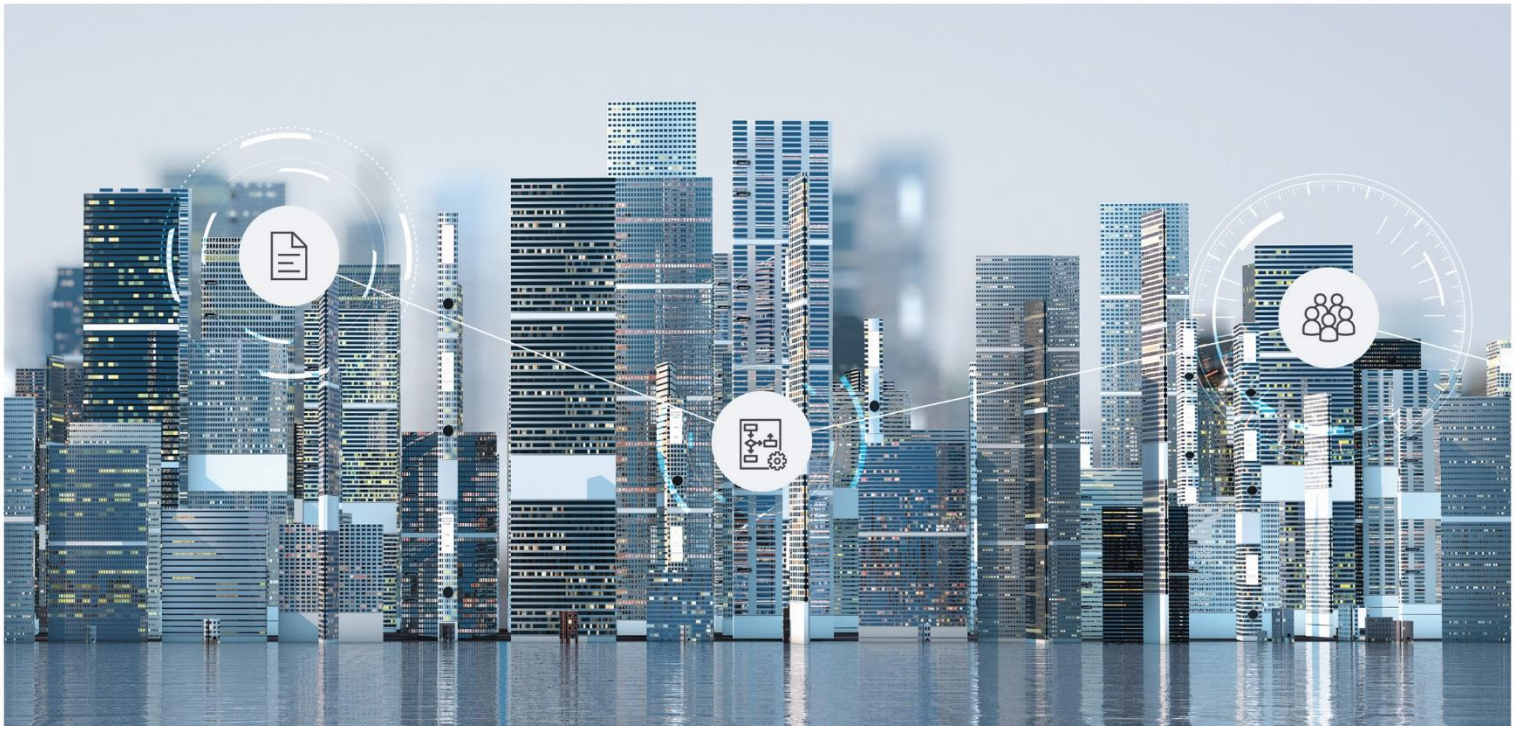
Fabasoft



Administrationshilfe

Fabasoft Cloud

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/-innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Inhalt

1 Einleitung

Die Fabasoft Cloud ermöglicht Lösungen über Organisations-, IT-Infrastruktur- und Länder-Grenzen hinweg. Basisfunktionalitäten, wie die intuitive Erstellung automatisierter Workflows, lückenlose Versionierung, digitale Signatur oder Volltextsuche ermöglichen ein breites Anwendungsspektrum. Informationen zu den einzelnen Lösungen finden Sie in der jeweiligen Lösungsdokumentation.

2 Organisation

Über Ihre Cloud-Organisation können Sie alle relevanten administrativen Tätigkeiten vornehmen. Zu den Verwaltungstätigkeiten gehören zum Beispiel die Mitgliederverwaltung, die Zuordnung von Lizenzen und die Authentifizierungseinstellungen.

Alle Organisationen bei denen Sie Eigentümer, Zahlungspflichtiger oder Administrator sind werden automatisch auf „Home“ abgelegt.

Klicken Sie auf die Organisation, um das Organisations-Dashboard zu öffnen. Im Werkzeugbereich können Sie häufig benötigte Aktionen direkt ausführen. Der Inhaltsbereich bietet eine Übersicht über die Organisation.

Hinweis:

- Eigentümer haben Zugriff auf alle Teamrooms der Organisation und können somit alle Daten einsehen. Administratoren können die Organisation verwalten, haben aber keinen Zugriff auf die Teamrooms der Organisation. Im Kapitel 3 „Organisationsrollen“ ist beschrieben, wie Sie diese ändern können.
- In den Eigenschaften der Organisation können Sie auf der Registerkarte „Organisation“ den Zugriffsschutz festlegen. Standardmäßig dürfen nur Mitglieder die Organisation suchen und lesen. Ist eine Organisation allgemein such- und lesbar, so kann diese von jedem Benutzer gesucht werden und beispielsweise bei Teamrooms eingetragen werden.

3 Organisationsrollen

Über die folgenden Organisationsrollen können Sie Benutzer festlegen, die für die Verwaltung der Organisation zuständig sind:

- Eigentümer bzw. Miteigentümer
  Der Eigentümer bzw. die Miteigentümer können die Organisation verwalten und haben Zugriff auf alle Teamrooms der Organisation und können somit alle Daten einsehen.
  Ein neuer Eigentümer kann nur vom bestehenden Eigentümer bestimmt werden.
  Miteigentümer können vom Eigentümer und anderen Miteigentümern festgelegt werden.
- Haupteigentümer
  Wenn ein Haupteigentümer definiert ist, erhält nur dieser die automatisch generierten E-Mail-Nachrichten, die die Organisation betreffen. Der Benutzer wird auch als Kontakt bei fehlenden Berechtigungen angeführt.
  Das Feld *Haupteigentümer* ist nur sichtbar, wenn mindestens ein Miteigentümer definiert ist.
- Zahlungspflichtiger
  Der Zahlungspflichtige kann Lizenzen erwerben (falls für die Organisation aktiviert) und Administratoren festlegen.

Der Zahlungspflichtige kann nur vom Eigentümer bzw. von den Miteigentümern festgelegt werden.

- Weitere Kaufberechtigte
  Kaufberechtigte können zusätzlich zum Zahlungspflichtigen Lizenzen erwerben (falls für die Organisation aktiviert).
- Compliance-Manager
  Aufgrund von rechtlichen Bestimmungen kann es notwendig sein, Benutzer zu anonymisieren. Wenn die Mitgliedschaft eines Benutzers beendet wird, werden die Compliance-Manager per E-Mail informiert. Die Compliance-Manager können den ausgetretenen Benutzer sofort anonymisieren, die Verknüpfungen mit dem Benutzer ermitteln oder eine Erinnerung für einen bestimmten Zeitpunkt definieren.
- Hauptadministrator bzw. Administratoren
  Der Hauptadministrator bzw. die Administratoren können die Organisation verwalten, haben aber keinen Zugriff auf die Teamrooms der Organisation. Der Hauptadministrator kann aus den Administratoren ausgewählt werden. Wenn ein Hauptadministrator definiert ist, bekommt nur dieser Administrator automatisch generierte Nachrichten, die die Organisation betreffen. Andernfalls erhalten alle Administratoren diese Nachrichten.
  Administratoren und der Hauptadministrator können vom Eigentümer bzw. von den Miteigentümern und vom Zahlungspflichtigen festgelegt werden.
  Das Feld *Hauptadministrator* ist nur sichtbar, wenn mindestens zwei Administratoren definiert sind.
- Support-Team
  Das Support-Team übernimmt die organisationsinterne Verwaltung von Support-Anfragen und kann gegebenenfalls im jeweiligen Kontext (App, Teamroom) anders definiert werden.

Um Organisationsrollen festzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard der Organisation auf *Erweiterte Einstellungen*.
2. Klicken Sie auf die Aktion „Organisationsrollen festlegen“.
3. Legen Sie die gewünschten Organisationsrollen fest.
4. Klicken Sie auf „Speichern“.

Hinweis: Organisationsrollen (bis auf *Eigentümer*) können auch Benutzern zugeordnet werden, die nicht Mitglied der Organisation sind.

4 Organisationsmitglieder

Um Benutzern den Zugriff zu ermöglichen, müssen diese als Organisationsmitglieder zur Organisation hinzugefügt werden.

Die Administration von Mitgliedern, externen Mitgliedern, Teams, Organisationseinheiten und externen Organisationen folgt einem einheitlichen Schema. Dadurch finden Sie sich in allen Bereichen der Mitgliederverwaltung rasch zurecht.

Listen in der Mitgliederverwaltung

- Listen bieten eine einfache Möglichkeit Operationen auf mehreren Benutzern gleichzeitig durchzuführen.

- Sie können Benutzer ausschneiden, kopieren bzw. einfügen und damit die Organisationsstrukturen effizient festlegen. Somit ist es zum Beispiel möglich, mit `Strg + X` die markierten Benutzer aus einem Team zu entfernen.
- Die Eigenschaften von Benutzern, Organisationseinheiten, externen Organisationen bzw. Teams können im Allgemeinen auch über die Spaltenbearbeitung (`F2`-Taste bzw. `Strg + C` und `Strg + V`) effizient geändert werden.

Ermittlung der Hauptorganisation

Ist ein Benutzer in mehreren Organisationen Mitglied, wird die Hauptorganisation folgendermaßen ermittelt:

1. Der Benutzer ist Mitglied der Organisation und die E-Mail-Domäne der Organisation stimmt mit der E-Mail-Domäne des Benutzers überein.
2. Der Benutzer ist Mitglied der Organisation.
3. Der Benutzer ist externes Mitglied der Organisation.
4. Der Benutzer ist Mitglied der Trial-Organisation und die E-Mail-Domäne der Trial-Organisation stimmt mit der E-Mail-Domäne des Benutzers überein.
5. Der Benutzer ist Mitglied der Trial-Organisation.
6. Der Benutzer ist externes Mitglied der Trial-Organisation.

4.1 Mitglieder importieren

Mithilfe des CSV-Imports können auch sehr viele Mitglieder komfortabel angelegt werden.

1. Klicken Sie im Dashboard der Organisation auf *Mitglieder*, um die Mitgliederverwaltung zu öffnen.
2. Klicken Sie auf die Aktion „Mitglieder importieren“.
3. Geben Sie im Feld *Inhalt* den Pfad zu der CSV-Datei ein, die die Mitglieder definiert.
   Hinweis: Über die Schaltfläche „CSV-Vorlage herunterladen“ erhalten Sie eine Vorlage, die die nötige Datenstruktur beschreibt.
4. Klicken Sie auf „Import starten“.
5. Nachdem der Import abgeschlossen wurde, klicken Sie auf „Weiter“.

Die importierten Mitglieder werden in der Mitglieder-Liste abgelegt. Bei einem erneuten Import, werden bereits bestehende Mitglieder aktualisiert. Die eindeutige Identifizierung der Mitglieder erfolgt über die E-Mail-Adresse.

Über die Aktion „Mitglieder zur Organisation einladen“ können Sie eine Einladungs-E-Mail an die importierten Mitglieder senden (siehe Kapitel 4.3 „Mitglieder einladen“).

Datenstruktur der CSV-Datei

CSV-Spalte	Beschreibung
`EMail`	E-Mail-Adresse für die Anmeldung (eindeutig; erforderlich) **Hinweis:** Wird als Schlüssel verwendet, wenn `objexternalkey` keinen Wert enthält.

`CN`	Common Name (wird für die Anmeldung mit Client-Zertifikat benötigt und muss mit dem CN des Client-Zertifikats des jeweiligen Benutzers übereinstimmen)
`PinPhone`	Telefonnummer, an die die SMS-PIN gesendet wird (wenn nichts angegeben wurde, wird die E-Mail-Adresse für die Anmeldung verwendet)
`PinEMail`	E-Mail-Adresse, an die die E-Mail-PIN gesendet wird (wenn nichts angegeben wurde, wird die E-Mail-Adresse für die Anmeldung verwendet)
`PinRadiusID`	Benutzerkennung im RADIUS-Server (wenn RADIUS entsprechend konfiguriert ist, kann hier die Benutzerkennung gemäß Ihrer Server-Konfiguration angegeben werden)
`PinOrder`	Versandart für Zwei-Faktor-Authentifizierung • `MPO_SMSFIRST` (SMS) • `MPO_EMAILFIRST` (E-Mail) • `MPO_RADIUSFIRST` (Verwende RADIUS-Server)
`samlemail`	E-Mail-Adresse für Active Directory / SAML 2.0
`FirstName`	Vorname (erforderlich)
`MiddleInitial`	weitere Vornamen
`Surname`	Nachname (erforderlich)
`Title`	Titel
`PostTitle`	nachgestellter Titel
`Sex`	Geschlecht (mögliche Werte: `SEX_FEMALE`, `SEX_MALE`, `SEX_DIVERSE`)
`Salutation`	Anrede
`Birthday`	Geburtsdatum (Format: `yyyy-mm-dd`)
`Street`	Adressen (Straße)
`PostOfficeBox`	Adressen (Postfach)
`ZipCode`	Adressen (Postleitzahl)
`City`	Adressen (Ort)
`State`	Adressen (Bundesland)

`Country`	Adressen (Land)
`Phone`	Telefonnummern (geschäftlich)
`Fax`	Telefonnummern (Fax)
`Mobile`	Telefonnummern (mobil)
`PrivatePhone`	Telefonnummern (privat)
`Function`	Funktion in der Organisation
`TeamKey`	Importkennung des Teams (wenn kein Team mit der Importkennung gefunden wird, wird ein neues erzeugt, sonst wird gegebenenfalls der Name aktualisiert)
`TeamName`	Name des Teams
`AdminTeamKey`	Team-Administrator (mögliche Werte: *Importkennungen* der zu administrierenden Teams getrennt durch „|“)
`Website`	Website
`Language`	Sprache (Schreibweise entsprechend der Sprache z. B. Español; die möglichen Werte finden Sie in der CSV-Vorlage oder in den „Grundeinstellungen“ unter *Sprache*; alternativ können Sprachkennungen gemäß ISO 639-1 verwendet werden)
`Solutions`	Lösungen (mögliche Werte: *Fabasoft Cloud ID* bzw. Referenz der Lösungen getrennt durch „|“)
`Apps`	Apps (mögliche Werte: *Fabasoft Cloud ID* bzw. vollständige Referenz der Apps getrennt durch „|“)
`InvalidAuthMethods`	Deaktivierte Authentifizierungsmethoden (möglicher Wert: `AuthenticationMethodUsernamePassword`)
`MainLocation`	Standard-Datenlokation (mögliche Werte: `at`, `de`, `ch`; nicht verfügbar in der Fabasoft Private Cloud)
`InvitationSent`	Eingeladen (mögliche Werte: `true`, `false`)
`ManageHome`	Home-Bereich verwalten (mögliche Werte: `true`, `false`)
`CreateTeamrooms`	Teamrooms erzeugen – alle Datenlokationen (mögliche Werte: `true`, `false`)

`CreateTeamrooms-LocationAustria`	Teamrooms erzeugen – Datenlokation Österreich (mögliche Werte: `true`, `false`; nicht verfügbar in der Fabasoft Private Cloud)
`CreateTeamrooms-LocationGermany`	Teamrooms erzeugen – Datenlokation Deutschland (mögliche Werte: `true`, `false`; nicht verfügbar in der Fabasoft Private Cloud)
`CreateTeamrooms-LocationSwitzerland`	Teamrooms erzeugen – Datenlokation Schweiz (mögliche Werte: `true`, `false`; nicht verfügbar in der Fabasoft Private Cloud)
`TransferTeamrooms`	Teamrooms übertragen (mögliche Werte: `true`, `false`)
`grpolicysearchaudit`	Suchordner für Audit-Logs verwenden (mögliche Werte: `true`, `false`)
`grpolicyaddmembers`	Mitglieder zur Organisation hinzufügen (mögliche Werte: `true`, `false`)
`grpolicyremovemembers`	Mitglieder von der Organisation entfernen (mögliche Werte: `true`, `false`)
`grorgstructmanagers`	Aufbauorganisation verwalten (mögliche Werte: `true`, `false`)
`grorgunitmanagers`	Teams verwalten (mögliche Werte: `true`, `false`)
`grpolicyaddexternal`	Externe Mitglieder zur Organisation hinzufügen (mögliche Werte: `true`, `false`)
`grextorgmanagers`	Externe Organisationen verwalten (mögliche Werte: `true`, `false`)
`grpolicyopenonlineex`	Office-Dokumente in Microsoft Office for the Web bearbeiten (mögliche Werte: `true`, `false`)
`grpolicyreadonworkspace`	Inhalte am Endgerät öffnen bzw. herunterladen (mögliche Werte: `true`, `false`)
`ImageName`	Foto (Name des Bilds, das zugeordnet werden soll)
`ImageTeamrooms`	*Fabasoft Cloud ID* des Teamrooms, indem die Bilder abgelegt sind
`objexternalkey`	Eindeutige ID **Hinweis:** Wird als Schlüssel verwendet, wenn ein Wert vorhanden ist (ermöglicht somit die Aktualisierung der E-Mail-Adresse, die ansonsten als Schlüssel verwendet wird).

`OverrideKeys`	CSV-Spalten von zu überschreibenden Eigenschaften getrennt durch Beistriche (ansonsten werden leere Werte ignoriert und bei Listen die Werte hinzugefügt) Für Adressen, Telefonnummern und Organisationsrichtlinien müssen folgende Schlüssel für die zusammengehörigen CSV-Spalten verwendet werden: `address`, `telephone`, `policies` (für die Adressen, Telefonnummern gilt: das Überschreiben gilt nur innerhalb der jeweilige Art, z. B. Fax; für die Richtlinien gilt: leere Zelle entspricht `false`)

Hinweis: Um mehrere Adressen zu hinterlegen oder Mitglieder mehreren Teams zuzuordnen, können in der CSV-Datei mehrere Zeilen mit derselben E-Mail-Adresse (`EMail`) angegeben werden.

4.2 Mitglieder hinzufügen

Zusätzlich zum CSV-Import können Mitglieder auch einzeln angelegt und administriert werden.

1. Klicken Sie im Dashboard der Organisation auf *Mitglieder*, um die Mitgliederverwaltung zu öffnen.
2. Klicken Sie auf die Aktion „Mitglieder hinzufügen“.
3. Geben Sie im Feld *Benutzer* die E-Mail-Adresse des Benutzers ein.
4. Klicken Sie im Dropdown-Menü auf einen bestehenden Benutzer, um diesen als Mitglied hinzuzufügen. Falls noch kein Benutzer mit der eingegebenen E-Mail-Adresse existiert, klicken Sie auf „Neuen Benutzer einladen“, um einen neuen Benutzer zu erzeugen.
5. Um mehrere Mitglieder gleichzeitig hinzuzufügen, wiederholen Sie Schritt 3 und 4.
6. Wählen Sie gegebenenfalls Teams bzw. Organisationseinheiten aus, denen die Benutzer zugeordnet werden sollen.
7. Klicken Sie auf die Schaltfläche „Hinzufügen“.
8. Ordnen Sie den Benutzern Lösungen und Apps zu und klicken Sie auf „Zuordnen“.
9. Klicken Sie auf „Einladen“, um pro Mitglied eine E-Mail zur Bestätigung der Mitgliedschaft zu senden. Klicken Sie auf „Später einladen“, um die Einladung später zu versenden (siehe Kapitel 4.3 „Mitglieder einladen“).

Die hinzugefügten Mitglieder können über den Kontextmenübefehl „Eigenschaften“ noch weiter bearbeitet werden.

4.3 Mitglieder einladen

Wenn Sie einen CSV-Import durchgeführt haben bzw. manuell hinzugefügte Mitglieder noch nicht direkt beim Hinzufügen eingeladen haben, können Sie dies über die Aktion „Mitglieder zur Organisation einladen“ nachholen.

Um Mitglieder einzuladen, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Organisation auf die Aktion „Mitglieder zur Organisation einladen“. Die Aktion ist nur sichtbar, wenn noch einzuladende Mitglieder vorhanden sind.

2. Legen Sie die Empfänger fest. Zur einfachen Auswahl der Empfänger, können folgende Empfängergruppen ausgewählt werden: *Nicht eingeladene Mitglieder*, *Nicht registrierte Mitglieder* und *Mitglieder mit offener Bestätigung*.
3. Die Felder *Betreff* und *Nachricht* sind bereits vorbefüllt. Nehmen Sie gegebenenfalls entsprechende Anpassungen vor.
4. Klicken Sie auf „Einladen".

Hinweis:

- Mitglieder können auch auf Ebene von Organisationseinheiten, Teams und externen Organisationen eingeladen werden.
- Der E-Mail-Standardtext kann in den Eigenschaften der Organisation (Registerkarte „E-Mail-Einladungen") festgelegt werden.

4.4 Statusinformationen

Um die Statusinformationen der Benutzer zu überprüfen, navigieren Sie in der Organisation in die Mitgliederliste. Die Statusinformationen sind standardmäßig als Spalten eingeblendet.

- *Status*
  Benutzer können Eigentümer, Mitglied bzw. externes Mitglied der Organisation sein. Falls der Status durch den Benutzer bestätigt werden muss und die Bestätigung noch ausständig ist, wird der Status „Bestätigung erforderlich" angezeigt.
- *Eingeladen*
  Zeigt, ob der Benutzer per E-Mail eingeladen wurde. Der Wert kann auch manuell auf „Ja" geändert werden, wenn der Benutzer zum Beispiel im „Mitglieder einladen"-Dialog nicht mehr berücksichtigt werden soll.
- *Registriert*
  Zeigt, ob der Benutzer registriert ist und sich somit anmelden kann.

Hinweis: Benutzer, die eine Einladung abgelehnt haben bzw. deren Mitgliedschaft beendet wurde, werden in der Organisation in der Mitgliederverwaltung unter „Austritte" angezeigt.

4.5 Mitgliedschaft ändern

Externe Mitglieder können in Mitglieder umgewandelt werden und umgekehrt.

Um die Mitgliedschaft eines Benutzers zu ändern, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard der Organisation auf *Mitglieder*.
2. Navigieren Sie zum gewünschten Mitglied bzw. externen Mitglied.
3. Führen Sie den Kontextmenübefehl „Mitgliedschaft ändern" aus.
4. Wählen Sie gegebenenfalls externe Organisationen, Teams bzw. Organisationseinheiten aus, denen der Benutzer zugeordnet werden soll und klicken Sie auf die Schaltfläche „Mitgliedschaft ändern".
5. Wenn ein Mitglied administrative Rechte in der Organisation hat, müssen Sie den Verlust der administrativen Rechte bestätigen.

Beim Ändern der Mitgliedschaft wird ein Mitglied aus allen Teams und Organisationseinheiten entfernt und ein externes Mitglied wird aus allen externen Organisationen entfernt.

4.6 Mitgliedschaft beenden

Mitglieder, deren Mitgliedschaft beendet wird, werden auch aus allen Planstellen, Teams und aus den Teamrooms der Organisation entfernt. Beim Entfernen eines Mitglieds kann ein Nachfolger festgelegt werden, der stattdessen in den Planstellen, Teams und Teamrooms der Organisation eingetragen wird.

Um die Mitgliedschaft eines Benutzers zu beenden, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu dem gewünschten Mitglied.
2. Klicken Sie im Kontextmenü des Mitglieds auf „Mitgliedschaft beenden“.
3. Legen Sie fest, ob das Mitglied per E-Mail informiert werden soll und der Benutzer deaktiviert werden soll. Geben Sie gegebenenfalls einen Nachfolger an.
    - Der Benutzer kann nur deaktiviert werden, wenn dieser von Ihrer Organisation verwaltet wird. Wenn der Benutzer in keiner weiteren Organisation Mitglied ist, wird dieser immer deaktiviert.
    - Als Nachfolger von Mitgliedern können nur Mitglieder ausgewählt werden. Als Nachfolger von externen Mitgliedern können Mitglieder und externe Mitglieder ausgewählt werden.
4. Klicken Sie auf „Mitgliedschaft beenden“, um den Ausschluss zu bestätigen.

Ausgeschlossene Mitglieder werden in der Organisation in der Mitgliederverwaltung unter „Austritte“ angezeigt. Hier können Sie auch den Verarbeitungsstatus des Austritts einsehen.

Verarbeitungsstatus:

- In Bearbeitung
  Der Austritt wird über eine Hintergrundaufgabe abgearbeitet. Falls ein Fehler auftritt, wird dieser Vorgang bis zu fünfmal wiederholt. Falls auch der fünfte Versuch nicht erfolgreich war, wird der Verarbeitungsstatus auf „Manuell“ geändert und die Organisations-Administratoren erhalten eine E-Mail, mit der Möglichkeit, die nicht behandelten Teamrooms manuell zu behandeln und die Zugriffsrechte zu entziehen.
- Erledigt
  Der Austritt wurde erfolgreich durchgeführt.
- Manuell
  Der Austritt konnte nicht vollständig automatisiert durchgeführt werden. Die Organisations-Administratoren erhalten eine E-Mail, mit der Möglichkeit, die nicht behandelten Teamrooms manuell zu behandeln und die Zugriffsrechte zu entziehen.

Hinweis:

- Benutzer, die über alle Rechte in den Organisations-Teamrooms verfügen und Mitglieder dieser Organisation sind, werden per E-Mail informiert. Diese Benutzer haben die Möglichkeit den entfernten Benutzer, sofern er nicht deaktiviert wurde, wieder in den Teamroom einzuladen. Falls der entfernte Benutzer das einzige Teammitglied mit allen Rechten auf einem Teamroom ist und kein Nachfolger definiert wurde, so wird der Eigentümer der Organisation bei diesem Teamroom mit allen Rechten eingetragen.
- Öffentliche Links, die dem ausgetretenen Benutzer zugeordnet sind, werden deaktiviert. Der Nachfolger kann über einen Link in der Benachrichtigungs-E-Mail die öffentlichen Links löschen bzw. übernehmen und somit wieder aktivieren.
- Aktivitäten im Arbeitsvorrat des Mitglieds werden automatisch dem Nachfolger zugeteilt.

- Wird beim Beenden der Mitgliedschaft eines Benutzers mit speziellen Organisationsrollen (z. B. Miteigentümer) ein Nachfolger definiert, wird der Nachfolger nicht bei den Organisationsrollen eingetragen.
- Das Austragen des Benutzers und Eintragen des Nachfolgers bei einem Teamroom wird asynchron durchgeführt und kann einige Zeit in Anspruch nehmen.
- Beim Beenden einer Mitgliedschaft in externen Organisationen, Organisationseinheiten bzw. Teams werden die Benutzer mit allen Rechten ebenfalls per E-Mail informiert, wenn der Teamroom auf die betroffene externe Organisation, Organisationseinheit bzw. auf das betroffene Team eingeschränkt wurde.
- Für Teamrooms anderer Organisationen gilt:
  - Wird die Mitgliedschaft des Benutzers in seiner Hauptorganisation beendet, werden auch Benutzer mit allen Rechten in Teamrooms anderer Organisationen über den Austritt und gegebenenfalls über den Nachfolger benachrichtigt. Die Zugriffsrechte können von einem Benutzer mit allen Rechten manuell angepasst werden.
  - Wird die Mitgliedschaft des Benutzers in einer seiner Nicht-Hauptorganisationen beendet, werden nur Teamrooms behandelt, die auf die betroffene Organisation eingeschränkt wurden.

4.7 Teams verwalten

Teams dienen zur informellen Strukturierung von Organisationsmitgliedern, externen Mitgliedern und Mitgliedern anderer Organisationen. Sie können zum Beispiel in Teamrooms dazu verwendet werden, um das gesamte Team zu berechtigen.

Um ein Team zu erzeugen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard der Organisation auf *Mitglieder* und dann auf *Teams*.
2. Klicken Sie auf die Aktion „Team erzeugen“.
3. Vergeben Sie einen Namen. Im Feld *Teammitglieder festlegen* können Sie Benutzer zum Team hinzufügen.
4. Klicken Sie auf „Erzeugen“.

Hinweis:

- Pro Lizenzart gibt es vordefinierte Teams, die automatisch aktualisiert werden. Diese können zum Beispiel in App-Konfigurationen hinterlegt werden, da die App-Rollen oft mit den Lizenzarten übereinstimmen.
- Für Teams können Sie Standard-Teamrooms festlegen (siehe Kapitel 8 „Standard-Teamrooms“).
- Als Organisationsadministrator können Sie Mitglieder festlegen, die alle Teams verwalten dürfen (Organisations-Dashboard > „Erweiterte Einstellungen“ > „Richtlinien festlegen“ > Registerkarte „Mitgliederverwaltung“ > *Teams verwalten*).
- Als Organisationsadministrator können Sie Team-Administratoren für einzelne Teams festlegen (über die Aktion „Administratoren festlegen“ im jeweiligen Team). Die entsprechenden Teams werden bei den Team-Administratoren auf „Home“ abgelegt. Team-Administratoren können folgende Aktionen durchführen:
  - Mitglieder hinzufügen, einladen und entfernen
  - Eigenschaften des Teams bearbeiten

- Bei Teams können auf der Registerkarte „Benachrichtigungseinstellungen“ die Einstellungen für Workflow-Ereignisse festgelegt werden. Die Benachrichtigungen werden an die erste, auf der Registerkarte „Adresse“ im Feld *E-Mail-Adressen* festgelegte E-Mail-Adresse gesendet. Somit werden nicht mehr alle Mitglieder des Teams benachrichtigt, sondern nur noch die definierte E-Mail-Adresse.
- Sie können für Teams einen Zugriffsschutz festlegen („Eigenschaften“ > Registerkarte „Sicherheit“). Somit können entweder nur Organisationsmitglieder oder alle Benutzer dieses Team suchen. Der Zugriffsschutz der Organisation wird nicht auf das Team übertragen.

4.8 Authentifizierung und zweiten Faktor festlegen

Die Anmeldung kann über Benutzername und Passwort, Digital ID, SAML 2.0, Active Directory oder Client-Zertifikate erfolgen.

Für die Zwei-Faktor-Authentifizierung steht Mobile PIN (SMS), E-Mail-PIN und Einmalpasswort über RADIUS-Server zur Verfügung.

Um die Einstellungen für einen Benutzer zu ändern, gehen Sie folgendermaßen vor:

1. Navigieren Sie in das gewünschte Mitglied und klicken Sie auf die Aktion „Eigenschaften“.
2. Auf der Registerkarte „Konto“ können Sie die Einstellungen zur Authentifizierung und zum zweiten Faktor vornehmen.
   - *Primäre E-Mail-Adresse*
     Mit dieser E-Mail-Adresse kann sich der Benutzer anmelden. Benachrichtigungen werden ebenfalls an diese E-Mail-Adresse gesendet.
   - *Alternative E-Mail-Adresse für Authentisierung*
     Mit dieser E-Mail-Adresse kann sich der Benutzer über Benutzername/Passwort, Active Directory bzw. SAML 2.0 anmelden (ein Anmeldeserver muss bei der Organisation konfiguriert sein). Die E-Mail-Adresse wird nur benötigt, wenn sie nicht mit der primären E-Mail-Adresse übereinstimmt. Somit kann zum Beispiel die primäre E-Mail-Adresse für den Empfang von Benachrichtigungen verwendet werden und die alternative E-Mail-Adresse für den Anmeldeserver.
   - *Common Name (CN)*
     Legt den Common Namen des jeweiligen Benutzerzertifikats fest (Zertifizierungsstellen müssen bei der Organisation hinterlegt sein).
   - *Standard-Methode für Zwei-Faktor-Authentifizierung*
     Legt den primären zweiten Faktor für den Benutzer fest. Abhängig davon muss entweder eine Mobiltelefonnummer, eine RADIUS-Benutzerkennung oder eine E-Mail in den folgenden Feldern hinterlegt sein. Sind mehrere Felder befüllt, kann der Benutzer bei der Anmeldung eine alternative Methode zum erneuten Versenden auswählen.
   - *Mobiltelefonnummer für Mobile PIN*
     An diese Telefonnummer wird die PIN gesendet.
   - *E-Mail-Adresse für Mobile PIN*
     An diese E-Mail-Adresse wird die PIN gesendet.
   - *Benutzerkennung am RADIUS-Server*
     Definiert die Verknüpfung des Benutzers mit dem RADIUS-Server (ein RADIUS-Server muss bei der Organisation konfiguriert sein).
   - *Deaktivierte Authentifizierungsmethoden*
     Um zu verhindern, dass sich der Benutzer mit bestimmten Authentifizierungsmethoden

anmeldet, können hier die nicht erlaubten Authentifizierungsmethoden festgelegt werden. Bevor Sie Authentifizierungsmethoden deaktivieren, sollten Sie sicherstellen, dass Sie den Benutzer nicht aussperren.

- *Anmeldeoptionen werden übernommen von*
  Zeigt die für den Benutzer geltenden Anmeldeoptionen (Active Directory/SAML 2.0, Zertifikat, RADIUS; falls vorhanden). Die Anmeldeoptionen werden für externe Mitglieder basierend auf folgender Auswertungshierarchie ermittelt (wenn keine Einstellungen vorhanden sind, wird die nächste Ebene berücksichtigt): primäre externe Organisation, "Alle externen Mitglieder von <Cloud-Organisation>" und Cloud-Organisation.

3. Klicken Sie auf „Weiter“, um die Änderungen zu speichern.

Hinweis:

- Nur Administratoren bzw. Eigentümer der primären Organisation des Benutzers können diese Eigenschaften ändern. Die primäre Organisation finden Sie in den Eigenschaften des Benutzers auf der Registerkarte „Benutzer“ im Feld *Organisation*.
- Die Einstellungen können auch mittels CSV-Import festgelegt werden.
- Damit sich Benutzer mit SAML 2.0 bzw. Active Directory anmelden können, müssen diese registriert sein. Benutzer werden automatisch registriert, wenn ein entsprechender Anmeldeserver konfiguriert ist und die E-Mail-Domäne übereinstimmt. Für nicht registrierte Benutzer kann auf der Organisation der Kontextmenübefehl „Mitglieder für SAML 2.0/AD FS registrieren“ ausgeführt werden. Der Kontextmenübefehl wird nur angezeigt, wenn nicht registrierte Mitglieder vorhanden sind und die Organisation für die Verwendung von SAML 2.0 bzw. Active Directory konfiguriert wurde.

4.9 Kontoaktivitäten der Mitglieder anzeigen

Um sich die Kontoaktivitäten der Mitglieder anzusehen, gehen Sie folgendermaßen vor:

1. Navigieren Sie zur gewünschten Organisation, externen Organisation, zum Team oder zu einem (externen) Mitglied.
2. Führen Sie den Kontextmenübefehl „Kontoaktivitäten anzeigen“ bzw. „Erweitert“ > „Kontoaktivitäten anzeigen“ aus.
3. Die Kontoaktivitäten des Mitglieds werden angezeigt und können über die Schaltfläche „Kontoaktivitäten als CSV-Datei exportieren“ heruntergeladen werden.
4. Klicken Sie auf „Schließen“.

Hinweis:

- Nur von Ihnen verwaltete (externe) Mitglieder werden angezeigt.
- Bei Mitgliedern, die sich noch nie angemeldet haben, werden in der CSV-Datei die Spalten mit „N/A“ befüllt.

4.10 Externe Mitglieder verwalten

Mitarbeiter von Kunden-, Lieferanten- bzw. Partner-Firmen können Sie als externe Mitglieder zu Ihrer Organisation hinzufügen. Um die organisationsübergreifende Zusammenarbeit weiter zu vereinfachen, stehen externe Organisationen zur Verfügung, um externe Mitglieder aufgrund ihrer Firmenzugehörigkeit zusammenzufassen und verwalten zu können.

Um externe Mitglieder zu verwalten, gehen Sie folgenderweise vor:

1. Klicken Sie im Dashboard der Organisation auf *Mitglieder*, um die Mitgliederverwaltung zu öffnen.
2. Unter *Externe Mitglieder* können Sie externe Mitglieder importieren, hinzufügen, einladen bzw. die Mitgliedschaft beenden.
3. Unter *Externe Organisationen* können Sie externe Organisationen anlegen, um die externen Mitglieder logisch zu strukturieren.

Hinweis:

- Beim Import von externen Mitgliedern (CSV-Spalten siehe Kapitel 4.1 „Mitglieder importieren“) stehen folgende zwei zusätzlich CSV-Spalten im Vergleich zum Import von Mitgliedern zur Verfügung: `ExtOrganizationKey` (Importkennung einer externen Organisation) und `ExtOrganizationName` (Name der externen Organisation). Zusätzlich gelten nur die Organisationsrichtlinien `grpolicyopenonlineex` und `grpolicyreadonworkspace` für externe Mitglieder. `AdminTeamKey` steht ebenfalls für externe Mitglieder nicht zur Verfügung.
- Externe Mitglieder verbrauchen wie Mitglieder Lizenzen.
- Externen Mitgliedern können wie Mitgliedern Lösungen und Apps zugeordnet werden.
- Externe Mitglieder können keine der Organisation zugeordneten Teamrooms erzeugen.
- Nur Administratoren bzw. Eigentümer der primären Organisation des Benutzers können die Benutzerdaten ändern. Die primäre Organisation finden Sie in den Eigenschaften des Benutzers auf der Registerkarte „Benutzer“ im Feld *Organisation*.
- Die standardmäßig angelegte externe Organisation ‚Alle externen Mitglieder von „<Organisation>“‘ enthält stets alle externen Mitglieder, unabhängig davon, ob die Mitglieder auch anderen externen Organisationen zugeordnet sind.
- Bei der externen Organisation ‚Alle externen Mitglieder von „<Organisation>“‘ (Registerkarte „Erweiterte Einstellungen“ > *Externe Mitglieder sind für alle Mitglieder der Organisation suchbar*) kann eingestellt werden, dass rechtemäßig die externen Mitglieder der Organisation wie Mitglieder der Organisation behandelt werden (d.h. die Mitglieder dürfen die externen Mitglieder finden und die sensiblen Eigenschaften lesen).
  Hinweis: Die Einschränkung gilt nicht für Eigentümer, Administratoren bzw. Benutzer, die mittels Richtlinie externe Mitglieder verwalten dürfen.
- Als Organisationsadministrator können Sie die primäre externe Organisation für ein externes Mitglied festlegen (Registerkarte „Organisationsmitgliedschaft“, Feld *Primäre externe Organisation*), wenn der Benutzer in mehreren externen Organisationen Mitglied ist. Falls der Benutzer in keiner externen Organisation Mitglied ist, wird das Feld nicht angezeigt. Wenn der Benutzer erstmalig zu einer externen Organisation hinzugefügt wird, wird das Feld automatisch befüllt.
  Die Einstellungen bzgl. der Anmeldeoptionen werden für das externe Mitglied basierend auf folgender Auswertungshierarchie ermittelt (wenn keine Einstellungen vorhanden sind, wird die nächste Ebene berücksichtigt): primäre externe Organisation, "Alle externen Mitglieder von <Cloud-Organisation>" und Cloud-Organisation.
  Die Administratoren der primären externen Organisation sind auch berechtigt, die externe Mitgliedschaft des Benutzers zu beenden.
- Als Organisationsadministrator können Sie Mitglieder festlegen, die alle externe Organisationen verwalten dürfen (Organisations-Dashboard > „Erweiterte Einstellungen“ > „Richtlinien festlegen“ > Registerkarte „Mitgliederverwaltung“ > *Externe Organisationen verwalten*).
- Als Organisationsadministrator können Sie Mitglieder bzw. externe Mitglieder als Administratoren für einzelne externe Organisationen festlegen (über die Aktion

„Administratoren festlegen“ in der jeweiligen externen Organisation). Die entsprechenden externe Organisationen werden bei den Administratoren auf „Home“ abgelegt. Administratoren können folgende Aktionen durchführen: externe Mitglieder hinzufügen, einladen und entfernen, externe Mitgliedschaften beenden (nur wenn die externe Organisation, die primäre externe Organisation des externen Mitglieds ist), Zertifikats- und RADIUS-Einstellungen festlegen, Eigenschaften der externen Organisation bearbeiten.

- Für externe Organisationen können auf der Registerkarte „Erweiterte Einstellungen“ vertrauenswürdige Netzwerke festgelegt werden. Nähere Informationen finden Sie im Kapitel 9.8 „Vertrauenswürdige Netzwerke festlegen“.
- Bei externen Organisationen können auf der Registerkarte „Benachrichtigungseinstellungen“ die Einstellungen für Workflow-Ereignisse festgelegt werden. Die Benachrichtigungen werden an die erste, auf der Registerkarte „Adresse“ im Feld *E-Mail-Adressen* festgelegte E-Mail-Adresse gesendet. Somit werden nicht mehr alle Mitglieder der externen Organisation benachrichtigt, sondern nur noch die definierte E-Mail-Adresse.

4.11 Aufbauorganisation verwalten

Die Aufbauorganisation dient zur hierarchischen Abbildung von Organisationseinheiten und Planstellen Ihrer Organisation. Die Aufbauorganisation finden Sie in Ihrer Organisation unter „Mitglieder“ > „Aufbauorganisation“.

- Organisationseinheit
  Eine Organisationseinheit fasst eine oder mehrere Planstellen zusammen und kann untergeordnete Organisationseinheiten enthalten. Die Hierarchie von Organisationseinheiten definiert sich einerseits durch die Baumstruktur in der Aufbauorganisation und andererseits durch die zugewiesenen Hierarchie-Ebenen (z. B. Segment, Bereich, Team).
- Planstelle
  Mit Planstellen bilden Sie die einzelnen Positionen in Ihrer Organisation und die Zuordnung zu Organisationseinheiten ab. Der Planstelle kann ein konkreter Benutzer zugeordnet werden. Es gibt zwei Planstellen-Typen: Leiter/-in und Mitarbeiter/-in. Diese Information kann im Workflow für Genehmigungen verwendet werden (z. B. Urlaubsantrag eines Mitarbeiters wird dem Leiter der jeweiligen Organisationseinheit zugewiesen).

Organisationsadministratoren bzw. Benutzer, die über die Organisationsrichtlinie „Aufbauorganisation verwalten“ berechtigt wurden, sind zuständig für die Pflege der Organisationseinheiten und Planstellen (z. B. Zuordnung eines Benutzers zu einer Planstelle).

Beim Löschen von Organisationseinheiten bzw. Planstellen werden diese zuerst in den Papierkorb gelegt. Dort können sie endgültig gelöscht oder wiederhergestellt werden.

4.11.1 Hierarchie-Ebenen festlegen

Wenn Sie sich in der Aufbauorganisation befinden, können Sie über die Aktion „Einstellungen“ die Hierarchie-Ebenen festlegen. Standardmäßig sind folgende Hierarchie-Ebenen vordefiniert:

- Management Board (Ebene 01)
- Segment (Ebene 02)
- Bereich (Ebene 03)
- Team (Ebene 04)

Über den Kontextmenübefehl „Eigenschaften“ können Sie den Namen und die Ebene anpassen. Neue Hierarchie-Ebenen erhalten Sie über den Hintergrund-Kontextmenübefehl „Neu“.

Hinweis: Organisationseinheiten können nur Organisationseinheiten mit größerem Ebenen-Wert enthalten (z. B. in Organisationseinheiten der Ebene 02 können sich nur Organisationseinheiten ab Ebene 03 befinden).

4.11.2 Organisationseinheiten erzeugen

Wenn Sie sich in der Aufbauorganisation befinden, können Sie über die Aktion „Organisationseinheit erzeugen“ Organisationseinheiten anlegen. Navigieren Sie in bereits erzeugte Organisationseinheiten, um untergeordnete Organisationseinheiten zu erzeugen.

Sie können folgende Werte festlegen:

- *Name*
  Definiert den Namen der Organisationseinheit.
- *Stabsstelle*
  Ist eine Organisationseinheit nicht Teil der linearen Hierarchie, kann sie als Stabsstelle gekennzeichnet werden.
- *Hierarchie-Ebene*
  Definiert die Hierarchie-Ebene der Organisationseinheit. Es werden nur Ebenen angezeigt, die einen höheren Wert aufweisen, als die bei der übergeordneten Organisationseinheit definierte Ebene.
  Hinweis: Die verfügbaren Ebenen können Sie in den Einstellungen der Aufbauorganisation festlegen.
- *Beschreibung*
  Definiert die Beschreibung der Organisationseinheit.
- *Importkennung*
  Wird die Aufbauorganisation extern verwaltet und importiert, kann eine Importkennung für die Organisationseinheit festgelegt werden. Damit wird eine Aktualisierung der Organisationseinheit durch einen Import ermöglicht.
- *Mitglieder mit der Rolle „Leiter/-in“*
  Geben Sie die Leiter der Organisationseinheit an. Die entsprechenden Planstellen werden automatisch erzeugt.
- *Mitglieder mit der Rolle „Mitarbeiter/-in“*
  Geben Sie die Mitarbeiter der Organisationseinheit an. Die entsprechenden Planstellen werden automatisch erzeugt.

Hinweis:

- Über den Kontextmenübefehl „Organisationseinheit verschieben“ können Sie die Organisationseinheit innerhalb der Aufbauorganisation verschieben.
- Teams können Sie über den Kontextmenübefehl „In Aufbauorganisation verschieben“ in Organisationseinheiten umwandeln.
- Bei Organisationseinheiten können auf der Registerkarte „Benachrichtigungseinstellungen“ die Einstellungen für Workflow-Ereignisse festgelegt werden. Die Benachrichtigungen werden an die erste, auf der Registerkarte „Adresse“ im Feld *E-Mail-Adressen* festgelegte E-Mail-Adresse gesendet. Somit werden nicht mehr alle Mitglieder der Organisationseinheit benachrichtigt, sondern nur noch die definierte E-Mail-Adresse.

4.11.3 Planstellen erzeugen

Wenn Sie sich in der Aufbauorganisation in einer Organisationseinheit befinden, können Sie über die Aktion „Planstelle erzeugen“ eine Planstelle zugehörig zur jeweiligen Organisationseinheit anlegen.

Sie können folgende Werte festlegen:

- *Typ*
  Legt fest, ob es sich um eine Mitarbeiter- oder Leiter-Planstelle handelt.
- *Stabsstelle*
  Ist eine Planstelle nicht Teil der linearen Hierarchie, kann sie als Stabsstelle gekennzeichnet werden.
- *Organisationseinheit*
  Die Planstelle ist der angezeigten Organisationseinheit zugeordnet.
- *Benutzer*
  Legt den der Planstelle zugeordneten Mitarbeiter fest.
- *Primäre Planstelle*
  Wenn ein Mitarbeiter mehreren Planstellen zugeordnet ist, kann eine Planstelle als primär markiert werden. Für die Auswertung des Vorgesetzten wird die primäre Planstelle herangezogen (z. B. im Workflow-Kontext).
- *Name*
  Definiert den Namen der Planstelle.

Hinweis:

- Über den Kontextmenübefehl „Planstelle verschieben“ können Sie die Planstelle innerhalb der Aufbauorganisation verschieben.
- Bei Verwendung der Fabasoft Personalakte stehen weitere Felder zur Verfügung.

4.11.4 Aufbauorganisation importieren

Wenn Sie sich in der Aufbauorganisation befinden, können Sie über die Aktion „Aufbauorganisation importieren“ die Aufbauorganisation mithilfe einer CSV-Datei importieren bzw. aktualisieren. Über die Schaltfläche „CSV-Vorlage herunterladen“ erhalten Sie eine Vorlage, die die nötige Datenstruktur beschreibt.

- Mithilfe der Option *Vollständiger Abgleich der Aufbauorganisation* können Sie festlegen, ob bestehende Planstellen und Organisationseinheiten, die nicht in der CSV-Datei vorhanden sind, gelöscht werden sollen.
- Mithilfe der Option *Aufbauorganisation nur aktualisieren* (nur sichtbar wenn *Vollständiger Abgleich der Aufbauorganisation* deaktiviert ist) können Sie festlegen, ob nur bestehende Planstellen und Organisationseinheiten aktualisiert werden. Es werden keine neuen Organisationselemente erzeugt.

Alternativ kann der Import auch über einen Eingangsordner erfolgen (Aktion „Daten importieren“, Import-Definition „Aufbauorganisation importieren“). Bei einem vollständigen Abgleich müssen Sie einen Benutzer angeben, der über den Workflow informiert wird, falls es zu löschende Organisationselemente gibt. Die Löschung erfolgt erst nach manueller Bestätigung.

Bei den CSV-Spalten handelt es sich im Allgemeinen um Freitextfelder vom Typ Zeichenkette. Mithilfe der Importkennung können Objekte aktualisiert werden. Folgende CSV-Spalten sind verfügbar:

CSV-Spalte	Feld	Möglicher Wert
`Key`	Importkennung	Zeichenkette
`Type`	-	Zeichenkette (`OrganizationalUnit`, `OrganizationalPosition`)
`ParentKey`	-	Zeichenkette (Importkennung der übergeordneten Organisationseinheit; leer auf oberster Ebene)
`Name`	Name	Zeichenkette
`Level`	Hierarchie-Ebene	Zeichenkette (Importkennung der Hierarchie-Ebene; nur bei Organisationseinheiten)
`StaffUnit`	Stabsstelle	Zeichenkette (`TRUE`, `FALSE`; nur bei Organisationseinheiten)
`UnitDescription`	Beschreibung	Zeichenkette (nur bei Organisationseinheiten)
`PositionType`	Typ	Zeichenkette (`HeadPos`, `StaffPos`; nur bei Planstellen)
`PrimaryPosition`	Primäre Planstelle	Zeichenkette (`TRUE`, `FALSE`)
`User`	Benutzer	Zeichenkette (Importkennung bzw. wenn nicht definiert die E-Mail-Adresse des internen Mitglieds; nur bei Planstellen)

Hinweis:

- Wenn Sie für ein bestehendes Organisationselement den Eintrag für `ParentKey` bzw. `Level` ändern, wird das Organisationselement entsprechend verschoben.
- Wenn die Fabasoft Personalakte lizenziert ist, können Sie weitere Metadaten importieren.

5 Lizenzverwaltung

Für die Verwendung Ihrer Lösung werden Lizenzen benötigt. Lizenzen können Sie in der gewünschten Anzahl erwerben und den Mitgliedern bzw. externen Mitgliedern Ihrer Organisation zuteilen. Die Zuteilung kann automatisch, manuell oder per Konfiguration erfolgen.

Für den Erwerb weiterer Lizenzen wenden Sie sich bitte an Fabasoft Cloud Support (cloudsupport@fabasoft.com).

5.1 Lösungen

Klicken Sie im Dashboard der Organisation auf *Lizenzen*, um die Lizenzverwaltung zu öffnen. Die in Ihrer Organisation verfügbaren Lizenzen werden als Liste dargestellt:

- Vollzugriff
  Ermöglicht den Vollzugriff (kann für Mitglieder und externe Mitglieder verwendet werden).
- Lesezugriff + Kommentieren
  Ermöglicht den Lesezugriff und das integrierte Kommentieren (kann für Mitglieder verwendet werden).
- Zugriff für externe Mitglieder
  Ermöglicht den Vollzugriff (kann für externe Mitglieder verwendet werden).
  Hinweis: Externe Mitglieder können unabhängig von der Lizenz keine der Organisation zugeordneten Teamrooms erzeugen.
- Zusätzliche Apps

Die Spalte *Zuordnung* zeigt die Art der Zuordnung an:

- „Manuell (Standard-Lösung für Mitglieder)", „Manuell (Standard-Lösung für externe Mitglieder)", „Manuell (Standard-Lösung für Mitglieder und externe Mitglieder)" bzw. „Manuell (Standard-App)"
  - Als Standard definierte Lösungen bzw. Apps werden neuen Mitgliedern automatisch zugeordnet. Organisationsadministratoren können die Lösungen bzw. Apps auch nachträglich zuordnen bzw. ändern.
  - Mindestens eine Lösung muss als Standard für Mitglieder bzw. externe Mitglieder definiert sein.
  - Pro Lösung kann eine Lizenzart als Standard für Mitglieder bzw. externe Mitglieder definiert sein.
- Manuell
  Bei manueller Zuordnung muss die Lösung bzw. App einem Mitglied explizit durch einen Organisationsadministrator zugeordnet werden.
- Konfiguriert
  Diese Apps bieten verschiedenartige Einstellungsmöglichkeiten und Rollen und werden deshalb mittels einer separaten Konfiguration verwaltet. Eine Änderung der Zuordnungsart ist nicht möglich.
- Volumenbasiert
  Um diese Apps nutzen zu können, ist eine volumenbasierte Lizenz nötig, die gesondert erworben werden muss.
- Gratis
  Gratis-Apps bieten folgende Zuordnungsarten:
  - Gratis (deaktiviert)
    Die App steht niemanden zur Verfügung.
  - Gratis (Standard-App)
    Die App wird neuen Mitgliedern automatisch zugeordnet.

- Gratis (manuell)
  Die App muss explizit durch einen Organisationsadministrator zugeordnet werden.

Über die Kontextmenübefehle „Als Standard für Mitglieder verwenden“, „Aktivieren“ und „Deaktivieren“ können Sie die Art der Zuordnung ändern.

Navigieren Sie in die jeweilige Lösung oder App, um die Liste der lizenzierten Mitglieder einzusehen. Über die Aktion „Mitglieder hinzufügen“ können Sie die Mitglieder festlegen, die über eine Lizenz verfügen sollen. Über den Kontextmenübefehl „Lizenz entfernen“ können Sie die Lizenz wieder entziehen.

5.2 Lösungen zuordnen

Lösungen bzw. Apps mit manueller Zuordnung, können Sie den einzelnen Mitgliedern zuordnen.

1. Klicken Sie im Dashboard der Organisation auf *Mitglieder*, um die Mitgliederverwaltung zu öffnen.
2. Navigieren Sie zu dem gewünschten Mitglied.
3. Klicken Sie Im Kontextmenü des Mitglieds auf „Lösungen zuordnen“.
   - *Lösungen*
     Wählen Sie die Lösungen aus, die Sie dem Benutzer zuordnen möchten.
   - *Apps*
     Wählen Sie die Apps aus, die Sie dem Benutzer zuordnen möchten.
4. Klicken Sie auf „Zuordnen“.

Hinweis: Markieren Sie mehrere Mitglieder, um die Zuordnung gemeinsam durchzuführen.

6 Berichte

Die folgenden Berichte stehen zur Verfügung.

Infizierte Dokumente

Es wird regelmäßig ein Virenscan durchgeführt. Hier finden Sie eine Liste aller infizierten Dokumente Ihrer Organisation.

Fehlgeschlagene Hintergrundaufgaben

Hintergrundaufgaben werden genutzt, um Aktionen zu einem bestimmten Zeitpunkt auszuführen. Konnte eine Hintergrundaufgabe nicht erfolgreich ausgeführt werden (z. B. wenn das betroffene Objekt gesperrt ist), wird versucht die Hintergrundaufgabe später nochmals auszuführen. Nach zehn erfolglosen Versuchen wird die Hintergrundaufgabe suspendiert und nicht mehr automatisch ausgeführt. Über suspendierte Hintergrundaufgaben im Kontext einer App werden die App-Administratoren per E-Mail informiert. Ansonsten werden die Organisationsadministratoren per E-Mail informiert.

Sie können folgende manuelle Aktionen bei Hintergrundaufgaben durchführen:

- Nächste Ausführung festlegen (nur sichtbar, wenn Sie alle Rechte auf dem Objekt haben)
  Legt einen Zeitpunkt fest, zu dem die Hintergrundaufgabe erneut ausgeführt wird.
- Link versenden
  Die Hintergrundaufgabe kann einem Benutzer mit entsprechenden Rechten weitergeleitet werden.

- Löschen (nur sichtbar, wenn Sie alle Rechte auf dem Objekt haben)
  Löscht die Hintergrundaufgabe auf dem betroffenen Objekt. Somit wird diese nicht mehr ausgeführt.

Hinweis: Das Widget „Fehlgeschlagene Hintergrundaufgaben“ ist nur sichtbar, wenn mindestens eine fehlgeschlagene Hintergrundaufgabe vorhanden ist.

Berichte für ungenutzte Teamrooms

Über die Schaltfläche „Bericht erzeugen“ können ungenutzte Teamrooms ermittelt werden. Teamrooms gelten als ungenutzt, wenn sie vor der festgelegten Zeitspanne erzeugt und zuletzt geändert wurden und seitdem kein Zugriff stattgefunden hat. Die Zugriffe werden auf Basis des Audit-Logs ermittelt.

Über die Aktion „Teamroom-Administratoren zur Prüfung auffordern“ beim Bericht können Teamroom-Administratoren per E-Mail dazu aufgefordert, die ungenutzten Teamrooms zu prüfen und gegebenenfalls alte, nicht mehr benötigte Daten zu löschen.

Dazu stehen Teamroom-Administratoren über den Link in der E-Mail folgende Möglichkeiten zur Verfügung:

- Schaltfläche „Geprüft“ bzw. „Alle Teamrooms geprüft“
  Teamrooms können als „Geprüft“ markiert werden. Dabei kann ein Datum festgelegt werden, bis wann die Teamrooms von den Berichten auszunehmen sind (standardmäßig ein Jahr). Wird das Datum entfernt, wird der Teamroom für den nächsten Bericht wieder überprüft.
- Schaltfläche „Auflösen“
  Nicht mehr benötigte Teamrooms können direkt aufgelöst werden.

7 Erweiterte Einstellungen

Um zu den erweiterten Einstellungen zu gelangen, klicken Sie im Dashboard der Organisation auf *Erweiterte Einstellungen*.

7.1 Dashboard

Abhängig von Ihren Lösungen und Apps stehen folgende Bereiche zur Verfügung.

Übersicht

Zeigt die wichtigsten Daten zur Organisation. Durch einen Klick auf „Anzeigen“ gelangen Sie zu den Eigenschaften der Organisation.

App-Konfigurationen

Falls Apps, die auf App-Konfigurationen basieren, lizenziert sind, werden die entsprechenden App-Konfigurationen hier angezeigt. Navigieren Sie in die *App-Konfigurationen*, um weitere Konfigurationen anzulegen.

Zieldomänen für „Teamroom übertragen“

Zeigt die Zieldomänen an, in die Teamrooms übertragen bzw. publiziert werden können. Navigieren Sie in die *Zieldomänen für „Teamroom übertragen“*, um weitere Domänen anzulegen.

OAuth-Clients

OAuth-Clients werden zum Beispiel für die Teamroom-übertragen-Funktionalität benötigt. Wenn Sie eine Zieldomäne für das Übertragen von Teamrooms aktivieren, wird in der Zieldomäne automatisch ein OAuth-Client angelegt. Navigieren Sie in die *OAuth-Clients*, um manuell OAuth-Clients anzulegen.

Bei in der Organisation definierten OAuth-Clients kann festgelegt werden, ob die Verwendung bestätigt werden muss.

Mindbreeze InSpire Services

Mindbreeze InSpire Services können dazu genutzt werden, um Dokumente automatisch zu klassifizieren. Navigieren Sie in die *Mindbreeze InSpire Services*, um weitere Services anzulegen. Ist nur ein Service vorhanden, ist dies automatisch das Standard-Service. Wenn mehrere Services vorhanden sind, kann ein Service über den Kontextmenübefehl „Als Standard festlegen" als Standard-Service festgelegt werden. Dieses wird verwendet, wenn im jeweiligen Kontext kein Service explizit festgelegt wurde (der Fallback gilt nicht für einen App-Room-Kontext).

Sie können folgende Einstellungen festlegen:

- *Name*
  Der Name des Service.
- *Filterservice-URL*
  Die URL zum Mindbreeze InSpire Filterservice (z. B. `https://mbinspire.example.com:8443/filter/23401`).
- *Mandant*
  Das Mindbreeze InSpire Predictionservice ist mehrmandantenfähig. Falls ein Mandant angegeben ist, wird dieser verwendet.
  Hinweis: Im Mindbreeze Management Center muss in der Eigenschaft *Tenant ID Pattern* folgender Wert hinterlegt sein: `{{_FSCMINDBREEZE_1_1001_fscmbtenant}}`
- *Projekt*
  Innerhalb eines Mandanten können mehrere Projekte verwaltet werden. Falls ein Projekt angegeben ist, wird dieses verwendet.
  Hinweis: Im Mindbreeze Management Center muss in der Eigenschaft *Project ID Pattern* folgender Wert hinterlegt sein: `{{_FSCMINDBREEZE_1_1001_fscmbproject}}`
- *Bereich*
  Innerhalb eines Projekts können mehrere Bereiche verwaltet werden. Falls ein Bereich angegeben ist, wird das diesem Bereich zugeordnete Modell verwendet. Ansonsten wird das Standardmodell verwendet.
  Hinweis: Im Mindbreeze Management Center muss in der Eigenschaft *Scope ID Pattern* folgender Wert hinterlegt sein: `{{_FSCMINDBREEZE_1_1001_fscmbscope}}`
- *Authentifizierung*
  Legt die Art der Authentifizierung am Filterservice fest.
- *Stamm- und Zwischenzertifizierungsstellen*
  Definiert die Stamm- und Zwischenzertifizierungsstellen für die Validierung des SSL-Server-Zertifikats des Filterservice.
- *Feedback an Mindbreeze InSpire Service senden*
  Legt fest, ob Feedback zur Korrektheit der Klassifizierung an das Mindbreeze InSpire Service übermittelt werden soll. Dadurch kann die zukünftige Klassifizierung verbessert werden.

- *Eigenes Mindbreeze InSpire Service für Feedbacks*
  Legt fest, ob das Feedback an ein dediziertes Mindbreeze InSpire Service gesendet wird. Wenn aktiviert, können die Daten (*Filterservice-URL*, *Mandant*, *Projekt*, *Bereich*, *Authentifizierung*) für das eigene Mindbreeze InSpire Service festgelegt werden.
- *Eigenes Mindbreeze InSpire Service für Trainingsdaten*
  Legt fest, ob die Trainingsdaten an ein dediziertes Mindbreeze InSpire Service gesendet werden. Wenn aktiviert, können die Daten (*Filterservice-URL*, *Mandant*, *Projekt*, *Bereich*, *Authentifizierung*) für das eigene Mindbreeze InSpire Service festgelegt werden.
- *Softwarekomponenten-Präfixe für die Zuordnung von Fabasoft Cloud Schlüsseln*
  Falls im Feld *Schlüssel-Zuordnung* keine vollständige Referenz angegeben wird, wird versucht, die Eigenschaft über die hier angegebenen Softwarekomponenten (z. B. `COOTC@1.1001`) zu ermitteln.
- *Schlüssel-Zuordnung*
  Falls die in Mindbreeze InSpire definierten Schlüssel nicht mit den Schlüsseln in der Fabasoft Cloud übereinstimmen, können entsprechende Abbildungen definiert werden. Als Schlüssel in der Fabasoft Cloud wird die Referenz der jeweiligen Eigenschaft herangezogen (z. B. `COOTC_1_1001_objcategory` für die Eigenschaft *Kategorie*). Im Fall von benutzerdefinierten Formularen wird der Programmiername der Eigenschaft als Schlüssel herangezogen.
  Bei Verwendung von kurzen Referenzen (z. B. `objcategory`), muss die entsprechende Softwarekomponente im Feld *Softwarekomponenten-Präfixe für die Zuordnung von Fabasoft Cloud Schlüsseln* angegeben sein.

Wenden Sie sich gegebenenfalls an den Mindbreeze InSpire Support um die konkreten Einstellungen zu treffen.

Feiertagstabellen

Feiertagstabellen ermöglichen die Definition von Feiertagen und Zeitspannen. Feiertage werden zum Beispiel im Workflow, Zeitspannen werden zum Beispiel bei Wiedervorlagen berücksichtigt.

Standardmäßig stehen Feiertagstabellen für Österreich, Deutschland und der Schweiz zur Verfügung. Falls im Feld *Feiertagstabelle* von App-Konfigurationen, App-Rooms bzw. Teamrooms keine bestimmte Feiertagstabelle ausgewählt wurde, wird die als Standard festgelegte Feiertagstabelle verwendet (Kontextmenübefehl „Als Standard festlegen“).

Über die Aktion „Feiertagstabelle erzeugen“ kann eine neue Feiertagstabelle angelegt werden. Gegebenenfalls kann auch eine bestehende Feiertagstabelle dupliziert werden.

Feiertage können über die Aktion „Feiertag erzeugen“ bzw. „Feiertage importieren“ erzeugt werden. Beim Import kann über die Schaltfläche „CSV-Vorlage herunterladen“ eine Beispiel-CSV-Datei heruntergeladen werden. Alternativ können auch die vom Produkt mitgelieferten Feiertagstabellen als CSV-Dateien heruntergeladen werden (Eigenschaften > Feld *Feiertage (CSV-Datei)*).

Zeitspannen können in den Eigenschaften der Feiertagstabelle im Feld *Zeitspannen* angelegt werden.

7.2 Kontaktdaten festlegen

Sie können die Adressen, Telefonnummern und E-Mail-Adressen Ihrer Organisation festlegen. Wenn Sie eine E-Mail-Adresse als Rechnungsadresse hinterlegen, werden Rechnungen von Online-Käufen an diese E-Mail-Adresse gesendet (anstatt an die E-Mail-Adresse des Zahlungspflichtigen). Um die E-Mail-Domänen für Ihre Organisation zu hinterlegen, wenden Sie sich bitte an den Fabasoft Cloud Support, da diese verifiziert werden müssen. Zum Beispiel werden Benutzer mit

einer E-Mail-Adresse, die einer Ihrer E-Mail-Domänen entspricht, als Mitglieder erkannt. Der Firmenname und die UID-Nummer können nur geändert werden, solange die Organisation nicht von Fabasoft überprüft und als vertrauenswürdig eingestuft wurde. Wenden Sie sich bitte an den Fabasoft Cloud Support, falls Änderungen erforderlich sind.

Um die Kontaktdaten festzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard der Organisation auf *Erweiterte Einstellungen*.
2. Klicken Sie auf die Aktion „Kontaktdaten festlegen".
3. Geben Sie die gewünschten Daten ein.
4. Klicken Sie auf „Speichern".

7.3 Logo festlegen

Um die Logos festzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard der Organisation auf *Erweiterte Einstellungen*.
2. Klicken Sie auf die Aktion „Logo festlegen".
3. Laden Sie die Logos hoch oder wählen Sie bestehende Logos aus. Überschreitet ein Logo die maximale Darstellungsgröße, wird es automatisch entsprechend verkleinert dargestellt.
   Hinweis: Das *Logo* wird ebenfalls in der Kopfleiste angezeigt, falls kein eigenes *Logo für die Kopfleiste* definiert wurde.
4. Laden Sie ein Hintergrundbild für den Home-Bereich hoch.
5. Geben Sie gegebenenfalls eine Hintergrundfarbe für die Kopfleiste (Hexadezimalwert, z. B.: #FF0000) an. Die Farben der Elemente in der Kopfleiste werden automatisch an die Hintergrundfarbe angepasst.
   Hinweis: Wenn Sie eine Hintergrundfarbe definieren, werden die Hintergrundfarbe und das Logo auch auf den Anmeldeseiten berücksichtigt. Wenn Sie keine Hintergrundfarbe definieren, wird die Kopfleiste grau dargestellt, da die meisten Logos für einen hellen Hintergrund ausgelegt sind.
6. Aktivieren Sie die Option *Logo in E-Mails verwenden*, um das Logo bzw. Logo für die Kopfleiste und die Hintergrundfarbe auch in den über die Cloud versendeten E-Mails Ihrer Organisation zu berücksichtigen.
7. Aktivieren Sie die Option *Logo und Hintergrundfarbe im Support-Dialog verwenden*, um das Logo bzw. Logo für die Kopfleiste und die Hintergrundfarbe im Support-Dialog für organisationsinterne Support-Anfragen zu verwenden.
8. Klicken Sie auf „Speichern".

7.4 Richtlinien festlegen

Sie können für Ihre Organisation zentral Richtlinien und Standardeinstellungen für Ihre Mitglieder festlegen. Somit können Sie auf effiziente Weise eine einheitliche Benutzererfahrung sicherstellen.

Um die Richtlinien festzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard der Organisation auf *Erweiterte Einstellungen*.
2. Klicken Sie auf die Aktion „Richtlinien festlegen".
3. Wechseln Sie auf die gewünschte Registerkarte und legen Sie Ihre Richtlinien fest. Nähere Informationen finden Sie in den folgenden Kapiteln.

4. Klicken Sie auf „Speichern“.

7.4.1 Registerkarte „Aktionen“

Legen Sie fest, welche Organisationsmitglieder berechtigt sind folgende Aktionen auszuführen:

- *Das Erzeugen von Teamrooms für jede Datenlokation getrennt erlauben*
  Legt fest, ob die Richtlinie *Teamrooms erzeugen* für alle Datenlokationen gemeinsam oder für die Datenlokationen einzeln definiert werden kann.
- *Teamrooms erzeugen* (alle Lokationen bzw. pro Datenlokation)
  Legt die Mitglieder fest, die einen Teamroom erzeugen dürfen.
- *Home-Bereich verwalten*
  Legt die Mitglieder fest, die Ihren Home-Bereich verwalten dürfen. Mitglieder, die den Home-Bereich verwalten dürfen, können Objekte auf Home ablegen bzw. entfernen.
- *Teamrooms übertragen*
  Legt die Mitglieder fest, die Teamrooms transferieren bzw. publizieren dürfen.
- *Formulare und Kategorien bearbeiten*
  Legt die Mitglieder fest, die Formulare und Kategorien erzeugen, bearbeiten und freigeben dürfen.
- *BPMN-Prozessdiagramme bearbeiten*
  Legt die Mitglieder fest, die BPMN-Prozessdiagramme erzeugen, bearbeiten und freigeben dürfen.
- *Eingangsordner-Regeln verwalten*
  Legt die Mitglieder fest, die Regeln für Eingangsordner erzeugen und bearbeiten dürfen.
- *Suchordner für Audit-Logs verwenden*
  Legt die Mitglieder fest, die Auditlogs einsehen dürfen.
- *Synchronisierungsart*
  Legt fest, auf welche Art der Cloud Ordner für die Synchronisierung mit dem Dateisystem von den Mitgliedern genutzt werden kann („Keine Synchronisierung“, „Synchronisierter Ordner“, „Synchronisierter Schreibtisch oder synchronisierter Ordner“).
  Keine Synchronisierung: Sie können verhindern, dass Mitglieder Ihre Daten mit dem Dateisystem synchronisieren.
  Synchronisierter Schreibtisch: Die Mitglieder können ihr gesamtes „Home“ synchronisieren.
  Synchronisierter Ordner: Die Daten im synchronisierten Ordner der Mitglieder werden synchronisiert.

Hinweis:

- Externen Mitgliedern stehen diese Aktionen grundsätzlich nicht zur Verfügung.
- Beim Organisationsmitglied finden Sie auf der Registerkarte „Administration“ die Einschränkungen, die diesen Benutzer betreffen. Wurde bei der Organisation „Ausführbar von allen Mitgliedern außer“ oder „Ausführbar von niemandem außer“ eingestellt, können auch hier die Einschränkungen für diesen Benutzer geändert werden. Wird eine Richtlinie über ein Team definiert, ist diese beim Benutzer nicht änderbar.

7.4.2 Registerkarte „Mitgliederverwaltung“

Legen Sie Einstellungen für die Mitgliederverwaltung fest.ö

- *Mitglieder zur Organisation hinzufügen*
  Legt die Mitglieder fest, die neue Mitglieder zur Organisation hinzufügen dürfen. Es können nur Mitglieder hinzugefügt werden, deren E-Mail-Adresse einer der E-Mail-Domänen der Organisation entspricht.
- *Externe Mitglieder zur Organisation hinzufügen*
  Legt die Mitglieder fest, die neue externe Mitglieder zur Organisation hinzufügen dürfen.
- *Mitglieder von der Organisation entfernen*
  Legt die Mitglieder fest, die Mitgliedschaften von Mitgliedern beenden dürfen.
- *Externe Mitglieder von der Organisation entfernen*
  Legt die Mitglieder fest, die Mitgliedschaften von externen Mitgliedern beenden dürfen.
- *Aufbauorganisation verwalten*
  Legt die Mitglieder fest, die die Aufbauorganisation verwalten dürfen.
- *Externe Organisationen verwalten*
  Legt die Mitglieder fest, die externe Organisationen verwalten dürfen.
- *Teams verwalten*
  Legt die Mitglieder fest, die Teams verwalten dürfen.

7.4.3 Registerkarte „Inhalt“

Legen Sie Einstellungen zu den erlaubten Inhalten fest.

- *Blockierte Dateitypen*
  Geben Sie pro Zeile eine nicht erlaubte Dateiendung an. Dateien mit diesen Dateiendungen können nicht hochgeladen werden.
- *Blockierte Dateitypen auch in ZIP-Archiven überprüfen*
  Legt fest, ob die Dateitypen auch in ZIP-Archiven überprüft werden.
- *Maximale Dateigröße (in MB)*
  Dateien können nur hochgeladen werden, wenn die Dateigröße den angegebenen Wert nicht überschreitet.
- *Maximale Anzahl der aufbewahrten Versionen*
  Bei einer Änderung von Objekten wird eine Version erstellt. Hier können Sie festlegen, wie viele Versionen maximal aufbewahrt werden.
- *Unterschriftenarten mit zusätzlicher Passwortabfrage (konform zu FDA 21 CFR Part 11)*
  Ermöglicht eine zusätzliche Passwortabfrage beim Anbringen einer in dieser Richtlinie definierten Unterschrift.
- *Office-Dokumente in Microsoft Office for the Web bearbeiten*
  Legen Sie die Benutzer fest, die Ihrer Organisation zugeordnete Dokumente mit Microsoft Office for the Web öffnen dürfen.
  Beachten Sie, dass Microsoft Office for the Web ein Service von Microsoft ist und daher die Verwendung den Nutzungsbedingungen und der Privacy Policy von Microsoft unterliegt. Um eine Datei anzeigen bzw. bearbeiten zu können, erstellt Office for the Web eine temporäre Kopie dieser Datei auf Office-for-the-Web-Servern.
  Wenn Sie verhindern möchten, dass Dokumente auf einen Office-for-the-Web-Server übertragen werden, wählen Sie den Eintrag „Niemandem“ aus.
- *Inhalte am Endgerät öffnen bzw. herunterladen*
  Legt fest, wer für Inhalte Ihrer Organisation die Aktionen bzgl. Bearbeiten und Herunterladen im Webbrowser-Client angeboten bekommt. Zusätzlich können Teamrooms und die

zugeordneten Objekte nicht dupliziert werden.
Zum Beispiel können Sie festlegen, dass niemand außer Organisationsmitglieder über diese Aktionen verfügen.

- *Inhalte über ein Netzlaufwerk (WebDAV) öffnen*
  Legt fest, wer auf die Inhalte Ihrer Organisation über ein Netzlaufwerk (WebDAV) zugreifen darf. Ist der Zugriff nicht erlaubt, werden die gängigen WebDAV-Clients blockiert.
- *Herunterladen von Inhalten über öffentliche Links blockieren*
  Wenn aktiviert, wird organisationsweit die Schaltfläche „Herunterladen" bei öffentlichen Links nicht angezeigt. Andernfalls kann beim Teamroom bzw. beim öffentlichen Link festgelegt werden, ob die Schaltfläche „Herunterladen" angezeigt wird.
- *Push-Benachrichtigungen für Ereignisse erlauben*
  Legt fest, ob Push-Benachrichtigungen für Ereignisse versendet werden. Falls das betroffene Objekt einer anderen Organisation zugeordnet ist, muss auch in dieser Organisation *Push-Benachrichtigungen für Ereignisse erlauben* aktiviert sein, damit die Push-Benachrichtigung versendet wird.
- *Erlaubte Mitglieder in Teamrooms*
  Standardmäßig können Benutzer, Teams und Organisationen in Teamrooms berechtigt werden. Sie können die erlaubten Mitglieder auf Teams und Organisationen einschränken.

7.4.4 Registerkarte „Teamroom"

Legen Sie die Standard-Sicherheitseinstellungen für neue Teamrooms der Organisation fest.

- *Zugriffsschutz*
  Legt fest, ob nur das festgelegte Team auf den Teamroom zugreifen darf oder jeder den Teamroom lesen aber nicht danach suchen darf.
- *Verknüpfungen im Teamroom einschränken*
  Definiert welche Art von Verknüpfungen im Teamroom abgelegt werden dürfen. Sie können die erlaubten Verknüpfungen auf Objekte, die der Organisation zugeordnet sind bzw. auf Objekte, die dem Teamroom zugeordnet sind, einschränken. Somit kann zum Beispiel verhindert werden, dass Verknüpfungen abgelegt werden, auf die die Mitglieder des Teamrooms keinen Zugriff haben.
- *Herunterladen bzw. Öffnen von Inhalten am Endgerät einschränken*
  Ermöglicht die Teammitglieder einzuschränken, die Inhalte am Endgerät öffnen bzw. herunterladen dürfen.
- *Rollen, die Inhalte am Endgerät öffnen bzw. herunterladen dürfen*
  Definiert über welche Berechtigungen ein Teammitglied verfügen muss, damit das Teammitglied Inhalte am Endgerät öffnen bzw. herunterladen darf.
- *Leseberechtigte Teammitglieder für alle Mitglieder sichtbar*
  Legt fest, ob alle Teammitglieder die leseberechtigten Mitglieder des Teams sehen dürfen. Wird die Einstellung deaktiviert, sind die leseberechtigten Teammitglieder nur für Mitglieder mit „Allen Rechten" sichtbar. Beachten Sie, dass durch das Deaktivieren dieser Einstellung auch weitere Anwendungsfälle eingeschränkt werden:
  - Nur Teammitglieder mit „Allen Rechten" steht die Aktion „Team" zur Verfügung und können Prozesse starten.
  - Neuigkeiten können für Teammitglieder, die nicht das Team sehen dürfen, generell deaktiviert werden. Ansonsten werden nur Neuigkeiten angezeigt, die keine Rückschlüsse auf Teammitglieder mit Leserechten zulassen.

- Teammitglieder mit Leserechten können keine Anmerkungen, Unterschriften, Prozesse verwenden und keine Newsfeeds kommentieren.
- Teammitglieder mit Leserechten können nicht als Teilnehmer in Prozessen ausgewählt werden.
- Teammitglieder mit Leserechten können keine öffentlichen Links erstellen.

- *Neuigkeiten für Benutzer ohne Rechte das Team einzusehen anzeigen*
  Legt fest, ob Neuigkeiten für Teammitglieder, die nicht das Team sehen dürfen, generell deaktiviert sind. Ansonsten werden nur Neuigkeiten angezeigt, die keine Rückschlüsse auf Teammitglieder mit Leserechten zulassen.
- *Alle Teammitglieder dürfen Mitglieder hinzufügen*
  Legt fest, ob alle Teammitglieder Benutzer zum Team hinzufügen dürfen oder nur Teammitglieder mit „Allen Rechten". Mitglieder mit Änderungsrechten dürfen anderen Mitgliedern Änderungsrechte bzw. Leserechte gewähren oder entziehen. Mitglieder mit Leserechten dürfen anderen Mitgliedern Leserechte gewähren oder entziehen.
- *Teammitglieder einschränken*
  Legt die Organisationen, Organisationseinheiten, Teams und externe Organisationen fest, deren Mitglieder zum Teamroom hinzugefügt werden dürfen. Falls die Liste keine Einträge enthält, können Mitglieder uneingeschränkt hinzugefügt werden.

7.4.5 Registerkarte „Schlüssel-Server"

Legen Sie Einstellungen bzgl. Schlüssel-Server fest.

- *Schlüssel-Server auswählen*
  Benutzer können beim Verschlüsseln einen Schlüssel-Server auswählen, wenn sie über die Organisationsrichtlinie dazu berechtigt wurden. Ansonsten wird der Standard-Schlüssel-Server automatisch verwendet.

7.4.6 Registerkarte „Prozesse"

Legen Sie Einstellungen bzgl. Prozesse fest.

- *Prozessadministratoren*
  Ein Prozessadministrator kann die Abläufe aller Prozesse in der Organisation überwachen und steuern.
- *Prozessstatistiken anzeigen für*
  Definiert für wen Prozessstatistiken angezeigt werden. Ein Prozessadministrator sieht die Statistiken für alle Prozesse in der Organisation. Ein Prozesseigentümer sieht die Statistiken der Prozesse für die er zuständig ist.
- *Intervall für die Berechnung der Prozessstatistiken*
  Definiert das Intervall für die Berechnung der Prozessstatistiken.
- *Nächste geplante Berechnung der Prozessstatistiken*
  Definiert wann die nächste Berechnung der Prozessstatistiken erfolgt.

7.4.7 Registerkarte „Authentifizierung"

Legen Sie Einstellungen bzgl. der Authentifizierung fest.

- *Einstellungen für die Anmeldesitzung*
  Definiert die Einstellungen für die Anmeldesitzung.

- *Gültigkeitsdauer*
  Definiert die maximale Gültigkeitsdauer einer Anmeldesitzung. Sie können einen Wert zwischen 2 Stunden und 3 Tagen wählen. Der Standardwert ist aktuell 16 Stunden.
- *Gültigkeitsdauer bei Inaktivität*
  Definiert die maximale Gültigkeitsdauer einer Anmeldesitzung bei Inaktivität des Benutzers. Sie können einen Wert zwischen 15 Minuten und 4 Stunden wählen. Der Standardwert ist aktuell 2 Stunden.
- *Wert für SameSite-Attribut des Sitzungs-Cookies*
  Legt den Wert des SameSite-Attributes des für die Anmeldesitzung verwendeten Webbrowser-Cookies fest. Mit dem Wert „Strict" bzw. „Lax" können Sie die Gefahr für Cross-Site-Request-Forgery (CSRF) reduzieren. Diese Werte schränken jedoch die Benutzerfreundlichkeit ein und es kann dazu führen, dass sich Benutzer häufiger anmelden müssen. Der Standardwert ist „Lax".
  Hinweis: Die Integration für Microsoft Teams und die Taskpane-Integration für Microsoft Office for the Web kann nur mit dem Wert „None" verwendet werden.

- *Vertrauenswürdige Netzwerke*
  Definiert IPv4-Adressen oder -Adressbereiche (in CIDR-Notation, z. B. 198.51.100.0/24) Ihrer vertrauenswürdigen Netzwerke, mit denen die Benutzer mit dem Internet kommunizieren. Dadurch kann z. B. die Bindung der Anmeldesitzung von einer IPv4-Adresse auf IPv4-Adressbereiche ausgedehnt werden.
- *Authentifizierungsmethoden, die keine Zwei-Faktor-Authentifizierung erfordern*
  Sie können festlegen, dass Single-Sign-on- bzw. Zertifikats-Authentifizierungsmethoden keinen zweiten Faktor benötigen. Wenn Sie den zweiten Faktor deaktivieren, muss Ihre IT-Abteilung durch geeignete Maßnahmen sicherstellen, dass das Authentisierungsniveau dennoch gegeben ist.
- *Dauerhafte Anmeldung*
  Definiert die Benutzer, die die dauerhafte Anmeldung nutzen können.
- *Gültigkeitsdauer für dauerhafte Anmeldungen*
  Definiert die maximale Zeitspanne, bis eine erneute explizite Anmeldung erforderlich ist.
- *Erlaubte Betriebssysteme für dauerhafte Anmeldungen*
  Definiert die Betriebssysteme, auf denen eine dauerhafte Anmeldung möglich ist.
- *Zertifizierungsstellen für Computerzertifikate für Microsoft Windows, Apple macOS und Ubuntu*
  Auf Endgeräten mit Microsoft Windows, Apple macOS bzw. Ubuntu ist aus Sicherheitsgründen eine dauerhafte Anmeldung nur möglich, wenn diese mit einem Computerzertifikat identifiziert werden können. Dadurch soll vermieden werden, dass Benutzer eine dauerhafte Anmeldung auf Endgeräten vornehmen, die nicht im Einflussbereich Ihrer Organisation liegen (z. B. auf privaten oder öffentlich genutzten Geräten). Legen Sie alle Zertifizierungsstellen fest, über die Computerzertifikate für Ihre Organisation ausgestellt werden, indem Sie die Zertifikate dieser Zertifizierungsstellen als CER-Datei im PEM-Format hochladen.
  Möchte ein Benutzer auf einem Endgerät eine dauerhafte Anmeldung vornehmen, wird geprüft, ob am Endgerät ein Computerzertifikat gefunden werden kann, das von einer der konfigurierten Zertifizierungsstellen für das Endgerät ausgestellt wurde. Dabei werden folgende Zertifikate herangezogen:
  - Microsoft Windows
    „Lokaler Computer" > „Eigene Zertifikate" > „Zertifikate"
    CN des Zertifikats: lokaler Hostname und Domänenname

- Apple macOS
  Standard-Schlüsselbund
  CN des Zertifikats: lokaler Hostname und Domänenname
- Ubuntu
  Netzwerkauthentifizierungszertifikat (802.1x)
  CN des Zertifikats: lokaler Hostname

- *Anmeldung mit OpenID Connect*
  Definiert Authentisierungseinstellungen für OpenID-Connect-Services.
  - *Gültigkeitsdauer*
    Definiert die maximale Gültigkeitsdauer für OpenID-Connect-Service-Sitzungen.
  - *Gültigkeitsdauer überschreiben*
    Überschreibt die maximale Gültigkeitsdauer von spezifischen OpenID-Connect-Services.

7.4.8 Standardeinstellungen

Auf den Registerkarten „Grundeinstellungen“, „Bedienungshilfen“, „Benachrichtigungen“, „Workflow“ und „Home“ können Sie Standardeinstellungen für Ihre Mitglieder festlegen. Zusätzlich können Sie definieren, ob diese von den Mitgliedern verändert werden dürfen. Über die Schaltfläche „Standardeinstellungen zurücksetzen“ können Sie die von Fabasoft vordefinierten Einstellungen wiederherstellen. In den Eigenschaften einzelner Mitglieder können Sie die Einstellungen auch individuell festlegen.

Hinweis:

- Wenn sich die Organisation ändert von der ein Benutzer verwaltet wird, werden die Standardeinstellungen der neuen Organisation für den Benutzer übernommen.
- Änderungen an den Standardeinstellungen wirken sich nur auf neue und nicht auf bestehende Mitglieder aus.
  Um geänderte Standardeinstellungen übernehmen zu können, steht der Kontextmenübefehl „Organisationseinstellungen übernehmen“ bei Benutzern, Teams, Organisationseinheiten, externen Organisationen und Organisationen zur Verfügung.

7.4.8.1 Registerkarte “Grundeinstellungen“

Legen Sie die Grundeinstellungen für Ihre Mitglieder fest. Benutzer finden die Einstellungen unter „Kontomenü (Benutzername)“ > „Grundeinstellungen“ > Registerkarte „Allgemein“.

Zusätzlich können Sie im Feld *Benutzern erlauben, die Datenlokation zu wechseln* festlegen, ob Benutzern ein Wechsel der Datenlokation ermöglicht werden soll. Wenn nicht, können Benutzer über das Datenlokationsmenü gegebenenfalls nur noch in die Standard-Datenlokation wechseln.

7.4.8.2 Registerkarte „Bedienungshilfen“

Legen Sie die Bedienungshilfen-Einstellungen für Ihre Mitglieder fest. Benutzer finden die Einstellungen unter „Kontomenü (Benutzername)“ > „Grundeinstellungen“ > Registerkarte „Bedienungshilfen“.

7.4.8.3 Registerkarte „Benachrichtigungen“

Legen Sie die Benachrichtigungs-Einstellungen für Ihre Mitglieder fest. Benutzer finden die Einstellungen unter „Kontomenü (Benutzername)“ > „Erweiterte Einstellungen“ > „Benachrichtigungen“ > Schaltfläche „Einstellungen“ > Registerkarte „Einstellungen“.

7.4.8.4 Registerkarte „Workflow“

Legen Sie die Workflow-Einstellungen für Ihre Mitglieder fest. Benutzer finden die Einstellungen unter „Kontomenü (Benutzername)“ > „Erweiterte Einstellungen“ > „Workflow“ > Registerkarte „Persönliche Einstellungen“.

7.4.8.5 Registerkarte „Home“

Legen Sie fest, welche Elemente auf Home für die Mitglieder der Organisation verfügbar sein sollen.

- *Verfügbare Elemente auf Home*
  Definiert welche Elemente auf Home verfügbar sind. Zusätzlich sind die Größe und Reihenfolge der Elemente definierbar.
- *Starten mit*
  Definiert ein auf Home verfügbares Element, das nach der Anmeldung initial angezeigt wird.
- *Weitere Elemente auf Home*
  Definiert weitere Elemente, die auf Home verfügbar sein sollen.
- *Organisationsverwaltung für Administratoren auf Home anzeigen*
  Legt fest, ob die Organisationsverwaltung den Administratoren der Cloud-Organisation auf Home angezeigt werden soll. Wenn Sie diese Option deaktivieren, können Administratoren nur ausgewählte Einstellungen über die Aktion "Einstellungen" eines persönlichen Dashboards einer App verwalten.

Ob Mitglieder ihren Home-Bereich selbst verwalten dürfen, können Sie über die Richtlinie „Home-Bereich verwalten“ festlegen (siehe Kapitel 7.4.1 ‚Registerkarte „Aktionen“').

7.4.9 Registerkarte „Fabasoft Cloud Client“

Legen Sie die Einstellungen für den Fabasoft Cloud Client für Organisationsmitglieder fest.

- *Zusätzlicher Beschreibungstext für die Installation des Fabasoft Cloud Enterprise Clients*
  Definiert einen mehrsprachigen Beschreibungstext, der im Webbrowserstatus angezeigt wird, wenn der Fabasoft Cloud Client nicht installiert oder nicht aktuell ist.
- *Link zum Fabasoft Cloud Enterprise Client im Softwarecenter*
  Ermöglicht Organisationsmitgliedern die Installation des Fabasoft Cloud Enterprise Clients über den Webclient aus Ihrem Microsoft Softwarecenter. Den entsprechenden Link finden Sie, wenn Sie im Softwarecenter zum Fabasoft Cloud Enterprise Client navigieren und auf die Schaltfläche „Freigeben“ rechts oben klicken.
  Hinweis: Der Link zum Fabasoft Cloud Enterprise Client im Softwarecenter muss nach jedem Update aktualisiert werden.
- *Link zum selbst bereitgestellten Fabasoft Cloud Enterprise Client*
  Definiert den Link zum Fabasoft Cloud Enterprise Client in einem alternativen Deployment-Werkzeug (kann eigenständig oder zusätzlich zum Softwarecenter-Link festgelegt werden).

- *Anzeigename für den Link zum selbst bereitgestellten Fabasoft Cloud Enterprise Client*
  Definiert den mehrsprachigen Anzeigenamen für den Link zum alternativen Deployment-Werkzeug.
- *Ausschließlich Versionen aus den Deployment-Tools bereitstellen*
  Legt fest, ob nur die Links zu den Deployment-Werkzeugen angezeigt werden.
  Hinweis: Wenn Sie diese Option nicht aktivieren, kann im Fehlerfall, z. B. wenn das Deployment-Werkzeug nicht erreichbar ist, der Fabasoft Cloud Client alternativ von der Cloud-Installation bezogen werden. Falls bereits ein Fabasoft Cloud Enterprise Client installiert ist, wird dieser für das Update heruntergeladen.
- *Link zum Fabasoft Cloud Enterprise Client anzeigen*
  Legt fest, ob im Webbrowserstatus der Link zum Fabasoft Cloud Enterprise Client angezeigt wird.
- Fabasoft Cloud Client Optionen
  Legt die Standardeinstellungen für den Fabasoft Cloud Client fest. Benutzer finden die Einstellungen unter „Kontomenü (Benutzername)“ > „Erweiterte Einstellungen“ > „Fabasoft Cloud Client“.

7.5 Anmeldeoptionen: Active Directory / SAML 2.0

Damit sich Mitglieder bzw. externe Mitglieder Ihrer Organisation über Active Directory bzw. SAML 2.0 anmelden können, müssen Sie die entsprechenden Anmeldeserver konfigurieren.

Konfiguration am Anmeldeserver

Führen Sie die im White Paper „Configuration of Single Sign-On“ beschriebenen Schritte durch:

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

Konfiguration in der Cloud-Organisation

Um die Konfiguration in der Cloud-Organisation durchzuführen, gehen Sie folgendermaßen vor:

1. Navigieren Sie in die erweiterten Einstellungen Ihrer Cloud-Organisation.
2. Klicken Sie auf die Aktion „Anmeldeoptionen“ > „Active Directory /SAML 2.0“.
3. Wählen Sie die Anmeldeart aus (Active Directory oder SAML 2.0) und laden Sie die Metadaten-XML-Datei Ihres Anmeldeservers hoch.
   Hinweis: Falls bereits ein Anmeldeserver konfiguriert ist, klicken Sie zuvor auf „Hinzufügen“.
4. Zusätzlich können Sie festlegen, ob für die Anmeldeart eine Zwei-Faktor-Authentifizierung erforderlich ist und ob Benutzer bei erstmaliger Anmeldung automatisch erzeugt werden sollen.
   Hinweis: Das automatische Erzeugen ist nur möglich, wenn die Benutzer, die auf der nächsten Seite angezeigte URL für die automatische Anmeldung verwenden.
5. Klicken Sie auf „Weiter“.
6. Geben Sie eine Kurzbezeichnung für den Anmeldeserver ein.
7. Geben Sie die E-Mail-Domänen an, die diesem Anmeldeserver zugeordnet werden sollen.
8. Sie können die angezeigte URL Ihren Benutzern zur Verfügung stellen, damit sich diese direkt über den Anmeldeserver anmelden können.
9. Legen Sie fest, ob die URL für die direkte Anmeldung über den Anmeldeserver auch bei versendeten Links verwendet werden soll.

10. Klicken Sie auf „Weiter“.

Hinweis:

- Wiederholen Sie die Schritte um zusätzliche Anmeldeserver hinzuzufügen.
- Bestehende Anmeldeserver können auch bearbeitet bzw. entfernt werden.
- Organisationsadministratoren erhalten im Welcome-Screen und per E-Mail eine Benachrichtigung, wenn das Metadaten-Zertifikat innerhalb der nächsten zwei Wochen abläuft bzw. abgelaufen ist.
- Wenn ein Benutzer automatisch erzeugt wird, wird dieser zum Mitglied, wenn die E-Mail-Domäne mit einer bei der Organisation hinterlegten E-Mail-Domänen übereinstimmt. Ansonsten wird der Benutzer zum externen Mitglied. Eine Änderung der E-Mail-Domänen der Organisation kann über den Fabasoft Cloud Support angefordert werden.

7.6 Anmeldeoptionen: Zertifikat

Damit sich Mitglieder Ihrer Organisation per Client-Zertifikat anmelden können, müssen Sie alle Zertifizierungsstellen, die Client-Zertifikate für Ihre Organisation ausstellen dürfen, als CER-Dateien im PEM-Format im entsprechenden Feld hinterlegen.

Zusätzlich müssen Sie für die ausstellenden Zertifizierungsstellen die übergeordneten Stamm- und Zwischenzertifizierungsstellen als CER-Dateien im PEM-Format im entsprechenden Feld angeben. Geben Sie für jede Stamm-, Zwischen- und ausstellende Zertifizierungsstelle die entsprechenden Zertifikatssperrlisten-URLs an. Sie können festlegen, ob eine Zwei-Faktor-Authentifizierung bei Zertifikatsanmeldung erforderlich ist.

Die CN der Zertifikate und die DN des Ausstellers dürfen keine Sonderzeichen enthalten.

Um die Konfiguration der Zertifikatsanmeldung für Ihre Organisation abzuschließen, müssen Sie noch für die Mitglieder Ihrer Organisation den Common Name des jeweiligen Benutzerzertifikats eintragen (siehe Kapitel 4.8 „Authentifizierung und zweiten Faktor festlegen“).

Hinweis: Sie können auch für externe Organisationen entsprechende Zertifikatseinstellungen treffen. Somit können sich Ihre externen Mitglieder auch über Zertifikate anmelden.

7.7 Anmeldeoptionen: RADIUS

Damit Ihre Organisationsmitglieder ein Einmal-Passwort über einen RADIUS-Server verwenden können, müssen Sie die Einstellungen des RADIUS-Servers bei Ihrer Organisation hinterlegen. Zusätzlich müssen Sie bei Ihren Organisationsmitgliedern die jeweilige *Benutzerkennung am RADIUS-Server* festlegen

Organisations-Einstellungen

Geben Sie den Rechnernamen und das Shared Secret des RADIUS-Servers an. Die Verbindung kann entweder über UDP (Port 1812) oder RadSec (Port 2083) erfolgen.

RADIUS-Server-Einstellungen

- In Ihrem RADIUS-Server müssen folgende IP-Adressen konfiguriert werden:
  - 194.247.47.120
  - 213.95.138.12
  - 46.140.135.213

- Ihr RADIUS-Server muss über einem der folgenden Ports erreichbar sein:
  - TCP/2083 (RadSec)
  - UDP/1812

Hinweis: Sie können auch für externe Organisationen entsprechende RADIUS-Einstellungen treffen. Somit können sich Ihre externen Mitglieder auch mit RADIUS anmelden.

7.8 SMTP-Einstellungen festlegen

Sie können einen eigenen SMTP-Server für E-Mails, die über die Fabasoft Cloud versendet werden, festlegen. Stellen Sie sicher, dass der definierte SMTP-Server für den Versand von E-Mails für die Domänen der angegebenen Absender-E-Mail-Adressen offiziell berechtigt ist (Sender Policy Framework).

7.9 Organisationsrollen festlegen

Über Organisationsrollen können Sie Benutzer festlegen, die für die Verwaltung der Organisation zuständig sind. Nähere Information zu den Rollen finden Sie im Kapitel 3 „Organisationsrollen“.

7.10 Verschlüsselung konfigurieren

Um Teamrooms mit Fabasoft Secomo verschlüsseln zu können, müssen Sie den Schlüssel-Server festlegen, der für die Verschlüsselung verwendet werden soll. Schlüssel, die beim Verschlüsselungsprozess generiert werden, werden von diesem Schlüssel-Server verwaltet.

Als Teil der initialen Konfiguration, werden Schlüssel für Ihre Organisation am Schlüssel-Server generiert. Nach Abschluss der Konfiguration steht die Verschlüsselungsfunktionalität zur Verfügung.

Hinweis:

- Wenn für Ihre Organisation mehrere Schlüssel-Server zur Verfügung stehen, können Sie den Standard-Schlüssel-Server festlegen.
- Mitglieder können beim Verschlüsseln einen Schlüssel-Server auswählen, wenn sie über die Organisationsrichtlinie dazu berechtigt wurden. Ansonsten wird der Standard-Schlüssel-Server automatisch verwendet.
- Wenn Sie über einen privaten Schlüssel-Server verfügen, können Sie in den Eigenschaften des Schlüssel-Servers im Feld *Berechtigte Organisationen* zusätzliche Organisationen hinterlegen, die Ihren Schlüssel-Server verwenden dürfen.

7.11 Digitale Signaturen konfigurieren

Um das digitale Signieren von Dokumenten mit eigenen Zertifikaten zu ermöglichen, müssen Sie die entsprechenden Zertifikate in Ihrer Organisation hinterlegen („Erweiterte Einstellungen“ > Aktion „Digitale Signaturen konfigurieren). Zusätzlich können Sie festlegen, welche Organisationsmitglieder mit den Zertifikaten digital signieren dürfen.

Neben Zertifikaten können Sie auch Stempel definieren. Klicken Sie dazu im Feld *Stempel* auf die Schaltfläche „Stempel hinzufügen“. Vergeben Sie einen Namen, legen Sie die Organisationsmitglieder fest, die den Stempel verwenden dürfen und laden Sie ein Bild als Stempel hoch.

Hinweis:

- Falls die Verwendung der hinterlegten X.509-Zertifikate eingeschränkt ist, wird eine der folgenden Verwendungsarten („Key Usage“) benötigt: „Digital Signature“ oder „Non Repudiation“.
- Zertifikate können über den Kontextmenübefehl „Aktualisieren“ aktualisiert werden. Organisationsadministratoren und Eigentümer erhalten im Welcome-Screen eine Benachrichtigung, wenn das Zertifikat innerhalb der nächsten zwei Wochen abläuft bzw. abgelaufen ist.
- Zertifikate können über den Kontextmenübefehl „Löschen“ gelöscht werden. Gelöschte Zertifikate können nicht mehr für das Signieren verwendet werden, bereits signierte Dokumente sind jedoch nicht betroffen.

8 Standard-Teamrooms

Als Organisationsadministrator können Sie bei Teams, externen Organisationen, Organisationseinheiten und bei der Organisation Standard-Teamrooms in der Organisationsablage hinterlegen. Die Standard-Teamrooms werden in den Organisationsablagen der jeweiligen Mitglieder angezeigt, die in den Teamrooms berechtigt sind.

Um einen Standard-Teamroom zu erzeugen, navigieren Sie im Dashboard der Organisation in den Bereich *Organisationsablage*. Über die Aktion „Teamroom erzeugen“ können Sie einen neuen Teamroom anlegen und in einem Schritt die Zugriffsrechte festlegen.

Hinweis:

- Neben Teamrooms können Sie auch Eingangsordner und Rooms mit Benutzerdaten als Standard-Teamrooms festlegen (z. B. Hintergrund-Kontextmenü „Neu“ > *Eingangsordner*).
- Die Organisationsablage von Teams, externen Organisationen und Organisationseinheiten finden Sie in deren Eigenschaften.
- Das Widget „Organisationsablage“ wird auf Home angezeigt, wenn Sie zumindest in einem Standard-Teamroom berechtigt sind. Über die Aktion „Neu“ können Sie zusätzliche Standard-Teamrooms für Teams, externe Organisationen, Organisationseinheiten bzw. für die Organisation erzeugen.

9 Weiterführende Verwaltungsmöglichkeiten

Folgende zusätzliche Verwaltungsmöglichkeiten stehen Ihnen zur Verfügung.

9.1 Benutzer anonymisieren

Aufgrund von rechtlichen Bestimmungen kann es notwendig sein, Benutzer zu anonymisieren. Anonymisieren bedeutet, dass der Benutzer im Organisationskontext in allen Verknüpfungen durch einen speziellen, für die Anonymisierung bereitgestellten Benutzer ersetzt wird. Eine derartige Verknüpfung ist zum Beispiel der im Feld *Erzeugt von* hinterlegte Benutzer bei einem beliebigen Objekt.

Das Anonymisieren umfasst auch gesicherte Versionen und Auditlog-Einträge. Abgeschlossene Dokumente und Dokumente mit Aufbewahrungsfrist sind jedoch von der Anonymisierung ausgenommen.

Mitgliedschaft beenden

Wenn Sie die Mitgliedschaft eines von Ihnen verwalteten Benutzers beenden, können Sie festlegen, ob der Benutzer deaktiviert werden soll. Beim Deaktivieren werden alle personenbezogenen Daten ausgenommen Vorname, Nachname und E-Mail-Adresse unwiderruflich gelöscht.

Anonymisieren durch einen Compliance-Manager

Die Compliance-Manager werden über die Organisationsrollen festgelegt. Wenn die Mitgliedschaft eines Benutzers beendet wird, werden die Compliance-Manager per E-Mail informiert. Die Compliance-Manager können den ausgetretenen Benutzer sofort anonymisieren, die Verknüpfungen mit dem Benutzer ermitteln oder eine Erinnerung für einen bestimmten Zeitpunkt definieren. Da die Anonymisierung bzw. das Ermitteln der Verknüpfungen eine gewisse Zeit in Anspruch nimmt, werden die Compliance-Manager über den Ausgang per E-Mail informiert.

Nach dem Ermitteln der Verknüpfungen können Compliance-Manager bei vorhandenen Zugriffsrechten die Verknüpfungen anzeigen bzw. die betroffenen Teamroom-Administratoren auffordern, die Verknüpfungen zu überprüfen. Über die Schaltfläche „Geprüft“ können die Teamrooms als geprüft markiert werden. Dabei muss angegeben werden, ob die Verknüpfungen nach Meinung der Teamroom-Administratoren anonymisiert werden dürfen. Nachdem alle Meinungen eingeholt wurden, kann der Compliance-Manager den Benutzer gegebenenfalls anonymisieren (Schaltfläche „Benutzer anonymisieren“).

Für Benutzer, die nicht mehr Mitglied der Organisation sind, können jederzeit über den Kontextmenübefehl „Benutzer anonymisieren“ die Anonymisierungs-Anwendungsfälle durchgeführt werden. Der Kontextmenübefehl kann auch auf der Organisation ausgeführt werden, um insbesondere Benutzer anonymisieren zu können, die zum Beispiel durch Zusammenarbeit in Teamrooms im Kontext der Organisation gearbeitet haben, aber nie Mitglieder waren.

Löschanfrage durch einen Benutzer

Geht bei Fabasoft eine Löschanfrage durch einen Benutzer ein, werden die Compliance-Manager der betroffenen Organisationen über die Löschanfrage informiert und zum Anonymisieren aufgefordert.

Löschen des Benutzers

Nachdem ein Benutzer in allen betroffenen Organisationen vollständig anonymisiert wurde, wird dieser automatisch gelöscht.

9.2 Alle Teamrooms auflösen

Achtung
Bevor Sie diesen Anwendungsfall ausführen, stellen Sie unbedingt sicher, dass Sie Ihre Daten nicht mehr benötigen. Dieser Schritt kann nicht rückgängig gemacht werden.

Als Eigentümer bzw. Miteigentümer haben Sie die Möglichkeit alle Teamrooms (inkl. App-Rooms und App-Konfigurationen) Ihrer Organisation aufzulösen und die enthaltenen Daten unwiderruflich zu löschen. Zusätzlich werden alle Objekte der Organisation mit dem Sicherheitskontext „ACL für Objekte ohne Teamroom“ gelöscht.

Zur Durchführung dieses Anwendungsfalls steht Ihnen auf Ihrer Organisation der Kontextmenübefehl „Erweitert“ > „Alle Teamrooms auflösen“ zur Verfügung.

9.3 Organisation deaktivieren und zurücksetzen

Achtung

Bevor Sie diesen Anwendungsfall ausführen, stellen Sie unbedingt sicher, dass Sie Ihre Daten nicht mehr benötigen. Dieser Schritt kann nicht rückgängig gemacht werden.

Als Eigentümer bzw. Miteigentümer haben Sie die Möglichkeit Ihre Organisation zu deaktivieren und zurückzusetzen. Dabei werden alle Mitgliedschaften beendet, alle Teams, Organisationseinheiten und externen Organisationen gelöscht und alle Einstellungen zurückgesetzt. Benutzer, die in keiner weiteren Organisation Mitglied bzw. externes Mitglied sind, werden deaktiviert (gilt auch für den Eigentümer).

Zur Durchführung dieses Anwendungsfalls steht Ihnen auf Ihrer Organisation der Kontextmenübefehl „Erweitert“ > „Organisation deaktivieren und zurücksetzen“ zur Verfügung.

Hinweis: Lösen Sie zuvor alle Teamrooms in allen Datenlokationen auf, um alle Ihre Daten zu löschen.

9.4 Neuigkeiten anzeigen

Damit die Nachvollziehbarkeit bei der Organisationsverwaltung gewährleistet ist, werden die entsprechenden Änderungen mitprotokolliert (z. B. Mitglied hinzugefügt oder Organisationsrolle zugewiesen). Um die Ereignisse anzuzeigen, navigieren Sie in Ihre Organisation und führen Sie die Aktion „Neuigkeiten anzeigen“ aus.

Über die Zeitreise gelangen Sie zu den Versionen, die bei den Änderungen erstellt wurden.

9.5 Teamroom-Nutzung anzeigen

Sie können sich einen detaillierteren Überblick über die Benutzer Ihrer Organisations-Teamrooms verschaffen. Die Auswertung kann auf Mitglieder eines Teams, einer Organisationseinheit, einer externen Organisation oder auf ein einzelnes (externes) Mitglied eingeschränkt werden.

1. Navigieren Sie zu dem gewünschten Organisationselement bzw. (externen) Mitglied.
2. Führen Sie den Kontextmenübefehl „Teamroom-Nutzung anzeigen“ aus.

Hinweis:

- Wenn Sie den Kontextmenübefehl auf einem Organisationselement ausführen, erhalten Sie zuerst eine Übersicht über die Teamrooms, in denen das Organisationselement berechtigt wurde. Über die Schaltfläche „Teamroom-Nutzung für Mitglieder anzeigen“ gelangen Sie zur Übersicht über die Mitglieder des Organisationselements.
- Über den Kontextmenübefehl „Details anzeigen“ erhalten Sie mehr Informationen zu dem jeweiligen Benutzer (z. B. Lösungen und Apps des Benutzers). Als Eigentümer/Miteigentümer sehen Sie zusätzlich die Teamrooms der Organisation, in denen der Benutzer Rechte besitzt. Sie können die Daten als CSV-Datei herunterladen.

9.6 Dauerhafte Anmeldung

Mithilfe einer Gerätebindung können Benutzer dauerhaft angemeldet bleiben (siehe auch Kapitel 7.4.7 „Registerkarte „Authentifizierung““). Über die Aktion „Endgeräte“ beim Organisationsmitglied können Sie ein dauerhaft angemeldetes Endgerät abmelden.

9.7 Datenschutzeinstellungen festlegen

Um Einstellungen bzgl. Datenschutz für Ihre Organisation festzulegen, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu Ihrer Organisation.
2. Klicken Sie im Kontextmenü der Organisation auf „Eigenschaften“.
3. Wechseln Sie auf die Registerkarte „Datenschutz“.
4. Geben Sie Ihre Daten ein.
   - *Vorname* und *Nachname*
     Definiert den Namen der Person, die bei Verletzung des Schutzes personenbezogener Daten benachrichtigt werden soll.
   - *Benachrichtigungsadresse*
     Legt die Postadresse bzw. E-Mail-Adresse für die Benachrichtigung fest.
   - *URL für datenschutzrechtliche Informationen*
     Der angegebene Link zu Ihren datenschutzrechtlichen Informationen wird im Registrierungsformular angezeigt.
5. Klicken Sie auf „Weiter“.

9.8 Vertrauenswürdige Netzwerke festlegen

Vertrauenswürdige Netzwerke werden z.B. bei der Validierung von cookiebasierten Benutzersitzungen verwendet. Im Zuge der Authentisierung wird zur Identifikation der Benutzersitzung ein Cookie ausgestellt. Dieses Cookie ist aus Sicherheitsgründen an das aktuelle Endgerät des Benutzers gebunden. Das Endgerät wird durch die IPv4-Adresse der Netzwerkverbindung identifiziert. Die Benutzersitzung wird ungültig, sobald sich die IPv4-Adresse ändert. In seltenen Fällen kann es vorkommen, dass die IPv4-Adresse trotz gleichbleibenden Endgeräts wechselt (z. B. wenn mehrere Proxies beteiligt sind oder die IPv4-Adresse des Endgeräts neu vergeben wird). In diesem Fall wird auch die Benutzersitzung ungültig und der Benutzer muss sich neu anmelden.

Durch die Definition sicherer Adressbereiche bleibt eine Benutzersitzung jedoch auch bei geänderter IPv4-Adresse gültig, sofern die neue IPv4-Adresse in dem konfigurierten Bereich liegt.

Um die vertrauenswürdigen Netzwerke für die Organisation festzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Dashboard Ihrer Organisation auf *Erweiterte Einstellungen*.
2. Klicken Sie auf die Aktion „Richtlinien festlegen“.
3. Wechseln Sie auf die Registerkarte „Authentifizierung“.
4. Geben Sie im Feld *Vertrauenswürdige Netzwerke* Ihre IPv4-Adressen bzw. Adressbereiche ein.
5. Klicken Sie auf „Weiter“.

Hinweis: Für externe Organisationen können auf der Registerkarte „Erweiterte Einstellungen“ vertrauenswürdige Netzwerke festgelegt werden.

9.9 Branding für die Organisation festlegen

Das Branding ermöglicht Ihnen personalisierte Teamrooms zu erstellen. Ist ein Branding bei einer Organisation hinterlegt, werden die Teamrooms mit diesem Branding vorinitialisiert. Das Branding ist sichtbar, wenn das Werkzeug „Branding“ eingeblendet ist.

Um das Branding für Ihre Organisation festzulegen, gehen Sie folgendermaßen vor:

1. Navigieren Sie in Ihre Organisation.
2. Öffnen Sie das Werkzeug „Branding“.
3. Aktivieren sie gegebenenfalls das Branding.
4. Klicken Sie unterhalb des Textes auf „Bearbeiten“.
5. Definieren Sie das Logo, den Titel und eine Kurzbeschreibung.
   Hinweis: Sie können die Beschreibung über den eingeblendeten HTML-Editor formatieren.
6. Klicken Sie auf „Speichern“.

Hinweis: Benutzer die über alle Rechte in einem Teamroom verfügen, können über das Werkzeug „Branding“ das Logo, einen Titel und eine formatierte Kurzbeschreibung für den jeweiligen Teamroom ändern.

9.10 E-Mail-Kommunikation

Um eine Übersicht über alle im Zuge von Organisations-Anwendungsfällen (Einladungen, Austritte usw.) versendeten E-Mails zu erhalten, werden Ihnen in den Eigenschaften der Organisation auf der Registerkarte „E-Mail-Kommunikation“ die entsprechenden E-Mails angezeigt.

9.11 Standard-Datenlokation festlegen

Damit alle Ihre Organisationsmitglieder standardmäßig in der gleichen Datenlokation arbeiten, können Sie diese in den Richtlinien Ihrer Organisation auf der Registerkarte „Grundeinstellungen“ im Feld *Standard-Datenlokation* festlegen. Um einzelnen Mitgliedern eine andere Standard-Datenlokation zuzuweisen, können Sie in den Eigenschaften des entsprechenden Benutzers auf der Registerkarte „Grundeinstellungen“ im Feld *Standard-Datenlokation* die Standard-Datenlokation ändern.

9.12 Überprüfung der Dateien auf Malware

Die Fabasoft Cloud verfügt über ein automatisiertes Malware-Scanning-Service mit dem in regelmäßigen Abständen die gespeicherten Dateien auf Malware geprüft werden. Dieses Service liefert im Falle einer entdeckten Infektion die eindeutige Fabasoft Cloud ID, den Erzeuger sowie die Eigentümer-Organisation der Datei. Die Teamroom-Administratoren werden über den Fund per E-Mail informiert. In der E-Mail befinden sich auch Links, über die die infizierten Dateien angezeigt werden können.

Es obliegt den Teamroom-Administratoren, wie die infizierten Dateien behandelt werden sollen. Fabasoft kann keine Bereinigung vornehmen, da Fabasoft keinen Zugriff auf die Dateien hat.

Wenn der Administrator der Cloud-Organisation keinen Zugriff auf die Datei hat, kann er entweder mit dem Erzeuger der Datei oder einem Eigentümer seiner Cloud-Organisation in Kontakt treten, um für eine Bereinigung der Datei zu sorgen. Es wird empfohlen, dass berechtigte Benutzer die infizierte Datei herunterladen und diese mit einer eigenen Virus-Scan-Software prüfen und

bereinigen. Die bereinigte Datei kann anschließend wieder hochgeladen werden. Alternativ können berechtigte Benutzer die infizierte Datei in der Fabasoft Cloud auch löschen.

Beachten Sie die Risiken beim Herunterladen infizierter Dateien auf Ihren Computer.

Das Malware-Scanning-Service läuft regelmäßig:

- Wöchentlich werden die Dateien, die in den letzten 31 Tagen hochgeladen wurden, geprüft.
- Monatlich werden alle Dateien geprüft.