univention
be open.

ICS app 1.0

Release 1.0

Univention GmbH

Aug 22, 2022

CONTENTS

Welcome to the documentation about the Univention **ICS** app. The app installs the Intercom Service, and intermediary for communication between applications like Nextcloud, OX and Synapse (Element). This program is required for the functionalities File-picker, Videoconference create and accessing the Univention-Portal navigation endpoint from other apps.

This documentation is for system administrators who operate the **ICS** app from Univention App Center connected to the LDAP directory in Univention Corporate Server (UCS). It covers the following topics:

1. *Overview* (page 9)
2. *Design decisions* (page 9)

This documentation doesn't cover the following topics:

- Usage of UCS (Univention Corporate Server), see *UCS 5.0 Manual* [1].

To understand this documentation, you need to know the following concepts and tasks:

- Use and navigate in a remote shell on Debian GNU/Linux derivative Linux distributions like UCS. For more information, see Shell and Basic Commands[1] from *The Debian Administrator's Handbook*, Hertzog and Mas [2].
- Manage an app through Univention App Center[2] in *UCS 5.0 Manual* [1].

Your feedback is welcome and highly appreciated. If you have comments, suggestions, or criticism, please send your feedback[3] for document improvement.

[1] https://www.debian.org/doc/manuals/debian-handbook/short-remedial-course.en.html#sect.shell-and-basic-commands
[2] https://docs.software-univention.de/manual/5.0/en/software/further-software.html#computers-softwareselection
[3] https://www.univention.com/feedback/?ics-app=generic

CHAPTER

ONE

INSTALLATION

You can install the **ICS** app like any other app with Univention App Center.

UCS offers two different ways for app installation:

- With the web browser in the UCS management system
- With the command-line

For general information about Univention App Center and how to use it for software installation, see Univention App Center[4] in *UCS 5.0 Manual* [1].

1.1 Installing this app has various prerequisites

1. ICS only supports OIDC, this means both *Nextcloud (>=23.0)* and *OX (>=7.10.6)* have to be authenticated via OIDC as well
2. For working CSRF protection all other Apps need to be up to date
3. ICS requires the "Nordeck"-Bot to be up an running for Matrix
4. ICS requires its four secrets to be provided before installation, see *Secrets* (page 5) for details
5. ICS requires correctly configured Keycloak (>=12.0), including a valid Intercom OIDC client before installation

   Create a new OIDC Client, the `Client ID` can be configured during ICS app installation, but by default you should use `intercom`, leave the `Root URL` empty and save.

   Select `Access Type` as `confidential`.

   Set `Service Accounts Enabled` and `Authorization Enabled` to `On`.

   Set `Service Accounts Enabled` and `Authorization Enabled` to `On`.

   Set `Backchannel Logout URL` to your intended ICS-domain with protocol and append the ICS backchannel logout path (requires Keycloak >=12.0.0), for example:

   ```
   https://ics.example-domain.example-tld/backchannel-logout
   ```

   Set the valid redirect URL to your intended ICS-domain with protocol and append the ICS callback path `/callback`, for example:

   ```
   https://ics.example-domain.example-tld/callback
   ```

   Go to the Tab *Credentials*, copy the secret and save it to `/etc/intercom-client.secret`.

[4] https://docs.software-univention.de/manual/5.0/en/software/app-center.html#software-appcenter

1.2 Installation with the web browser

To install ICS from the UCS management system, use the following steps:

1. Use a web browser and sign in to the UCS management system.
2. Open the *App Center*.
3. Select or search for *ICS* and open the app with a click.
4. To install ICS, click *Install*.
5. Leave the *App settings* in their defaults or adjust them to your preferences. For a reference, see *Settings* (page 6).
6. To start the installation, click *Start Installation*.

Note: To install apps, the user account you choose for login to the UCS management system must have domain administration rights, for example the username `Administrator`. User accounts with domain administration rights belong to the user group `Domain Admins`.

For more information, see Delegated administration for UMC modules[5] in *UCS 5.0 Manual* [1].

1.3 Installation with command-line

To install the **`ICS`** app from the command-line, use the following steps:

1. Sign in to a terminal or remote shell with a username with administration rights, for example `root`.
2. Choose between default and custom settings and run the appropriate installation command.

   For installation with default settings, run:

   ```
   $ univention-app install ics
   ```

   To pass customized settings to the app during installation, run the following command:

   ```
   $ univention-app install --set $SETTING_KEY=$SETTING_VALUE ics
   ```

   Caution: Some settings don't allow changes after installation. To overwrite their default values, set them before the installation. For a reference, see *Settings* (page 6).

   Example: To define a different administration user in ICS, run:

   ```
   $ univention-app install --set OPTION=VALUE
   ```

[5] https://docs.software-univention.de/manual/5.0/en/central-management-umc/delegated-administration.html#delegated-administration

CHAPTER

TWO

CONFIGURATION

The **ICS** app offers various configuration options. Some settings don't allow changes after installation. Therefore, you must set them carefully **before** installation. You find those settings marked with *Only before installation* in *Settings* (page 6). You can change all other settings at any time after the installation.

To change settings after installation, sign in to the UCS management system with a username with administration rights and go to *App Center ▸ ICS ▸ Manage Installation ▸ App Settings*. On the appearing *Configure ICS* page, you can change the settings and apply them to the app with a click on *Apply Changes*.

The App Center then *re-initializes* the Docker container for the ICS app. *Reinitialize* means the App Center throws away the running ICS Docker container and creates a fresh ICS Docker container with the just changed settings.

2.1 ICS

The **ICS** app provides the backend for inter-app communication of Nextcloud, the Portal, UMC, Synapse (Nordeck) and OX.

> **Warning:** This app does not configure any Keycloak settings, it requires an existing client and realm setup in Keycloak.

Note: This documentation may refer to an IdP or OIDC in general, but UCS currently only supports Keycloak.

2.2 Secrets

The ICS app requires secrets, that are not currently automatically generated. Those secrets are:

/etc/intercom-client.secret
: The client secret for authenticating with the IdP. This client secret can be retrieved from the Keycloak admin console in the *Authorization*-tab of the intercom-client.

/etc/intercom.secret
: This secret is an internal secret for the Node-server running intercom. I can be freely chosen.

```
pwgen -s 30 > /etc/intercom.secret
```

/etc/matrix.secret
: The secret for backend-communication with the Matrix server. It can be retrieved from the auto-join-app-service on the system running Matrix (MAV).

```
kubectl exec --stdin --tty synapse-0 -n matrix-000-prod -- \
      /bin/bash -c "cat /data/autojoin-appservice.yaml | \
      grep as_token | \
      sed -e 's/as_token. \(.\+\)/\1/'"
```

/etc/portal.secret
The secret to communicate with the Univention-Portal navigation service. Usually this can be retrieved from `/etc/portal-navigation-service.secret`.

2.3 Settings

The following references show the available settings within the **ICS** app. Univention recommends to keep the default values.

intercom/settings/client-id
Defines the OIDC client name of ICS in Keycloak. The file `/etc/ics_client.secret` stores the secret of this client.

Required	Default value	Set
Yes	`intercom`	Only before installation

intercom/settings/intercom-url
Defines the fully qualified URL with protocol, on which ICS is reachable. This needs to be a externally reachable address as it's used by the browser to connect to ICS.

Required	Default value	Set
Yes	`https://ics.@%@domainname@%@`	Only before installation

intercom/settings/base-url
Defines the base-URL used to identify with the IdP. Accordingly this URL must match the base URL set in the OIDC client used on the IdP. Usually this should be the same as *intercom/settings/intercom-url*.

Required	Default value	Set
Yes	`https://ics.@%@domainname@%@`	Only before installation

intercom/keycloak/url
URL of the Keycloak instance to be used as the IdP. This value is ignored if *intercom/settings/issuer-base-url* is set.

Required	Default value	Set
Yes	`https://id.@%@domainname@%@`	Only before installation

intercom/keycloak/realm-name
Name of the realm containing the configured OIDC Intercom client. This value is ignored if *intercom/settings/issuer-base-url* is set.

Required	Default value	Set
Yes	`UCS`	Only before installation

intercom/settings/issuer-base-url
Defines a full base URL for the OIDC token issuer. This variable overwrites *intercom-service/keycloak/url* and *intercom-service/keycloak/realm-name*. Only set this variable if you really need to change the default URL generated from the before mentioned variables, this should not be necessary on normal setups.

Required	Default value	Set
No	`None`	Only before installation

intercom/settings/origin-regex
Defines the origin CORS regex. Normally this will be the shared domain name. Changing this value may have security implications.

Required	Default value	Set
Yes	`@%@domainname@%@`	Only before installation

intercom-service/settings/proxy
This setting is passed to node-axios within the container, it allows or disallows connections via proxy server instead of connection to the backends directly.

Required	Default value	Set
Yes	`False`	Only before installation

intercom/matrix/url
Defines the URL on which the Matrix server is reachable. The file `/etc/ics_matrix_as.secret` stores the matrix secret.

Required	Default value	Set
Yes	`https://matrix.` `@%@domainname@%@`	Only before installation

intercom/matrix/server-name
Defines the server name of the matrix server. The matrix server name is a unique identifier set in matrix, it is not necessarily the server name defined in *intercom/matrix/url*.

Required	Default value	Set
Yes	`matrix.@%@domainname@%@`	Only before installation

intercom/matrix/login-type
Defines the login-type ICS should use on the matrix server. Refer to the Matrix documentation for more information about login types. Normally the default value will be the correct setting.

Required	Default value	Set
Yes	`uk.half-shot.msc2778.login.` `application_service`	Only before installation

intercom/matrix/nordeck-mode
Defines the connection mode of the Nordeck-bot.

Possible values `test`, `live`, `test proxies`.

For more information refer to the Nordeck documentation.

Required	Default value	Set
Yes	`test`	Only before installation

intercom/matrix/nordeck-url
Defines the URL on which Nordeck-bot is listening.

Required	Default value	Set
Yes	`https://meetings-widget-bot.@%@domainname@%@`	Only before installation

intercom/portal/portal-url
Defines the URL on which the Univention-Portal is listening. The file `/etc/ics_portal.secret` stores the Portal API key.

Required	Default value	Set
Yes	`@%@ucs/server/sso/fqdn@%@`	Only before installation

intercom/ox/ox-origin
Defines the OX CORS origin setting. Usually this will be the same as the OX external address.

Required	Default value	Set
Yes	`https://webmail.@%@domainname@%@`	Only before installation

intercom/ox/ox-audience
Defines the OIDC audience settings for the OX token request send to the IdP

Required	Default value	Set
Yes	`oxoidc`	Only before installation

intercom-service/nextcloud/url
Defines the URL on which Nextcloud is listening on.

Required	Default value	Set
Yes	`https://fs.@%@domainname@%@`	Only before installation

intercom-service/nextcloud/origin
Defines the Nextcloud CORS origin. Usually this will be the same as *intercom-service/nextcloud/url*.

Required	Default value	Set
Yes	`https://fs.@%@domainname@%@`	Only before installation

CHAPTER

THREE

ARCHITECTURE

The **ICS** app architecture consists of the following elements:

- The operating environment UCS with the App Center and the Docker engine running the ICS-Container.
- The ICS software based on nodejs running in the ICS-Container.
- The Keycloak Identity Access Management, which is used by ICS to authenticate sessions and obtain login tokens for applications.
- A Redis container to store OIDC sessions.
- The following sections may refer to `the browser` rather than to `the client` to avoid confusion with OIDC clients configured in Keycloak.
- `Backend communication` as referred to in the following section is not related to `Backchannel Logout`, which is a specific OIDC protocol.

3.1 Design decisions

The **ICS** app aims to provide a simple way to facilitate CORS-conform communication to different backends directly from the browser. It can proxy, modify and authenticate requests and use Keycloak and its own sessions storage to hold OIDC session. It can acquire those sessions via a silent background login, provided a valid OIDC cookie is already available in the browser.

3.2 Overview

Starting from the basics, ignoring everything related to login, authentication and sessions for now, this is how ICS works on a basic level.

- The browser opens the intended app normally.
- The app contains ICS related (JavaScript-)code as part of it's normal responses.
- This code will instruct the browser to send a requests to ICS, once communication to a separate app is required.
- The ICS then acts as a middleware to modify and forward those requests appropriately to the relevant, second app using a backend communication channel.
- ICS receives the response back and finally sends an appropriately modified response back to the browser.

Refer to Figure 3.1 for a visual representation.

Let's consider how this fits into the wider OIDC authentication scheme. (see Figure 3.2)

- The browser starts unauthenticated at the login endpoint of an ICS supporting app.
- The browser follows the OIDC login procedure, getting redirected to Keycloak and, assuming successful login, causing the App and by extension the browser to be assigned an OIDC session.

- The browser requests an action, for example creating a video conference, as part of a calendar entry. This means an interaction from OX to Element (more specifically the Nordeck-bot running in Element) is requested.
- A silent login happens in the background. This silent login uses the information stored in the browser to authentication the ICS with Keycloak via a hidden iframe.
- The actual functional interaction begins, displayed in Figure 3.1.
- A requests to the correct backend (usually another Univention-app) is sent.
- ICS acts as a middleware between the browser and the backend (app)

Note: ICS may use shared secrets rather than relying on OIDC authentication when communicating with app-backends.

Warning: Backend communication is only safe if done via HTTPS or a secured network. Secrets may be exchanged on Application-Layer.

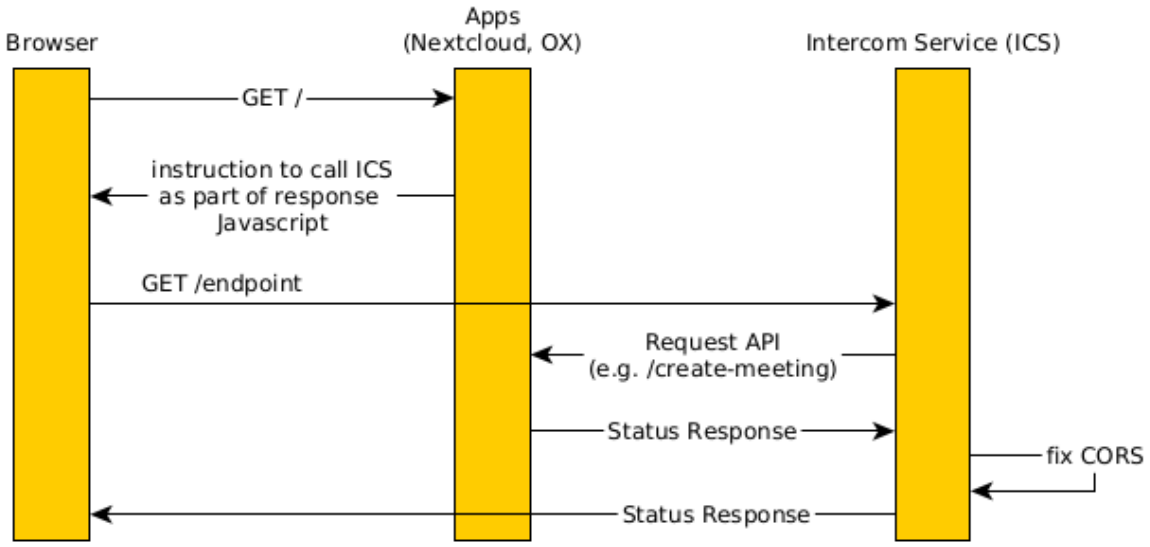

Figure 3.1: Interactions of ICS without OIDC

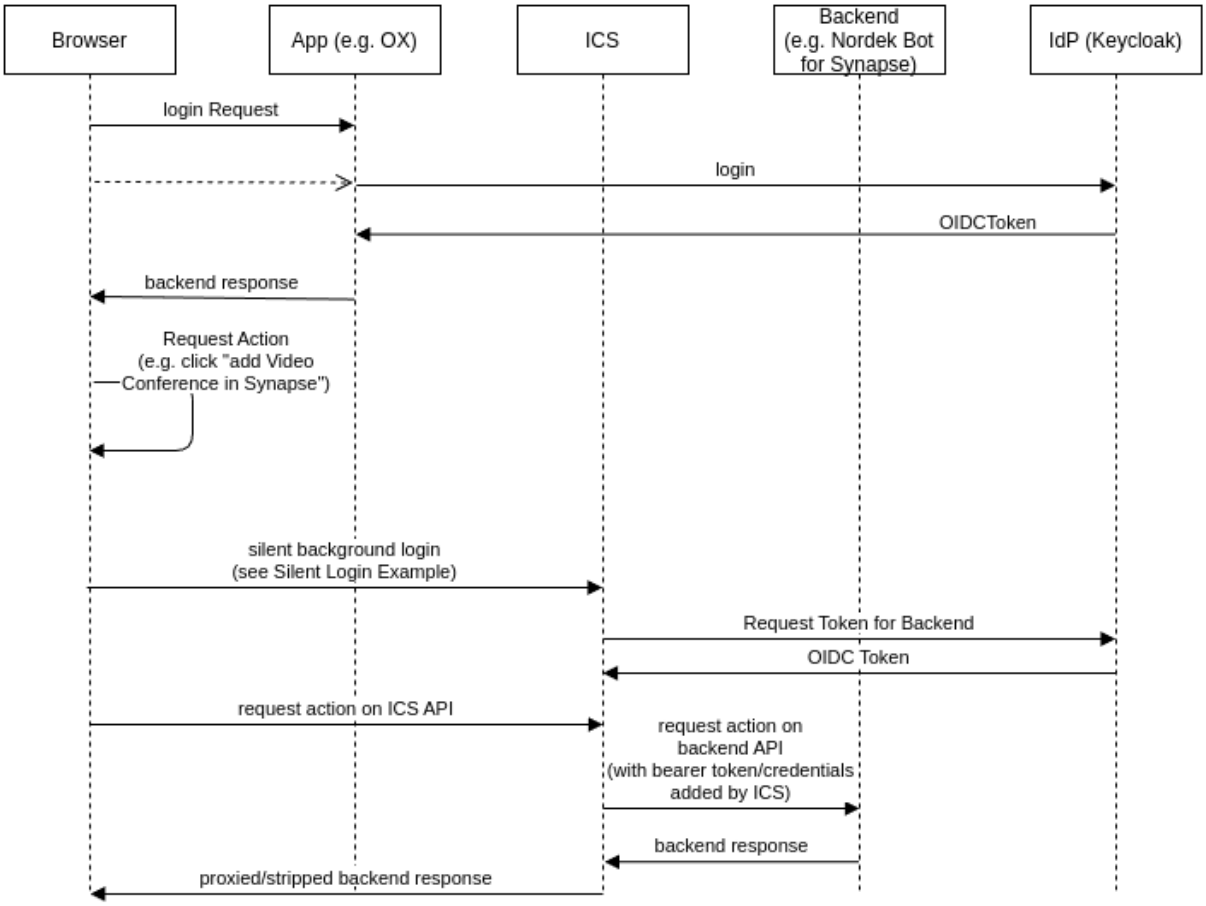

Figure 3.2: Interactions of ICS with OIDC, OX and Nordeck

3.3 Portal Navigation

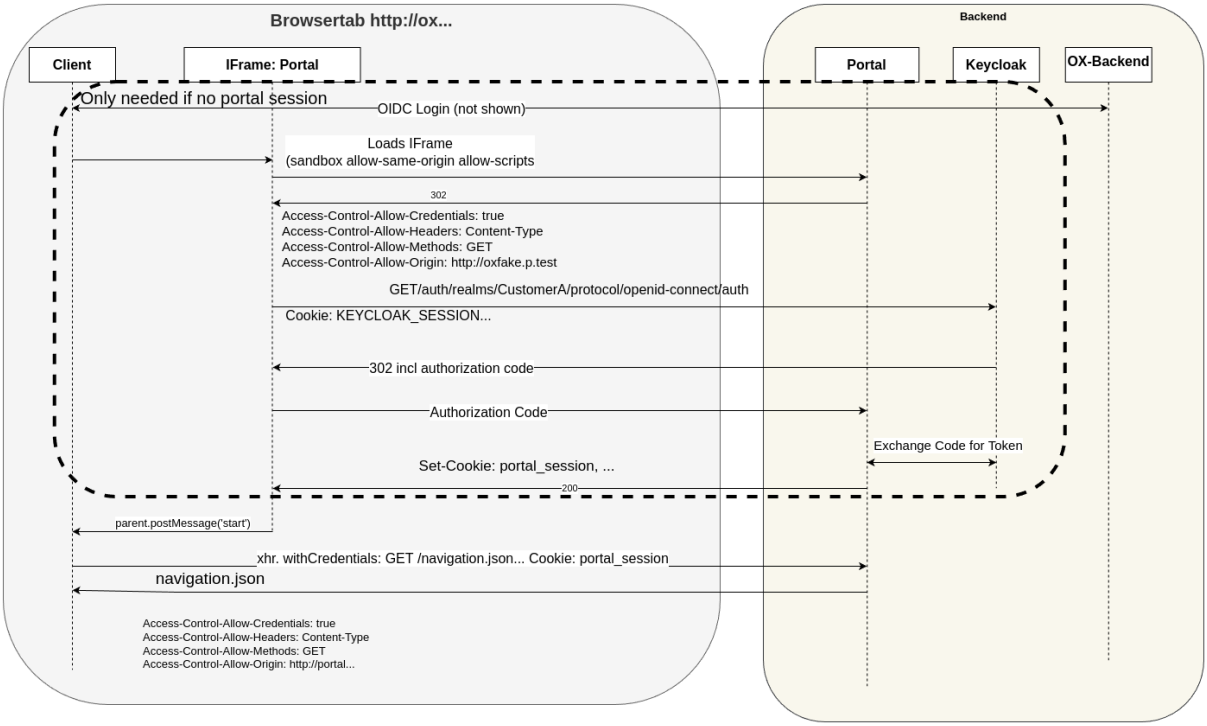

Figure 3.3: Communication overview for the `Central Navigation` functionality, which requires cross-app communication between OX and the Univention-portal.

3.4 Filepicker

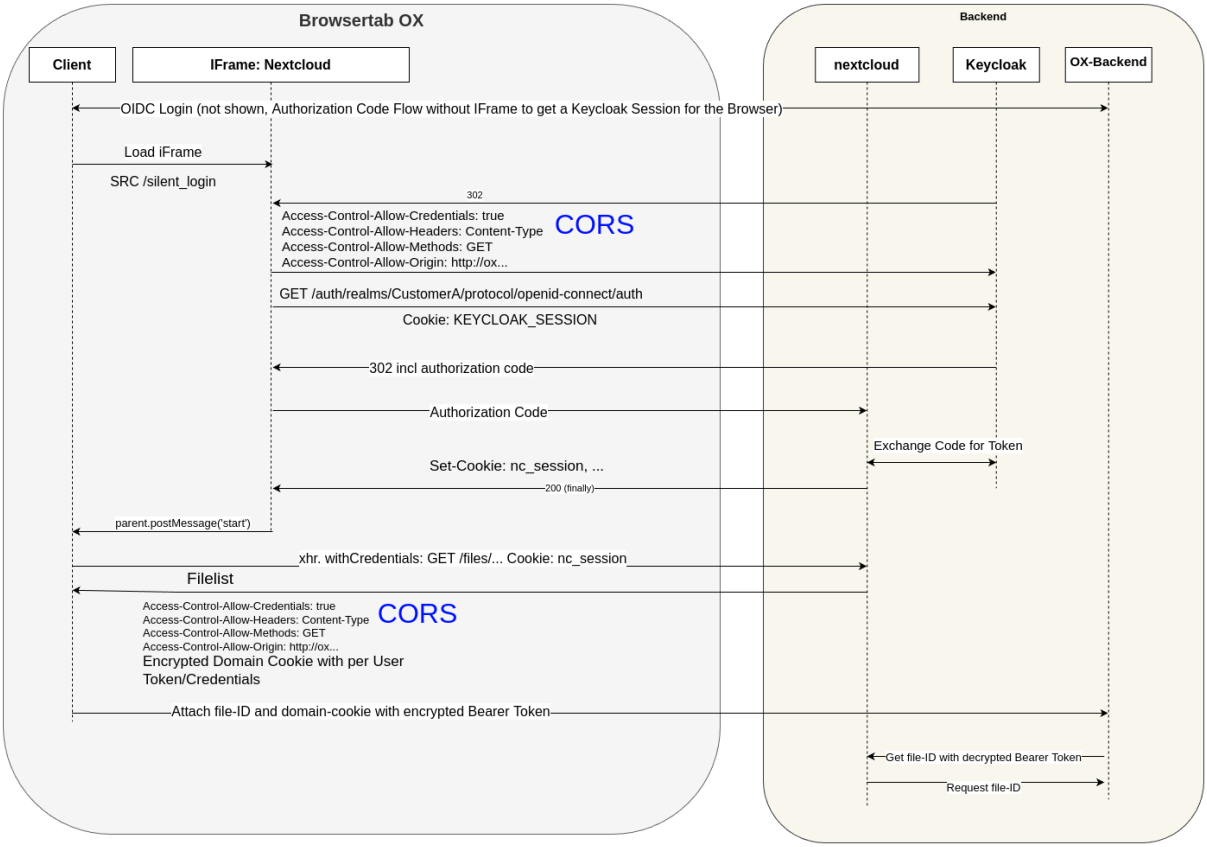

Figure 3.4: Communication overview for the `Filepicker` functionality, which requires cross-app communication between OX and Nextcloud.

3.5 General

/
: Alive test only

/silent
: Silent (OIDC) login endpoint

/backchannel-logout
: Endpoint for OIDC backchannel logout requests

3.6 App-Specific

/fs
: Proxy for Nextcloud

/navigation.json
: Proxy to Univention-portal for central navigation data

/nob
: Proxy for the Nordeck-bot. This endpoint may also be used to send requests to the plain Matrix `UserInfo`-service in a testing environment.

CHAPTER

FOUR

REQUIREMENTS AND LIMITATIONS

To ensure a smooth operation of the **ICS** app on UCS, administrators need to know the following requirements and limitations:

4.1 CSRF Protection

Warning: CSRF protection was not extensively tested and may break at any time.

Cross-Site-Request-Forgery protection may not be working for OX, Matrix and Nextcloud version released before 09.2022.

CHAPTER

FIVE

TROUBLESHOOTING

When you encounter problems with the operation of the **ICS** app, this chapter providers information where you can look closer into and to get an impression about what is going wrong.

5.1 Log files

The **ICS** app produces different logging information in different places.

/var/log/univention/appcenter.log Contains log information around activities in the App Center.

The App Center writes ICS relevant information to this file, when you run app lifecycle tasks like install, update and uninstall or when you change the app settings.

/var/log/univention/join.log Contains log information from join processes. When the App Center installs ICS, the app also joins the domain.

ICS Docker container The app uses a custom builder node image. The App Center runs the container. You can view log information from the ICS Docker container with the following command:

```
$ univention-app logs ics
```

/var/log/apache2/*.log Reverse proxy logs may contain relevant information for queried URLs by **ICS**, for example the status of middleware queries to other components. Please note that for externalized setups, like for example the BMI-UX setup, the queries will be proxied through the external HA-Proxy and therefore logs will be located in `/var/log/haproxy.log` on the haproxy-server.

5.2 Common Problems

Failing to provide the protocol (http or https) for middleware relevant URLs like *intercom-service/nextcloud/url*, *intercom/portal/portal-url*, *intercom/matrix/nordeck-url* will lead to an error during the request in the form of:

```
TypeError: Cannot read properties of null (reading 'split')
  at required (/app/node_modules/requires-port/index.js:13:23)
```

CHAPTER

SIX

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] *UCS 5.0 Manual*. Univention GmbH, 2021. URL: https://docs.software-univention.de/manual/5.0/en/.

[2] Raphaël Hertzog and Roland Mas. *The Debian Administrator's Handbook*, chapter Shell and Basic Commands. Freexian SARL, First edition, 2020. URL: https://www.debian.org/doc/manuals/debian-handbook/short-remedial-course.en.html#sect.shell-and-basic-commands.

INDEX

E