

Welcome @ IFI

Hello and welcome! In the following you'll find basic information to facilitate your beginnings at the IfI.

1st step: Setup your IfI account credentials

Learn here how to setup your account password and how to set up 2-factor authentication (the later is currently in the testing stage and therefore not yet required). Please note, that the information here concerns your **IfI account**. The instructions on how to setup your UZH account has or will be sent to you by postal mail.

Password Authentication: On account creation, we sent you an **initial password** and/or a **link to reset your password** – together with instructions on how to set a password. Please act accordingly and you are set and ready to continue.

Important: please also read more on [passwords](#), [phishing and malware](#) (note that you need to login to access these pages, a perfect way to test if your IfI credentials work), plus the [Guidelines and Security Rules](#) (UZH).

2-factor Authentication (2FA): 2FA makes the process of identifying user (authentication) more secure, by requiring a 2nd factor in addition to the password. If one factor (usually the password) becomes known, due to fishing or a data leak for example, the 2nd factor is still necessary to log in. This makes such attacks much harder.

2FA is right now in the testing/migration stage. This means, that if you do not have a 2nd factor configured, you will not need to provide one when logging in. If you would like to test our 2FA, all you need to do is to setup a 2nd factor (see below).

Setup your first 2nd factor: The 2nd factors for IfI accounts are managed in our PrivacyIDEA server. To add a 2nd factor, do the following steps:

1. Log in on the privacyIDEA server: pi.ifi.uzh.ch
2. In the left-side menu click **Enroll Token** (Tokens are the 2nd factors in the privacyIDEA terminology).
3. By default, a PUSH token will be installed. But you can also choose other token types, such as TOTP.
PUSH: this is the most seamless of the 2nd factors. You only need to confirm your login on your mobile phone.
TOTP: this is the most common of the 2nd factors. You will need to type a 6-digit number when logging in.
privacyIDEA authenticator app: for the PUSH token to work, you need to install it to your mobile phone (use the QR codes provided).
The TOTP token can be added to any authenticator app (Google, Microsoft, FreeOTP, etc.)
We recommend to use the privacyIDEA authenticator (you can add Microsoft and EduID TOTP

tokens used for UZH services to the privacyIDEA authenticator too, so you have everything in one place).

4. Click **Enroll Token** (bottom) and proceed according to the instructions given (which differ for different token types).
5. After that, you are ready to go. We recommend to read more on [passwords](#), [phishing and malware](#) (note that you need to login to access these pages, which is perfect way to test if your Ifl credentials/2nd factors work), plus the [Guidelines and Security Rules](#) (UZH).

2FA-enabled Services: As noted above, we are currently in the implementation and testing stage. Please check on [Ifl and UZH Services](#) for which of our services 2FA has already been activated. NOTE: as indicated above, as of now, no 2nd factor is necessary, as long as you do not setup a token (see above).

Further steps

1. Read about the distinction between your [Ifl account and your UZH account](#).
2. Glance through the list of [Ifl and UZH Services](#) in order to learn what you can do with these accounts.
3. **Important:** do not confuse your Ifl and UZH accounts. Use your UZH account credentials for logging in to UZH services, and your Ifl account credentials to access Ifl services. The rule of thumb is:
 1. for services with URLs like `servicename.ifi.uzh.ch` use your **Ifl account** credentials to log in
 2. for services with URLs like `servicename.uzh.ch` use your **UZH account** credentials
4. Invest some time into the [guidelines and security rules](#) of the UZH. As a member of the Ifl you are also a member of the University of Zurich, and as such you have to comply with these guidelines. *Not knowing them is no excuse.*
5. If you have an Ifl e-mail address, find out about Ifl [e-mail](#) setup and usage.
6. If you have an UZH account, learn how to work with [Office 365](#) (UZH e-mail, calendars, Teams, etc.).
7. If you have an UZH account, learn how to setup [UZH VPN access](#) in order to work from outside the UZH network.
8. Setup [Seafile](#) and make yourself familiar with it's features.
9. Install [printers](#) according to your needs.

If you have any questions on IT infrastructure we are happy to [help](#) you.

For any request involving facility assets, such as disposal of electronic devices, light or air conditioning related issues, please file a report at the [UZH Facility Management Services](#).

Other sources of information

- [IFI Homepage](#)
- [IFI Intranet](#) (use your Ifl account credentials to log in)
- [UZH Central IT](#) (often referred as "ZI")

- [Research Groups](#)

From:

<https://moritz.ifi.uzh.ch/> - **Welcome to the IT documentation of the
Department of Informatics (IfI)**

Permanent link:

<https://moritz.ifi.uzh.ch/doku.php?id=overview:new&rev=1763982805>

Last update: **2025/11/24 12:13**

