TechFak-Jabber

Jabber/XMPP is a distributed instant messaging network and the Fachschaft is running a server for the Technical Faculty. It can be used by all students and employees, basically everyone with a TechFak-account. As it's not operated by a company with commercial interests, you don't have to worry about anyone profiling you or selling your data (unless you use a commercial client).

You can find all information to get started with your Jabber account here. The whole documentation is written in a Questions & Answers style.

Quickstart Guide

Get an account	You already have one if your TechFak account was created after 2015-10-16.
Protocol	XMPP (required by some clients)
Jabber ID	<TechFak account>@techfak.de
Password	Initially the same as your TechFak services password; must be changed before you can log in
Change password	Run `tfpasswd jabber` on a TechFak PC
Chatrooms	<room name>@conference.techfak.de
Can’t connect?	See here.

Getting Started --- Account Setup

Which Jabber client should I use?

There are several Jabber clients and apps available and you can use whichever you want.

You can find a list of maintained Jabber clients at the xmpp foundation's website.

On PCs with **Linux**, **Mac OS X** or **Windows** we recommend *Gajim* (check for activated OMEMO Plugin for end-to-end encryption), *Psi* or *MCabber*, a console client.

For **Android** devices, you can use *Conversations*.

For **iOS** devices there are *ChatSecure* and *Monal*.

If you are not completly new to Jabber, *Dino* for Linux is also a good client, but very new and not yet fully stable.

Where do I get an account?

Your Jabber account is tied to your TechFak PC account, so if you don't have a TechFak account, you cannot use our Jabber service.

If your TechFak account was created after 2015-10-16, you already have a Jabber account and only have to set a password.

If your TechFak account was created before 2015-10-16, please contact the RBG support, tell them your account name and ask them to activate it for the Jabber service. If your friends or colleagues also want to use Jabber, please write one mail with all accounts names in it to speed things up. Do not mail them any passwords.

What's my Jabber address?

Your user name is the same as your account name; the domain is *techfak.de*. So if your account name is *juser*, your Jabber ID (JID) is *juser@techfak.de*.

What's my password?

By default, your Jabber password is the same as your TechFak services password or the one you received on a piece of paper. You have to change it before you can log in to Jabber.

As you will probably be saving the password on your PC or mobile device, do not use the same password as for your other TechFak logins.

How do I change my Jabber password?

You can change your password on any TechFak netboot PC, including the `compute` server. Simply run the command `tfpasswd jabber` and follow the instructions.

If you haven't used your Jabber account before, your old password is either the same as your services password or the one you received on a piece of paper from the RBG. If neither one works, see below under I forgot my password.

If you can't change your password with that command and get a list of realms instead, your account is not activated for Jabber yet.

Problems --- Troubleshooting

I forgot my password.

Ask the RBG support to reset your Jabber password and tell them your account name. Your password will probably be reset back to the services password. Do not send them any passwords.

Remember to change your Jabber password to something secure and unique afterwards.

Why can't I talk to users of some other Jabber domains?

Our Jabber server enforces secure connections with forward secrecy. As long as the other server doesn't support that, you're out of luck.

To check if another server supports forward secrecy, test it at check.messaging.one and see if there are any ciphers with forward secrecy listed.

If the server does support forward secrecy but you still can't contact any of its users, please tell our server administrators about it.

Please don't ask us to support outdated ciphers without forward secrecy. We won't.

Why do I keep getting only "Connection refused" errors?

If you are using an older or not fully featured client or your Windows PC is being weird, you might need to specify the server's address manually. The host name is `xmpp.techfak.de` and the port is 5222. The server only supports TLS encryption and no legacy encryption. *Note that the domain of your Jabber address is still `techfak.de`.* Look for *Advanced Settings* or something like that in your client to enter the server address.

If you use *Jitsi* or another Java-based client, be aware that you need OpenJDK 7 or newer. Oracle Java and older OpenJDK versions will fail to connect.

Why won't my Pidgin use AES 256 bit encryption?

For some reason, most Pidgin installations don't enable any 256 bit encryption by default. To enable it, look for the „NSS Preferences“ in the Pidgin preferences and enable `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`, but don't blindly enable everything with `AES_256` in it. If you can, you should also enable the even better `TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256` so that your client uses it once the server supports it. If you disable all other ciphers, you might not be able to connect to other servers anymore. You should, however, disable anything with `RC4` or `DES` in it.

I entered my password incorrectly and now I can't connect anymore.

If you try to log in with an incorrect password too often, you get banned automatically. Just wait for at least 15 minutes and try again.

Why am I getting SSL or TLS errors with Adium on Mac OS

X?

Sorry, but Adium apparently doesn’t have any trustworthy encryption enabled. Please choose a different client, such as Psi or Gajim.

Why am I getting "SSL connection failed" errors? I have Pidgin 2.10.7 on Windows.

Older versions of Pidgin don't support our certificate. Version 2.10.8 and newer should work.

Questions & Answers

Do you offer multi-user chats?

Yes, any TechFak user can create chat rooms at `conference.techfak.de`. Once a chat room has been created, users from other servers can join it too.

Do you offer transports for ICQ or similar?

No, we don't. We would have to store the passwords of your other accounts for that and it would make the service less secure.

Please use a multi-protocol client like Pidgin instead.

I'm leaving the TechFak. Can I keep using my Jabber account?

No. Your Jabber account will be deleted along with your TechFak account when you leave. But one of the main benefits of a federated protocol like Jabber is that you can create a new account at a different provider after leaving TechFak and keep all your contacts and use the same clients.

Who operates this server?

The server is operated by students from the Fachschaft. It is endorsed by the RBG.

Why do I have to ask the RBG to activate my account and change my password?

The Jabber server uses the TechFak infrastructure to authenticate you when you log in. That way, new users will get Jabber accounts automatically and we won't have to store passwords on this server.

I want to use XMPP in my research project. Can I use your server?

You can use our server for whatever legal purpose you want. However, please keep in mind that we do not offer extra accounts for temporary projects and that this server is speed-limited.

If you need custom accounts or want to send lots of data, you can set up your own XMPP server and connect it to ours via XMPP federation. If you plan to do that, please contact us.

I have another problem or question; who should I ask?

You can contact the administrators of our Jabber service by mail: jabber@fachschaft.techfak.de

Please do not contact the RBG support. They will probably not be able to help you with our service.

Security and Privacy Concerns

From your perspective, this service is operated by a bunch of students and you may not want to trust us. It’s good that you’re thinking about the security and privacy of your data, so we’ll try to address your concerns.

Purpose of this service

This free Jabber service is available to all TechFak members for exchanging messages for any legal purpose, especially sending private instant messages. We like Jabber and we want to offer a secure as possible service to all TechFak members, free of tracking, profiling and spying. If you want a less altruistic reason: We want to securely communicate with other TechFak members. This service shall always be free, because the infrastructure for this service is provided for free by the faculty’s RBG and there’s no need for us to try to make any money with this.

Should I trust you?

Not just because we say so. You shouldn’t trust anyone who says “Trust me”. Research yourself and

draw your own conclusions. Here are some pointers to get you started.

Legal obligations --- good for you

We as the operators of the Jabber service have to obey the German Fernmeldegeheimnis law, which forbids us to read your messages. We also have to obey various German and European laws about information privacy, which forbid us to sell or share any of your data without your consent. We're not asking for your consent because we're not selling or sharing any of your data.

Legal obligations --- bad for you

Like all service operators, we may be required to hand over stored data to law enforcement, but only if they have a valid court order.

Data we store

We store data necessary to provide the Jabber service to you, like your roster, your vcard and your offline messages (until you pick them up). Multi-user chat rooms store the last 20 messages so that they can be displayed when a user joins the room. Older chat room messages are deleted. We also log IPs and connection attempts to combat abuse. Logs are deleted after seven days. If you enable the Message Archiving extension, we will also store your messages as instructed by your client (see below).

Data we don't store

We don't store when or who you talk to or the content of your messages, unless you receive an offline message or enable Message Archiving (see below). There is no other archive, log or history for direct messages on our server that law enforcement or miscreants could get their hands on (note the multi-user chat exception above).

What is Message Archiving?

By default, messages are only sent to the clients you are logged in with at the moment and it isn't possible to view them later on other clients or devices. With Message Archiving (XEP-0136), your client can store received and sent messages on the server so that you can view them with other clients and on other devices. How many and for how long messages are stored is determined by your client's archive settings. We have no influence on it.

Password security

We or anyone who breaks into the server (or your smartphone) could steal your password, which is why you should change it to something secure and unique, as mentioned above. We could still steal your password, even if you change it, but then we could only mess with your Jabber account. But we could do that even without your password, if we wanted to, because we administrate the server and its database.

Connection encryption settings

We enforce encryption with forward secrecy. You can inspect our settings on check.messaging.one (formerly xmpp.net) here.

Who are the administrators?

The Jabber service is administrated by members of the Fachschaft, usually two, which are chosen based on prior conduct and knowledge about IT administration and IT security. Usually, they are paranoid enthusiasts who try to make the service as secure as reasonably possible.

I don’t trust you, but I want to use Jabber. What should I do?

Change your Jabber password to something secure and unique. Use end-to-end encryption with OMEMO.

I’m still concerned…

Please contact us. If you don’t want to discuss your concern by mail, you can ask us to meet you in the Fachschaft’s office or lounge.