How to configure Tor Messenger

As of march 2018 the Tor Messenger has been discontinued - Tor Project as well as us don't recommend using it anymore!

> ⓘ An Alternative, which suits high security standards could be Riot Messenger based on the Matrix protocol. It's available for all big operating systems.
>
> Further infos on this can be found here: https://about.riot.im/
>
> Also Signal is a messenger that's often recommended by security experts.
>
> Mailbox.org offers support for XMPP with your own domain.

Torproject.org has recently released the Beta version of the Tor Messenger. You can use the Tor Messenger in combination with our Jabber/XMPP service – anonymously and without fear of unwarranted surveillance.

We offer two possibilities:

1. Configure MapAddress to set the Tor exit node
2. Use the Tor Hidden Service

1.) Configure MapAddress to set the Tor exit node

In order to offer users of Tor Onion Router maximum security against attacks via bad exit nodes, we operate a dedicated Tor exit node in our data centre. In order to use this node, all you need to do is specify a MapAddress statement in the Tor daemon configuration. This is a better and more secure way than just using the Tor Hidden Service for Jabber/XMPP, because SSL certificate errors can be avoided.

Open the file **Messenger/TorMessenger/data/Tor/torrc** in a text editor of your choice and insert the following line:

```
# access mailbox.org Jabber/XMPP Server MapAddress xmpp.mailbox.org xmpp.mailbox.org.
85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit
```

After saving and closing the file, you can proceed with starting the Tor Messenger and setting up your account.

Account setup

After starting up the Tor messenger, the account setup assistant will be run. Simply follow the steps. In the first, select *XMPP* as account type:
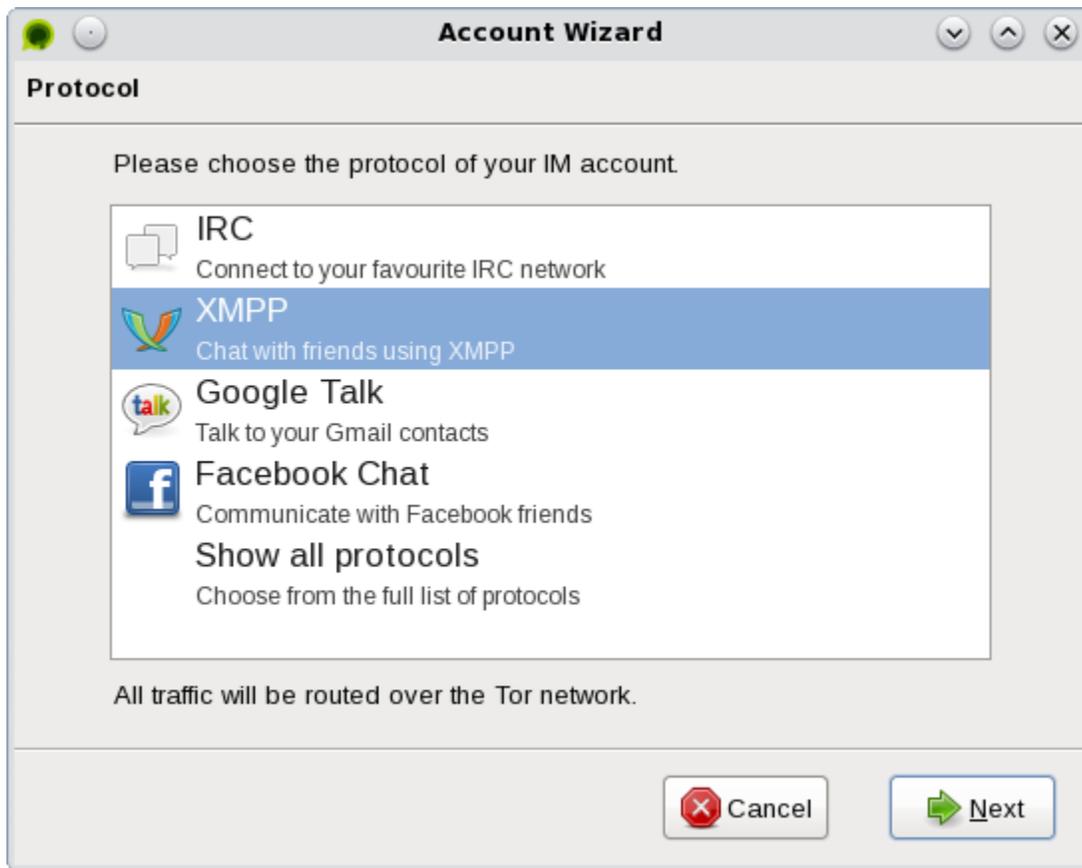
In the next step, enter as a **Username** the part before the @ symbol in your mailbox.org main address. So for instance, if your address was *user123@mail box.org*, your Username for the messenger would be *user123*. As a domain, put down **mailbox.org.** You do not need to create a new account on the server because your existing mailbox.org account can be used.

That's it – no further settings needed. Feel free to let the messenger software remember your password, or keep entering it every time you log in instead.

2.) Use the Tor Hidden Service

If you do not wish to configure a mapped address for the Tor daemon, you can use an alternative way of connecting by means of a Tor Hidden Service. We offer this for use with the Jabber/XMPP-Server in order to avoid the risks related with bad Tor exit nodes.

Open the advanced settings for your account, look for the XMPP options, and enter the Onion address **kqiafglit242fygz.onion** as a connect server (see screen shot below).
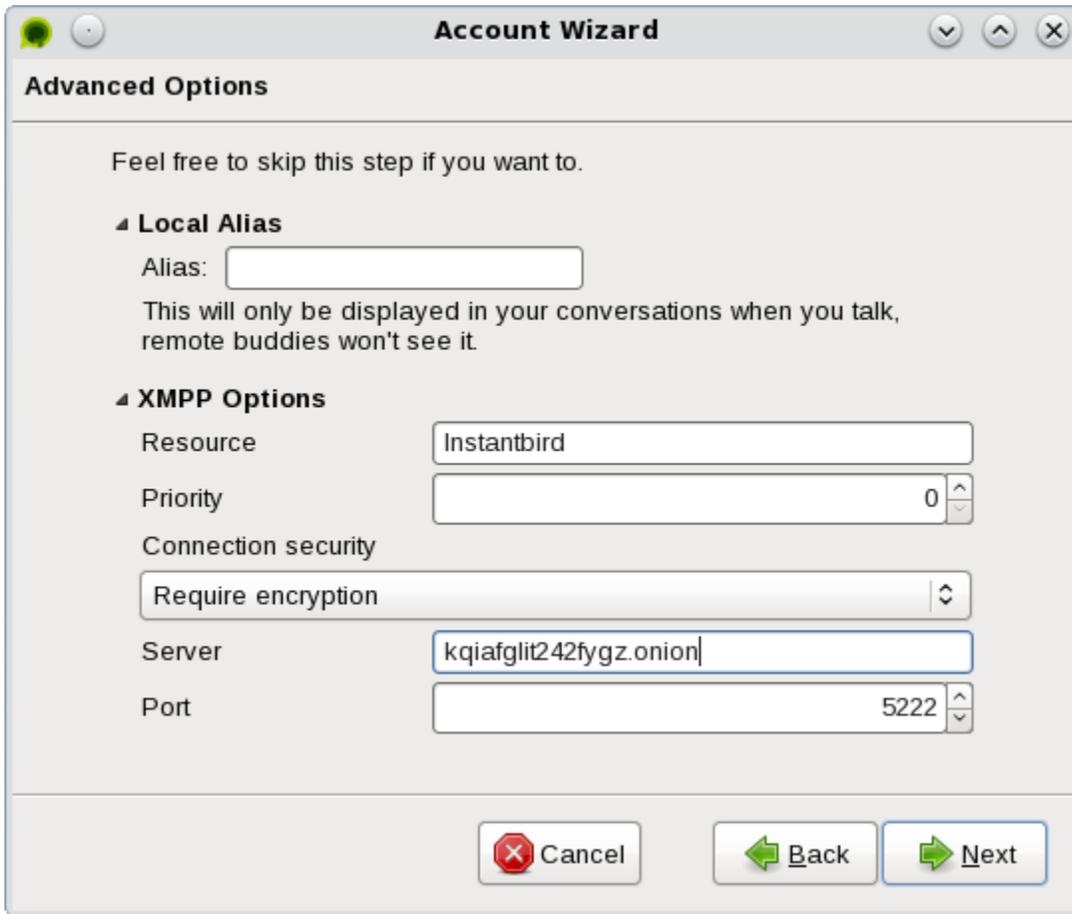
When connecting to the Tor Hidden Service for the first time, users may experience a warning or error message related to the SSL certificate. This is because the certificate used for the Tor Hidden Service is registered for the domain mailbox.org, and not for the Onion domain.
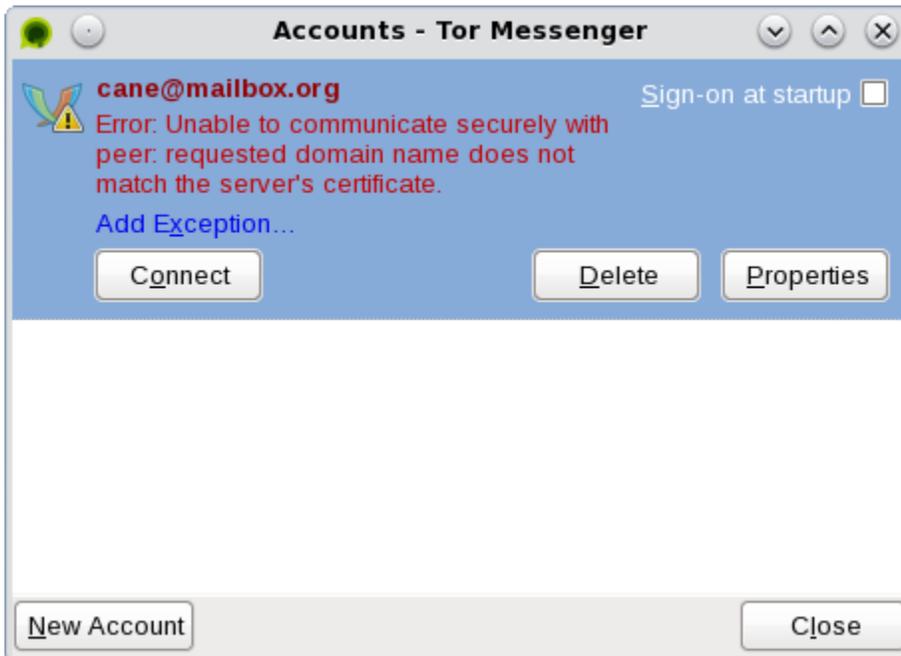
Simply click on the link **Add Exception** and verify the SSL certificate manually, using the information in the image below:

Certificate Viewer:"*.mailbox.org"

General Details

Could not verify this certificate because the issuer is unknown.

Issued To
Common Name (CN)   *.mailbox.org
Organization (O)   <Not Part Of Certificate>
Organizational Unit (OU) Domain Validated Only
Serial Number   3E:04:55:F8:C3:C1:81:C6:CF:65:89:97:66:94:4F

Issued By
Common Name (CN)   SwissSign Server Silver CA 2014 - G22
Organization (O)   SwissSign AG
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity
Begins On   04.12.2014
Expires On   04.12.2019

Fingerprints
SHA-256 Fingerprint   3D:81:9D:C9:CC:31:19:46:BF:D8:EE:9D:27:72:35:06:
                         8B:3E:B4:75:99:A5:04:73:41:30:2E:34:04:96:32:CD

SHA1 Fingerprint   BC:A2:F2:6F:7C:82:FA:E9:F4:D0:FD:46:BB:3D:E8:75:0B:CA:21:6B

Close

Related Articles