**Tools**

*These links are for your use only, as sources of images used below if they are not high quality enough in this doc.*

1. Adium tool guide [– Link](https://ssd.eff.org/en/module/how-use-otr-mac)
2. Basic Security Setup for Android - [Link](https://securityinabox.org/android_basic)
3. ChatSecure tool guide - [Link](https://ssd.eff.org/en/module/how-install-and-use-chatsecure)
4. Cobian Backup Guide - [Link](https://securityinabox.org/cobian_main)
5. How to change your Facebook privacy settings - [Link](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)
6. How to opt-out of Facebook's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)
7. How to opt-out of Twitter's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)
8. Jitsi Tool guide – [Link](https://securityinabox.org/jitsi)
9. K9 & APG tool guide – [Link](https://securityinabox.org/k9_apg_main)
10. KeePassX tool guide – [Link](https://securityinabox.org/keepass_main)
11. ObscuraCamTool guide – [Link](https://securityinabox.org/obscuracam_main)
12. Orbot & Orweb tool guide – [Link](https://securityinabox.org/Orbot_main), [Link](https://securityinabox.org/orweb_main)
13. PGP for Linux tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-linux)
14. PGP for Mac O SX tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x)
15. PGP for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-windows-pc)
16. Pidgin tool guide – [Link](https://ssd.eff.org/en/module/how-use-otr-windows)
17. Psiphon3 tool guide – [Link](https://www.level-up.cc/leading-trainings/training-curriculum/deepening/psiphon3)
18. Recuva – File Recovery Guide – [Link](https://securityinabox.org/recuva_main)
19. Redphone Tool guide – [Link](https://ssd.eff.org/en/module/how-use-redphone-android)
20. Signal Tool guide – [Link](https://ssd.eff.org/en/module/how-use-signal-%E2%80%93-private-messenger)
21. TextSecure tool guide – [Link](https://ssd.eff.org/en/module/how-use-textsecure-android)
22. Tor for Mac tool guide – [Link](https://www.torproject.org/projects/torbrowser.html.en#macosx)
23. Tor for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/)
24. TrueCrypt Tool Guide – [Link](https://securityinabox.org/truecrypt_main)

**HOW TO CHANGE YOUR FACEBOOK PRIVACY SETTINGS**

**How to change your Facebook privacy settings**

**Lesson to read: Social Media**

**Level:**Beginner

**Time required:** 10 minutes

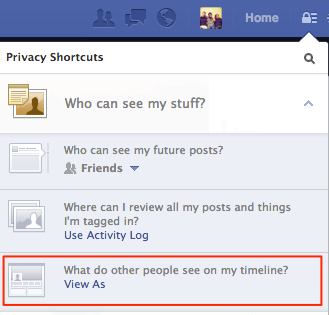
**How to Protect Your Privacy from Facebook's Graph Search**

Facebook now has a feature—Graph Search—that has been the subject of many privacy concerns. Graph Search allows users to make structured searches to filter through friends, friends of friends, and strangers. This feature relies on your profile information being made widely or publicly available, yet there are some Likes, photos, or other pieces of information that you might not want out there.

Since Facebook removed the ability to remove yourself from search results altogether, the Electronic Frontier Foundation put together a quick how-to guide to help you take control over what is featured on your Facebook profile and on Graph Search results – we have outlined it below. (Facebook also has a new [video](https://www.youtube.com/watch?v=bSji6Y66aKo) explaining how to control what shows up in Graph Search.)

**What's public on my profile?**

Click on the lock in the top menu bar, and under "Who can see my stuff?" click "View As." This will take you to the public view of your profile. Here you can see exactly what information, photos, and posts are available to the public. If there's anything you don't want the whole Facebook universe to be able to see, you can change individual settings to hide particular items.



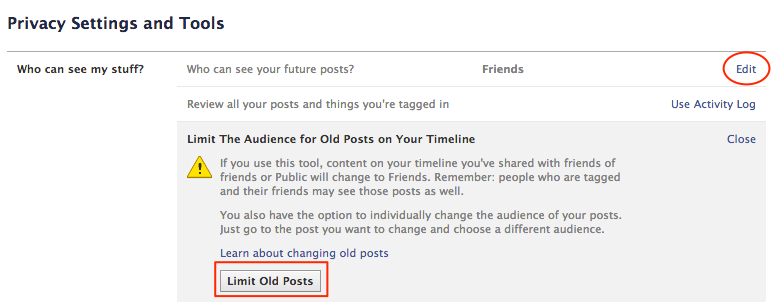
**How do I hide my general information?**

Go to your profile page and click "Update Info." You can control who is able to see what personal information you've listed—and if they're able to see it, they're able to search it.



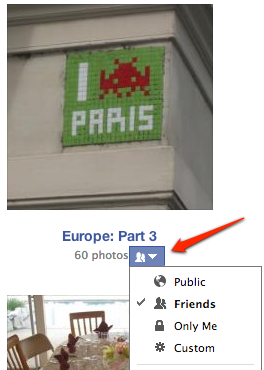
**Who can see my posts, both past and future?**

You can access your [privacy settings](https://www.facebook.com/settings?tab=privacy) by clicking on the lock in the top menu bar, then clicking "See More Settings." From here, you can choose your audience for future posts (including photos), and you can also limit who has access to previous posts that were more widely accessible.



**How do I hide my photo albums?**

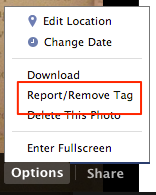
Go to your profile page and click on "Photos," then "Albums." You can configure who has access to each album.

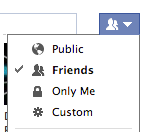


Note that tagging others in a photo by default gives their friends the ability to see that photo. Also note that removing a photo from your Timeline does not remove it from being searched, especially if it is someone else's photo.

In order to make sure that photo is not searchable, you must detag yourself or report the photo. Facebook has another [great video](https://www.youtube.com/watch?v=CaJYQXiu3PY) about how to do just this.

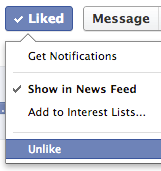
To detag yourself, click on a photo, and on the bottom of the picture click on "Options." Next, click "Report/Remove Tag." This gives you the option to remove your tag, as well as to notify the poster that you'd like the photo to be taken down.





**How do I hide my "Likes"?**

Go to your profile page and click on "Likes." Click "Edit" on the top right. From there, you can edit who can see your liked pages in each individual category.

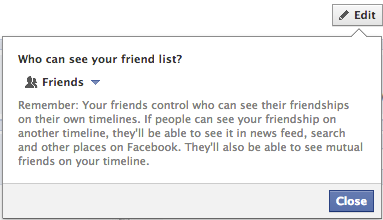
**Do I actually "Like" these things?**

While you are configuring your "Likes," we encourage you to take a moment to reassess the pages you have listed. A few years later, you may not like "Free Booze Fridays" anymore. Unliking is as simple as going to a particular page, hovering your mouse over "Liked," and clicking "Unlike."

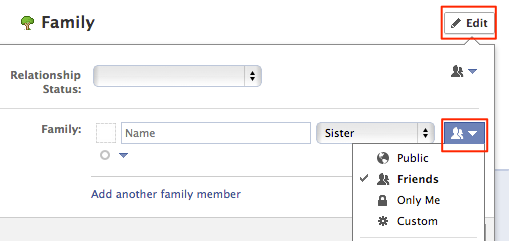
**How do I hide my friends and relationships?**

Besides locking down your own personal information, it turns out that your friends and relationships can appear in searches associated with you. Because [they have no control](https://www.eff.org/deeplinks/2013/01/facebook-graph-search-privacy-control-you-still-dont-have) over how they appear in such searches, we strongly encourage you to do the altruistic thing and lock down your friendship settings. Here's how to set your privacy settings to keep your friendships and relationships—and therefore related search results—limited in visibility to only whom you want.

First, go to your profile and click on "Friends." On the top right of the page, click on the "Edit" button. This allows you to select who can see your friend list.



Next, you should adjust the settings of your relationships and family associations. Go to your profile and click "Update Info," then scroll down to "Family" on the bottom left. When you click "Edit," you can choose the specific privacy settings for each relationship.



**Keep it up!**

The most important think you can do is to check your privacy settings often—especially after new features are released. Facebook has done a better job of making new privacy settings more accessible while also notifying users of any changes. Their explanations, however, can lose sight of bigger picture concerns.

**HOW TO HOW TO OPT-OUT OF FACEBOOK'S DATA BROKER RELATIONSHIPS**

**How to opt-out of Facebook's data broker relationships**

**Lesson to read: Social Media**

**Other reading:** <https://www.eff.org/deeplinks/2012/04/4-simple-changes-protect-your-privacy-online>

**Level:**Beginner

**Time required:** 30 minutes

Facebook is teaming up with four of the world’s largest corporate data brokers to “enhance” the ad experience for users. Datalogix, Epsilon, Acxiom, and BlueKai obtain information gathered about users through online means (such as through cookies when users surf the web) as well as through offline means (such as through loyalty cards at supermarkets and product warranty cards).  Facebook will use this information to tailor its ads. The Electronic Frontier Foundation describes what this means and how you can avoid it.

In practical terms, this means that limiting how much information you put on Facebook is not enough to limit how ads are targeted to you on Facebook. Your interests, age, shopping history (including offline), web browsing, location, and much more could be stored by these data brokers and utilized to market to you – even if you’ve been careful not to share this type of information with Facebook.

So, what can users do? If you’re concerned about this practice, you can opt out of the targeted advertisements by individually visiting each of the data broker partners currently working with Facebook. We've got directions below for opting out of each site.

We also have two general tips:

**1.  Install an add-on to protect your privacy online**. Facebook is using "blind cookie-matching" to match up users of online marketer BlueKai with specific Facebook accounts. Blocking trackers is a good general practice for stopping this type of tracking. We recommend you use a tool such as [Ghostery](http://www.ghostery.com/) (now available on Firefox, Safari, Chrome, Opera and Internet Explorer).

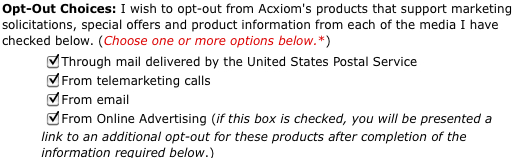
**2. Avoid giving your phone number and email address to companies when possible.** Facebook and these companies are primarily using hashed email addresses to match users between databases, though they may also use hashed phone numbers. If you’re filling out a survey or signing up to receive email updates from a website, consider creating and using a different email address than the one you associate with your Facebook account. Similarly, consider setting up an alternate phone number you can give to companies apart from the phone number you connect with your social media accounts.

**Opt Out Instructions:**

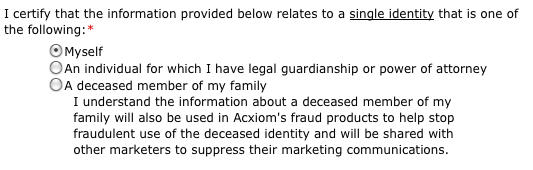
Note that in general, opting out of data brokers will not necessarily result in your data being removed from their lists. Instead, these companies will generally 'suppress' your information from certain uses -- including, hopefully, in the batches of data sent to Facebook. The process below takes a bit of effort, but you really do need to opt out of all four data brokers separately to get out of this program.

**Acxiom**

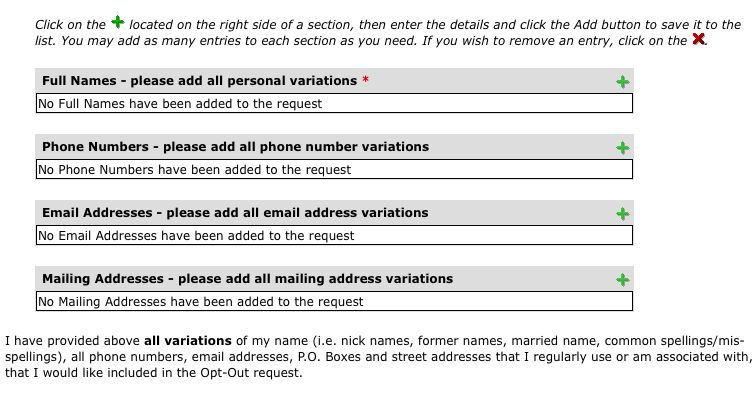
1. To get started, visit Acxiom's [Opt Out Form](https://isapps.acxiom.com/optout/optout.aspx). Then scroll down until you see your "opt-out choices." Here there will be a list of the types of media you would like to opt out of (mail, telemarketing, email, and online advertising).  You can check all four, though note that their online advertising opt-out is cookie-based, meaning it will disappear every time you clear your cookies.



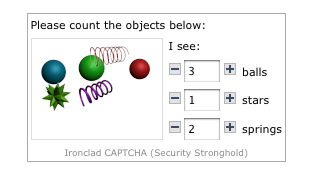
2. Certify that you are just a single person.



3. Fill out the form with your personal information. In order to be sure that Acxiom doesn't target advertisements at you through Facebook, you'll want to provide Acxiom with the phone number and email address associated with your Facebook profile. Use the green + signs on the form to add information.



4. Click submit. After you hit submit (and get through a CAPTCHA), you'll be offered a chance to install Acxiom's opt out cookie. You can choose to do this or not, but remember that this is not a persistent method of protecting your privacy: the opt out cookie will disappear as soon as you clear your cookies. See instructions below for opting out of BlueKai for advice on dealing with web tracking.



5.  You will then receive an email with a link in it from Acxiom. You can click on this link or else copy and paste it into a new browser window. Visiting this page will take you to another CAPTCHA. Fill this out.

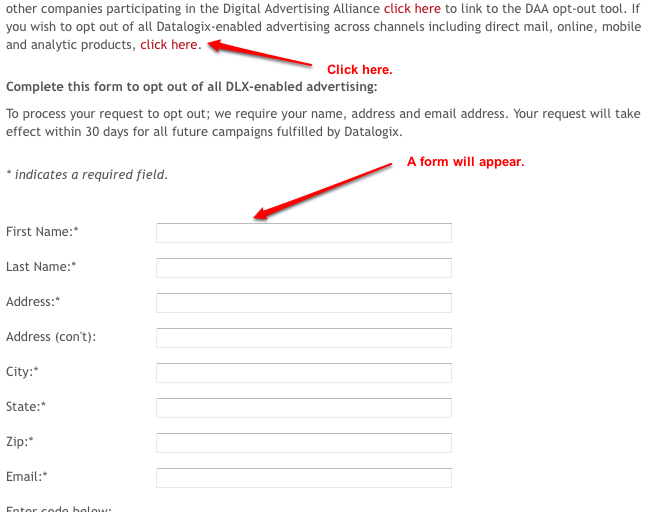
Congratulations - you've opted out of Acxiom!

**Datalogix**

**1.**To opt out of this program, visit the Datalogix.com [privacy page](https://www.datalogix.com/privacy/). Scroll down to the word “Choice” and the last sentence in the first paragraph says:

*“If you wish to opt out of all Datalogix-enabled advertising across channels including direct mail, online, mobile and analytic products, click here.”*

2. Click there and a form will pop up that asks for your name, address, and email address. Fill this out and click submit.



Datalogix promises that the opt-out will take effect within 30 days. Once you’ve been opted out, Datalogix will no longer include your information in the hashed data they provide to Facebook.

**Epsilon**

As Epsilon explains on their [Consumer Preference Center](http://www.epsilon.com/consumer-preference-center) page, there are several ways to opt out of the Epsilon marketing database:

**EMAIL:** Email [optout@epsilon.com](mailto:optout@epsilon.com) and include the following information:

* full name (including middle initial)
* current address
* previous address if you have been at your current address fewer than six months

**PHONE:**Phone 1.888.780.3869 and leave the above information.

**MAIL:**Mail the above information to the below addresses:

**U.S. Consumers:** Epsilon  
P.O. Box 1478  
Broomfield, CO 80036

**Canadian Consumers:** Epsilon  
41 Metropolitan Rd.  
Toronto, Ontario  
M1R 2T5

We note that not all of these methods require you to provide an email address.  Epsilon may have methods to match your name with your email, but you can also provide your email address to be sure.

Note that opting out doesn't actually remove the data from Epsilon's database but rather just marks it as "suppressed" to they will stop sharing it for marketing purposes. This means that if the information is ever re-submitted, you won't be added back to the list.

**BlueKai**

Unlike the other data brokers Facebook is working with on this new project, BlueKai does not directly collect data from your offline activities. Instead, they use tracking cookies that collect data about your online browsing habits and then use that information to infer what types of products you might like to buy.

**The best way to opt out of this is to use a browser add-on to block third-party tracking.**

Rather than try to block only BlueKai, we recommend you block all third-party trackers. You can use a tool such as [Ghostery](http://www.ghostery.com/) (now available on Firefox, Safari, Chrome, Opera and Internet Explorer) as noted earlier.

**CONGRATULATIONS** -- you've managed to get out of Facebook's new data broker-driven targeted marketing, and helped protect yourself from several important data brokers.

**JITSI TOOL GUIDE**

# Jitsi Tool Guide

**Secure Audio, Video and Instant Messaging**

**Lesson to read: Making a Call**

**Download Location:** [***https://jitsi.org/Main/Download***](https://jitsi.org/Main/Download)

**Computer requirements** All Windows Versions, Mac OS X, Ubuntu, Linux

**Version used in this guide:** Jitsi 2.4

**License:** Free and Open-Source Software

**Level:**Beginner

**Time required:** 15-20 minutes

**1.1 Getting started**

**Using Jitsi will give you:**

* A secure alternative to Skype that encrypts calls, messages and video all the way from your computer to the recipient's computer.
* The ability to register various accounts that you may already have (such as Facebook, MSN, Google Talk or Yahoo Messenger), with Jitsi and use it to communicate in them simultaneously.
* The ability to communicate securely and simultaneously with other programs recommended in this app such as Pidgin, Adium and ChatSecure.

## 2.1 How to Install Jitsi

To install **Jitsi**, perform the following steps:

**Step 1**. **Double click “**jisi-2.4-latest-x86.exe”; the Open File - Security Warning dialogue box may appear. If it does, **click**“Next” to activate the Windows Installer screen, followed by the Welcome to the Jitsi Setup Wizard window.

**Step 2**. **Click**“Next” to activate the End User License Agreement window; **check**the I accept the terms in the License Agreement option to enable the Next button, and then **click**“Next” to activate the Destination Folder window.

**Step 3**. **Click**“Next” to activate the Additional Tasks window and accept the default settings as presented.

**Note**: Enabling the Auto-start when computer restarts or reboots option may slow down the overall function of your computer, especially if you already have multiple applications configured to run when your computer starts up.

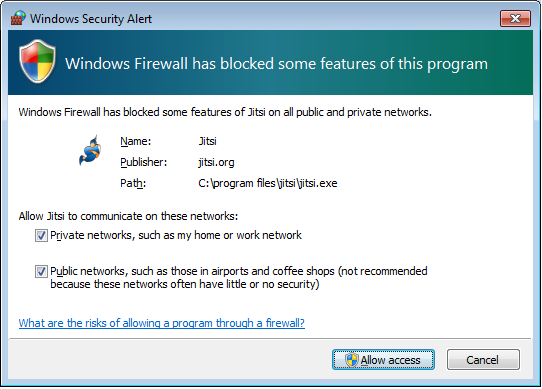
**Step 4**. **Click**“Next” to activate the Ready to Install Jitsi window, and then **click**“Install” to activate theInstalling Jitsi window displaying the installation progress bar.

**Step 5**. **Click**“Finish” to complete the installation process and automatically launch the **Jitsi** Sign in window as follows:



**Note**: In some instances, installing and launching **Jitsi**for the first time triggers a Windows Security Alert prompt screen, as shown below.

**Step 6**. **Select**both **Private** and **Public** networks check-boxes, and then **click**Allow access\*\*\* to see the***Jitsi***Sign in window or main user interface window.



## 2.2 How to Add Accounts in Jitsi

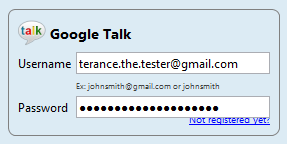
Please note that even with **Jitsi**encryption, account providers like **Google**or **Facebook**are monitoring the very fact that you are communicating (and perhaps with whom you are communicating), and may share this information with third-parties, such as corporations or governments. Therefore it is perhaps best to avoid using those accounts for very sensitive communication even with **Jitsi**encryption.

### 2.2.1 How to Add a Gmail/Google Account

**Note**: The example which follows is based on a **Google Talk**account, the set-up process for the other communication protocols is similar. Communications or some encryption features may not work between users of different account providers (like Facebook, Gmail, Yahoo, etc.). However, they should work when communicating between two accounts from the same provider.

**Step 1**. **Select Start > Jitsi** or **double-click** the **Jitsi**desktop icon to open **Jitsi**.

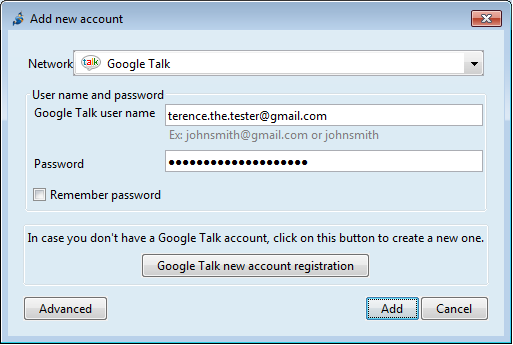
**Step 2**. In the sign in window, **type in** the username and password of the **Gmail**account you would like to use for chat purposes, so that it resembles the following:



**Note**: You can add multiple accounts using different protocols at the same time.

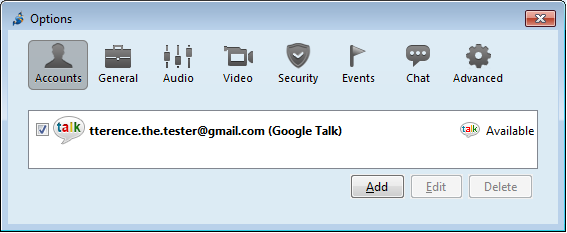
**Step 3**. **Click**“Sign in” to activate your account chat window.

**Note:** If you closed Sign in window, or you want to add another account, you can add it by **selecting File > Add new account...**menu. In the new window **select Network** as Google Talk and **type in** the user name and password of the **Gmail**account as shown on the image below:



To verify that you have registered your **Gmail**account with **Jitsi**, perform the following steps:

**Step 1**. **Select Tools > Options** in the menu to activate the following window:



**Note:** If you are using 2-step verification to protect access to your **Gmail**account, when you try to log in from **Jitsi**with your regular password you may see a message like the one below. To log in using **Jitsi**, you will need to generate an "application-specific password". See Google's [instructions on how to do this](https://support.google.com/accounts/answer/185833?hl=en).

### 2.2.2 Registering new Jabber/XMPP or SIP account and adding it to Jitsi

**Jabber/XMPP**and **SIP**are open standards of text and voice communication. There are many servers that offer free accounts which you can use with Jitsi. Below we are recommending some of the servers that you could use for sensitive communication.

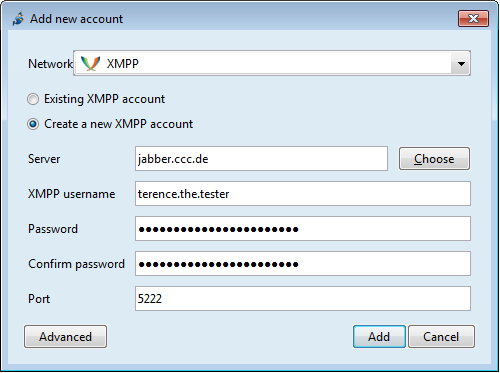
* **Riseup.net** Jabber/XMPP account

If you have account on the Riseup.net secure email service (located in the USA) you may use this account also to communicate over Jabber/XMPP network by adding this account to Jitsi - see below on how to add existing Jabber/XMPP account.

* **Jabber.ccc.de** and other Jabber/XMPP accounts

You can register an account on Jabber.ccc.de server (located in Germany) by taking following steps:

**Step 1**. In **Jitsi, select File > Add new account...** in the menu. In the new window, **select Network: XMPP** and **check**the Create a new XMPP account\*\*\* option. In \*Server, **type**jabber.ccc.de, **type**in the XMPP username you would like to create, and **fill in**the Password and Confirm password fields so that it resembles the following:



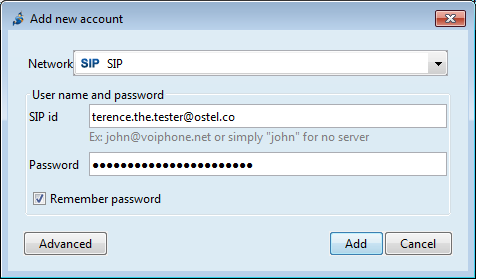
**Step 2**. **Click Add**. After successful registration you will be presented with a window similar to thatabove.

If the username which you requested is already taken by somebody else, the registration process will fail with the message We failed to create your account due to the following error: Could not confirm data. You can try again by repeating the process and selecting a different username.

**Note** that if you do not log in to your jabber.ccc.de for longer than 12 months your account will be automatically removed from the server and the username will become available for registration by other people.

* **ostel.co** SIP account

**SIP** accounts cannot be registered from within the **Jitsi**program. The **ostel.co** server (located in USA) offers [registration on their web page](https://ostel.co/users/sign_up). **Select**a username, password and provide your existing email address and **click**the Sign up button on the web page. After successful registration come back to Jitsi program. **Select File > Add new account...** in the menu, **select Network: SIP**, **type in** your username (e.g. terence.the.tester@ostel.co) and the password you created during the web registration and **click Add**. See following image for reference:



* **Adding existing Jabber/XMPP or SIP account to Jitsi**

If you already have Jabber/XMPP or SIP account you can add it to **Jitsi**by **selecting File > Add new account...** in the menu and selecting the appropriate **Network** (either XMPP or SIP depending on the account type).

### 2.2.3 How to Add a Facebook Account

**Facebook**has two settings that you may need to change before **Jitsi**can connect to your Facebook Chat.

* **Facebook Username**

**Facebook**requires a username for **Jitsi**to connect to Facebook chat. Many **Facebook**users already have a username. To check your username, **log in**to your **Facebook**account: your username is what appear in the location bar of your browser afterhttps://www.facebook.com/ when you view your Timeline or Page. Your username is also in your **Facebook**email address for your personal account (ex: username@facebook.com). You can see or change the username or get one by going to your Account Settings > General section or by visiting <https://www.facebook.com/username>. To set username **Facebook**may ask you for your account verification which may require sending SMS to a mobile phone number which you will need to provide to **Facebook**in the process of verification.

* **App Settings**

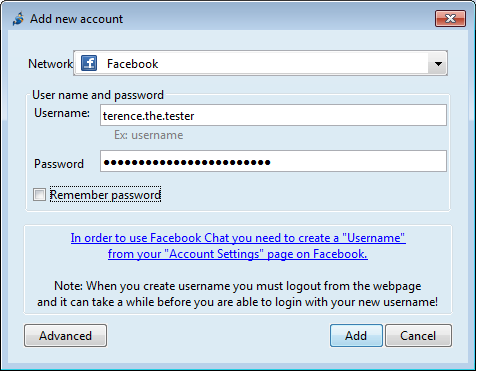
**Facebook’s**“application platform” must be turned on before **Jitsi** can connect to Facebook Chat. Visit your **Facebook**Account Settings > Apps section and check that the setting for Apps you use is turned On. This turns "application platform" on for your account.

**Note** that that turning **Facebook’s** "application platform" opens up much of your **Facebook**data to third-party application developers. This data is available not only to the **Facebook**applications that you use, but also **Facebook**applications used by any of your friends. After turning on **Facebook’s** "application platform", be sure to check the settings under "Apps others use". This setting allows you to hide some personal information from applications used by your friends. Unfortunately, **Facebook**does not offer settings to hide all personal information. Certain categories of information (like your friend list, gender, or info you have made public) are visible as long as **Facebook**’s "application platform" is turned "on". It is up to you to determine whether this is an acceptable tradeoff of your privacy.

Now you are prepared to add your **Facebook**account to **Jitsi**. To do this follow the steps below:

**Step 1**. From the main menu **select File > Add New Account...**

**Step 2**. In the Add New Account dialogue, **Network** menu choose Facebook, **enter your username and password** and **Click "Add"**



## 2.3 How to change password for account with Jitsi

It is important element of security to know how to change the password for each account that one has. Many of the accounts that you can use with Jitsi offer changing password as a part of their settings, which are accessible over web interface. However some Jabber/XMPP and SIP account will not have any web interface to manage them. You can change password for those account using Jitsi by following steps below:

**Step 1**. **Select Tools > Options** in the menu, **select**the **Accounts** tab

**Step 2**. **Click on Edit** button on the bottom to activate a new window.

**Step 3**. **Click on Change account password** to activate Change account password window.

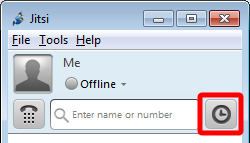
**Step 4**. Enter new password**and**Re-enter passwordand **click on OK** button to close this window.

**Step 5**. Close Account Registration Wizard.

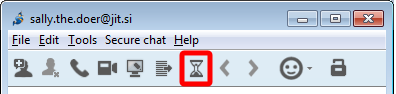
## 2.4 How to configure Jitsi to improve it's security

### 2.4.1 Disable and remove call and chat history

**Jitsi**by default stores information about the incoming and outgoing voice/video calls and the history of your text chats -- all messages that you sent and received. You can access voice/video calls by **clicking**on the clock icon on the main Jitsi window:



You can see the text chat history by **clicking**on the egg-timer like icon in the text chat window while chatting with a contact:



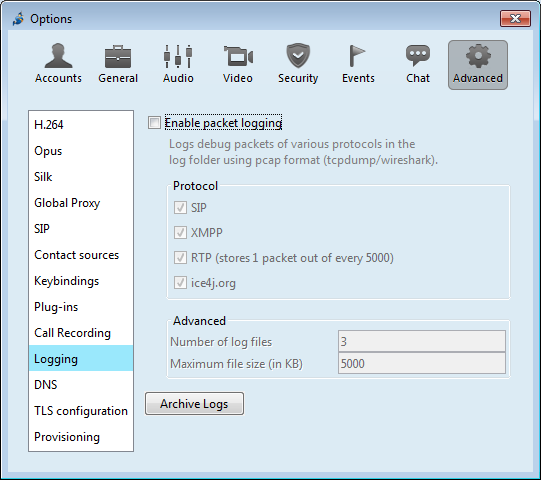
**Even if you encrypt the text chat with OTR all the text messages you send and receive are stored on your computer in open text format.**

To prevent Jitsi collecting this information (and remove already gathered data), **you and your contact should take the following steps.**

#### To disable Jitsi from collecting the information:

**Step 1**. **Select Tools > Options** in the menu, **select**the **General** tab and **uncheck**the **Log chat history** option.

**Step 2**. in the Options window, first **select the Advanced** tab, then **select the Logging** section, and then **uncheck the Enable packet logging** option as shown below:



Your changes will take effect after you **restart Jitsi**.

#### To remove already collected information about your calls and text messages:

**Step 1**. **Quit**Jitsi.

**Step 2**. Remove the entire log history folder history\_ver1.0 from the **Jitsi**user profile folder. You can remove a sub-folder of history\_ver1.0 if you want to dispose of only part of the history. The location of the user profile and log history folders depends on the operating system:

* On Windows XP and earlier, this is located in C:\Documents and Settings\<Windows login/user name>\Application Data\Jitsi\history\_ver1.0
* On Windows Vista, 7, 8, this is C:\Users\<Windows login/user name>\AppData\Roaming\Jitsi\history\_ver1.0
* Mac OS X: from your home folder ~/Library/Application Support/Jitsi/history\_ver1.0
* Linux: from your home folder ~/.jitsi/history\_ver1.0

See the **Secure Deleting lesson** for more on how to dispose of information securely.

### 2.4.2 Require private messaging when text chatting

It is recommended that you set **Jitsi**up to require private and encrypted text messaging using OTRencryptionwhenever possible. To do this, **select Tools > Options** in the menu, **select the Security** tab, **select the Chat** sub-tab and **check Require private messaging** at the bottom of the screen.

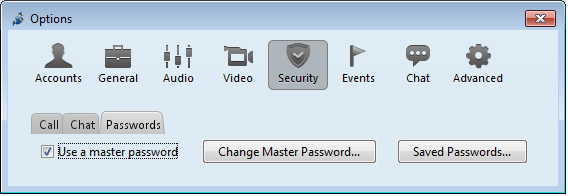
### 2.4.3 Protect passwords to your accounts with master password

It is best not to let Jitsi remember passwords to your accounts. If you decide otherwise for ease of use anybody who gets access to your computer will be able to log in to your accounts by simply starting Jitsi. It will also be possible to view your passwords in the Options window. It is therefore **strongly recommended** to protect passwords to your accounts with good **master password**. Once you set up the master password, Jitsi will ask you for it upon starting the program.

**Step 1**. **Open**the Options window by **selecting Tools > Options** in the menu, **select the Security** tab and **Passwords** sub-tab, and **check Use a master password** to activate the **Master Password** window.

**Step 2**. In the new window, **type in your password**. For more on creating a strong password, see the **Password lesson**.

**Step 3**. **Click OK** to confirm the password and activate a new window which should say **Master Password successfully set up**. **Click "OK"** to close it and come back to the Options window which should resemble below:



**Note**: The **Change Master Password** button lets you change the master password and the **Saved Passwords...** button lets you access the list of passwords remembered by Jitsi and remove them if need be.

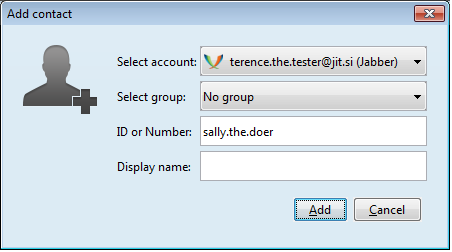
# Jitsi - Add contacts and communicate text & voice

## 3.1 Add contacts (buddies) to Jitsi

After adding at least one account to Jitsi and logging in, you are ready to add your contacts and communicate with them.

**Step 0**. Open the Jitsi main window by **selecting Start > Jitsi** or **double-clicking**the **Jitsi**desktop icon.

**Step 1**. **Select File > Add contact...** which will open the following window:



**Step 2**. **Select**which of your accounts you would like to add this contact to (for example terance.the.tester@jit.si).

**Optional**: You may also add the contact to a group among your other contacts. However, first you must create the group. You can do this by selecting **File > Create group...** from the menu).

**Type in** your contact's user name or address into the **ID or Number** field (for example, sally.the.doer@jit.si).

You can choose the name or nickname for the contact, which will be visible in your contacts list in the **Jitsi**main window; **type it into the Display name** field.

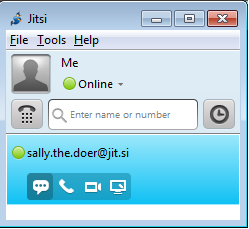
**Step 3**. **Click**on Add to close the Add contact window and come back to Jitsi main window. In your contact list you will now see your new contact added with the note "Waiting for authorisation".

**Step 4**. When your contact (sally.the.doer@jit.si) logs in to her account, a pop-up window will inform her that you have requested to add her to your list of contacts:

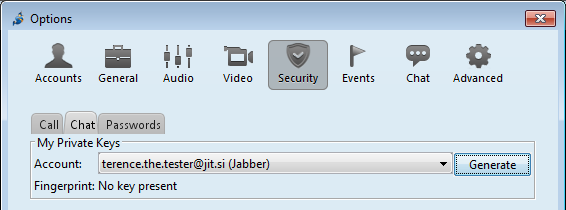
Your contact has a choice of selecting the Ignore option, in which case your request will continue awaiting authorisation; Deny, in which case you will receive information that your request was rejected; and Authorise, in which case you will receive information that your contact has accepted your authorisation request, and the entry for your contact in your contact list will become active.

## 3.2 Text chat (Instant Messaging) with OTR encryption

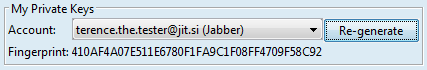
Now that you added and authorised your contact, you can click on their name in the contact list and initiate text conversation, voice or video calls, and desktop sharing, by choosing the relevant icon under their name:



**Step 1**. We will now explore one of Jitsi's most important features: the ability to text chat securely, encrypting your messages with OTR. OTR functions in a similar manner to GPG/PGPdescribed in other chapters in this toolkit. Just as with PGP, before you and your contact can encrypt your communications, you both need to configure **Jitsi**to generate your encryption keys. You can do this by **selecting Tools > Options** menu and **selecting the Security** tab and **Chat** sub-tab. You will then see a window similar to one shown in the image below:



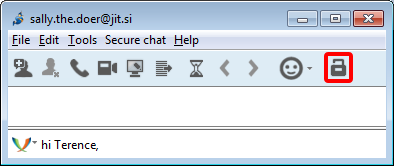
**Step 2**. Next, **click**the **Generate** button. As a result you will see the fingerprint of the key that has been generated:



One key is generated per account. You only need to do this again if you add a new account or install Jitsi on another device and do not move the existing keys to it.

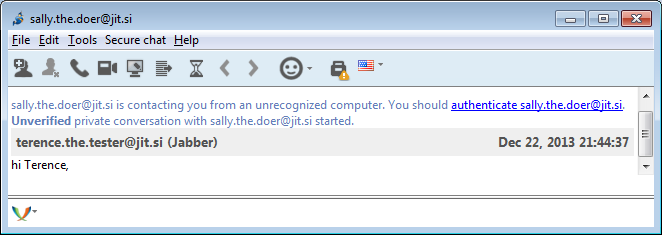
Now you are ready to communicate:

**Step 3**. **Select a contact**from Jitsi main window and **click**on the send message icon (first from the left under the contact's name) to open a text chat window:



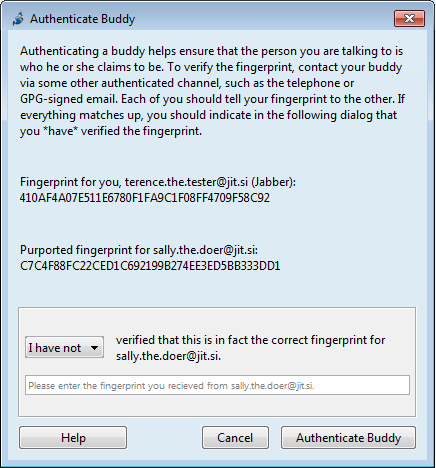
Note the Encrypt chat with OTR icon, the open padlock on the right-top side of the window. This inconspicuous symbol informs you whether the chat is encrypted or not. Now the lock is open (there is a tiny space between handle and the body of the lock!).

**Step 4**. **Click on the Encrypt chat with OTR icon**. Note the changes in the window:

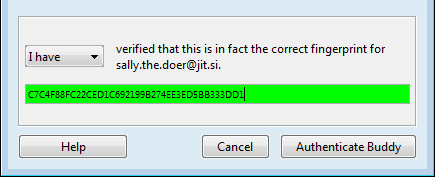


Observe that the padlock is now locked. This means that whatever messages you and your contact send to each other are encrypted. Note the message that this is an unverified private conversation and that you should authenticatesally.the.doer@jit.si.

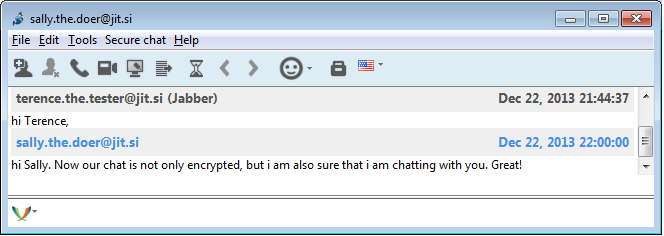
**Step 5**. **Click on the link authenticate sally.the.doer@jit.si** to open the Authenticate Buddy window:



Note the message that encourages you to compare the fingerprints of your keys with your contact over another channel (not this text chat). In doing this, you can be more certain that you are communicating with your contact and not somebody else. A good choice for key comparisons is to do it face to face, or via video or voice communication as these provide easier means to authenticate the identity of the other person. After you compare fingerprints, **select**the option **I have verified** the fingerprint from the pull-down menu and **click on Authenticate Buddy**:



Closing the Authenticate Buddy window returns you to the chat window.



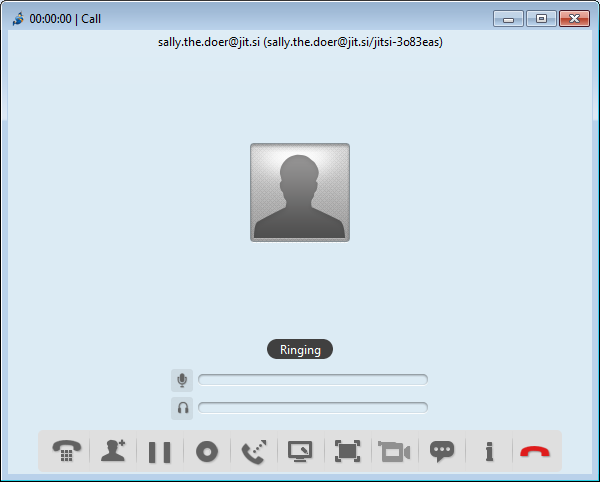
Note that padlock no longer includes the orange triangle with the white exclamation mark. This means that you have authenticated your contact. **The authentication should be done only once per contact.** If the triangle with exclamation mark returns, it means that you are chatting to somebody who you have not yet authenticated. This can happen when your contact moves to another device with another encryption key (another installation of Jitsi, or another OTR enabled program, etc.). In this case you will need to re-authenticate each other again to be sure of the identity of person with whom you communicate.

**Jitsi**allows you to text chat with more than one person in the same time. OTR encryption will only work when chatting to one person.

## 3.3 Voice and video chat with ZRTP encryption

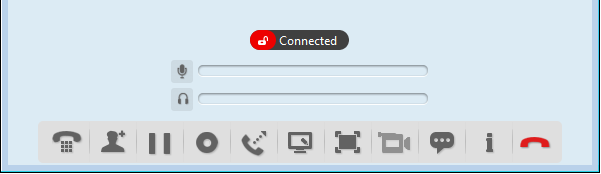
**Jitsi**offers voice and video chats which can be independently encrypted with open standard called ZRTP. In order to initiate the chat you need to

**Step 1**. **Click**on the contact in **Jitsi**contact list and **click**on the voice (second icon from the left under the contact's name) or video (third) icon. A new window will appear indicating that **Jitsi**is establishing the connection:



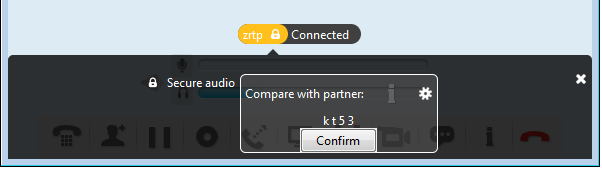
Your contact will see an incoming call notification.

**Step 2.** If your contact **accepts the call**you will receive information that you are connected:

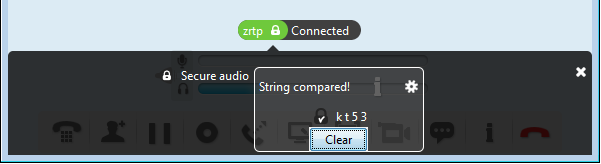


**Note** the red open padlock. This means that your call is not yet encrypted with ZRTP.

**Step 3.** **Wait...**Your and your contact's programs are establishing an encrypted connection, which may take a moment. If they succeed you will see the letters zrtp appear against an orange background with a closed padlock like below. If they don't succeed in establishing a connection, you still can chat but without encryption. You can disconnect, restart **Jitsi**and try again to see if this time the programs will connect with encryption. ZRTP may not work in calls between accounts from different providers (such as between Google and Jit.si).



**Step 4**. **Observe**the section under the letters zrtp and padlock with the message "Compare with partner" followed by 4 characters. **Read**these letters to your contact and ask if she sees the same characters. If she does, it means that your communication is encrypted and nobody is interfering with it. You can **click Confirm**. The orange zrtp field will turn green:



**Step 5**. You may close the black confirmation section of the window by clicking on the white x sign on upper-right part of the black section:

**Jitsi**lets you voice and video chat with more than one person. **Note**that with this communication, ZRTP encryption can be engaged between initiator of the call and other parties, but not between parties themselves.