# ADIUM TOOL GUIDE

Adium & OTR  
Secure instant messaging for Mac --------------------------------

**Lesson to read:** [**Sending a Message**](umbrella://lesson/sending-a-message)  
**Download Location:** <https://adium.im/>  
**Computer requirements** (Adium 1.5 or later): Mac OS X 10.6.8 or newer, an Apple-branded Macintosh computer.  
**Version used in this guide:** Adium 1.5.9  
**License:** GNU GPL  
**Other reading:** <https://pressfreedomfoundation.org/encryption-works>;<https://adium.im/help/>  
**Level:** Beginner-Intermediate  
**Time required:** 15-20 minutes

Adium is a free and open source instant messaging client for OS X that allows you to chat with individuals across multiple chat protocols, including Google Hangouts, Yahoo! Messenger, Facebook chat, Windows Live Messenger, AIM, ICQ, and XMPP.

OTR (Off-the-record) is a protocol that allows people to have confidential conversations using the messaging tools they?re already familiar with. This should not be confused with Google's ?Off the record,? which merely disables chat logging, and does not have encryption or verification capabilities. For Mac users, OTR comes built-in with the Adium client.

OTR employs end-to-end encryption. This means that you can use it to have conversations over services like Google Hangouts or Facebook without those companies ever having access to the contents of the conversations. This is different from the way in which Google and AOL use the term ?off the record? to mean that a conversation is not being logged; that option does not encrypt your conversation.

### Why should I use Adium + OTR?

When you have a chat conversation using Google Hangouts or Facebook chat on the Google or Facebook websites, that chat is encrypted using HTTPS , which means the content of your chat is protected from hackers and other third parties while it?s in transit. It is not, however, protected from Google or Facebook, which have the keys to your conversations and can hand them over to authorities.

After you have installed Adium, you can sign in to it using multiple accounts at the same time. For example, you could use Google Hangouts, Facebook, and XMPP simultaneously. Adium also allows you to chat using these tools without OTR. Since OTR only works if both people are using it, this means that even if the other person does not have it installed, you can still chat with them using Adium.

Adium also allows you to do out-of-band verification to make sure that you?re talking to the person you think you?re talking to and you are not being subject to a MITM attack. For every conversation, there is an option that will show you the key fingerprints it has for you and the person with whom you are chatting. A "key fingerprint" is a string of characters like "342e 2309 bd20 0912 ff10 6c63 2192 1928,? that?s used to verify a longer public key. Exchange your fingerprints through another communications channel, such as Twitter DM or email, to make sure that no one is interfering with your conversation.

### Limitations: When should I not use Adium + OTR?

Technologists have a term to describe when a program or technology might be vulnerable to external attack: they say it has a large ?attack surface.? Adium has a large attack surface. It is a complex program, which has not been written with security as a top priority. It almost certainly has bugs, some of which might be used by governments or even big companies to break into computers that are using it. Using Adium to encrypt your conversations is a great defense against the kind of untargeted dragnet surveillance that is used to spy on everyone's Internet conversations, but if you think you will be personally targeted by a well-resourced attacker (like a nation-state), you should consider stronger precautions, such as PGP -encrypted email.

### Installing Adium + OTR On Your Mac

Step 1: Install the program

First, go to <https://adium.im/> in your browser. Choose ?Download Adium 1.5.9.? The file will download as a .dmg, or disk image, and will probably be saved to your ?downloads? folder.

Double-click on the file; that will open up a window that looks like this:

Move the Adium icon into the ?Applications? folder to install the program. Once the program is installed, look for it in your Applications folder and double-click to open it.

Step 2: Set up your account(s)

First, you will need to decide what chat tools or protocols you want to use with Adium. The setup process is similar, but not identical, for each type of tool. You will need to know your account name for each tool or protocol, as well as your password for each account.

To set up an account, go to the Adium menu at the top of your screen and click ?Adium? and then ?Preferences.? This will open a window with another menu at the top. Select ?Accounts,? then click the ?+? sign at the bottom of the window. You will see a menu that looks like this:

Select the program that you wish to sign in to. From here, you will be prompted either to enter your username and password, or to use Adium?s authorization tool to sign in to your account. Follow Adium?s instructions carefully.

### How to Initiate an OTR Chat

Once you have signed in to one or more of your accounts, you can start using OTR.

**Remember: In order to have a conversation using OTR, both people need to be using a chat program that supports OTR.**

Step 1: Initiate an OTR chat

First, identify someone who is using OTR, and initiate a conversation with them in Adium by double-clicking on their name. Once you have opened the chat window, you will see a small, open lock in the upper left-hand corner of the chat window. Click on the lock and select ?Initiate Encrypted OTR Chat.?

Step 2: Verify your connection

Once you have initiated the chat and the other person has accepted the invitation, you will see the lock icon close; this is how you know that your chat is now encrypted (congratulations!) ? But wait, there?s still another step!

At this time, you have initiated an unverified, encrypted chat. This means that while your communications are encrypted, you have not yet determined and verified the identity of the person you are chatting with. Unless you are in the same room and can see each other?s screens, it is important that you verify each other?s identities. (For more information, read the EFF module on [Key Verification](https://ssd.eff.org/en/module/key-verification#overlay=en/node/37/).)

To verify another user?s identity using Adium, click again on the lock, and select ?Verify.? You will be shown a window that displays both your key and the key of the other user. Some versions of Adium only support manual fingerprint verification. This means that, using some method, you and the person with whom you?re chatting will need to check to make sure that the keys that you are being shown by Adium match precisely.

The easiest way to do this is to read them aloud to one another in person, but that?s not always possible. There are different ways to accomplish this with varying degrees of trustworthiness. For example, you can read your keys aloud to one another on the phone if you recognize each other?s voices or send them using another verified method of communication such as PGP. Some people publicise their key on their website, Twitter account, or business card.

**The most important thing is that you verify that every single letter and digit matches perfectly.**

Now that you have initiated an encrypted chat and verified your chat partner?s identity, there?s one more thing you need to do. Unfortunately, Adium logs your OTR-encrypted chats by default, saving them to your hard drive. This means that, despite the fact that they?re encrypted, they are being saved in plain text on your hard drive.

To disable logging, click ?Adium? in the menu at the top of your screen, then ?Preferences.? In the new window, select ?General? and then disable ?Log messages? and ?Log OTR-secured chats.? Your settings should now look like this:

Also, when Adium displays notifications of new messages, the contents of those messages may be logged by the OS X Notification Center. This means that while Adium leaves no trace of your communications on your own computer or your correspondent's, either your or their computer's version of OS X may preserve a record. To prevent this, you may want to disable notifications.

To do this, select "Events" in the Preferences window, and look for any entries that say "Display a notification." For each entry, expand it by clicking the gray triangle, and then click the newly-exposed line that say "Display a notification," then click the minus icon ("-") at the lower left to remove that line." If you are worried about records left on your computer, you should also turn on full-disk encryption, which will help protect this data from being obtained by a third party without your password.