

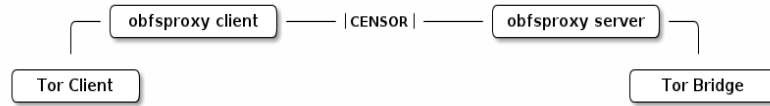
HOME » PROJECTS » OBFSPROXY

Software &amp; Services

**Tor Tip**

Tor is written for and supported by people like you. [Donate today!](#)

## Setting up an Obfsproxy Bridge on Debian/Ubuntu



**Hey!** If you are **not** using Debian or Ubuntu, you better look [at this other guide](#) which sets up Obfsproxy from source.

This is a **Debian/Ubuntu** guide for installing the Python version of obfsproxy. If you are still using the C version, we recommend you to upgrade to the Python version!

### Step 0: Install a recent version of Tor (>= 0.2.4.1)

Add the [official Tor APT repository](#) and run the specified commands to install tor and deb.torproject.org-keyring. You need *Tor 0.2.4.x* because it knows how to automatically report your obfsproxy address to [BridgeDB](#).

### Step 1: Install obfsproxy

Since you installed the Tor APT repository, installing obfsproxy is now a matter of running a command:

```
# apt-get install obfsproxy
```

### Step 2: Configure Tor

Edit your `/etc/tor/torrc` to add:

```
SocksPort 0
ORPort auto
BridgeRelay 1
Exitpolicy reject *:.*

## CHANGEME_1 -> provide a nickname for your bridge, can be anything you like
#Nickname CHANGEME_1
## CHANGEME_2 -> provide some email address so we can contact you if there's a problem
#ContactInfo CHANGEME_2

ServerTransportPlugin obfs3 exec /usr/bin/obfsproxy managed
```

Don't forget to uncomment and edit the *CHANGEME* fields!

### Step 3: Launch Tor and verify that it bootstraps

Restart Tor to use the new configuration file. (Preface with `sudo` if needed.)

```
# service tor restart
```

Now check `/var/log/tor/log` and you should see something like this:

```
Nov 05 16:40:45.000 [notice] We now have enough directory information to build circuits.
Nov 05 16:40:45.000 [notice] Bootstrapped 80%: Connecting to the Tor network.
Nov 05 16:40:46.000 [notice] Bootstrapped 85%: Finishing handshake with first hop.
Nov 05 16:40:46.000 [notice] Bootstrapped 90%: Establishing a Tor circuit.
Nov 05 16:40:48.000 [notice] Tor has successfully opened a circuit. Looks like client functionality
Nov 05 16:40:48.000 [notice] Bootstrapped 100%: Done.
```

If Tor is earlier in the bootstrapping phase, wait until it gets to 100%.

### Step 4: Set up port forwarding if needed

If you're behind a NAT/firewall, you'll need to make your bridge reachable from the outside world — both on the ORPort and the obfsproxy ports. The ORPort is whatever you defined in step two above. To find your obfsproxy ports, check your Tor logs for a line similar to this one:

```
Oct 05 20:00:41.000 [notice] Registered server transport 'obfs3' at '0.0.0.0:42000
```

The last number in each line, in this case *26821* and *42000*, is the TCP port number that you need to forward through your firewall. (The ports are randomly chosen the first time Tor starts, but Tor will cache

and reuse the same number in future runs.) If you want to change the number, use Tor 0.2.4.7-alpha or later, and set something similar to "ServerTransportListenAddr obfs3 0.0.0.0:26821" in your torrc.



Trademark, copyright notices, and rules for use by third parties can be found [in our FAQ](#).

#### About Tor

[What Tor Does](#)  
[Users of Tor](#)  
[Core Tor People](#)  
[Sponsors](#)  
[Contact Us](#)

#### Get Involved

[Donate](#)  
[Mailing Lists](#)  
[Mirrors](#)  
[Hidden Services](#)  
[Translations](#)

#### Documentation

[Manuals](#)  
[Installation](#)  
[Guides](#)  
[Tor Wiki](#)  
[General Tor FAQ](#)

