I2P

The Invisible Internet Project

Welcome to the Invisible Internet

The Invisible Internet is a privacy by design, people-powered network. It is a truly free and anonymizing Internet alternative. Get I2P.

Get I2P 0.9.50

What is I2P?

The Invisible Internet Project (I2P) is a fully encrypted private network layer. It protects your activity and location. Every day people use the network to connect with people without worry of being tracked or their data being collected. In some cases people rely on the network when they need to be discrete or are doing sensitive work.

I2P Cares About Privacy

I2P hides the server from the user and the user from the server. All I2P traffic is internal to the I2P network. Traffic inside I2P does not interact with the Internet directly. It is a layer on top of the Internet. It uses encrypted unidirectional tunnels between you and your peers. No one can see where traffic is coming from, where it is going, or what the contents are. Additionally I2P offers resistance to pattern recognition and blocking by censors. Because the network relies on peers to route traffic, location blocking is also reduced.

Peer-to-Peer

The network is people powered . Peers make a portion of their resources, particularly bandwidth, available to other network participants. This allows the network to function with relying on centralized servers. **Learn more about the Protocol Stack.**

Privacy and Security By Design

I2P has created transport protocols that resist DPI censorship, and continuously improves its end to end encryption. **Read the I2P Transport Overview.**

Built For Communication

I2P has an application layer with easy to use **APIs** for creating your own privacy - aware apps.

News & Updates

2021-05-17 - **0.9.50 Release**

2021-02-17 - **0.9.49 Release**

2020-12-10 - **Hello Git, Goodbye Monotone**

2020-11-30 - **0.9.48 Release**

2020-08-24 - **0.9.47 Release**

2020-06-07 - **Help your Friends Join I2P by Sharing Reseed Bundles**

2020-05-25 - **0.9.46 Release**

2020-03-18 - **Using a git bundle to fetch the I2P source code**

More blog posts...

Windows
Mac OS X
GNU/Linux / BSD / Solaris
Debian / Ubuntu
Android
Source package
Automatic updates
Manual updates

I2P for Mac OS X

Latest version: 0.9.50.jar

⬇ **Download**

Installation Instructions

You will need Java to run I2P

select alternate mirror sig

What is this?

SHA256:
34902d2a7e678fda9261d489ab31566

What is this?

I2P for Android

Latest version: 0.9.50.jar

Outside I2P

Google Play

F-Droid

Installation Instructions

Android comes with a Java virtual machine as part of the platform, which I2P for Android uses. Therefore it is not necessary to install Java to use I2P for Android.

select alternate mirror sig

What is this?

SHA256:
34902d2a7e678fda9261d489ab31566

What is this?

Updates from earlier releases:

Both automatic and manual upgrades are available for the release.

If you are running 0.7.5 or later, your router should detect the new release. To upgrade simply click the 'Download Update' button on your router console when it appears.

Since 0.9.23, some releases are signed by str4d, whose signing key has been in the router since 0.9.9. Routers older than 0.9.9 will fail to verify update files signed by str4d, and will need to be manually updated using the process below.

Download I2P for Manual updates

i2pupdate_0.9.50.zip

select alternate mirror

Windows
Mac OS X
GNU/Linux / BSD / Solaris
Debian / Ubuntu
Android
Source package
Automatic updates
Manual updates

I2P for Docker
Latest version: 0.9.50.jar

Docker Hub

I2P is now available as a Docker package from the Docker Hub. You may retrieve the image by running the 'docker pull' command.

`docker pull geti2p/i2p`

Installation Instructions

I2P Source Package
Latest version: 0.9.50.jar

⬇ Download

Alternately, you can fetch the source from monotone or via Git from git.repo.i2p or Github.

Run (`tar xjvf i2psource_0.9.50.tar.bz2 ; cd i2p-0.9.50 ; ant pkg`) then either run the GUI installer or headless install as above.

Android source is in git and on Github. Android builds require the I2P source. See the documentation in the Android source for additional build requirements and instructions.

select alternate mirror sig

What is this?

SHA256:
34902d2a7e678fda9261d489ab31566

What is this?

Updates from earlier releases:

Both automatic and manual upgrades are available for the release.

If you are running 0.7.5 or later, your router should detect the new release. To upgrade simply click the 'Download Update' button on your router console when it appears.

Since 0.9.23, some releases are signed by str4d, whose signing key has been in the router since 0.9.9. Routers older than 0.9.9 will fail to verify update files signed by str4d, and will need to be manually updated using the process below.

Download I2P for Manual updates

i2pupdate_0.9.50.zip
Mirror: 🇺🇸 Launchpad

select alternate mirror sig

1. Download the file to your I2P installation directory and **rename as**

Will update these boxes. Screenshots from website.

Your download will begin shortly. If it doesn't start within 5 seconds, click here.

When your download is complete, choose the instructions for your operating system and follow the steps in the Installation Instructions. You will also configure your browser and take additional steps in the Configuration page after you have completed the installation.

Choose the installation instructions for your operating system:

Mac OS Instructions	Linux Instructions	Docker Instructions
Windows Instructions	Android Instructions	Debian and Ubuntu Instructions

Mac, Windows, and Linux:

Java is required the run I2P. Download it here.
Directions for terminal and command line (headless) install.

For Android:

Android comes with a Java virtual machine as part of the platform, which I2P for Android uses. Therefore it is not necessary to install Java to use I2P for Android

Debian and Ubuntu:

On Debian and Ubuntu when using a .deb package to install, the system will

Download Java

Download Java if you have not already. Otherwise, jump to I2P Installation.

Since the I2P software is not from the app store, Apple lets us know that. The message warns us that the developer is not known, but we can go ahead and click okay. The I2P software is open source, and we can see who maintains it and active development. Once we get comfortable, we might even want to help them out!
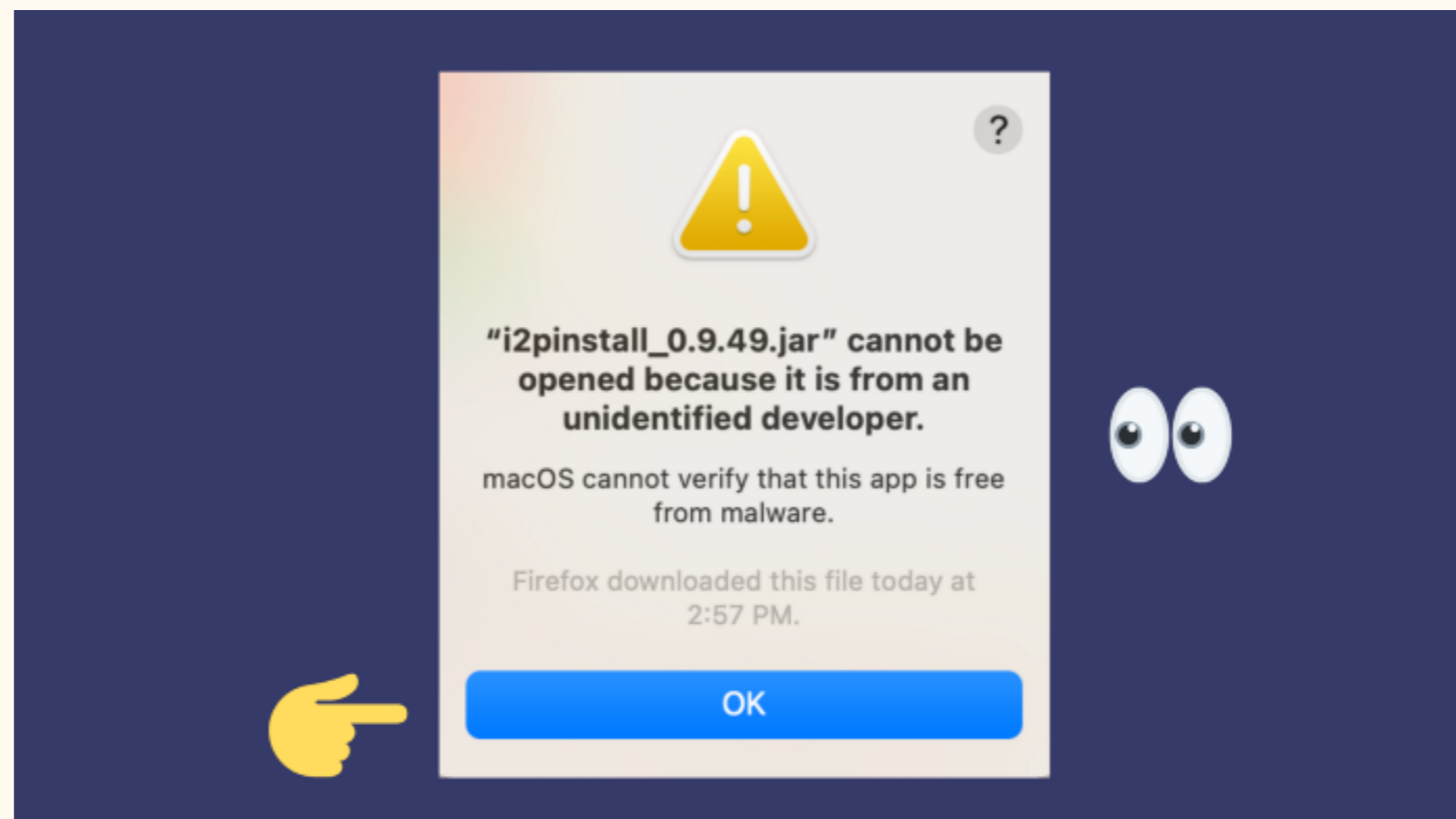

To install the software on our computer, we need to confirm that we are making an informed choice to open it.
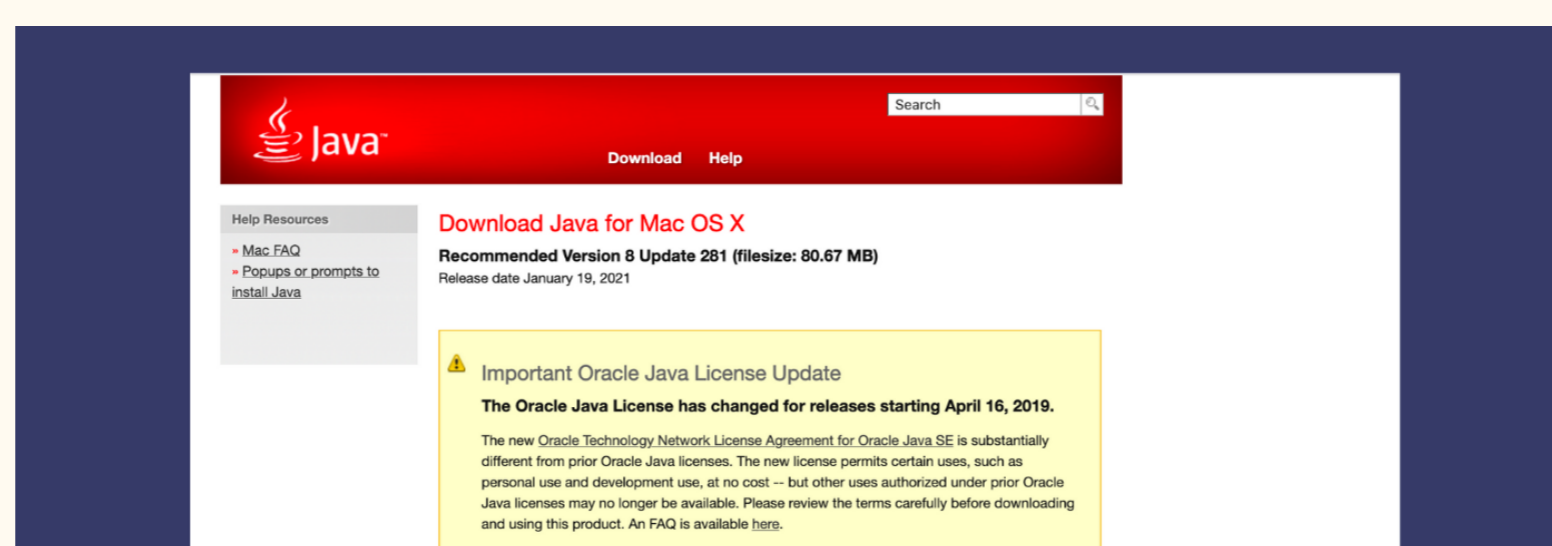
To do this, go to your Apple icon, then to System Preferences, and then to Security and Privacy. You will end up here where a message that your I2P install process has been blocked. Click on "Open Anyway."
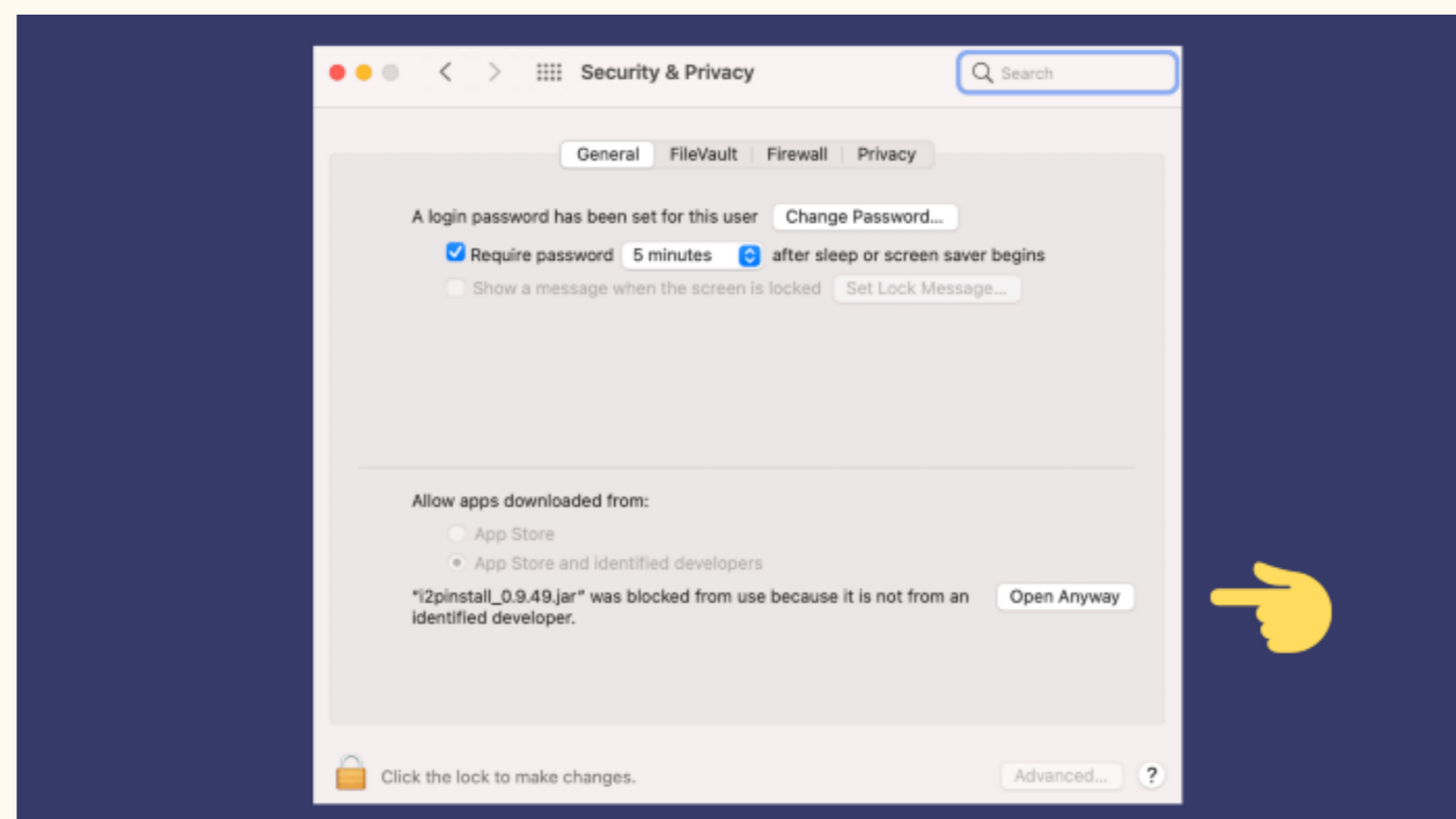
We appreciate the abundance of caution, and the message letting us know what our consequences are. The message options here will default to "Cancel," but we will choose "Open" instead.
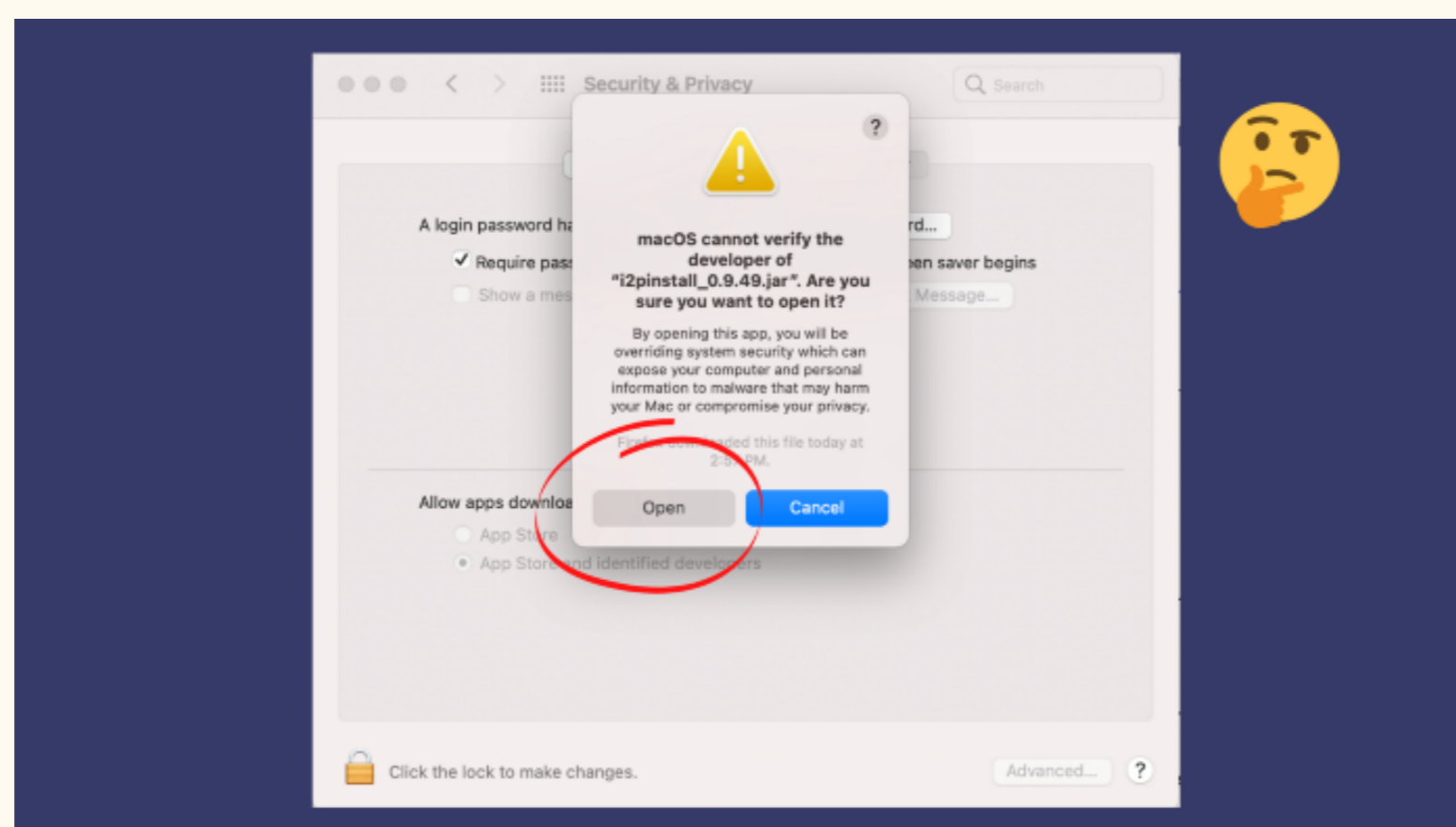
Whups! We went through all of that and it cannot be completed! That's right — we need Java for I2P to work.

Configuring Your I2P Network Connections

Browser Configuration ▼

This page will become very long. Can we tuck some info away in one of those drop downs with an arrow

- Firefox
- Chrome
- Android
- Internet Explorer 8

### Firefox

Experimental, extension-based Configuration

A new way of automatically configuring the I2P Browser is currently being tested. It uses the Firefox's "Container Tabs" to build private browsing tools for use with I2P and I2P applications.
It does pre-configuration of your browser by enabling some of the privacy Browser Settings like ResistFingerprinting, and enforces WebRTC proxy obedience. It also contains menus, shortcuts, and monitoring tools improving Firefox's integration with I2P. It is a by-product of the I2P Browser project.

The extension, I2P in Private Browsing, can be obtained from the Mozilla add-on store.

Instructions for Firefox 57 and above:

From the Menu button in the top right, select *Preferences*. Scroll down until you see the *Network Proxy* section, as shown in the screenshot below. Click on *Settings*
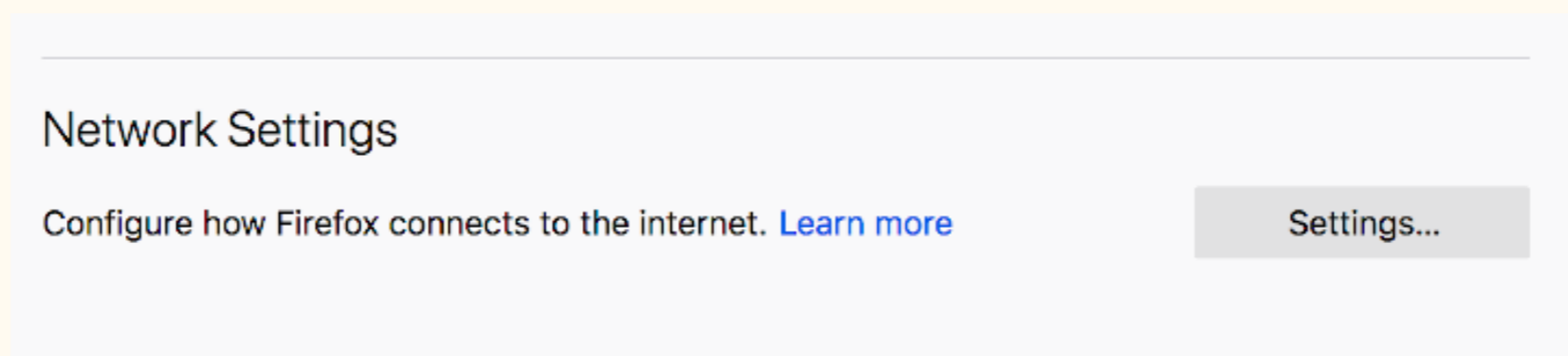
In the *Connection Settings* pop-up, select *Manual proxy configuration*. Set both the HTTP and SSL Proxy to address 127.0.0.1 with port 4444 as shown in the following screenshot.
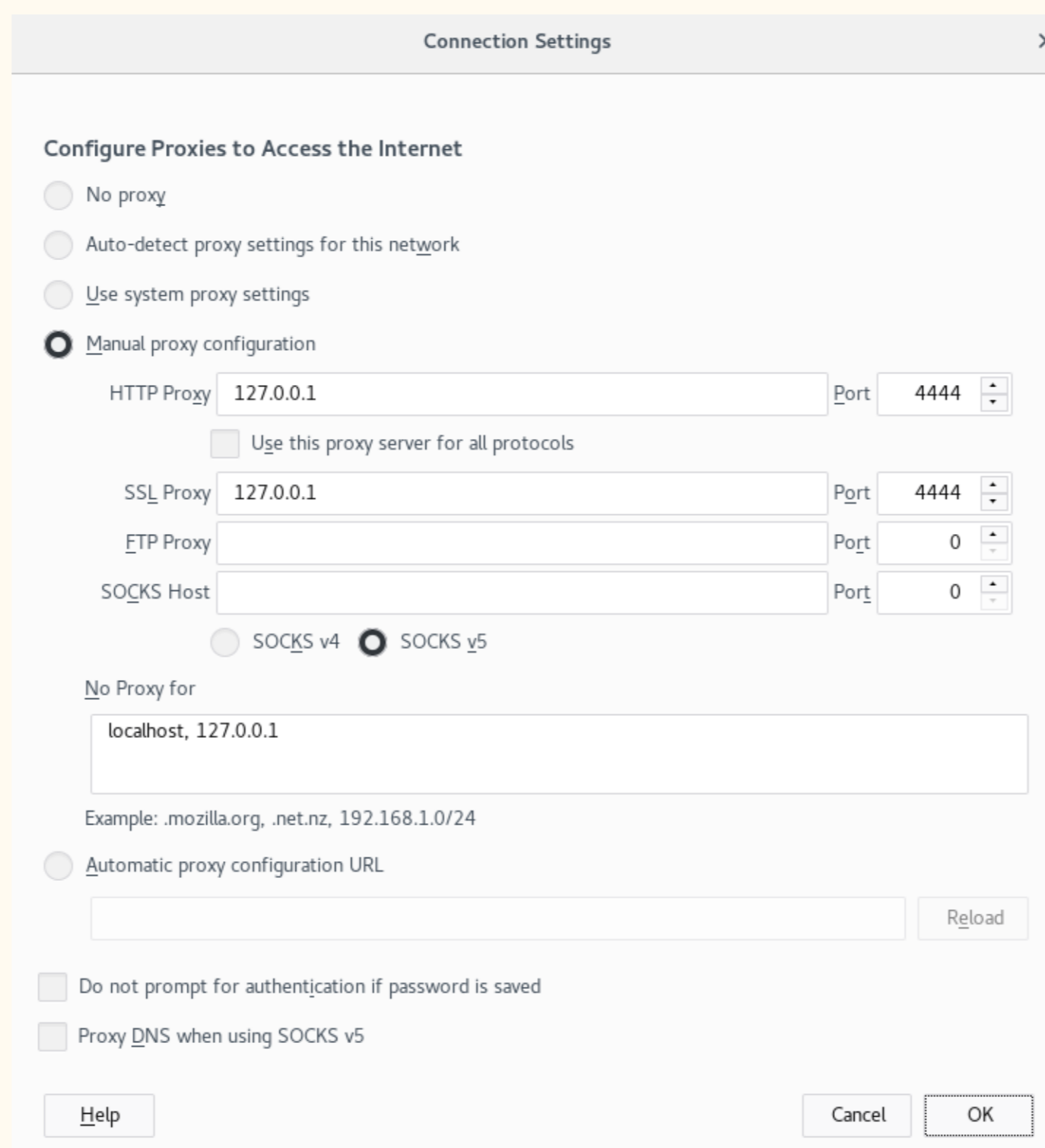
Finally, go to the address *about:config* and find the property media.peerConnection.ice.proxy_only. Ensure that this setting is True.