Configuring FProxy

Before you can start developing modifications, you need to:

1. Initialize a directory for your site's modification content.
2. Install the SSL certificate for the FProxy server, if you're using HTTPS.

Make sure you also understand where the FProxy configuration files are located.

You can remove initialized directories that you no longer need.

Initializing a directory for a site

Initializing a directory means setting up a **sites directory** for storing the modification content for one or more sites. Once you've set up a sites directory, you can download modification content to it, and you can then edit the content locally rather than in the Frosmo Control Panel. The modification content is stored in individual **site directories** inside the sites directory.

You can initialize as many sites directories as you want. For example, if you have multiple sites, you can initialize one directory per site, or you can initialize a single directory for all the sites. However, if you try to initialize a sites directory for a site whose settings are already stored in another sites directory, FProxy will prompt you to move the site from the other directory to the current one. You can also initialize the same sites directory multiple times, in which case you can add new sites to the directory.

To initialize a sites directory for a site:

1. In your terminal, go to the directory that you want to initialize. If the directory does not exist, create it. The following example creates and opens the `/dev/my_sites` subdirectory in your home directory:

   ```
   mkdir ~/dev/my_sites
   cd ~/dev/my_sites
   ```

   In Windows, the `/dev` directory would be a symbolic link from the WSL to the Windows main system, so that you can edit the modification content files in a Windows application yet still manage the files with FProxy in the WSL.

2. Start the initialization process:

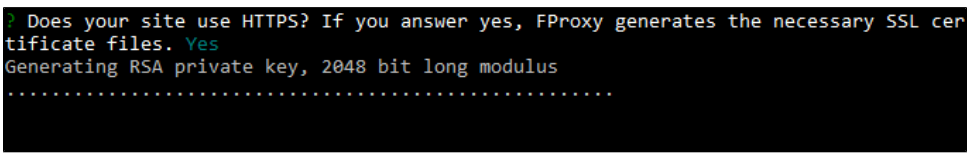
   ```
   fproxy init
   ```

   If you exit the initialization process before completing the final step, run `fproxy init` again.

3. Define the port number for the FProxy server. To use the default port number, simply press **Enter**. To use a custom port number, enter the port number, and press **Enter**.

   Once you've selected the port number, FProxy will no longer prompt for it on subsequent initializations. If you want to later change the port number, edit the `~/.fproxy/config.json` file, and change the `port` value to the new port number.

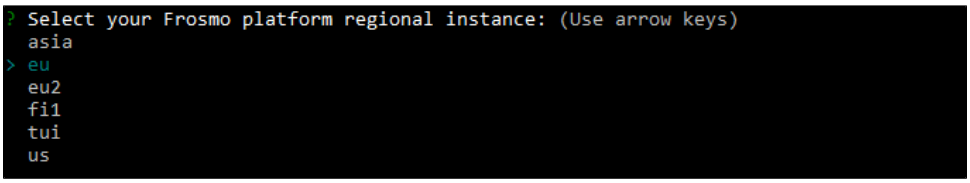
4. Select whether you want to use HTTPS with the FProxy server. If you do, enter "y", and press **Enter**. Otherwise, enter "n", and press **Enter**. If you select to use HTTPS, FProxy generates the necessary SSL certificate files and stores them in the `~/.fproxy/certificates` directory.

   If any of your sites uses HTTPS, you need to use HTTPS also with the FProxy server.

   Once you've selected whether or not to use HTTPS, FProxy will no longer prompt for it on subsequent initializations. If you later change your mind, edit the `~/.fproxy/config.json` file, and change the `port` value to `0` (without quotation marks). When you next initialize a sites directory, FProxy again prompts for HTTPS use.

5. Select the Frosmo Platform regional instance in which your site is hosted. Use the arrow keys to select the correct region, and press **Enter**.



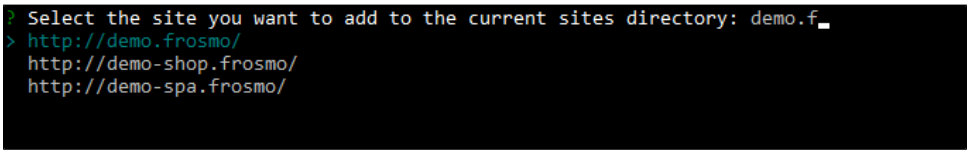
6. Provide your personal Graniitti API access token. Press **Enter** to open your default text editor, paste the token into the editor, save the changes, and exit the editor. FProxy stores the access token in a `~/.graniitti/graniitti_<domain>.token` file. For instructions on how to get the token, see the Graniitti API guide.

   > Check that the access token is pasted in full. Some editors may clip parts of the token. If this happens, check the paste settings for your editor.

   > Once you've provided the access token, FProxy will no longer prompt for it on subsequent initializations. If you want to later change the access token, either edit the `~/.graniitti/graniitti_<region_domain>.token` file, and replace the existing token with the new one, or delete the file, and run directory initialization to get a reprompt for the token.

   > FProxy will notify you when the token has expired. For instructions on how to get a new token, see the Graniitti API guide.

7. Select the site for which you want to initialize the directory. Use the up and down arrow keys to scroll the list and select the site you want, and press **Enter**. You can also filter the site list by typing the site name or origin.



8. Define the site directory name. To use the default name, simply press **Enter**. The default name is the Frosmo origin for the site, with periods and slashes replaced with underscores. To use a custom name, enter the name, and press **Enter**.

You have initialized the sites directory for the selected site. You can now download the site's modification content to the directory.

FProxy saves the site settings to the `.fproxy/sites.json` file in the sites directory and the global settings to various files in the `~/.fproxy directory`. For more information, see Configuration files.

Configuration files

The FProxy initialization process creates and updates the following configuration files. The scope indicates whether the file is global, meaning the settings affect FProxy at large, or local, meaning the settings are specific to each sites directory (and its sites).

Table: Configuration files

File	Description	Scope
`~/.fproxy/config.json`	General configuration settings, such as the FProxy server port number and certificate file names, and the locations of the `directories_config` and `sites_directory` configuration files.	Global
`~/.fproxy /directories_config. json`	Settings for the sites directories that FProxy currently has initialized.	Global
`~/.fproxy /sites_directory.json`	Settings for the site directories that FProxy currently has initialized.	Global
`~/.fproxy /certificates`	Self-signed SSL certificate files for use with the FProxy server.	Global
`~/.graniitti /graniitti.<domain>. token`	Graniitti API access token for a given Frosmo Platform regional instance.	Global
`<sites_directory>/. fproxy/sites.json`	Settings for the sites for which this sites directory has been initialized.	Local
`<sites_directory> /certs`	SSL certificate files used to generate the final self-signed certificate files stored in the `~/.fproxy /certificates` directory.	Local

Removing obsolete directories

You can remove site directories and whole sites directories that you no longer need.

To remove a directory:

1. In your terminal, remove the directory. The following example removes the `/dev/my_sites` sites directory and all its contents in your home directory:

   ```
   rm -rf ~/dev/my_sites
   ```

2. Remove the directory settings from the FProxy configuration:

   ```
   fproxy prune
   ```

   FProxy updates its configuration as follows:

   - If you removed a site directory, FProxy removes the site from the `~/.fproxy/sites_directory.json` and `<sites_directory>/.fproxy/sites.json` files.
   - If you removed a sites directory, FProxy removes the directory from the `~/.fproxy/directories_config.json` file and all related sites from the `~/.fproxy/sites_directory.json` file.

Installing the SSL certificate

If you selected to use HTTPS with the FProxy server, you must install an SSL certificate for the server on your browser. If you use a browser other than Firefox, such as Chrome or Safari, it is enough that you install the certificate on your operating system. Your browser will then automatically use that certificate. If you use Firefox, you need to additionally define a security exception for the certificate.

Installing the SSL certificate on Linux

To install the SSL certificate on Linux, follow the instructions for your Linux distribution. You can find the FProxy certificate files in the `~/.fproxy/certificates` directory.

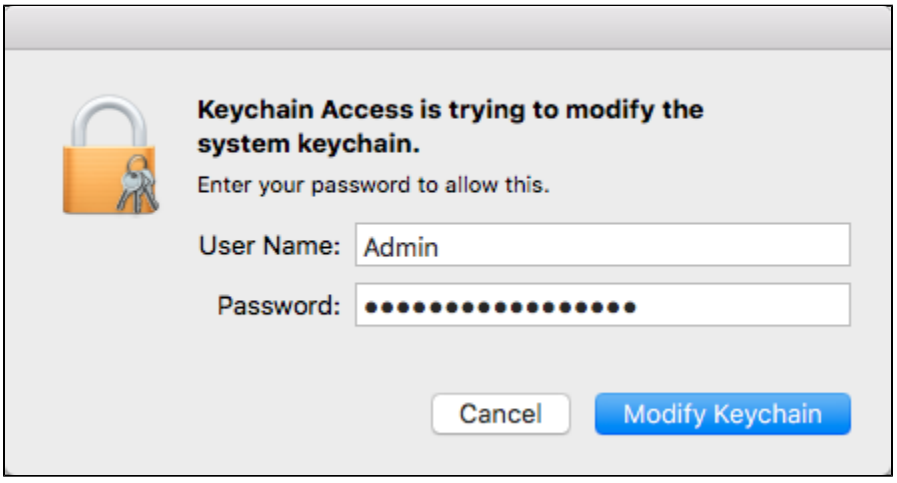
Installing the SSL certificate on macOS

To install the SSL certificate on macOS:

1. Open Finder, and navigate to the `~/.fproxy/certificates` directory.

   > To show hidden files in Finder, press **CMD + SHIFT + .** (period).

2. Double-click the `localhost.crt` file. Keychain Access opens.
3. In the **Add Certificates** window, in the **Keychain** field, select **System**. Click **Add**.
4. Enter your password, and click **Modify Keychain**.

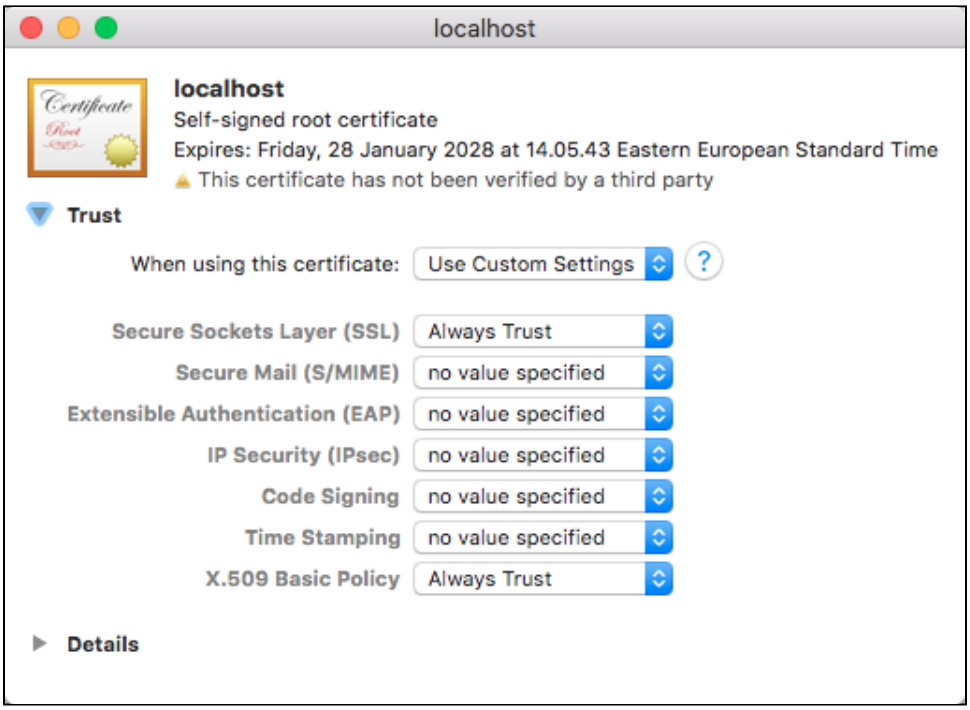


5. Select **Keychains > System**, and select **Category > Certificates**.

6. In the certificates list, select **localhost**, and click **i**.

7. Expand the **Trust** section, and change the following settings to **Always Trust**:

   - **Secure Sockets Layer (SSL)**
   - **X.509 Basic Policy**



8. Close the windows.

> You may need to restart your browser for the certificate to be loaded.

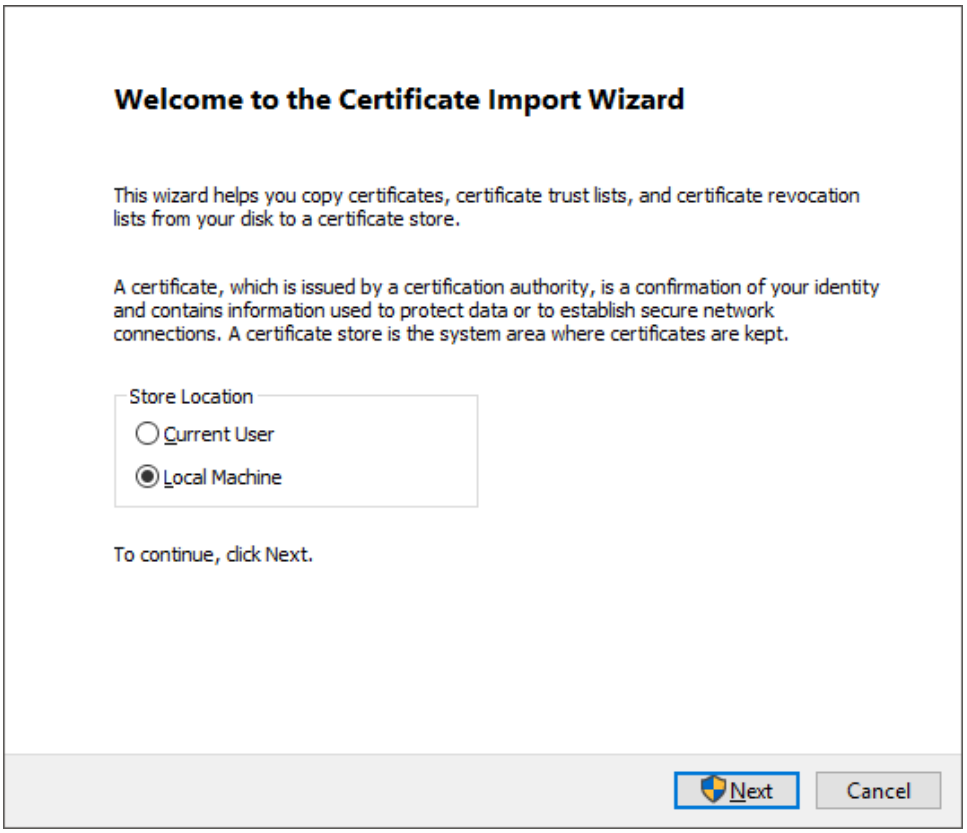
Installing the SSL certificate on Windows 10

To install the SSL certificate on Windows 10:

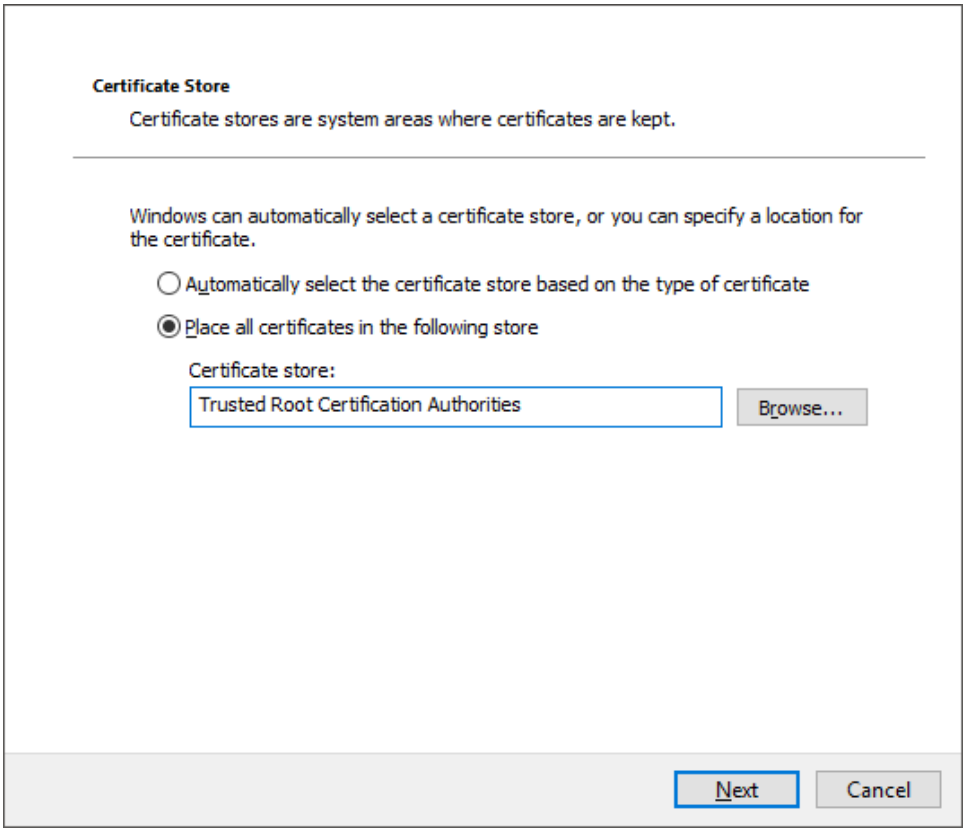
1. In your terminal, copy the certificate files from the `~/.fproxy/certificates` directory to your Windows storage directory. The following example copies the `certificates` directory to `dev`, which is a symbolic link to a Windows directory.

   ```
   cp -r ~/.fproxy/certificates ~/dev
   ```

2. Open File Explorer, and navigate to the directory where you copied the certificate files.
3. Right-click the `localhost.crt` file, and select **Install Certificate**. The Certificate Import Wizard opens.
4. Select **Local Machine**, and click **Next**.



5. If you get a User Account Control prompt for application permission, click **Yes**.
6. Select **Place all certificates in the following store**, click **Browse**, find and select **Trusted Root Certification Authorities**, and click **OK**. Click **Next**.



7. Click **Finish**.
8. Click **OK**.

You may need to restart your browser for the certificate to be loaded.

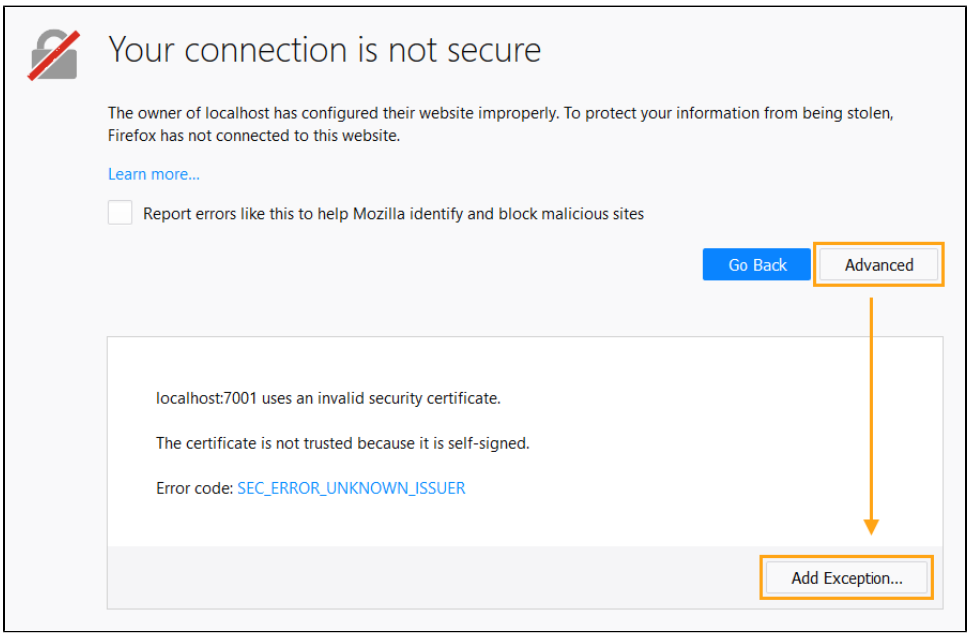
Installing the SSL certificate on Firefox

To install the SSL certificate on Firefox:

1. Install the certificate on your operating system. For more information, see Installing the SSL certificate on macOS or Installing the SSL certificate on Windows 10.
2. Open Firefox.
3. In the URL field, enter your FProxy URL and port number. For example:

   ```
   https://localhost:7001/
   ```

   Firefox opens an insecure connection error page.
4. On the page, click **Advanced**, and click **Add Exception**.



5. At the bottom of the window, select **Permanently store this exception**, and click **Confirm Security Exception**.