# FMProxy Trial Documentation

---

Thank you for taking the time to try out a beta version of FMProxy.

In this document you will find information on installing, configuring and running FMProxy, as well as guidance on how to interpret log files.

## Why does FMProxy exist?

We built FMProxy as a security and observability tool for FileMaker Server.

When you run FMProxy in front of your FileMaker Server it will continuously analyze the network packets going in and out of the server (from and to the connecting clients). This gives you information about who is connecting to your server with what kind of client setup (e.g. version, serial number, operating system), and can also alert you in case any unusual/suspicious traffic is being detected.

We invested a substantial amount of time to understand the communication protocol between FileMaker Server and its clients. During this research, we found several ways to bypass authentication and authorization mechanisms and found issues concerning the availability as well. Several of these vulnerabilities were already reported by us and fixed by Claris.

With regular new releases, further research and newly evolving attack patterns, we think there is a constant need for administrators to have more insight into their FileMaker Server's and hosted solutions' activity, and be able to detect specific exploitation attempts targeting FileMaker's network protocol.

FMProxy has knowledge about several FileMaker-specific vulnerabilities (both publicly known and not-yet known) and will write log entries whenever a potential security issue is detected. Beyond this, known malicious payloads to crash the FileMaker Server database process can even be terminated before ever reaching your server.

Finally, you can give FMProxy a list of trusted client IDs such that you will be informed whenever new/unknown clients connect to your server (even before logging in).

## What is the development state of FMProxy?

Currently, FMProxy is still in a beta phase to validate feasability and reliability of our approach. A fully featured trial version was given to you for testing/evaluation.

Please note that this trial version will expire after 60 days. We continue development and will create new builds every now and then.

During the beta phase, we hope to receive feedback from you and will continue to provide you access to new versions as they are released. Please be prepared that the software might undergo certain changes during this process.

Please do not use FMProxy for any production/critical workloads during the beta phase!

## Can attacks/detections be demonstrated?

We have developed several tools to demonstrate attacks against different versions of FileMaker Server including the latest one. Performing these demonstrations will allow you to see FMProxy's detection capabilities.

For obvious reasons we don't distribute the attack tools publicly, so please contact us at support@fmproxy.com to setup a meeting with us and lets us know about your target (test) server.

## How to run/install FMProxy?

There are two ways of running/installing FMProxy.

1. Manually via the Command Line, without installation. Useful for experimentation and easy modification of configuration parameters.
2. Using the provided installer which installs FMProxy as a background service. The installer also makes sure to modify the FileMaker Server configuration as required.

FMProxy should always run on the host which also runs FileMaker Server. For experimentation, you can also run the proxy on a separate machine. Please be aware, though, that there could be connection issues, added latency and potential problems with container data in this scenario. Also, the installer can only be used when FMProxy is installed on the same machine as FileMaker Server.

### Examples of manually running FMProxy

When running FMProxy manually, you have to adjust the port FileMaker Server is listening on (as the proxy has to take over port 5003).

To do this, please first completely shutdown FileMaker Server, then make the following changes in `FileMaker Server/Data/Preferences/dbs_config.xml`. The `DataPort` setting must be changed to any available port (e.g. 5004) and the `UseSecureConnection` setting to the value of `0`.

While you can also run the proxy on any other port, 5003 is recommended as FileMaker Pro client default to using this port. In any case it is recommended to use a non-privileged port (i.e. a port >= 1024) such that FMProxy can run without root permissions.

The `UseSecureConnection` setting will turn off transport encryption. Since you will run FMProxy in front of FileMaker Server, clients will still be able to establish a secure connection to the proxy if you have specified a certificate/private key. Unencrypted traffic never leaves the local host.

To start the proxy on port 5003 on all interfaces, with FileMaker Server running on localhost port 5004, use the following command:

```
./fmproxy --proxy 0.0.0.0:5003 --target 127.0.0.1:5004
```

To start the proxy on localhost port 5003, with FileMaker Server running on a remote host on port 5003, use the following command (experimental):

```
./fmproxy --proxy 127.0.0.1:5003 --target 1.2.3.4:5003
```

To use a TLS/SSL certificate for client connections, use the `--certificate` and `--private-key` options:

```
./fmproxy --proxy 0.0.0.0:5003 --target 127.0.0.1:5004 --certificate /path/to/certificate.pem --private-key /path/to/private/key.pem
```

Tip: if you already have a certificate installed on FileMaker Server, you can just specify the path to the existing certificate and key files to `FileMaker Server/CStore/serverCustom.pem` and `FileMaker Server/CStore/serverKey.pem`, respectively.

#### Using a config file (recommended)

In addition or alternatively to specifying all options via the command line, you can also pass a JSON config file to FMProxy using the `--config` option. The keys in the JSON file are named the same as the command line arguments with the exception of underscores replacing the dashes. Here is an example config:

```
{
    "proxy": "0.0.0.0:5003",
    "target": "127.0.0.1:5004",
    "debug": true,
    "trusted_clients": "trusted_clients.txt",  # note the underscore (compared to --trusted-clients)
    "log_dir": "/tmp"
}
```

If you pass both a config file and command line arguments, the command line options take precedence.

When you install FMProxy using the provided installer, a default config file will be placed at `/etc/fmproxy`.

#### Getting help

To get help on all available options, use the `--help` flag:

```
$ ./fmproxy --help

FMProxy - Security proxy for FileMaker Server

Usage: fmproxy [OPTIONS]

Options:
      --config <CONFIG>
          Path to a JSON config file
      --proxy <PROXY>
          Address of proxy server (e.g. 0.0.0.0:5003)
      --target <TARGET>
          Address of target server (e.g. 1.2.3.4:5004)
      --debug
          Enable debug output
      --certificate <CERTIFICATE>
          Path to TLS/SSL certificate in pem format
      --private-key <PRIVATE_KEY>
          Path to private key in pem format
      --trusted-clients <TRUSTED_CLIENTS>
          Path to text file consisting of persistent IDs of trusted clients (one ID per line)
      --log-dir <LOG_DIR>
          Path of directory where log files should be stored. Default is current directory. Directory must already exist.
      --cache-dir <CACHE_DIR>
          Path to a directory where cache files should be stored. Directory must already exist.
      --no-cache
          Don't load cache files at startup
      --passive
          Prevents the proxy from actively fetching data from FileMaker Server (e.g. information about available databases and their attributes)
  -h, --help
          Print help
  -V, --version
          Print version
```

### Using the installer

#### macOS

Coming soon...

#### Windows

Coming soon...

#### Linux

After downloading the FMProxy package, you can extract the archive and then run the provided installer (make sure you have the package for the correct architecture, i.e. x86 or arm).

The following commands will install the FMProxy debian package, create required directories and configurations, and adjust your FileMaker Server to listen on a different port (note: FileMaker Server will be shut down and started again during this process!). You will be prompted for a few settings. If you are unsure what to select, just press return to accept the default setting. All configuration options can be changed after the install as well (requires restart of FMProxy).

```
$ tar xvzf fmproxy-*-linux-x86_64.tar.gz
$ cd fmproxy-*-linux-x86_64/
$ sudo ./install.sh

# sample output:
[+] Package installed.
[*] FileMaker Server config found.
[*] Stopping FileMaker Server...
[+] FileMaker Server stopped.
[*] FMS config backup already exists, skipping.
[+] Added fmproxy user to fmsadmin group.
[*] TLS certificates found:
[*]   Certificate: /opt/FileMaker/FileMaker Server/CStore/serverCustom.pem
[*]   Private key: /opt/FileMaker/FileMaker Server/CStore/serverKey.pem
Would you like to use these certificates for fmproxy? [Y/n] Y
[+] TLS configured.
[*] Original FMS DataPort: 5003
Set FMS DataPort to [5004]:
[+] FMS DataPort set to 5004.
[+] fmproxy target set to 127.0.0.1:5004.
[+] FMS UseSecureConnection set to 0.
[*] Starting FileMaker Server...
[+] FileMaker Server started.
[*] Waiting for FileMaker Server to complete startup.
[*] Enabling and starting fmproxy...
Created symlink /etc/systemd/system/multi-user.target.wants/fmproxy.service → /lib/systemd/system/fmproxy.service.
[+] fmproxy service enabled and started.
[+] fmproxy is running.

[+] Installation complete.
[+] fmproxy config:     /etc/fmproxy/fmproxy.json
[+] Install state:      /etc/fmproxy/install.state
[+] FMS config backup:  /opt/FileMaker/FileMaker Server/Data/Preferences/dbs_config.xml.pre-fmproxy
```

You can install new versions of FMProxy in the same manner as described above and also run the installer multiple times. Your configuration will be retained.

Please note that the service file of FMProxy uses sandboxing. If you prefer FMProxy to write/read to/from different paths (e.g. for logging or configuration), please create a unit file override with `systemctl edit fmproxy.service` and adjust the `ReadWritePaths`. If you are fine with the defaults, there's nothing to do here.

You can uninstall FMProxy using the same installer file. It will revert the FileMaker Server config changes, uninstall the package and perform a cleanup.

```
sudo ./install.sh --uninstall
```

Please note that this does not remove the default config, log directories and user/group. If you want everything gone, please use `apt-get purge fmproxy` after the uninstall.

## Where can I find the log files?

FMProxy writes three types of log files:

- **access.log** – This log file contains information about every new connection to your FileMaker Server. In case of a valid FileMaker client connection, you can also find additional details of the connecting client (e.g. version, platform, serial number) in here. Please note that the connection establishment is normal to happen before (!) a login.
- **security.log** – This log contains security events. Each event comes with a security event ID (SEC-xxxx). Please find the reference of all possible event IDs at the end of this document.
- **runtime.log** – These log files contain runtime information about the FMProxy process itself. When FMProxy is run with the `--debug` flag, these logs can grow fast. You only have to refer to these logs if you experience issues with FMProxy and/or want to report a problem to us.

The log directory can be specified using the `--log-dir` command line argument or `log_dir` key in the JSON config file. Without any configuration file or flags, logs are written into the current working directory.

When you install FMProxy using the installer, the logs can be found in `/var/log/fmproxy/` (Linux). To access the log files, use the root account or add your user to the `fmproxy` group (`sudo usermod -a -G fmproxy <username>`, then re-login).

Please note that the native `Access.log` of FileMaker Server will show all connections as originating from `127.0.0.1` (or wherever the proxy runs). This is due to the fact that from the perspective of FileMaker Server all client connections are established from the proxy server.

## How to give feedback?

We are looking to get your feedback on any issues you encounter during installation, configuration and operation of FMProxy. Also, if you have ideas for new features, feel free to tell us as well.

To give us feedback, please send an email to support@fmproxy.com.

When reporting any kind of issue, please include the runtime log files (`runtime.log`) found in the log directory (current directory or configured `--log-dir`).

Ideally, if you can reproduce an issue, start the proxy with the `--debug` flag, which will produce much more verbose log files.

Please always mention the version of FMProxy that you are using. You can get the version number by looking at the FMProxy startup logs or by running `./fmproxy --version`.

## Reference of Security Events

FMProxy logs security related events with a security ID. Below is a reference of event IDs and their meaning.

| Event ID | Description |
|---|---|
| SEC-0001 | Detection of a request with an unknown session ID. Repeated events of this kind could be an indication of session ID brute-forcing.<br><br>Session IDs are given out by the server when a client connects (before authentication). If a session ID for an already authenticated client is "guessed" by brute-force, it can allow an attacker to hijack that session and perform actions on behalf of the authenticated client. |
| SEC-0002 | Detection of a client downloading or attempting to download data from a database which is not part of the session used to initiate the download (i.e. no authentication was performed for this database during this session). |
| SEC-0003 | Detection of a client downloading or attempting to download a list of all scripts with an unauthenticated account. |
| SEC-0004 | Detection of a client downloading or attempting to download a list of all scripts with a non-"Full Access" account. This is benign if the authenticated account is not a Full Access account but has the permissions to modify scripts. |
| SEC-0005 | Detection of a client downloading or attempting to download data from a specific database without the corresponding account being authenticated. |
| SEC-0006 | Detection of a client accessing account information for an account other than self while the proxy has insufficient information about the privilege set / permissions of the authenticated account.<br><br>With data going over the wire the proxy builds a representation of the privileges for different accounts. When a request is made to download data for another account, this representation is in most cases sufficient to judge if it's a legit request or not. This event will be raised if the information is incomplete to judge the legitimacy of the request. |
| SEC-0007 | Detection of a client accessing account information for an account other than self while being authenticated but not having Full Access privileges.<br><br>This message is benign if a non-Full Access account is configured with permissions to manage other accounts. |
| SEC-0008 | Detection of a client connecting with a persistent ID which is not present in the list of trusted clients.<br><br>This event can only appear if the proxy was started with a list of trusted clients. |
| SEC-0009 | Detection of a client connecting with an invalid persistent ID. This could be an indicator of an attacker using a crafted payload using a custom tool. FileMaker clients will always connect with a valid ID. |
| SEC-0010 | Detection of a failed login. This event is always logged when a login fails (e.g. wrong account name / password combination).<br><br>When automatic logins are configured, you might see this event appearing before a login prompt is shown to a user. |
| SEC-0011 | Detection of known payloads that will crash FileMaker server (denial of service) due to memory issues. |
| SEC-0012 | Detection of successful login. |
| SEC-0013 | Detection of non-FileMaker traffic on the listening port. This event will occur more frequently on public servers which experience probing traffic (bots trying to check for open ports and analyze what software is running). |