

SECURITY

STORAGE SECURITY

It is advised to activate file storage encryption to guarantee that if someone steals your computer or your hard disk, this person will not be able to access the original DICOM files.

On Mac computers, macOS offers a built-in solution to securely encrypt your hard disk: FileVault.

You can activate it in macOS System Preferences : Security & Privacy: FileVault panel.

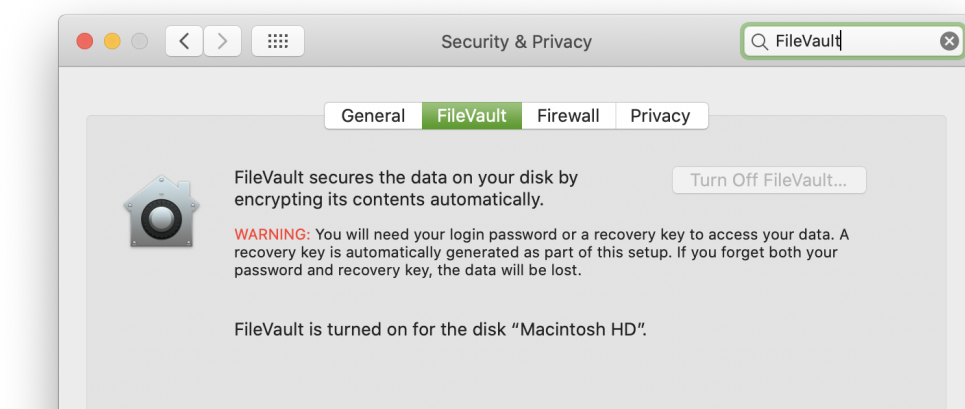


Figure 42: FileVault settings

OsiriX does not include a back-up system for the storage.

It means that if your hard disk, where the database is stored, is corrupted, you will lose your studies.

If you store original DICOM files or want to be sure that you will not lose your files (hardware failure or manipulation error), it is advised to use a back-up system.

You can use Time Machine from macOS to automatically create snapshots of your database (more information on Apple web site <https://support.apple.com/en-us/HT201250>).

You can also manually copy your OsiriX Data folder at regular intervals.

And finally, you can use commercial software to create incremental back-up.

NETWORK SECURITY

If you use your computer in an unknown or untrusted network (intranet or internet), it is advised to secure the network services offered by OsiriX.

To protect the network communications between computers in an untrusted environment, several technologies are available, based on:

Encryption transforms meaningful data into what looks like gibberish using a secret that can also be used to reverse the process.

Authentication is the process of convincing a gatekeeper that you are who you say you are, typically by proving that you know a secret (username and password).

You can use these two global technologies to protect your network from unauthorized accesses:

VPN

A Virtual Private Network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. It relies on encryption and authentication technologies.

Firewall

A computer firewall is a software program that prevents unauthorised access to or from a private network.

You can configure it to block/authorise specific network ports to block/authorise only specific services.

To configure a VPN or a firewall, contact your local IT support.

OsiriX offers several network services that can be activated & configured:

1. *Standard DICOM network protocol*
2. *XML-RPC and osirix:// URL scheme messages*
3. *Database sharing*
4. *Web Portal*

If you are unfamiliar with these concepts and settings, it's recommended to check with your local IT support, if your environment is secured.

You can find here detailed information about these services and security:

1. Standard DICOM network protocol (No encryption & No authentication)

This is the original protocol to exchange DICOM files between computers and software. The original protocol has been created in 1985. At this time, security was not a major concern. That's why the original standard doesn't include encryption and authentication. Hence, if you run OsiriX in an untrusted environment, turn off the C-GET SCP, C-MOVE SCP, and C-FIND SCP in *Preferences*→*Listener* window, or block the port (displayed in the Preferences) in your Firewall, or use it through a VPN.

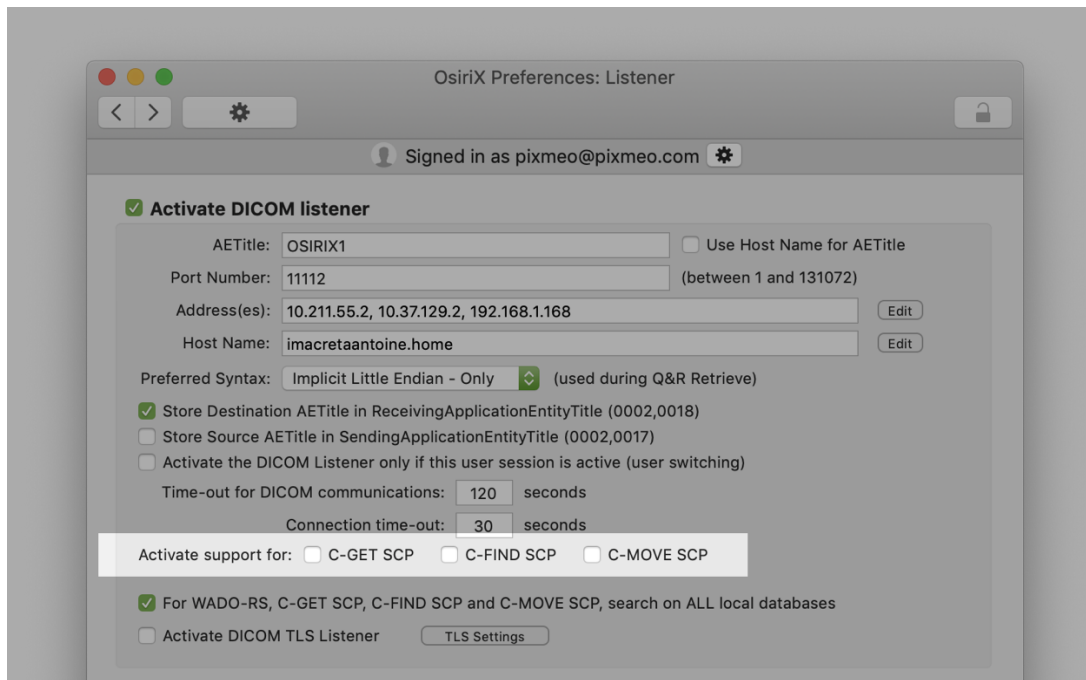


Figure 43: Deactivating C-GET SCP, C-MOVE SCP, and C-FIND SCP.

2. XML-RPC and osirix:// URL scheme messages (No encryption & No authentication)

This protocol authorise another computer or software to send messages to OsiriX. These messages can open a study or query the database list. You cannot exchange images with this protocol. If you run OsiriX in an untrusted environment, turn it off in *Preferences*→*Listener* window, or use it through a VPN.

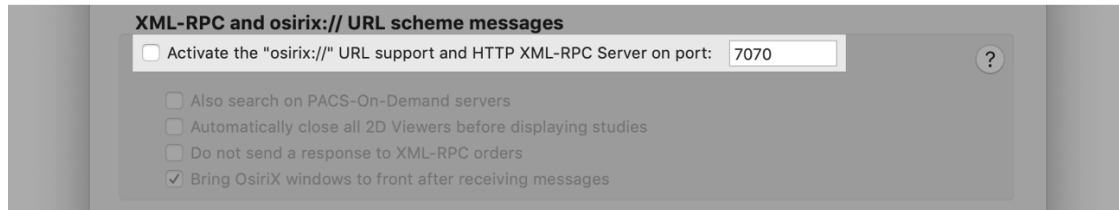


Figure 44: Deactivating XML-RPC and osirix:// URL scheme

3. Database sharing (encryption: yes, authentication: optional)

This feature allows you to share your OsiriX database with another computer. The data exchanged is automatically encrypted with the TLS protocol, provided by the operating system. If you run OsiriX in an untrusted environment, activate the authentication (password) in *Preferences*→*Listener* window to avoid unauthorised access.

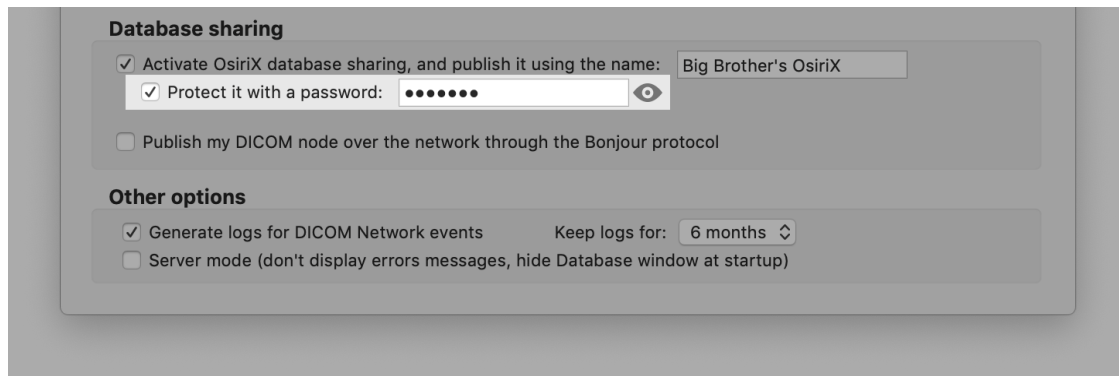


Figure 45: Activating Database sharing authentication.

4. Web Portal (encryption: optional, authentication: optional)

This feature give access to your database from an Internet web browser, such as Safari or Chrome. The connected user can navigate in your database and view the images. The Web Portal supports TLS encryption (HTTPS protocol), through official & trusted Web certificates. The Web Portal supports also user authentication with username & password, including a 2 factors authentication option (SMS token). If you run OsiriX in an untrusted environment, activate HTTPS encryption & authentication in *Preferences*→*Web Portal* window, or block the port (displayed in the Preferences) in your Firewall.

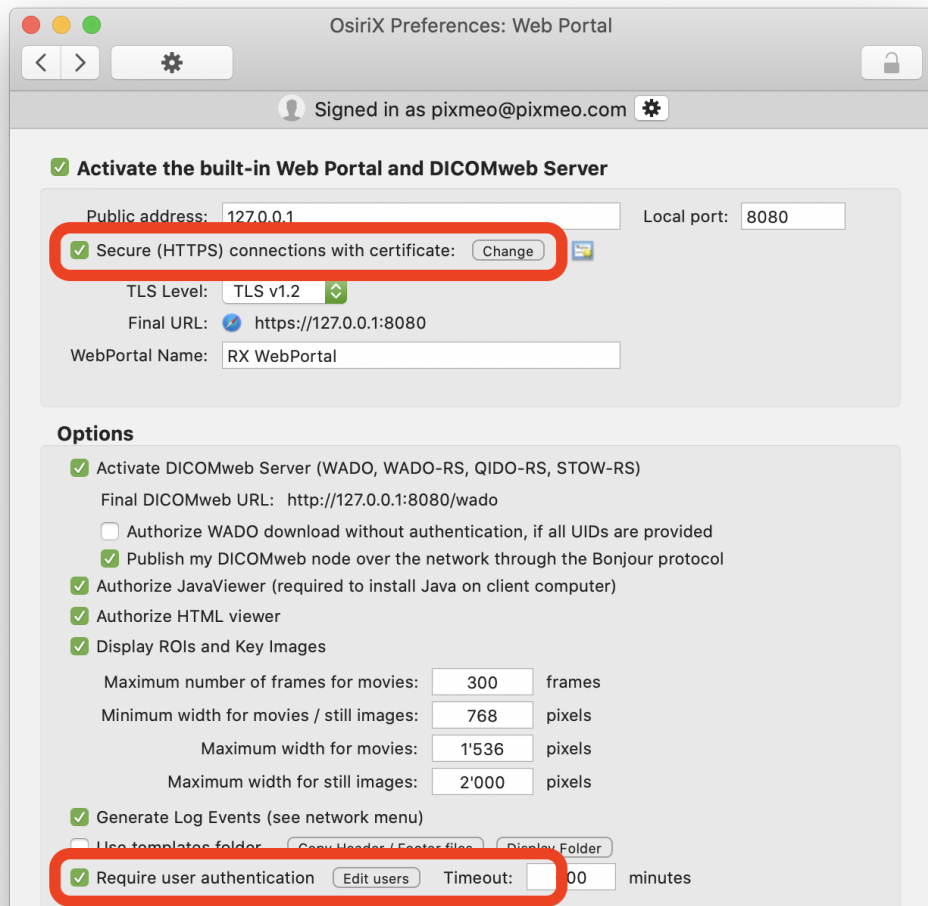


Figure 46: Activating Web Portal authentication

DICOM TLS

This section provides a short description of the TLS (Transport Layer Security) support available for DICOM communications in OsiriX.

Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications. It is used in OsiriX as the security layer for DICOM communications (Query & Retrieve and listener).

In OsiriX, both unilateral and bilateral authentication modes are implemented:

- The authentication is unilateral: only the server is authenticated (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous).
- The authentication is bilateral: both parties can be sure who they are communicating with.

You can configure it in Preferences→Listener window.

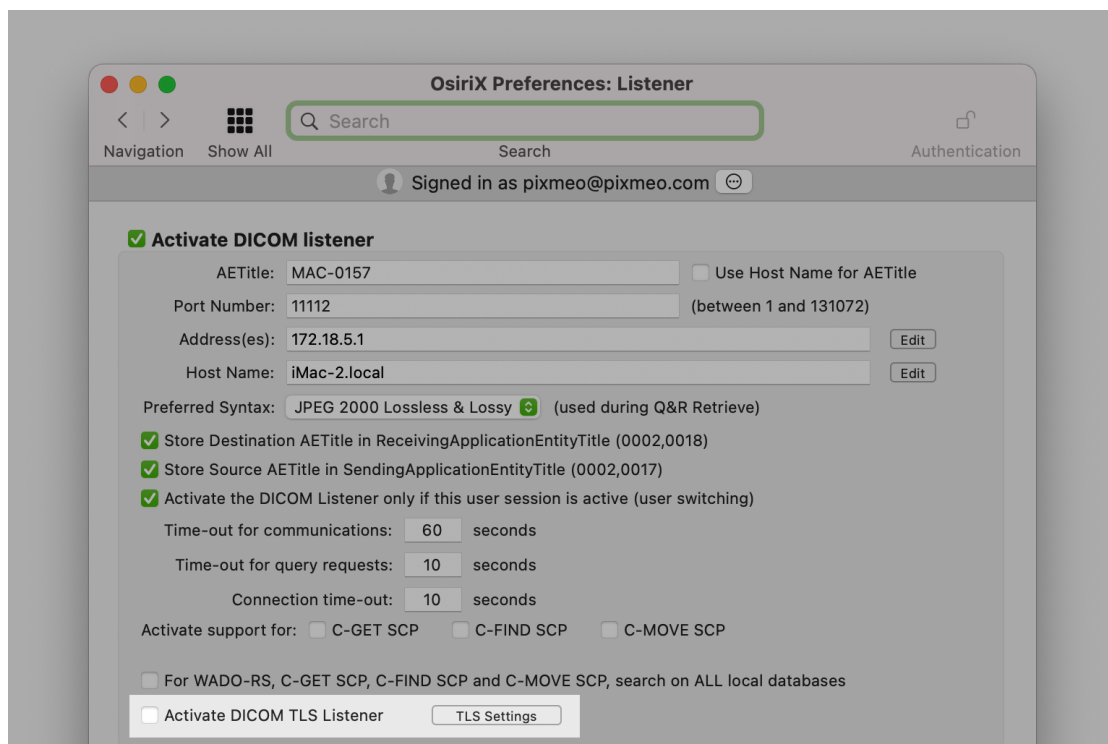


Figure 47: Activate DICOM TLS Listener