Vault Deployment for Administrators

Set up XQFS

Before running XQFS, you must set up the program. Refer to the following instructions to set up XQFS:

Step 1

Install Homebrew by copying and pasting the following command into your Terminal:

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Ensure you follow the **Next steps:** instructions in the Terminal before proceeding to Step 2. For more information on Homebrew, see Homebrew's website.

Step 2

Install **OpenSSL** and **OpenSSL-devel** packages by copying and pasting the following commands into your Terminal:

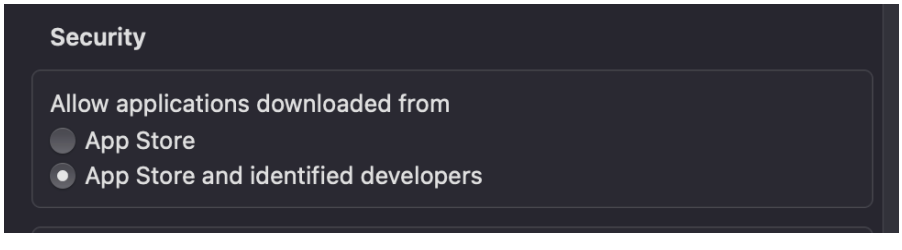
```
brew install openssl
export LDFLAGS="-L/opt/homebrew/opt/openssl@3/lib"
export CPPFLAGS="-I/opt/homebrew/opt/openssl@3/include"
```

Step 3

Install **macFuse 4.4.1** and **SSHFS 2.5.0** from the following URL: https://osxfuse.github.io/.

During installation may have to edit your security permissions:

1. Open **System Settings** and select **Privacy and Security**.
2. Under **Allow applications downloaded from**, click the **App Store and Identified Developers** radio button:



3. Select **Yes** to update security permissions for MacFuse.

Note: You may need to adjust your Startup Security Utility settings in addition to editing your security permissions. If you are prompted to do this, see Apple's guide on Changing security settings on the startup disk.

Step 4

Create a **fuse.ini** file containing the following information:

```
[Connections]
Quantum = https://quantum.xqmsg.net/v2
Val = https://validation.xqmsg.net/v2
Sub = https://subscription.xqmsg.net/v2
Saas = https://dashboard.xqmsg.net/v2

[ApiKeys]
XQ=XQ GENERAL API KEY
Dashboard=XQ DASHBOARD API KEY

[XQFS]
#The file suffix for encrypted files.
Suffix=.xqf

#The team ID used for authentication.
Team=TEAM ID

#The trusted range secret key.
Key=TRUSTED RANGE SECRET KEY

#The desired device name which will be registered on the dashboard.
Device=DEVICE NAME

#The recipients who will be able to access files written by the FS.
Recipients=device-PublicIPAddress@TeamID.trusted.local or user@email.com

#The number of DAYS before transferred files expire.
Expiration=60
#Auth may be "device" or "user
Auth=device or user
# If using auth=user, a "User" parameter must be set. An authentication code will
be sent to that email
#User=test@xqmsg.com
Roaming=yes

#This is the folder where the secure content will be stored
Target=/Path/To/Directory/you/want/to/store/encrypted/content/
```

Step 5

Generate **API Keys** from the XQ Dashboard using the following steps:

1. Log in to your XQ Dashboard at manage.xqmsg.com.

2. Click **Personal Dashboard** at the top right of the Dashboard and select **Create a new team**. Provide a team name, click **NEXT**, and select **Skip for now**.
3. Click **Applications** from the Dashboard's navigation menu and create an application.

Create two API Keys: a **Dashboard API Key** and a **General API Key**.

Step 6

Locate your **Team ID** using the following steps:

1. From the XQ Dashboard, click on your profile name and select **Account & Billing** from the drop-down menu.

Your Team ID is located under the **Organization** section.

Step 7

Generate a **Trusted Range Key** using the following steps:

1. From the XQ Dashboard, click **Trusted Ranges** from the navigation menu.
2. Add a new trusted range by clicking on the **+ icon**.

Give the trusted range a **Tag Name** and provide your IP address. Your IP address can be identified using whatsmyip.org.

Run XQFS

After setting up XQFS, you can ensure the file is executable and run the program. Refer to the following instructions to run XQFS:

Step 1

Ensure the file is executable by running the following command:

```
chmod 777 xqfs
```

Step 2

Run XQFS by running the following command:

```
./xqfs -c /path/to/the/fuseini/file -o /path/to/public/mount/target
```