# FileWave Central Preferences

## Accessing the FileWave Preferences

Now that you have logged in to FileWave Central, we will need to configure a few settings via the FileWave Preferences. The Preferences mentioned in this section are required for all FileWave installations. Any Preferences not covered in this section will be addressed in their own OS-specific section within the Evaluation Guide or linked to the FileWave KB.

macOS: FileWave Admin > Preferences

Windows: File > Preferences

## Secure Preferences

Each instance of FileWave has a super user account 'fwadmin'. This account has permissions for all items. Other Administrators may be created and allowance of permissions may be granted, as set out in the KB:

Manage FileWave Administrators

Some settings though, will always require a password to be entered when attempting to make alterations, even where settings are granted. When prompted to enter a password, it should be the password of the FileWave Admin currently signed in.

Examples of items which will always password prompt, include:

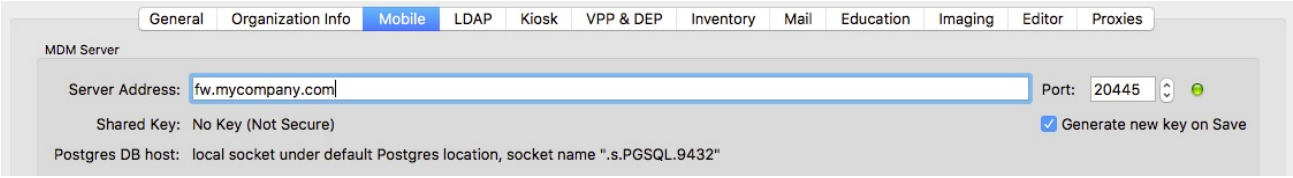
- Uploading a new PKCS12 server certificate
- Download the Apple DEP Certificate
- Configure DEP tokens
- Editing SIS details
- Manage Apple Classroom Certificate

> Permissions will still need to be granted for any FileWave Administrator requiring the ability to even attempt to change these settings.

## "Mobile" Preferences

The "Mobile" Preferences pane is one of the most important throughout FileWave as it sets the server's address so FileWave Central knows where to connect to.

1. Verify that the "Server Address" is correctly set to the fully qualified domain name (FQDN) of the your FileWave Server.
   - If you see an IP address, please log out of FileWave Central and attempt to log back in using the FQDN of the FileWave Server.
2. Verify that the green light is visible to the right of the "Port" field.
   - Do not continue if the light is red and please address any DNS issues and/or configure FQDN for the FileWave Server.
   - Do not change the "Port" field value.
3. If "Shared Key" is set to "No Key (Not Secure)", please verify that the "Generate new key on Save" is checked.
   - This will only apply to fresh on-premise installations, Cloud-Hosted will have shared key preset.
4. After "Generate new key on Save" is checked, immediately click "OK" to save and close the Preferences window.
   - If the Shared Key is already generated, please proceed without "OK".




## "General" Preferences

The "General" Preferences is the second most important Preferences pane as it controls the SSL Certificate used to protect all FileWave communications. We highly recommend using a true CA-signed SSL Certificate versus a self-signed certificate or free certificate available from services like Let's Encrypt. If you already have a wildcard certificate that covers the top level domain the FileWave server will be hosted on then you can use it without needing to purchase another certificate. FileWave Cloud-Hosted Servers will have the SSL Certificate pre-installed.

### Installing a Commercial Certificate from a Trusted Certificate Authority

1. Follow the instructions here for creating a .p12 certificate file from the .crt file provided by your certificate vendor. To ensure that you receive your certificate as a .crt file pick Apache HTTP for the download format. You will need to merge your SSL .crt file, private key, and possibly any required intermediate certificates into a single .p12 file. SSL vendors often provide multiple intermediate certificates in .crt format.
2. In the "SSL Certificate Management" section of the of the _"General" P_references tab of FileWave Central console click the "Upload PKCS12 Certificate" button, authenticate, and select the .p12 certificate file generated from Step 1.
   - You'll also want to store a copy of this .p12 file in a safe place for disaster recovery purposes should your FileWave server suffer a catastrophic hardware failure.
3. Click the "OK" button to save the Preferences.
4. Ensure that the FQDN assigned to the FileWave Server is resolvable externally and that TCP port 443 has been forwarded correctly if your server is hosted inside of your firewall with a private IP. Verify the certificate trust chain externally using one of the external SSL checkers below.

https://www.sslshopper.com/ssl-checker.html

https://www.digicert.com/help

https://www.geocerts.com/ssl_checker

https://www.rapidsslonline.com/ssl-tools/ssl-checker.php

https://certlogik.com/ssl-checker

The FileWave Dashboard can also be configured to alert you via email pending a SSL certificate expiration.

### Generating a Self-signed Certificate

If you are unable to acquire a commercial SSL certificate from a trusted Certificate Authority then you should ask your FileWave Sales Engineer about testing on a hosted server that has a filewave.net DNS name. You may decide to stick with that for when you move to production as well.

## "Manage Administrators" Assistant

So far we've only discussed logging into FileWave Central using the default superuser account "fwadmin". Let us change the "fwadmin" password followed by creating a new user account for our normal daily actions or for another team member.

### Change password for "fwadmin"

1. Open "Manage Administrators" from the "Assistants" menu in the main topmost menubar of FileWave Admin.
2. Select the "fwadmin" account on the left and select "Set password".
3. This password should be stored securely as it will be used for modifying several Preferences that require "superuser" permissions.
4. Click "Apply" to save the changes.

### Create a new user account

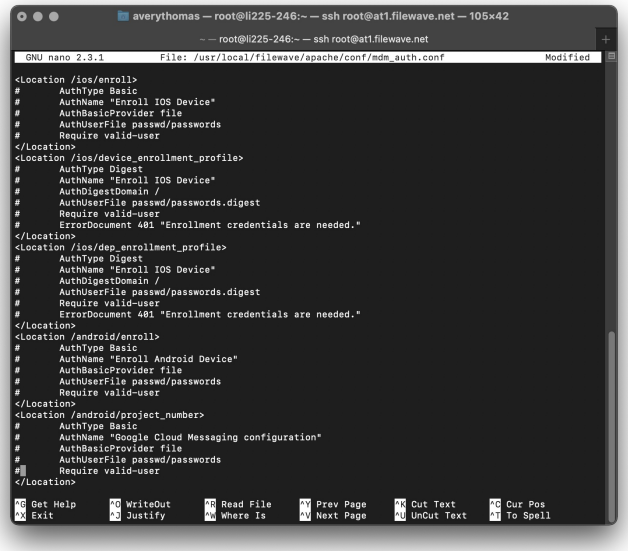
1. Open "Manage Administrators" from the "Assistants" menu in the main topmost menubar of FileWave Admin.
2. Click the "[+]" button in the lower left-hand corner and select "Local Account".
   - Authenticating using Active Directory via "LDAP Group Account" will not be available until a LDAP Server has been configured via the "LDAP" Preferences. More info here.
3. Specify at least the "Login name" and "Set password".
4. Navigate to the "Permissions" tab and review all permissions you'd like to grant to the new user.
5. Click "Apply" to save the changes.

### Allow new users to access existing VPP Tokens

After importing your organization's Apple VPP Tokens, we will need to allow each new user or LDAP group the ability to access the VPP tokens.

1. Open "Manage Administrators" from the "Assistants" menu in the main topmost menubar of FileWave Admin.
   1. Click the "Manage VPP Tokens" button from the lower section.
   2. Authenticate using the "fwadmin" superuser credentials.
   3. Click the boxes for each token and user you'd like to grant access to the VPP token.

## Disable iOS/macOS URL and DEP Authentication




By default, the FileWave Server will have generic authentication enabled for iOS/macOS URL and DEP enrollments. For testing purposes, it is recommended to disable this authentication to better streamline the MDM enrollment of your Apple devices. Most customers also choose to keep the authentication disabled in their production environments so that DEP devices automatically enroll into FileWave with requiring credentials. This speeds up the enrollment process and allows a Lost or Stolen device to automatically enroll back under your control with Location Tracking capabilities. If a device is Lost or Stolen with authentication enabled, the next user will not be able to authenticate and enroll into FileWave and the device is essentially a brick and may get discarded as such. If you still desire authentication during MDM enrollments, please consider configuring the "LDAP" FileWave Admin Preferences to automatically configure MDM authentication.

Any Cloud-Hosted Server requested by your FileWave SE will have authentication disabled unless instructed otherwise.

1. Access the FileWave Server's Command Line Interface (CLI) via direct console access or via SSH using the default username "root" and default password "filewave".
   SSH into FileWave Server
   ```
   ssh root@myorg.filewave.net
   ```
2. Install "nano" for easier modification of text files.
   Install nano
   ```
   yum install -y nano
   ```
3. Comment out all lines between the "<Location> </Location>" tags using "#" in the file "/usr/local/filewave/apache/conf/mdm_auth.conf".
   Edit mdm_auth.conf
   ```
   nano /usr/local/filewave/apache/conf/mdm_auth.conf
   ```
4. Save changes and exit nano.
   Save and quit "nano"
   ```
   Ctrl + X
   y
   Enter
   ```
5. Restart the FileWave Apache process.
   Restart Apache
   ```
   /usr/local/filewave/apache/bin/apachectl graceful
   ```
6. Verify the changes by visiting your FileWave URL Enrollment page. Ex: https://myorg.filewave.net:20443/ios
7. The "enroll.mobileconfig" should download without need for authentication.

---

Revision #7
★Created 9 June 2023 16:21:20 by Josh Levitsky
Updated 11 July 2024 14:30:44 by Sean Holden