FileWave Server Installation & Upgrade

FileWave Server Installation

FileWave Server is the key component to device management. The setup process will require not only a FileWave Server installation, but basic configuration will require the FileWave Central App (macOS or Windows). Some additional configuration may also be achieved through the web admin: FileWave Anywhere.

Other appliances not covered in this chapter are:

- Boosters
- IVS

Overall requirements

FileWave server installation. This can be hosted or on-premise. For on-premise, FileWave Download pages not only provide the installer, but pre-built VMs are available for quick setup.

Manual Installation

If not using a pre-built VM:

- Download the latest server version and copy to the FileWave Server
- If using a shell, open this to the server, e.g. ssh, putty, etc. and elevate to the root user
- Unzip the download
- Run the installer

Follow the instructions, regarding the commands required, from the matching download pages.

FileWave Server networking

Please review the Default TCP and UDP Port Usage and also review FileWave Server should not have IPv6 enabled.

FileWave Access - Passwords

FileWave Administrator

FileWave installations provide an initial user which has full permissions. On initial launch, this password should be changed as a matter of security. The default account is:

- Name: fwadmin
- Password: filewave

The password may be changed in the FileWave Central software application Menus, through:

- Assistants > Manage Administrators

Select the 'fwadmin' account, followed by the 'Set Password' radial button. Enter the chosen secure password

SSH

SSH is initially enabled and the root account of the default setup has the same password as fwadmin, however, they are not aligned. Consider immediately changing the root users account password and disable the ability to access SSH to the server from the internet.

Log into a shell on the server as root and run the following command:

```
passwd
```

A prompt will require input of the new password and secondary confirmation of this new password.

FileWave Server On-Premise

Where servers are installed in on-premise environments, a couple of basic procedures should follow immediately.

Server Name

Arguably, the local server name need not necessarily matter, but the FileWave Server name is very much something to consider carefully.

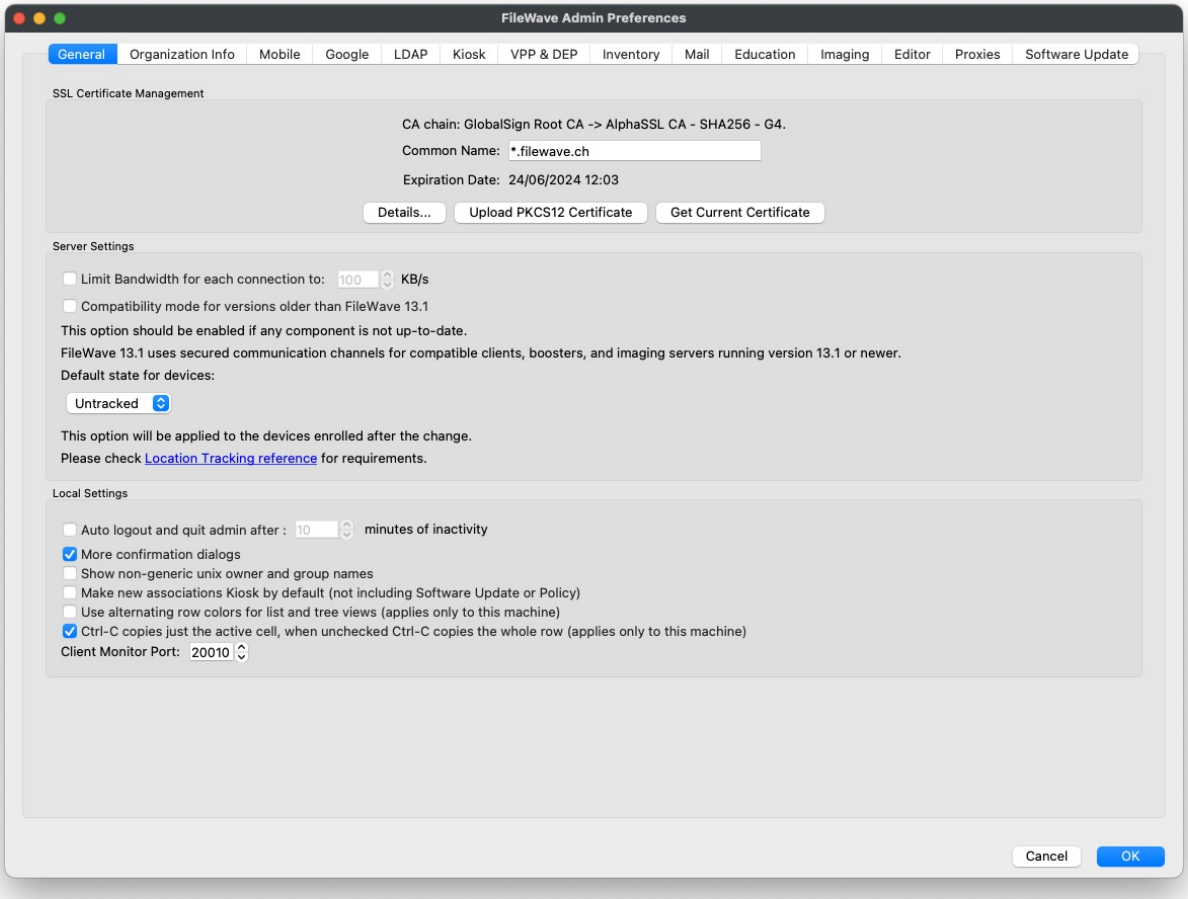
> ✓ When naming the server, always provide a Fully Qualified Domain Name. This should be a name that could be used externally, even if that is not the initial plan at inception. Subsequently changing the server name has massive impact or devices already enrolled. Using a name that could be used at a latter date, provides future-proofing, extensively simplifying workload.

Certificates

A cert will need to be generated with a Subject Alternate Name (SAN) which matches the chosen server name. Please see our KB pages on certificates:

https://kb.filewave.com/books/certificates

Once a P12 certificate is generated, it may be uploaded to the FileWave Server through the FileWave Central Application.



SSL Certificate Management

CA chain: GlobalSign Root CA -> AlphaSSL CA - SHA256 - G4.

Common Name: *.filewave.ch

Expiration Date: 24/06/2024 12:03

Server Settings

□ Limit Bandwidth for each connection to: 100 KB/s

□ Compatibility mode for versions older than FileWave 13.1

This option should be enabled if any component is not up-to-date.

FileWave 13.1 uses secured communication channels for compatible clients, boosters, and imaging servers running version 13.1 or newer.

Default state for devices:

Untracked

This option will be applied to the devices enrolled after the change.

Please check Location Tracking reference for requirements.

Local Settings

□ Auto logout and quit admin after : 10 minutes of inactivity

☑ More confirmation dialogs

□ Show non-generic unix owner and group names

□ Make new associations Kiosk by default (not including Software Update or Policy)

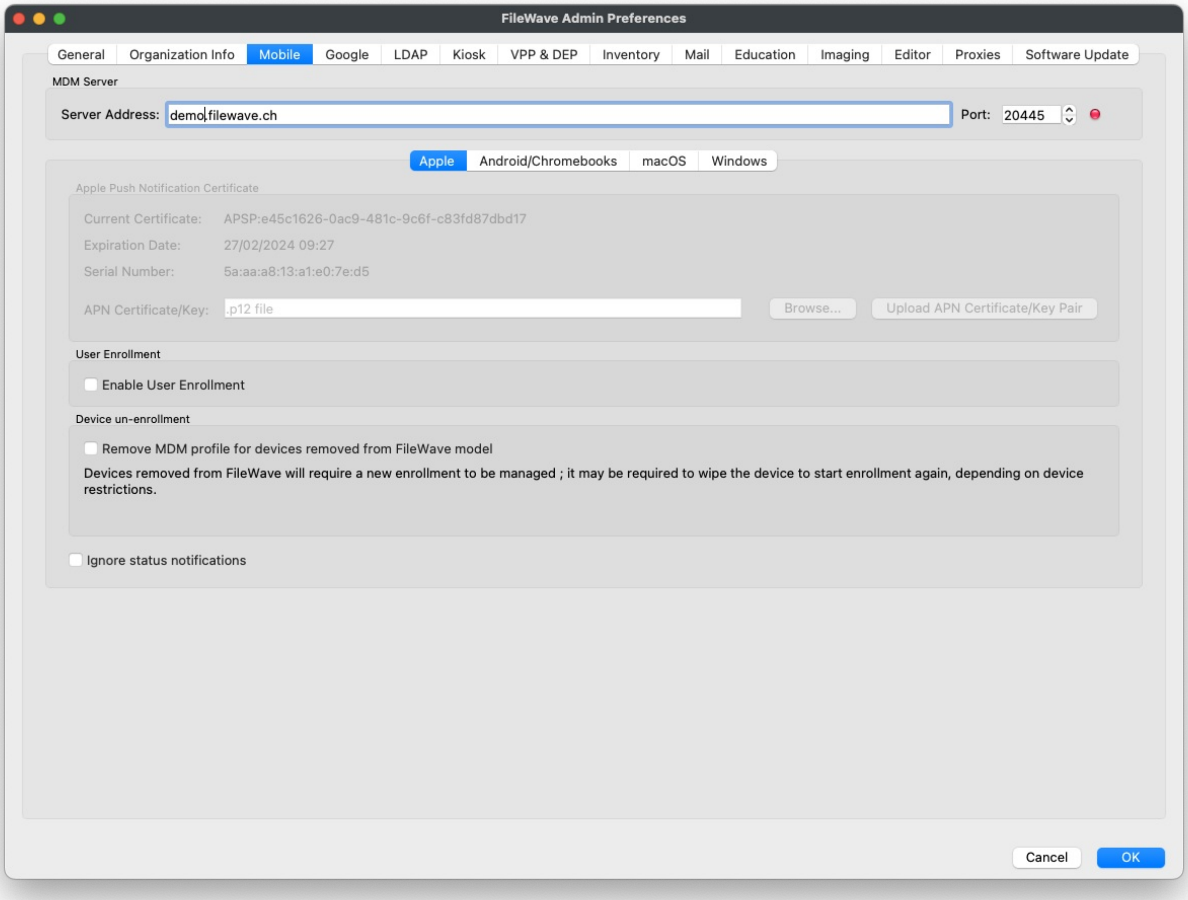
□ Use alternating row colors for list and tree views (applies only to this machine)

☑ Ctrl-C copies just the active cell, when unchecked Ctrl-C copies the whole row (applies only to this machine)

Client Monitor Port: 20010

Naming the Server

The chosen name should be entered into the FileWave Central application's Mobile tab. For example, for a server called 'demo.filewave.ch':



MDM Server

Server Address: demo.filewave.ch

Port: 20445

Apple Push Notification Certificate

Current Certificate: APSP:e45c1626-0ac9-481c-9c6f-c83fd87dbd17

Expiration Date: 27/02/2024 09:27

Serial Number: 5a:aa:a8:13:a1:e0:7e:d5

APN Certificate/Key: .p12 file

User Enrollment

□ Enable User Enrollment

Device un-enrollment

□ Remove MDM profile for devices removed from FileWave model

Devices removed from FileWave will require a new enrollment to be managed ; it may be required to wipe the device to start enrollment again, depending on device restrictions.

□ Ignore status notifications

Server Command Line Configuration

With a certificate and name configured, there is a small amount of input required via the server's command line.

Hosts File

The server's host file should be edited to ensure the FileWave Server name is entered. Take the following example hosts file:

```
127.0.0.1       localhost
::1             localhost
```

From the same above example 'demo.filewave.ch', the hosts file may edited in one of two ways. Either:

```
127.0.0.1       localhost demo.filewave.ch
::1             localhost demo.filewave.ch
```

or

```
127.0.0.1       localhost
127.0.0.1       demo.filewave.ch
::1             localhost
::1             demo.filewave.ch
```

It does not matter if the additional entry is space separated on the same line or a new line entry, either method does the same process.

Apache Conf File

This is only required if the local server name does not match the FileWave Server name.

Edit the following file:

`/usr/local/filewave/apache/conf/httpd_custom.conf`

Add the following entry for ServerName:

```
ServerName      demo.filewave.ch
```

Restart Server Process

After configuration change, the server process should be restarted. This command should be ran as root.

```
fwcontrol server restart
```

FileWave Server Time

Time is critical with servers and acceptance of certificates and communication. As such, it is imperative that time is kept in sync. It is possible to run one-off commands to achieve this, but better still, consider enabling automated time sync.

macOS

macOS devices may just have time configured through the System Preferences or Settings

Linux

For linux servers, check out our KB on this topic:

Set date/time on Virtual Appliances

FileWave Server Upgrades

Upgrading for hosted servers will be a matter of communication between FileWave and hosted customers. However for on-premise, consider the following process

Upgrade Process

1. Download the chosen upgrades from the FileWave Download Pages. This will be at the very least the FileWave Server and FileWave Central application
2. Copy FileWave server installer to the server
3. Copy FileWave Central installer to a chosen macOS or Windows device
4. Lock all devices, from the right click contextual menu 'Lock' (Mobile and Computer devices can be locked separately from the relevant client View. Multiple devices may be selected and actioned in one go.)
5. Run an Update Model
6. Run a backup
7. If this is a VM, stop the FileWave Server process and take a snapshot
8. Follow upgrade instructions from the download pages matching the installer version, including updating the server OS.
9. Once completed, instal or upgrade FileWave Central application
10. Connect and test a Model Update
11. Unlock an example, test device and ensure all is well
12. Either test further or once satisfied, unlock all other devices necessary

> ✓ Before locking clients, confirm none are already locked for an alternate reason. Once completed and unlocking, these devices may then be targeted to remain locked.