

1. Installation and Setup

Please follow this "Installation and Setup" guide step by step to determine how FileWave will fit into your existing environment.

- [FileWave Server Setup](#)
- [FileWave Central Setup](#)
- [FileWave Central Preferences](#)
- [Client Group Structure](#)
- [Software Group Structure](#)

FileWave Server Setup

What server type is best for me?

The first step to begin your FileWave Evaluation is to determine your FileWave Server hosting preference. FileWave offers both a Cloud-Hosted server and an on-premise virtualized server appliance for either Hyper-V or VMWare.

Cloud-Hosted Server

If you desire a [FileWave Cloud-Hosted server](#) and have not already received the login information, please request a Cloud-Hosted server from your dedicated FileWave SE and they will provide you with the server's Address, Username, and Password. The FileWave Cloud-Hosted Server will be a "production" server so that any progress you make during the evaluation will persist if you choose to purchase FileWave.

Please note that choosing a Cloud-Hosted Server may be an additional cost depending on the licensing structure selected at the time of your purchase. Also, to better manage the cost incurred by FileWave during your evaluation, your FileWave SE will discuss your organization's timeline to determine the best possible start date and expiration date for your evaluation. Thank you in advance for your understanding in regards to these matters.

Pros of FileWave's Cloud-Hosted Server

- Near instant availability with limited setup time required
- Managed public fully qualified domain name and SSL certificate
- Ability to manage devices on any network with Internet connection
- Free "hands-off" upgrades of FileWave
- Guaranteed server uptime
- Automated Backups
- Low maintenance

On-Premise Server

If you desire to host the FileWave Server on-premise by installing on a macOS machine or virtualizing our pre-built appliance in Hyper-V or VMWare, please continue to read the following section.

Requirements

Most steps required for an on-premise server will be in regards to your local network's infrastructure including virtual environment, DNS, and Firewall/Content Filter. If you do not have direct access to these systems, please coordinate with your Network Administrator or other qualified personnel before proceeding.

Before importing the FileWave Server virtual appliance we recommend setting aside a static IP and DNS name for it. This will make it easier to move the server to another IP in the future and possible to manage off-premise devices over the Internet. Although technically possible, it is highly unrecommended to only use an IP address to reference the FileWave Server so please configure a valid and potentially publicly-resolvable fully qualified domain name (FQDN) for the FileWave Server.

Note that the FQDN selected must be resolvable on all network segments you plan to manage the client devices from. If you want to manage devices both on and off your network then the same FQDN must be resolvable both on and off your network. Inside your LAN this FQDN will resolve to the internal IP address of your FileWave server. Externally that same FQDN will resolve to the public IP address of the internet router in front of the FileWave Server. With mobile devices like iPhones and iPads that have a high possibility of leaving your LAN, it is essential that they be able to access the FileWave Server at all times, especially when they are off-network.

Off-Premise device management via Internet

A static IP allows you to easily forward the ports used by the FileWave server to its internal IP on your LAN, ensuring that requests from client devices are still able to reach it even when they are off-network. The following ports must be forwarded to the FileWave Server. Some of the ports such as 20016 and 20446 are optional if IT staff will only be accessing the FileWave Admin while on the LAN. A full listing of FileWave ports and port diagrams are available [here](#).

FileWave Server Installation

The FileWave Server can be installed onto any macOS 10.13+ machine with minimum specs of 8GB RAM / 4 CPU or virtualized in either Hyper-V or VMWare using our pre-built virtual appliance based on Debian. If virtualization is available, we highly recommend using our pre-built server appliance versus a macOS machine because of the flexibility to extend allotted server resources. When choosing a virtualization platform for your FileWave Server virtual appliance, we recommend a server platform such as vSphere or Hyper-V over a client platform like VMware Workstation/Fusion or VirtualBox. A VM server platform does not require that you be logged into a user session for the VM to be running. Also in the event the physical system hosting the VM server restarts the VMs hosted on it can also be

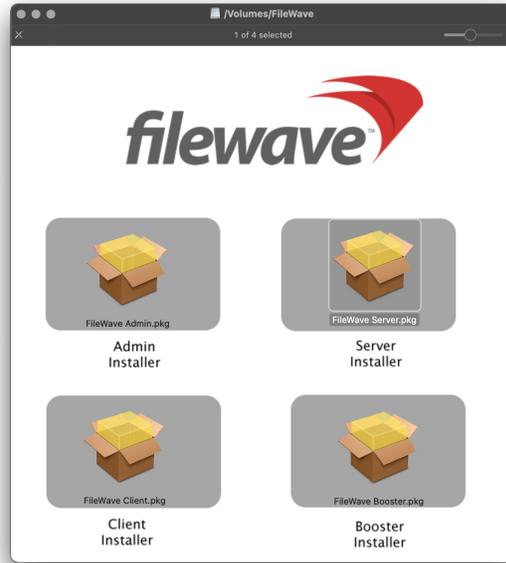
configured start up automatically also.

Software Downloads

All software downloads outlined in the following steps can be found [here](#). Please always select the latest version of FileWave unless instructed otherwise by your FileWave SE.

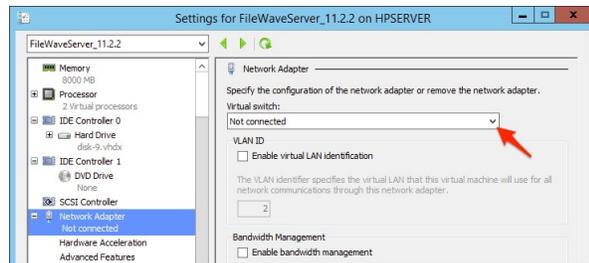
macOS

1. Mount the FileWave_macOS_XX.X.X.dmg downloaded from the FileWave Software Downloads page.
2. Double click the FileWave Server.pkg
3. Click Continue and then Agree to the license.
4. Click Install and enter your admin credentials to complete the installation.



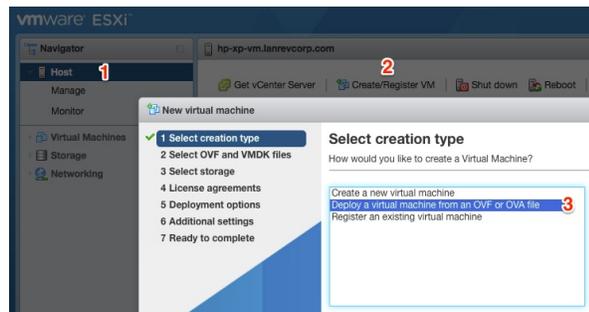
Hyper-V Linux Appliance Import

1. Extract the contents of the FileWaveServer_XX.X.X_VHD.zip file to a convenient location, like your desktop, on your Hyper-V system.
2. Launch Hyper-V Manager, highlight your server on the left-hand pane, and go to Action > Import Virtual Machine.
3. Click Next, then Browse, select the folder that the FileWave Server virtual appliance was extracted to (e.g. FileWaveServer_XX.X.X), and click the Select Folder button. If it reports that it can't file a VM to import follow the instructions [here](#).
4. Keep clicking Next until you reach the Choose Import Type screen. Select Copy the virtual machine (create a new unique ID).
5. Continue to click Next and then Finish to complete the VM import.
6. Select the FileWave server VM in the list of VMs and go to Action > Settings.
7. Click Network Adapter in the list of Hardware settings for the VM and click the Virtual switch pull-down to connect it to your network.
8. If there is no virtual switch available go to Action > Virtual Switch Manager to add one. For the connection type be sure to select External network.

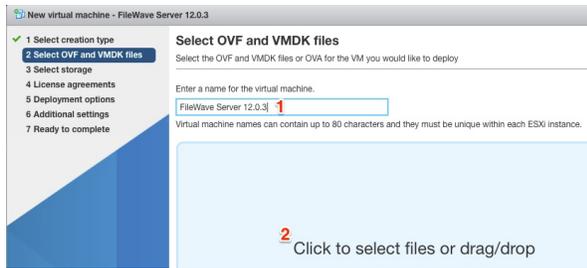


VMware ESXi Linux Appliance Import

1. Log into the VMware web console on your ESXi sever, go to Host on the left, choose Create/Register VM on the right, select Deploy a virtual machine from an OVF or OVA file, and click the Next button.
2. At the Select OVF and VMDK files screen enter a display name for your VM.
3. Drag the FileWaveServer_ova file into the blue field at the lower right and click Next.
4. Select the datastore where you want to import the VM to and click Next.
5. At the Deployment options screen select your VM Network and choose "Thin" for Disk provisioning.
6. Click Finish to begin the VM import. You can monitor the import by watching the Recent tasks pane in the Hosts area of the vSphere web console. After the Upload disk and Import vApp tasks are done your VM should appear in the list of Virtual Machines on the left-hand Navigator pane.

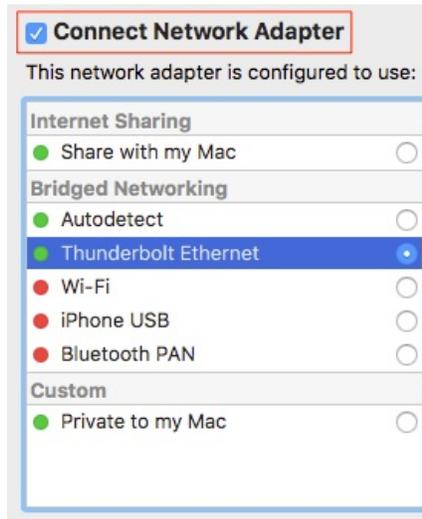


Task	Target	Initiator	Queued	Started	Result	Completed
Upload disk - File Wave Server_11.2.2	FileWave Server 11.2.3	root	05/04/2017 21:23:25	05/04/2017 21:23:25	✓	Running... 21 %
Import vApp	Resources	root	05/04/2017 14:20:38	05/04/2017 14:20:38	✓	Running... 21 %



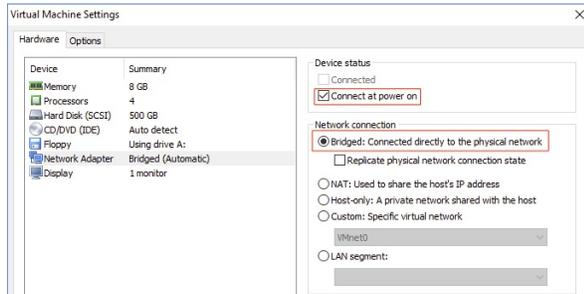
VMware Fusion Linux Appliance Import

1. Launch Fusion and go to File > Import > Choose File.
2. Select the FileWave_Server.ova file and click Open and then Continue.
3. Choose the path where you would like to copy the VM to and click Save.
4. Click the Customize Settings button at the Finish screen to bring up the settings screen for the VM.
5. In the Network Adapter section ensure that Connect Network Adapter is checked and then select an Ethernet based option under Bridged Networking.



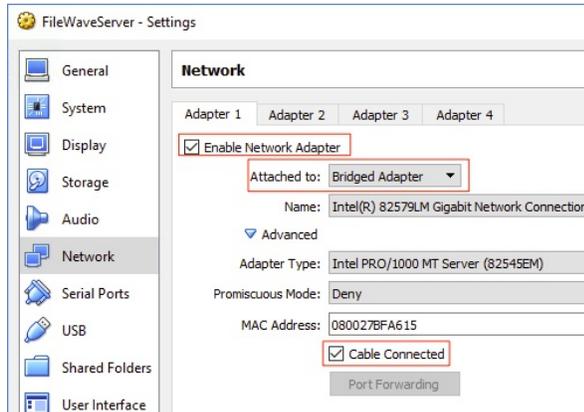
VMware Workstation Linux Appliance Import

1. Launch VMware Workstation and click Open a Virtual Machine in the Home tab. Alternatively you can also go to File > Open.
2. Browse to the FileWave_Server_ova file and click Open.
3. Change the storage path for the VM if desired and click Import.
4. Edit the network settings for the VM and ensure that Connect at power on is checked and that Bridged: Connected directly to the physical network is selected.
5. Click OK.



VirtualBox Linux Appliance Import

1. Launch VirtualBox, go to File > Import Appliance, select the FileWave_Server_ova file, and click Open.
2. Check Reinitialize the MAC address of all network cards and click Import.
3. Select your the FileWave server VM and click the Settings icon in the icon bar.
4. In the Adapter 1 tab ensure that Enable Network Adapter and Cable Connected are checked and that Attached to is set to Bridged Adapter.
5. Click OK when you are done.



Debian (not appliance)

In the case maybe you need to setup your own Debian OS. This is fine to do. Refer to the Debian section of the latest version of FileWave that is on the [Downloads](#) page to see the commands to run to install or upgrade. It's the same commands. One thing to note is that Webmin won't be installed, but you could download and easily install it if desired. Aside from Webmin there is not much different between a stock install and our Appliance.

Check the [Downloads](#) page for the most recent. Below is an example:

```
# login via ssh as root or use sudo for every line
below
# OS Upgrades:
sudo apt update -y
sudo DEBIAN_FRONTEND=noninteractive apt-get
upgrade -y -o Dpkg::Options::="--force-confold"
# Download and Install:
wget
https://fwdl.filewave.com/15.2.1/fwserver_15.2.1_
amd64.deb
sudo dpkg -i ./fwserver_15.2.1_amd64.deb
# If dependencies are not met then the below will
install them allowing for the FW server to
install:
sudo apt-get install -f
# If you needed to use the above command for
dependencies then run the next line again.
# It will succeed once all dependencies are
handled which can take a couple of tries:
sudo dpkg -i ./fwserver_15.2.1_amd64.deb
sudo reboot
```

Configuring the Linux Appliance Network Settings

Once you are done importing the FileWave Server Linux appliance, please power it on and configure the network settings using one of the guides below. Once the network settings have been configured, please create an internal DNS A-Record to set a fully qualified domain name (FQDN) for your FileWave Server that points to the Static IP Address configured below. If you plan on managing devices off-network, please ensure the FQDN is resolvable via the Internet and that you have the ability to obtain an SSL certificate that can protect your FQDN.

You will find two sections below, Command Line and Webmin GUI. Please select only one of the two sections based on your preference to configure the settings.

Please disregard this section if using a macOS FileWave Server as you will configure macOS System Preference to configure Static IP address.

Debian Command Line

▼ Debian Command Line Networking

Access FileWave Server's Command Line Interface (CLI) via direct console access or SSH using the "fwadmin" user and password "filewave" and you will be prompted to change the password. (For FileWave prior to 15.5.0 the user was root.)

SSH into FileWave Server

```
ssh fwadmin@192.168.1.85
```

Change the FileWave Server's password when prompted and take note of it in a secure location. You will not see password being typed, press Enter when finished.

The following guide is tailored for Debian servers using the interfaces file, but you could also use Webmin (below) on your server assuming the server comes online initially with DHCP.

1. Locate Network Interface:

First, identify the network interface you wish to configure. You can list all network interfaces using:

```
networkctl list
```

```
admin@ip-172-30-3-220:/etc/network$ networkctl list
```

IDX	LINK	TYPE	OPERATIONAL	SETUP
1	lo	loopback	carrier	unmanaged
2	ens5	ether	routable	configured

2 links listed.

2. Edit the /etc/network/interfaces file: Using 'nano', edit the interfaces file to set the network configurations.

```
nano /etc/network/interfaces
```

Your default interfaces file should look something like this (your interface name may be different):

```
# The loopback network interface
auto lo eth0
iface lo inet loopback

# The primary network interface
iface eth0 inet dhcp
```

Change the file to look like this, using your network preferences (note 'dhcp' has been changed to 'static' in line 6)

```
# The loopback network interface
auto lo eth0
iface lo inet loopback

# The primary network interface
iface eth0 inet static
address 192.168.10.33
netmask 255.255.255.0
broadcast 192.168.10.255
dns-nameservers 192.168.10.254 192.168.10.255
```

3. Verify Resolv.conf, hosts and hostname files: Verify that these files in /etc/ are configured correctly for your network and server.

/etc/resolv.conf: This file should list your DNS servers

/etc/hosts: This file should point your FQDN to localhost (127.0.0.1)

/etc/hostname: Specifies the hostname for your server. This is filewave by default.

4. Restart/Check Network Status:

```
systemctl restart networking.service

systemctl status networking.service
```

5. Verify IP:

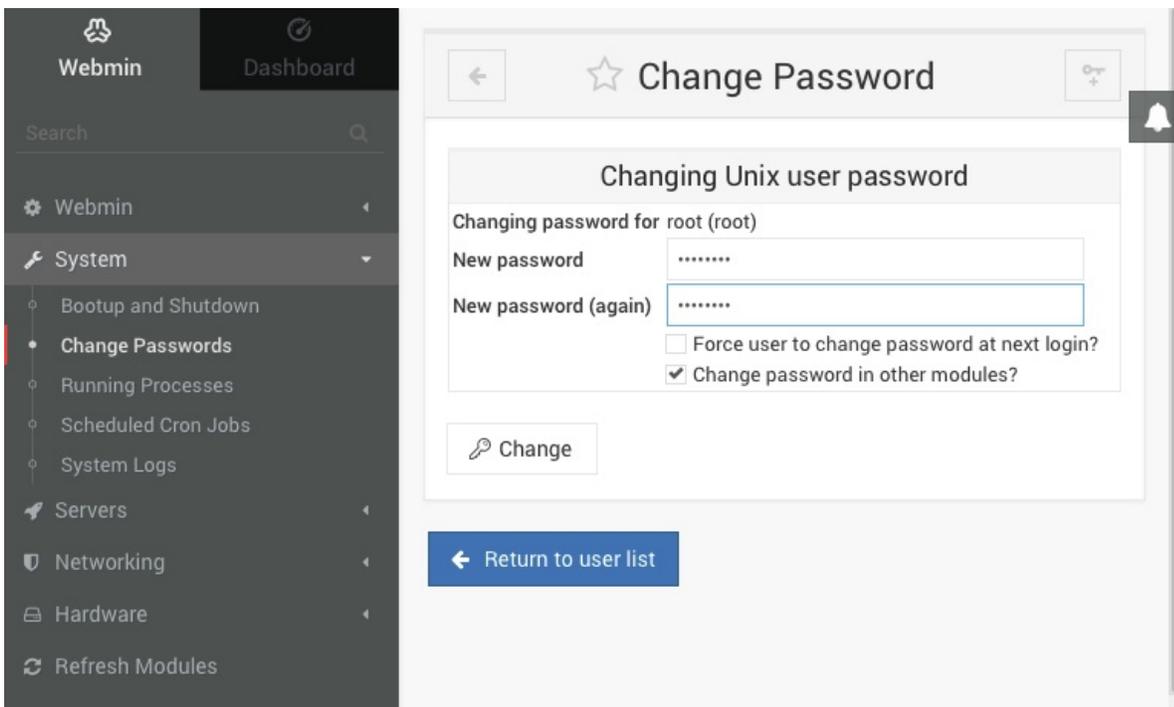
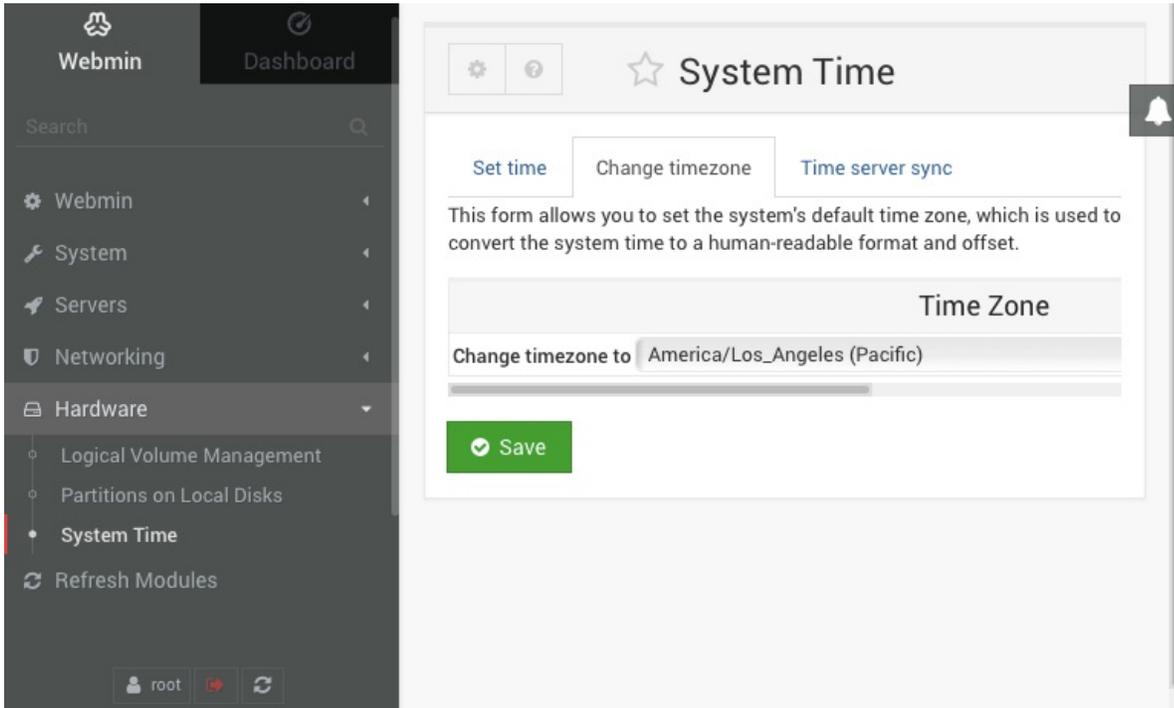
```
ip a
```

Webmin GUI

▲ For Webmin on Debian know that you will need to go to Webmin -> Webmin Configuration -> Operating System and Environment and make sure it's set to Debian 12.4 (Or whatever version we are at when you set up your system. You can see this with `cat /etc/debian_version` on the server.

1. At the login screen note the URL to remotely manage the server, ex: <https://myorg.filewave.net:10000>
 - If there is no IP address specified because DHCP is not available on the subnet for your FileWave Linux Appliance, login with the username "fwadmin" with password "filewave" and in prior versions of FileWave it was username "root" with the same password.
 - CentOS (Deprecated): Run "nmtui" at the command prompt to launch the Network Manager Text UI so you can configure the networking for the FileWave VM appliance. You'll need to reload the IP stack with "service network restart".
 - Debian: Please see our KB on network configuration: [Networking - Assign static IP Address for a FileWave Appliance](#)
 - Skip the network configuration steps later in the Webmin.
3. Browse to this URL and log in with username "fwadmin" and password "filewave". We will change this password later.

4. Browse to Hardware > System Time on the left, pick the Change timezone tab on the right, pick your time zone and click Save. North American time zones all start with "America".
5. Go to System > Change Passwords on the left and select the "root" account on the right from the list of usernames. Enter a new root password, confirm it, and click Change. Note that this will change the default password for the root account used to log into the server from "filewave" to whatever you choose so enter a secure password that is easy for you to remember.
6. Choose Networking > Network Configuration on the left, and Network Interfaces on the right. Click the blue link labeled "ens160" or "ens32" for the Ethernet adapter. Change the IPv4 address settings to "Static configuration", enter a static IP, enter a subnet mask, and click Save at the bottom to continue configuring the DNS and routing.
7. You will no longer be able to access the Webmin UI for the FileWave servers via its old DHCP IP address. Change the address in your browser's address bar to use the new static IP address for the FileWave server that you configured in the previous step. Browse to Networking > Network Configuration on the left, and Hostname and DNS Client on the right. Enter the IP address for your DNS server and click Save.
8. Select Networking > Network Configuration on the left, and Routing and Gateways on the right. Pick "ens160" or "ens32" from the Default routes pull-down, enter the default gateway address for the subnet the FileWave server is hosted on, and click Save.
9. Go to System > Bootup and Shutdown_ on the left, scroll to the bottom on the right, and click the Reboot System button. When asked to confirm if you want to reboot the system with "shutdown -r now" click the Reboot System button again.



Webmin Dashboard

Search

- Webmin
- System
- Servers
- Networking
 - FirewallID
 - Network Configuration
- Hardware
- Refresh Modules

root

Boot Time Interface Parameters

Name *ens160*

Activate at boot? Yes No

No address configured
 From DHCP
 From BOOTP

IPv4 address

Static configuration
 IPv4 address: 10.10.10.40
 Netmask: 255.255.255.0
 Broadcast: Automatic 10.10.10.255

IPv6 disabled
 From IPv6 discovery

IPv6 addresses

IPv6 address	Netmask
	64

MTU Default

Virtual interfaces 0 (Add virtual interface)

Webmin Dashboard

Search

- Webmin
- System
- Servers
- Networking
 - FirewallID
 - Network Configuration
- Hardware
- Refresh Modules

root

DNS Client Options

Hostname localhost.localdomain

Update hostname in host addresses if changed?

Hosts file:

DNS:

Resolution order: Local hostname

None Listed ..

DNS servers:

Search domains:

Webmin Dashboard

Search

- Webmin
- System
- Servers
- Networking
 - FirewallID
 - Network Configuration
 - Hardware
- Refresh Modules

root

Routing and Gateways

Boot time configuration | Active configuration

This section allows you to configure the routes that are activated when the system boots up, or when network settings are fully re-applied.

Routing configuration activated at *boot time*

	Interface	Gateway	IPv6 gateway
Default routes	ens160	10.10.10.1	

Act as router? Yes No

	Interface	Network	Netmask	Gateway
Static routes				

	Interface	Network	Netmask
Local routes			

Save

Webmin Dashboard

Search

- Webmin
- System
 - Bootup and Shutdown
 - Change Passwords
 - Running Processes
 - Scheduled Cron Jobs
 - System Logs
 - Servers

webmin Start or stop the Webmin server

Select all | Invert selection | Create a new systemd service

Start | Stop | Restart | Start On Boot

Disable On Boot | Start Now and On Boot

Disable Now and On Boot

Reboot System
Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Shutdown System
Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

FileWave Central Setup

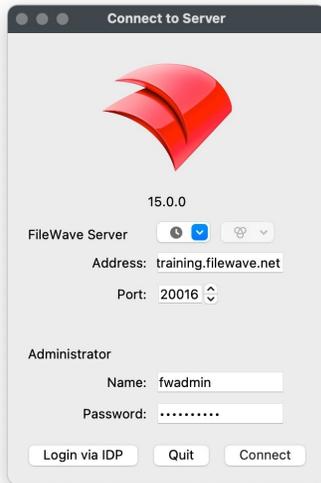
Let's login!

Now that you have the FileWave Server up and running, it is time to connect using FileWave Central. FileWave Central is a native application capable of running on macOS or Windows and is currently considered to be the "daily-driver". Starting with FileWave 14, you can now access the FileWave interface via a web browser to accomplish any Inventory, Location Tracking, or Deployment needs (Fileset creation not yet supported).

Download and Install the FileWave Admin

1. Visit FileWave's Software Downloads page [here](#).
2. Click the "Release Notes and Download" link for the version of your FileWave Server.
3. Scroll down to either "macOS Downloads" or "Windows Downloads".
4. Download either the "macOS Admin" or "Windows Admin".
5. Run the FileWave Admin PKG or FileWave Admin MSI and accept the licensing agreement.

Log into FileWave Admin



Open the FileWave Admin

- Windows: "Start Menu>FileWave>Admin"
- macOS: "/Applications/FileWave/FileWave Admin.app"
 - "Applications/FileWave/FileWave Admin (root).app" is only required for Fileset Magic.

Enter the Server Address, Username, and Password and then "Connect"

- Do not include "https://" in "Address" field
- Do not change the "Port" from "20016"

Credentials

- Hosted Servers: Address, Username, and Password will be provided by your FileWave Sales Engineer.
- On-Premise Server: Username: "fwadmin" Password: "filewave"

How to Save and Commit changes

As you will see, the FileWave Admin interface is simply laid out and intuitive however, one thing that may be unfamiliar is the concept of "Update Model". The "Update Model" button is essentially the FileWave "Save" button. For example, when you associate a software package to a Client device, FileWave will not apply that change in real-time but yet wait until you "Update Model" to commit the changes to the device. This gives you a window of opportunity to correct any accidental associations, deletions, or any other unwanted modifications.

After "Update Model" you will notice the "Model Number" will increment by one in the lower right-hand side of the FileWave Admin. Your Clients will check in periodically (Tickle Interval; 120 seconds) to see if there is a new Model version available. If there is a new Model available, the Client will download a new user-manifest and apply any changes that have been made for that Client. If there are no new changes for the Client or new Model, the Client will continue to idle for another 120 seconds.

The screenshot displays the FileWave Admin interface. At the top, navigation buttons include "Update Model" (highlighted with a green box), "Refresh", "Open in browser", and "Copy URL". The main dashboard area is titled "Dashboard overview & performance" and includes an "Alert Settings" link.

Primary Services:

- Boosters Info:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM. Message: "Some Boosters have errors. Please investigate." Includes a "Go to Boosters" link.
- Classroom Certificates Info:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM.
- DEP Accounts:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM.
- Email settings:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM.
- LDAP Extraction status:** Status Updated: a few seconds ago Feb 24, 2021 7:38:11 AM.
- APN for MDM:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM. Includes a "Go to Settings" link and an expiration date of "in 21 days Mar 17, 2021 9:01:14 AM".
- SSL certificate:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM.
- VPP Tokens:** Status Updated: a few seconds ago Feb 24, 2021 7:38:38 AM.

Sync Status:

Service	Last Sync Attempt
DEP Accounts	<ul style="list-style-type: none"> 6 hours ago Avery Feb 24, 2021 2:00:45 AM 6 hours ago Avery DEP Feb 24, 2021 2:00:45 AM 6 hours ago FileWave Feb 24, 2021 2:00:45 AM
LDAP Extraction status	<ul style="list-style-type: none"> 2 hours ago activedirectory.filewave.ch Feb 24, 2021 5:37:11 AM 2 hours ago ldap.jumpcloud.com Feb 24, 2021 5:37:11 AM
Tokens	<ul style="list-style-type: none"> avery.thomas+vpp@filewave.com - Users: 3 minutes ago Feb 24, 2021 7:35:45 AM - License: 3 minutes ago Feb 24, 2021 7:35:45 AM
Smart Group Count	9 days ago Feb 15, 2021 12:06:33 PM

Server Performance Status:

- Drive Space (GB):** Donut chart showing 57% used (blue) and 43% free (grey). Total: 157.4GB.
- CPU Usage (%):** Donut chart showing 99% used (blue) and 1% idle (grey). Cores: 4. Average: 1% per core.
- RAM (GB):** Donut chart showing 8GB used (blue) and 0GB free (grey). Total: 7.8GB.

Mail Queue: Last Check: a few seconds ago Feb 24, 2021 7:38:38 AM.

Update Server Model Dialog: A modal window titled "Update Server Model" displays a red checkmark icon and the text "Model Updated Successfully" with an "OK" button.

Left Sidebar (Client Inventory):

- Dashboard: 2
- Clients
- Filesets
- Associations
- Imaging
- Classroom
- iOS Inventory
- License Management: 1
- Boosters
- Inventory Queries
- Sample Queries:
 - All macOS: 14
 - macOS 10.10, 10.11, 10.12: 2
 - macOS 10.12 Sierra: 2
 - All Windows: 17
 - Windows 7: 2
 - Windows 7 Service Pack 1: 0
 - Windows 8: 0
 - Windows 8.1: 0
 - Windows 10: 0
 - All iOS: 6
 - iOS 7: 0
 - iOS 8: 0
 - iOS 9: 3
 - iOS: tracking enabled and out da...: 0
 - All Android: 2
 - Android 4.4 (KitKat): 0
 - Android 5 (Lollipop): 1
 - All Mobile: 14
 - CS 6 Design and Web Premium ...: 0
 - CS 6 Design Standard Collection: 0
 - CS 6 Master Collection: 0
 - CS 6 Production Premium Collec...: 0

Footer: "Everything is OK" on the left and "Licenses Used/Total: Computers 26/50000, Mobile 8/50000, Chromebooks 6/6" and "Model Number: 1799" on the right.

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:

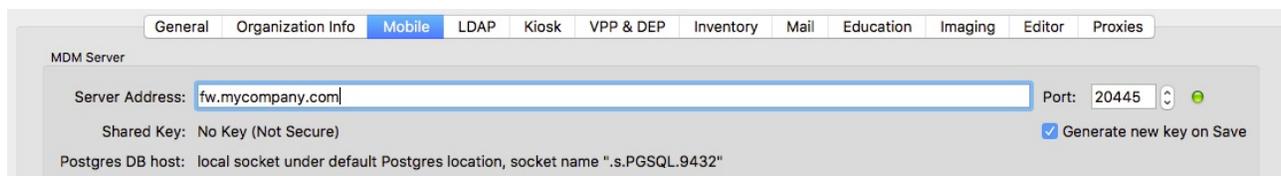
- Uploading a new PKCS12 server certificate
- Download the Apple DEP Certificate
- Configure DEP tokens
- Editing SIS details
- Manage Apple Classroom Certificate

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 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" Preferences 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 an 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 menu bar 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 menu bar 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 menu bar 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

```
GNU nano 2.3.1 File: /usr/local/filewave/apache/conf/mdm_auth.conf Modified
<Location /ios/enroll>
# AuthType Basic
# AuthName "Enroll iOS Device"
# AuthBasicProvider file
# AuthUserFile passwd/passwd
# Require valid-user
</Location>
<Location /ios/device_enrollment_profile>
# AuthType Digest
# AuthName "Enroll iOS Device"
# AuthDigestDomain /
# AuthUserFile passwd/passwd.digest
# Require valid-user
# ErrorDocument 401 "Enrollment credentials are needed."
</Location>
<Location /ios/dep_enrollment_profile>
# AuthType Digest
# AuthName "Enroll iOS Device"
# AuthDigestDomain /
# AuthUserFile passwd/passwd.digest
# Require valid-user
# ErrorDocument 401 "Enrollment credentials are needed."
</Location>
<Location /android/enroll>
# AuthType Basic
# AuthName "Enroll Android Device"
# AuthBasicProvider file
# AuthUserFile passwd/passwd
# Require valid-user
</Location>
<Location /android/project_number>
# AuthType Basic
# AuthName "Google Cloud Messaging configuration"
# AuthBasicProvider file
# AuthUserFile passwd/passwd
# Require valid-user
</Location>
Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
```

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 without 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.

```
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.

```
Ctrl + X
y
Enter
```

5. Restart the FileWave Apache process.

```
/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.

Client Group Structure

You get a group and you get a group, everybody gets a group!

Staying organized in life is important and it's no different within FileWave. This section will outline some workflows and best practices when it comes to grouping and organizing your Client devices. Leveraging FileWave Smart Groups, LDAP-based Smart Groups, and Clones, FileWave allows you to organize your devices no matter how advanced your Org structure is.

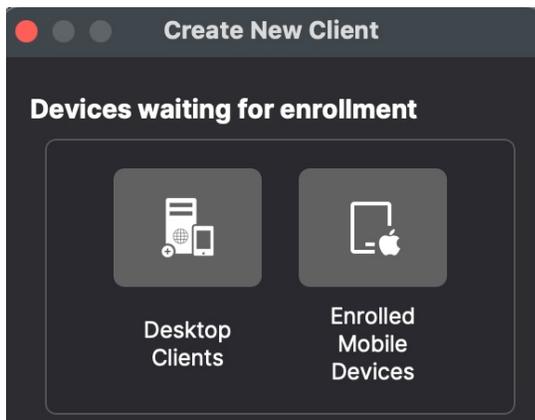
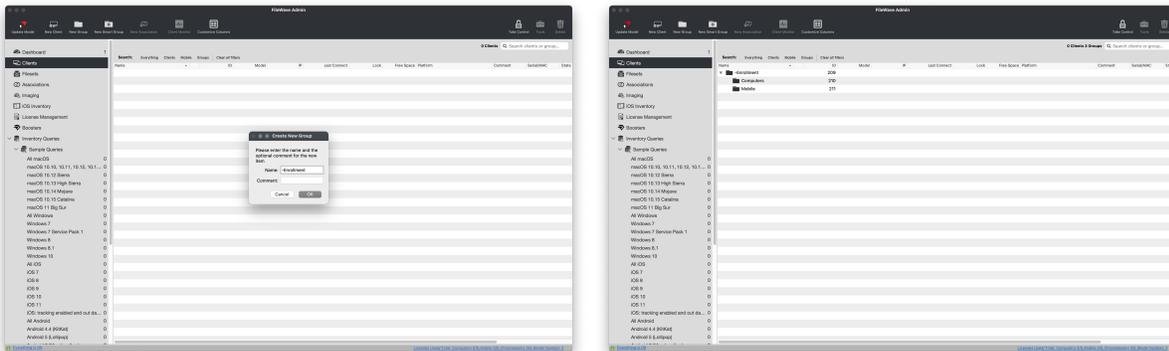
Creating a basic structure for automatic device enrollment

The first two groups we will create are to enable automatic device enrollment for both Client (Windows, macOS) and Mobile (iOS, tvOS, Android) devices. This "-Enrollment" group will contain all of the original device records within FileWave, therefore it is recommended to treat this group as a "safe zone". We will create other group structures to associate software and settings to your devices based on more granular criteria.

Create a New Group

1. Open FileWave Admin and navigate to "Clients" from the left pane.
2. Click "New Group" from the black menubar.
3. Name the first group as "-Enrollment".
 - We use a "-" so that the group floats to the top when sorted alphabetically.

We will now repeat this process to create a "Computers" group a "Mobile" group within the "-Enrollment" group. If you accidentally create a New Group outside of its intended group structure, simply drag-n-drop the group to its desired location.



Enable automatic device enrollment

By default, new devices will come into a "waiting area" so that you can manually add them to FileWave. We are going to make this process more efficient by enabling automatic device enrollment.

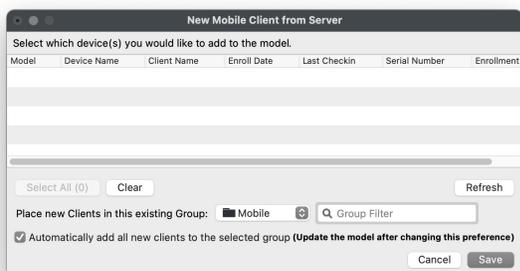
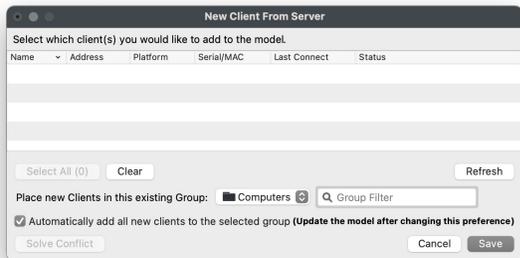
1. Select the "Computers" group from the previous section.
2. Click "New Client" from the black menubar.
3. Select "Desktop Clients" from the "Devices waiting for enrollment" section.
4. Check the box for "Automatically add all new clients to select group" unless you always want to approve new clients. This is

discussed in more detail in [Conflict Resolution](#).

5. Click "Save".

We will now repeat this process for the "Mobile" group by selecting "Enrolled Mobile Devices" from the "Devices waiting for enrollment" section.

And finally, as stated in the New Client window, we must "Update Model" to save our changes and finalized automatic device enrollment.



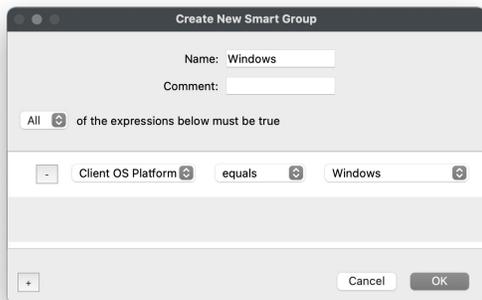
Creating Smart Groups

A Smart Group is a group that automatically "clones" devices based on a set of Inventory data points. These data points include hardware information, software information, LDAP information, and unique Custom Fields. If a device meets the specified criteria, it will be automatically "cloned" or duplicated into the Smart Group, and if it no longer meets the criteria it will be removed from the Smart Group. This allows for very dynamic associations to software and settings. For example, deploy Adobe Creative Suite to all macOS devices that have a custom "Department" field set to "Media".

For demonstration purposes we will create several Smart Groups based on the device's Operating System Platform. These Smart Groups can be used in production when establishing a baseline software group for each specific OS type.

Create "Platform" Smart Groups

1.



Open FileWave Admin and navigate to "Clients" from the left pane.

2. Create a standard Group named "-Platform" following the steps above.
3. Select the "-Platform" group and click "New Smart Group" from the black menubar.
4. Name the Smart Group based on the Operating System. We will first start with "Windows".
5. Click the "[+]" button in the lower left-hand corner.
6. Select "Client OS Platform" from the dropdown menu on the left.
7. Select "Windows" from the dropdown menu on the right.
8. Click "OK" to save the changes.

We will repeat these steps for:

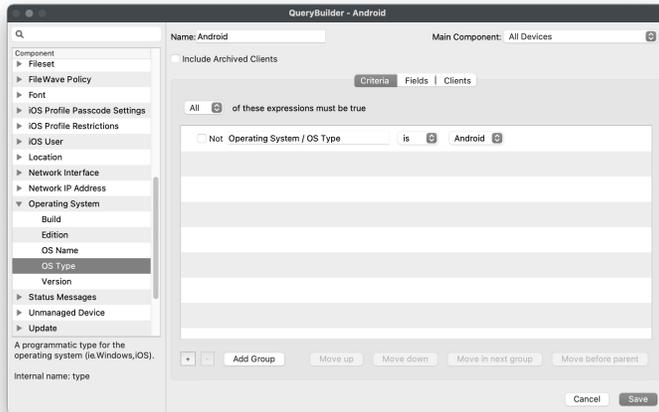
- macOS - Client OS Platform [equals] macOS
- iOS - iOS Device Type [equals] Any iOS Device

Creating more advanced Smart Groups

We will now create a slightly more advanced Smart Group that leverages FileWave's more robust Inventory Query Builder. The Inventory Query Builder will give us access to over 1000 data points that FileWave natively collects from the different device types along with any Custom Fields you have imported.

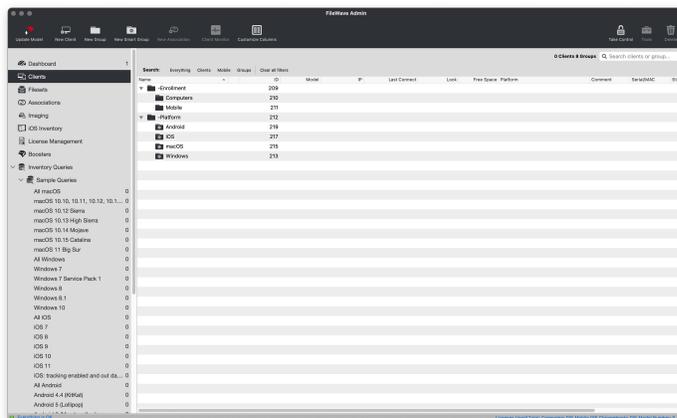
The next steps will outline how to use the Inventory Query Builder to round out our "-Platform" group by targeting Android devices.

1.



- Open FileWave Admin and navigate to "Clients" from the left pane.
- Select the "-Platform" group and click "New Smart Group" from the black menubar.
- Name the Smart Group based on the Operating System, in this case "Android".
- Click the "[+]" button in the lower left-hand corner.
- Select "Inventory Query" from the dropdown menu on the left.
- Click the "[...]" button to the right.
- Find the criteria that will be targeted using "Search" or by opening each sub-group, in this case "Operating System > OS Type".
- Drag-n-Drop the desired criteria from the left pane into the right-hand side "Criteria" pane.
- Verify that the expected results are returned in the right-hand side "Clients" pane.
- "Save" the Inventory Query and "OK" the Smart Group window.

Finishing up



Now that you have defined your Platform-based Smart Groups, any time a new device enrolls it will be automatically "cloned" into its respective Smart Group. It is recommended that you target these Smart Groups when deploying content to an OS type rather than targeting devices within the "-Enrollment" groups. Please note that Chromebook devices will adhere to their own group structure and will not belong to any other typical FileWave groups.

And as always, please "Update Model" to save your group modifications.

Cloning devices

If you find yourself needing to group devices that don't have any unique attributes that you can target in a Smart Group, you can simply "clone" the devices into any group you'd like. This allows you to still have flexibility with content associations while not jeopardizing the original Client record in the "-Enrollment" group. You can delete or move a clone of a device without affecting the original Client record or any other clones of that same device. For example, Tommy participates in both "Interactive Media" and "STEM" classes during first semester but in second semester he only participates in "Interactive Media". Since Tommy's device no longer needs the "STEM" software, we can delete his cloned device from the "STEM" Client group without affecting his "Interactive Media" content associations.

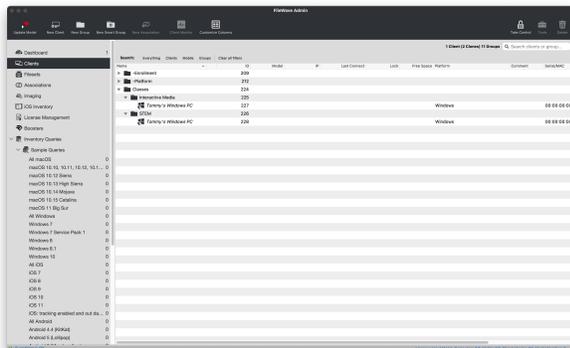
Creating a clone

1.



Right-click on any device or device clone and select "Create Clone".

2. Select the Client group where you want the clone to be created.
3. You will now see a new clone indicated by italics font and an upwards facing arrow on the Client's icon.



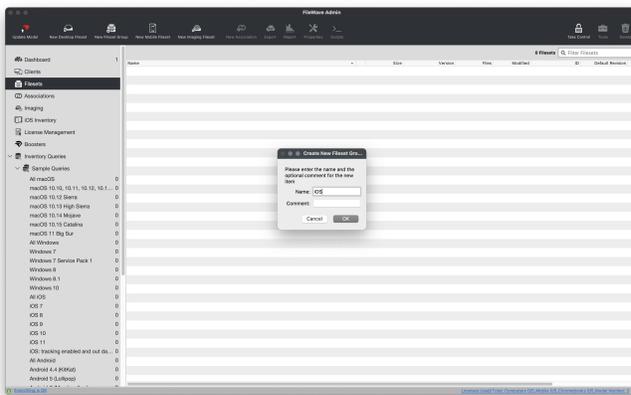
Software Group Structure

You get a group and you get a group, everybody gets a group!

Again, really? Yep. We recommend that you stay just as organized with your Software (Fileset) groups as you do with your Client groups. This will enable you to do "Group to Group" associations, allowing for even more dynamic and automated deployments. For example, if we have an "Interactive Media" Client group and an "Interactive Media" Software group, we can associate them at the group level so any time a new piece of software gets added to the Software group it will be deployed to all devices in the Client group... and vice versa, a new Client gets added to the Client group and it will receive all software in the Software group, all without having to make a new Association.

Creating Software (Fileset) Groups

Your group structure will great depend on your organization's structure but a good place to start is by sorting out your software by the intended Operating System.

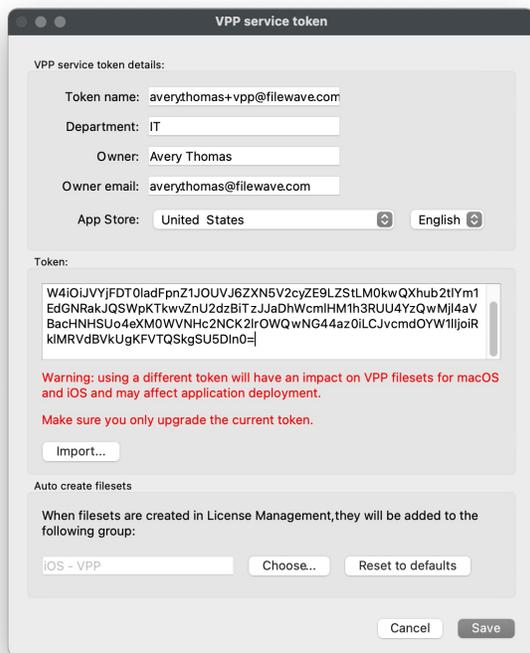


New Fileset Group

1. Open FileWave Admin and navigate to "Filesets".
2. Click "New Fileset Group" from the black menubar and name accordingly, in this case "iOS".
3. That's it! You can now create additional sub-groups if desired.
 - FileWave honors the "parent/child" relationship when associating content.

Configuring automatic VPP Fileset imports

This section is intended for those going to sync with Apple's Volume Purchase Program as described in this future [section](#). When syncing VPP licenses into FileWave, you can specify which group each VPP Token's Fileset will be created within. This is very helpful especially if you have multiple VPP Tokens designated for different departments and/or sites.



Auto create VPP Filesets

1. Ensure that you have the target group created prior, we will be using the "iOS - VPP" group.
2. Open "FileWave Admin > Preferences > VPP & DEP", click "Configure tokens" from the "Volume Purchase Program" section, and authenticate.
3. Double-click your existing VPP Token.
4. Click "Choose" from the "Auto create filesets" section and select your desired Fileset group, in this case "iOS - VPP".
5. Click "Save" on the "VPP service token" window, "Close" and "OK" the other Preferences windows.
6. Repeat these steps for any other VPP Tokens.