FileWave Administration

Planning, Setup, Installation and Operation

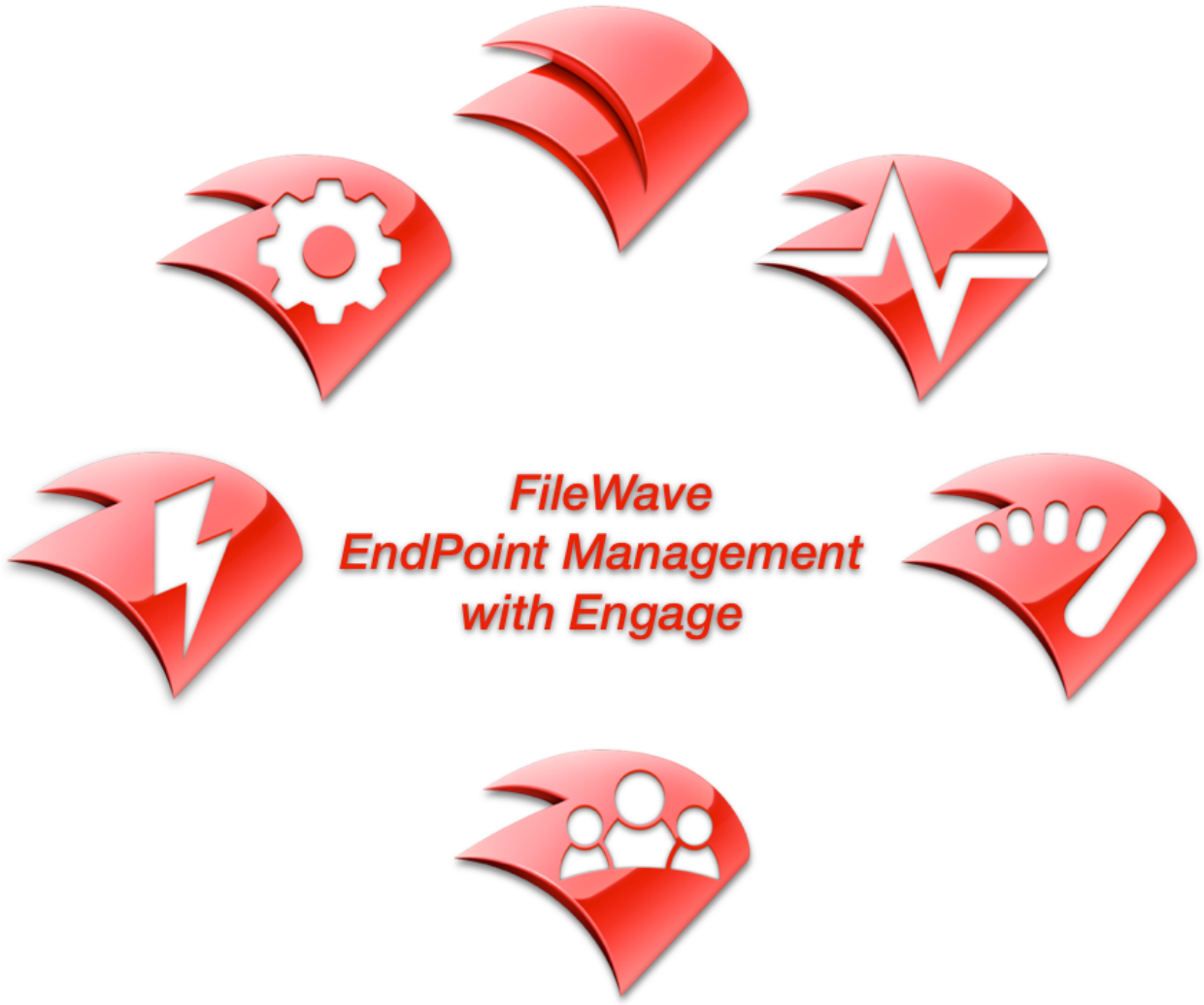


Image / Deploy / Manage / Maintain / Engage

Version 10.0

Copyright and disclaimer

FileWave (USA), Inc.
10711 America Way
Fishers, IN 46260

FileWave (Europe), Gmbh of Switzerland
St. Gallerstrasse 1
9500 Wil, Switzerland

Overview

This manual is designed to cover the essential information and workflows that would allow a systems administrator to install, configure, and operate the various components of the FileWave Systems Management suite. The document is broken into sections describing the key operations of FileWave to include:

- Chapter 1 - Overview of FileWave capabilities and components
- Chapter 2 - Planning and deployment workflows
- Chapter 3 - Installation and configuration of the FileWave servers, including Imaging and Engage VMs
- Chapter 4 - Installation and configuration of FileWave Boosters
- Chapter 5 - Installation and configuration of the FileWave Client plus Apple's Device Enrollment Program (DEP)
- Chapter 6 - Working with Filesets for application, ebook and content distribution, plus Fileset Magic
- Chapter 7 - Working with License Management and Apple's Volume Purchase Program (VPP)
- Chapter 8 - Using FileWave to provide mobile device management (MDM)
- Chapter 9 - Working with FileWave Inventory, including iOS inventory, smart groups, and reporting
- Chapter 10 - Imaging with FileWave, including using Lightning
- Chapter 11 - Working with FileWave Engage for classroom management
- Appendices - Network port numbering, FileWave Command line tools, Certificate management, and more

Note: This document is focused on FileWave version 10.0. For information on version 9, see the previous manual.

Screenshots are from FileWave running on OS X and Windows - the functionality is identical between the two versions. (Most screenshots are from the v10 beta, labelled 9.9.0.)

Some of the graphics used in this document represent possible future versions of FileWave artwork. The presence of these items is not a product announcement.

This document is the primary reference for FileWave technical operations. It is supplemented with technical and Quick Start guides plus recipes to show you how to get more out of your deployment. These items are posted on the FileWave site under Support. https://www.filewave.com/quick-starts

ChangeLog

9/30/15 - First publication of v10.0 manual

Compatibility

FileWave 10.0 OS Version Support						
OS	**OS Version**	**Server**	**Booster**	**Admin**	**Client**	**MDM Client**
OS X	10.7	■	■	△	***Legacy Support**	
	10.8	■	✓	△	✓	
	10.9 - 10.11	✓	✓	✓	✓	
Windows	XP		■	△	***Legacy Support**	
	7		✓	✓	✓	
	8		✓	✓	✓	
	8.1		✓	✓	✓	
	10		✓	✓	✓	
	Server 2008 R2	✓	✓			
	Server 2012	✓	✓			
	Server 2012 R2	✓	✓			
Linux	5.11	✓	✓			
	6.6	✓	✓			
iOS	8					✓
	9					✓
Android	4.1 - 5+					✓

Legend

✓ FileWave 10 will be fully supported.
■ New features of FileWave 10 will not be supported.
△ Admin can only be used for Fileset creation.
***Legacy Support**: Supported using FileWave version 9 client. Does not support new FileWave 10 features/functionalities.

* See the FileWave downloads page for specific patch versions of supported operating systems.

Notices:

- Support for OS X Snow Leopard (10.6) was deprecated as of FileWave version 8.5 (If you are supporting 10.6 clients, you must continue to use the FW v8.1.5 client on those devices.)
- FileWave Server must be version 7.x or higher for upgrade to v10
- Due to changes in how profiles are installed on OS X v10.10 and higher, if you install a profile that has “Controls when the profile can be removed” set to “**Never**”, FileWave will not be able to remove that profile through dis-association of the Fileset. The action will require local admin intervention. The workaround is to use a password protected removal with the “With Authorization” option.

What's in FileWave v10.0

FileWave version 10.0 is a significant upgrade from earlier versions. The list of new capabilities is extensive:

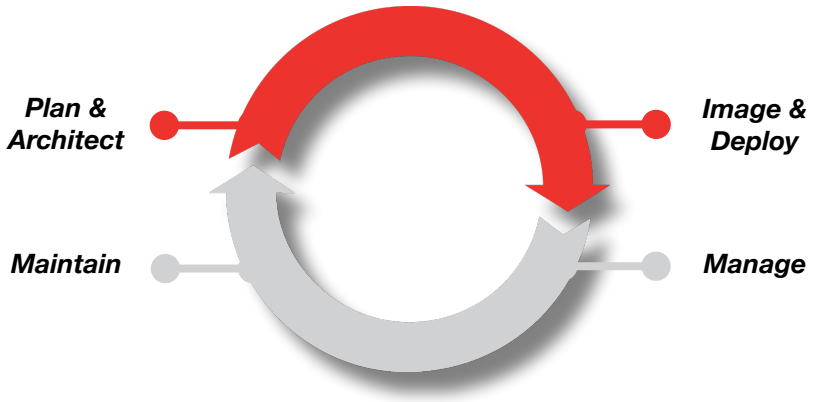
- Support for a new NAT-capable Remote Control functionality built into the FileWave Client
- Fileset dependencies to allow setting Filesets to be dependent on other Filesets being installed first
- A modernized "flat feel" User Interface to better match with current operating systems
- Improved MDM security supporting uploaded SSL certificates to simplify manual enrollment
- Enhanced Admin console to include customizable columns, increased information in the Client Info view
- Improved MSI Fileset functionality - MSIs will now use **uninstall** when Fileset is removed
- Additional command line functionality
  - Ability to use names as well as IDs for clients/groups, Filesets and associations
  - Ability to import Filesets / images into a Fileset group, allows for use of **AutoPKG** scripts
  - Added ability to root imports into different locations within a Fileset
- Improved Imaging functionality, to include avoidance of accidental mass image associations and better control over which sub-admins can cause computers to re-image
- Redesigned Kiosk with a "Show always" menubar item, client info display pane, and providing rich text content
- Smarter Smart Groups that can have delays set to avoid network issues with updates, and the ability to convert smart groups into static groups
- Software Updates now contain iOS v9 updates that can be scheduled in the background, as well as OS X 'El Capitan' updates **(iOS v9 updates scheduled for a 'dot' release post v10.0)**
- Engage flexible device control that allows teachers to control a wider range of MDM settings through profiles that are made available to the teachers
- Support for Apple's System Integrity Protection (SIP) for OS X v10.11 with Inventory reporting compliance
- Improved Device Enrollment Program (DEP) functionality, including:
  - Control options for AppleID, Touch ID, Payment, Zoom, Siri
  - Support for Apple Configurator 2 based Auto Enrollment
  - Support for "Wait for device configuration" to insure all profiles and settings are installed before releasing control to the user
  - Support for device naming where the actual physical device name is changed per settings in DEP profile
  - Support for creation of a local non-admin user account, as well as a hidden local admin account in OS X
- Improved Volume Purchase Plan (VPP) functionality, including:
  - App assignment direct to device allows institutions to bypass AppleID requirements
  - Support for VPP account protection that keeps any admin from taking over any VPP token that is in use, such as Apple Configurator taking over (stealing) an active FileWave VPP token
  - Additional backend functionality to improve network performance and avoid VPP errors
- Profile management improvements, including:
  - Search within active profile payloads for keywords, allowing display of configured settings only
  - Preference payloads now support opt-in/opt-out options and third party preference panes
  - Profile Filesets can now be exported
  - Login Window's Access tab now supports network users as well as local users
- New iOS v9 / OS X v10.11 payloads including:
  - Usage restrictions
  - FileVault profiles
  - Mail Drop
  - Single Sign On
- Install Media - an iTunes Fileset containing an eBook link will install the book directly into a user's iBooks Library; plus FileWave can deliver in-house PDF/ePub/iBooks content to the user's iBooks Library

1. What is FileWave?

FileWave is a multi-platform, unified endpoint management solution set that provides IT systems administrators with the capabilities to image, deploy, manage and maintain their infrastructure in real time across a wide variety of devices using an architecture that scales to meet current and future needs. It is designed to be a key part of your deployment lifecycle.

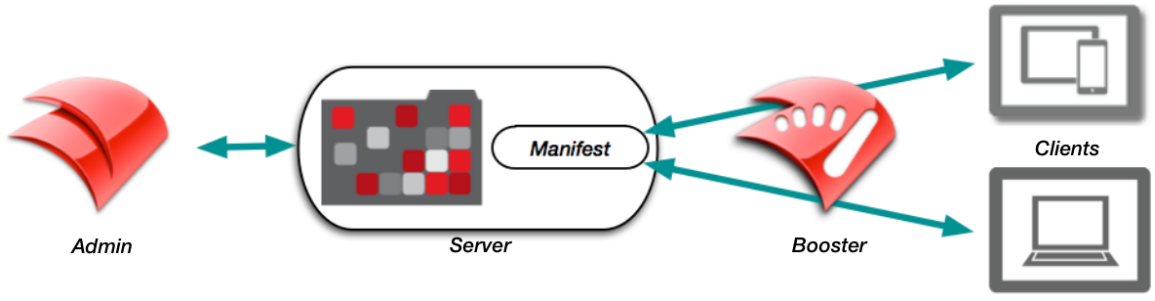
Institutions dependent on technology generally follow a deployment cycle. This cycle involves architecting and planning the use of the technology as defined by the needs of the institution, imaging and deploying the technology to the designated end user devices, managing the technology as needed to ensure either a consistent behavior of the devices or providing the best possible user experience, and maintaining the technology throughout the cycle. This practice ensures the end user's ability to meet the various needs and missions of their teams, departments and institutions.

FileWave is designed to fulfill the needs of the IT support group in accomplishing its systems management tasks. The cycle of imaging, deploying, managing and maintaining your institution's technology is critical to mission accomplishment. The use of a robust, scalable systems management solution will serve to enhance your support capabilities.



1.1. How does FileWave work?

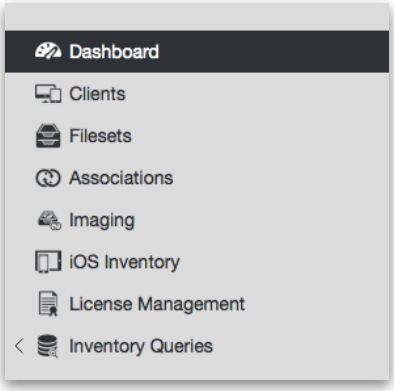
FileWave is a combination of tools and services all integrated through a common administrative application front end. Since the FileWave Admin application is multi-platform - Apple's OS X and Microsoft Windows - a systems administrator is not limited to a single platform for performance of day-to-day lifecycle management. The FileWave basic workflow involves the 'push-pull' interaction between the FileWave Admin, FileWave server, and FileWave clients; as well as other important services and tools.



The **FileWave Admin** creates a **Fileset** which resides on the FileWave server. **Filesets** contain applications, images, profiles, books, settings, or other content are associated with client devices. The **FileWave client** is sent a **Manifest** that identifies a new Fileset. The Client then requests the **Fileset**, that may be cached at a **FileWave Booster** in order to provide better scalability. A basic FileWave configuration consists of a single administrator user connecting to a **FileWave server** to manage and maintain a set of clients. Multiple administrators may be in use, as well as

Boosters to decrease network load by distributing Filesets closer to the client systems. Each of the major components is described in the following section.

1.2. FileWave Components



In this section, we will describe the key FileWave components:

FileWave Server

The FileWave Server is the central repository to host every file to be delivered to Clients. It consists of five processes and a web server. The first process interacts with logged-in Administrators. The second process services incoming requests from Clients and boosters. The third process interacts with a directory server through LDAP. The fourth process communicates with Apple and Microsoft software update servers to download the current lists of available software updates. The fifth process is the Postgres database service for Inventory and MDM. Finally, the web server is the FileWave MDM Server; it handles Mobile Device Management (MDM) components. Detailed information on setting up the FileWave server is covered in chapter **3** of this manual.

FileWave Admin application

The FileWave Admin application is the primary interface to the FileWave Server. The FileWave Admin displays eight views that give a representation of the FileWave Server's database. These views are the Dashboard, Clients, Filesets, Associations, Imaging, iOS Inventory, License Management, and Inventory Queries views. FileWave Admin also acts as the unified management console for creating and administering FileWave administrator accounts; network imaging for the Imaging Appliance; managing Apple DEP and VPP associations; software updates for iOS 9(+), OS X and Windows; and overall management of all devices and Filesets. Multiple instances of the FileWave Admin application can be in use at the same time with specific devices, groups and Filesets assigned to various administrator accounts. Detailed information on configuring and using the FileWave Admin application is in chapter **3** of this manual.

FileWave Client (OS X and Windows)

The FileWave Client has two processes, **fwcld** and **fwGUI**. The first runs as a LaunchDaemon on OS X and a service on Windows. This means it runs in the background without any user interface. The client starts automatically after being installed and each time the device boots. The fwcld process always runs with root (OSX) or local system (Win) privileges to allow for maximum access by any management operations. The second process, **fwGUI**, handles user interaction with the client, such as asking the client to quit open applications and informing them of the status when activating rebooting Filesets. The **fwGUI** process is what provides the **Kiosk** / self-service functionality. The new **Imaging Virtual Server** (IVS) contains a modified version of the **fwcld** for reporting its status back to the FileWave Admin. Chapter **4** of this manual covers the installation and configuration of the FileWave client.

Filesets

FileWave's patented Fileset technology provides the ability to distribute applications, content, and management settings at the file level. While FileWave supports distribution of the standard **pkg** and **msi** packages, its capability to distribute individual files, application bundles, content and management profiles allows for a level of granular control missing from other systems management solutions. Filesets can be distributed to clients and cached for activation at a later date; a process that provides maximum scalability and control over the deployment cycle.

When a Fileset is distributed, it is protected from network outages. If there is an interruption in the transmission, FileWave will resume the distribution as soon as the network is restored. Filesets can also be modified after distribution. If any portion of the Fileset is modified by the administrator, only that specific portion of the Fileset is sent out to the associated clients. This process greatly reduces the network traffic for deployments. Another feature is the ability to deploy content and roll back to the previous version of that item if there is a problem with the deployed item. Self-healing functionality allows a Fileset to automatically repair itself if the end user deletes a portion of the payload. Chapter **6** of this manual covers the creation, configuration, distribution, and management of Filesets.

Self-service Kiosk

FileWave's self-service Kiosk provides you with the ability to allow end users access to unique content at their own device. In a BYOD deployment, you could post institutionally owned applications, documents, updates, and even iTunes content, such as podcasts, for the end users to install at their convenience. In most of the deployment models (discussed in the **Planning** section), you can assign custom application sets to groups as needed. Users do not need to be local administrators in order to install applications or content. End users can be provided with new applications,

updates, documents, and other key content needed. The end user also has the option of un-installing that same content to free up space as needed on a device. Use and configuration of the **Kiosk** is covered in chapter **5**.

Booster

The FileWave Booster is designed to act as a Fileset caching device for clients assigned to it. Unlimited Boosters are allowed, regardless of license count or type. The FileWave Booster allows administrators to increase the speed and scale of the Server's distribution of Filesets to Clients. When a set of Clients are connected to a Booster, their total network load on the Server will be roughly equivalent to a single Client connecting directly to the Server from that location. The use of Boosters can benefit remote sites with bandwidth constraints by providing a focused, local target for clients as well as a single point of distribution from upstream. While the Booster caches Filesets, all other traffic to and from the client - inventory information and manifests - are still communicated directly with the FileWave server.

Boosters are designed to work with Windows, OS X, and Android clients. iOS clients do not have the ability to use a booster for cached Filesets. You should take this into consideration when planning the FileWave server device type. Chapter **4** covers the planning, setup and configuration of **Boosters**.

Imaging Virtual Server (IVS)

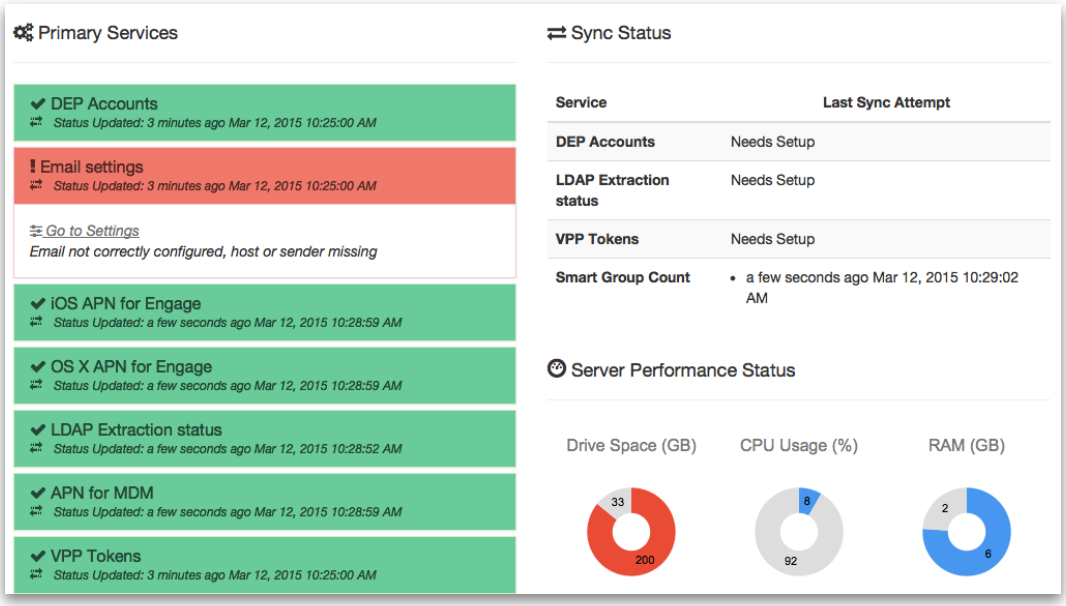
The FileWave Imaging Virtual Server is a standalone Linux container (CentOS) that you can download from the Support site and run on any device that supports a Virtual Machine application, such as VMware™. The IVS provides NetBoot and PXE boot engines. Storage for network images for OS X and Windows, as well as Windows Drivers images is now on the FileWave server. The FileWave Admin provides the management console for associating network images with designated client devices. Setup of the **IVS** preferences is in chapter **3**, chapter **10** focuses on Imaging workflows and best practices.

Engage Virtual Server (EVS)

Engage is an education-focused, classroom management tool. Engage has three primary components - the Engage server, the FileWave server, and the Engage client. The Engage server provides caching of the SIS DB and storage of study content and polls. The FileWave server component provides linkage between the Apple Push Notification service, Inventory, and the client applications. The Engage client provides both teachers and students with access to the various functions of Engage, such as polling, Eyes Up Front, and Single App Mode. Setup of the **EVS** is in chapter **3**, chapter **10** focuses on the Imaging workflows and best practices.

Dashboard

FileWave provides an integrated Dashboard displaying a snapshot of the current status of the FileWave infrastructure. The dashboard can be “torn off” to run on a separate display, and you can copy the URL of the dashboard to provide to another systems administrator for viewing on their own device, including on a tablet. The information posted includes the status of all major services, such as DEP, VPP, and LDAP; account sync status; server performance status; and server licenses; plus much more. Chapter **3** covers Dashboard configuration and use.

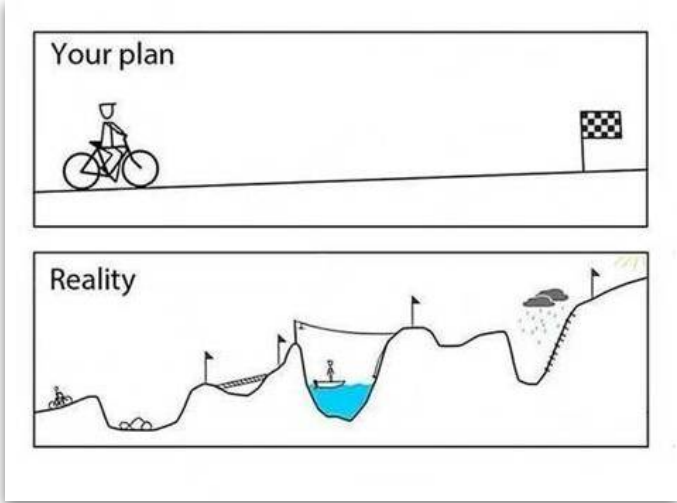


1.3. FileWave Terminology

- *Fileset* - A set of common Files and Folders meant for delivery to a FileWave Client. The Files and Folders contained in a Fileset represent the files and folders installed on a computer by a specific software application's installer.
- *Kiosk* - The self-service portal to the FileWave server for a specified device. The Kiosk contains an Install pane with associated applications and content for that device/AppleID, and in the case of OS X/Windows devices, an Info pane with device configuration information and a Verify button for the user to initiate a request to the server to verify, update, and repair any associated Filesets.
- *File* - A File in a Fileset represents a File that will be delivered to a specific location for a FileWave Client. Files have Attributes and Permissions.
- *Folder* - Files in a Fileset are organized into Folders. A File is activated in the corresponding Folder on the Startup Disk of the FileWave Client. Folders do NOT have Attributes ONLY Permissions.
- *Attributes* - Properties of Files that specify how the Files are treated once the FileWave Client activates them.
- *Permissions* - Properties of Files and Folders that specify the access rights of the Files and Folders. Permissions are set when the FileWave Client activates the Files and Folders in a Fileset. Self-healing also sets permissions during the verification phase.
- *Clients* - A Client represents one computer with the FileWave Client software installed or a mobile device that has been enrolled.
- *Client Group* - A Client Group is a container of like Clients and/or Client Groups.
- *Clone* - A Clone is an alias or shortcut of a Client or Client Group that can exist in many Client Groups.
- *Associations* - An Association is made between a Fileset and a Client or Client Group and represents the link between the two objects. Time-based attributes can be assigned to the Association. Associations are how distributions are made. You can also make associations between images and clients, licenses and Filesets, and VPP users and devices.
- *Time Attribute* - A Time Attribute is a property of an Association that specifies the time a FileWave Client executes actions.
- *Archive* - To archive a device is to remove it from active monitoring. The device remains in the database with its last reporting information intact; but the device is no longer counted as an active client.
- *Administrator* - A user that may log into the FileWave Server via the Admin application. Your license code determines the maximum number of administrators that can be logged in concurrently.
- *Model Update* - The command that is issued to the FileWave server to lock in all changes that have been made by an administrator. During a model update, all modified Filesets are updated on the server, the server model is incremented, and the automatic backup process stores the previous model. Filesets are activated based on their scheduled attributes the next time the client checks in with the server.

2. Planning your deployments

Deployment planning is contingent on understanding these key factors - infrastructure, deployment models, and systems management solutions. All of these items will have a direct impact on the success of your deployment.



"In theory, theory and practice are the same. In practice, they aren't."

2.1. Infrastructure planning

When planning a deployment, you should always take the time to evaluate these questions - what is the status of my current infrastructure, what is the mission of my institution, and what changes do I need to make in order to match my infrastructure to the needs of the mission? While this may sound somewhat esoteric, what you are really looking at is "do I have the ability to help my users get their jobs done?" The guidelines for planning in this section are here to assist you in moving from where you are to where you could be, and we will be using the capabilities of FileWave to get you there. Let's begin by evaluating the existing infrastructure.

All aspects of your current infrastructure should be evaluated on a regular basis. They consist of these areas:

- Electrical wiring and load capabilities
- Wired and wireless networking coverage and capacity
- Network services and accounts
- Network storage, backup and file sharing capabilities
- Availability and functionality of collaboration services
- Institutional training capability
- Institutional customer support capability (help desk)
- Security and disaster recovery

Electrical

Once upon a time, when all of the technology in a business or school sat in a single room, your ability to plan for electrical load and capacity was pretty easy. Now, with hundreds, if not thousands of users carrying devices that need charging, desks with computers and monitors, and auditoriums needing high resolution projection systems, your power needs can become one of the largest stumbling blocks in a deployment. Do you have the capacity for your users to recharge mobile devices during breaks or between classes? Are the offices and classrooms wired to allow for all of the tech that may be used there?

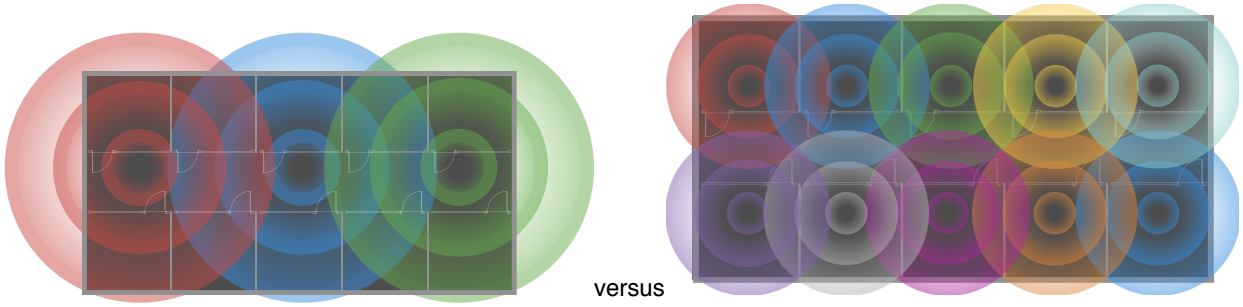
For example, in the US, the average laptop uses a 50-60W charger, for a classroom with a cart of 30 laptops you would need a circuit able to handle between 12.5 and 15 Amps. If it was a cart with 30 tablets, then the requirements would be around 2.5 and 4 Amps per cart. This is not counting lighting, desktop systems, projectors, and other electrical needs in that room. Building a good electrical load map would be an excellent way of determining where your efforts need to be when that 7000 device 1:1 project begins.

Wired and Wireless Networking

As with electrical needs, networking needs are often relegated to the “been there, done that” mode. It is important, however, to review your networking needs in conjunction with an influx of new equipment. Much of the wired networking at many sites was designed around a central server model with limited user content going back and forth. A lot of the wireless networking was done back when the design focused on just getting a WiFi signal to each room instead of concentrating on density and capacity. Re-evaluating the network needs in response to new service needs may be a valuable exercise. What services have changed since you last configured your network? How much traffic is centralized versus decentralized?

An example of a network needing reassessment is one that was designed when users were on fixed systems with a network login to a network home directory, and the expectation was for basic document creation with limited Internet access. Compare that with a building full of users on mobile devices using iCloud or Google Docs, and constantly moving within that building. You should also be looking at the WiFi capacity of a building in terms of density versus coverage. While you might have a signal on your mobile device, not having the bandwidth to do your job (or your classwork) will be detrimental to the overall success of the deployment. A good test series to run on both your wired and wireless portions of your network are speed tests and packet loss tests. Run some capacity tests to ensure that all of your users can get acceptable performance wherever they may be - such as having an entire auditorium filled with users - online - at the same time.

Networks need to be designed for **capacity** versus **coverage** due to the increased numbers of devices being deployed. Think in three dimensions of the number of Access Points (APs) needed to provide a solid, high-speed internet connection. Just insuring a signal is no longer enough. You need to imagine a building populated with thousands of devices, all requiring a high speed connection, at all hours of the day or night.



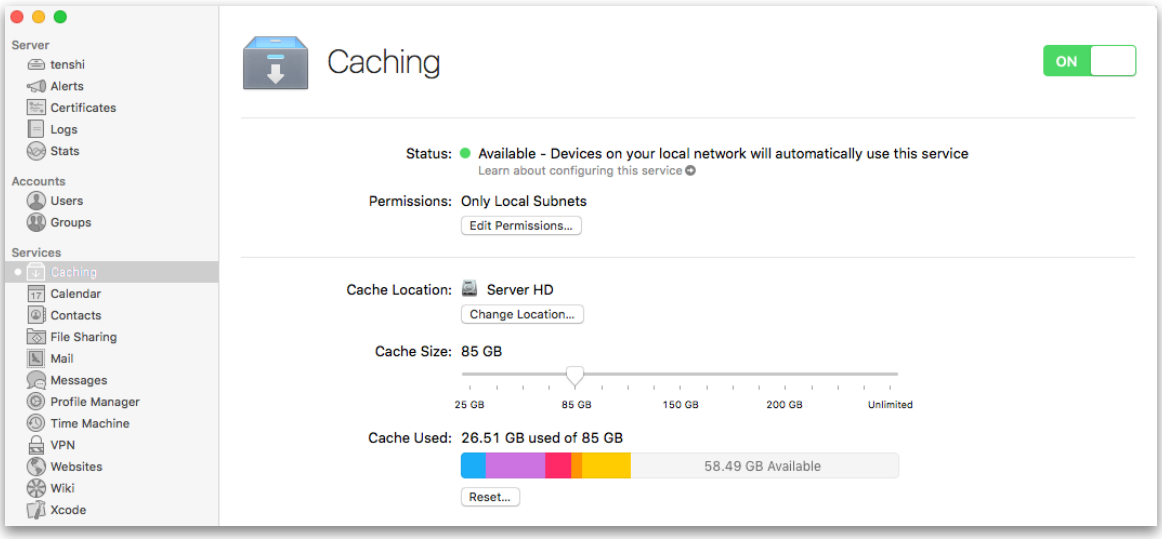
Modern networks with a predominance of 1:1 and BYOD deployments may no longer require users to access an LDAP directory in order to use their device. While that procedure was useful in the days of network home directories, a user on their own laptop, or even desktop, would probably need to access LDAP-based services at random intervals. This change could reduce network traffic and binding issues significantly. While much of the information on properly designing your wireless network will come from your chosen wireless provider, Apple has published some very useful information in its deployment guides: Apple iOS Deployment Guide - WiFi and Apple OS X Deployment Guide - WiFi. Take special notice of the information on roaming with Apple devices.

Another network requirement may be supporting Apple TV and AirPlay. You should evaluate the number of Apple TVs you will need as well as the policies that will control access to those devices. FileWave supports profiles that control access to specific Apple TVs, as well as deciding which devices will be allowed to use AirPlay. The Engage app allows teachers the ability to direct a student device to present to a designated Apple TV.

Network Services

The services provided on your network should enhance the user experience and assist in securing the network from external threats. Services such as DNS, DHCP, VLANs, LDAP, and VPN are all necessary; but should be evaluated regularly for reliability and scalability. A service such as DNS should be provided as close to the end users as possible in order to reduce lag times when contacting external services. Caching DNS servers are a great tool for this process. Users can be placed on unique VLANs in order to streamline communication between like groups; however, a little caution is called for when creating those boundaries. For example, educators and students should be on the same network segments, when possible, in order to facilitate their inter-communication. If there are secure services the educators need access to, then providing them with VPN access to those services is better than isolating them from their students.

If you are going to be deploying a large number of iOS or OS X devices, then you should explore deploying Apple OS X servers running the **Caching** server process. The caching server speeds up the download of software distributed by Apple through the Internet. It caches all software updates, App Store purchases, iBook downloads, iTunes U downloads (apps and books purchases only), and Internet Recovery software that local Mac and iOS devices download. You can find the current list of supported content types in the Apple Support article Content types supported by the Caching service. The caching server supports clients with OS X v10.8.2 or later and iOS 7 or later, and by default is configured to support clients that share the same public IP address behind a NAT.



Network filtering, proxies, and content filters are all part of a modern deployment; but they shouldn't interfere with end users being able to do their jobs. Take time to test your filtering and network shaping from the perspective of the various end users. If you can work with the same restrictions they have for a week or two, then odds are, they can too.

File Sharing, Storage, and Backup Services

File sharing has evolved from the simple network home directory to a series of collaborative services such as DropBox, Google Drive, and iCloud Drive. With many, if not most, users keeping their files on the same device they carry, the need for ad hoc storage is important. Users collaborate more, with larger and larger files, and the ability to support that kind of random access storage is very important. This also affects the need, or lack thereof, for network directory binding. While single sign-on can be an important service, if users are spending more time away from the institutional network than on it, then the possible interference with their operational use of their device from constant attempts of the directory service client and server to communicate can be a Bad Thing™.

For end users on iOS and/or OS X devices, opening up the network to iCloud™ storage provides built-in backup and document storage in the cloud. It can also be accessed from Windows devices.

Another factor affecting many 1:1 deployments is the lack of a dedicated backup capability for end users. A simple backup operation could consist of offering training on using simple backup solutions such as Apple's Time Machine and an institutional deal for external storage devices, such as SSD drives. On the other hand, setting up a dedicated network backup solution, such as Code42's CrashPlan, that can be automated may be a better approach. A solution such as this could be automated so that end users need only follow some simple instructions to login and set a timer. The outcome of this process would be a lot less angst when the time comes to either replace a user's device or perform a full erase and restore.

Collaboration Services

Explore the abilities you have to provide collaboration and file sharing services. Collaboration services can include Jabber and other chat functions, video conferencing, screen sharing, and texting applications. Many educational applications for teachers also include some type of chat functionality. Are you providing support for these services, or restricting them? What is the impact on the organizational mission(s) from the loss of these functions? Remote meetings and other such services have become a standard for both business and education. Being able to promote

and support these types of services may mean the difference between a successful organization and a frustrated one.

Examples of useful collaboration tools range from remote control of a user's device from the institution's Help Desk to using Apple's AirDrop capability for a team to rapidly share group files. All of these kinds of services should be explored first from the "how useful to the end users is this" point of view before jumping on the "how much of a problem is this to support?" point of view.

Training Capability

Two types of training can affect an institution's deployment cycle - end user training and IT staff training. End user training should focus on helping the user achieve independence in their use of deployed devices. This can range from learning how to use the most common applications to being able to troubleshoot and back up their device. The goal is to reduce users' need for IT stepping in to perform day to day operations for the end user. Studies have shown that an IT shop that promotes end user training and personal responsibility has significantly fewer support calls and issues than the shop that focuses on end user control and restrictions.

The second area of training is support staff training. A good measure of capability and functionality in an IT staff is the amount of cross-training and technical training that is done. If your team can substitute for each other in using the systems management tools, and can step in to support your end users regardless of the devices they are using; then you have a confident, well trained staff. Training for either group can be online, leader-led, or class labs. The advantage FileWave brings to the IT staff is providing a single, unified administrator console for all device management.

Customer Support

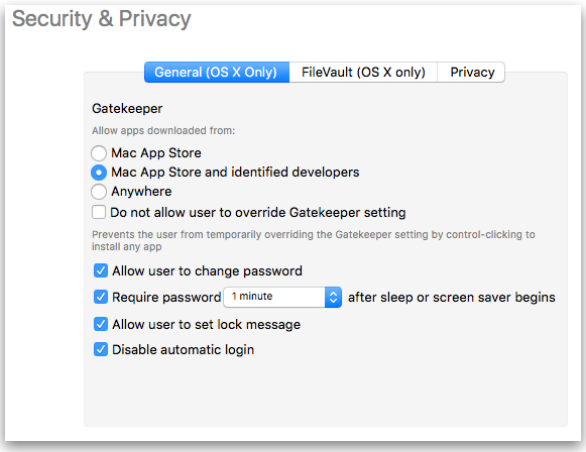
The question you should ask yourself as you prepare for the deployment cycle is "do we have a formal help desk operation?" If your organization can keep track of technical issues, understand what problems the end user community encounters, and can access a common database of solutions, then you have a formal help desk system. This is no longer something that 'might' be needed. Institutions are trying to deal with deployments of hundreds, or thousands, of systems, keep those systems up and running, and keep the users trained on how to best employ those systems in order to meet organization goals and missions. An ad-hoc support plan will do a disservice to the institution and to your staff.

Security and disaster recovery

The realm of security ranges from securing a network against intrusion to end user passwords written on sticky notes. Overall, the exercise of security constraints must achieve a balance between caution and functionality. While the most secure computer in the world is one that is powered off and buried in concrete, it isn't very functional. At the same time, using the exact same administrative password for every server process running at an institution may allow for maximum functionality, it is an open invitation to security breaches.

User passwords, AppleIDs and other fun things

Education is the best way to insure that your users understand the need to maintain reasonably secure passwords. However, it isn't a necessity to have 2d Grade students create 32 character passwords every 30 days. Determine the realistic worth of the information being protected (yes, Joey's science project is critical data to him; but hackers generally aren't concerned) and implement a flexible security plan. Creating a thousand AppleIDs to be managed by the institution may sound like a great idea; but if you use the same password on all of them, are they secure? More importantly, if a user just tries to to enter the password once too often and disables that account, what is the impact on the rest of the end users getting their work done? In this case, you might be better off just having the end users apply their own AppleIDs to the devices.



Disaster recovery

Backup of both the server environment and end user data are critical areas of planning. Backup of your servers can be as simple as taking snapshots of the VMs at regular intervals. The FileWave server is running a database using SQL, and as such, you cannot use normal backup solutions to insure its safety. Use the information on the FileWave Support site to make sure you properly back up the server. End user data is also critical. Everything from the most current ad campaign, to gradebooks, to Joey's science project, are all critical to the user involved. If you happen to have a lot of leftover storage from the days of network home directories, you have a source for online backup storage. Allowing your users to take advantage of their cloud storage - iCloud, Google Docs, DropBox, etc., all help move the backup offsite, and provide a secure way for users to store their files.

Network Security

How much security you use on your network should be conditioned on a realistic threat assessment. For example, the network used by in a business needs more security than that of a K-12 school district. Yet each can be secured by simple precautions of placing secure data storage behind VPN access, as well as physical access control to devices and networks with direct contact with sensitive data.

A rather sobering example is of a very, very large corporation that has an open WiFi network at most of its offices. You could sit in the parking lot and surf the Internet on their network; but you couldn't get to anything remotely important. In order to access secure information, you would need to either VPN into the secure network, or use a badge to access the secure offices with a direct network link to the internal servers. Even then, without the correct and proper credentials, you would be unable to access more than a select amount of data (it's called compartmentalization). Just ask anyone who has worked at Apple how that has worked out for them.

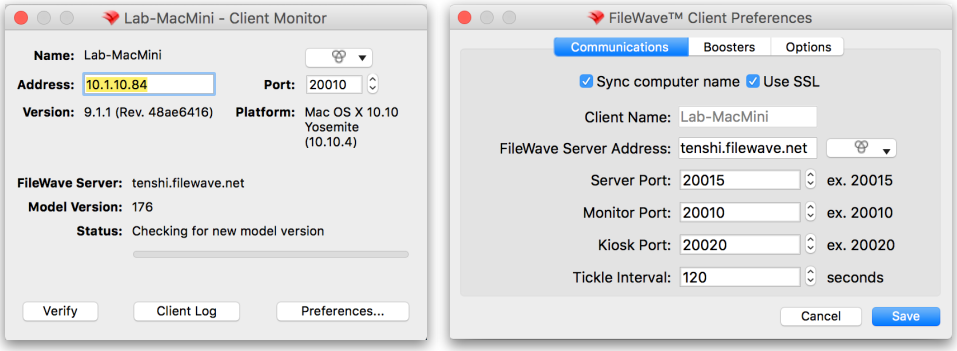
Security and FileWave

FileWave uses SSL, certificates, and secure tokens for much of its primary device and content management. Fileset technology is a patented, proprietary wrapper for content. Instead of sending a standard pkg or msi installer package to the client, we wrap the content inside a Fileset. Because this is a proprietary container, the security of the content is assured. If someone was to capture the bits belonging to a specific Fileset, determining the purpose or content of that Fileset would be very difficult.

FileWave client security

Communications between the FileWave client and either the server or any Boosters is done through SSL.

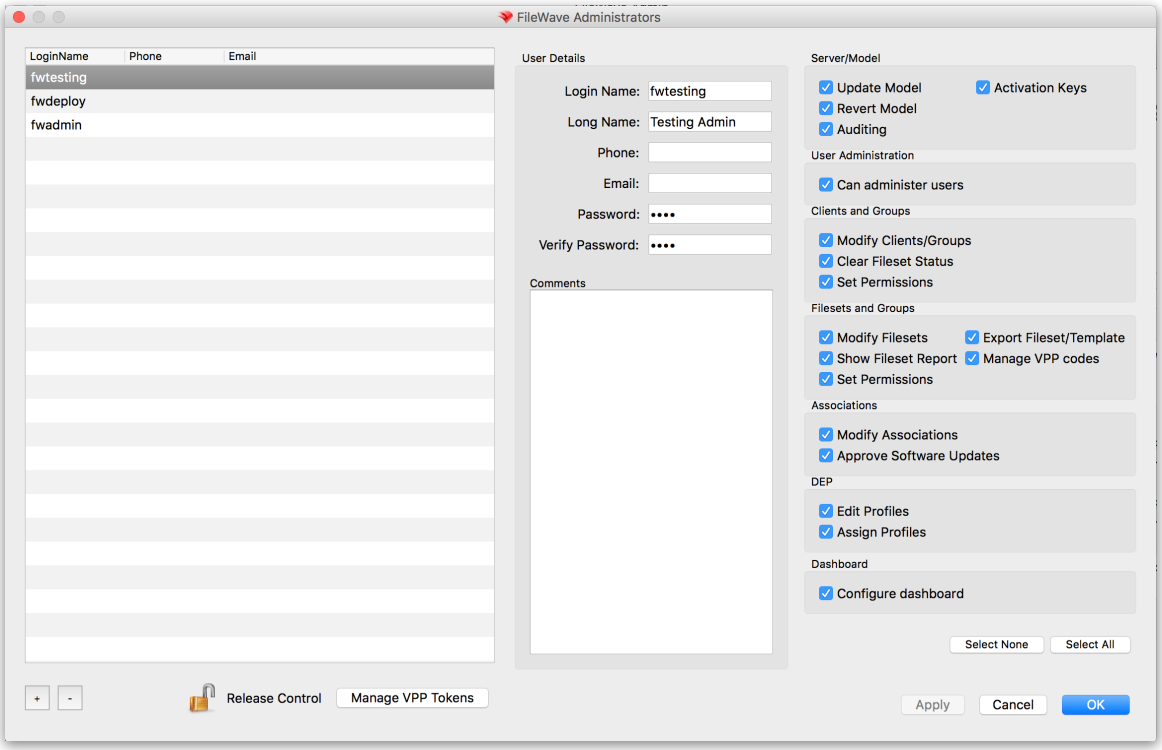
The FileWave client is tracked by device name in **Inventory**. Admin changes to client configurations are either done through a specific Fileset, called a **SuperPrefs** Fileset, or through the client monitor. All Filesets are proprietary containers that are not accessible by non-FileWave sources. The contents of a SuperPrefs Fileset are secure from external packet sniffing, package viewer tools, and brute force access. The Client Monitor settings are protected by a unique password assigned by the FileWave Admin at the time of installation of the FileWave client. This password is not readily available to the device's local administrator.



FileWave clients with the same name (possibly from imaging) report in using different details for Inventory, providing a different fingerprint to the server. This is actually a benefit for some customers because they can "Replace" a downed/broken machine with zero IT involvement from the FileWave Admin as long as the name stays the same. In a higher security environment, the client name would be based off of something less trivial (e.g. serial number or MAC address), and therefore would be more difficult to properly clone. Having a FileWave administrator approve each incoming device rather than enrolling into FileWave automatically is another line of security.

FileWave Server security

The FileWave client talks to the proper FileWave server by the server's DNS or IP added into the FileWave client preferences, using SSL by default. The preferences are accessed through the Client Monitor and can be protected with a password. If someone set up a malicious FileWave server on your secured network, then tried to access your client device and change the server address, they wouldn't have access without the password you have already set. The FileWave server supports multiple sub-administrators. The biggest concern is proper password and account management; but each sub-admin can be limited as to their level of access to clients, Filesets, and services.



2.2. User Deployment models and workflows

Once you have reviewed and updated your infrastructure, you can begin planning your deployment from a user workflow point of view. It is important to remember that all of the infrastructure, tools, techniques, and support capabilities exist to ensure that the institutional goals and missions are successful. A huge part of this success is dependent on user workflows. You are not required to choose any one of these workflows; but understanding them will help you employ them as needed in different areas of the institution in order to meet the overall goals.

If you are deploying Apple devices, you might want to review their deployment guides for specific information and requirements - Apple OS X Deployment Guide and Apple iOS Deployment Guide.

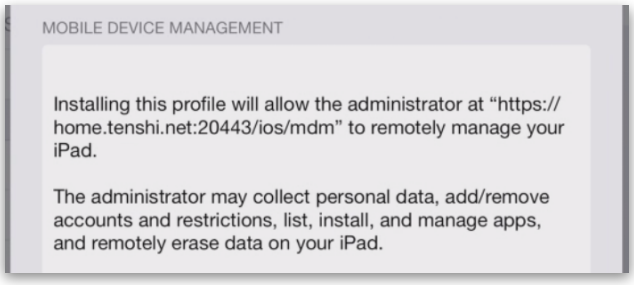
Who is responsible?

There are three primary workflows - user owned (BYOD), institutionally owned 1:1, and institutional shared, plus a plethora of variations between each of them. We will focus on the primary workflows, then discuss a few of the more obvious alterations to the models. The focus in all of these models is on the assignment of responsibility. There are two possible ways to look at the assignment of responsibility in a deployment - who is responsible for the device or who is responsible for the apps and content. The outcome of this assignment has a direct and lasting impact on both the user experience and the ability of the institution to meet its mission goals. The more responsibility placed onto the end user, the less responsibility - and hence, the less work - placed on the IT support staff in terms of direct interaction with the deployed devices. Let's explore the options.

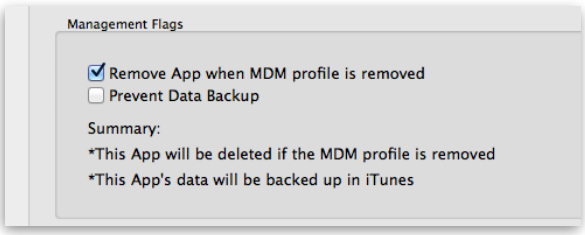
User owned (BYOD) model

The BYOD or Bring Your Own Device model is actually one of the oldest models of device deployment. It hearkens back to the late 1970's when Apple introduced the Apple II and VisiCalc. People would bring their own home computer to work, or to school, to get things done they couldn't do on the institutional mainframe. Nowadays, this model has taken on two differing aspects. One version is the institution allowing the user to bring in their own device - smartphone, tablet, laptop - but adhering to a distinct set of policies and rules. The other version is an institution that cannot afford to provide a 1:1 experience, so it encourages or even requires users to bring in their own devices.

The responsibility for the device is directly on the end user. They purchased the device, and have no intention of allowing anyone else to perform direct management of that device. Systems management in this model is a delicate matter of balancing the rights of the user with the policies of the institution. A well-tested model for this is the "carrot and stick" approach to management.



You ask the user to enroll their device in the FileWave MDM, or to install the FileWave client on their laptop. With that enrollment, you can inventory their device, see what version of OS they are running, see the versions of the installed applications, and be allowed to provide them with content. Using that permission, you can install profiles, such as WiFi and basic restrictions that limit use of cameras, for example. They can be provided with the self-service Kiosk, and you can associate institutionally owned or licensed applications, books, and other content with their device. All of the items you provide constitute the "carrot." The user is responsible for their personally owned device at all times.



The “stick” in this process is that they must keep the device enrolled and the profiles installed. Otherwise, any of the applications you have licensed for them, or institutionally owned ones, are revoked and removed from their device. You may, in some cases, lose the books that you have provided; for example, Apple iBook assignments are permanent. That, however, doesn’t diminish the effect of a user losing use of applications that may be essential to their job or class. This model is quite effective, and also positions IT as the helpful team who can advise the end user on application and OS upgrades, provide critical content, and assist remotely when needed. The other part of the “stick” is also that if the device has confidential information that needs to be protected, an enrolled device can be remotely wiped if necessary.

Institutionally owned 1:1

The concept of an institutionally owned 1:1 deployment follows many of the same ideas as the BYOD with the major difference being that the institution purchases the devices for assignment to end users. This model harkens back to the early 1980’s when IBM introduced the IBM PC with a 3270 or 5250 terminal emulator card installed. It was designed to replace the ‘dumb terminal’ at the user’s desk; but was also very heavily controlled and managed by the newly created IT shop. The deployment model is based on the same rules as the BYOD with a few more restrictions possible. The device is usually asset tagged by the institution, then assigned to an end user. That user is given responsibility for the device and is usually the primary local administrator of the device. The role of IT in this deployment is to provide the policies, profiles, and core applications required for the device based on institutional goals and mission needs.

In a 1:1 deployment, the device itself may have been configured or imaged centrally. It may have institutional applications and content that are site licensed for use by all users, or a specific set of users, depending on the scale of the deployment. A key factor making this a true 1:1 deployment is that the device is assigned to the user to perform basic setup and configuration with the exception of pre-installed items such as the FileWave client or an enrollment profile. Configuration of the device with other local administrator accounts or restrictions on the end user’s ability to manage the device may interfere with the end user’s ability to properly use the device. With iOS devices, you can configure the devices to be supervised, which will provide more management controls; yet still allow the end user to set up the device. Apple’s DEP (device enrollment program) supports the 1:1 model for iOS and OS X devices by allowing you to configure the setup assistant in advance and turn it over to the end user for final set up and configuration.

The “carrot and stick” management model still applies in this model; but in this case, you can make them eat carrots. It can be modified in that the device may have core profiles and applications installed in advance of the device being turned over to the user. This would alleviate the need to have the user enroll or register the device with the FileWave server or MDM service. It still leaves the user with the ability to remove any management profiles, at the expense of losing critical content and having the device show up in the FileWave reports as un-enrolled. Once again, the main

difference between this model and BYOD is that the institution still maintains ownership of the device; but the user is assigned responsibility for normal maintenance (backups, software updates, etc) and application/content installation.

This model works well with designated Fileset groups for content distribution as well as with the self-service Kiosk. Users can be assigned to specific groups for some content, and have the freedom to install optional content at will. The greatest strengths of this model are that the user has maximum flexibility in use of the device, behavior of the device is identical on and off the institution's network, and the day to day operational maintenance - updates, backup, and content installation are the responsibility of the end user, not IT. In a large scale deployment, this is the optimum model.

Institutional Shared deployment model

Due to constraints in equipment, support, and infrastructure, institutions have often been required to meet goals and mission needs with much less capability than desired. The original computer labs were an example of the institutional shared model. Currently, the laptop or tablet carts are the same model in a mobile format. When faced with reduced resources, IT must help deploy a heavily managed configuration to provide the best possible use of limited equipment. The BYOD and 1:1 models are focused on user flexibility; the institutional shared model is focused on consistency of the user experience. The devices in use must maintain a common workflow regardless of how many users interact with them.

This model is achieved by imaging or configuring devices to meet common goals and consistent behavior. Devices are configured with institutional local administrator accounts and/or AppleIDs, as needed. Usage management, or client management, is done through locked-in profiles or management settings. Devices are usually bound or linked to network directories and users are seldom allowed to store or maintain unique content on the devices. The use of online - network or internet - storage is common for most user data; for example, Google Docs.

Some common attributes of the devices are that they are imaged or configured in such a way that a device can be re-imaged or restored without any effect on the end user. An example is using Apple Configurator to create iPad configurations that are supervised. The iPad can be erased any time and restored to a common configuration for any user. Institutional AppleIDs are used to place content on the devices, and users do not have any unique content. Another example would be setting up a lab with common images for the desktop/laptop devices. The image would be configured with a local administrator account and institutionally owned applications. Users would log in on the device with either a Guest account (self-deleting at logout) or a network directory account with temporary local storage. The user would keep any important content on an attached removable storage device (e.g. flash drive) or an online storage container. Apple's DEP (device enrollment program) is designed around the idea of auto-enrolling institutionally purchased devices. In the case of iOS, this produces supervised devices that enroll over the air (OTA) without having to physically interact with all the devices using Apple Configurator.

Institutionally shared devices are usually locked into the local network and offsite use is either limited or non-existent. In business, this model is often used for common area access - kiosks, guests, and testing. In education, this model is often used for young students, and for situations where users save their files to external storage.

Note: While it may seem easier to use a deployment model that locks the device down, in many cases, this becomes self-defeating, especially with iOS devices. When a user logs into an iOS device with their own AppleID, they can defeat many of the management options, such as application assignment. Fortunately, updates to the Apple MDM capabilities now allow assignment of apps and content directly to the device instead of the user (AppleID). That doesn't help when the user needs access to all of their content regularly, and you have to erase the device between users. Test your shared deployment in a pilot program before jumping into it full force. You may find that sharing certain devices between users just doesn't fit your functional requirements.

Custom deployment models (Layered)

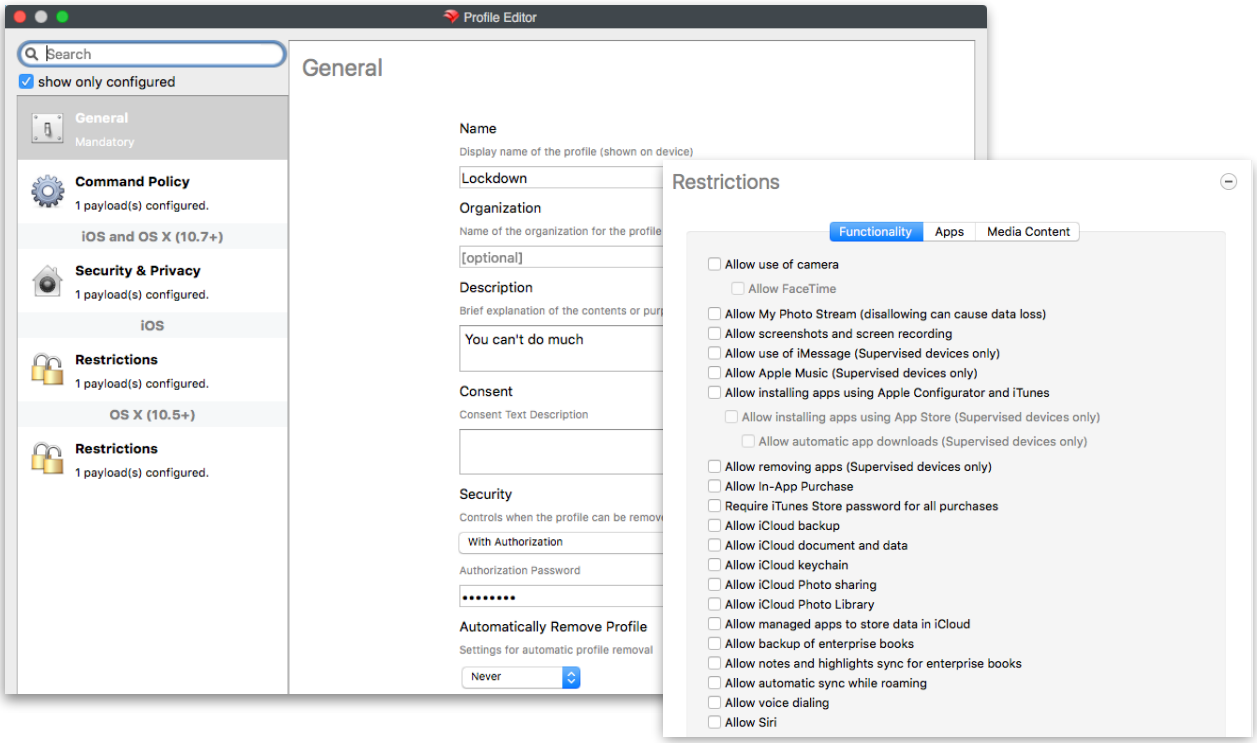
The previous models are at opposite ends of a configuration matrix that stresses freedom of use and flexibility at one end versus ease of management and consistency of behavior at the other end. The design of a model in between the 1:1 model and the institutional ownership model is ofter referred to as the "layered" model. Use of this model will impact the effectiveness of either support or the end user - it is all about compromise.

One possible custom model involves starting with the 1:1 model and adding an institutional local administrator account to the build. This can be done with desktop/laptop devices. The concept is to configure a device with institutionally owned applications and content, then add a local administrator account that the assigned user does not have the password to. The user may still set up the device as their own system; but the central office will be able to perform maintenance on the device as needed without end user permission. One caution about this model is that if the end user is a local administrator also, they can remove your local admin account if they desire, with only a policy telling them they aren't supposed to. From a FileWave deployment point of view, this model can work with the user as

a local admin, or as a non-admin account. With the FileWave client installed, IT can perform maintenance on the device without the need for an additional administrator account. The **direct device assignment** capability in FileWave MDM allows you to manage institutional content on the device, regardless of the end user's role.

This same model on an iOS device is done either by setting up the device in Apple Configurator and supervising it or using Apple's DEP to preload the device with an enrollment profile, then turning it over to the user to run the setup assistant as they would normally. Institutional content can be installed using the **direct device assignment** capability in FileWave MDM; but the user enters their own AppleID to manage the device and add their own content. A key point here is that the end user will not be able to update any of the institutionally installed applications. That will be done through FileWave. This is because the institutional AppleID won't be on the device - the end user's will be. Because the device is supervised, the end user cannot remove the profiles laid down by the institution.

The concepts for all the differing models are based on where the responsibility and workload is placed. The more responsibility the user is given, or assumes, the more work they will do to maintain their device. The more control taken by IT on the device, the more IT's work load in keeping the device running. While this may seem an easy way to approach deployment models, the key is - do you have the resources to personally keep hundreds or thousands of devices running properly so the end users can accomplish their goals?



Impact of AppleIDs on deployments

In institutional deployments, the use of AppleIDs has to meet different criteria than it does for personally owned devices. For example, Apple does not support (or legally allow) the use of a single AppleID for multiple devices in an Education or Enterprise deployment. This means that the IT shop would have to create multiple AppleIDs - one per device. If someone tries, and fails, to enter the correct password for an AppleID on a device too often, it can result in the AppleID being disabled for that device. If you are deploying thousands of devices, that could mean all of your time spent recovering AppleIDs.

Apple purposely designed their devices around a single user with a single AppleID. It's difficult, at best, to fight back against that model. Fortunately, with iOSv9 and OS X v10.11, you can now have devices registered with your FileWave MDM and directly assign applications to the device through VPP. This means that you can allow a user to log into that device with their own AppleID independently of any management settings or applications being managed by you.

Plan carefully for the workflows you are using, and stay aware of how AppleIDs, either internally owned or personally owned, can impact the flow of content and applications to and from your devices.

2.3. The “non-technical” side of planning

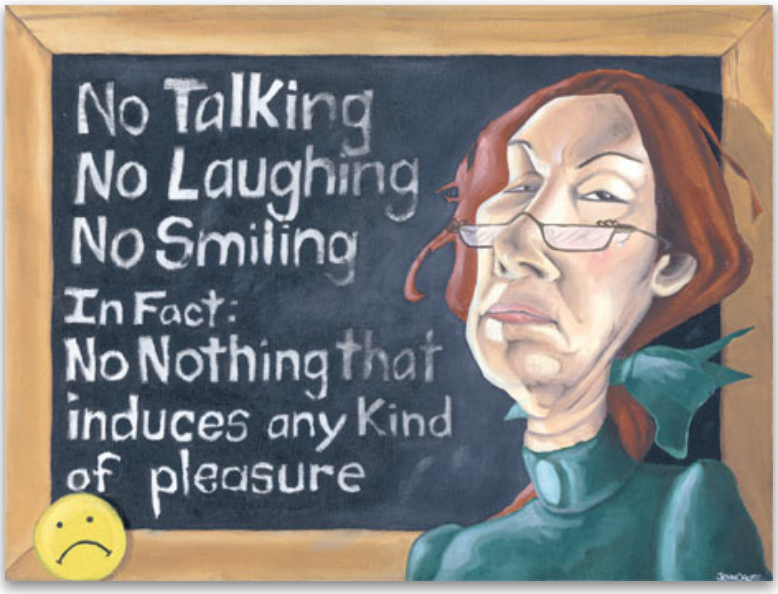
Some of the other aspects of planning a deployment have little to do with bits, bytes, and bandwidth. It’s the non-technical issues that can rear up well after the deployment is under way and wreak havoc with your well-laid plans. It has been said that three things interfere with deployments more than technical issues: policies, politics, and money.

Acceptable Use Policies (AUP)

For example, all institutions have some form of an acceptable use policy to help shape user interaction with institutional networks and devices, as well as overall behavioral rules of use. A key to setting up one of these policies is to both insure that it is workable and that it is enforceable. An example of workability is examining restrictions versus workflows. While the instinct in many IT shops is to shut off many new features introduced on the possibility that “someone might do the wrong thing,” you might try to pilot those restrictions in the IT shop itself; just to see if those settings interfere with the ability of anyone to do their job. When messaging, such as iChat, became available, many IT shops shut it down right away; while many faculty and students were trying to use the capability to keep in touch across campus.

Enforceability is more of a political hot potato than a technical issue; but it can create a very hostile environment. If the AUP states that something will result in severe sanctions for an employee, the workers will greatly resent the IT shop pointing out that they are exempt from those restrictions. History has shown that if a department that makes money for the company complains that they are restricted from being able to accomplish their mission due to IT policy, the fallout doesn’t land on the regular users. In education, if your AUP cannot be enforced in the face of angry parents, then you either wasted your time drafting the policy, or you need to rethink the restrictions.

A best practice is to test any policy at the top down, then revise as needed. And be willing to stand your ground.



Budgeting

Face it, no organization ever has all the money it needs to do what it plans. Experience has shown that there is a distinct path of success with entire process of budgeting for a large scale deployment. One factor is to avoid the “we have just get all the devices we can and get them out there now” attitude. Not that there is anything wrong with purchasing a lot of devices; but ask yourself this question - “Is my infrastructure ready?” If your electrical grid isn’t up to speed to support a lot of new devices, you will have problems. If your network, more significantly, your wireless network, isn’t capable of efficiently handling lots of new devices, focus there sooner than later. Is your training budget in place? All in all, look long term to solve the entire lifecycle of your deployment and things will work out much better.

If you are planning a 1:1 deployment and seem to be running short on funds; before you drop back to deploying carts, look into leasing or even BYOD. Shared devices are significantly less operational than individually assigned devices.

Don’t think so? Just take away all but 2 devices from the IT shop, and spend the next month trying to accomplish anything with everyone sharing one laptop and a single tablet. The long term cost of 1:1 deployments has much less impact than the long term effects of users without their own assigned devices in this day and age.

No matter what your long term technology plan is, the best approach is always - plan, test, execute, review, repeat.

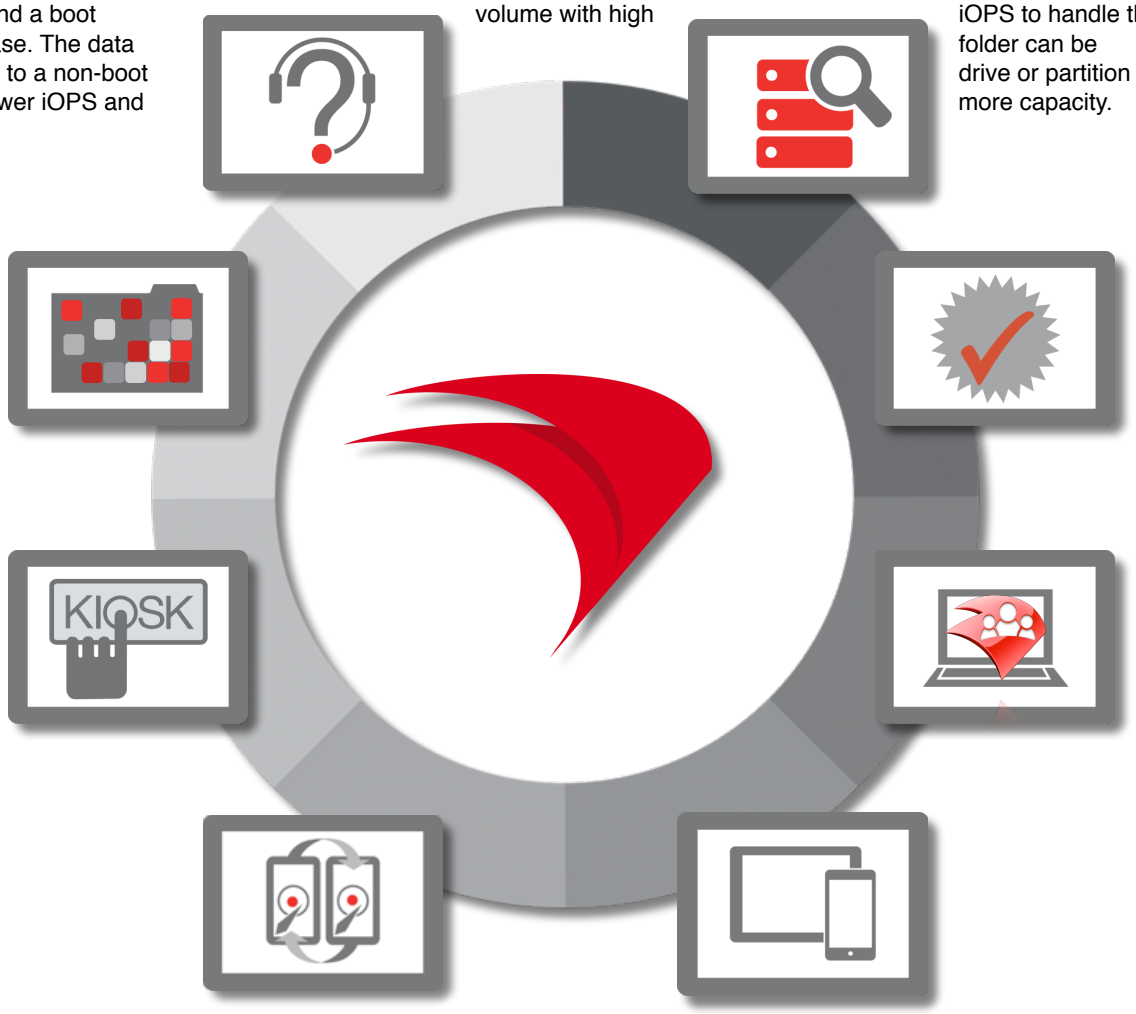
3. Installation and Setup of FileWave servers (FW / IVS / EVS)

The process of setting up FileWave involves installing and configuring the FileWave server, FileWave Admin and FileWave clients, at a minimum. You may also have to install and configure FileWave Boosters. For Imaging, you will need to download and setup the Imaging Appliance. To use Engage, you will need to download the Engage server and setup the Engage services. This section focuses on the installation and configuration of the various servers and configuring the FileWave Admin application. Following sections describe setting up Boosters and Clients, as well as working with the remainder of the FileWave components.

3.1 FileWave Server Installation

Overall requirements

Primary requirements are a 64-bit quad-core CPU, 4+GB of ram, and a boot volume with high iOPS to handle the database. The data folder can be moved to a non-boot drive or partition with lower iOPS and more capacity.



Specs	Macintosh	Windows	Linux
Operating System	OS X v10.9 x86 +	Win Server 2008/2012	CentOS 6.6 x86 64bit
Memory	Min 4GB	Min 4GB	Min 4GB
Hard Drive	100GB+	100GB+	100GB+
Network	Dedicated Interface, fixed IP address, and FQDN (recommended)		

FileWave Server network ports

80	TCP/IP	outgoing for FileWave Software Updates (apple.com & microsoft.com)
443	TCP/IP	outgoing for FileWave License Server (fwks.filewave.com)
20015	TCP/IP	incoming for client-server
20016	TCP/IP	incoming for admin-server
20017	TCP/IP	incoming for client-server secure (SSL)
20443	TCP/IP	incoming for client-server profiles
20445	TCP/IP	incoming for client-server inventory

Install versus Upgrade

As long as you are running FileWave server version 7.x or higher, you can install the new server over top of the existing one. It is recommended that you do a backup of your server first before proceeding (see below). If you were running beta versions of the server, you should move your Data folder to another drive and erase all FileWave parts before install.

Upgrading your FileWave server (Best Practice)

There is a sequence of events that should be followed in order to properly upgrade a FileWave server and the rest of the FileWave architecture. The steps listed below are considered "**best practice**".

Back up your FileWave server

You can run the instructions below to back up only your database, or use the info on the FileWave Support page for full backup information:

http://www.filewave.com/support/kb/article/automated-backup

Backing up current FW database only

Shut the server down using:

```
sudo fwcontrol server stop
```

Then make a Database Backup using:

```
cp -rp /fwxserver/DB /fwxserver/DB<_give it a name or datetime group>
```

Then lock all your clients:

```
sqlite3 /fwxserver/DB/server.sqlite 'update user set status = 1;'
```

Then you can run the Installer or ***rpms***.

After that, the server will be up and running again automatically.

Updating FW Admin and running client test

Update your FileWave administrator to the same version as the server. Connect to it and run model update once you're convinced everything looks as it should. After that, unlock a test client by right-clicking it and observing it for 15-20 Minutes to make sure it doesn't do anything unexpected.

Download Client Upgrade Fileset

During those 15-20 minutes, please download and import the Client Upgrade Fileset of the same version , available on the download page where you got the Installer or ***rpms*** as well as the FW Admin application.

After you're sure the client is behaving, associate the client upgrade Fileset to it, and update the model.

Observe for another 15-20 minutes to ensure that clients talking to the server do not produce any unwanted results.

Once that's done, you can associate the client upgrade Fileset to all your clients and unlock them all.

For more details on best practices while upgrading FileWave, visit :

https://www.filewave.com/index.php/component/maqmahelpdesk/support/kb/article/upgrade-filewave?Itemid=750

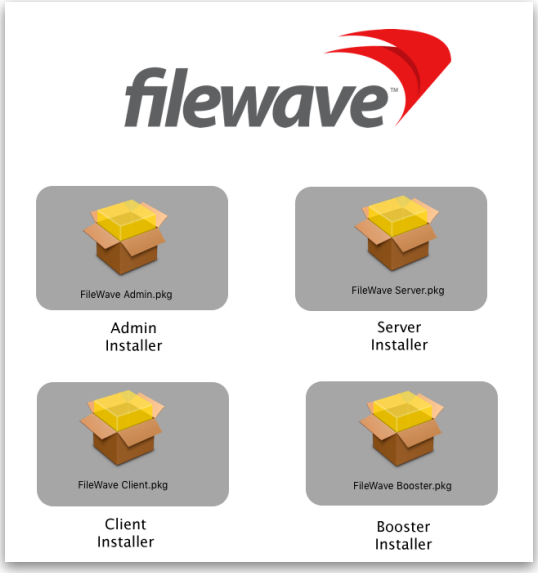
OS X FW server install

System Requirements

Any 64bit Macintosh system running OS X version 10.8 and above will work for FileWave server; however, in order to use all the features of FileWave version 10, you need to start with OS X v10.9 or higher. This does not require an OS X server. Make sure you use a system that is on an optimal network location, has sufficient disk space to handle all of your distribution content, and has at least 4GB of ram (8GB+ recommended). The server will run as a background process; but the system it is running on should be a dedicated device. The server is running an active SQL database, and that DB uses lots of ram. The more you can provide, the better behaved your server will be.

Setup

The FileWave server is installed from the FileWave disk image. Download the latest image from the FileWave Support site. The disk image contains all the components to install the Server, the Admin application, the FileWave Client for OS X, and the FileWave Booster.



Location of key files

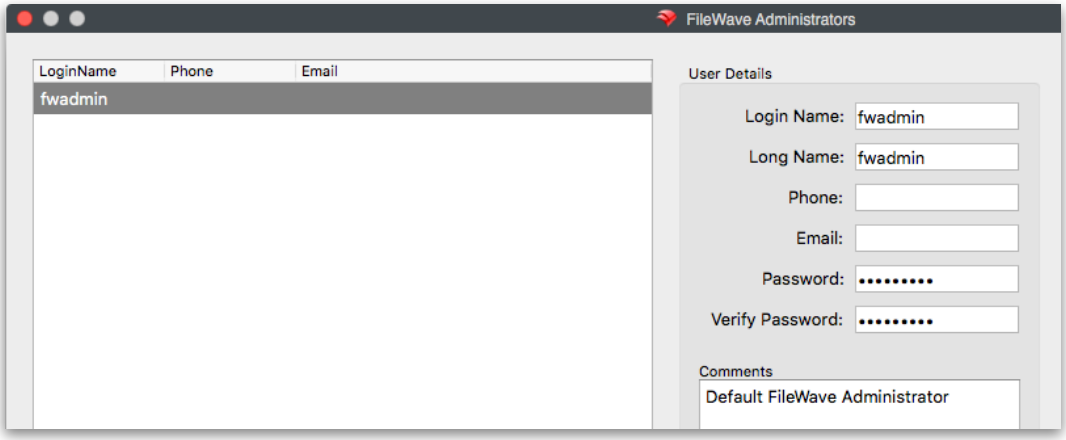
The server process is located in **/usr/local/sbin/fwxserver**. All content for the server is located in /fwxserver on the root of the main hard drive.

Backup procedures

See the section above on Upgrading.

Security - change the primary password

Once you have the FileWave Server up and running, you should change the password from the default (“filewave”) to something a little more secure. The default master administrator account is **fwadmin**. You change the administrator’s password by selecting the **Manage Administrators…** command from the **Assistants** menu.



Windows FW server install

System Requirements

FileWave server requires Windows Server 2008/2012 with at least 4GB of ram and 100GB of hard drive space.

Setup

Download the latest **.msi** from the FileWave support site. **Note: You should use a local administrator account to run the server installer instead of a domain administrator account.**

Location of key files

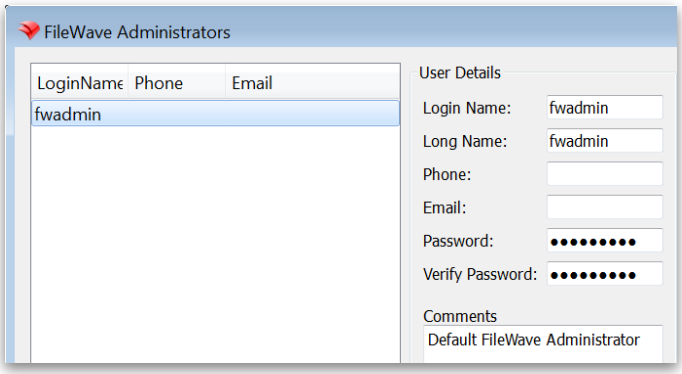
The server process is running in **C:\Program Files(x86)\FileWave\fwxserver.** Important data is located in C:\ProgramData\FileWave\FWServer.

Backup procedures

See the section above on Upgrading.

Security - change the primary password

Once you have the FileWave Server up and running, you should change the password from the default (“filewave”) to something a little more secure. The default master administrator account is **fwadmin**. You change the administrator’s password by selecting the **Manage Administrators…** command from the **Assistants** menu.



Linux (CentOS) FW server install

System Requirements

FileWave server has been tested on CentOS 6.6 x86 64bit.

Backup procedures

See the section above on Upgrading.

Setup

Download the latest FileWave binaries for Linux on the following Website:

http://www.filewave.com/index.php/support/manuals-downloads/software-downloads/category/server

To download the newest binaries, click on the newest version, then scroll down until you see Linux installers.

Copy the Zip file directly to your Linux Server inside the root folder **/root/**

Login with SSH to the Server (on windows use putty, on OS X use Terminal) make sure you login as *root*

Unzip the file with the following commands: (use two dashes in the nogpgcheck option)

```
#(this changes you to the root directory)
cd /root/
unzip uploadedfile-filewave-binarys.zip
yum install --nogpgcheck fwxserver*.rpm
yum install --nogpgcheck fw-mdm-server*.rpm
```

If there are any questions, answer them with *yes* or *accept*.

After everything is installed, you can connect to the server with your FileWave administrator console from either OS X or Windows.

Security - change the primary password

Once you have the FileWave Server up and running, you should change the password from the default ("filewave") to something a little more secure. The default master administrator account is **fwadmin**. You change the administrator's password by selecting the **Manage Administrators…** command from the **Assistants** menu.

Note: If you are running a VM environment, you can download a full Linux container of both server and booster from FileWave Support.

3.2. Imaging Virtual Server installation and setup

Your ability to perform network imaging for OS X and Windows is based on the FileWave imaging server. This virtual machine contains all the components of an OS X NetBoot server and a Windows PXE-boot server. You will upload your image sets to this container, and manage all of this through the **Imaging** pane in FileWave Admin.

System Requirements

The virtual server has been tested on:

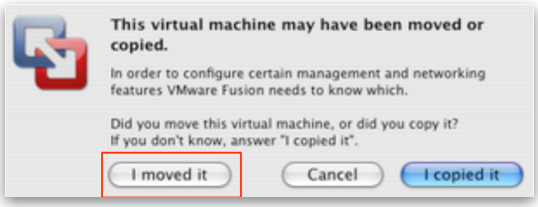
- VMWare VSphere ESX installations, Fusion, and VMWare Player and Workstation
- Virtual Box

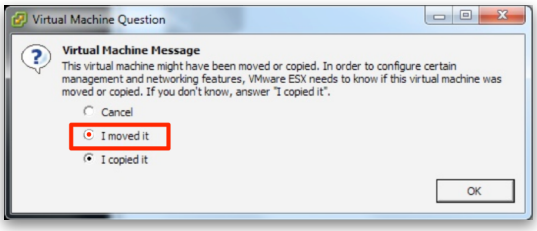
Installation

You will download the imaging VM from the FileWave Support site - http://www.filewave.com/support/software-downloads Follow your VM software instructions to activate the server and complete the configuration instructions below.

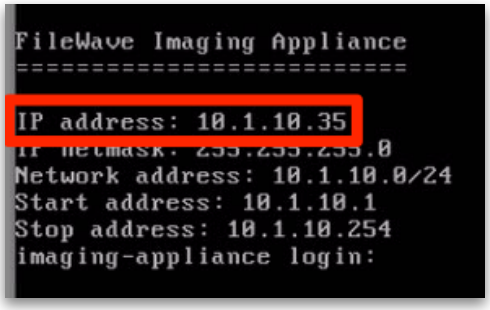
Configuration

When loading the VM you may be asked if you have moved or copied it. Please select "**Moved**".





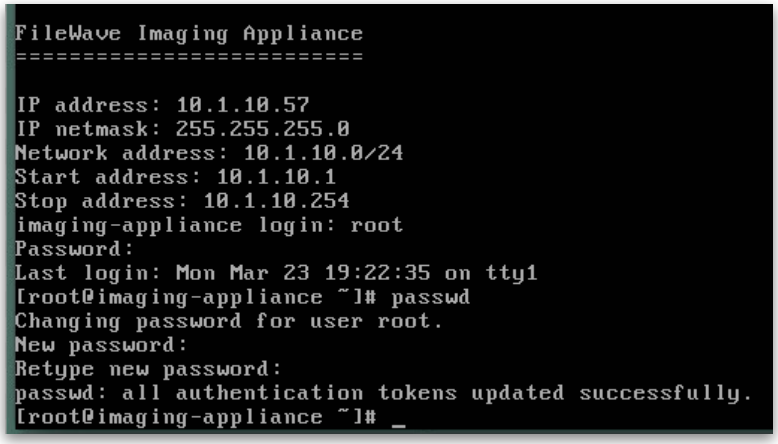
The FileWave Imaging Virtual Server is running on CentOS 6.6 and will use DHCP to automatically configure itself for your network. Please make note of the assigned IP address at the login window:



The default TCP management port for FileWave Imaging access is **20444**. This is not the same as the ports for PXE-Boot and NetBoot. Details on that are covered in the **Imaging** section of this guide. All other imaging configuration will be done from the Imaging pane in the main FileWave Admin window.

Security - change the primary password

Once you have the IVS up and running, you should change the password from the default ("filewave") to something a little more secure. This is easily done using the **passwd** command. At the login prompt, enter the primary account name ***root*** and the default password ***filewave*** to get logged in. Type the command **passwd** which will then prompt you for a new password. Enter a password that you prefer, then confirm it by entering it again. (Make sure you save the new password somewhere secure for retrieval.)



Networking - assign a fixed IP address

The IVS should be using a fixed IP address. There are two methods for setting this up. The first would be to configure your DHCP server to use a static address for the MAC address of your IVS. Getting that information would depend on the VM engine you are running, and your network administrator.

The second method is to use the new command line calls built into the IVS for versions 3.0.2 and above. The process is quite simple:

- Log into your IVS (default acct - **root** and password - **filewave** - which you just changed, of course)
- Type the following command:

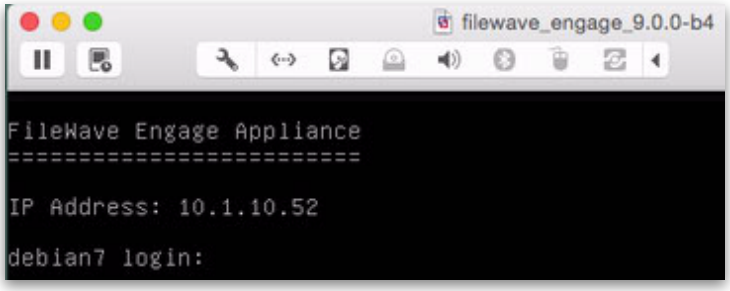
  `sudo imaging-control networksetup static`

  This will send you through a series of requests to enter a new IP address, subnet mask, router address, and DNS server address.

Once you completed the sequence, your IVS will reset to the new values, and you can type "**exit**" to leave the command line. More command line functionality for the IVS is covered in the Appendix.

3.3. Engage Virtual Server setup

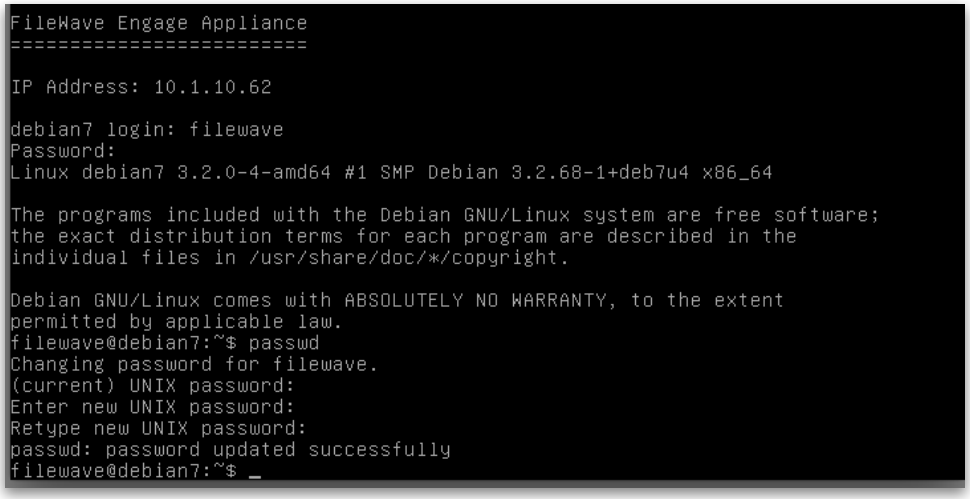
The Engage server VM is downloaded from the FileWave support site in the same location as the rest of your FileWave components. The VM is compatible with VirtualBox or VMware.



Once launched, the Engage VM will boot and display an IP address - that address will be gathered from the DHCP server on the host device's subnet. For the VM software, you should have the network setting to "bridged" and not "NAT." Login for the VM is "**filewave** / **filewave**" (account / password) by default. You should change the password and assign a static IP address as soon as possible. Note the IP address for use in the FileWave Admin Engage preferences.

Security - change the primary password

Once you have the Engage server up and running, you should change the password from the default ("filewave") to something a little more secure. This is easily done using the **passwd** command. At the login prompt, enter the primary account name ***root*** and the default password ***filewave*** to get logged in. Type the command **passwd** which will then prompt you for a new password. Enter a password that you prefer, then confirm it by entering it again. (Make sure you save or record the new password somewhere secure for retrieval.)



Networking - assign a fixed IP address for your Engage server

The process for setting a static IP address on the Engage server involves editing a text file inside the server using command line. The example shown here is using ***nano***, a command line editor. If you are not familiar with ***nano***, then you should check out this site first - http://staffwww.fullcoll.edu/sedwards/Nano/IntroToNano.html.

Log on to your Engage server (default acct / pwd - filewave / filewave)

1) Make a backup of the network configuration file:

```
sudo cp /etc/network/interfaces /etc/network/interfaces.bak
```

2) Open the network configuration file so you can edit it: (using **nano** editor in example)

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

It will look like this:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
```

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp
```

3) In the file you need to add the ip address, net mask and gateway and set **eth0** to be static.

```
iface eth0 inet static
address IP_ADDRESS_HERE
netmask NETMASK_HERE
gateway GATEWAY_HERE
```

So your final **interfaces** file after editing will look like this: (The IP addresses used are examples. Make sure you enter values to be used on your network.)

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 10.1.10.10
netmask 255.255.255.0
gateway 10.1.10.1
# These are values for the Engage server
```

4) Configure your DNS:

```
sudo nano /etc/resolv.conf
```

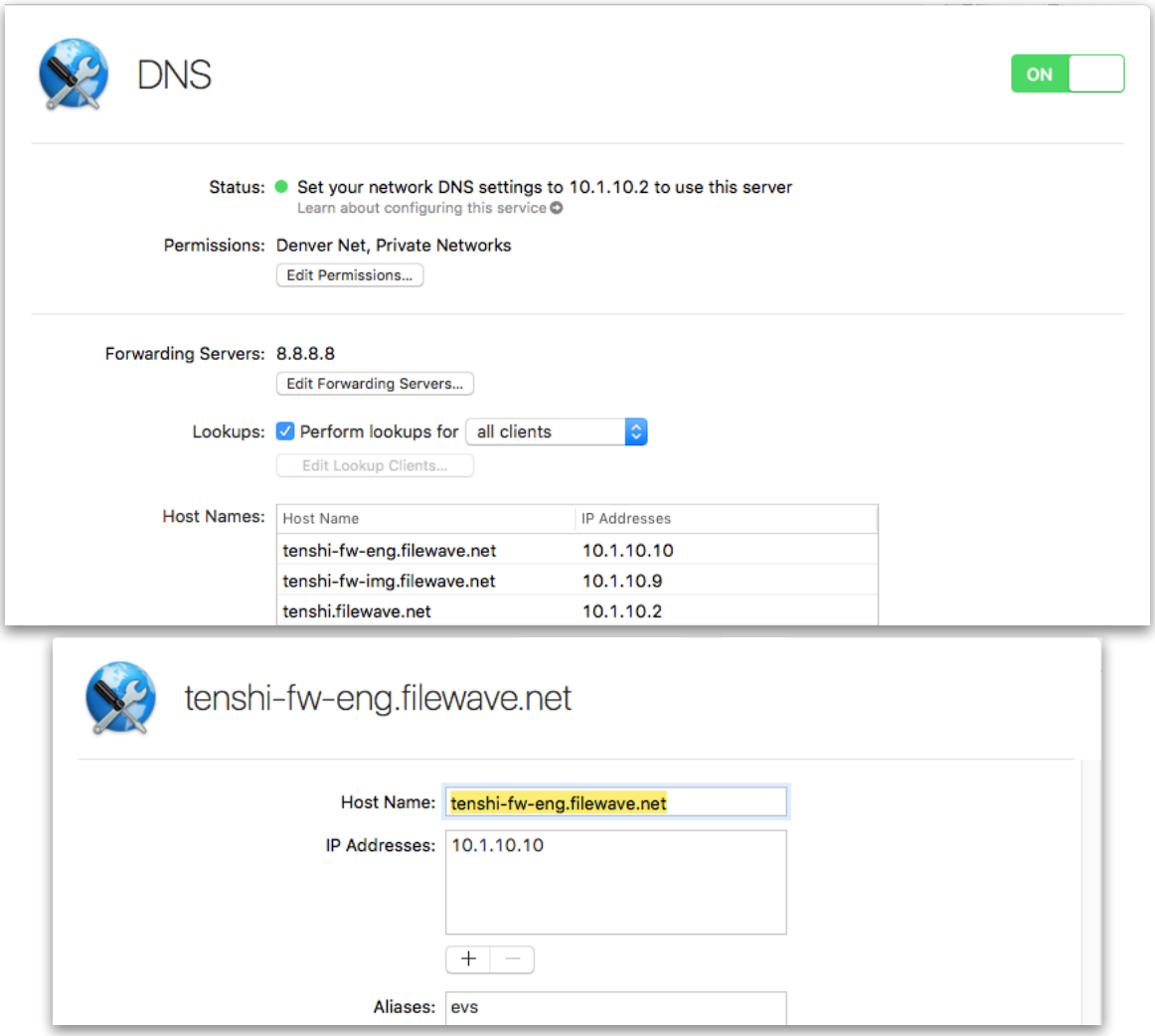
and enter your DNS server(s) like this: (these are example DNS entries, use valid ones for your own network)

```
nameserver 10.1.10.2
nameserver 4.4.4.4
nameserver 8.8.8.8
```

5) Save the file, and reboot the Engage server appliance using your VM controls.

Finishing touch - FQDN and alias for the Engage server (EVS)

A best practice for any server on a network is to assign a Fully Qualified Domain Name (FQDN) for that fixed address. You should have your network support person (it may be you, in which case, there will be no argument…) assign a name to the Engage server's IP address. Here's an example using the very simple DNS configuration from Apple's Server administration application:


DNS
ON
Status: Set your network DNS settings to 10.1.10.2 to use this server
Learn about configuring this service
Permissions: Denver Net, Private Networks
Edit Permissions...
Forwarding Servers: 8.8.8.8
Edit Forwarding Servers...
Lookups: Perform lookups for all clients
Edit Lookup Clients...
Host Names:
Host Name
IP Addresses
tenshi-fw-eng.filewave.net
10.1.10.10
tenshi-fw-img.filewave.net
10.1.10.9
tenshi.filewave.net
10.1.10.2

tenshi-fw-eng.filewave.net
Host Name: tenshi-fw-eng.filewave.net
IP Addresses: 10.1.10.10
Aliases: evs

3.4. MDM service installation

Mobile device management from FileWave supports Apple's Push Notification Service (APNS) and Google's Cloud Messaging service (GCM), and provides services for iOS, OS X and Android. **Installation of the MDM server is a requirement for FileWave to function correctly. You must complete this install, it is not an option.**

Requirements

- *Domain name for your MDM Server*. The devices must be able to connect to the FileWave MDM Server on ports 20443 and 20445 through a registered DNS address. The APN certificate (see below) must match this domain; devices will to use this address in order to enroll.
- *Apple Push Notification Certificate/Key Pair*. In order to send push notifications to devices (for issuing commands, executing profile installations, etc), your MDM Server must have access to an Apple Push Notification certificate. The process for obtaining an APNs is explained in the Appendix.
- *Google Cloud Messaging service Project Number and Server API key*. These items can be created at the Google Developer Console. Details on this are provided in the Appendix.

Note: The process for generating the proper certificates is detailed in the Appendix for Apple's push notification system (APNs) and for Google's cloud messaging system (GCM).

- *FileWave Server running on OS X 10.7 or higher (10.9+ for the new features in iOSv9/OS X v10.11), many different Linux distributions or Windows 2008 R2*. If you are attempting to run a FileWave MDM Server and are missing one of the above items, please contact FileWave support for details.

Installation and setup of MDM on OS X FileWave server

The MDM server is installed as part of the FileWave Server package for OS X, there is no additional software installation required. If you are not using LDAP authentication for enrollment, you must prepare the FileWave server for MDM clients by opening a Terminal session to your FileWave server and creating at least one generic account.

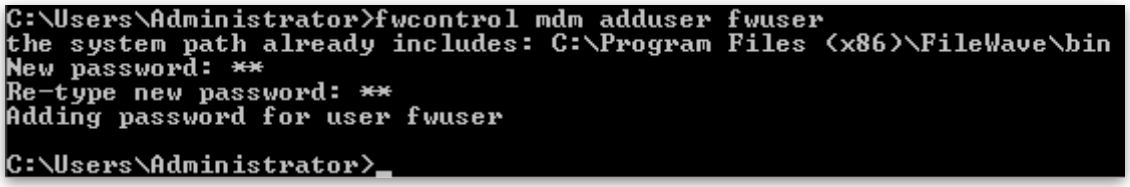
The command is **sudo fwcontrol mdm adduser <mdm account name>**, then you authenticate as the local administrator (your OS X system, not the FileWave administrator), followed by entering a password to be associated with the new MDM account, and verify. You can create multiple MDM enrollment accounts for use by your various FileWave administrators. You will use these accounts when you start enrolling devices. Here is an example of a remote connection to add a new mdm user account called **fwmdm**):

```
johnd-MBP13: johnd$ ssh admin@tenshi.filewave.com
Password:
Last login: Thu Feb 10 13:44:27 20154 from xxx.xxx.xxx.xxx
home:~ admin$ sudo fwcontrol mdm adduser fwmdm
Password: {this is your local admin password to use sudo}
New password: {this is the password for your new fwmdm account}
Re-type new password: {retype the new password for the fwmdm account}
Adding password for user fwmdm
```

Note: You must perform this action if you are not using LDAP for MDM authentication! LDAP authentication conf files are covered in section 3.5.

Installation and setup of MDM on Windows FileWave server

The MDM server is installed from the FileWaveMDM.exe application provided with the FileWave Windows installation download from the FileWave Support site. To prepare the server to support MDM clients, you need to create one or more MDM accounts to be used for device enrollment.



From the server, open a command prompt and type: **fwcontrol mdm adduser <name>** - where <name> is the name of the account, then enter a password for this account and verify.

You can create multiple MDM enrollment accounts for use by your various FileWave administrators. You will make use of these accounts when you start enrolling MDM devices.

Note: You must perform this action if you are not using LDAP for MDM authentication! LDAP authentication conf files are covered in section 3.5.

Installation and setup of MDM on Linux FileWave server

The MDM server is installed through either a script or manually. You can download the components needed from the FileWave Support site.

To install or upgrade the FileWave server or MDM service, use the following command after downloading and un-zipping the installers : (this is for version 10 only)

```
yum install -y --nogpgcheck fw-mdm-server-10*.rpm fwxserver-10*.rpm
```

To install or upgrade the FileWave booster , use the following :

```
yum install -y --nogpgcheck fwbooster-10*.rpm
```

To prepare the server to support MDM clients, you need to create one or more MDM accounts to be used for device enrollment.

From the server, open a Terminal session and type: **fwcontrol mdm adduser <name>** - where <name> is the name of the account, then enter a password for this account and verify.

You can create multiple MDM enrollment accounts for use by your various FileWave administrators. You will make use of these accounts when you start enrolling MDM devices.

Note: You must perform this action if you are not using LDAP for MDM authentication! LDAP authentication conf files are covered in section 3.5.

3.5. Configuring LDAP authentication

You can use pre-designated, fixed account names and passwords to enroll devices in MDM, or you can use your existing LDAP (Active Directory, eDirectory, Open Directory, etc) database as the credentials for enrollment. To set this up, you will edit a configuration file on your FileWave server. This can be done at any time during your server server setup; as long as it is complete before you begin enrolling MDM clients.

This procedure consists of:

1 - Backing up the current config (initially, it will be the default config)

2 - Editing a new config file to properly read the LDAP structure

3 - Restarting the Apache Process so it reads the new config file

Getting the files ready

Open a Terminal Window or use SSH to get into the computer running FileWave Server

Gain root credentials

```
sudo -s
```

Enter your root/login password

Navigate to the FileWave Apache configurations folder:

```
Windows:  C:\Program Files(x86)\FileWave\apache\conf
```

```
OS X / Linux: cd /usr/local/filewave/apache/conf/
```

Backup your current mdm_auth.conf by making a copy

```
cp mdm_auth.conf mdm_auth.conf.bac
```

Make a copy of the LDAP example and rename it

```
cp mdm_auth.conf.example_ldap_auth mdm_auth.conf
```

Making the changes

Open *mdm_auth.conf* up using your preferred text editor

```
nano mdm_auth.conf
```

or

```
vi mdm_auth.conf
```

On a Mac, you can also use the Finder to locate the file, then drag a copy to your Desktop and edit it with a text editor, such as **TextWrangler**. When done, you will delete the copy in the **.../conf/** folder and replace it with your edited copy.

Note: Active Directory (AD) by default requires you bind to the directory to read. Many directory admins create a read-only directory account for this purpose.

Make the appropriate changes (see example below) and then save the .new conf file.

Example of edited mdm_auth.conf conf file

Your edited mdm_auth.conf file should resemble this example:

```
<Location /ios/enroll>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll IOS Device"
       AuthLDAPURL “ldap://tenshi.filewave.net:389/
cn=Users,dc=tenshi,dc=filewave,dc=net?uid”
       Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /ios/device_enrollment_profile>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll IOS Device"
       AuthLDAPURL “ldap://tenshi.filewave.net:389/
cn=Users,dc=tenshi,dc=filewave,dc=net?uid”
       Require valid-user
        ErrorDocument 401 "Enrollment credentials are needed."
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /ios/dep_enrollment_profile>
# This is an example of ldap based user auth
```

```
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll IOS Device"
       AuthLDAPURL “ldap://tenshi.filewave.net:389/
cn=Users,dc=tenshi,dc=filewave,dc=net?uid”
       Require valid-user
        ErrorDocument 401 "Enrollment credentials are needed."
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /android/enroll>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll Android Device"
       AuthLDAPURL “ldap://tenshi.filewave.net:389/
cn=Users,dc=tenshi,dc=filewave,dc=net?uid”
       Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /android/project_number>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Google Cloud Messaging configuration"
       AuthLDAPURL “ldap://tenshi.filewave.net:389/
cn=Users,dc=tenshi,dc=filewave,dc=net?uid”
       Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
```

Restart FileWave Apache process

Once saved, restart the FileWave Apache process/service:

For Windows:

Go to: Services > FileWave, MDM Apache > Select:, Restart

For OS X / Linux:

```
sudo /usr/local/filewave/apache/bin/apachectl graceful
```

Now when a user attempts to enroll their device (by pressing the Enroll Device option on the site). They will be prompted to enter their username and password from the directory server.

3.6. Server Backup and Recovery

Normal, operational backup of the FileWave server will depend on the currently installed version. Please follow the knowledge base article listed below.

Due to the nature of the FileWave databases, using active backup solutions, such as Time Machine or CrashPlan, can corrupt the FW DB.

See the KB article here: http://www.filewave.com/support/kb/article/automated-backup for more information on the best practices for setting up backup routines for your FileWave server.

Your VM's should be shutdown, then cloned as needed. See your specific VM software help/manual for details.

3.7. Installing the FileWave Admin application

Depending on deployment plans, the FileWave Admin application can be installed on two different types of systems; the systems administrator's primary workstation, and a desktop or portable being used for creation of Fileset Magic filesets and/or primary images for the Imaging Appliance.

System Requirements for the FileWave Admin application

The FileWave Admin application runs on both OS X and Windows devices with the following requirements:

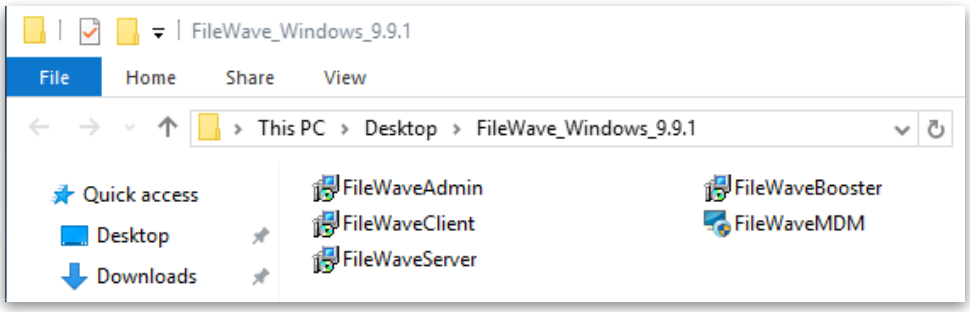
	OS X	*Windows*
Version	*10.7 and higher (Intel only)*	*Win 7, 8, 10*
Memory	*2GB*	*2GB*
*Disk Space**	*100MB*	*100MB*
*HD Space***	*40-60GB*	*40-60GB*

* Required disk space for the Installer

** Disk Space required for FW Admin running on a system to be used for Fileset Magic and/or imaging master

Installing the FW Admin application

Download and open the FileWave .pkg/.msi from the FileWave Software Downloads site http://www.filewave.com/support/software-downloads Select the **Admin Installer** and double-click or open it. You will be required to authenticate as a local administrator on your target machine in order to complete the installation.



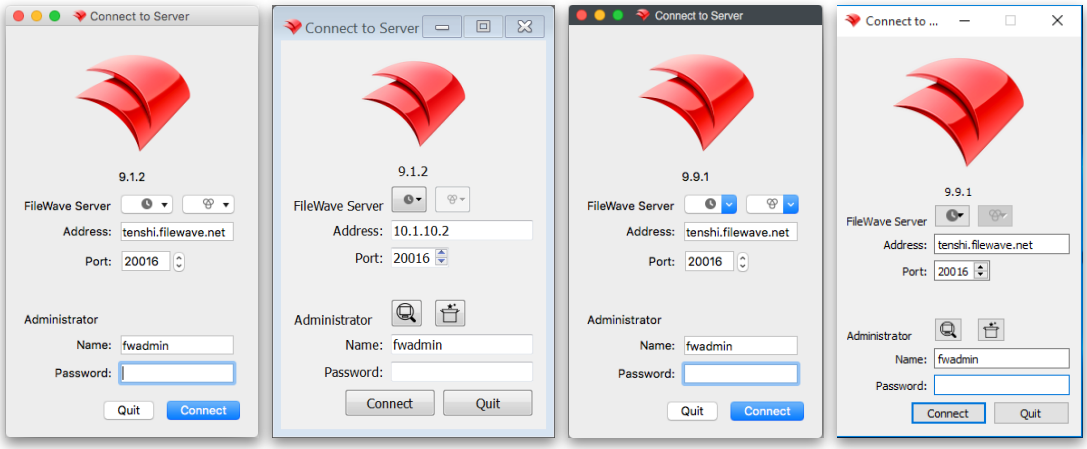
Once the FW Admin application is installed, you will launch it and begin the configuration.

Logging into FileWave server from the FW Admin application

When you launch the FileWave Admin application, you will be presented with a login window. You can search for FileWave Servers in your network with the Bonjour menu (OS X only). Recent server connections are saved in the

Recent Servers Menu. In case your Server operates on another port than the default (20016), specify the port needed. Otherwise please leave the port on the default. Enter the IP address or domain name (FQDN) of the FileWave server you are going to administer.

Note: The default administrator account is "**fwadmin**" and the default password is "**filewave**". (You should change the primary admin password when you first set up the server. See section **3.1/Security** or continue to the **Security section below.**)



Click on **Connect** to log into the server and you will be presented with the default layout.

Note: The Windows version of FileWave Admin has two additional buttons:

 - Client Monitor. Allows you to view the status of any FW client without logging into the FW Admin application.

 - Fileset Magic. Allows you to open Fileset Magic to create custom filesets without logging into FW Admin.

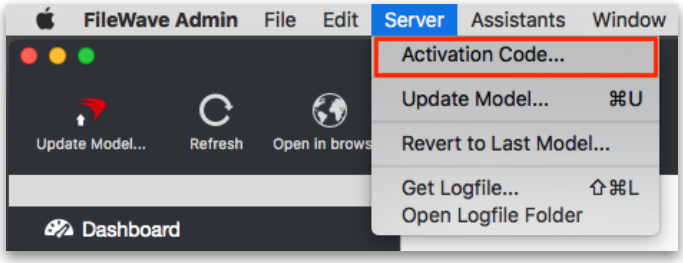
3.8. Configuring FileWave server from FileWave Admin

All of the settings that are used to establish the core configuration of FileWave server are performed within the **Preferences** panes located under the **FileWave Admin** menu item. However, before you can begin configuring your settings, you must activate your FileWave server with the license you purchased. This is a one time task, unless you purchase a larger license later on.

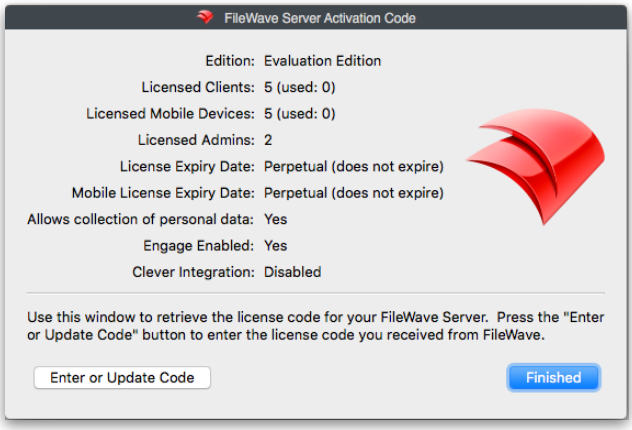
Activating the FileWave server

FileWave server requires an activation code if you are going to manage more than the Evaluation version (1 administrator user, 5 laptop/desktops, 5 mobile). Upon purchase of the FileWave solution, you are provided a custom activation code created specifically for the number of licensed devices you will manage. The activation code will also let you create additional FileWave administrators above and beyond the single "super-administrator" account provided by default (**fwadmin**). If you are going to use Engage, make sure you have included that in your license.

To activate your FileWave server, select **Activation Code…** from the **Server** menu.

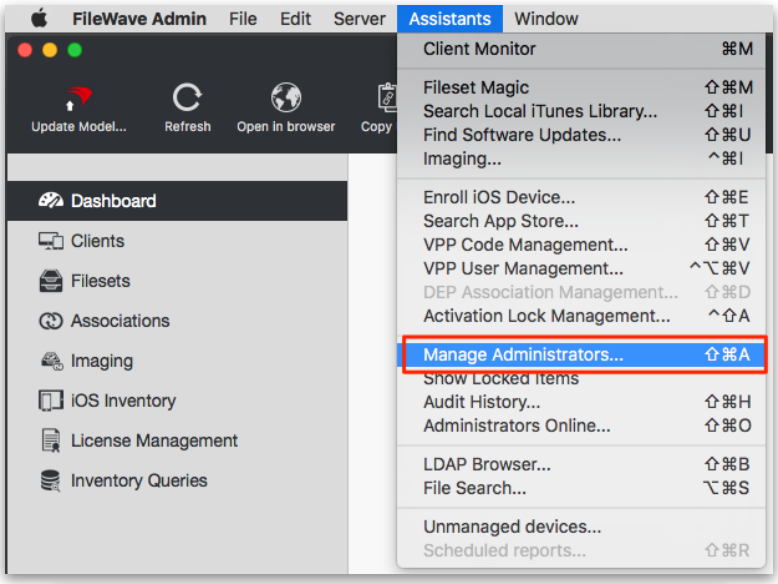


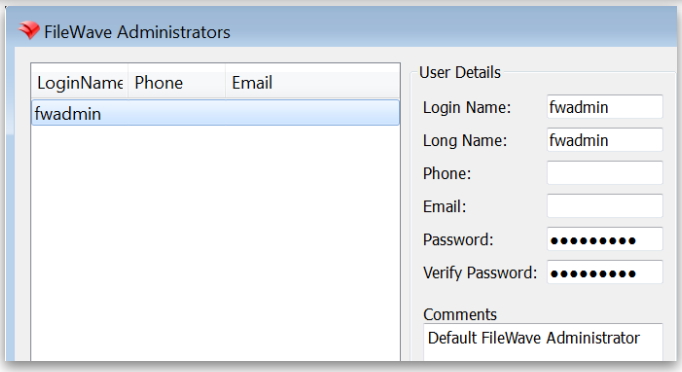
Select the **Enter or Update Code** button, and paste the activation code you received from FileWave with your purchase. Only one code can be stored at a time. If you upgrade your server by adding more client or mobile licenses, then you will overwrite the existing activation code with a new one.



Security - change the primary password

Once you have the FileWave Server up and running, you should change the password from the default ("filewave") to something a little more secure. The default master administrator account is **fwadmin**. You change the administrator's password by selecting the **Manage Administrators…** command from the **Assistants** menu, then select the **fwadmin** account and replace the default password (*filewave*):





Prevent user data collection via license

If your institution or locality requires that you **not** track user data within the FileWave Inventory database, you must request a special “non-tracking” license. When this license is entered, the user data will not be collected by the FileWave client for reporting to the server. If, at some point, you desire to activate user data tracking, you may request a standard license. In order to activate the user tracking capabilities, you will enter the new license and reboot your server. By default, the full capabilities of FileWave inventory are enabled. This includes the ability to track application usage, install dates, launch times, current user and login dates. If an organization feels they don't need this information or that this information would be too sensitive to retain, they should contact support with a request to "Please change my FileWave inventory license to not retain user and app usage information"

The next series of tasks are to get the key FileWave Admin preferences configured.

3.9. Configuring basic FileWave preferences

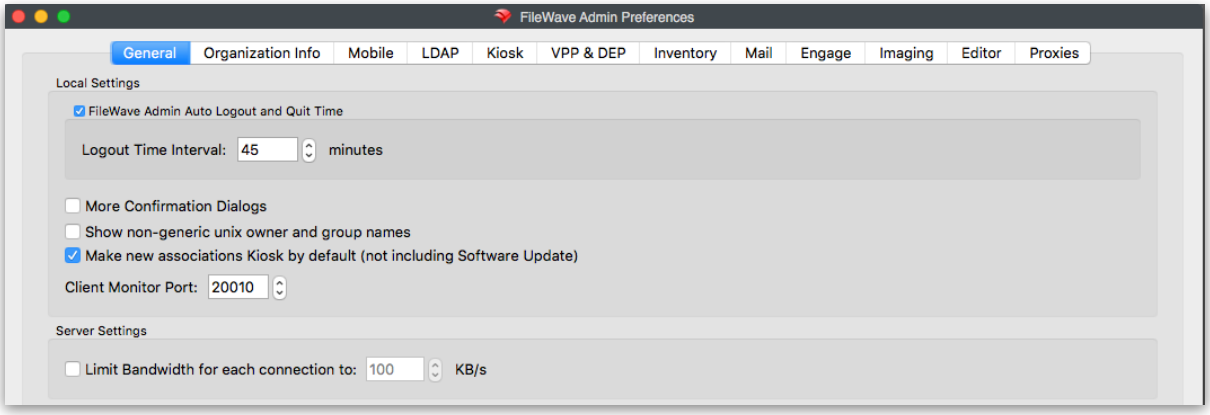
This section covers the basic FileWave preferences of **General, Organization Info, Kiosk, Inventory, Mail, Editor** and **Proxies**. The complex preferences - *Mobile, LDAP, VPP&DEP, Engage* and *Imaging* are covered in their own sections.

General preferences

FileWave General settings break down into four sections:

Local settings

These are settings for each computer the FileWave Admin application is installed on. These are items that effect the interaction of the FW Admin with the FW server.



• *FileWave Admin Auto Logout and Quit Time*. Defines the longest interval the FW Admin application will sit idle before logging out the connected administrator and quitting.

• *More Confirmation Dialogs*. Enables extra confirmation dialog boxes when moving/deleting items in the various panes.

• *Show non-generic unix owner and group names*. If enabled, unix user ids in Fileset contents windows will resolve to the local user account names.

• *Make new associations Kiosk by default (not including Software Update).* Sets all new Fileset/device associations to automatically use the self-service Kiosk as their distribution method. This does not apply to filesets created from the software update pane. **Note: If you are doing a 1:1 as your primary deployment, you may want to use this setting for all non-core applications/content to allow the user to choose what they add to their device.**

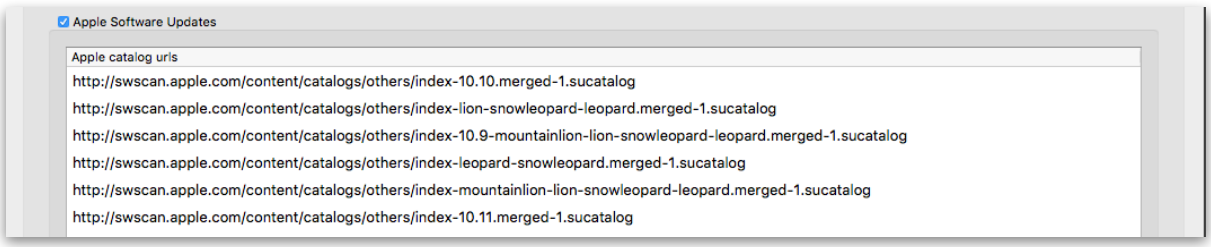
• *Client Member Port:* The default TCP/IP port for a client to contact the FileWave server is **20010**. You can change this value if needed, based upon network infrastructure requirements.

Server settings

The only setting here is your ability to limit the bandwidth for Fileset transfers from the server to boosters or clients. Check with your network support before establishing a setting here.

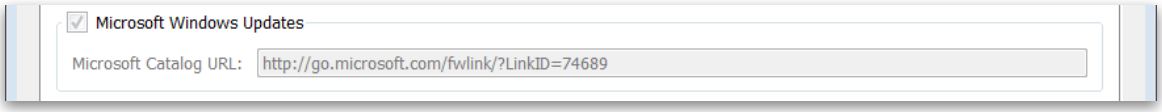
Apple Software Updates

These values define the URLs for the various Apple Software Update Servers’ catalogs based on differing versions of OS X. The values are current as of publication of this document.



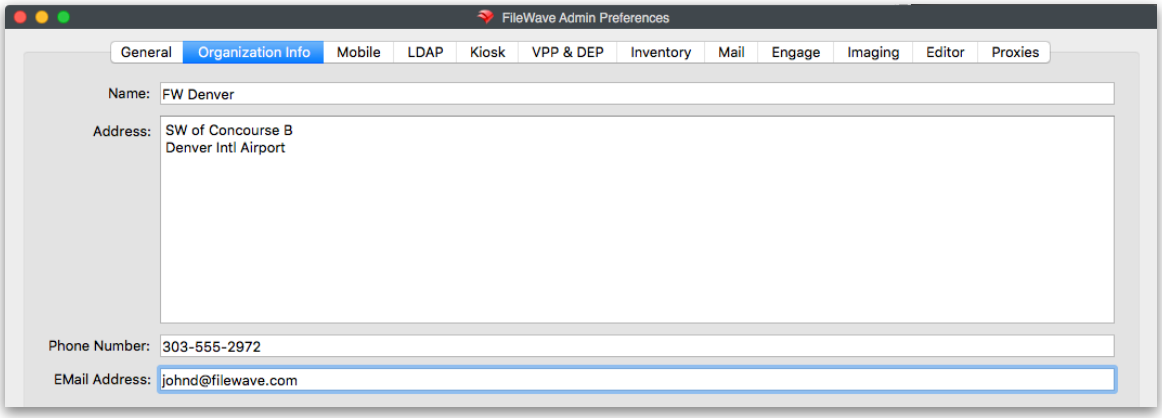
Microsoft Windows Updates

This is the known URL of the Microsoft software update catalog as of the publication of this document.



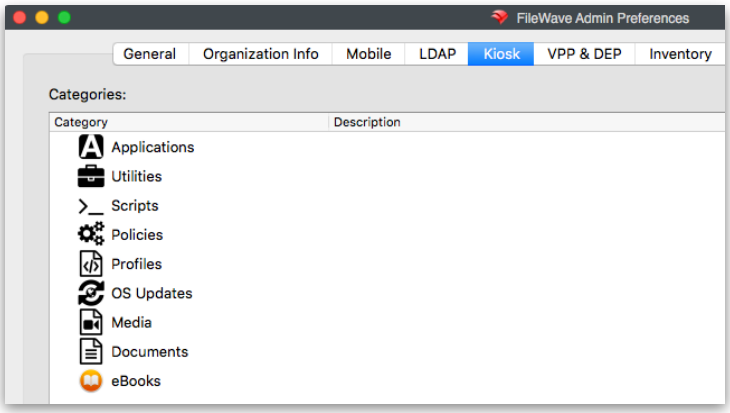
Organizational Info preferences

This setting pane provides the basic information concerning the managing organization. The data provided here will be shown as part of the overall device information.



Kiosk preferences

The self-service Kiosk preferences allow you to create and edit the various categories of Kiosk items offered to end users. You can also change the icon for an existing Kiosk item.



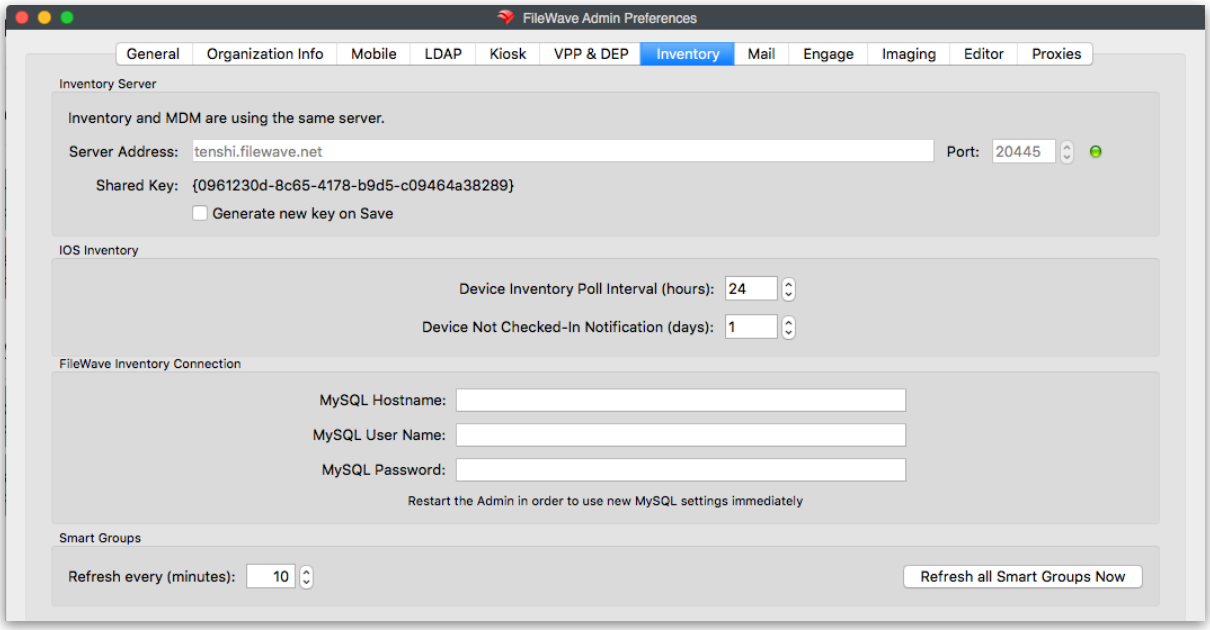
Use the **[+]** or **[-]** buttons to add or delete a Kiosk item. When you have selected an existing Kiosk item, clicking on the **[+]** button allows you to create sub-categories. Double-clicking on the title of a category allows you to change the name of the category. The **Change Icon** button lets you select a new graphic to display as the icon for a category. Icons should be in .png, .tiff, or .jpg format. They should also be no larger than 512x512 pixels in size. This is to keep the file size reasonable.

Tip: You can select an application or other file with an icon you prefer. FileWave 'borrows' that icon. The example above is using the icon from iBooks to display a new Kiosk item for eBooks.

If you want to clear out your category set and return the FileWave defaults, click on the **Revert to Defaults** button and you will return to the eight (8) entries you started with. The Kiosk can be further customized with background images and titling. See the FileWave Support site for more information and directions.

Inventory preferences

The current version of FileWave has the asset management process, Inventory, included in the main FileWave server install. Earlier versions of FileWave supported an Inventory server that could run on a different device. The settings for Inventory on the current version can be left at the defaults; but information on the provided settings is below:



Inventory Server

The FileWave Inventory server and MDM server are now running on the same device. The server address should be a valid FQDN (fully qualified domain name). The default TCP port is 20445. If you change the Shared Key in Inventory, it will break any RESTful API scripts or interfaces you are using, until they are updated to use the new key.

iOS Inventory

- *Device Inventory Poll Interval* - Default is 24hrs. This setting is how often all iOS devices will report their profiles, application, security and device settings.
- *Device Not Checked-In Notification* - When an iOS device exceeds the timeframe set, the device color changes to alert the administrator that that device has not checked in with the MDM server.

FileWave Inventory Connection (deprecated)

If you were using the legacy Inventory server, you would enter the required hostname, username and password to allow the FileWave server to communicate with the Inventory server. These settings are not required for using the built-in Inventory in the current version of FileWave.

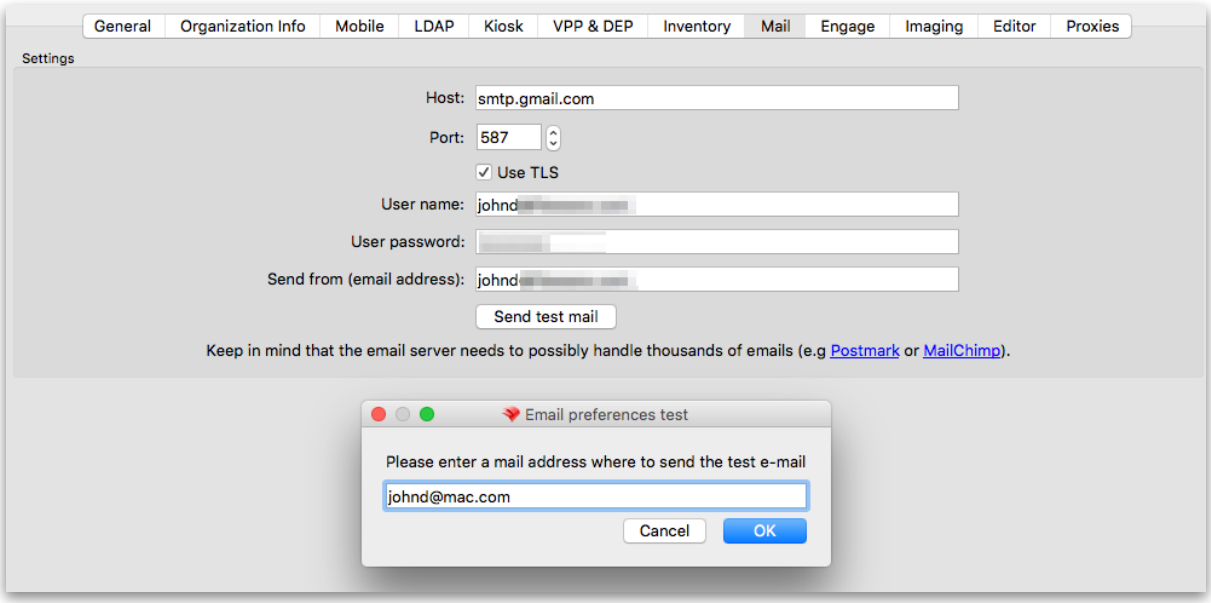
Smart Groups

The button **Refresh all Smart Groups** forces a systemwide refresh of all the data requested by existing Smart Groups. (Smart Groups are discussed in detail in chapter **9 Inventory**.)

Mail preferences

The mail preferences in the FileWave server are used to support both scheduled reports and VPP email invitations. Both of these capabilities are covered in later portions of this manual. Setting up the mail preferences involves you having a common email account that will act as the sender or source of all outgoing mail from the FileWave server. This account will show as the source of emails sent for scheduled reports and VPP MDM invitations.

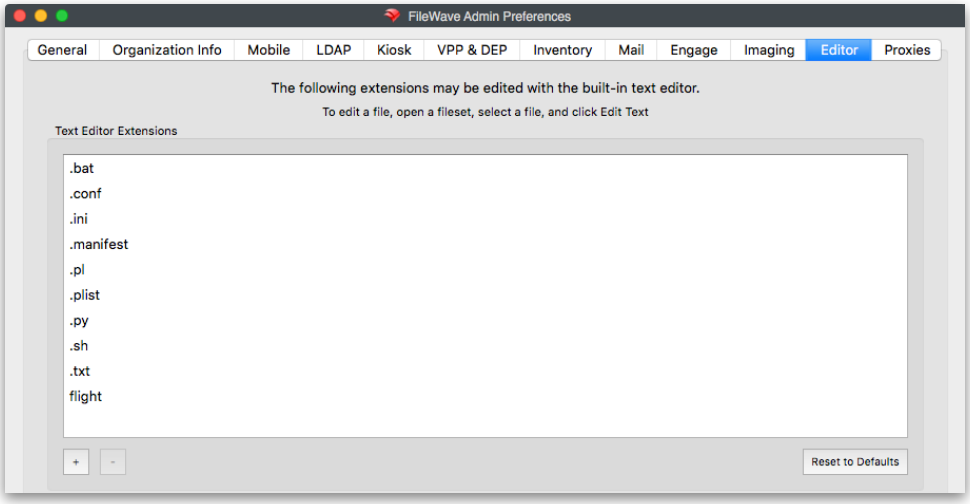
You can select the sending (smtp) server, port number (default is 587 with TLS), and whether to use encrypted email (TLS - transport layer security - recommended). You must enter a valid email account that can send mail from the designated email host. The **Send test mail** button allows you to verify that your settings work. It will have the FileWave server generate a test message that will be sent from the host server, using the account you specify, and will come to the inbox of a designated user account.



Editor preferences

FileWave's Filesets can contain plain text files, such as batch (.bat), configuration (.conf), and property list (.plist). The Editor tab allows you to customize which extensions can be edited within the Fileset Contents Window's text editor. This capability allows you to make simple changes to a file, even a script, inside a Fileset.

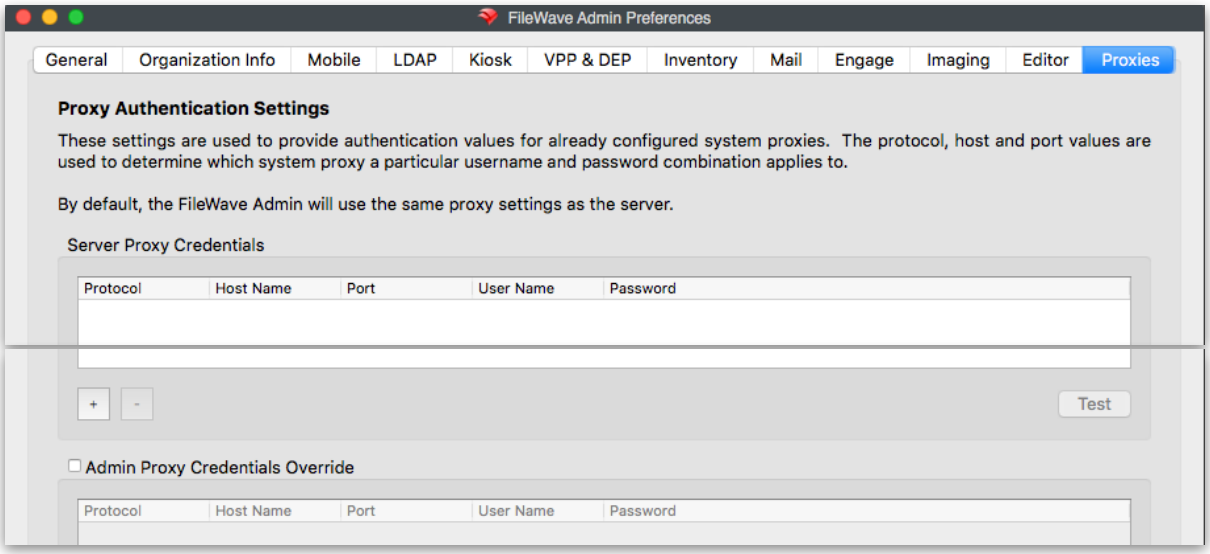
You can add the extension of a specific type of file so that it can be edited within the FileWave editor. File types are usually limited to those that contain UNIX or Windows line endings. You should test any file type that you plan on supporting before making that extension known to all of your FileWave administrators. More information on this capability and its use is in the **Filesets** chapter of this guide.



Proxies preferences

If you are using proxy servers in your environment, this preference pane will allow you to enter the credentials needed to let your FileWave server authenticate with that proxy service. For example, if your users devices must go through a proxy server to access the FileWave server from outside your network, then you will need to add credentials here to allow your FileWave server to respond through that same proxy. You may also create unique *override* credentials for your FileWave Admin to use or bypass the proxy service, as needed.

Working with proxy services may require collaboration with your network services staff.



Server Proxy Credentials

HTTP and SOCKS5 are your two protocol options, followed by host name, port, username and password.

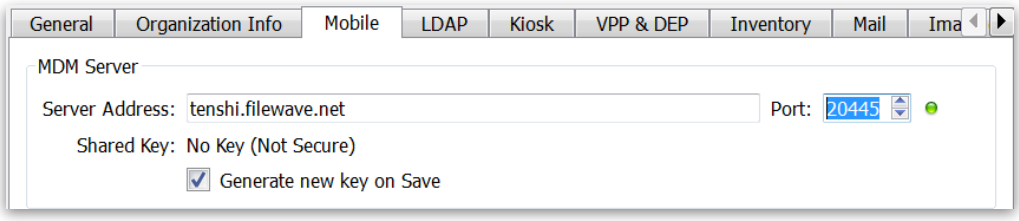
Admin Proxy Credentials Override

HTTP and SOCKS5 are your two protocol options, followed by host name, port, username and password.

A **Test** button has been provided in the bottom right of each section to give feedback for your entered settings.

3.10. Mobile preferences - iOS / Android

The Mobile preferences are designed around **Mobile Device Management** for Apple's iOS/OS X and Google's Android. This section discusses setting up the basic components in FileWave Admin/Preferences. Mobile Device Management is covered in detail in the section on **Modern Device Management**. The certificate workflow for MDM is covered in the Appendix.



Configure MDM Server

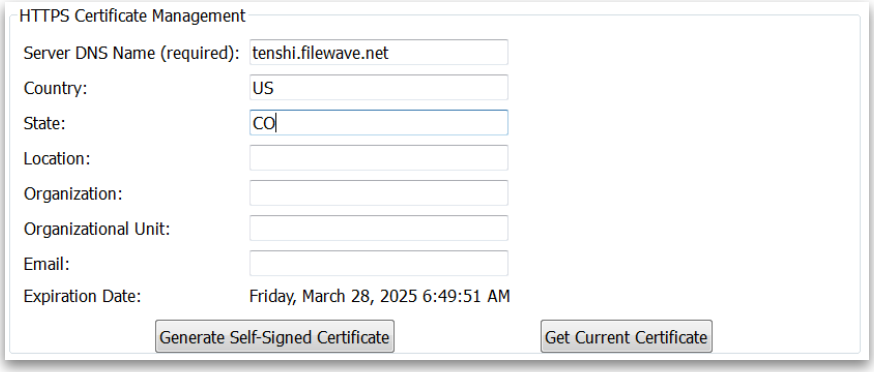
- *MDM Server Address* - Enter the FQDN to your MDM server. If you are running MDM on the same system as your FileWave server, you still need to enter the FQDN for the MDM server in this field.
- *Port* - The default port for FileWave MDM is **20445**. If you are going to change this, check with your network support people first.

- *Shared Key* - This is used to create a secure connection between the MDM Server and the FileWave Server. **Generate a new key on Save** only needs to be done once and is applied when the preferences are closed with the OK button.

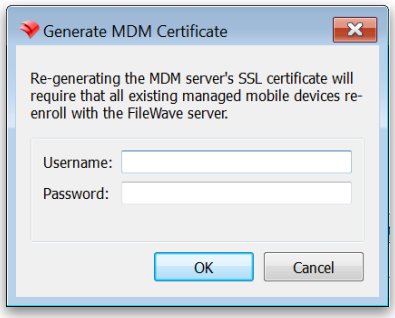
Mobile Certificate Management (APNs)

This section shows the information used by FileWave to create a valid certificate that will be used to authenticate the FileWave MDM server with your clients and with Apple's Push Notification System.

- *Server DNS Name* - The FQDN of your FileWave MDM server. This **must** match the value used in the **MDM Server Address** in the first section of this window pane above.
- *Country / State / Location / Organization / Organizational Unit* - These are all optional fields that can be filled in to expand the information included in the certificate.
- *Email* - enter the AppleID you used to create Apple Push Cert so other administrator's can know what AppleID needs to be used for renewal
- ***Generate Self-Signed Certificate*** - Click here to create a certificate to facilitate communication between the FileWave MDM server and your iOS devices. More certificate management instructions are in the Appendix.
- **Get Current Certificate** - Once you have a valid certificate, you can download a copy to be used with Apple Configurator.



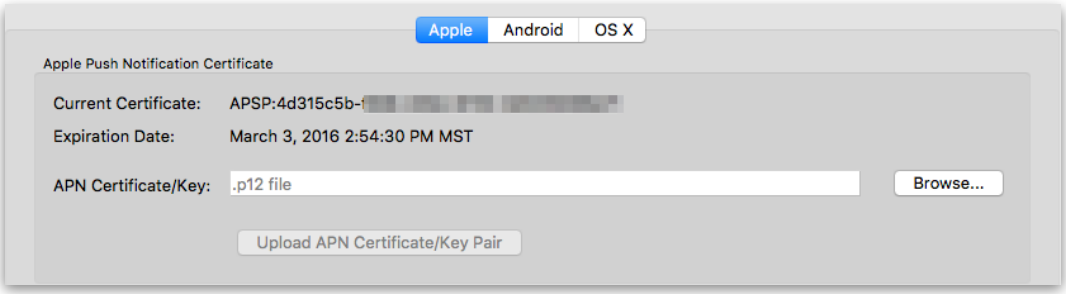
Note: If you need to update your certificate, do NOT select the *Generate Self-Signed Certificate* button. Use the information in the Appendix, or online in FileWave Support to update your certificate. You do not want to see this dialog:



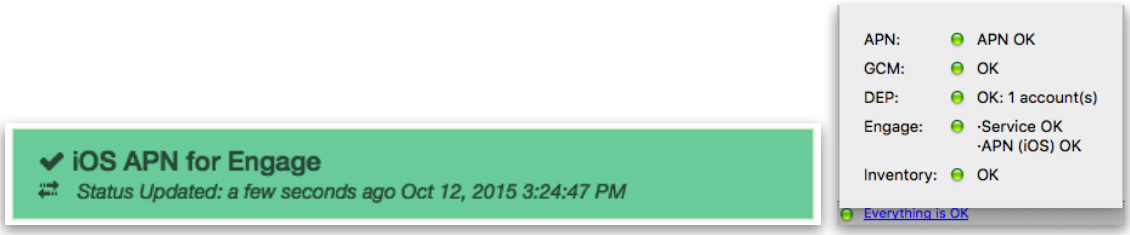
Apple Push Notification Certificate (APN) for iOS

The APN certificate is required to allow the application developers to send notifications to their applications, such as the Weather app getting current storm alerts. In order to allow the applications you deploy to your mobile devices to get these notifications, you request a secure certificate from Apple. The process for getting the certificate is detailed in the Appendix for FileWave administrators running either OS X or Windows.

Once you have gotten your APN Certificate from Apple, you will add it in the settings pane displayed below. When the certificate is uploaded, you will click on the **Upload APN Certificate/Key** Pair button. This will configure your FileWave MDM server to support secure communications between Apple's Push Notification service and your server.

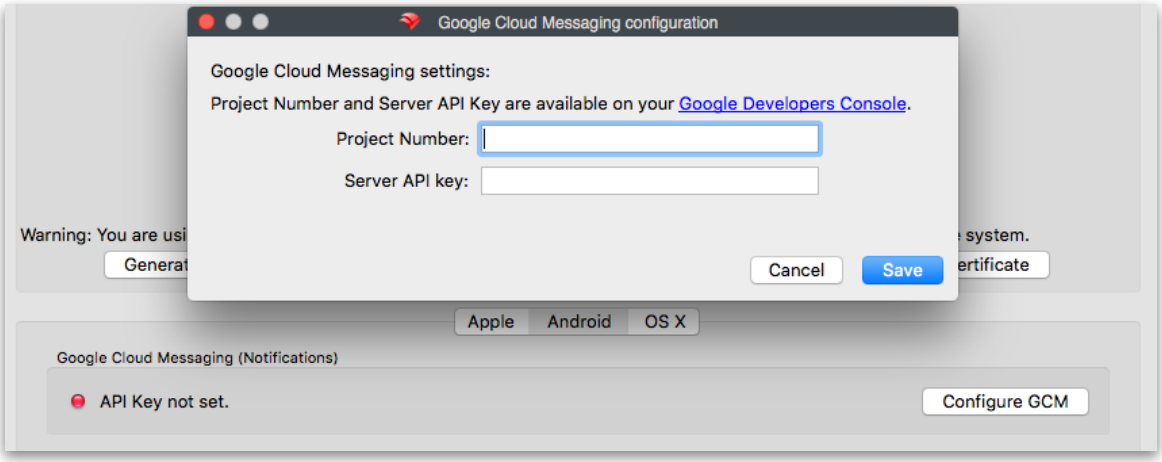


You should get a solid green 'jelly' for iOS MDM in the status section of the main FileWave Admin window as well as a green banner in the Dashboard.



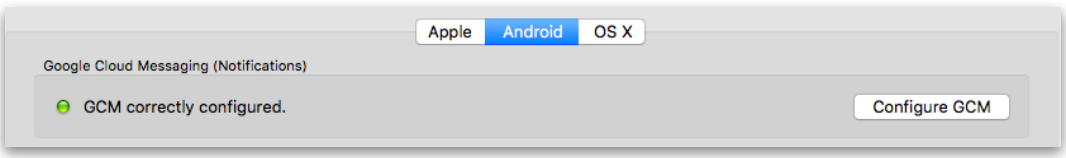
Android MDM Configuration

If you are deploying Android clients, then you will need to configure the Android section of the Mobile preferences. You will need to get a **Project Number** and **API key** from Google. Instructions on how to accomplish that task are in the Appendix. Once you have those two items, go to the FileWave Preferences / Mobile pane and select the **Android** tab.



Select the **Configure GCM** button, authenticate as the FileWave super administrator, then enter the *Project Number* and the *Server API key* you were given.

Click on **Save** and you should immediately see that GCM is correctly configured. If there is a problem, go back to the **Configure GCM** button, click on the link to the *Google Developers Console* to check your information.



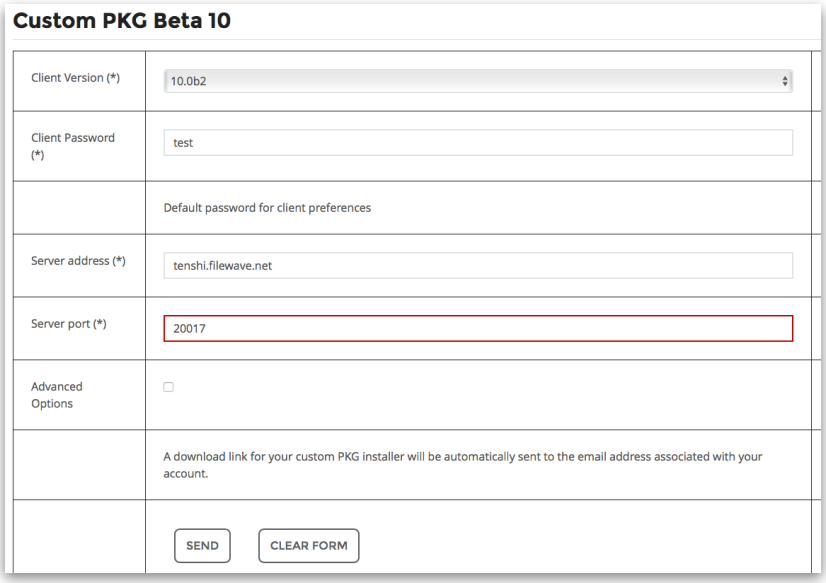
Override FileWave Server configuration

The Android client is a composite of the desktop and iOS client. It must connect to both the FileWave server and the FileWave MDM server. Enrollment is done the "iOS" way through the MDM portal; but the client must also connect to the main FileWave server for additional functionality. In most cases, this is not an issue because the FileWave server and the FileWave MDM server are on the same system. However, it is possible for you to configure the two services to run on different systems with differing external IP addresses.

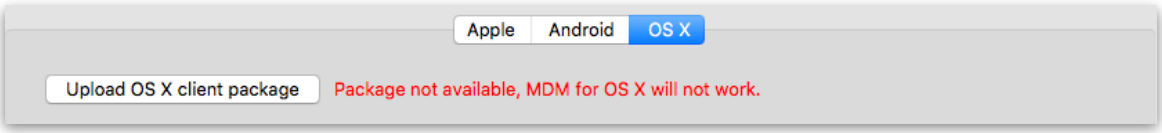
If you are hosting the MDM service on a different system, then you will need to check the **Override FileWave server configuration** checkbox and enter the FQDN / DNS name of your main FileWave server. Do **not** enter anything in this section if you are running your FileWave MDM services on the same system as your primary FileWave server.

OS X MDM configuration

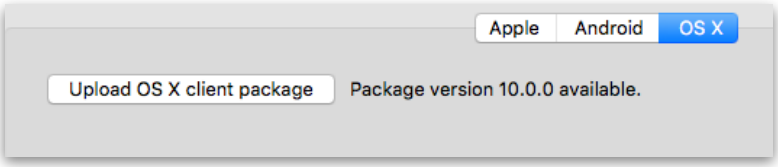
For OS X devices, you will need to request a custom FileWave client installation package (.pkg) and upload it to your FileWave server. This allows FileWave to provide the package for Apple Device Enrollment Program (DEP) devices. When a DEP device is added to your FileWave server, it will automatically receive the client installer package and will be configured as one of your client devices. The first step is to go to the FileWave Support site and request a custom installer: https://www.filewave.com/support/custom-pkg



This request will be answered with an email from FileWave Support containing a link to the requested package. When you have downloaded the package, you will upload it to your FileWave Server using the button in the OS X MDM preferences pane:

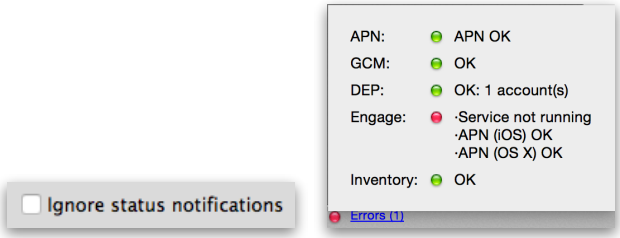


Authenticate as the FileWave Admin superuser (**fwadmin**), then locate the newly downloaded package. **Note: You must unpack/unzip the package before being able to upload it to your server!**



Ignore status notifications

In the lower left corner of the main FileWave Admin window is the status box for your key external services - Apple Push Notification (APN), Google Cloud Messaging (GCM), Apple Device Enrollment Program (DEP), Engage server (if used) and Inventory. In versions 7 and 8 of FileWave, these services run on the same computer/system. (Inventory used to be a separate product from FileWave.) You have the option of installing the MDM services on a different system, or not needing APN, DEP, GCM, or Engage at all - assuming you aren't using any iOS devices, OS X systems with VPP, or Android devices. If any of these services are not running, the status indicators will show that there is a problem. You can disable status notifications and FileWave Admin will report only the services you are using.



3.11. LDAP preferences

FileWave supports connecting your LDAP network directory - Active Directory, Open Directory, or eDirectory - to your FileWave server. This capability provides access to directory information for use in smart groups and parameterized profiles. You can also use LDAP for enrollment authentication.

LDAP preferences versus LDAP authentication

When you first installed your FileWave server, you may have created a generic MDM authentication account to allow your mobile devices to enroll with that specific name and password. Using LDAP to authenticate your devices gives you a more granular, trackable mechanism for device enrollment. Review sections **3.4** and **3.5** on setting up generic MDM authentication and configuring the LDAP configuration file inside your FileWave server. The preferences you will set up here will allow you to have LDAP **Smart Groups** containing your LDAP directory groups for application and content assignment. The preferences here will also allow you to support **parameterized profiles** which are used in certain Profiles to autofill the fields with values from your LDAP directory, such as email addresses.

Creating an LDAP server entry in Preferences

Use the **[+]** button to create a new LDAP server entry and enter the needed connection information as described below:

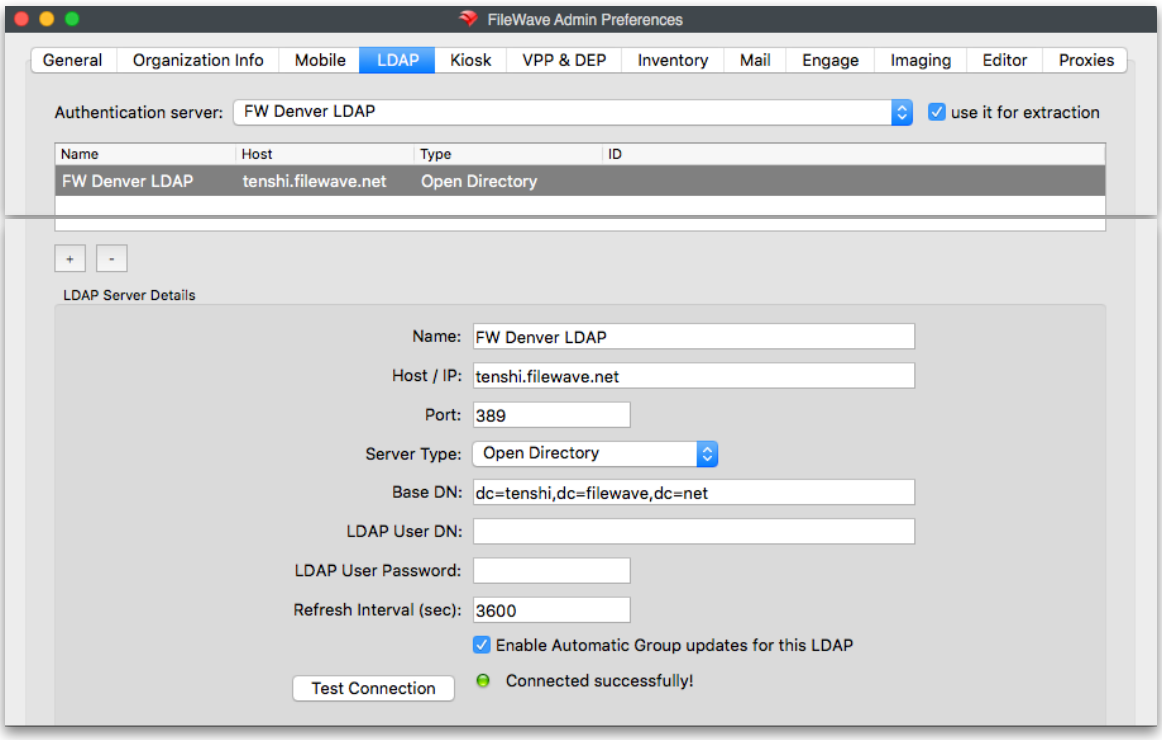
- *Name* - a reference name used by you to differentiate your LDAP servers
- *Host / IP* - enter either a FQDN or IP address for your LDAP server
- *Port* - enter the TCP port required to access your LDAP server (you may need to check with your network support)
- *Server Type* - choose **Active Directory, Open Directory, or eDirectory**
- *Base DN* - enter the primary distinguished names (DN) for your LDAP server using the domain components separated by commas. For example, if the LDAP server is running on the same box as the FileWave server, your base DN may be as simple as "dc=home,dc=local"; but if the LDAP server is running on a different system, the value of the base DN may be involve using a more extended value, such as "dc=tenshi,dc=filewave,dc=net".
- *LDAP User DN* - if you are doing authenticated binds to your LDAP server, you will need to enter a valid user account that has been designated for binding. If you are doing anonymous binding, this entry is left blank.
- *LDAP User Password* - enter a password to complete the authenticated bind; not needed for anonymous binds
- Refresh Interval (sec) - enter a value in seconds for the FileWave server to contact the LDAP server to refresh the available data. If you are just setting up a FileWave server on a network with an established LDAP server, you

should set the interval relatively short (~120 seconds) while you are testing and making changes. Once you go into production mode, you should change the interval to 24hr (86400 seconds).

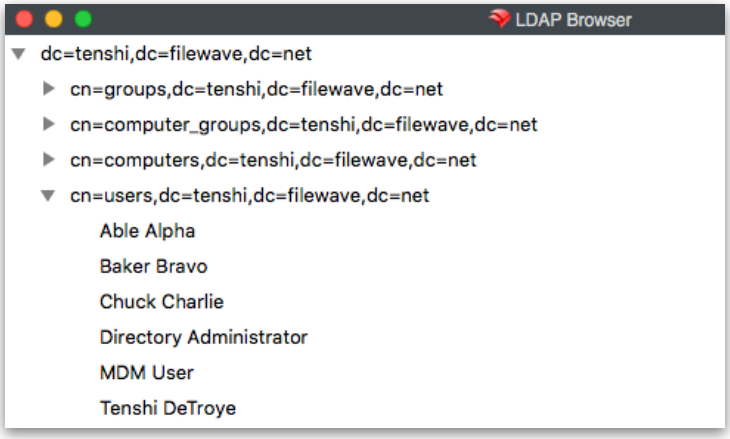
Note: Choosing to enable the automatic group updates creates a visible set of entries in the Clients pane of the FileWave Admin application, and keeps that information up to date; however, for an LDAP environment of over a few hundred records, the load on the LDAP server can get extremely heavy.

The **Test Connection** button pings the server to see if it is online; but does not verify all connection settings. You should always use an LDAP browser tool to verify the link to your server.

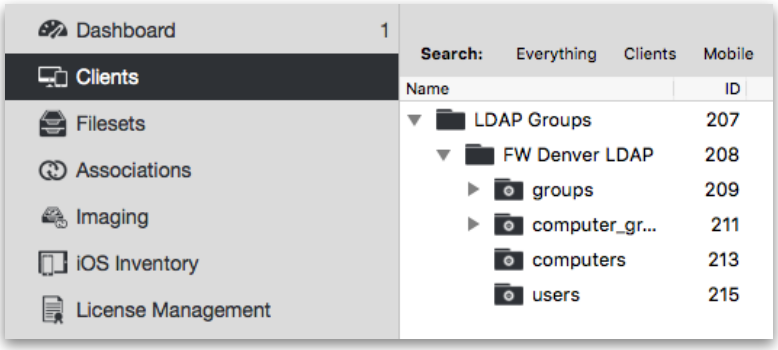
You can create entries for multiple LDAP servers, and an LDAP server can be running on the same device or VM as the FileWave server.



An LDAP server can be chosen as the **Authentication server** which, in this case, means that the directory for that server will be used for profiles that support parameterized settings. Selecting the **use it for extraction** setting adds the directory information to the FileWave database. You can view the LDAP settings in the **Assistants/LDAP Browser** in FileWave Admin.



Choosing the **Enable Automatic Group updates for this LDAP** creates a visible set of entries in the **Clients** pane under an LDAP designator. These entries are smart groups and will be updated by FileWave at the designated refresh interval. For example, if you create a new network directory group on your LDAP server, FileWave will automatically create a smart group containing those records.



The information provided in the Clients pane for LDAP is a one-way view of your directory server. While changes made at the LDAP server are automatically reflected in FileWave; changes made in FileWave Admin do not affect the LDAP directory information.

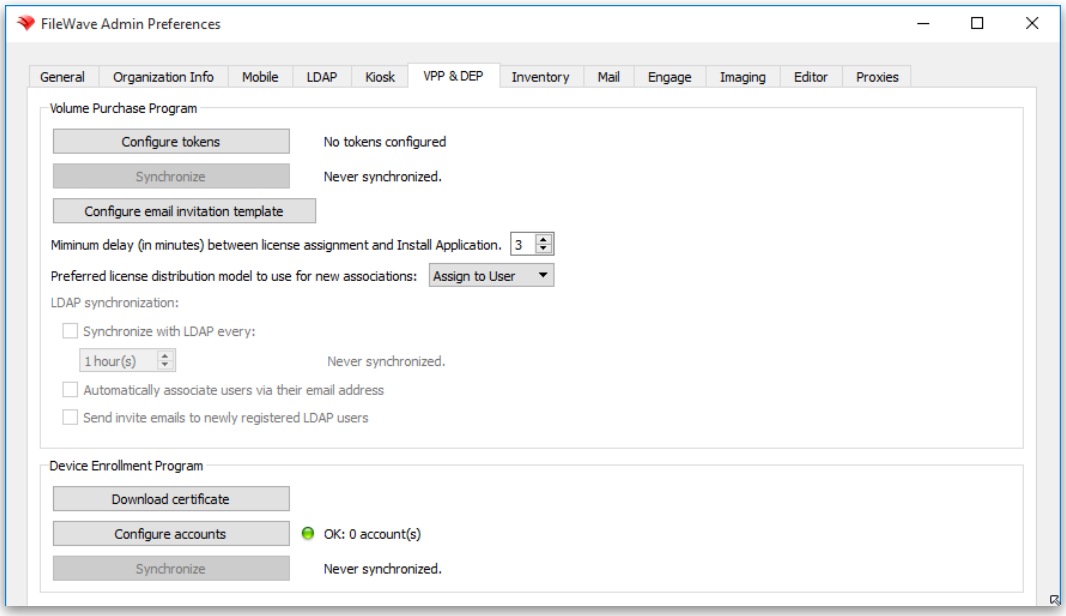
3.12. VPP and DEP preferences

FileWave supports both Apple's Volume Purchase Program (VPP) and Device Enrollment Program (DEP). In order to get these working within FileWave, you will need to configure certain preferences. Chapter **7** of this manual goes into great depth on the configuration and operation of VPP for iOS and OS X devices. Chapter **5** discusses DEP in depth. This section just discusses the settings required in the Preferences.

Note: Instructions for joining and working with the Apple VPP and DEP programs from the Apple side are outlined in detail on this web site - https://help.apple.com/deployment/programs/#/

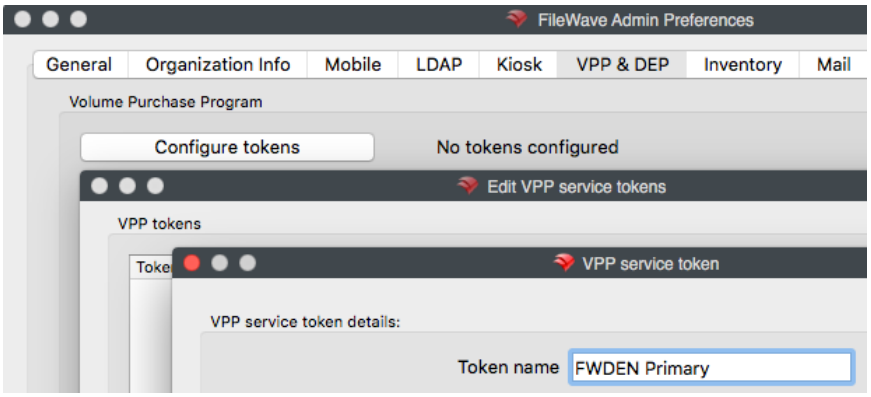
Warning: All of the configuration steps in this section must be done while signed in as fwadmin.

FileWave supports multiple tokens for the VPP service. This allows you to create multiple purchase authorities for your institution's App Store content. Content is automatically synchronized every 24 hours with the Apple VPP service. You may force a full synchronization when you are deploying a large number of App Store items, or any time that a delay may interfere with operational needs by holding down the **Option** key and clicking on the **Synchronize** button.



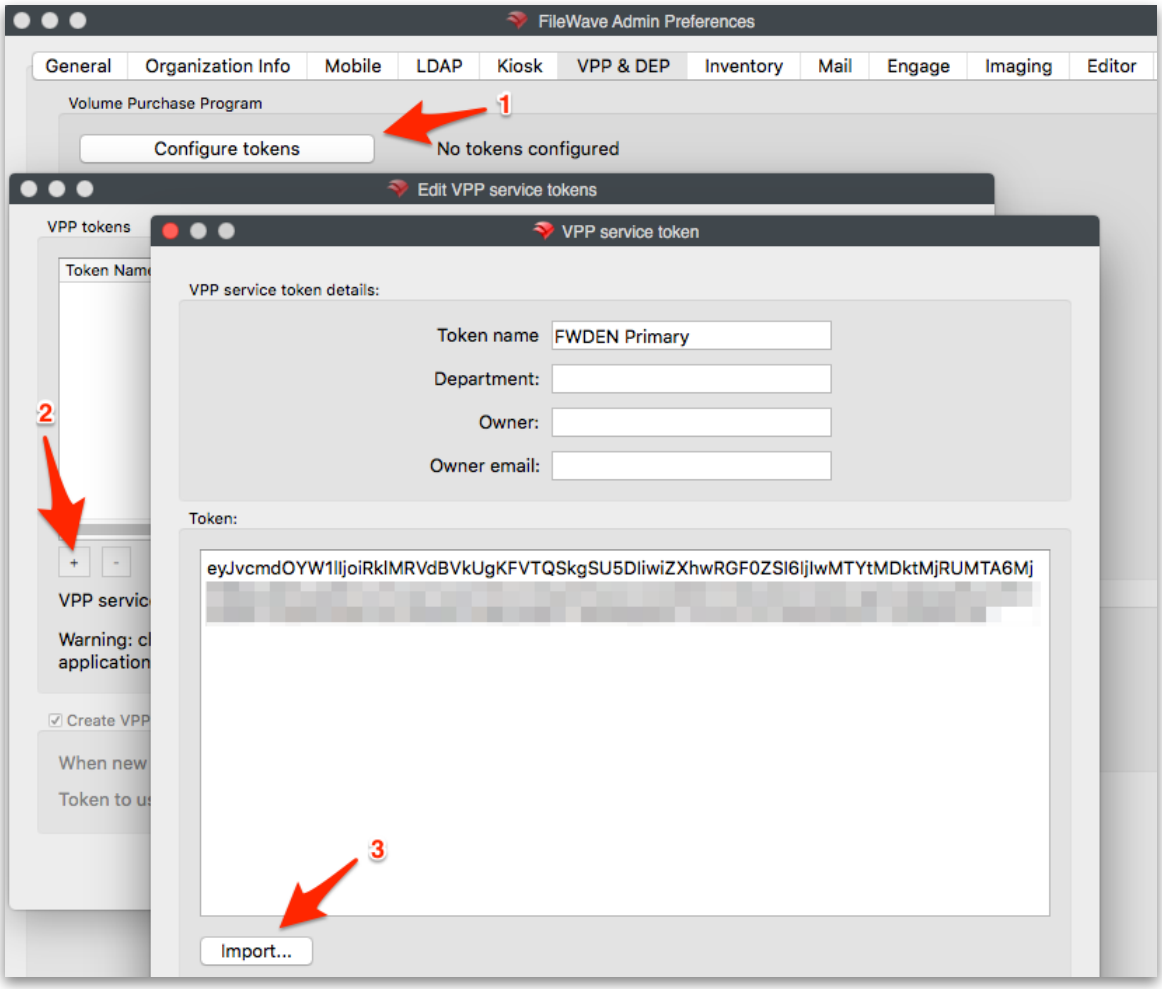
Volume Purchase Program preferences

This pane contains the information for your VPP account with Apple. In order to proceed, you will have to have created a VPP for Education or VPP for Business account with Apple. Information on that process is provided at Apple's website. Once you have a VPP account, you can download your VPP token for inclusion into FileWave. You may add as many tokens as you have purchasing agents.



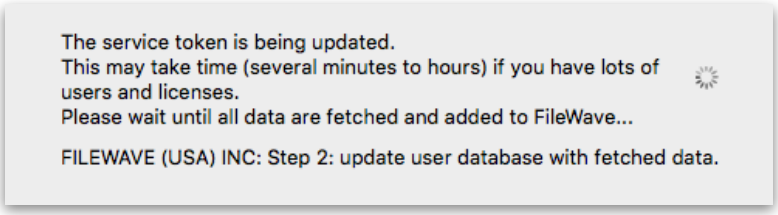
Configure VPP token(s)

Select the **Configure tokens** button (1). You will have to authenticate as the primary FileWave Admin (default is "fwadmin" with "filewave" as the password - hopefully, you've changed that password by now).



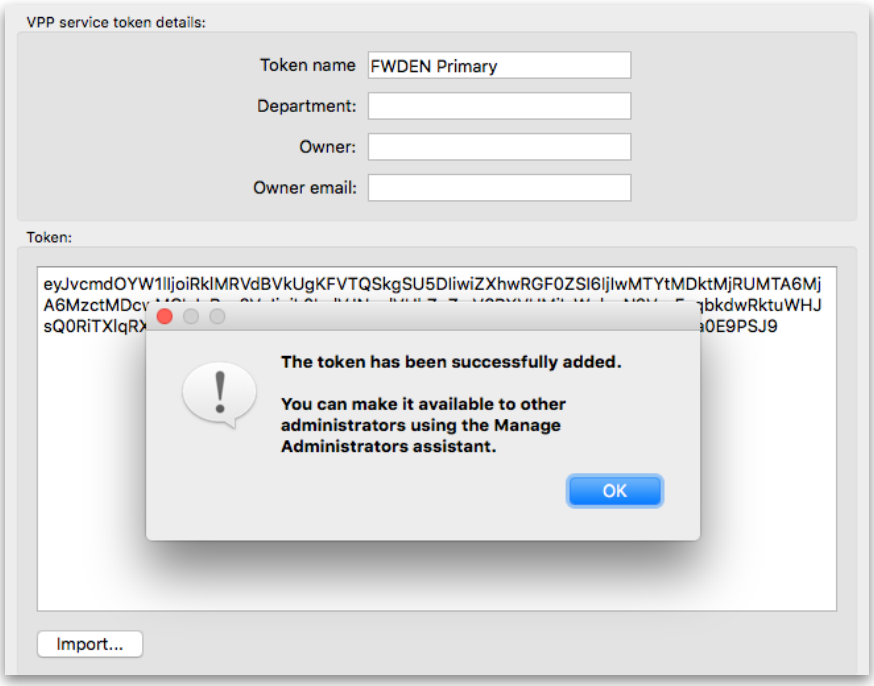
Adding a VPP service token

Click on the **[+]** button (2) and import your downloaded VPP token (3). When you import the token into this pane, you will see a long alphanumeric hash as shown. Continue these actions until you have added all of the VPP tokens you plan to use for content distribution. As the token is being added, it will contact Apple and you will see the following dialog:



Note: Make sure you are not using your VPP token on more than one MDM server. Problems, such as loss of control of the token or automatic VPP user retirement, can result.

Once the token has been properly imported, you will see a dialog pop up telling you that everything is in order.



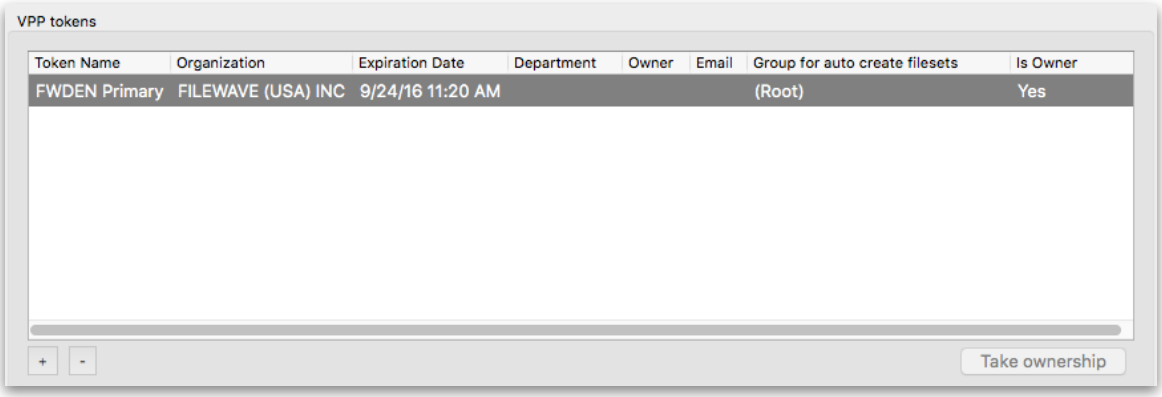
If you want more than the FileWave superuser/admin account (**fwadmin**) to be able to manage VPP applications later on, you will need to use the **/Assistants/ Manage Administrators…** pane to assign other administrators to manage the VPP token(s). This is covered at the end of this chapter in section **3.15**.

Auto-create filesets

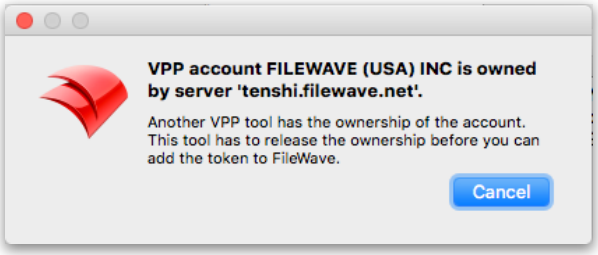
The first time you set up VPP, you will get Filesets automatically created for each of your existing VPP purchases. You can assign those Filesets to a designated FileWave group for management. The default is the **(Root)** group. VPP Fileset creation is covered in detail in chapter **7 License Management**.

VPP account protection (aka "Take ownership")

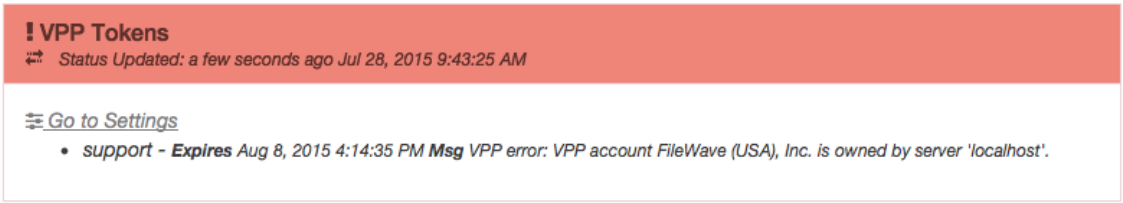
One of the new features in FileWave v10 is protection of the VPP accounts and tokens that you use with your server. The concept is very simple: an identifier (called "client context") is sent to Apple for a given VPP account. When an MDM server has to use a VPP account, it will query this identifier and compare with its own; if they match, everything is fine. If they don't match, the server should not use the token.



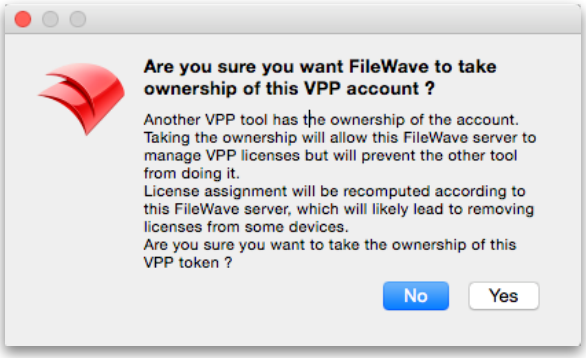
As long as you are the confirmed owner of the token, the **Is Owner** flag says *Yes*; but if you have changed servers, or let another process, such as Apple Configurator, use that VPP token, then you will get an alert like this:



If you have a mismatch, your VPP token entry will turn **red**, and you will not be able to use that token. Your first indication of an issue may be an alert in your Dashboard:



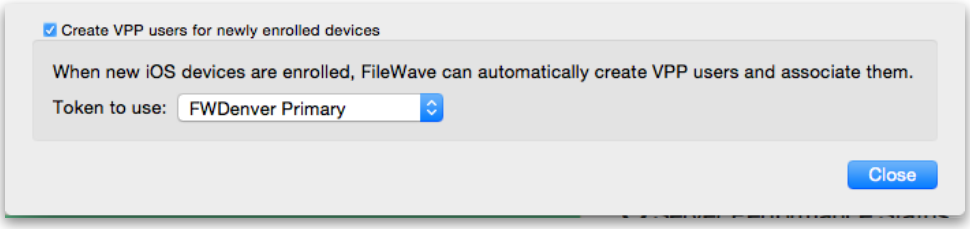
In order to regain control of the token, you will need to select the token entry and click on the **Take ownership** button in the lower right corner of the VPP tokens pane. Once you have done that, you will get a confirmation dialog:



Key to this process is to make sure you do not apply any of your VPP tokens to a different server, tool, or application. If you are running a test/beta FileWave server, you should create a unique VPP account and token for that purpose. If you are running **Apple Configurator**, you should definitely create a unique VPP account and token for that purpose.

Create VPP users for newly enrolled devices

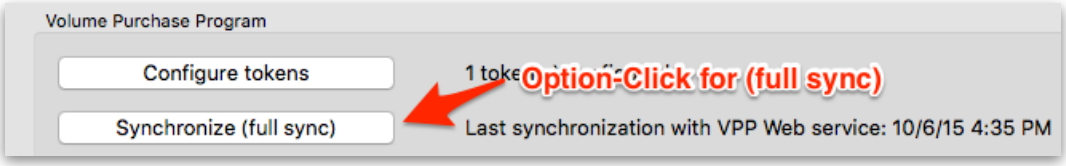
Back in the Volume Purchase Program pane, you can elect to **Create VPP users for newly enrolled devices**. VPP users are internally created accounts that link your enrolled device to the FileWave VPP management process. It's not an actual "user" account; but more of a placeholder for the assignment of VPP apps and books. Each VPP user account may contain a link to an actual end user's AppleID.



If this checkbox is selected, then newly enrolled devices will automatically get a VPP user and that user account will be associated with the device. This can speed up mass deployments, as well as reduce the overhead on 1:1/BYOD deployments. Used in conjunction with settings in the VPP Assistant, your FileWave server can then automatically notify new user's to register their AppleID with your FW MDM server. You can select a single VPP token to be the primary token related to those VPP users. Also, you can change which tokens are associated with specific VPP users as you need.

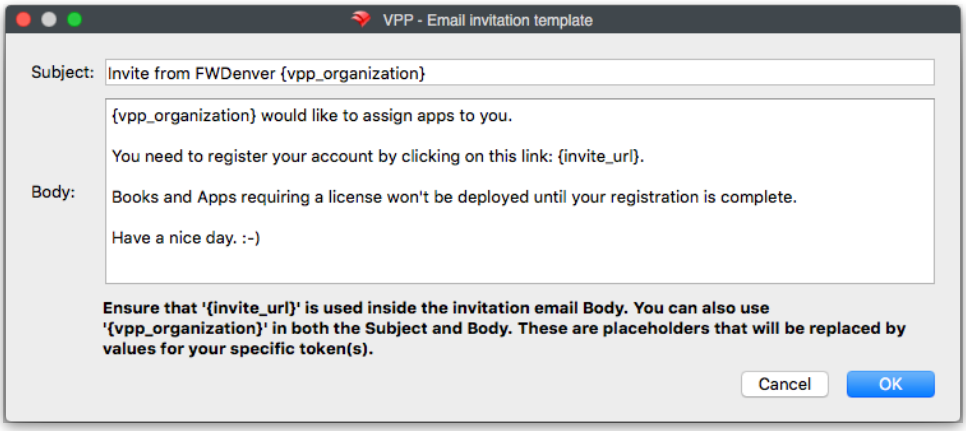
Synchronization

The VPP Synchronization setting lets you determine how often the FW MDM server will match data with your assigned VPP token account. You can push an incremental synchronization by clicking on the **Synchronize** button; and you can force a full synchronization by holding down the **Option** key while pressing the Synchronize now button.



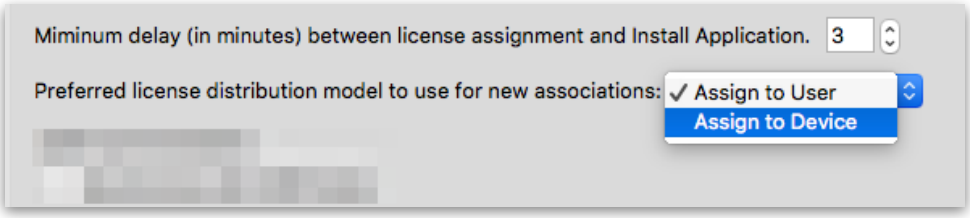
Configuring VPP email invitation template

This template will be used by your FileWave server to send an invite to users enrolling in your MDM from iOS and OS X devices. If you have configured your setup to use LDAP authentication for enrollment (see Section 12.), then your users will get an email addressed to the mail account in their LDAP record. It will contain a custom URL pointing them to the Apple App Store where they will authenticate with their AppleID to register that ID with your FileWave MDM.



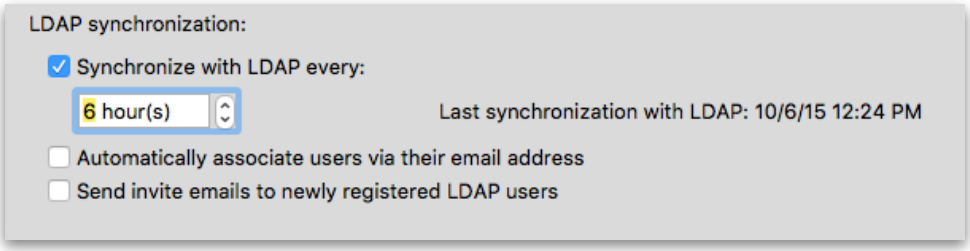
Minimum delay and Preferred Distribution

New in FileWave v10(+) is the ability to establish a delay between the time you associate a VPP application with a license and the application is made available to install at the client. This avoids issues during large scale deployments where clients are trying to install VPP applications; but haven't gotten their license assignment yet.



Preferred Distribution allows you to choose the method of deploying a VPP application. The original method has been to assign an application to a registered AppleID. The license shows up in the user's Purchases, and the license can be managed by the FileWave MDM. The new method, supported in iOS9+ and OS X 10.11+, allows you to assign VPP applications directly to an enrolled device. This method applies only to VPP applications - iBooks are still required to be assigned to individual AppleIDs. There is a detailed discussion of this process in chapter **7 License Management**.

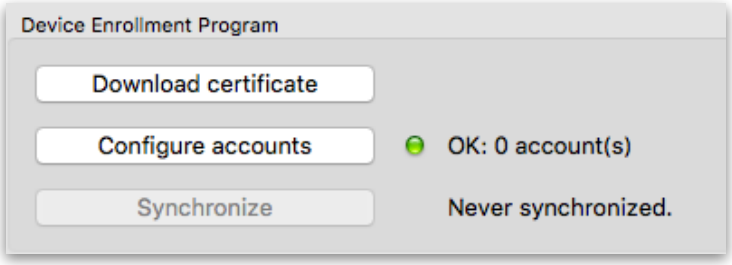
Using **LDAP synchronization** allows you to link your LDAP users with VPP users, who can then be associated with their email addresses (if those exist in the LDAP directory). This allows you to have VPP/MDM emails automatically sent to those users. This process is important because of the way VPP can link users to devices through their AppleIDs for application assignment to users, if you are going to assign iBooks to the users. This process can be left off if you are going to use **device assignment** of all your distributed VPP applications.



Device Enrollment Program preferences

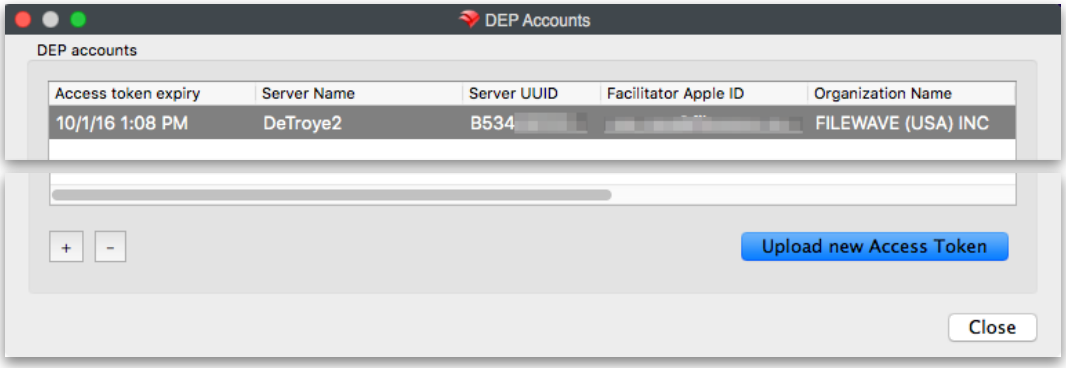
Apple's Device Enrollment Program is designed to support OTA (over the air - WiFi) supervision of devices. FileWave supports iOS and OS X devices using DEP. Apple provides a list of approved devices in these links: Apple DEP info for iOS and Apple DEP info for OS X. Institutionally purchased devices are registered with Apple, and Apple provides a DEP token for you to link your FileWave MDM server to the DEP service. When a device comes up online, it is

recognized by the Apple DEP service, matched to the downloaded token, and automatically configured for supervised management with your FileWave MDM. The preferences you set to get this process up and running are shown below.

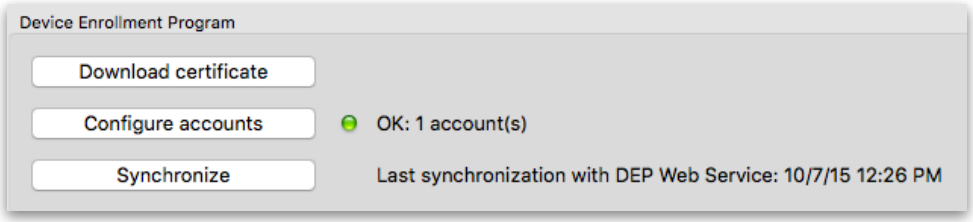


Using the “Download certificate” button, download a special “FileWave DEP” certificate to your administrator machine. You will be required to authenticate with the **fwadmin** FileWave Admin account. Use that certificate to get a DEP token from the Apple DEP site (https://deploy.apple.com).

Select the “Configure accounts” button, and authenticate using the primary **fwadmin** account. You’ll be presented with the option of uploading new tokens. You can have a token for each of the DEP facilitators you have.



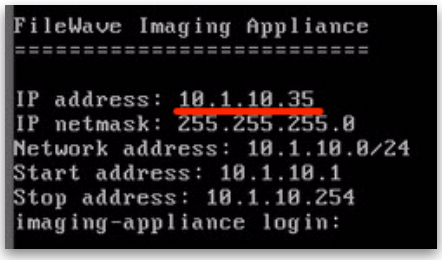
The **Synchronize** button works the same as the VPP synchronize button. DEP will synchronize between Apple and your server once a day. You can hold the alt/option key down to force a full, immediate synchronization. Use that sparingly, since it may take a long time to synchronize with lots of devices in the system.



More information on the workings of VPP and DEP are in chapters **5** and **7** of this manual.

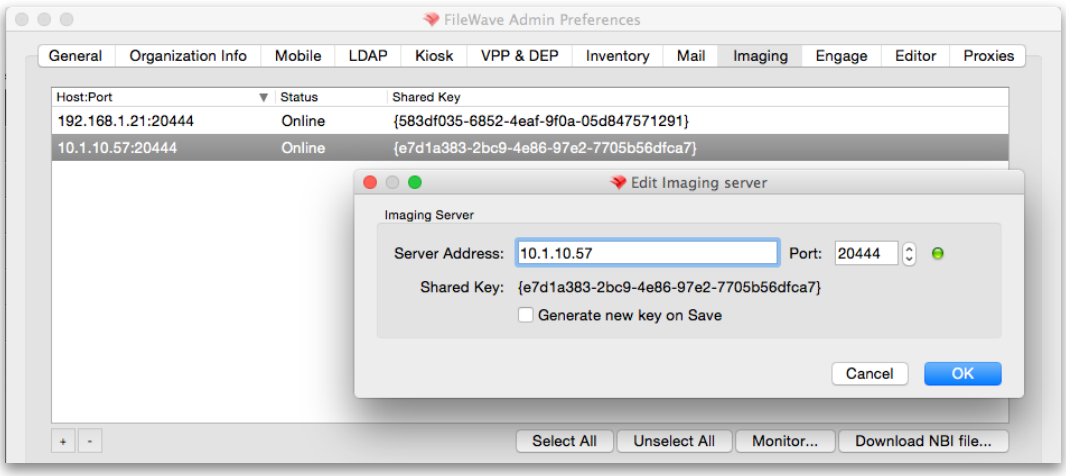
3.13. Imaging preferences

The FileWave Imaging Virtual Server is linked to the FileWave server through these preference settings. You install the **IVS** inside your own virtual machine software, on a device of your choosing (to install the **IVS,** see the information in chapter **3**). More information on using the Imaging Virtual Server is in the **Imaging** chapter of this guide. Once you have the VM running, you will see a terminal window that will contain the IP address of the imaging server. By default, the IVS will grab a DHCP address from the subnet it is activated in.



Copy that address and add it to the *Server Address* in the **Imaging** tab. You can also set up a fixed IP address for your IVS, if you are running IVS version 3.0.2 or above. That is recommended for more stable behavior. The process is explained in section **3.2.** Do this task for each of the IVS configurations you set up across your network.

Note: You should set up only one IVS per subnet. Multiple NetBoot/PXEboot servers on the same subnet can be problematic.



The default TCP port for FileWave Imaging management is **20444**. This is not the same as the ports for PXEboot and NetBoot. Details on that are covered in the **Imaging** chapter of this guide.

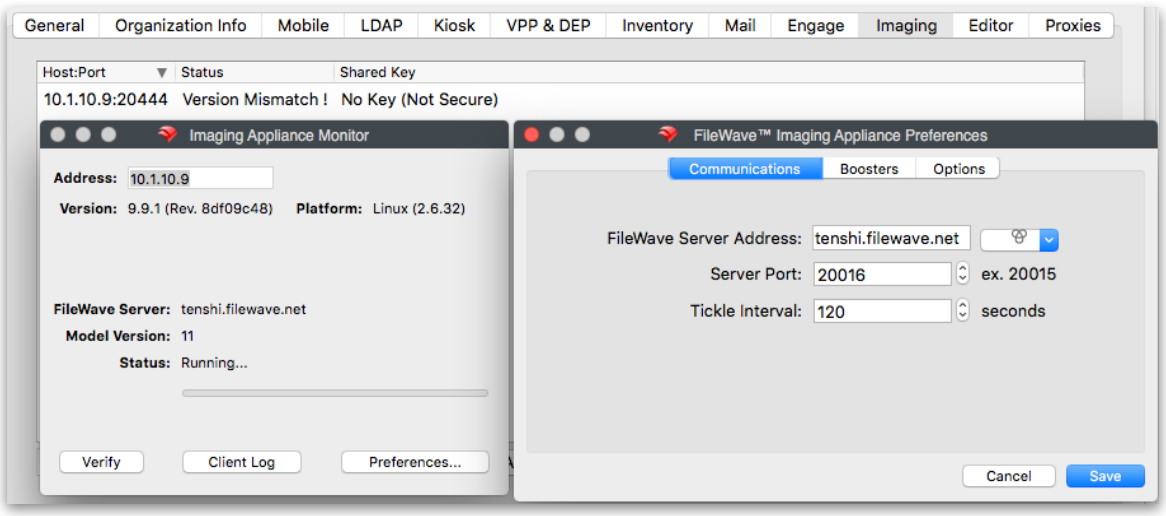
Shared Key and Imaging

The Shared Key in Imaging supports secure communication between the server and client, as well as any Boosters associated. Once the Shared Key is set, you should not change it. Doing so will require that you re-run the **create-nbi.sh** script.

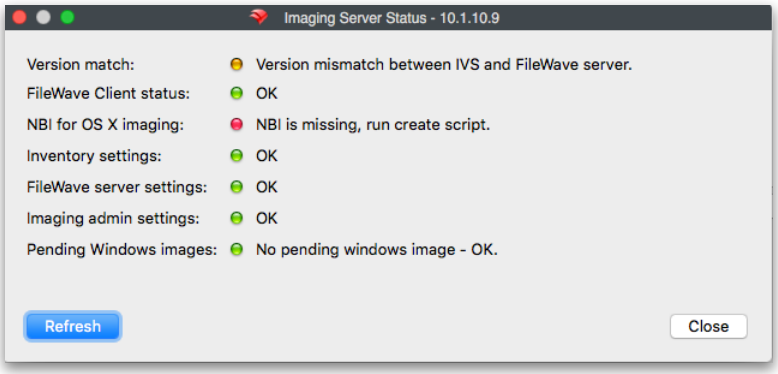
Monitoring

The IVS is also a FileWave client. An **Imaging Appliance Monitor** is accessed through the ***Monitor…*** button. This allows access to the IVS console log as well.

You **must** select the **Preferences** button in the **Monitor** pane, authenticate using the password of your IVS (default is *filewave* and you should change it), and set the IVS to communicate with your FileWave server.

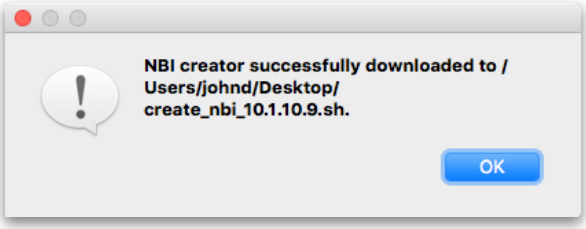


You can check to see that the settings are correct by checking the **Status…** button in the main **Imaging** Preference pane: (Note: In this version of the manual, the beta IVS was in use - so there was a Version mis-match.)



Download NBI file…

This button downloads a script that you will then run on an OS X system to create and upload the NBI to your IVS. Each IVS must have a boot image for initiating NetBoot. This NBI (NetBoot Image) is the system image that OS X devices will boot from within their subnet. The NBI will then use a designated disk image to perform the actual imaging of the client. Each IVS must have this task performed in order for NetBoot to function. Instructions for running the script are in chapter **10**. It is also important for you to understand that the NBI is OS specific. You must run the script on a Mac with a recovery partition, and it will create an NBI for that version of OS X only, and send the image to the specific IVS named in the script (note the filename of the script). You can run separate IVSs to store differing versions of OS X NetBoot images.



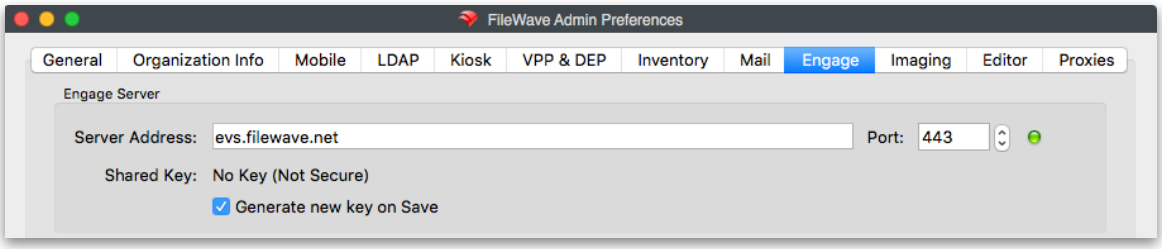
All other imaging configuration will be done from the **Imaging** pane in the main Admin window. See chapter **10** for more details on IVS and Imaging.

3.14. Engage preferences

Engage is the classroom management tool introduced with FileWave version 9. Setup and configuration of the Engage server VM (EVS) is covered in chapter **3.** For details on the use of the Engage applications, see chapter **11** in this manual.

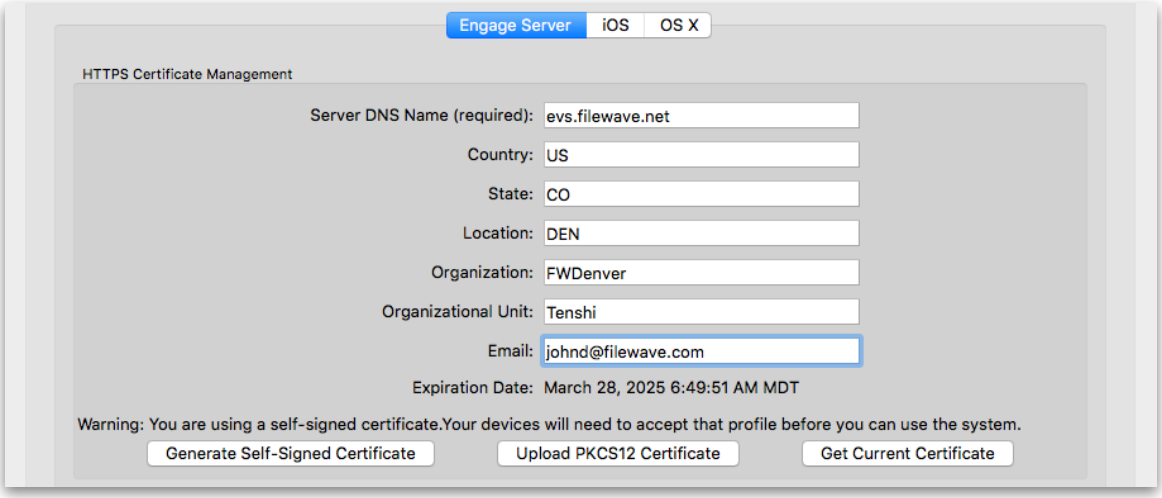
Engage Server

Enter the server address for your Engage server VM. It should be a FQDN or fixed IP address, if possible. The default TCP port for Engage is 443.



HTTPS Certificate Management

There are two options for securing the communications between the Engage server and its clients - a self-signed certificate or a valid SSL certificate in .p12 format. There are also specific push certificates for iOS and OS X that will be provided by FileWave as part of your software download.



Self-signed certificate for https

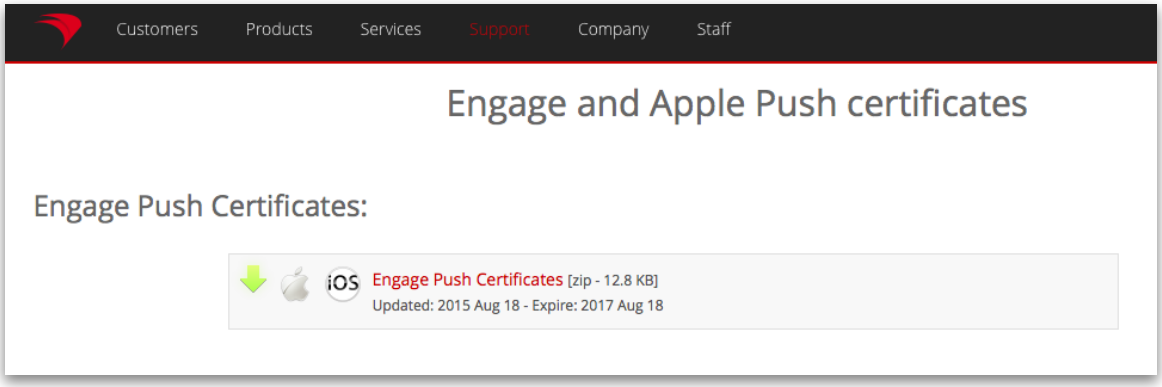
Fill in the data fields in the **HTTPS Certificate Management** pane of the Engage preferences. Click on the button ***Generate Self-Signed Certificate***, then click on the button ***Get Current Certificate***. You will download the self-signed certificate and import it into FileWave Admin as part of a Certificate profile. See the section on working with Filesets for further information on profiles. This certificate profile must be associated with all iOS and OS X clients before they launch the Engage application for the first time. Otherwise, the client will display an error that it “cannot connect to server” - meaning the Engage server.

3rd Party certificate for https

You can use a known 3rd party for a valid certificate with Engage, companies such as StartSSL, VeriSign, etc. Follow the instructions on their site to download a valid server certificate in **.p12** format. Upload that certificate into FileWave Admin Engage preferences using the ***Upload PKCS12 Certificate*** button. When you have done this, you will get an alert to restart the Engage server.

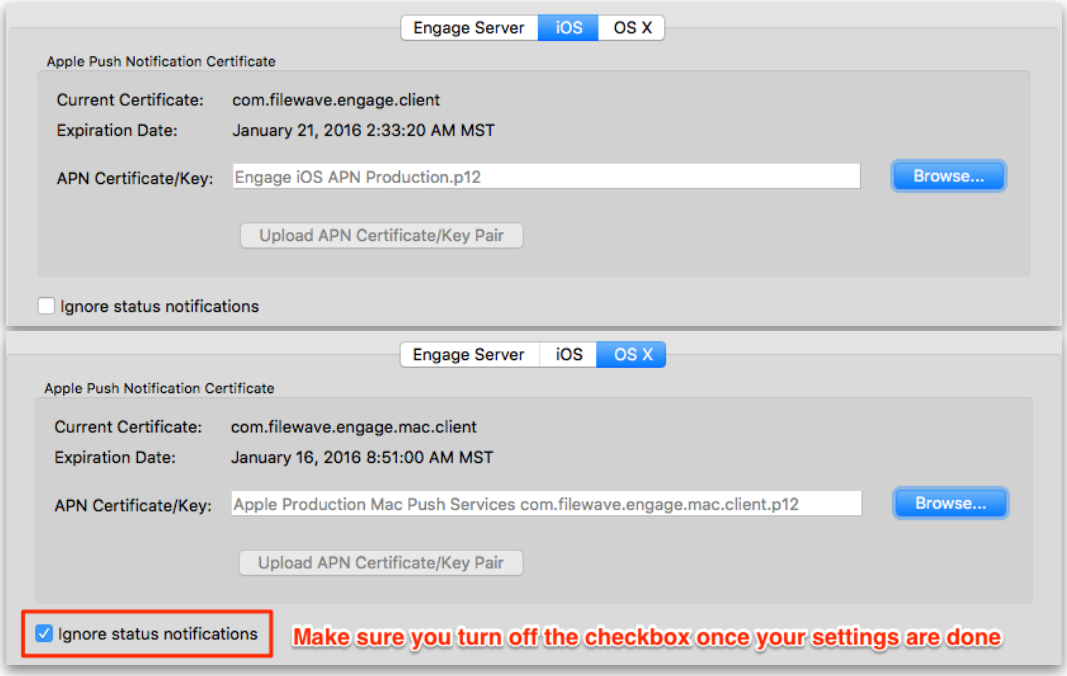
iOS / OS X push certificates

The push certificates you need for Engage will be provided by FileWave. These certificates are provided by FileWave from the FileWave Support site: https://www.filewave.com/support/csr-portal



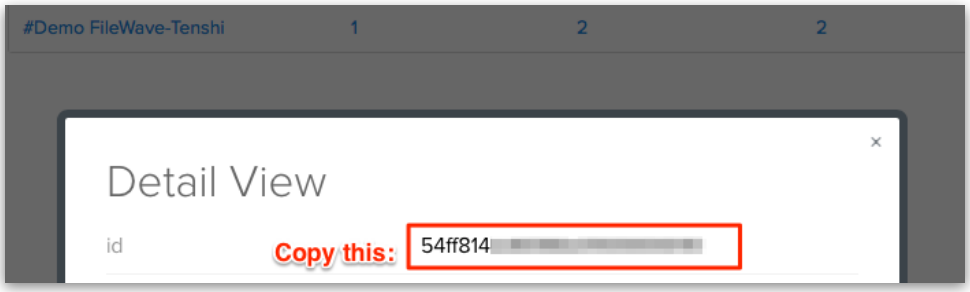
Download the certificates and unzip/unpack them.

In **Engage** preferences, select the tab (iOS or OS X) for the certificate you are going to import, then click on the ***Browse*** button. Locate the appropriate certificate and select ***Open***. Finally, click on the button ***Upload APN Certificate/Key Pair*** to complete the settings. Turn off the *Ignore status notifications* checkboxes as you complete each of the settings; otherwise, the Dashboard will not display the status properly.

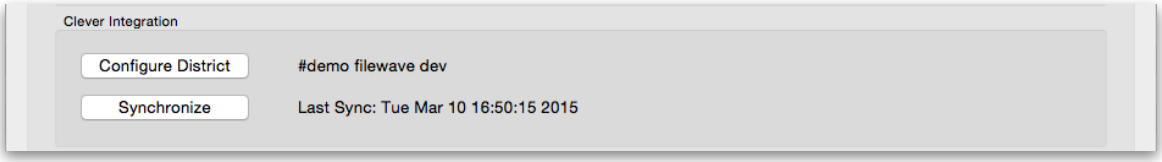


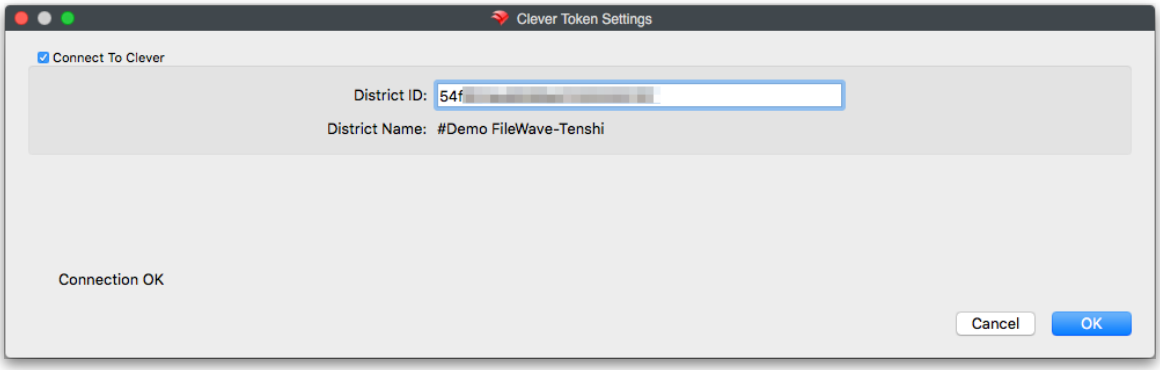
Clever Integration

Clever integration is provided for free by FileWave. The process for this is very simple. Go to http://www.clever.com and log in using the account and password provided to you by Clever. That will present you with your district/site web page. Select **Browse** from the **Data** section. Select your district, then copy your **District ID**.

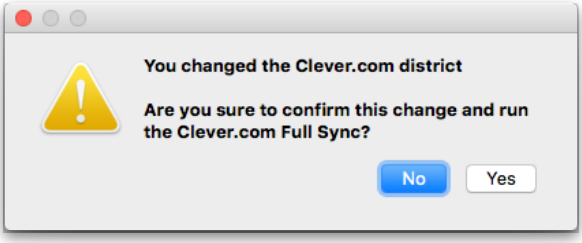


In the Engage preferences, click on the ***Configure District*** button, authenticate as the FileWave Admin superuser (fwadmin), and paste the *district ID* into the data field.

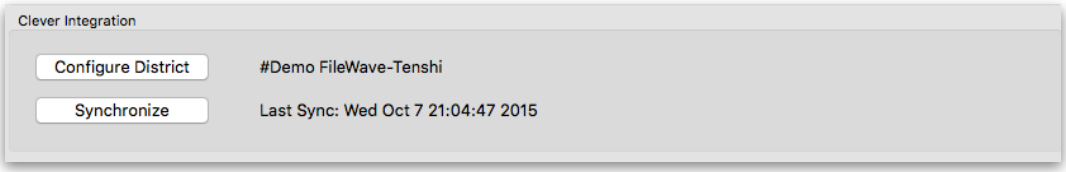




You should see the following dialog pop up. It's just making sure that you wanted to use that district ID, and that it may take a while to cache all of the data from Clever to your EVS.

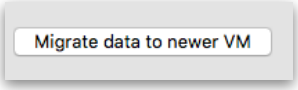


Once all the settings are completed, you should see information like the example below, showing that you are connected to Clever and syncing data.



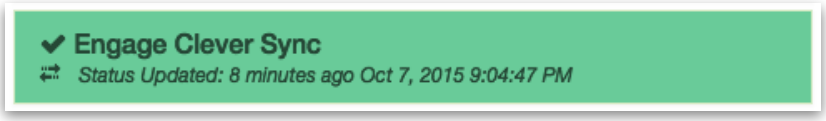
Migrate data to new Engage server

If you plan to upgrade to a new VM of the Engage server, you don't want to lose any of the data or settings you have established. This checkbox allows you to set up a new Engage server VM and transfer your current settings.



The setup will ask for the address of the new EVS, transfer your data, then remind you to change the network settings of the new EVS to match those of the previous EVS.

Once all of your settings are filled in, and correct, you will see the status on the Dashboard show that everything is in order:

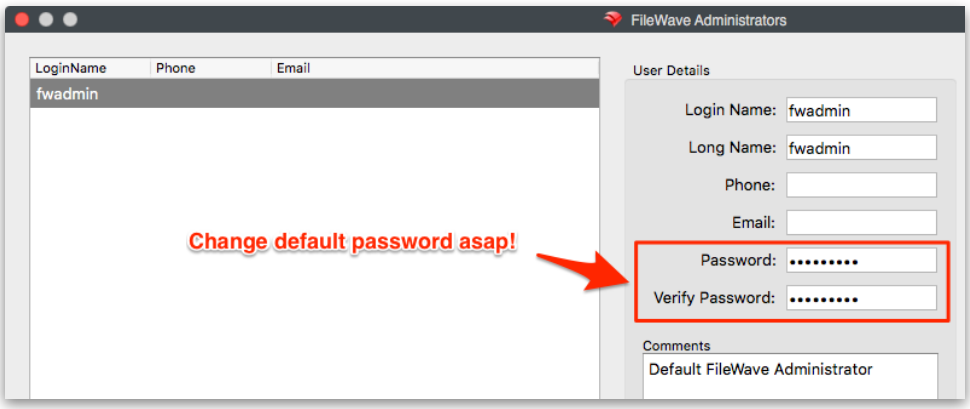


3.15. Managing FileWave Administrators

FileWave supports tiered administration. You can create additional administrators in order to spread the workload. For example, if you have someone designated to manage only the iOS devices, or just the Windows systems, you can create an administrator who will be allowed to manage only those specified devices. You can have administrators designated for a location, a department, or even a classroom. More information on the administrator assignments is included under the **Clients** and **Filesets** sections in this guide. If you are planning on having more than one FileWave Admin account, contact FileWave Support - your license will need to be updated to support multiple administrators. (There is no cost for this - additional administrators are free.)

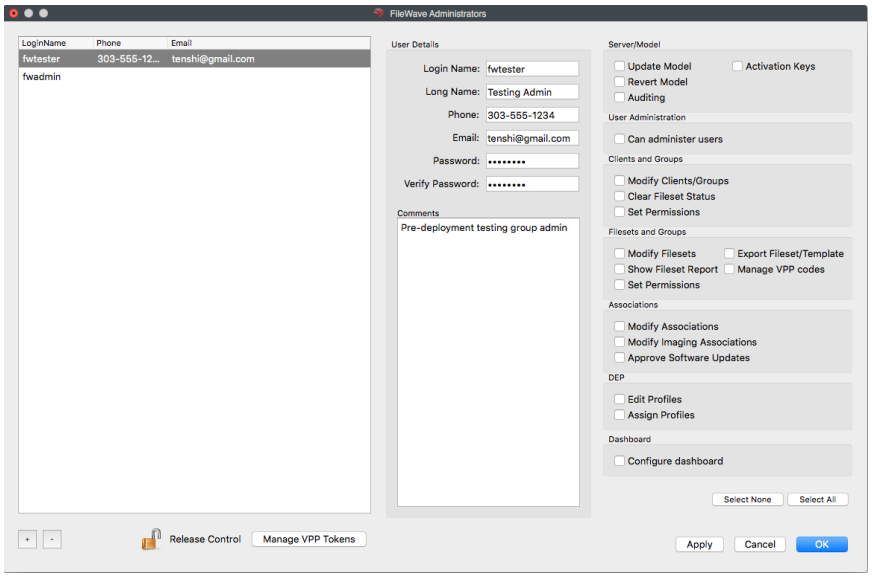
Configuring the primary FileWave administrator

The primary FileWave Administrator (**fwadmin** - by default) is commonly referred to as the “super administrator” or “superadmin” and has the ability to create/edit/delete all other administrators. When you first set up FileWave, you will need to go to **Assistants/Manage Administrators…** and change the default password for the primary administrator account. By default, the password is “**filewave**” and you should change that to something a little more secure. You can then move on to create additional administrators.

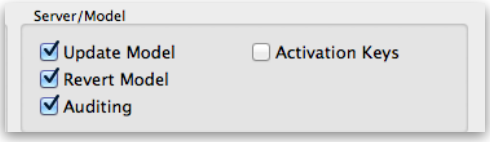


Configuring a sub-administrator account

A “sub-administrator” account can be assigned as many privileges and options as the primary FileWave Administrator account. The best practice is to create accounts to manage specific aspects of the management suite. To create an administrator account, you select the [+] button at the bottom left of the FileWave Administrators pane. You may then fill in the user details as you see fit, and assign permissions as needed:

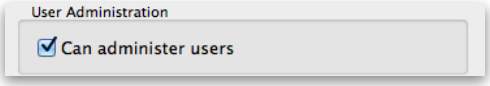


Server / Model



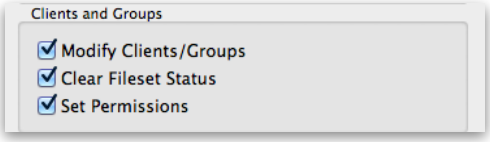
- *Update Model* - allows the administrator to approve changes to the server model. Updating the model sends notifications to all FW clients of any possible changes to any filesets they have.
- *Revert Model* - allows the administrator to cancel changes made at the last model update and revert to the previous model version.
- *Auditing* - allows the administrator to view the Audit History of all actions logged by FileWave.
- *Activation Keys* - allows the administrator to enter, change, or update the activation keys for the FileWave server.

User Administration



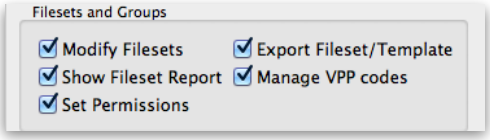
- *Can Administer users* - allows administrator to add, edit, or delete administrative users.

Clients and Groups



- *Modify Clients / Groups* - allows administrator the ability to add, edit, and delete FW clients and client groups.
- *Clear Fileset Status* - allows administrator the ability to remove all messages in the client info window for a designated client.
- *Set Permissions* - allows the administrator to assign clients and client groups to specific administrators.

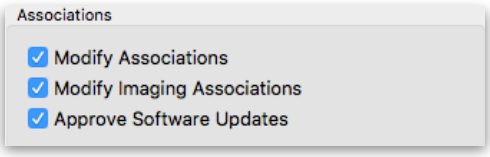
Filesets and Groups



- *Modify Filesets* - allows administrator to edit filesets, add or delete content within a Fileset.
- *Show Fileset Report* - allows administrator to view the Fileset report showing the status of that Fileset.
- *Set Permissions* - allows the administrator to change the permissions within a Fileset or Fileset group.
- *Export Fileset / Template* - allows the to export a specific Fileset or a template for use on another FileWave server, or for archival purposes.
- *Manage VPP codes* - allows the administrator to access the management settings under the Assistants menu for Apple's VPP code management. This includes the following menu items:
    - *VPP Code Management*
    - *Manage VPP Users (iOS 7+)…*
    - *Manage VPP Licenses (iOS 7+)…*

Note: If you do not allow an administrator to *Manage VPP codes* then they will not be able to see any of the VPP purchased applications or ebooks. This is especially important if you have multiple token support.

Associations



Modify Associations - allows the administrator to change the associations settings between a client or client group and any Fileset or Fileset group.

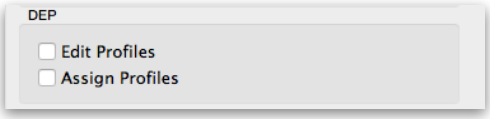
Modify Imaging Associations - allows the administrator to change which Imaging Filesets are associated with which devices

Approve Software Updates - allows the administrator to designate specific software updates as pre-approved for association by other administrators.

DEP

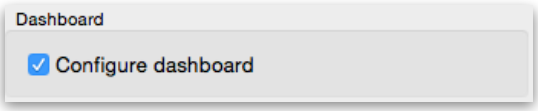
- *Edit Profiles* - allows the administrator to change the characteristics of DEP profiles, including naming conventions, setup assistant workflow, and certificate assignment.
- *Assign Profiles* - allows the administrator to designate specific client devices to be managed by certain DEP profiles.

Note: If you do not allow a sub-administrator to edit/assign profiles, then all DEP management must be done by the main *fwadmin*.

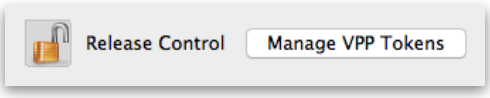


Dashboard

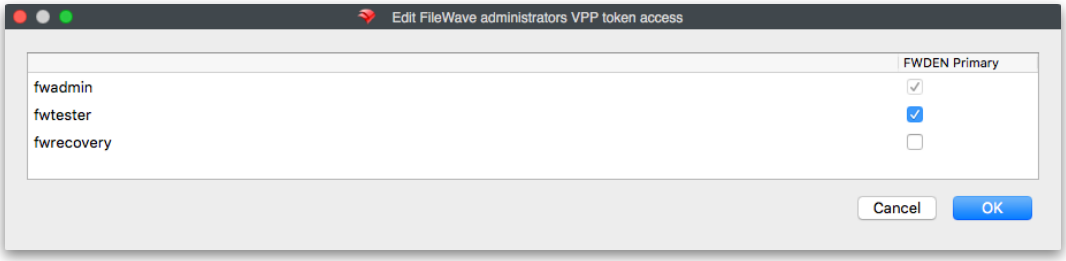
Hides the notification settings links for administrators not allowed to configure the Dashboard



Control *and* ***Manage VPP tokens***

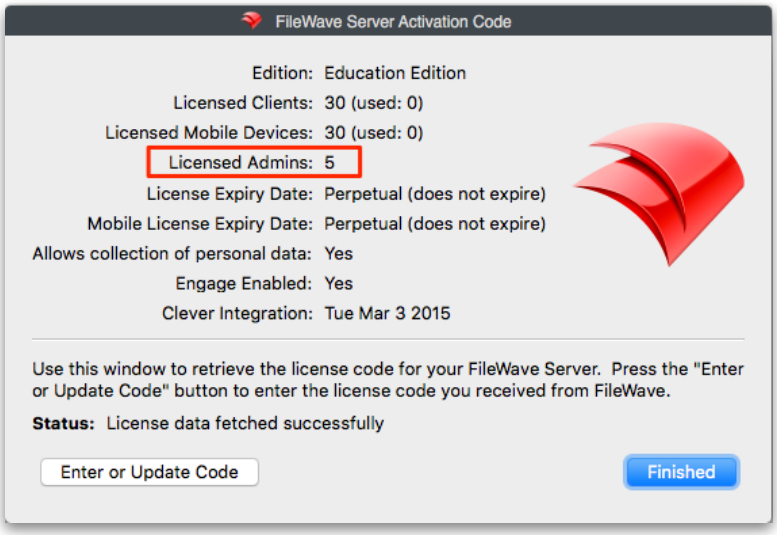


- *Take/Release Control* - administrator can take control of the other administrator accounts, locking them out from FileWave Admin while administrator privileges are being edited.
- *Manage VPP Tokens* - allows the administrator to designate which other administrators are allowed to perform tasks with the VPP tokens, to include changing the association of a token and a Fileset. (This button opens a settings dialog - see below)



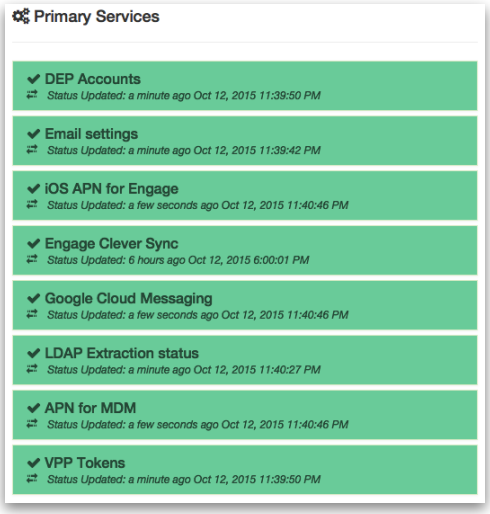
Note: If you do not allow a sub-administrator to manage VPP tokens, then all VPP management must be done by the main *fwadmin*.

The use of tiered administrators will benefit almost any size organization. Being able to parse out your deployment and management workflow to other administrators will help keep the overall workflow on task and on time.



3.16. Configuring and using the Dashboard

In FileWave Admin, the Dashboard is the first view an administrator gets of their FileWave environment. The Dashboard is designed to give the FileWave administrators a quick view of their server and be able to focus in on a missing setting, or a possible service interruption. There are seven major sections on the Dashboard.

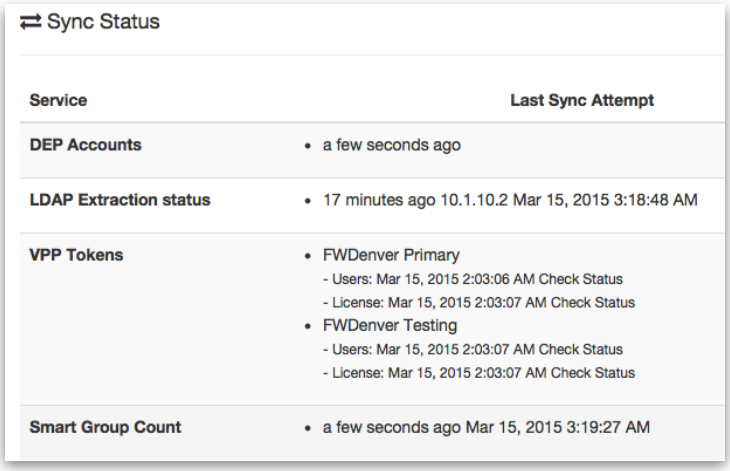


Primary Services

This section shows the major services - DEP, VPP, Email, etc with last update and, if there is an error, a direct link to the settings that can address that error.

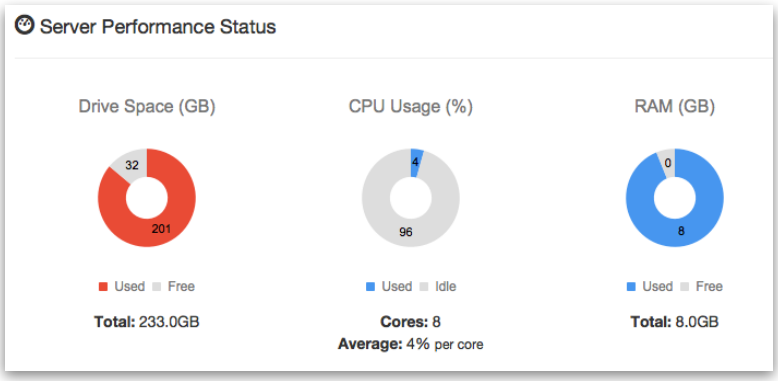
Sync Status

This section shows the latest 'check-in' times for certain services, such as VPP, DEP, LDAP, and Smart Groups. These services all have preferences requiring synchronization between a remote service, for example your LDAP server, and the FileWave server.



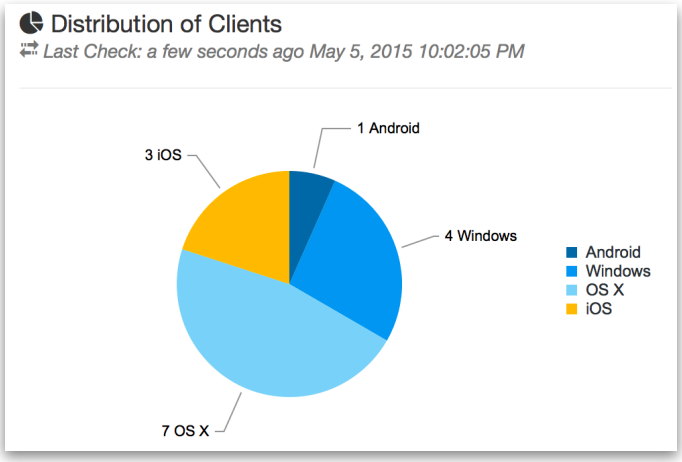
Server Performance Status

This section is an active chart of the status of the primary FileWave server's storage space, CPU usage, and ram utilization.

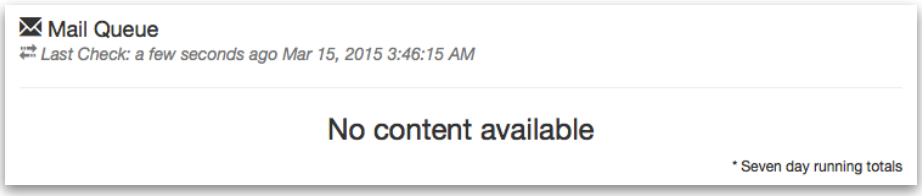


Distribution of clients

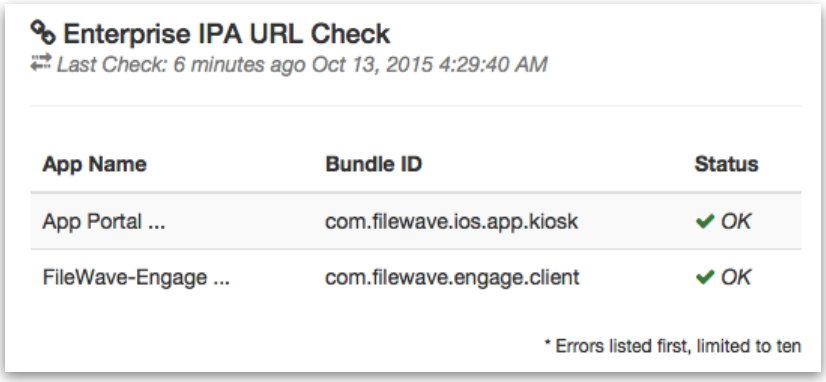
This section displays a graph showing the breakdown of FileWave clients based on operating system.



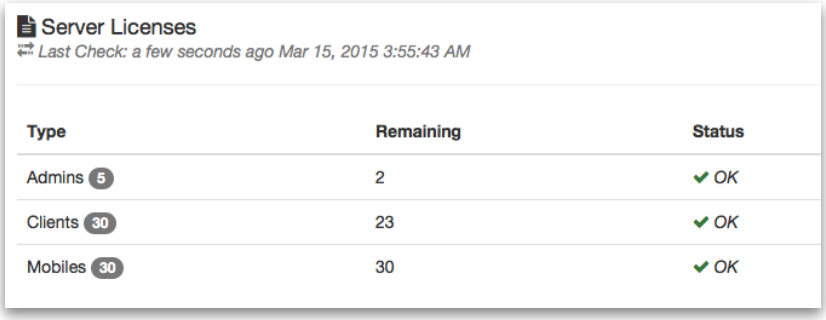
Mail Queue
This section displays a running graph of the status of emails sent from the FileWave server. The focus will be on the VPP / MDM invitation emails. This will help you see situations where your local email server may be getting overwhelmed by the large number of MDM invitations going out at the same time.



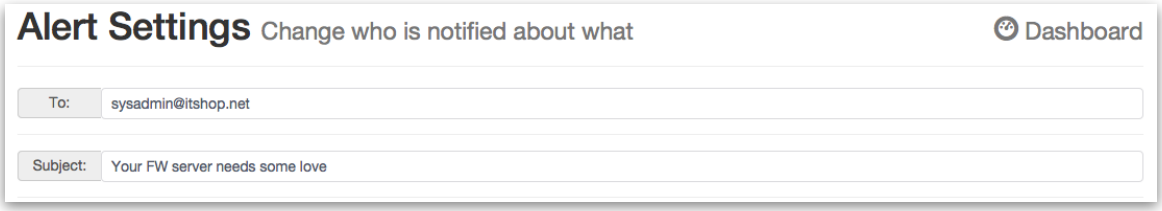
Enterprise IPA URL Check
This section shows the validity of your institutionally created iOS apps as well as the enterprise apps provided by FileWave (iOS App Portal / Kiosk and Engage).

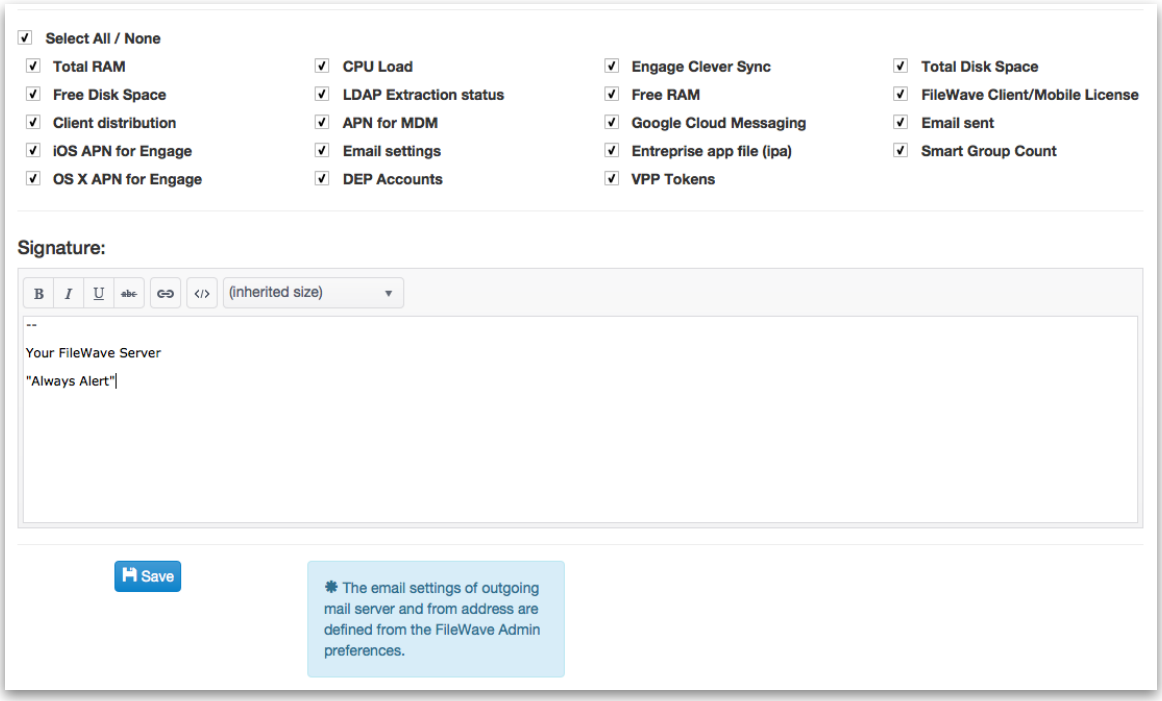


Server Licenses
This section shows the current status of your FileWave server license, how many licenses exist and the number of remaining / unused licenses.

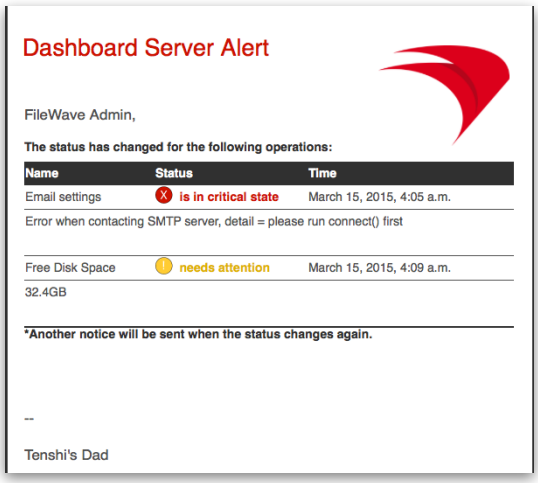


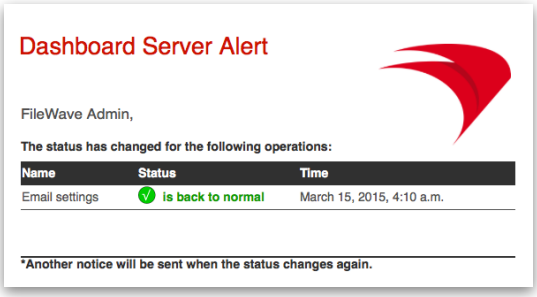
Alert Settings
The Dashboard provides the FileWave Admin with the ability send notifications out to individuals at status changes on the server. You toggle between the **Alert Settings** and the **Dashboard** in order to configure the types of alerts sent out and who they are sent to.





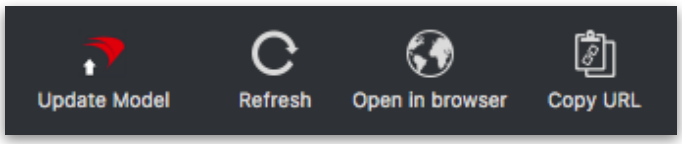
The result is an email when an event is triggered being sent to the designated email account, such as below:





"Wandering" Dashboard

The Dashboard is part of the FileWave Admin application; but it can also be dragged off to be viewed as a separate window on the administrator's computer, opened in your own browser, or provided as a URL to other interested parties to view on their own computers, or tablets, as desired.



Dashboard Alert details

A table with explanations of all of the available alert items from the Dashboard is available in the **Appendix**.

3.17. Migrating Server Info and Moving Data

When the time comes to replace your FileWave server with new hardware, you can migrate all of the relevant information to the new hardware easily. If you are only looking at moving the data (Filesets, Inventory data) to a different drive/storage area, the process for doing that is reasonably straight forward.

Migrating server info

1) On the target server, install the FileWave server components - Server and Admin application

2) On the target server, shut down the FileWave services using

```
sudo fwcontrol server stop
```

3) Share and mount the target server's drive via afp/smb onto the source server

4) On the source server, shut down the FileWave services using

```
sudo fwcontrol server stop
```

5) Use "ditto" to copy over /fwxserver, /usr/local/etc and /usr/local/filewave to the target server's mounted drive

```
ditto /fwxserver/ /Volumes/<MY-SHINY-NEW-TOY>/
```

6) Once the copy is complete, start the FileWave server on the destination using

```
sudo fwcontrol server start
```

At this point, you should shut down the source server and change the target server's IP address to the same IP address as the source server. This would let all the clients use the same settings as before to connect to the new FileWave server. If that is not possible, change the DNS entry that pointed to the old server to match the new server. A third option would be to use the old server to send out a "Superprefs" fileset to send your clients to the new server before you take the old server offline..

Storing FileWave data on a different hard drive

By default, FileWave stores all Inventory data and a copy of every Fileset on the primary volume that FileWave server is installed on. You can move this entire data set to another drive to avoid disk space issues and improve performance. Check your pathnames very carefully!

Start by stopping the FileWave server

```
fwcontrol server stop
```

Then move the FileWave Data folder to the new drive

```
mv /fwxserver/Data\ Folder /Volumes/<my_super_fast_SSD>
```

Link the old data folder location to the new data folder location

```
ln -s /fwxserver/Data\ Folder /Volumes/<my_super_fast_SSD>/Data\ Folder
```

Finally, restart the FileWave server

```
fwcontrol server start
```

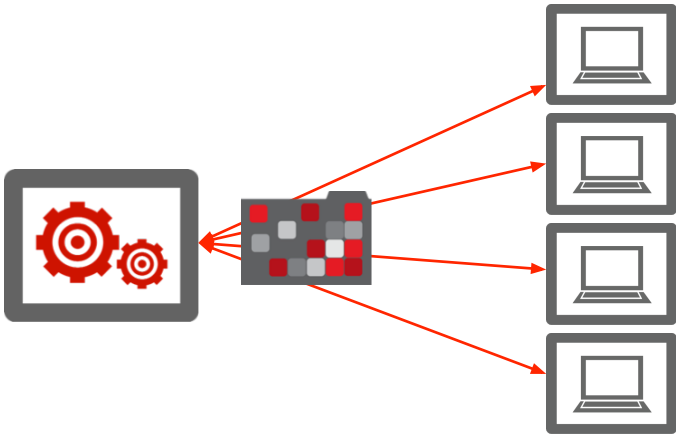
-This page intentionally left blank-

4. FileWave Boosters - installation, configuration, and management

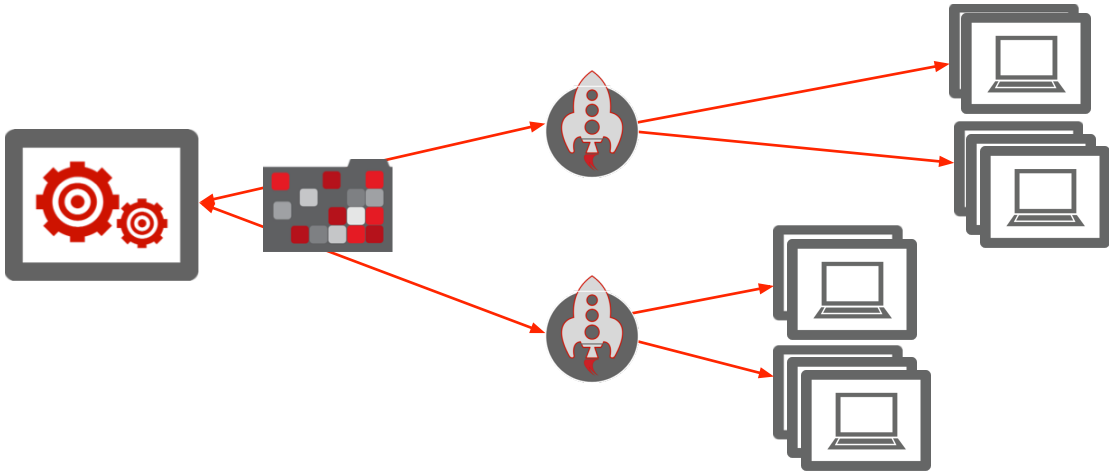
Scalability for a systems management solution is essential. FileWave can manage an Inventory of hundreds of thousands of various devices in the main server; but the distribution of a large number of Filesets with needed applications and content can overload a network if all the downloads are forced through a single connection. The FileWave Booster exists to help distribute the Filesets closer to the deployed devices, significantly reducing the network load from the central server.

Note: The FileWave booster caches and forwards Filesets for desktop/laptop devices as well as Android. Apple iOS device Filesets exist only at the main FileWave server and do not use the boosters for caching.

Instead of forcing the server to do all of the work:



You will see the server send a single copy of a Fileset to a booster, then the booster redistributes to the clients as needed:



When you set up your FileWave server, the default configuration is to configure the clients to talk to the server directly. Therefore, every Fileset you create will exist on the FileWave server, and each client associated with that Fileset will get it directly from the FileWave server. This process will work well up to a point; but as anyone who has done network tuning will see that eventually, the bandwidth between the server and clients will no longer be able to efficiently provide timely file transfers. Boosters exist to help cache Filesets from the FileWave server closer to groups of clients that need those Filesets.

Configuration of the FileWave client to use boosters is limited to desktop/laptop devices running OS X or Windows plus Android devices. iOS devices cannot take advantage of booster technology at this time. If you are going to deploy large numbers of iOS devices, you should schedule some time to discuss best practices and hardware requirements for an optimal FileWave server configuration to best support that deployment model.

Boosters can be configured to cache content from other boosters, allowing the entire architecture to scale to any size needed. This scalability allows you place boosters across a campus, a company, or even around the globe for international deployments. The central server would contain a single copy of each Fileset; but the boosters would handle the bulk of the traffic. Large scale operations where one group of devices needed to get dozens of new Filesets would show a minor amount of network traffic while the Filesets were copied down to the specific boosters; then the greatest traffic load would be on a local subnet where the device group needed to be configured.

The Booster keeps local copies of all Filesets sent to connected Clients (Android, OS X and Windows). As soon as a request for a Fileset comes to the Booster from a Client, the Booster tries to fulfill this request by sending that particular file to the Client. If the Fileset is not already present in the Booster's data folder, then the Booster contacts the FileWave Server to download this item and provide it to the Client. Neither this Booster nor any connected Clients will ever contact the Server for this item in the future - unless the contents of the Fileset are changed. The Client has the ability to connect up to 5 Boosters in sequence .

This “booster cascade” is used when a FileWave Booster cannot be reached. If the last Booster fails, then the FileWave Client will go directly to the FileWave Server to download the Fileset. This cascade can also be used if you are using FileWave in different offices or locations. Placing a FileWave Booster in each location will prevent the Clients from downloading Filesets directly from the central FileWave Server. Instead the local FileWave Clients will download the Filesets from the local Booster. This is much faster and much more cost efficient. All Images associated with clients are also stored on Boosters located in the same subnet as the IVS.

Note: Boosters can only be assigned for Android, OS X and Windows devices. iOS devices do not have a mechanism to use a booster; they contact the FileWave server directly.

4.1. Booster deployment planning

Scalability is largely determined by how many devices can be maintained simultaneously in a managed environment. A standalone FileWave server can support a limited number of devices. Linux and OS X servers can support between 1000-1500 desktop/laptop devices, and a Windows server can reliably support only about 500 devices (due to a problem with Apache and web services in Windows not playing well together). Because the Filesets sent to iOS devices usually consist of either profiles or URLs to the iTunes/App Store, the size of the traffic flow is lesser, and a FileWave server can support many more iOS devices.

If you plug caching servers into the mix, you now have the capability to greatly expand the flow of Filesets from the main server to the FileWave client devices. Here is an example scenario:

Scenario: Large institutional site with 40 separate locations. Device density from a few dozen to over 1000 client devices per site. Access to Filesets must be on the internal LAN and as well as for external devices. The device map looks like this (total sites reduced for space):

Planning for this deployment can be met with some very basic core principles:

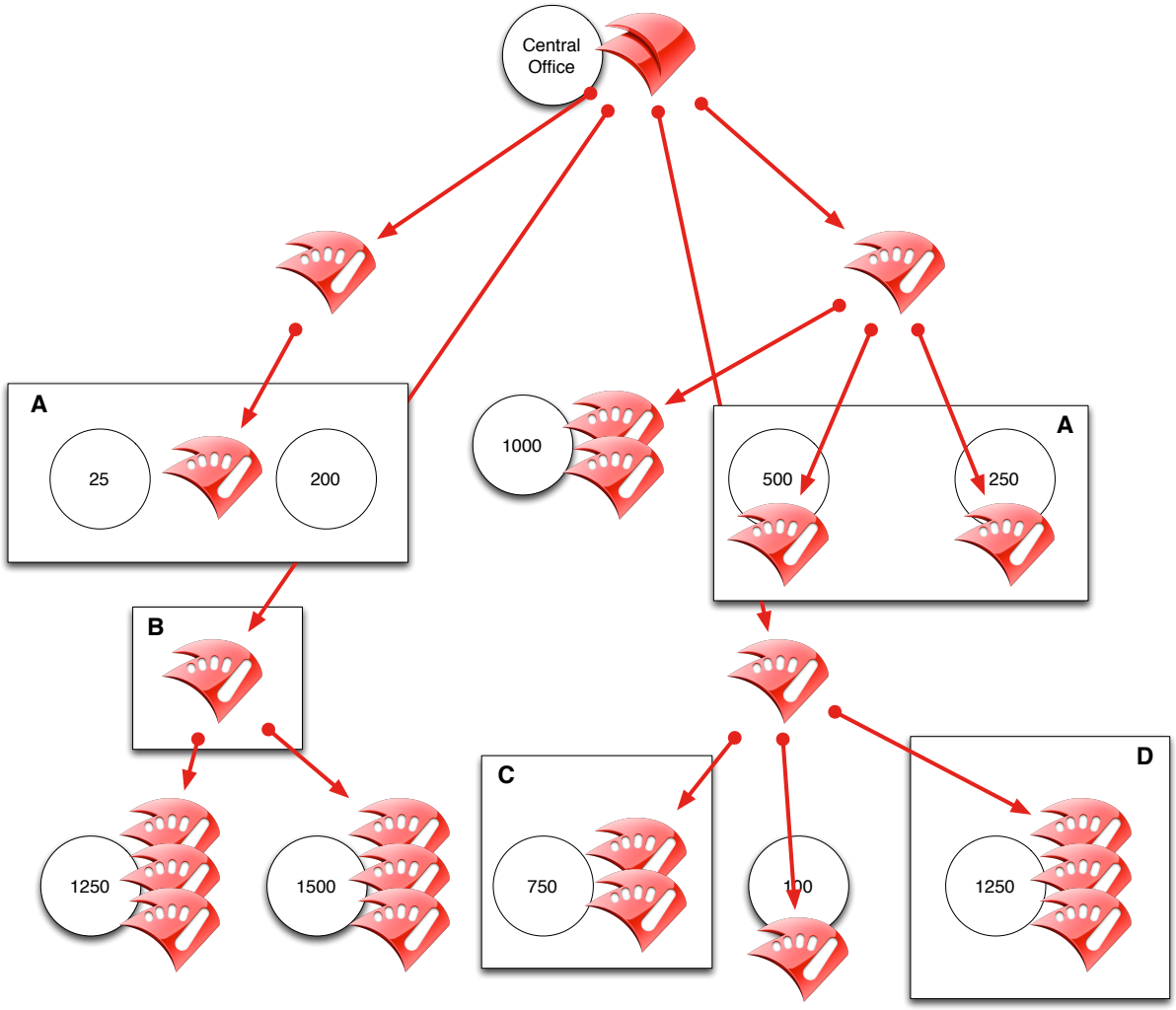
(A) - a booster should be configured for every set of 500 or less devices. For sites / departments / schools with fewer systems could be consolidated to use a single booster, as long as the network throughput is adequate.

(B) - a booster should be configured to support every physical location, such as a building, campus or city. These boosters are for the (A) boosters to connect to. This spreads the load out geographically; which is often important due to varied Internet connections.

(C) - a booster should be configured for every 500 devices, or portion thereof, within a specified site / department / school that has greater than 500 systems. A site with 750 systems should get (500) + (250) = 2 boosters.

(D) - for sites with greater than 1000 devices a load balancing system should be configured. This is a series of boosters configured with unique IP addresses; but assigned the same FQDN for DNS resolution. This creates a “round robin” lookup for devices assigned to the booster “cluster” and provides a much greater load capacity than just one booster per 500 devices. This model can also be used for any configuration of more than 500 systems if you have the resources.

The end result of the configuration model above is that each of the sites has between 1-3 FileWave Boosters, some of which are serving a couple of locations due to lighter loads, and some are consolidated into a “round robin” load balancing cluster. There are a series of boosters directly connected to the FileWave server to begin spreading out the load, then those boosters provide Filesets to the individual site configurations. Following a booster configuration model as shown provides you with a huge load potential and tremendous scalability.



Boosters and Imaging

Since FileWave v9, Imaging has been able to take advantage of Boosters. Images are stored as Filesets, and as such, can be cached on Boosters. When you create an Image Fileset to use in deployment, the Imaging Virtual Server (IVS) handles the network boot drive for either NetBoot or PXEboot; but the Image Fileset that is used in the deployment is stored at the main FileWave server - unless there is a Booster on the subnet where the IVS resides. In that case, the original Fileset will remain on the main server; but the Image Fileset that is used for the imaging process will come from the Booster on that subnet. You can improve imaging performance and latency by adding Boosters onto the Imaging network.

4.2. Booster system requirements

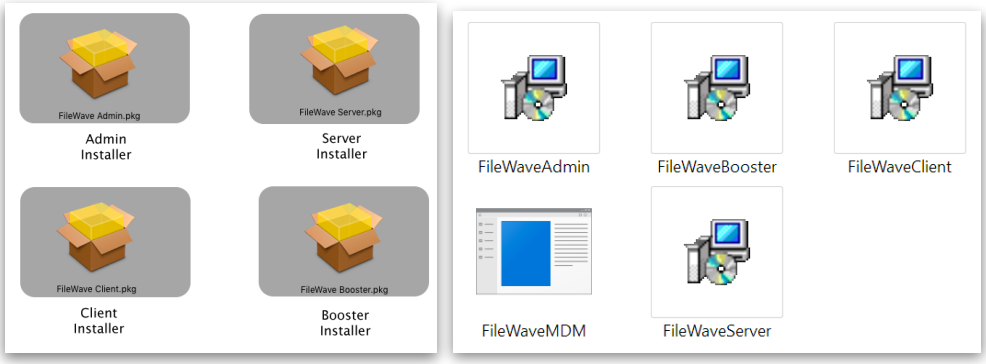
Minimum Config	Macintosh	Windows	Linux
OS	OS X 10.7x86 and higher	Windows 7 & 8, Server 2008/2012	Linux CentOS 5.9 (v7) & CentOS 6.5x86 (v8)
Memory	4 GB	4 GB	4 GB
Space for Install	100 MB	100 MB	100 MB
Hard Drive	80 - 100 GB	80 - 100 GB	80 - 100 GB
Network	Dedicated Interface	Dedicated Interface	Dedicated Interface

FileWave Booster can also be run in a Virtual Machine. **Note: Make sure you have enough space on your hard disk to store the cached Filesets for your FileWave Clients. A booster could conceivably contain a full mirrored set of all Filesets on the main FileWave server.**

4.3. Booster installation

OS X and Windows Booster install

Basic booster installers are included with the FileWave downloads. You run the installer from **pkg/msi** within the installer set.



The FileWave Booster executable resides in one of these platform-dependent locations:

Windows: `c:\Program Files\FileWave\fwbooster.exe`

Mac OS X, Linux: `/usr/local/sbin/fwbooster`

The OS X and Windows versions look about the same at install; but the Windows installer allows more features:

You can repair a booster's settings and delete the booster from within the Windows installer. For both platforms, once you have installed the booster, you will use the **Booster Monitor** to set and edit the preferences for that booster. Booster Monitor is installed into **/Applications/FileWave/**.

Installing the Booster on Linux

Download the latest FileWave binaries for Linux on the following Website:

http://www.filewave.com/support/software-downloads To download the newest binaries, click on the newest version of FileWave, then scroll down until you see Linux installers.

Download the Linux Installers.

Copy the Zip file directly to your Linux Server inside the root folder **/root/**

Login with SSH to your Linux Server (on Windows you will need an **ssh** application, on OS X use **Terminal**), and login as ***root***

Unzip the file with the following commands:

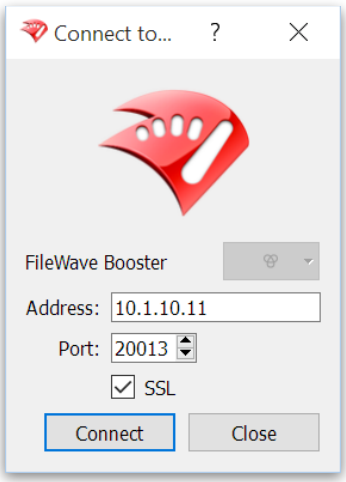
```
cd /root/
unzip yum install -y --nopgcheck fwbooster-*.rpm
```

Answer the install question with **yes**

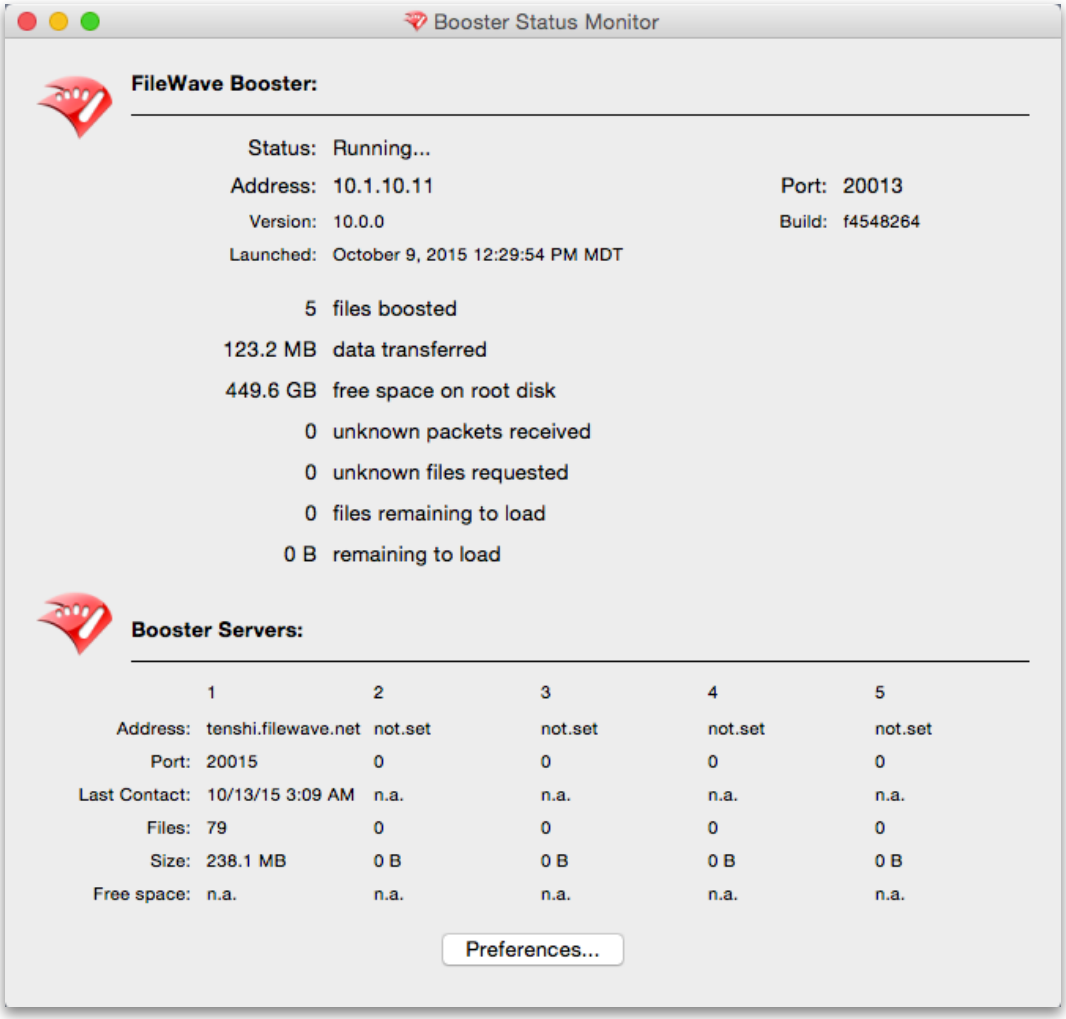
Your Booster is now installed

4.4. Booster Monitor and configuration settings

When you first launch Booster Monitor, it will attempt to connect to the booster at the default address of **127.0.0.1** with the assumption you are running the monitor on the system you installed it on. You can change that address to any valid IP address or FQDN of a booster you have installed. The default password will be "**filewave**".



Once you have connected with your booster, you will see a status window:



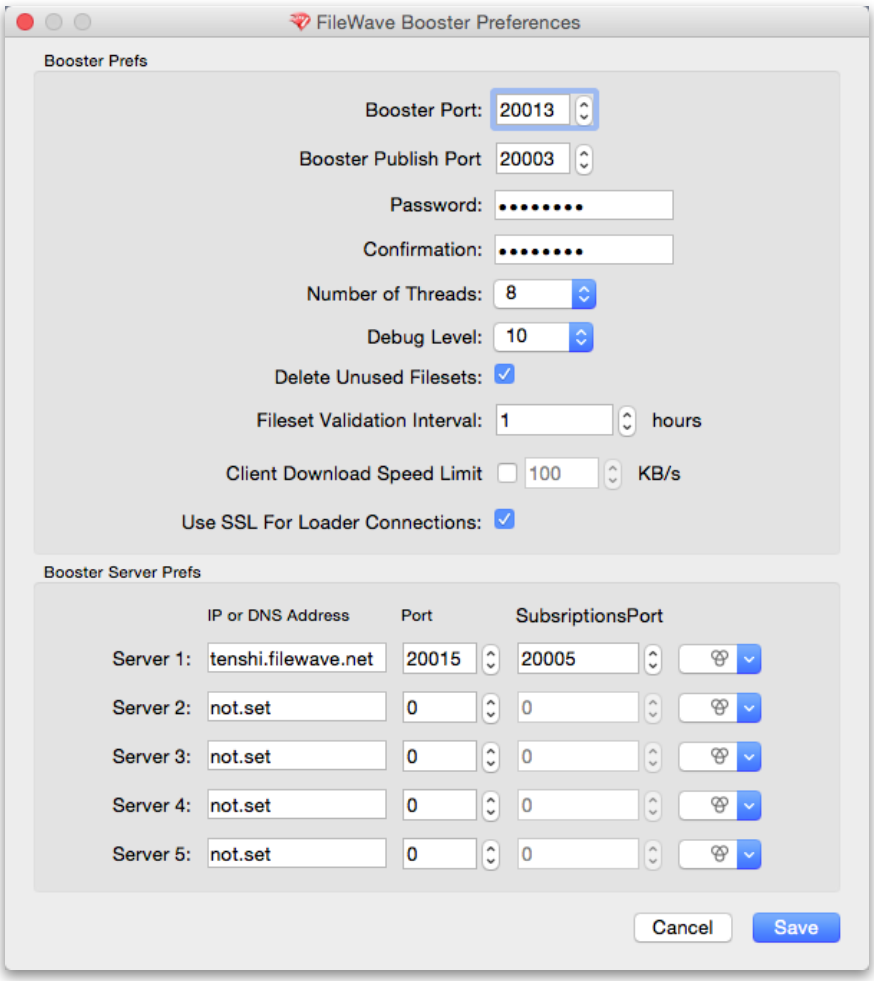
The status window lets you see the current settings and cache of the booster.

You can set the booster preferences to choose how the booster can be reached, and how it works with other boosters, the main FileWave server, and how it handles lots of network traffic.

Booster Prefs

- *Booster Port* - by default, this is **20013**; but you can change it to any valid TCP port that won't interfere with active connections on your network. This port should also be open in the network firewall for external connections.
- *Booster Publish Port* - this setting provides the port for the **remote control VNC relay**. See chapter **5 (Clients)** for more information on the VNC relay and its functionality. Port 20003 is the default and should not be changed. Booster Publish Port defines which port this Booster publishes messages on and should be consistent with subscription ports for all Boosters and clients that connect to this Booster.
- *Password / Confirmation* - the default password is "**filewave**" and you should change it something a little more obscure
- *Number of Threads* - this is the number of threads spawned by the *fwbooster* process. You can choose between 4-128 threads. If you are running a Booster on a client system in the background and only have a few devices connected, the lower value is better. If you are running the Booster on a dedicated device with plenty of ram and network throughput, you can maximize the count.
- *Debug Level* - you will change this value if you are troubleshooting an issue with FileWave Support. The higher the level, the more log files generated.

- *Delete Unused Filesets* - this setting will cause the Booster to delete any Filesets that have been deleted at the main FileWave server. If you leave this setting unchecked, then the Booster will keep every Fileset it has cached. This can come in handy as an ad-hoc backup of all your Filesets for recovery purposes.
- *Fileset Validation interval* - this value determines how often the Booster checks to make sure it has every Fileset that the clients have requested, and that the versions of the Filesets are correct and up to date.
- *Client Download Speed Limit* - you can use this setting to throttle the Booster if the device it is running on would react badly to having all of its network bandwidth used at times.
- *Use SSL For Loader Connections* - this value will alter the port used by the Booster to **20014** and encrypt the traffic **Note: You won't see the Booster Port value change; but the Booster will be on port 20014**



Booster Server Prefs

These settings are where you build your distribution "tree" by assigning where this Booster connects. The best way to set this up is to follow these guidelines:

- Set **Server 1** to be the next booster upstream from your Booster. This may be the main FileWave server, or another booster between this one and the main server. Use the diagram at the beginning of this section as a guide.
- Set the other servers to be boosters in the same general area or location as this Booster. Do not set these to the other Boosters in a DNS "round robin" configuration - that would leave these boosters all asking each other for Filesets none of them may have.
- **If you have not entered the main FileWave server as server 1, set the last value in the table to the main server.** This guarantees that if all the other Boosters never respond, the main server will be contacted.

- The **Subscriptions Port** is used for the Booster to contact the FileWave server to pass along the VNC relay communications. Only the first Booster in the chain provides this service. If the first entry is the actual FileWave server, the port is **20005**. If the first entry is the primary Booster in the chain, then the port is **20003**.

Booster optimization and troubleshooting

Network tuning

The TCP ports **20015** (primary FileWave server) and **20013** (booster) are default values. Make sure you check with your network administrator before changing any of these values. Also, make sure you check your client installer settings to insure they match the port numbers. Tracking down the “why doesn’t anything connect” issue on a large LAN is not a fun exercise.

Setting up DNS Round Robin

For a large deployment, you might want to have several FileWave Boosters acting as a big caching farm. You do this by setting up several systems with IP addresses (10.1.10.6, 10.1.10.7, 10.1.10.8, 10.1.10.9 - for example); then in your DNS configuration, assign the same FQDN to all of these devices (or more technically, those IP addresses to the same FQDN). When you configure your FileWave clients, and any other Boosters upstream, you just plug in the FQDN and the clients will request Filesets from the general name. Over time, all of the Boosters in that caching pool will end up with all required Filesets.

5. FileWave clients - installation, enrollment, configuration, and Apple DEP

The FileWave desktop/laptop client runs on both OS X and Windows devices. When installed, it will allow the client device to maintain contact with the FileWave database. The installer also places the self-service Kiosk into the toolbar or menubar of the client device. iOS devices get their management from the profile enrollment process which will then install the self-service Kiosk. Android devices get their client directly from the FileWave MDM server.

FileWave version 10 introduces some significant changes in the FileWave client. An integrated VNC relay has been built in, allowing the FileWave Admin to contact any FileWave client without worrying about the installation or activation of another remote control process. Apple's Device Enrollment Program changes have been implemented, so institutionally purchased OS X devices can be pre-configured with a hidden local administrator account and a non-admin local account for restricted use. Other new features will be called out within the chapter.

5.1. Understanding FileWave Clients, Groups, and Smart Groups

Client operations

The FileWave Client needs to be installed on every client computer and the FileWave Client needs to be given a unique name so that the FileWave Server can identify and authenticate the FileWave Client. During startup, the FileWave Client reads its configuration file to initialize its settings. The most important setting (aside from Client Name) is the Server address. The Client uses this IP or DNS address to attempt to connect to the FileWave Server.

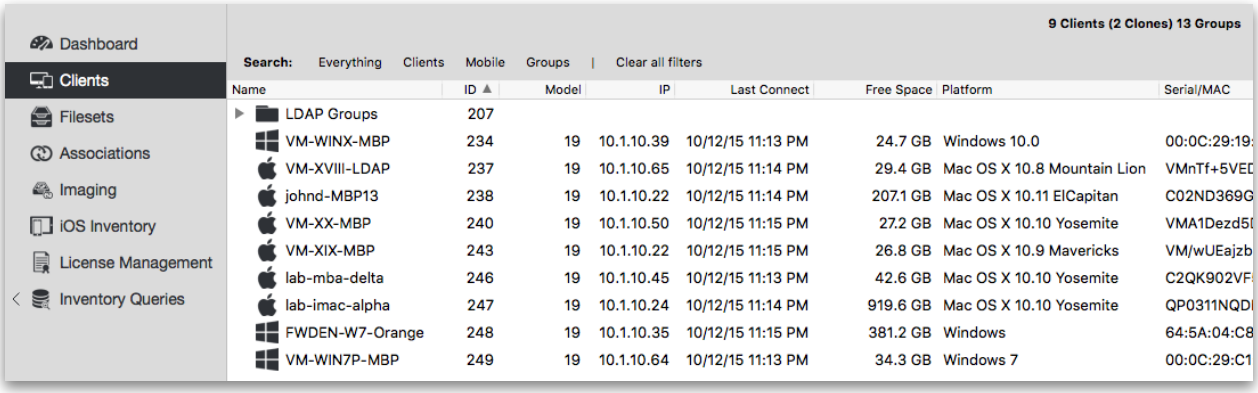
If the address is correct and the Client's name has been accepted on the Server, then the Server will authenticate the Client. If the FileWave Server can't be accessed for some reason, the FileWave Client waits for a specified amount of time (Tickle Interval - default is 120sec, and can be altered as needed) before it tries to connect again. If the FileWave Server is available and the FileWave Client authenticated successfully, then the FileWave Client checks the model version on the FileWave Server. If the model version of the Server is greater than the last value found by the FileWave Client, then the FileWave Client will request to download a manifest for the current model.

The manifest is a list of Filesets that are associated with this Client. The database model version is incremented each time an administrator updates the model. Following a model update, the Client reads the new manifest and executes any actions required. This includes download and activation of Filesets (adhering to any time attributes), deletion, make passive, and update commands for existing Filesets. When downloading files, the Client attempts to download from the first Booster listed in its preferences, or the Server if no Boosters are set.

One other piece of the workflow that may be needed is Apple's Configurator tool. If you are deploying iOS devices and want to supervise those systems, you will be able to use Apple's Device Enrollment Program (DEP) or Apple Configurator.

FileWave Client

The FileWave client itself is a process (fwcld) that runs in the background on a client device. The visible effect of a client is usually the **Kiosk**, our self-service tool. On OS X and Windows devices, the FileWave client is installed using a **pkg** (OS X) or **msi** (Win). On an Android device, the client is downloaded and installed as an **apk** directly from FileWave during the enrollment process. All FileWave clients include the self-service Kiosk, which will be visible when content is assigned to the device for user-controlled install, and can be made permanently visible through a configuration setting.



FileWave Groups

FileWave clients can be gathered into fixed groups for convenience in managing. The groups can be named and populated as needed. The advantage of fixed groups is the ability to associate content with groups versus having to pick out individual clients.

Smart Groups

In FileWave, you can create groups based upon selective criteria, such as “All devices with these fonts” or “Devices that are not running the latest security update.” A smart group allows you to isolate specific devices and perform actions on them as part of your management workflow.

Groups and Smart Groups are discussed in much greater detail later in this chapter, as well as in the **Inventory** chapter.

Clones

Instead of assigning FileWave clients to a single group, you might want to have a device assigned to several groups - such as “Building 7” and “Admin Dept” at the same time. Creating clones can make this possible. A clone is essentially an alias of the client. A device can have several clones. All assigned to different groups. Clones can have content (Filesets) associated with them, just as clients can. More information is provided later in this chapter on how clones, clients, and groups all interact.

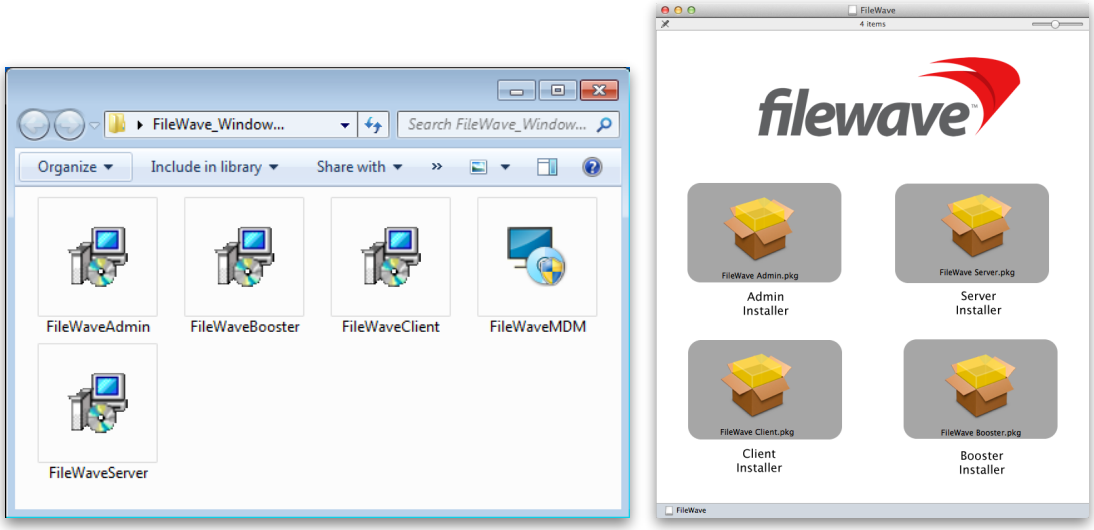
5.2. Desktop/laptop Client Install and Configure

The FileWave Client runs on both OS X and Windows devices with the following requirements:

	OS X	*Windows*
Version	*10.7*, 10.8 and higher (Intel only)*	*Win XP*, Win 7, 8, 10*
Memory	*2GB*	*2GB*
*Disk Space***	*100MB*	*100MB*
	** Legacy support only*	*** Minimum for client only*

Downloading the FileWave client installer

The FileWave client installer is available as part of the FileWave bundle for the specific operating system. The most current version, as well as selected older versions, of the installer are located on the FileWave web site under the *Support* tab: http://www.filewave.com/index.php/support/ For the devices mentioned under *Legacy Support,* you will need to install the FileWave v9.1.2 client, or keep any older client already installed.

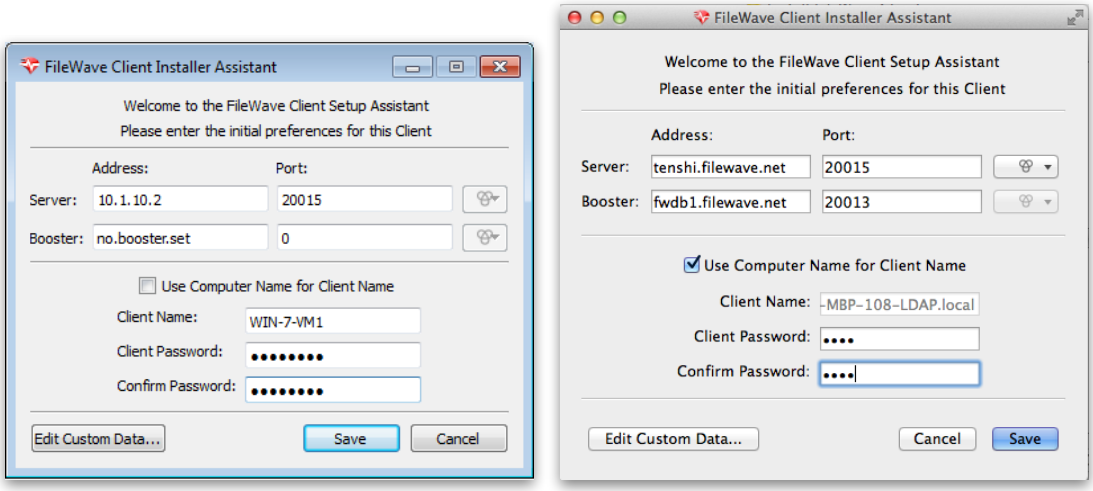


You should download all installers you will need for your deployment at the same time. They can be stored on a file server, or on a flash drive in Windows format for cross platform compatibility (OS X systems can read Windows-formatted drives without additional drivers).

Note: The installer instructions for the Linux server and booster are also located on the same page of the web site. Server installation instructions are covered at the beginning of section 3. There is no Linux client.

Installing the FileWave client

Client installers for both OS X and Windows use the same general dialogs. You will need to read and accept the license agreement, and you will be presented with a dialog window asking you for specific information to connect your client.



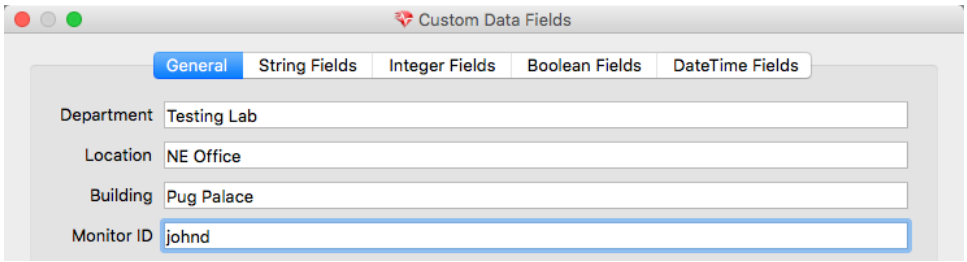
Installation settings

- *Server address / port* - Enter the IP address or FQDN of your FileWave server. Enter the TCP port number for the client to communicate with the server (default is 20015 or 20017(SSL)).
- *Booster address / port* - If your client is going to get its filesets from a booster, enter the IP address or FQDN of the FileWave booster. Enter the TCP port number for the client to communicate with the booster (recommend using 20013 or 20014(SSL) - do not use values below 1024). If you choose port 20015, the client will report directly to the FileWave server.

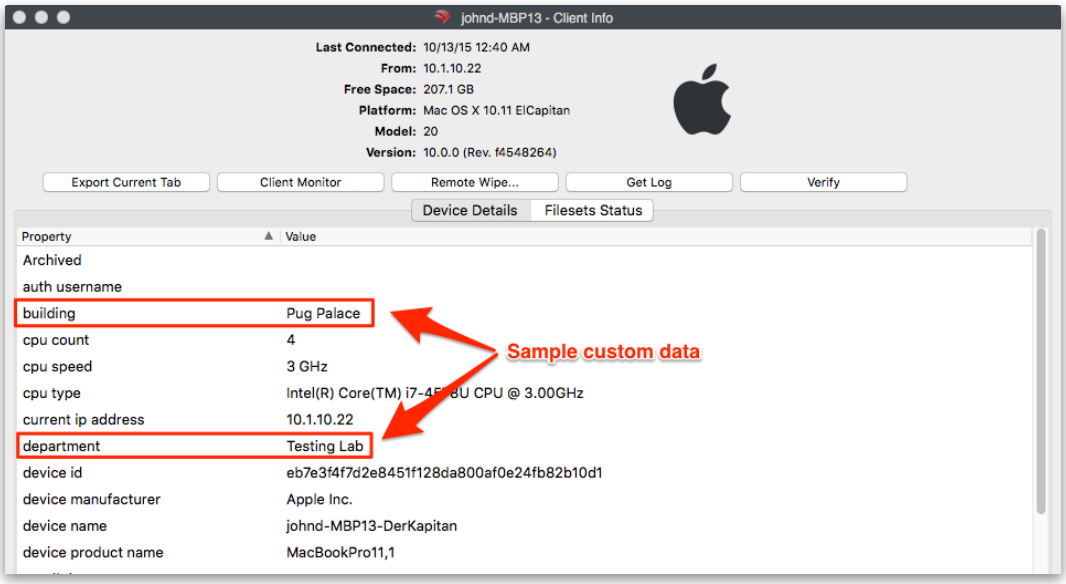
Note: More on working with FileWave Boosters in chapter 4.

- *Use Computer Name for Client Name* - this box allows you to use the device's computer name as its FileWave client name.
- *Client Name* - enter a valid name based on any criteria you have for your deployment. It is recommended that you do not use special characters in the client name. Dashes, underscores, and slashes are ok.
- *Client Password / Confirm…* - enter a password for the FileWave Admin to connect to the client. This does not need to be an administrator password that you are using for that device locally. **Note: You must provide a password in order for the Remote Control/VNC relay to function.**

Edit Custom Data…



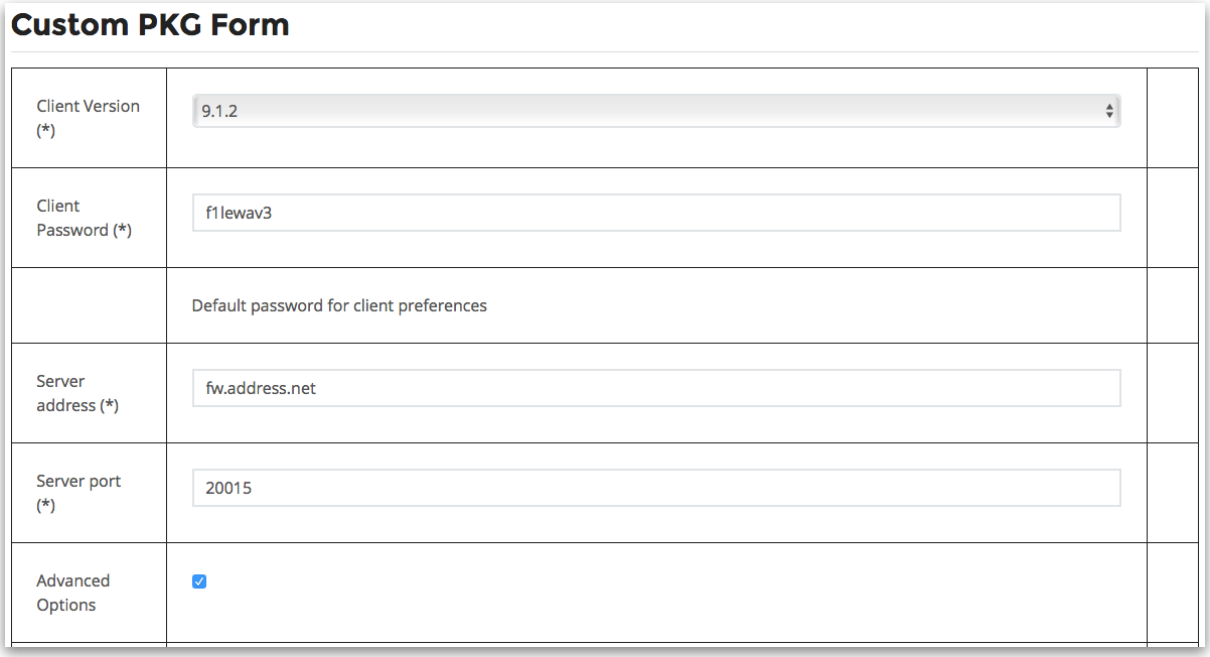
The custom fields consist of a series of optional Inventory data fields that can be used to provide more detailed information on any client. This information cannot be set in the automated installer, and must be applied manually. The information provided will be displayed as part of the **Client Info** in the **Clients** pane of the main FileWave Admin window by right-clicking on any client and selecting the **Client Info…** menu item, as well as in **Inventory queries**.



Automating installation with a custom client installer

While the manual method of running the installer and entering all of the connection information works fine for small deployments, FileWave provides you with the ability to perform larger scale installations. A customized client installer is available through the FileWave website: http://www.filewave.com/support/custom-pkg (for OS X) and http://www.filewave.com/support/custom-msi (for Windows)

The customized client for OS X is required for MDM/DEP support and is required to be uploaded as part of the Mobile preferences in FileWave Admin.



Items with an asterisk (*) are required fields. Note that the default port is 20015. If you want SSL, set it to 20017.

Advanced Options

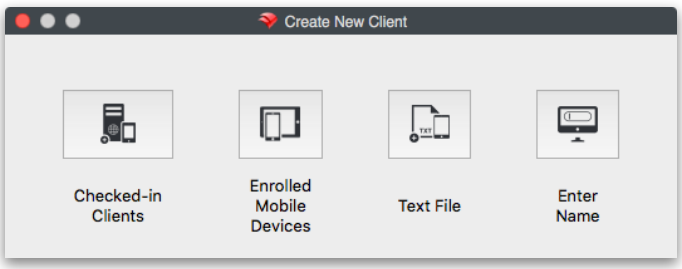
Advanced Options	☑	
Booster address (*)	no.booster.set	
Booster port	20013	
Enable SSL	☐	
Tickle Interval (seconds)	120	
	Tickle interval is the frequency on which the client phones the server for new jobs/installations. A higher value is recommended when managing over 2000 computers (example: 240 seconds)	
Don't sync	☐	
	If this is checked, "Sync Computer Name" will be disabled. You will need to create a static name using the options below:	

The custom installer does not ask the user for any device specific information, and can be distributed through several means:

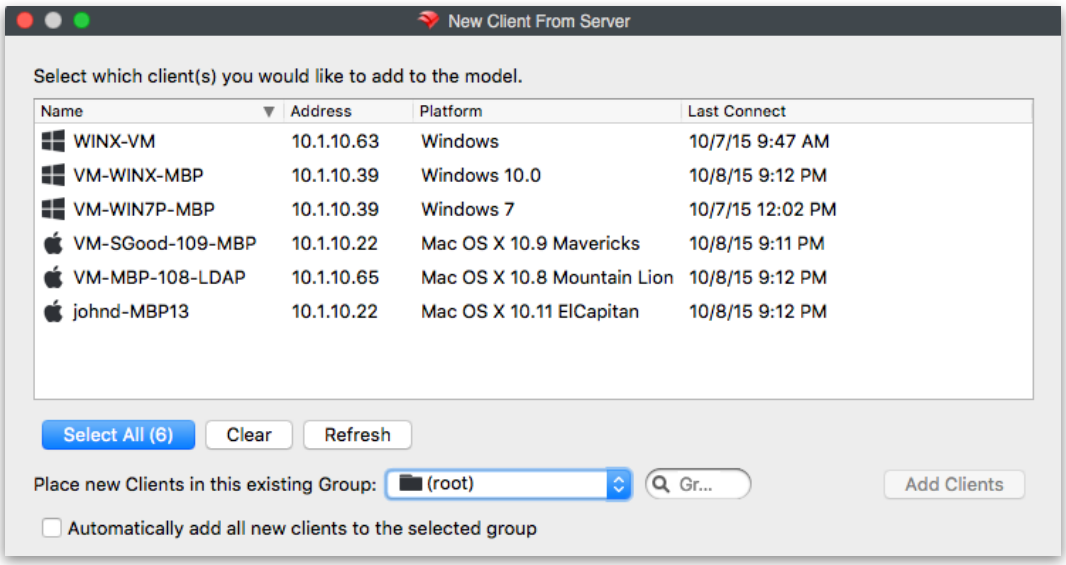
- Apple's Device Enrollment Program (DEP) uses the custom installer to enroll institutionally purchased devices automatically with your FileWave server (See the DEP section later in this chapter for more details).
- Add the custom installer to an image set when doing direct or network mass imaging (See the Imaging chapter of this manual for more details).
- Use a remote installation tool, such as Apple Remote Desktop, to distribute the custom installer to large numbers of existing devices.
- Use a 3rd party imaging tool, such as DeployStudio, to build a custom client set.

Note: FileWave provides "recipes" of possible deployment workflows for the custom installer on our website.

5.3. Enrolling desktop/laptop clients



Desktop clients will show up in the ***New Client From Server*** window once the FileWave client on the device checks in with the designated FileWave server specified in the client settings. Those settings are either manually entered when installing the client, or specified when you request a custom client installer from FileWave support.



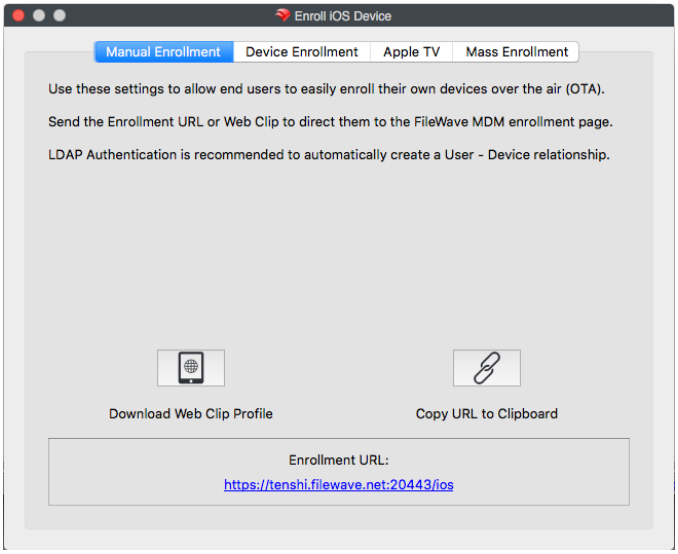
You can select clients and assign them to a group, or leave them in the **root** group. You can always place clones of the clients into any groups you wish to administer them from. You may also pre-assign clients into a specific group by checking the ***Automatically add all new clients to the selected group*** checkbox. If you are going to be creating new clients in waves, you can change this selection between each new batch of clients.

5.4. Enrolling mobile devices

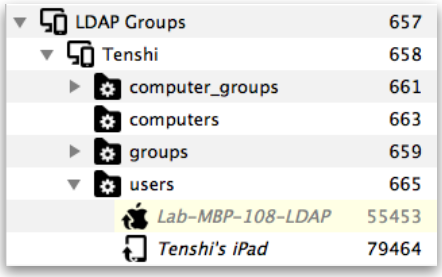
Mobile devices (iOS and Android) can be enrolled to become clients on your FileWave server manually, or through an automated process, such as Apple Configurator. Apple iOS/OS X devices can also be enrolled through Apple's **Device Enrollment Program** (DEP). An enrolled device will contain a FileWave certificate and MDM profile that will allow you and your other administrators the ability to manage and maintain that device. In a BYOD deployment, you will normally perform enrollment through access to a web page generated by your FileWave server. In a 1:1, you might pre-install the enrollment profile onto your devices before handing them over to the end user. For the institutional deployment model, you will probably want to preconfigure the device(s) and, in the case of iOS, supervise the devices in Apple Configurator.

Web-based enrollment - iOS

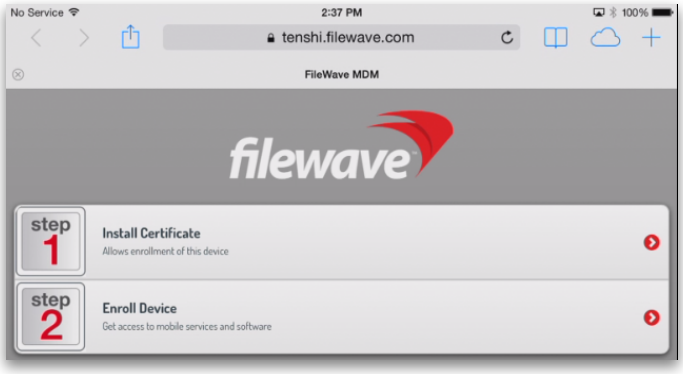
For your users to enroll their mobile devices over the Internet, they will need a URL that points them to your FileWave MDM server. You can find that URL in FileWave Admin under **/Assistants/Enroll iOS Device:**



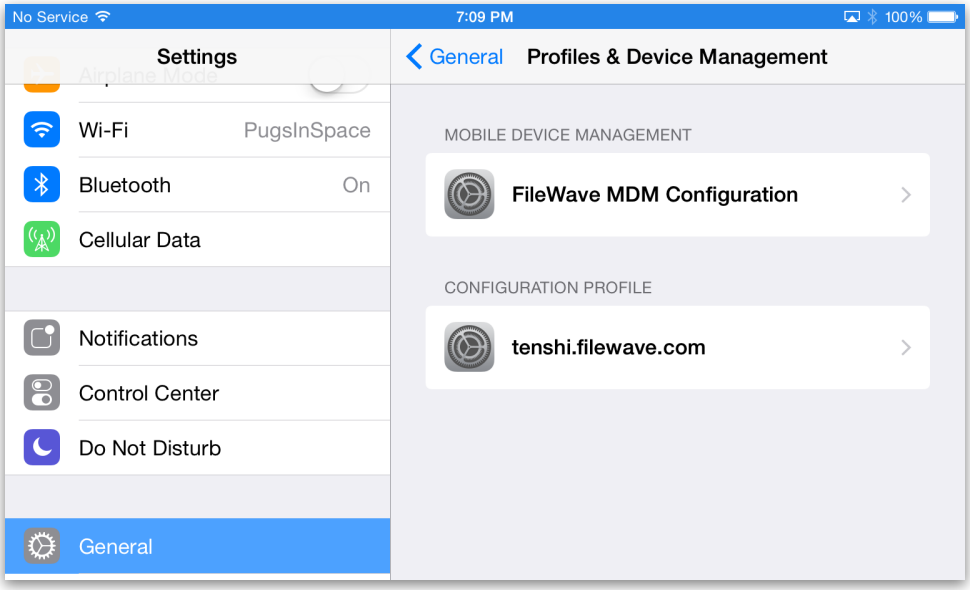
You can create a Web Clip with that URL embedded or copy the URL to the Clipboard and email it to your end users. When they go to that URL on their mobile device, they will get instructions on how to properly enroll their device with your server. Having your FileWave server linked to your LDAP server allows the users to authenticate as themselves, instead of as a generic user account. This provides the benefit of having the user's LDAP record link its account information to the device. Another result of this is that the user can be automatically invited to link their AppleID with your FileWave VPP service.



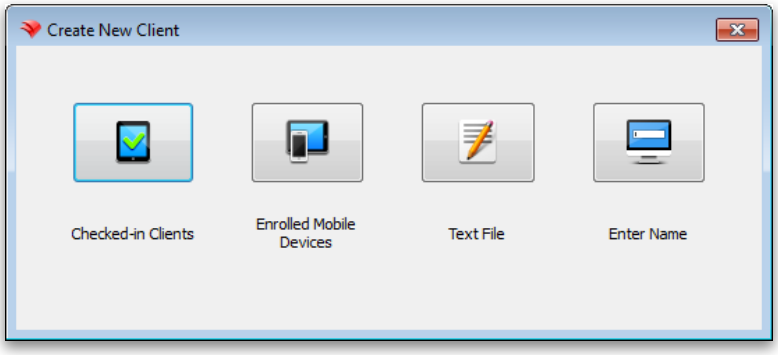
The user is presented with a dialog asking them to install an MDM server certificate, then enroll their device. The second step is when the user will be asked to authenticate - and this is where LDAP integration comes in handy.



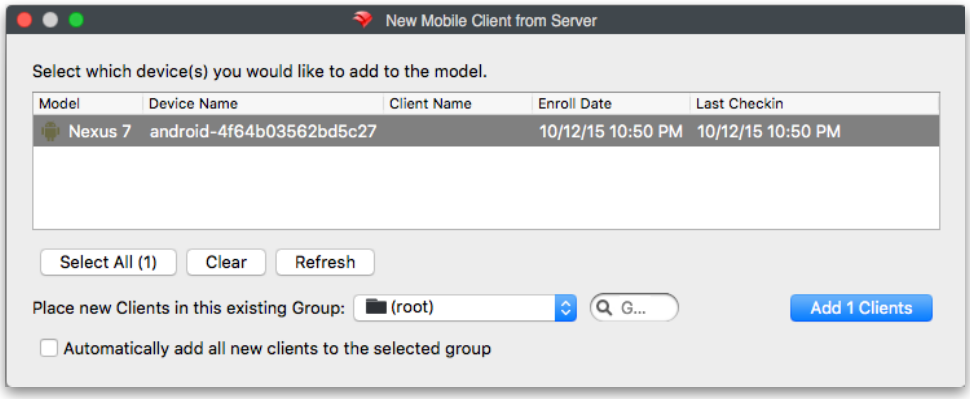
Once the user has completed these two steps, the device will display the new profiles that have been installed:



If the user's device is not yet a FileWave client, it will need to be captured in FileWave Admin. You will go to the **Clients** pane, select **New Client** from the toolbar. That will give you this window:



Then select **Enrolled Mobile Devices** and you will get the list of all mobile devices that have performed an online enrollment, or have been activated by Apple Configurator:



The device(s) can be automatically added to an existing client group, or you can manually add them to group, if desired. If you have devices set to be automatically added to a specific group, then you will just see them appear as members in that group.

Note: Unless you want all devices that enroll during a specific timeframe to end up in a designated group, you might leave automatic placement off. You should also think about using clones instead of the actual device client as members of any groups.

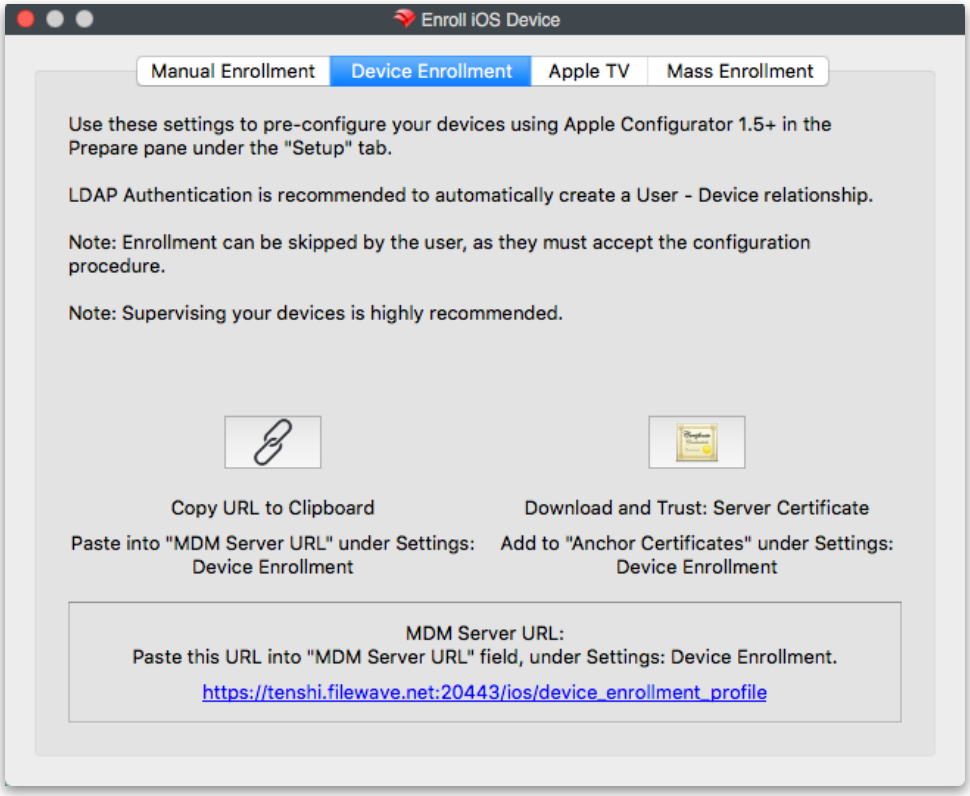
Automatic or Forced Enrollment - iOS

Another option for enrollment is using an embedded enrollment profile as part of a mobile device configuration. Apple Configurator allows you to import a FileWave MDM enrollment profile, which will then be used to assign the device to your FileWave MDM server.

Instructions are included here for Apple Configurator v1.7 and the new Apple Configurator v2.0. Some of the dialogs are slightly different; but the general setup follows the same guidelines. AC2 is much more streamlined and supports multiple devices simultaneously.

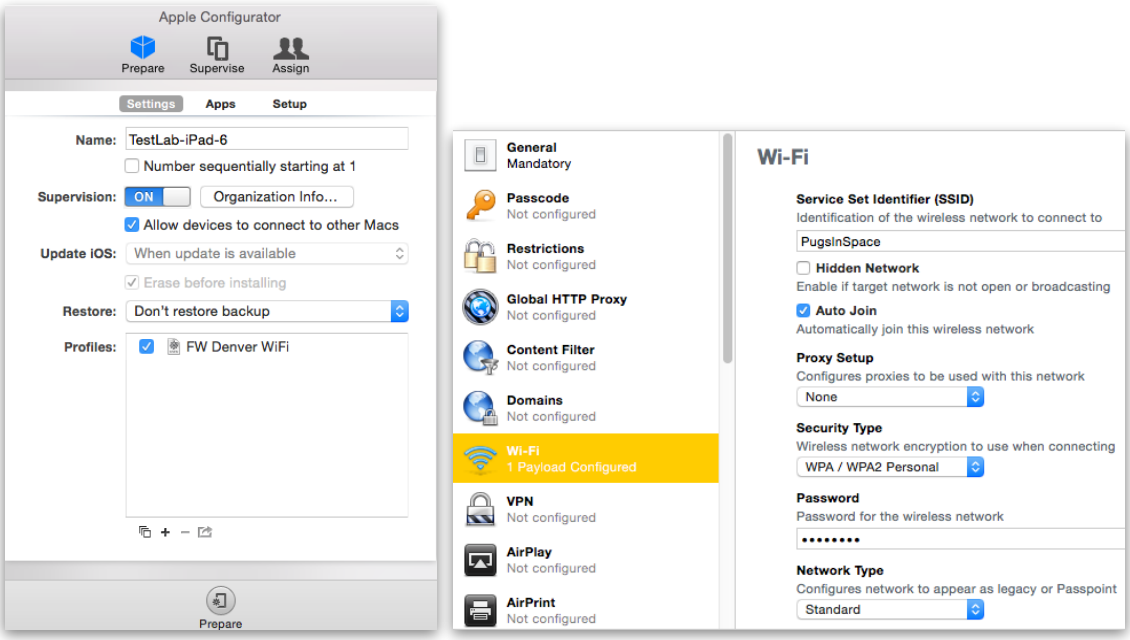
Single device enrollment

In FileWave Admin, under **/Assistants/Enroll iOS Device**, you select **Device Enrollment**:

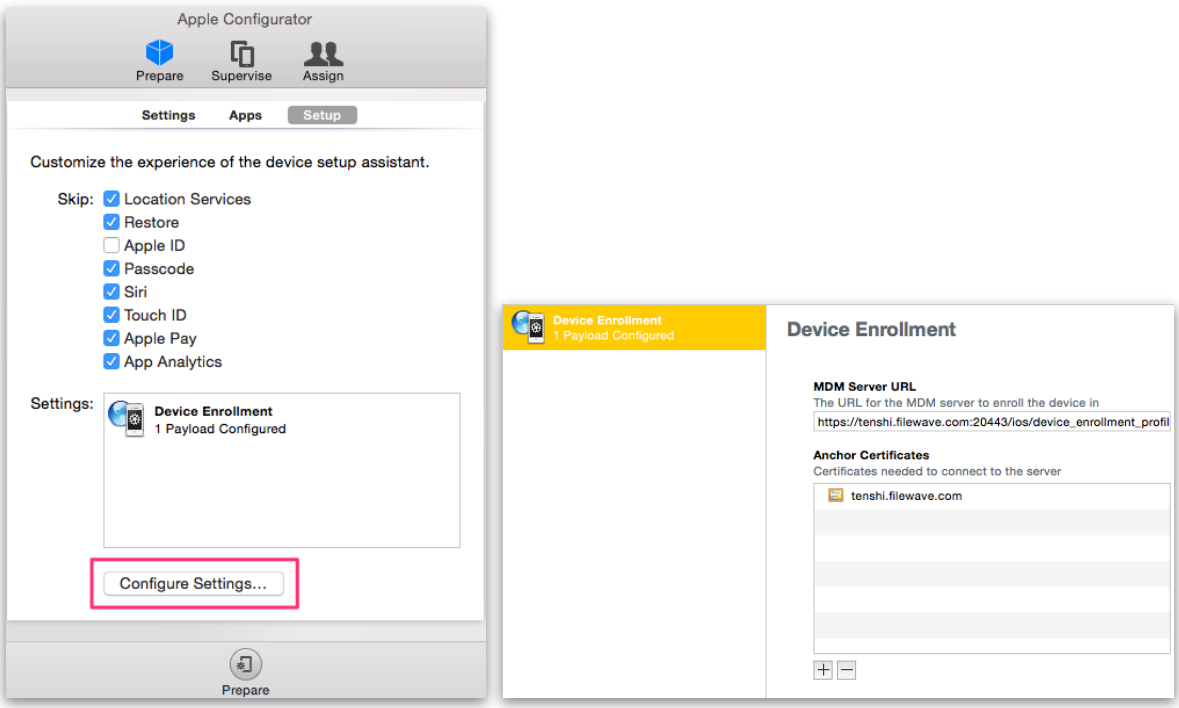


Apple Configurator v1.7 screens

The screens below match the steps you would take within Apple Configurator. You copy the MDM server URL, download and trust the server certificate, and paste the MDM server URL into the designated field in Configurator.



Apple Configurator v1.7



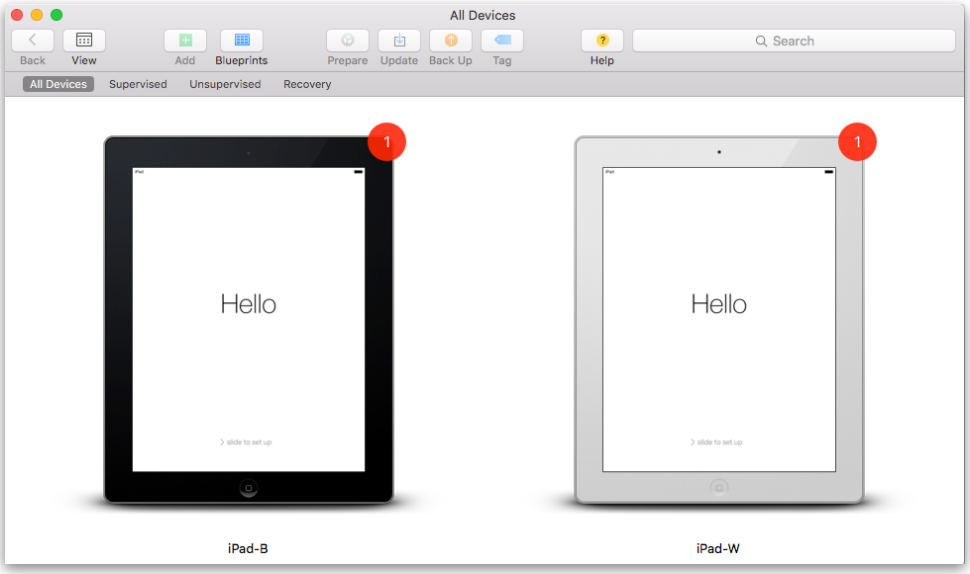
Apple Configurator v1.7

You should also create the much needed WiFi profile - since the goal is to have these devices come up on the network a FileWave clients. At this point, the device(s) will show up as enrolled clients for inclusion into FileWave groups.

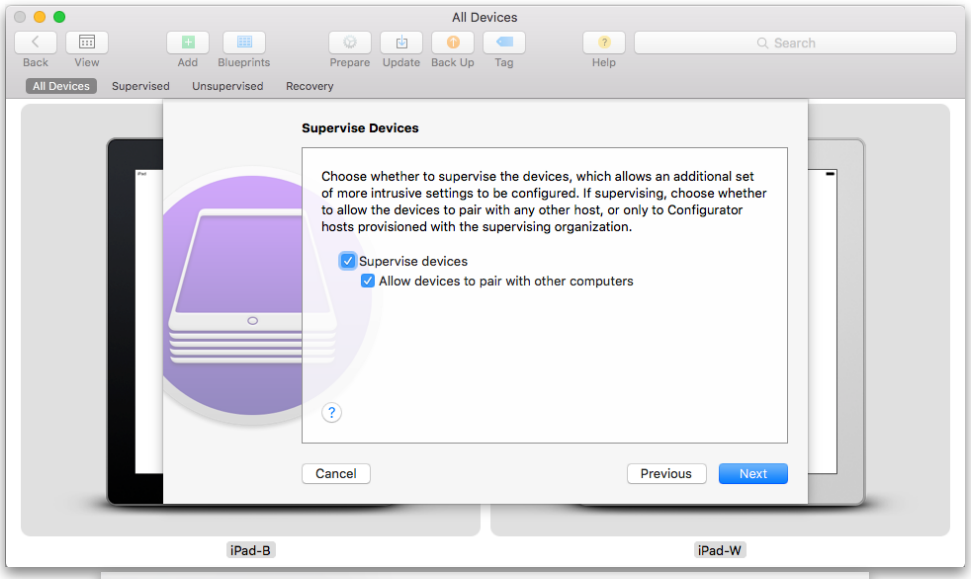
Note: Make sure you use Keychain Access to "trust" the server certificate. When you download the certificate and add it to Configurator, Keychain Access will ask if you want to trust it. If you skip that step, this process will not work.

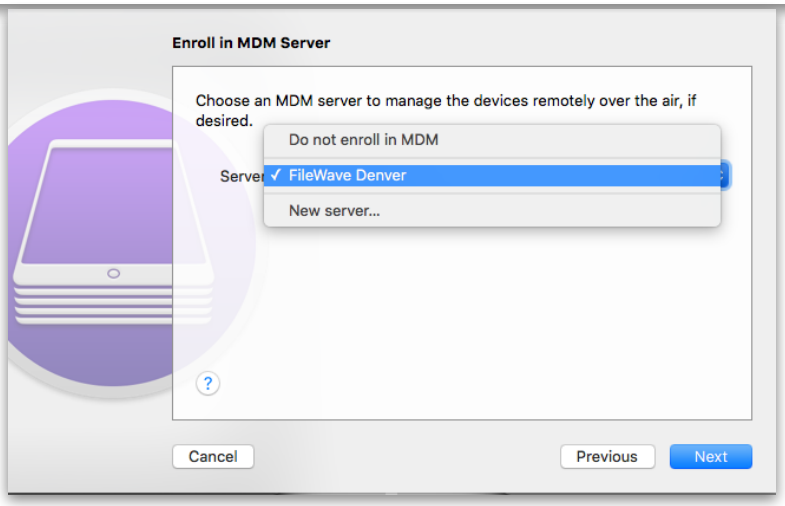
Apple Configurator v2.0 screens

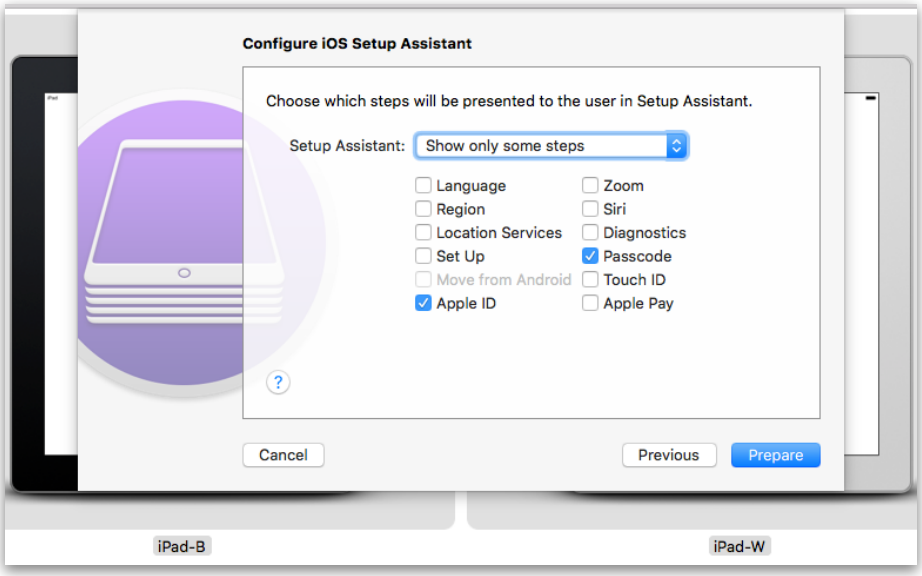
The following screenshots show the same process as above; but done from the view of the new Apple Configurator version 2. Key differences include being able to work on multiple devices at the same time.



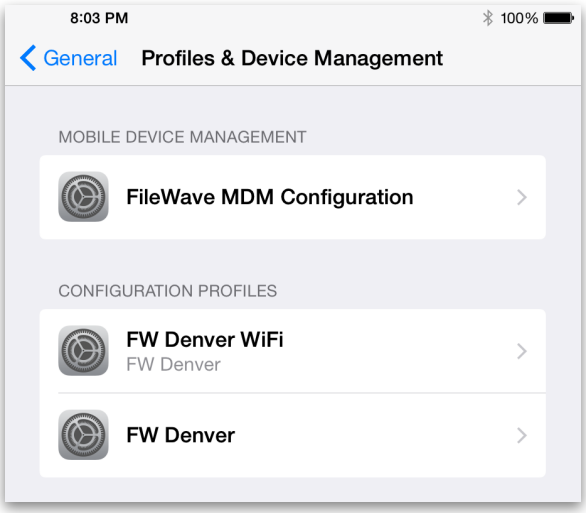
AC2 allows you to configure sets of devices, re-installing iOS, setting up profiles, and assigning to an MDM server.


All Devices
Back
View
Add
Blueprints
Prepare
Update
Back Up
Tag
Help
Search
All Devices
Supervised
Unsupervised
Recovery
Supervise Devices
Choose whether to supervise the devices, which allows an additional set of more intrusive settings to be configured. If supervising, choose whether to allow the devices to pair with any other host, or only to Configurator hosts provisioned with the supervising organization.
Supervise devices
Allow devices to pair with other computers
Cancel
Previous
Next
iPad-B
iPad-W


Enroll in MDM Server
Choose an MDM server to manage the devices remotely over the air, if desired.
Do not enroll in MDM
Server
FileWave Denver
New server...
Cancel
Previous
Next


Configure iOS Setup Assistant
Choose which steps will be presented to the user in Setup Assistant.
Setup Assistant:
Show only some steps
Language
Region
Location Services
Set Up
Move from Android
Apple ID
Zoom
Siri
Diagnostics
Passcode
Touch ID
Apple Pay
Cancel
Previous
Prepare
iPad-B
iPad-W

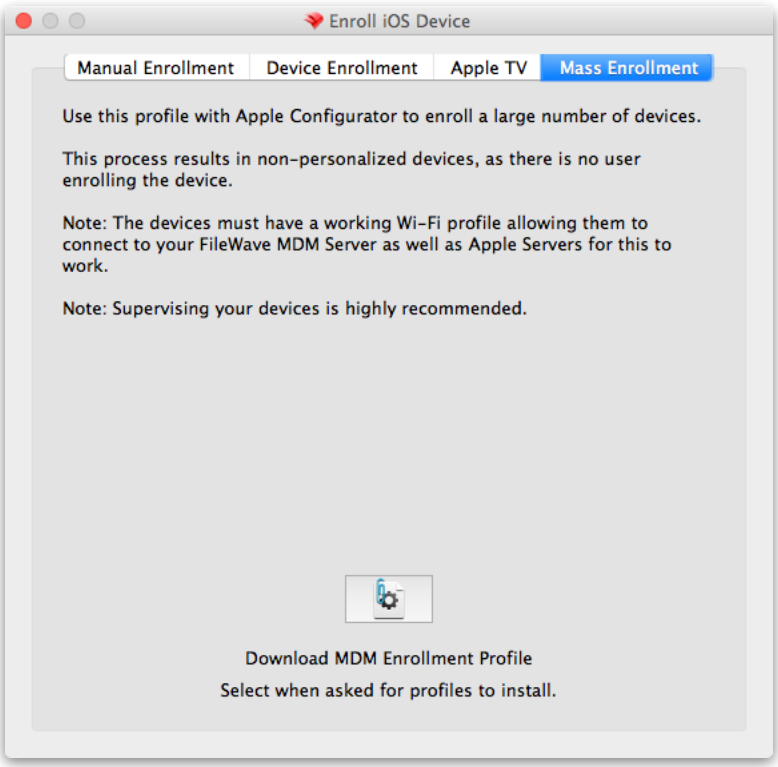
Once you have enrolled your mobile devices, and added them as clients, you should see a set of installed profiles like the ones below.



For additional information on setting up Apple Configurator, see help.apple.com/configurator/mac/1.7/# .

Mass Enrollment for iOS

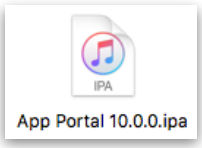
You can set up Apple Configurator v1.7 for bulk enrollment of preconfigured iOS devices by using this option in the ***Enroll iOS Device*** assistant. The device **must** be connected to WiFi already before this process will work. If not, then make sure you add a WiFi profile to your Apple Configurator setup. This process is built into AC2 using the steps above, since it already supports setting up multiple devices simultaneously.



In this case, you would just download the MDM Enrollment profile, import it into Apple Configurator v1.7, and apply it to a set of iOS devices that were cloned with wireless settings, or a profile, already in place.

FileWave Enterprise App Portal for iOS

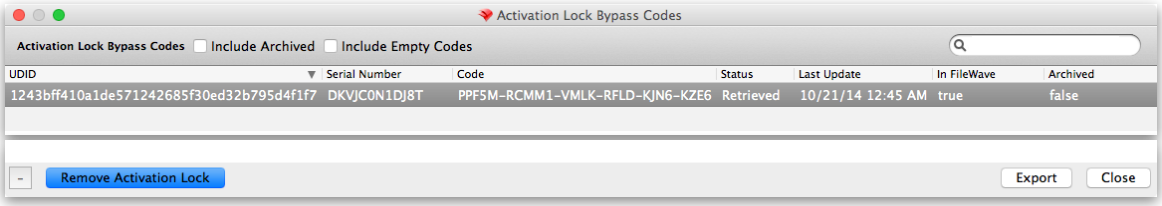
Starting with FileWave version 8.5, iOS devices running iOS 7 and greater use a native iOS App Portal (Kiosk) instead of the web clip. iOS 8+ devices must use the App Portal. Instructions on how to deploy the App Portal are covered in chapter **6** on mobile Filesets. When iOS devices are enrolled, they get the web clip version of the Kiosk. The new Enterprise App Portal automatically replaces the web clip and provides a more robust, responsive self-service tool.



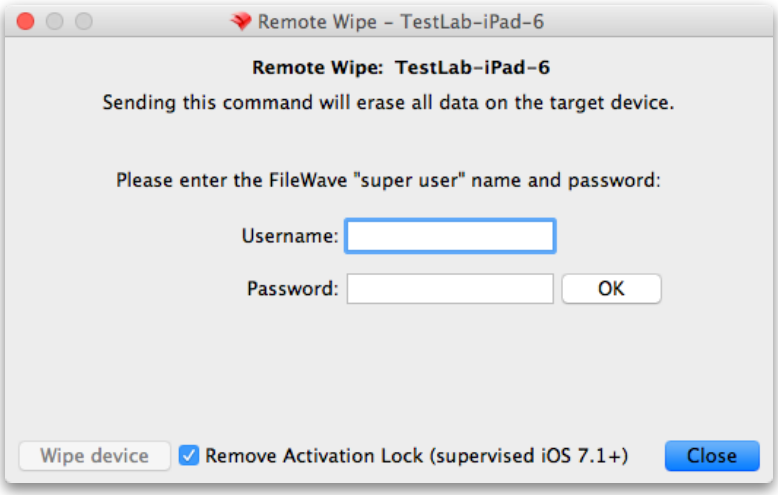
Activation Lock Bypass

With the introduction of iOS 7, device users have been able to enable a feature known as *Activation Lock* - which is linked to *Find My iPhone*. This feature ties a device to a specific AppleID. In order to activate a device with an Activation Lock after a wipe or reset, the AppleID credentials of the locking account are required. Where this can become problematical is having a 1:1 deployment where a user sets the Activation Lock on their device, then leaves without de-activating the lock. Prior to iOS 7.1, this issue was limited to unsupervised devices, since supervision inhibited the activation lock. Apple has provided a process now to supervise a device, yet still provide the activation lock - as well as a way to deactivate the lock when necessary.

FileWave Admin contains a new Assistant labeled **Activation Lock Management.** When an iOS device is enrolled in the FileWave MDM, its activation lock is stored in the FileWave server.



If a device is sent a remote wipe command, the activation lock can be disabled at the same time.



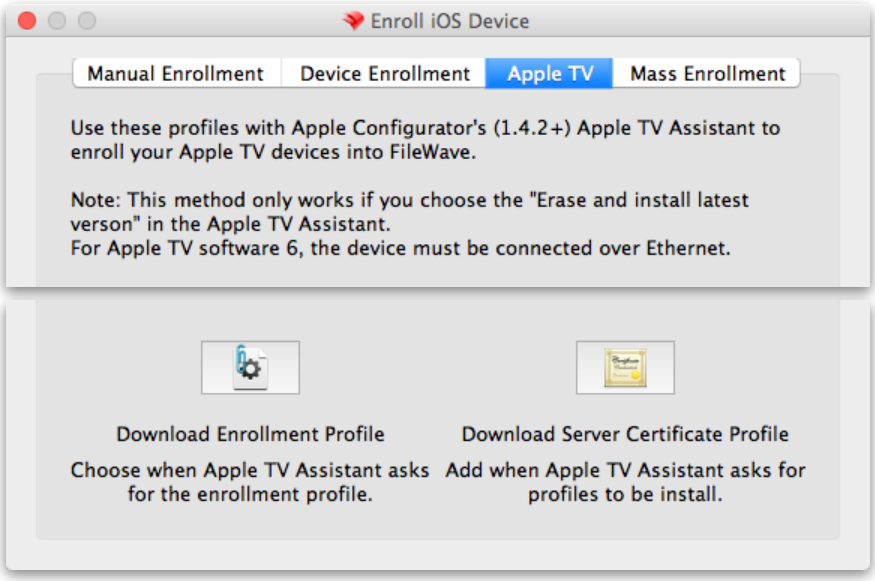
These lock bypass codes are stored in the FileWave server, and remain even when the device has been un-enrolled. The information concerning devices with bypass codes is even provided in Inventory queries. Best practice is to

maintain the codes for institutional devices, regardless of the device's enrollment status, as a safety measure. If the device is no longer used, or taken offline, do **NOT** delete the device from your FileWave database, just archive the device. Once the device has been deleted, the activation lock information is deleted also.

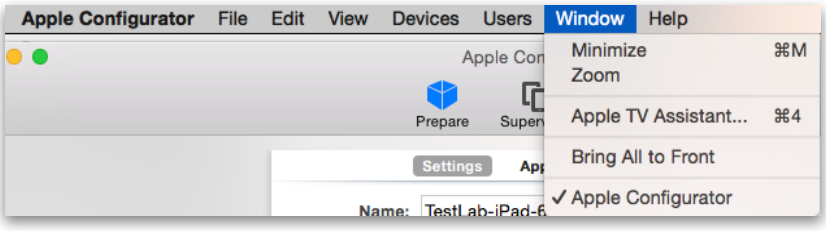
Note: In order to access the Activation Lock Bypass controls in FileWave Admin, you must login as the superuser (fwadmin, by default).

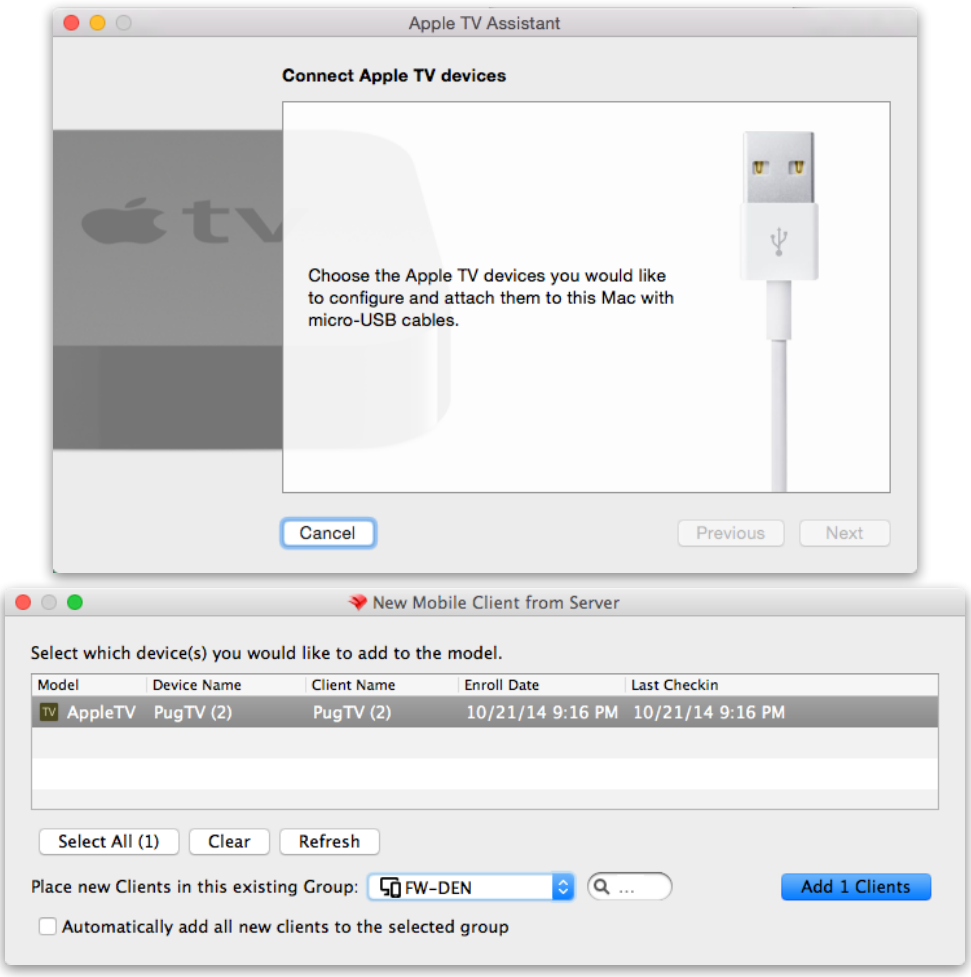
5.5. Enrolling AppleTV into FileWave MDM

FileWave now supports the option of configuring and enrolling AppleTV's into the FileWave MDM. This is done through the ***Enroll iOS Device*** assistant by running the *Apple TV Assistant* in Apple Configurator. You can import the Enrollment Profile, a WiFi profile (if needed), and the Server Certificate Profile. The AppleTV will be rebuilt as a managed device in your FileWave MDM.



Just follow the instructions in Apple Configurator to set up basic management of your devices.

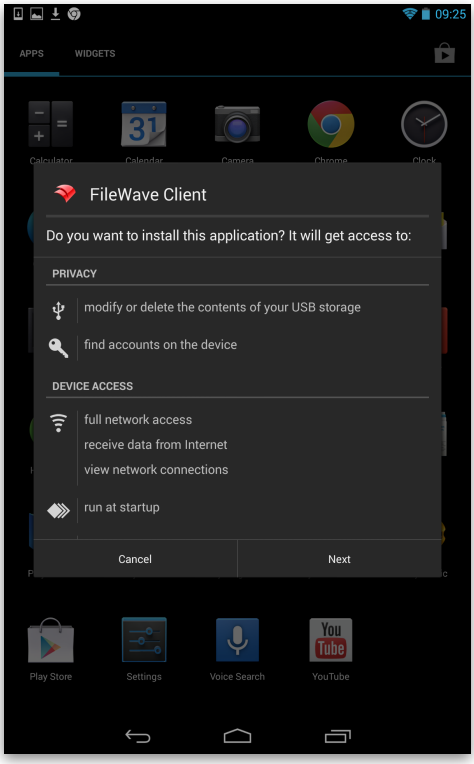


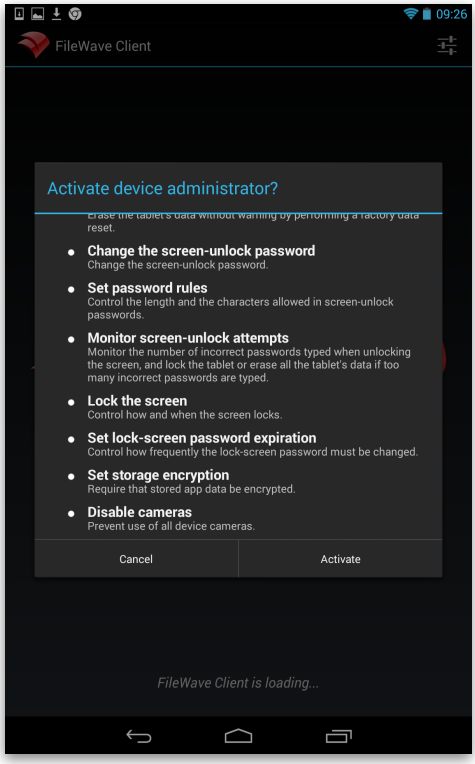


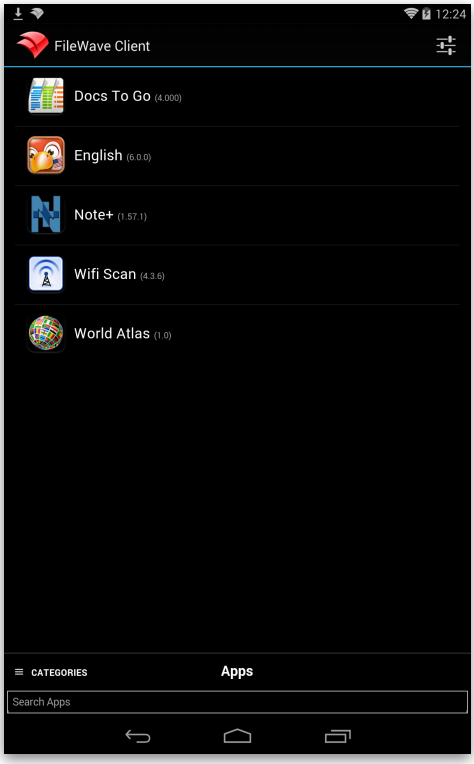
5.6. Installing the Android client

With FileWave, you have Android support for installing applications and Inventory. The Android client installation process resembles the iOS workflow, with a few exceptions. The basic steps are as follows:

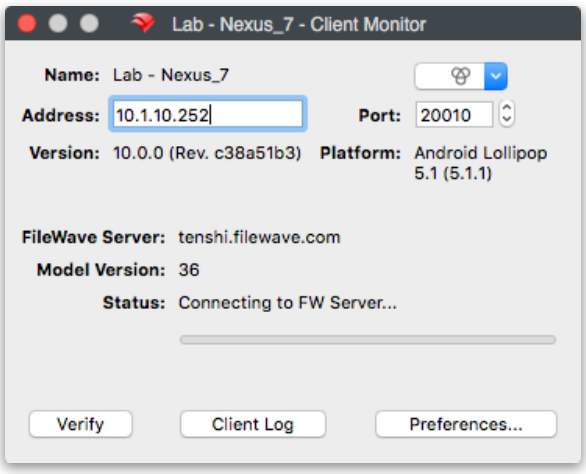
- Connect to the FileWave Android portal on your server (*https://<your_FW_MDM_server>:20443*)
- Download and install the Android client **.apk**
- Enroll your Android device
- Associate applications in **apk** format to the device
- User installs applications from within the Kiosk





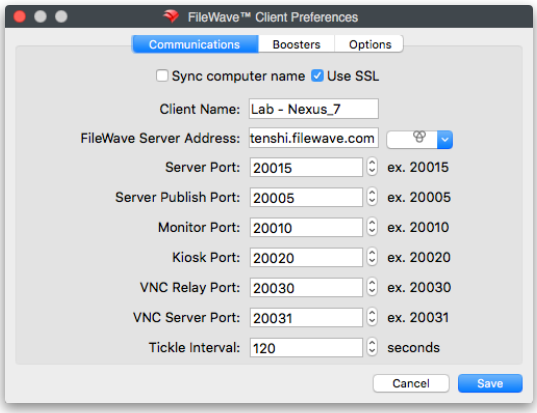


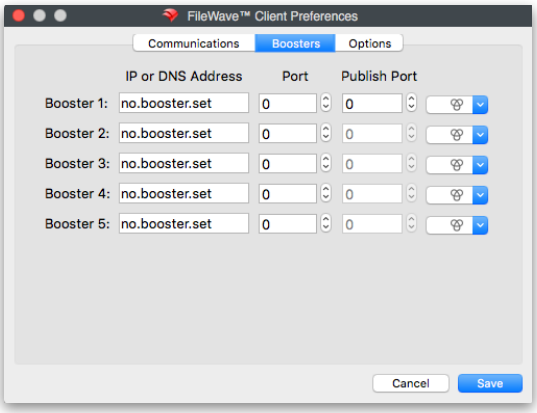
The actual workflow will vary depending on your specific Android device. Essentially, you will connect to the FileWave MDM server to get the client installer, install that client, and enroll your device. Once that is done, you will be able to view your device in Inventory, manage it and deploy applications with Filesets.

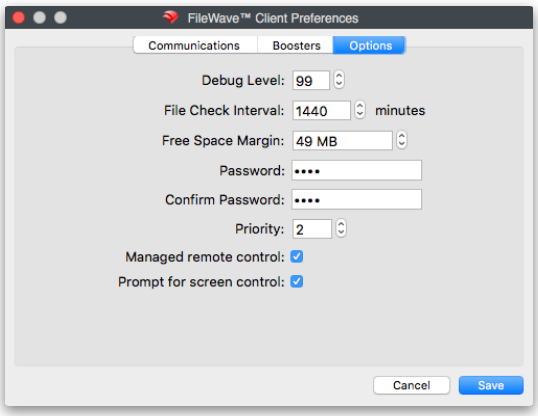


Android devices can be assigned boosters through the **Preferences…** in the **Client Monitor**, or through a *SuperPrefs* Fileset. The Android client doesn't have a customizable installer like the desktop/laptop clients do; so you can't designate boosters during the enrollment process.

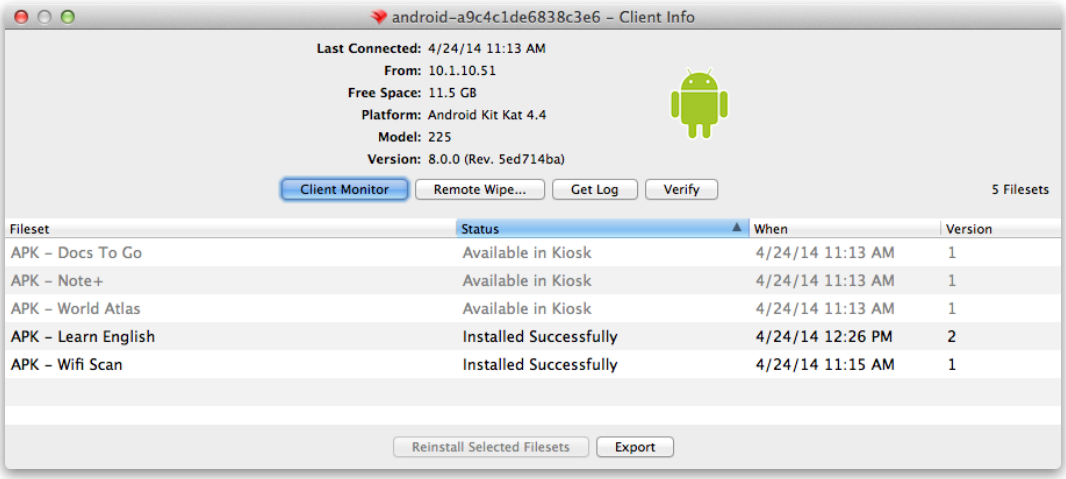
Once the Android device is reporting to the FileWave server, you can select the device in the **Clients** window, choose **Client Monitor** from the toolbar, then click on **Preferences…**







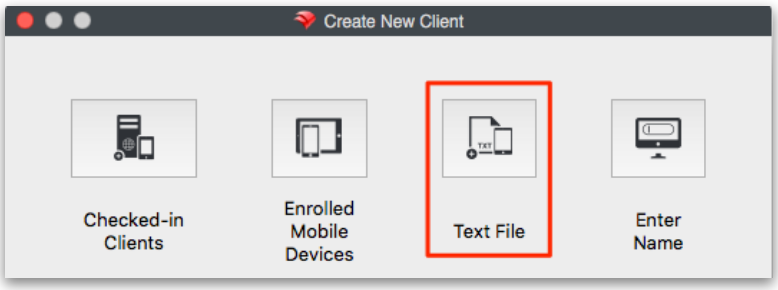
All other information is accessed the same way as for any desktop or laptop device using the **Client Monitor** or the **Client Info** panes. The Android client can be configured with Boosters, as well as many of the other key settings supported by OS X and Windows clients.



5.7. Importing Clients from a File

In previous versions of FileWave, you could create a file that contained the computer names in order to create a client set. That file has expanded to include MAC addresses for WinPC's or serial numbers for the Macs. You can import this data to pre-load your client database while you are still unpacking new devices, or you can use this data to prepare your Imaging configurations by pre-assigning devices to be imaged.

The import location is now in the **New Client** pane:



The new format looks like this:

```
#Name              Comment            Serial or MAC
FWDen-MBA-01       Testing station    YC61234ZZRT
FWDen-MBP-15       Preso system       YK345PTR22
FWDen-Win8-11      WOT station        00:11:22:33:44:55
```

Name is mandatory, **Comment** is optional, **Serial** or **MAC** is optional if you are going to be adding clients that are already named later; otherwise, you must provide either a serial number or MAC address. **MAC** address formats can have colons (:) between octets. For serial numbers, only capital letters (A-Z) and ordinal numbers (0-9) are allowed. Create the text file using a text editor that can save the file in plain text format with UNIX or Windows line endings.

5.8. Working with Apple's Device Enrollment Program (DEP)

Note - This section is for FileWave version 9.1 and above only. DEP only works with devices purchased from Apple authorized sources. Devices purchased with personal accounts cannot be managed within the Device Enrollment Program. For information on approved devices in DEP, see the following references: Apple DEP info for iOS and Apple DEP info for OS X.

Apple has introduced a process for managing institutionally purchased iOS and OS X devices with limited effort on the part of the FileWave administrator. The concept is that you can bulk purchase devices, register those devices with your FileWave MDM in advance, and have those devices auto-enroll when they are turned on for the first time.

The features of DEP include:

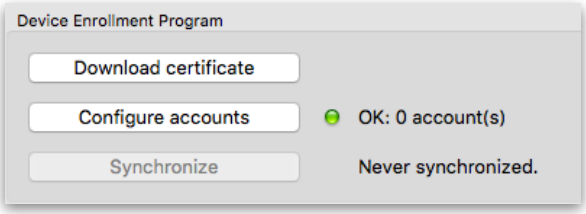
- *Zero-touch configuration* - devices can have configurations preset to take place at activation with pre-assigned applications, profiles and settings.
- *Automatic enrollment and management* - devices can be configured to instantly enroll with the FileWave MDM server and receive management profiles without hands-on by the IT staff. Devices can also be locked into management settings so the user cannot remove profiles.
- *Over the air supervision* - iOS devices can be put into **supervised** mode over the wireless network, providing an added layer of management settings, such as single-app mode for iOS or turning off iMessage.
- *Streamlined setup assistant* - devices can be configured to skip certain steps in the setup assistant, preloading some settings.

DEP workflow (short version)

1. IT signs up for DEP account (or accounts)
2. Institution purchases devices
3. IT doesn't see devices in the online DEP list until the shipping confirmation arrives from Apple (prior to that, Apple doesn't know what serial numbers are going to be shipped)
4. IT assigns the devices from the online DEP list to the FileWave MDM server by serial number
5. Everyone waits for the DEP list and the FileWave MDM list to synchronize (at least 24 hours)
6. IT assigns DEP profiles to the serial numbers of the devices prior to arrival
7. Devices arrive and, at first boot, are auto-enrolled and configured as managed devices (OS X devices will auto-enroll if connected to the Internet for push notification and the MDM server for enrollment.)

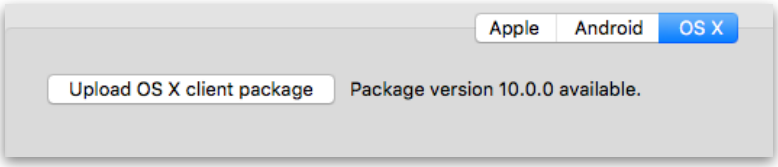
Configuring DEP with FileWave

On Apple side, a DEP account allows you to create "Virtual Servers", which are identified by a token. This token is different from the one you may have used to set up VPP on your server. DEP configuration is done within the FileWave Admin Preferences. This process is covered in chapter **3** in the **VPP & DEP Preferences** section.



FileWave Client for OS X DEP

The OS X devices that are being brought into FileWave through Apple's DEP require a custom FileWave client installer. To be installed via MDM, filewave client pkg needs to be signed. The supported way is to generate your package via our web site, so you can pre-configure it (https://www.filewave.com/support/custom-pkg). When you have filled in the web form, you will get an email with a download link to the custom client installer package (.pkg). Download that custom installer, then go to your **FileWave Admin Preferences/Mobile** to add the custom package to the FileWave server.



Understanding devices and profiles for DEP

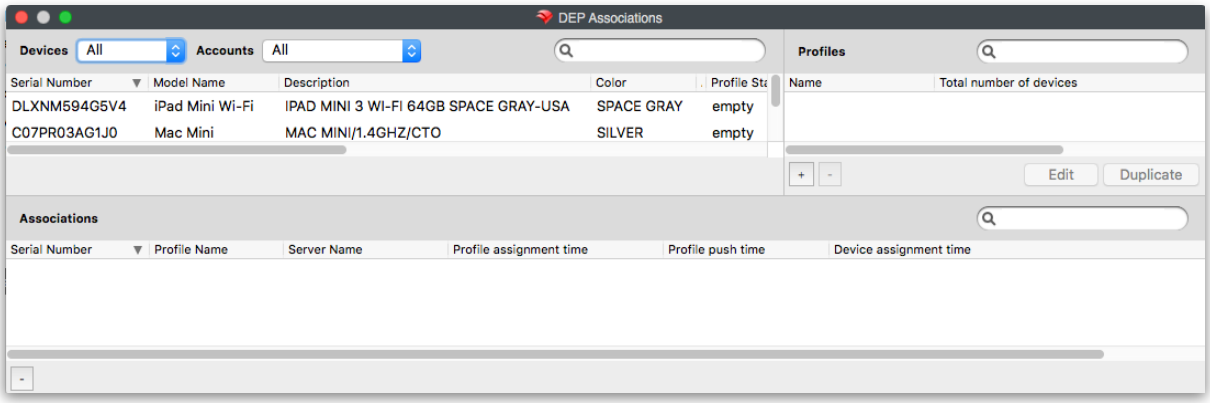
Once you have registered your FileWave server with the DEP system, you can begin setting up your devices for automatic enrollment and management. You will be able to view a list of your devices along with certain characteristics of those devices, such as model number, color of the device, asset tag information, and serial number.

You will also be able to apply a "profile" to the device.

The "profile" in DEP is not the same as a management profile. Instead of a property list (plist), the DEP profile is a set of data formatted in **JSON** (JavaScript Object Notation) format. The profile is applied through Apple when the device is initialized. It will contain settings that you configure including:

- the MDM server URL
- MDM options, such as supervision and management profiles
- MDM server certificate(s)
- Pairing certificates
- Device setup assistant options

The process for setting up your devices is done through the **/Assistants/DEP Association Management…** pane:



The **DEP Assistant** looks similar to other FileWave windows with the three sections. In this case, they are the **Device list** in the upper left, which you can filter by the different accounts devices are purchased under; the **Profiles list** in the upper right, which lists all of the profiles available to associate to devices with the number of devices each is assigned to; and the **Associations list** on the bottom, which displays the device by serial number, the name of the profile it is associated with, and various datetime groups showing assignment times and dates.

Security prerequisites for DEP

DEP uses Basic and Digest Authentication. Basic is for iOS v7.1(+) devices, and we implemented Digest Authentication for iOS v7.0.x devices. In order to set up your FileWave MDM server for Digest Authentication, you need to use a separate command, similar to the **fwcontrol mdm adduser** command used for your MDM server configuration. The new command is:

```
sudo fwcontrol mdm adddepuser <user_name>
```

As with the **adduser** command, the **adddepuser** command requires you to provide a user name in the command, and respond to the prompt to add a password for that user. This user name and password will be requested by the device during DEP enrollment. These commands are issued on the FileWave MDM server either directly or remotely through terminal services. It looks like this in action: <items in the brackets are notes - do not type those>

```
tenshi:~ admin$ sudo fwcontrol mdm adddepuser depuser <this is the new DEP user acct>
Password:<type in your admin password to authenticate for sudo>
Adding password for depuser in realm Enroll IOS Device.
New password: <enter a password that will be used to enroll your DEP user>
Re-type new password: <retype the new password>
```

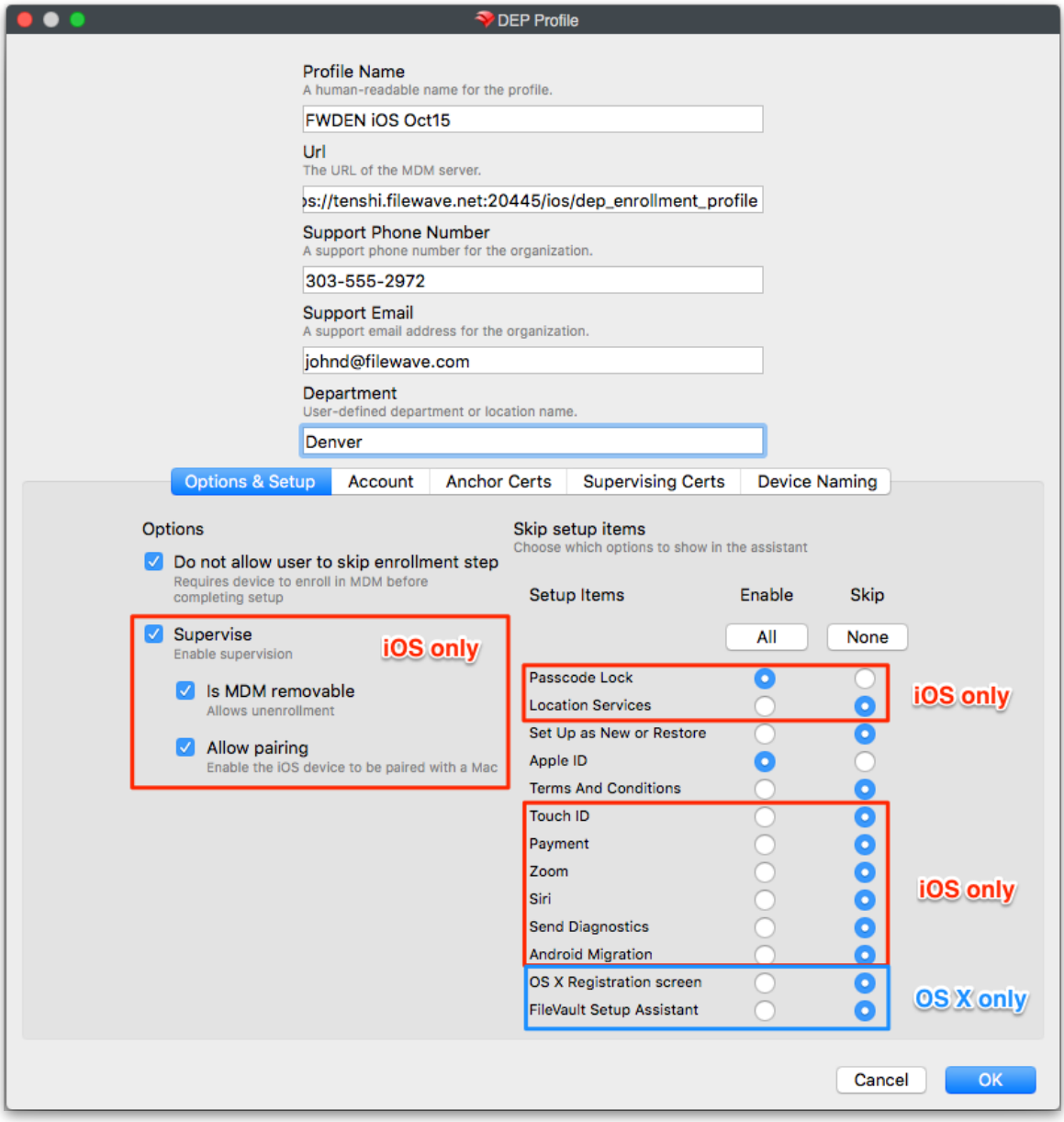
Authentication with LDAP

LDAP with Digest Authentication does not work. So if you need LDAP and DEP, you'll have to use 7.1.x(+) devices.

This is why the mdm_auth.conf.example_ldap_auth file we provide is based on basic authentication while the default is using digest. If you already created/edited the **mdm_auth.conf** file when setting up the MDM server, then you are ahead of the game. If not, and you are going to use LDAP authentication, review the information in chapter **3**.

Configuring DEP profiles

From within the **DEP Assistant** you will create the custom profiles to be assigned to your registered iOS devices depending on the deployment workflow you are using. Here is a view of the **DEP Profile** windows:



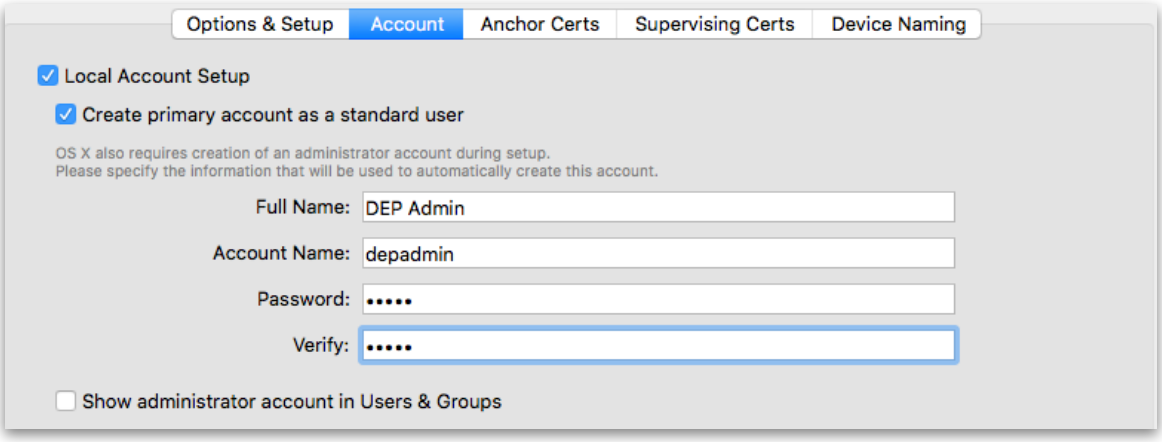
Options & Setup

These settings are for the key behaviors of the registered device:

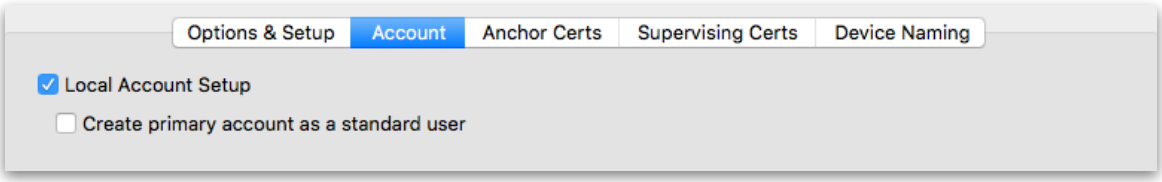
- *Do not allow user to skip enrollment step* - the device must become enrolled in order to complete setup
- *Supervise (iOS only)* - the device will have supervision enabled
  - *Is MDM removable* - if unchecked, the MDM profile is locked to the device and cannot be removed by the user through the UI
  - *Allow pairing* - if checked, the user can pair the device with their own iTunes account to synchronize personal content
- *Skip setup items* - this allows the FileWave administrator the ability to configure which portions of the setup assistant are made available to the end user when they configure the device. If none of the items are allowed, then the device must be configured with all of the appropriate settings to ensure functionality

Account (requires client running OS X v10.11+)

A new feature in DEP is the ability to create a local administrator account, and hide that account, in advance of a user being guided through creating their own local account. If you configure this pane with a local administrator account, then the user will be allowed to create a local account of their own; but it will be a non-admin user.

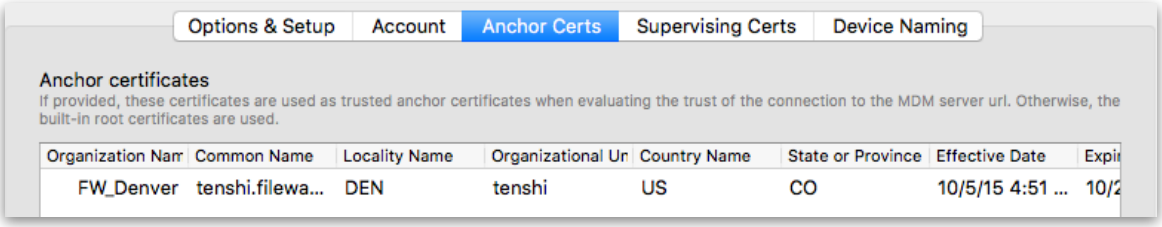


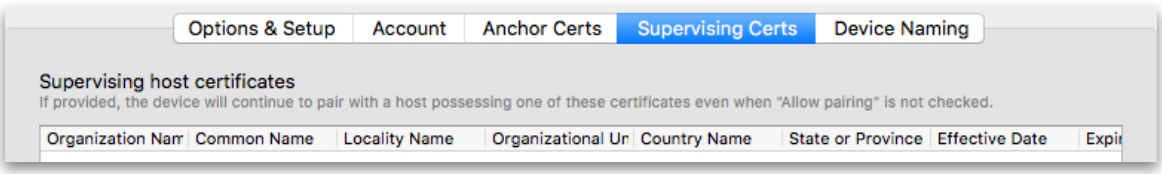
If this pane is configured with only the local account setup, the user setting up the device will be guided through setting up a local administrator account of their own.



"Certs"

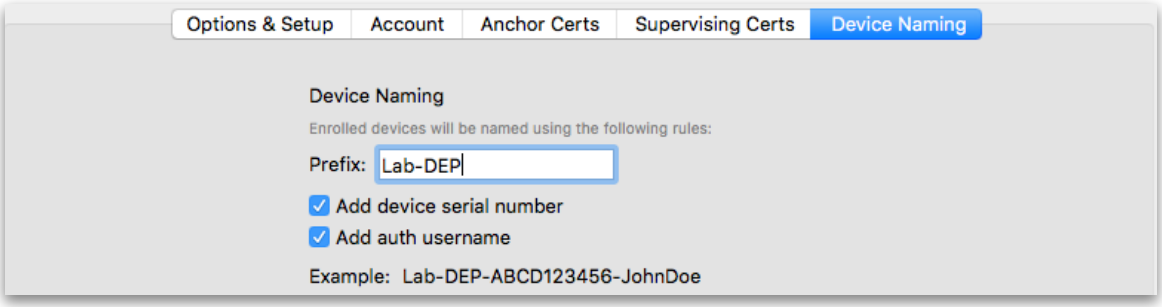
The "Certs" tabs are for adding the necessary certificates to the device to allow trusted connections and specialized pairing permissions. The FileWave MDM server certificate is automatically added to the **Anchor Certs** list.





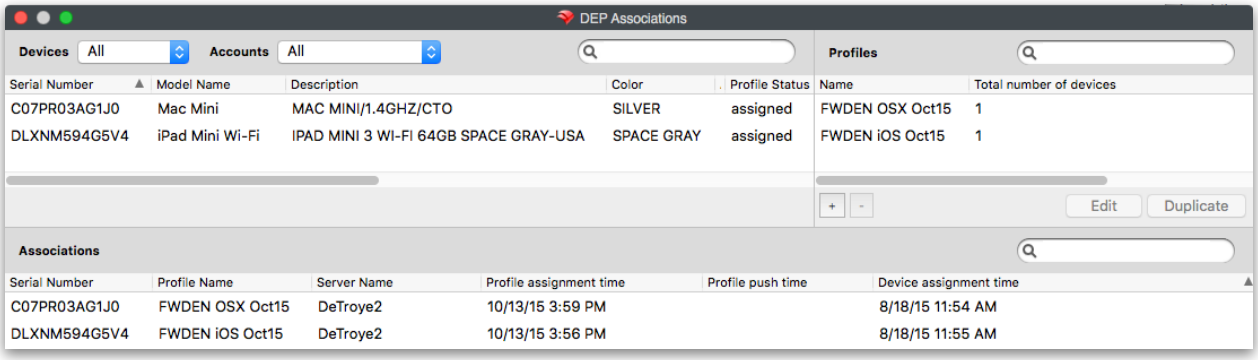
Device Naming

The devices being enrolled can have a rule-based name applied. In a 1:1 deployment where the users are authenticating to their LDAP server, the device name can reflect an institutionally derived naming convention punctuated by the user's name. This function is limited to supervised devices.



Associations

Associating a DEP profile to a device or set of devices is done using the same drag & drop functions used in the other FileWave associations panes. You can drag a profile on top of a device, or select a set of devices and drag them on top of a profile. The associations will appear in the lower section of the **DEP Associations** window. The device will have the associated profile applied upon activation.



End Result of DEP associations

The end result of associating DEP profiles to devices is that upon activation of the device, it will automatically become a FileWave client with specific setup settings. You can have device placeholders prepositioned in your FileWave clients view, assigned to groups, with Filesets ready to activate as soon as the device checks in. This process gives you the capability of unboxing hundreds, or thousands, of devices that upon being powered up, will become instant FileWave clients with applications, content, and management profiles being installed and activated.

Note: Perform a full sync of your DEP account in Preferences after setting up your associations.

Disowning devices

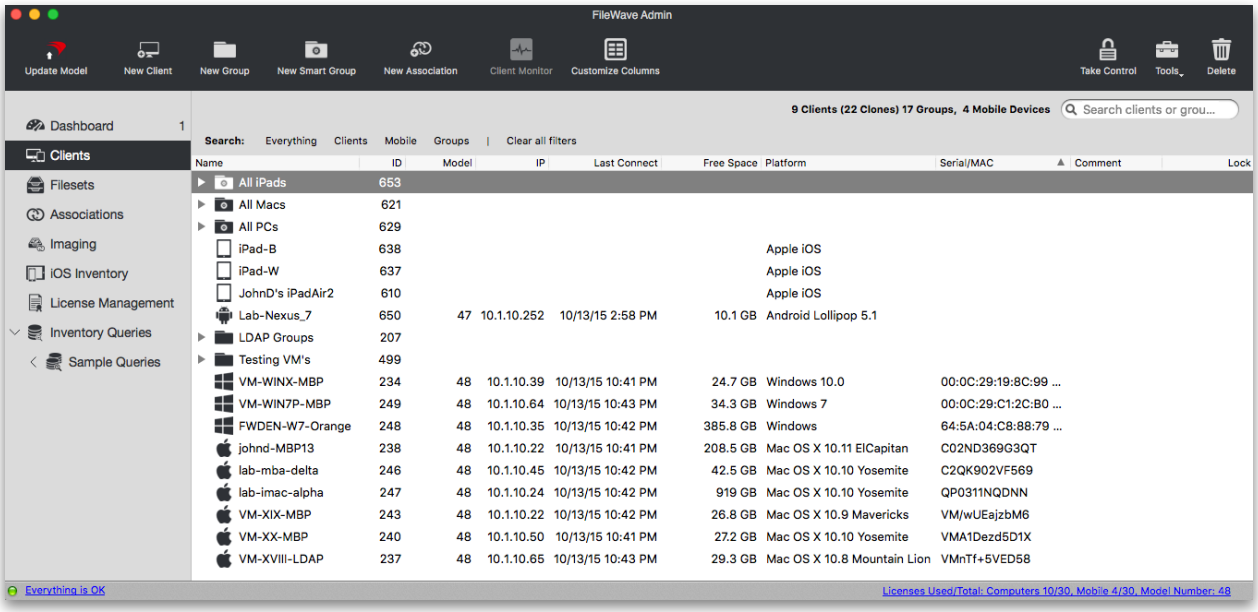
The most serious operation you are allowed in DEP is disowning a device. When you contact Apple and register your devices for DEP, they are checked against a database that proves your institution purchased those devices and plan on managing them. This option should only ever be used if the device is going to released from the institution's management forever - for example, when the device is past its lease period and is going to sold to an end user. Specifics on joining Apple's DEP and device requirements are covered in these documents from Apple - Apple DEP info for iOS and Apple DEP info for OS X.

5.9. Working with FileWave Clients

Once the various devices have had the FileWave client installed, and they are enrolled with your FileWave server, there are several options for configuring and working with these clients. This section will cover some of the common configurations and additional settings.

Clients View information

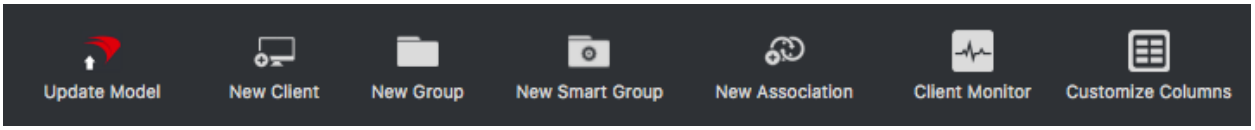
Within the **Clients** pane, you are presented with key information that helps you keep track of the status of your devices.



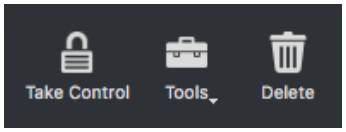
- *Name* - The device or device group name, or the smart group name
- *ID* - A unique ID created by FileWave to identify all devices, device groups, or smart groups
- *Model* - the latest version of the FileWave model to have been loaded onto the device or group
- *IP* - the IP address of the device as reported to FileWave (devices behind a firewall may all report using a NAT'd IP)
- *Last Connect* - the date time group showing the last time the device reported to the FileWave server
- *Lock* - shows whether the device has been locked by another FW administrator
- *Free Space* - shows the amount of free space reported by the device
- *Platform* - shows the reported operating system of the device
- *Comment* - custom comment entered by a FW administrator concerning that device or group
- *Lock* - shows if the device has been locked down so that it cannot be affected by any model updates

When devices are enrolled into the FileWave database, you can start performing administrative and management tasks on these systems. The next section discusses the types of tasks that you have access to from the **Clients** pane.

Client toolbar options



The toolbar that is active when the **Client** pane is selected gives you many options for performing various tasks on your devices. You can add new clients, create client groups, create smart groups, associate devices with Filesets, monitor your clients, and perform several administrative tasks. First, we need to look at the global toolbar items; then we will explore the direct action tools for specific clients or client groups.



Update Model

When you perform actions on your client devices, such as adding new clients, distributing content through Filesets, or create a new Smart Group, you should update the “Model”. The *Model* is a snapshot of the FileWave database at one specific moment. When the Model is updated, all pending actions are written to the database and a new Manifest is generated for every device detailing any changes that have taken place. A good rule of thumb in FileWave management is to update the model whenever you do anything, to anything, within the FileWave Admin.

New Client

This tool allows you to create a new client from either a desktop/laptop device that had the FileWave client installed, or from a mobile device that enrolled with the FileWave server. Details on this process are covered earlier in this chapter.

New Group

The **New Group** tool allows you to create a named group that will include individual devices.

New Smart Group

This tool allows you to create a named group of devices based upon logical criteria.

New Association

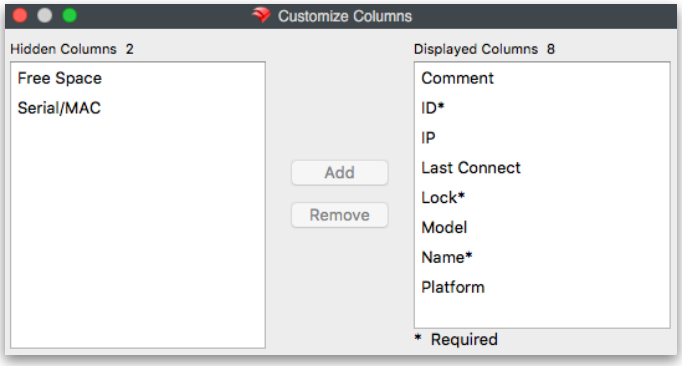
The focal point of FileWave is being able to create and distribute Filesets to devices. This tool provides one approach for you to associate a Fileset or Fileset group with a client or client group. See chapter **6** for details on using associations.

Client Monitor

The client monitor lets you view the current status of your client. It provides you with quick look at the current FileWave model running on that client, as well as allowing you to send a command to the device to verify its status with the FileWave server and view the client’s FileWave log file.

Customize Columns (FWv10 new feature)

You can now edit the **Client** pane view by adding/subtracting data columns. You can remove all but three of the data fields (Name, ID, and Lock status).



Take Control

By “taking control” in FileWave Admin, your administrator locks out all other FW administrators from making any changes to the FileWave model. This level of control is global, in that any other administrators, no matter where they are, cannot push any Filesets or changes to client devices or groups. This ability is very useful when you are making large, detailed changes to clients or Filesets and do not need those changes being preemptively sent to your

managed devices before you are finished. When you have finished being in “control” remember to release the lock so other FW Admins can access their assigned clients.

Tools

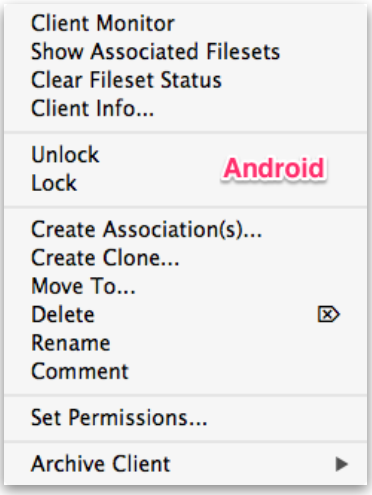
The client tools are tasks that you can perform on a selected client or group. The specific tasks available vary between the different types of client devices or groups. The next section will go into detail on each of the tools as they relate to the various types of clients and client groups.

Delete

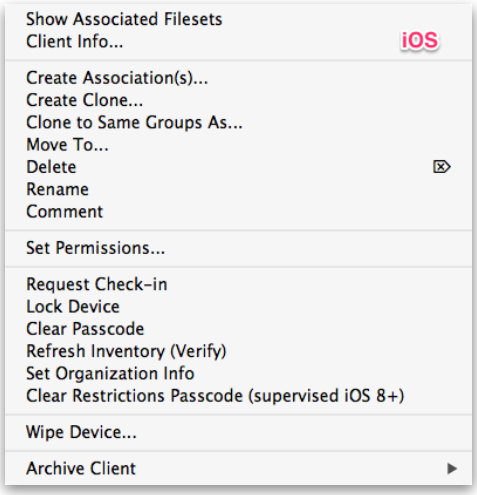
As you may have guessed, the Delete tool will remove your client device or group from the database. If you delete a group, then all nested items within that group will also be deleted.

Client Tools

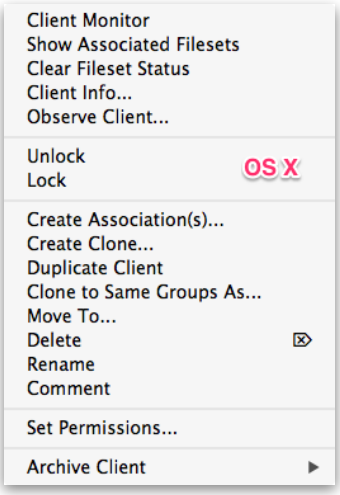
Now, let’s look at the tools we have to directly impact a specific client. Depending on the client device, you will see differing settings.



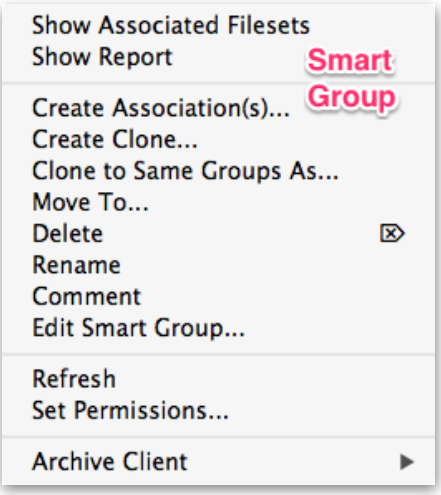
Android



iOS



OS X

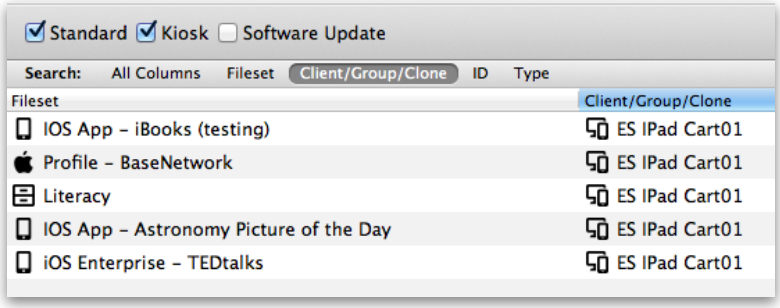


Smart Group

When you right-click on a listed client device, or select a client device, then select the **Tools** task bar item, you will see the listed tools that are available to interact with your client. The same happens if you select a device group or smart group, with a lesser number of options. Let's take a look at the various options available in the Tools:

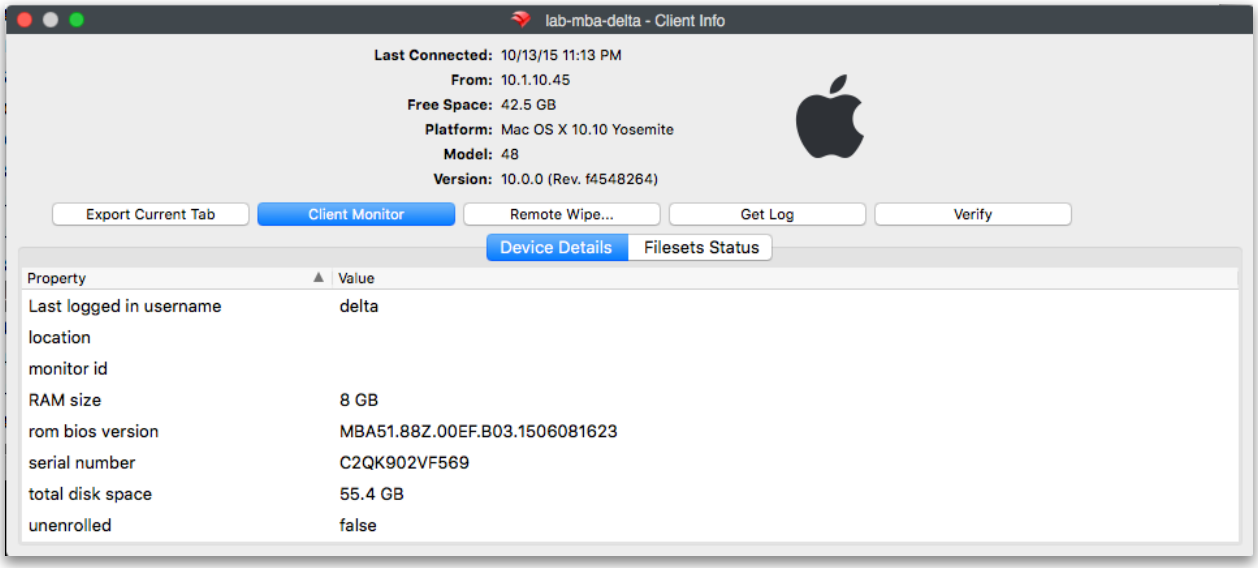
Show Associated Filesets

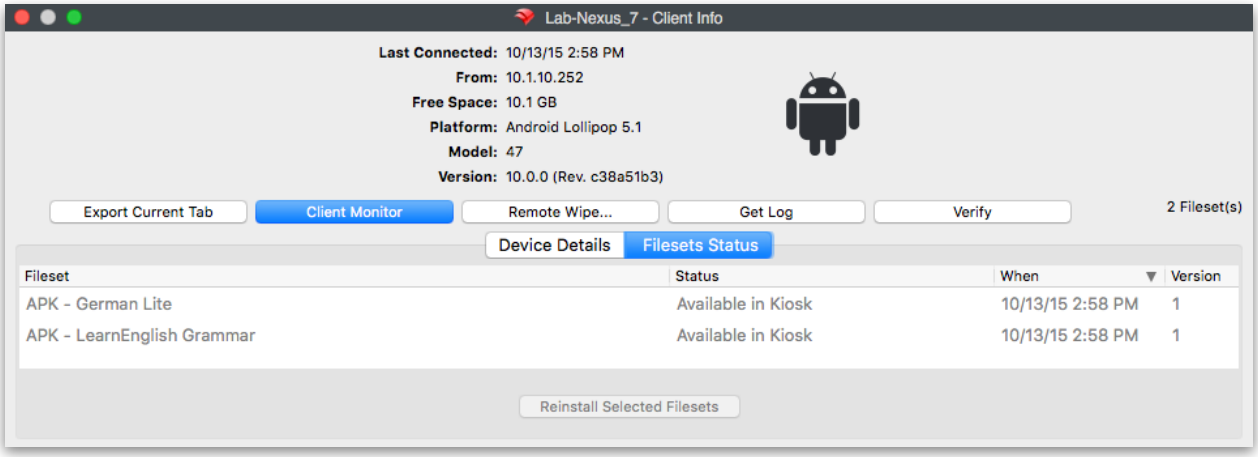
When a client or group has had Filesets assigned, or associated, with them, you can view those with this tool. The view will come from the **Associations** pane in FileWave Admin.



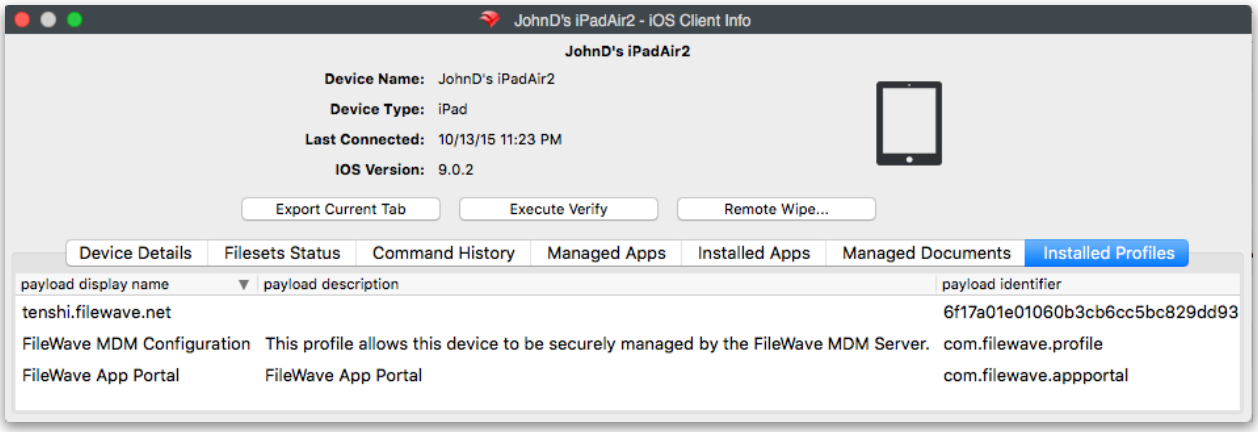
Client Info…

The client information window gives you a snapshot of the condition of your device through *Device Details* and *Filesets Status*. You can see the status of associated Filesets, open the client monitor, send a remote wipe command, view the current log file, and push a verify command. Depending on the device, you will get differing amounts of information. For example, a MacBook Air, a Windows laptop, or an Android device will display basic Fileset information as well as an overview of their Inventory information.

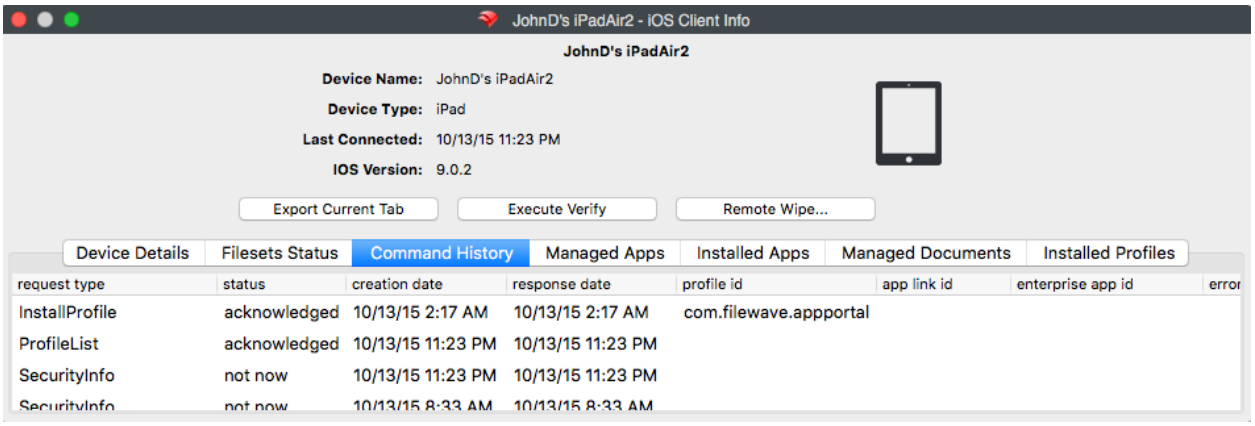




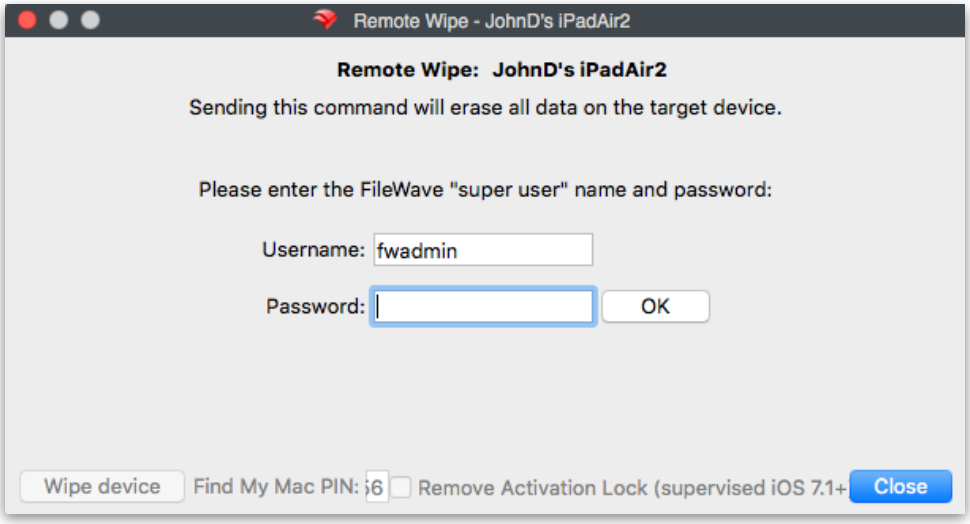
However, a mobile device, such as an iPad, will display much more information, beyond device details, with Command History, Managed Apps, Installed Apps, and Installed Profiles:



A full command history, with error messages from the FileWave server, showing what actions were performed:

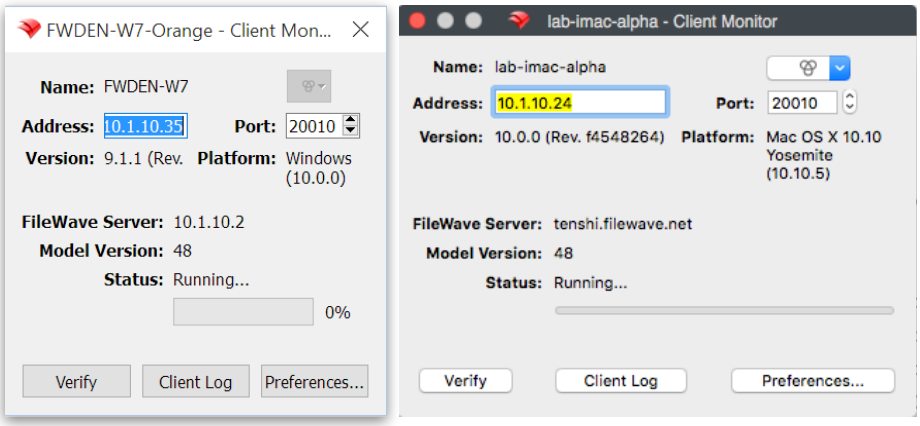


You can look at any managed (VPP) applications assigned to the device, all applications installed by FileWave, and all profiles installed by FileWave. All devices have the *Verify* button and the remote wipe capability.

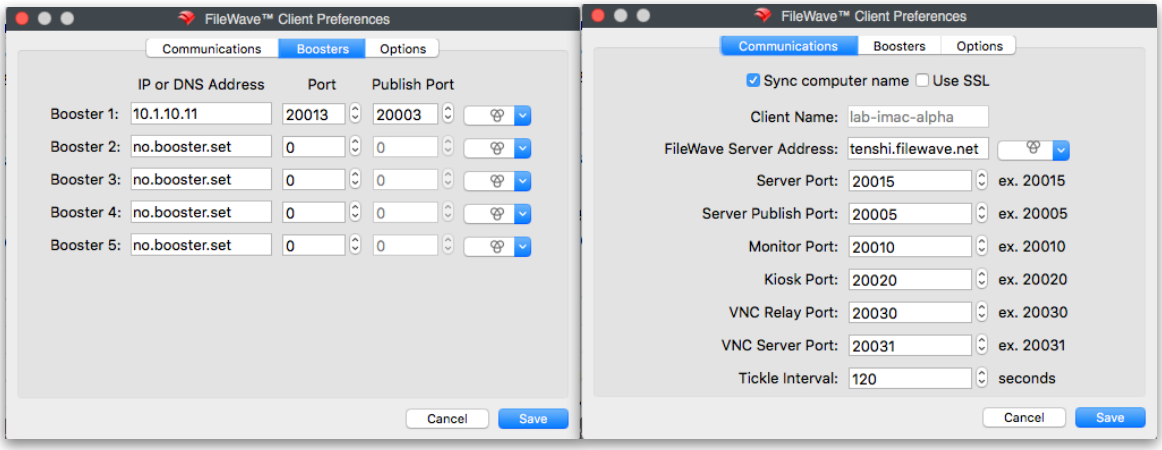


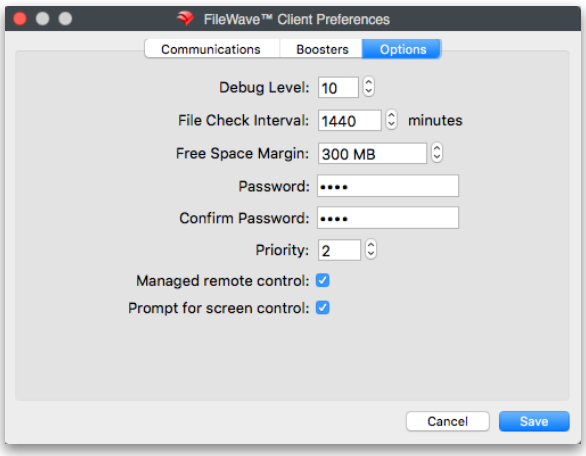
Client Monitor

The client monitor lets you view the current status of your client. It provides you with quick look at the current FileWave model running on that client, as well as allowing you to send a command to the device to verify its status with the FileWave server, and view the client's FileWave log file.



The Client Monitor also lets you change several of the preferences used by the FileWave client.

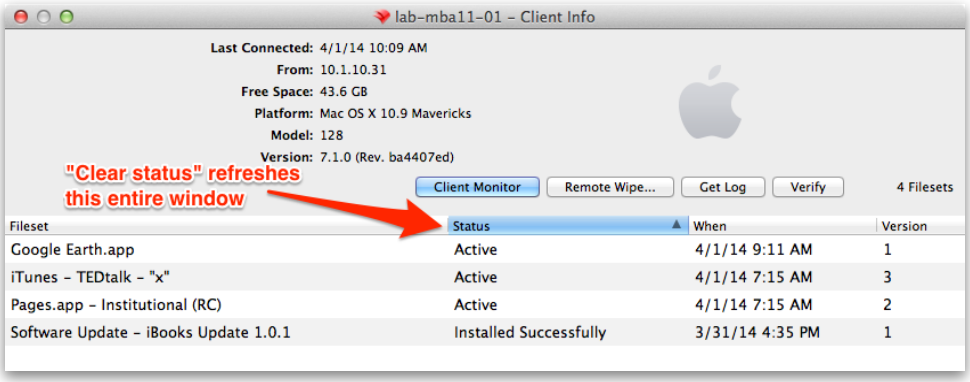




Many of these Preference settings can be configured during installation of the client; however, some of them exist only in the Client Monitor and in a **SuperPrefs** fileset.The extras include settings such as the Debug level (10 is default, 1 is the highest amount of logging) and the amount of free space that will trigger a disk full message.

Clear Fileset Status

When you have been adding and removing a lot of Filesets on client devices, the status window in Client Monitor can become difficult to review. Using this task will refresh the window. This is especially helpful if you have been testing adding and removing many of the same Filesets.



Observe Client…

This task allows you as the FileWave Admin the ability to observe or control your designated user's device. Before FileWave v10, you would need to have screen sharing active on OS X devices and a VNC server instance running on Windows. You would connect to the device using the designated account/password for observing/controlling that device. FileWave v10 introduces an entirely new method of remote observation and control with a built-in VNC relay in the FileWave Client. An in-depth discussion of this capability is in a later section. There is no remote screen sharing capability for iOS devices (this is different from programs such as Reflection that allow iOS device users to display their screen onto a desktop device).

Lock / Unlock

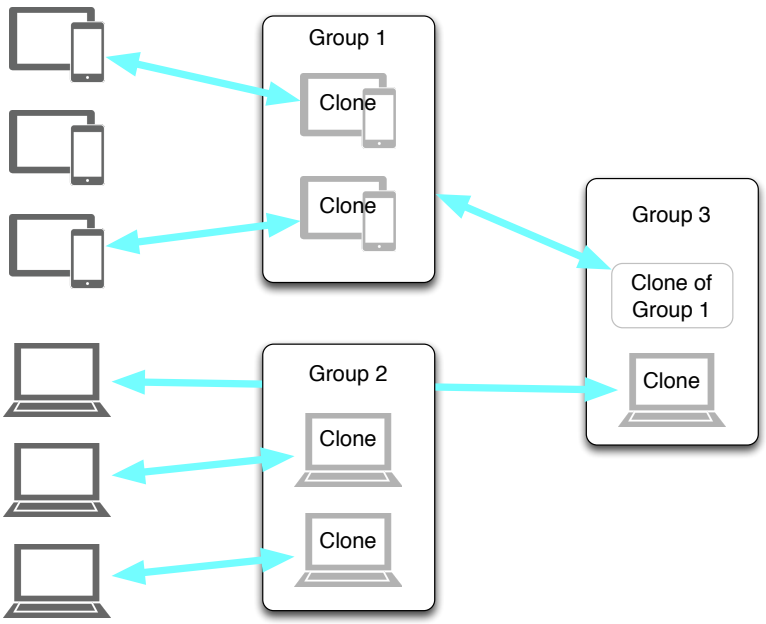
When a client device is locked, it can no longer receive model updates from the FileWave server. You might use this setting if a device is being used for some operation that would be interrupted during a Fileset activation.

Create Association(s)…

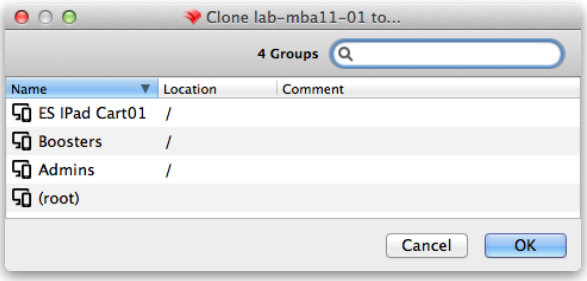
The primary function of FileWave Admin is to associate devices and groups with Filesets. This task will send you to the **Associations** pane and allow you to select Fileset(s) for association with the selected device. Detailed instructions on using Filesets and associations are in chapter **6**.

Create Clone…

Clones give you great flexibility with FileWave management. You create clones of a device to add them to different groups instead of dragging the device itself into a group. This allows you to let a client belong to several client groups based on organizational needs, geographies, or even just for application usage. A client/device can belong to several groups, and any associations made to any of those groups will be reflected at the client.

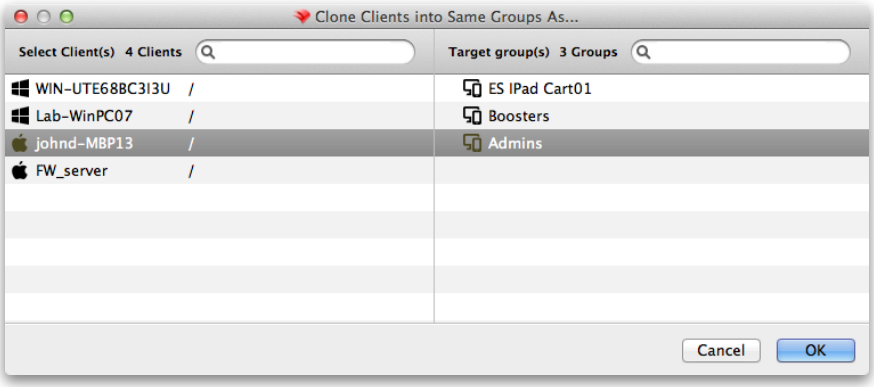


Since a clone is essentially an alias of the original device, you leave the device sitting in the “root” group of the client directory, and do all of your group assignments by way of clones. This way, if you delete a clone from a group, you have not impacted the original client record. You may also create a clone of a group if you are going to add several sub-groups into a larger group. The **Create Clone…** task presents you with a list of your groups for inclusion:



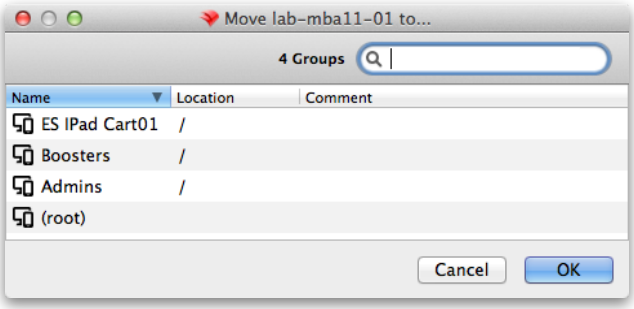
Clone to Same Groups As…

This task lets you choose another client device as the template to create clones of your client. If the chosen device has clones in several groups, then your client device will end up with matching clones in those groups.



Move To…

This task lets you move your client into a designated group. This does not create a clone; but places the original client record into that group.



Delete

If you no longer need a specific client or group in the FileWave database, you can delete it with this command. If you delete a group, then all clones and original clients situated inside that group are also deleted. Original clients outside the group would not be deleted, even if their clone was inside that group.

Rename

To rename your client or group, use this command. You can also click twice on your client (slower than a double-click) to edit the name.

Comment

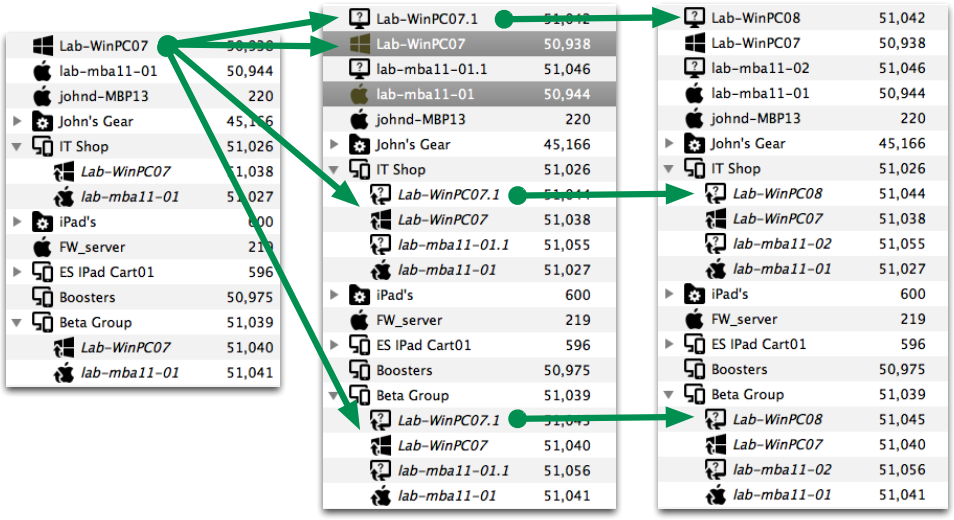
This task allows you to add a comment to your client or group record. This could be a good way of adding information that wouldn't necessarily show up in a database, such as "part of the new testing lab," or "temporarily assigned to RJ Squirrel."

Set Permissions…

This task lets you specify which FileWave Admin accounts can access a specified client or group. You use this assignment capability to manage large deployments with many sub-administrators. For example, you could have an administrator designated to manage and maintain only the Windows devices and another to manage only the iPad cart in a classroom. Some administrators could be assigned only read permissions in order to create reports.

Duplicate Client

This task lets you take a client as a template and create a new client that can be renamed to match an, as yet, un-enrolled device. When the new device enrolls, it will assume the identity of that duplicated client, as well as automatically being part of every clone used by that duplicated client. For example, *Lab-WinPC07* belongs to two groups - *Beta Group* and *IT Shop;* the client gets duplicated and it's new name is *Lab-WinPC07.1* When the duplicate is renamed, all of it's clones get renamed also, and when you enroll the new device with the name *Lab-WinPC08*, the new client automatically belongs to all the correct groups.



Add Client…

This task is for adding a client into the selected group. Selecting this task opens the **New Client** window.

Add Group…

This task adds a group to the selected group. Selecting this task opens the **Create New Group** window.

Edit Smart Group…

This task allows you change the settings and criteria for a smart group.

Request Checkin

This task sends a command to the mobile device to check in with the MDM server. Sending the check-in command will send along every item in the command history that has not been received.

Lock Device

This task sends the command to the mobile device to return it to the lock screen (as if the power button had been pressed).

Clear Passcode

This task turns off any passcode set on the mobile device.

Refresh Inventory (Verify)

This task sends a request to the client to perform a complete inventory of itself and report back to the FileWave server. This is more inclusive than the **Check-in** command in that the client gets a push command to supply the following information:

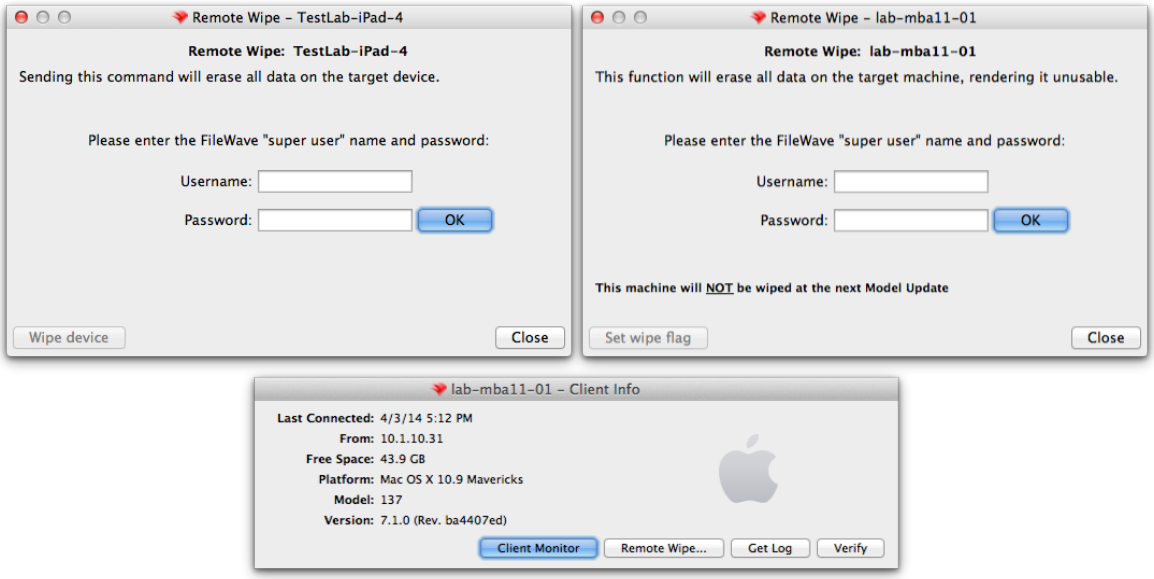
- Managed Application list
- Security info
- Restrictions
- Installed Application list
- Profile list
- Device information

Plus perform any self-healing needed and install/remove any Filesets that have been modified.

Wipe Device…

This task sends a command to mobile devices to erase all content and settings. For mobile devices, the command is located in the right-click popup. For desktop/laptop devices, it is located in the **Client Info…** window.

You must enter the FileWave "super administrator" (the primary FW administrator account) name and password in order to proceed with the device wipe.



Set Organization Info (iOS only)

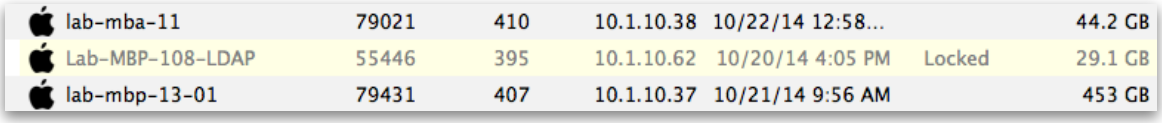
This command appends the *Organization Info* that is configured in FileWave Admin/Preferences to the selected device. This information is sent to the device at enrollment; but if the information changes, it needs to be manually updated using this menu item.

Clear Restrictions Passcode (supervised iOS 8+)

This command will flush the passcode set on a supervised iOS device.

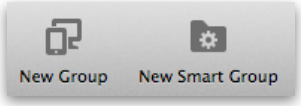
Archive Client

This command allows an administrator to remove a device from active participation in the FileWave database. All inventory data on the device is frozen and the device is no longer counted as a client for license purposes. An example would be a device that is undergoing repair, or has been taken out of circulation for a period of time. The device appears as locked, and the device license is incremented, showing that the archived device is no longer counted as active.



In order to re-add the client to the active FileWave database, you must fully remove it from FileWave, then re-add it through the ***New Client*** window.

Groups & Smart Groups



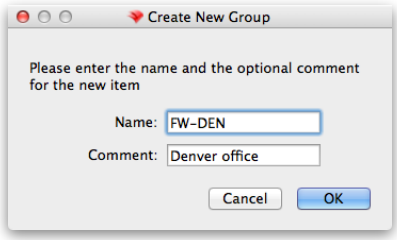
Putting clients into groups gives you tremendous flexibility in overall control and management of your deployment. With groups, you can configure sets of clients by type, function, location, and any other association that you can think of. Smart groups go even further by letting you create criteria that will automatically assemble sets of clients. The real power of groups in FileWave comes from being able to associate Filesets with entire groups of clients at the same time, instead of having to match individual clients with specific Filesets.

Examples of groups would be putting all of the clients in a certain department together, or all the clients in a lab, cart, or classroom into unique groups. Groups defined by location or geography could be managed by different FileWave administrators. You can also make groups of groups, such as having groups based on different projects or curricular needs all combined into a group defined as the overall department or building.

Smart groups will provide you with dynamic membership. An example is a smart group with the criteria of being in a certain subnet, or having a specific version of operating system or application. When a client meets that criteria, a clone of that client is automatically added as a member of that group. Once the client's criteria changes, it drops from that group. You can add Inventory queries to group criteria. This gives you the ability to have clients assigned dynamically to a group as they meet complex criteria. An example of this would be having specific Filesets assigned to devices with certain characteristics, who are also on a specific subnet, and have a certain qualifier in their name.

Creating a Group

You can use any criteria you desire to create a Group. Select the **New Group** tool from the toolbar and fill in the name of the group and, if desired, a comment on the group, such as its purpose.

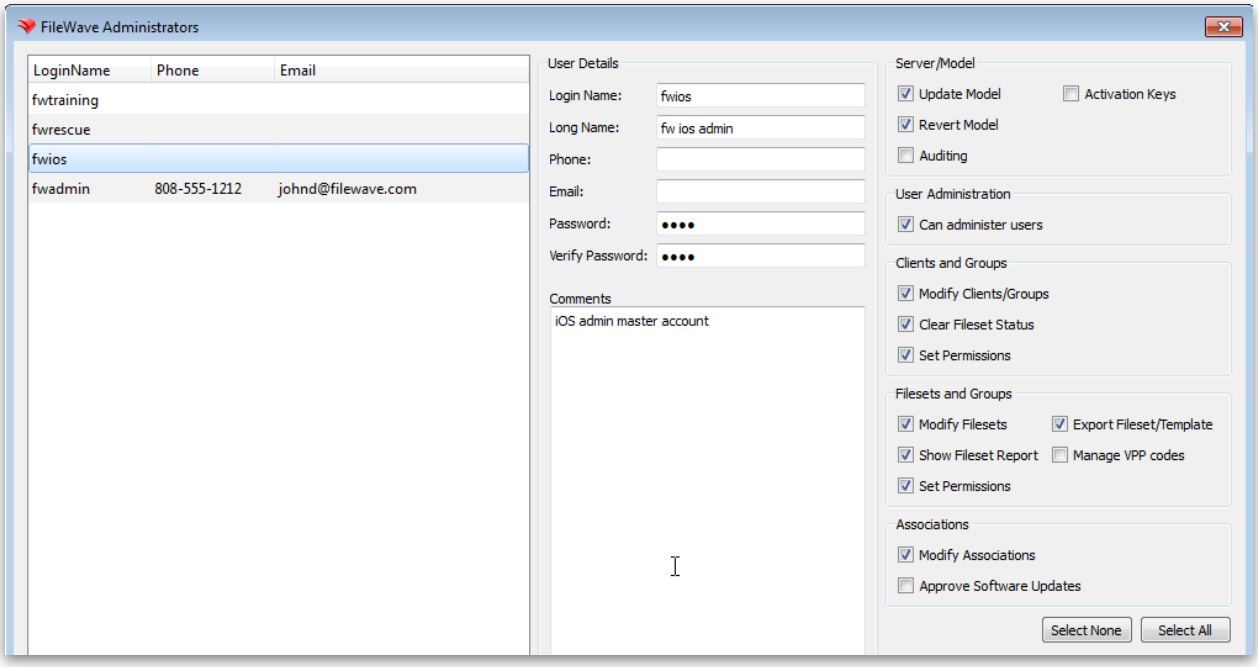


Once the group is created, you can assign clients to it either with the pop-up menu (right-click on the group, select **Add Client…**) or you can add a clone of a client to the group by holding down the Alt-key (Windows) or the Option-key (OS X), selecting the client and dragging the clone onto the group icon. You can also use the **Create Clone…** command to build a clone of a client, then add the clone to the group. Finally, you can create groups to be sub-groups, then add those groups to the "upper" group. When you associate Filesets with the uppermost group in a set, all of the clients assigned to that group, or to groups inside that group, will all get those associations.

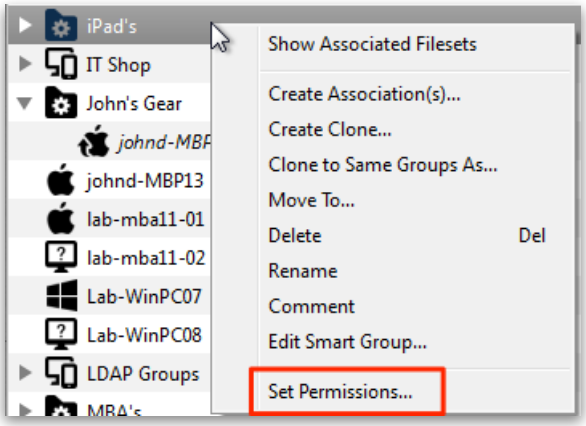
Setting permissions for a Group

Once you have created one or more groups, you might want to distribute overall management and maintenance of those groups. The "Super Admin" account (fwadmin - if you left the account name intact) will always be able to edit or delete any client or group in FileWave Admin. What you might want to have is several "sub-administrators" who can take over maintenance of one or more specific groups. This is where the **permissions** come in.

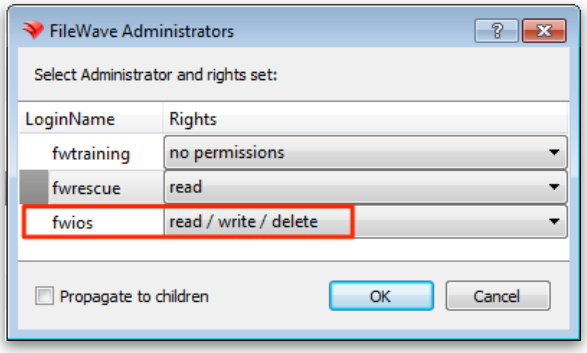
For example, in our sample configuration, we created an administrator account called "fwios" who can be assigned to support one or more iOS accounts.



If we select one of the groups that has iOS devices in it, we can right-click on the group (or select the **Tools** item in the toolbar) and choose **Set Permissions…**

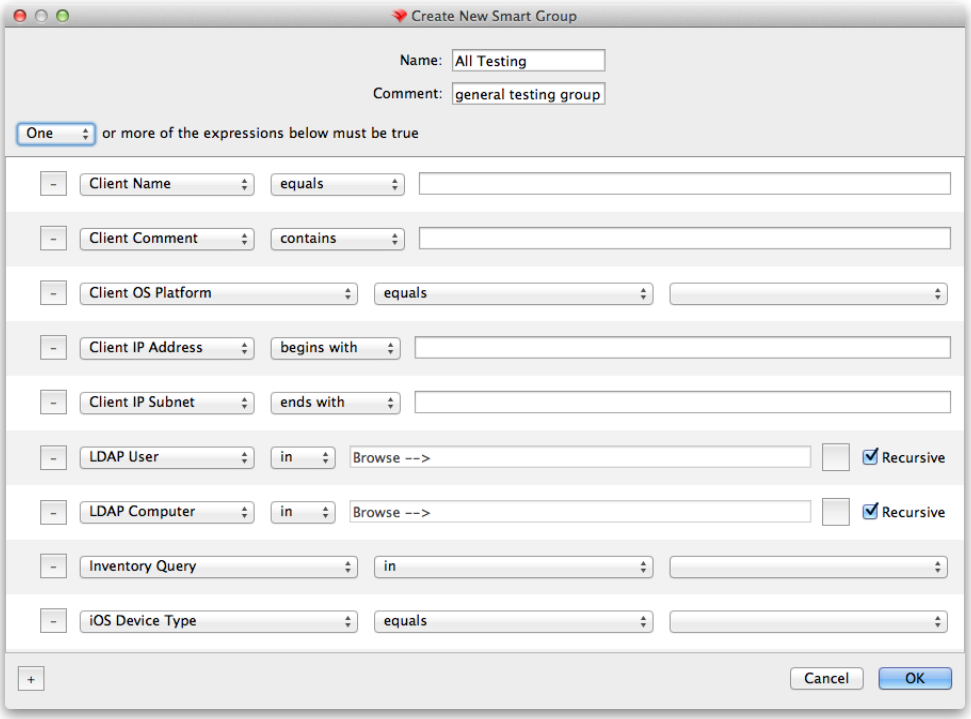


All of the FileWave Admin accounts will be available and you can choose which administrators have permission to work with the selected group. Your choices are to let them have full support (read/write/delete), partial support (read/write), view only (read), or no access (no permissions). If you have an administrator account who will be just adding or deleting Filesets, you can assign just read/write permissions. An account that creates reports can get by with only read access. The permissions can also be set to **Propagate to children** which then assign the same permissions to any group embedded in that designated group.



Creating Smart Groups

The smart group is a collection of clones based on specific criteria. To use smart groups, you must have installed the FileWave MDM server. The options you can choose for smart groups are extensive:



You can pick and choose criteria as needed, and decide if all or only one of the criteria must match to include a client. The specific criteria are defined as follows:

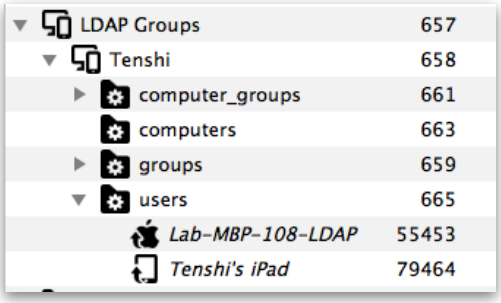
Search Type	*Qualifiers*	*Criteria*
Client Name	equals / contains / begins with / ends with / less than / greater than	alphanumeric text of a client name or portion of a name
Client Comment	equals / contains / begins with / ends with / less than / greater than	Any alphanumeric text comment or portion of a comment
Client OS Platform	equals	OS X (Intel / PPC, 10.3 -10.9), Windows (XP, 2000, Vista, 7, 8)
Client IP Address	equals / contains / begins with / ends with	Any logical numeric value that meets standard IP address format (xxx.xxx.xxx.xxx)
Client IP Subnet	equals / contains / begins with / ends with	Any logical numeric value that meets standard IP address format (xxx.xxx.xxx.xxx)
LDAP User	in	A user name in an associated LDAP directory server database
LDAP Computer	in	A computer name in an associated LDAP directory server database
Inventory Query	in	Any valid Inventory Query from the MySQL server (v.9.x) or from Inventory (FW v8.x)
iOS Device Type	equals	iPad / iPod / iPhone / Any

Once you have selected one or more search types and filled in the criteria, FileWave will automatically add a clone of the qualified clients to the group. You can use these types of groups to track devices as they move around the institution, fall behind in updates, have their name changed, or any other combination of conditions you desire.

Permissions for smart groups are set up with the same steps used to set permissions for regular groups.

Using LDAP / Directory Services Groups

FileWave can create smart groups based on your LDAP server directories. If you have added LDAP server(s) to your preferences, then your Clients pane will be populated with an LDAP smart groups set:



These groups will be automatically populated with the user groups (workgroups), computers that are bound to the directories, and the computer groups that are part of the directories. Devices are tracked by name and a clone is automatically created for each entry that matches the group criteria. You can associate Filesets and set permissions for any of these groups. Devices registered by users with their LDAP credentials show up under Users. This links the user to the device for tracking purposes. To set up LDAP for authentication, see chapter **3.**

5.10. Self-service Kiosk

FileWave supports two methods of distributing content. The first is direct interaction from the FileWave Admin(s) where applications and other content are associated with devices or groups of devices as part of a centrally managed deployment scheme. The second method is by using the self-service **Kiosk** and allowing the end user to choose the items to be installed on their device. In a BYOD or 1:1 deployment, your challenge is providing the appropriate mix of applications and content needed by many different groups. Instead of trying to build unique image sets for each group, or trying to force specific content on devices that may not have the space for all possible combinations of content, you can use the Kiosk to allow the end user to install and un-install items as they are needed, or as space is made available. Because the FileWave processes run at root level, the end user does not need to be a local administrator in order to install applications and content through the Kiosk.

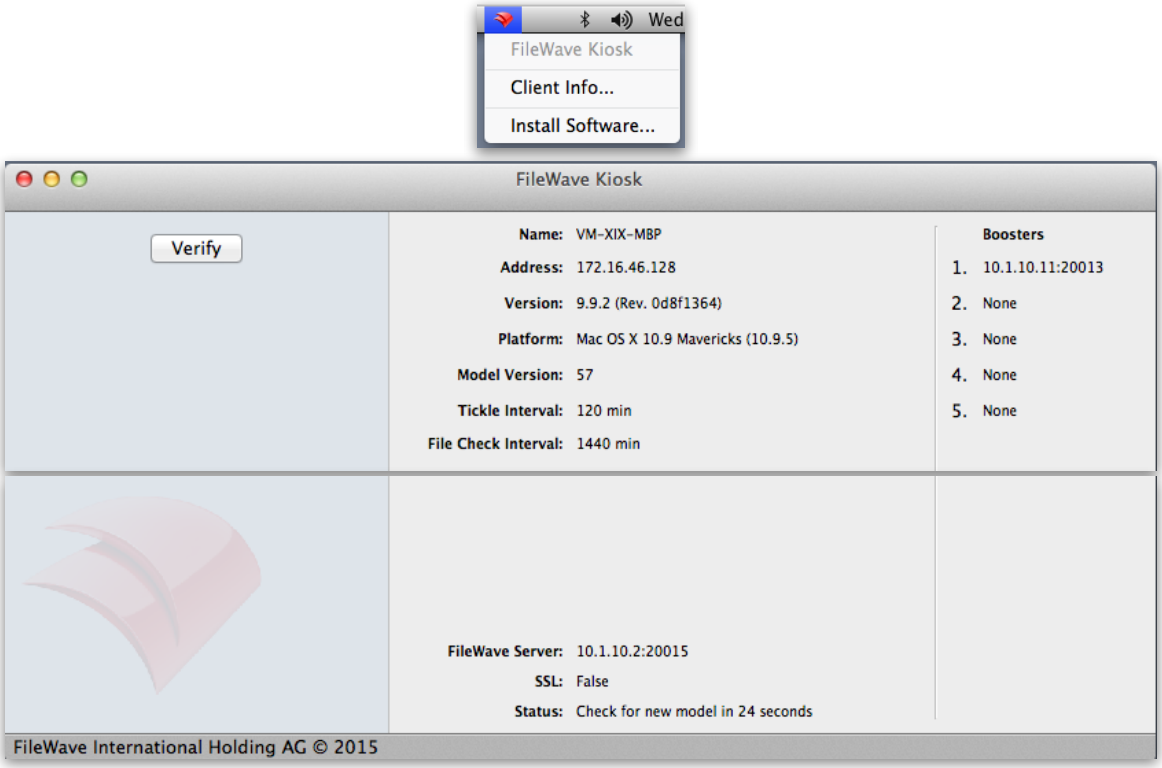
The Kiosk is activated on a laptop or desktop device by installing the FileWave client and, usually, one Fileset is associated with the Kiosk. The Kiosk is activated on a mobile device when that device enrolls with the FileWave MDM. Since the Kiosk is completely multi-platform capable, you can configure unique content sets based on platform as well as operational/educational needs.

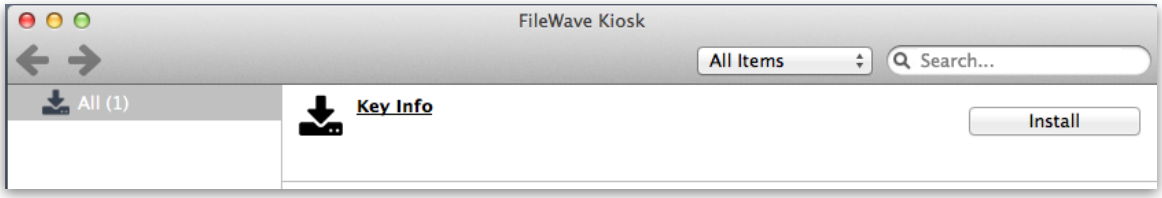
Filesets can be configured as Kiosk items in FileWave Admin and can be added to unique categories, such as a specific department or class, or just by application type. You can even create a Kiosk Fileset of an iOS application from the App Store. The user gets the link to the store and the application or book would be downloaded from Apple when they request it. Kiosk items can be managed using Apple's new VPP Managed Distribution model so that assigned applications can be installed by a user; but returned to the FileWave Admin for re-use at a later date.

Mobile Kiosk versus Desktop Kiosk

The Kiosk on a mobile device (Android/iOS) is a permanent feature. Once the device is enrolled, the Kiosk appears. On a desktop/laptop device (OS X/Windows) the Kiosk appears once a Fileset has been associated with that device. The desktop Kiosk can be configured to always stay visible on a device by editing a file on the client. The process is outlined here - https://www.filewave.com/item/customize-kiosk - and includes methods to customize the look and feel of the Kiosk also.

With FileWave v10, the desktop Kiosk took on additional functionality. It now contains an extra pane that displays basic Client Monitor information, as well as a button to force a Verify with the FileWave server.





5.11. Remote Control (FWv10+)

Previous versions of FileWave had to rely on outside software, such as Apple's Remote Desktop, or third party VNC tools to support remote observation and/or control of client devices. FileWave v10 changes all that by imbedding a NAT capable VNC functionality directly into the FileWave client. The implementation is based on VNC (Virtual Network Computing) with the support of a VNC server running on the FW client machine and a VNC viewer that will be launched on the FW administrator's desktop.

Features

- Network Address Translation (NAT) issues solved using new VNC relay functionality built into the FileWave server
- Deployment of an independent VNC server on Mac and Windows platforms, with integrated management to ensure existing VNC server deployments are not affected
- Native VNC viewer used on Mac and deployment of independent VNC view on Windows
- Encrypted connections
- Cross-platform support from single Administrator GUI
- Managed VNC server can be administered using Super Preferences & Client Preferences

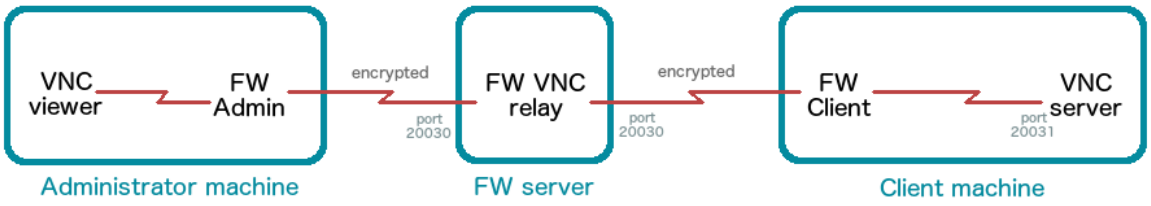
Requirements

- FileWave servers, Boosters, and the Administrator GUI must have been upgraded the FileWave v10.
- Clients must be upgraded to FileWave v10 to take advantage of managed VNC server and avoid NAT issues.
- For clients that have not been upgraded, native remote desktop must be active on the client machine for viewing via a direct connection, a feature that has also been extended to support viewing Mac clients from a Windows Administrator GUI, with the limitation that VNC password authentication is configured for the remote desktop.

How it works

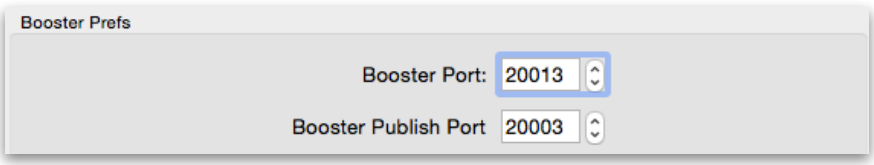
A FileWave Admin selects a client device and chooses to **Observe Client…** from either the **Tools** toolbar item, or from the pop-up menu on the client entry. The VNC viewer will then be launched on the administrator's desktop and, if all is well, a communication channel will be established to the client machine.

To avoid issues related to network address translations, FileWave manages the communication channel via a relay on the FileWave server. All channels between the administrator and the client, via the relay, are encrypted. The managed VNC server deployed with the FileWave client only accepts connections from local processes (i.e. the FW Client) for better security. In other words, the VNC communication is tunneled inside the normal FileWave Admin to client traffic. This provides robust security, and insures that as long as the FileWave client can talk to the server, the Admin can talk to the client.

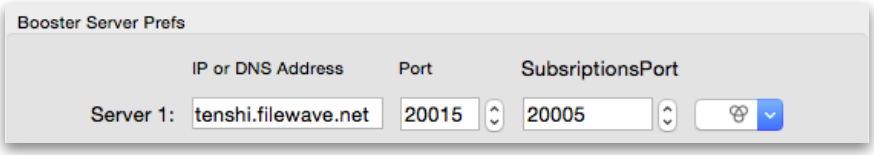


Configuration

The communication can be from the FW Admin to the client, or it can pass through a Booster. Any Boosters set up in this environment must be configured to listen for, and pass on, traffic as required.



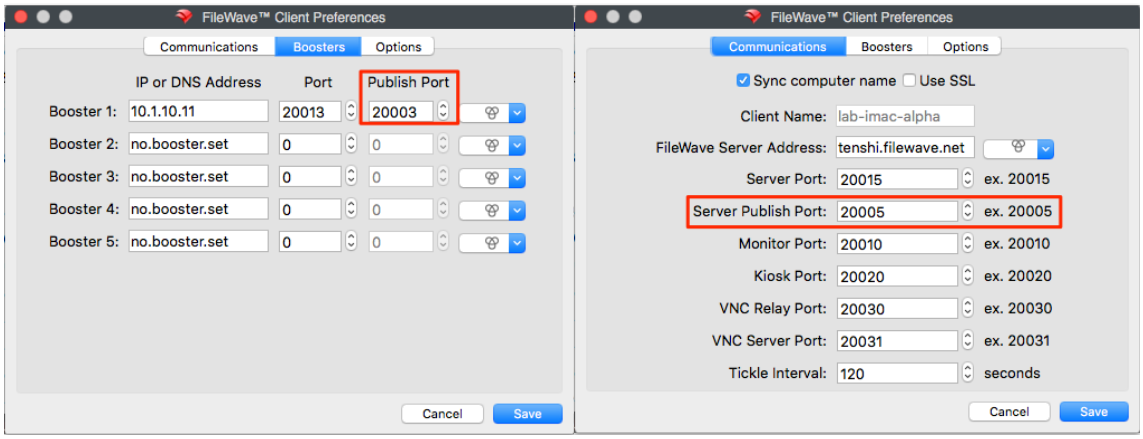
First, the Booster will “publish” any observe/control communication on its designated Publish port (default is 20003). The Booster will also “subscribe” to any observe/control traffic from other Boosters and clients on port 20005.

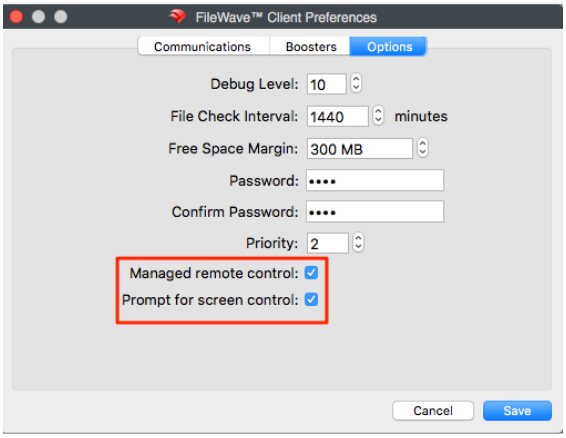


Client Configuration

There are only a few key settings to be aware of for your FileWave clients in order to allow the remote control to work properly. First, all clients must have a password set in their client preferences. This allows the secure communications between the FileWave server and client already. Second, the user can have the ability to “opt-out” of the communication.

The best part of all of this is that as a FileWave Admin, you don’t have to do any extra work to have this running. It “piggybacks” on the normal FileWave traffic, and is available to all FileWave Admins.





Note the **Server Publish Port**, the **Booster Publish Port**, and the two settings for **Managed remote control** and **Prompt for screen control**. All of these must be checked for the correct values. You can configure a **SuperPrefs** Fileset to configure much of this, if necessary.

6. Working with Filesets

Core to the functionality of FileWave is Fileset technology. All application and content distribution is done through the use of Filesets. Except Apple packages (**.pkg**) and Microsoft installers (**.msi**) which are run as normal installations, all content distributed by FileWave is done at the file level. Items are copied to the client with all permissions intact, and can be configured to self-heal if the user removes protected parts of the set. Imaging Filesets are part of FileWave v9, and behave differently from regular Filesets.

6.1. General Fileset workflow

Distributing content with FileWave is done with a simple workflow that can add complexity as needed. All of the information below is discussed in much more detail later in this chapter. The basic workflow runs as follows:

- *Select Fileset type* - you choose the type of content (files / folders / profiles / iTunes / scripts / etc)
- *Configure Fileset or add content* - provide settings or assign content to the Fileset
- *Associate Fileset to client(s)* - you attach or associate a Fileset with a specific client or group
- *Update server model* - you commit the changes to the server and the Fileset actions are performed by the client(s)

A more complex model may include some or all of the following additional steps (Some items are specific to desktop or mobile Filesets only):

Post-creation

- *Specify Details* - settings can include forcing the Fileset to be redeployed if removed and/or causing the deployed application to be removed if the FileWave profile is removed
- *Provide Kiosk information* - you can provide information for the user concerning this item
- *Edit Payload* - you can open the Profile Editor and make changes to the settings
- *Edit Settings* - you can specify the OS and other defaults for this payload
- *Add items* - you can add more files / folders to this Fileset
- *Edit files inside Fileset* - you can edit files directly within a payload

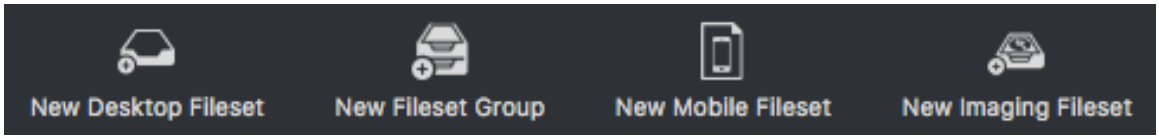
Post-Association

These settings are covered in detail in the next section on Associations.

- *Specify a download time* - you can choose to deploy this Fileset at another time than immediately after the model is updated
- *Specify an activation time* - you can choose to activate the payload at a later time than right after download is complete
- *Specify a deactivation time* - you can choose a time to make this payload inactive, rendering it invisible to the user
- *Specify a deletion time* - you can choose a time to remove the payload completely from the client
- *Designate Fileset as a Kiosk item* - you can choose to make the Fileset self-installable by the end user
- *Specify Fileset dependencies* - determine if a Fileset requires another Fileset in order to function properly

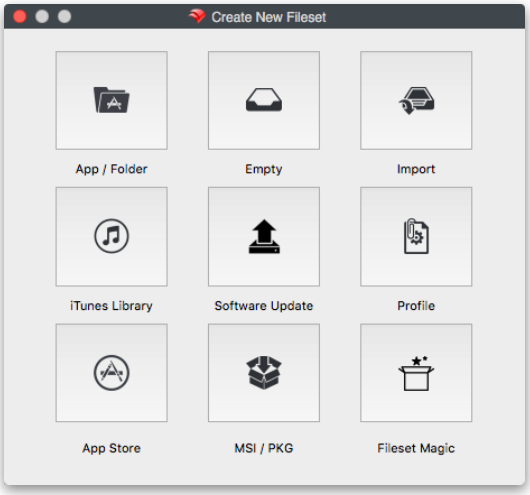
You have great flexibility with all aspects of Fileset deployment. You can choose to make certain Filesets react to conditions at the client, specify certain Filesets for deployment at staggered intervals, pre-stage Filesets on clients while you are still testing them for performance, and you can edit Filesets after deployment to add or subtract content as needed. Actions like these, and many more, give you the freedom to control your management at file level, resulting in lower network loads, faster response times, and built-in self-healing of applications and content for your end users.

Filesets can be grouped for curricular or functional needs in order to maximize your deployment workflows.



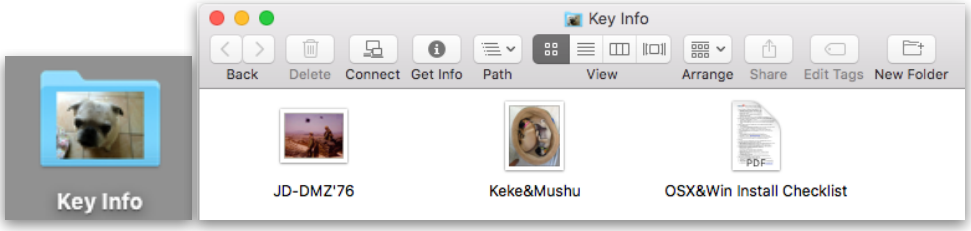
6.2. Desktop Filesets

Desktop / laptops Filesets are designed for use on Apple OS X and Microsoft Windows systems. The Fileset types are shown below:



App / Folder Fileset

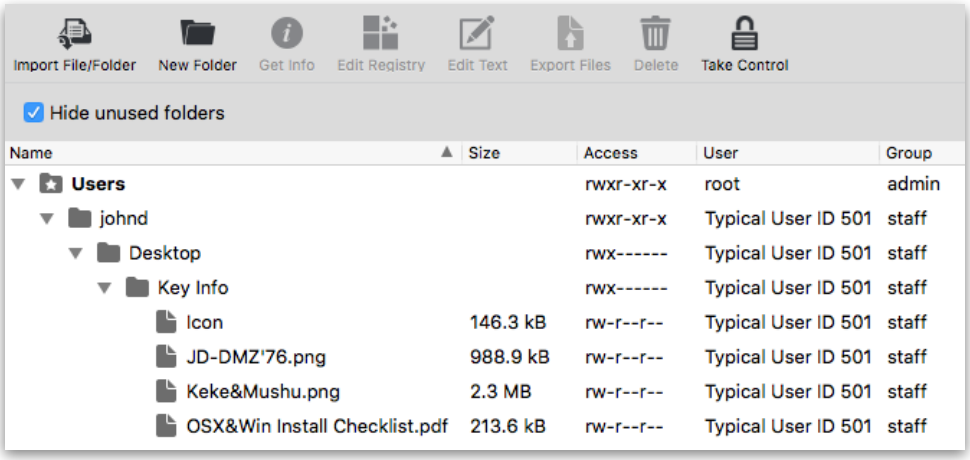
This is the most basic Fileset. You select a file or a folder from your working system; then assign the location for distribution. For example, if you needed to take a set of content files for distribution every user who logs into a computer. First, you would select the files, in this case “Key Info”:



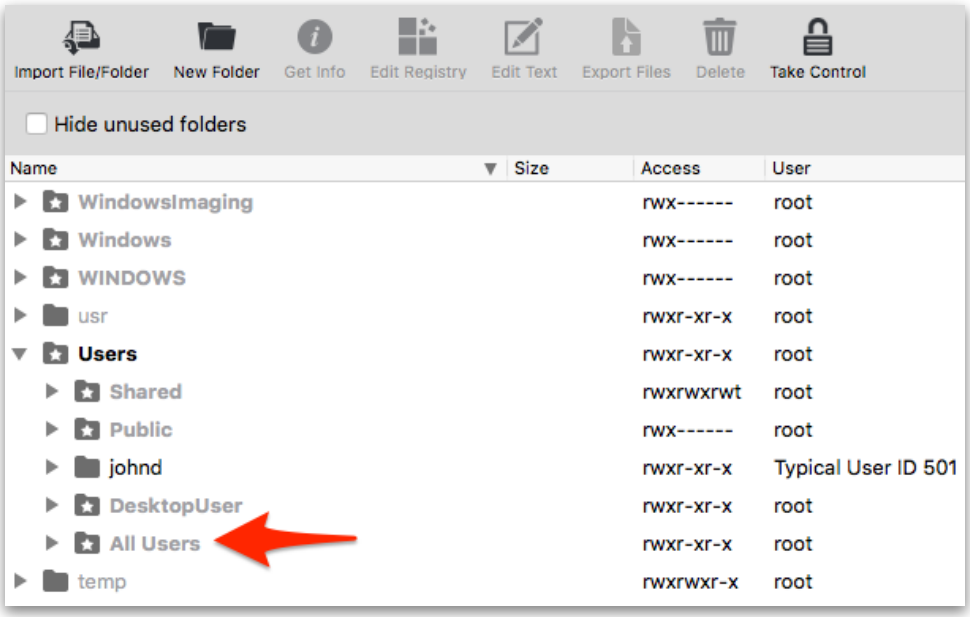
FileWave creates a Fileset from this folder and displays it in the **Fileset** pane in FileWave Admin.

The “Key Info” Fileset was created from a folder with 3 files inside. Since it is a new Fileset, and the server model has not been updated, it shows as a modified Fileset. FileWave assigns a database ID to every component.

In order to prepare this Fileset for distribution, you double-click on it. This exposes the contents of the Fileset and allows you to specify the exact location for its distribution.

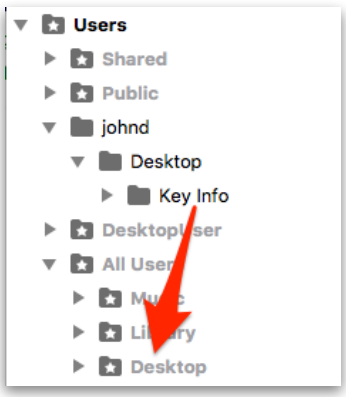


In order to make sure the files end up where you want them, you uncheck the box for **Hide unused** folders. FileWave allows you to send files not just to the exact same path you captured the files from (in this case - */Users/johnd/Desktop/Key Info*); but to a special location called **All Users**.



If you look at the various folders shown above, you will notice that most of them are the standard items that show up on any computer. In fact, the folders with ID numbers below **200** are permanent items in the Fileset Contents window, such as **/Users/Shared**. The items with higher ID numbers are created whenever a Fileset is made with folders containing special pathnames, such as the set for **johnd** which is a unique user name.

The **All Users** folder (ID 115) is there to allow you to take an item and drag it from the location path where you originally found it into a folder that will be placed onto every user's system. In this case, we captured the folder item **Key Info** from the path **/Users/johnd/Desktop** and we want it to be distributed into the Desktop folder of every user who access a FileWave controlled computer. What you would need to do is locate the original location in the Fileset Contents window, and drag that item into the final distribution location, as shown below:

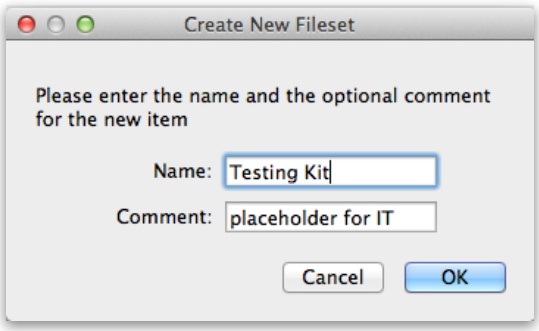


becomes…

This change will result in the *Key Info* folder and its contents being copied to every user's Desktop folder when they are on a FileWave system that this Fileset is associated with. A significant strength of this type of Fileset is that you can make changes to it at any time, update the model, and those changes propagate out to the associated clients, such as adding another document to the set, or replacing one.

Empty Fileset

Empty Filesets are best used for placeholders. You get an empty container that you can add content to at any time. This is an excellent Fileset to use as a 'kickstart' for Kiosk. You would create this Fileset, associate it with a client or group, and designate it as a Kiosk item. This would activate the Kiosk on your clients, and you can place any content in here that would be of use to your users. (There is another way to customize the Kiosk so that it is always visible. This is covered in the section on the Kiosk later in this chapter.)



Once created, you can double-click on the Fileset to view the content window and add items as needed.

Scripts in Filesets

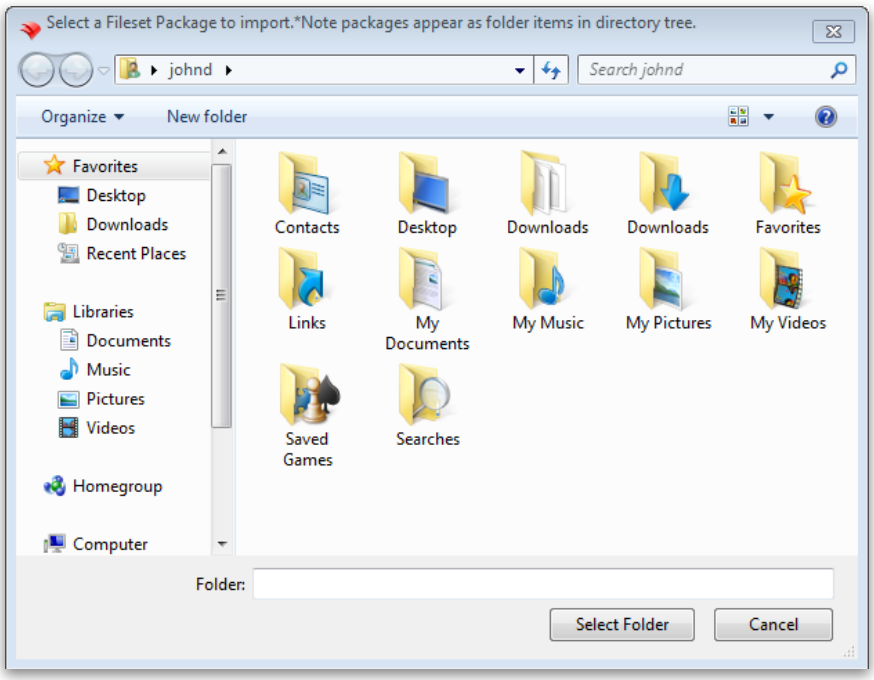
Empty Filesets can also be used to deploy scripts. You can create a script, save it as a *shell script* file, for example <myscript>.sh, and place that into a Fileset. The template for any script is simple:

```
#!/bin/sh

# Put any script content here

exit 0
```

You can use any of the common shell dialects, such as **sh, bash, tsch, or zsh**. By default, the script is executed once, by **root,** when the Fileset is deployed to the client device. You would set a path for the script to be placed in a location that allows the system to access the appropriate controls, such as in **/usr/local/etc/**. Once the script file is added to the Fileset, you can set its permissions and other variables using the **Contents** window - which is accessed by double-clicking the script file inside the Fileset.

Import

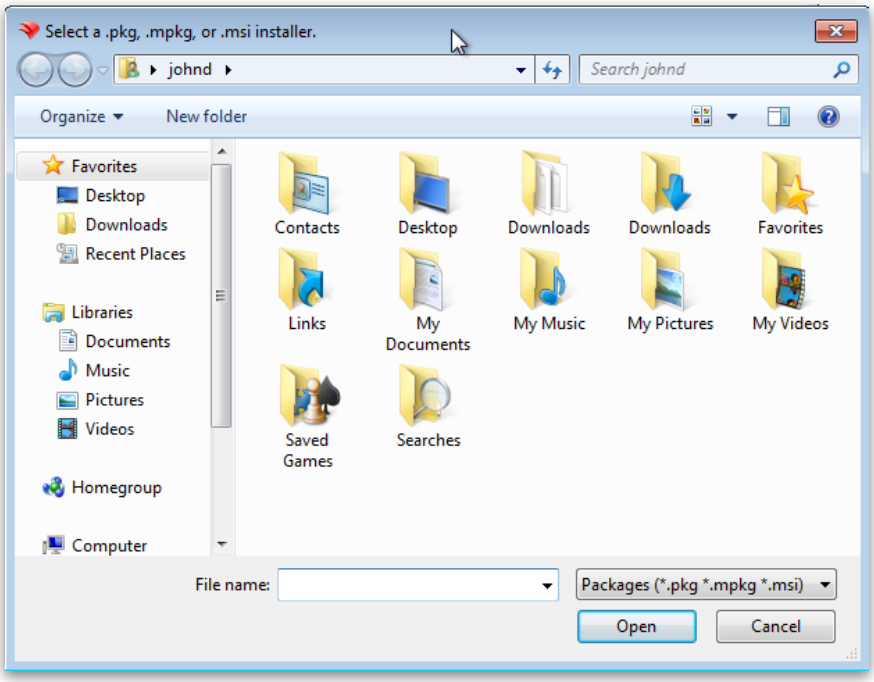
The *Import* Fileset is actually a dialog that allows you to import previously created Filesets. These could be Filesets that you created in another location, or Filesets downloaded from the FileWave Support site.



MSI / PKG Fileset

The one Fileset that does not store its contents as individual files is the *MSI/PKG* Fileset. For this Fileset, you select a downloaded installer for either Windows (.msi) or OS X (.pkg and .mpkg). When the Fileset is deployed to the client, upon activation it will run as an installer with local administrator privileges.

Under FileWave v10, Filesets based on **msi** will uninstall the contents when the Fileset is removed/disassociated. Instead of just removing the installer, the Fileset will perform an actual un-install process.



Windows based distributions may come pre-packaged in the Microsoft Installer format or MSI. Customizations to MSI files can be made through MST files or Microsoft Transform files. FileWave supports MSI and MST through its Patch Installer feature. Patch Installer Filesets are created by the FileWave Admin application by pressing the New Fileset button, followed by navigating and selecting an MSI file or by dragging and dropping an MSI file into the Filesets view of the FileWave Admin application. The MSI file must have a lower case MSI extension, such as *Application Installer.msi*, for the MSI file to be recognized by the Admin software.

MST is supported by modifying a Patch Installer Fileset. An MST file must be copied into the same directory in the Fileset Contents Window as the MSI file. (This location is generally *FileWave\FileWaveInstallers\Application.msi*). Additionally, the MST file must be named exactly the same as the MSI file with a lower case MST extension such as "*Application Installer.mst*".

Installations with Setup.exe Installers

Complex installations are contained in an executable file often named "*Setup.exe*". Examples include Hotfixes and other Security Patches from Microsoft. It may be simpler to deploy the executable file and have it run on the local computer rather than creating a Fileset based on snapshots. FileWave WinClient and FileWave Admin have features to handle the deployment of Setup.exe style installers.

The steps for this kind of deployment is as follows:

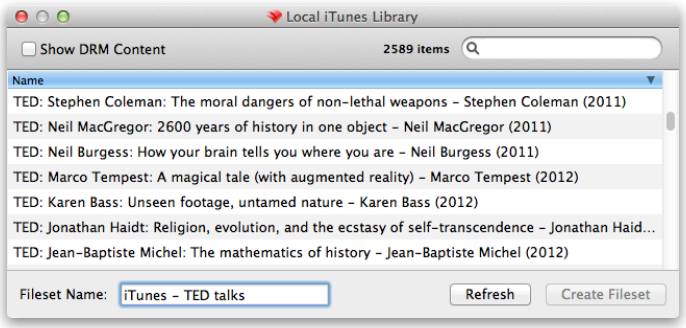
- Copy the Setup.exe file to the Desktop of the computer where the FileWave Admin program is running connected to a FileWave Server.
- Create a New Empty Fileset, give it a name and optional comment.
- Open the Fileset & uncheck the "Hide used folders" checkbox.
- Create a folder structure of where you would like the EXE file deployed. A good place is *Documents* and *Settings\All Users\Application Data\FileWave\Installers*.
- Copy the Setup.exe file from the Desktop of the Admin's computer into the folder created in the Fileset Contents Window. This will be the folder where the Setup.exe will be delivered to on the client computers.
- Select the Setup.exe file in the Fileset Contents Window and click on the Get Info button in the toolbar.
- Click on the tab labeled Executable.

- Check the checkbox labeled "Execute once when activated".
- Add any arguments or options to include as part of the installation process. Some times it is preferable to run installers silently. Many Setup.exe installers take a /quiet or /s or /silent argument.

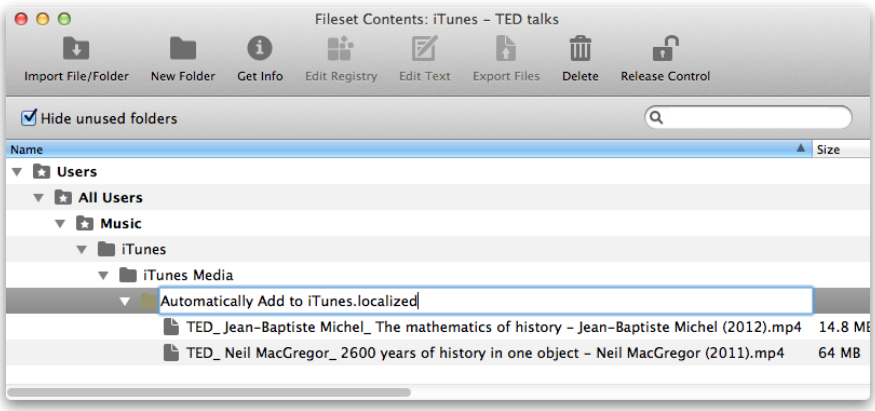
Note: If you are unsure about the arguments, try dragging the Setup.exe into a Windows Command Prompt window and pass the /h or /help or /? argument to see a number of argument possibilities.

iTunes Library Fileset

Being able to provide your users with non-DRM content from your iTunes library (content not protected by your AppleID) is a powerful tool for use in reference material and teaching. For example, you can select podcasts that are needed by your users and distribute those items directly into those user's iTunes library.



This type of Fileset shows the power of the Fileset technology. If you look at the content of this Fileset, you'll see the specific podcasts we added:



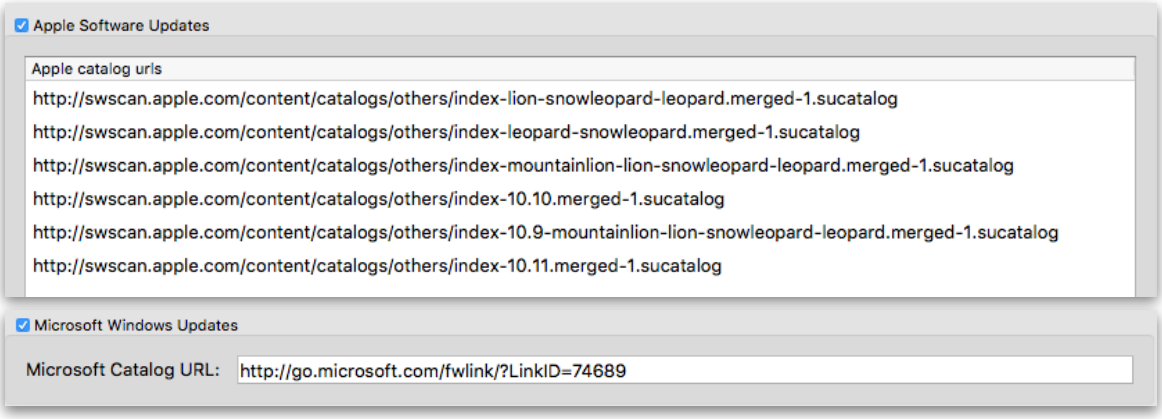
Note: The default location shows as "Automatically Add to iTunes" - with newer versions of iTunes and OS X v10.9+, you must add ".localized" to the path name.

The strength of this type of Fileset is that you can add and subtract content directly from this Content window. When the FileWave server model is updated, all clients associated with this Fileset will automatically get the newest content. The previous content will stay, since in iTunes, we can't tell if the user has moved any of the items (in this case, iTunes itself moved the items into the Podcasts folder); but the new content will get sent down, and new clients will only get the revised Fileset contents.

If you send content that has DRM, then the user will be asked for the content owner's AppleID when they attempt to play or access that content.

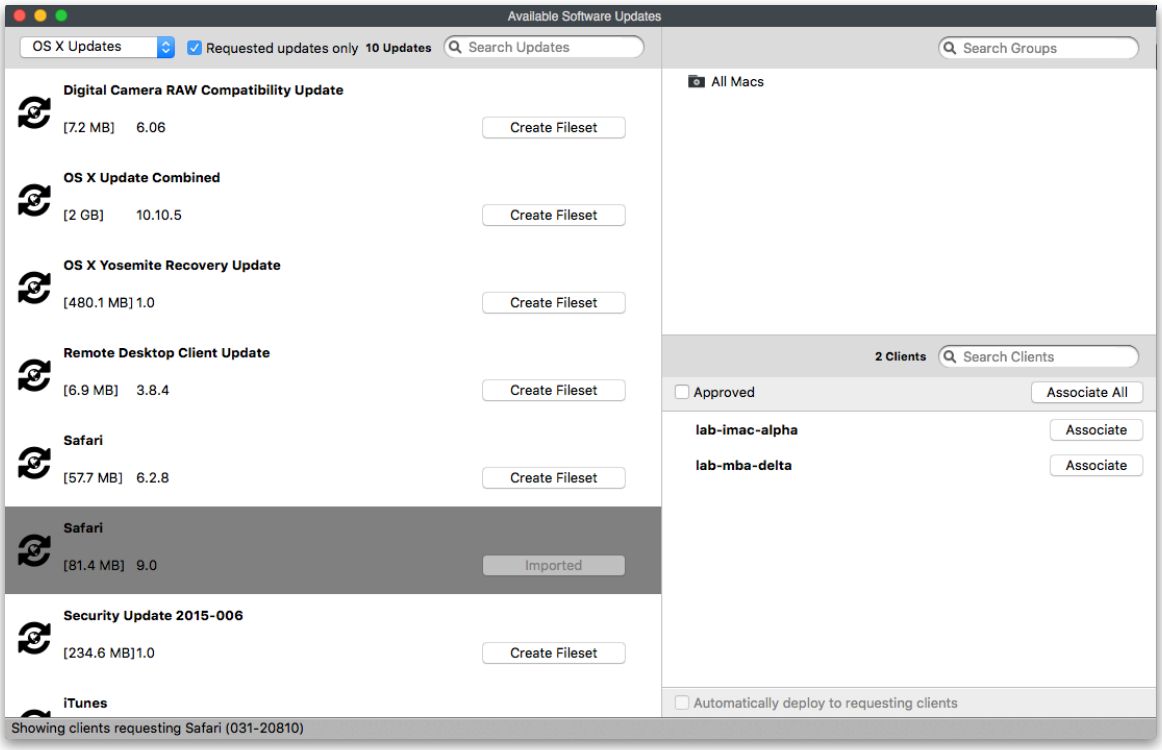
Software Update Fileset

FileWave allows you to capture the software updates provided by both Apple and Microsoft through their software update mechanisms and convert those updates to Filesets. The list of software update servers used by both providers is located in the FileWave Preferences under the General settings: (current as of Oct 2015)

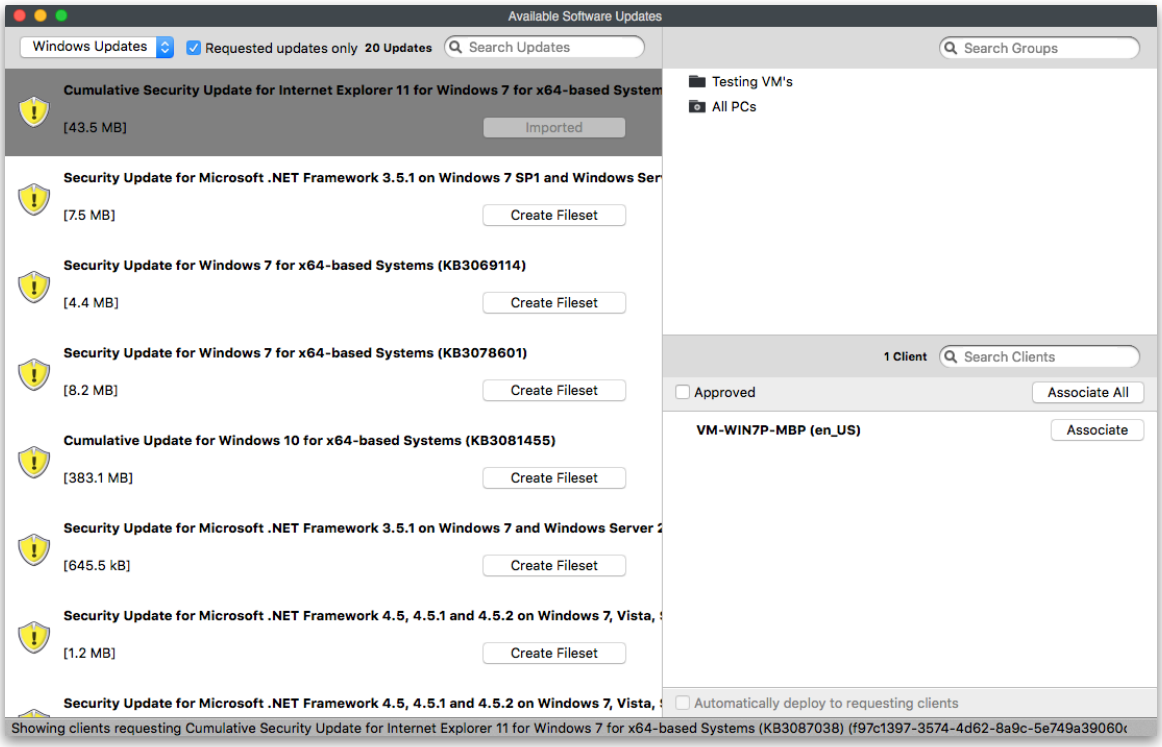


These URLs can be edited as changes are made. The updates do not include items that Apple is providing only through the iTunes or Mac App Stores. If you are deploying a large number of OS X and/or iOS devices, you should also plan to add one or more OS X servers running the Caching server process. This process caches all requests for Mac Store and iTunes Store content locally as devices request those items. See https://www.apple.com/support/osxserver/cachingservice/ for more information.

When you choose to create a Software Update Fileset, you will see a window that shows you either every software update available for the selected OS platform (iOS, OS X or Windows), or just the updates requested by your clients. With FileWave Admin, you will be able to capture the updates you want as Filesets. This allows you to test updates on your test clients before releasing them to your production systems. You can stage the updates at the clients, complete your testing, then activate the updates if testing is successful, or delete the updates if there is an issue.

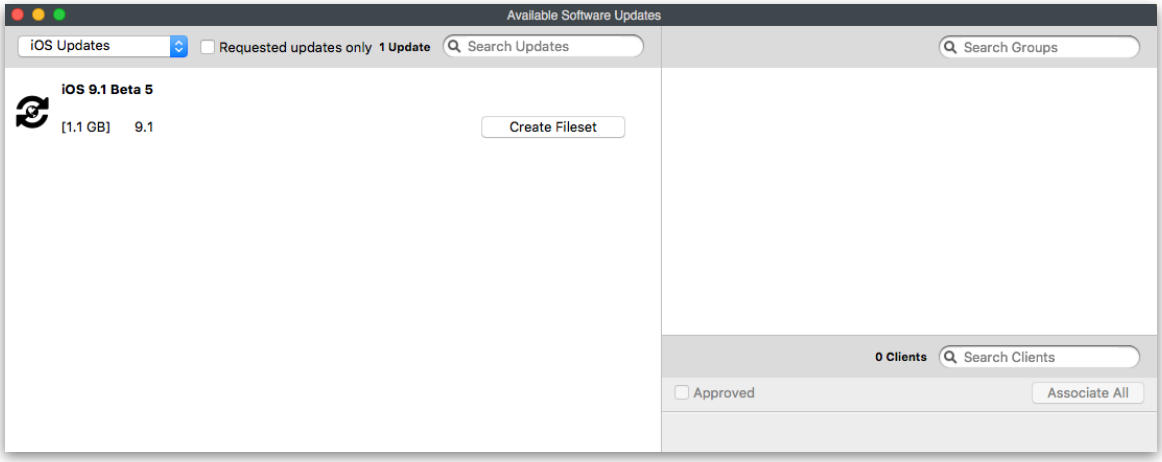


Above is a list of all OS X updates, with one update shown as already imported as a Fileset. Below is the same view of the Windows software updates, with just the requested updates and the client systems who have asked for these items.



You can filter the selections by choosing a specific group in the Groups window (upper right). For example, by selecting the “Testing VM’s”, only the devices in that group would be visible, along with any updates requested by those devices..

New to FileWave v10 is the ability to see iOS updates. The iOS updates will show up here. **Note: These updates do not include all of the items from the iTunes or App Store that need regular maintenance.**

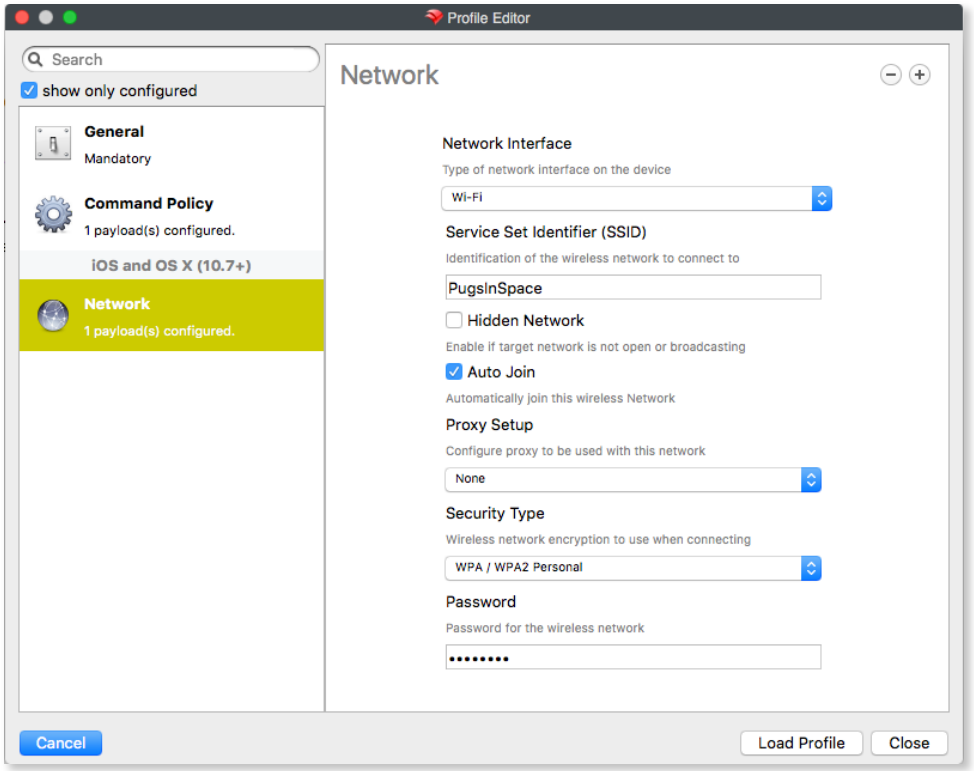


Once you create a Fileset from any of the updates, you can then select the clients to associate with that update. You can also choose to associate all of your clients with an update, approve the update to be associated by sub-administrators, and even choose to automatically deploy the selected update to any client who would request that update in the future.

Be careful of manually associating Software Update Filesets with any client. You should associate the Filesets with requesting clients only. As always, test any updates on a non-production device before mass deployment.

Profile Fileset

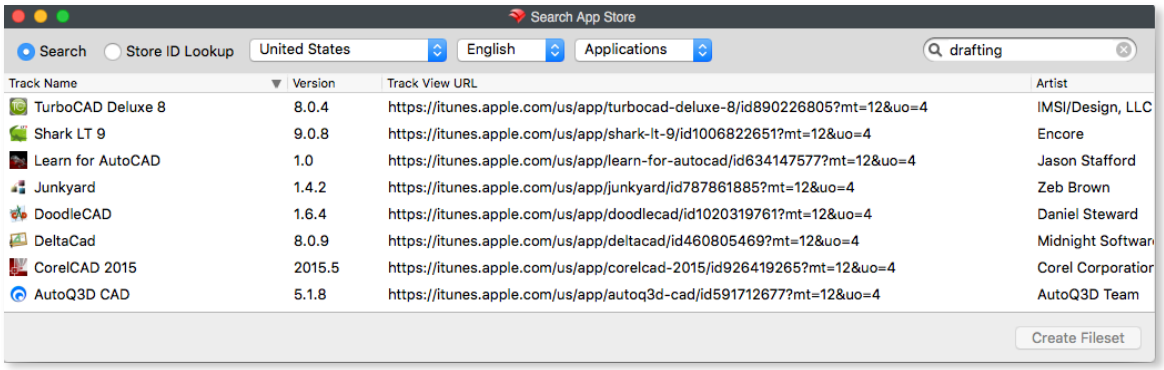
The Profile Fileset contains all of the settings used for both desktop and mobile device management on OS X and iOS. Items that used to covered in the *Policies* Fileset (pre-FWv7) are now merged into this single interface. You can create management settings for your legacy Macs, current Macs, and iOS devices using the same tool. Settings that will be sent to pre-Lion OS X systems will be converted automatically to *Managed Client (mcx.plist)* files as if you had used Apple's Workgroup Manager (requires the older version of the FileWave client). Settings for current OS X systems will be sent as profiles. iOS settings will be sent as profiles. The selection in the Desktop Fileset window is identical to the one in the Mobile Fileset window.



Details on creating and configuring Profile Filesets are in chapter **8** on *Modern Device Management*.

App Store Fileset

You can create Filesets for OS X clients using content from the Mac App Store. As with the iOS App Store Fileset, you are not actually storing the application or eBook inside the Fileset; but providing the URL to the content online.



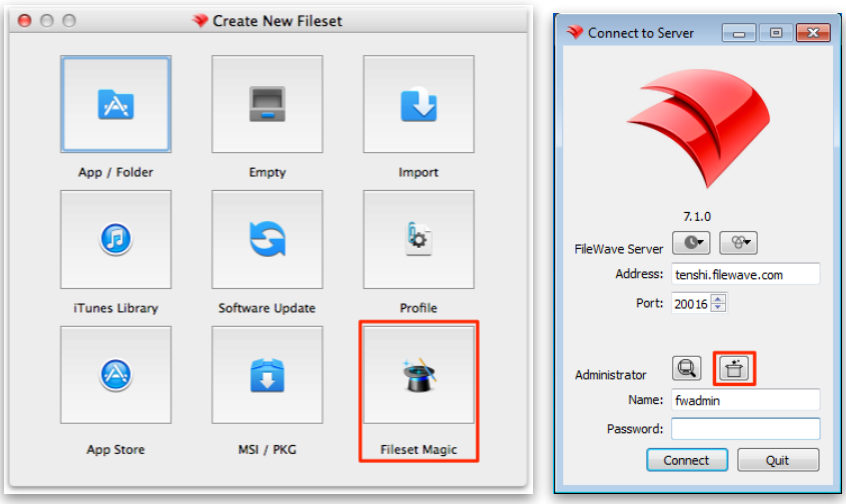
Filesets created in this manner can be distributed to a user's device and require the user to enter their AppleID in order to access the content, or you can link the Fileset to the Apple VPP store and provide either redeemable codes or managed distribution licenses for the provided content. The process of linking the Fileset to VPP is covered in-depth in chapter **7**.

With FileWave v10, you will have the ability to associate App Store content directly to a device, or to a user's AppleID as part of a VPP distribution.

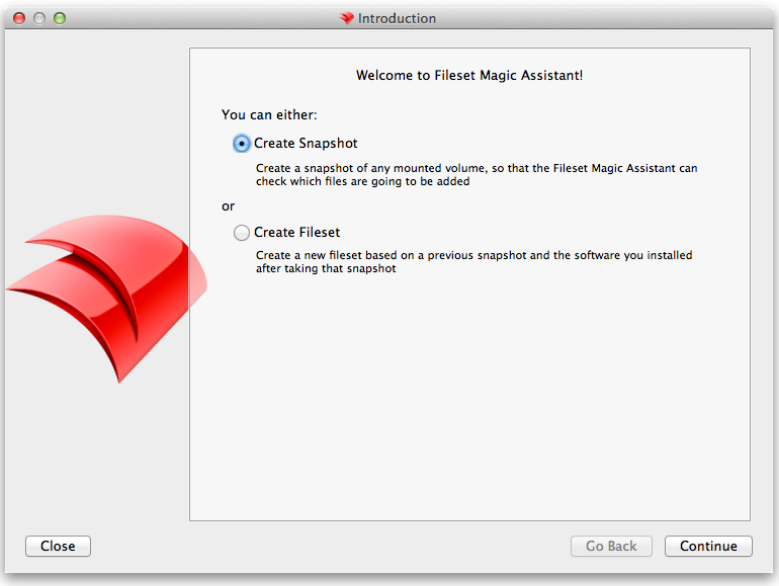
Fileset Magic

Sometimes, the content you want to distribute cannot be found in a completely deployable state. Fileset magic allows you to build a Fileset from system snapshots taken before and after creating the application and/or content you want to deploy. For example, if you are deploying software downloaded from online, and it requires several updates before it is current, then you would use Fileset Magic to create a Fileset of the final custom installation.

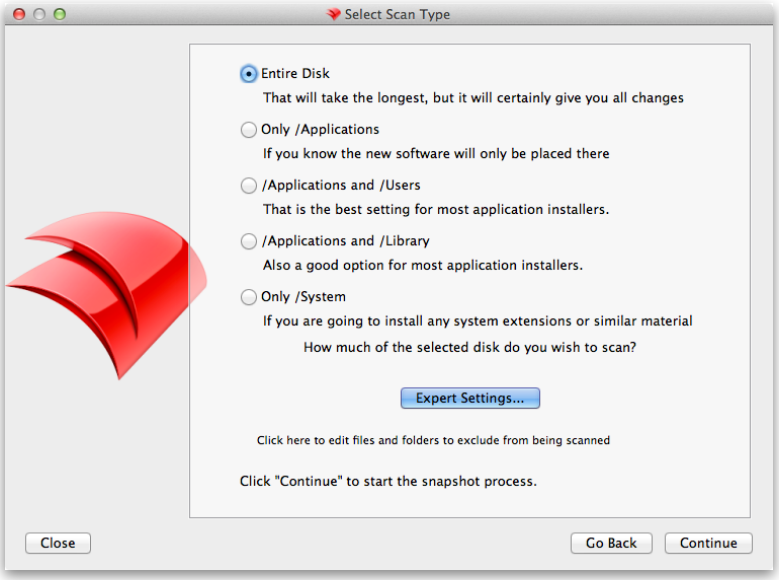
Fileset Magic on OS X is accessible from FileWave Admin; but there is a special version of the Admin application for use with Fileset magic - labeled **FileWave Admin (root)** - which runs as a root process in order to capture all possible file system changes needed to build a complete distribution. For Windows administrators, Fileset Magic can be accessed from the FileWave Admin login window as well as inside the Admin application. This allows you to run a Fileset magic snapshot without the FileWave Admin interfering with Registry changes.



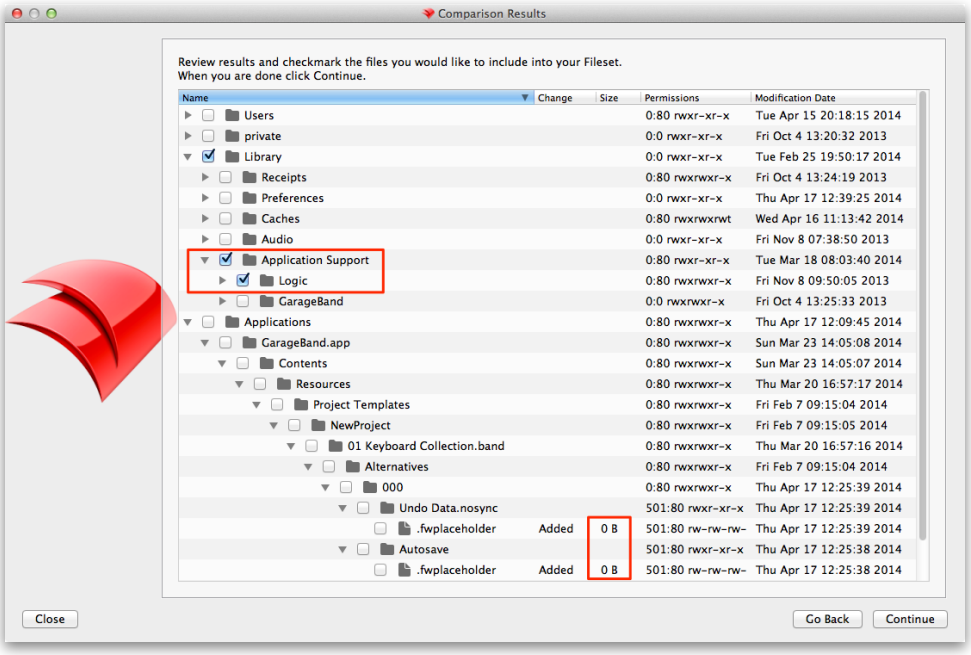
Note: When using Fileset Magic, you should quit all other running applications besides the required installers or updaters for your custom Fileset.



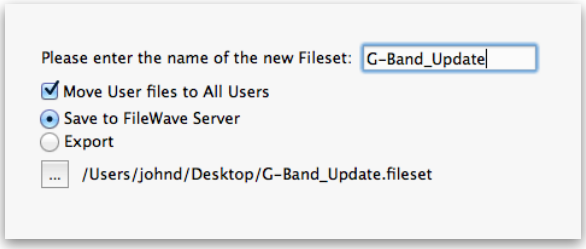
Once you have quit all unneeded applications, you create a snapshot of your system. It is a good practice to use a clean system for this process instead of your normal administrator machine. Try to keep the device as uncluttered as possible, even reformatting it between projects. This will ensure that you are working with the files you want to add and avoiding dealing with all the additional files that get created on a production system from normal use.



Next, you choose the level of scan desired. Depending on what you are installing or modifying, you may need to deep scan the entire system. If you know where the contents are going to be placed, you can narrow down the scan. The **Expert Settings…** button lets you choose exactly what folders/directories you want scanned.



Once the scan is complete, you perform your installs and updates as needed. Run the second scan to get a comparison between the two scans, and choose which files you want to keep in your new Fileset. Pay careful attention to 'zero byte' or empty files that were created; but are not used for your Fileset. Once you have picked the files you need, you will name the Fileset and save it.



You can also choose to move any files that are needed by all users from the local account where they showed up into the **All Users** location in Fileset Contents. This would be general user-level application support files or specific settings for a local user. As with the **App/Folder** and **Empty** Filesets, you can open the Fileset by double-clicking on it and edit / add / delete contents as needed.

For Windows systems, you will need to pay close attention to the Registry. Make sure you do not overwrite any Registry items that existed prior to your Fileset creation unless you are absolutely sure those changes are needed. You should also try to disable any virus-scanning software, backup utilities, and other software that might generate unnecessary files or Registry changes during the construction of the Fileset.

Installations with Setup.exe Installers

Sometimes complex installations are contained in an executable file often named "Setup.exe". Examples include Hotfixes and other Security Patches from Microsoft. Usually, it is simpler to deliver the executable file and have it run on the local computer rather than creating a Fileset based on snapshots. FileWave WinClient and FileWave Admin have features to handle the deployment of Setup.exe style installers.

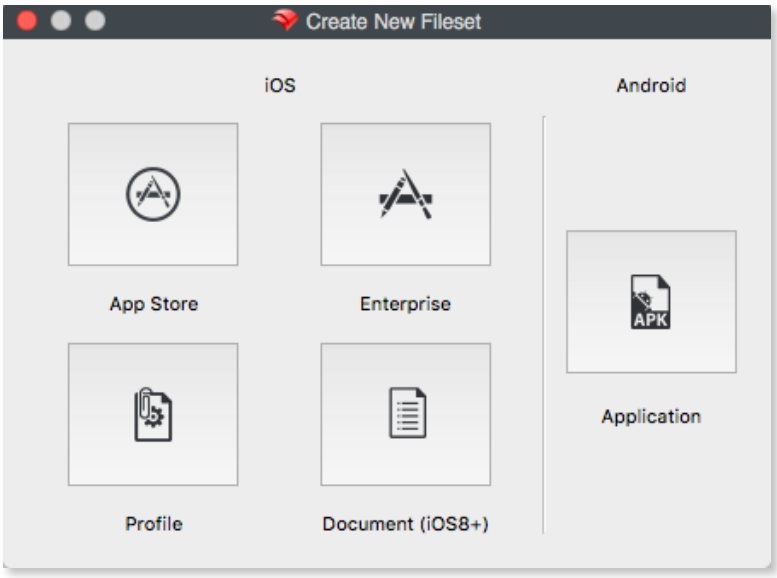
The steps for this kind of deployment are as follows:

- Copy the Setup.exe file to the Desktop of the computer where the FileWave Admin program is running connected to a FileWave Server.
- Create a New Empty Fileset, give it a name and optional comment.
- Open the Fileset & uncheck the "Hide used folders" checkbox.
- Create a folder structure of where you would like the EXE file deployed. A good place is Documents and Settings\All Users\Application Data\FileWave\Installers.
- Copy the Setup.exe file from the Desktop of the Admin's computer into the folder created in the Fileset Contents Window.
- This will be the folder where the Setup.exe will be delivered to on the client computers.
- Select the Setup.exe file in the Fileset Contents Window and click on the Get Info button in the toolbar.
- Click on the tab labeled Executable.
- Check the checkbox labeled "Execute once when activated".
- Add any arguments or options to include as part of the installation process. Many times it is preferable to run installers silently. Many Setup.exe installers take a /quiet or /s or /silent argument.
-

Note: If you are unsure about the arguments try dragging the Setup.exe into a Windows Command Prompt window and pass the /h or /help or /? option to see a number of argument possibilities.

6.3. Mobile Filesets

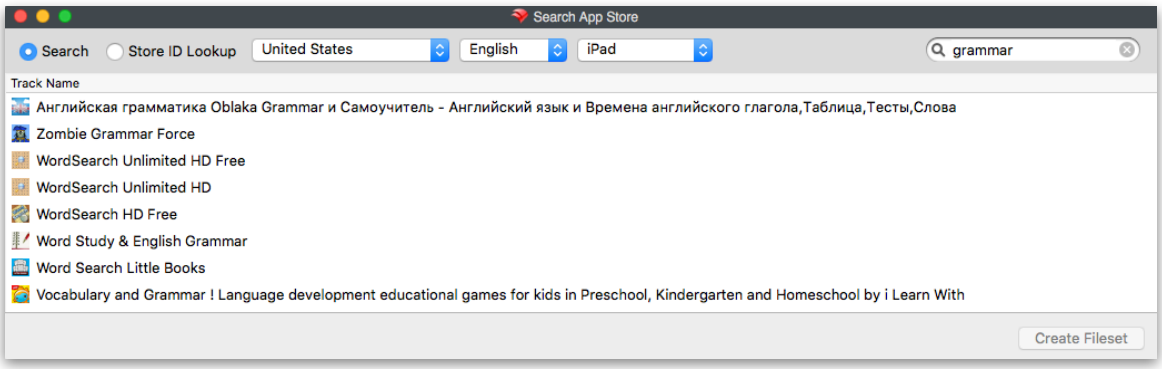
For your mobile devices, the selection of possible Filesets is much smaller. You can choose between App Store, Enterprise, Profile, or Document Filesets, and Android Application Filesets.

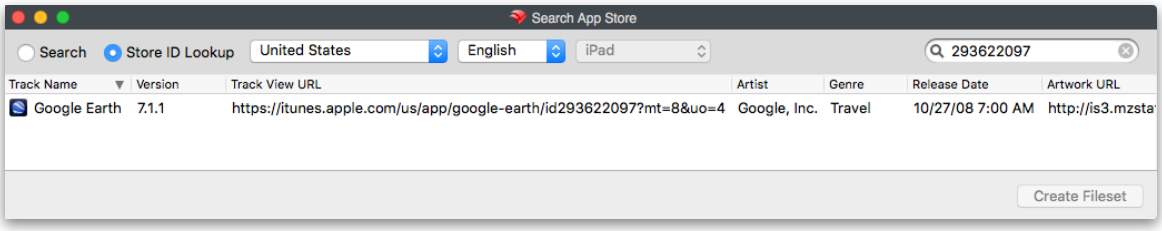


App Store Fileset

The App Store Fileset was designed around the BYOD or 1:1 deployment models with iOS devices. This Fileset can be used for two types of distributions - ad hoc or VPP. In an ad hoc distribution, you are sending a link to the application or eBook to the end user. This can be done either directly or by using the Kiosk (recommended). The user will then be required to enter their AppleID to purchase and install the item. For a VPP distribution, you are attaching either a code or a license to the Fileset, which will pre-authorize the item for that user. FileWave v10 supports the ability to associate VPP application Filesets either to an AppleID, or directly to a device. More on the use of VPP for distributions in chapter **7**.

You enter either a name or an iTunes ID code to search for the content to be deployed:



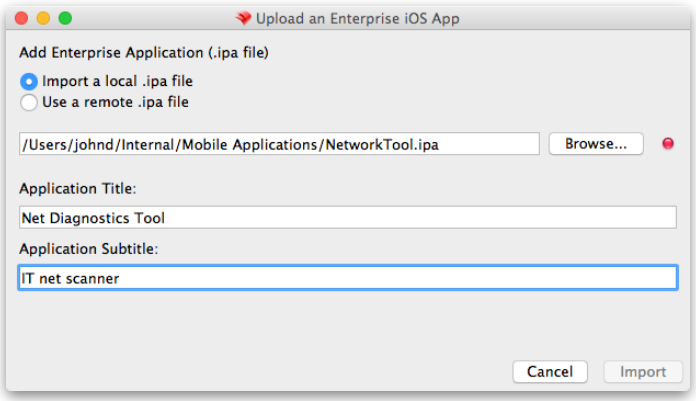


Once you have created the Fileset, you can double-click on it to view extra settings, such as setting Kiosk information. This Fileset does not download the item - application or eBook - but maintains a link to the iTunes Store for that item.

Enterprise Fileset

The Enterprise Fileset is designed for you to distribute **internally created** content. There has been confusion around the use of this Fileset to distribute Apple App Store or iTunes Store content - Apple does not condone or support this method, and FileWave will not support this method either. From a technical perspective, the DRM used on Apple content has been changing and could render any application distributed using this process as invalid. You would get reports of previously functional applications asking for the AppleID of the item's owner.

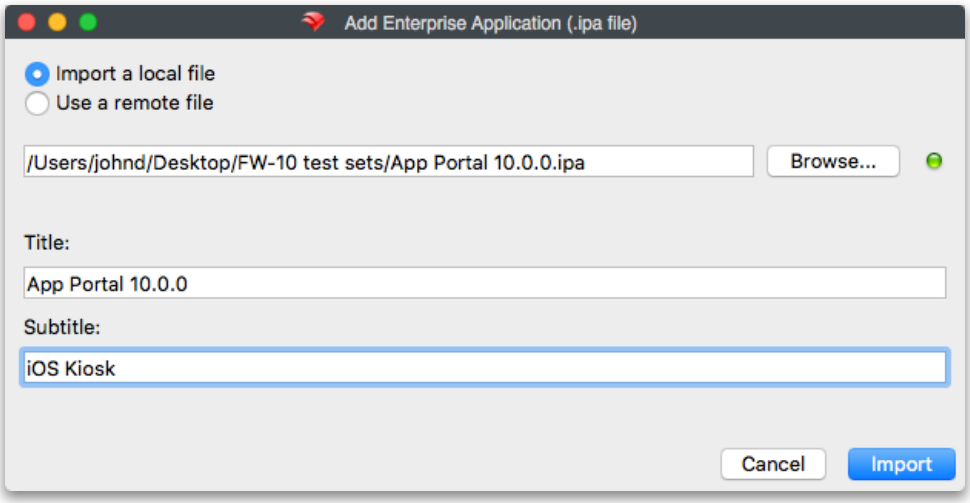
You can easily distribute software you have created with this Fileset by locating the **.ipa** file of the application on your administrator system and adding it to the Fileset list. All of the custom controls and settings are available for use with this distribution. You can select a remote location for the .**ipa** distribution. Normal configuration is to import the **.ipa** into your FileWave server and wrap it up as a Fileset. The new method allows you to enter a URL to the **.ipa**, such as a web server, where the item can reside. This can be a good practice for large distributions of a critical application where the FileWave server itself may not have the horsepower to handle all the traffic.



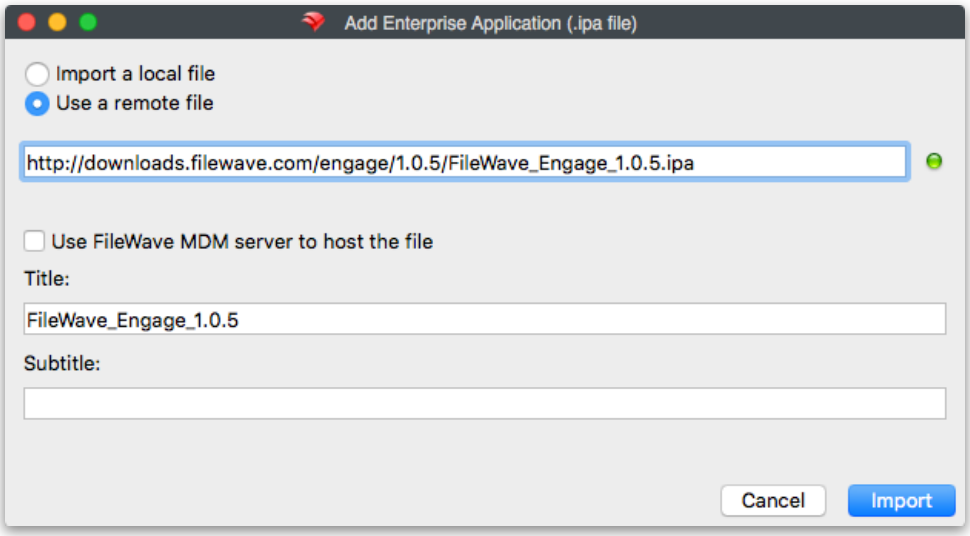
Special Cases - the FileWave Enterprise App Portal (Kiosk) and Engage for iOS

FileWave makes the native iOS App Portal available from FileWave Support for distribution as a Fileset, as well as the **Engage** for iOS application. There are two methods for sending out these items.

Local distribution puts the app into the FileWave server as a Fileset. Keeps all the traffic local and works well for a sub-1000 unit deployment. Remote distribution pulls the app from the FileWave support servers. This is a best practice for large (>1000 unit) deployment over a wide geographic region. The local method looks like this:



The remote distribution references the URL of the remote location for the **.ipa**:



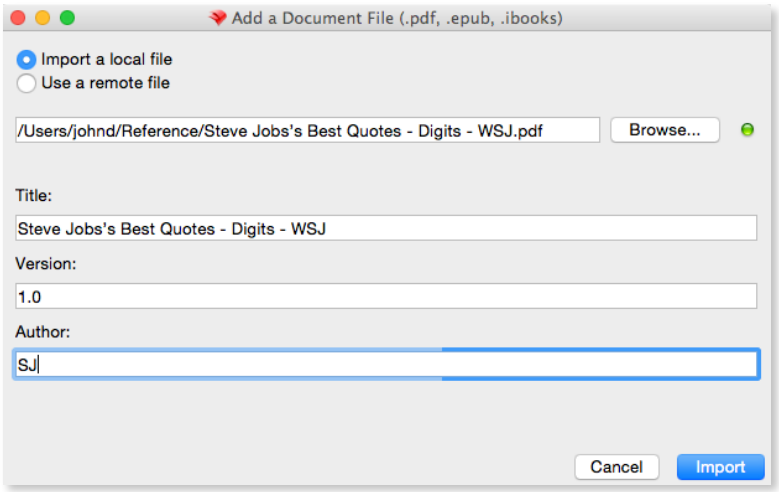
Profile Fileset

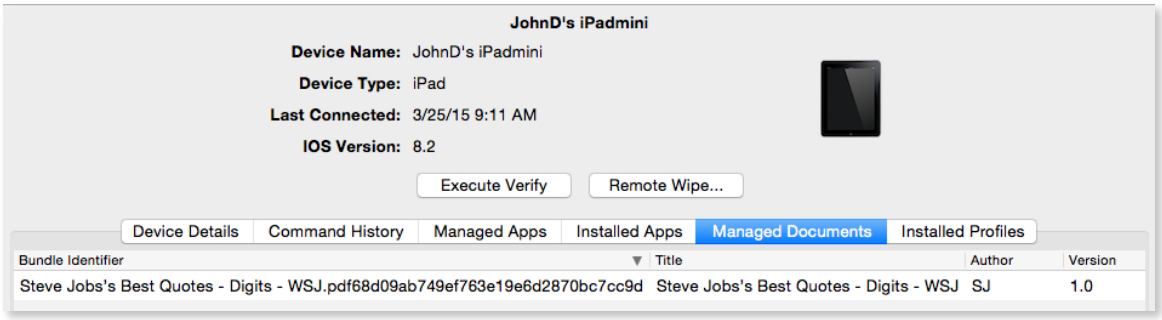
The Profile Fileset takes you to the same window you see when you select Profile Fileset in the **New Desktop Fileset** tool. Profiles supported in FileWave cover iOS versions from iOS v7 through iOS v9. The specific profiles are broken out into sets based on newer capabilities in more current versions of iOS.

Detailed information on Profiles is covered in chapter **8** of this manual.

Document (iOS 8+) Fileset

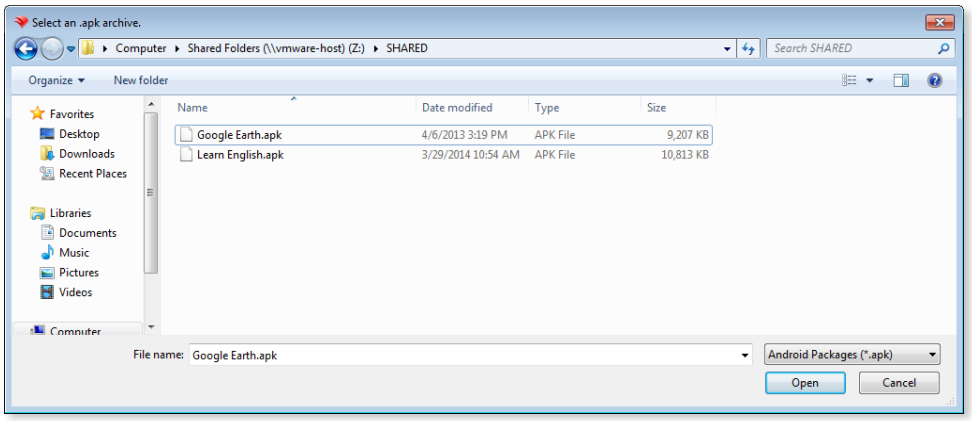
With the ability to set “Open in…” characteristics in iOS 8+, you can also create Filesets with document content. This type of Fileset can contain **pdf**, **ePub**, and **iBooks** formatted items. They are delivered to the iBooks Library as a **managed document** which means it can be given, and taken away.

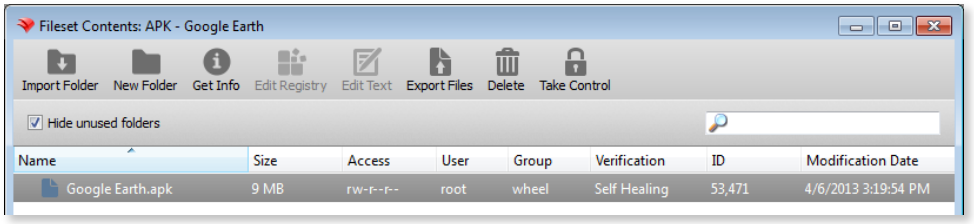




Android Fileset

You can add Android devices as clients and deploy Filesets to them. Unlike the process for iOS and OS X, the process for creating an Android Fileset resembles the Enterprise method. You must locate the application or content you wish to deploy in **.apk** format online, download it, then import it into FileWave to make the Fileset.

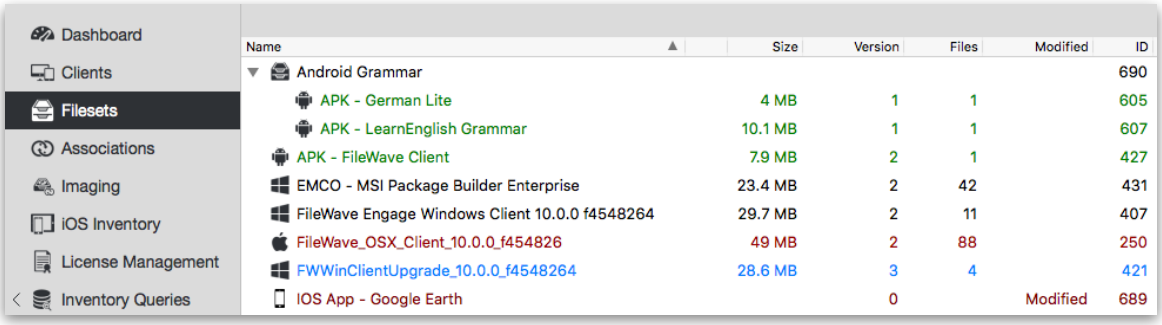




The Android Fileset can be set to self-heal, scheduled for distribution, and re-installed as needed. All Android Filesets should be designated as Kiosk items.

6.4. Fileset Groups

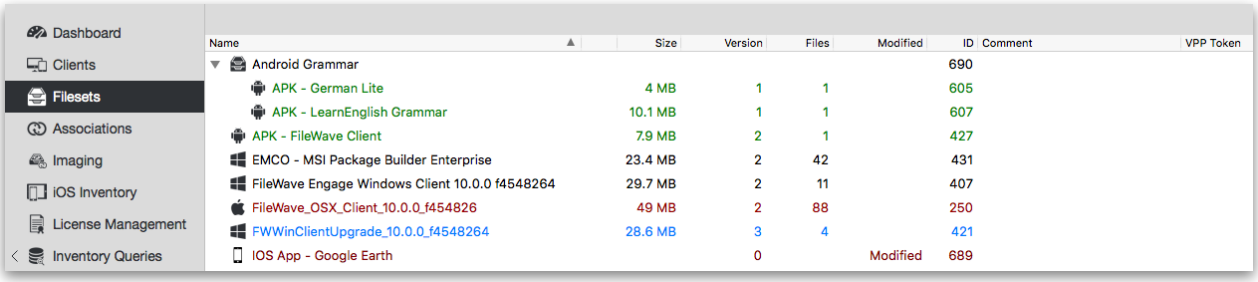
You can cluster different Filesets into groups for easier deployment workflows. Fileset Groups can be used to organize logical groups of Filesets into larger distribution units. Fileset Groups can be nested into other Fileset Groups, much like Client Groups. Once a Fileset group is created by clicking the New Fileset Group button, existing Filesets may be dragged and dropped into the group. Filesets and Fileset Groups cannot be cloned, so they can only reside in one group at a time. Fileset Groups may be associated to a Client or Client Group. When a Fileset Group is associated, all Filesets contained within the Fileset Group will be distributed upon model update.



Note that when you assign or associate Fileset groups to client groups, the listing of Filesets associated may not show up when looking at individual clients. Fileset Groups allow you assign the deployment times or setting as a Kiosk item to be mass applied to several Filesets at the same time. There is more information on displaying lists of associated Filesets in the section on Associations.

6.5. Advanced Editing - Contents, properties, settings, and dependencies

While you can create a Fileset and associate it with a client without doing any additional steps, your ability to customize the Fileset contents, specify its properties, and alter its settings gives you a tremendous amount of flexibility in your deployment models. Once you have created a Fileset, it will appear in the main **Filesets** window. The basic properties of that Fileset are shown in the window menubar:



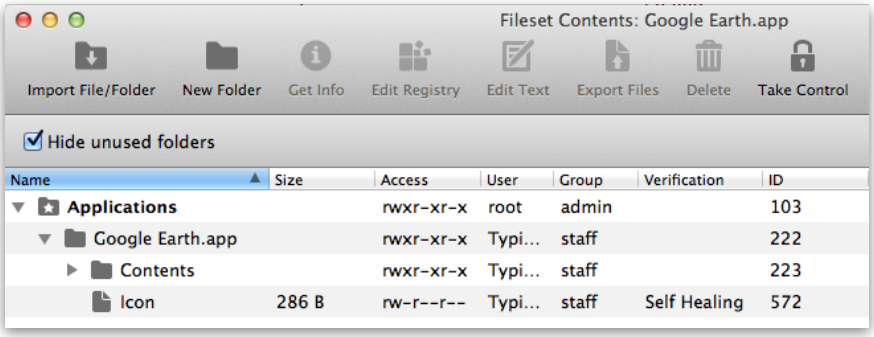
- *Name* - the title of the Fileset you created

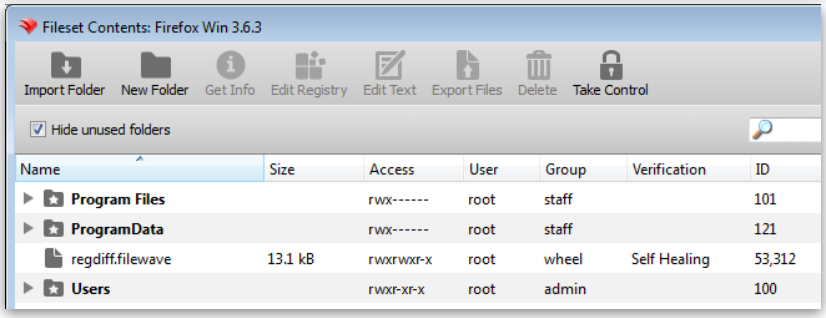
- *Size* - the size of the Fileset in Bytes as it is stored on the FileWave server. This can also affect your Boosters in terms of how much storage they will need to handle cached Filesets
- *Version* - When a Fileset is first created, it is version “0” until you edit the Fileset and update the server model. As you make changes to the Fileset, its version number will increment.
- *Files* - the total number of files contained in the Fileset
- *ID* - a unique identifier used by the FileWave server to keep track of your Filesets
- *Comment* - any text you enter to add information about the Fileset
- VPP Token - designates which of your Apple Volume Purchase Program tokens is assigned to that Fileset

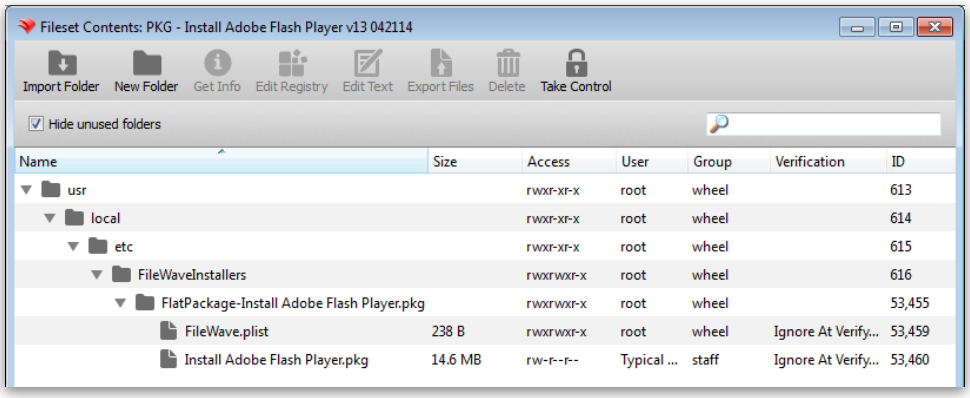
The contents of a Fileset can be edited and altered as desired, depending on the type of Fileset. You can get specific information on items within a Fileset in order to customize its behavior when distributed. By double-clicking on a Fileset, you will see one of three different windows depending on the Fileset type - desktop, iOS app, or OS X app / iOS book. You can also use the search field to find specific Filesets.

Desktop Fileset contents

The Desktop Fileset contents are the specific items to be installed within their designated paths. Examples are:

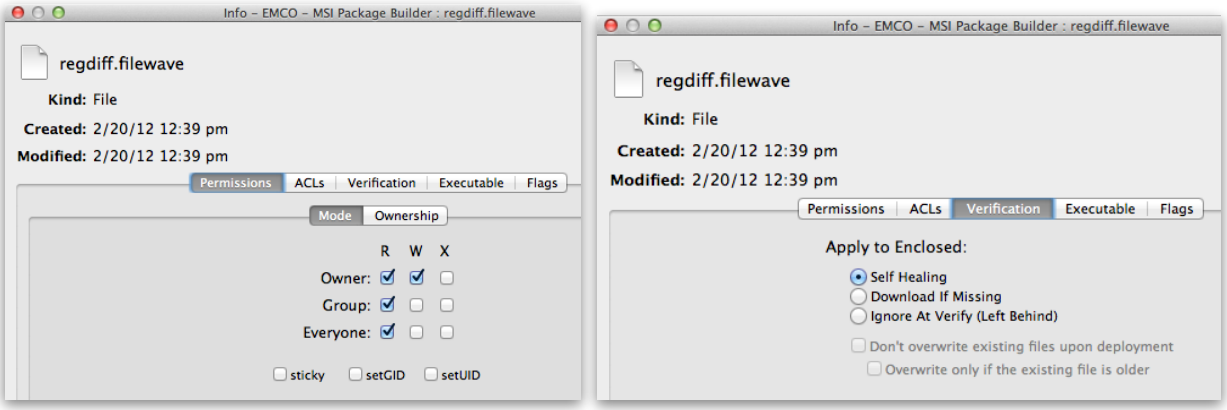






You can add items to the contents with the **New Folder** and **Import Folder** buttons. You can also remove any items that you are sure will not be needed in the final Fileset. Other key tasks in Contents are “Get Info”, “ACLs”, “Verification”, “Executable”, and “Flags”.

By double-clicking on a specific item or selecting an item and clicking on the **Get Info** tool, you can inspect file level information. It includes basic file information, permissions, ACLs if any are in use, Verification settings, script Executable details, and Flags that can be set.



FileWave, by default, sets many of these values correctly for the type of Fileset you are distributing. It is important, however, that you understand the **Verification** settings and how they impact the Fileset.

Verification

There are three primary verification settings - “*Self Healing*”, “*Download if Missing*” and “*Ignore At Verify (Left Behind)*”. Each of these settings causes the related file to behave differently once it is deployed.

- *Self Healing* - a file designated as self-healing will always be repaired or replaced by the FileWave server if it is altered in any way. If you have items deployed that require their contents remain unchanged and intact at all times, you would set the files to be self-healing.

- *Download if Missing* - this setting will force a client to re-download the file if the FileWave client reports this portion of a Fileset as missing. This is a lesser setting than self-healing in that the file will not be replaced if it has been altered; but only if it is deleted.

- *Ignore At Verify (Left Behind)* - Some files need to be dropped onto a client and left alone. This setting tells the FileWave client to ignore any changes in this portion of the Fileset during a verification. An example of this is content sent to the iTunes Library on a client. The content is sent to the “Automatically Add to iTunes” folder and iTunes then moves that file to the appropriate category area, such as Music, Podcasts, Movies, etc. If the file was not set to be ignored, then every time FileWave verified the Fileset, it would send another copy of the item.

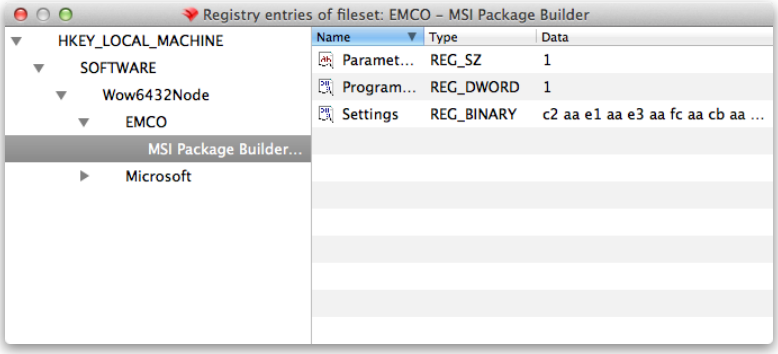
- *Don’t overwrite existing files upon deployment* - this setting can be chosen to go with either the *Download if Missing* or *Ignore At Verify*. You can tell FileWave to not write over top of any files that already exist when the Fileset is activated. This could be used to avoid replacing a document or file that was part of an earlier Fileset; but has been edited since it was distributed.

- *Overwrite only if the existing file is older* - this setting is a subset of the one above in that you might choose to allow older files to replaced only by newer versions of the same item.

Note: All file comparisons are done by filename and modification date.

Edit Registry

When you are working with Windows Filesets, you may need to explore the Registry entries. Within Fileset Contents, you can select the registry file and edit the contents online. If you need to distribute a Registry file, you can add one to an empty Fileset.

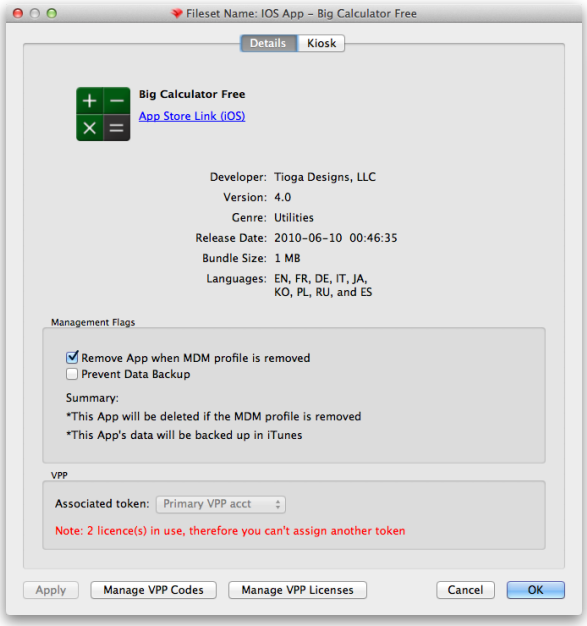


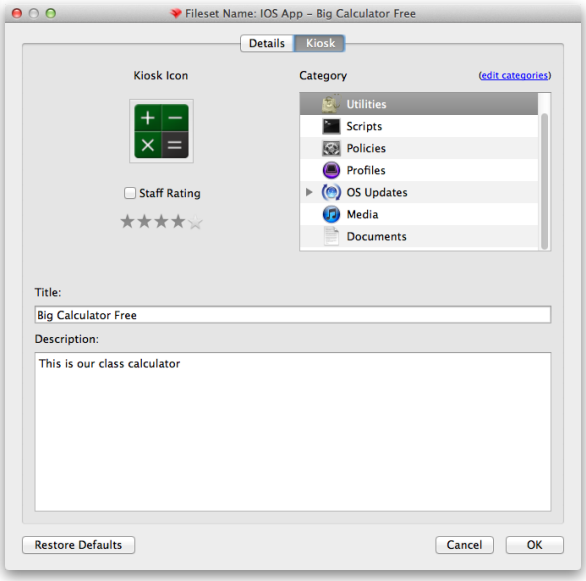
- *Edit Text* - you can edit many of the text based files in a Fileset directly. In FileWave/Preferences, you will see all of the various file type extensions that are supported. This is a very handy process when you need to tweak a script or a property list.
- *Export Files* - any file in a Fileset can be exported for use elsewhere. This capability can be used to open a complex Fileset and export portions of it for use in another Fileset.

iOS App and Enterprise Fileset contents

Filesets for iOS applications are focused more on behavior and end user information than actual file level content. The content consists of two panes - Details and Kiosk.

Details contains general application information, management flags, and VPP information. The management flags include the ability to force application removal when the MDM profile is removed, and the ability restrict application data from being backed up in iTunes. VPP shows the possible connection with the Fileset and a VPP account. A warning is shown if a VPP token is associated with the application noting that the Fileset cannot be attached to a different VPP account token.

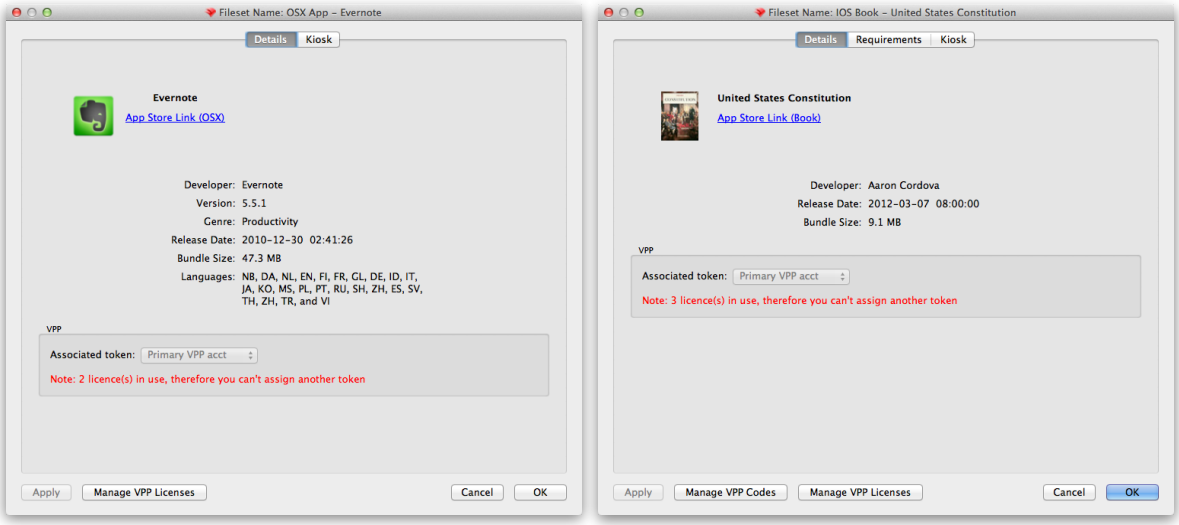




Kiosk displays the information from the iTunes Store, online review ratings, and allows you to choose a category for the item when displayed in the Kiosk. You can edit the text of the application title, as well as the description. This allows you to personalize the information for your organization versus using the marketing material provides by the developer to the iTunes/App Store.

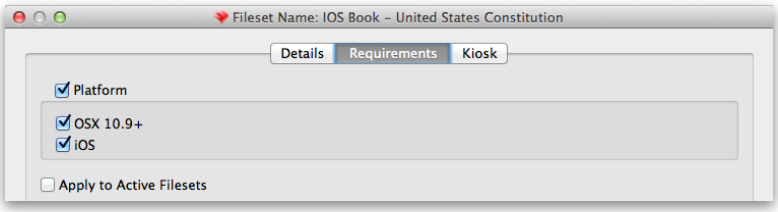
OS X App / iOS book Fileset contents

Application Filesets for OS X and eBook Filesets contain the same type of content information in the Details pane, to include the VPP token information. The Kiosk pane contains the same information as discussed in the iOS App Fileset contents.



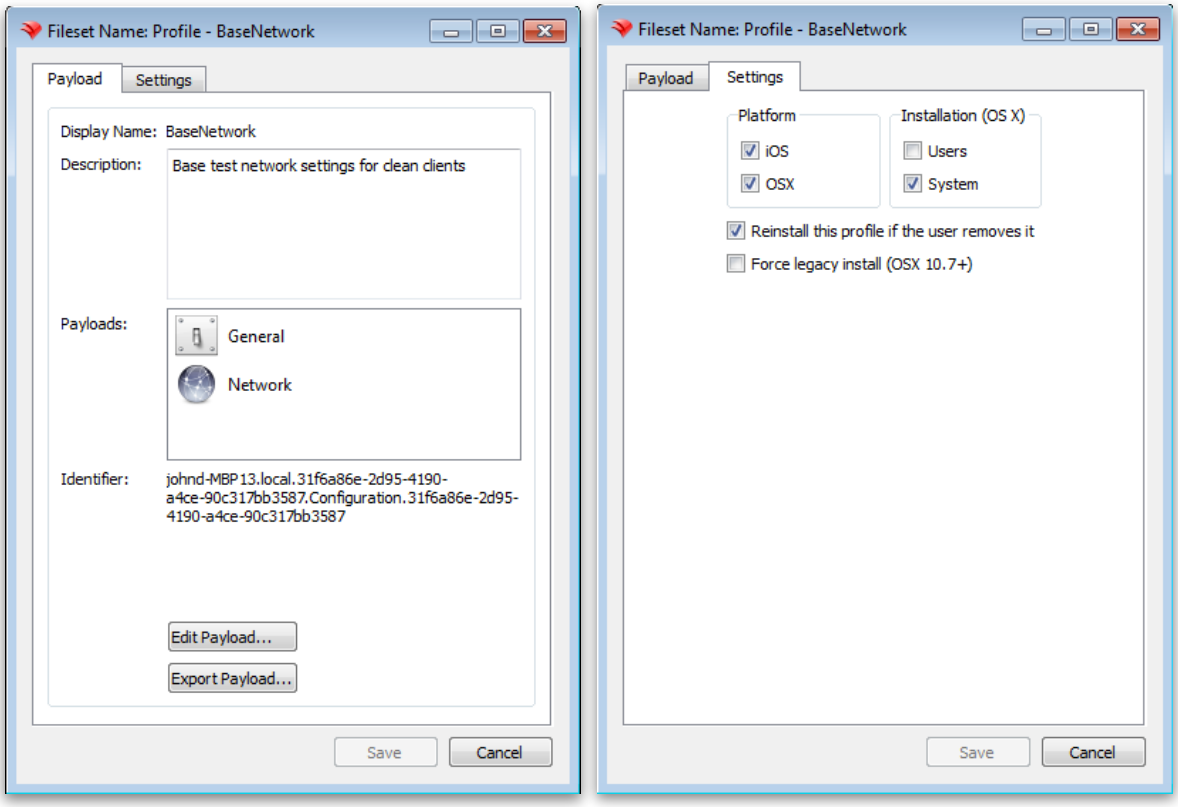
The Requirements pane determines the platforms the eBook can be distributed to and allows you to retroactively change these settings on actively deployed Filesets. Selecting *Apply to Active Filesets* lets you retroactively correct Filesets that are deployed.

Kiosk settings are the same across all Fileset types. You can set the category of the item, and edit the title and item description to better match your organizational needs. If you select *Restore Defaults*, the item title and description will revert to what is posted in the iTunes/App Store online.



Profile Fileset contents

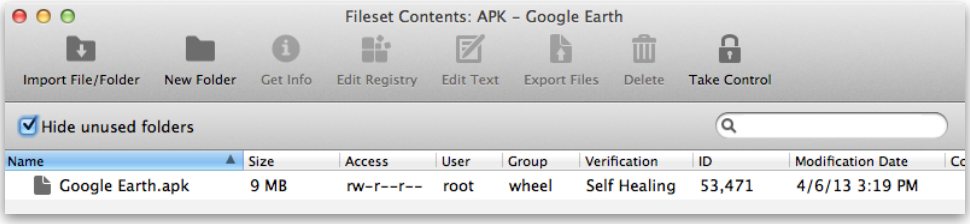
Filesets for desktop/mobile device management have a simple contents window. You can view the various payloads that are contained in the profile, edit the payloads, export payloads, and choose the device settings. Settings includes platform choices which must match the categories in Profile Editor. The installation choice determines whether the profile will be activated at system level which is prior to Login Window, or at user level which is at Finder launch. You can also force the profile to be deployed as an **mcx** property list to newer OS X systems, and force the profile to reinstall if the user removes it.



Details on profiles and configuring them are in section 8 **Client and Mobile Device Management**.

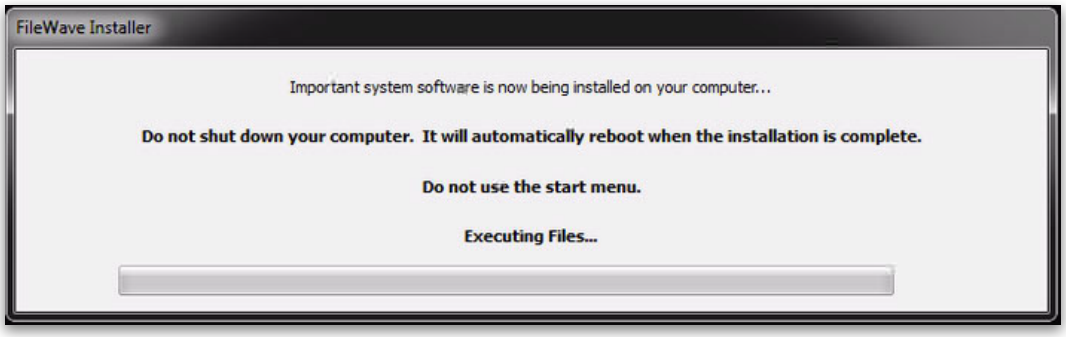
Android Fileset contents

The Fileset created for Android contains only the **.apk** file. The file cannot be relocated, and other files should not be added to the set. The *Get Info* button exposes the permissions and other settings; but those values should not be changed from the defaults.



Fileset Properties

Once you have created a Fileset, you can access a wide range of properties that enhance the effectiveness of that Fileset in your deployment. The properties available vary depending on the specific type of Fileset. In most cases, the information presented does not need to be altered or edited; but this information is presented to allow you to understand the depth of control you have over your file level deployments.

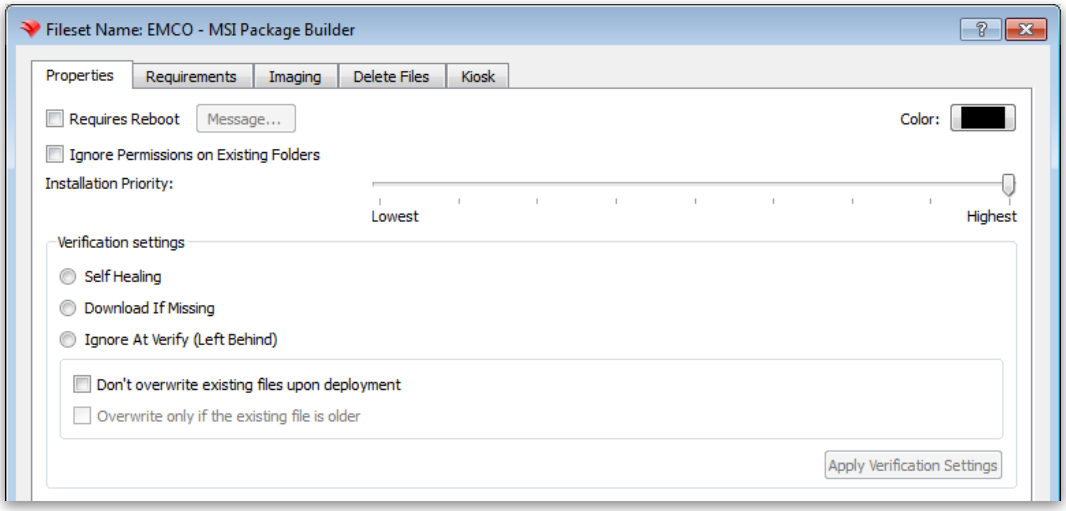


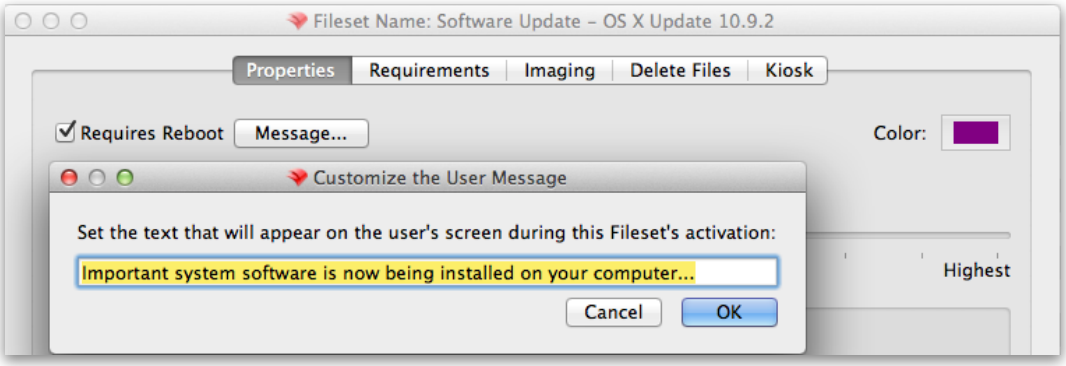
Note: Making changes to Filesets can result in unexpected behavior, please test on a non-production device prior to mass deployment. Better yet - just test everything on a non-production system first.

Properties - basic settings

The first tab is the primary properties for the Fileset. The basic options are:

- *Require Reboot (with Message)* - in most cases, you won't need to require the device to reboot; but software update Filesets usually do. FileWave recognizes most cases where a reboot is required and will preset this for you. You may also provide a message to be displayed for the end user as a warning that significant things are happening to their device and it might be a good idea to go take a break or feed the dog.
- *Ignore Permissions on Existing Folders* - Normally, the Fileset will overwrite permissions on existing files and folders during a distribution. You can choose to leave permissions in place; but recognize that in some cases, portions of the Fileset may not be installed.
- *Installation Priority* - when you are working with a Fileset group or a series of Filesets to be distributed as a single workflow, the deployment often requires certain items installed before others. The Installation Priority lets you assign an order of activation. Highest items first, then lower priorities. Also - when the installation priority is the same, the Fileset ID determines priority with lower ID numbers having the higher priority.
- *Color* - you can assign colors to your Filesets to differentiate them when browsing the Fileset view



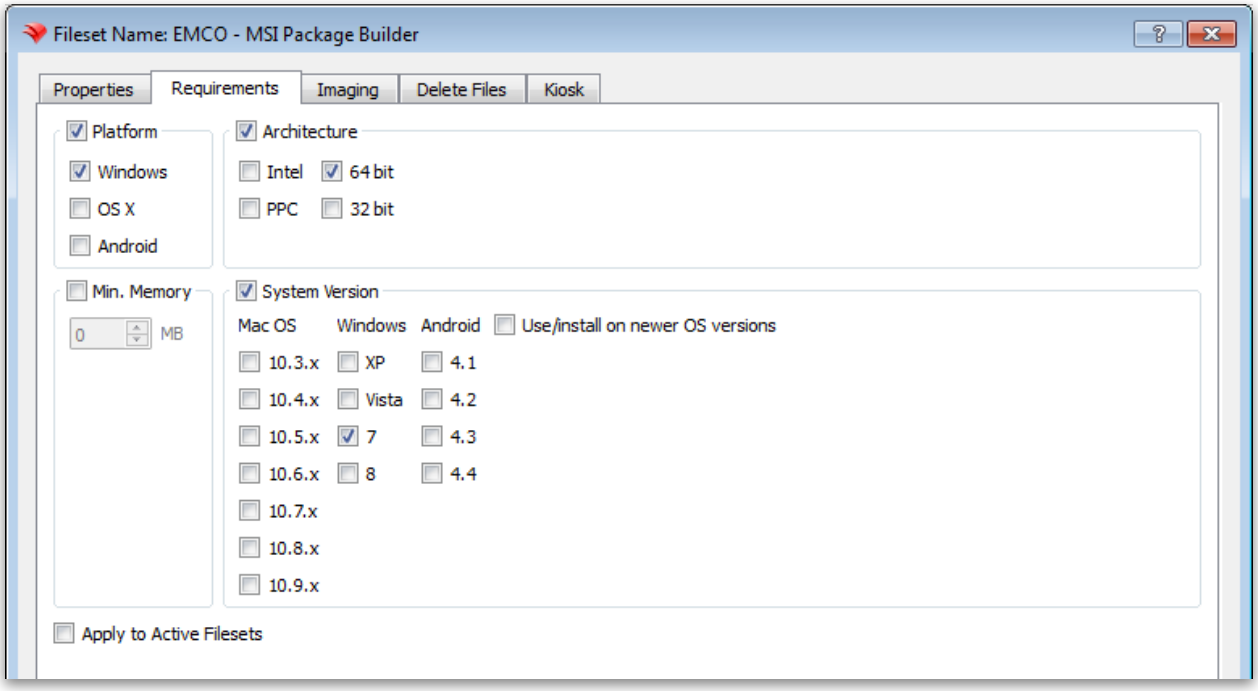


Properties - Verification settings

- *Self Healing* - use this setting to force the re-distribution of the file if any changes have been made to the existing Fileset files that have this label. This function will repair settings and other files that were accidentally or purposely changed.
- *Download If Missing* (1) - During verification, if a file is no longer present, it will be replaced from the master Fileset.
- *Ignore At Verify (Left Behind)* (2) - This setting will tell the verification to ignore anything with this label. This setting is often used in files that are meant to be dropped into a location once, and ignored after that. It also works for iTunes content because the content is sent to the *Automatically Add to iTunes* folder, then sent elsewhere, such as Podcasts or Movies. If the files were not labelled to be ignored, you would get a new copy of the file every time FileWave server verified the associated Filesets.
- *Don't Overwrite existing files upon deployment* - This setting is a subset of items (1) and (2). It allows you to keep any existing files from being overwritten by other files with the same names.
- *Overwrite only if existing file is older* - As above, this setting is also a subset of (1) and (2), and can be activated if the above setting is in effect. It will allow only older versions of the same named files to be replaced.

Properties - Requirements

These settings establish the device definition that will allow download and activation of the Fileset. When you create a Fileset for a specific platform, these settings are usually auto-set. Just selecting criteria here will not necessarily allow the Fileset to work on any device. You can choose specific operating system platforms, architectures, memory and system versions. Note that if you choose a specific version (or versions) of an operating systems as criteria, selecting the *"Use/Install on newer OS versions"* is meant to be used in conjunction with a single OS choice. It says that the system version you chose was the minimum acceptable, and that newer versions will be allowed.



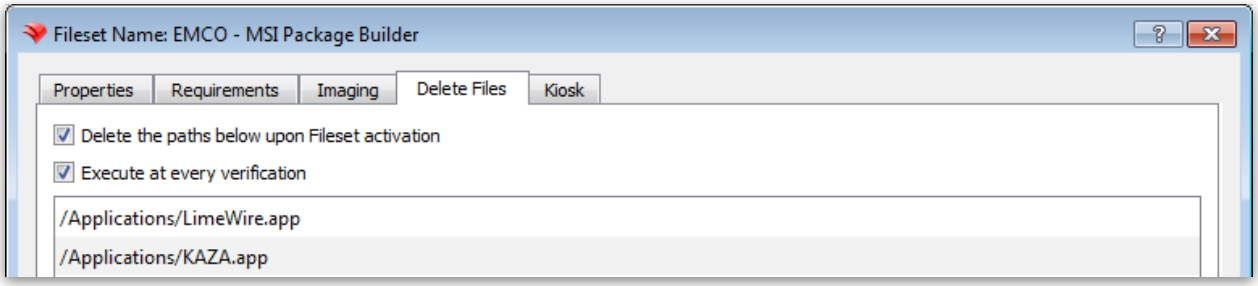
Selecting *Apply to Active Filesets* will force these settings to be re-applied on deployed Filesets. If a device no longer meets the verification criteria, the Fileset will be dis-associated and removed.

Properties - Imaging

This tab has been deprecated. Older (pre-version 6) Imaging Filesets will still show up here; but all imaging functionality has been moved into the **Imaging Virtual Appliance**.

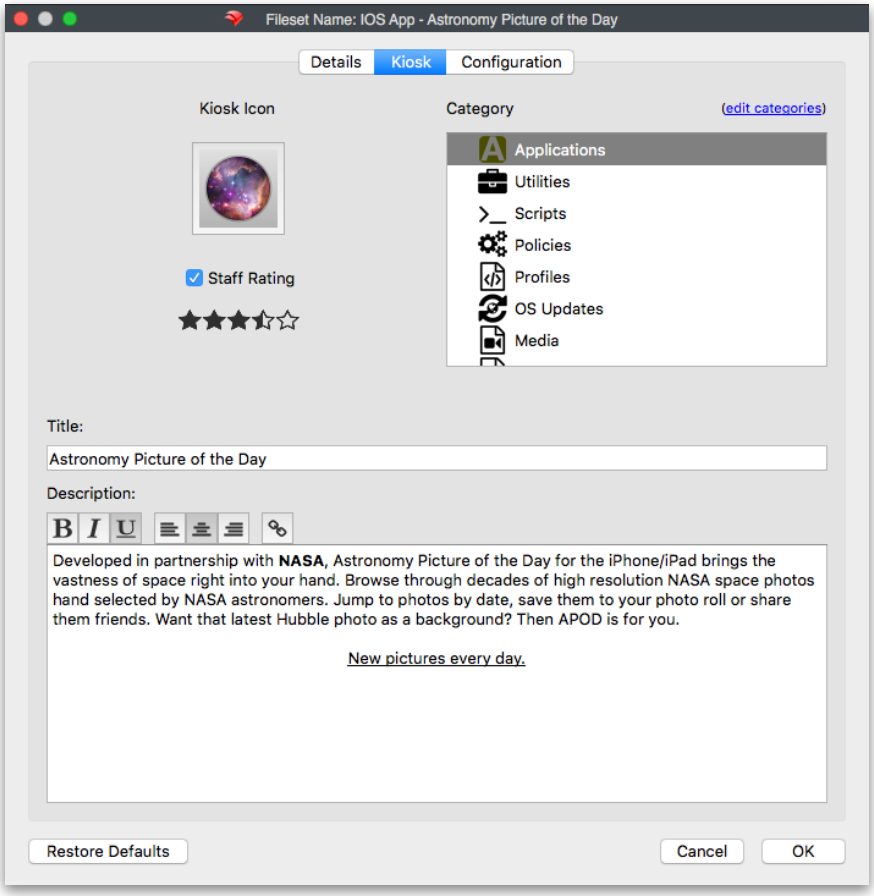
Properties - Delete Files

Use this tab to provide the file pathnames of items that need to be deleted when this Fileset activates. For example, you could create an Empty Fileset that does nothing but delete certain files at every verification (think Minecraft…).



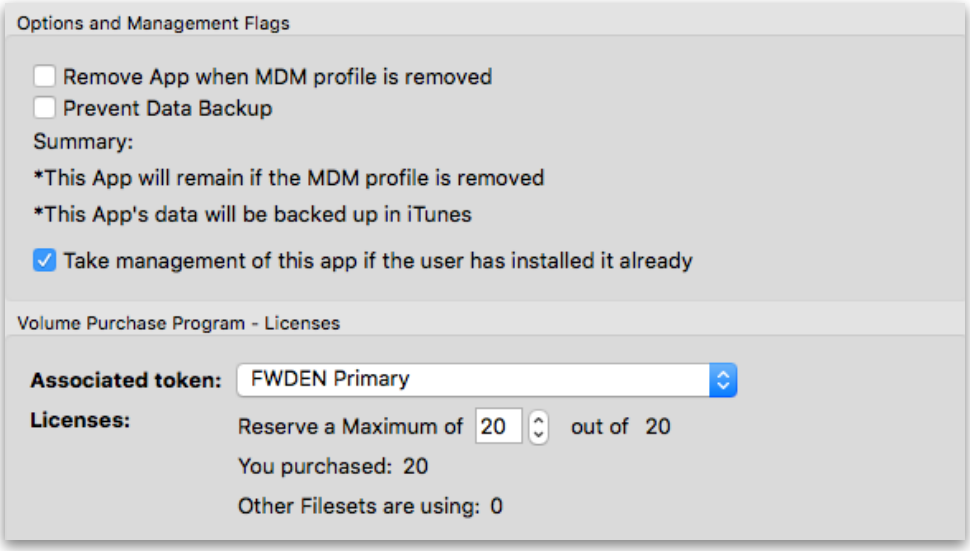
Properties - Kiosk

You will use this tab to configure the appearance of your Fileset in the Kiosk. You can can change the icon, place the Fileset into a designated category, and edit the title and description of the Fileset. This includes changing the information provided from the iTunes/App Store to be something more oriented toward your institutional needs. With FileWave v10, you can use Rich Text formatting to improve the look and feel of the Description.

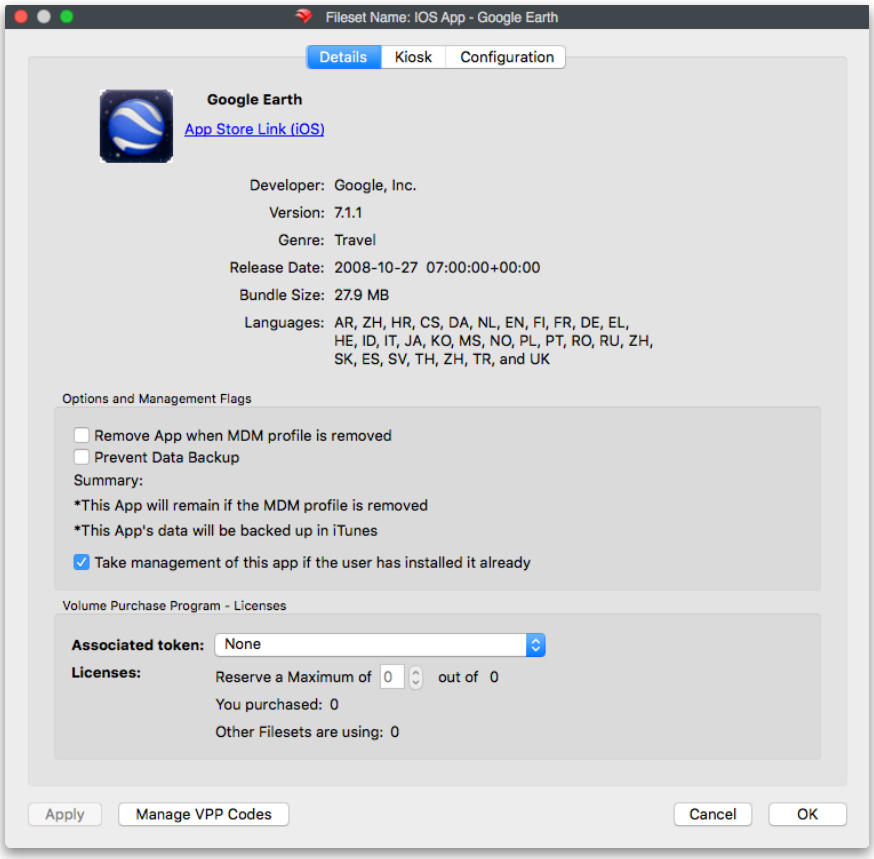


Properties - Details

Details contains general application information, management flags, and VPP information. The management flags include the ability to force application removal when the MDM profile is removed, and the ability restrict application data from being backed up in iTunes. VPP shows the possible connection with the Fileset and a VPP account. A warning is shown if a VPP token is associated with the application noting that the Fileset cannot be attached to a different VPP account token.



It is the same information you would see on that Fileset if you double-clicked on it or selected *Get Info* for that item. Those settings are reserved for Filesets from Apple App Store or iTunes Store content.



Exporting Filesets

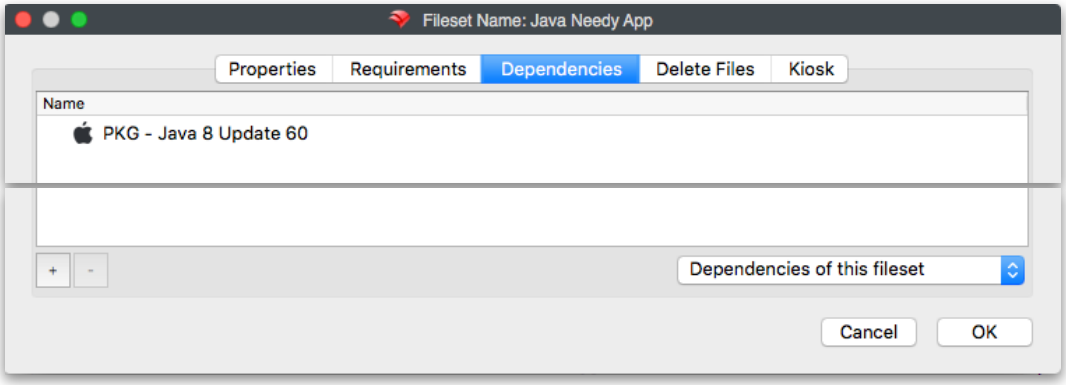
Filesets can be exported for transfer to another FileWave server and they can be compressed and stored for future use or archive. iOS Filesets cannot be exported.

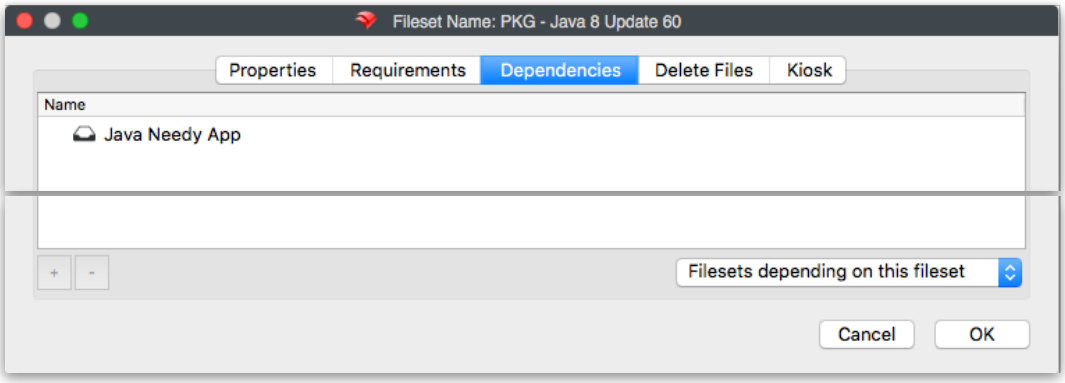
Dependencies (new in FWv10)

FileWave Admins no longer need to keep detailed records of all the linkages between different Filesets and how they inter-relate. Filesets can now display and react to their dependencies on other Filesets. This need to track dependencies includes such situations as a school using **MatLab** where they need to make sure the proper version of Java is installed before MatLab. You might have a Certificate Fileset that must be activated before a WiFi profile Fileset.

It works by allowing you to designate one of more Filesets that must be activated/installed before another. For example, if the “Java Needy App” could not be deployed unless Java was installed on a device, you can create a dependency. If you associate a Fileset that has dependencies, then the other Filesets will automatically get associated and will be applied before the dependent one. It works with multiple, cascading dependencies also.

In the Properties of a Fileset that has dependencies, you just click on the [+] to add any Fileset that must be activated prior to your dependent Fileset. You can also drag and drop Filesets within the Dependency pane to rearrange them in order of need. The first one to get activated will be at the top of the list.

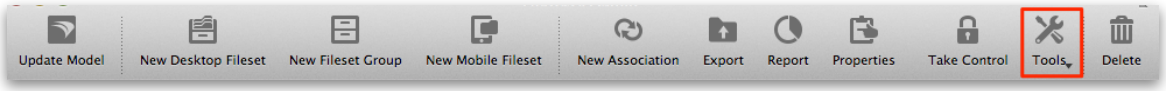


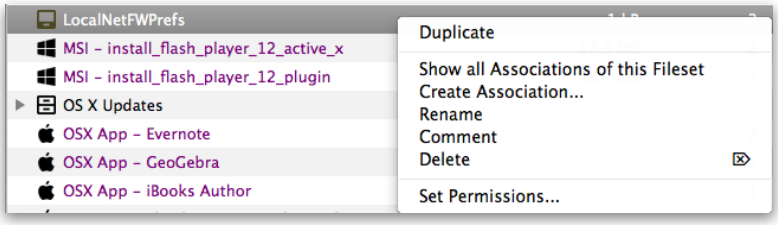


The only Filesets that do not contain the ability to show dependency are the Apple App Store and iTunes Store Filesets.

6.6. Fileset Tools

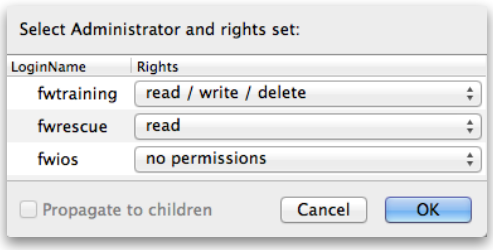
Along with all of the editing and modification capabilities you have with Filesets, there is also a basic set of tools that you can use to make simple changes. These tools support some of the most common tasks you will need to perform as you manage large collections of clients and Filesets. The *Tools* are found by selecting the icon in the main toolbar, or right-clicking on any Fileset.





- *Duplicate* - you can take a fully configured Fileset and create an exact clone with the suffix “copy”. This should be done whenever you want to assign a Fileset to more than one administrator for different deployment options, or when using VPP tokens that require different licenses assigned to the same content.

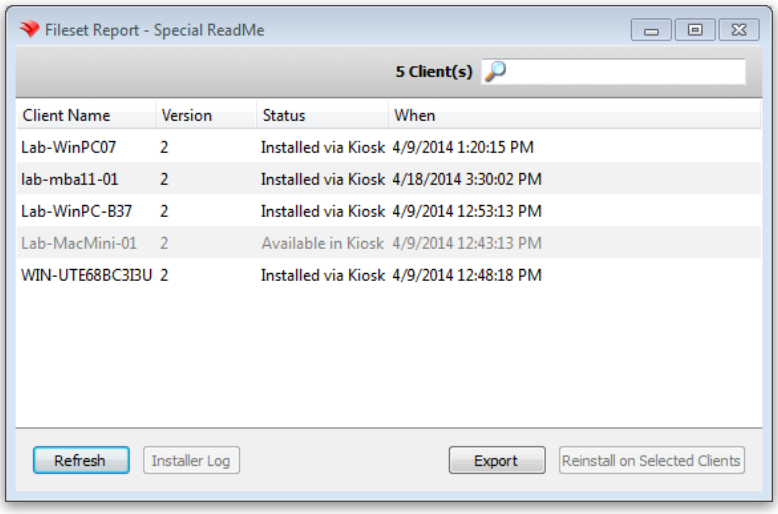
- *Show all Associations of this Fileset* - this will take you to the **Associations** pane where you can view the Fileset and its assigned clients
- *Rename* - change the name of the Fileset post-creation
- *Comment* - add a comment to assist you in managing and keeping track of your Filesets
- *Delete* - trash the selected Fileset
- *Set Permissions* - specify the access level of your various sub-administrators. This capability, used with the *Duplicate* command can allow you to create custom deployment sets that being to designated administrators.



6.7. Fileset Reports

When you select a Fileset or a group of Filesets, you can select the **Report** toolbar button to see the status of the selected item(s).

The report will show the clients that have been associated with the Fileset, the version of the Fileset that is present on the client, its status as to whether it has been installed or is available, and the date-time group of when the client reported the Fileset as active. The report can be exported in *.csv* format. If the Fileset includes an installer, such as a .pkg or .msi Fileset, you can review the installer log for that installation. You can also select the client and force a re-install of the Fileset.

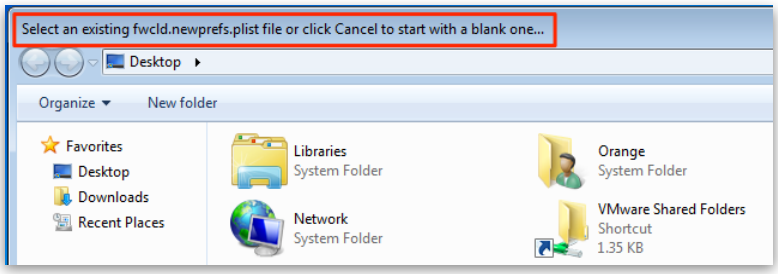


6.8. Using the SuperPrefs Editor

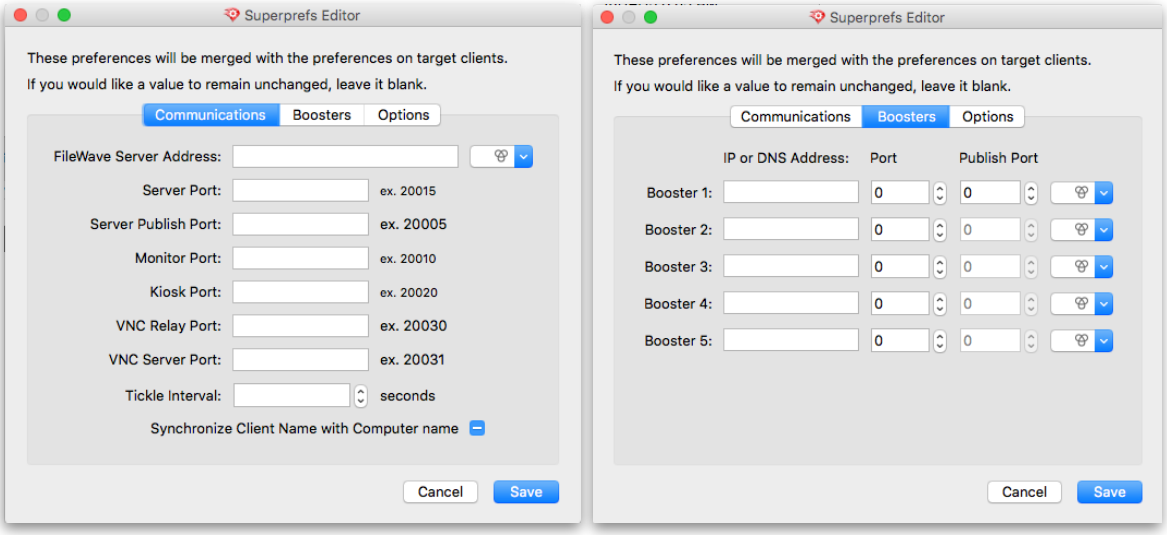
There are times when you may need to make significant changes to the client settings for your devices. You can use *SuperPrefs* to migrate clients to new Boosters, change verification check in intervals and switch connection ports. Instead of re-installing the FileWave client software on all your devices, you can use the *SuperPrefs Editor* to provide your clients with a new configuration remotely.

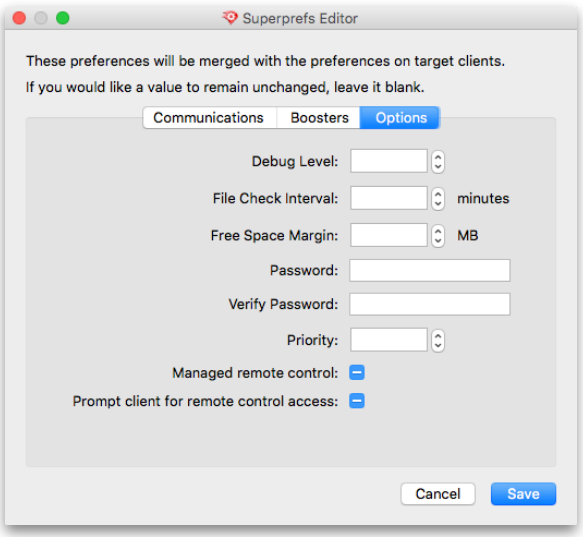
The FileWave SuperPrefs Editor allows you to deploy client preferences in a Fileset by delivering a file named "fwcld.newprefs.plist" to your FileWave clients. This file may be delivered to any location on the Client, and will work with Android, Windows and OS X clients. When a FileWave client activates this file, it merges the contents of this file with its own local config file, replacing any fields that contain older information with the data from the Fileset.

To create a SuperPref, simply open the FileWave SuperPrefs Editor, which has been installed into FileWave folder as part of the FileWave Admin toolkit.



Fill in the fields with the values you want clients to inherit, leave any fields you don't want to change blank and then click the OK button to save the file and exit the application.





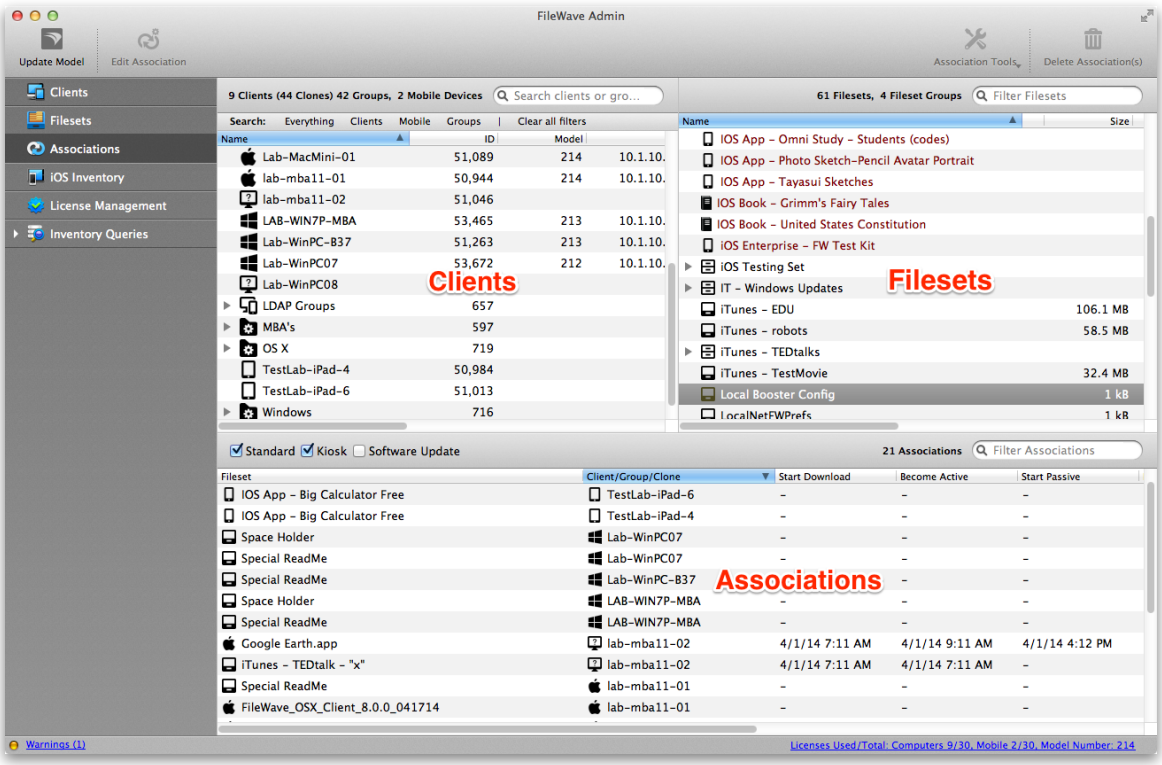
The file is automatically saved to your desktop on the computer running the FileWave SuperPrefs Editor. Open FileWave Admin and follow the next steps:.

- Import the fwcld.newprefs.plist into any folder as long as it does not conflict with another fwcld.newprefs.plist file in a different Fileset (If you drop it into an Empty Fileset, it will go to the root of the client HD, picking a hidden folder)
- Associate the Fileset with the clients you wish to update
- Update the server model

Once your clients have gotten the new information, they will begin checking into the FileWave server using the new settings.

6.9. Using Associations with Filesets

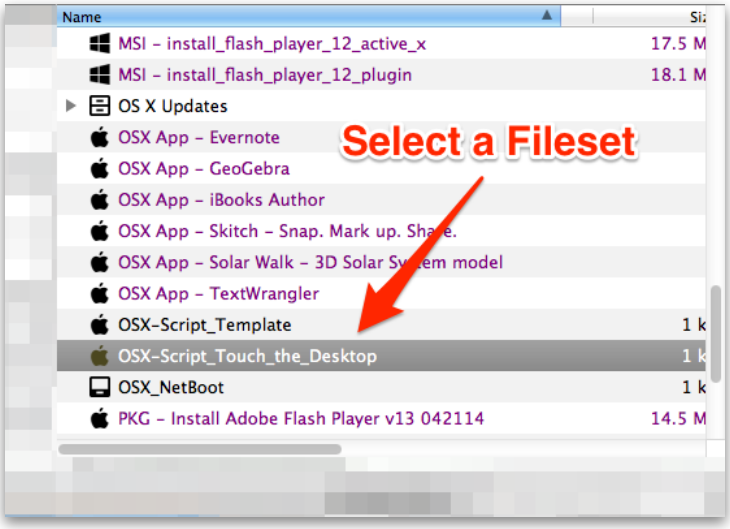
The **Associations** pane is the primary location where you will connect your Filesets to your clients. The window has three primary sections:



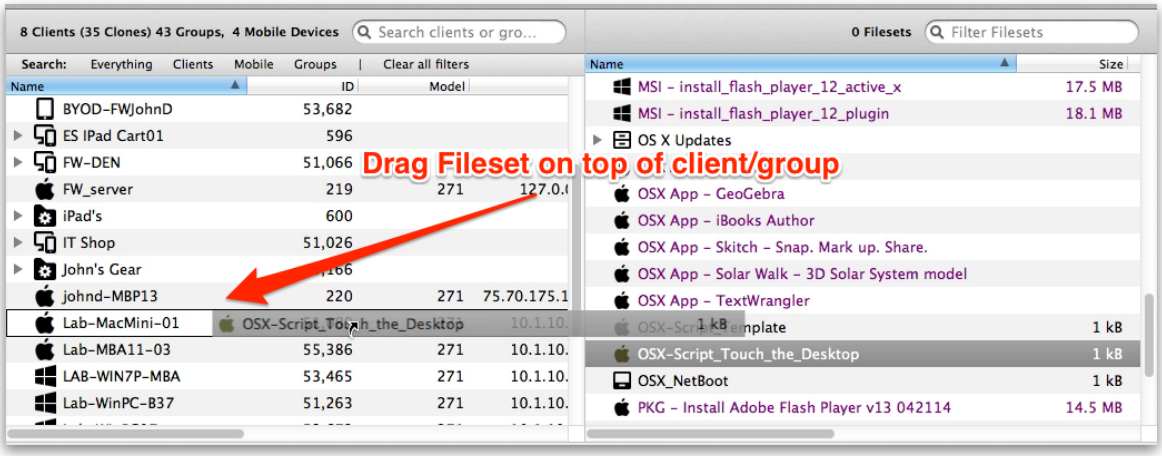
The link between a Fileset and a Client, or client group, is called an Association. In order to distribute the contents of a Fileset, you *associate* a Fileset to a client or group.

Basic Association Workflow

The basic workflow is selecting a Fileset, linking it to a client/group, updating the server model. You choose a Fileset from the upper right pane:



Click and drag the Fileset to the left into the Clients window and drop it on top of client or client group you want to associate it to.



Finally, select the **Update Model** tool in the main toolbar, or use *Cmd-U (OS X)* or *Ctrl-U (Win)*, to lock in the change and distribute the Fileset to the client.

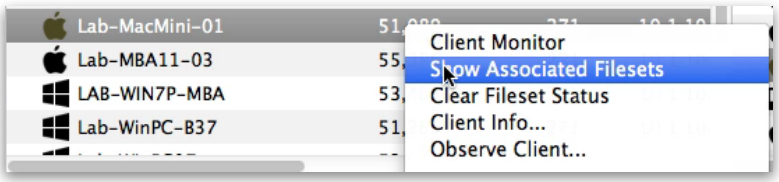
Customizing the Association

The basic workflow will associate a Fileset with a client; then when the server model is updated, the Fileset will be sent to the client for whatever action is applied - install something, place files into proper locations, execute a script.

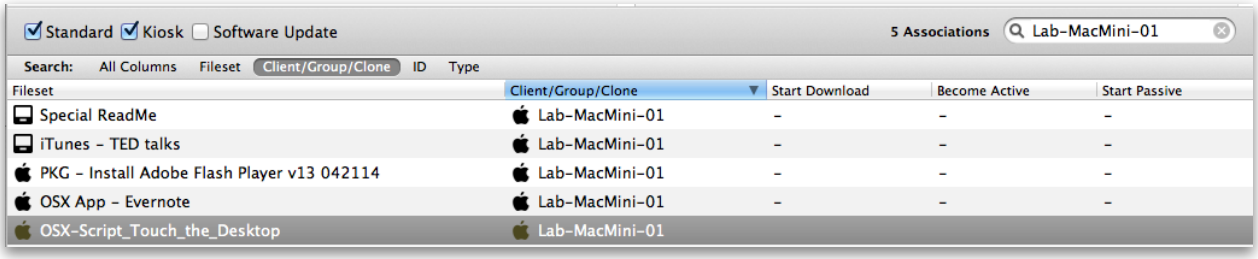
The power of Filesets and associations is that you can enhance the basic workflow with options that provide significant improvement in the deployment process, as well as expanded control of the workflow.

Viewing Associations for a single client / group

The first improvement over the basic workflow is being able to look at the Filesets that are associated with a specific client or group. You do this by right-clicking on the client or group in the Clients portion of the Associations window and electing **Show Associated Filesets**.



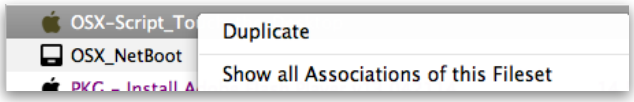
That action will present you with this view in the lower portion of the main window:



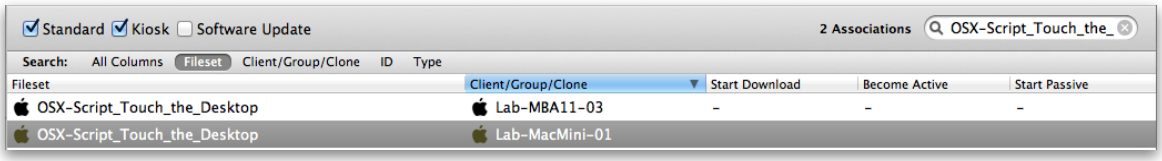
This view shows you all of the Filesets that have been **directly** associated with that specific client (in this case - *Lab-MacMini-01*). We stress -directly- because you can associate Filesets with groups of clients also. Those associations would not show up in this view. This concept is important because you may find yourself in a situation where you see something happening to a client; but you don't see the Fileset that would create the situation in its direct associations. The solution to this situation is to look from the "other side" by selecting a Fileset and asking to view all of its associations. Associations may also be made to Smart Groups, clones, and groups.

Viewing clients associated with a single Fileset

If you select a Fileset, you can right-click to view all associations that have been made for that specific Fileset. Doing this can resolve the problem you may have in tracking down how many different places a Fileset has gone.

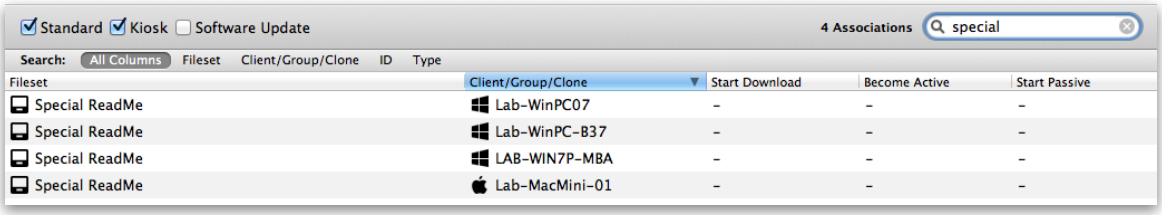


That action presents this view:



Searching and filtering the Associations window

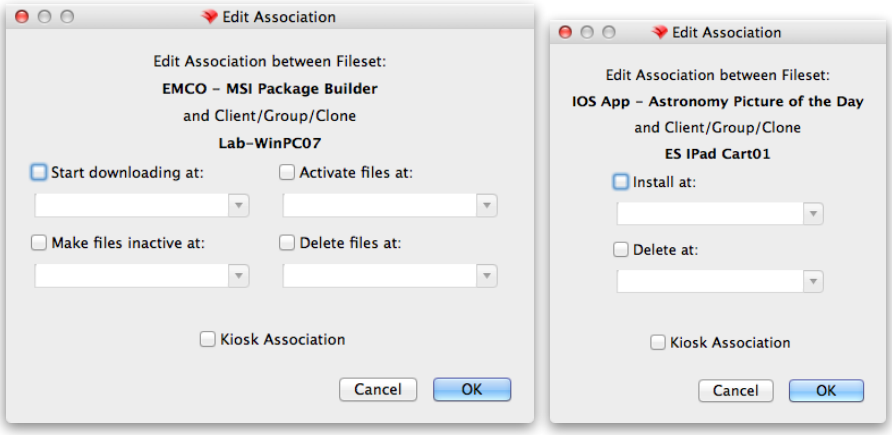
Another powerful function is in the Search / Filter window. You can enter any text into the Search window, press *Return* then choose the criteria for your view of any association that is active:



Your criteria can be to look for a Fileset with that text, a client, group or clone, a Fileset ID, of Fileset type (such as Kiosk), or just select *All Columns* to let the search find every association that has that text in it no matter what it applies to.

Editing the Association

Another (some say the most) powerful capability of the Associations window is the ability to edit Fileset associations. Within this functionality, you have the power to designate the deployment schedule, change the type of Fileset from standard to self-service Kiosk, and choose when the Fileset is deactivated and removed from the client.



There are two Edit windows available, depending on the type of Fileset being deployed. Most desktop and Android Filesets have the ability to designate a full range of settings:

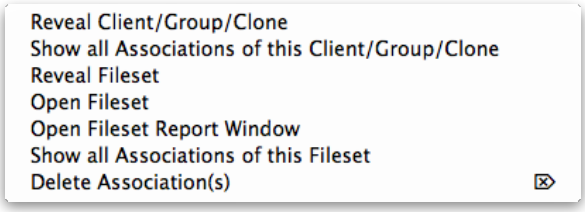
- *Start downloading at:* - tell the client to start downloading the Fileset at this specific time. The Fileset is cached locally and is inert. This allows the FileWave administrator to pre-stage Filesets out on clients using a staggered deployment schedule prior to activation. Using a staggered schedule would allow systems administrators to avoid network traffic surges while distributing large deployment sets. This action can also be used when you have staged a Fileset that is still being tested, and there was a problem with the test results. Instead of having to reset devices, you just delete the Fileset prior to activation.
- *Activate files at:* - tell the client to activate the Fileset. Installers will run, shell scripts will execute, and any files will be placed into their proper places. Since this command is only a signal to the client to have the Fileset perform its action, the network traffic is minimal.
- *Make files inactive at:* - tell the client to locate and move all components of that Fileset back into the local cache.
- *Delete files at:* - tell the client to delete the Fileset at this time.
- *Kiosk Association* - convert the Fileset from a standard distribution to a self-service Kiosk item. Filesets that have been distributed as standard items can be converted to Kiosk mode and vice versa.

iOS Filesets can be installed, deleted and changed to Kiosk items. Books can be installed and changed to Kiosk items. Books cannot be deleted - once deployed, they are the property of the end user.

Note: Filesets within Fileset Groups that are associated to clients or client groups will all get the same settings you designate with the *Edit Association* pane. If you want to provide custom settings for deployment times to a large number of Filesets, using a Fileset Group is the best way to achieve this goal.

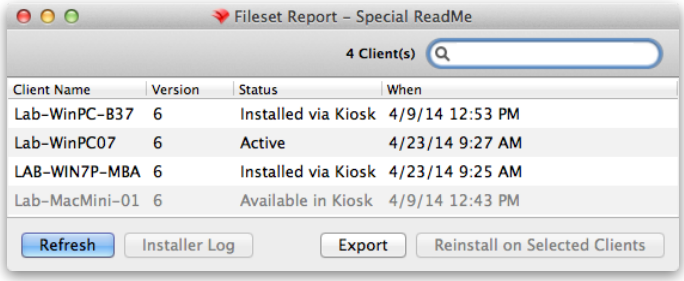
Association sub-menus

The tools and actions available to associations allow you to see the various aspects of the association:

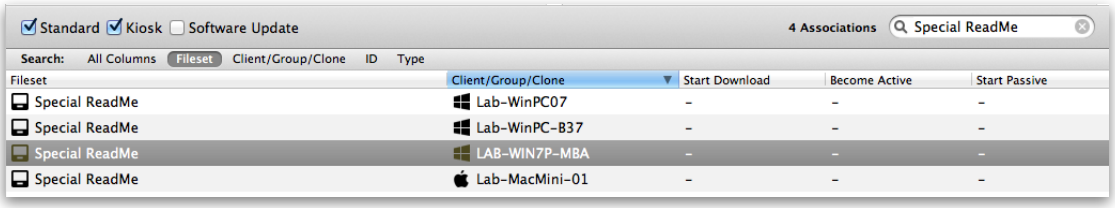


- Reveal Client/Group/Clone - displays and highlights the client/group/clone related to this association in the upper left window
- Show all Associations of this Client/Group/Clone - displays and highlights all associations related to the client/group/clone in the lower window

- Reveal Fileset - displays and highlights the Fileset in the upper right window
- Open Fileset - displays the contents of the Fileset (same as double-clicking on Fileset in Filesets pane)
- Open Fileset Report Window - displays the report showing the status of that Fileset's distribution



- Show all Associations of this Fileset - displays all of the clients associated with this Fileset



- Delete Association(s) - remove the linkage between the client/group and the Fileset. In most cases, this will result in the Fileset contents being removed from the client/group. With VPP managed distribution, the license is revoked.

Association conflict resolution

The algorithm for computing which client machines receive which associations is quite complex. As a result, you may end up "double associating" a Fileset to a client (e.g. if it is cloned into two groups, both groups are associated with the same Fileset). We have solved this issue by allowing only one Association-Fileset-Client chain. A Fileset can only be associated to a client via one Association. The chosen Association's commands will be followed, and all other associations ignored. The "winner" association is determined by *association distance*.

Association Distance

The FileWave Server resolves conflicting associations by choosing the most direct association. For example, an association directly from a Fileset to a client is more direct than to its group, and an association to a client's direct parent is closer than an association to its grandparent. Clones also increase distance. **Closer** associations always win. **Equidistant** Associations are treated by ID-descending, meaning that new associations(higher ID numbers) beat old ones.

Smart Groups

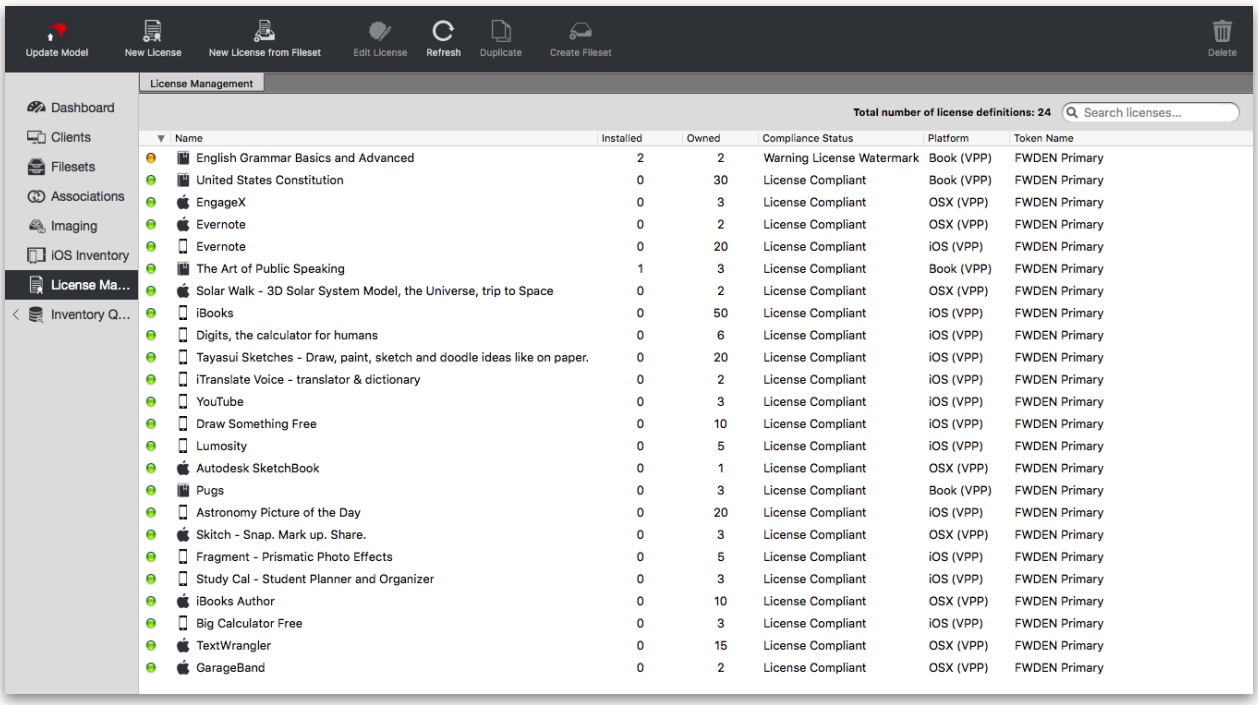
Smart group associations are calculated separately, following the same distance method. However, if a client is associated by both a smart group and a regular association, the regular association will always win. When you view Associations, you will only see the Filesets that are directly associated with that device or group. Associations made to a smart group will not show up when viewing the device associations and vice versa.

Imaging associations

Imaging Filesets and their associations are covered in chapter **10 Imaging**.

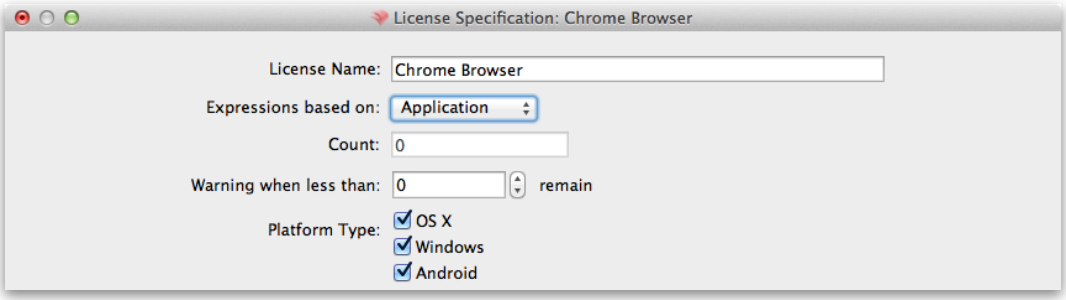
7. License Management and Apple's Volume Purchase Program (VPP)

FileWave supports a powerful license management functionality, allowing you to keep track of your software licenses manually using purchase orders, Apple's VPP managed distribution items, and fonts. You can set triggers or watermark levels to let you know when you are running out of licenses for a specific application.



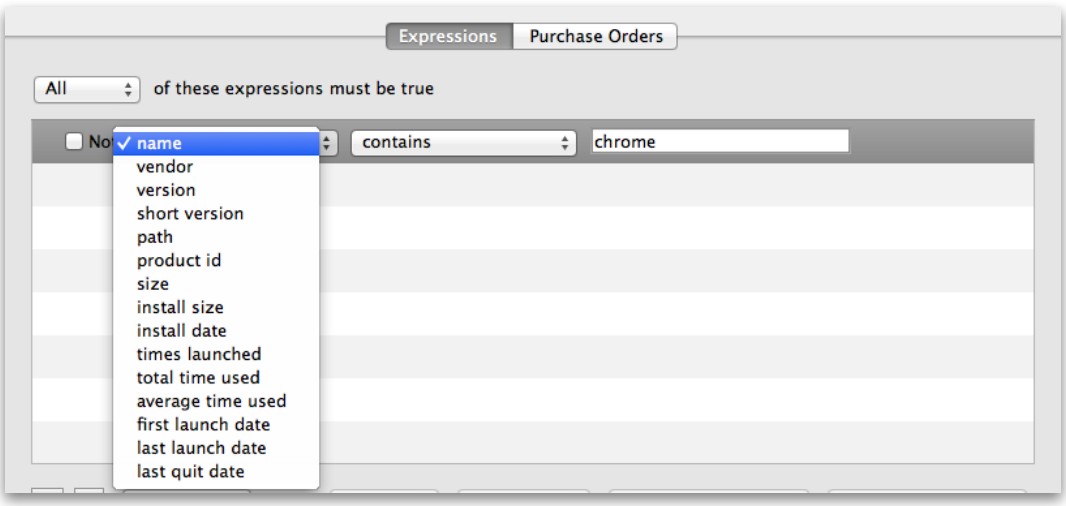
7.1. Manual Licenses

The first method for managing software licenses is to manually create the query. You select **New License** from the toolbar and give it a name.

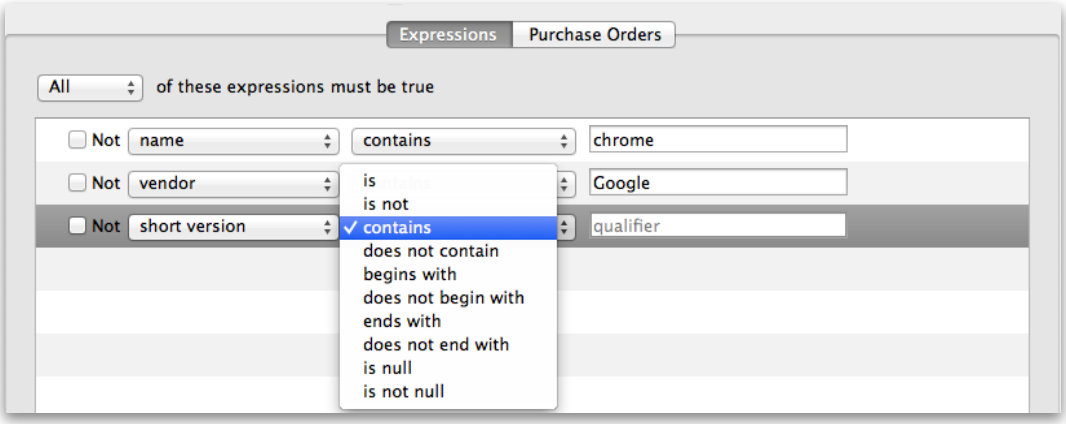


Then you set the license expression to be based on managing an application or a font. In this example, we will be looking at Google's Chrome browser. Notice that you can choose to manage items installed in all three of the operating systems FileWave supports from a "desktop" point of view. (Android, due to its FileWave client, is managed as a hybrid between the desktop and mobile world.)

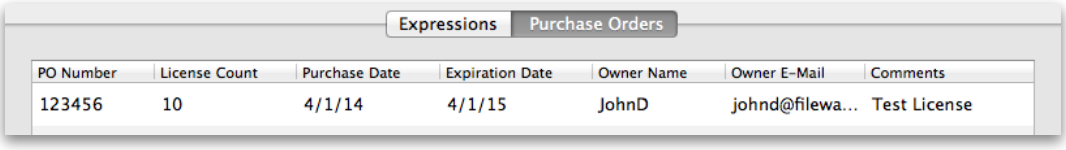
Next, we have to create the criteria by which we identify our item, e.g. the Chrome browser, as just that.



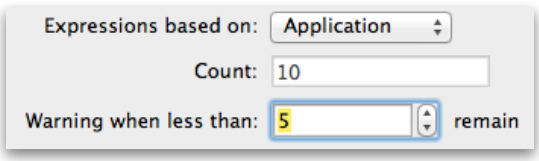
For this license, we only need to know the name of the application. We could clarify the expressions by getting very granular. You can create license queries for different versions of the same software - such as tracking every version of Adobe Player that may be in use, or all of the different versions of MS Office.



Now, we need to gather a count of the licenses we control. This can be done by entering purchase order information, or just using whatever accounting method you have to create a pseudo-purchase order. You can enter multiple license purchases here. It will give you an accounting history as well as let you manage multiple licenses in one location.

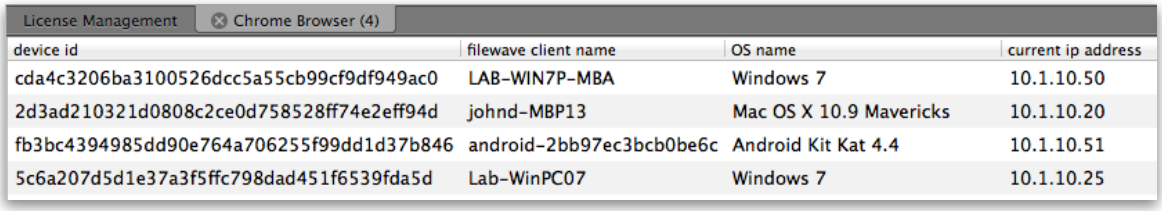


Then we add a watermark or trigger value to warn us when we are running out of licenses.



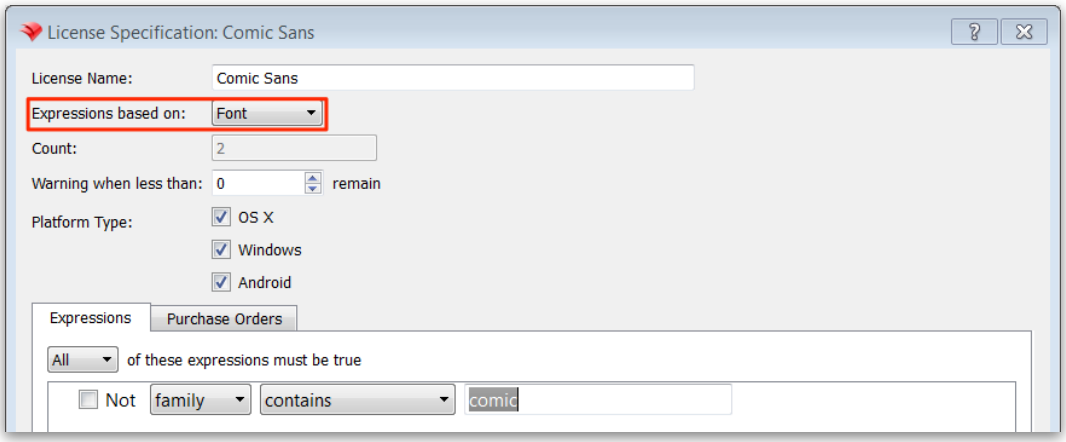
That will complete our license query. Looking at the result in the License Management pane yields:

And when you double-click on the license, you will see the details of the query displayed. The window will actually display a significant amount of information about your search results, including detailed device info:

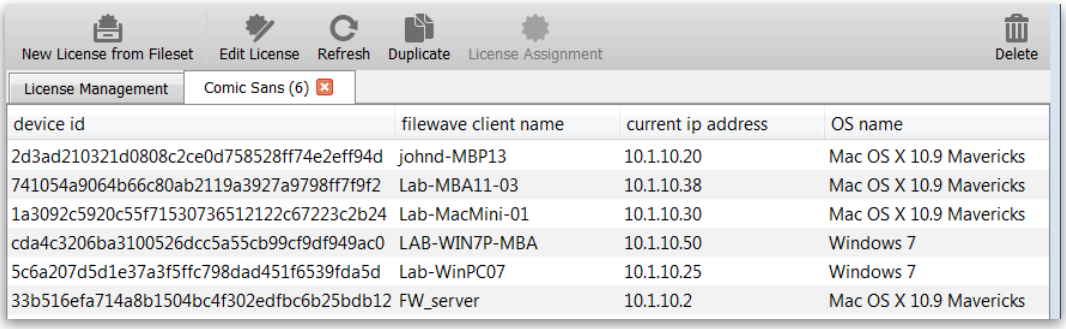


7.2. Font Licenses

Many institutions or departments have purchased commercial fonts for use in their design, graphics, or marketing groups. FileWave provides you with the ability to track and manage the use of those fonts. The workflow for setting up a font license is roughly the same as that for an applications. First, you create and name the license; but this time, designate the expressions based on “font”:



While this example is based on a common font type (Comic Sans), you can easily configure custom licenses based on commercial font libraries. This example also shows the result of a query that shows when you are outside of the allowed license boundary:



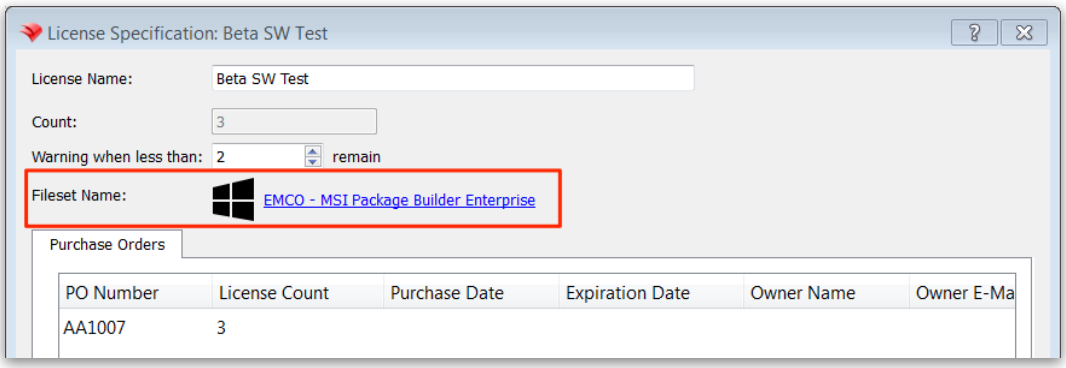
device id	filewave client name	current ip address	OS name
2d3ad210321d0808c2ce0d758528ff74e2eff94d	johnd-MBP13	10.1.10.20	Mac OS X 10.9 Mavericks
741054a9064b66c80ab2119a3927a9798ff7f9f2	Lab-MBA11-03	10.1.10.38	Mac OS X 10.9 Mavericks
1a3092c5920c55f71530736512122c67223c2b24	Lab-MacMini-01	10.1.10.30	Mac OS X 10.9 Mavericks
cda4c3206ba3100526dcc5a55cb99cf9df949ac0	LAB-WIN7P-MBA	10.1.10.50	Windows 7
5c6a207d5d1e37a3f5ffc798dad451f6539fda5d	Lab-WinPC07	10.1.10.25	Windows 7
33b516efa714a8b1504bc4f302edfbc6b25bdb12	FW_server	10.1.10.2	Mac OS X 10.9 Mavericks

When your licenses are in compliance, you will see a green “jelly” in the main License Management window. When you have crossed the watermark trigger point, the “jelly” turns yellow. Finally, when you are out of compliance, you will see red.

7.3. Creating Licenses from Filesets

As you add applications and other content to your Fileset database, you will realize that the power behind license management is that you can track anything - applications, fonts, books, iTunes content, etc. Since the FileWave client can deep scan your client systems, it can find any file that meets the criteria you wish to be aware of. This functionality also exists in the primary **Inventory** pane in FileWave Admin; but the License Management section allows you to tag the query with the watermark triggers. This gives you a quick look into your environment, and helps avoid embarrassing situations later on.

For example, you might have purchased or just deployed a few systems running an application that is being tested for later widespread deployment. You want to keep an eye on that application to make sure unauthorized copies of it don’t leak out. Since you created a Fileset for the application to deploy it in the first place, you can easily create a license to track it.



Instead of having to create any criteria for locating the applications, FileWave uses the Fileset definition. At the same time, it will key in on any copies of that specific package, should it show up on more devices than specified.

7.4. Apple’s Volume Purchase Plan (VPP) and License Management

What is VPP?

VPP, or more formally, Apple’s Volume Purchase Program, is a mechanism by which an organization or institution can purchase OS X and iOS applications and books in bulk and provide those items to their end users. The process revolves around creating a VPP administrator account, creating one or more VPP facilitator accounts, enrolling devices into the MDM (mobile device management) system, and assigning applications and books to the end users. More details on Apple’s requirements and capabilities with VPP are here - VPP for iOS and VPP for OS X

Apple's Volume Purchase Program (VPP) is supported in FileWave for both iOS and OS X. There are two mechanisms for assigning applications and books to clients - **redeemable codes** and **managed distribution licenses**. Apple's new Managed Distribution capability in their Volume Purchase Program (VPP) changes the way systems administrators can use FileWave to manage and distribute applications and books for their iOS and OS X users. While the older VPP process provides a set of redeemable codes to be used for content distribution, Managed Distribution provides licenses that can be associated and revoked. This allows you, as a FileWave administrator, the ability to assign institutionally purchased applications to end users as needed; then revoke the licenses for those apps at a specific time, returning the licenses to your control. If you have students under 13 years old, you should explore Apple's "AppleID for Students" program.

Prerequisites for using VPP

In order to set up VPP on your FileWave server, you must have already configured a FileWave server to support MDM (mobile device management). You must also have enrolled devices that you are going to deploy content to, and have them listed as clients in your FileWave database.

Differences between redeemable codes and managed distribution licenses

The original model for mass deployment of content is using redeemable codes. The VPP administrator purchases applications from the Apple VPP site. Apple provides a set of codes in a spreadsheet that can be downloaded. Those codes are then used to create an application Fileset for installation on managed devices, or are provided to the end user for them to redeem. Once a code has been redeemed, it cannot be reclaimed by the MDM administrator. VPP redeemable codes are available for applications and books. **Note: With the current VPP system, free apps and books cannot be obtained with redeemable codes, only managed licenses.** It is also possible to have all of your redeemable codes exchanged for Managed Distribution licenses. Contact your Apple sales team for more information.

Apple's newer model for application license management allows you to assign licenses to users and revoke those licenses at a future date. The new mechanism is called **Managed Distribution** and it applies to VPP purchases of any free content, applications, and books. When a license is assigned to a user, that user sees the item in their Purchases list, as well as in FileWave's Kiosk. When the application is no longer needed, or the user is no longer associated with that institution, the MDM administrator can revoke or remove the license. FileWave regains that license for distribution to another user. This process is only valid for applications since Apple requires all book distributions to be permanently assigned to personal AppleIDs.

Managed Distribution and user versus device assignment

Initially, Managed Distribution required association to an AppleID for all of the content. With the release of iOSv9 and OS X v10.11, VPP has added the ability to assign applications directly to a device. This method opens up a huge benefit in layered deployment models. Now an institution can assign core applications directly to devices in carts, labs, or even on 1:1 deployments. Users can use their own AppleID to put other content, and get books, onto their device. This new method will probably become the default deployment method.

How FileWave works with VPP

There are several approaches to using FileWave with Apple's VPP. The deployment workflows relate to the overall control of the application(s) to be deployed. If you are going to be doing a 1:1 or BYOD deployment, you can use either redeemable codes or managed distribution licenses. For shared devices or institutional owned devices, the best practice is to use redeemable codes. The actual workflows discussed are covered in detail later in this section.

Redeemable Codes - A Fileset is created that links to the App Store and provides a redeemable code for each device that is associated with that Fileset. When the user accepts the installation, the code is redeemed against that user's AppleID. This process is best used with Kiosk mode deployments; but will work in managed Filesets. The code, once redeemed, belongs to the end user and cannot be retrieved by the FileWave administrator. If the user refuses the installation, the code is reserved for the next 24 hours against that device, then it is returned to the pool for that Fileset. **Note: This method is not supported for OS X deployments. Under OS X, all application associations must be done as Kiosk items.**

Managed Distribution licenses - For the managed distribution method, FileWave doesn't manage users directly; but associates users with specific devices. All of this is done through the linkage of an AppleID and the FileWave MDM.

Whether you use individual AppleIDs, in the case of a BYOD or full 1:1 deployment, or institutional AppleIDs in the case of a managed lab or cart, the application licenses remain under your control.

When you assign or associate Apple Store content with a device through a Fileset, the end user will see that content in their Purchases in the App Store. If you are using FileWave's Kiosk, then your users on their devices will get direct access to their associated content. Possible workflows are:

- *Institutional Assignment* - With the new version of VPP supported in FileWave v10, you can assign applications directly to an OS X device. This is the least painful method of deployment using VPP. Licenses can be revoked as needed, then assigned to other OS X devices.

- *Individual Assignment* - for all BYOD and 1:1 deployments, as well as temporarily assigned institutional devices (such as iPad carts), you would associate an individual's AppleID with that device, and assign applications and/or books to that device through FileWave. As with the other model, you may revoke licenses for applications at future dates, returning use of the license to your control.

- *Layered Deployment* - FileWave can work with a layered deployment model where you image or configure the device with institutional software and content, then turn it over to an end user for additional application and content management. For a desktop/laptop system, this would mean that you image the device and install applications owned by the institution using VPP direct device association. Then you would sign the device over to the end user and allow them to use their own AppleID to install additional applications and content. For iOS devices, you could use Apple Configurator to prepare, and possibly supervise, the device; then turn it over to an end user to add their own content using their personal AppleID. Or, you could use VPP direct device association to place the applications onto the device, then let the user add items as they see fit. With this model, you, as the FileWave administrator, would be responsible for maintaining the institutional content and software, while the end user would be responsible for any applications and content they install.

Setting up your FileWave server for VPP

In order to provide your users with content from the Apple Volume Purchase Program, you will need to establish an institutional VPP account and link that account with your FileWave server. If you are an educational institution, you need to follow the steps provided by Apple on setting up VPP for Education - http://www.apple.com/education/it/vpp/ If you are a business or enterprise institution, you will need to use the VPP for Business instructions - http://www.apple.com/business/vpp/

Once you have your VPP account, you are ready to configure FileWave for VPP support.

Important - Ensure you do not have another VPP system, such as Apple's Profile Manager, active with your VPP token when you set up FileWave for VPP. This could cause problems with your ability to manage VPP user accounts.

Set the VPP token(s)

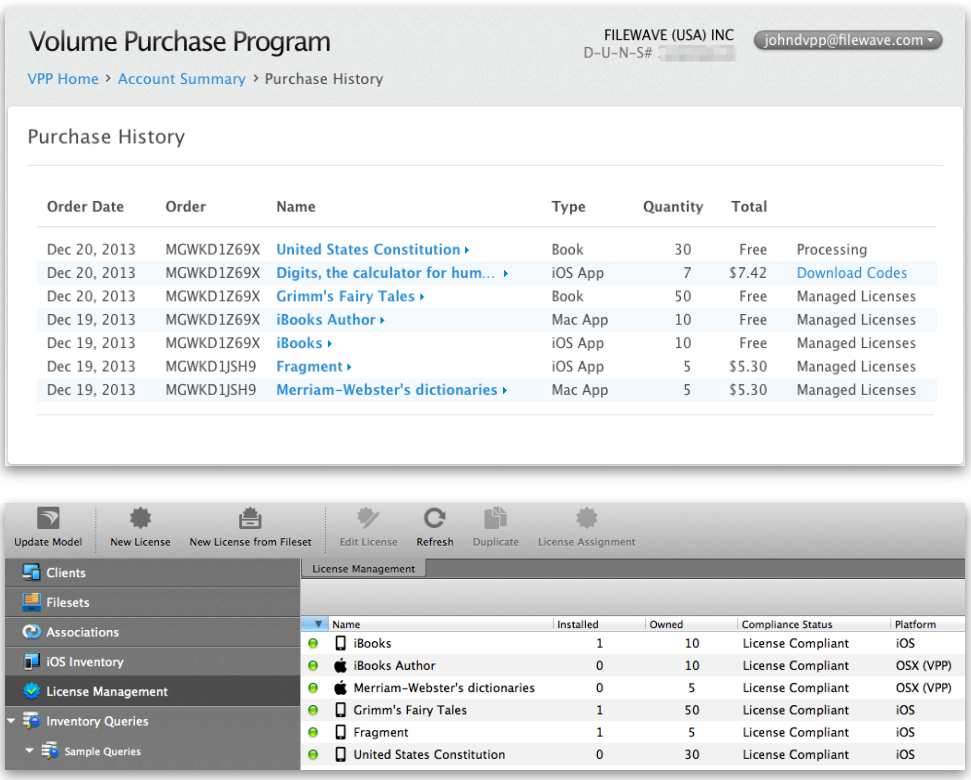
When you signed up for your VPP account, you were provided a coded token that allows you to configure FileWave for VPP service. Use the instructions in chapter **3** to configure your FileWave server preferences for VPP.

Synchronize data with the VPP server for VPP

Once your token(s) are active, the FileWave server will automatically synchronize with the Apple VPP server. Depending on how many items you have in your purchase list, this process may take a while. When you have synchronized your VPP data with your FileWave server, you should see any VPP Managed Distribution purchases listed in the **License Management** section of FileWave Admin. Depending on synchronization delays, you may have to wait for a few moments to see the information.

The first time after you set up VPP, you can force a full synchronization by holding down the option key, and clicking on the **Synchronize** button.

Looking at the License Management section, you should see entries that match your purchase history. Here is an example of a VPP purchase history and its corresponding view in the FileWave Admin / License Management section:



Note: Only VPP managed distribution licenses will be displayed here. The older VPP redeemable codes are still located in the "VPP Code Management" section in FileWave Admin / Assistants.

Adding licensed applications to your FileWave server

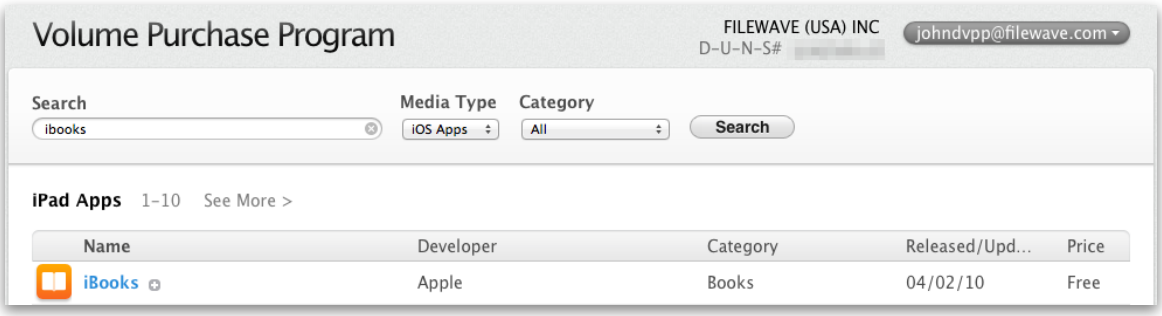
The process of adding content for VPP code redemption or managed distribution is generally the same. Let's walk through adding some content and see how it is done.

First, we will locate a couple items and add them to our VPP account. Let's look at the difference between a free application, a paid application, and a book.

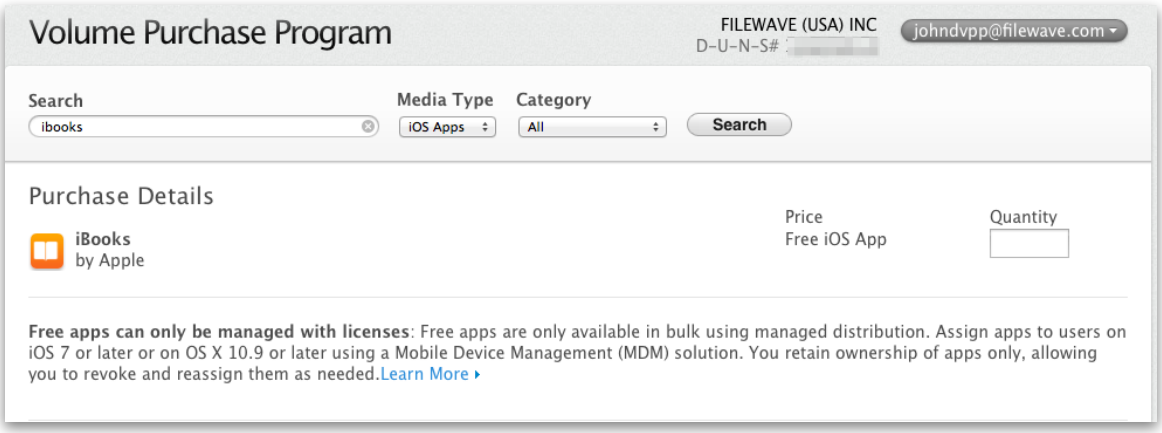
Free applications

Our first item will be **iBooks** which is a free application.

Log into the VPP Store with your credentials, and type in "ibooks" in the Search field.



Select "iBooks" and you will be directed to the purchase page.



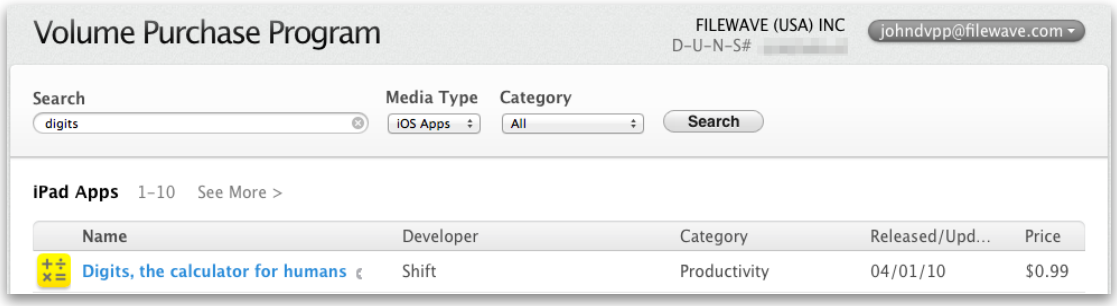
Free applications/books can only be purchased with managed distribution licenses now. You can bulk order the item and you will get a set of managed licenses that you can assign and revoke as needed for the applications.

Note: Books must be assigned to personal AppleIDs and their licenses cannot be revoked.

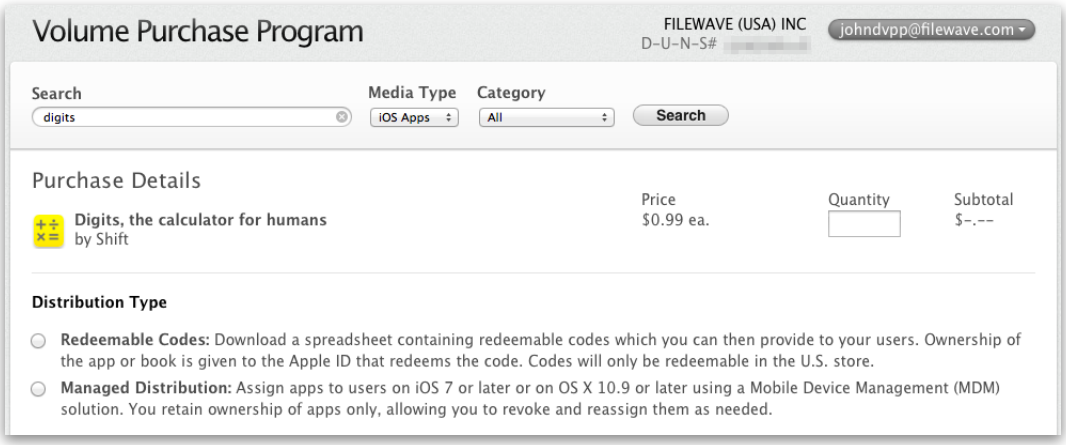
Paid applications

Now let's look at a paid application and see the difference. In this case, we are going to add "Digits", a calculator app, to our distribution model.

In the VPP Store, enter "Digits" into the **Search** field, and locate the app.



When the app is selected, the purchase page has some new features.



Redeemable Codes - The codes are part of the original VPP mechanism. When you purchase the codes, you must then download and import the spreadsheet into FileWave. Another use for the codes is as consumable items in a BYOD or true 1:1 deployment where end users are provided codes as needed. In these models, you cannot retrieve any codes that you, or the user, redeem.

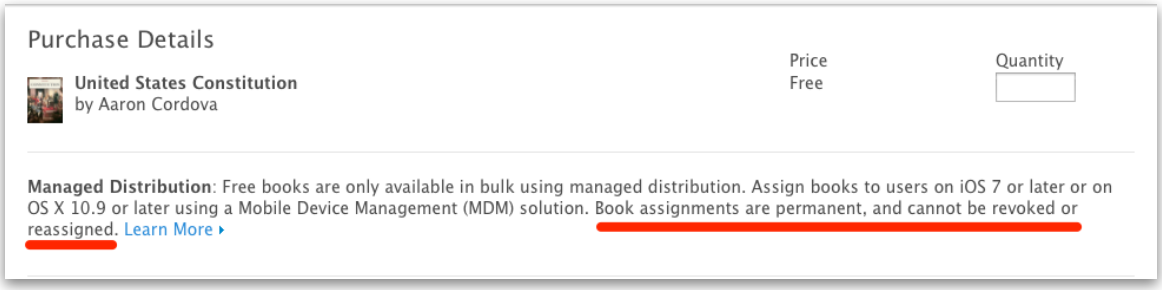
You can also migrate all of your older redeemable codes to managed distribution licenses. This is a one way process, and when you do this, all of your codes are converted. For more information, see the Apple document posted here: https://support.apple.com/en-us/HT202863

Managed Distribution - Using the managed distribution licenses allows you to assign the application to a user and revoke that assignment at a later date. Your option here would let you provide the application to the user during a class or training, then retrieve that license when the class or training has ended, and assign the application to another user.

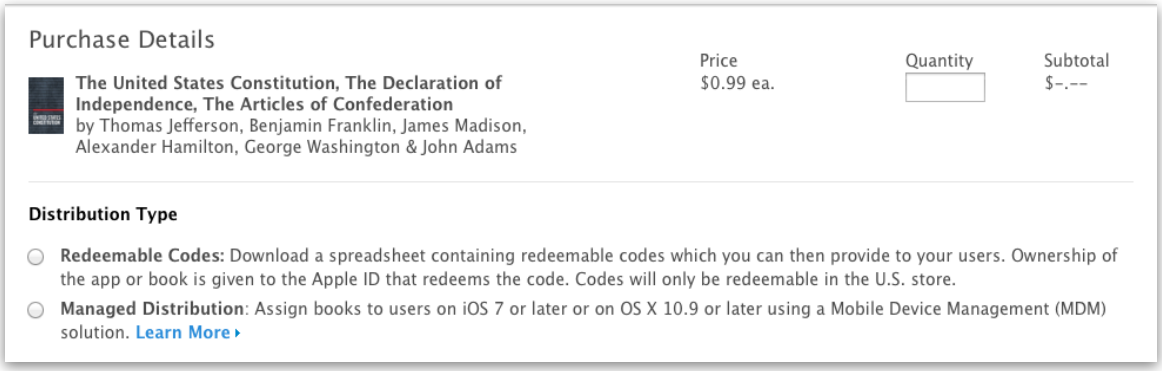
Choose whichever distribution type best matches your deployment model.

Books

If you purchase managed distribution licenses, you have control over the assignment of those licenses to end users, regardless of the deployment model. The one exception to this is with books. Free books can only be provided with managed distribution licenses, yet the item becomes permanent property of the assigned user, as noted below.



Books available for a cost do allow the use of redemption codes; but the same rules apply - books cannot be revoked or reassigned. *Books must also be assigned to personal AppleIDs; they are not allowed to be assigned to institutional AppleIDs per Apple's legal guidelines.*



Note - From Apple's VPP Store - "Revoke and reassign apps as needed. Book assignments are permanent and cannot be revoked or reassigned."

If you use redeemable codes for your book purchases, you will have to download the spreadsheet for that purchase. When you purchase books with managed distribution licenses, you will see those purchases appear in the **License Management** pane of FileWave Admin.

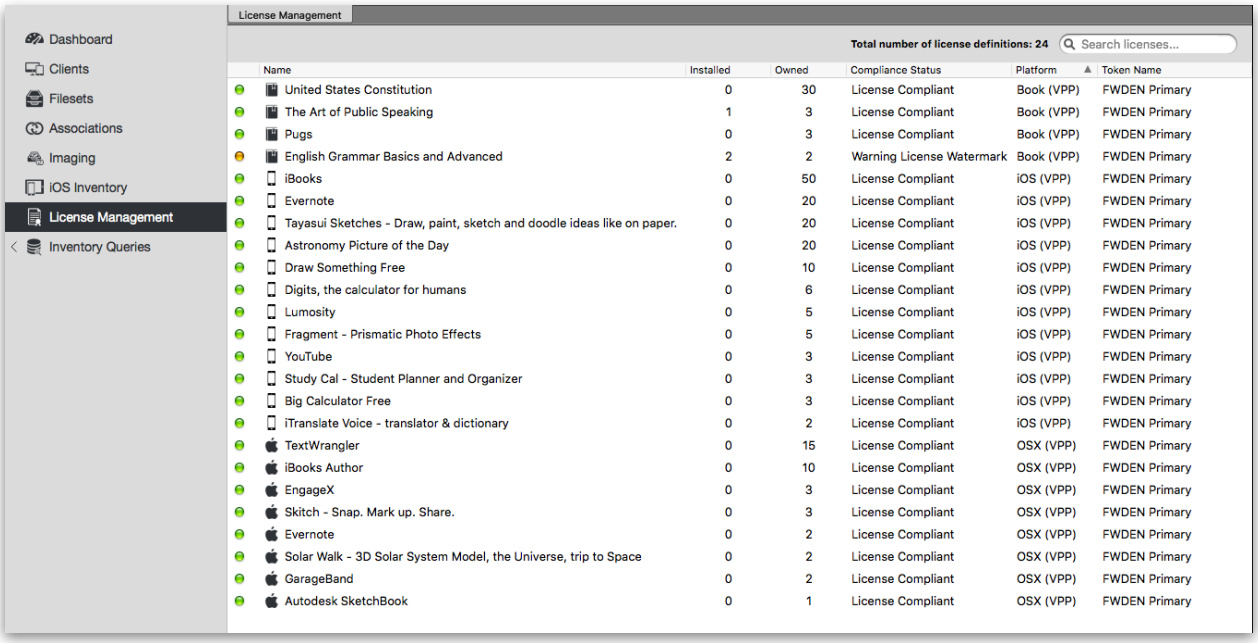
Now that you have seen the examples, you can make some VPP purchases and move on to the deployment of those purchases.

Creating filesets from VPP managed distribution content

Once you have begun to build up your collection of applications and content for distribution, you may need to create filesets for each of the items so that FileWave can associate those items with your managed devices. Just as you did for VPP redeemable code content, you can create filesets to split licenses between different departments, sites, or classes, as needed. For an in-depth look at Filesets, see chapter **6 Filesets**.

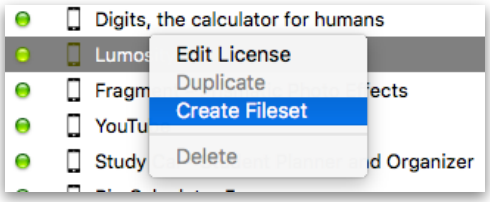
Create a mobile Fileset for each purchased managed content item.

All VPP purchases now appear in **License Management** as soon as the FileWave server syncs with the Apple VPP site.



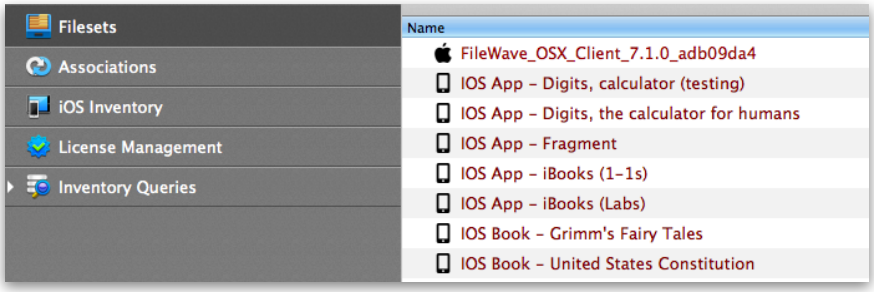
Name	Installed	Owned	Compliance Status	Platform	Token Name
United States Constitution	0	30	License Compliant	Book (VPP)	FWDEN Primary
The Art of Public Speaking	1	3	License Compliant	Book (VPP)	FWDEN Primary
Pugs	0	3	License Compliant	Book (VPP)	FWDEN Primary
English Grammar Basics and Advanced	2	2	Warning License Watermark	Book (VPP)	FWDEN Primary
iBooks	0	50	License Compliant	iOS (VPP)	FWDEN Primary
Evernote	0	20	License Compliant	iOS (VPP)	FWDEN Primary
Tayasui Sketches - Draw, paint, sketch and doodle ideas like on paper.	0	20	License Compliant	iOS (VPP)	FWDEN Primary
Astronomy Picture of the Day	0	20	License Compliant	iOS (VPP)	FWDEN Primary
Draw Something Free	0	10	License Compliant	iOS (VPP)	FWDEN Primary
Digits, the calculator for humans	0	6	License Compliant	iOS (VPP)	FWDEN Primary
Lumosity	0	5	License Compliant	iOS (VPP)	FWDEN Primary
Fragment - Prismatic Photo Effects	0	5	License Compliant	iOS (VPP)	FWDEN Primary
YouTube	0	3	License Compliant	iOS (VPP)	FWDEN Primary
Study Cal - Student Planner and Organizer	0	3	License Compliant	iOS (VPP)	FWDEN Primary
Big Calculator Free	0	3	License Compliant	iOS (VPP)	FWDEN Primary
iTranslate Voice - translator & dictionary	0	2	License Compliant	iOS (VPP)	FWDEN Primary
TextWrangler	0	15	License Compliant	OSX (VPP)	FWDEN Primary
iBooks Author	0	10	License Compliant	OSX (VPP)	FWDEN Primary
EngageX	0	3	License Compliant	OSX (VPP)	FWDEN Primary
Skitch - Snap. Mark up. Share.	0	3	License Compliant	OSX (VPP)	FWDEN Primary
Evernote	0	2	License Compliant	OSX (VPP)	FWDEN Primary
Solar Walk - 3D Solar System Model, the Universe, trip to Space	0	2	License Compliant	OSX (VPP)	FWDEN Primary
GarageBand	0	2	License Compliant	OSX (VPP)	FWDEN Primary
Autodesk SketchBook	0	1	License Compliant	OSX (VPP)	FWDEN Primary

The first time you access this area after setting up your FileWave server, you will get a dialog box telling you that a Fileset can be created for each of the licenses. You can also right-click on any purchase and create a Fileset.



Duplicate filesets as needed to allow for more granular deployments

If you have tiered administration in effect, and want to have other systems administrators assist in the deployment cycle, you can split your licenses into easily managed chunks. Select a Fileset in the **Filesets** section of FileWave Admin, then right-click and choose “Duplicate” from the popup menu. Rename the Fileset as needed. Note the examples below:

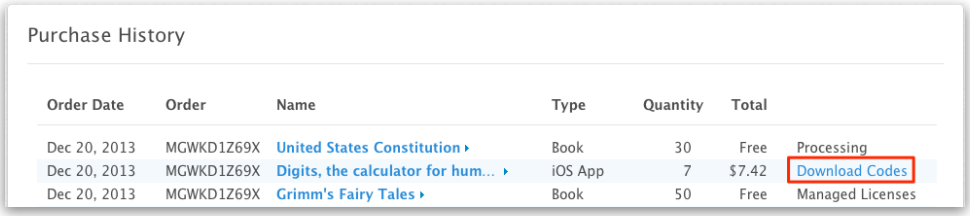


This process allows wider levels of management of filesets across large scale deployments.

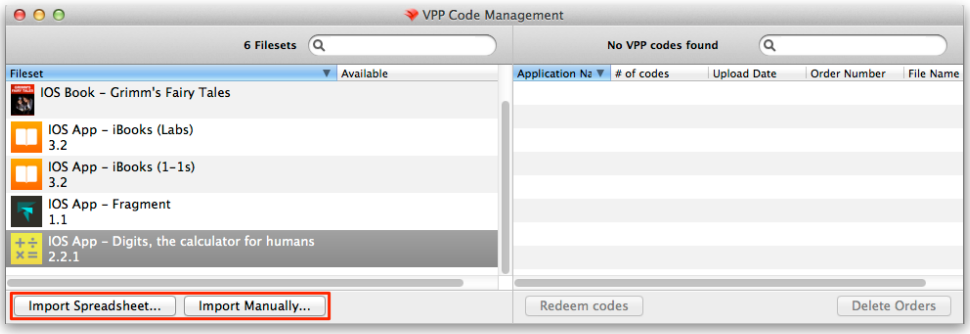
Assign licenses to specific filesets as needed

In order to track and assign codes or licenses, you need to match them to the filesets you have created.

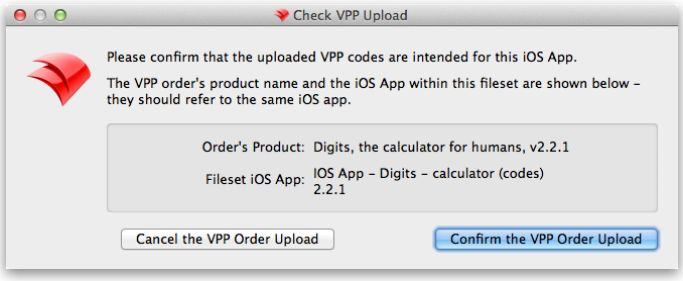
Redeemable codes - For redeemable codes, you will need to download the code spreadsheets. Log into your VPP account online, and select your *Purchase History*. For any content that you purchased using redeemable codes, you will see that you are able to download the codes in the form of an .xls spreadsheet. **Note: This spreadsheet will always be kept up to date on the VPP site. As you, or your users, redeem codes, the online spreadsheet will be updated to show remaining codes.**



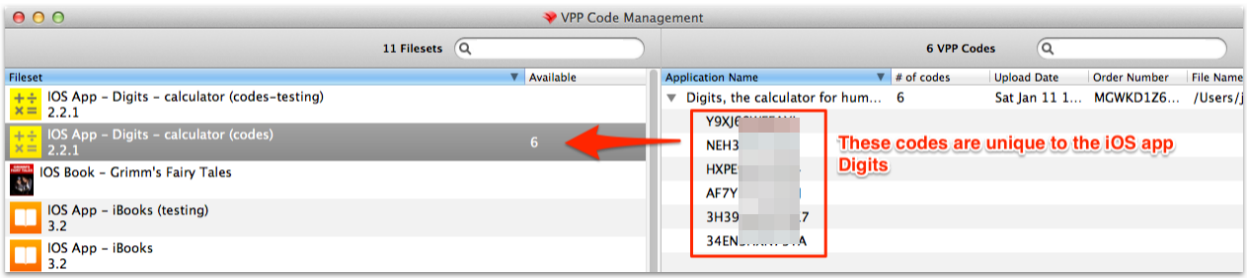
Once you have downloaded the spreadsheet(s) as needed, you will need to go to **Assistants / VPP Code Management**. This pane is used only for linking redeemable codes to filesets. You have two methods for bringing codes into FileWave Admin, by importing the spreadsheet or manually entering the code information.



The **Import Spreadsheet…** method is quite simple. Select the Fileset (if there are multiple filesets for a purchased item, just pick one), then click on the **Import Spreadsheet…** button, locate your downloaded VPP .xls file, and import it. The dialog box tells you to verify that the codes you are uploading into FileWave Admin match the item you want to link them too. You will get errors if you try to match codes to the wrong content, or try to import an older spreadsheet into the set once you have begun redeeming codes.

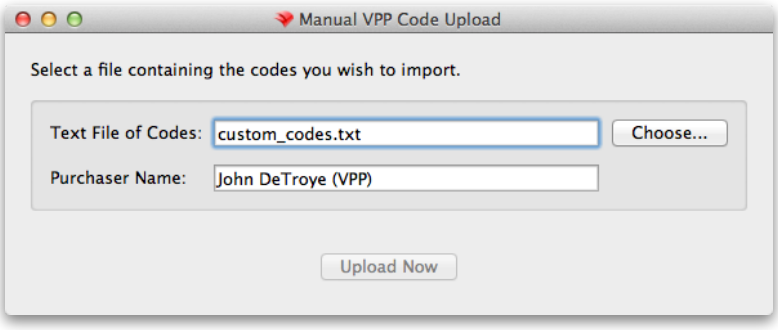


Once you have imported codes, you will see them listed next to your selected Fileset.

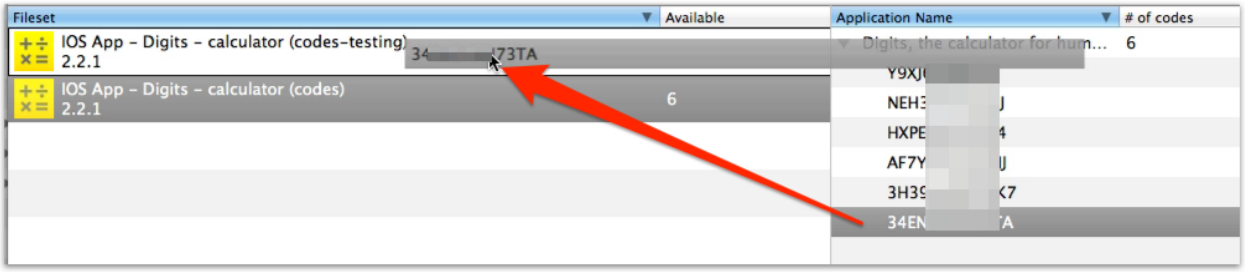


The **Import Manually…** button lets you import a custom text file you create. The format is the URL as you would see it on the App Store or on the VPP spreadsheet, or just the redeemable codes. For example, the file *custom_codes.txt could look like this*:

https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/freeProductCodeWizard?code=Y6XJ69TFXDEJ
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/freeProductCodeWizard?code=Y7XJ69HYIGFJ
Y3XJ69EDSERM
Y4XJ69HYTFEB

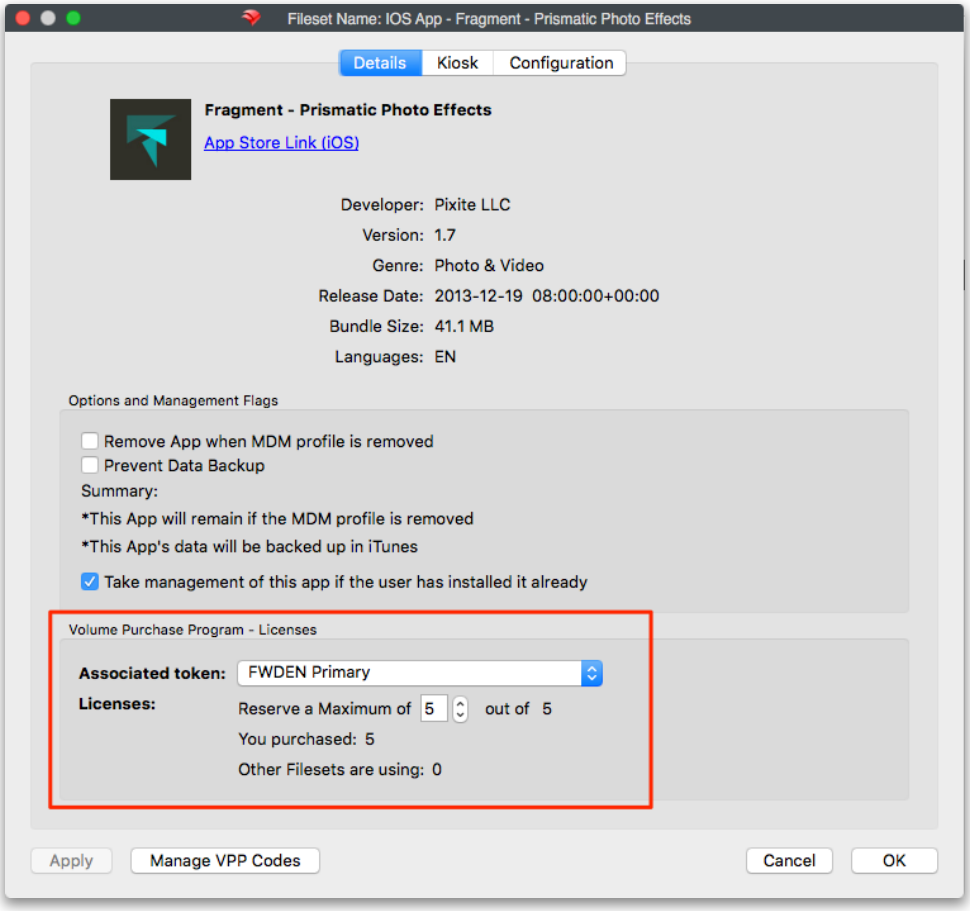


A benefit of using FileWave for working with redeemable codes is that you don't need to breakdown your spreadsheets into separate sections to match the different sets of the same content you plan to deploy. You can just select the number of codes you want to assign to specific Fileset and drag those codes onto that designated Fileset. Our example here is dragging one code from the main Fileset for Digits onto the Fileset meant for the testing team.



This capability allows you to work with your tiered administrators to centrally purchase licenses, yet distribute the ability to provide codes (and licenses, as you will see) to other FileWave admins in different departments, locations, and even classrooms.

Managed Distribution Licenses - The managed distribution content licenses are assigned to specific filesets the same way they are done using redeemable codes; but you no longer see them as manageable items. The licenses are treated as part of a pool now. When you look at each Fileset, you can see the status of your licenses:



VPP Managed Distribution User Management

The most complex portion of the VPP Managed Distribution system is the interaction of the end user and the VPP license architecture. There are two workflows - the older one, and the new direct device association.

The newer process looks like this:

- Select a Fileset with a VPP app
- Associate it with one of your devices/device groups
- Update the model
- Take a nap

The older process breaks down into these steps:

- User agrees to link their AppleID with your VPP MDM solution
- The MDM solution associates managed distribution content licenses with a linked user
- The user sees all assigned content in their own AppleID-based purchases in the iTunes/App Store
- If the user has auto-install enabled, the content automatically appears on the user's device
- If/when the MDM systems administrator revokes a license, the end user may be allowed up to 30 days to continue use of that application while the MDM systems administrator regains use of the license for another distribution. That timeframe is entirely up to the application developer. It is not a value that you can set or change. You would need to check with the specific app developer to get their assigned revocation timeframe.
- If the user purchases the revoked application within the developer allotted timeframe, they maintain all of their sandboxed content. If not, the application and content are deleted (iOS only).

Variations to this process relate to books and certain deployment models. Books, free or otherwise, always become property of the end user under their personal AppleID. This is in accordance with Apple's legal requirements. **Note: Never use your VPP account AppleID for personal purchases.**

Possible deployment examples

Here are examples of various VPP deployment scenarios.

Institutionally Owned devices

A deployment model that has only an institutional AppleID associated with a device, such as in an educational iPad cart deployment, for example, can follow a unique process. You can use the new direct device association method to assign applications directly to the device, and don't need to match up AppleIDs anymore.

Note: The new direct device association method easily replaces the multiple AppleID process.

Remember, you are not allowed to assign books from the iBooks Store to institutional AppleIDs.

Layered Model deployment

In the Layered model, you will configure your iOS devices using direct device association to assign core applications. Once you are done with that process, you will turn the device over to an end user for additional configuration. That user will use their personal AppleID to provide additional content. This is a very good use of the FileWave self-service Kiosk. You can provide additional vetted applications and content for the user; but they install only items they have need and/or space for.

1:1 / BYOD model

The best practice deployment model is to have a user sign for the device and use their own personal AppleID for app/content deployment. You will have the users enroll with your FileWave MDM, associate their AppleID with your

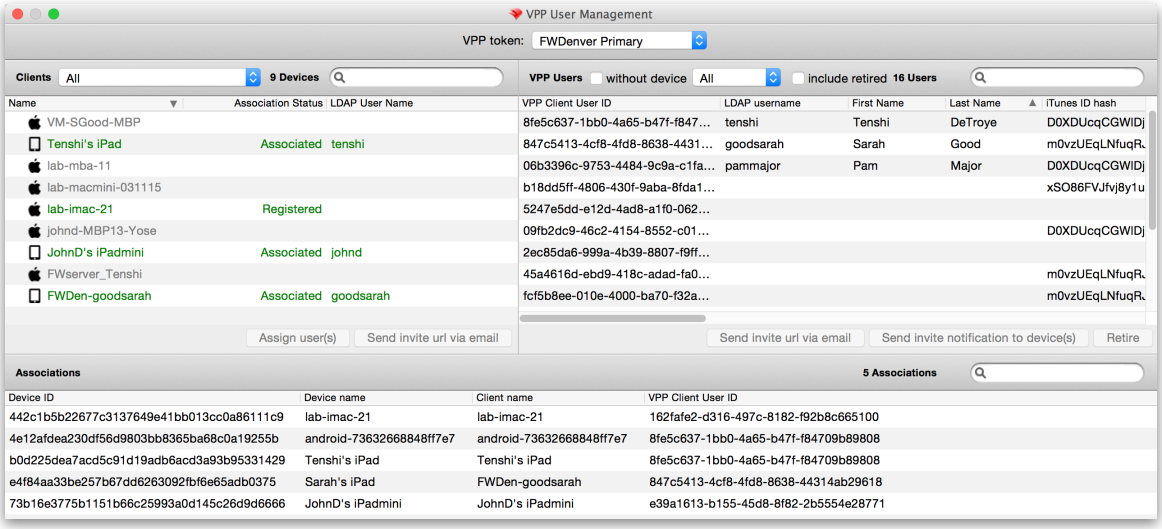
FileWave MDM, then you assign and revoke apps/content licenses as needed. This model supports assigning both applications and books to the end user.

Note - this entire process was designed by Apple around the concept of a BYOD or 1:1 deployment, where a user registers a device under their AppleID, then enrolls in your FileWave MDM. When that is done, the managed distribution participation becomes automatic. The idea is that you provide the "carrot" - services, applications, and content the user needs - balanced by the "stick" where if the user un-enrolls/deletes their MDM profile, they lose all those benefits.

That said, let's look at what you need to set up your FileWave MDM VPP Managed Distribution users and devices. For this, you need to select **VPP User Management** from the **Assistants** menu item in FileWave Admin.

Creating users for your devices

Apple's VPP manages licenses that are either assigned to a device, or assigned to specific user's AppleID. In the **Assistants / VPP User Management** pane, you can see all of your enrolled devices, and a list of VPP users.

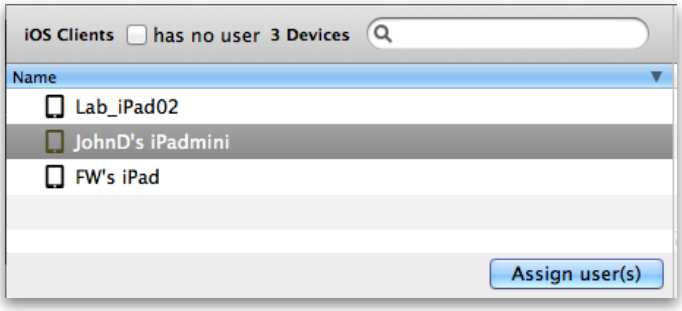


In the upper left is the list of enrolled devices. In the upper right is the list of VPP users you need to create. The lower portion of the window displays the device and users who are associated with each other for management purposes.

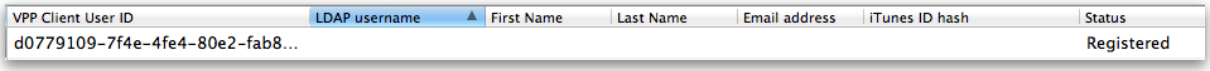
Note - You do not need to do this process manually for a population of several thousand users. FileWave provides the ability for you to link your LDAP directory and your enrolled devices together automatically.

The option also exists to have a VPP user created automatically as each device enrolls. When doing batch rollouts of iOS devices, this may be your best option.

In the VPP User Management pane, we can manually assign a new VPP user for each device:

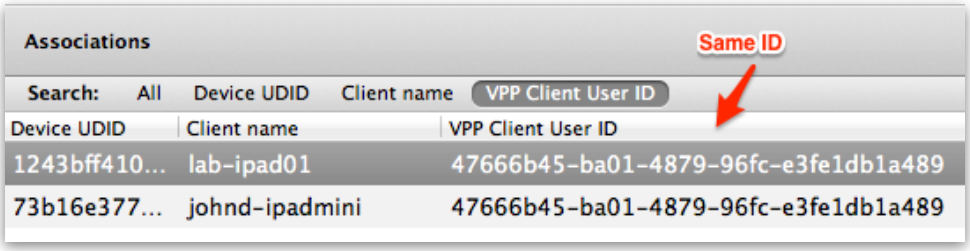


This will give us a VPP user account with blank fields:



The VPP Client User ID is a construct that is used by FileWave to facilitate the association of a device - which FileWave can manage - to an AppleID - which belongs to a user. The account is unique, and has one of three states - registered, associated, or retired. **Registered** means that the account is assigned to your FileWave MDM by Apple. **Associated** means that the account is linked to an AppleID through an iTunes ID hash and the user can have licenses assigned to them. **Retired** means that all licenses assigned to that VPP Client User ID are revoked and can be used again.

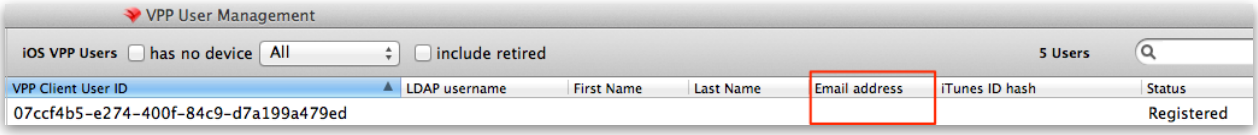
An AppleID can be associated with multiple VPP Client User ID's; but only one VPP Client User ID can be associated with an enrolled device. It also allows users with multiple iOS/OS X devices to have a single VPP Client User ID associated with those devices, if you are managing all of those devices.



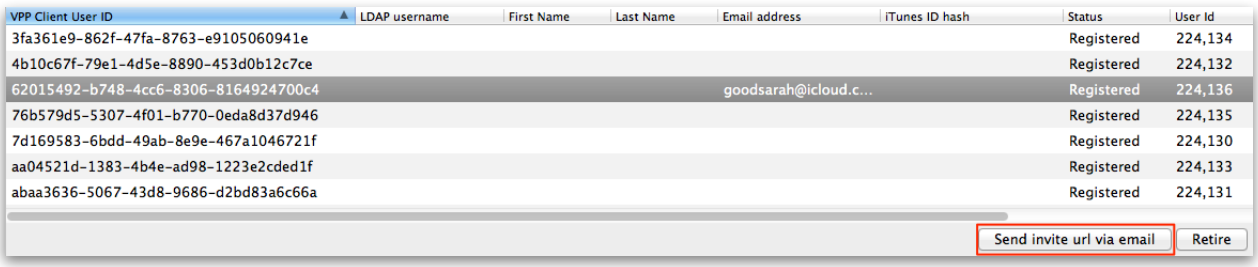
If you link your LDAP accounts to FileWave, then the directory service will have the users associated with a VPP account. This will fill in those blanks, and make the next step easier. More on this in section **12.7**.

Inviting users to the FileWave MDM VPP

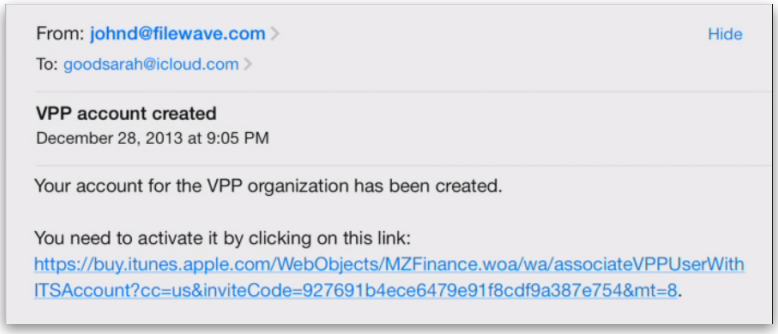
Apple requires the end user to actively link their AppleID to your FileWave MDM. You must send an email to each VPP user account after you have provided their email address. Click in the **Email Address** field for the VPP user account and enter a valid email address. The does not need to be a user's AppleID email address, just an address where the user can get a VPP MDM request.



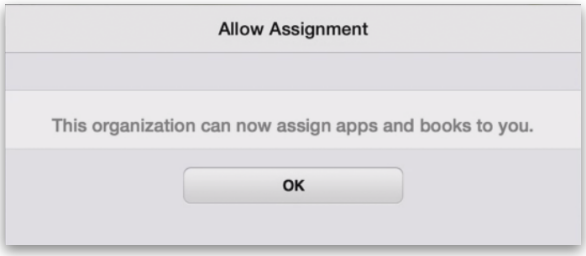
Once you have entered a valid email address, the button to send an invite to the user will be active.



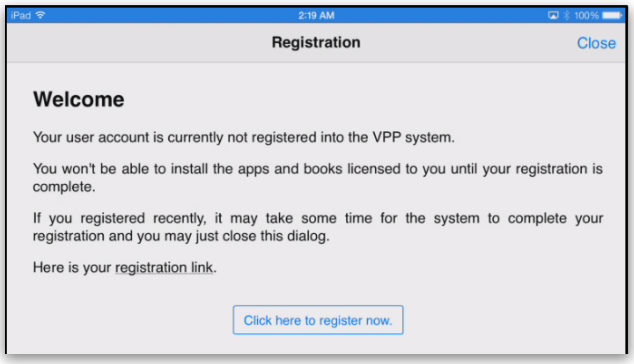
The user will get an email asking them to activate the link to their “VPP organization”; i.e, your FileWave MDM server. This email account does not need to be the email that person uses for their AppleID. It can be an internal email address used within your organization/institution, or any common email address the user may provide. This process will link that user’s AppleID to your FileWave MDM so that you can assign applications and content to them. You will never see the user’s AppleID unless they give you the email account they use for their AppleID as their contact email.



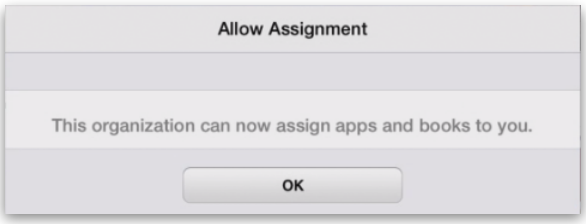
The user will be required to authenticate to the iTunes Store, and will then get notified that they can now be provided with content from your FileWave MDM.



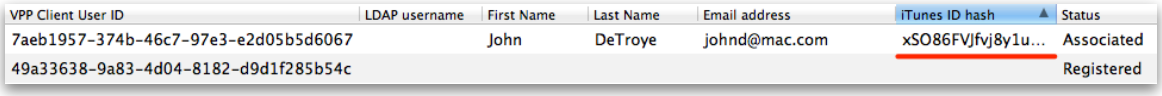
If you are doing this as part of a BYOD or 1:1, this process can be sped up by having the end users register themselves with FileWave. An enrolled iOS device will have the App Portal installed, the user opens the App Portal and will be greeted with this dialog, asking them to register their AppleID:



The user will authenticate to the iTunes Store and be presented with this dialog telling them that you are now able to assign applications and content to them:

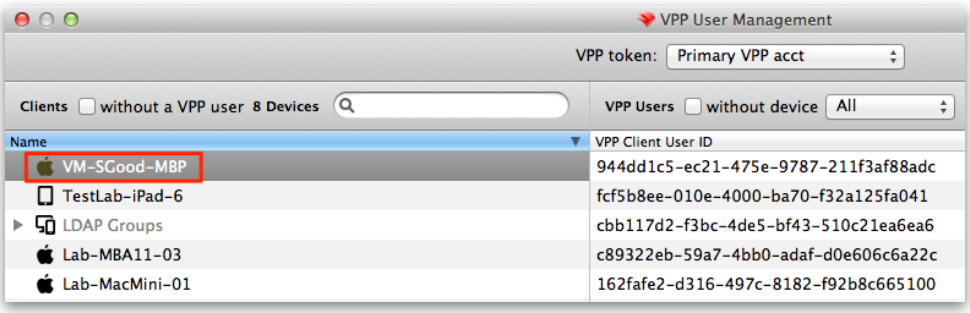


Once a user's AppleID is associated with the VPP user account, you will see the link in the VPP User Management pane. Note the iTunes ID hash. This value is your proof that the AppleID is associated with the FileWave MDM. You will not see the user's AppleID unless that is also the user's email registered with your institution.

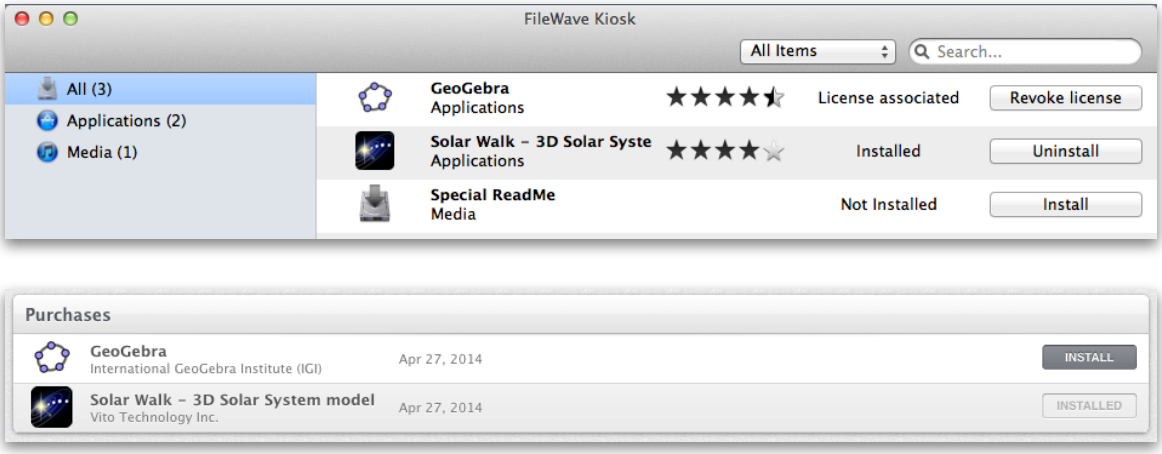


FileWave and OS X VPP users

The process for OS X devices and users is almost identical to that of iOS users. When you add an OS X device as a FileWave Client, it will show up in the **Manage VPP Users…** window.



You will still go through the user assignment unless you automated that in the VPP preferences. The user email will have to be entered unless the user logged into the device with an LDAP account and that account had a valid email account attached. If so, you can have the FileWave server automatically send off an invitation to associate that user with the FileWave VPP. Whichever process you use, the end user will still have to agree to associate with your system. Once that is done, you will be able to assign applications and books to that user through Filesets linked to the VPP managed distribution system. Here's the final view of the Kiosk and the App Store after some Filesets are associated with the client.



Retirement

The VPP Client User ID is owned by Apple. Your FileWave MDM is managing that ID and associating it with devices enrolled into your server. At some point, that account may become stale, the AppleID may become invalid, or you may no longer need that user associated with your management setup. When this happens, you can retire the account; and in certain cases, Apple may retire the account. You can view any retired accounts by selecting the **include retired** checkbox in your VPP User management window.

Note: If you retire a VPP user account, it cannot be used again. It is strongly suggested that you do not test "retiring" VPP user accounts on actively enrolled users.

If you do retire a VPP Client User ID by accident, you can just attach a user's email address to a new VPP Client User ID, and repeat the invitation process. The problem that gets created with unintentional retirement is that the user will have all of their managed distribution licenses revoked, and you may have to go back and re-add that user to the system.

At this point, we can finally begin assigning licenses to devices (actually to their associated users) by associating filesets with the enrolled devices.

Note: Do not try to use your VPP token on more than one MDM server. Doing so may result in all of your VPP user accounts being automatically retired.

Deploying VPP content through filesets

Note: This is the older method of associating content to a device through a user's AppleID. The newer process is described above - and has way fewer steps.

We have purchased redeemable codes and managed distribution content licenses; created filesets; associated, or linked, users to our enrolled devices; and are ready to deploy our content to devices.

Note: The method of downloading an Apple App Store application's .ipa file and manually distributing that as a Fileset is not supported by Apple or FileWave. The Enterprise Fileset is meant to be used only with internally created content, such as the new FileWave App Portal.ipa and the Engage.ipa

Streamlining the installation process

In order to make content that is assigned to a user and their device show up automatically, the enrolled device must either be in supervised mode, or you need to tell the end users to turn on auto-install. (iOS devices only)

If automatic download is not active, the user will get dialog boxes informing them that there is new content for them to accept. (Note: Currently, there seems to be a bug in iOS that displays the dialog box some times anyhow.)

Associating (distributing) redeemable code content

There are two supported methods for deploying applications with redeemable codes.

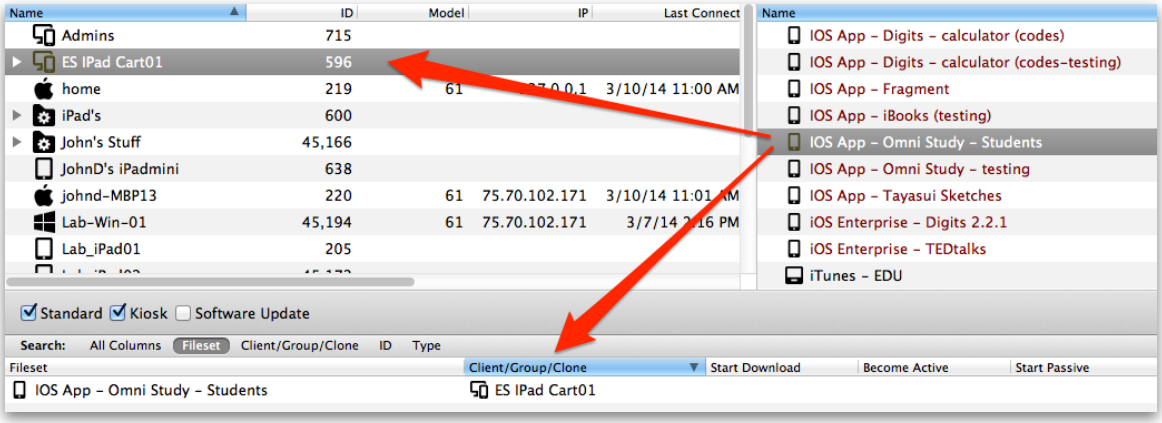
The first is to just associate the codes with the devices and they will be redeemed against the institutional AppleID registered with that device. A single code will be redeemed against that AppleID; so multiple devices under the same institutional AppleID will show as only a single code redeemed. You must then track the number of devices that have that application installed and manually count the codes as redeemed. The manual sections on **Inventory** and **License Management** will assist you in doing that. One way to avoid manually tracking the licenses would be to generate an institutional AppleID for each iOS device to be deployed. This method is unrealistic outside of the deployment of a few institutionally owned devices. Check with your Apple Sales team for more information on creating large numbers of institutional AppleIDs. This is not the same idea as capturing an **.ipa** file and copying it to multiple devices - that is the Enterprise Fileset model and it is not supported for App Store content. If you want to mass deploy an application like that you must use **Apple Configurator**.

This method is also the way many institutions distribute books that they create internally, such as books created with **iBooks Author**.

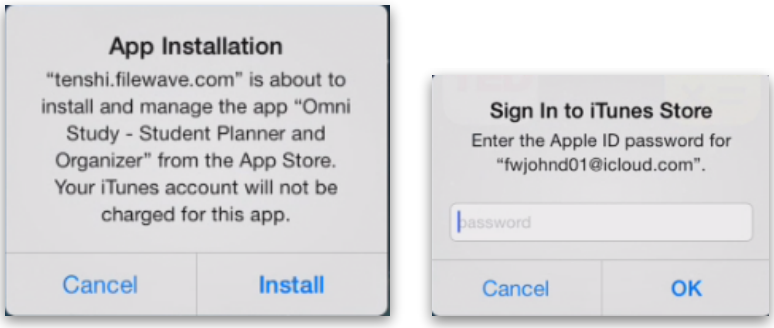
The second method can be used with 1:1's and BYOD's. You associate the application Fileset with the device that is using a personal AppleID. The user gets credit for that application in their iTunes Purchases. This method has the added benefits of being able to be used with books from the iTunes Store, as well as putting the onus onto the user for updating any provided applications and/or books. If you distribute content to a personally managed device, FileWave will record every instance of a code redemption by those personal AppleIDs. An optional distribution method is to send the user the URL to the redeemable code and they handle the redemption and installation themselves.

Method 1 - Direct Association

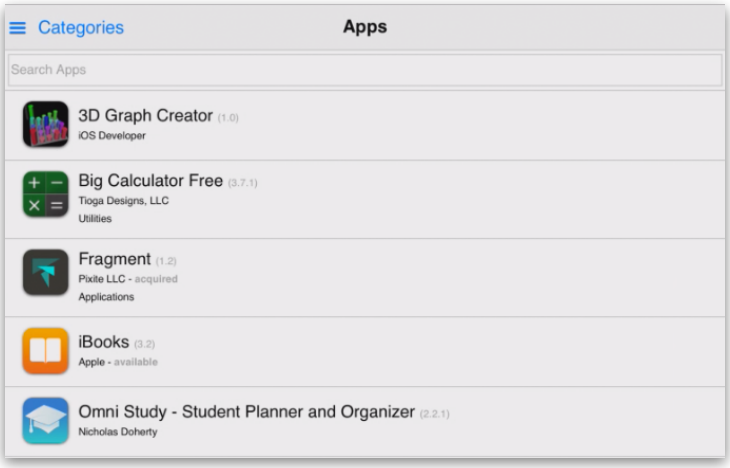
In FileWave Admin, select **Associations** in the main FileWave Admin window. Choose the Fileset you wish to deploy, and drag it over the client device or device group. Once you have done that, you will see an association in the lower window showing that the Fileset is linked, or associated, with that device.



We would then update the model, and see the application get installed. If the device is not supervised (and sometimes, just because iOS decides to), you will see the dialog that the FileWave MDM is about to install the application. The application will be credited to the AppleID of the user account associated with that iOS device - whether it is an institutional account or individual's personal AppleID. Since it is also going through the iTunes Store, unless the device is supervised using Apple Configurator, the administrator will have to enter their institutional AppleID password to accept the application. You can see how this method is dependent on direct interaction unless it is supervised.

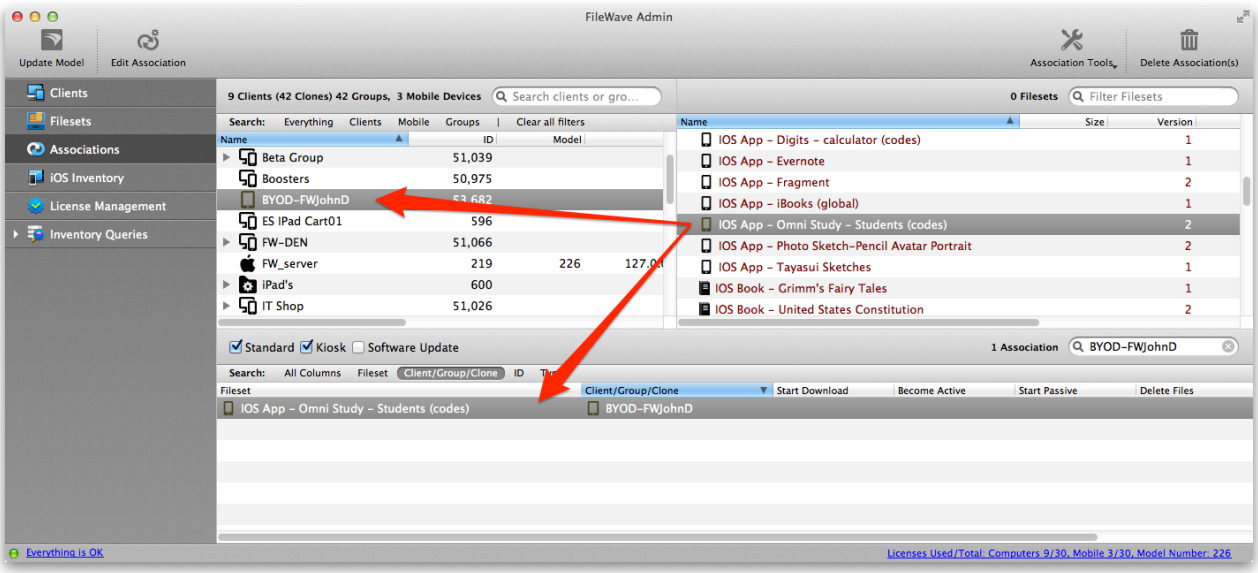


The application is also immediately available inside the App Portal:

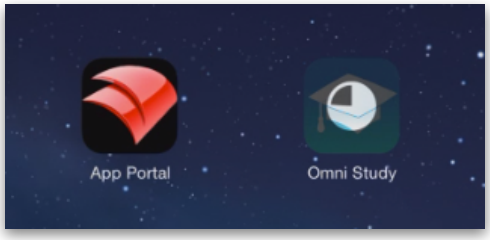


Method 2 - Personal AppleID

A Fileset that has manage licenses is located and associated with an individual user's iOS device. You may also associate the Fileset with a group of devices, and as each device installs the application, a license will be redeemed against that device.

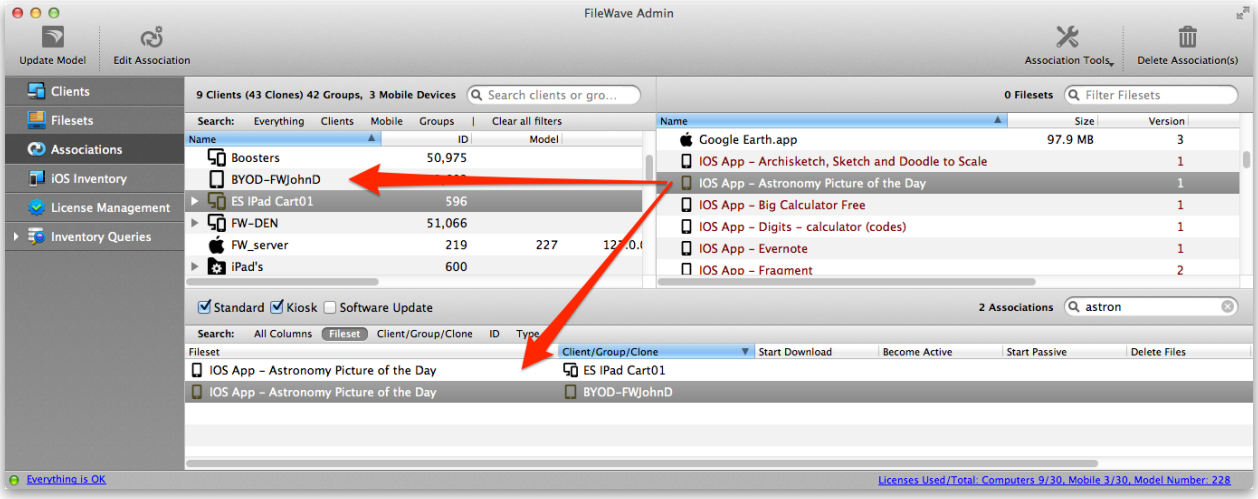


When we update the model, the client devices will see the application install:

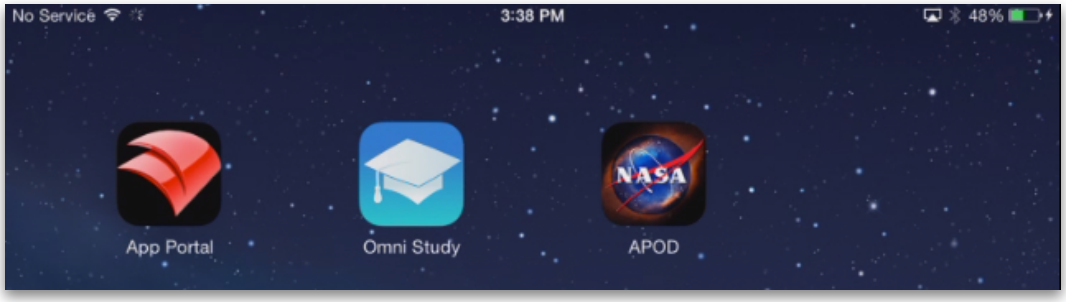


Associating (distributing) the managed distribution content

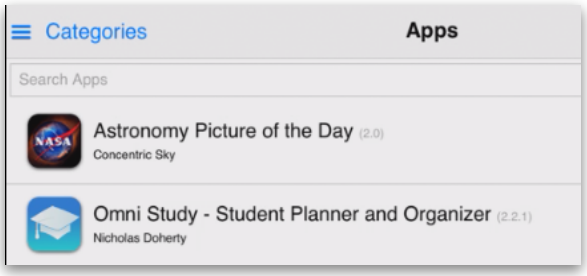
Select **Associations** from the main FileWave Admin window, and we will drag the “Astronomy Picture of the Day” Fileset over top of “BYOD-FWJohnD” to associate the two.



You can double-click on the associated Fileset to set its activation time, or just update the model which will cause the activation to happen right away. We are not making this a Kiosk item. Update the model, and the client device will get the new application almost immediately.



A major benefit FileWave brings to this process is that the user doesn't need to go to iTunes or the App Store to see content that is assigned; they can just open the App Portal.



If you add books to the mix, do not forget to create a Fileset for the **iBooks** application from your VPP purchases. Books sent to the user's device will show up inside the FileWave App Portal. Those items are also permanently assigned to the user. You cannot get book licenses back from iTunes. And (yes, this yet another reminder), remember that you may not assign licenses for books from the iTunes Store to non-personal AppleIDs.

Where OS X VPP differs

One key difference between iOS and OS X VPP managed distribution is in the way the applications are installed. You will be asked on the client if you want to turn on automatic application installs; **but** it refers to apps downloaded onto other devices. What that means is if the end user has a single device, they will get apps showing up in their App Store / Purchases section and those apps will not automatically install on the device. The user must do that.

This also affects Kiosk operations. If an application is in the Kiosk, just selecting it and telling it to install may not result in it showing up in the user's Applications folder - until they go to the App Store / Purchases list and install it from there.

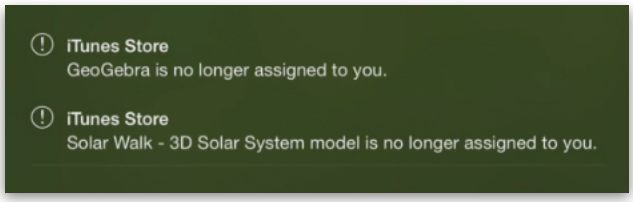
Revoking licenses using FileWave MDM with VPP managed distribution

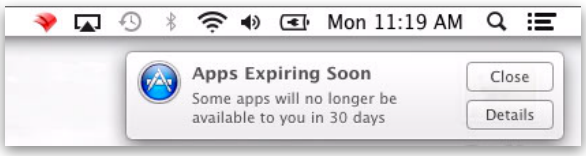
When a user is no longer part of an institution, or is no longer working on a project or class that requires a costly application you have a limited number of licenses for, you can revoke the managed distribution license for that application and return it to FileWave's inventory.

The process is the same as you may have already used to remove any other assigned item to a managed device with FileWave - you merely dis-associate the Fileset. Once the model has been updated, you will see the application licenses returned to your license management pool. The behavior of the application on the client device is dependent on the way the application developer designed the revocation settings into the app. A developer can set the app to continue to exist for up to 30 days on a user's device. This also means that the application will remain in the user's purchased list in iTunes. The user may get a notice saying that they need to purchase their own copy of the

application. On the other hand, the user may get no warning, and the application - along with any sandboxed data - will just disappear from their device.

Note: OS X devices may take several minutes before noticing the applications are no longer assigned to them. In some cases, if the user has both an iOS and OS X device associated with your VPP system, you may see notifications pop up on the iOS device before the OS X device gets the word.

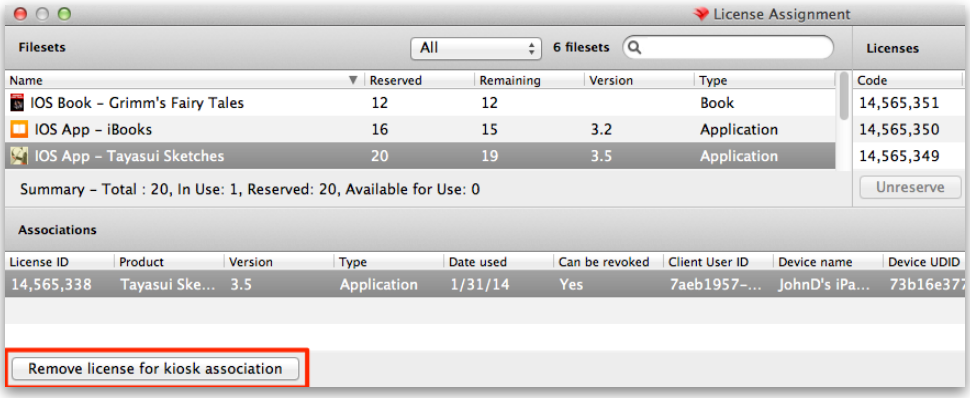




One control you have as the FileWave systems administrator is that you can also set a trigger on the Fileset for that application to delete its contents if the end user removes the MDM profile. This creates what is known as the “Carrot and Stick” management model. In this model, you provide services, such as the SSID and password inside a WiFi profile for an enrolled user. Add to that certain key applications they need for school or work. If the user decides to delete the FileWave MDM profile, all their access to the network, as well as their key applications disappear.

You can also assign filesets to Kiosk mode only, allowing the users the opportunity to install content as needed. If you do this with managed distribution content, you can revoke the license for the AppleID associated with that device by using the button **Remove license for kiosk mode** and the content is removed from the Kiosk on that device.

Note: The content will be removed from all devices associated with that AppleID.

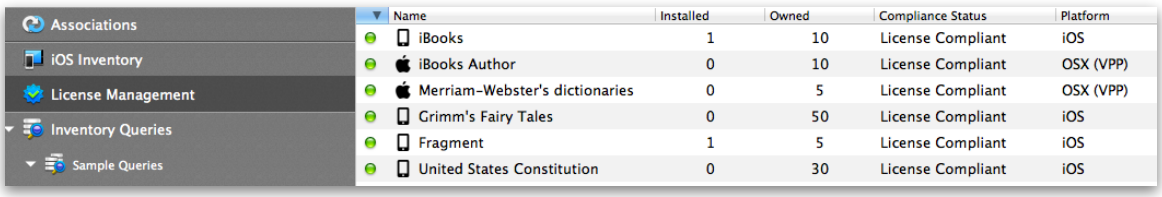


Customizing your VPP configuration

Here are a few more best practices and ideas to make using the new Apple Managed Distribution VPP a great addition to your systems management toolbox.

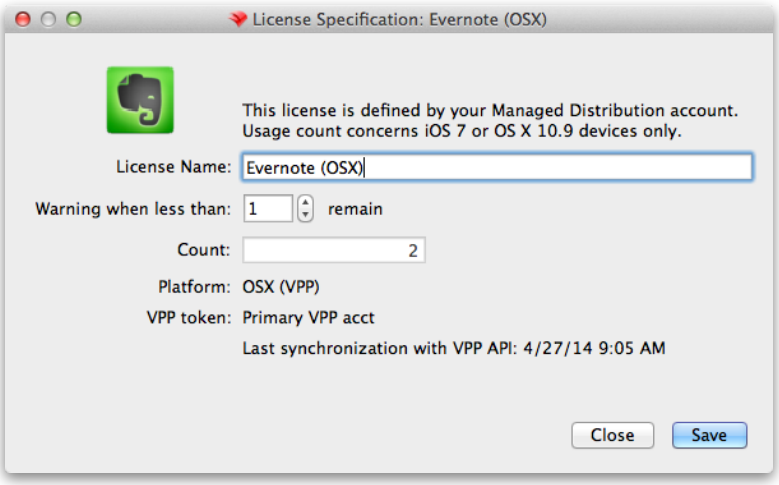
Inventory and licenses

Since FileWave already manages licenses for your desktop systems by keeping track of deployed applications, purchase orders, and license definitions, having it also keep track of your VPP licenses will help a lot.



You can see all the licenses that have been purchased, including OSX (VPP) licenses that are supported in FileWave.

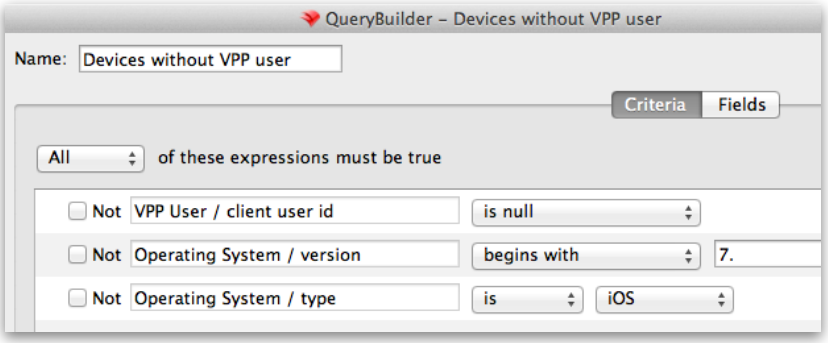
The view of the license information is different from the manually created licenses for non-VPP items being tracked:



Note that you can assign warnings to keep you informed of low license counts with VPP licenses just like desktop licenses.

Inventory queries and VPP

FileWave supports an extensive set of options for digging into its database. This capability provides a great benefit for VPP management. For example, you could have a query that shows you all devices that do not have an assigned VPP user - plus you can make that a scheduled report that gets emailed to you regularly as users enroll in a 1:1/ BYOD.



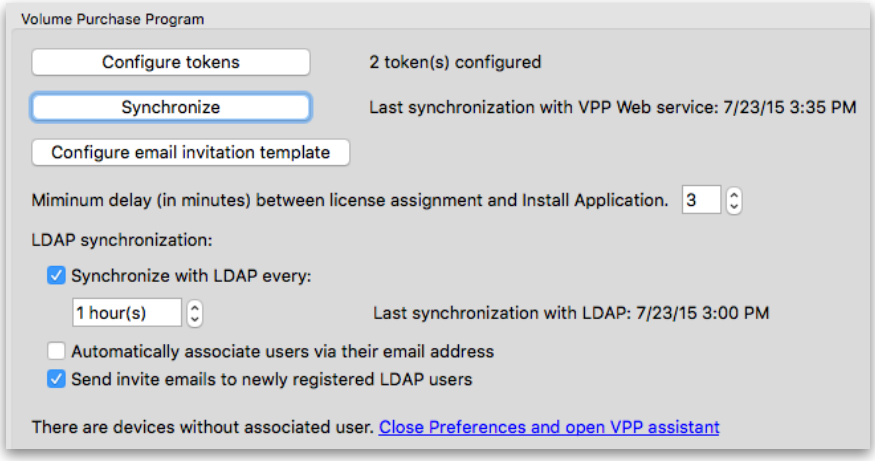
Status messages

FileWave also allows you to see status messages as part of the Inventory and reporting process. This can be especially useful as you are busy associating a lot of managed distribution content with a lot of devices. See the section on **Inventory** for more information on this capability.

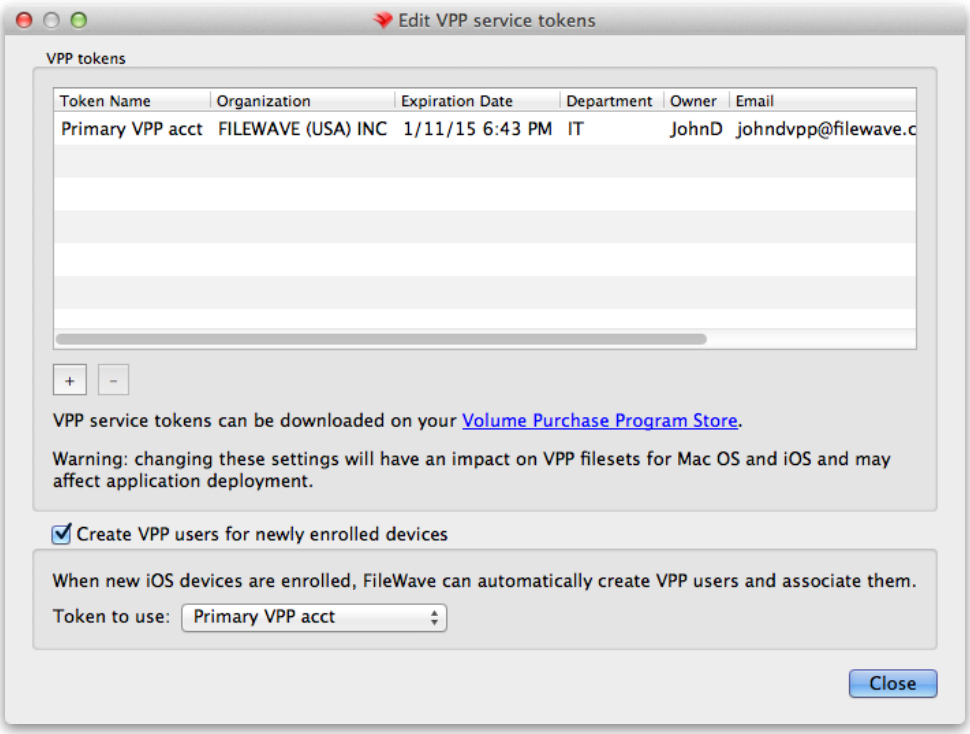
LDAP integration and VPP

If you are using FileWave's LDAP integration, your ability to create a bulk list of VPP users is greatly enhanced. Follow the basic FileWave server instructions to add your LDAP (AD,OD, eD, raw LDAP) directory to your FileWave server. If you want your users to enroll their devices using LDAP, then use this document: **Using LDAP to enroll iOS/ Android devices** (https://www.filewave.com/support/kb/article/enroll-ldap) - this will also work for users logging onto LDAP-bound OS X systems. The instructions for setting up LDAP enrollment are also covered in Appendix**.**

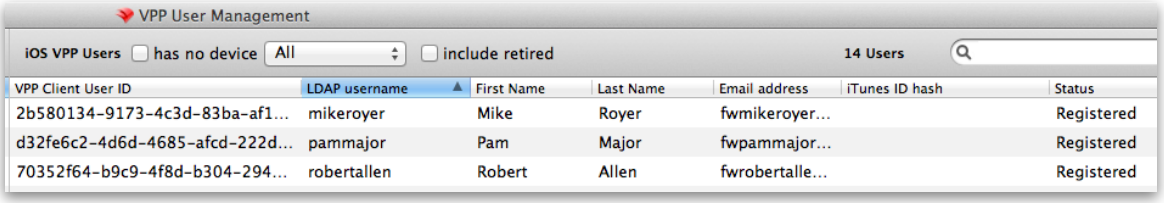
In the FileWave Admin Preferences, under VPP, you will see a set of options that are available when you have linked your FileWave server to an LDAP directory. These options allow you automatically create users connected to their AppleIDs, if that is also their primary email address; as well as sending the linkage email VPP needs to connect a user to your FileWave MDM configuration. Here are the VPP preferences:



The pref pane for automatic VPP user creation is tied to the token preferences:



With your LDAP directory sync'd with FileWave, you will be able to set the VPP preferences to support drawing from the LDAP users to populate the VPP users table. If the **Automatically create VPP users with new devices** check box is selected in the VPP preferences, then as your users enroll into FileWave with their LDAP credentials, a new VPP Client User ID will be created with that user's LDAP account automatically entered.



Once the users are in the VPP User Management window, you can send invitation emails to their internal (or external) email account, requesting that they register their Apple ID with your FileWave MDM. Once the users have done that, your users will be associated with their iOS device, and ready to receive applications and books from your FileWave MDM.

8. “Modern” Device Management (MDM)

FileWave supports both iOS and OS X management through its Profile Editor. Android and Windows management is handled through Filesets. Mobile Device Management (MDM) has evolved into “Modern” Device Management with the inclusion of more varied types of devices into the “mobile” realm, as well as the blurring of the lines when it comes to managing laptops and tablets in the same environment.

With FileWave’s Fileset technology, you can provide many levels of management. Depending on your institutional mission and requirements, as well as the end user (your customer) needs and requirements, you can provide a range of items from simple self-service content distribution to fully locked down systems. Each of the major operating systems supported by FileWave can be managed in some form.

Setting up MDM in FileWave is done with the installation of the FileWave MDM server. Instructions for server setup and configuration are in section **3** of this manual.

8.1. Managing Windows / Android

Windows management under FileWave is done through the use of Filesets to establish application control. It is possible to deploy Filesets with **regdiff** files that change settings on the Windows machine getting the Fileset. Android management, outside of assigned applications, is beyond the scope of this manual currently.

One mechanism that makes application management interesting is the ability to create a Fileset to override items installed by a user. For instance, if a user installs an application that is not allowed, you can create a Fileset with that application in it, associate that Fileset with the user’s client device, then de-activate the Fileset, removing the application from operation.

8.2. Managing OS X

Apple’s OS X (oh-ess-ten) has two different mechanisms for client management - the legacy Managed Client property lists (mcx.plist) and the managed Profile. All supported versions of OS X can use the older form of management; but only OS X v10.7 (Lion) and newer can use Profiles. The Profile Editor uses a unified interface to provide settings for all of the supported OS X systems. Settings that cross over between the two mechanisms of management are automatically configured to be mcx.plists for pre-Lion systems and profiles for Lion and above. App Store Profiles can also be associated with Apple’s VPP system for better management of application licenses.

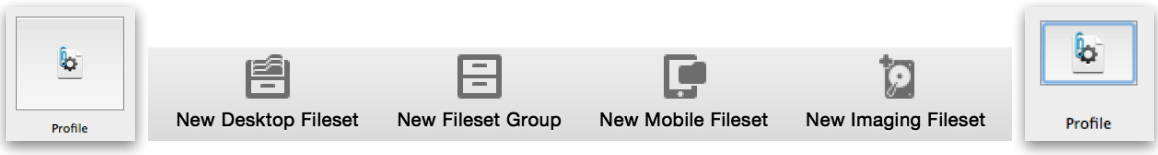
8.3. Managing iOS (MDM)

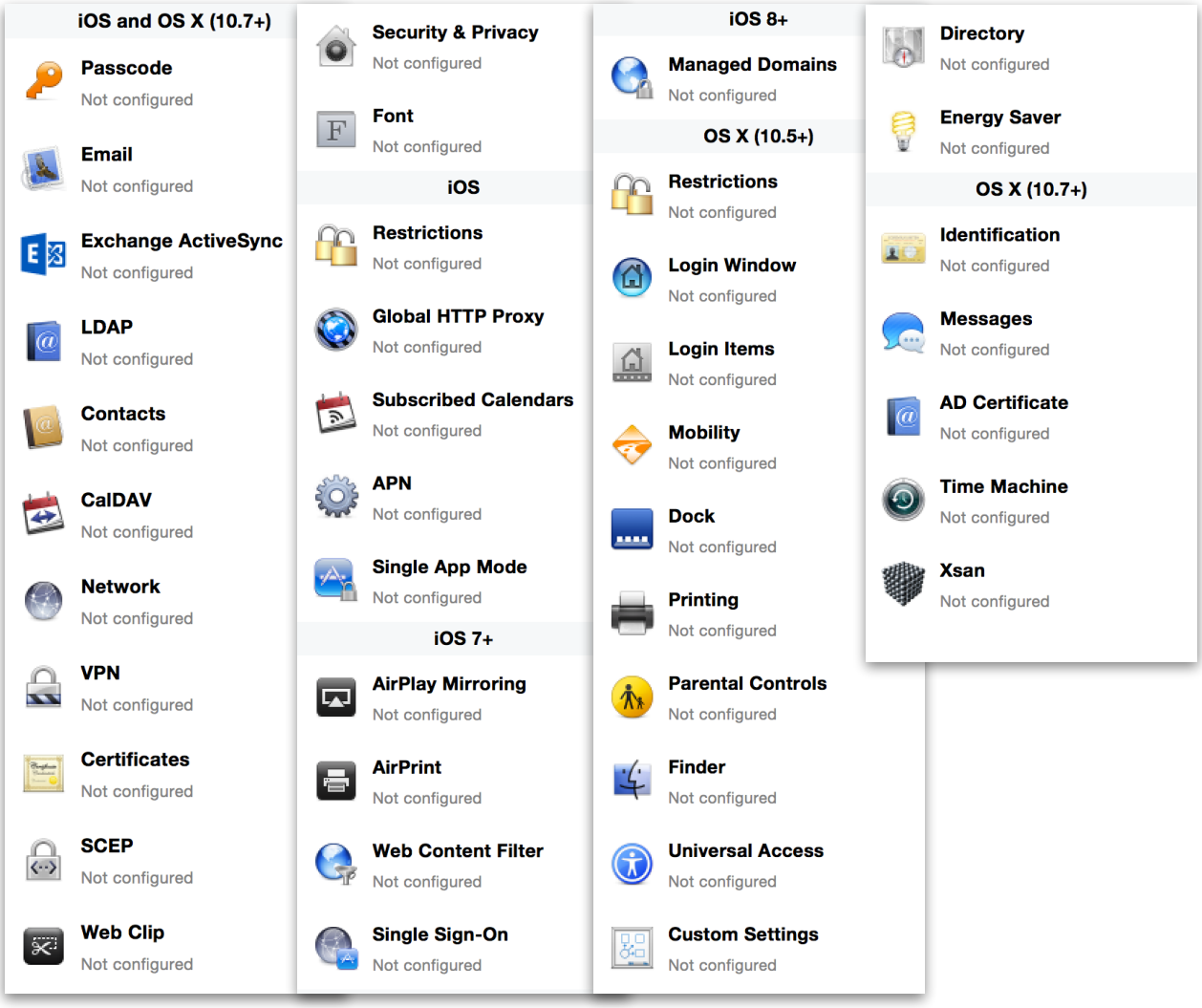
Apple iOS devices are managed with Profiles. Associating Profiles with iOS devices can be done after the device has been enrolled with the FileWave MDM server. The instructions on performing enrollments are in section **3** of this manual. Once the iOS device is enrolled, you can provide content, profiles and applications as needed using Filesets. FileWave has the capability of applying all of the management settings that Apple has provided for MDM coverage of iOS devices and Apple TVs. As with OS X, App Store profiles can be associated with Apple’s VPP system for better application license management.

The ability to establish complete supervised control over an iOS device requires the use of Apple Configurator or enrolling your iOS device in Apple’s DEP (device enrollment program).

8.4. Profile Editor details

The primary management tool for client management / MDM on iOS and OS X is the Profile Editor. It can be accessed through either the Desktop Fileset or Mobile Fileset tool - the Profile Fileset is the same regardless of which tool you use. More information on creating and editing Filesets can be found in section **5** of this manual.





General settings

The first item encountered in Profile Editor is the **General** settings. This is not a profile; rather a header for any profile to be created. Best practice for profiles is to create a single payload setting within each profile, giving it an understandable name in the General settings. While you can configure multiple payloads per profile, troubleshooting and detailed management are made much more difficult.

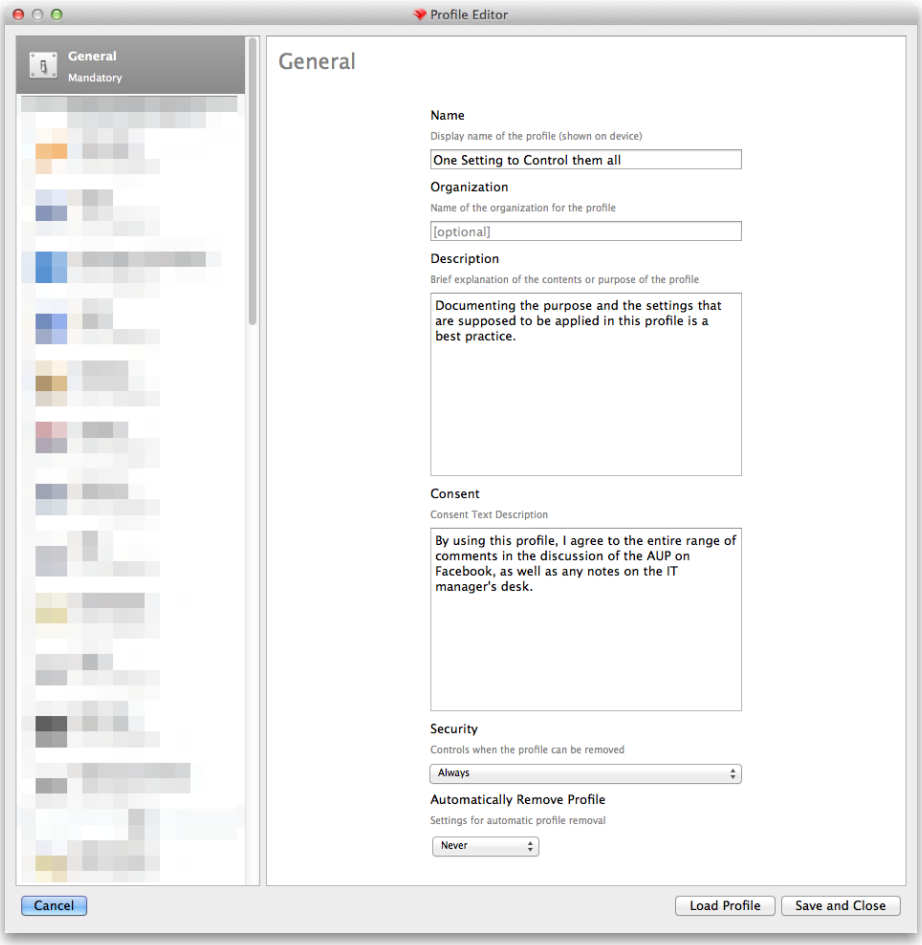
General settings

The key settings to note are the **Name, Security** and **Automatically Remove Profile**. All other settings are optional; but recommended. You must give the Profile a name for tracking purposes. The **Security** setting lets you decide if the profile can be removed by the end user or not. Unsupervised iOS devices can remove profiles regardless of the settings here.

Note: Due to changes in how profiles are installed on OS X 10.10+, if you install a profile on which you have set Security to *Never,* FileWave will not be able to remove the profile on its own, and will ask for admin credentials on the client machines. The workaround is to use a password protected removal with the *With Authorization* option.

Automatically Remove Profile settings will disable the profile after a specific time interval or on a specific date. We recommend you leave this set to *Never* and use FileWave to remove the profile when necessary.

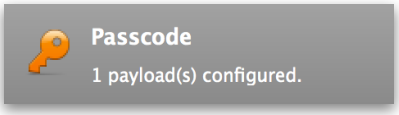
The other settings, **Description** and **Consent**, are fields used to provide more detail for troubleshooting purposes, and to display a text block asking the user to agree to the content of the Consent text when installing this profile manually. If the profile is installed as part of a FileWave Fileset, the end user will not see this.



Universal settings - iOS and OS X (10.7+)

These settings are unified and can apply to any supported iOS device as well as any OS X device running 10.7 Lion or higher.

Passcode



Passcode allows you to establish a more complex passcode rule for end users, including requiring a minimum length, alphanumerics, and time limits. A few of the key settings are:

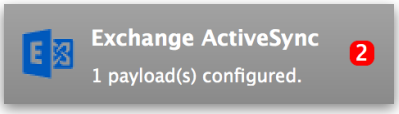
- Maximum passcode age: requires user to change passcode within defined timeframe
- Auto-Lock: defines the amount of time the device can be idle before it locks

- Grace period for device lock: defines the amount of time after the device locks before a passcode is required

Email

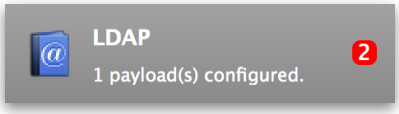
Email settings allow the systems administrator to predefine key SMTP or IMAP settings for users, such as host server, requirement to use only a defined server for sending mail, use of S/MIME, and SSL. This is one of the profiles that can be configured for parameterized profile settings if the client device is associated with an LDAP directory.

Exchange ActiveSync



Exchange ActiveSync is a payload that lets you predefine settings for users' access to MS Exchange services. The Exchange ActiveSync settings are supported for iOS, and the Exchange WebServices are supported for OS X. This payload supports parameterized profiles.

LDAP



The LDAP payload provides the ability to link the device to an LDAP server for lookup and configuration access. You can provide authentication for secure server access, or use just the hostname to gain anonymous access to the network directory. Some of the settings include: SSL usage and search criteria. This is not a binding profile since iOS devices cannot be bound to a network directory. For OS X devices, use the Directory payload for binding.

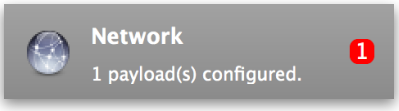
Contacts

The Contacts payload provides settings to allow access to CardDAV servers. This payload supports parameterized profiles.

CalDAV

The CalDAV payload provides settings for access to CalDAV (Calendar) servers. This payload supports parameterized profiles.

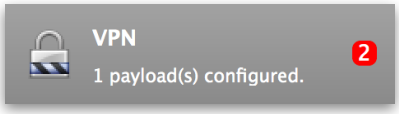
Network



The Network payload can be one of the most important payloads used for a profile. This payload allows you to preconfigure network settings for your devices, and use those settings as a key "carrot" in a 1:1 or BYOD deployment. As long as the user has this payload installed as part of a profile set, they have access to network services - and you have the ability to manage their device. If the user deletes the profile with this payload, they lose

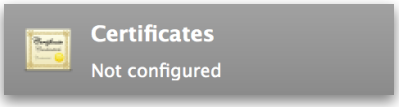
access to the network and its resources. You can define WiFi or Ethernet (OS X only) settings, including Auto Join, Proxy, WiFi Security and 802.1x.

VPN



Use the VPN payload to establish settings for a device to connect to a virtual private network. Settings include the user and machine authentication methods (including shared secret or certificate), proxy settings, and ability to force all network traffic through the VPN portal.

Certificates

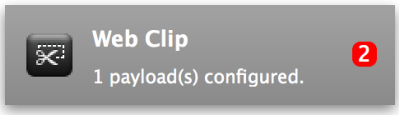


The Certificates payload lets you designate PKCS1 or PKCS12 certificate data to be stored on managed devices. You can specify institutional certificates or any other certificates required for access to your network services.

SCEP

The SCEP, or Simple Certificate Enrollment Protocol, payload is used to define the X.500 information needed by an institution for a connected device. You may also import a certificate to provide all the needed settings.

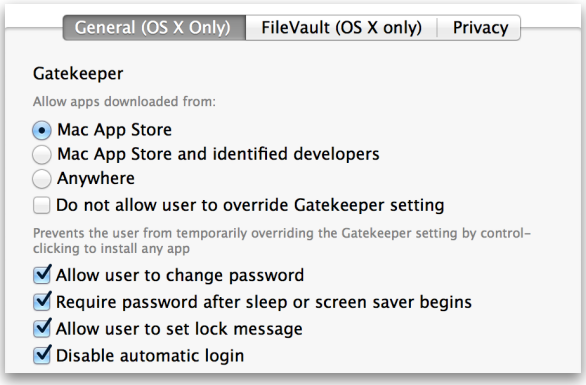
Web Clip

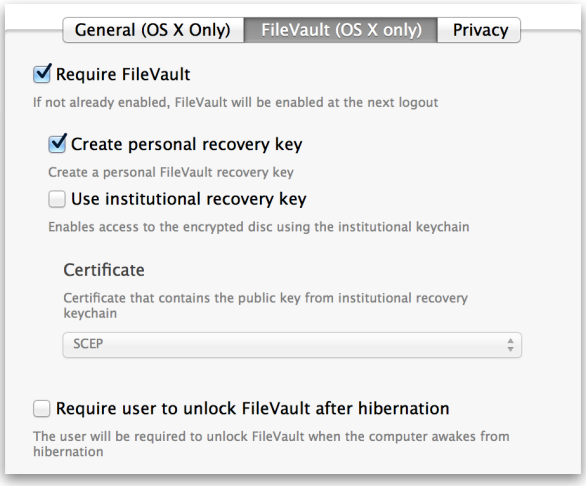


The Web Clip payload lets you assign URL's as 'miniApps' to a managed device. Settings include the URL for the clip, an icon for the item, and the ability to force the clip to open as a full screen application. The Web Clip is deployed as a regular application on iOS and as a Dock item on OS X.

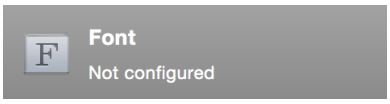
Security & Privacy

The Security & Privacy payload allows managed devices to be configured with access to specific sources for application downloads (OS X only Gatekeeper), force the use of Filevault (OS X only), and specify if diagnostic information is be sent to Apple or not. Here are views of the two main settings panes:





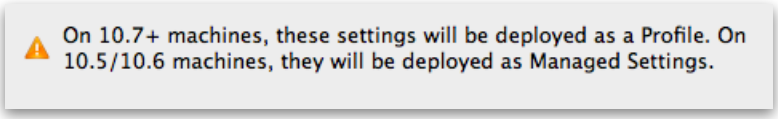
Font

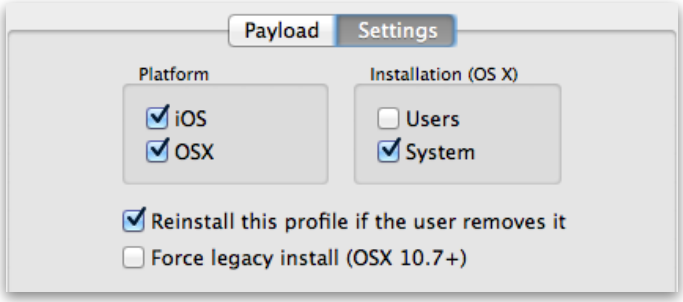


The Font payload allows you send a specific font set to a device. This capability is very handy for insuring and iOS device has the same font installed for a document that is also being worked on with an OS X device.

OS X only (10.5+)

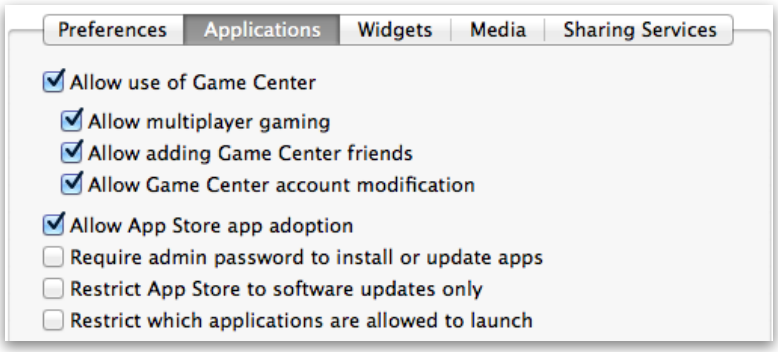
These settings are for OS X only. Settings applied to systems running OS X pre-Lion will be sent as Managed Client property lists (mcx.plists); settings sent to OS X 10.7+ will be sent as managed profiles. You have the option of selecting all settings to sent as Managed Client property lists (legacy install) in the Fileset Properties. **Note: In order to keep using mcx.plists, you must be using the 8.1.5 version of the FileWave client. Newer versions of the client do not convert profiles to mcx.plists.**

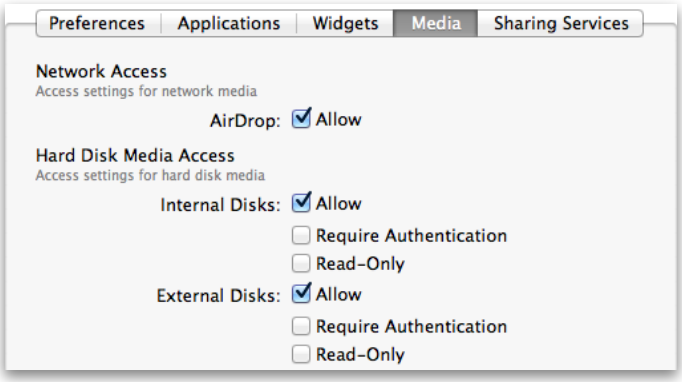




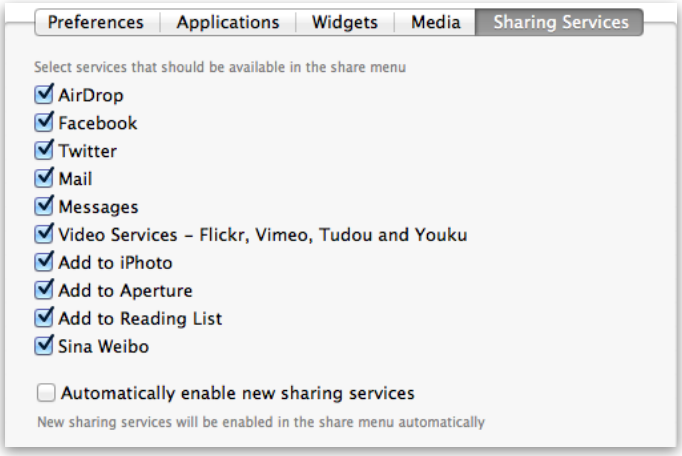
Restrictions

Restrictions payload contains settings to limit access to system preferences, applications, Widgets, media, and sharing services. For application control, the best practice is to designate the 'safe' paths for applications, such as /Applications; then designate restricted paths to 'unsafe' areas. Do not try to specify all 'allowed' applications because you will also have to locate all helper and sub-launched apps.

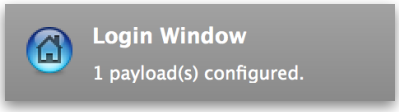




Some of the settings include control over AirDrop and App Store app adoption, Other settings include the ability to manage access to media, such as external drives, USB flash drives, and Game Center; plus the ability to manage access to shared services such as Twitter and Facebook.

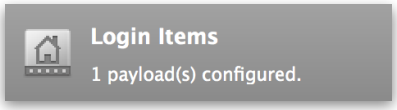


Login Window



The Login Window payload lets you configure the login window with a message, designate the type of login display (name/pwd or list), allow local administrators to bypass management, allow the Guest account, configure a login window screen saver, limit device access to certain groups, and imbed login/logout scripts.

Login Items



Login Items is a payload that can contain specified applications and sharepoints to be activated at user login. The designated items will launch or mount after the user logs in and the Finder launches.

Mobility

Mobility allows you to create mobile accounts - network user accounts with local home directories. Used in conjunction with the Login Window payload, you can specify support for the External account, which is a mobile account with an externally attached home directory. The idea is to have managed systems, bound to a network directory, where the user carries their home directory (USB/Tbolt drive) from device to device; but still logs in as a network directory account.

Dock

The Dock payload can be configured for shared devices that need to have a consistent look and feel regardless of user at the Finder level.

Printing

Printing payloads allow the assignment of network printers to managed devices, as well as the ability to force all print jobs to contain the identity of the managed device.

Parental Controls

Parental Controls were designed to support 1:1's where policies required content filters for managed devices when they were away from the managed network, as well as being able to set curfews and usage time limits for younger users. The payload is also very useful in open labs where the ability to deny non-administrator access to systems past a certain time of day is recommended.

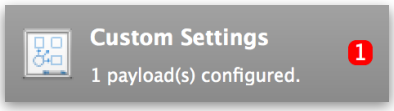
Finder

The Finder payload is designed to allow for limited access to external devices as well as hiding commands such as Shutdown or Go to Folder on common use / shared use systems.

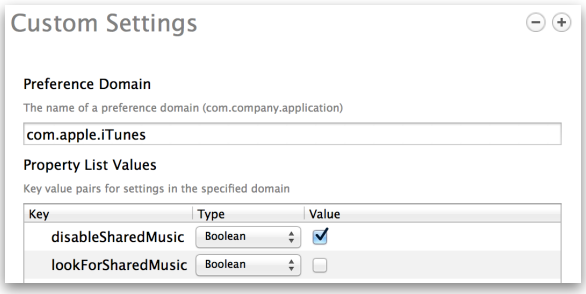
Universal Access

Universal Access payload settings are not just for special needs; but also contain settings for open labs and users who need additional services, such as zoom. Examples are having screens flash at alerts versus beeping in an open lab, or configuring a group of users' devices to support zoom with the trackpad.

Custom Settings



Custom Settings payloads allow you to greatly expand your ability to provide templates and special settings for managed devices. You configure the preferences for any application that supports property lists (plist files), upload that configured plist file, edit out the unneeded portions, and your managed systems will see that payload as a managed set of settings to follow. An example would be configuring iTunes to deny the use of both finding shared libraries and sharing any libraries. You set up the preferences in iTunes to turn off those settings, import your edited com.apple.itunes.plist, and edit out all the settings that don't apply. Here's an example of that:



Directory

The Directory payload allows you to configure **binding** to LDAP directories for your OS X systems. You can set up anonymous or authenticated bindings. If this payload is applied as a profile for newly imaged systems, along with a Network profile, your managed devices will boot as full network enabled devices.

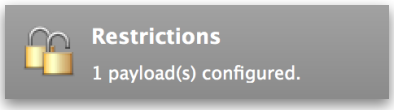
Energy Saver

Energy Saver payload settings allow the systems administrator the ability to preconfigure managed devices with the settings to optimize battery life in portables, as well as force desktop systems in a lab to sleep or wake when needed for online maintenance.

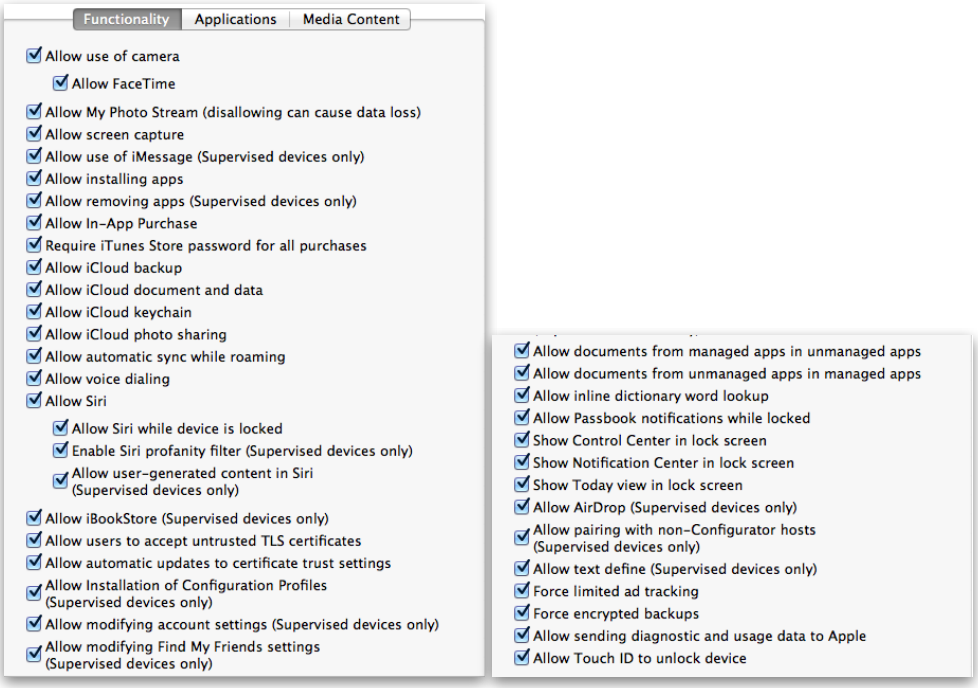
8.4.4. iOS (any) settings

These payloads apply to all supported iOS devices.

Restrictions



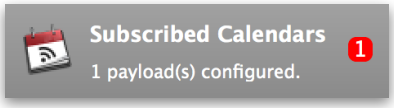
Restrictions allow the systems administrator to establish tight controls over institutional iOS devices, and could be used for managing BYOD/1:1 devices under certain deployment requirements, depending on the site. These settings include controlling access to the camera, Siri, iTunes, and iCloud. This payload also contains 'Manage open in' and GameCenter controls, as well as content management by age appropriate settings. Here are some of the settings:



Global HTTP Proxy

Global HTTP Proxy payload settings allow supervised iOS devices (see Apple Configurator info) to be linked to a master network proxy for web content.

Subscribed Calendars

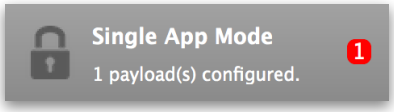


The Subscribed Calendars payload lets you provide predefined shared calendar information for your end users on managed devices. The settings work with parameterized profiles.

APN

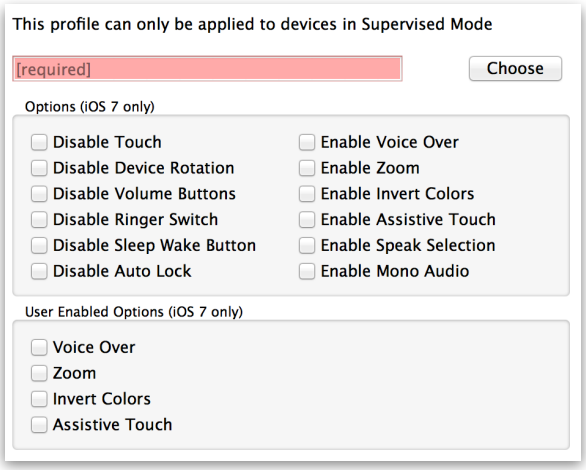
The APN payload allows systems administrators the ability to manage GPRS Access Point Name configuration for iOS devices with cellular services enabled.

Single App Mode



The Single App Mode payload is designed to allow you to configure supervised iOS devices so that they open into a single application. If a user turns the device off, when restarted, it will reopen into the designated app as long as the profile is active on the device. This payload is best used to in testing or kiosk environments. Setup requires the use of Apple Configurator to force the device into supervised mode. The payload also allow you to deactivate several other options, such as Auto Lock, Device Rotation, and Volume buttons.

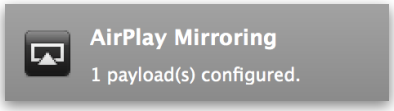
You select the app from the list of iOS apps added to Filesets. The iOS app Fileset must also be associated with the device in order for this process to work.



iOS 7+ settings

Payloads for iOS devices running iOSv7 and higher.

AirPlay Mirroring



AirPlay Mirroring payloads are for assignment of specific AirPlay devices to designated AppleTV's. A group of iOS devices can be assigned to a certain AppleTV with the password imbedded in the profile. Other devices would not be able to connect to that AppleTV. You can also provide a set of whitelisted AppleTV's that the managed device can use for AirPlay.

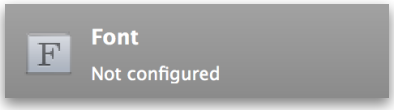
AirPrint

Use the AirPrint payload to designate AirPrint capable printers for managed iOS devices. The settings can be manually entered IP addresses or discoverable (Bonjour) devices.

Web Content Filter

The Web Content Filter payload supports whitelists and blacklists for web access, as well as setting a basic content filter looking to control access to adult content.

Font



Font payloads can contain unique font libraries that are needed by certain iOS devices. This is a good way to manage custom fonts purchased by an institution for use on defined devices only. It is also an excellent way to push fonts that need to be common across devices for better document appearance.

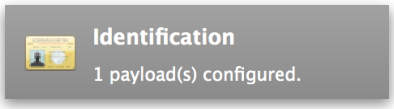
Single Sign-On

The Single Sign On (SSO) payload allows you to configure Kerberos access for your managed device to specific services and applications.

OS X (10.7+) settings

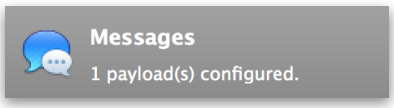
These settings are OS X running v10.7 (Lion) or higher only.

Identification



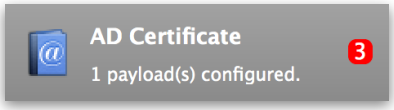
The Identification payload, using parameterized profile settings, can allow you to preconfigure user identity information for multiple service in OS X. You can define just a user's name, or nothing at all other than a prompt text that tells the user what to do the first time they log in. This information would then be saved for use in any service that can take advantage of Apple's Identity framework.

Messages



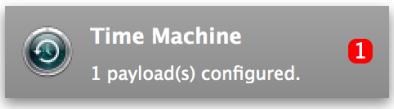
Messages allows you to preload the settings for user access to Jabber or AIM chat services. It can use parameterized profile settings for this payload.

AD Certificate



Configuring the AD Certificate payload lets you set up other payloads, such as VPN or Network, more easily. This payload provides the authentication data that will validate access to other services dependent on Active Directory certificates.

Time Machine

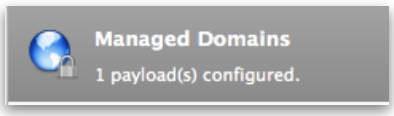


For environments using Time Machine servers or Time Capsules, this payload lets you set up the access information for backup of managed devices. In a group or departmental 1:1, this payload can alleviate some of the problems of getting users to take the time to configure their Macs for backup by doing it as a managed service.

iOS 8+

These settings are for iOS 8 or higher only.

Managed Domains



Managed domains can be set for mail and web sites. For mail, you specify “safe” email domains; e.g. filewave.com and any mail coming from, or being sent to another domain will be highlighted. On the web side, documents from approved domains will be considered as managed. This will allow a Web Clip from an approved domain to function while a PDF from an unapproved domain won’t be allowed to open in any managed application.

8.5. Parameterized profiles

FileWave allows you to use Directory based variables in your iOS profile payloads. You can insert the following options into your profiles based on LDAP information for a particular user:

%first_name%	%last_name%	%full_name%	%short_name%
%email%	%job_title%	%mobile_phone%	%guid%

You can reference specific information about the device as well, directly from FileWave Inventory. Those fields are:

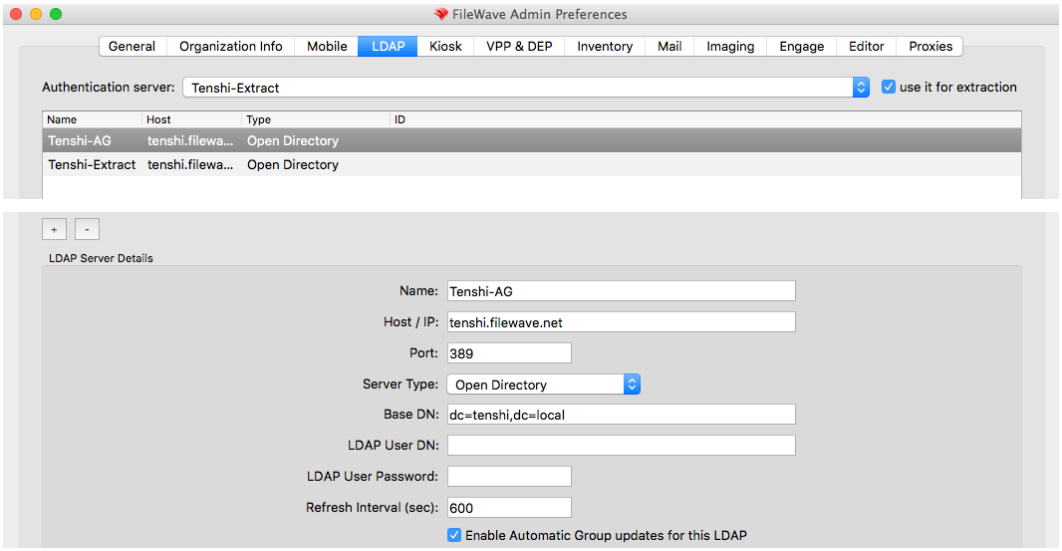
%OSVersion%	%SerialNumber%	%ProductName%	%BuildVersion%
%WIFIMAC%	%ICCID%	%IMEI%	

Setting Up LDAP for parameterized profiles

Setting up a directory server for use with Parameterized Profiles is easy. Navigate to the FileWave Preferences Screen and fill out the appropriate information for your OpenDirectory, Active Directory or E-Directory LDAP server. For issues and troubleshooting related to your LDAP preferences, please refer to section **3** of this manual.

You must also be using LDAP authentication for iOS device enrollment. Instructions for that setup are in the MDM portion of this manual. To add LDAP parameters to your profiles, simple replace the normal value with one from the list above.

Note: The directory that you create for pulling Profile variables should ONLY be used for that task. If you are using the same Directory Server for LDAP Smart Groups, you should create a duplicate entry in FileWave. One entry for LDAP smart groups and one for Parameterized Profiles (extraction).


FileWave Admin Preferences
General
Organization Info
Mobile
LDAP
Kiosk
VPP & DEP
Inventory
Mail
Imaging
Engage
Editor
Proxies
Authentication server:
Tenshi-Extract
use it for extraction
Name
Host
Type
ID
Tenshi-AG
tenshi.filewa...
Open Directory
Tenshi-Extract
tenshi.filewa...
Open Directory
+
-
LDAP Server Details
Name:
Tenshi-AG
Host / IP:
tenshi.filewave.net
Port:
389
Server Type:
Open Directory
Base DN:
dc=tenshi,dc=local
LDAP User DN:
LDAP User Password:
Refresh Interval (sec):
600
Enable Automatic Group updates for this LDAP

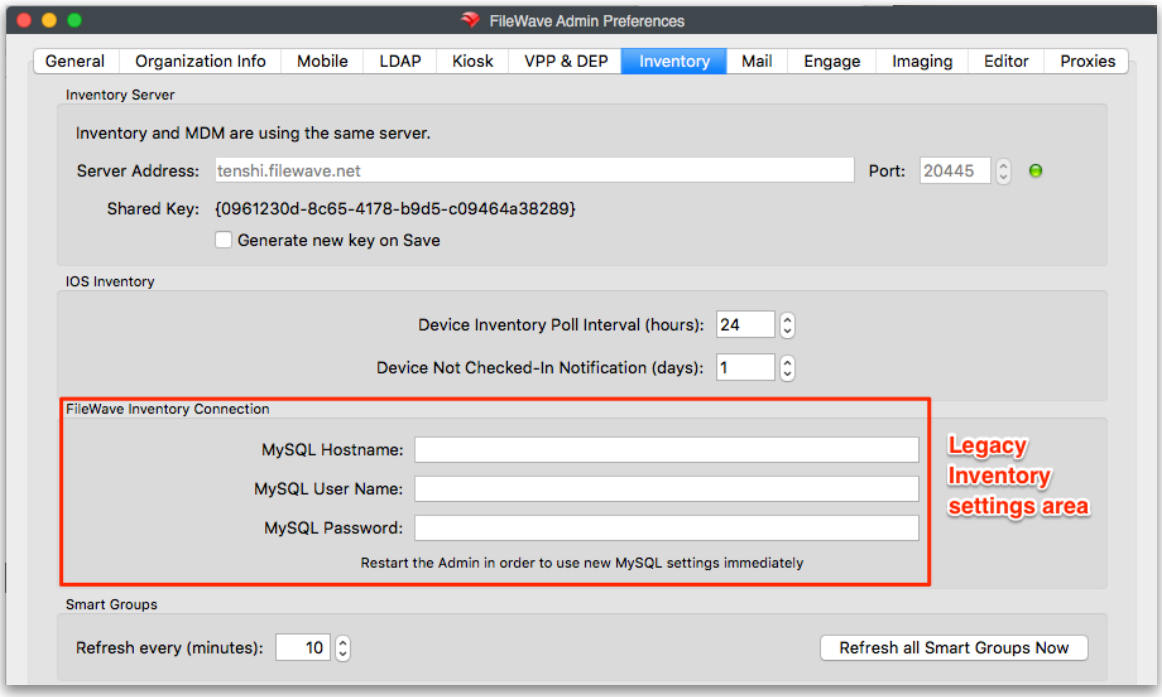
9. Working with Inventory and iOS Inventory

Integrated Inventory is a big part of the power of FileWave. The SQL database on a FileWave server can handle millions of data points, and scales into the 10's of thousands of clients. You can build simple or detailed custom queries based on both hardware and software information, obtain information about software titles in use, and generate automatic reports on a query to be sent to requestors on a schedule. With the ability to create your own datasets using custom fields, you can track more than just your devices - you can track peripherals, assignments, locations - it's entirely up to you. In FileWave, iOS devices have their own unique Inventory area. While the iOS devices show up in the Clients pane, as well as in the common Inventory query areas, they have a custom area to display great details about the devices.

The strongest feature of FileWave Inventory is the ability to use the customized queries you build as the core components of Smart Groups. You can build your deployment workflows around criteria that assigns clones of client devices to a group based on detailed Inventory searches. This dynamic assignment will be associated with specific Filesets tailored to meet the needs of that group. As a device absorbs the contents of those Filesets, the characteristics of that device change, resulting in it meeting the criteria of, and switching to, a completely different group - all based on custom Inventory queries.

9.1. Configuring Inventory preferences

With version 6 and higher, FileWave integrated Inventory into the main FileWave server. With version 8, FileWave introduced Smart Groups with Inventory queries. Due to this evolution, the legacy FileWave Inventory product - formerly Asset Trustee - is End of Life (EOL). The Inventory preferences now consist of a legacy connection to the EOL'd Inventory plus basic settings:



iOS Inventory

These settings only apply to the iOS Inventory section of FileWave. iOS devices show up in the normal Clients section of FileWave Admin as well as in the iOS Inventory section.

- *Device Inventory Poll Interval* - Default is 24hrs. This setting is how often all iOS devices will report their profiles, application, security and device settings unless a **Verify** command is sent.

- *Device Not Checked-In Notification* - When an iOS device exceeds the timeframe set, the device color changes to alert the administrator that that device has not checked in with the MDM server.

FileWave Inventory Connection

If you are using the legacy Inventory server, you would enter the required hostname, username and password to allow the FileWave server to communicate with the Inventory server. These settings are not required for using the built-in Inventory.

Authenticate with Inventory Server

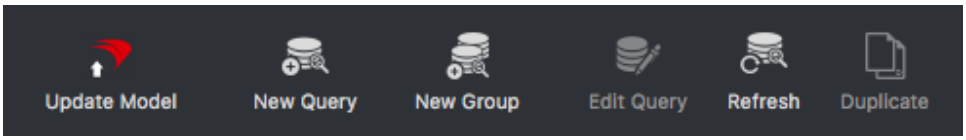
This checkbox is only selected if you are using a separate MDM server and your Inventory server is on this system.

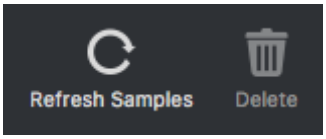
Smart Groups

The button **Refresh all Smart Groups** forces a refresh of all the data requested by existing Smart Groups.

9.2. Inventory Toolbar

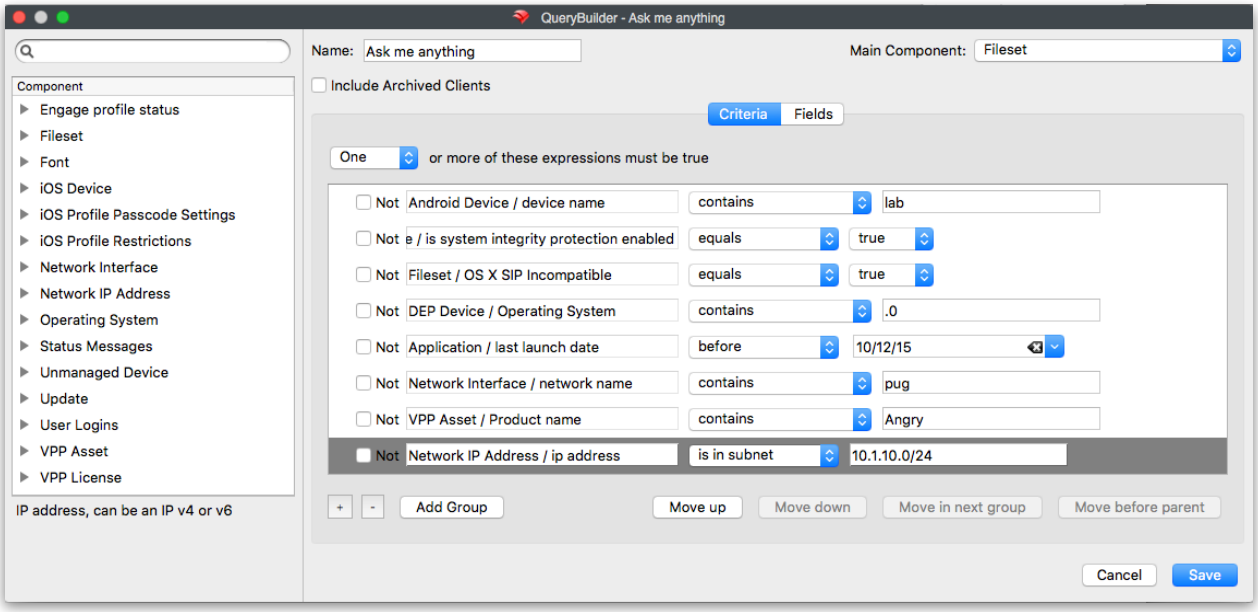
The Inventory toolbar consists of six simple tools plus the Delete item:



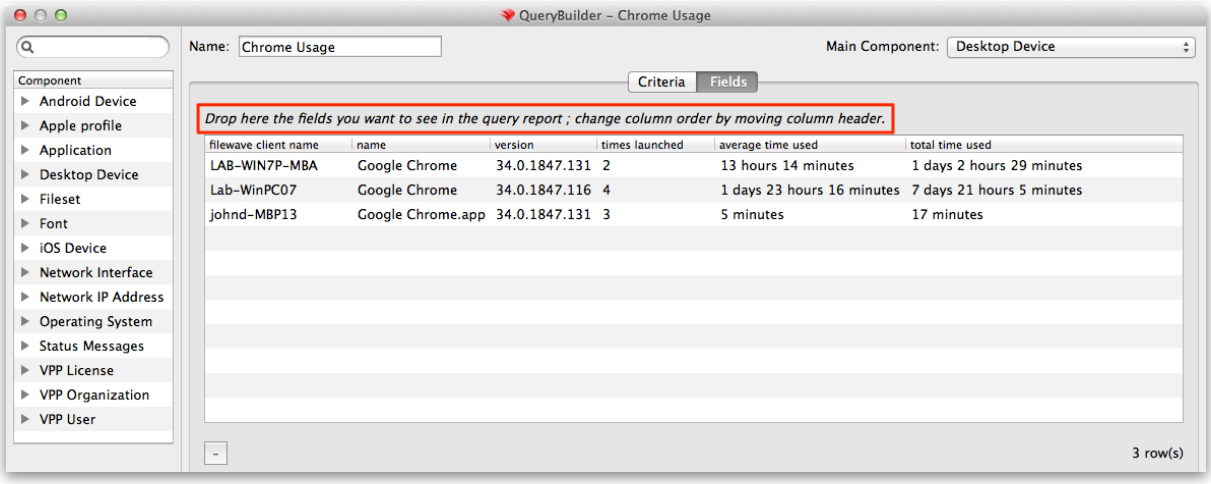


- *New Query* - create a new blank query
- *New Group* - create a new query group to contain queries specific to any criteria you choose, such as “Browsers”
- *Edit Query* - opens the designated query for alteration
- *Refresh* - forces a rescan of the Inventory database to reload the data for that query
- *Duplicate* - creates an identical copy of a query so you can edit a copy and not the original
- *Refresh Samples* - restores the default sample set we provide to their original state

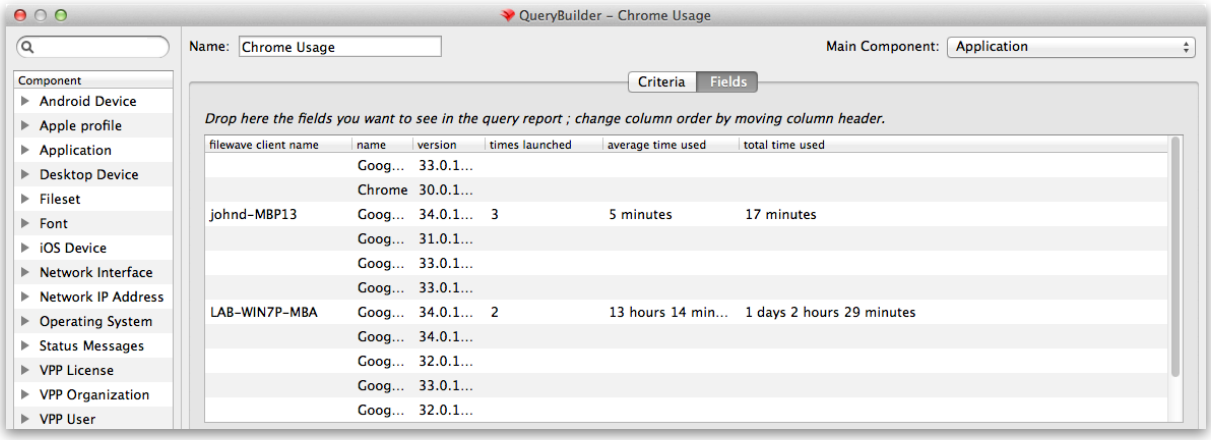
9.3. Creating and Editing a query



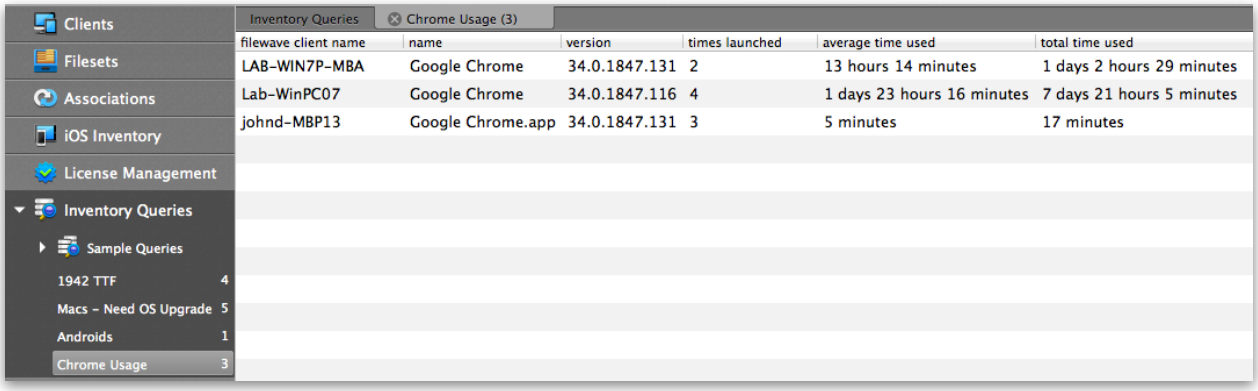
When you create a new query, you start by giving it a name and choosing a starting criteria - in this case, we want to have all of our clients report back if they have an application containing the name “chrome”. Next, we decide what fields will be displayed when the query executes.



As you drag and drop component fields into the display window, FileWave immediately begins filling in the blanks with data from your clients. You can re-order those fields by dragging them back and forth until you are satisfied with the results. You will also want to choose a **Main Component** which is the index field for the query. For example, in this query, if the main component was the *application*, then you would get a report that showed every instance of “chrome” that existed in the database. The results would display every instance of the Chrome application, even if it was stored away from the Applications folder and not being used.

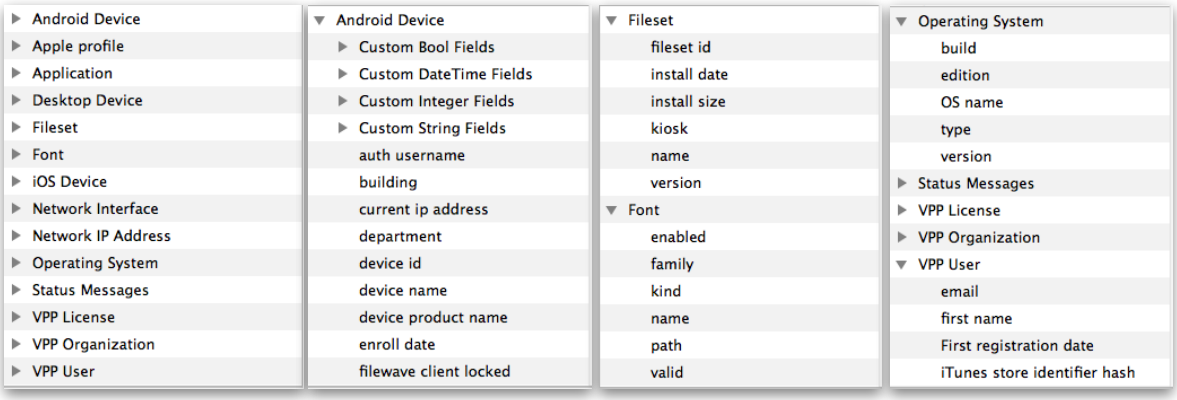


By choosing the correct component, and the right criteria, you can create queries that will tell you exactly what you want to know. In the main Inventory window, you can select your query so that it will display just by clicking on it.



Components

Key to being able to create a useful query is understanding the components you have access to. Here is a sampling of those items:



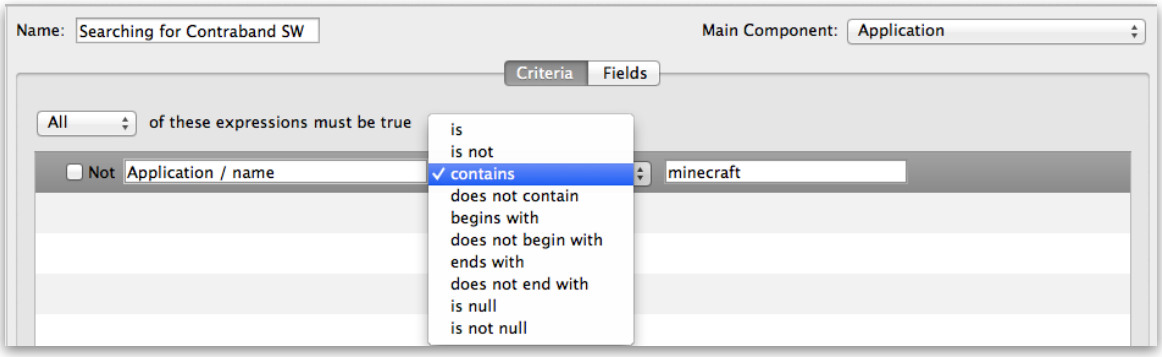
One of the most important new component types is the custom field. There are four different sets - *Boolean, DateTime, Integer, and String*. You can create custom fields to go beyond the basic information provided by the clients to look for unique combinations that include searching for files created prior to a certain date, or add marker files to clients that include a filename or text that meets custom criteria. Instructions on how to create and use the custom fields is posted on the FileWave Support site: https://www.filewave.com/item/add-filewave-custom-inventory-fields-remotely-using-a-fileset?category_id=98

Expressions

When building a query, you all be confronted with an array of logical expressions needed to create that query. While it is way beyond the scope of this manual to educate you on logic, we can provide you with some basic examples to get you started.

When you add an expression, the logic generally revolves around “is this thing true or not?” What you actually get to work with is a list of possibilities, such as “this is exactly what I am asking for”, “this contains the thing I am asking for somewhere in the field I am looking”, “this begins/ends with the thing I am looking for”, or the all time favorite “is null” - which means the field I am looking at has no value set at all. Of course, you also have the opposite of all these with *not - is not, does not, etc.*

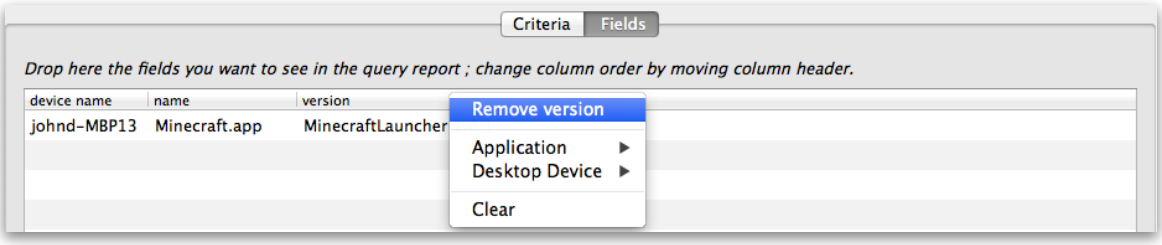
In our example, we are looking for any instance of an application where the name contains the text “minecraft” -



Field values

The whole purpose behind the query is to get useful information out of the exercise. You do this by adding fields to display the results of answers to your criteria. In Inventory, you access the same components you use as criteria for the search as the display fields. In our example, we are looking for “minecraft” but if we left it at that, all we would get back from the FileWave database is “yup, I found it. Now what?”

Here’s the result without us asking for a more detailed result. This is the database telling us that it found “minecraft” with no clue as to where it is on any of the clients. So now, we are going to clean up the view and add the component “device name” so that our query will tell us what device this is on.



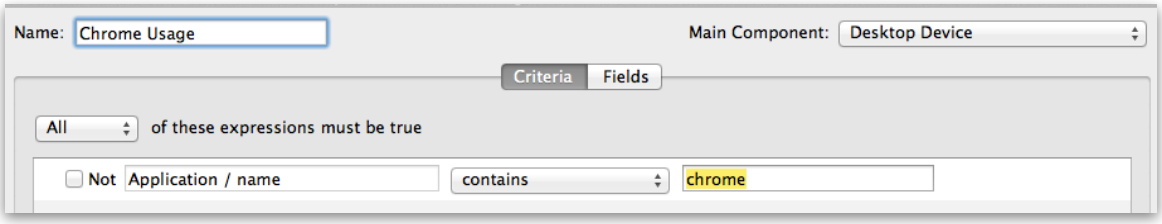
Now that we have added the *device name* to the query fields, we can see that “Minecraft.app” is sitting on the systems administrator’s machine, so there is no cause to be concerned. Move along, nothing to see here…

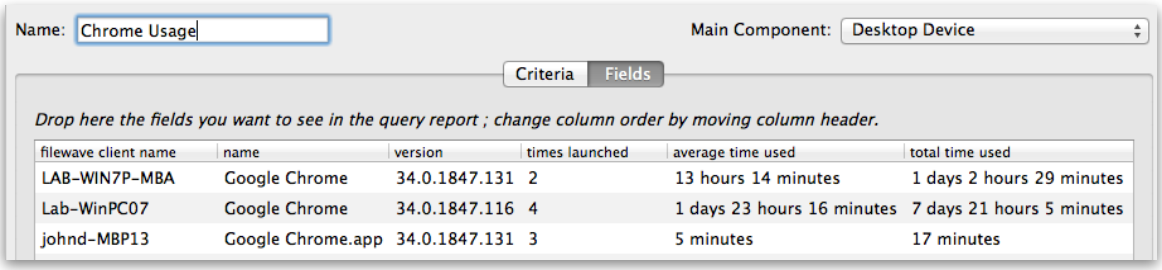
You can see how a simple query can be constructed, and that it can prove quite useful to just look for some simple answers. Next, we are going to look at some more powerful examples of queries that you can put to use.

Example - Tracking application usage

Another powerful tool in the License Management kit is the ability to track application usage. You can create queries that display the amount of time any managed device is using any installed application. An easy example here would be to look at who is using a specific browser and how often.

The query is built based on locating an application - in this case, Google’s Chrome web browser. However, instead of just locating the application as we did in the first example, we are going to find out how often that item gets used. FileWave provides application usage components for this purpose. Here’s the query with its display fields:

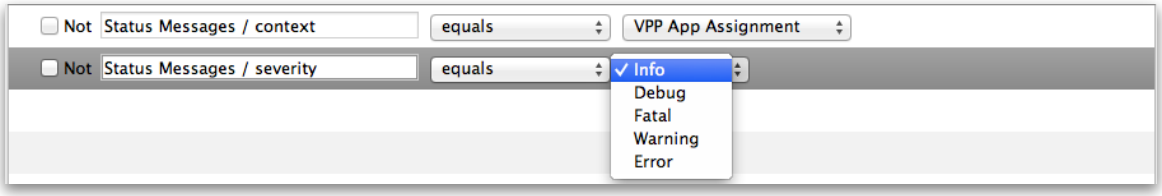




You can see that adding the proper fields, as well as choosing the proper index or Main Component for the display, you are gleaning a good bit of information from this query. An interesting add-on to this would be to look up the usage patterns for every browser installed.

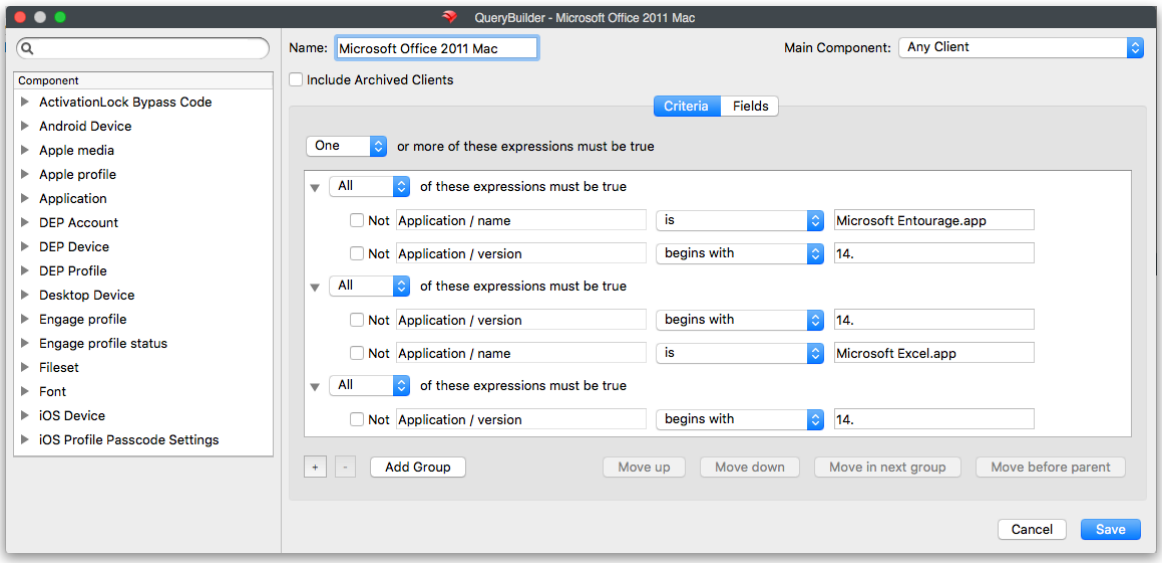
Example - Monitoring device status

In FileWave, devices send back status reports all the time to the server. As FileWave administrator, you can view these reports from within the **Client Info** pane, one at a time. Using the *Status Messages* components, you can create queries that will display all of the messages from your clients simultaneously.



9.4. Using the Sample Queries

In order to get you started using Inventory queries in FileWave, we have provided a set of extensive, and sometimes complex, pre-built queries for your use. You can duplicate any of them to use for your own, or use them as they are. These queries are a great example of the level of detail you can use to build a responsive Inventory system.



9.5. Creating Query Groups

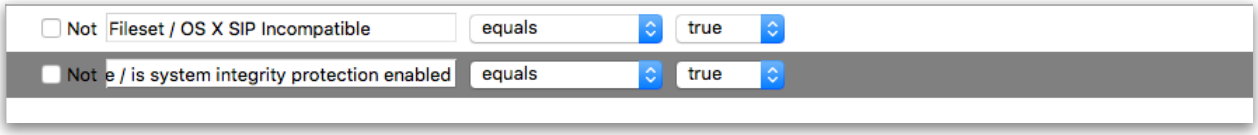
The idea behind *Query Groups* is that you might need to isolate queries into families of devices, operating systems, applications, or even based on results. Groups such as iOS Devices, Denver Office, Campus ConfRms, etc. would all make sensible Inventory groups. Just create the group, name it, and drag the appropriate queries into it.

9.6. Using queries to create Smart Groups

Outside of creating queries for informational purposes, FileWave can help you create powerful, dynamic Smart Groups. The concept behind a smart group is to gather clients together who meet a certain set of criteria. That would be, for example, all of the devices residing on a certain IP subnet. By adding Inventory queries to the criteria, then adding Filesets to the group, you can create a smart group that will gather a client device due to its meeting specified criteria, perform Fileset actions on that device, and as a result, the client no longer meets the criteria and drops out of the group.

Locating Filesets that contain *SIP* violations

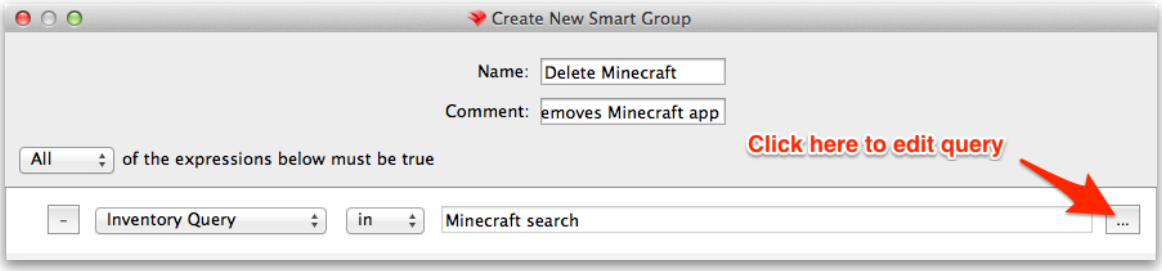
Apple has released a new security policy with OS X v10.11 called **System Integrity Protection**. In a nutshell, it says that no process will be able to have write access to any area of the OS that is protected. FileWave administrators may have scripts that violate this policy, and need to find out instead of just seeing their Fileset fail. There are two new fields in Inventory that identify whether or not a Mac has SIP active or not, and another field that identifies files that contain code that would violate the SIP rules. Here are the two query items:

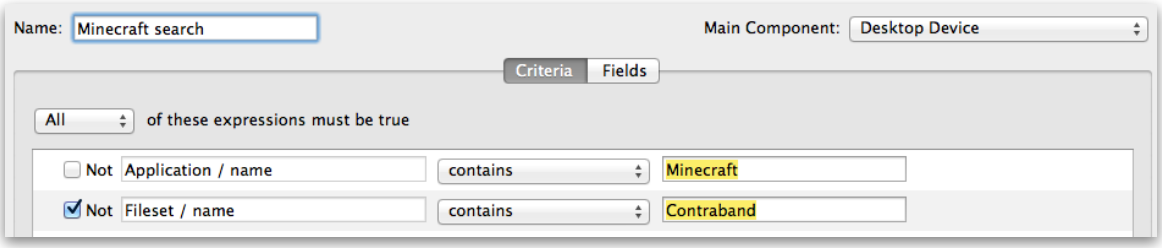


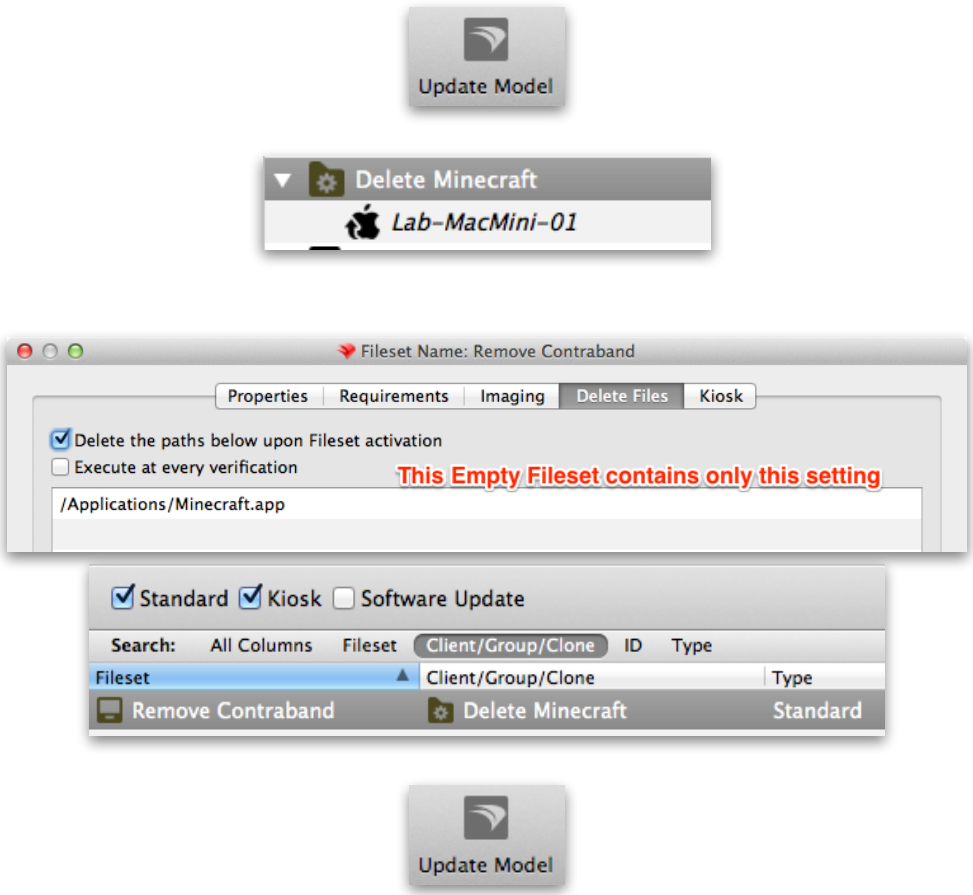
Removing contraband software

For example, you need to scan your clients for contraband software. If the client meets the criteria of having the software you are looking for, then you will have a Fileset execute that will remove that software. Since the group is dynamic, as soon as the device responds that it no longer has the software and it has that Fileset installed, it will no longer qualify for that group, and will drop out.

Here is the workflow for setting this up:



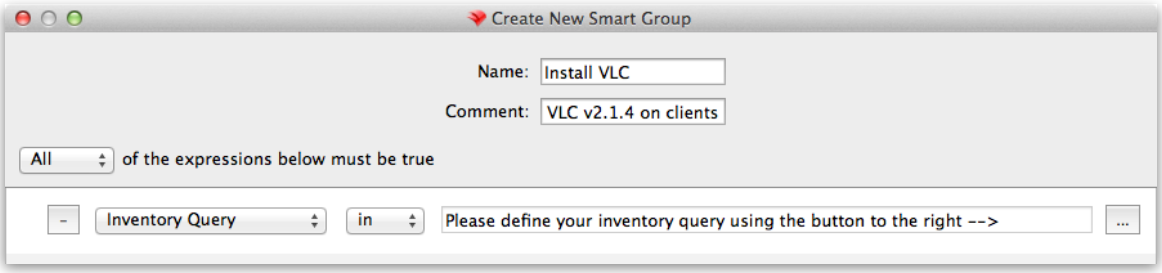


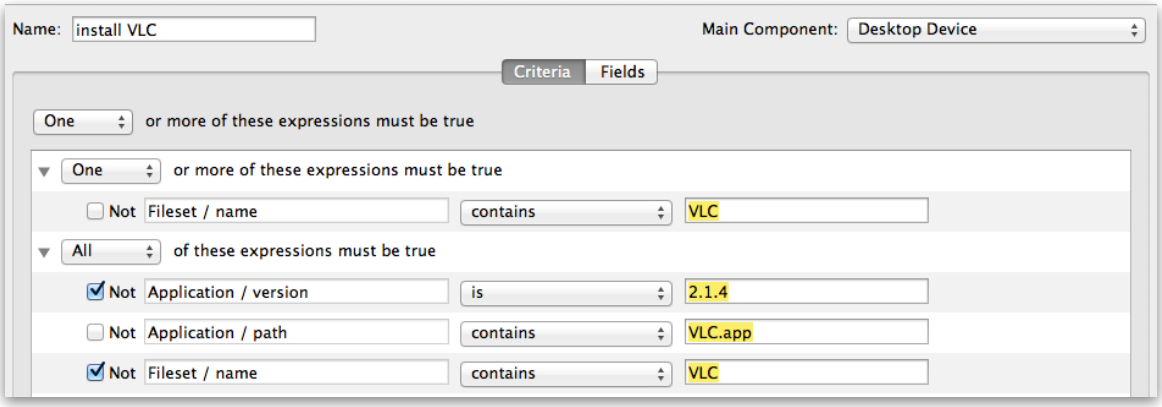


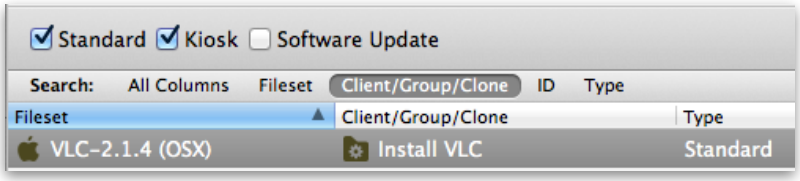
Once you have executed the **Update Model** command, the Fileset will execute and delete the software. It will re-check every 30 mins for the criteria, just to make sure.

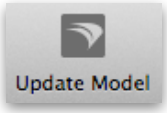
Example - Installing VLC

This Smart Group is designed to look for clients who do not have VLC version 2.1.4 and install it. Once the software is installed, then the device will no longer meet the criteria and will be dropped from the group. The qualifiers for inclusion are that the right version of VLC is not present and that it does not have the VLC Fileset associated. The criteria for exclusion is that the VLC Fileset is present. Both of those expressions must be evaluated. If the existence of the VLC Fileset was not verified, then the Smart Group would just keep pushing the VLC Fileset every 30 minutes. Here's the workflow:





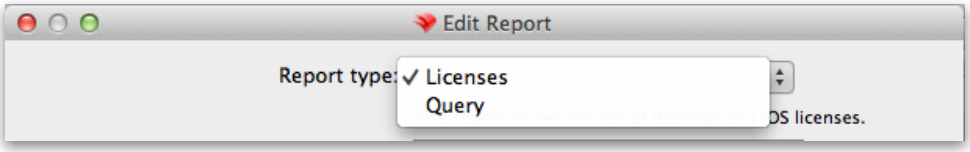




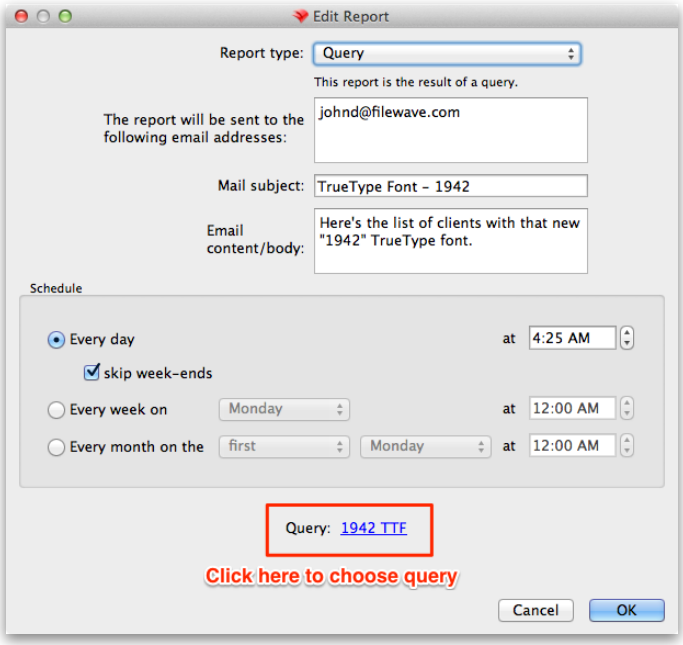
9.7. Generating scheduled reports

Being able to look at the various queries while online as the FileWave Admin is one thing. Being able to have the results of a query automatically sent to your email inbox at the same time every week is much better. FileWave supports creating schedules reports from queries, and the process is very simple.

First, you select **/Assistants/Scheduled Reports…** from the FileWave Admin menubar. Then click on the [+] button in the lower left of the window to create a new report.



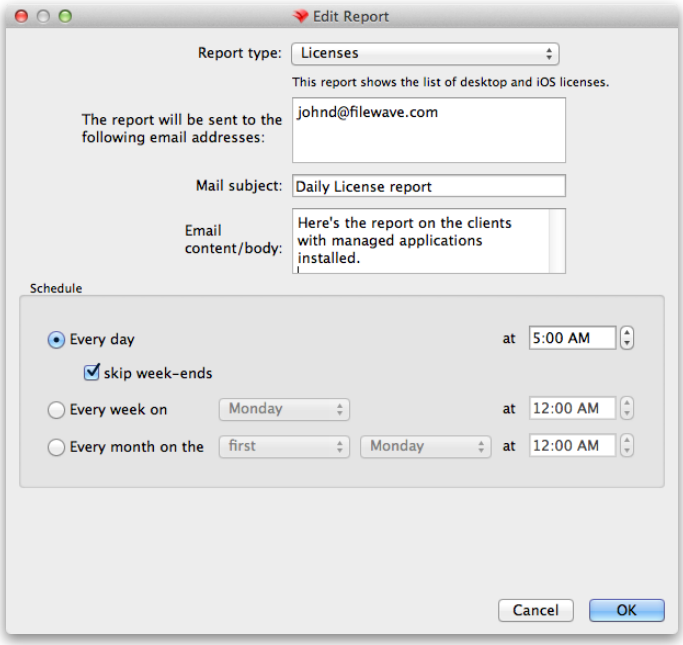
You can choose between a Licenses report or a Query report. We will look at the output of both types; but we'll start with the Query report.



The output is in **tab-delimited** format:

```
device name   name         family              path
home          1942.ttf     1942 report         /Volumes/Server HD2/1942.ttf
johnd-MBP13   1942.ttf     1942 report         /Library/Fonts/1942.ttf
johnd-MBP13   1942.ttf     1942 report         /Users/johnd/Demo Content/1942.ttf
LAB-WINPC07   1942.ttf     1942 report (TrueType)
```

The License report is generated the same way, except you choose a license definition from **License Management** for the input.

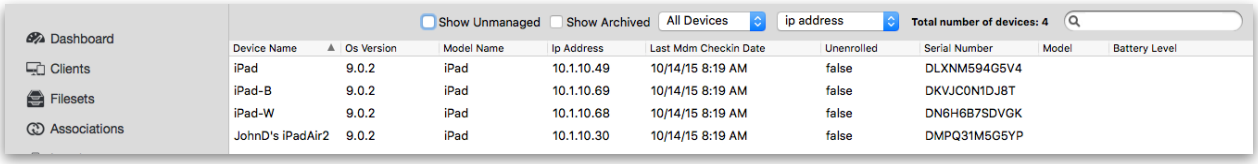


The output is in **tab-delimited** format and includes all managed license information.

License Name	Installed	Owned	Compliance Status	Platform	Organization
Comic Sans	8	2	License out of Compliance	Desktop	None
Big Calculator Free	1	3	Warning License Watermark	iOS	Primary VPP acct
Astronomy Picture of the Day	1	20	License Compliant	iOS	Primary VPP acct
Beta SW Test	0	3	License Compliant	Desktop	None
Chrome Browser	4	10	License Compliant	Desktop	None
Draw Something Free	0	10	License Compliant	iOS	Primary VPP acct
Evernote (OSX)	0	2	License Compliant	OSX	Primary VPP acct
Evernote (iOS)	0	20	License Compliant	iOS	Primary VPP acct
Font-1942	3	21	License Compliant	Desktop	None
Fragment	0	5	License Compliant	iOS	Primary VPP acct
GeoGebra	0	5	License Compliant	OSX	Primary VPP acct
Grimm's Fairy Tales	2	50	License Compliant	Book	Primary VPP acct
Lumosity	0	5	License Compliant	iOS	Primary VPP acct
Merriam-Webster's dictionaries	0	5	License Compliant	OSX	Primary VPP acct
Office 2012	0	100	License Compliant	Desktop	None
Skitch - Snap. Mark up. Share.	0	3	License Compliant	OSX	Primary VPP acct
Solar Walk - 3D Solar System model	0	2	License Compliant	OSX	Primary VPP acct
Tayasui Sketches	0	20	License Compliant	iOS	Primary VPP acct
TextWrangler	0	15	License Compliant	OSX	Primary VPP acct
United States Constitution	3	30	License Compliant	Book	Primary VPP acct
YouTube	0	3	License Compliant	iOS	Primary VPP acct
iBooks (iOS)	1	50	License Compliant	iOS	Primary VPP acct
iBooks Author	0	10	License Compliant	OSX	Primary VPP acct
iTranslate Voice - translator & dictionary	0	2	License Compliant	iOS	Primary VPP acct

9.8. Working with iOS Inventory

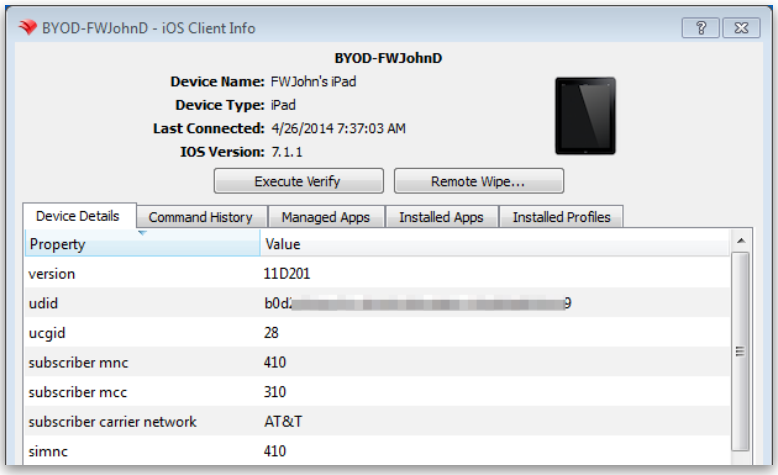
The **iOS Inventory** pane exists for you to have instant access to the attributes of your iOS devices. Unlike the normal **Inventory** pane, the iOS Inventory behaves more like a dashboard view of your iOS devices.



The iOS Inventory view is a read-only list of attributes for enrolled iOS devices. Each enrolled device automatically appears in this list which provides details retrieved about the device. The three toolbar items you use in this pane are the **Device Info**, **Refresh**, and **Customize Columns**.

Device Info

This window is identical to the one you see when you select **Client Info** in the **Clients** pane. The **Execute Verify** button forces the device to refresh all of its information with your FileWave server. The **Remote Wipe…** button allows the FileWave super administrator to remotely reset the iOS device, erasing all settings and content.



The window also provides all of the key details about your iOS device:

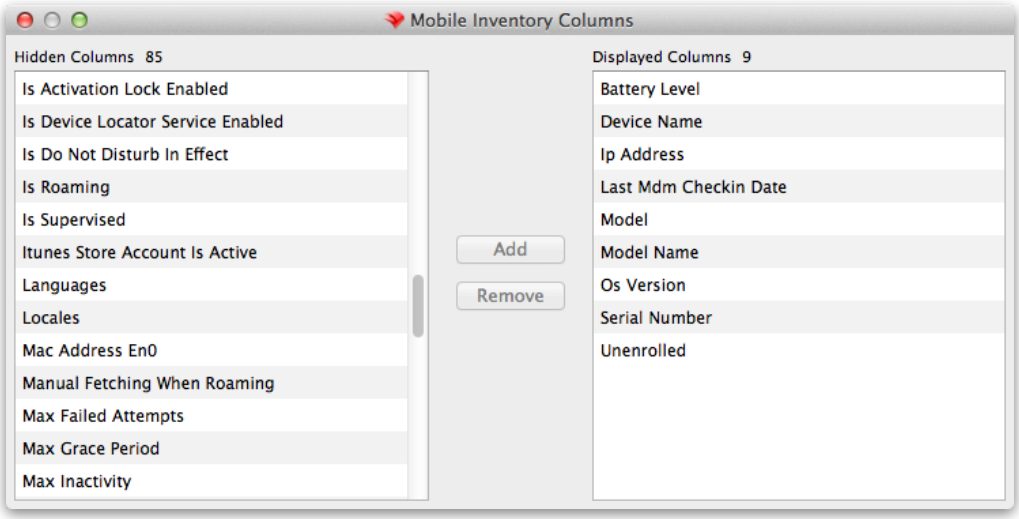
- *Device Details* - this view displays technical information on the device to include UDID, serial number, profile settings, and enrollment info
- *Command History* - displays the commands sent from FileWave server to the device with actions and results
- *Managed Apps* - the view shows the applications sent from FileWave as Filesets
- *Installed Apps* - this view displays all applications, other than the built-in one, that were not sent by FileWave. Will include applications installed by the user.
- *Installed Profiles* - the view displays the profiles on the device from the the FileWave MDM server

Refresh

This toolbar command forces the devices listed to be refreshed from information on the FileWave server. The display window does not dynamically refresh. If the iOS database is very large, the refresh could take a long time.

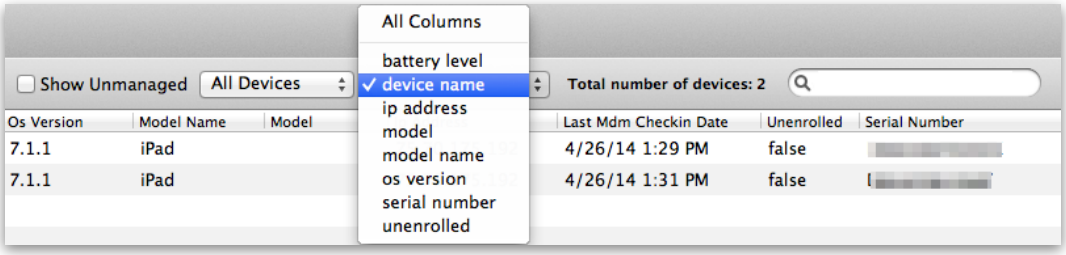
Customize Columns

You can edit the display of your iOS devices by customizing the column view in the main window.



Searching and managing window contents

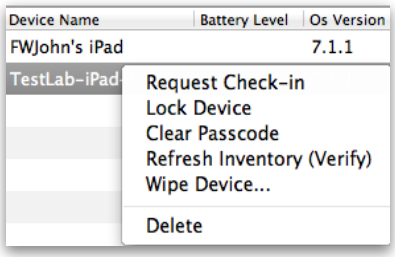
The main window can also be managed to view a restricted set of iOS devices depending on the specific devices you are looking for.



You can select to see only iPads, iPods, or iPhones, and search for devices using the column data you have displayed. If you choose to see **Unmanaged** devices, it will show iOS devices you have added as clients that have not enrolled. These would be devices you added from a text file in bulk while preparing for a large roll out.

Extra controls - pop-ups

The pop-up menu from right-clicking a device itself gives you a subset of the controls you see in the Clients pane. These include the ability to clear the passcode and lock the device remotely, which activates the screen lock.

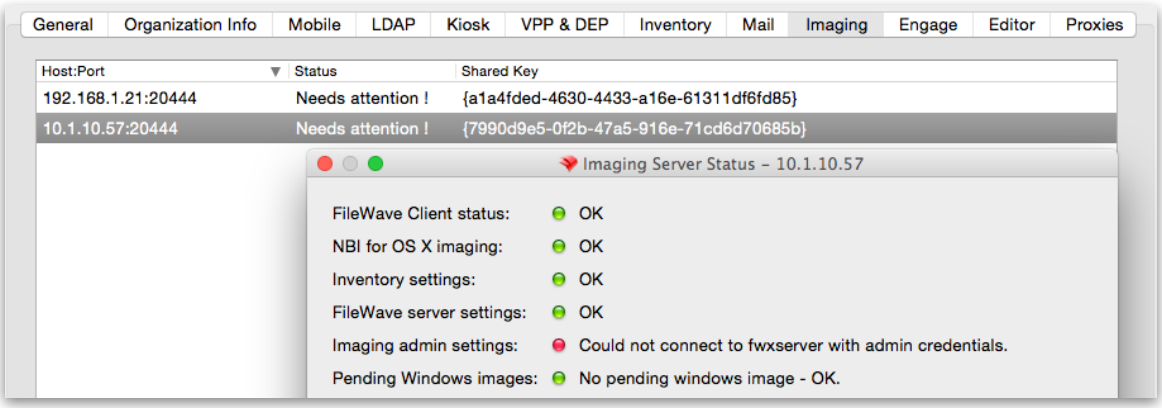


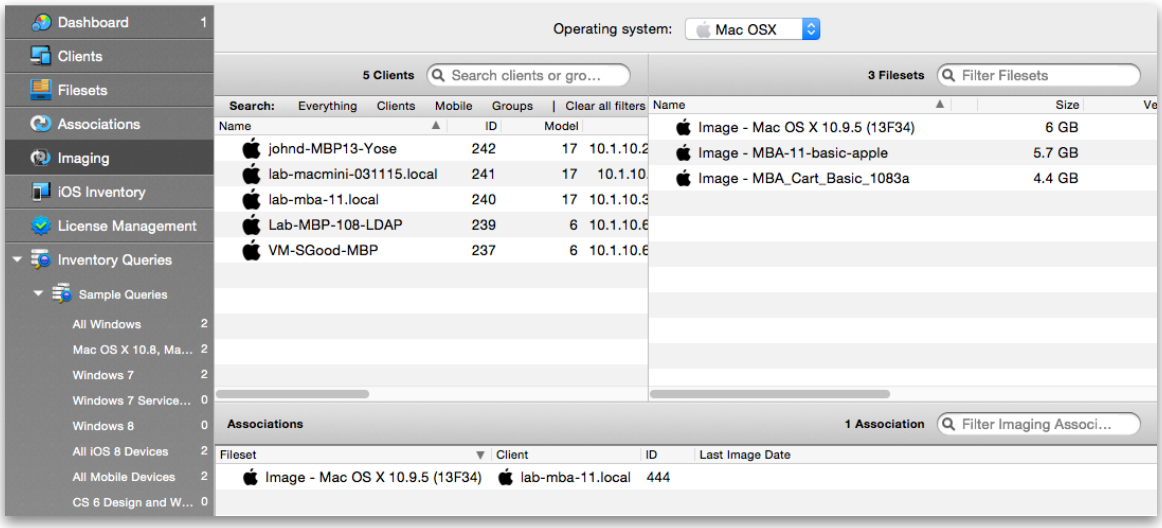
10. Imaging with FileWave

FileWave supports direct imaging for OS X systems using the **Lightning** application. This method works over Firewire and Thunderbolt. Network imaging is supported over Ethernet using the FileWave **Imaging Virtual Server.** It uses the **PXEboot** system for Windows devices and **NetBoot** for OS X devices. In section **3** of this guide, you saw how to install the Imaging Server (IVS). This section will go into the process for setting up images and associating those images with a client system.

Under version 9 of FileWave, the imaging process has been greatly improved. A new client process (imaging-fwcld) is running on the IVS, reporting back in to the FileWave server and Admin. Images are now Filesets and can be presented directly to a client from the server - or though a Booster. The imaging configuration is completely integrated into the FileWave Admin.

While in earlier versions of the IVS, you had to worry about IP routing and network traffic due to your NetBoot/ PXEboot server being on a different network from your clients, IVSv3 in FileWave v9 supports multiple imaging servers across several subnets as desired. You can set up an IVS in the IT shop for testing and another in the building where the devices will be imaged. Both of these servers will be managed from FileWave Admin at the same time.





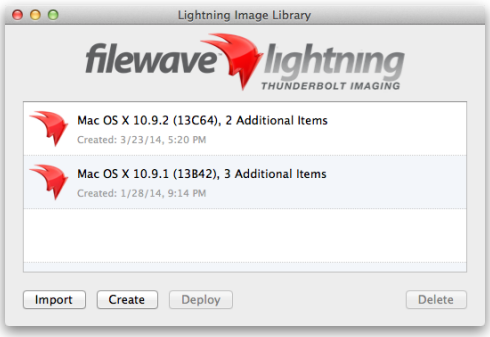
The biggest change with FileWave v9 is that image sets are now Filesets. Images are dragged into the Filesets window, then associated with devices. This removes a great deal of the complexity that used to exist before FWv9.

Since the images are Filesets, that means they will distribute through Boosters. This process will get a much deeper workflow description in an update to this manual.

10.1. OS X local Imaging - Lightning

The focus for local imaging is the FileWave Lightning application. Lightning was designed to help you create and deploy two basic types of images:

- *Known good device* - this is an image made from an OS X system with all of the settings and configurations complete and functional. An example of this would be building a lab or cart of Macs that need to be exactly the same; so you would create the first system with the local administrator account, all the applications, and configure it as needed. You then capture that Mac as an image and bring it into Lightning for deployment.
- *Clean device* - this is a Mac built from the ground up using the OS X installer, new settings, and applications. Since the Mac has never actually been booted, the result can be a system that has most of its contents; but has not gone through the setup assistant. This is the most flexible type of image master.



One variation on these types is the baseline image - you build a system so that it contains only the absolute bare minimum of content. This could be a known good device with nothing but the FileWave client and a WiFi profile configured on it, and the setup assistant running at first boot. This Mac would be the perfect candidate for a 1:1 deployment. The end user signs for the Mac, boots it, runs the setup assistant and once they are up and running, FileWave checks the device characteristics and provides Filesets as needed.

Imaging preparation - OS X

You can download the Lightning application from the FileWave support site. Prior to first launch, you should gather the items you are going to use to build your images. If you are already using other tools such as DeployStudio, you can collect the images you have created for inclusion into Lightning.

Basic tools and supplies

You will need access to Disk Utility, the latest OS X installer, applications you wish to install (must be either in **.pkg** installer format or **.app** format), and sufficient storage space for the images. If you are going to be using known good devices, then you will need those systems within Firewire or Thunderbolt cable range of your mastering system.

OS X dependencies

If you plan on imaging Macs with older version of OS X, you will need a mastering system that can run that version of the OS. For example, if you are planning on imaging some OS X Lion (10.7) machines, you will need to be on a Mac that can download the Lion installer from the Mac App Store. If you are running a Mac that has been upgraded several times over the past few years, you may find that you can download and install several versions of OS X onto that machine. Be careful - you should work from a clean system, if at all possible. Downgrading and upgrading your own production Mac is not a good idea - use a lab system that you can erase without data loss.

Setting up Lightning

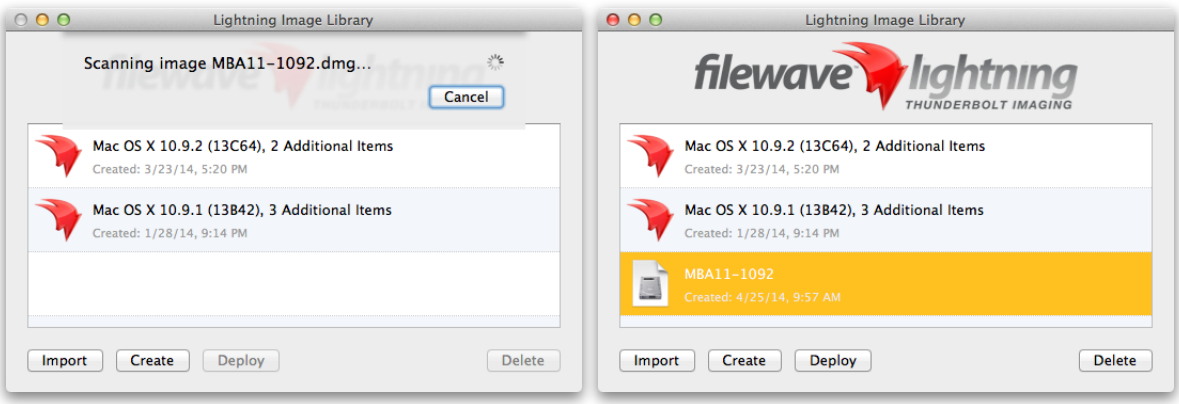
Once you have gathered your supplies and downloaded Lightning, you can begin the image creation. If you are going to be using a known good device (KGD), then you must follow these steps in Disk Utility (or complete the same actions using another disk tool):

- Boot the known good device in target disk mode and attach it to the mastering system

- In **Disk Utility**, create a “New Image from Folder” and select your KGD, create the image as compressed
- (Optional) Once the image is created, select “Scan image for restore” in order to prep the image for ASR (Apple Software Restore) - Lightning will also scan the image as it imports it.

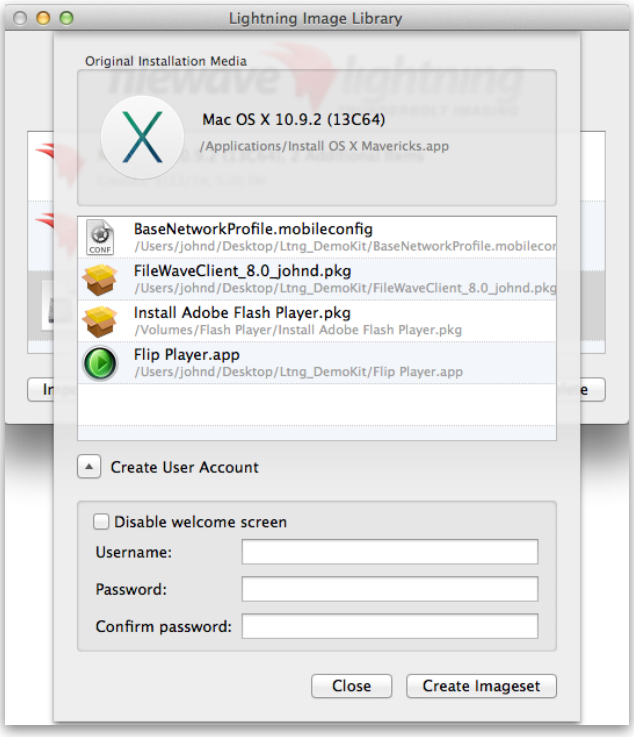
Adding a known good device image

Launch Lightning, and select the **Import** button. Locate and add your newly created image.



Creating a new clean device image

A new image that has never been booted is created by selecting the **Create** button, then dragging the OS X Installer application plus additional content as needed into the window.



Lightning supports files in the following formats:

- *.mobileconfig* - exported profiles from Filesets, Profile Manager, etc

- *.pkg* - installer packages (the installer must be able to run without dialogs or conditional stop points)
- *.app* - drag and drop applications

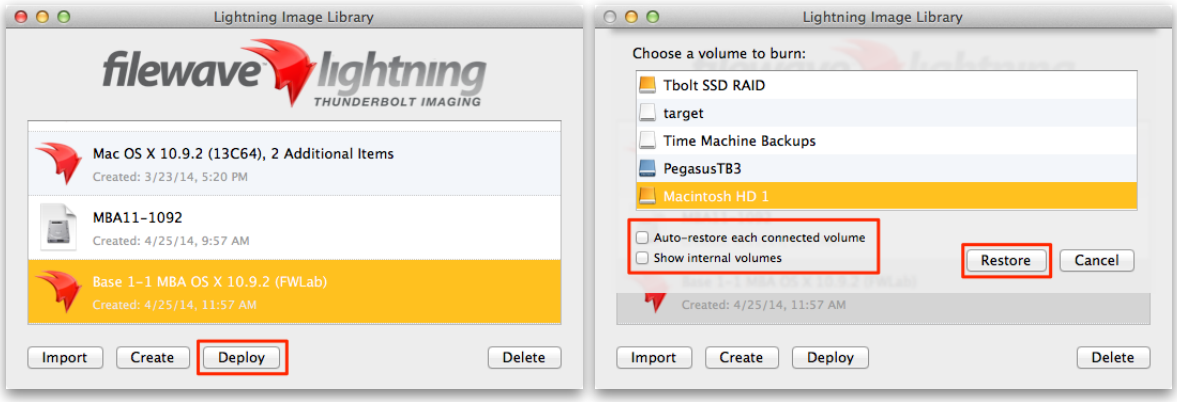
In this case, the client will be imaged with the latest version of Mavericks (as of release of this manual), a networking profile to join it to a specific WiFi network, a custom FileWave client that joins the client to a specified FileWave server, the custom IT version of the Adobe Flash installer, and a copy of the Flip Player to allow diverse media formats. Note that the **Create User Account** is not active. This is so the client will boot to the setup assistant as a new device. There are other options for this setting.

Using the Create User Account setting

The Create User Account allows you to create a local administrator account on the imaged system. You can also choose to disable the welcome screen, which disables the setup assistant. (It places the file */var/db/.AppleSetupDone* onto the client.) If you add the local administrator account and allow the setup assistant to run, the first user will still be able to create another local administrator account. In some modified deployment workflows, this may be the desired outcome - having a local administrator account created by IT as well as the user creating their own local account.

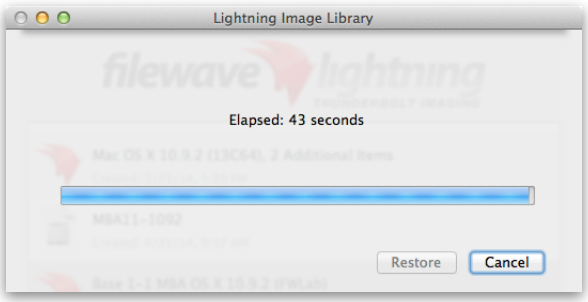
Imaging a client system

Once the image is created, you can click on it to rename it, and prepare to deploy the image.



You'll boot your client machines into **Target Disk mode** by holding down the "T" key and powering them up. Connect the client to the master system with a Firewire or Thunderbolt cable (USB works too; but is really, really slow…). The client will pop up in the imaging window. At this point, you have two additional options:

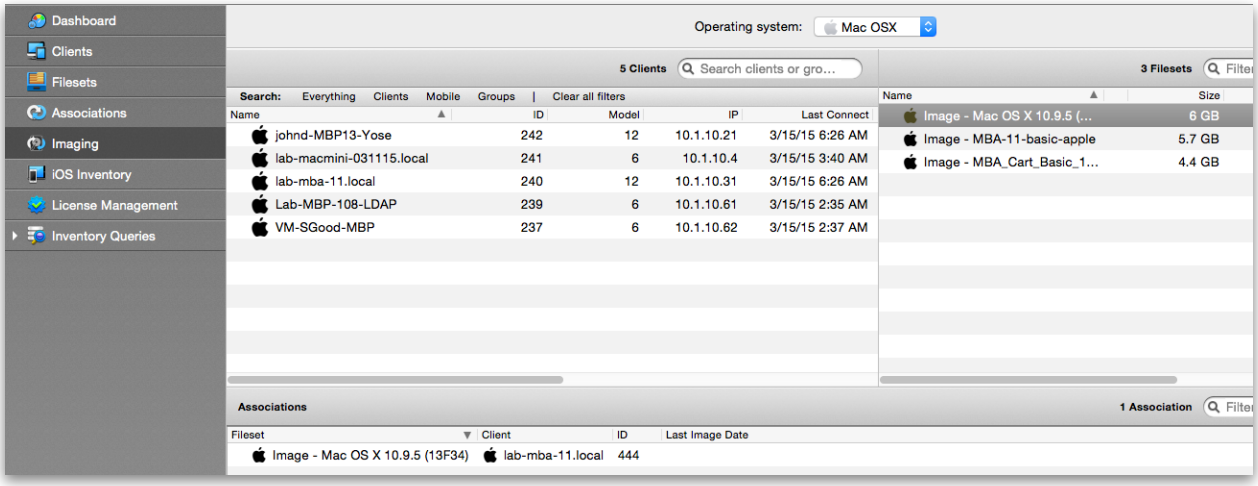
- *Auto-restore each connected volume* - this will start the restore process automatically on each client that gets connected to your master system while Lightning is actively deploying an image. Best practice is to keep anything not to be imaged away from the imaging system for the duration of your deployment.
- *Show internal volumes* - this displays the **root** drive as well as any partitions except the Apple Restore partition. You can use this process to restore the image onto an internal partition of your system.



The imaging process will run, giving you progress updates, and when finished, it will unmount the newly imaged client system. This allows you to just unplug the imaged Mac and plug in the next one to keep the process moving. Some tests have shown that using 4 mastering systems, you can image approximately 200 Macs in about 90 minutes using Lightning and Thunderbolt.10.2. OS X NetBoot Imaging

FileWave's NetBoot imaging process mimics Apple's system used for imaging large numbers of systems since the late 1990's. You will use Lightning to create the image(s) in the same way you did for the direct imaging process. Once your image(s) are completed, you upload them to the imaging server, associate them with specific OS X clients, and reboot them. The only additional step will be to create the master NetBoot shell that will contain the **system.dmg**.

In FileWave Admin, select the "Imaging..." view. The pane on the top left displays a list of client machines, the pane on the top right will be a list of your images. The bottom pane displays a list of Image associations.



The OS X network imaging process workflow for FileWave v9 consists of the following workflow:

- Setup Imaging server (IVS)
- Create a valid NBI
- Upload Images as Filesets
- Associate Images in FileWave Admin
- NetBoot OS X clients

Build NBI

For our imaging server to work properly, we have to provide "Network Boot Images" (NBI) across the network to our OS X clients. We will create those using an automated NBI creation script. This script is located on the Imaging Appliance, and will be downloaded through the administrator.

Install the FileWave Admin app on an OS X client machine running a version of OS X that you can use to boot **all** of your Macs. All 64bit Intel systems should be able to boot to OS X v10.10 Yosemite. If there is a problem with older systems, you may want to configure a second IVS to handle them. You can manage multiple imaging servers in FileWave preferences.

Log into the FileWave Admin app and open the "Imaging..." preferences, select the IVS you are going to boot your clients from, click the "Download NBI file…" button. This will download the creator script to your current desktop. The script will be named **create_nbi_< IVS IP address >.sh** and you must set proper permissions and activate the script.

You will need to perform two actions:

- Open the terminal (/Applications/Utilities/Terminal.app)
- Type the following commands (note: you will be prompted for an administrator password to use sudo commands):
- You can also just type the beginning of the command, then drag the file on top of Terminal so that the correct pathname and filename get used

```
sudo chmod 755 ~/Desktop/create_nbi_<your IVS IP address>.sh
sudo ~/Desktop/create_nbi_<your IVS IP address>.sh
```

You will see the script begin to create the NBI using the local recovery partition on your current machine. If you use this script on a 10.9 machine, the resulting NBI will be compatible with all 10.9 capable client hardware. If you use this script on a 10.10 machine, the resulting NBI will be compatible with all 10.10 capable client hardware. The script may take a few minutes to create and upload the NBI.

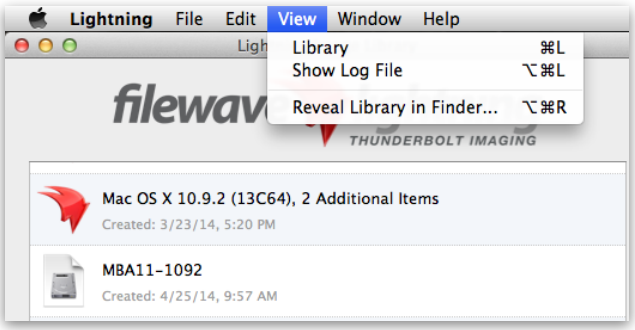
Once the script has finished, your NBI will have been successfully created and uploaded to the Imaging Virtual Server. You are now ready to upload images to your FileWave server.

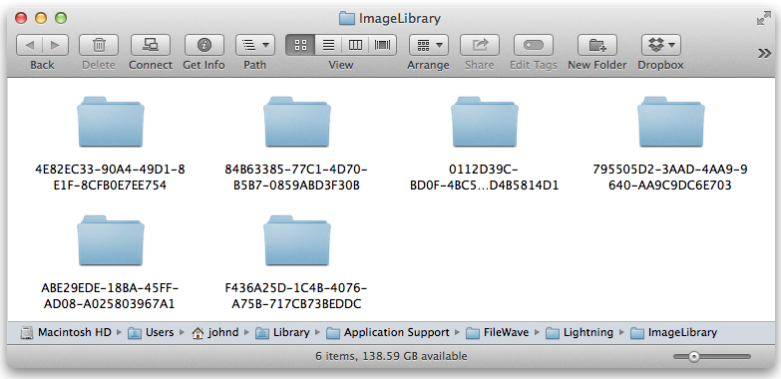
Create and Upload Images

Create your Images using FileWave Lightning, or drag prebuilt images into Lightning.

Note: If you are building your images from scratch, be sure to include a custom FileWave client pkg installer for your FileWave client machines. Lightning will not do this automatically.

FileWave Lightning will automatically scan prebuilt images and prepare them for deployment. Once you have added and named all of your images appropriately, select "Reveal Library in Finder" from the "View" menu in Lightning.app.

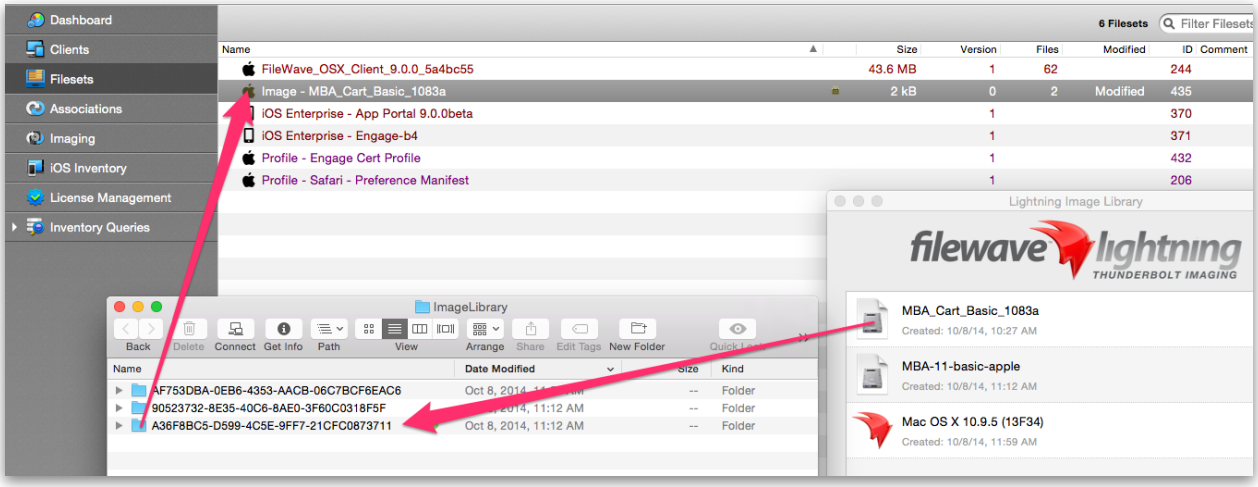




This will open your Image Library. You'll notice all of your images have an ID assigned to them, they will be similar to this: **F436A25D-1C4B-4076-A75B-717CB73BEDDC**

FileWave v9 method

Drag and drop the image folder into the Fileset window. There is no step two. You will have to go to the Imaging pane after that and associate the image with a client, or clients; but the drag and drop method replaces the previous versions need to perform command line magic.

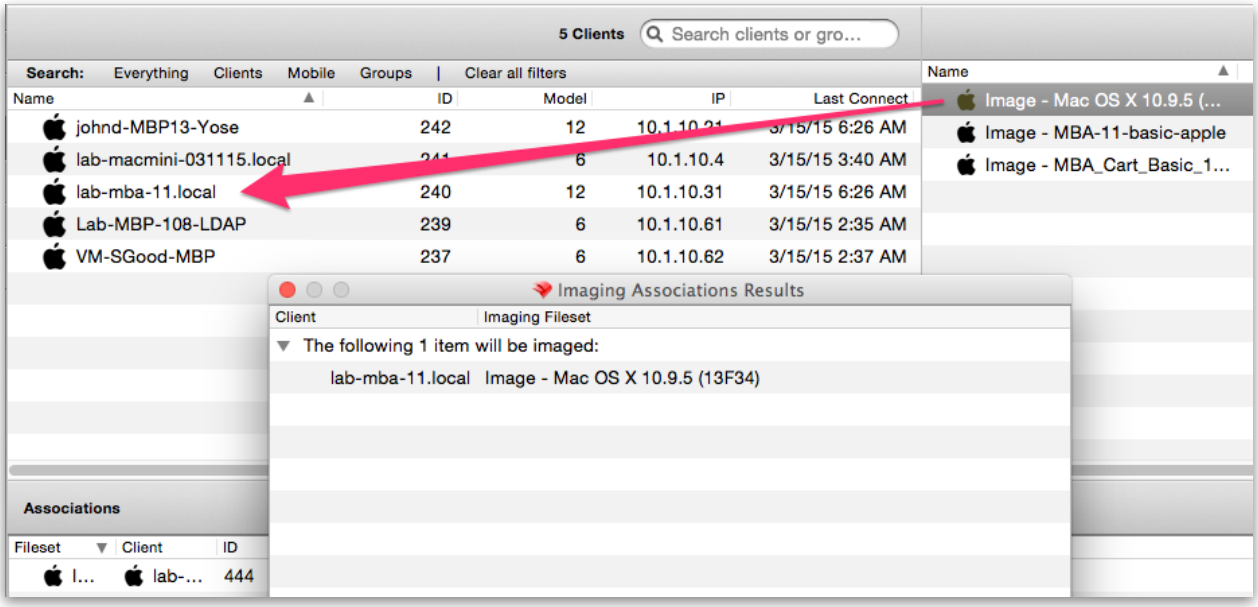


Pre-FileWave v9 method

Refer to the earlier version of this manual.

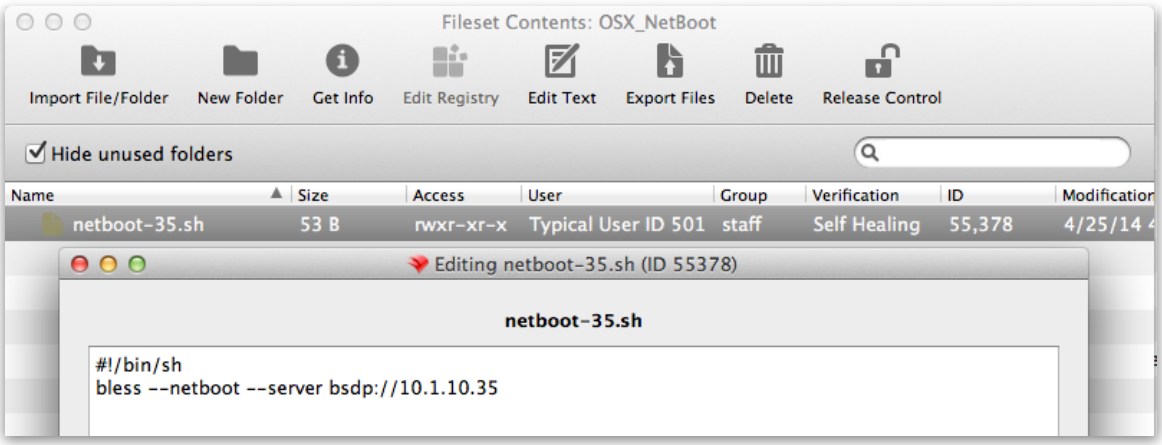
Bare Metal Imaging (Mac)

Clients that are already in FileWave will show up in the **Imaging** view. You associate an image with a client by drag-and-drop.



If your client machines are not yet in FileWave, you can still associate them with an image by uploading a text file that contains the machine name and serial number. See section 11.4 for the format.

You can netboot your client machines using a Fileset, or you can manually net boot the machines by holding down the "N" key during startup. An example of a Fileset that will set the client to boot from the Imaging Appliance NetBoot server looks like this:

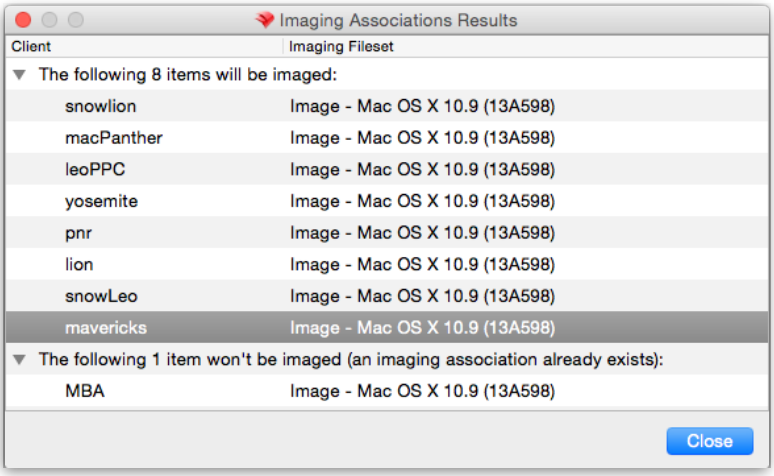


It's a simple shell script (use your **own** Imaging server IP address!) included inside an Empty Fileset. No extra settings. Associate the Fileset, update the model and reboot the client. Imaging kicks in right away.

With FileWave v9+, you now treat imaging workflows the same as application/content work flows. Image sets are now Filesets. Client devices get associated with an image Fileset, then netbooted and imaged.

Image Filesets and Associations

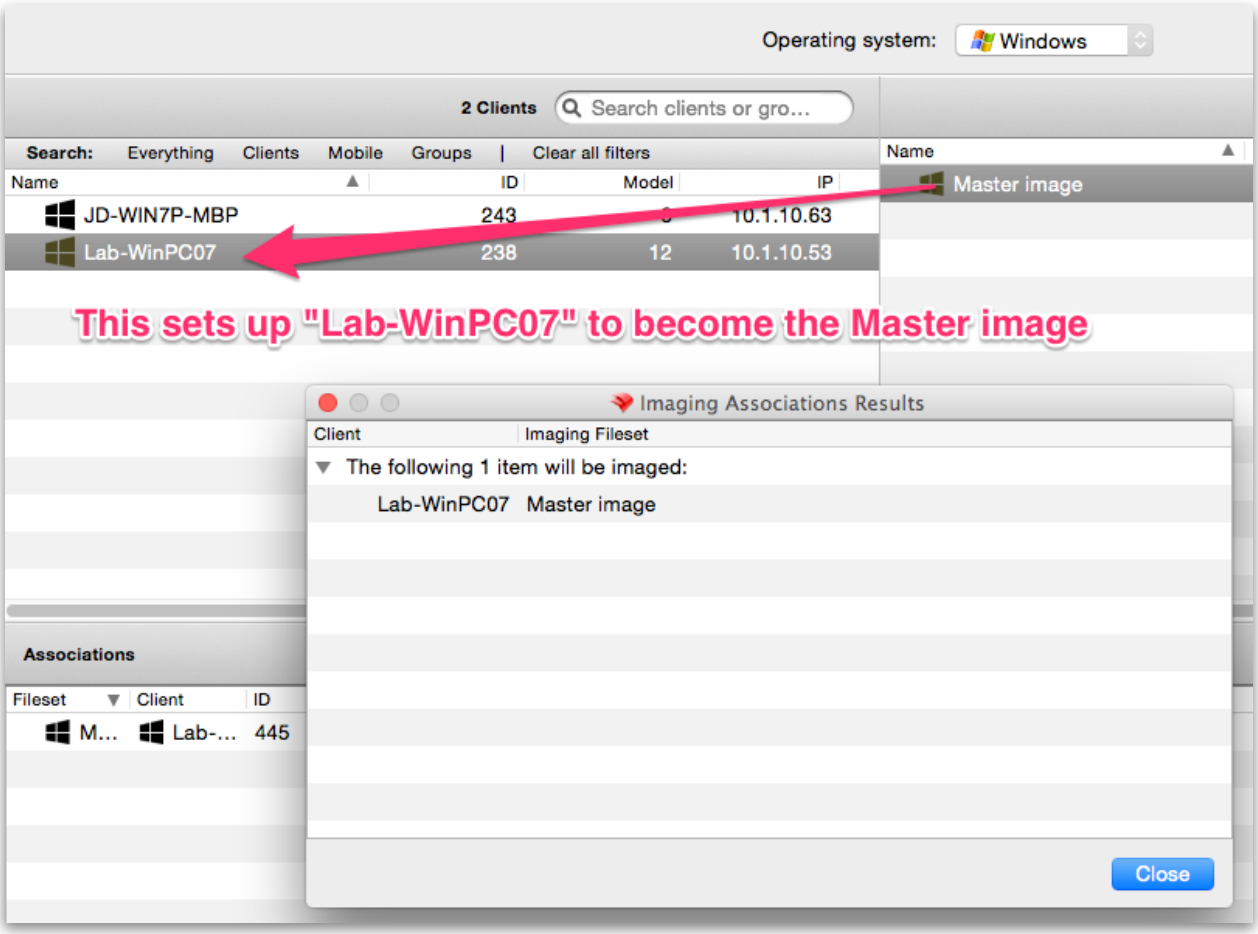
When you create a new image and an imaging association, then do a Model Update, the FileWave Server will build an Imaging Manifest, which gets downloaded by each IVS when it next contacts the FileWave Server. By default, this happens every 120 seconds.


Imaging Associations Results
Client
Imaging Fileset
The following 8 items will be imaged:
snowlion
Image - Mac OS X 10.9 (13A598)
macPanther
Image - Mac OS X 10.9 (13A598)
leoPPC
Image - Mac OS X 10.9 (13A598)
yosemite
Image - Mac OS X 10.9 (13A598)
pnr
Image - Mac OS X 10.9 (13A598)
lion
Image - Mac OS X 10.9 (13A598)
snowLeo
Image - Mac OS X 10.9 (13A598)
mavericks
Image - Mac OS X 10.9 (13A598)
The following 1 item won't be imaged (an imaging association already exists):
MBA
Image - Mac OS X 10.9 (13A598)
Close

10.2. Windows PXEboot Imaging

Using the same administrative interface you use to image a Mac OS X system with NetBoot, you can image a Windows PC using PXEboot. The same general principles apply. Windows imaging in FileWave also supports adding driver sets to Windows clients as part of the imaging process. What is important to understand is that images and driver sets are all Filesets now under version 9 of FileWave.

Under the "Assistants" Menu, click on the "Imaging..." option. This will open the "Imaging" assistant. Select "Windows" from the drop down menu at the top of the view.



The pane on the top left displays a list of client machines, the pane on the right will be a list of your images. The Pane at the bottom pane displays a list of Image associations.

Windows Imaging workflow

The imaging process workflow consists of the following steps:

- Create a clean Windows client with FileWave client installed
- Add new Windows client to FileWave Admin
- Associate "Master" Image with clean FileWave Client or Mac Address
- PXEboot Windows "Master" to imaging server
- Follow prompts to create a Windows Image

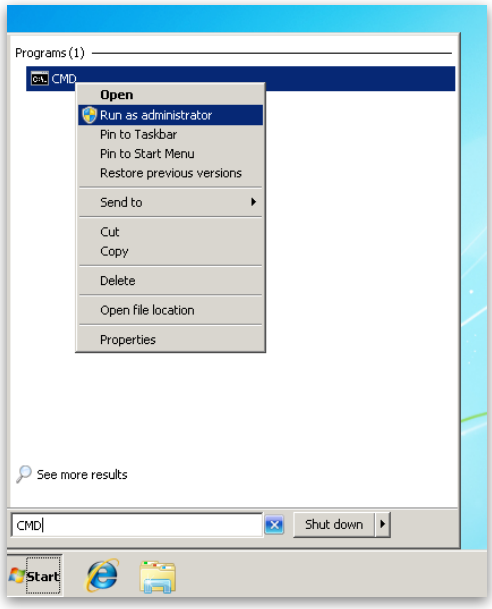
- Associate Images in FileWave Admin
- Update model
- PXEboot client machines

Create your Master Image (Windows)

On a new or clean PC, install Windows 7 from disc or other source. **DO NOT** restore a previous image from another imaging tool.

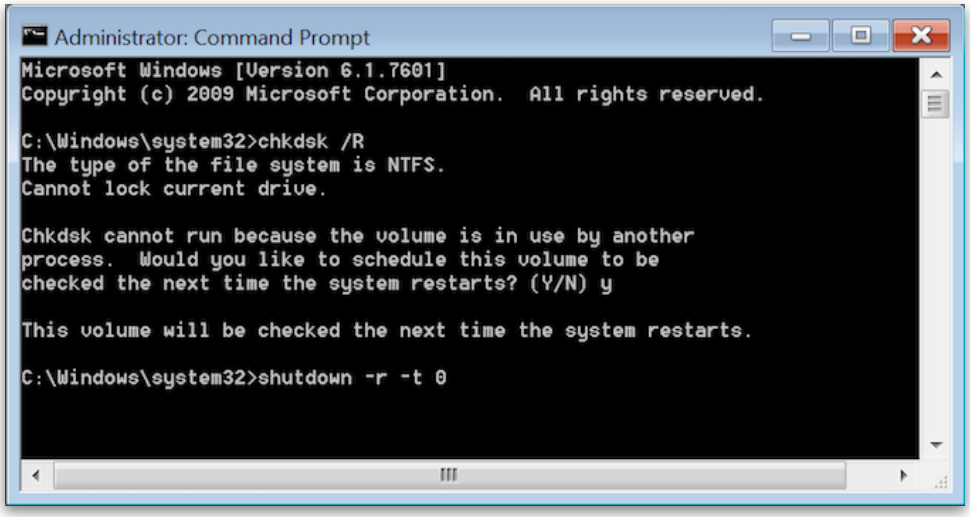
Once you have setup and configured the machine with the options you want (including the FileWave Client), you will need to setup your client machine to run CHKDSK (as administrator) using the following command:

```
>chkdsk /R
```



You will be asked if you would like to run CHKDSK at the next startup, press “Y”; then you can either go to the Start menu and restart, or use the following command to restart your device:

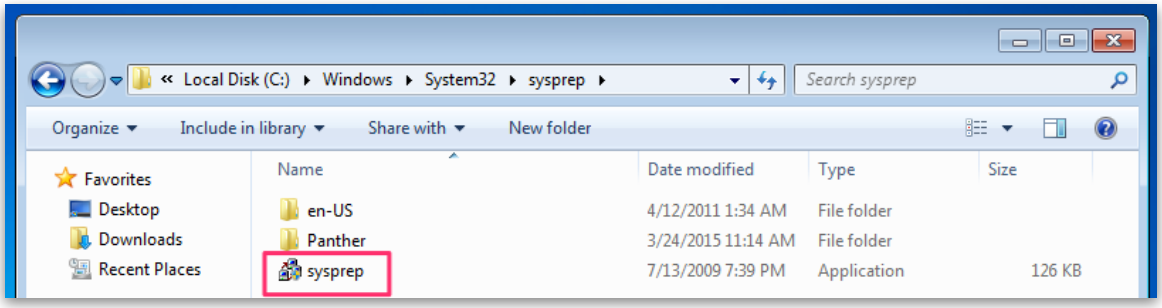
```
>shutdown -r -t 0
```

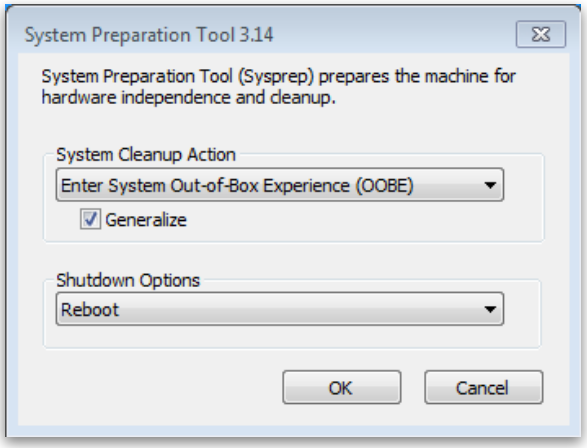


When you have completed your *chkdsk* process and are ready to create your master you will need to run the ***Sysprep*** tool from Microsoft.

Sysprep is part of Windows and you can find out more information about Sysprep here:
http://technet.microsoft.com/en-us/library/cc766049%28v=ws.10%29.aspx

You must use only the version of Sysprep that is installed with the Windows image that you intend to configure.
Sysprep is installed with every version of Windows and must always be run from the *%WINDIR%\system32\sysprep* directory.
It must only be run on clean installations, not on upgraded systems.



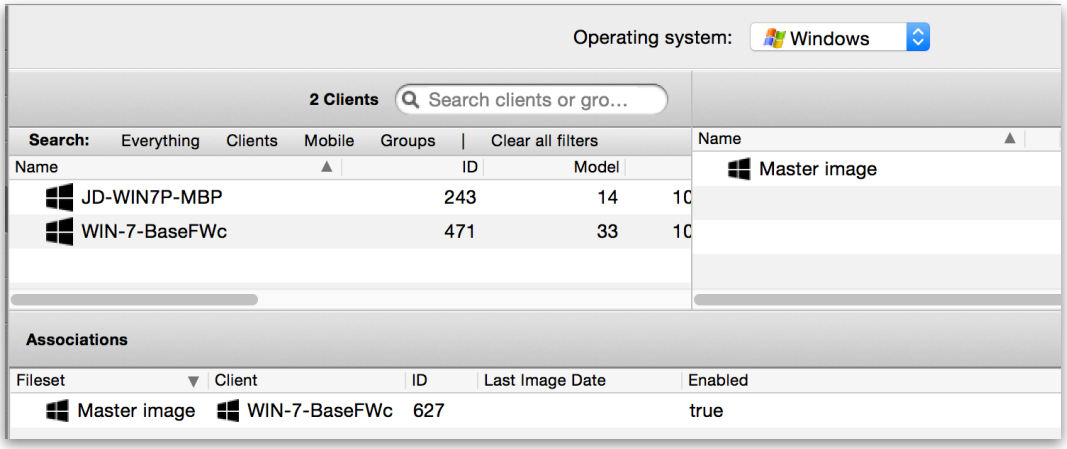


Your client is now configured to create a master image. Booting your machine into PXE mode will cause it to connect to the filewave server. Follow the prompts to name your new image:

Image your Clients

Once you have completed uploading the images to FileWave, you are ready to begin imaging your client machines.

Login to FileWave Admin. You should see your images listed on the right hand window pane when you access the "Imaging" window. To associate client machines from the left hand side, simply drag them to a particular image. They will be associated in the associations box below, and the association will take effect when you click OK. It never hurts to update the model - after all, you are working with Filesets and associations.



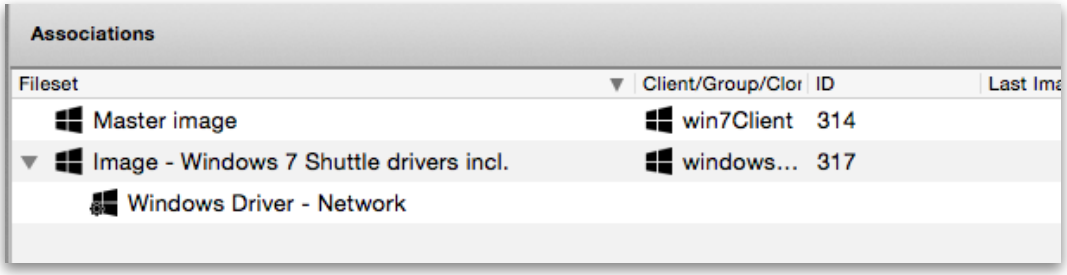
You will want to make sure that your Windows Client machines are set to PXE boot first in the boot order. Machines that PXE boot to the Filewave server and do not have an association will boot to the local drive, as will clients that have an association that is set to "Disabled". You may choose to re-enable a disabled association at any time.

Drivers for Windows images

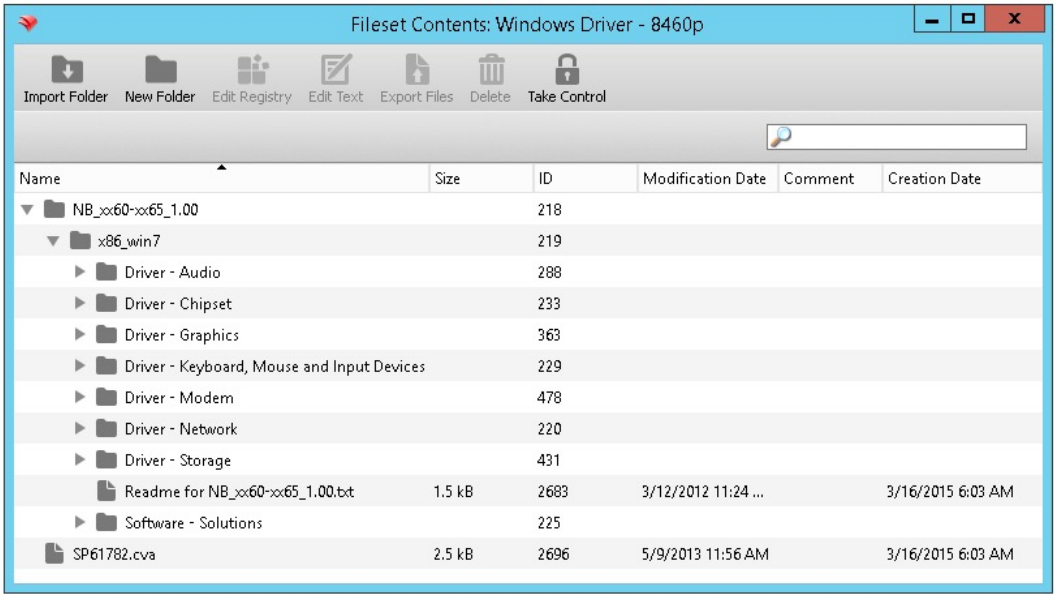
Version 9 of FileWave and Imaging v3 brings the ability to associate PnP drivers with Windows machines. Your base image may not contain all of the drivers needed to run on your target PC. FileWave can deploy those drivers now by copying the driver files into *C:\drivers* on the newly imaged PC and modifying the Registry to tell Windows to look into the C:\drivers location if needed. Details on PnP drivers is available at this link for Microsoft:

http://support.microsoft.com/kb/254078/en-us

During the Imaging process, the files will be deployed to the device and Windows registry will be updated.

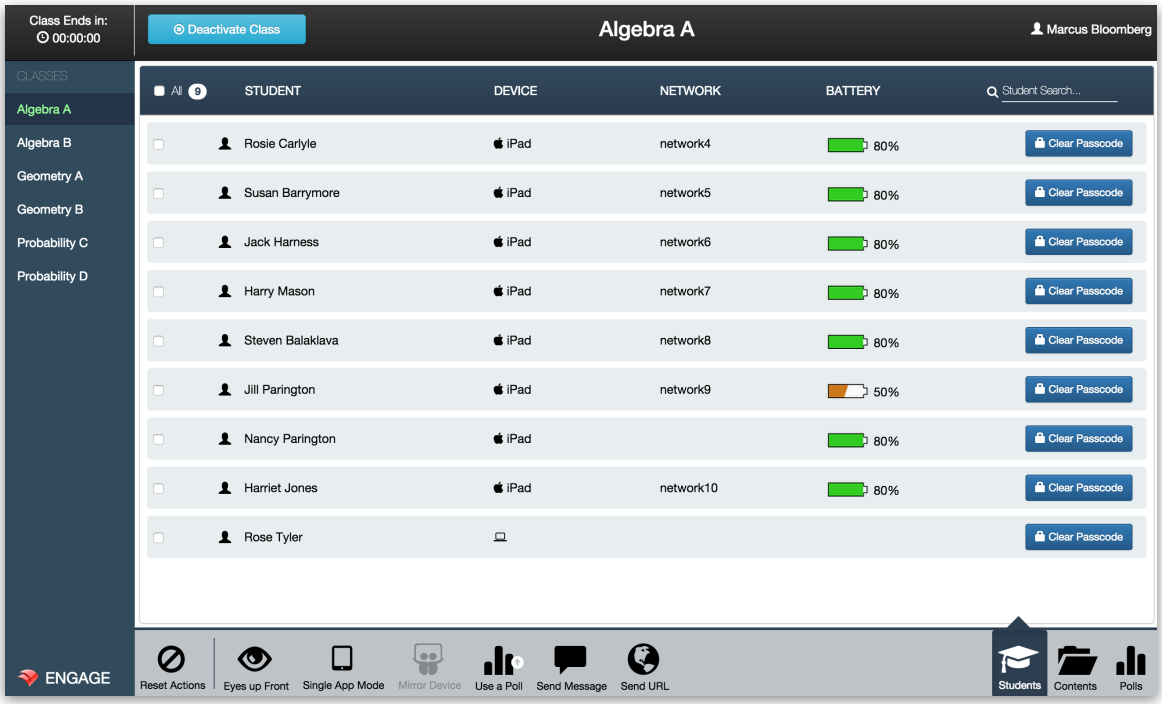


Note: FileWave is not installing drivers - only copying files into a given location on the Win PC and telling the PC to look into that directory.


Fileset Contents: Windows Driver - 8460p
Import Folder
New Folder
Edit Registry
Edit Text
Export Files
Delete
Take Control
Name
Size
ID
Modification Date
Comment
Creation Date
NB_xx60-xx65_1.00 218
x86_win7 219
Driver - Audio 288
Driver - Chipset 233
Driver - Graphics 363
Driver - Keyboard, Mouse and Input Devices 229
Driver - Modem 478
Driver - Network 220
Driver - Storage 431
Readme for NB_xx60-xx65_1.00.txt 1.5 kB 2683 3/12/2012 11:24 ... 3/16/2015 6:03 AM
Software - Solutions 225
SP61782.cva 2.5 kB 2696 5/9/2013 11:56 AM 3/16/2015 6:03 AM

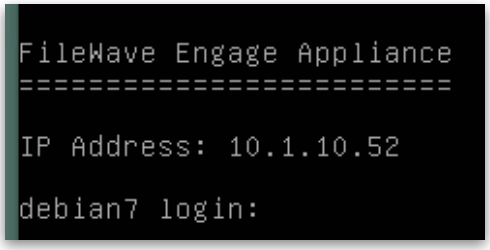
11. Classroom Management with Engage

While FileWave provides the essential lifecycle management tools for the IT staff, there was a recognized need for a tool designed specifically for teachers and classroom management. ***Engage*** was developed to provide a mechanism for teachers to interact with their students during class. The idea is to present an active view of the students in a designated class, be able to keep the students focused on the session, and interact with them to ensure that they are keeping up. Linking the institution's classes, teachers, and students can be done through a simple text file import, or by integrating the school's SIS through the use of Clever (http://www.clever.com).



11.1. Engage server

For caching the SIS information, as well as the polls and content links, Engage uses a VM that is provided as part of your component download from the FileWave Support site. The virtual machine runs on most common VM engines, such as VMware. When the server boots, it will grab a DHCP address that you need to record:

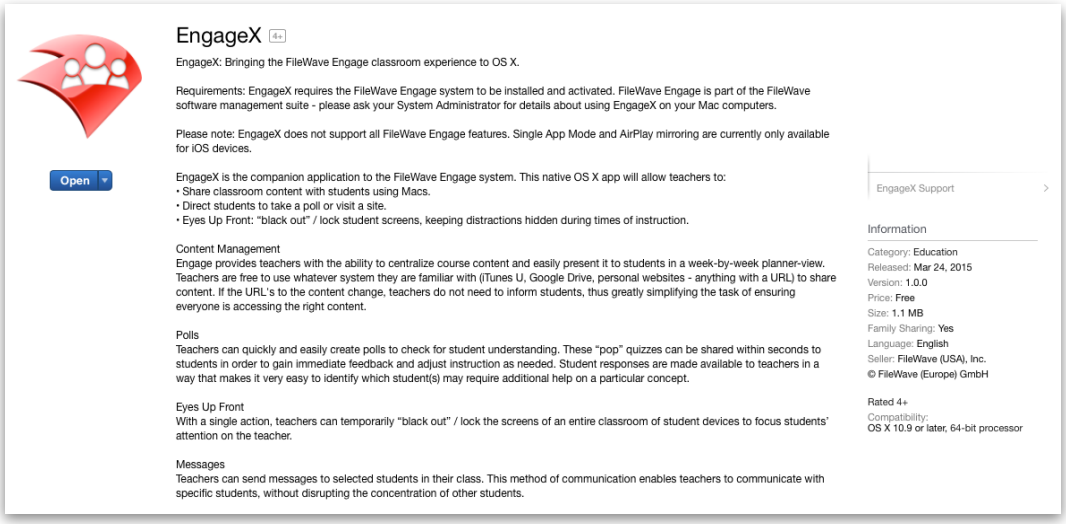


The login and password for the Engage server, by default, is ***filewave / filewave.*** You can use the **passwd** command to change the default password to something a little more secure.Record the IP address for use in the Engage preferences.

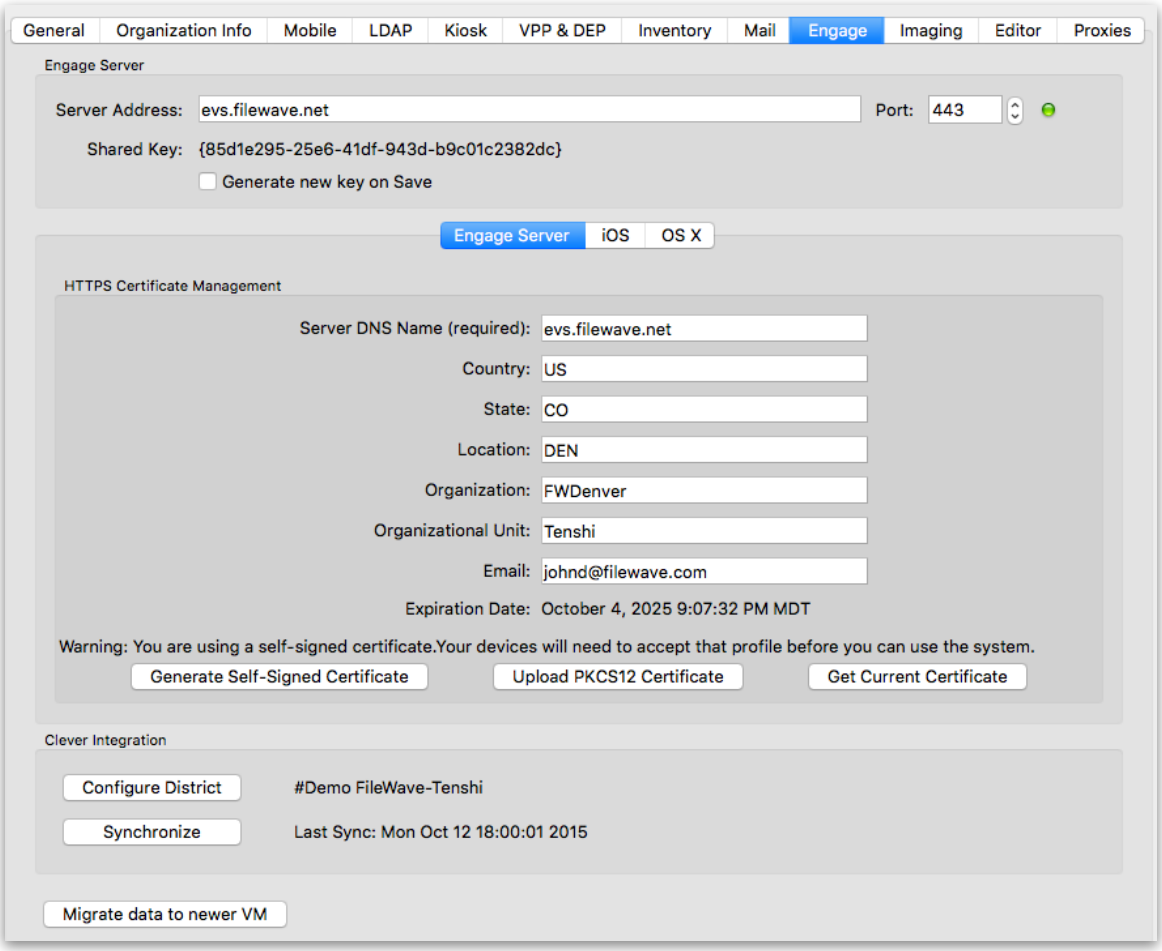
11.2. Engage applications

All interactions between teachers and students take place from the Engage application. There is an iOS version of the Engage application provided to you as an **ipa** file download from the FileWave site. For OS X, the Engage application is available as a free download from the Mac App Store. The OS X app can also be "purchased" (it is free)

from the Apple VPP Store for inclusion into your License Management schema. Both teachers and students use the same application; the Engage application reacts with a different UI based on the person logging in.



11.3. Engage preferences in FileWave Admin



Engage Server

Enter the server address for your Engage server VM. It should be a FQDN or fixed IP address, if possible. The default TCP port for Engage is 443.

HTTPS Certificate Management

There are two options for securing the communications between the Engage server and its clients - a self-signed certificate or a valid SSL certificate in .p12 format. There are also specific push certificates for iOS and OS X that will be provided by FileWave as part of your software download.

- Self-signed certificate for https

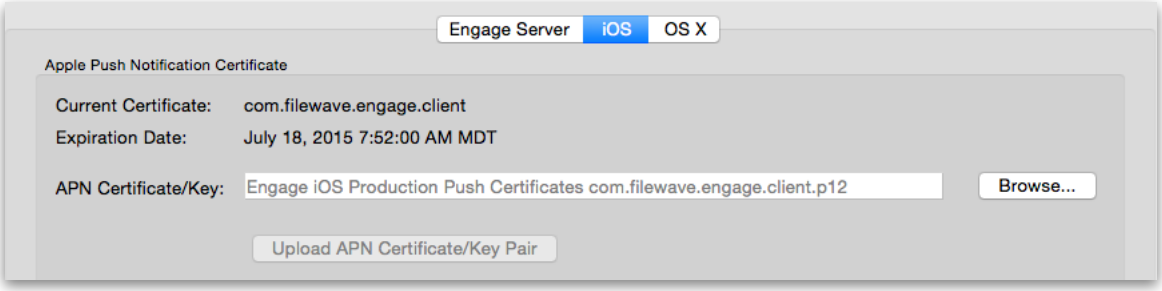
Fill in the data fields in the **HTTPS Certificate Management** pane of the Engage preferences. Click on the button ***Generate Self-Signed Certificate***, then click on the button ***Get Current Certificate***. You will download the self-signed certificate and import it into FileWave Admin as part of a Certificate profile. See the section on working with Filesets for further information on profiles. This certificate profile must be associated with all iOS and OS X clients before they launch the Engage application for the first time. Otherwise, the client will display an error that it "cannot connect to server" - meaning the Engage server.

- 3rd Party valid certificate for https

You can use a known 3rd party for a valid certificate with Engage, companies such as StartSSL, VeriSign, etc. Follow the instructions on their site to download a valid server certificate in **.p12** format. Upload that certificate into FileWave Admin Engage preferences using the ***Upload PKCS12 Certificate*** button. When you have done this, you will get an alert to restart the Engage server.

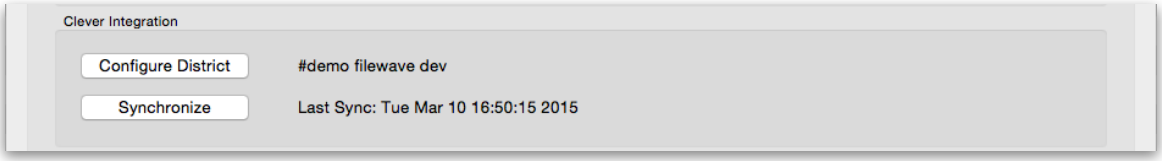
iOS / OS X push certificates

The push certificates you need for Engage will be provided by FileWave. Select the tab for the certificate you are going to import, then click on the ***Browse*** button. Locate the appropriate certificate and select ***Open***. Finally, click on the button ***Upload APN Certificate/Key Pair***



Clever Integration

Unless you are going to use a manually created CSV file with all of your class / teacher / student data, odds are you will want to integrate your institution's SIS with FileWave / Engage using Clever. The process for this is very simple. First, you go to http://www.clever.com and log in using the account and password provided to you by Clever. That will present you with your district/site web page. From that page, you will need to copy your **district ID**.

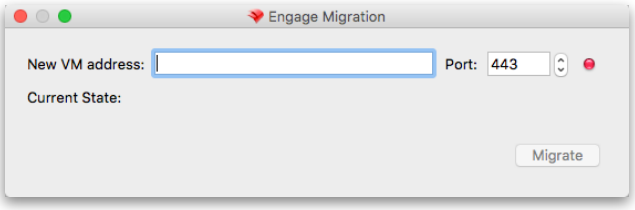


In the Engage preferences, click on the ***Configure District*** button, authenticate as the FileWave Admin superuser (fwadmin), and paste the *district ID* into the data field.

Note: DO NOT use the Engage OS X or iOS .p12 certificate as your MDM certificate to Apple. This will not work, and will cause your device to fail to communicate with your MDM service.

Migrate Data to a newer VM

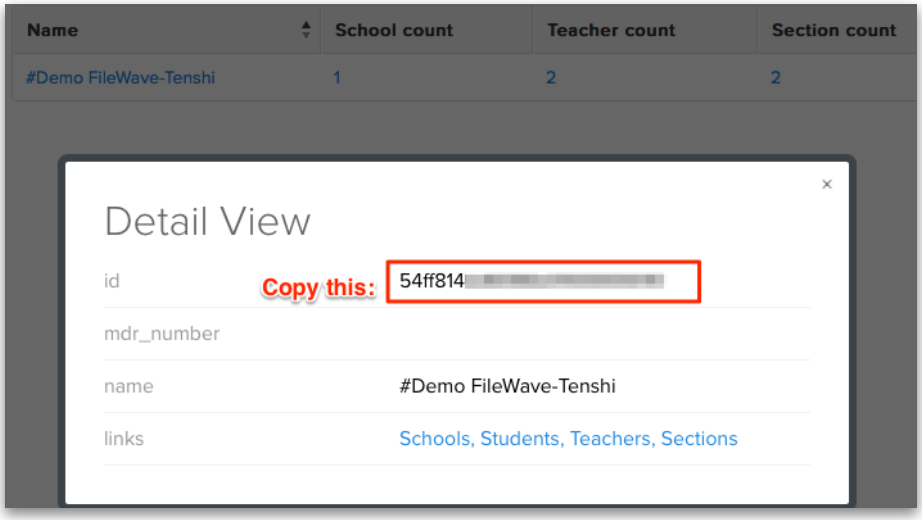
If the time comes where you need to upgrade or replace your VM engine, or the Engage VM itself, this button provides a way to migrate all of your Engage data you have created into the newer Engage VM. You set up your new Engage VM, then enter that newer IP address (or FQDN) into the migration dialog. The FileWave server handles the rest by transferring all of the data. Then you shut down the old VM and update your Engage Preferences.



11.4. SIS integration with Clever

A major strength of Engage is the ability to synchronize institutional data from a Student Information System (SIS) with the Engage server. This allows the teachers and students to log into Engage using the same credentials they use every day for curriculum applications and gradebooks. Of the two mechanisms for SIS integration, the use of Clever is by far the easiest. FileWave customers with a current SIS get Clever support from FileWave for free; so they can get up and running with a fully populated Engage environment in no time. Here are the steps to get Clever and Engage running together.

The process of setting up the Clever integration involves linking your institutional Clever ID, or District ID, to FileWave. The District ID is found when you log into the Clever web site (http://www.clever.com) and select your District name from the District overview window:



That ID number goes into the field in the Engage preferences as shown in the section above. Once you are connected, Clever will synchronize all of your SIS data with the Engage server every 24 hours around midnight. You can force a sync by holding down the *alt/option* key clicking on the **Synchronize** button in the Engage preferences.

The SIS data is cached as read-only on the Engage server for the purpose of login and aligning teachers and students with the correct classes.

11.5. CSV data import

If your institution does not have an SIS, or does not wish to synchronize data through Clever, you can manually import all of your information using **csv** formatted text files. Engage supports direct data import. The files you must create are: students, teachers, and classes. There are two forms of these files - a "full" set for initially entering large amounts of data, and an "incremental" or "update" set for entering changes to the data that exists. The formats for these files is as shown below:

Teachers-full: username,password,email,first_name,last_name,district,school,title

marcus,marcus,marcus.bloomberg@filewave.org,Marcus,Bloomberg,South FileWave,Engage University,Prof. Marcus Bloomberg

Students-full: username,password,email,first_name,last_name,district,school,birth_date,grade

rosie,rosie,rosie@stu.filewave.org,Rosie,Carlyle,Bloomberg,South FileWave,Engage University,1990-01-29,13

susan,susan,susan@stu.filewave.org,Susan,Barrymore,Bloomberg,South FileWave,Engage University, 1990-02-29,13

Classes-full: class_id,name,owner,students

101,Academic Lab,marcus,rosie|susan|jack|harryl|steven|jill|nancy|harriet|rose|rory|river|elizabeth|sandy|phill|alex

102,Composition,marcus,rosie|susan|jack|harryl|steven|jill|nancy|harriet|rose|rory|river|elizabeth|sandy|phill|alex

(The format for student names is each login name separated with a vertical bar and no spaces.)

The incremental / update file formats are similar; but contain only changes to be made; such as in the students_update.csv shown below. Only changed or added items need to be included. Data fields left out will not change. Index fields are **class_id** and **username**., and must be included at all times.

username,password,first_name,last_name

rosie,rosie,Rosie,Carlyle

susan,susan,Susan,Barrymore

CSV structure

Each file is a CSV with a header. In the header you have to specify which fields you want to insert/update for each of the records. Each entity type has a field that uniquely identifies it. When a CSV file is imported, we try to find the corresponding record in the DB with that identifier. If we can, we update the fields that are specified in the file (and leave the other fields as they were before). The default for values is an empty string.

Importing the csv files into the Engage server

The process of importing the data into the Engage server is done through the command line. Either at the Engage VM itself, or remotely, using **ssh**, you enter the following command sequence:

```
engage-control synchronize_engage --classes classes.csv --teachers teachers.csv
--students students.csv [--full|–incremental]
```

The different options are:

- --classes classes.csv: gives the path to the CSV file that defines the classes to import
- --teachers teachers.csv: gives the path to the CSV file that defines the teachers to import
- --students students.csv: gives the path to the CSV file that defines the students to import

- --full or --incremental (default is --full): That is about full vs incremental sync. The full sync is handled so that a record that is in the DB but not in the file is marked as inactive (for later deletion). An incremental sync is just updating or inserting records without touching the ones that are not referenced.

The login for the VM is “filewave / filewave” (name / password) by default. A remote connection would look like this:

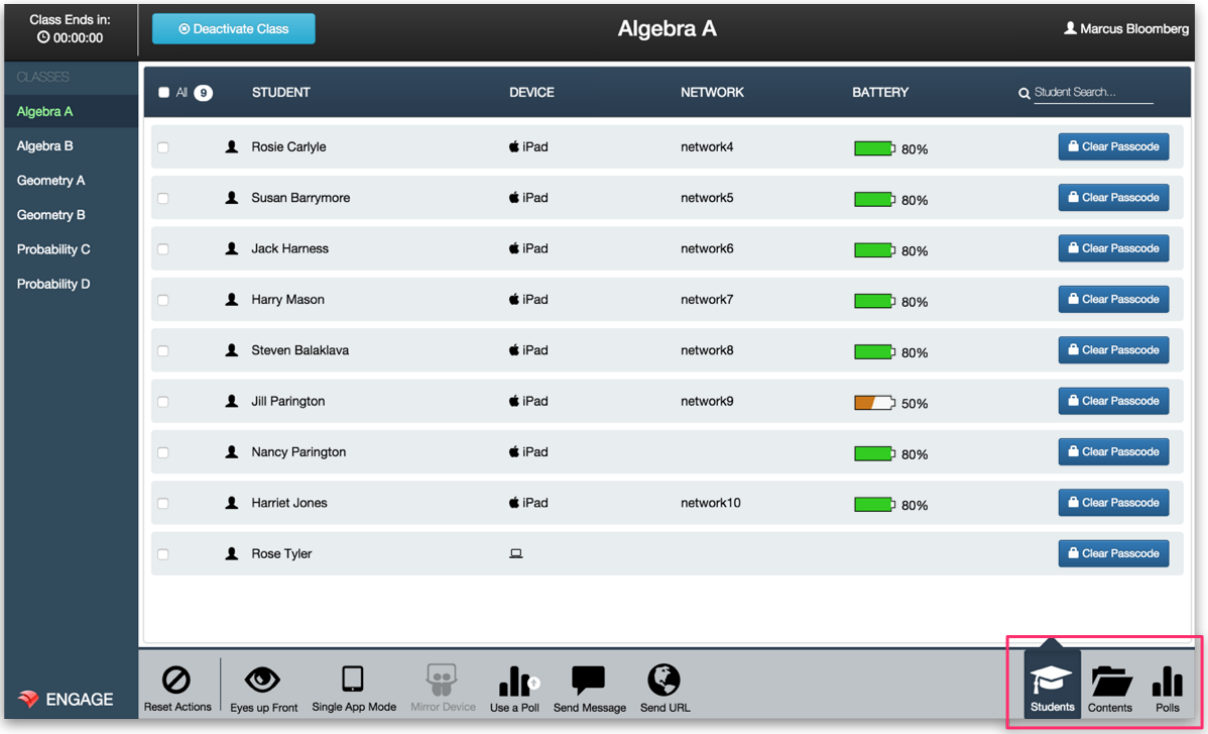
```
ssh filewave@<Engage_server_IP_or_FQDN>
```

Example:

```
johnd-MBP13-Yose:Desktop johnd$ ssh filewave@tenshi-fw-eng.filewave.net
filewave@tenshi-fw-eng.filewave.net's password:
Linux debian7 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1+deb7u2 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 25 03:07:13 2015
filewave@debian7:~$
```

11.6. Teacher Interface

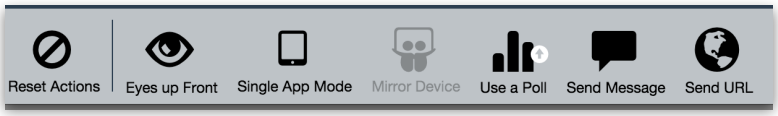
The teacher interface in Engage shows three primary views: Students, Content, and Polls.



Teacher Interface: Students view

The Students view shows the currently active class, the students by name in that specific class, select status items, and some control buttons and actions. In this window, the teacher can select a class, activate/deactivate that class, send specific commands to some or all of the students, and clear the student's passcode on their device.

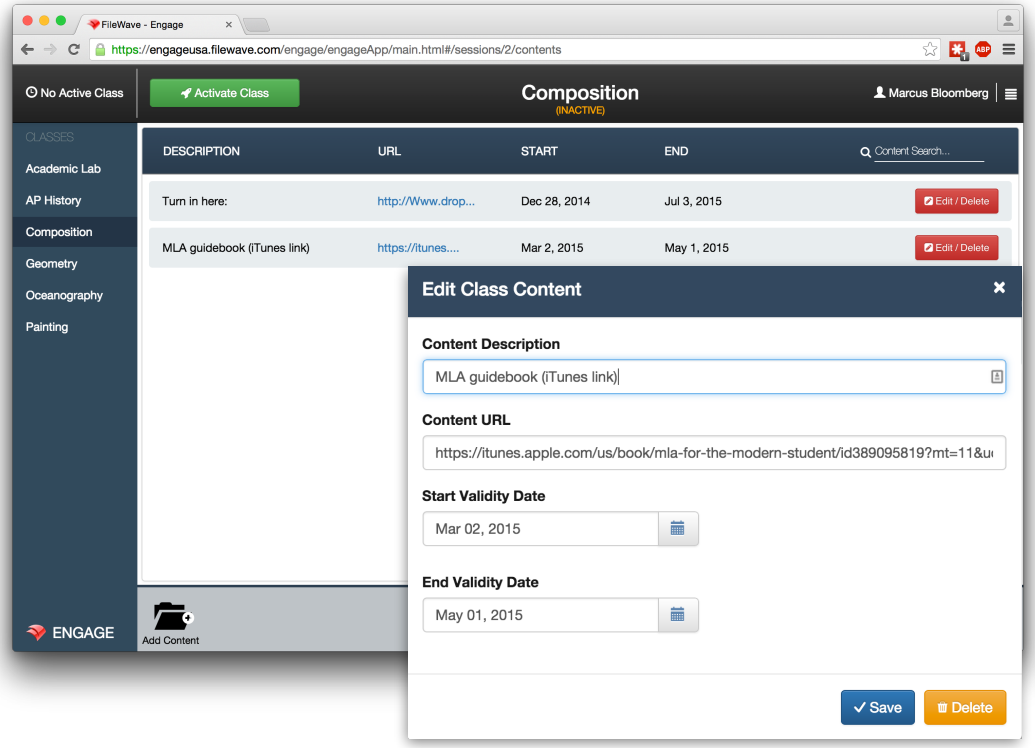
The commands the teacher can send are as shown:



- *Reset Actions* - returns all devices to a neutral state, clearing any locked screens, messages, and AirPlay
- *Eyes Up Front - sends a message to all designated users to get their attention. Devices in Single App mode cannot dismiss the message.*
- *Single App Mode* - forces supervised iOS devices into a single, designated application. Engage can be designated for single app mode.
- *Mirror Device* - uses the AirPlay profile to force a supervised iOS device to display on a selected AppleTV. Devices must be on the same network. Requires the use of an AirPlay profile on the teacher's device.
- *Use a Poll* - provides the teacher with a mechanism to check on student progress through a simple Q&A process
- *Send Message* - unlike the Eyes Up Front dialog, this dialog can be dismissed by users. Can be used to send reminders, hints, or just pass along information to selected students.
- *Send URL* - the teacher can send a URL to the student that links them to a web site, a document, or anything that can be designated with a URL.
- *Clear Passcode* - Clears the passcode on designated iOS devices (uses the same code as the MDM command)

Teacher Interface: Contents view

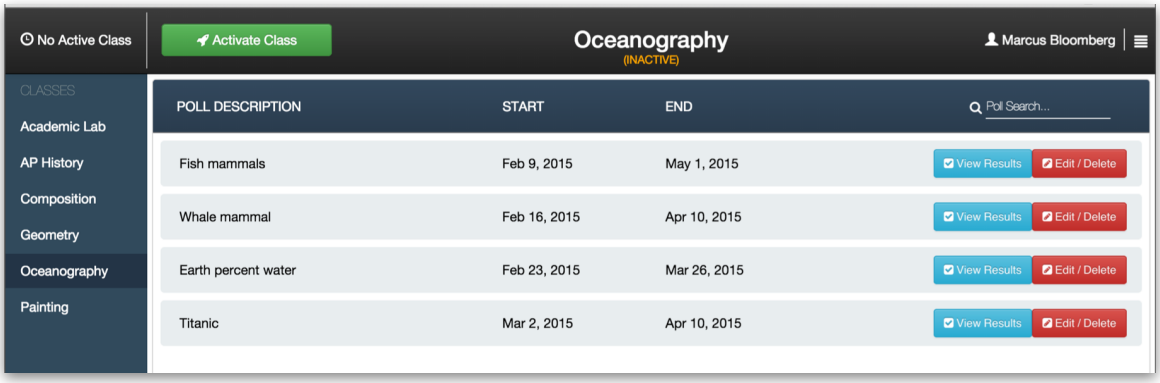
This view allows the teacher add or edit content for use by the students. Contents allow you to use any container for the resources provided because it is done through the use of URLs. Examples of content URLs can be simple web site URLs, Google Drive items, LMS items, iTunesU content, and any other item reachable with a URL.



Teachers can also set availability of the content by setting start and end dates for access to the items.

Teacher Interface: Polls

The Polls view provides the teacher with a mechanism for creating “quick check” sessions to see if the students are paying attention, or just to quickly check progress. When students take a poll, the teacher will see all responses, along with the correct and incorrect answers, if necessary.



The teacher interface is designed to allow a teacher the ability to concentrate on their class and students, without encumbering them with a lot of extraneous tools.

11.7. Student Interface

Using the same Engage application, the student interface contains a simpler set of data:

- *Student view* - displays current content and polls for all classes a student is registered in.
- *Content and Polls* - view and use available content and/or polls
- *Eyes Up Front / Messages* - “pay attention” notes from the teacher

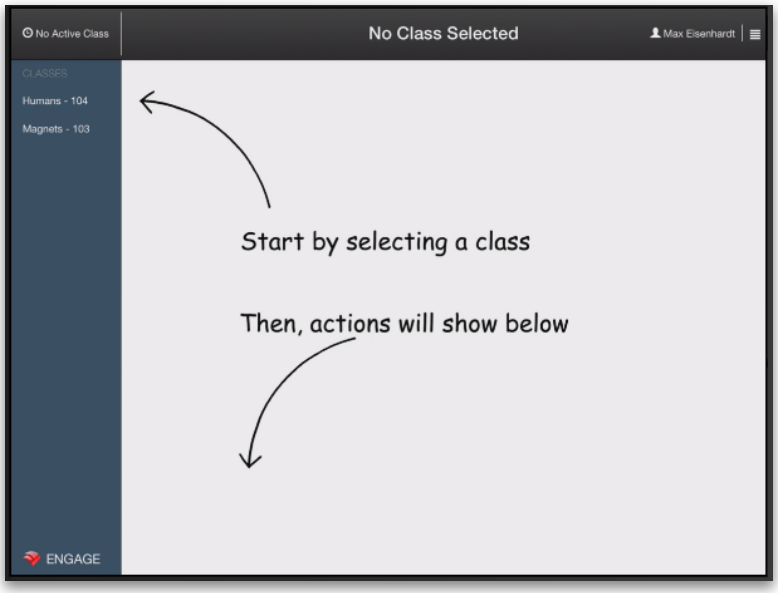
11.8. Sample Workflow “A Day in the Life”

In this section, we will follow a teacher and a student as they use Engage for a class. The interface is the same for users on iOS and OS X devices. The only difference comes from supervised versus unsupervised iOS devices. Supervised iOS devices are the only ones who can be forced into Single App Mode or locked down in Eyes Up Front.

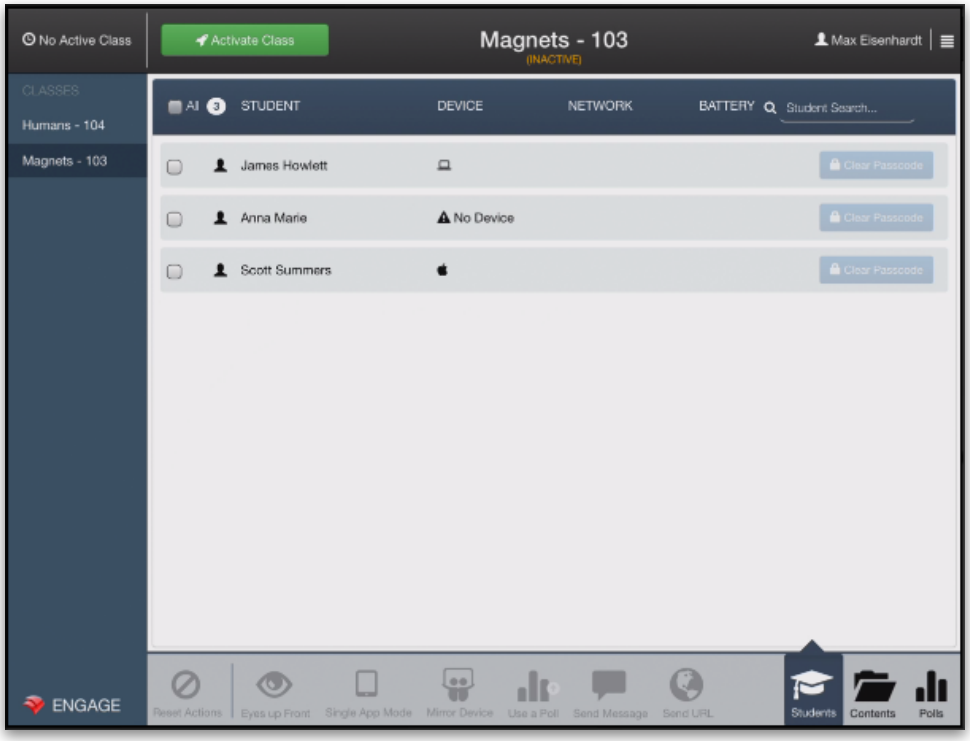
Logging in

The teacher and student must both log in using their institutional credentials. In this case, the teacher with the username of “magneto” is connecting on an iPad.

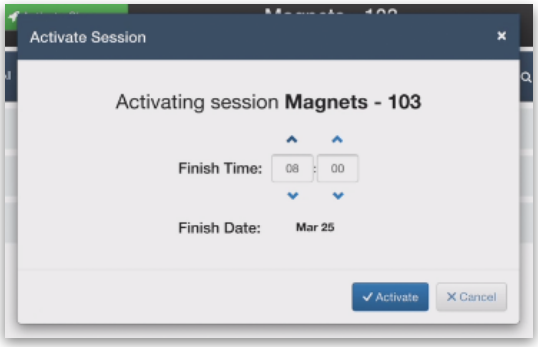
Once logged in, they are presented with a view with helpers:



Those arrows are meant to help teachers get started with Engage easily. So Max (our teacher) will select the class for today - **Magnets - 103** and will be presented with the primary view of his class.



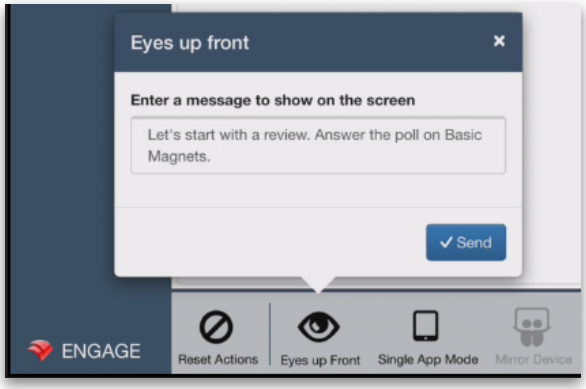
Up at the top left of the widow, Max sees the **Activate Class** button. This button will allow the teacher to begin the class by locking in the students assigned by the SIS to this class and setting the end time.



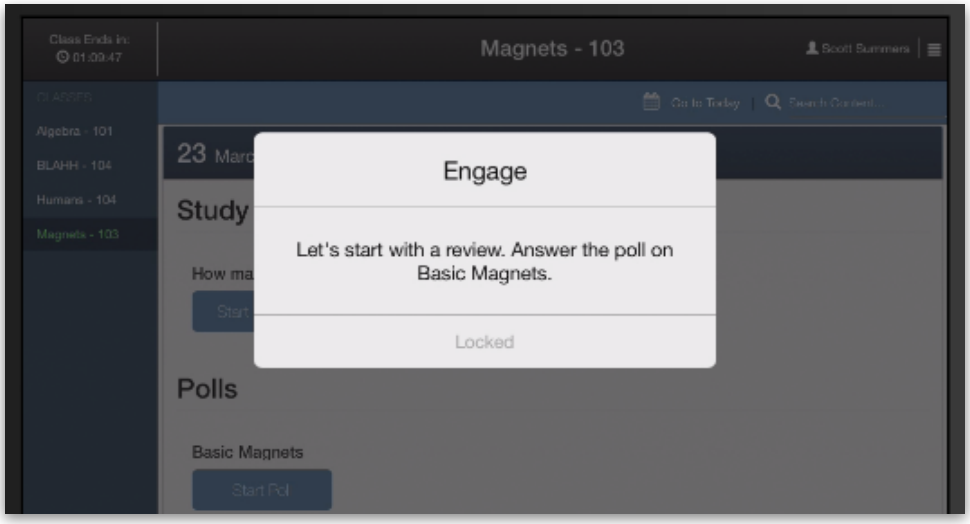
Max can set the finish time to be 0800 (8am - a very early class). Once that happens he sees the students who have checked into the class.

Note some of the indicators on the teacher's view. Anna Marie (username - rogue) is absent, or hasn't checked in. James Howlett (username - wolverine) has checked into the class and is on an OS X device. Scott Summers (username - cyclops) has checked in and is on an iOS device. He is the only one with the **Clear Passcode** button available.

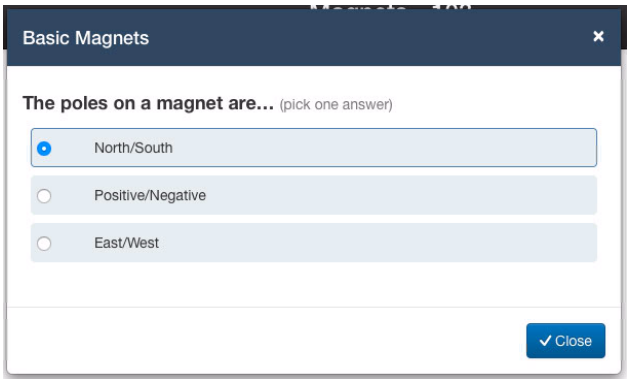
At this point, our teacher Max can send out simple directions to the students, or send an Eyes Up Front message to get everyone on task.



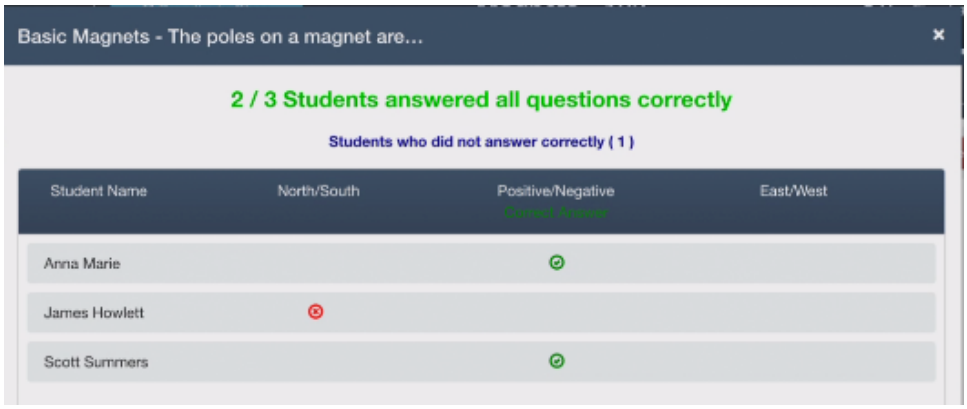
What everyone sees is this:



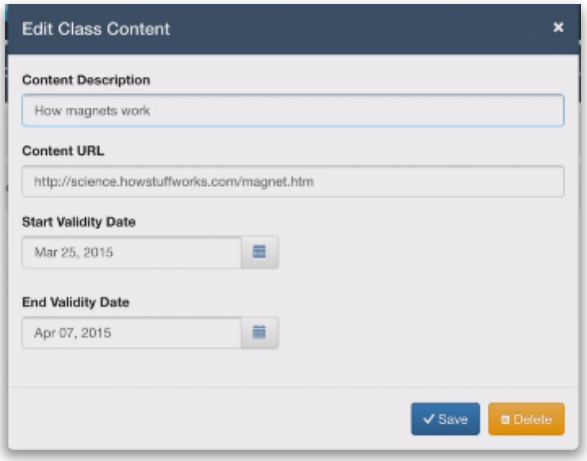
At this point, Max clicks on the **Reset Actions** button to clear the alert, and the students tackle the poll on magnets.



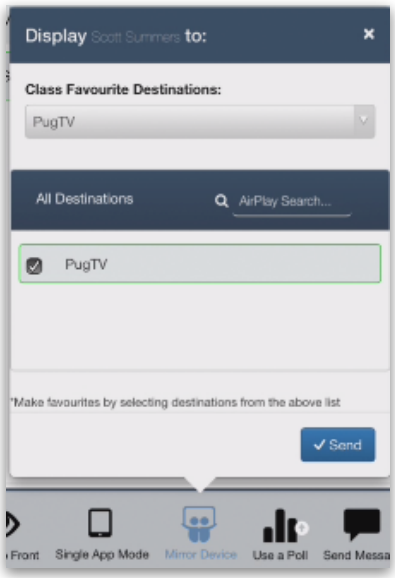
Of course, someone gets the wrong answer, and our teacher sees that right away by checking the poll results.



Since James was not paying attention, Max creates a special content item for him:



While James is working on his study content, Max can ask Scott to show how he found additional research material on magnetic clip on sunglasses by setting Scott's iPad to go into AirPlay mode to the classroom AppleTV.

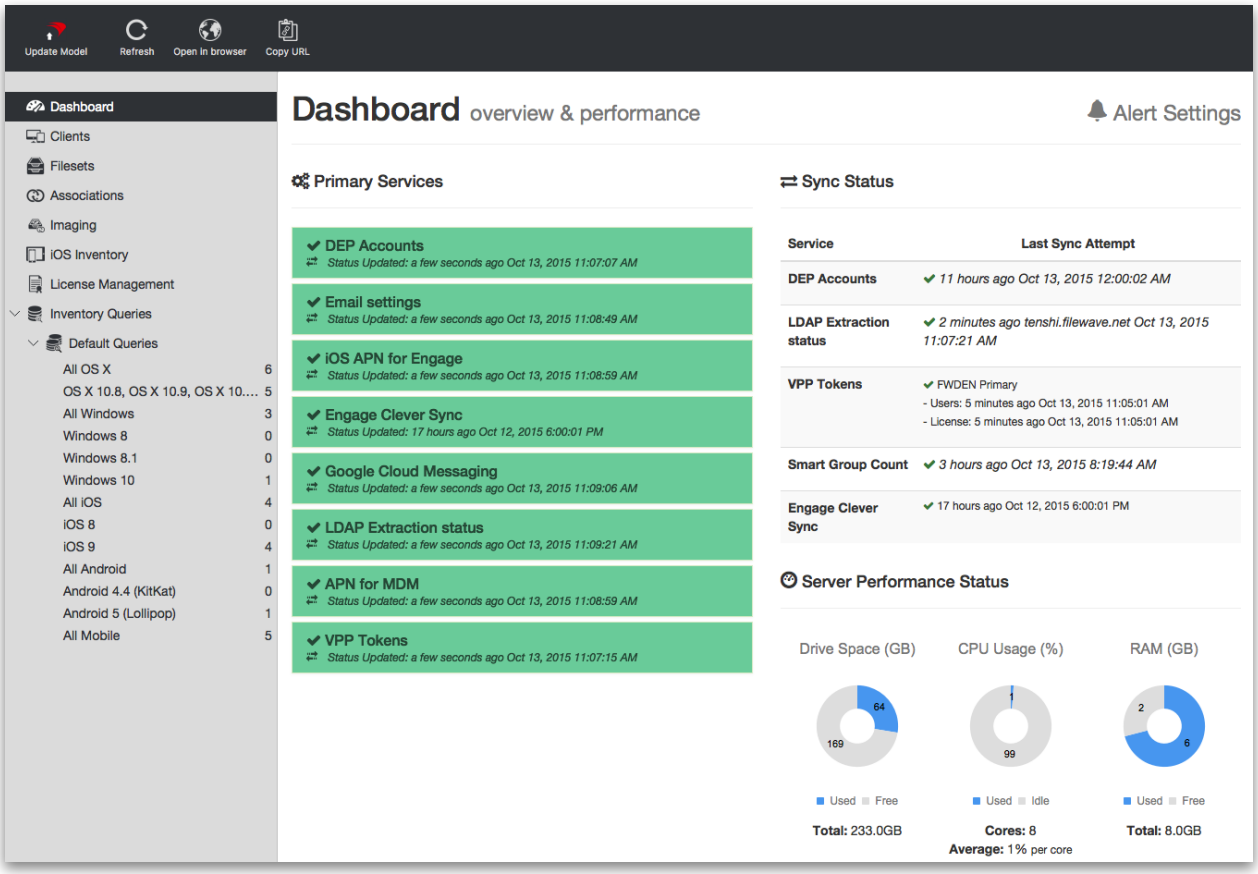


And the process goes on, Max can keep tabs on the students with polls, provide content when needed, and reign in the class when they begin to get off task.

Engage is a teacher's tool, designed for teachers to help them accomplish their most important mission - teaching.

Conclusion

The broad array of features in FileWave support the full spectrum of the deployment lifecycle. With Engage, the curricular folks are now given a solid tool to help reinforce their ability to manage the classroom. FileWave's approach of a unified end point for management that is cross-platform and easy to use is designed to help the IT support staff concentrate on helping their end user community accomplish the mission of their institution or business, without introducing unneeded complexity.



Appendices

A.1. Command Line tools in FileWave

Basic FileWave commands

The basic command line commands in FileWave are based on **fwcontrol:**

fwcontrol

These tasks include starting/stopping/restarting the different components, getting versions, status, and some server activities. **fwcontrol** requires root authorization in order to perform its tasks.

fwcontrol takes commands of the type:

```
(sudo) fwcontrol <component> <command>
```

For example, this command would restart the booster:

```
sudo fwcontrol booster restart
```

This command stops the client service

```
sudo fwcontrol client stop
```

Finally, this command will compact the Server's database:

```
sudo fwcontrol server dbcompact
```

Compacting the Database

The FileWave Server has a built-in database rebuilding feature. In the event of database corruption, perform following command in the Terminal:

```
sudo fwcontrol server dbcompact
```

Server verification

This command rebuilds the database files, which contain all User, Fileset, Associations, and Model information.

```
sudo fwcontrol server stop
sudo /usr/local/sbin/fwxserver -F
```

(enter administrative password)

Automatic Database Backups & Restoration

Every time a model update takes place, a copy of the FileWave database at the new model number is created, compressed, and backed up inside the DB folder:

```
/fwxserver/DB/committed.sqlite_<model number>
```

where "model number" is the number of the new model.

The server automatically stores the last 20 model updates in this folder. At any time, you can choose to restore to one of the previous database models using the following shell commands:

```
sudo fwcontrol server stop
/usr/local/sbin/fwxserver -restore <model number>
sudo fwcontrol server start
```

where <model number> is replaced with the model number you wish to restore to.

Once you start the server, you may log in and the database should be just as it was at the appropriate model update. Note that data files deleted or added will not be restored to their previous condition.

General fwcontrol information

```
> fwcontrol server help

|----------------------|
| Welcome to fwcontrol |
|----------------------|

Usage: (sudo) fwcontrol <component> <command>

Examples:

sudo fwcontrol server stop
sudo fwcontrol client start
sudo fwcontrol booster restart
sudo fwcontrol booster connectedclients
sudo fwcontrol client version
fwcontrol fwgui showKiosk

MDM:

sudo fwcontrol mdm adduser <new_user_name>
sudo fwcontrol mdm addadminuser
sudo fwcontrol mdm initdb

Additional Commands:

sudo fwcontrol server dbcompact
sudo fwcontrol server restore [version]
sudo fwcontrol server resetinventory
sudo fwcontrol client status
sudo fwcontrol postgres start|stop|restart

Inventory:

sudo fwcontrol postoffice stop
sudo fwcontrol scanner fullscan
sudo fwcontrol pinger restart
```

Imaging Virtual Server commands

The key commands for the IVS are based upon **imaging-control** (requires root authorization):

Examples:

```
sudo imaging-control networksetup static
```

```
sudo imaging-control networksetup dhcp
sudo imaging-control subnet add
sudo imaging-control subnet remove
sudo imaging-control increase harddrive
sudo imaging-control list macimages
sudo imaging-control list windowsimages
sudo imaging-control disable macimaging
sudo imaging-control disable windowsimaging
sudo imaging-control enable macimaging
sudo imaging-control enable windowsimaging
```

Configuring the IVS network interface

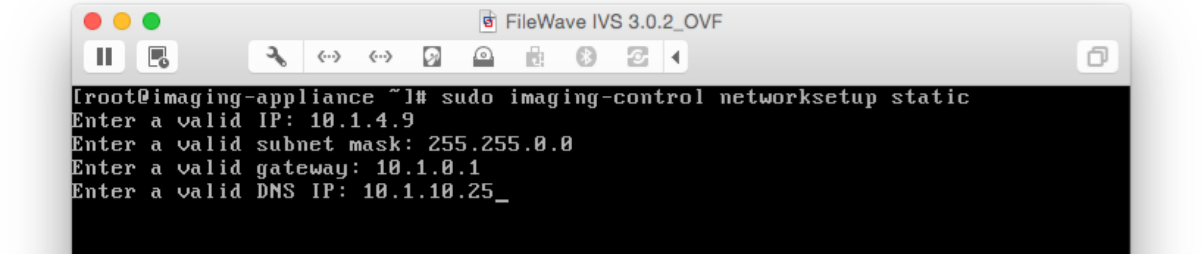
The FileWave IVS network is configured to use dhcp by default. This command has 2 options:

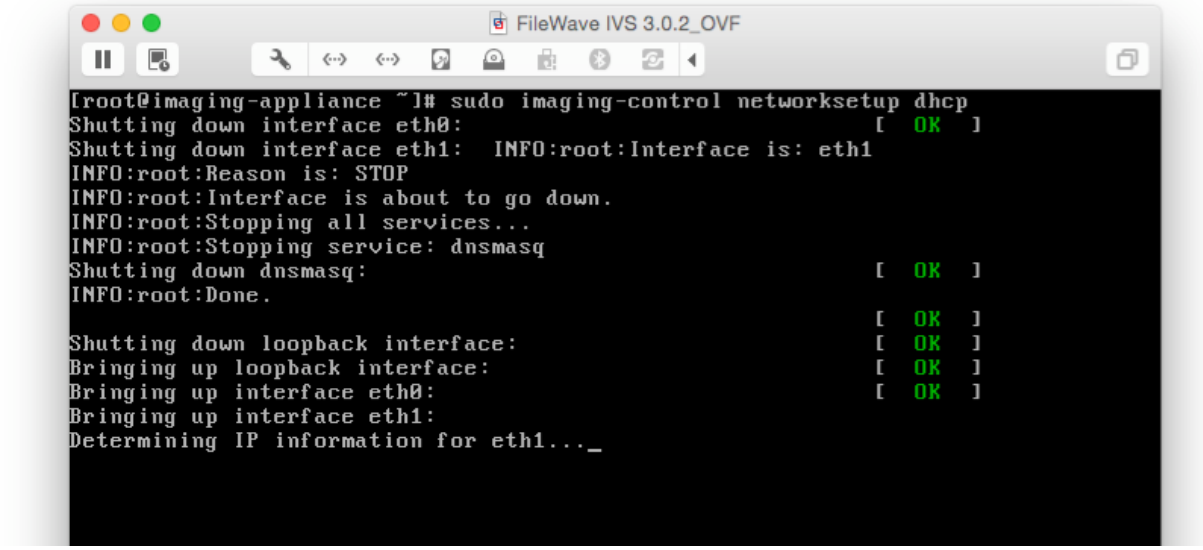
```
sudo imaging-control networksetup static
```

This command will prompt for static ip information and re-configure the network interface.

```
sudo imaging-control networksetup dhcp
```

This command will switch the IVS networking interface back to dhcp.



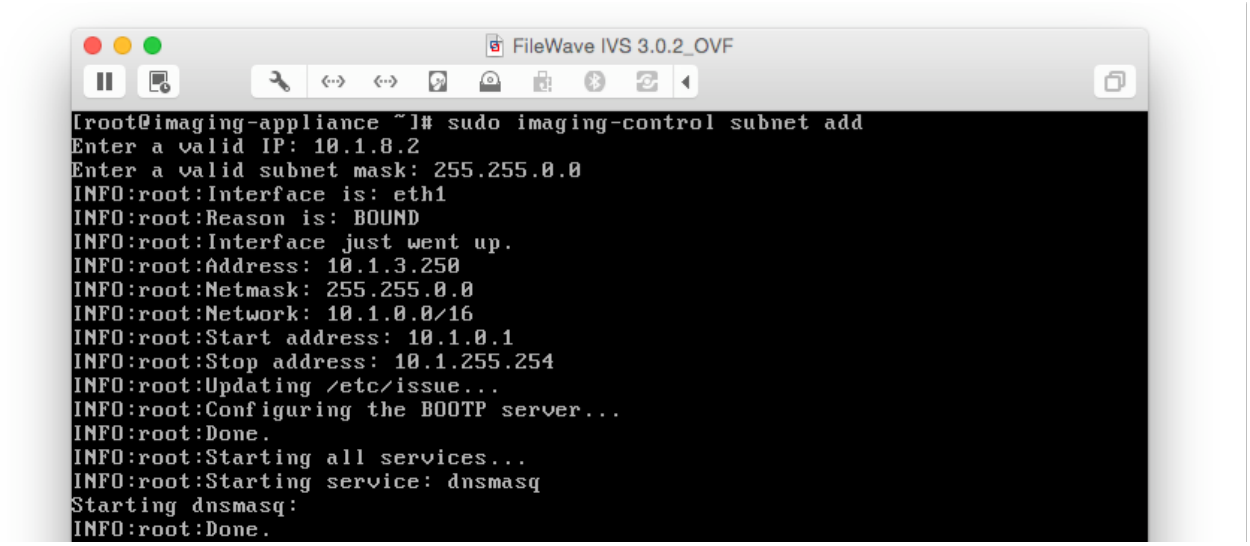


Configuring subnets on the IVS

The FileWave IVS will default to listening only on the subnet that it's ip address is contained within. This command can be used to add subnets for the IVS to listen to or remove subnets:

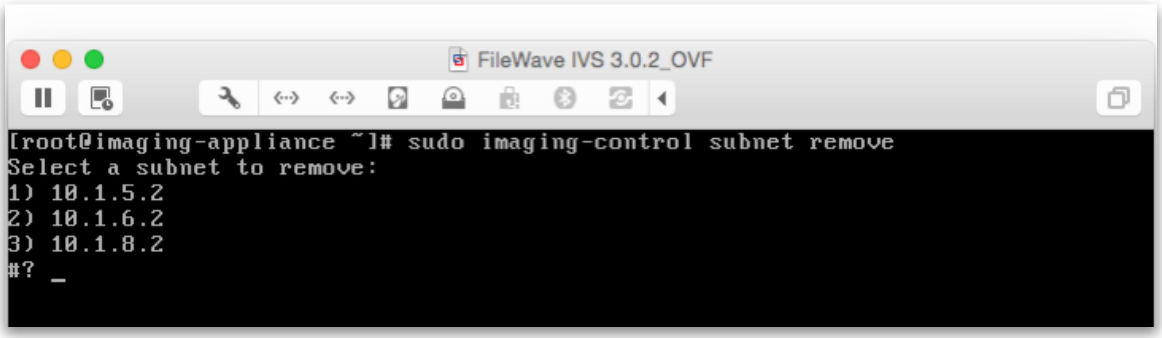
`sudo imaging-control subnet add`

This command will prompt for a valid ip address from the subnet and the subnet mask.



`sudo imaging-control subnet remove`

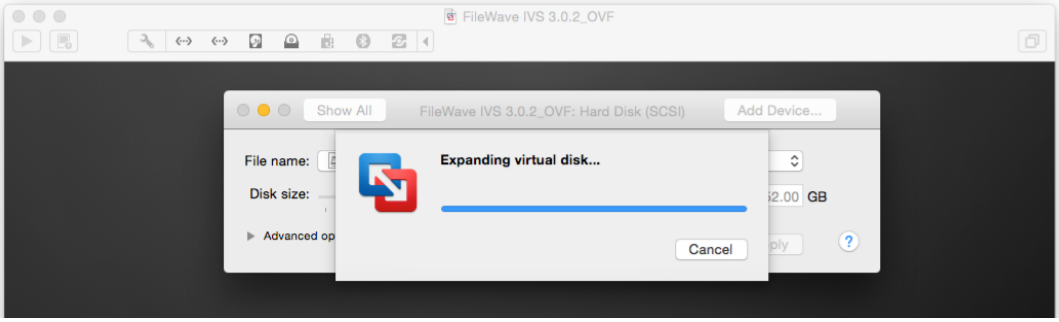
This command will display the subnets that the IVS is currently listening to and allow removal.

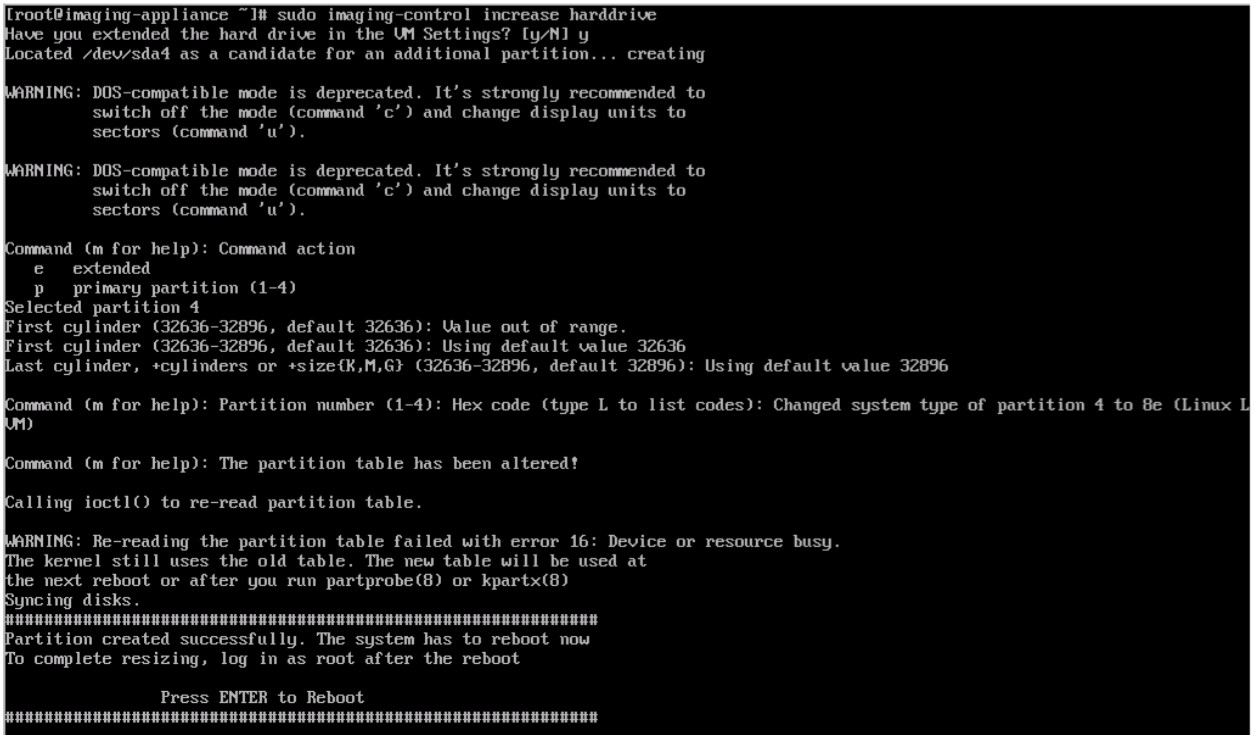


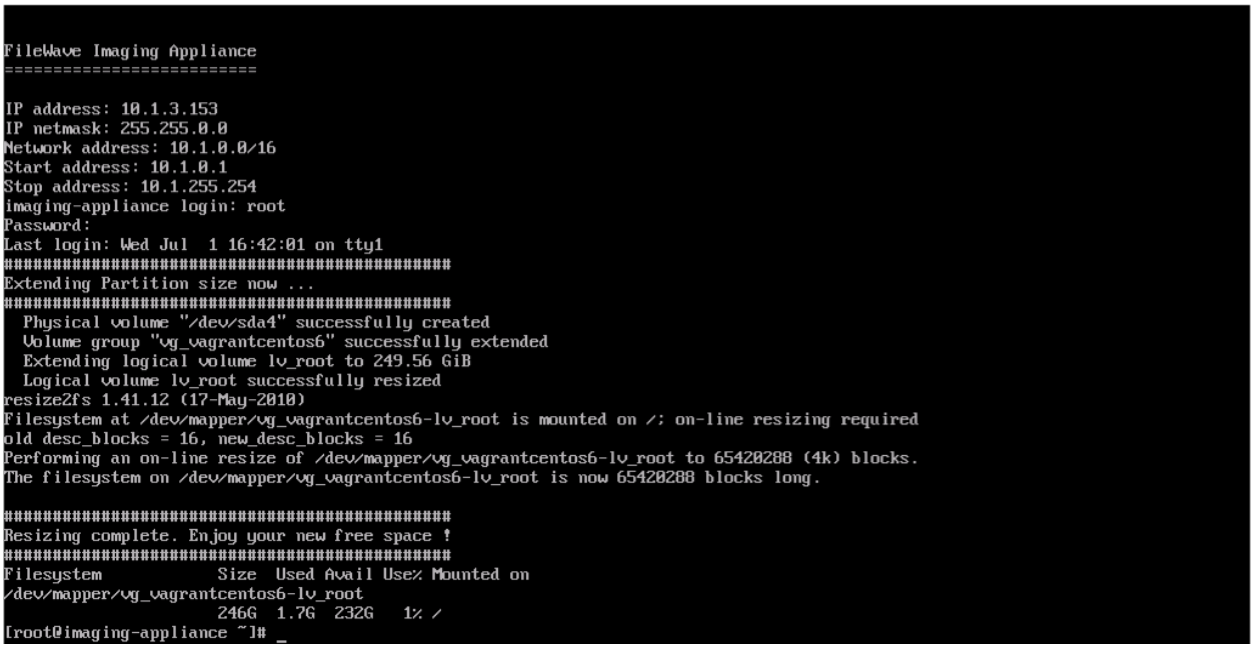
Increasing the IVS hard drive

`sudo imaging-control increase harddrive`

This command will allow the virtual disk on the IVS to be increased. The default size is 250gb. This command will require that the IVS be shutdown and the hard drive expanded in the vm settings.



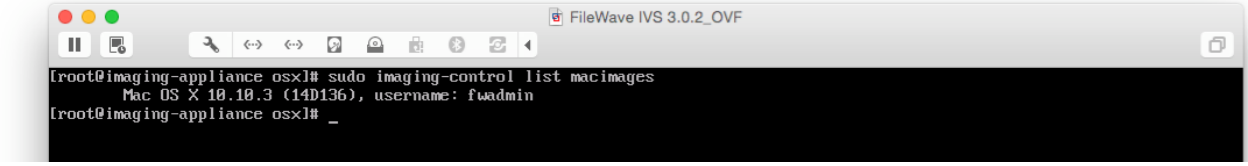




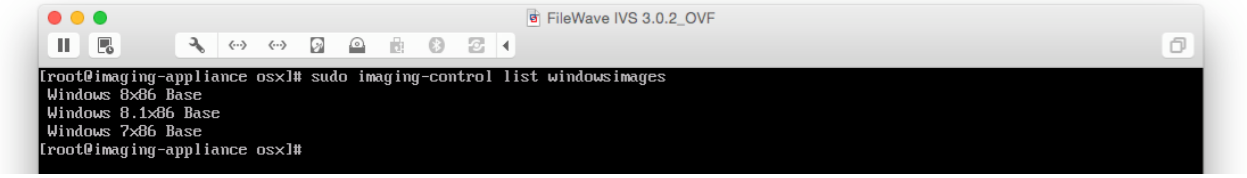
Viewing list of images on IVS

These commands will list Mac and Windows images being hosted on the IVS currently:

```
sudo imaging-control list macimages
```



`sudo imaging-control list windowsimages`



Configuring the IVS for Mac or Windows

The default settings on the IVS allow for Mac and Windows imaging. These commands will allow you to disable/enable Mac or Windows imaging on the IVS.

`sudo imaging-control disable macimaging`

This command disables Mac imaging on the IVS.

`sudo imaging-control disable windowsimaging`

This command disables Windows imaging on the IVS.

`sudo imaging-control enable macimaging`

This command enables Mac imaging on the IVS. (default setting)

`sudo imaging-control enable windowsimaging`

This command enables Windows imaging on the IVS. (default setting)

A.2. FileWave Admin command line access

Starting with FileWave 9.0, some of the administrator features are available via command line.

- End user side
- Exit codes
- Commands (9+)
- Options:

End user side

First open terminal and cd to the directory that the FileWave Admin app is in.
Admin tool can be started by running the Admin executable. For instance, on OS X:

```
./FileWave\ Admin.app/Contents/MacOS/FileWave\ Admin -h
```

will display the help text.

```
Usage: /Applications/FileWave/FileWave Admin.app/Contents/MacOS/FileWave Admin
[options]
FileWave Command Line Tool

Options:
  -h, --help                Displays this help.
  -v, --version             Displays version information.
  -u <user>                 The filewave administrator username.
  -p <password>             The filewave administrator password.
  -H <host>                 The filewave server hostname.
  -P <port>                 The filewave server port number (defaults to
                            20016).
  --listClients             Lists all the client client/clone/group
                            information.
  --listFilesets            Lists all the Fileset information.
  --createFileset <name>    Creates a new empty Fileset with the specified
                            name.
  --importFolder <path>     Imports a folder as a Fileset (not as a package).
  --importPackage <path>    Imports a package (pkg, flat, mpkg or msi) as a
                            Fileset.
  --importImage <path>      Imports an image as a Fileset.
  --deleteFileset <id>      Deletes a Fileset by ID.
  --listAssociations        Lists all the associations held in the system.
  --createAssociation       Create an association between a client/clone/group
                            ID and a Fileset ID.  Use the --clientgroup_id and
                            --fileset_id options.
  --deleteAssociation <id>  Deletes an association between a client/clone/group
```

```
                          ID and a Fileset ID.
  --clientgroup_id <id>   The integer ID value of a client, clone or group
                          object.
  --fileset_id <id>       The integer ID value of a Fileset object.
  --kiosk                 Make this a kiosk association.
  --software_update       Make this a software update association.
  --updateModel           Updates the FileWave model (as long as no other
                          admins have locked objects).
  --name <name>           The name value which will be applied to any newly
                          created object.
  --comment <comment>     The comment value which will be applied to any
                          newly created object.
  --target <id>           The ID of the target container, if not specified
                          all objects are created in their respective root
                          container.
  --listExitCodes         Lists all exit codes and their description.
** You are seeing this because the -h option was used **
```

You always need to provide connection details:

```
-u user -p <password> -H <host>
```

for instance:

```
-u fwadmin -p <password> -H tenshi.filewave.net
```

Running admins

Any running administrator with the same credentials will be kicked out. The command line tool is doing the same thing as if you launched the GUI Admin app and logged in.

Exit codes

A successful command will return 0 as an exit code.

--listExitCodes option will list currently available options:

Exit codes in 9+

```
0: No Error
100: Unknown Error
101: The given Fileset does not exist
102: The given client does not exist
103: The given group does not exist
104: The given target is not a group
105: Database internal error
```

```
106: Error while uploading Fileset
107: Error while updating the model
108: Login Error
109: Error while importing a Fileset
110: Package Type not supported for import
111: Command line parse failed
```

Commands (9+)

```
-h, --help #Displays this help.
```

Displays list of available commands.

```
-v, --version #Displays version information. Displays FileWave's version.

--listClients #Lists all the client user/clone/group information.
```

Returns a JSON list of clients and groups:

```
id: ucgid
name: name
parent_id: parent id
type: (client, group, clone)
children: for groups, list of children

--listFilesets #Lists all the Fileset information.
```

Returns a JSON list of filesets and filesets groups:

```
name: name
parent_id: parent id
type: (Fileset, group)
size: for Fileset, content size
children: for groups, list of children

--createFileset <name> #Creates a new empty Fileset with the specified name. Returns
"new Fileset xxx created with name 'xxx' “
```

--comment and --target options can be used.

```
--importFolder <path> #Imports a folder as a Fileset (not as a package).
```

Returns "a new Fileset with ID xxx was created with a name 'xxx' "
Displays progress during import.
--name --comment and --target options can be used.

```
--importPackage <path> #Imports a package (pkg, flat, mpkg or msi) as a Fileset.
```

Returns a new Fileset with ID xxx was created with a name 'xxx' "

Displays progress during import.

--name --comment and --target options can be used.

```
--deleteFileset <id> #Deletes a Fileset by ID.
```

--listAssociations Lists all the associations held in the system.

Returns JSON array with associations

```
assoc_id : association id
client_id: client / group id
fileset_id : Fileset / Fileset group id
kiosk: true if kiosk association
sw_update: true if software update association
--createAssociation #Create an association between a user/clone/group ID and a Fileset
ID. Use the --clientgroup_id and --fileset_id options.
```

--clientgroup_id and --fileset_id options MUST be provided.

--target, --kiosk, --software_update options can be used

```
--deleteAssociation <id> #Deletes an association between a user/clone/group ID and a
Fileset ID.

--updateModel #Updates the FileWave model (as long as no other admins have locked
objects).

--listExitCodes #Lists all exit codes and their description.
```

Options:

```
-u <user> #The filewave administrator username.
-p <password> #The filewave administrator password.
```

Authentication options

```
-H <host> #The filewave server hostname.
-P <port> #The filewave server port number (defaults to 20016).
```

Connectivity options

```
--clientgroup_id <id> #The integer ID value of a client, clone or group object. Allows
to specify a client/group.
```

Used in --createAssociation

`--fileset_id <id> #The integer ID value of a Fileset object. Allows to specify a Fileset/ Fileset group.`

Used in --createAssociation

`--kiosk #Make this a kiosk association.`

Used in --createAssociation

`--software_update #Make this a software update association.`

Used in --createAssociation

`--name <name> #The name value which will be applied to any newly created object.`

--comment <comment> The comment value which will be applied to any newly created object.

Allows to specify name (and comment) when using --importFolder and --importPackage command. If not used, default name based on folder or package and empty comment will be used.

`--target <id> #The ID of the target container, if not specified all objects are created in their respective root container.`

Allows to specify the parent container (group) when creating a Fileset.

A.3. MDM Certificate Management

When setting up your MDM service in FileWave, you will need to generate certificates for use in enrolling and managing devices. The flowing section has the procedures for generating and adding those certificates for installations of OS X, Windows and Linux.

MDM Certificate Generation for OS X

The FileWave MDM Server requires two certificates - one to send push commands to Apple and another for iOS devices to communicate securely with the FileWave (MDM) Server.

Apple Push Notification System (APNS) Certificate

1. Open **Keychain Access.app** from Macintosh HD > Applications > Utilities > Keychain Access.app
2. Start the Keychain Assistant by selecting the **Keychain Access** menu
3. Select **Certificate Assistant > Request a Certificate From a Certificate Authority...**
4. Enter your email and a common name (ex. *FW push cert*), and change Request is to **Saved to disk** (the CA Email Address is not required)
5. Click Continue and save to your desktop.
6. Go to http://www.filewave.com/pushcert and log in with your FileWave.com user name. (Your username is not always your email address)
7. Click on “Manage Certificate” under the “Support” menu
8. Browse to and submit the request on your desktop
9. Download the signed request.
10. Go to https://identity.apple.com/pushcert and log in with an Apple ID (You cannot use any account being associated with VPP purchases.)
11. Click the “Create a Certificate” button and upload the signed csr downloaded from the FileWave site.
12. Download the MDM_ FileWave (Europe) Gmbh_Certificate.pem
13. Open the MDM_ FileWave (Europe) Gmbh_Certificate.pem in **Keychain Access.App/File/Import Items…** If prompted, add it to the login keychain.
14. With **login** selected under keychains and **Certificates** selected under category, toggle the disclosure triangle on the left of the **APSP** certificate you just imported
15. Right-click the private key inside, choose your certificate and select **Export Items…**
16. Do not enter a protect password and save the **Certicates.p12** to your desktop. You should change the name to something you can recognize, such as *FWAPNSCert032016,* or any name that helps you track it.
17. Quit Keychain Access
18. Open **FileWave Admin** and connect to your FileWave Server.
19. Go to the FileWave menu, then to **Preferences**.
20. From the Mobile tab, click **Browse...** in the **iOS Apple Push Notification Certificate** section
21. Select **Certificates.p12** on the desktop.
22. Select **Upload APN Certificate/Key Pair** section
23. Click **OK** to close the window

Note: The APNC expires in 365 days, you should create a reminder of some kind. When it comes time to renew, be sure to use the same Apple ID used in step nine. Creating a new certificate, or creating a certificate

with a different Apple ID, rather then renewing, will require re-enrollment of all devices. You should renew a week or more before expiration.

Mobile Certificate Management (MCM) (FileWave specific)

In this portion, we will create the certificate to facilitate communication between your FileWave MDM server and your iOS devices.

1. Open FileWave Admin and connect to your FileWave Server.
2. Go to the FileWave menu, then to **Preferences**.
3. From the Mobile tab, enter the **FQDN** (Fully Qualified Domain Name) of the server into the “MDM Server Address” and the “Server DNS Name”.
4. Click **Generate Self-Signed Certificate** and enter the *fwadmin* credentials (default password is *filewave*).
5. Click OK to close the window.

Note: Keep in mind that if this certificate is generated again. All devices must be manually re-enrolled to receive the new certificate.

MDM Certificate Generation for Windows

The FileWave MDM Server requires two certificates - one to send push commands to Apple Inc. and another for iOS devices to communicate securely with the MDM Server.

Apple Push (APNS)

Evaluation users, make sure you have applied for an evaluation account (http://www.filewave.com/eval) first.

1. Go to http://www.openssl.org/related/binaries.html and download the appropriate version of OpenSSL for your environment. Win64 OpenSSL v1.0.0k or Win32 OpenSSL v1.0.0k depending on your server architecture. OpenSSL also requires Visual C++ 2008 Redistributable's which are linked to on the OpenSSL download page.

2. From a command prompt type:

```
C:\OpenSSL-Win64\bin\openssl.exe req -out %userprofile%\Desktop\request.csr -new -newkey rsa:2048 -nodes -keyout %userprofile%\Desktop\privateKey.key -config C:\OpenSSL-Win64\bin\openssl.cfg
```

You will be prompted to enter some information for your certificate request. Resulting in a **request.csr** and a **privateKey.key** on your desktop

3. Go to *http://www.filewave.com/pushcert* and log in with your FileWave.com user name. (Your username is not always your email.)

4. Click on **Manage Certificate** under the “Support” menu and upload the **request.csr** from your desktop.

5. Go to https://identity.apple.com/pushcert and log in with an Apple ID (You can not use any account being associated with VPP purchases.)

6. Click the **Create a Certificate** button and upload the signed csr downloaded from the FileWave site.

7. Download the MDM_ FileWave (Europe) Gmbh_Certificate.pem.

8. From a command prompt type:

```
C:\OpenSSL-Win64\bin\openssl.exe pkcs12 -export -in %userprofile%\Downloads\MDM__FileWave_(Europe)_ Gmbh_Certificate.pem -inkey %userprofile%\Desktop\privateKey.key -out %userprofile%\Desktop\push_cert.p12 -name fw-apns
```

You will be prompted to enter an export password, which you can leave blank. This will merge the MDM_ FileWave (Europe) Gmbh_Certificate.pem in the downloads folder with the privateKey.key from step two on your desktop resulting in a push_cert.p12 on your desktop.

9. Open FileWave Admin and connect to your FileWave Server.

10. Go to the FileWave menu, then to **Preferences**

11. From the Mobile tab, click **Browse** in the in the **APNC** section

12. Select **push_cert.p12** on the desktop.

13. Select **Upload APN Certificate/Key Pair** section

14. Click **OK** to close the window

The final steps will be done in FileWave Admin. See section **3.3.6.** on setting up VPP preferences for more information.

Note: The APNC expires in 365 days, it is recommend that you create a reminder of some kind. When it comes time to renew, be sure to use the same Apple ID as step nine. Creating a new certificate, or creating a certificate with a different Apple ID, rather then renewing, will require re-enrollment of all iOS devices.

MDM Certificate Generation for Linux

The FileWave MDM Server requires two certificates - one to send push commands to Apple Inc. and another for iOS devices to communicate securely with the MDM Server.

Apple Push (APNS)

Evaluation users, make sure you have applied for an evaluation account (http://www.filewave.com/eval) first.

1. Open SSL is required and should have been installed as a dependency for FileWave Server. The Firefox web browser will need to be installed as well.

2. From a command prompt type:

```
yum install firefox
```

3. From a command prompt type:

```
openssl req -out request.csr -new -newkey rsa:2048 -nodes -keyout priv.key
```

Resulting in a **request.csr** and a **privateKey.key**

4. Using Firefox, go to *http://www.filewave.com/pushcert* and log in with your FileWave.com user name. (Your username is not always your email.)

5. Click on **Manage Certificates** under the “Support” menu and upload the **request.csr** file.

6. Go to *https://identity.apple.com/pushcert* and log in with an Apple ID

(You can not use any account being associated with VPP purchases.)

7. Click the “Create a Certificate” button and upload the signed csr downloaded from the FileWave site.

8. Download the **MDM_ FileWave (Europe) Gmbh_Certificate.pem**

9. From a command prompt type: openssl pkcs12 -export -in MDM_ FileWave (Europe) Gmbh_Certificate.pem -inkey priv.key -out push_cert.p12 -name fw-apns

This will merge MDM_ FileWave (Europe) Gmbh_Certificate.pem with the privateKey.key from step three resulting in push_cert.p12

The final steps will be done in FileWave Admin. See section **3.3.6.** on setting up VPP preferences for more information.

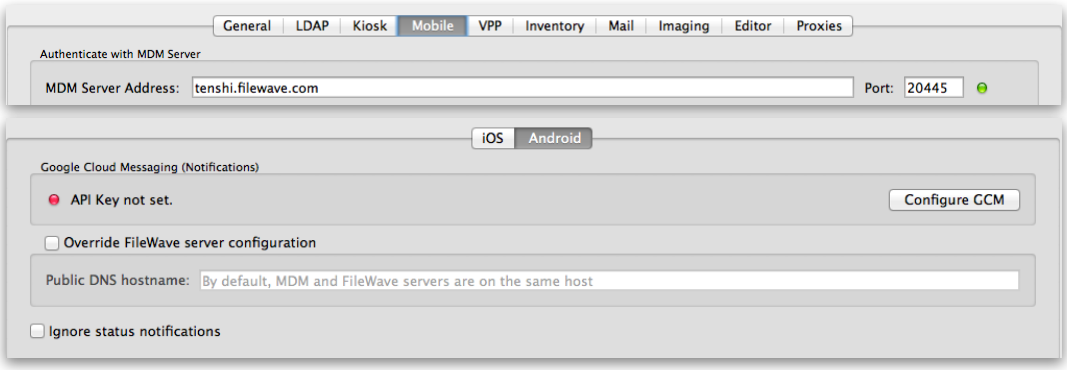
Note: The APNC expires in 365 days, it is recommend that you create a reminder of some kind. When it comes time to renew, be sure to use the same Apple ID as step nine. Creating a new certificate, or creating a certificate with a different Apple ID, rather then renewing, will require re-enrollment of all iOS devices.

A.4. Configuring Google Cloud Messaging (GCM) for Android

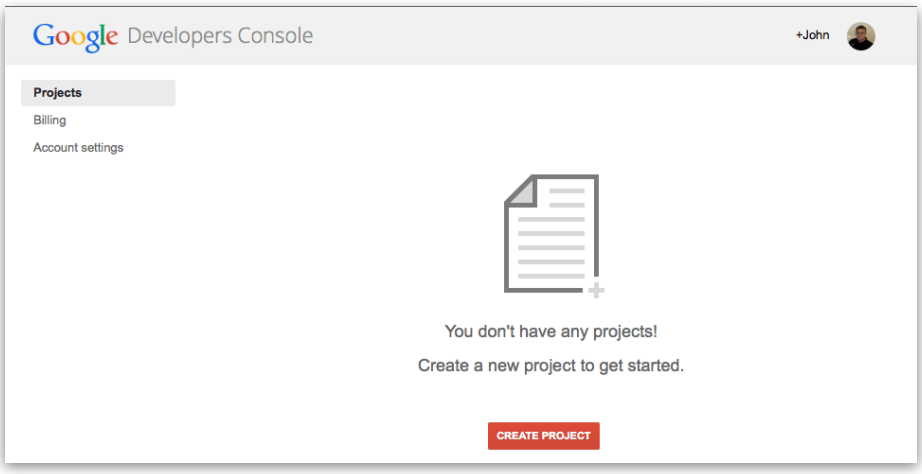
In order to bring Android devices into the FileWave server and provide MDM services, you need to set up a messaging and notification system. The Google Cloud Service will allow the FileWave server to contact the Android devices and provide Filesets as needed. Follow the steps here to create the proper credentials so you can configure your FileWave server for Android support.

Getting a Project Number

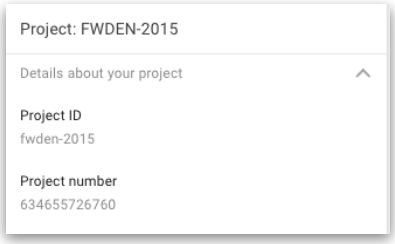
FileWave needs a Project Number and a server API key in order to support Android.



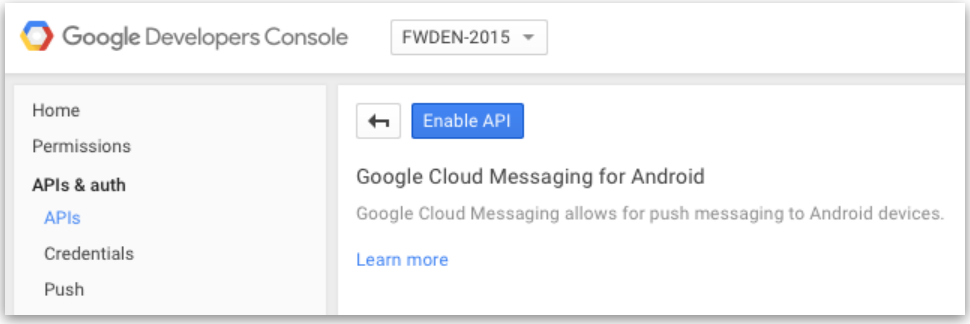
Log onto https://cloud.google.com/console/project



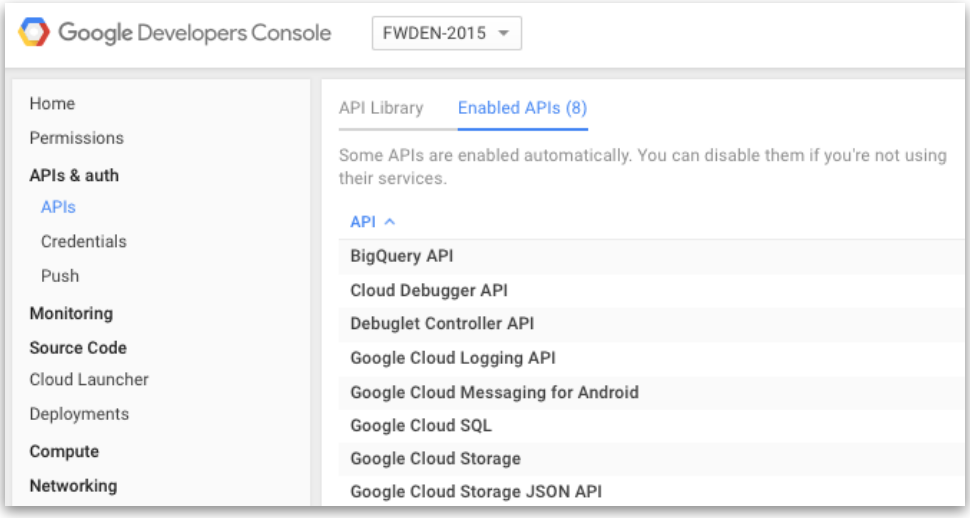
Select *CREATE PROJECT* and fill in the fields with a Project name (should have something to do with your institution). In a few seconds, you will get a project ID:



Select **APIs & auth / APIs** from the sidebar:

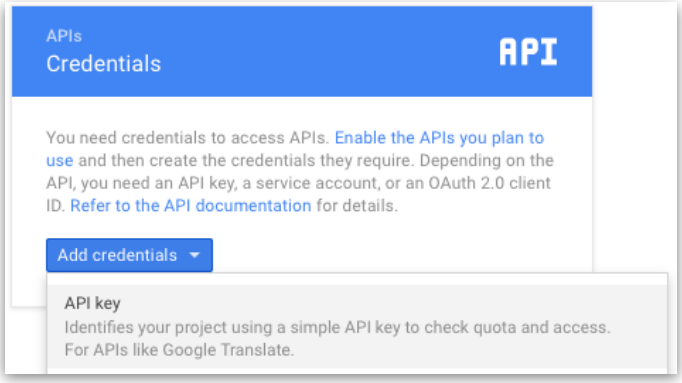


Enable the Google Cloud Messaging for Android (GCM) API. You will be able to see your active APIs.

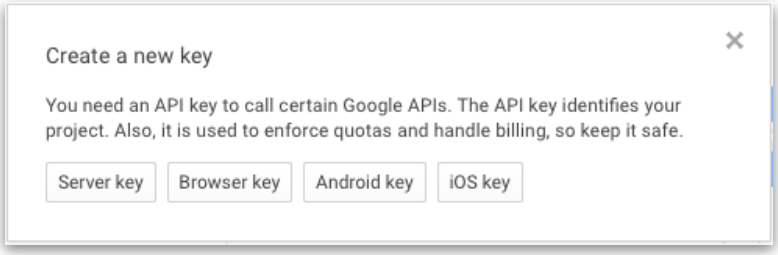


Create a Public Access API key

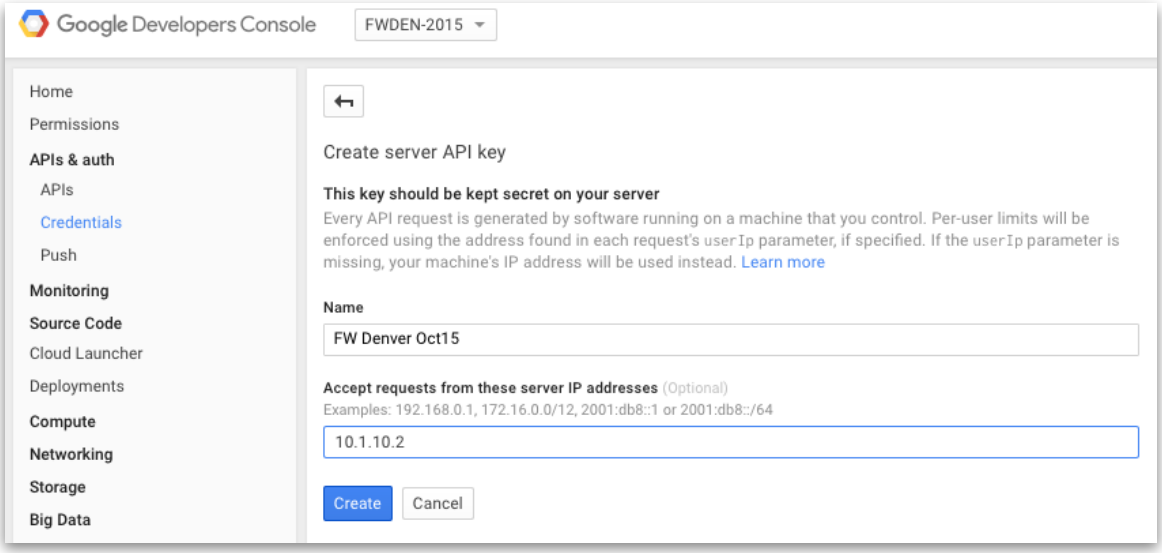
Next, click on the **Credentials** link, then on the *Add credentials* menu, and choose API Key.



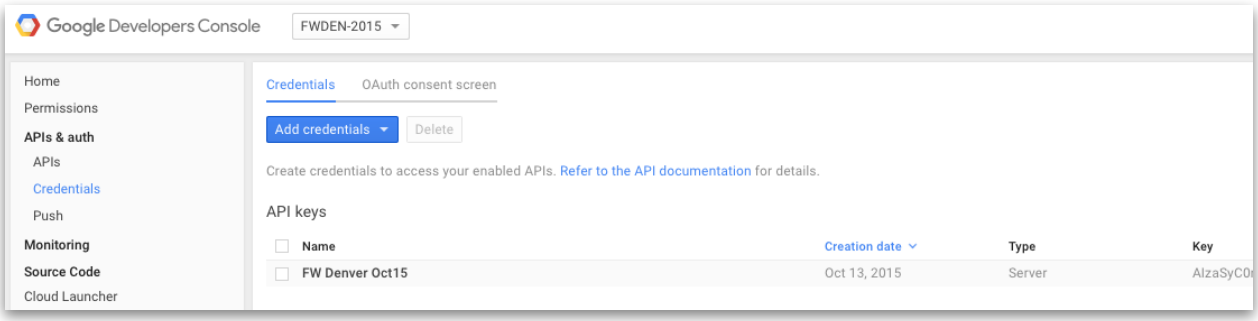
In the dialog box that pops up, choose “Server key”…



You will be presented with a dialog box asking you to enter the IP address(es) that will be used to contact your MDM server. You should enter both internal and external addresses used, if necessary.



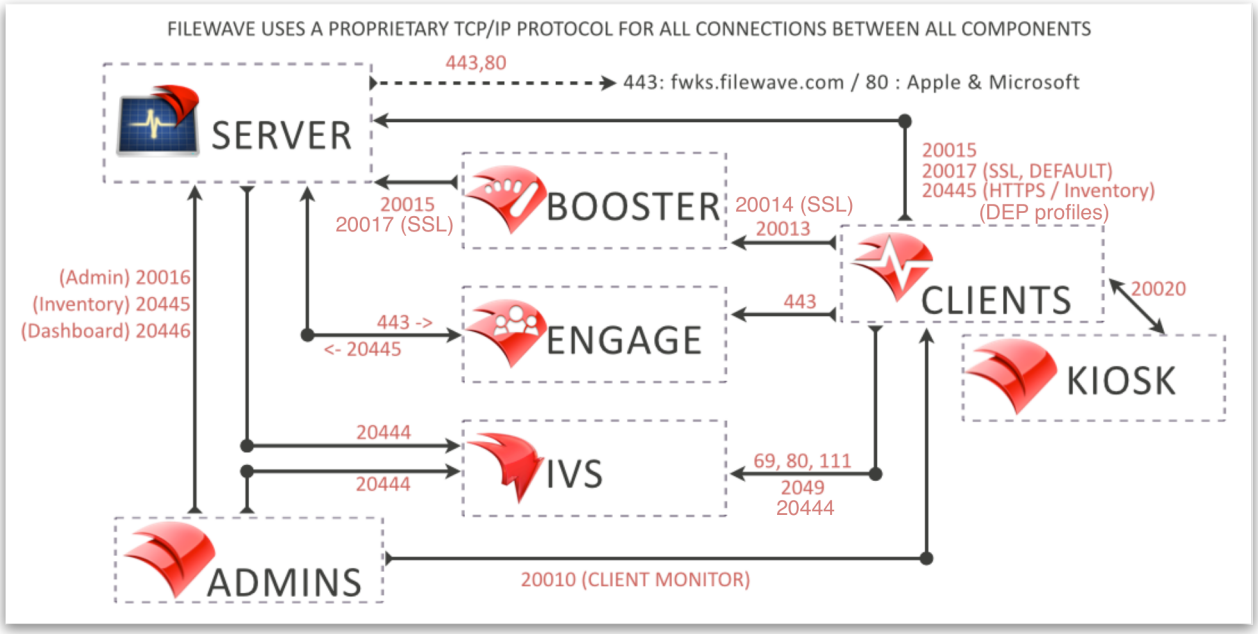
At this point, you are done and have your API key. Copy that information and store it with your Project Number.



You can always log back into the site and get your project number and server key.

You can now go into FileWave Admin and configure your Android MDM service.

A.5. Network Ports reference



FileWave Server and Booster TCP/IP Server Settings

Preferences for controlling the low level network settings timeouts and number of open sockets for the FileWave Server and Booster can be found in their settings files. Consult with a FileWave Support Engineer before making changes to these settings. The settings can be found at:

Mac OS

/Library/Preferences/com.filewave.fwxserver.plist

/Library/Preferences/com.filewave.fwbooster.plist

Windows Registry

HKEY_LOCAL_MACHINE\Software\FileWave\fwxserver

HKEY_LOCAL_MACHINE\Software\FileWave\fwbooster

Linux

/etc/xdg/filewave/fwxserver.conf

/etc/xdg/filewave/fwbooster.conf

FileWave TCP/IP Port Usage

By default the FileWave software uses these TCP/IP ports listed below. These are the defaults and they can be configured to listen on different ports if required. New ports numbers (version 10+) are in red.

Any updates or changes will be posted to: http://www.filewave.com/kb/tcp

FileWave Client Ports

20010 TCP/IP incoming for administrator-client (Client Monitor: OS X, Windows & Android)
20020 TCP/IP local loopback for fwgui process to fwcld process (Kiosk)

FileWave Server Ports

80 TCP/IP outgoing for FileWave Software Updates (apple.com & microsoft.com)
443 TCP/IP outgoing for FileWave License Server (fwks.filewave.com)

20015 TCP/IP incoming for client-server
20016 TCP/IP incoming for administrator-server

20017 TCP/IP incoming for client-server secure (SSL)
20445 TCP/IP incoming for client-server inventory

FileWave MDM ports

2195 TCP/IP outgoing port used to send APNs to Apple's server (17.0.0.0/8)
5223 TCP/IP outgoing port used by IOS devices to connect to Apple's APN server (17.0.0.0/8)
5228,5229 & 5230 TCP/IP outgoing ports, server to Google push, mobile to Google push (android.googleapis.com)
20080 TCP/IP incoming non-SSL http port (unused in 5.6 and up)
20443 TCP/IP incoming for mobile-server HTTPS (Android and iOS)
20445 TCP/IP incoming for administrator-server HTTPS

FileWave Booster Ports

20013 TCP/IP incoming for booster-client
20014 TCP/IP incoming for booster-client secure (SSL)

IVS (imaging) Ports

67 (DHCP)
69 (TFTP)
80 (HTTP) and 20444 (HTTPS) during a restore operation
22 (SCP) incoming for image uploads
111 (TCP,UDP) and 2049 (TCP,UDP) are used for NFS access

FileWave PostOffice Ports

20030 TCP/IP for Scanner and PostOffice communication

FileWave Inventory Web Server

80 TCP/IP for Web Server Access

FileWave VNC / Remote Control Relay Ports and default settings

FW Server

20005 publish port

20006 router port (not directly configurable - always publish port + 1)

20030 VNC relay

Booster

20003 publish port

20004 router port (not directly configurable - always publish port + 1)

Client

20031 VNC server port

managed VNC: true

prompt for screen control: true

A.6. Upgrading your FileWave server

There is a sequence of events that should be followed in order to properly upgrade a FileWave server and the rest of the FileWave architecture. The steps listed below are considered "**best practice**".

1) We recommend shutting the server down using

```
sudo fwcontrol server stop
```

Then taking a Database Backup using

```
cp -rp /fwxserver/DB /fwxserver/DB<_give it a name or datetime group>
```

Then locking all your clients as per best practice

```
sqlite3 /fwxserver/DB/server.sqlite 'update user set status = 1;'
```

Then you can run the ***rpms***.

After that, the server will be up and running again automatically.

2) Please update your FileWave administrator to the same version as the server, connect to it and run model update once you're convinced everything looks as it should. After that, unlock a test client by right-clicking it and observing it for 15-20 Minutes to make sure it doesn't do anything unexpected.

During those 15-20 minutes, please download and import the Client Upgrade Fileset of the same version , available on the download page where you got the ***rpms*** as well as the Admin.

After you're sure the client is behaving, associate the client upgrade Fileset to it, and update the model.

Observe for another 15-20 minutes to ensure that clients talking to the server do not produce any unwanted results.

Once that's done, you can associate the client upgrade Fileset to all your clients and unlock them all.

For more details on best practices while upgrading FileWave, please visit :

https://www.filewave.com/index.php/component/maqmahelpdesk/support/kb/article/upgrade-filewave?Itemid=750

A.7. Sample"Create NBI" script

```
#!/bin/sh

# uncomment next line for debugging
set -x

########################################################################
function get_recoverydisk()
{
for disk in `diskutil list | grep "/dev"`; do
	for disk_slice in `diskutil list ${disk} | tail -n+4 | awk '{print$NF}'`; do
		volume_name=`diskutil info -plist /dev/${disk_slice} | /usr/bin/python -c
"import plistlib; import sys; print
plistlib.readPlistFromString(sys.stdin.read()).get('VolumeName')"`

		if [ "$volume_name" == "Recovery HD" ]; then
			recovery_disk="/dev/${disk_slice}"
		fi
	done
done

echo ${recovery_disk}
}

# The script must be run as root
if [ `whoami` != "root" ]
then
	echo "This script must be run as root. Aborting." 1>&2
	exit 1
fi

recovery_disk=`get_recoverydisk`

echo "Recovery disk is: $recovery_disk"

OSX_VERSION=`sw_vers -productVersion | sed -E 's/(([0-9]+)\.([0-9]+)).*/\1/'`

WORKING_DIR=$(
if [ -e "$0" ]; then
	prog=$0
else
	prog=$(command -v -- "$0") || exit
fi
```

```
cd -P -- "$(dirname -- "$prog")" && pwd -P
)

SOURCE_DISK_MOUNTPOINT="/tmp/source-disk"
NBI_DIR="$WORKING_DIR/Image.nbi"

echo "Working in: " "$WORKING_DIR"

# We mount the recovery disk
mkdir -p "$SOURCE_DISK_MOUNTPOINT"
mount -r -t HFS $recovery_disk "$SOURCE_DISK_MOUNTPOINT"

if [ "$?" -ne 0 ]
then
       echo "Could not mount the recovery partition. Exiting." 1>&2
       exit 1
fi

# We need to rm any old output files before we start
rm -rf "$WORKING_DIR"/tmp
mkdir -p "$WORKING_DIR"/tmp/

# We'll do the conversion using a shadow file mount of the base image
SHADOW_FILE="$WORKING_DIR/tmp/img.shadow"
BASE_IMAGE="$SOURCE_DISK_MOUNTPOINT/com.apple.recovery.boot/BaseSystem.dmg"

# In 10.9, for instance, the free space is very small, make it bigger
hdiutil resize -size 1500m -growonly "$BASE_IMAGE" -shadow "$SHADOW_FILE"

# The final mount point depends on the OS X version, so we parse it here
HDI_OUT=$(hdiutil attach -owners on -nobrowse "$BASE_IMAGE" -shadow "$SHADOW_FILE" |
grep '^/dev/disk' | awk -F'\t' '{ print $3; }')

if [ "$?" -ne 0 ]
then
       echo "Could not mount the recovery base system (com.apple.recovery.boot/
BaseSystem.dmg). Exiting." 1>&2
       rm -rf "$WORKING_DIR"/tmp

       # We unmount the recovery disk
       umount $recovery_disk
       exit 1
```

```
fi

OSX_BASE_SYSTEM=$(echo $HDI_OUT | sed -e 's/^\s*//g' -e 's/\s*$//g')

# We create the destination directory and copy needed files from recovery image
mkdir -p "$NBI_DIR"/i386/x86_64
cp "$SOURCE_DISK_MOUNTPOINT"/com.apple.recovery.boot/kernelcache "$NBI_DIR"/i386/
x86_64/
cp "$SOURCE_DISK_MOUNTPOINT"/com.apple.recovery.boot/boot.efi "$NBI_DIR"/i386/booter
cp "$SOURCE_DISK_MOUNTPOINT"/com.apple.recovery.boot/PlatformSupport.plist "$NBI_DIR"/
i386/

# We mount the resources share
mkdir -p /Volumes/resources
mount -t nfs tenshi-fw-img.filewave.net:/imaging/resources /Volumes/resources

# Copy Over bootup_script App
cp -R -v /Volumes/resources/generic/bootup_script.app "$OSX_BASE_SYSTEM/Applications/"

# Make sure bootup_script doesn't have any gatekeeper restrictions
xattr -dr com.apple.quarantine "$OSX_BASE_SYSTEM/Applications/bootup_script.app/"

# Copy Over Lightning App
cp -R -v /Volumes/resources/generic/Lightning.app "$OSX_BASE_SYSTEM/Applications/"

# Make sure Lightning doesn't have any gatekeeper restrictions
xattr -dr com.apple.quarantine "$OSX_BASE_SYSTEM/Applications/Lightning.app/"

# Copy over the taskrunner
mkdir -p "$OSX_BASE_SYSTEM/Library/LaunchDaemons/"
cp -R -v /Volumes/resources/generic/com.filewave.strikeof.lightning.taskrunner.plist
"$OSX_BASE_SYSTEM/Library/LaunchDaemons/"
mkdir -p "$OSX_BASE_SYSTEM/Library/PrivilegedHelperTools/"
cp -R -v /Volumes/resources/generic/Lightning.app/Contents/Library/LaunchServices/
com.filewave.strikeof.lightning.taskrunner "$OSX_BASE_SYSTEM/Library/
PrivilegedHelperTools/"
xattr -dr com.apple.quarantine "$OSX_BASE_SYSTEM/Library/PrivilegedHelperTools/"

# Lightning needs to have images in ImageLibrary. The NFS share on the server will be
mounted in /Volumes/images
# but as the filesystem is readonly, the symlink must be created now to be in the
image
mkdir -p "$OSX_BASE_SYSTEM/Volumes/images"
```

```
mkdir -p "$OSX_BASE_SYSTEM/private/var/root/Library/Application\ Support/FileWave/
Lightning"
ln -s /Volumes/images/ "$OSX_BASE_SYSTEM/private/var/root/Library/Application\
Support/FileWave/Lightning/ImageLibrary"

if [ ! -e /Volumes/resources/$OSX_VERSION/NBImageInfo.plist ]; then
    echo "File /Volumes/resources/$OSX_VERSION/NBImageInfo.plist does not exist. NBI
script can't be generated properly."
    exit 1
fi
cp /Volumes/resources/$OSX_VERSION/NBImageInfo.plist "$NBI_DIR"/NBImageInfo.plist

# Uncomment the line below when Lightning is fixed
#cp /Volumes/resources/$OSX_VERSION/Utilities.plist "$OSX_BASE_SYSTEM/System/
Installation/CDIS/OS\ X\ Utilities.app/Contents/Resources/Utilities.plist

# We synchronize writtings
sync

# We can now unmount the resources share
umount /Volumes/resources

# Find the line where we want to inject
linenumber=$(grep -n "Start the installer, optionally with a custom package"
"$OSX_BASE_SYSTEM/etc/rc.install" | sed -e 's/\:\#.*$//')

# Determine the length of the entire file
rcinstallength=$(wc -l "$OSX_BASE_SYSTEM/etc/rc.install" | awk {'print $1'})

# Calculate the number of lines left after the injection
linesafter=$(echo $rcinstallength - $linenumber | bc)

# Create temporary file with first lines until the one we're injecting at
head -n $linenumber "$OSX_BASE_SYSTEM/etc/rc.install" > "$WORKING_DIR"/tmp/
rc.install.tmp

# Append the stuff we're injecting:
# 1. Mount the NFS image folder (directory created in the image creation step +
symlink for lightning)
# 2. Run bootup_script with correct parameters
cat <<EOF >> "$WORKING_DIR"/tmp/rc.install.tmp
```

```
/Applications/bootup_script.app/Contents/MacOS/bootup_script --shared-key= --root-
url=https://tenshi-fw-img.filewave.net:20444/  > /private/var/tmp/bootup_script.log
2>&1

mount -t nfs tenshi-fw-img.filewave.net:/imaging/images/osx /Volumes/images

launchctl load /Library/LaunchDaemons/com.filewave.strikeof.lightning.taskrunner.plist

EOF

# Append the remainder of the original file to ensure the boot menu works still
tail -n $linesafter "$OSX_BASE_SYSTEM/etc/rc.install" >> "$WORKING_DIR"/tmp/
rc.install.tmp

rm "$OSX_BASE_SYSTEM/etc/rc.install"
mv "$WORKING_DIR"/tmp/rc.install.tmp "$OSX_BASE_SYSTEM/etc/rc.install"

# Set an environment variable for Lightning
touch "$OSX_BASE_SYSTEM/etc/launchd.conf"
cp "$OSX_BASE_SYSTEM/etc/launchd.conf" "$WORKING_DIR"/tmp/launchd.conf
rm "$OSX_BASE_SYSTEM/etc/launchd.conf"
cat << EOF >> "$WORKING_DIR"/tmp/launchd.conf

setenv FILEWAVE_IMAGING_APPLIANCE 1

EOF

mv "$WORKING_DIR"/tmp/launchd.conf "$OSX_BASE_SYSTEM/etc/launchd.conf"

echo "Finalizing the image..."

# Close the Image in order to have shadow conversion work
hdiutil detach "$OSX_BASE_SYSTEM/"

# Finalize the Image
hdiutil convert -format UDZO -o "$NBI_DIR"/NetBoot.dmg "$BASE_IMAGE" -shadow
"$SHADOW_FILE"
chflags nohidden "$NBI_DIR"/NetBoot.dmg

# We unmount the recovery disk
umount $recovery_disk

#remove tmp dir
```

```
rm -rf "$WORKING_DIR"/tmp

# Let's copy the result to the server
mkdir -p /Volumes/netboot
mount -t nfs tenshi-fw-img.filewave.net:/imaging/netboot /Volumes/netboot

rm -rf /Volumes/netboot/NetBoot
mkdir -p /Volumes/netboot/NetBoot/NetBootSP0
xattr -c -r "$NBI_DIR"
cp -r -v "$NBI_DIR" /Volumes/netboot/NetBoot/NetBootSP0/
rm -rf "$NBI_DIR"

# We synchronize writings
sync

# We can now unmount the netboot share
umount /Volumes/netboot
```

A.8. Enabling LDAP authentication and enrollment

This process consists of:
1- Backing up the current config
2- Editing a new config file to properly read the LDAP structure
3- Restarting the Apache Process so it reads the new config file

Getting the files ready

Open a Terminal Window or use SSH to get into the computer running FileWave Server

Gain root credentials

```
sudo -s
```

Enter your login password

Navigate to the FileWave Apache configurations folder:

```
Windows:  C:\Program Files(x86)\FileWave\apache\conf
OS X / Linux: cd /usr/local/filewave/apache/conf/
```

Backup your current mdm_auth.conf by making a copy

```
cp mdm_auth.conf mdm_auth.conf.bac
```

Make a copy of the LDAP example and rename it

```
cp mdm_auth.conf.example_ldap_auth mdm_auth.conf
```

Making the changes

Open *mdm_auth.conf* up using your preferred text editor (**nano mdm_auth.conf** or **vi mdm_auth.conf**). Make the appropriate changes and then save the .conf file.

(You can also use the Finder to locate the file, then drag a copy to your Desktop and edit it with a text editor, such as **TextWrangler**. When done, you will delete the copy in the **.../conf/** folder and replace it with your edited copy.)

Note: Active Directory (AD) by default requires you bind to the directory to read. Many people create a read-only directory account.

It will look like this:

```
<Location /ios/enroll>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll IOS Device"
       AuthLDAPURL "ldap://10.1.10.2:389/cn=Users,dc=tenshi,dc=local?uid"
       Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
```

```
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /ios/device_enrollment_profile>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll IOS Device"
       AuthLDAPURL "ldap://10.1.10.2:389/cn=Users,dc=tenshi,dc=local?uid"
       Require valid-user
        ErrorDocument 401 "Enrollment credentials are needed."
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /ios/dep_enrollment_profile>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll IOS Device"
       AuthLDAPURL "ldap://10.1.10.2:389/cn=Users,dc=tenshi,dc=local?uid"
       Require valid-user
        ErrorDocument 401 "Enrollment credentials are needed."
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /android/enroll>
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Enroll Android Device"
       AuthLDAPURL "ldap://10.1.10.2:389/cn=Users,dc=tenshi,dc=local?uid"
       Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
<Location /android/project_number>
```

```
# This is an example of ldap based user auth
       AuthType Basic
       AuthBasicProvider ldap
       AuthName "Google Cloud Messaging configuration"
       AuthLDAPURL "ldap://10.1.10.2:389/cn=Users,dc=tenshi,dc=local?uid"
       Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
#      LDAPReferrals Off
</Location>
```

Once saved, restart the FileWave Apache process/service:

Windows:
Go to: Services > FileWave, MDM Apache > Select:, Restart

OS X / Linux: /usr/local/filewave/apache/bin/apachectl graceful

Now when a device attempts to enroll (by pressing the Enroll Device option on the site). They will be prompted to enter their username and password from the directory server.

A.9. Dashboard Error messages

The table below matches the various alerts from the Dashboard.

Alert Item	Definition
Free Disk Space	Free disk space on fwxserver (db location). Warning if < 50GB or < 20% Total space, Error if < 25GB or < 10% total space.
CPU Load	CPU Load on fwxserver. Displays value always, no alert.
Google Cloud Messaging	Returns Google Cloud Messaging status. Cached 1 minute. Error if configuration is not correct.
OS X APN for Engage	Returns OS X APN certificate status for Engage. Cached 1 minute. Warning if certificate expires in less than 30 days. Error if certificate is missing, expired, or Root certificate is missing.
Total Disk Space	Total disk space on fwxserver (db location).
Free RAM	Free RAM on fwxserver. Always OK as some systems like OS X will free memory on demand only.
APN for MDM	Returns APN certificate status for MDM. Cached 1 minute. Warning if certificate expires in less than 30 days. Error if certificate is missing, expired, or Root certificate is missing.
VPP Tokens	Returns VPP token(s) status. Cached 5 minutes. Warning if token expires in less than 30 days. Error if token is expired or incorrect.
FileWave Client/Mobile License	Returns License Status. Cached 1 minute. If you have more than 50 licenses: warning if available count goes below 10, error when 0. If you have less than 50 licenses: warning if available count goes below 4, error when 0.
Engage Clever Sync	Information about the last sync from Engage to Clever.com. Warning if last synchronization occured more than 1 week ago, Error if synchronization failed.
Entreprise app file (ipa)	Check ipa status. Cached 1 hour. Warning if .ipa file is local but does not have expected size. Error means .ipa file is not on disk for local .ipa, or not reachable for external .ipa.
DEP Accounts	Returns DEP Accounts status. Cached 5 minutes. Warning if access token expires in less than 30 days. Error if token is expired or incorrect.
Email settings	Returns email settings status. Cached 5 minutes. Error means no connection to SMTP server.
LDAP Extraction status	LDAP Extraction status. Warning if one or more servers have not been contacted yet, Error if there was an error during extraction.
Total RAM	Total RAM on fwxserver.
iOS APN for Engage	Returns iOS APN certificate status for Engage. Cached 1 minute. Warning if certificate expires in less than 30 days. Error if certificate is missing, expired, or Root certificate is missing.
Smart Group Count	Number of evaluated SmartGroups. Warning if last report occured more than 1h ago, error if 2h ago.

A.10. Inventory Components

The following list contains all of the currently accessible Inventory components for creating queries and smart groups:

• ANDROID
gcm registration id
filewave model number
filewave client version
filewave client locked
enroll date
device id
device name
device product name
last check in
current ip address
free disk space
total disk space
serial number
filewave id
filewave client name
department
building
location
monitor id
auth username
unenrolled

• APPLE PROFILES
payload identifier
payload version
payload display name
payload description
payload organization
payload removal disallowed
has removal passcode
is encrypted

• APPLICATION
name
vendor
version
short version
path
product id
size
install size

install date
times launched
total time used
average time used
first launch date
last launch date
last quit date

• DESKTOP DEVICE
cpu count
cpu speed
cpu type
device manufacturer
RAM size
rom bios version
filewave model number
filewave client version
filewave client locked
device id
device name
device product name
last check in
current ip address
free disk space
total disk space
serial number
filewave id
filewave client name
department
building
location
monitor id
auth username
unenrolled

• FILESET
Fileset id
name
version
install size
install date
kiosk

• FONT
name

family
kind
vendor
version
path
valid
enabled

• iOS DEVICES
product
model
battery level
product name
meid
languages
locales
apple device id
organization info
itunes store account is active
is supervised
is device locator service enabled
is do not disturb in effect
is activation lock enabled
eas device identifier
enroll date
device id
device name
device product name
last check in
current ip address
free disk space
total disk space
serial number
filewave id
filewave client name
department
building
location
monitor id
auth username
unenrolled

• iOS CARRIER SETTINGS
carrier settings version
current carrier network

current mcc
current mnc
data roaming enabled
iccid
imei
modem firmware version
phone number
sim carrier network
simcc
simnc
cellular technology
is roaming
subscriber mcc
subscriber mnc
subscriber carrier network
voice roaming enabled
ethernet macs
personal hotspot enabled

• iOS PASSCODE SETTINGS
allow simple
force pin
manual fetching when roaming
max failed attempts
max grace period
max inactivity
max pin age in days
min complex chars
min length
pin history
require alphanumeric

• iOS RESTRICTIONS
allow adding game center friends
allow app installation
allow assistant
allow camera
allow cloud backup
allow cloud document sync
allow explicit content
allow global background fetch when roaming
allow in app purchases
allow itunes
allow multiplayer gaming
allow photo stream

allow safari
allow screen shot
allow untrusted tls prompt
allow video conferencing
allow voice dialing
allow you tube
force encrypted backup
force itunes store password entry
rating apps
rating movies
rating tv shows
safari accept cookies
safari allow auto fill
safari allow java script
safari allow popups
safari force fraud warning

• iOS SECURITY SETTINGS
hardware encryption caps
passcode present
passcode is compliant
passcode is compliant with profiles

• NETWORK INTERFACE
interface name
mac address
network name
current

• NETWORK IP ADDRESS
ip address
ip version

• OPERATING SYSTEM
OS name
type
version
build
edition

• STATUS MESSAGES
context
date
description
severity

• VPP LICENSE
itunes id
product name
product version
developer
itunes url
artwork url
category
release date
bundle identifier
bundle size
languages
ipod screenshots
ipad screenshots
itunes lookup locale
price
currency
formatted price
platform
License identifier
iTunes App identifier
License irrevocable flag
Pricing parameter
Product type identifier
Product type name
status
Last date used

• VPP USER
Local user identifier string
LDAP user name
first name
last name
email
iTunes store identifier hash
status
User identifier
First registration date
The invitation URL