Management manual

FileWave Administration
Planning, Setup, Installation and Operation

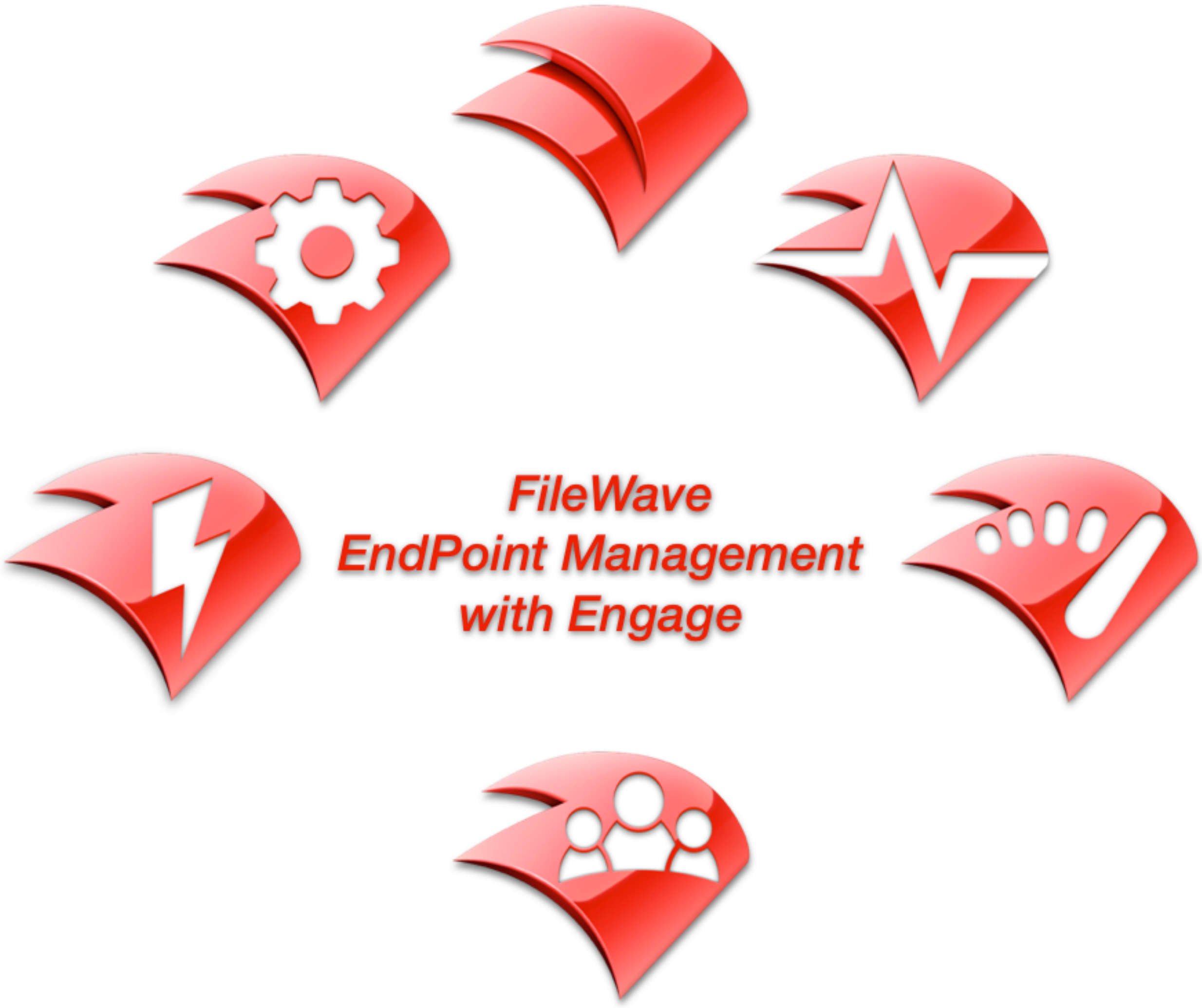


Image / Deploy / Manage / Maintain / Engage

This manual is a living document which will continually be updated to give you the latest information for FileWave and all of its components. Accessing the manual through the FileWave Knowledge Base will allow you to always have the newest information at your fingertips. The manual is exported as a PDF two weeks after a new FileWave release is made, which can be found below under: **Exported Manual Versions (PDF)**.

The FileWave manual will describe all features of FileWave, examples, and other important information. Step by step guides on how to configure each specific setting will be linked in the manual to a KB article.

> **Online Manual vs. PDF Manual**
> It is recommend to access the live manual online, so you always have the latest information when it's available. It is possible that a change to the manual can happen a week after the PDF is made available from FileWave, at which point the PDF is already out of date compared to the online version.

Exported Manual Versions (PDF):

Click here for the latest and past archived versions of the FileWave Manual

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 - Installation and configuration of the FileWave servers, including Imaging and Engage VMs
- Chapter 3 - Installation and configuration of FileWave Boosters
- Chapter 4 - Installation and configuration of the FileWave Client plus Apple's Device Enrollment Program (DEP)
- Chapter 5 - Working with Filesets for application, ebook and content distribution, plus Fileset Magic
- Chapter 6 - Working with License Management and Apple's Volume Purchase Program (VPP)
- Chapter 7 - Using FileWave to provide mobile device management (MDM)
- Chapter 8 - Working with FileWave Inventory, including iOS inventory, Smart Groups, reporting, and Custom Fields
- Chapter 9 - Imaging with FileWave, including using Lightning
- Chapter 10 - Working with FileWave Engage for classroom management
- Chapter 11 - Apple Classroom and Shared iPad Support
- Chapter 12 - Network Discovery
- Chapter 13 - Chromebooks
- Chapter 14 - Web Console

> Note: This manual is focused on FileWave versions 13.x.x For information on older versions of FileWave, please see the appropriate version of the manual. Screenshots are from FileWave running on macOS and Windows - the functionality is identical between the two versions.

Some of the graphics used in this manual represent possible future versions of FileWave artwork. The presence of these items is not a product announcement. Likewise, some of the screenshots are from older versions of the software.

This manual 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://help.filewave.com

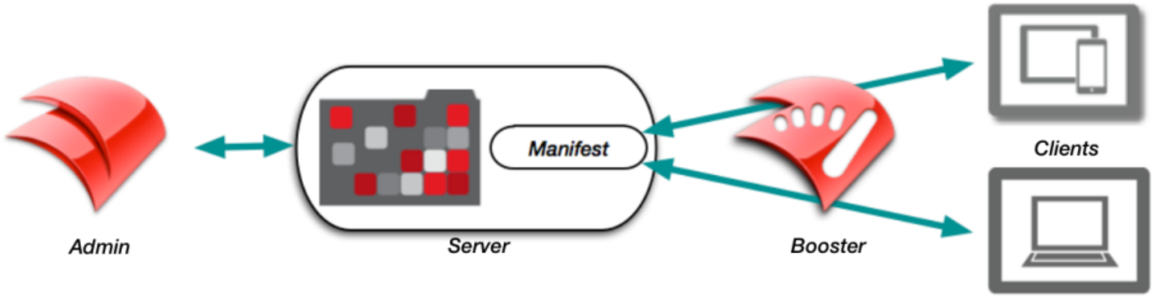
Copyright and disclaimer

FileWave, Inc.

Although the greatest care has been taken in the preparation and compilation of this document, no liability or responsibility of any kind, including responsibility for negligence, is accepted by FileWave, Inc., its servants or agents. All information gathered is believed correct as of the release date of this document. All corrections should be sent to FileWave, Inc. for consideration in future editions.

1.1. How does FileWave work?

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



A FileWave administrator 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 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 as well as, with FileWave handling all Client-Server communications, with the exception of inventory. 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 hosting 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 **2** of this manual.

FileWave Admin application

The FileWave Admin application is the primary interface to the FileWave Server. The FileWave Admin displays different views that give a representation of the FileWave Server's database. These views are the Dashboard, Clients, Filesets, Associations, Imaging, optional Classroom, iOS Inventory, License Management, Boosters, 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; system software updates for iOS 9+, OS X (macOS) 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 **2** of this manual.

FileWave Web Console

The FileWave Web Console is an Inventory tool designed to help with quick FileWave inventory references for specific clients in your server. Within the Web Console you will be able to view all devices currently enrolled, their Filesets, installed applications, users who have logged in, what groups they are apart of, and in the case of MDM enrolled Apple devices the command history. For more information please visit the page linked here.

FileWave Client (OS X and Windows)

The FileWave Client has two processes, **fwcld** and **fwGUI**. The first runs as a Launch Daemon on OS X (macOS) and as 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 computer boots. The fwcld process always runs with root (Mac) 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 Filesets that require rebooting. The **fwGUI** process is what provides the **Kiosk** / self-service functionality. The **I maging 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 client 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. 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 **5** of this manual covers the creation, configuration, distribution, and management of Filesets.

Self-service Kiosk

FileWave's self-service Kiosk provides the ability to allow end users access to content with their own device. In a BYOD deployment, you could post institutionally owned applications, documents, and updates for the end users to install at their convenience. In most of the deployment models, 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. Use and configuration of the **Kiosk** is covered in Chapter **4**.

Booster

The FileWave Booster is designed to act as a Fileset caching device for computer clients assigned to it as well as as to handle all Client-Server communications. Unlimited Boosters are allowed, regardless of license count or type. The FileWave Boosters allow administrators to increase the speed and scale of the Server's distribution of Filesets to Clients as well as offloading the overhead for constantly opening sockets for Client communications. 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.
Boosters are designed to work with Windows, OS X (macOS), and Android clients. iOS clients do not have the ability to use a Booster for cached Filesets, but they can utilize a Mac caching server, part of the $19.99 Server.app that runs just fine on a Mac mini. Chapter **3** 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 PXEboot services. Storage for network images for Mac and Windows, as well as Windows Drivers images is now on the FileWave server. FileWave Admin provides the management console for associating network images with designated client computers. Setup of the **IVS** preferences is in Chapter **2**; Chapter **9** 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 Student Information System (SIS) database 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 **Engage** is in Chapter **10**.

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 **2** covers Dashboard configuration and use.

1.3. FileWave Terminology

- ***Fileset*** - A set of common files and/or folders (directories) meant for delivery to a FileWave Client with a wrapper that contains a detailed listing of the Fileset contents, including permissions and a checksum for each part (to facilitate non-corrupt delivery to clients).
- ***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/Apple ID, and in the case of OS X (macOS)/Windows computers, 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 can be organized into Folders (directories). A file is activated in the corresponding folder on the boot volume of the FileWave Client. Folders do NOT have attributes; they only have 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 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 an action.
- ***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. Archiving a Client frees up one Client license.
- ***Administrator*** - A user that may log into the FileWave Server via the Admin application. The 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.
- ***Client State*** - The current condition of a client device as reported to the Admin. The states are: Normal, Missing, Not Tracked, or Archive. A **Normal** device is fully accessible by the FW Admin and the location is being tracked. A **Missing** device has been reported as stolen or not where it belongs and tracking is active. **Not Tracked** means that the device is monitored by FW Admin for all standard characteristics; but location tracking is disabled. An **Archived** device has been placed into stasis. It is no longer actively monitored by FW Admin; but the last known device settings are available in Inventory.
- ***Management Mode*** - In FileWave 11, we added a new client flag (for computer clients). It has two values: Managed (normal mode) and Inventory only. The latter setting allows you to have your client reporting data to FileWave, but will not be affected by any Filesets except for upgrade Filesets. Inventory only does consume a client license.

1.4. FileWave Security

FileWave SSL Certificates

> Using self-signed certificates should be avoided as much as possible in production environments; while it may make sense in some

closed environments, using Globally trusted CAs is our recommended approach.

The FileWave Server and other FileWave Components (e.g. Clients, Web Console, IVS, etc.) use the MDM server SSL certificate to validate communication. This certificate needs to be uploaded into the SSL Certificate Management pane, in the General tab inside FileWave Admin Preferences. This validation check will ensure secure and trusted communication between your FileWave server and the various FileWave components in your environment. Even though a self-signed certificate is supported, having a root trusted certificate from a CA is the best and most recommend option.

For more information on creating a root trusted certificate

How your FileWave environment will be affected by have a self-signed certificate

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 packages to the client, we wrap the content inside a Fileset. Because this is a proprietary container, the integrity of the delivered content is assured.

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. 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 Server security

The FileWave client communicates to the FileWave Server using SSL. 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.

Client tracking

A device can be tracked from FileWave Admin. Activating tracking involves setting the client state of the device to Normal and the current user of the device will receive a notification asking them to approve tracking (iOS and OS X only). Android devices will request that all client permissions be granted at installation, and Windows devices do not provide any user notification. Only devices on Wi-Fi will be tracked.

These tracking options can be disabled for any FileWave administrator account by modifying their permissions in the FileWave Admin. You can also have a global change on your FileWave license by requesting to disable Personal Data Collection. Keep in mind, disabling Personal Data Collection will not only prevent FileWave from gathering location data but also other personal data on the device.

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. Automated Backup

2.1. FileWave Server Installation

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 Virtual Server. To use Engage, you will need to download the Engage Server and setup the Engage services. This Chapter 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.

Overall requirements (for version 12)

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 volume with lower IOPS and more capacity. As with most servers, the more RAM that can be devoted to it, the better.

Operating Systems Supported:

- macOS 10.12 through 10.13 (binaries are 64 bit only)
- Windows Server 2012 R2 and Server 2016
- Linux CentOS 6.9 x86_64, and 7.4 x86_64 (binaries are 64 bit only)

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)
20005	TCP/IP	incoming for remote control publishing
20006	TCP/IP	incoming for remote control routing
20015	TCP/IP	incoming for client-server
20016	TCP/IP	incoming for admin-server
20017	TCP/IP	incoming for client-server secure (SSL)
20030	TCP/IP	incoming for remote control data
20443	TCP/IP	incoming for client-server profiles
20445	TCP/IP	incoming for client-server inventory

Full list of ports: Default TCP and UDP Port Usage

Install versus Upgrade

Before attempting to do any updated with FileWave, point your browser to our support site's software download page (https://www.filewave.com/support/software-downloads) and check for special instructions.
You must be at version 10 of the FileWave Server before you can upgrade to v11. As long as you are running FileWave Server version 7.x or higher, you can upgrade your existing server to v10, then run the Migration Checker script (available here: https://mc.filewave.com/). This script will verify your ability to migrate your system to the new all PostgreSQL database used in FileWave v11. The results will be emailed to the address you provide at the end of the command, and will come from noreply@filewave.com. The email subject will be either [FAIL] Upgrade check report or [PASS] Upgrade check report depending on what the script has discovered. If your FileWave v10 Server passes, you can upgrade to v11 without issue; if it fails, contact FileWave Support who will get the issues resolved and get you p-upgraded to v11.
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)

Generally, this is the workflow (specifics follow):

1. Do a backup following these instructions: Automated Backup
2. Lock computer clients.
3. Upgrade the server.
4. Upgrade the Admin(s).
5. Update the Model.
6. Upgrade Boosters
7. Unlock a couple of clients. Verify that they see the Model number change. Deploy the upgrade Fileset to these test clients and ensure they upgrade without issue.
8. Unlock and upgrade the other computer clients.
    - Use the Upgrade Fileset for upgrading existing Clients. The standard or custom .pkg/,msi should only be used for computers that do not have FileWave installed.
9. Ensure iOS device communication. Skip if you have no iOS. Go into iOS Inventory, refresh from the toolbar, total count is accurate, sort by Last MDM Check-in Date, open Client Info, Command History and verify the device is receiving commands.

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

macOS FW Server install

System Requirements

Any 64-bit Macintosh system running macOS version 10.12+ will work for FileWave Server; and this does not require the OS X Server software. 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 macOS, 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 at the root of the boot volume.

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 2012 R2 and Server 2016 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.

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 is supported on Linux CentOS 6.9 x86_64, and 7.4 x86_64 (binaries are 64 bit only.

Setup

Download the latest FileWave binaries for Linux on the following Website:
http://www.filewave.com/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 if necessary (on Windows use PuTTY, on macOS use Terminal) and 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 FileWave_Linux_<FILEWAVEVERSION>.zip
yum install -y --nogpgcheck fwxserver*.rpm
yum install -y --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 macOS 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.

2.2. Imaging Virtual Server installation and setup

Your ability to perform network imaging for macOS and Windows is based on the FileWave Imaging Virtual Server (IVS). This virtual machine contains all the components of an macOS NetBoot server and a Windows PXEboot 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:

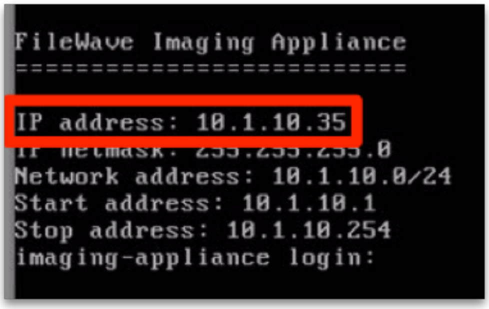
- VMWare VSphere ESX, Fusion, VMWare Player, and VMWare Workstation
- Virtual Box
- Hyper-V

Installation

You download the imaging VM from the FileWave Support site - https://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:



```
FileWave Imaging Appliance
==========================

IP address: 10.1.10.35
IP netmask: 255.255.255.0
Network address: 10.1.10.0/24
Start address: 10.1.10.1
Stop address: 10.1.10.254
imaging-appliance login:
```

The default TCP management port for FileWave Imaging access 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 manual. 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

Like all servers, 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:

```
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 "**sudo reboot**" to commit your changes and leave the command line. More command line functionality for the IVS is covered in the Appendix.

Upgrading from IVS 3.2 to 4.0

We have provided a method to upgrade, in place, existing IVS 3.2 servers to IVS v4. Check the software download page for instructions on how to do this: https://www.filewave.com/support/software-downloads.

2.3. 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 restart networking using the following command:

```
service networking restart
```

(or use your VM controls to restart the EVS)

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 assign a name to the Engage server's IP address.

2.4. 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.

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 Fully-Qualified Doman Name (meaning there has to be an "A" record in DNS for the server) or a routable IP address. The APN certificate (see below) must match this domain name or IP address; 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.), the MDM Server must have access to an Apple Push Notification certificate. The process for obtaining an APNs is explained in Appendix A.3.
- *Google Cloud Messaging service Project Number and API key*. These items can be created at the Google Developer Console. Details on this are provided in Appendix A.4.
- *FileWave Server running on OS X v10.9+(for the new features in iOS 9+, use OS X v10.10+), 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 server on macOS

The MDM server is installed as part of the FileWave Server package for macOS. 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.

Installation and setup of MDM on Windows FileWave server

The MDM server is now installed along with the FileWave Server 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>` **- w**here <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.

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.

2.5. 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) 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 setup; as long as it is complete before you begin enrolling MDM clients.
This process consists of:

1.
   a. Backing up the current config file;
   b. Editing a new config file to properly read the LDAP structure; and,
   c. Restarting the Apache Process so it reads the new config file.

Getting the files ready

1. Open a Terminal Window or use SSH to get into the computer running FileWave Server
2. Gain root credentials

```
sudo -s
```

1. Enter your login password
2. Navigate to the FileWave Apache configurations folder:

Windows: `C:\Program Files(x86)\FileWave\apache\conf`
macOS / Linux: `cd /usr/local/filewave/apache/conf/`

1. Backup your current mdm_auth.conf by making a copy

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

1. Make a copy of the LDAP example and rename it

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

1. Making the changes
2. Open *mdm_auth.conf* up using your preferred text editor (**nano mdm_auth.conf** or **vi mdm_auth.conf**). Make the appropriate changes (the sample file is appropriately commented) 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.

1. Once saved, restart the FileWave Apache process/service:

Windows: Go to: Services > FileWave, MDM Apache > Select:, Restart
macOS / Linux: /usr/local/filewave/apache/bin/apachectl graceful
Now, when a user attempts to enroll a device in your MDM server, he or she will use their LDAP credentials to authenticate.

2.6. 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.

Automated Backup

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

2.7. 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.

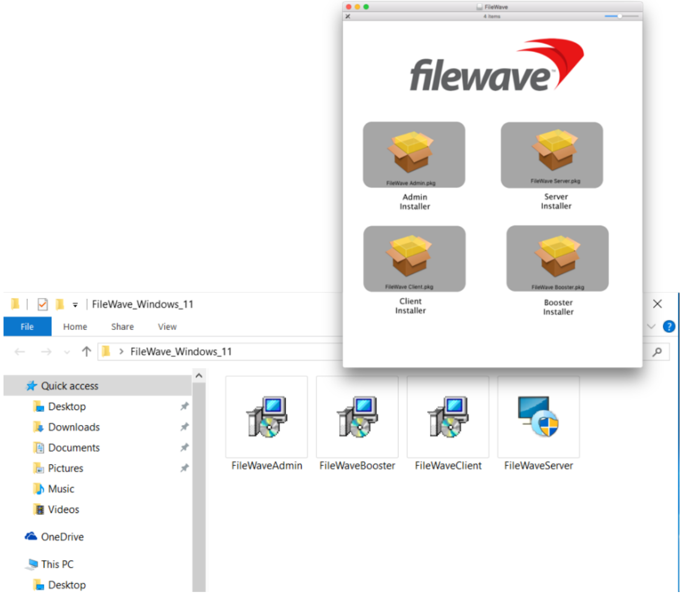
System Requirements for the FileWave Admin application

The FileWave Admin application runs on both OS X and Windows computers supporting the following operating systems:

- OS X v10.11 / macOS 10.12
- Windows 7 / 8.1 / 10

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. Se lect 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 the **Security** section on the next page).
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.

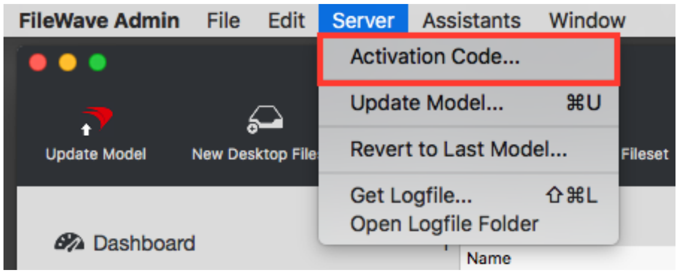
- Fileset Magic. Allows you to open Fileset Magic to create custom Filesets without logging into FW Admin.

2.8. 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 different number of licenses in the future.

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 clients). Upon purchase of the FileWave solution, you are provided a custom activation code created specifically for the number of licensed devices you specified in your order. The activation code will also let you create additional FileWave administrators above and beyond the single "super-administrator" account provided by default (**fwadmin**). The license code will also specify the number of administrators who can be logged in simultaneously. 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 can 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.

2.9. Configuring Basic FileWave Preferences

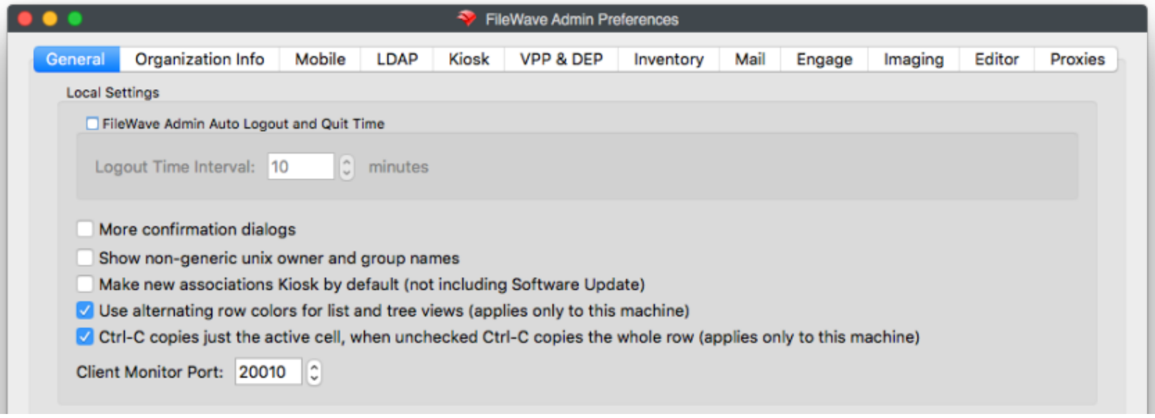
This section covers the basic FileWave preferences of **General, Organization Info, Kiosk, Inventory, Mail, Editor** and **Proxies**. The more complex preferences - *Mobile, LDAP, VPP&DEP, Engage,* and *Imaging* are covered in their own sections.

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.



Local Settings

☐ FileWave Admin Auto Logout and Quit Time

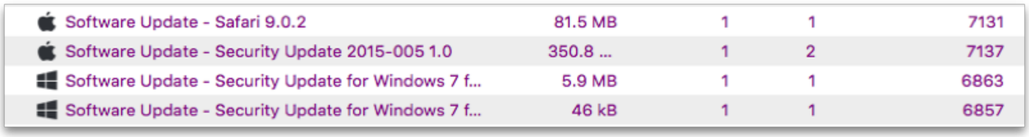
Logout Time Interval: 10 minutes

☐ More confirmation dialogs
☐ Show non-generic unix owner and group names
☐ Make new associations Kiosk by default (not including Software Update)
☑ Use alternating row colors for list and tree views (applies only to this machine)
☑ Ctrl-C copies just the active cell, when unchecked Ctrl-C copies the whole row (applies only to this machine)

Client Monitor Port: 20010

- *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.
- *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.
- *Use Alternating row colors….* Changes the view in the Admin panes to display a spreadsheet-like array of rows.



Software Update - Safari 9.0.2	81.5 MB	1	1	7131
Software Update - Security Update 2015-005 1.0	350.8 ...	1	2	7137
Software Update - Security Update for Windows 7 f...	5.9 MB	1	1	6863
Software Update - Security Update for Windows 7 f...	46 kB	1	1	6857

- *Ctrl-C copies just the active cell….* Allows the administrator to copy cells or entire rows of data within the various panes.
- *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.

Apple Software Updates

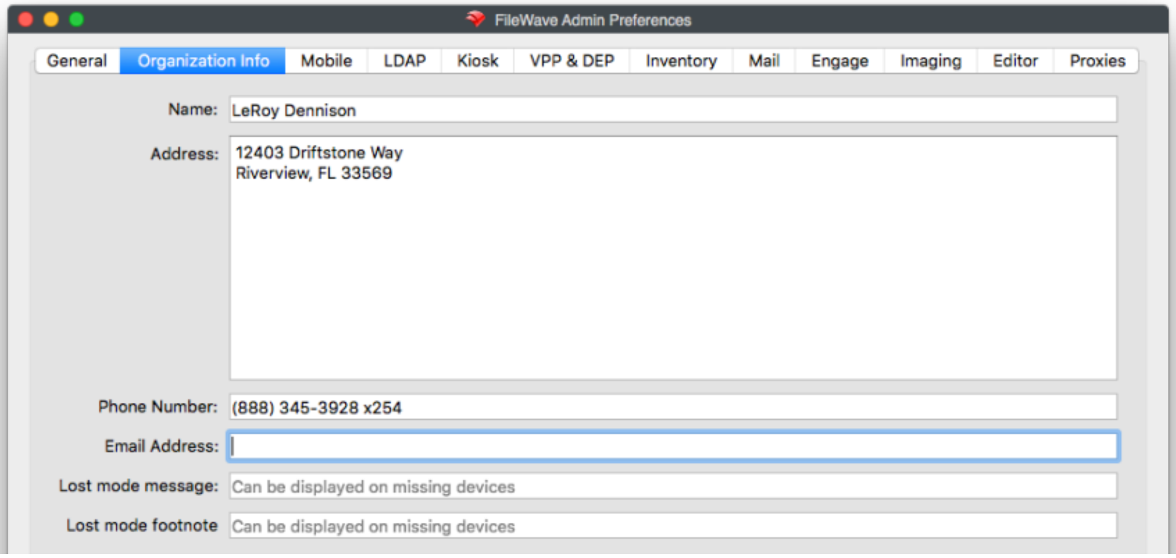
These values define the URLs for the various Apple Software Update Servers' catalogs based on differing versions of OS X..

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.



Name: LeRoy Dennison

Address: 12403 Driftstone Way
Riverview, FL 33569

Phone Number: (888) 345-3928 x254

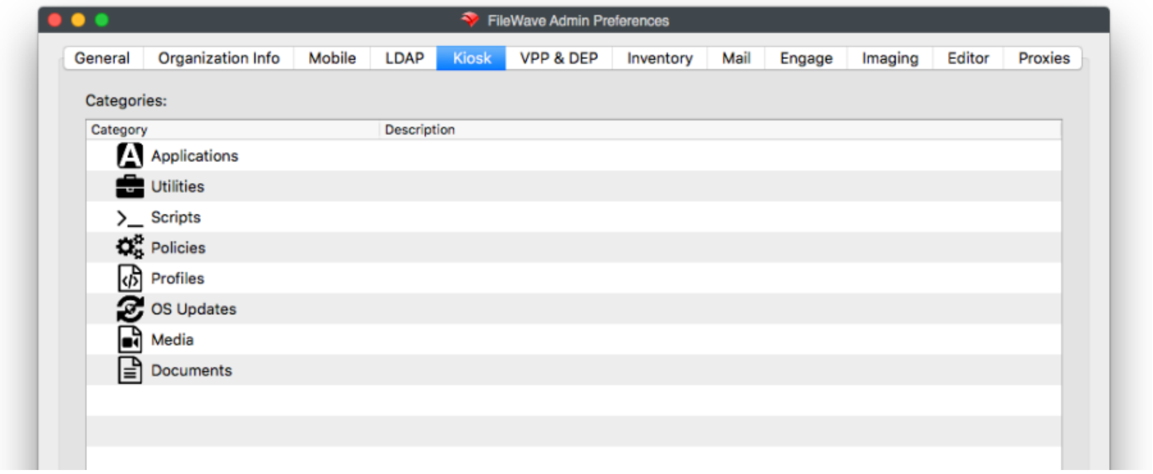
Email Address:

Lost mode message: Can be displayed on missing devices

Lost mode footnote Can be displayed on missing devices

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.



Categories:

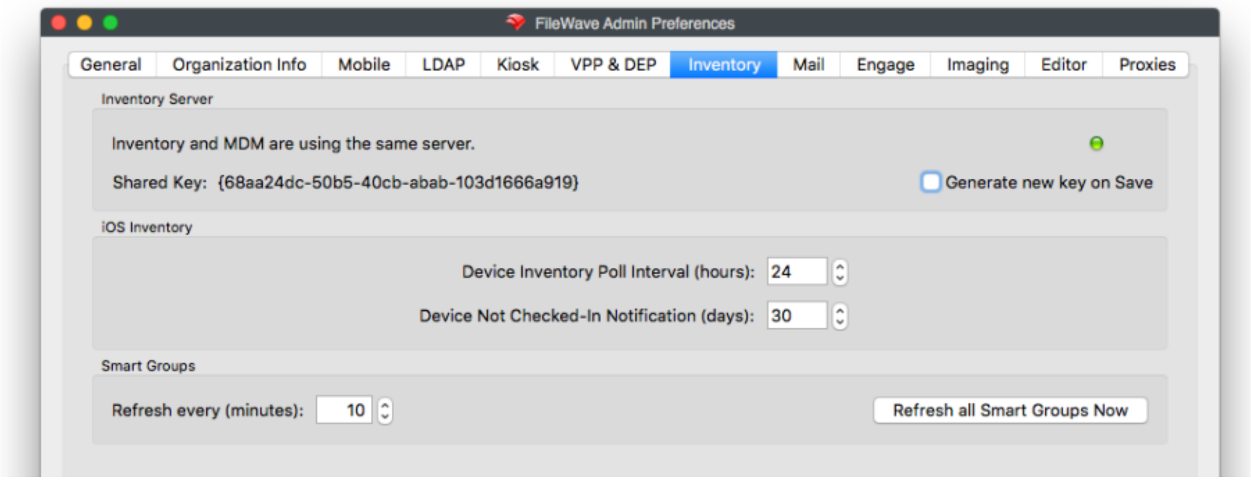
Category	Description
Applications	
Utilities	
Scripts	
Policies	
Profiles	
OS Updates	
Media	
Documents	

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.

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 computer. The settings for Inventory on the current version can be left at the defaults; but information on the provided settings is below:



Inventory Server

Inventory and MDM are using the same server. ●

Shared Key: {68aa24dc-50b5-40cb-abab-103d1666a919} □ Generate new key on Save

iOS Inventory

Device Inventory Poll Interval (hours): 24

Device Not Checked-In Notification (days): 30

Smart Groups

Refresh every (minutes): 10

Inventory Server

The FileWave Inventory server and MDM server are now running on the same server. 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.

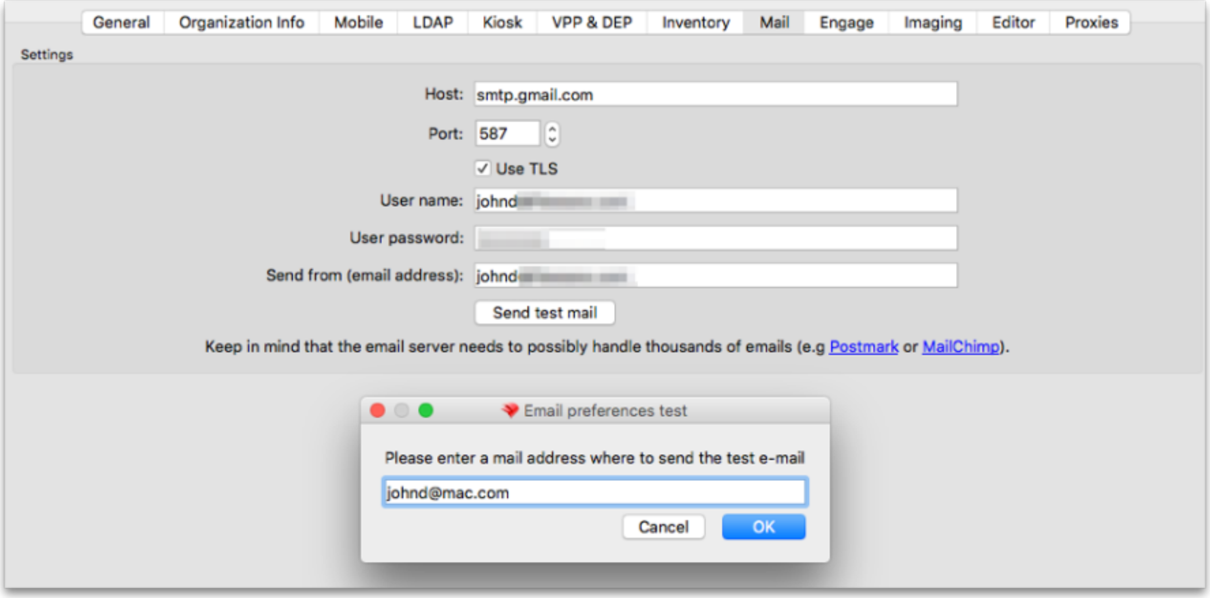
- *Device Not Checked-In Notification* – Default is 30 days. When an iOS device exceeds the timeframe set, the device color changes to alert the administrator that that device has not checked in with the MDM server.

Smart Groups

The button **Refresh all Smart Groups** forces a system-wide refresh of all the data requested by existing Smart Groups. (Smart Groups are discussed in detail in Chapter **8**.)

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). 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.



Host: smtp.gmail.com

Port: 587

☑ Use TLS

User name: johnd[redacted]

User password: [redacted]

Send from (email address): johnd[redacted]

Keep in mind that the email server needs to possibly handle thousands of emails (e.g Postmark or MailChimp).

Email preferences test

Please enter a mail address where to send the test e-mail

johnd@mac.com

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 the proxy service. 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.

- *Server Proxy Credentials* – HTTP and SOCKS5 are the two protocol options, followed by host name, port, username and password.
- *Admin Proxy Credentials Override – HTTP and SOCKS5 are the 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.

2.10. Mobile preferences - iOS _ Android

The Mobile preferences are designed around **Mobile Device Management** for Apple's iOS/macOS and Google's Android/Chromebooks. This section discusses setting up the basic components in FileWave Admin/Preferences. Mobile Device Management is covered in detail in Chapter **7**. The certificate workflow for MDM is covered in the Appendix.

Configure MDM Server

- *MDM Server Address* - Enter your MDM server's FQDN or routable IP address.
- *Port* - The default port for FileWave MDM is **20445**.
- *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 (HTTPS Certificate Management)

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.

- **Details** – Shows the details of the current certificate uploaded.
- ***Upload PKCS12 Certificate*** - This is used to upload a SSL certificate issues by a Certificate Authority.
- ***Get Current Certificate*** - Once you have a valid certificate, you can download a copy to be used with Apple Configurator.

Note: Self-signed certificates are no longer able to be generated in FileWave. A certificate signed by a CA is required for iOS, MDM enrolled Macs, and Chromebooks.

Apple Push Notification Certificate (APN) for iOS

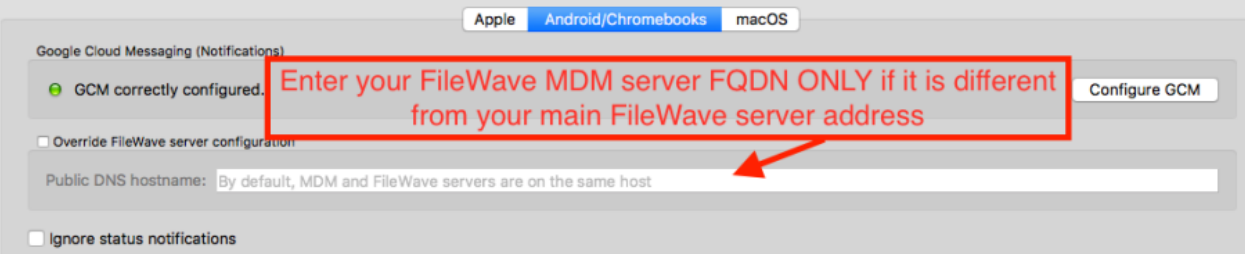
The APN certificate is required to allow the application developers to send notifications to their applications, such as the Weather app getting current storm alerts. In order to allow the applications you deploy to your mobile devices to get these notifications, you request a secure certificate from Apple. The process for getting the certificate is detailed in the Appendix for FileWave administrators running either OS X or Windows.
Once you have received your APN Certificate from Apple, you will add it by clicking on the **Upload APN Certificate/Key** Pair button. This will configure your FileWave MDM server to support secure communications with Apple's Push Notification service.

Android/Chromebooks MDM Configuration

If you are deploying Android clients, then you will need to configure the Android/Chromebooks 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/Chromebooks** 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.

Override FileWave Server configuration

The Android client is a composite of the computer 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 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.



Google Cloud Messaging (Notifications)

● GCM correctly configured.

Enter your FileWave MDM server FQDN ONLY if it is different from your main FileWave server address

□ Override FileWave server configuration

Public DNS hostname: By default, MDM and FileWave servers are on the same host

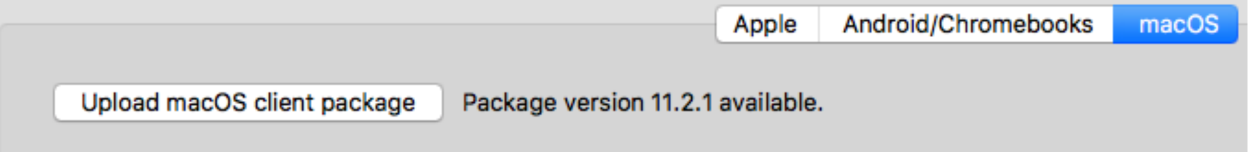
□ Ignore status notifications

macOS MDM configuration

For macOS 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 all MDM enrolled devices. When a MDM macOS 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.

> **macOS Client Package Installation Triggers**
> The FileWave macOS client package will install on newly enrolled DEP and Profile MDM enrolled macOS devices. The macOS client package will also get pushed out to **ALL** existing enrolled MDM clients if you upload a new macOS client package into the FileWave Preferences. Be sure not to accidently upload the non-custom client pkg or upload a custom client pkg with the wrong FileWave server address, if you do then all exsisting MDM enrolled macOS devices will install the newly uploaded client and then in turn lose connection to your FileWave server.

The first step is to go to the FileWave Support site and request a custom installer: https://www.filewave.com/support/custom-client-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:

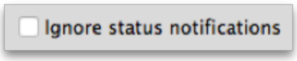


Package version 11.2.1 available.

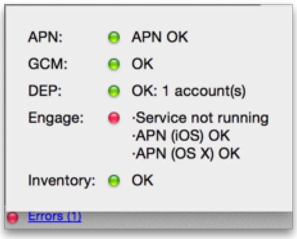
Authenticate as the FileWave Admin superuser (**fwadmin**), then locate the newly downloaded package. **Note: You must unpack/unzip the package before being able to upload it to your server!**

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. 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, macOS 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.



□ Ignore status notifications



APN:	●	APN OK
GCM:	●	OK
DEP:	●	OK: 1 account(s)
Engage:	●	·Service not running ·APN (iOS) OK ·APN (OS X) OK
Inventory:	●	OK

● Errors (1)

2.11. 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. Using LDAP to authenticate your devices gives you a way to know who (which LDAP user) enrolled what device.

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)
- *Protocol* – select LDAP, LDAPS, STARTSSL. For LDAPS and STARTSSL you have a checkbox that you can potentially uncheck so that the server certificate is not checked against the machine's trust store. NOTE: IF LDAPS or STARTSSL it is recommended to be using a trusted LDAP cert.
- *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=tanner,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 24 hr. (86,400 seconds).
- *Change Limit (%)* - LDAP related items will not be removed if more than the given percentage of the items disappear after a sync. This is to avoid loss of data if something goes wrong with the LDAP configuration.

Note: Choosing to enable the automatic Group updates creates a visible set of entries in the Clients pane of FileWave Admin, 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.

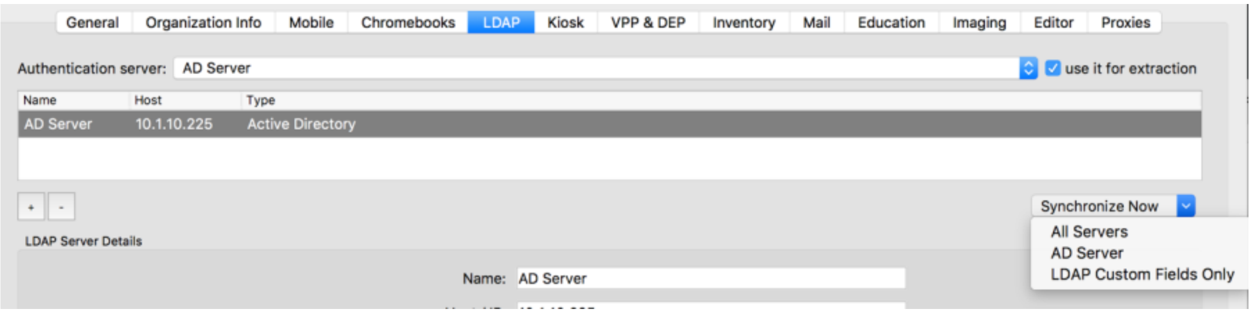
You can create entries for multiple LDAP servers, and an LDAP server can be running on the same device or VM as the FileWave Server.

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 (Smart Groups) in the **Clients** pane under an LDAP designator. These Smart Groups will be updated by FileWave at the designated refresh interval

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.

At the Bottom right of the LDAP server pane, there is a Synchronize Now option. This option will allow you to synchronize all your LDAP servers, just one, or sync LDAP Custom Fields.



Authentication server: AD Server ☑ use it for extraction

Name	Host	Type
AD Server	10.1.10.225	Active Directory

Name: AD Server

2.12. 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 **6** of this manual goes into great depth on the configuration and operation of VPP for iOS devices and macOS computers. Chapter **4** 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 these web sites:

https://help.apple.com/deployment/business/
https://help.apple.com/schoolmanager/
https://help.apple.com/deployment/ios/
https://help.apple.com/deployment/macos/

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

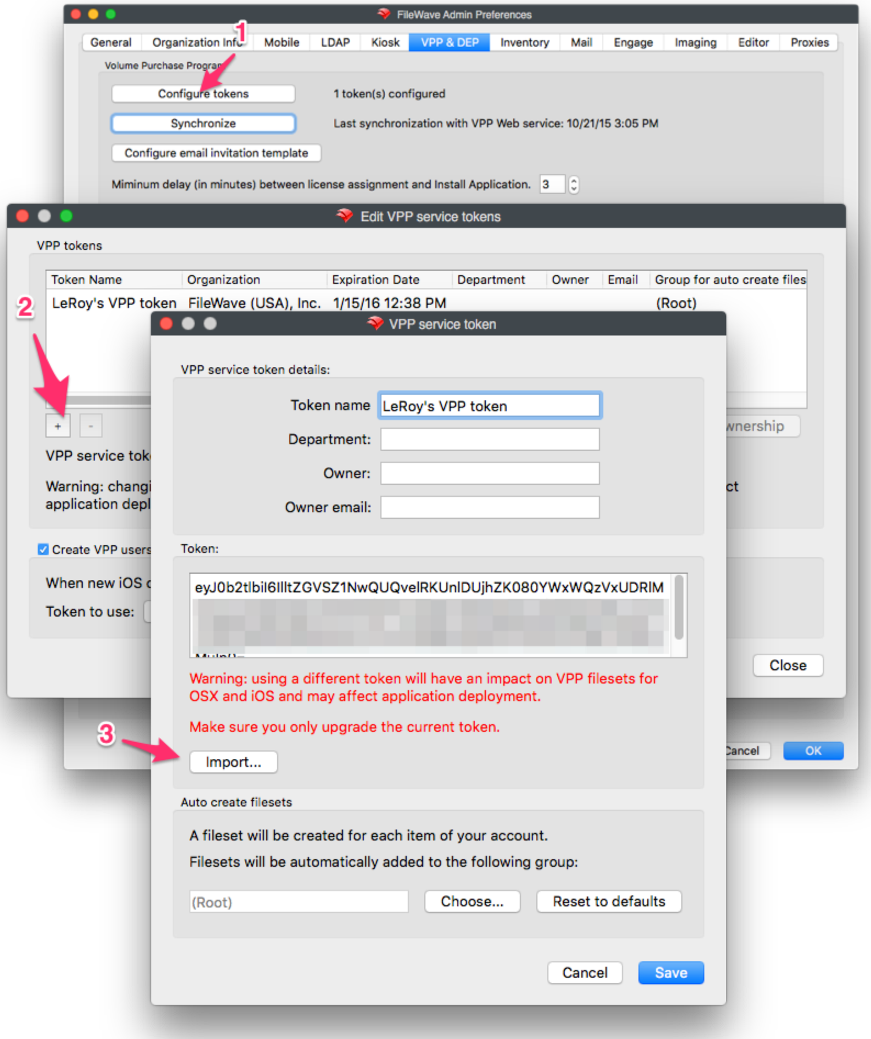
This pane contains the information for your VPP account with Apple. In order to proceed, you will have to have created a VPP for Education or VPP for Business account with Apple. Once you have a VPP account, you can download your VPP token for inclusion into FileWave. You may add as many tokens as you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

Configure VPP token(s)

Select the **Configure accounts** button (1 in the graphic on the next page). You will have to authenticate as the primary FileWave Admin (fwadmin).

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.



1 token(s) configured

Last synchronization with VPP Web service: 10/21/15 3:05 PM

Miminum delay (in minutes) between license assignment and Install Application. 3

VPP tokens

Token Name	Organization	Expiration Date	Department	Owner	Email	Group for auto create files
LeRoy's VPP token	FileWave (USA), Inc.	1/15/16 12:38 PM				(Root)

VPP service tok

Warning: changi
application depl

☑ Create VPP users

When new iOS c

Token to use:

VPP service token details:

Token name: LeRoy's VPP token

Department:

Owner:

Owner email:

Token:

eyJ0b2tlbil6IlltZGVSZ1NwQUQvelRKUnlDUjhZK080YWxWQzVxUDRlM
[redacted]

Warning: using a different token will have an impact on VPP filesets for OSX and iOS and may affect application deployment.

Make sure you only upgrade the current token.

Auto create filesets

A fileset will be created for each item of your account.

Filesets will be automatically added to the following group:

(Root)

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

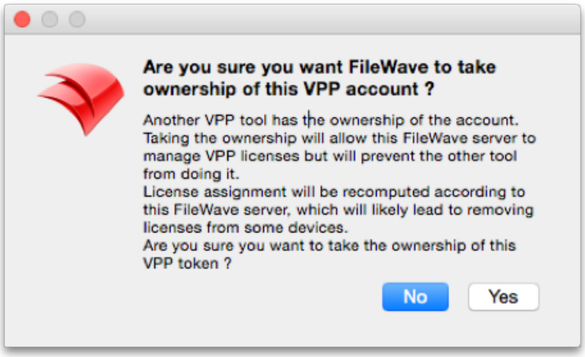
Once the token has been properly imported, you will see a dialog pop up telling you that everything is in order.
If you want more than the FileWave superuser/admin account (**fwadmin**) to be able to manage VPP applications later on, you will need to use the **/Assistants/ Manage Administrators…** pane to assign other administrators to manage the VPP token(s). This is covered at the end of this chapter.

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 **6**.

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*;. If you have changed servers, or let another process, such as Apple Configurator, use that VPP token, then you will get an alert stating that the token is owned by another server.
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:



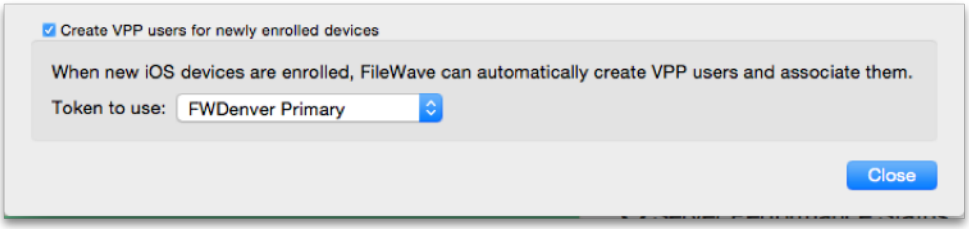
Are you sure you want FileWave to take ownership of this VPP account ?

Another VPP tool has the ownership of the account.
Taking the ownership will allow this FileWave server to manage VPP licenses but will prevent the other tool from doing it.
License assignment will be recomputed according to this FileWave server, which will likely lead to removing licenses from some devices.
Are you sure you want to take the ownership of this VPP token ?

The key to this process is making 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 or **Apple Configurator**, you should 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 Apple ID.



☑ Create VPP users for newly enrolled devices

When new iOS devices are enrolled, FileWave can automatically create VPP users and associate them.

Token to use: FWDenver Primary

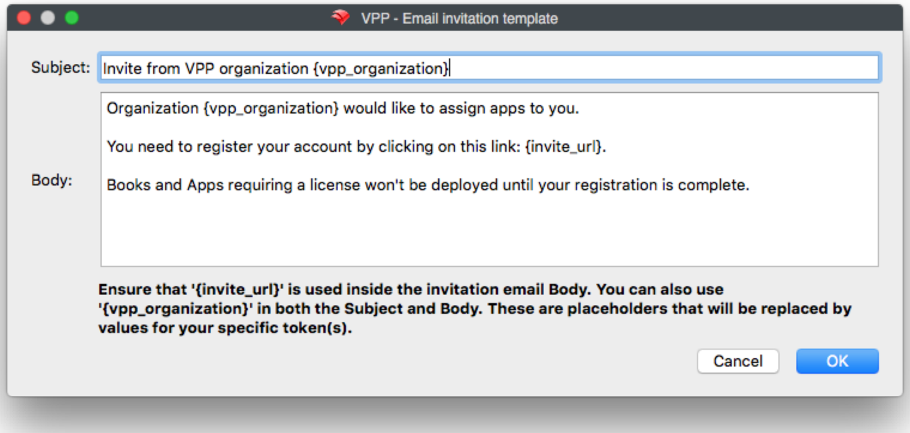
If this checkbox is selected, then newly enrolled devices will automatically get a VPP user and that user account will be associated with the device. This can speed up mass deployments, as well as reduce the overhead on 1:1/BYOD deployments. Used in conjunction with settings in the VPP Assistant, your FileWave server can then automatically notify new user's to register their Apple ID 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. **Note: If you are using VPP device assignment for application distribution (versus assignment by user - Apple ID), a "ghost" or invisible VPP user account is created. This account is not visible within the VPP User Management pane.**

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 devices and macOS computers. If you have configured your setup to use LDAP authentication for enrollment, 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 Apple ID to register that ID with your FileWave MDM.



Subject: Invite from VPP organization {vpp_organization}

Body:

Organization {vpp_organization} would like to assign apps to you.

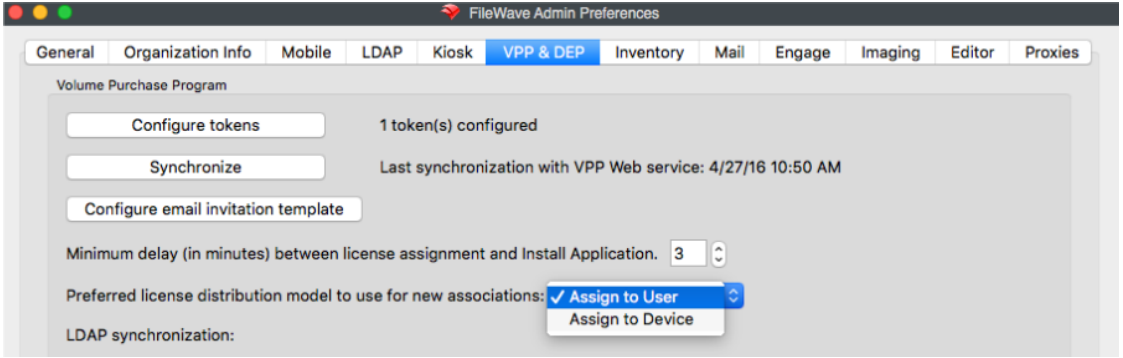
You need to register your account by clicking on this link: {invite_url}.

Books and Apps requiring a license won't be deployed until your registration is complete.

Ensure that '{invite_url}' is used inside the invitation email Body. You can also use '{vpp_organization}' in both the Subject and Body. These are placeholders that will be replaced by values for your specific token(s).

Minimum delay and Preferred Distribution

Starting with FileWave v10, you have the ability to establish a delay between the time you associate a VPP application with a license and when 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 Apple ID (User). The license shows up in the user's Purchases, and the license can be managed by the FileWave MDM. The new method, supported in iOS 9+ and OS X v10.11+, allows you to assign VPP applications directly to an enrolled device (provided the app developer has coded the app to support this). This method applies only to VPP applications - iBooks are still required to be assigned to individual Apple IDs. There is a detailed discussion of this process in Chapter **6**.



Volume Purchase Program

1 token(s) configured

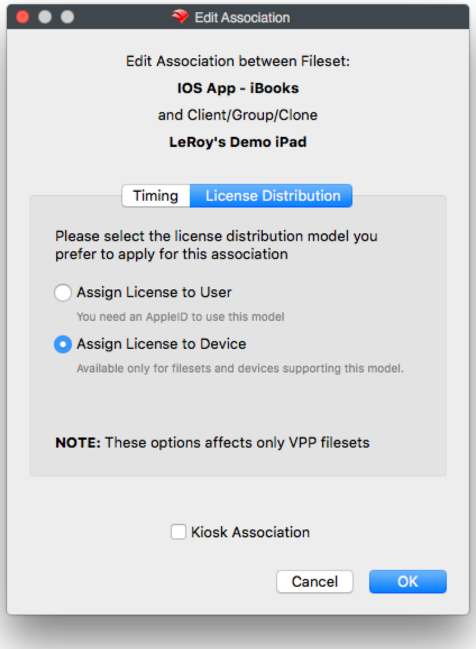
Last synchronization with VPP Web service: 4/27/16 10:50 AM

Minimum delay (in minutes) between license assignment and Install Application. 3

Preferred license distribution model to use for new associations: ✓ Assign to User

LDAP synchronization:

The default setting can be overwritten for a given association of a managed license Fileset.



Edit Association

Edit Association between Fileset:

IOS App - iBooks

and Client/Group/Clone

LeRoy's Demo iPad

Please select the license distribution model you prefer to apply for this association

○ Assign License to User

You need an AppleID to use this model

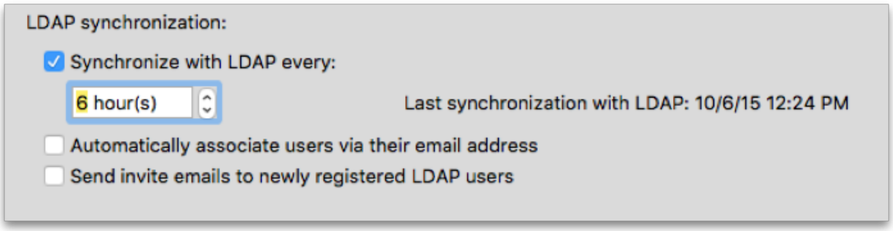
● Assign License to Device

Available only for filesets and devices supporting this model.

NOTE: These options affects only VPP filesets

□ Kiosk Association

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 can be left off if you are going to use **device assignment** of all your distributed VPP applications.



LDAP synchronization:

☑ Synchronize with LDAP every:

6 hour(s)

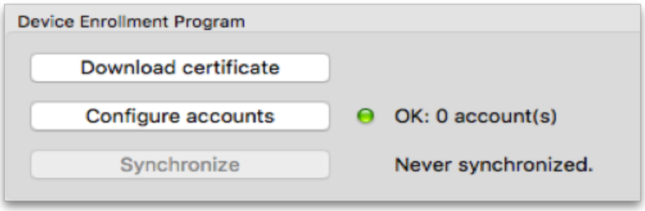
Last synchronization with LDAP: 10/6/15 12:24 PM

□ Automatically associate users via their email address

□ Send invite emails to newly registered LDAP users

Device Enrollment Program preferences

Apple's Device Enrollment Program is designed to support OTA (over the air - Wi-Fi) supervision of devices. FileWave supports iOS devices and macOS computers using DEP. 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.

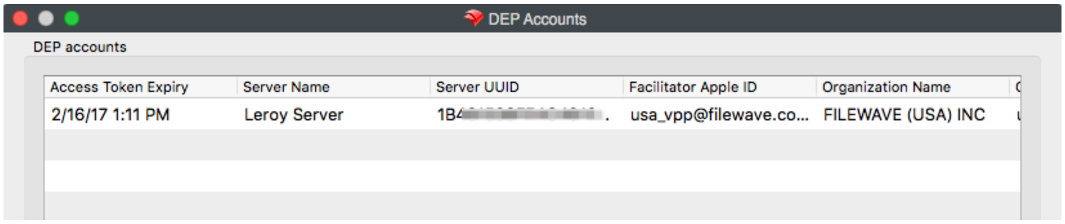


Device Enrollment Program

● OK: 0 account(s)

Never synchronized.

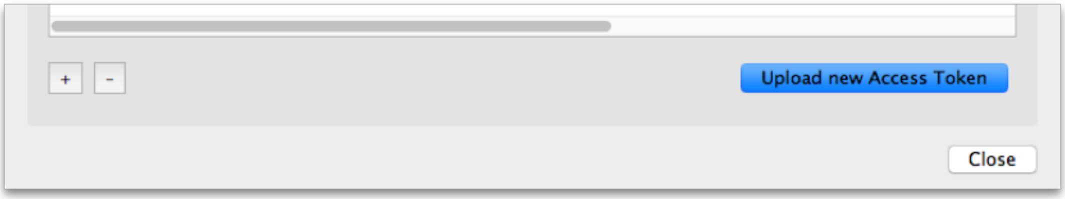
Using the "Download certificate" button, download a special "FileWave DEP" certificate to your administrator machine. You will be required to authenticate with the **fwadmin** FileWave Admin account. Use that certificate to get a DEP token from the Apple DEP site (https://deploy.apple.com or https://school.apple.com).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



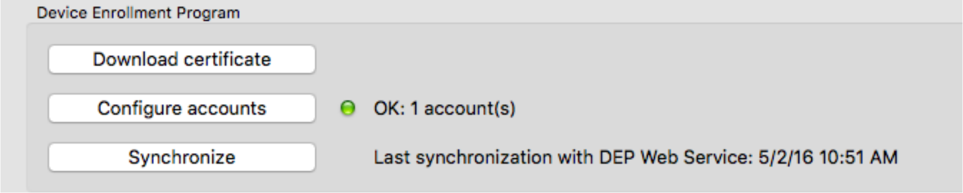
DEP Accounts

DEP accounts

Access Token Expiry	Server Name	Server UUID	Facilitator Apple ID	Organization Name	C
2/16/17 1:11 PM	Leroy Server	1B4[redacted].	usa_vpp@filewave.co...	FILEWAVE (USA) INC	u



The **Synchronize** button works the same as the VPP synchronize button. DEP will synchronize between Apple and your FileWave 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.



Device Enrollment Program

OK: 1 account(s)

Last synchronization with DEP Web Service: 5/2/16 10:51 AM

2.13. 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 Section 2.2 of this Chapter). 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. 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.
Copy that address and add it to the *Server Address* in the **Imaging** tab... 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*, you should change it), and set the IVS to communicate with your FileWave server by entering either the FQDN or IP address of the FileWave Server.
You can check to see that the settings are correct by checking the **Status…** button in the main **Imaging** Preference pane.

Download NBI file…

This button downloads a script that you will then run on a macOS 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 macOS computers do a network boot from. 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 **9**. It is also important for you to understand that the NBI is OS specific. You must run the script on

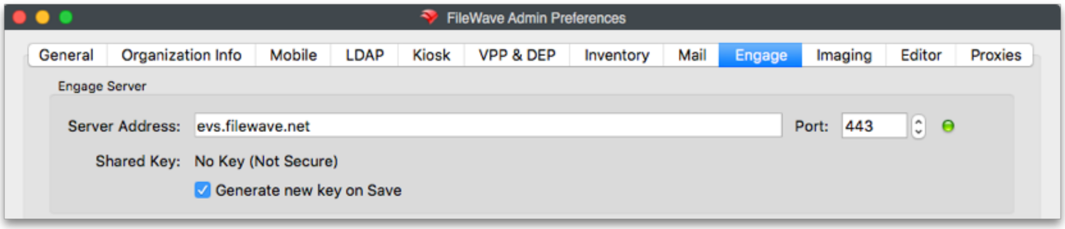
a Mac with a recovery partition, and it will create an NBI for that version of macOS or OS X only, and send the image to the specific IVS named in the script. You can run separate IVSs to store differing versions of macOS/OS X NetBoot images.
All other imaging configuration will be done from the **Imaging** pane in the main Admin window. See Chapter **9** for more details on IVS and Imaging.

2.14. 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 Section 2.3 of this Chapter**.** For details on the use of the Engage applications, see Chapter **10** in this manual.

Engage Server

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



Server Address: evs.filewave.net

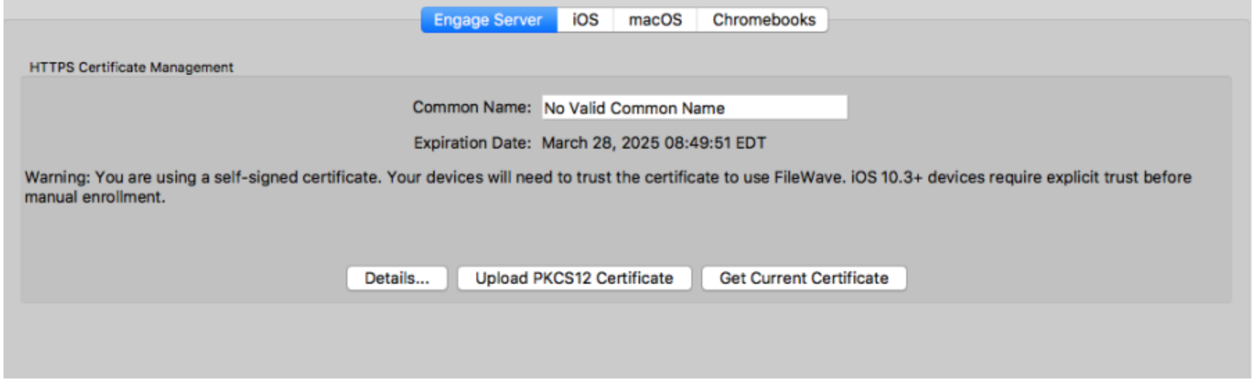
Port: 443

Shared Key: No Key (Not Secure)

☑ Generate new key on Save

HTTPS Certificate Management

You will need a valid SSL certificate in .p12 format. for the communications between the Engage server and its clients. There are also specific push certificates for iOS and macOS / OS X that will be provided by FileWave as part of your software download.



Common Name: No Valid Common Name

Expiration Date: March 28, 2025 08:49:51 EDT

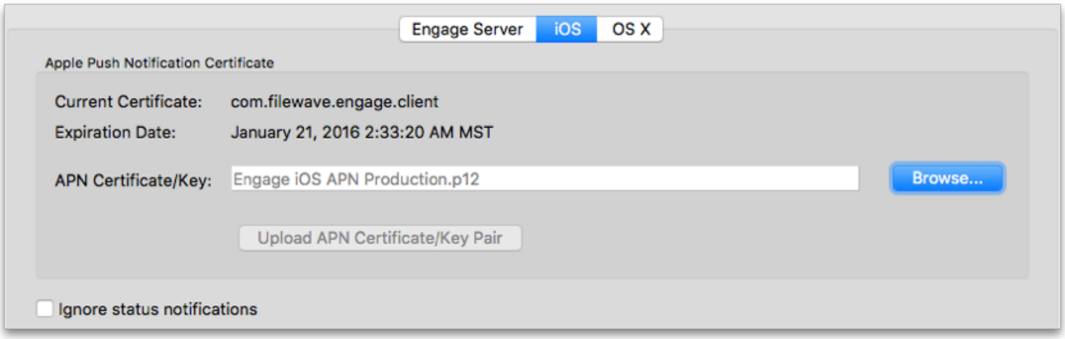
Warning: You are using a self-signed certificate. Your devices will need to trust the certificate to use FileWave. iOS 10.3+ devices require explicit trust before manual enrollment.

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. and import it into FileWave Admin as part of a Certificate profile. See the Chapter on Mobile Device Management 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.

iOS / macOS 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 macOS) 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.



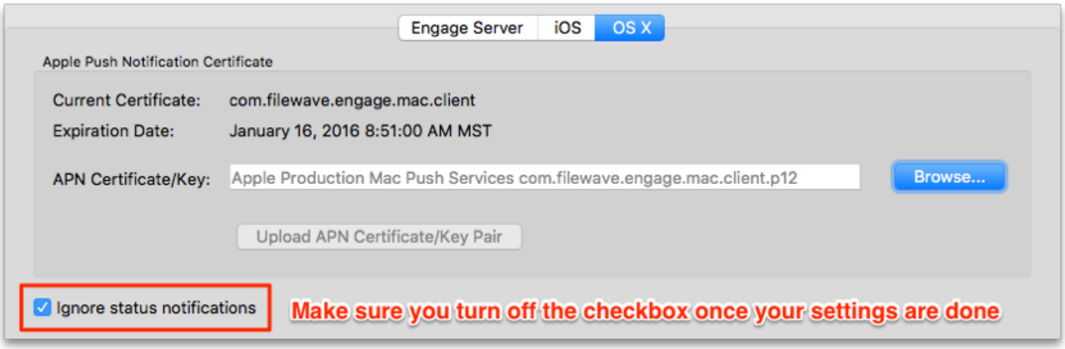
Apple Push Notification Certificate

Current Certificate: com.filewave.engage.client

Expiration Date: January 21, 2016 2:33:20 AM MST

APN Certificate/Key: Engage iOS APN Production.p12

□ Ignore status notifications



Apple Push Notification Certificate

Current Certificate: com.filewave.engage.mac.client

Expiration Date: January 16, 2016 8:51:00 AM MST

APN Certificate/Key: Apple Production Mac Push Services com.filewave.engage.mac.client.p12

☑ Ignore status notifications

Make sure you turn off the checkbox once your settings are done

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 a confirmation dialog. It's 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 a dialog showing that you are connected to Clever and syncing data.

Migrate data to new Engage server

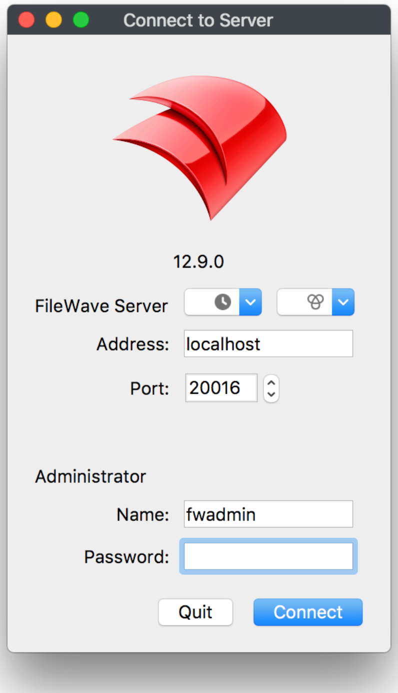
If you plan to upgrade to a new VM of the Engage server, you don't want to lose any of the data or settings you have established. This checkbox allows you to set up a new Engage server VM and transfer your current settings.
The setup will ask for the address of the new EVS, transfer your data, then remind 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:

2.15. Managing FileWave Administrators

FileWave supports tiered administration so you can create additional administrators in order to spread the workload, you are not limited to the amount of admins you can have in FileWave.

How to log into FileWave Admin

When you log into the FileWave Admin to access the FileWave Server you will be asked for the server address, and user credentials which can be a local account or an LDAP account.



Connect to Server

12.9.0

FileWave Server

Address: localhost

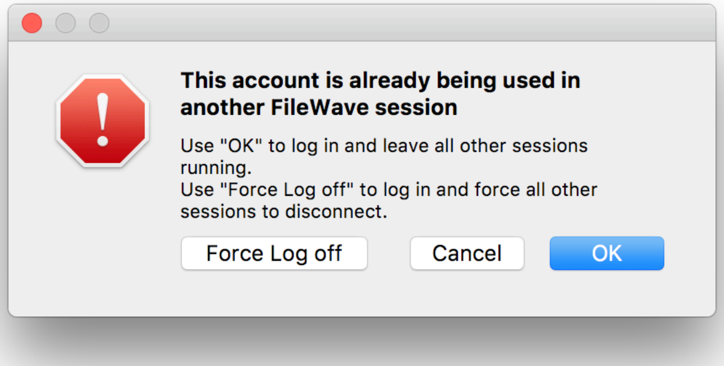
Port: 20016

Administrator

Name: fwadmin

Password:

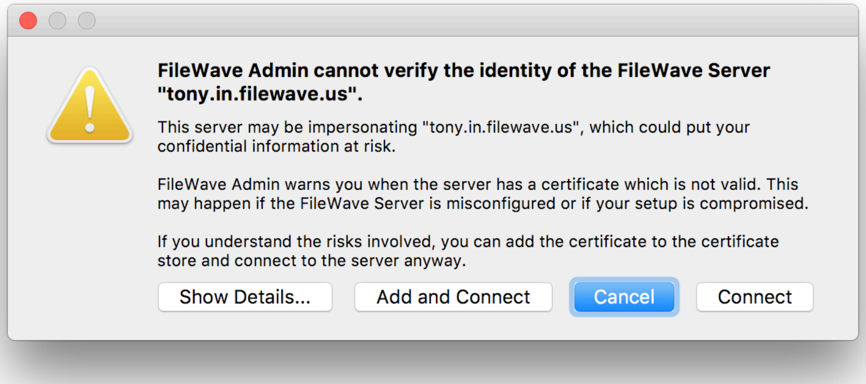
FileWave supports multiple admin connections from the same or separate admin accounts. If you try to log in with the same account that is already connected somewhere else you will get prompted to either end that first connection, start a second connection, or cancel.



This account is already being used in another FileWave session

Use "OK" to log in and leave all other sessions running.
Use "Force Log off" to log in and force all other sessions to disconnect.

If you are currently using a self-signed certificate then you may also get a prompt that the Admin cannot verify the identity of the FileWave server. The recommend way to fix this is to, hit connect and then switch to a root trusted certificate. Please visit the KB linked here for instructions on how to do this.



FileWave Admin cannot verify the identity of the FileWave Server "tony.in.filewave.us".

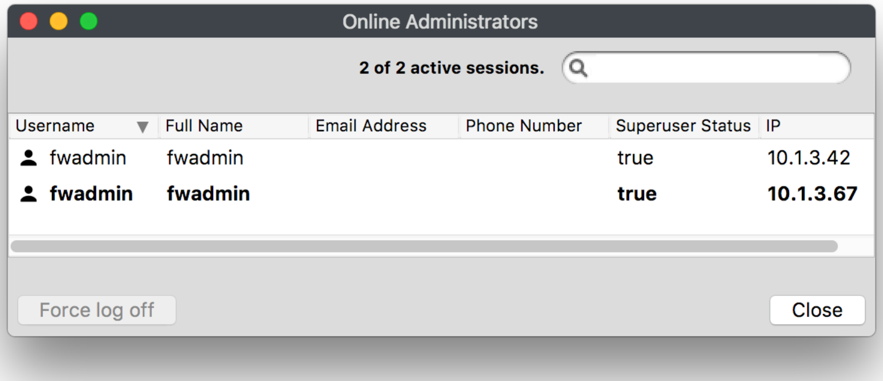
This server may be impersonating "tony.in.filewave.us", which could put your confidential information at risk.

FileWave Admin warns you when the server has a certificate which is not valid. This may happen if the FileWave Server is misconfigured or if your setup is compromised.

If you understand the risks involved, you can add the certificate to the certificate store and connect to the server anyway.

You will also be able to see two active connections if you look in the **Administrators Online...** window located under the **Assistants** menu

> The bolded entry is your current connection



Online Administrators

2 of 2 active sessions.

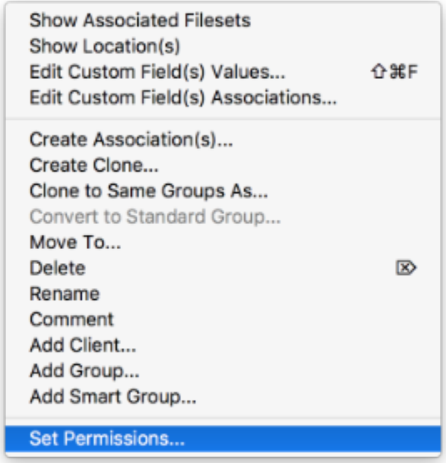
Username	Full Name	Email Address	Phone Number	Superuser Status	IP
fwadmin	fwadmin			true	10.1.3.42
fwadmin	**fwadmin**			**true**	**10.1.3.67**

FileWave Administrators and Inventory

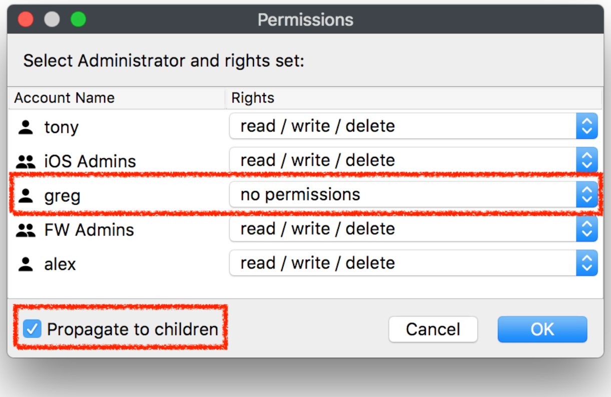
In the FileWave Admin console you have the ability to set read/write/delete permissions to specific objects which include devices, filesets, and groups. These permissions will follow the user all the way into inventory so that only what the current administrator has access too can be seen in the inventory results.

Example:

1. Right click on an object (user, group, fileset) and select **Set Permissions**



2. Select the permissions you would like for each administrator. Setting it to **No Permissions** will make that object no longer visible for the administrator.



Permissions

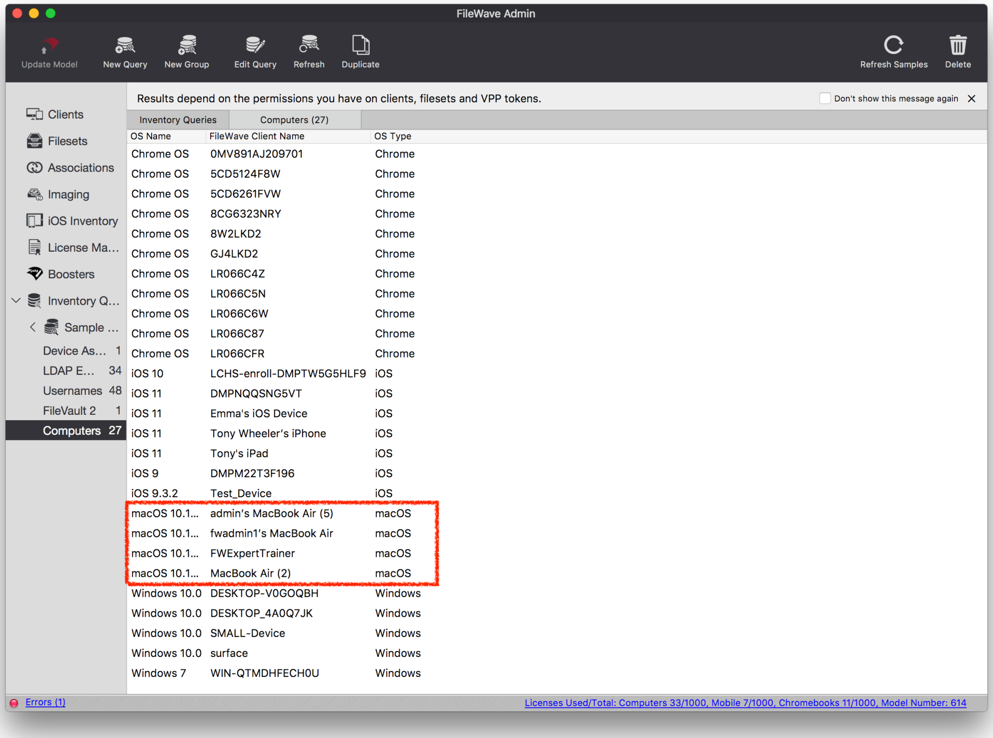
Select Administrator and rights set:

Account Name	Rights
tony	read / write / delete
iOS Admins	read / write / delete
greg	no permissions
FW Admins	read / write / delete
alex	read / write / delete

☑ Propagate to children

- You have to select **Propagate to children** if you are setting permissions on a group and want those permissions to be added to sub-objects.
- read/write/delete permissions are received from the original object and the clones will get the same permissions. If you modify these permissions on a clone, only this specific clone will get them not the original or other clones.

3. In this case the user **greg** has no permissions for the group selected which is for all macOS devices and these permissions have been propagated to all sub-objects. So as you can see below the first screenshot shows what the user with full permissions sees and the second screenshot shows inventory information with the new permissions.

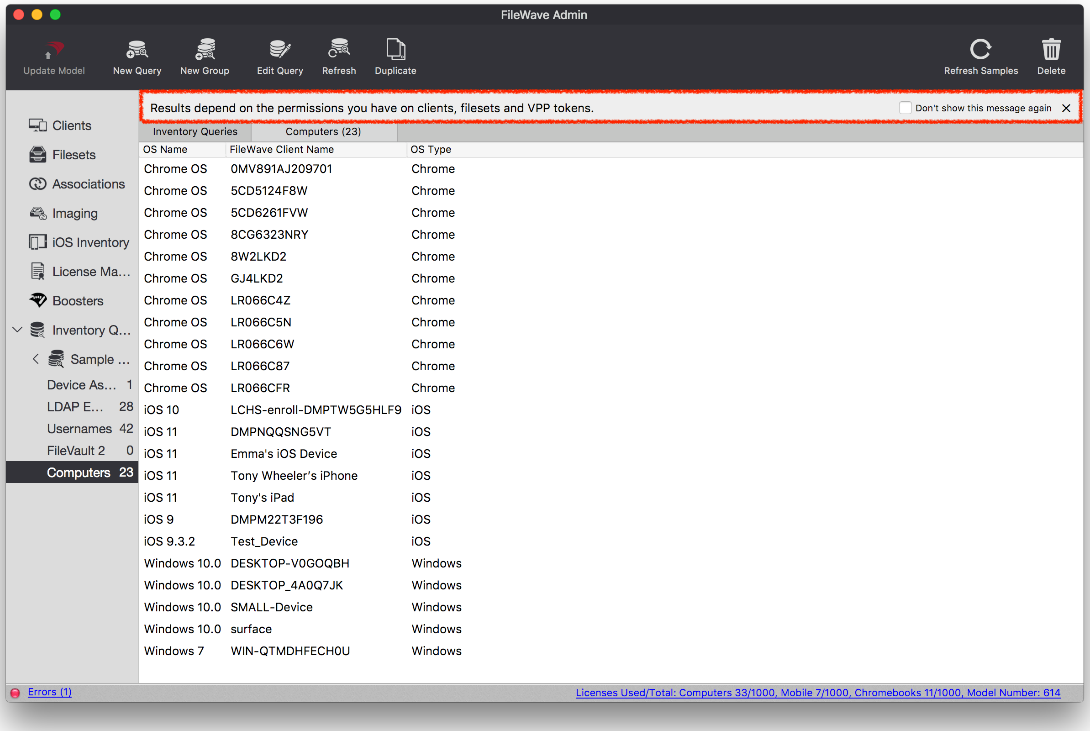


Results depend on the permissions you have on clients, filesets and VPP tokens.

OS Name	FileWave Client Name	OS Type
Chrome OS	0MV891AJ209701	Chrome
Chrome OS	5CD5124F8W	Chrome
Chrome OS	5CD6261FVW	Chrome
Chrome OS	8CG6323NRY	Chrome
Chrome OS	8W2LKD2	Chrome
Chrome OS	GJ4LKD2	Chrome
Chrome OS	LR066C4Z	Chrome
Chrome OS	LR066C5N	Chrome
Chrome OS	LR066C6W	Chrome
Chrome OS	LR066C87	Chrome
Chrome OS	LR066CFR	Chrome
iOS 10	LCHS-enroll-DMPTW5G5HLF9	iOS
iOS 11	DMPNQQSNG5VT	iOS
iOS 11	Emma's iOS Device	iOS
iOS 11	Tony Wheeler's iPhone	iOS
iOS 11	Tony's iPad	iOS
iOS 9	DMPM22T3F196	iOS
iOS 9.3.2	Test_Device	iOS
macOS 10.1…	admin's MacBook Air (5)	macOS
macOS 10.1…	fwadmin1's MacBook Air	macOS
macOS 10.1…	FWExpertTrainer	macOS
macOS 10.1…	MacBook Air (2)	macOS
Windows 10.0	DESKTOP-V0GOQBH	Windows
Windows 10.0	DESKTOP_4A0Q7JK	Windows
Windows 10.0	SMALL-Device	Windows
Windows 10.0	surface	Windows
Windows 7	WIN-QTMDHFECH0U	Windows

Errors (1)

Licenses Used/Total: Computers 33/1000, Mobile 7/1000, Chromebooks 11/1000, Model Number: 614



Results depend on the permissions you have on clients, filesets and VPP tokens.

OS Name	FileWave Client Name	OS Type
Chrome OS	0MV891AJ209701	Chrome
Chrome OS	5CD5124F8W	Chrome
Chrome OS	5CD6261FVW	Chrome
Chrome OS	8CG6323NRY	Chrome
Chrome OS	8W2LKD2	Chrome
Chrome OS	GJ4LKD2	Chrome
Chrome OS	LR066C4Z	Chrome
Chrome OS	LR066C5N	Chrome
Chrome OS	LR066C6W	Chrome
Chrome OS	LR066C87	Chrome
Chrome OS	LR066CFR	Chrome
iOS 10	LCHS-enroll-DMPTW5G5HLF9	iOS
iOS 11	DMPNQQSNG5VT	iOS
iOS 11	Emma's iOS Device	iOS
iOS 11	Tony Wheeler's iPhone	iOS
iOS 11	Tony's iPad	iOS
iOS 9	DMPM22T3F196	iOS
iOS 9.3.2	Test_Device	iOS
Windows 10.0	DESKTOP-V0GOQBH	Windows
Windows 10.0	DESKTOP_4A0Q7JK	Windows
Windows 10.0	SMALL-Device	Windows
Windows 10.0	surface	Windows
Windows 7	WIN-QTMDHFECH0U	Windows

Errors (1)

Licenses Used/Total: Computers 33/1000, Mobile 7/1000, Chromebooks 11/1000, Model Number: 614

Types of Administrator Accounts

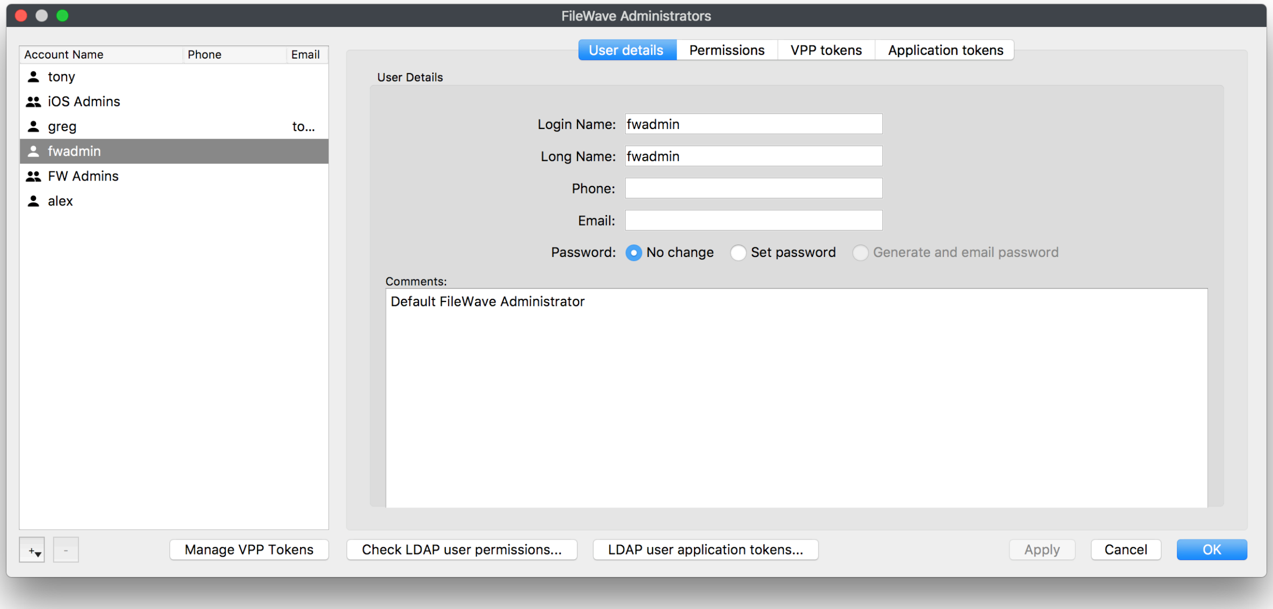
FileWave has three different account types;

- Superuser - This will be the fwadmin account that came with FileWave by default, and is required for certain setup options in FileWave.
- Local User - A user name and password created directly from the FileWave Admin and saved on the server.
- LDAP Group User - Admin credentials are pulled from LDAP (Active and Open Directory)

Other than the Superuser, which has full rights by default, you have the ability set granular permissions for your Local and LDAP users.

Superuser

The default credentials for your Superuser account is **fwadmin/filewave** which FileWave highly recommends that you change so the password is something more secure!



FileWave Administrators

Account Name	Phone	Email
tony		
iOS Admins		
greg		to...
fwadmin		
FW Admins		
alex		

User Details

Login Name: fwadmin

Long Name: fwadmin

Phone:

Email:

Password: ● No change ○ Set password ○ Generate and email password

Comments:

Default FileWave Administrator

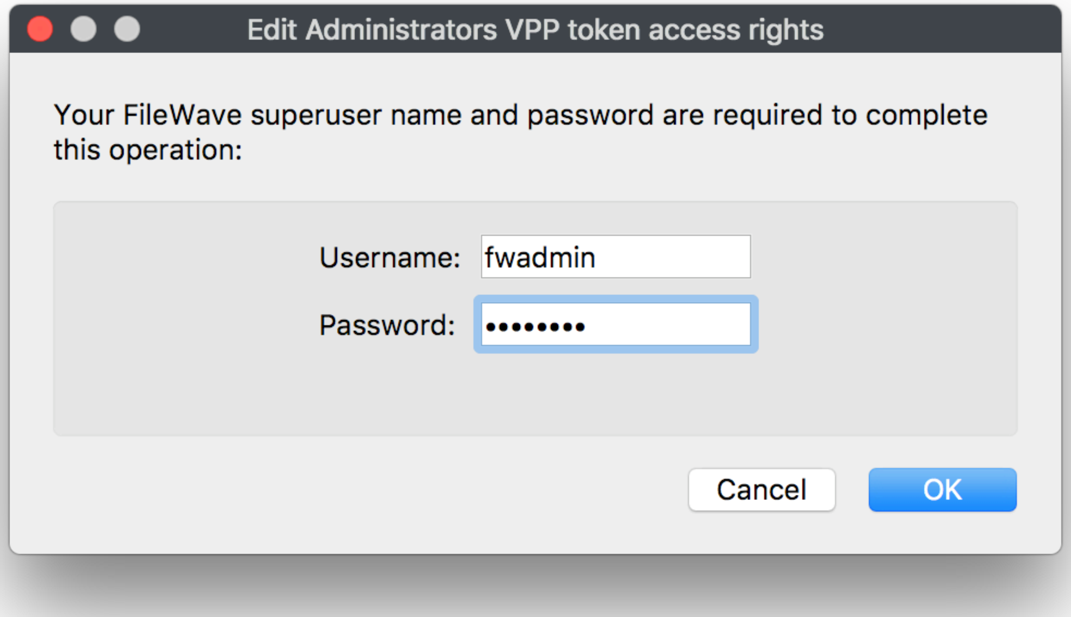
There are areas and features in FileWave that can only be accessed with the FileWave Superuser account. Three of these sections won't even be visible to any other Admin account, one (Software Update) is grayed out for all but the Superuser, and the other features will trigger a dialog window requesting the Superuser credentials to be entered.

Only Visible from the Superuser logged in:

- Activation Lock Management (**Assistants Activation Lock Management)**
- Force Logoff Admin (**Assistants Administrators Online...**)
- Scheduled Reports Owner (**Assistants Scheduled Reports.. "+" Owner section)**
- Software Update Sources Apple / Microsoft **(Preferences General)**

All Admins will be prompted for Superuser credentials:

- VPP & DEP setup (**Admin Preferences VPP & DEP)**
- Configure OAuth token (**Admin Preferences Chromebooks**)
- Upload PKCS12 Certificate (**Admin Preferences Mobile HTTPS Certificate Management**)
- Configure GCM (**Admin Preferences Mobile Android/Chromebooks**)
- Upload macOS client package (**Admin Preferences Mobile macOS**)
- SIS - Edit Settings... (**Admin Preferences Education SIS**)
- Engage - Upload PKCS12 Certificate (**Admin Preferences Education Engage Engage Server**)
- Apple Classroom - Manage Certificates (**Admin Preferences Education Apple Classroom**)
- Force log off (**Assistants Administrators Online...**)
- Manage VPP Tokens (**Assistants Manage Administrators Manage VPP Tokens**)



Your FileWave superuser name and password are required to complete this operation:

Username: fwadmin

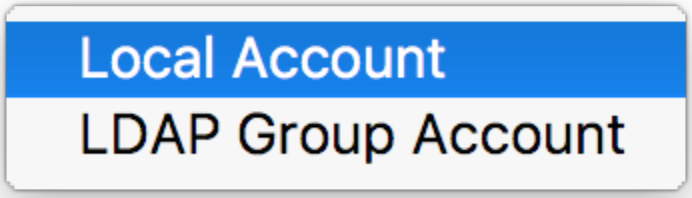
Password: ••••••••

Local Account

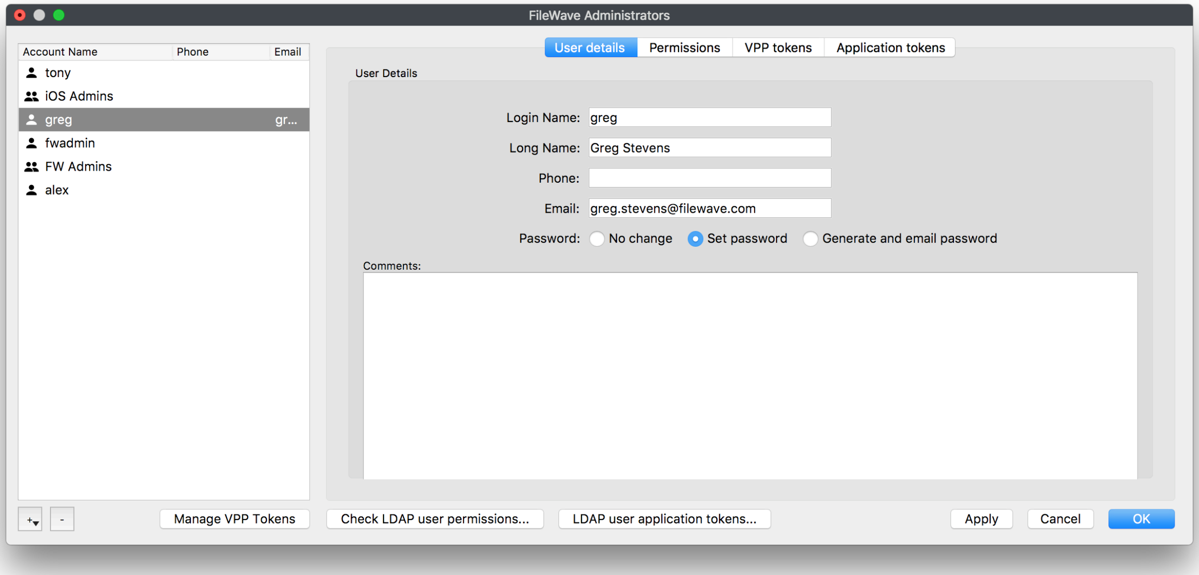
Local Accounts can be created very simply and then given whatever permissions you wish them to have. Keep in mind even if a Local Administrator Account is given full rights they will still be prompted for Superuser credentials in the areas listed in the Superuser section above.

To create a Local Account for the FileWave Admin follow the steps below:

1. Go to **Assistants Manage Administrators**
2. Click on the the "+" sign at the bottom left
3. Then select Local Account



4. You will now be able to fill in the user information under the **User details** tab. Since this is a new user you will also have to set a default password by selecting **Set Password** or **Generate and email password** (this will only work if you provided an email for this user and you also have the Email settings completed in the Admin Preferences)



Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

User Details

Login Name: greg

Long Name: Greg Stevens

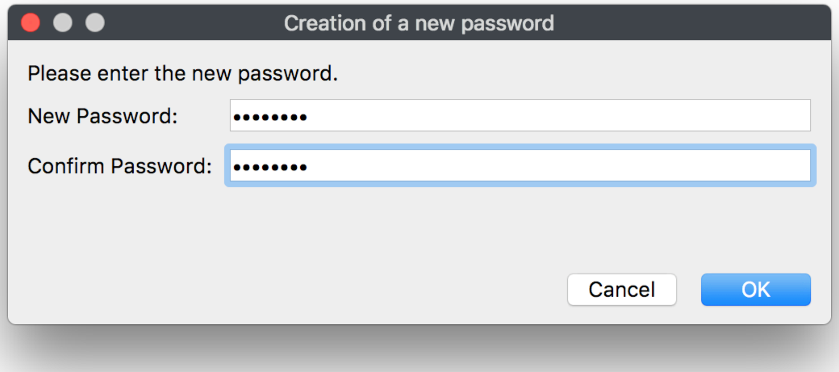
Phone:

Email: greg.stevens@filewave.com

Password: ○ No change ● Set password ○ Generate and email password

Comments:

If you selected **Set password** you will get the following window to type in the user's password:

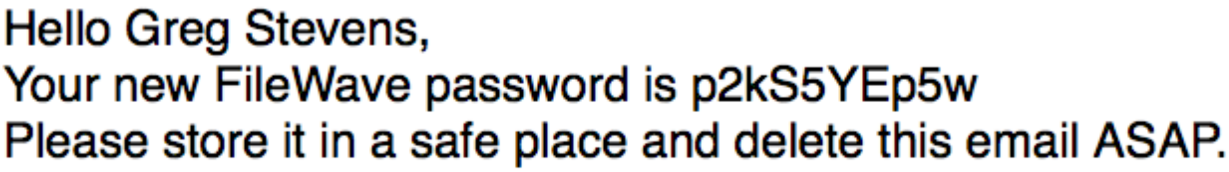


Please enter the new password.

New Password: ••••••••

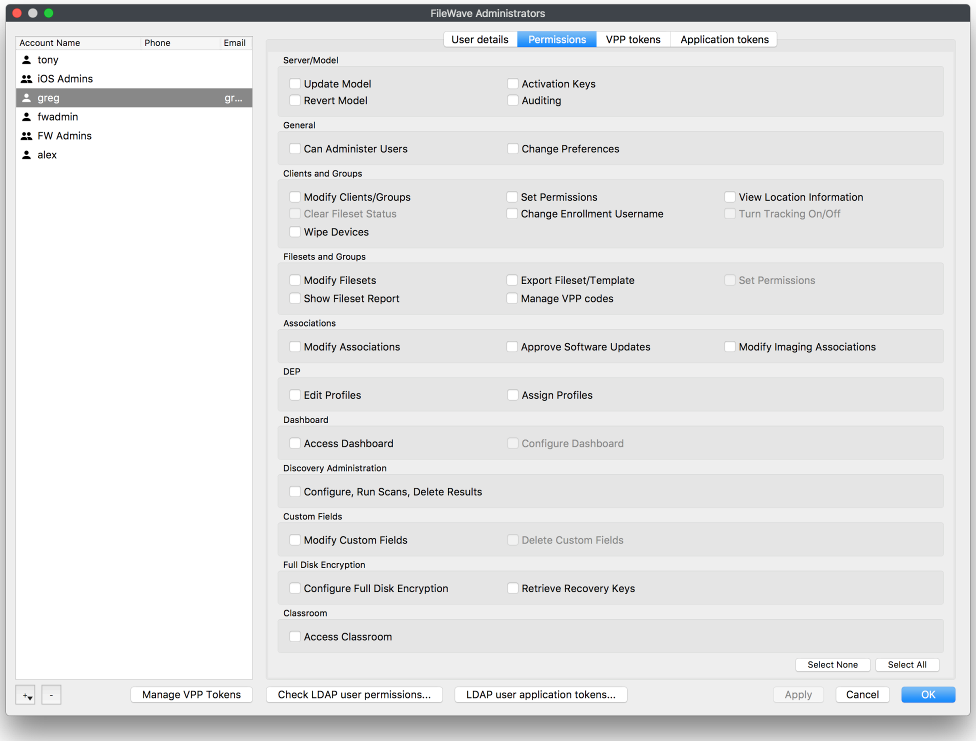
Confirm Password: ••••••••

If you selected **Generate and email password** you will need to hit the **Apply** button at the bottom of the **FileWave Administrators** window and you will then get an email with the following information:



Hello Greg Stevens,
Your new FileWave password is p2kS5YEp5w
Please store it in a safe place and delete this email ASAP.

5. Next you will need to give this user permissions in FileWave. You do this by selecting the user and going into the **Permissions** tab and checking which options you want this user to have. (There will be more information on what each of these options do at the end of this section)



Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

Server/Model

□ Update Model □ Activation Keys
□ Revert Model □ Auditing

General

□ Can Administer Users □ Change Preferences

Clients and Groups

□ Modify Clients/Groups □ Set Permissions □ View Location Information
□ Clear Fileset Status □ Change Enrollment Username □ Turn Tracking On/Off
□ Wipe Devices

Filesets and Groups

□ Modify Filesets □ Export Fileset/Template □ Set Permissions
□ Show Fileset Report □ Manage VPP codes

Associations

□ Modify Associations □ Approve Software Updates □ Modify Imaging Associations

DEP

□ Edit Profiles □ Assign Profiles

Dashboard

□ Access Dashboard □ Configure Dashboard

Discovery Administration

□ Configure, Run Scans, Delete Results

Custom Fields

□ Modify Custom Fields □ Delete Custom Fields

Full Disk Encryption

□ Configure Full Disk Encryption □ Retrieve Recovery Keys

Classroom

□ Access Classroom

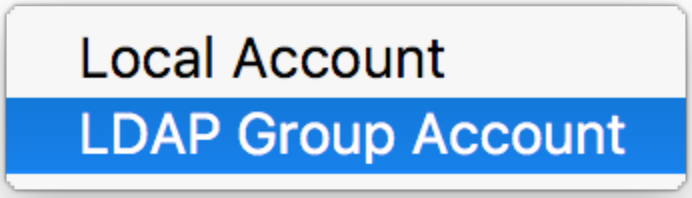
LDAP Group Account

If you have a LDAP server configured within your FileWave Preferences, administrators can authenticate using credentials stored in the LDAP server, based on Group membership. If a user is a member of multiple Groups, the final permissions will be the UNION of the permissions of these Groups. Only Active Directory is able to detect recursive membership. FileWave will not be able to detect nested Groups in an Open Directory or eDirectory.

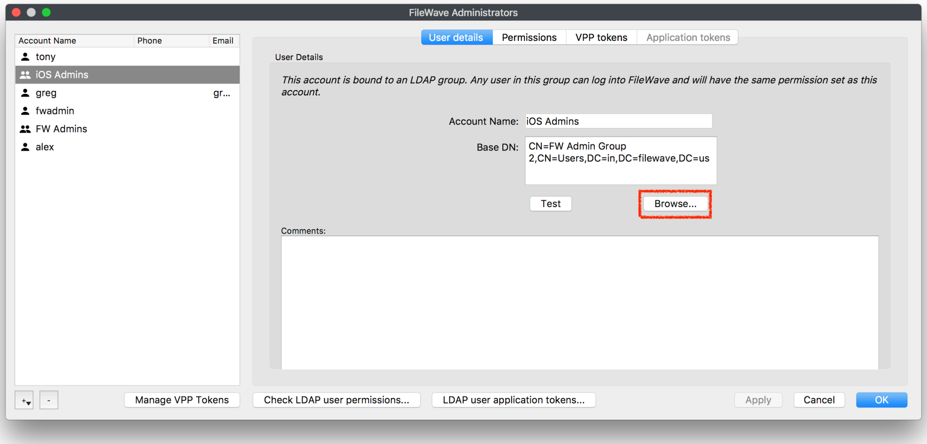
> To setup LDAP please see: 2.11. LDAP preferences

To create a LDAP Group Account for the FileWave Admin follow the steps below:

1. Go to **Assistants Manage Administrators**
2. Click on the the "+" sign at the bottom left
3. Then select LDAP Group Account



4. You will now be able to link this LDAP Group Account with a Group from your directory service. Click the **Browse...** button in the **User details** tab
   From here you will search through your LDAP structure to find the group you would like to use:



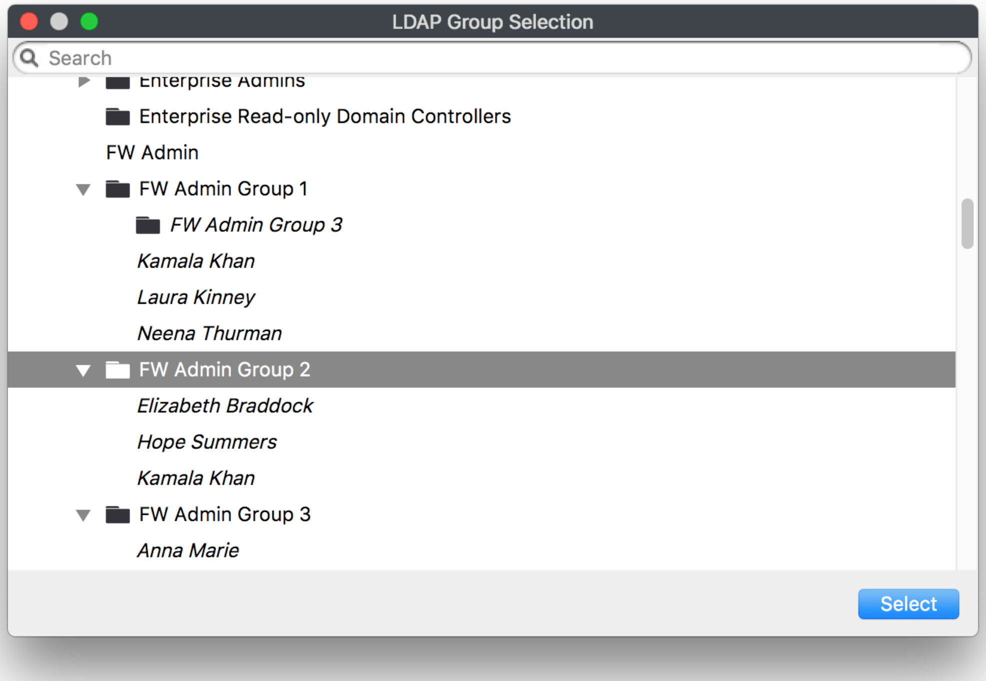
Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

This account is bound to an LDAP group. Any user in this group can log into FileWave and will have the same permission set as this account.

Account Name: iOS Admins

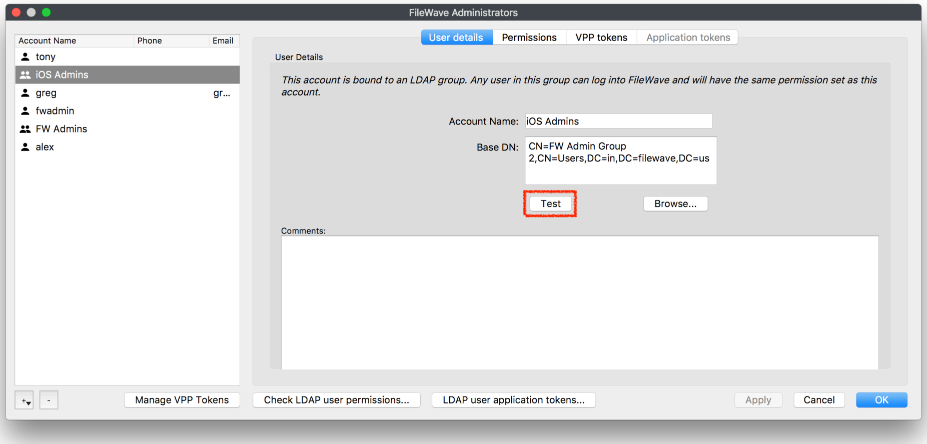
Base DN: CN=FW Admin Group 2,CN=Users,DC=in,DC=filewave,DC=us

Comments:



Enterprise Admins
Enterprise Read-only Domain Controllers
FW Admin
FW Admin Group 1
FW Admin Group 3
Kamala Khan
Laura Kinney
Neena Thurman
FW Admin Group 2
Elizabeth Braddock
Hope Summers
Kamala Khan
FW Admin Group 3
Anna Marie

5. (OPTIONAL) After the group is selected you can hit the Test button, this is used mainly if you typed in the DN instead of searching for the group in the browser



Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

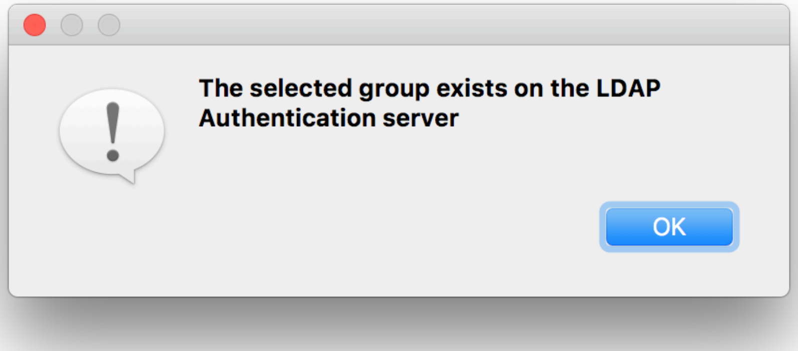
User Details

This account is bound to an LDAP group. Any user in this group can log into FileWave and will have the same permission set as this account.

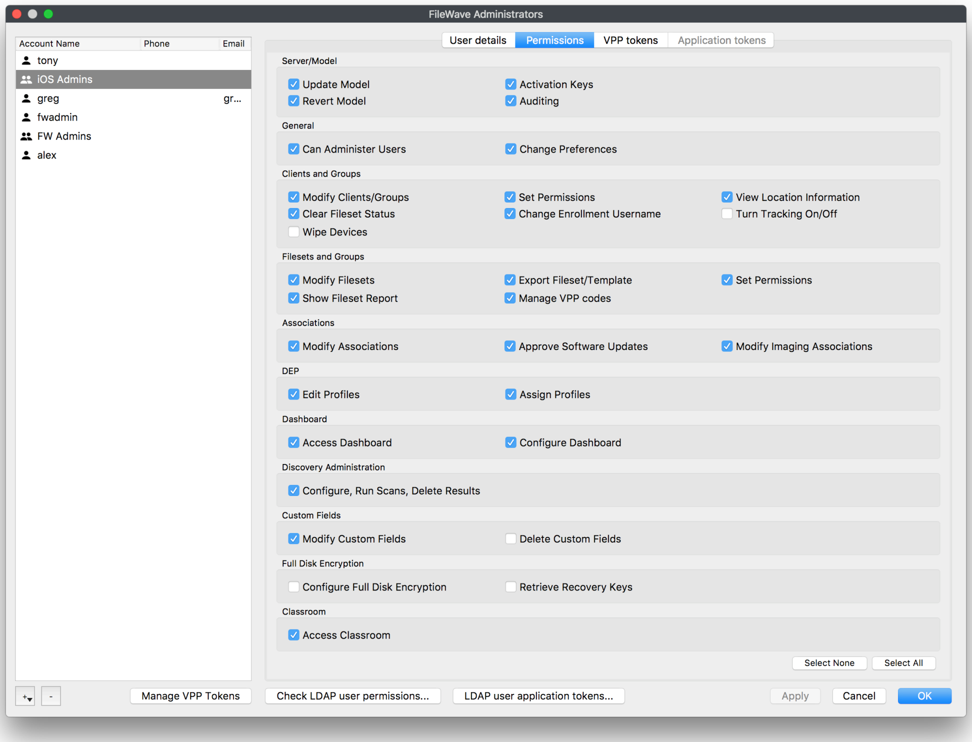
Account Name: iOS Admins

Base DN: CN=FW Admin Group 2,CN=Users,DC=in,DC=filewave,DC=us

Comments:


The selected group exists on the LDAP Authentication server

6. Next you will need to give this user permissions in FileWave, you do this by selecting the user and going into the **Permissions** tab and checking which options you want this user to have. (More information on what each of these options do at the end of this section)


FileWave Administrators

Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

Server/Model
☑ Update Model ☑ Activation Keys
☑ Revert Model ☑ Auditing

General
☑ Can Administer Users ☑ Change Preferences

Clients and Groups
☑ Modify Clients/Groups ☑ Set Permissions ☑ View Location Information
☑ Clear Fileset Status ☑ Change Enrollment Username □ Turn Tracking On/Off
□ Wipe Devices

Filesets and Groups
☑ Modify Filesets ☑ Export Fileset/Template ☑ Set Permissions
☑ Show Fileset Report ☑ Manage VPP codes

Associations
☑ Modify Associations ☑ Approve Software Updates ☑ Modify Imaging Associations

DEP
☑ Edit Profiles ☑ Assign Profiles

Dashboard
☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration
☑ Configure, Run Scans, Delete Results

Custom Fields
☑ Modify Custom Fields □ Delete Custom Fields

Full Disk Encryption
□ Configure Full Disk Encryption □ Retrieve Recovery Keys

Classroom
☑ Access Classroom

Select None
Select All
+
-
Manage VPP Tokens
Check LDAP user permissions...
LDAP user application tokens...
Apply
Cancel
OK

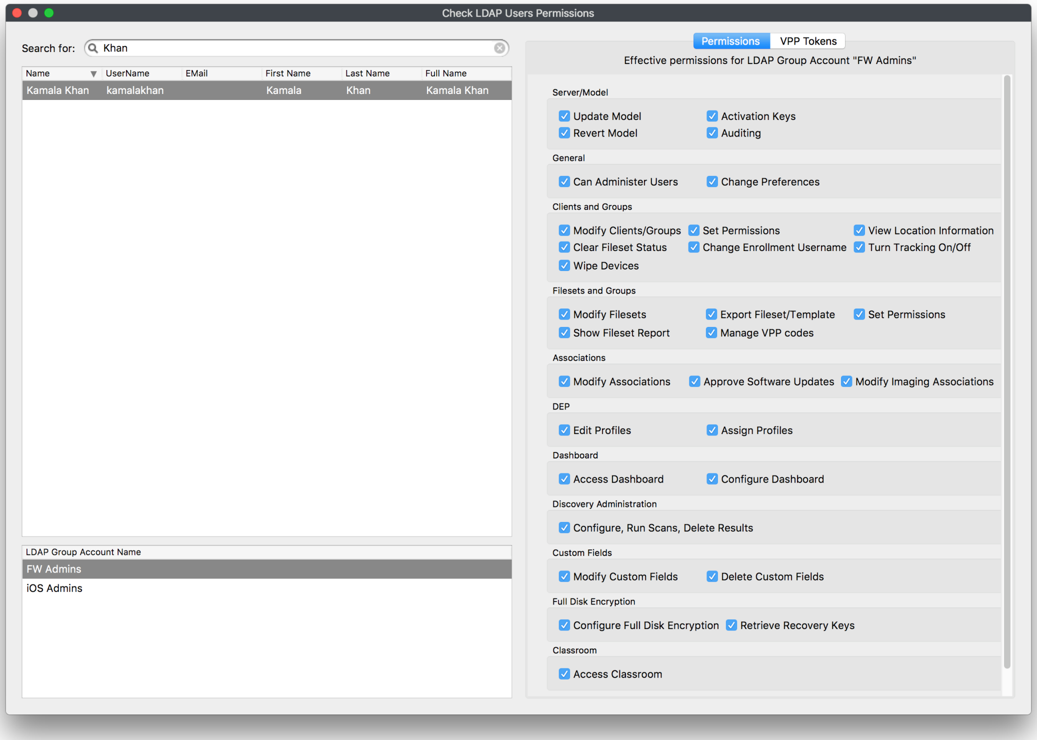
Permissions

Account permissions will determine what the Administrator can and cannot do in the FileWave Admin.

Selecting your Local Account or LDAP Group account and then going into the Permissions tab will give you all the permissions you can select for that user or group of users from LDAP.

LDAP Group Account Permissions:

If you have a user in multiple LDAP Group Accounts the user will take the collective permissions from each group. You can check on what permissions a LDAP user will get by selecting the **LDAP user application tokens...** and searching for that user:



Search for: Khan

Name	UserName	EMail	First Name	Last Name	Full Name
Kamala Khan	kamalakhan		Kamala	Khan	Kamala Khan

LDAP Group Account Name
FW Admins
iOS Admins

Effective permissions for LDAP Group Account "FW Admins"

Server/Model

☑ Update Model ☑ Activation Keys
☑ Revert Model ☑ Auditing

General

☑ Can Administer Users ☑ Change Preferences

Clients and Groups

☑ Modify Clients/Groups ☑ Set Permissions ☑ View Location Information
☑ Clear Fileset Status ☑ Change Enrollment Username ☑ Turn Tracking On/Off
☑ Wipe Devices

Filesets and Groups

☑ Modify Filesets ☑ Export Fileset/Template ☑ Set Permissions
☑ Show Fileset Report ☑ Manage VPP codes

Associations

☑ Modify Associations ☑ Approve Software Updates ☑ Modify Imaging Associations

DEP

☑ Edit Profiles ☑ Assign Profiles

Dashboard

☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration

☑ Configure, Run Scans, Delete Results

Custom Fields

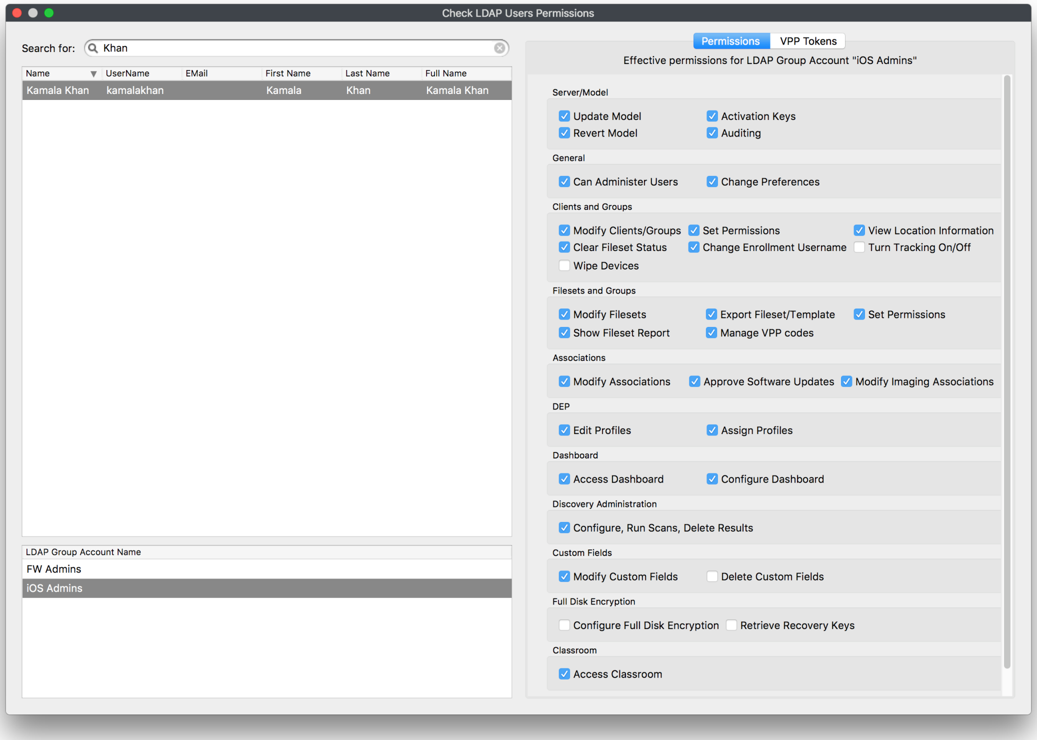
☑ Modify Custom Fields ☑ Delete Custom Fields

Full Disk Encryption

☑ Configure Full Disk Encryption ☑ Retrieve Recovery Keys

Classroom

☑ Access Classroom



Search for: Khan

Name	UserName	EMail	First Name	Last Name	Full Name
Kamala Khan	kamalakhan		Kamala	Khan	Kamala Khan

LDAP Group Account Name
FW Admins
iOS Admins

Effective permissions for LDAP Group Account "iOS Admins"

Server/Model

☑ Update Model ☑ Activation Keys
☑ Revert Model ☑ Auditing

General

☑ Can Administer Users ☑ Change Preferences

Clients and Groups

☑ Modify Clients/Groups ☑ Set Permissions ☑ View Location Information
☑ Clear Fileset Status ☑ Change Enrollment Username □ Turn Tracking On/Off
□ Wipe Devices

Filesets and Groups

☑ Modify Filesets ☑ Export Fileset/Template ☑ Set Permissions
☑ Show Fileset Report ☑ Manage VPP codes

Associations

☑ Modify Associations ☑ Approve Software Updates ☑ Modify Imaging Associations

DEP

☑ Edit Profiles ☑ Assign Profiles

Dashboard

☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration

☑ Configure, Run Scans, Delete Results

Custom Fields

☑ Modify Custom Fields □ Delete Custom Fields

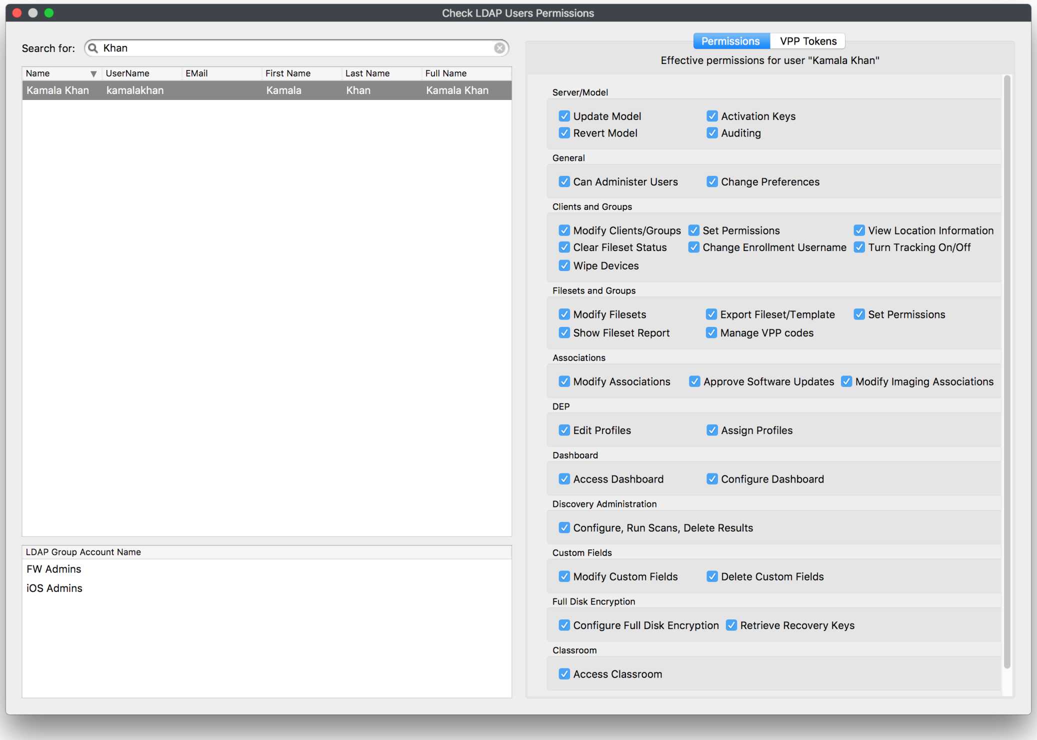
Full Disk Encryption

□ Configure Full Disk Encryption □ Retrieve Recovery Keys

Classroom

☑ Access Classroom

As you can see in the screenshots above the user Kamala Khan is in both the FW Admins and the iOS Admins LDAP Group which has fewer permissions than the FW Admins group does. So this user will use the permissions gathered from both of these groups which will give her full access as you can see in the screenshot below:



Check LDAP Users Permissions

Search for: Khan

Name	UserName	EMail	First Name	Last Name	Full Name
Kamala Khan	kamalakhan		Kamala	Khan	Kamala Khan

LDAP Group Account Name
FW Admins
iOS Admins

Effective permissions for user "Kamala Khan"

Server/Model

☑ Update Model ☑ Activation Keys
☑ Revert Model ☑ Auditing

General

☑ Can Administer Users ☑ Change Preferences

Clients and Groups

☑ Modify Clients/Groups ☑ Set Permissions ☑ View Location Information
☑ Clear Fileset Status ☑ Change Enrollment Username ☑ Turn Tracking On/Off
☑ Wipe Devices

Filesets and Groups

☑ Modify Filesets ☑ Export Fileset/Template ☑ Set Permissions
☑ Show Fileset Report ☑ Manage VPP codes

Associations

☑ Modify Associations ☑ Approve Software Updates ☑ Modify Imaging Associations

DEP

☑ Edit Profiles ☑ Assign Profiles

Dashboard

☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration

☑ Configure, Run Scans, Delete Results

Custom Fields

☑ Modify Custom Fields ☑ Delete Custom Fields

Full Disk Encryption

☑ Configure Full Disk Encryption ☑ Retrieve Recovery Keys

Classroom

☑ Access Classroom

What are all the permissions you can choose from?

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.

General

- *Can Administer users* - allows administrator to add, edit, or delete administrative users.
- *Change Preferences* - allows administrator to access the FileWave Admin Preferences

Clients and Groups

- *Modify Clients / Groups* - allows administrator the ability to add, edit, and delete FW clients and client Groups.
- *Set Permissions* - allows the administrator to assign clients and client Groups to specific administrators.
- *View Location* - Location map will be shown if the device is reporting location data.
- *Clear Fileset Status* - allows administrator the ability to remove all messages in the client info window for a designated client.
- Change Enrollment Username - this allows the administrator to change the enrollment username for MDM enrolled device, located in the client tools.
- *Turn Tracking On/Off* - gives the administrator the ability to switch the client state of a device for location tracking to Normal, Missing, or Not Tracked.
- *Wipe Devices* - this allows administrators the ability to wipe devices in the FileWave Admin.

Filesets and Groups

- *Modify Filesets* - allows administrator to edit Filesets , add or delete content within a Fileset.
- *Export Fileset / Template* - allows the user to export a specific Fileset or a template for use on another FileWave server, or for archival purposes.
- *Set Permissions* - allows the administrator to change the permissions within a Fileset or Fileset Group.
- *Show Fileset Report* - allows administrator to view the Fileset report showing the status of that Fileset.
- *Manage VPP codes* - with this unchecked and disallowed this will prevents administrators from accessing all VPP settings and menus, will also prevents the admins access to setup DEP tokens.
  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 VPP 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.
- *Approve Software Updates* - allows the administrator to designate specific software updates as pre-approved for association by other administrators.
- *Modify Imaging Associations* - allows the administrator to change which Imaging Filesets are associated with which devices

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.

Dashboard

- *Access Dashboard* - Which administrators can see the Dashboard in the FileWave Admin or via web browser.
- *Configure Dashboard* - This determines which administrators have access to Dashboard Alert settings.

Discovery Administration

- *Configure, Run Scans, Delete Results* - administrator can configure and control network scans and delete discovery results.

Custom Fields

- *Modify Custom Fields* - Allows administrators to create, modify, and assign custom fields to devices.
- *Delete Custom Fields* - This will allow the deletion of custom fields

Full Disk Encryption

- *Configuration Full Disk Fields* - allows the FileWave administrator to access and configure **FDE Configure Management** located in the **Assistant** menu
- *Retrieve Recovery Keys* - allows the FileWave administrator to access and configure **FDE Recovery Key Management** located in the **Assistant** menu

Classroom

- *Access Classroom* - allows the administrator to access the Classroom section in the FileWave Admin, this includes carts, cart clones, cart associations

> **Important Note:**
> If you are upgrading from below FileWave 12.9 this Classroom option will be unchecked by default. So you will no longer able to view Classroom in FileWave until this is checked for selected administrators.

Application tokens

FileWave security for inventory has been built on top of a shared secret, which is a long token generated randomly and shared between the server (inventory server) and clients (admin, FileWave server, client machines, scripts, etc)

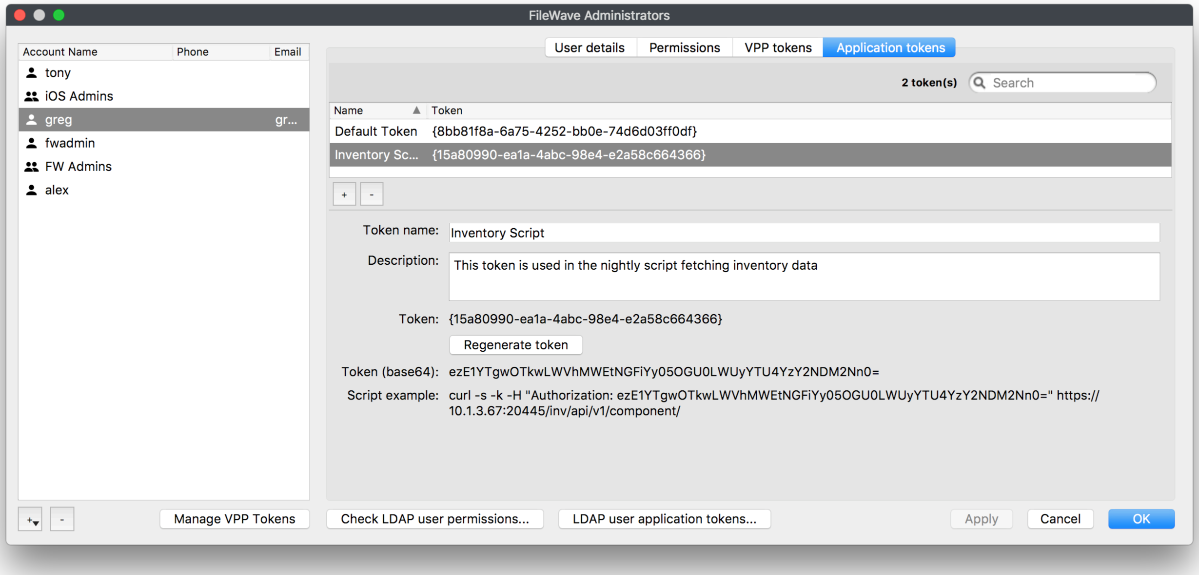
Any script or 3rd party component that needs access to FileWave Inventory will need to have this token that has been assigned to a user. These tokens can be revoked, re-generated, and a user can have multiple tokens assigned to it.

Every Local account starts with a Default Token which can be used along with any news ones that are created.

> The **Default Token** for your Superuser will be the same token that was originally in the **Inventory** tab in FileWave Preferences in versions 12.8.1 and below. If you upgraded from 12.8.1 or below then all communication with this token will stay intact unless you **Regenerate** the default token.

Local Account New Application Token Setup:

1. Select your Local Account and go into the **Application tokens** tab
2. Once there hit the "+" at the bottom left of the tokens pane
3. This will then allow you create a new token



Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

2 token(s)

Name	Token
Default Token	{8bb81f8a-6a75-4252-bb0e-74d6d03ff0df}
Inventory Sc...	{15a80990-ea1a-4abc-98e4-e2a58c664366}

Token name: Inventory Script

Description: This token is used in the nightly script fetching inventory data

Token: {15a80990-ea1a-4abc-98e4-e2a58c664366}

Token (base64): ezE1YTgwOTkwLWVhMWEtNGFiYy05OGU0LWUyYTU4YzY2NDM2Nn0=

Script example:

```
curl -s -k -H "Authorization: ezE1YTgwOTkwLWVhMWEtNGFiYy05OGU0LWUyYTU4YzY2NDM2Nn0=" https://
10.1.3.67:20445/inv/api/v1/component/
```

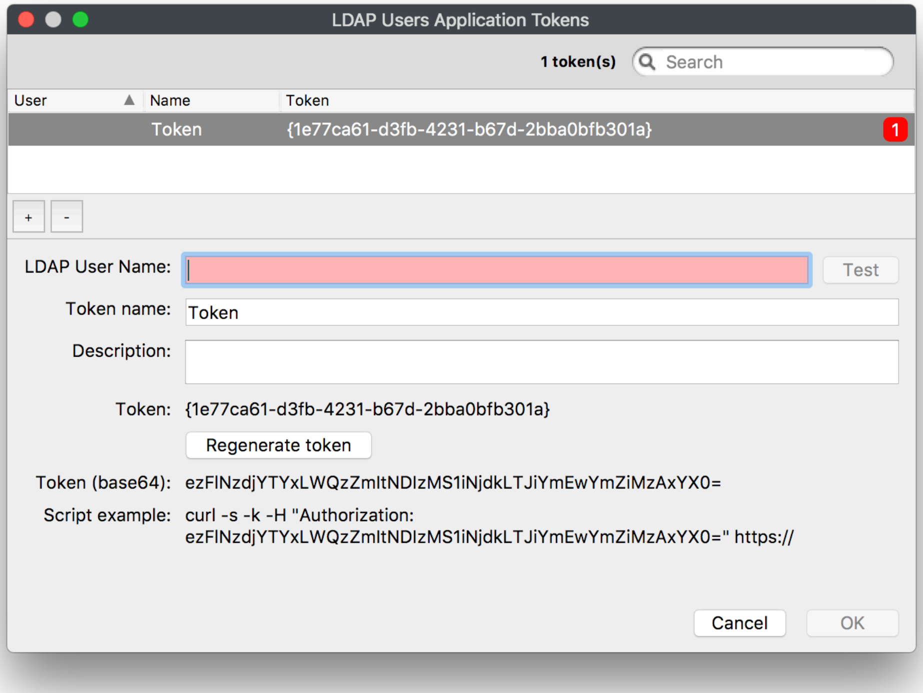
4. This will show
    a. The raw token
    b. base64 encoded token
    c. An example script you can copy and paste to test with

LDAP user application tokens

Just like Local Accounts it is possible to define application tokens for LDAP users as well. This will not be done at the group level but for the specific LDAP Users.

To setup the application tokens for LDAP users follow the steps bellow:

1. In the **FileWave Administrators** window click on the **LDAP user application tokens...** button located at the bottom middle of the window
2. You will then get the **LDAP Users Application Tokens** window, click the "+" at the bottom left of the token pane to create a new token



User	Name	Token
	Token	{1e77ca61-d3fb-4231-b67d-2bba0bfb301a} 1

LDAP User Name:

Token name: Token

Description:

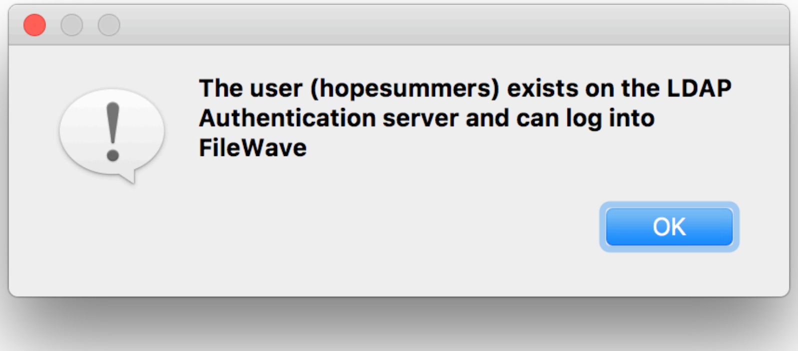
Token: {1e77ca61-d3fb-4231-b67d-2bba0bfb301a}

Token (base64): ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=

Script example:

```
curl -s -k -H "Authorization:
ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=" https://
```

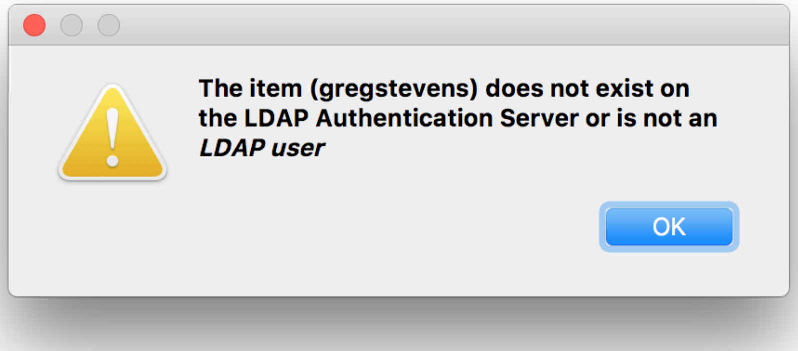
3. Then you will need to type in the LDAP user you would like to use and click the **Test** button to confirm it



The user (hopesummers) exists on the LDAP Authentication server and can log into FileWave

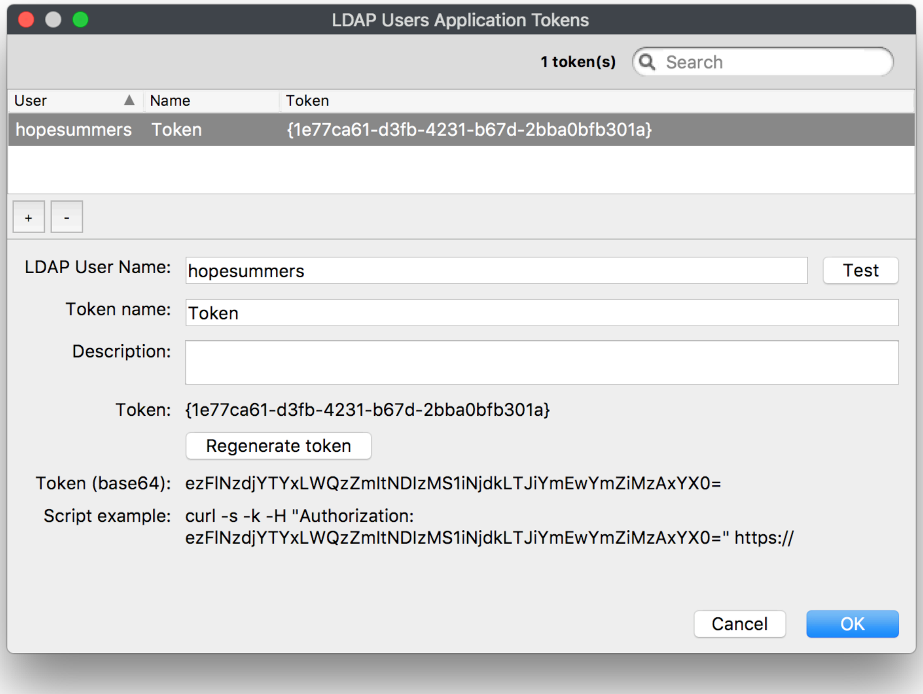
LDAP User TEST
The test will make sure the user belongs to the LDAP server configured for authentication in the FileWave Preferences and will also make sure the user belongs to at least 1 LDAP group defined in the main FileWave Administrators window.
Note: The part of the test to check for the LDAP group in FileWave is cached for 1 hour. The cache is reset every time you save the user dialog, or change the LDAP server in preferences or if you do a LDAP "synchronize".

If you search for a user that is not in your directory service or it doesn't belong to an LDAP Group Account in FileWave it will fail.



The item (gregstevens) does not exist on the LDAP Authentication Server or is not an *LDAP user*

4. Once it has confirmed you are ready to use the token



LDAP Users Application Tokens

1 token(s)

User	Name	Token
hopesummers	Token	{1e77ca61-d3fb-4231-b67d-2bba0bfb301a}

LDAP User Name: hopesummers

Token name: Token

Description:

Token: {1e77ca61-d3fb-4231-b67d-2bba0bfb301a}

Token (base64): ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=

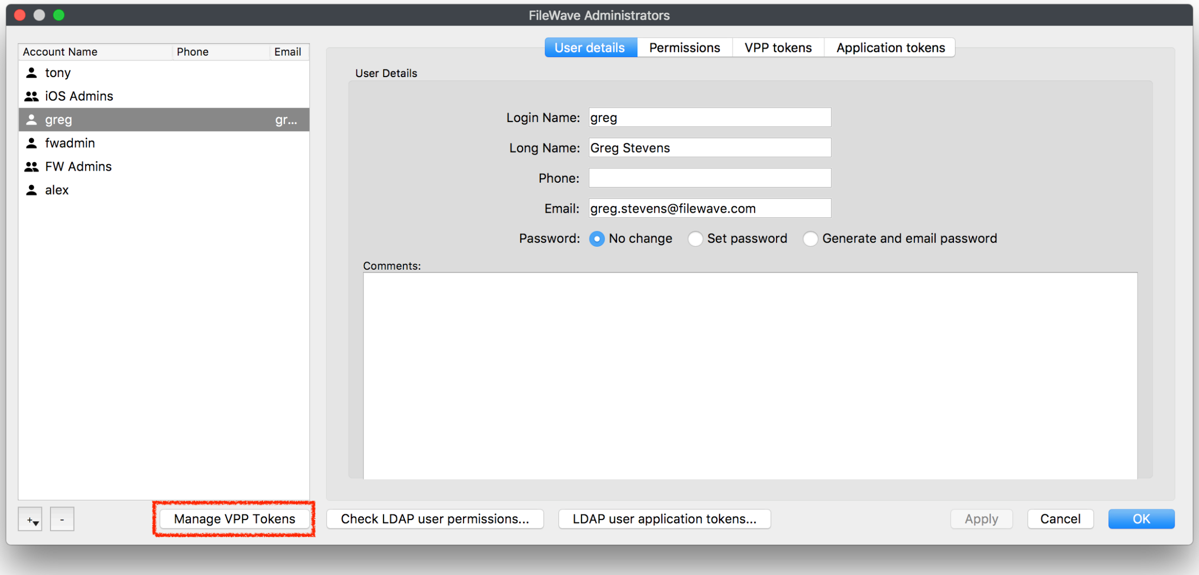
Script example: curl -s -k -H "Authorization: ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=" https://

Manage VPP Tokens

To allow specific FileWave Administrators to access and see VPP purchases they will need to be given access using this **Manage VPP Tokens** option in the **Manage Administrators...** section.

By default only the Superuser (fwadmin) has access to new VPP tokens imported in FileWave any other Administrators created needs to be given access.

1. Click the **Manage VPP Tokens** button at the bottom



FileWave Administrators

Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

User Details

Login Name: greg

Long Name: Greg Stevens

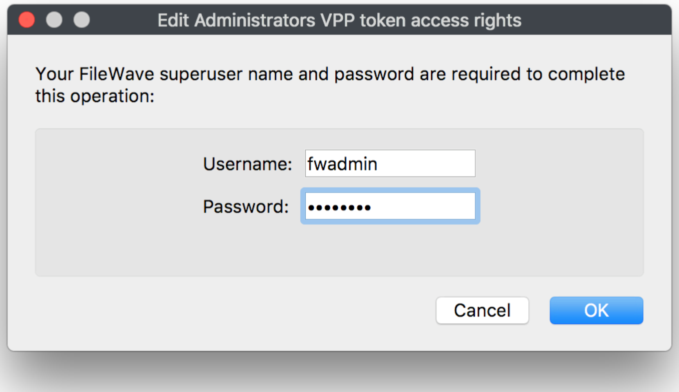
Phone:

Email: greg.stevens@filewave.com

Password: ● No change ○ Set password ○ Generate and email password

Comments:

2. You need to authenticate with the Superuser



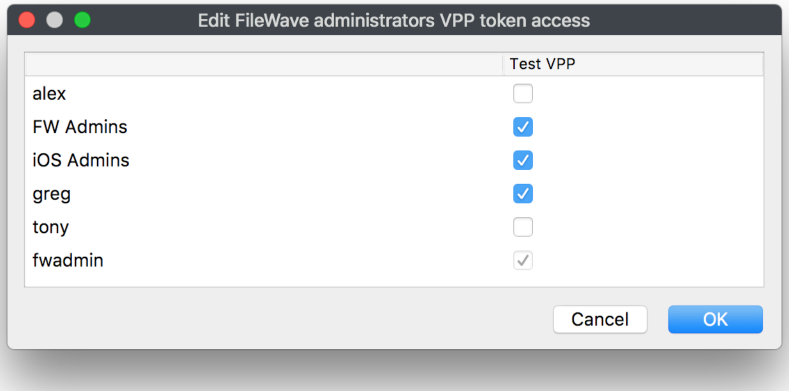
Edit Administrators VPP token access rights

Your FileWave superuser name and password are required to complete this operation:

Username: fwadmin

Password: ••••••••

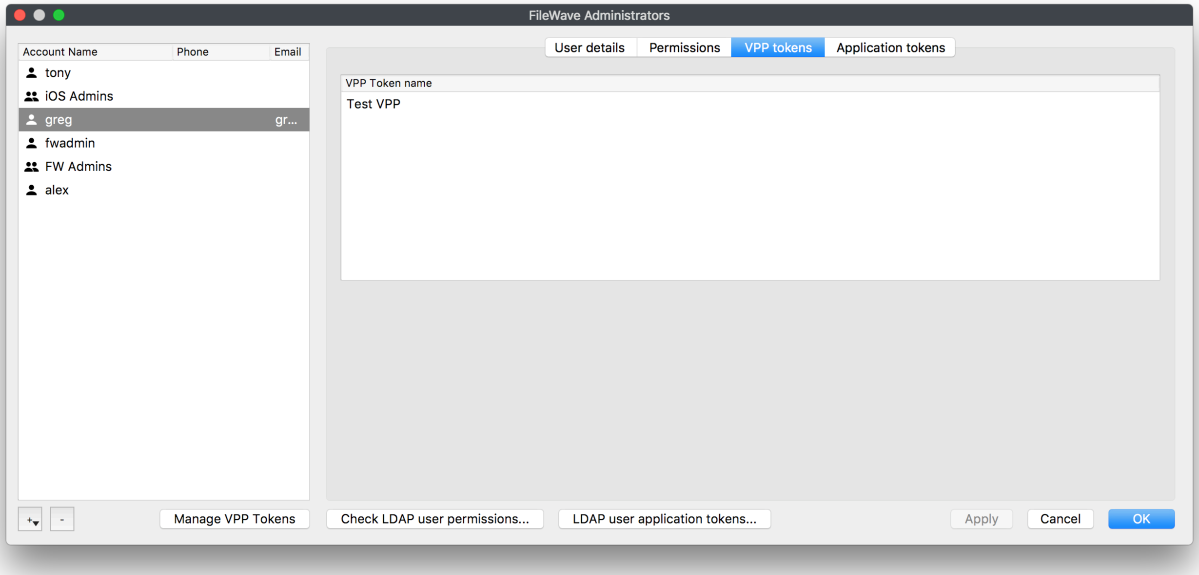
3. Now you will check which users you would like to manage which VPP Token



Edit FileWave administrators VPP token access

	Test VPP
alex	☐
FW Admins	☑
iOS Admins	☑
greg	☑
tony	☐
fwadmin	✓

4. Once you click **OK** you will be able to view which tokens a specific user has access to by looking in the **VPP tokens** tab



Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

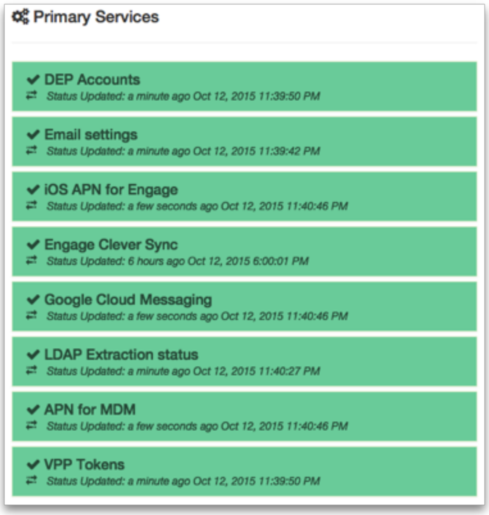
VPP Token name
Test VPP

2.16. 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.


Primary Services

✓ DEP Accounts
Status Updated: a minute ago Oct 12, 2015 11:39:50 PM

✓ Email settings
Status Updated: a minute ago Oct 12, 2015 11:39:42 PM

✓ iOS APN for Engage
Status Updated: a few seconds ago Oct 12, 2015 11:40:46 PM

✓ Engage Clever Sync
Status Updated: 6 hours ago Oct 12, 2015 6:00:01 PM

✓ Google Cloud Messaging
Status Updated: a few seconds ago Oct 12, 2015 11:40:46 PM

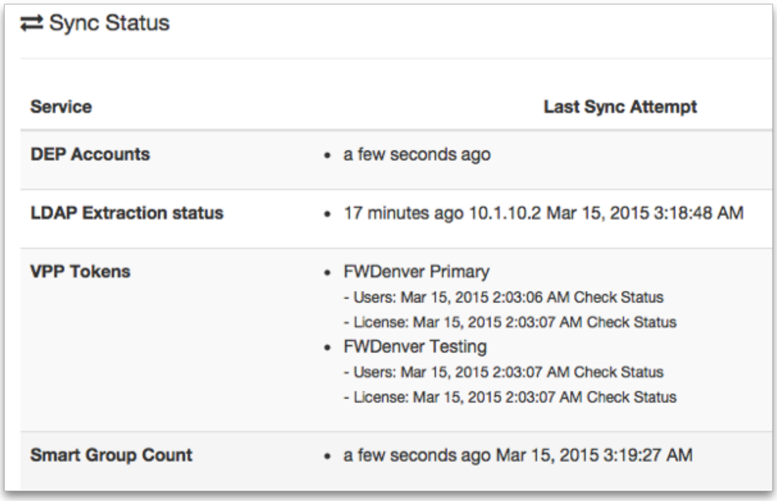
✓ LDAP Extraction status
Status Updated: a minute ago Oct 12, 2015 11:40:27 PM

✓ APN for MDM
Status Updated: a few seconds ago Oct 12, 2015 11:40:46 PM

✓ VPP Tokens
Status Updated: a minute ago Oct 12, 2015 11:39:50 PM

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.

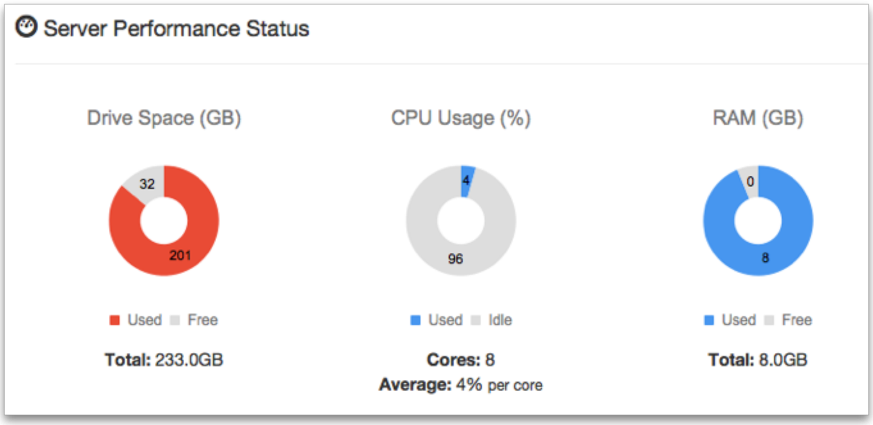


⇄ Sync Status

Service	Last Sync Attempt
DEP Accounts	• a few seconds ago
LDAP Extraction status	• 17 minutes ago 10.1.10.2 Mar 15, 2015 3:18:48 AM
VPP Tokens	• FWDenver Primary - Users: Mar 15, 2015 2:03:06 AM Check Status - License: Mar 15, 2015 2:03:07 AM Check Status • FWDenver Testing - Users: Mar 15, 2015 2:03:07 AM Check Status - License: Mar 15, 2015 2:03:07 AM Check Status
Smart Group Count	• a few seconds ago Mar 15, 2015 3:19:27 AM

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.



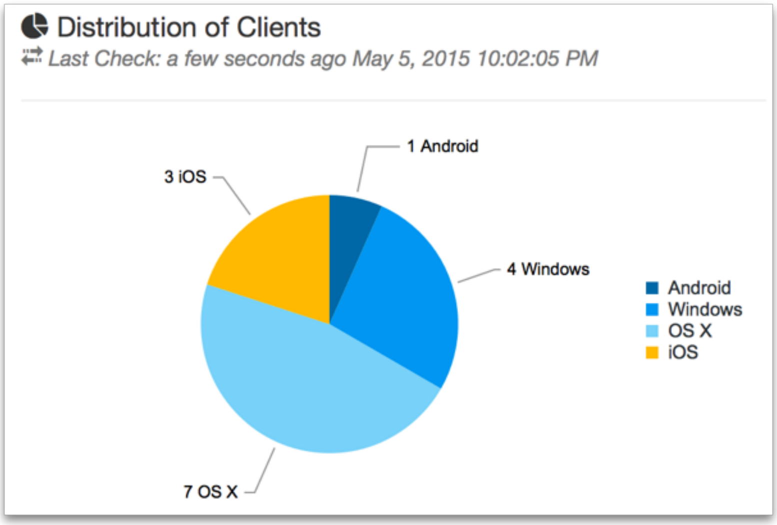
Total: 233.0GB

Cores: 8
Average: 4% per core

Total: 8.0GB

Distribution of clients

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

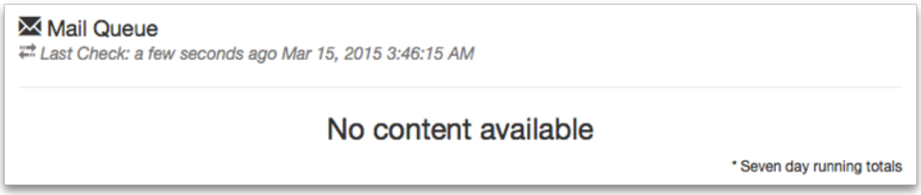


Distribution of Clients

Last Check: a few seconds ago May 5, 2015 10:02:05 PM

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.



Mail Queue

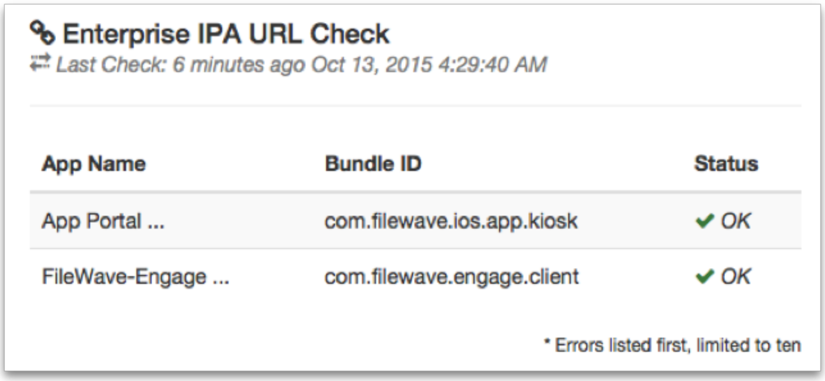
Last Check: a few seconds ago Mar 15, 2015 3:46:15 AM

No content available

* Seven day running totals

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).



Enterprise IPA URL Check

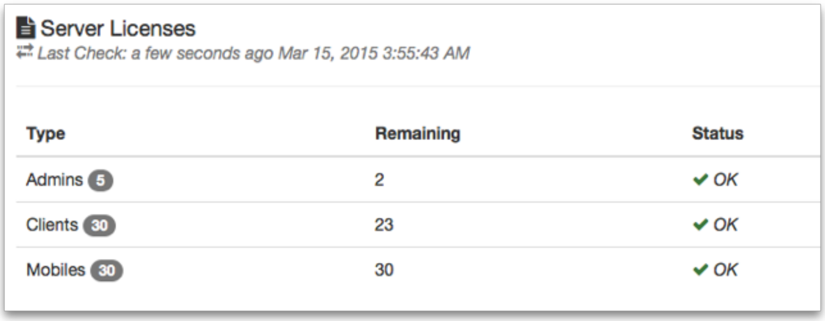
Last Check: 6 minutes ago Oct 13, 2015 4:29:40 AM

App Name	Bundle ID	Status
App Portal ...	com.filewave.ios.app.kiosk	✓ *OK*
FileWave-Engage ...	com.filewave.engage.client	✓ *OK*

* Errors listed first, limited to ten

Server Licenses

This section shows the current status of your FileWave server license.



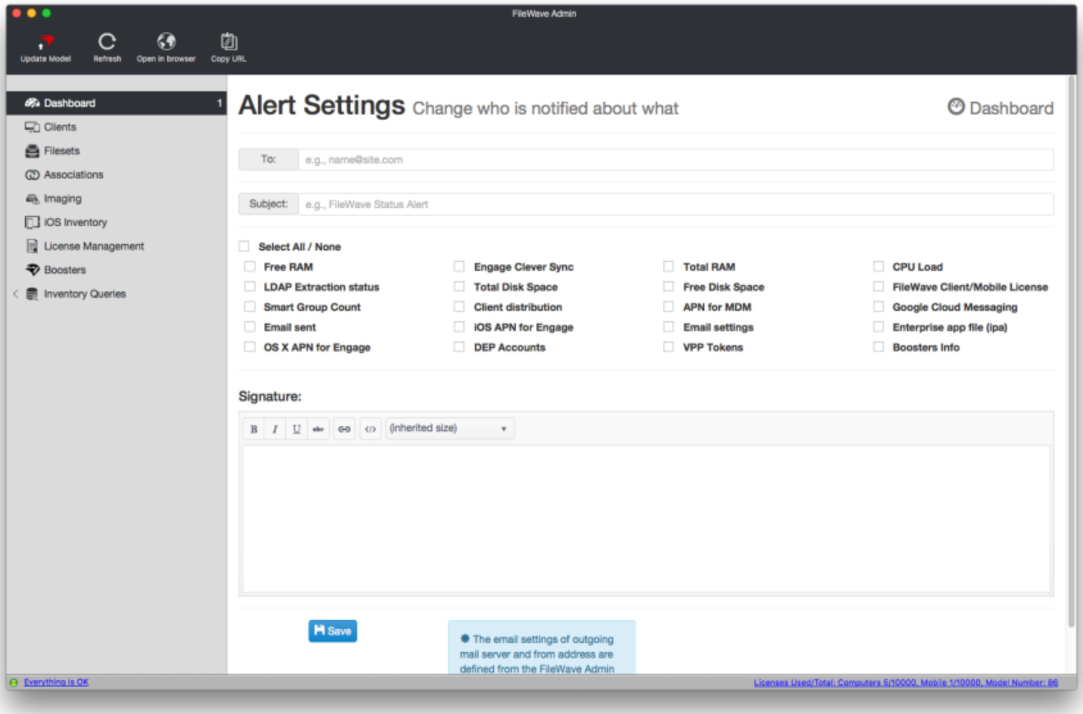
Server Licenses

Last Check: a few seconds ago Mar 15, 2015 3:55:43 AM

Type	Remaining	Status
Admins 5	2	✓ OK
Clients 30	23	✓ OK
Mobiles 30	30	✓ OK

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.



Alert Settings Change who is notified about what

To: e.g., name@site.com

Subject: e.g., FileWave Status Alert

□ Select All / None

□ Free RAM
□ LDAP Extraction status
□ Smart Group Count
□ Email sent
□ OS X APN for Engage
□ Engage Clever Sync
□ Total Disk Space
□ Client distribution
□ iOS APN for Engage
□ DEP Accounts
□ Total RAM
□ Free Disk Space
□ APN for MDM
□ Email settings
□ VPP Tokens
□ CPU Load
□ FileWave Client/Mobile License
□ Google Cloud Messaging
□ Enterprise app file (ipa)
□ Boosters Info

Signature:

The email settings of outgoing mail server and from address are defined from the FileWave Admin

Licenses Used/Total: Computers 5/10000, Mobile 1/10000, Model Number: 86

The result is an email when an event is triggered being sent to the designated email account.

"Detachable" 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 a browser, or provided as a URL to other interested parties to view on their own computers or devices.

Dashboard Alert details

A table with explanations of all of the available alert items from the Dashboard is available in the Dashboard Warning levels and Descriptions KB.

2.17. Migrating FileWave Server Info and Moving Data

When the time comes to upgrade or 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 and Inventory data) to a different drive/storage area, the process for doing that is reasonably straight forward.

Migrating FileWave Server

The best practice for migrating your FileWave Server is to follow the instructions in this link: Migrating your FileWave Server to new Hardware
It is always a good idea to check in with FileWave Support before the migration to see if there are any tips or revised instructions.

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 improve performance. Check your pathnames!
Start by stopping the FileWave server (Linux, OS X):

```
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
```

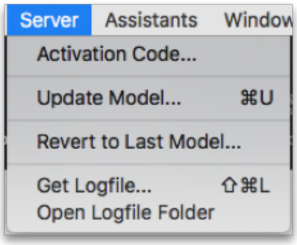
Finally, restart the FileWave server

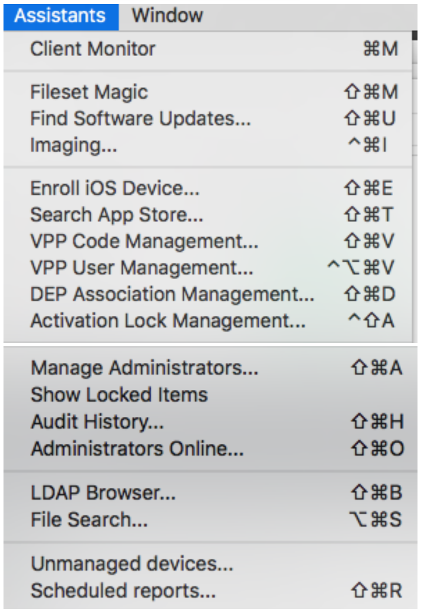
```
fwcontrol server start
```

For more information on this topic, please see: Store the FileWave Server/Booster data on a separate volume

2.18. FileWave Admin - additional settings_menu items

In the FileWave Admin application, there are several other settings and menu items that come into play as you manage and configure your devices. They appear in two menu sets (Server & Assistants) as shown:





Some of these items have already been covered, and others will be discussed in depth later in this manual. Here are basic descriptions of the function of these menu items.

Activation Code…

This is the access to the code you received when you purchased your FileWave license. Setting this up was discussed early in Chapter **2**.

Update Model…

FileWave, at its core, is a SQL database. As such, it is constantly managing large amounts of data as you, and possibly other administrators, add new clients, create Filesets for new content distribution, and manage your devices. When you are performing many of these operations, the information is being written into RAM on the server. A **Model** is an instance in time for the FileWave database. When you choose the **Update Model**, you are telling the server to write the changes you have made into the database, and create a **manifest** for the Clients. This manifest is sent to each Client when it checks in, telling it what changes have been made. If there is a change that effects the Client, it will then request any new or updated Filesets and will then make the appropriate changes on the device. Whenever you make changes to device(s), edit Filesets, or do anything that may affect the relationship between a device and the server, you should update the model.

Revert to Last Model…

If you have made a change to the **Model**, then realize that you may have damaged a setting, or distributed a broken application, you can revert to the previous model within the FileWave database. In many cases, this can be done without any irreversible changes to the client devices.

Get Logfile…

This menu item allows you to grab a copy of the latest FileWave server process log. It will tell you how your server is behaving, and what is going on. It is very useful for troubleshooting problems.

Open Logfile Folder

This menu item opens the folder on the FileWave Admin system that contains all of the logfiles that have been requested by that administrator. These are copies of the FileWave server logs retrieved when you selected the **Get Logfile…** menu item.

Client Monitor

The Client Monitor is a tool used to observe the status of a specific device. It displays the current state of the device, the current Model number on the device, and you can see if the device is reacting to changes being made by clicking on the **Verify** button. Detailed information on Client Monitor is in the Chapter **Clients**.

Fileset Magic

Custom content can be created using the **Fileset Magic** tool. It allows you to take a snapshot of the current status of a device, install and configure new content, take a second snapshot, and build a distribution Fileset from those changes. More on Fileset magic in the Chapter on **File sets**.

Find Software Updates…

This menu item opens a management pane to look for all iOS / macOS / Windows software updates that are available. The updates can be viewed by just the ones that your devices have been requesting, or by every update published for that platform. The use of this capability is covered in the Chapter on **Filesets**.

Imaging…

This item opens the **Imaging** pane that allows you to associate disk images with OS X and Windows devices for re-imaging. All of Chapter **9** is devoted to Imaging.

Enroll iOS Device…

This item opens the pane with the various settings for enrolling iOS devices, and AppleTV, either manually or automatically. Details on this process are covered in Chapter **4**.

Search App Store…

This menu item opens a search pane to look for content on the Apple App Store. Details on using this item are in the Chapter on **Filesets**.

VPP Code Management… / VPP User Management…

These two menu items relate to Apple's Volume Purchase Program within FileWave. They allow you to manage the distribution of institutionally purchased content. VPP operations are covered in detail in both Chapter **5 (Filesets)** and Chapter **6 (License Management)**.

DEP Association Management…

This menu item relates the Apple Device Enrollment Program within FileWave. You use this pane to configure DEP profiles, and associate them to institutionally purchased devices. DEP is covered in Chapter **4 (Clients)**.

Activation Lock Management…

This menu item displays the status of your supervised iOS devices with activation lock active. The bypass codes are stored on the FileWave server for your use when taking these devices out of service. More on this in Chapter **7 (Mobile Device Management)**.

Manage Administrators…

This menu item opens the management pane for creating, editing, and managing the FileWave administrator account and sub-admin accounts. This operation is covered earlier in this Chapter.

Show Locked Items

This menu opens the window with a display of any and all aspects of the FileWave Admin UI that has been "taken control of" using the **Take Control** button, or that is in use by another FileWave administrator. For example, when an administrator needs to work on editing the sub-administrators, changing some settings in Clients, or editing a Fileset, they can **Take Control** of those specific items (and when they are finished, they can **Release Control**).
In the meantime, any administrator trying to work on those areas, can use the **Show Locked Items** menu to view areas they cannot control.
If an administrator has left items locked too long, or walked away from their system with items still locked, you can force quit that administrator (see **Administrators Online…** below). You should also make sure your sub-administrators set a reasonable auto-logout time in the **General** preferences of their FileWave Admin application.

Audit History…

This menu item displays a log of all actions taken by FileWave administrators, broken out by day.

Administrators Online…

This assistant menu lets you view the status of all of the FileWave administrators. If an administrator has been logged in too long, or has locked something you need access to, and they are not at available, you can force logoff that user.

LDAP Browser…

This menu selection displays a tree of your LDAP configuration that matchs what you entered in the **LDAP** preferences.

File Search…

This item displays a search window that allows you to locate any item in a Fileset using a text string search.
Once you have located your item, you can click on **Reveal in Fileset** to display the contents of the Fileset with that specific item.

Unmanaged Devices…

This menu item displays a pane with the "non-client" devices you are keeping track of. You can enter items such as printers, scanners, cameras, etc. to the set by clicking on [+] in the window.

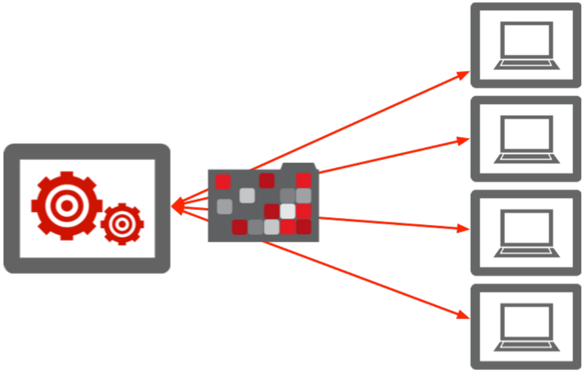
Scheduled Reports…

This menu item allows you to create and generate Inventory reports that are automatically sent to designated email accounts. The process for doing this is covered in detail in Chapter **8 (Inventory)**.

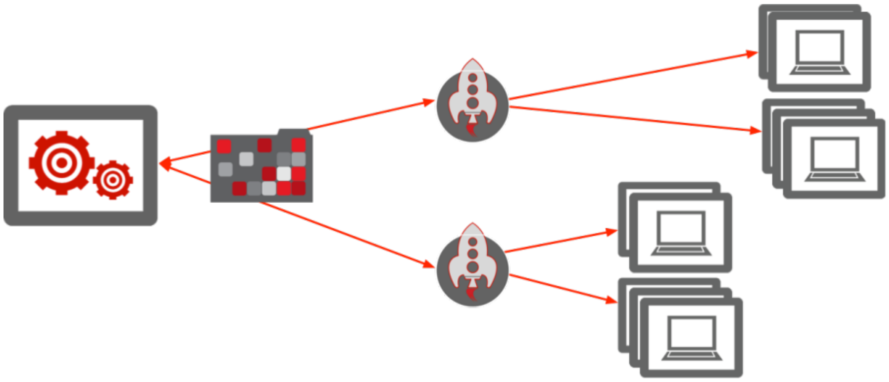
3. FileWave Boosters - installation, configuration, and management
Scalability for a systems management solution is essential. FileWave can manage an Inventory of thousands of devices in the FileWave Server; however, the distribution of a large number of Filesets with needed applications and content 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 computers. This, coupled with the changes to Booster messaging introduced in FileWave 11.1 which offloads the Client—Server communication (Clients check in at regular intervals – the default is every 120 seconds) to the Boosters (Clients communicate to with the Booster; the Booster rolls up all Client communications into a single Booster—Server socket connection), significantly reducies the network load on the FileWave Server.
Besides the new Discovery features, FileWave Admin v11.2.0 has an improved user interface for the Boosters view – a new "card layout" – that gives administrators clear information about the status of all running Boosters (Note: Card View requires OpenGL on the administrator machine running FileWave Admin). If an administrator is interested in a more detailed view of the Boosters, this is available as well.
The Booster status reporting has been improved. The status now reflects whether a given Booster is running or not running. Additionally, a new Booster state measurement has been added – "Booster Overload." It informs an administrator if there are any clients' requests that could not be served by a given Booster.
You can assign a human readable name to the Booster as well as a location. These options are configured using preferences in Booster Monitor.

Note: The FileWave Booster caches and forwards Filesets for computers and Android devices. It also handles all Client-Server communications, except for inventory data. Apple iOS device Filesets exist only at the main FileWave server and do not use Boosters for caching.

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 eventually the bandwidth between the Server and Clients will no longer be able to efficiently provide timely file transfers. Boosters exist to help offload the communication overhead between Clients and the FileWave Server and to cache Filesets from the FileWave Server closer to Groups of Clients that need those Filesets.
You can go from this



To this



Boosters can be configured to cache Filesets 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 FileWave 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. As soon as a request for a Fileset comes to the Booster from a Client, if the Fileset is not already present in the Booster's data folder the Booster contacts the FileWave Server to download this item, which it then sends the Client. 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 an Imaging Virtual Server.

3.1. 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 macOS-based FileWave 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 amount of data sent from the FileWave Server is a lot less with iOS devices, so a FileWave server can support many more iOS devices than it can computers.

If you include Apple caching servers into your environment this will then allow iOS and MDM enrolled macOS devices to download VPP apps from your Apple caching servers instead of having to leave your network to get them.

Some rules-of-thumb for Booster planning:

1. A Booster should be configured for every set of 2,000 or less devices.
2. A Booster should be configured to support every physical location, such as a building, campus, or city.
3. If there are multiple locations in a given geographic area that is removed from the data center hosting the FileWave Server, each of the location Boosters should connect to a central area Booster; e.g., city A has an area Booster, sites 1 – 4 each has at least one Booster, that is connected to Booster A, which in turn is connected to the FileWave Server.

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 Boosters.

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.

3.2. Booster system requirements

Operating Systems Supported:

- OS X v10.9 - v10.11 / macOS 10.12
- Windows 7 / 8 / 8.1 / 10
- Windows Server 2008R2 / 2012 / 2012R2
- CentOS 5.11 / 6.7 / 7.2

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.**

3.3. 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 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/**.
The FileWave Booster executable resides in one of these platform-dependent locations:
Windows: C:\Program Files\FileWave\fwBooster.exe
macOS, Linux: /usr/local/sbin/fwBooster

Installing the Booster on Linux

Download the latest FileWave binaries for Linux on the following Website:
http://www.filewave.com/support/software-downloads

1. To download the newest binaries, click on the newest version of FileWave, then scroll down until you see Linux installers.
2. Download the Linux Installers.
3. Copy the Zip file directly to your Linux Server inside the root folder **/root/**
4. Login with SSH to your Linux Server (on Windows you will need an **ssh** application, on OS X use **Terminal**), and login as ***root***
5. Unzip the file with the following commands:

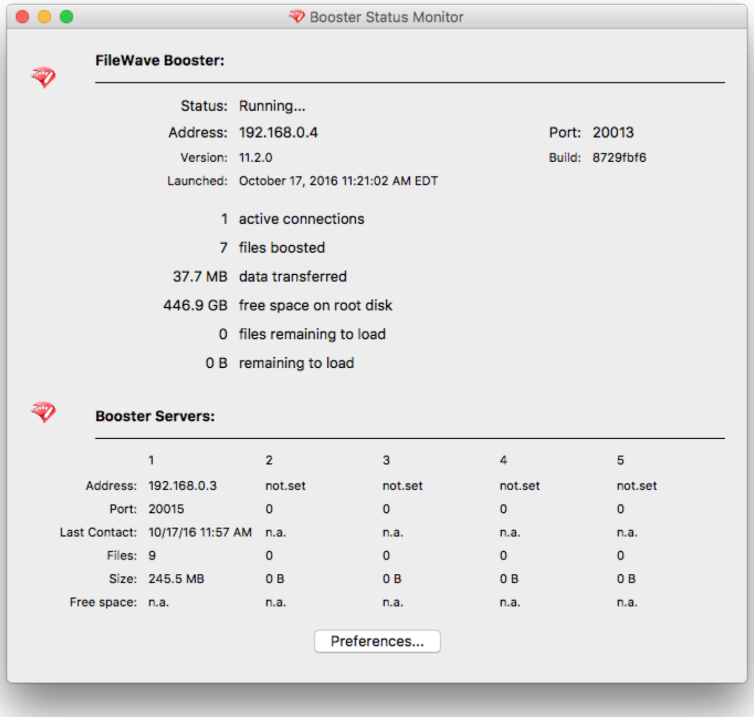
```
cd /root/
unzip yum install ~~y --nopgcheck fwBooster~~*.rpm
```

1. Answer the install question with **yes**

Your Booster is now installed

3.4. 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 its Status Monitor window:



Booster Status Monitor

FileWave Booster:

Status: Running...

Address: 192.168.0.4 Port: 20013

Version: 11.2.0 Build: 8729fbf6

Launched: October 17, 2016 11:21:02 AM EDT

1 active connections

7 files boosted

37.7 MB data transferred

446.9 GB free space on root disk

0 files remaining to load

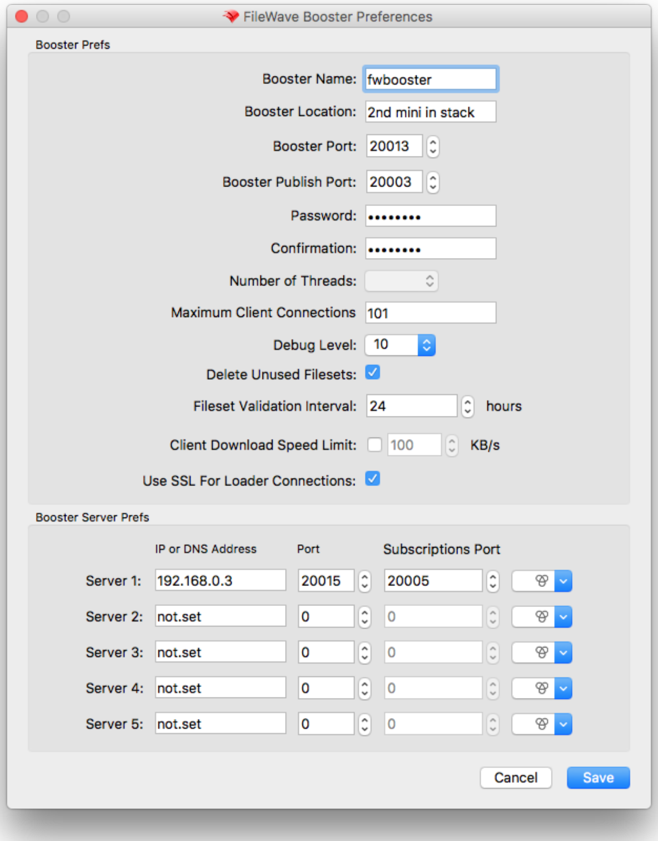
0 B remaining to load

Booster Servers:

	1	2	3	4	5
Address:	192.168.0.3	not.set	not.set	not.set	not.set
Port:	20015	0	0	0	0
Last Contact:	10/17/16 11:57 AM	n.a.	n.a.	n.a.	n.a.
Files:	9	0	0	0	0
Size:	245.5 MB	0 B	0 B	0 B	0 B
Free space:	n.a.	n.a.	n.a.	n.a.	n.a.

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 network traffic.

Booster Prefs



FileWave Booster Preferences

Booster Prefs

Booster Name: fwbooster

Booster Location: 2nd mini in stack

Booster Port: 20013

Booster Publish Port: 20003

Password: ••••••••

Confirmation: ••••••••

Number of Threads:

Maximum Client Connections 101

Debug Level: 10

Delete Unused Filesets: ☑

Fileset Validation Interval: 24 hours

Client Download Speed Limit: ☐ 100 KB/s

Use SSL For Loader Connections: ☑

Booster Server Prefs

	IP or DNS Address	Port	Subscriptions Port
Server 1:	192.168.0.3	20015	20005
Server 2:	not.set	0	0
Server 3:	not.set	0	0
Server 4:	not.set	0	0
Server 5:	not.set	0	0

- ***Booster Name*** – this is an identifier for you to distinguish a Booster in the FileWave Admin GUI. It does not have to be the hostname of the Booster, but would be a good practice to follow.
- ***Location*** – this is a text field to help someone know the physical location of the Booster (it shows in the Booster view of FileWave
- ***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 **4 (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**"
- *Number of Threads* – this is the number of threads spawned by the *fwBooster* process. With FileWave 11, this value is no longer user-adjustable. The value will be automatically adjusted depending upon the hardware resources available to the f*wBooster* process.
- ***Debug Level*** – you can 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 bandwidth that the Booster will utilize with a given client. A word of caution though, if the Booster is feeding an IVS, you probably don't want to limit the download speed between the Booster and the IVS, as images can be quite large and take a lot of time to copy when unrestricted.
- ***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

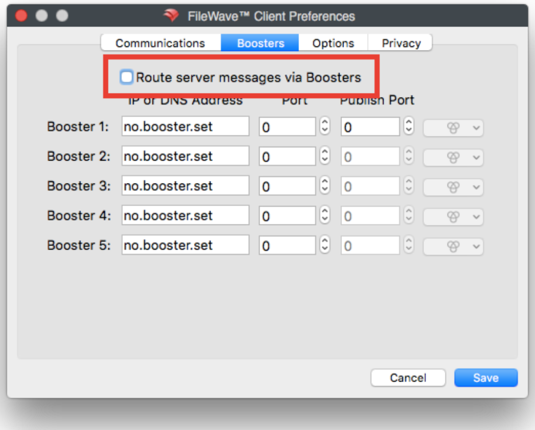
These settings are where you build your distribution "tree" by assigning where this Booster connects. This specifies the order in which connection attempts will be made. The best way to set this up is to follow these guidelines:

- Set **Server 1** to be the next Booster upstream from your Booster. This may be the main FileWave Server, or another Booster upstream from this one.

- Set the other servers to be Boosters in the same general area or location as this Booster or ones that are upstream from each other (e.g., #2 would be upstream from #1). 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 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 FileWave 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**.

Configuring Clients to use Boosters for Server Messages

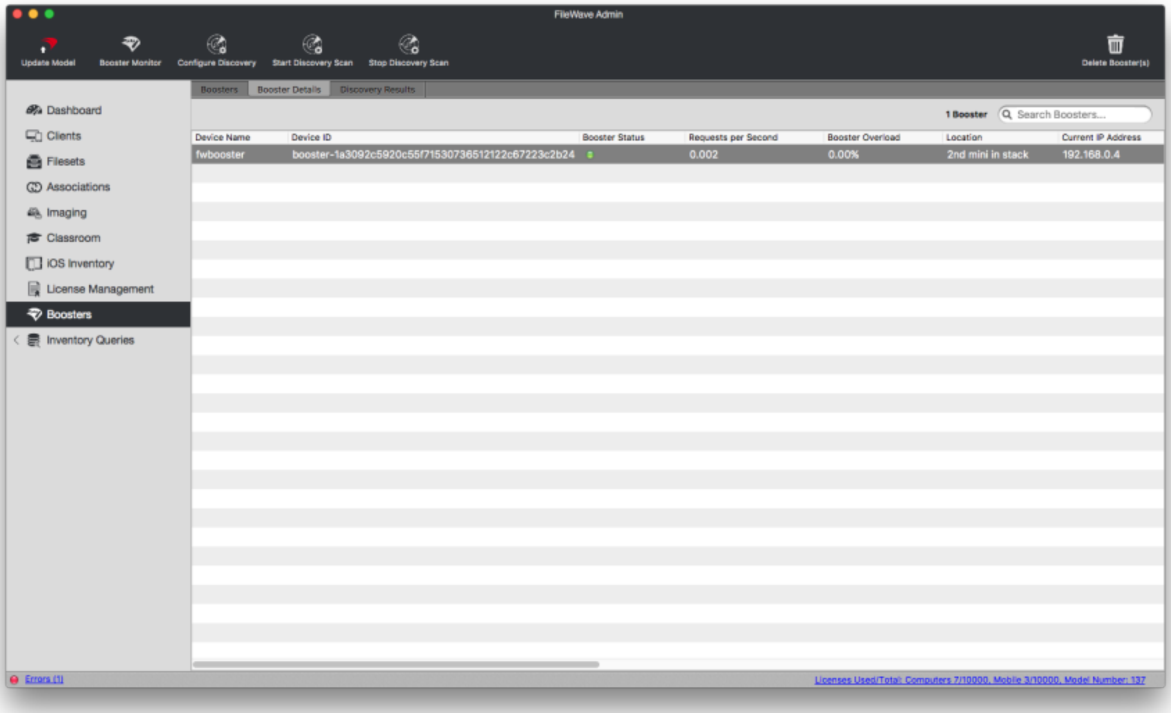
To activate the server message routing functionality introduced with FileWave 11, you must enable it using either the option on the Booster page of Superprefs or Client Preferences. This should not be done until all Boosters in the related clients' communication paths have been upgraded to FileWave 11+.



☐ Route server messages via Boosters

	IP or DNS Address	Port	Publish Port
Booster 1:	no.booster.set	0	0
Booster 2:	no.booster.set	0	0
Booster 3:	no.booster.set	0	0
Booster 4:	no.booster.set	0	0
Booster 5:	no.booster.set	0	0

Boosters view



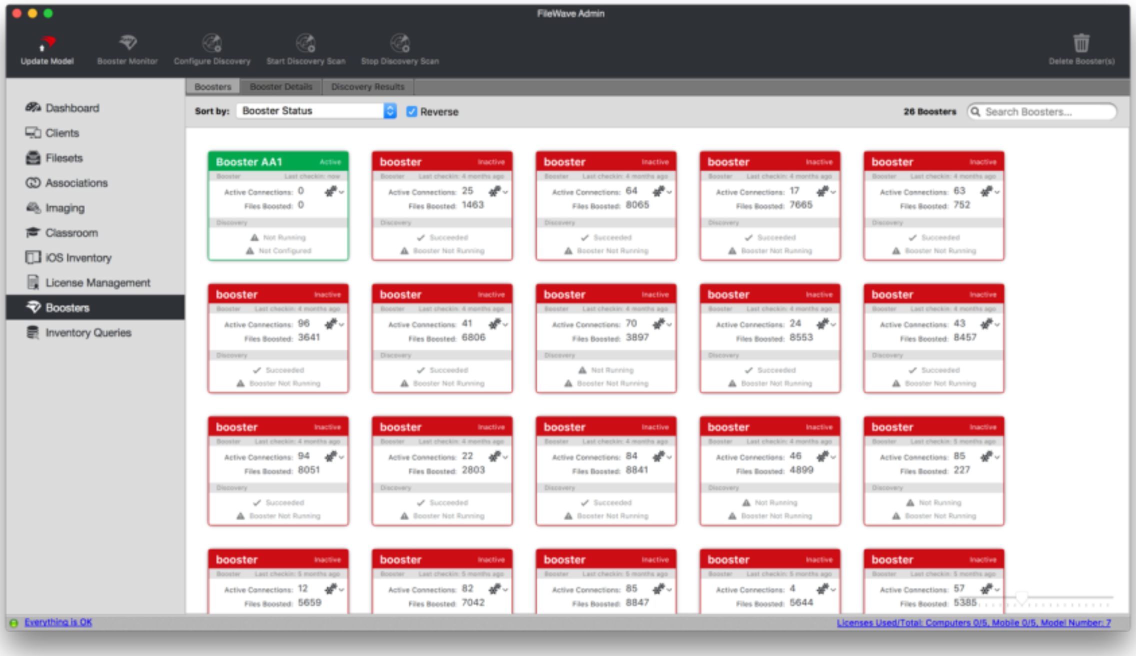
Device Name	Device ID	Booster Status	Requests per Second	Booster Overload	Location	Current IP Address
fwbooster	booster-1a3092c5920c55f71530736512122c67223c2b24	🟩	0.002	0.00%	2nd mini in stack	192.168.0.4

Licenses Used/Total: Computers 7/10000, Mobile 3/10000, Model Number: 137

On the above screenshot you can see new options in the Boosters tab in Boosters view:
"**Configure Discovery**" button opens the Discovery Configuration dialog. Note: Network Discovery is covered in depth in Chapter 12
"**Start Discovery Scan**" button immediately starts a scan using the existing configuration, if a scanner configuration is currently disabled then the configured will be enabled at this point.
"**Stop Discovery Scan**" button immediately stops the current scan, if the configuration is enabled then it's also disabled.
"**Device Name**" column contains name of the Booster. This is configured in Booster's preferences.
"**Booster Status**" column indicates green/orange/red icon based on last check-in time:
green = check-in within last 5 minutes;
orange = check-in between last 5 and 10 minutes;
red = check-in more than 10 minutes ago).
"**Next Scan Start Time**" column indicates start time of the next scan
"**Last Discovery Scan Status**" column shows the various statuses of a discovery scan and the discovery application (success, network scanner fail, network scanner crash, discovery application crash, discovery stop, generic failure).
"**Requests per Second**" column indicates number of Booster requests per second within the last 15 minutes. Additionally, Booster statistics are sent by the Booster every 15 minutes at fixed times e.g. 0:00, 0:15, 0:30, 0:45.
"**Booster Overload**" column indicates if there are any clients' requests that couldn't be served by Booster. This doesn't necessarily mean the Booster is failing; it simply implies that the client has been told to retry later.
"**Location**" column contains location configured in Booster's preferences.

View modes

The Boosters view offers two primary view modes: the Cards view (requires OpenGL on the administrator machine running FileWave Admin) and the Details view. These modes operate independently. Double-clicking on a Booster in either view opens the Booster Monitor for that particular Booster.



Sort by: Booster Status ☑ Reverse 26 Boosters

Booster AA1 Active
Booster Last checkin: now
Active Connections: 0
Files Boosted: 0
Discovery
Not Running
Not Configured

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 25
Files Boosted: 1463
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 64
Files Boosted: 8065
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 17
Files Boosted: 7665
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 63
Files Boosted: 752
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 96
Files Boosted: 3641
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 41
Files Boosted: 6806
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 70
Files Boosted: 3897
Discovery
Not Running
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 24
Files Boosted: 8553
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 43
Files Boosted: 8457
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 94
Files Boosted: 8051
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 22
Files Boosted: 2803
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 84
Files Boosted: 8841
Discovery
✓ Succeeded
Booster Not Running

booster Inactive
Booster Last checkin: 4 months ago
Active Connections: 46
Files Boosted: 4899
Discovery
Not Running
Booster Not Running

booster Inactive
Booster Last checkin: 5 months ago
Active Connections: 85
Files Boosted: 227
Discovery
Not Running
Booster Not Running

booster Inactive
Booster Last checkin: 5 months ago
Active Connections: 12
Files Boosted: 5659

booster Inactive
Booster Last checkin: 5 months ago
Active Connections: 82
Files Boosted: 7042

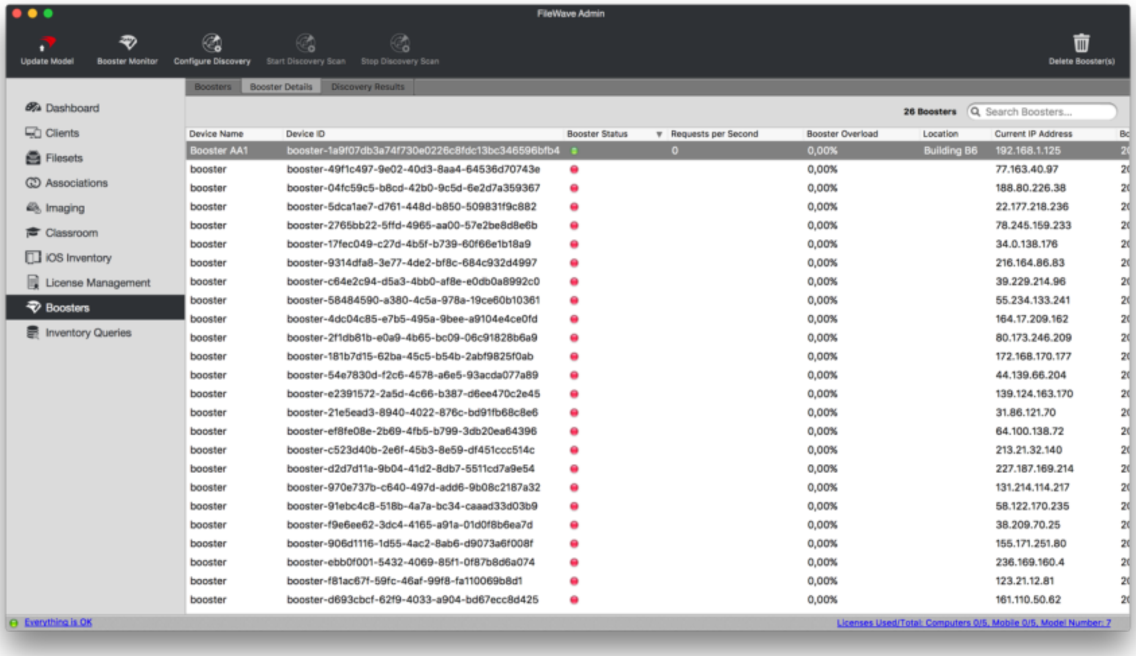
booster Inactive
Booster Last checkin: 5 months ago
Active Connections: 85
Files Boosted: 8847

booster Inactive
Booster Last checkin: 5 months ago
Active Connections: 4
Files Boosted: 5644

booster Inactive
Booster Last checkin: 5 months ago
Active Connections: 57
Files Boosted: 5385

In the Cards view, each Booster is displayed as a card, with just an overview of its status. Besides using the contextual menu, on the top-right corner of each card there are two gears that when clicked open the same menu.

When the Booster Details tab is clicked on, the Boosters tab switches to the Details view. In this mode, a list with many columns is displayed instead:



26 Boosters

Device Name	Device ID	Booster Status	Requests per Second	Booster Overload	Location	Current IP Address	Bo
Booster AA1	booster-1a9f07db3a74f730e0226c8fdc13bc346596bfb4	🟢	0	0,00%	Building B6	192.168.1.125	20
booster	booster-49f1c497-9e02-40d3-8aa4-64536d70743e	🔴		0,00%		77.163.40.97	20
booster	booster-04fc59c5-b8cd-42b0-9c5d-6e2d7a359367	🔴		0,00%		188.80.226.38	20
booster	booster-5dca1ae7-d761-448d-b850-509831f9c882	🔴		0,00%		22.177.218.236	20
booster	booster-2765bb22-5ffd-4965-aa00-57e2be8d8e6b	🔴		0,00%		78.245.159.233	20
booster	booster-17fec049-c27d-4b5f-b739-60f66e1b18a9	🔴		0,00%		34.0.138.176	20
booster	booster-9314dfa8-3e77-4de2-bf8c-684c932d4997	🔴		0,00%		216.164.86.83	20
booster	booster-c64e2c94-d5a3-4bb0-af8e-e0db0a8992c0	🔴		0,00%		39.229.214.96	20
booster	booster-58484590-a380-4c5a-978a-19ce60b10361	🔴		0,00%		55.234.133.241	20
booster	booster-4dc04c85-e7b5-495a-9bee-a9104e4ce0fd	🔴		0,00%		164.17.209.162	20
booster	booster-2f1db81b-e0a9-4b65-bc09-06c91828b6a9	🔴		0,00%		80.173.246.209	20
booster	booster-181b7d15-62ba-45c5-b54b-2abf9825f0ab	🔴		0,00%		172.168.170.177	20
booster	booster-54e7830d-f2c6-4578-a6e5-93acda077a89	🔴		0,00%		44.139.66.204	20
booster	booster-e2391572-2a5d-4c66-b387-d6ee470c2e45	🔴		0,00%		139.124.163.170	20
booster	booster-21e5ead3-8940-4022-876c-bd91fb68c8e6	🔴		0,00%		31.86.121.70	20
booster	booster-ef8fe08e-2b69-4fb5-b799-3db20ea64396	🔴		0,00%		64.100.138.72	20
booster	booster-c523d40b-2e6f-45b3-8e59-df451ccc514c	🔴		0,00%		213.21.32.140	20
booster	booster-d2d7d11a-9b04-41d2-8db7-5511cd7a9e54	🔴		0,00%		227.187.169.214	20
booster	booster-970e737b-c640-497d-add6-9b08c2187a32	🔴		0,00%		131.214.114.217	20
booster	booster-91ebc4c8-518b-4a7a-bc34-caaad33d03b9	🔴		0,00%		58.122.170.235	20
booster	booster-f9e6ee62-3dc4-4165-a91a-01d0f8b6ea7d	🔴		0,00%		38.209.70.25	20
booster	booster-906d1116-1d55-4ac2-8ab6-d9073a6f008f	🔴		0,00%		155.171.251.80	20
booster	booster-ebb0f001-5432-4069-85f1-0f87b8d6a074	🔴		0,00%		236.169.160.4	20
booster	booster-f81ac67f-59fc-46af-99f8-fa110069b8d1	🔴		0,00%		123.21.12.81	20
booster	booster-d693cbcf-62f9-4033-a904-bd67ecc8d425	🔴		0,00%		161.110.50.62	20

4. FileWave clients - install / enroll / configure plus Apple DEP

The FileWave computer client runs on both macOS and Windows computers. When installed, it will allow the Client device to maintain contact with the FileWave Server. The installer also places the self-service Kiosk into the toolbar or menu bar of the client computer. 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 introduced some significant changes in the FileWave client. An integrated VNC relay is included, allowing the FileWave Admin to observe/control 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 macOS 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.

4.1. Understanding FileWave Clients, Groups, and Smart Groups

Client operations

The FileWave Client needs to be installed on computers that you want to manage with FileWave. The FileWave Client should to be given a unique name so that the FileWave Server can identify 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 FileWave Server address. The Client uses this IP or DNS address to attempt to connect to the FileWave Server.

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 (stored in it's Catalog file), 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 downloading and activation of Filesets (adhering to any time attributes), deletion of Filesets, deactivating Filesets (but leaving the contents in place on the computer for possible future reactivation), and update commands for existing Filesets . When downloading Filesets, 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 have to either use Apple's Device Enrollment Program (DEP) or Apple Configurator, which requires 'tethering' the devices using a Lightning cable.

FileWave Client

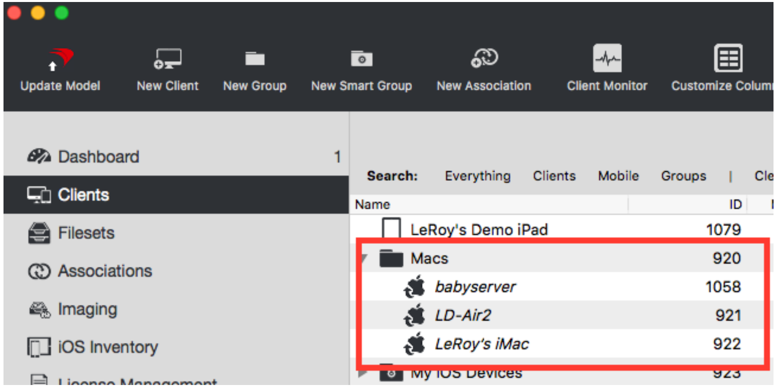
The FileWave Client itself is a process (*fwcld*) that runs as a daemon on a Client. The visible effect of a client is usually the **Kiosk**, FileWave's self-service tool. On macOS and Windows computers, the FileWave Client is installed using a .**pkg** (macOS) or .**msi** (Win). On an Android device, the Client is downloaded and installed as a .**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

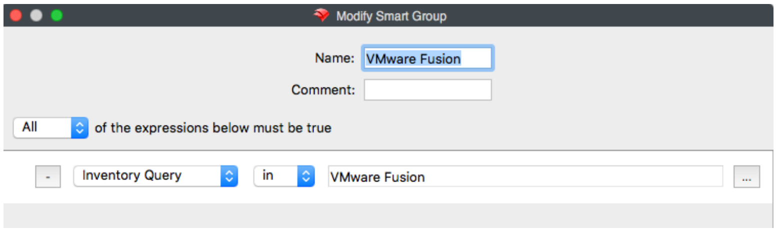
FileWave Clients can be gathered into fixed Groups for convenience. The Groups can be named and populated as needed. The advantage of fixed Groups is the ability to associate content with Groups versus having to pick out individual clients. A FileWave Client can be assigned directly to a Group, or you can create a **Clone** of that Client to assign it to the Group.

Smart Groups

In FileWave, you can create dynamic Groups based upon selective inventory queries, 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. The devices that show in Smart Groups are Clones, as distinguished by the *italicized* Client name as well as the upward hooking arrow on the lower-left side of the Client type symbol.



Name	ID
LeRoy's Demo iPad	1079
Macs	920
babyserver	1058
LD-Air2	921
LeRoy's iMac	922
My iOS Devices	923


Modify Smart Group

Name: VMware Fusion

Comment:

All of the expressions below must be true

- Inventory Query in VMware Fusion ...

More ideas for Smart Groups are provided in the **Inventory** Chapter, such as using a Smart Group to track down and remove rogue software from devices.

Clones

Instead of assigning FileWave Clients to a single Group, you might want to have a Client 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. The advantage of using Clones is that you can assign Clones of a client to many Groups; but you can assign a Client device itself to only one Group. Groups, Smart Groups, and Clones are discussed in much greater detail later in this Chapter, as well as in the **Inventory** Chapter.

4.2. Desktop_laptop Client Install and Configure

The FileWave Client runs on both OS X/macOS and Windows computers with the following requirements:

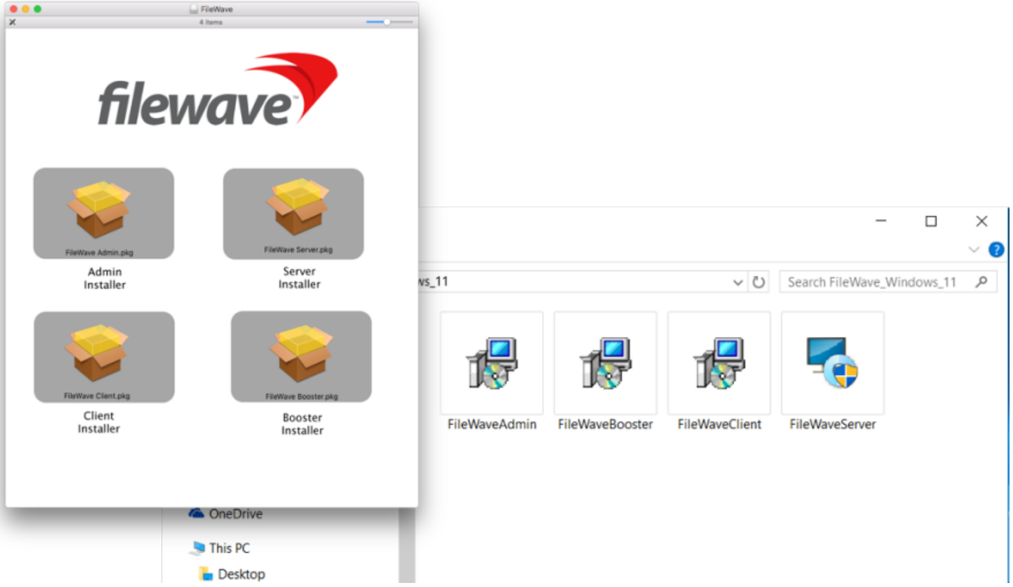
Operating Systems Supported:

- OS X v10.7*& v10.8* / OS X v10.9 - v10.11 / macOS 10.12
- Windows XP* / 7 / 8 / 8.1 / 10
- Windows Server 2008R2 / 2012 / 2012R2

- Limited Legacy Support

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: https://www.filewave.com/support/software-downloads. For the computers mentioned under *Legacy Support,* you will need to install the FileWave v9.1.2 client, or keep any older client already installed.

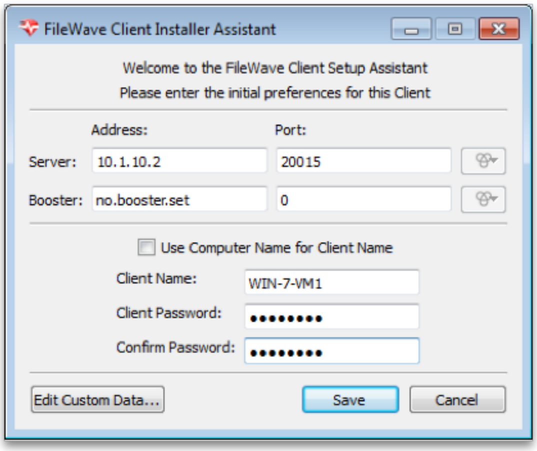


You should download all installers you will need for your deployment at the same time. They can be stored on a file server, or on a flash drive in Windows format for cross platform compatibility (OS X / macOS systems can read Windows-formatted drives without additional drivers).

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 Chapter 2. There is no Linux client.

Installing the FileWave client

Client installers for both macOS 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. Note: on some Windows computers, the FileWave Client Installer Assistant window is positioned directly behind the installer window, which you need to move to get to the Installer Assistant to complete the installation.



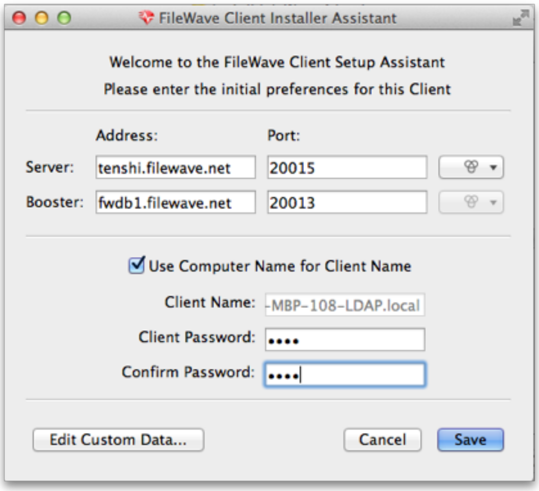
FileWave Client Installer Assistant

Welcome to the FileWave Client Setup Assistant
Please enter the initial preferences for this Client

	Address:	Port:
Server:	10.1.10.2	20015
Booster:	no.booster.set	0

□ Use Computer Name for Client Name

Client Name: WIN-7-VM1
Client Password: ••••••••
Confirm Password: ••••••••



Welcome to the FileWave Client Setup Assistant

Please enter the initial preferences for this Client

	Address:	Port:
Server:	tenshi.filewave.net	20015
Booster:	fwdb1.filewave.net	20013

☑ Use Computer Name for Client Name

Client Name: -MBP-108-LDAP.local

Client Password: ••••

Confirm Password: ••••

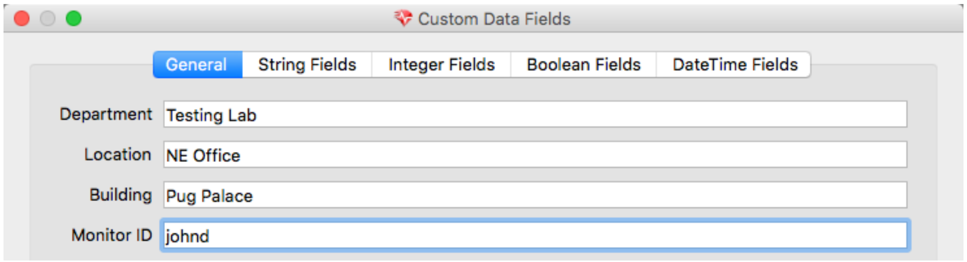
Installation settings

- ***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 3.

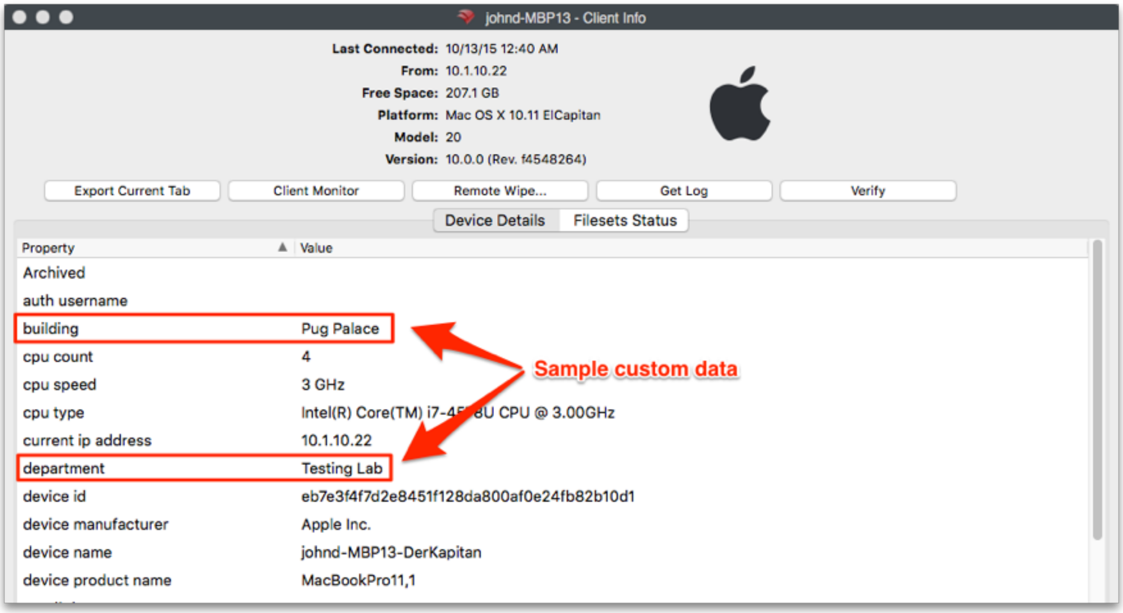
- ***Use Computer Name for Client Name*** - this box allows you to use the device's computer name as its FileWave client name.
- ***Client Name*** - enter a valid name based on any criteria you have for your deployment. It is recommended that you do not use special characters in the client name. Dashes, 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 <u>must</u> provide a password in order for the Remote Control/VNC relay to function.**

Edit Custom Data…



Department	Testing Lab
Location	NE Office
Building	Pug Palace
Monitor ID	johnd

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**.

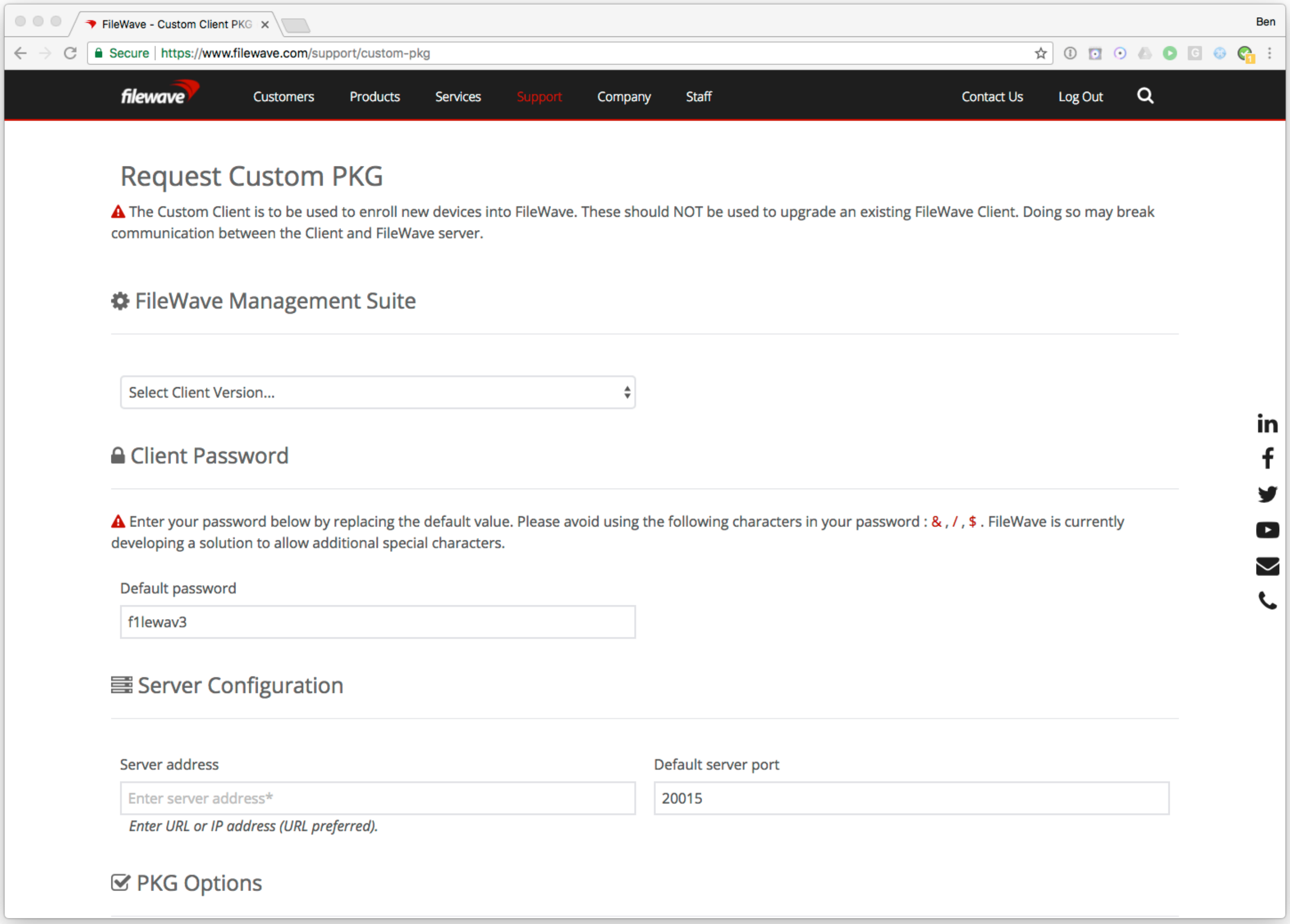


Last Connected: 10/13/15 12:40 AM
From: 10.1.10.22
Free Space: 207.1 GB
Platform: Mac OS X 10.11 ElCapitan
Model: 20
Version: 10.0.0 (Rev. f4548264)

Property	Value
Archived	
auth username	
building	Pug Palace
cpu count	4
cpu speed	3 GHz
cpu type	Intel(R) Core(TM) i7-4578U CPU @ 3.00GHz
current ip address	10.1.10.22
department	Testing Lab
device id	eb7e3f4f7d2e8451f128da800af0e24fb82b10d1
device manufacturer	Apple Inc.
device name	johnd-MBP13-DerKapitan
device product name	MacBookPro11,1

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:
For macOS: https://www.filewave.com/support/custom-pkg
For Windows: https://www.filewave.com/support/custom-msi
The customized client for macOS X required for MDM/DEP support and is required to be uploaded as part of the Mobile preferences in FileWave Admin.
The form is shown on the next page.


FileWave - Custom Client PKG
Ben
Secure | https://www.filewave.com/support/custom-pkg
filewave
Customers
Products
Services
Support
Company
Staff
Contact Us
Log Out

Request Custom PKG

⚠ The Custom Client is to be used to enroll new devices into FileWave. These should NOT be used to upgrade an existing FileWave Client. Doing so may break communication between the Client and FileWave server.

FileWave Management Suite

Select Client Version...

Client Password

⚠ Enter your password below by replacing the default value. Please avoid using the following characters in your password : & , / , $. FileWave is currently developing a solution to allow additional special characters.

Default password: f1lewav3

Server Configuration

Server address: Enter server address*

Enter URL or IP address (URL preferred).

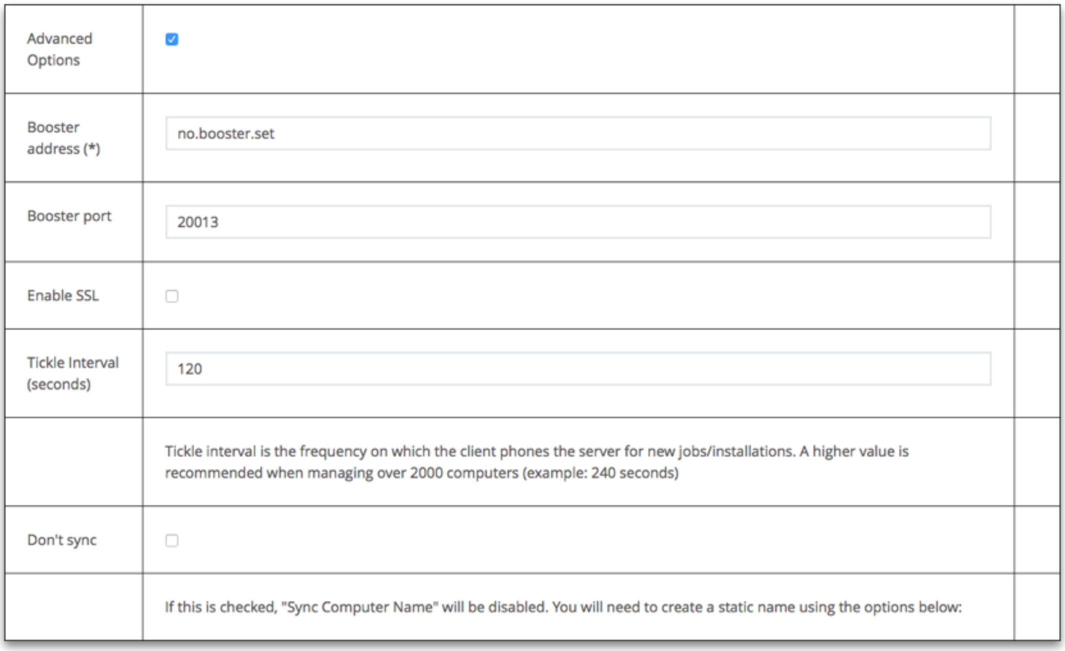
Default server port: 20015

PKG Options

Many fields are required.

Note that the default port is 20015. If you want SSL, do not set it to 20017; click the "Advanced Options" box, which will display more options (shown on the next page), one of which is Enable SSL. Therefore, if you want SSL, leave the Server port set to 20015, then click the "Enable SSL" check box which will result in the proper setting for using SSL.

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:

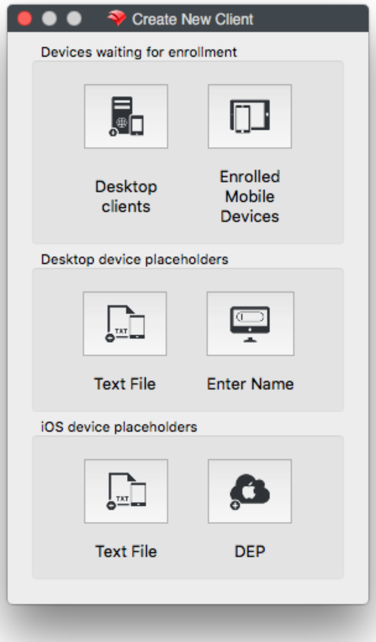
The custom installer does not ask the user for any device specific information, and can be distributed through several means:

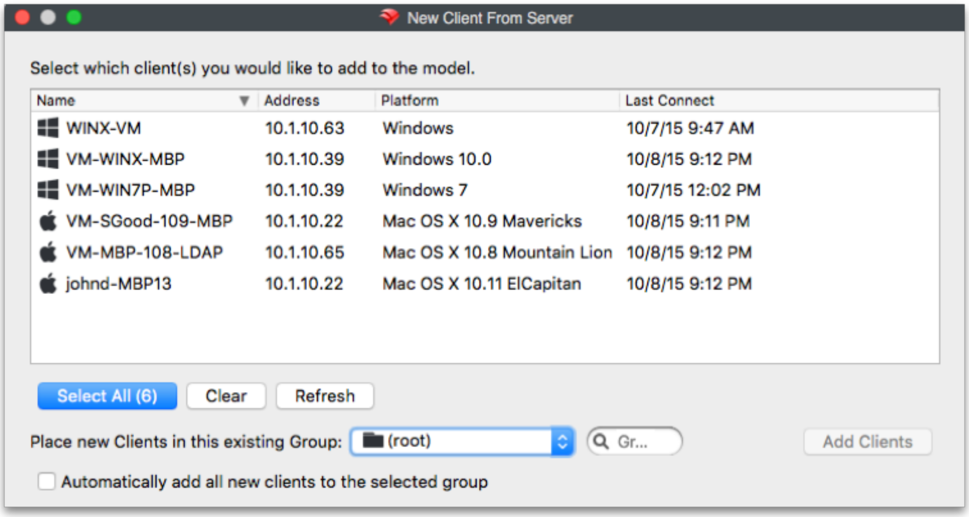
- Apple's Device Enrollment Program (DEP) uses the custom installer to enroll institutionally purchased devices automatically with your FileWave server (See the DEP section later in this Chapter for more details).
- Add the custom installer to an image set when doing direct or network mass imaging (See 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.

4.3. Enrolling Computer Clients

Click on the **New Client** toolbar icon will bring up the **Create New Client** window. Clicking on **Desktop clients** will open the **New Client From Server** window, which is where computer clients will show up once the FileWave client on the device checks in with the designated FileWave server specified in the client settings. These settings were either manually entered when installing the client or specified when a custom client installer was produced using the FileWave Support webpage.





Select which client(s) you would like to add to the model.

Name	Address	Platform	Last Connect
WINX-VM	10.1.10.63	Windows	10/7/15 9:47 AM
VM-WINX-MBP	10.1.10.39	Windows 10.0	10/8/15 9:12 PM
VM-WIN7P-MBP	10.1.10.39	Windows 7	10/7/15 12:02 PM
VM-SGood-109-MBP	10.1.10.22	Mac OS X 10.9 Mavericks	10/8/15 9:11 PM
VM-MBP-108-LDAP	10.1.10.65	Mac OS X 10.8 Mountain Lion	10/8/15 9:12 PM
johnd-MBP13	10.1.10.22	Mac OS X 10.11 ElCapitan	10/8/15 9:12 PM

Place new Clients in this existing Group: (root)

□ Automatically add all new clients to the selected group

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.

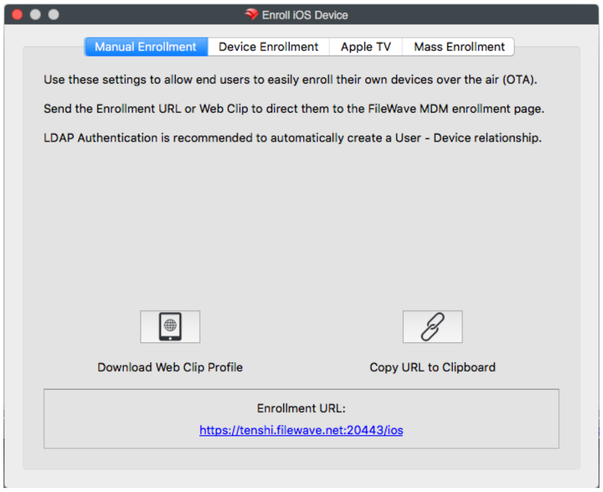
4.4. Enrolling Mobile Devices

Before FileWave 11.1, iOS devices needed to enroll in MDM before they could be imported into FileWave Admin. Starting with FileWave 11.1, it's possible to pre-import iOS devices; i.e., make placeholders for them in the database, before they enroll either using a CSV file containing serial numbers+Client names or from a DEP account. After a placeholder record is created, it's possible to create associations. Any associated Filesets will be deployed to the device as soon as it actually enrolls. In other words, you can create workflows in advance of devices actually enrolling that will automatically occur once the devices enroll.

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 devices and macOS computers 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 management of that device.

Web-based enrollment - iOS

For 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:**



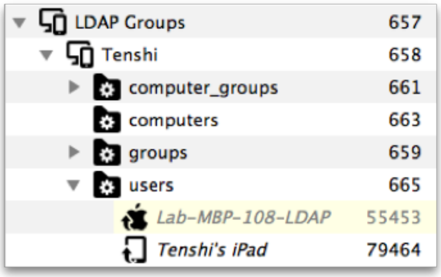
Use these settings to allow end users to easily enroll their own devices over the air (OTA).

Send the Enrollment URL or Web Clip to direct them to the FileWave MDM enrollment page.

LDAP Authentication is recommended to automatically create a User - Device relationship.

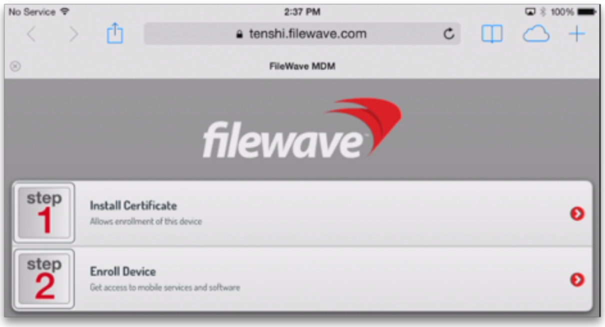
Enrollment URL:
https://tenshi.filewave.net:20443/ios

You can create a Web Clip with that URL embedded or copy the URL to the Clipboard and email it to your 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 using 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 Apple ID with your FileWave VPP service.



LDAP Groups	657
Tenshi	658
computer_groups	661
computers	663
groups	659
users	665
Lab-MBP-108-LDAP	55453
Tenshi's iPad	79464

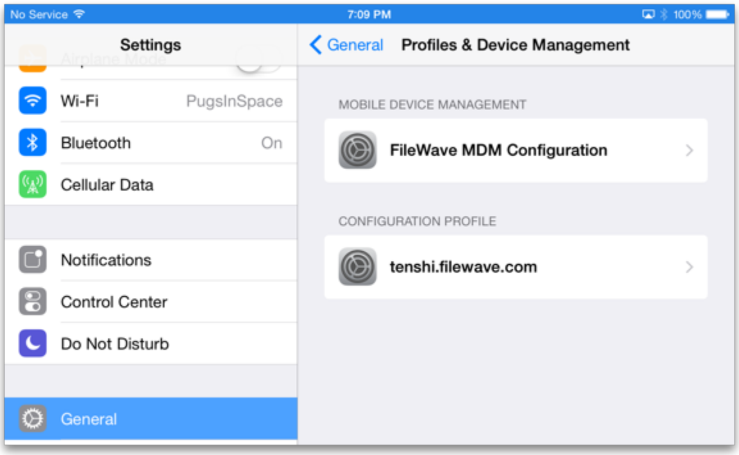
The user is presented with a dialog prompting to install a MDM server certificate, then enroll the device. The second step is when the user will be asked to authenticate - and this is where LDAP integration comes in handy. If not using LDAP, you need to inform users of the generic credential to use, or else they will not be able to proceed with step 2.



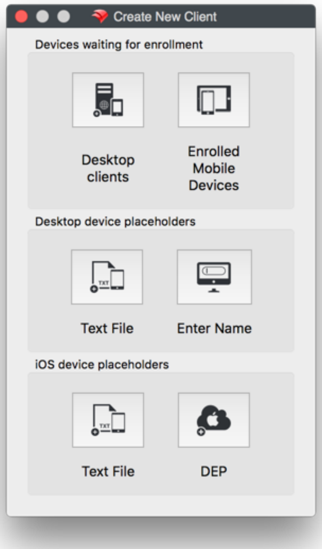
step 1 Install Certificate
Allows enrollment of this device

step 2 Enroll Device
Get access to mobile services and software

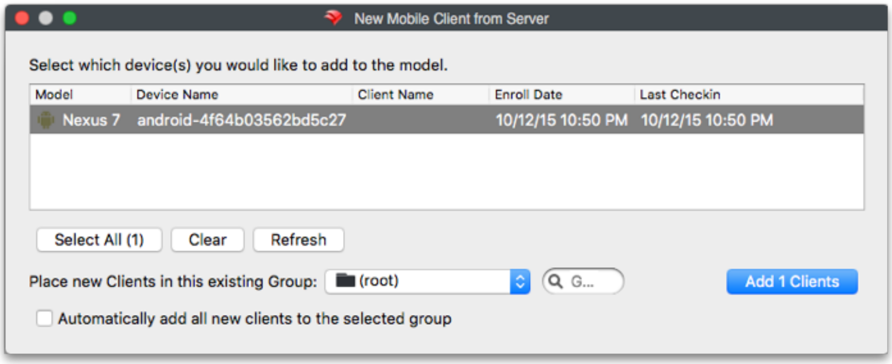
Once the user has completed these two steps, the device will display the new profiles that have been installed:



If the user's device is not yet a FileWave Client (no placeholder record previously created), it will need to be captured in FileWave Admin. You will go to the **Clients** pane, select **New Client** from the toolbar.



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:


New Mobile Client from Server

Select which device(s) you would like to add to the model.

Model	Device Name	Client Name	Enroll Date	Last Checkin
Nexus 7	android-4f64b03562bd5c27		10/12/15 10:50 PM	10/12/15 10:50 PM

Place new Clients in this existing Group: (root)

□ Automatically add all new clients to the selected group

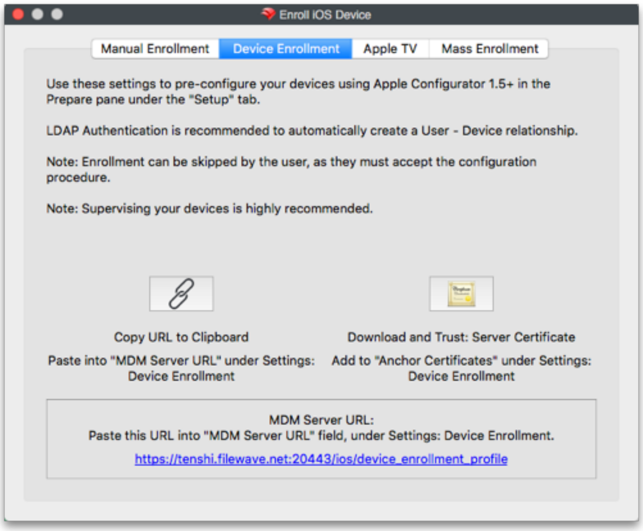
The device(s) can be automatically added to an existing client Group, or you can manually add them to a Group, if desired. If you have devices set to be automatically added to a specific Group, then you will just see them appear as members in that Group.
Note: Unless you want all devices that enroll during a specific timeframe to end up in a designated Group, you should leave automatic placement off. You should also think about using Clones instead of the actual device client as members of any Groups. (Review section 5.1 on Clones if necessary.)

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 v2.2.1.

Single device enrollment

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



Use these settings to pre-configure your devices using Apple Configurator 1.5+ in the Prepare pane under the "Setup" tab.

LDAP Authentication is recommended to automatically create a User - Device relationship.

Note: Enrollment can be skipped by the user, as they must accept the configuration procedure.

Note: Supervising your devices is highly recommended.

Copy URL to Clipboard

Paste into "MDM Server URL" under Settings: Device Enrollment

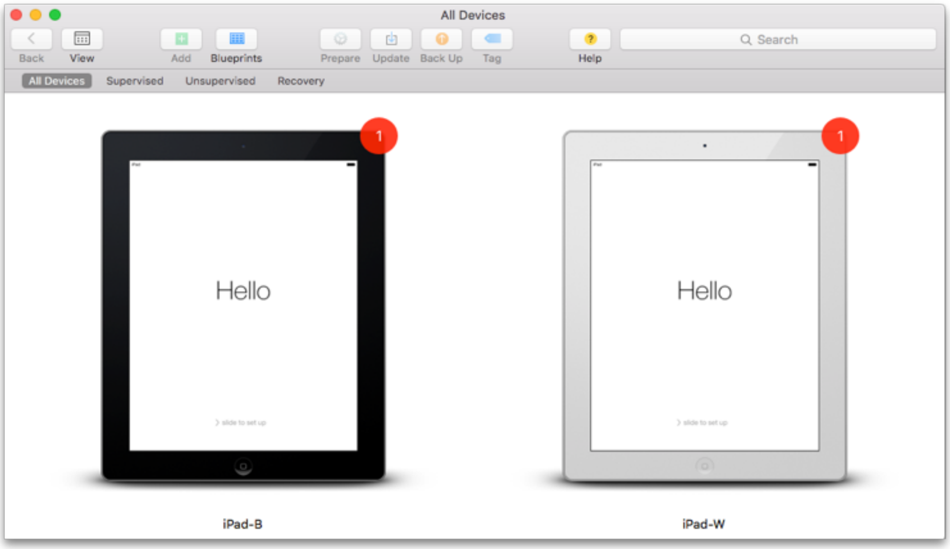
Download and Trust: Server Certificate

Add to "Anchor Certificates" under Settings: Device Enrollment

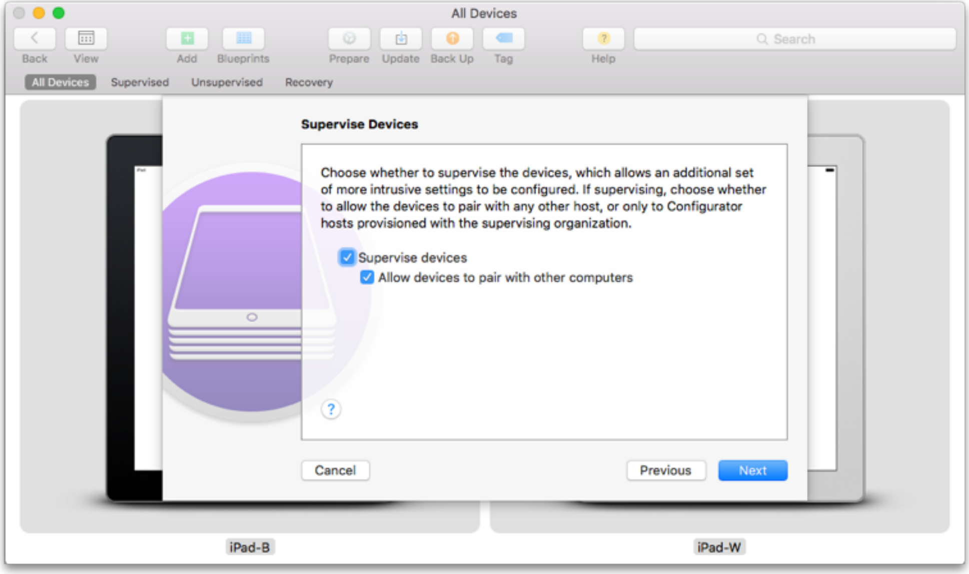
MDM Server URL:
Paste this URL into "MDM Server URL" field, under Settings: Device Enrollment.
https://tenshi.filewave.net:20443/ios/device_enrollment_profile

Apple Configurator v2.2.1

Apple Configurator 2's blueprints let you record actions that can be applied to devices. You add configuration profiles and apps to blueprints, just as you would add them to a physical device. You can prepare a blueprint so it has the MDM data and supervision identify attached. Once you have the blueprint the way you want, you can apply it to a device. For detailed info on how to use Apple Configurator 2, see: http://help.apple.com/configurator/mac/2.0/
To create a blueprint, click
▦
in the toolbar, select **Edit Blueprints**, then click on **New** in the bottom left corner to create a new blueprint. Perform your edits. When you finish, click **Done**.



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

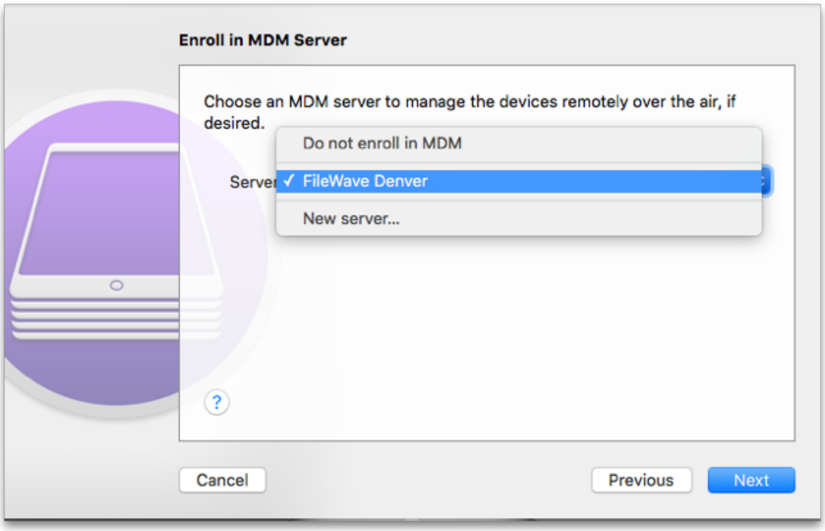


Supervise Devices

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

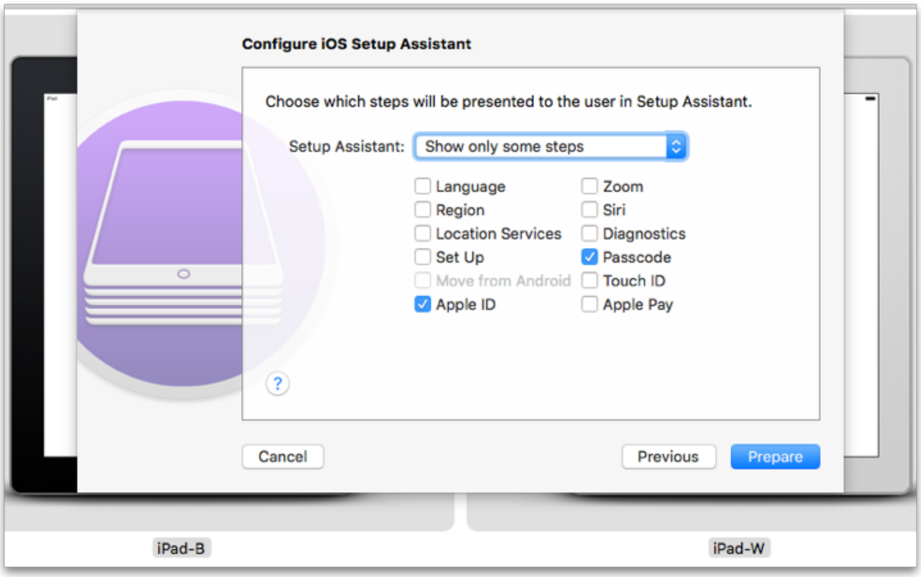
☑ Allow devices to pair with other computers



Enroll in MDM Server

Choose an MDM server to manage the devices remotely over the air, if desired.

Server: FileWave Denver



Configure iOS Setup Assistant

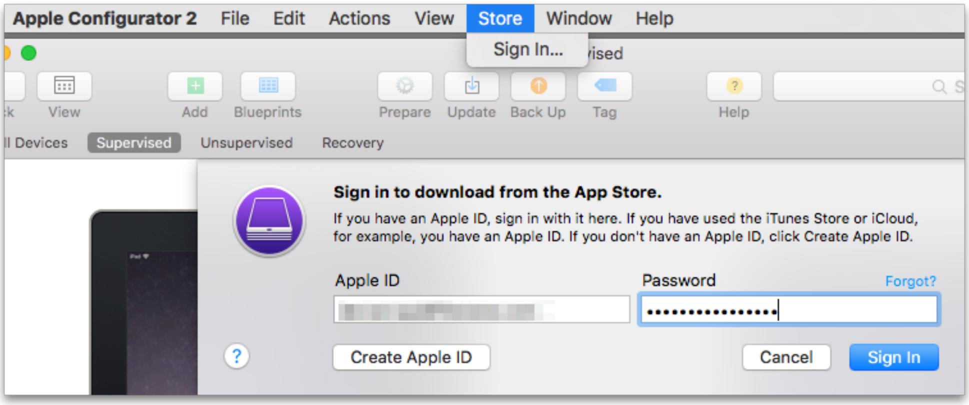
Choose which steps will be presented to the user in Setup Assistant.

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

Apple Configurator 2 supports using an Apple VPP account to assign purchases to attached devices. You should only set this up if you are not

going to be using VPP from your FileWave server to associate licensed content, or if you are going to use a separate account to apply specific core content to your iOS devices outside of any FileWave workflows.
Note: You <u>cannot</u> use the same VPP account token you are using on your FileWave server to distribute content!



Sign in to download from the App Store.

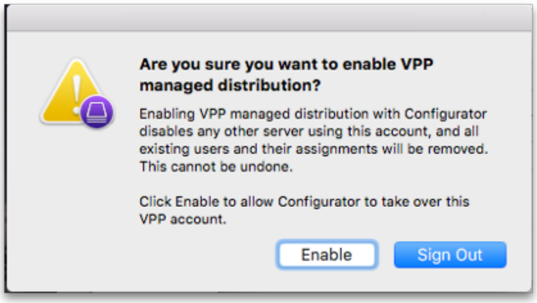
If you have an Apple ID, sign in with it here. If you have used the iTunes Store or iCloud, for example, you have an Apple ID. If you don't have an Apple ID, click Create Apple ID.

Apple ID: [redacted]

Password: ••••••••••••••••

App Store account

You can sign in to the App Store using the following:
Volume Purchase Program (VPP) account: You log in with the Apple ID associated with your VPP account or the Apple ID associated with a purchaser you specify
Your personal account: This is the iTunes account you use to purchase personal apps
WARNING: If your VPP account is already associated with another instance of Apple Configurator 2 or an MDM solution, all app assignments from those previous associations will be revoked.

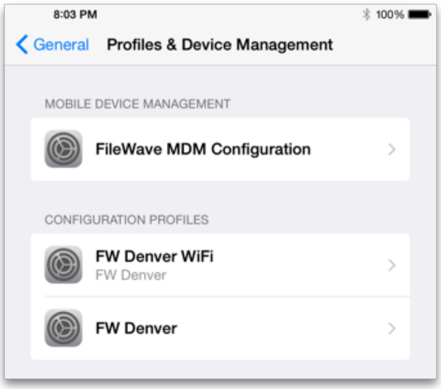


Are you sure you want to enable VPP managed distribution?

Enabling VPP managed distribution with Configurator disables any other server using this account, and all existing users and their assignments will be removed. This cannot be undone.

Click Enable to allow Configurator to take over this VPP account.

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



MOBILE DEVICE MANAGEMENT

FileWave MDM Configuration

CONFIGURATION PROFILES

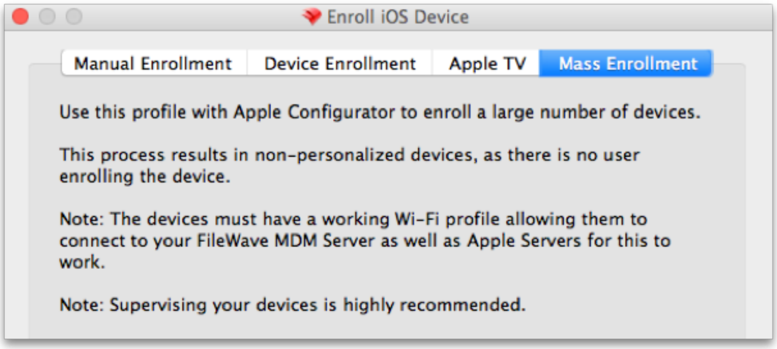
FW Denver WiFi
FW Denver

FW Denver

Using AC2 for direct assignment of applications allows you to preload your iOS devices with core applications without requiring user interaction. The workflow would create a layer in your deployment model that lets you preconfigure devices that will become FileWave Clients for all day-to-day operations and management; but come equipped with a starting set of tools.

Mass Enrollment for iOS

You can set up Apple Configurator for bulk enrollment of preconfigured iOS devices by using this option in the **Enroll iOS Device** assistant. The device **must** be connected to Wi-Fi already before this process will work. If not, then make sure you add a Wi-Fi 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.

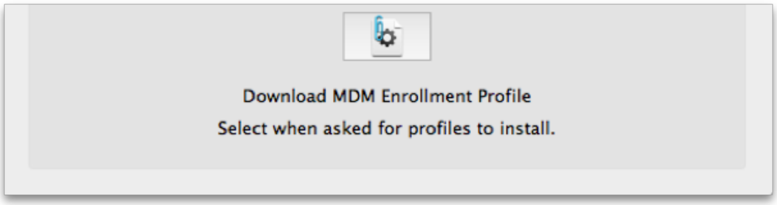


Use this profile with Apple Configurator to enroll a large number of devices.

This process results in non-personalized devices, as there is no user enrolling the device.

Note: The devices must have a working Wi-Fi profile allowing them to connect to your FileWave MDM Server as well as Apple Servers for this to work.

Note: Supervising your devices is highly recommended.



Select when asked for profiles to install.

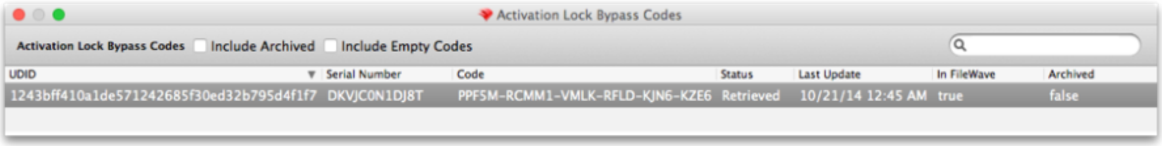
In this case, you would just download the MDM Enrollment profile, import it into Apple Configurator, and apply it to a set of iOS devices that were cloned with wireless settings, or a profile, already in place.

FileWave Enterprise App Portal for iOS

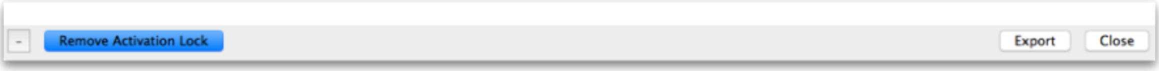
Starting with FileWave 8.5, iOS devices running iOS 7+ use a native iOS App Portal (Kiosk) instead of the web clip. iOS 8+ devices must use the App Portal. Instructions on how to deploy the App Portal are covered in Chapter **5** on mobile Filesets. When iOS devices are enrolled, they get the web clip 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

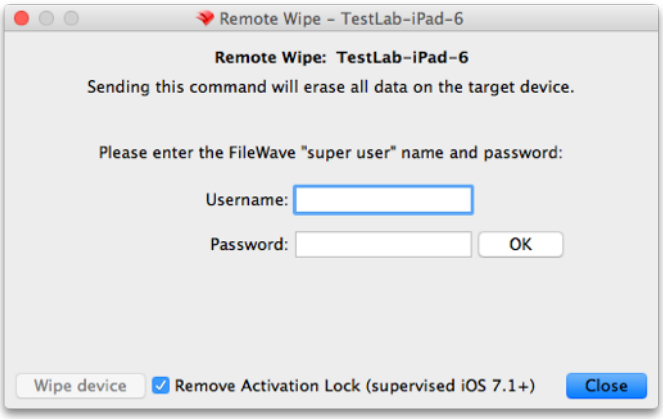
Since the introduction of iOS 7, device users have been able to enable a feature known as *Activation Lock* - which is linked to *Find My iPhone*. This feature ties a device to a specific Apple ID. In order to activate a device with an Activation Lock after a wipe or reset, the Apple ID credentials of 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.



UDID	Serial Number	Code	Status	Last Update	In FileWave	Archived
1243bff410a1de571242685f30ed32b795d4f1f7	DKVJC0N1DJ8T	PPF5M-RCMM1-VMLK-RFLD-KJN6-KZE6	Retrieved	10/21/14 12:45 AM	true	false



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



Remote Wipe - TestLab-iPad-6

Remote Wipe: TestLab-iPad-6

Sending this command will erase all data on the target device.

Please enter the FileWave "super user" name and password:

Username:

Password:

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).

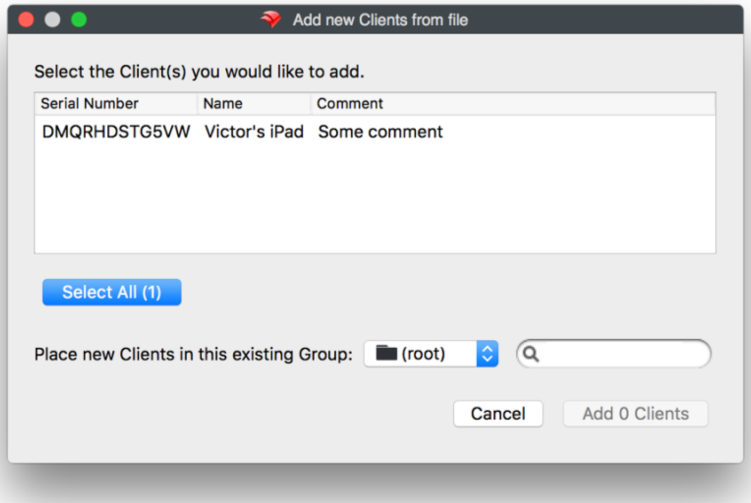
iOS Placeholders

iOS Devices from CSV

When importing from a CSV file, FileWave Admin will ask for the CSV file first. The following fields are supported:

- serial number of the iOS device;
- client name; and,
- comments (optional).

After opening the file, a dialog opens with the list of parsed devices, allowing you to select which devices to import. The dialog is the same as for importing text files.



Add new Clients from file

Select the Client(s) you would like to add.

Serial Number	Name	Comment
DMQRHDSTG5VW	Victor's iPad	Some comment

Place new Clients in this existing Group: (root)

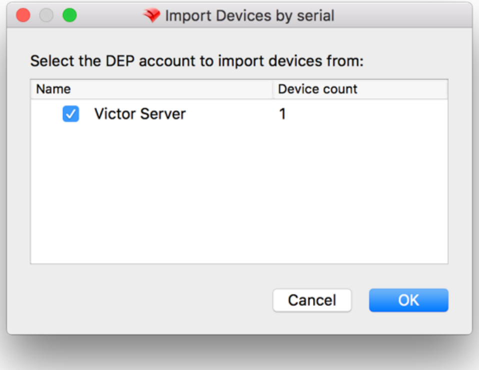
Just select any devices and click **Add X Clients**. After doing that, the new devices will appear in the Clients view. However, there's almost no information provided for them.

It'is possible to create associations and manage licenses (VPP for instance) on placeholder records the same way as if the devices had already enrolled. Update the model and any associated Filesets will be deployed automatically when the devices enroll.

iOS Devices from DEP

A DEP account must be configured in FileWave Admin before being able to pre-import from DEP.

When importing from DEP, FileWave Admin will show the list of DEP accounts and the number of devices associated to that account that are iOS devices and whose serial number are not already used with your FileWave Server.


Import Devices by serial

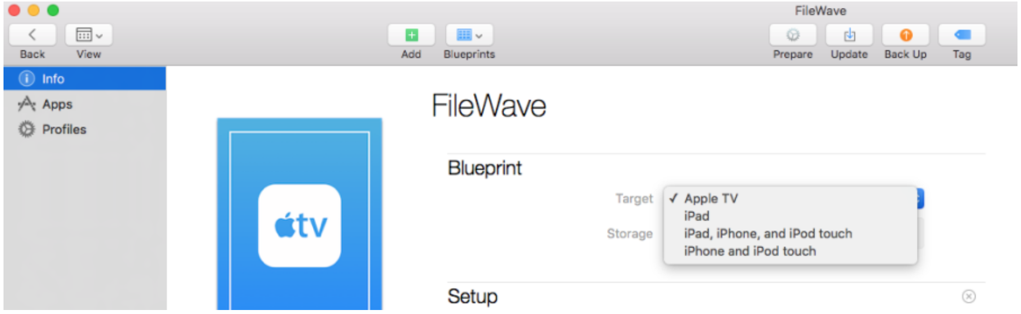
Select the DEP account to import devices from:

Name	Device count
☑ Victor Server	1

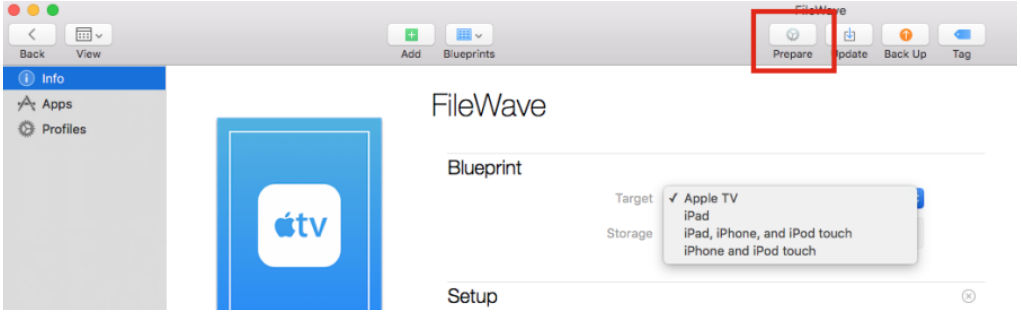
You check the DEP accounts from which you want to import devices, then click **OK**. After doing so, placeholders for all devices from the selected account will be created. You can create associations as usual, update the model, and their corresponding Filesets will be deployed when the devices enroll.
Once the device is enrolled, its name in FileWave transitions from the serial number to the actual device name. If there is a DEP naming convention, that will automatically apply.

4.5. Enrolling AppleTV into FileWave MDM

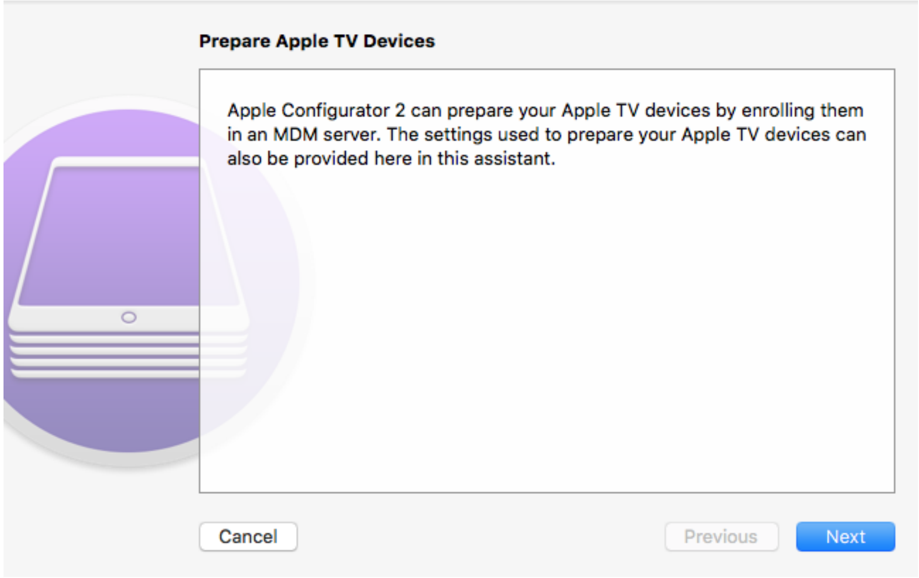
You can use Apple Configurator 2 to enroll Apple TVs in FileWave. The below screenshots show this process:
In AC2, create a new blueprint, setting the target for Apple TV.



Click on the **Prepare** icon



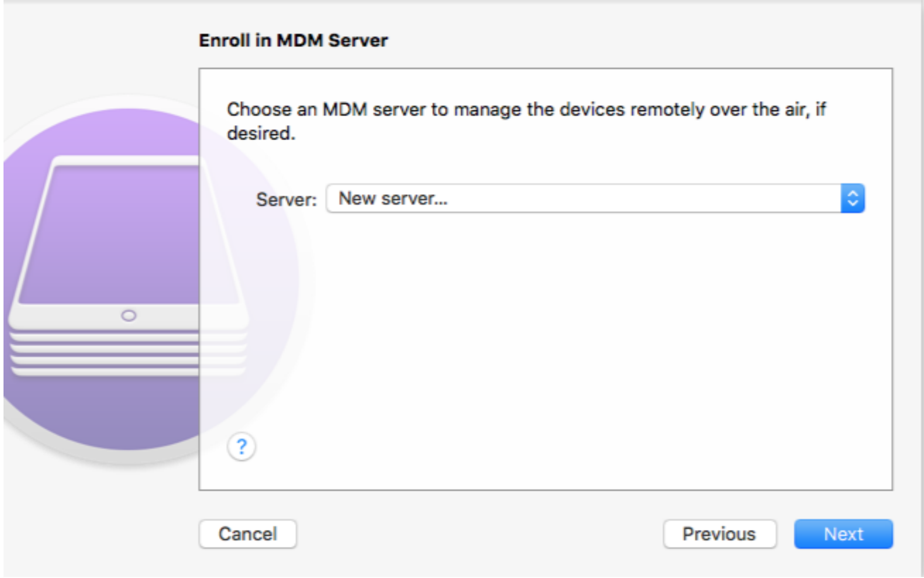
This opens the dialog box



Prepare Apple TV Devices

Apple Configurator 2 can prepare your Apple TV devices by enrolling them in an MDM server. The settings used to prepare your Apple TV devices can also be provided here in this assistant.

Click on **Next**.
Select **New server…** in the Server selection box, then click **Next**

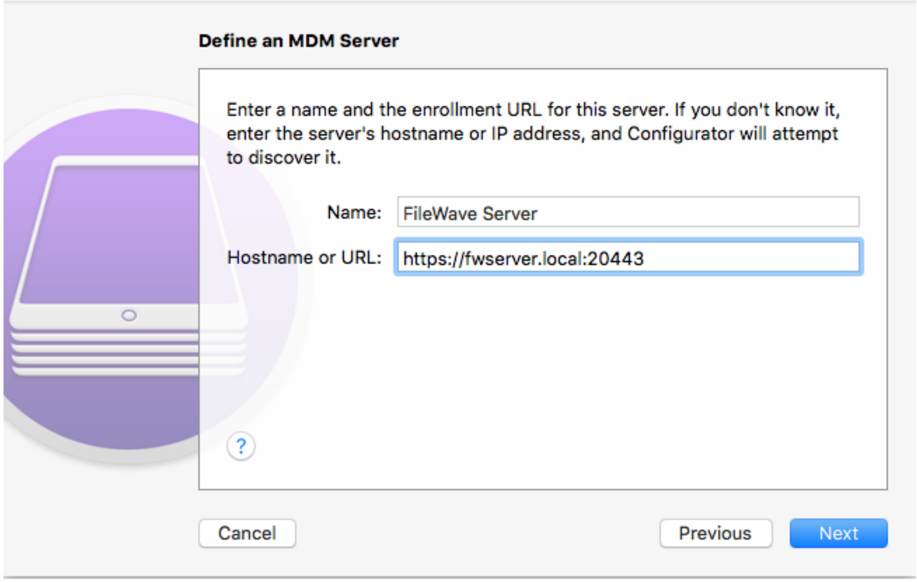


Enroll in MDM Server

Choose an MDM server to manage the devices remotely over the air, if desired.

Server: New server...

Enter your server name (does not have to be a host name and has no bearing on DNS records; this is for your identification purposes) and the URL for over-the-air enrollment (don't forget the port number at the end of the URL), then click **Next**.



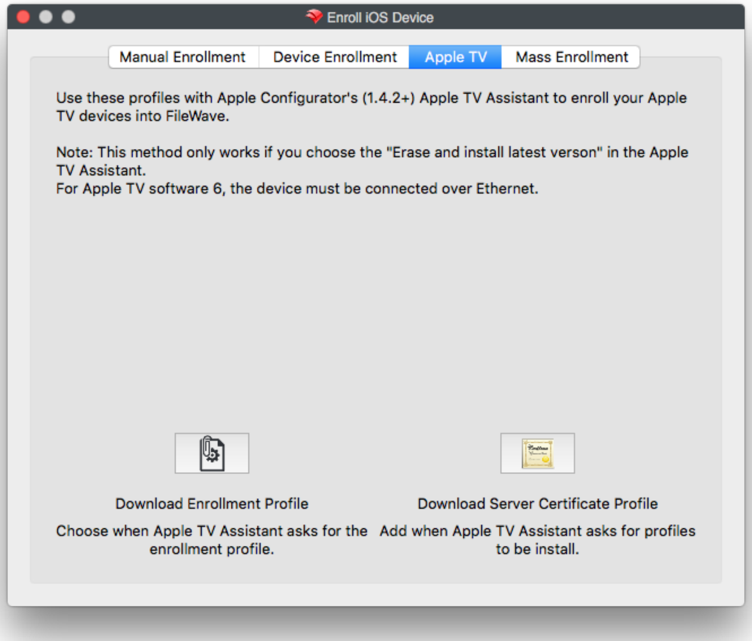
Define an MDM Server

Enter a name and the enrollment URL for this server. If you don't know it, enter the server's hostname or IP address, and Configurator will attempt to discover it.

Name: FileWave Server

Hostname or URL: https://fwserver.local:20443

Provided AC2 is able to connect with your FileWave Server, it will show the trust profile and the FileWave Root Certificate. For the needed Enrollment Profile, you get that from the **Enroll iOS Device** assistant's Apple TV tab in the **Enroll iOS Device** windows (found under the **Asistants** pull-down menu) in FileWave Admin.



Enroll iOS Device

Use these profiles with Apple Configurator's (1.4.2+) Apple TV Assistant to enroll your Apple TV devices into FileWave.

Note: This method only works if you choose the "Erase and install latest verson" in the Apple TV Assistant.
For Apple TV software 6, the device must be connected over Ethernet.

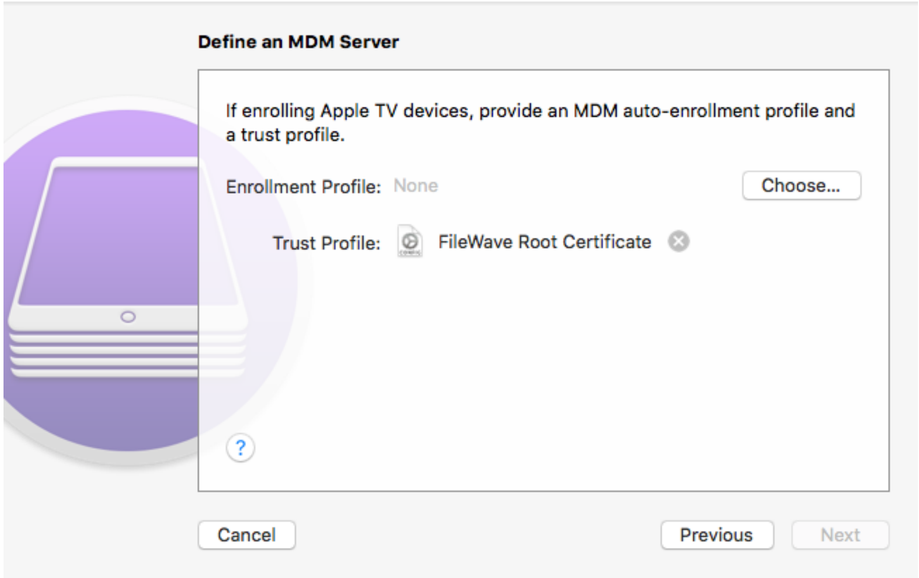
Download Enrollment Profile

Choose when Apple TV Assistant asks for the enrollment profile.

Download Server Certificate Profile

Add when Apple TV Assistant asks for profiles to be install.

Click **Choose…** and navigate to where you saved the Enrollment Profile.

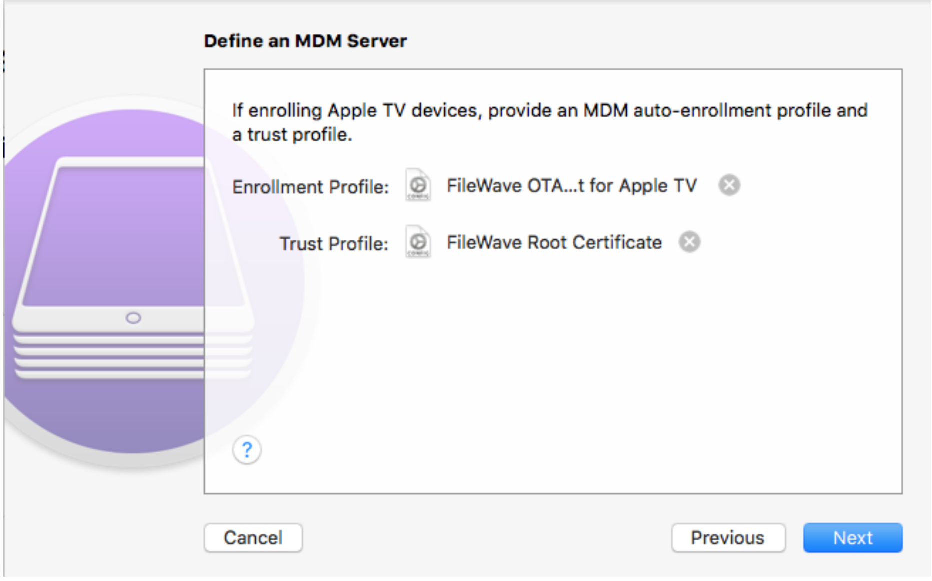


Define an MDM Server

If enrolling Apple TV devices, provide an MDM auto-enrollment profile and a trust profile.

Enrollment Profile: None

Trust Profile: FileWave Root Certificate



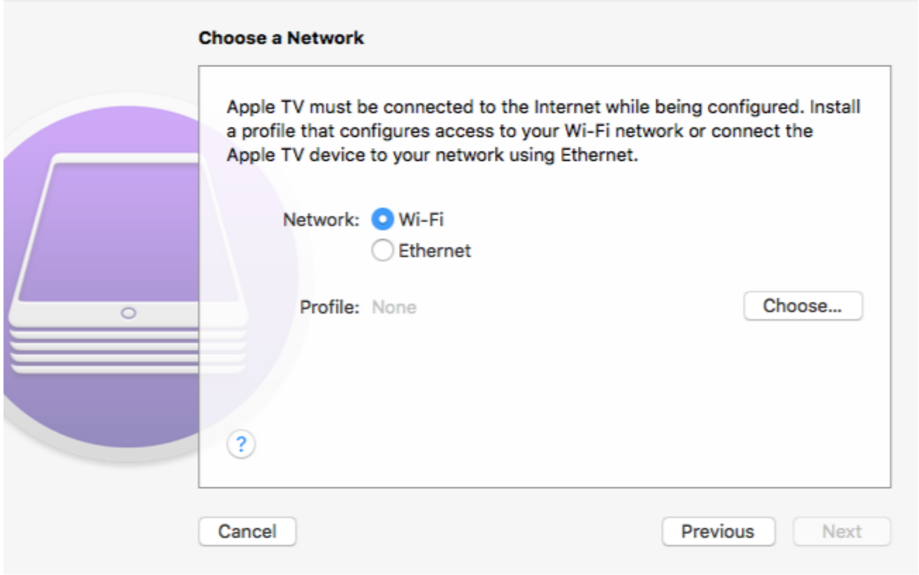
Define an MDM Server

If enrolling Apple TV devices, provide an MDM auto-enrollment profile and a trust profile.

Enrollment Profile: FileWave OTA...t for Apple TV

Trust Profile: FileWave Root Certificate

Now that you have all the needed items in this window, click **Next**. In FileWave, create a profile for Wi-Fi with the SSID and password necessary for the Apple TV to join the wireless network and import that using the **Choose…** button to navigate to its location to add it to the blueprint.



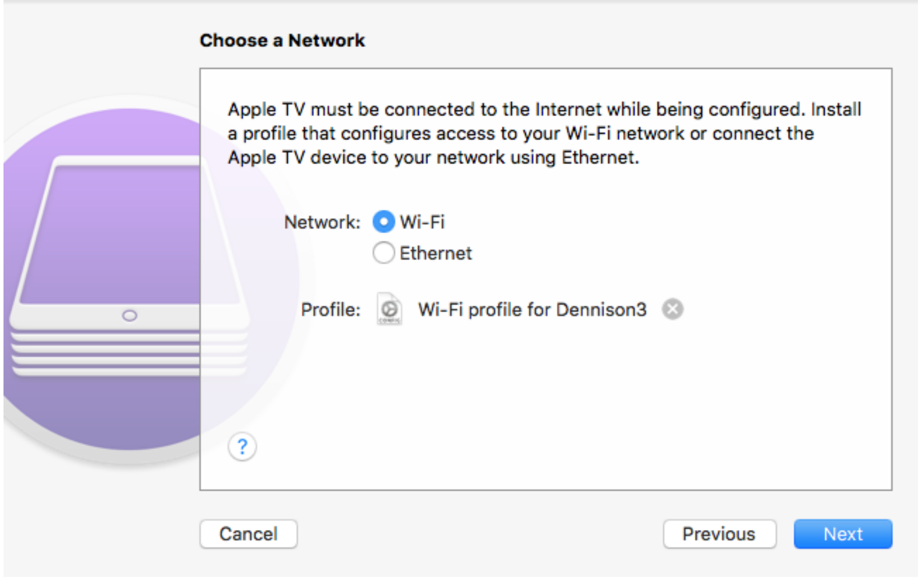
Choose a Network

Apple TV must be connected to the Internet while being configured. Install a profile that configures access to your Wi-Fi network or connect the Apple TV device to your network using Ethernet.

Network: ● Wi-Fi
○ Ethernet

Profile: None

Now, click **Next**.



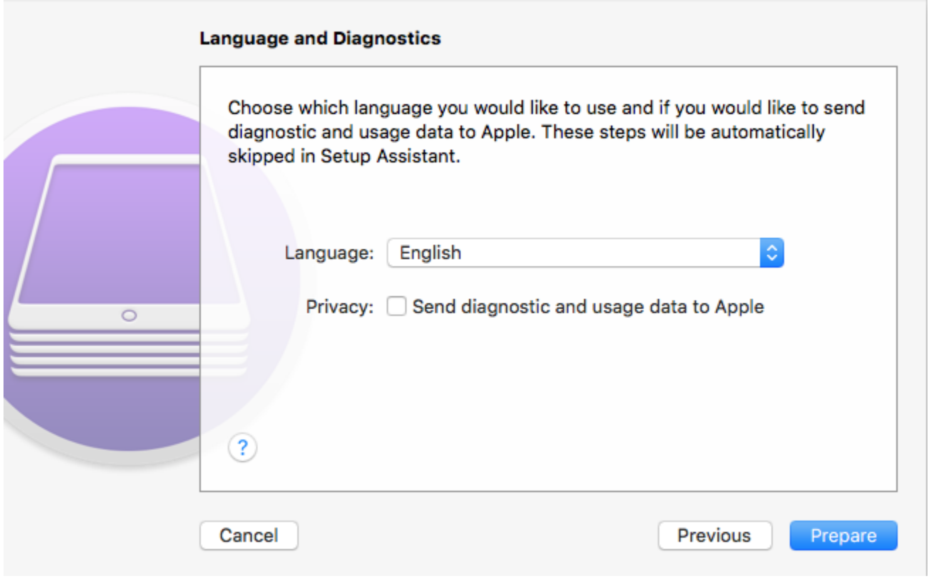
Choose a Network

Apple TV must be connected to the Internet while being configured. Install a profile that configures access to your Wi-Fi network or connect the Apple TV device to your network using Ethernet.

Network: ● Wi-Fi
○ Ethernet

Profile: Wi-Fi profile for Dennison3

Select the language you want to use and whether or not you want diagnostic and usage data sent to Apple, then click **Prepare**.



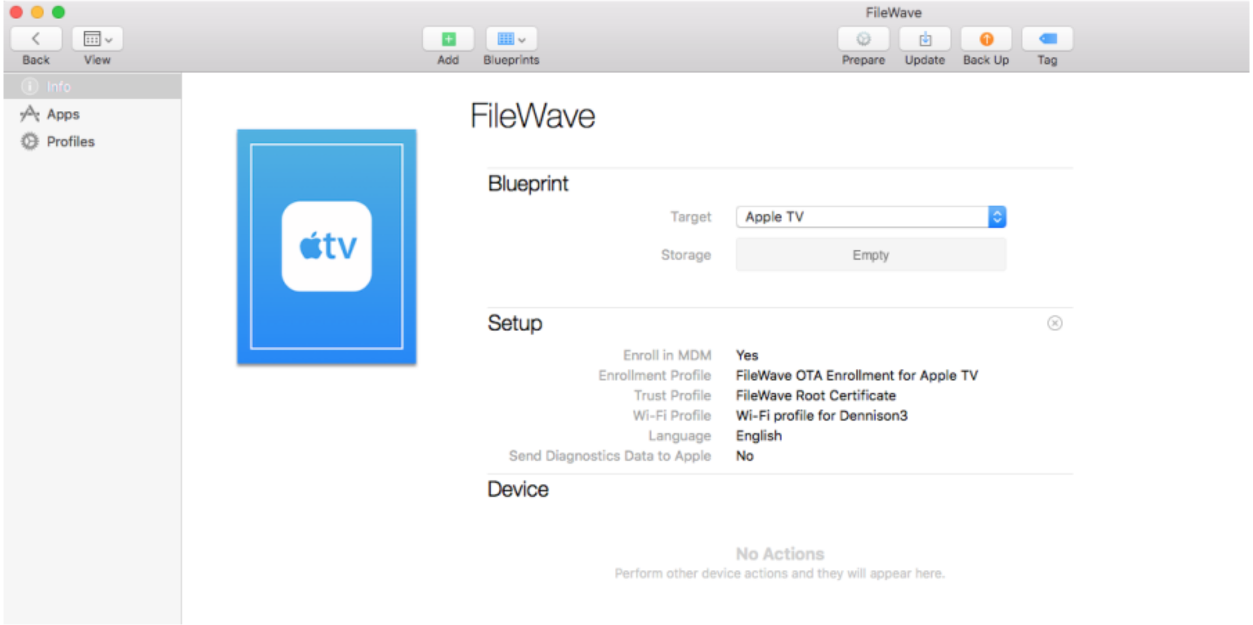
Language and Diagnostics

Choose which language you would like to use and if you would like to send diagnostic and usage data to Apple. These steps will be automatically skipped in Setup Assistant.

Language: English

Privacy: □ Send diagnostic and usage data to Apple

Now, all the pieces are in place and this blueprint can be applied to a connected device.



FileWave

Blueprint

Target: Apple TV

Storage: Empty

Setup

Enroll in MDM: Yes
Enrollment Profile: FileWave OTA Enrollment for Apple TV
Trust Profile: FileWave Root Certificate
Wi-Fi Profile: Wi-Fi profile for Dennison3
Language: English
Send Diagnostics Data to Apple: No

Device

No Actions
Perform other device actions and they will appear here.

4.6. Installing the Android client

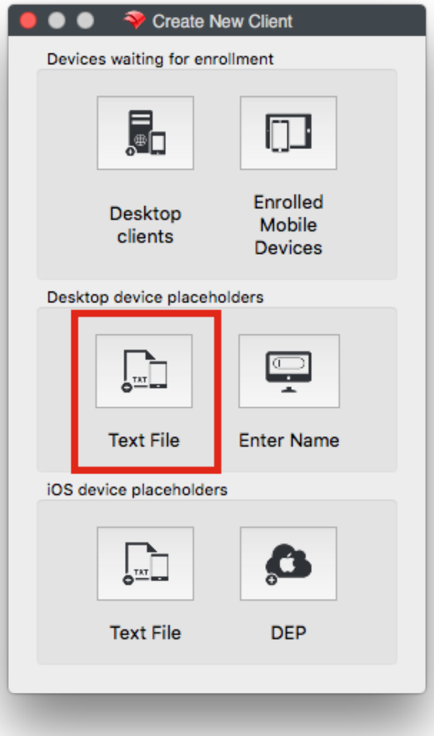
With FileWave, you can install Android applications and get inventory data. The Android client installation process resembles the iOS workflow, with a few exceptions. The basic steps are as follows:

- 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.
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…**
Android devices can be assigned Boosters through the **Preferences…**, 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.
All other information is accessed the same way as for any computer Client (Android Clients are a hybrid Mobile/Computer Client) using the **Client Monitor** or the **Client Info** panes.

4.7. Importing Computer Clients from a File

You can import a "tab-delimited" text file (not a CSV file).
The import location is in the **Create New Client** pane:



The new format looks like this:
Client Name <tab> Comment <tab> Serial or MAC
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.

4.8. 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. For information on approved devices in DEP, see the following reference:
https://help.apple.com/deployment/business/
The features of DEP include:

- *Zero-touch configuration* - devices (iOS and macOS) 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 automatically 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 control.
- *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. Wait 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

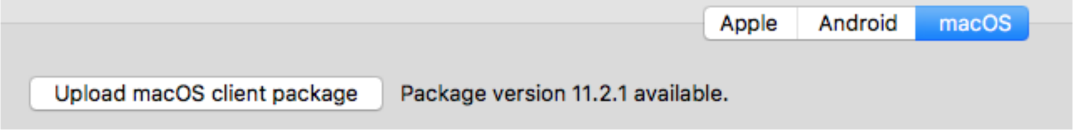
7. Devices arrive and, at first boot, are auto-enrolled and configured as managed devices (macOS computers will auto-enroll if connected to the Internet for push notification and the MDM server for enrollment.)

Configuring DEP with FileWave

This process is covered in Section **2.12**.

FileWave Client for OS X DEP

The macOS computers that are being brought into FileWave through Apple's DEP require a custom FileWave client installer. To be installed via MDM, the 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 for use by macOS Clients.



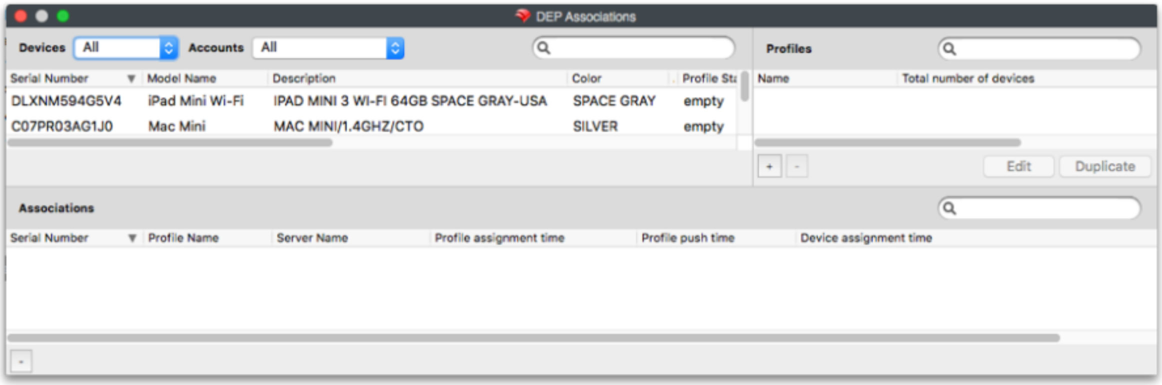
Package version 11.2.1 available.

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:



Serial Number	Model Name	Description	Color	Profile Sta
DLXNM594G5V4	iPad Mini Wi-Fi	IPAD MINI 3 WI-FI 64GB SPACE GRAY-USA	SPACE GRAY	empty
C07PR03AG1J0	Mac Mini	MAC MINI/1.4GHZ/CTO	SILVER	empty

Name	Total number of devices

Serial Number	Profile Name	Server Name	Profile assignment time	Profile push time	Device assignment time

The **DEP Associations** pane looks similar to other FileWave windows with 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 date-time Groups showing assignment dates and times.

Security prerequisites for DEP

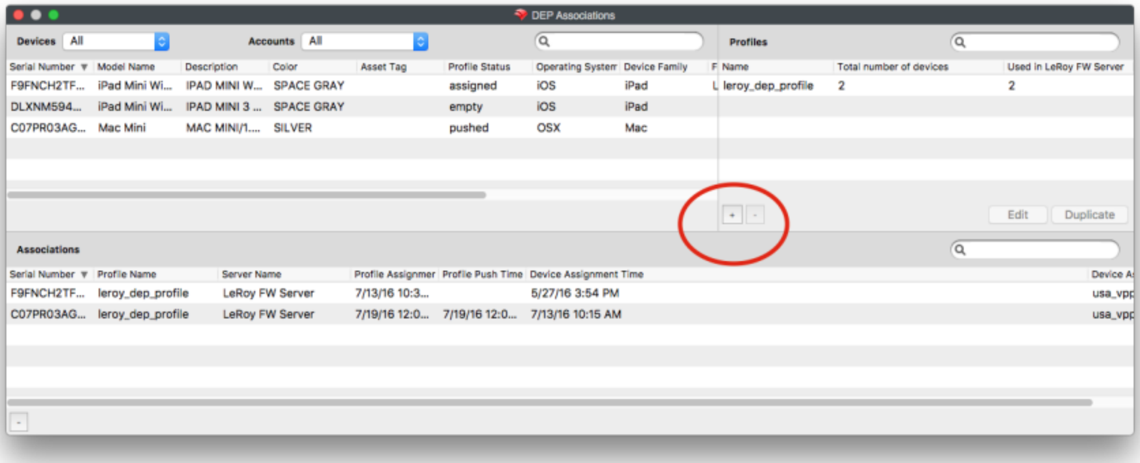
DEP uses Basic and Digest Authentication. Basic is for iOS v7.1(+) devices, and we implemented Digest Authentication for iOS v7.0.x devices. In order to configure up your FileWave MDM server for Digest Authentication, you need to use a separate command, similar to the **fwcontrol mdm adduser** command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

Authentication with LDAP

If you are using LDAP and DEP, you will have to use iOS v7.1.x(+) devices. The *mdm_auth.conf.example_ldap_auth* file we provide is based on basic authentication, while the default is using digest. If you have not already edited the **mdm_auth.conf**, then review the information in Section **2 .11**.

Configuring DEP profiles

You create DEP profiles within the **DEP Associations** pane by clicking on the **+** button in the profile section of the window.



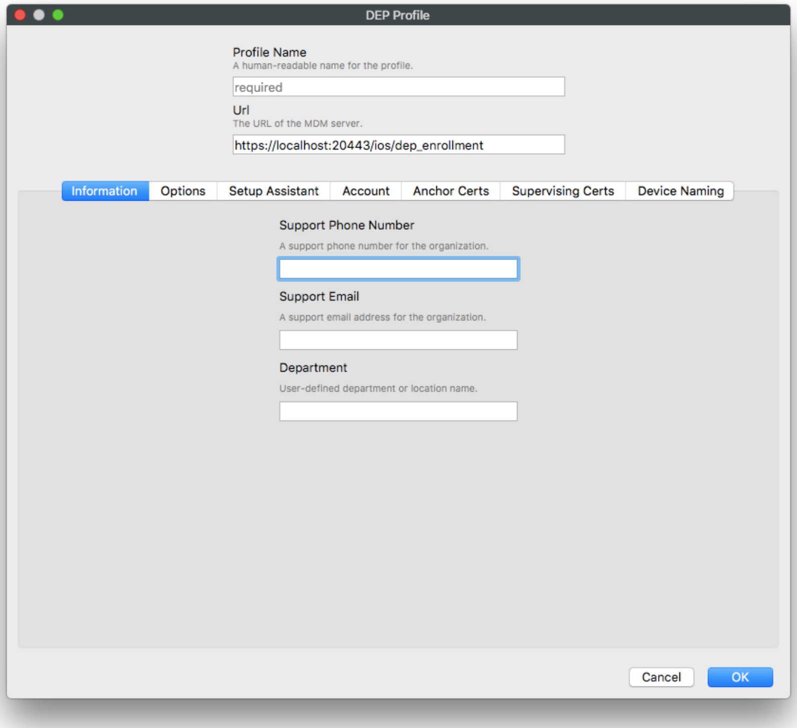
Serial Number	Model Name	Description	Color	Asset Tag	Profile Status	Operating System	Device Family	F
F9FNCH2TF...	iPad Mini Wi...	IPAD MINI W...	SPACE GRAY		assigned	iOS	iPad	L
DLXNM594...	iPad Mini Wi...	IPAD MINI 3 ...	SPACE GRAY		empty	iOS	iPad	
C07PR03AG...	Mac Mini	MAC MINI/1....	SILVER		pushed	OSX	Mac	

Name	Total number of devices	Used in LeRoy FW Server
leroy_dep_profile	2	2

Serial Number	Profile Name	Server Name	Profile Assignmer	Profile Push Time	Device Assignment Time	Device A:
F9FNCH2TF...	leroy_dep_profile	LeRoy FW Server	7/13/16 10:3...		5/27/16 3:54 PM	usa_vpp
C07PR03AG...	leroy_dep_profile	LeRoy FW Server	7/19/16 12:0...	7/19/16 12:0...	7/13/16 10:15 AM	usa_vpp

Here is a view of the **DEP Profile** creation window:

Information



Profile Name
A human-readable name for the profile.
required

Url
The URL of the MDM server.
https://localhost:20443/ios/dep_enrollment

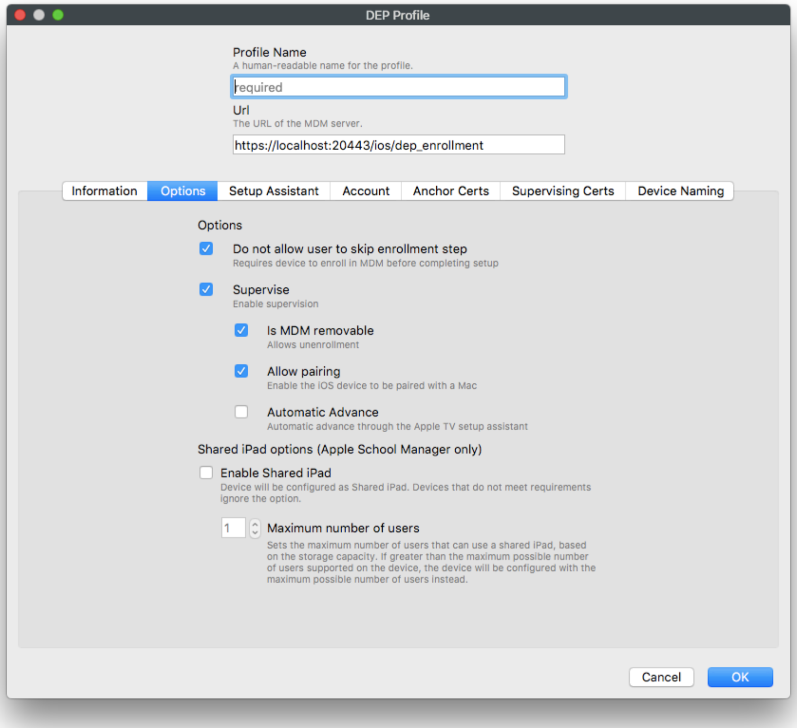
Support Phone Number
A support phone number for the organization.

Support Email
A support email address for the organization.

Department
User-defined department or location name.

This information will be set in the MDM profile once installed on the MDM device.

Options



Profile Name
A human-readable name for the profile.
required

Url
The URL of the MDM server.
https://localhost:20443/ios/dep_enrollment

Options

☑ Do not allow user to skip enrollment step
Requires device to enroll in MDM before completing setup

☑ Supervise
Enable supervision

☑ Is MDM removable
Allows unenrollment

☑ Allow pairing
Enable the iOS device to be paired with a Mac

□ Automatic Advance
Automatic advance through the Apple TV setup assistant

Shared iPad options (Apple School Manager only)

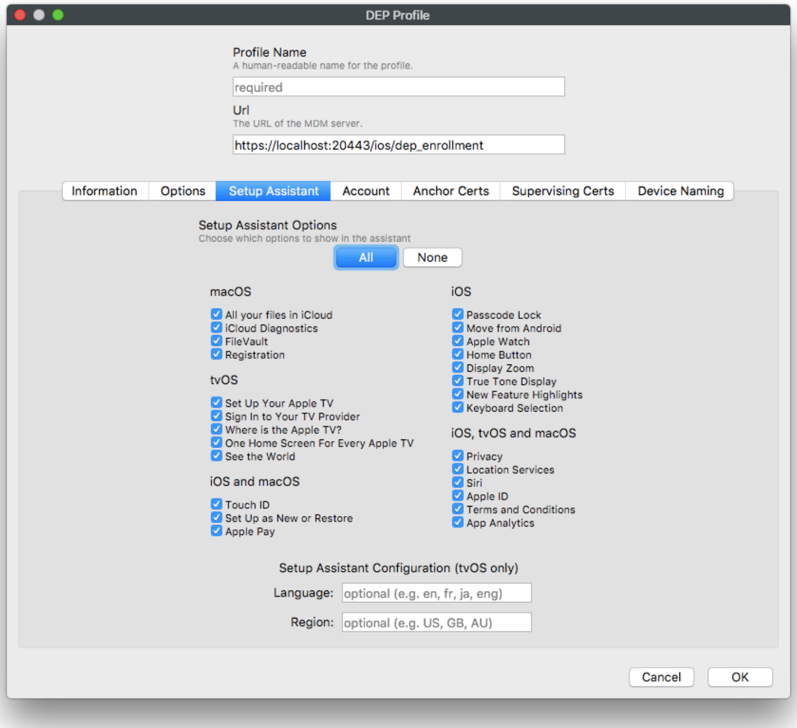
□ Enable Shared iPad
Device will be configured as Shared iPad. Devices that do not meet requirements ignore the option.

1 Maximum number of users
Sets the maximum number of users that can use a shared iPad, based on the storage capacity. If greater than the maximum possible number of users supported on the device, the device will be configured with the maximum possible number of users instead.

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
  - ***Automatic Advance*** - if checked, the Apple TV will automatically advance through setup assistant (If you use the remote on the Apple TV this option will be canceled)
- ***Enable Shared iPad*** - Device will be configured as a Shared iPad. Devices that do not meet reuirements ignore the option.
  - ***Maximum number of users*** - Sets the maximum number of users that can use a shared iPad, based on the storage capacity. If greater than the maximum possible number of users supported on the device, the device will be configured with the maximum possible number of users instead.

Setup Assistant



Profile Name
A human-readable name for the profile.
required

Url
The URL of the MDM server.
https://localhost:20443/ios/dep_enrollment

Setup Assistant Options
Choose which options to show in the assistant

macOS

☑ All your files in iCloud
☑ iCloud Diagnostics
☑ FileVault
☑ Registration

tvOS

☑ Set Up Your Apple TV
☑ Sign In to Your TV Provider
☑ Where is the Apple TV?
☑ One Home Screen For Every Apple TV
☑ See the World

iOS and macOS

☑ Touch ID
☑ Set Up as New or Restore
☑ Apple Pay

iOS

☑ Passcode Lock
☑ Move from Android
☑ Apple Watch
☑ Home Button
☑ Display Zoom
☑ True Tone Display
☑ New Feature Highlights
☑ Keyboard Selection

iOS, tvOS and macOS

☑ Privacy
☑ Location Services
☑ Siri
☑ Apple ID
☑ Terms and Conditions
☑ App Analytics

Setup Assistant Configuration (tvOS only)

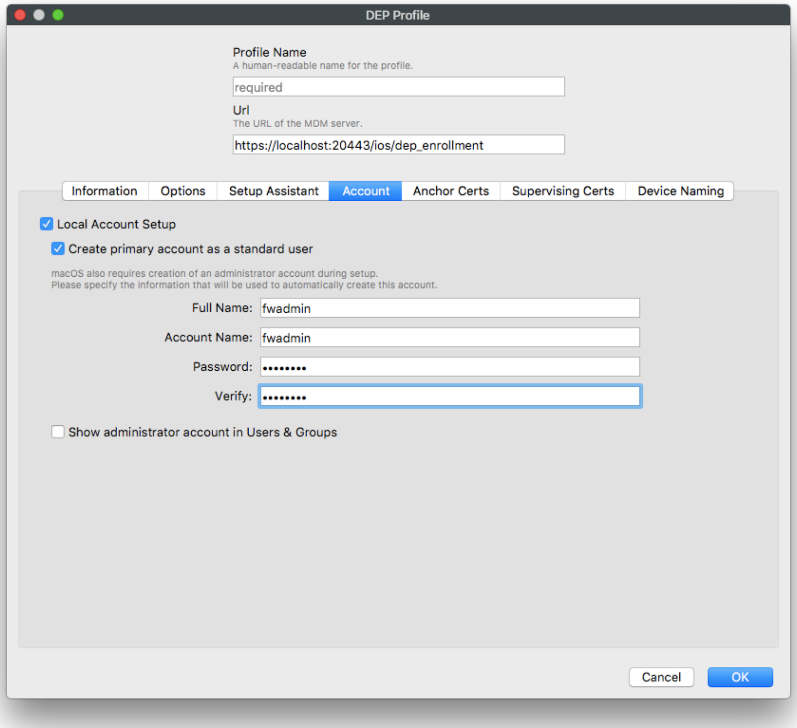
Language: optional (e.g. en, fr, ja, eng)

Region: optional (e.g. US, GB, AU)

- ***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 pre-configured using MDM profiles with all of the appropriate settings to ensure functionality.

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

A feature in DEP is the ability to create a local administrator 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. The local admin account can be somewhat hidden (the home directory will still be in /Users/ but it will not show up in the Users and Groups System Preference pane).



Profile Name
A human-readable name for the profile.
required

Url
The URL of the MDM server.
https://localhost:20443/ios/dep_enrollment

☑ Local Account Setup

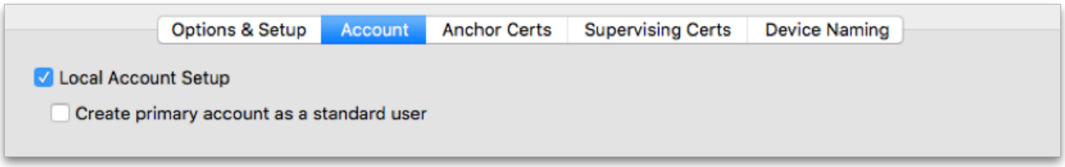
☑ Create primary account as a standard user

macOS also requires creation of an administrator account during setup.
Please specify the information that will be used to automatically create this account.

Full Name: fwadmin
Account Name: fwadmin
Password: ••••••••
Verify: ••••••••

☐ Show administrator account in Users & Groups

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.



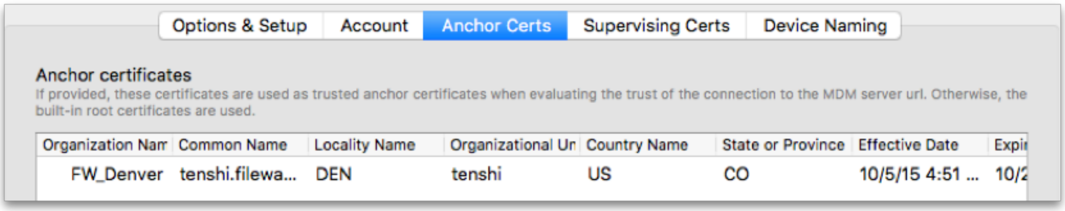
☑ Local Account Setup

☐ Create primary account as a standard user

Note: Disallowing "Local Account Setup" During DEP enrollment may prevent your machines from completing their enrollment steps unless the local administrator account logs in on the machine.

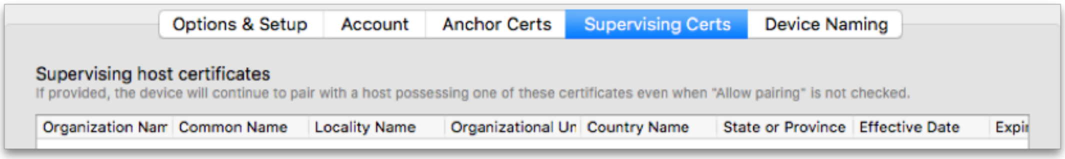
"Certs"

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.



Anchor certificates
If provided, these certificates are used as trusted anchor certificates when evaluating the trust of the connection to the MDM server url. Otherwise, the built-in root certificates are used.

Organization Nam	Common Name	Locality Name	Organizational Un	Country Name	State or Province	Effective Date	Expi
FW_Denver	tenshi.filewa...	DEN	tenshi	US	CO	10/5/15 4:51 ...	10/2

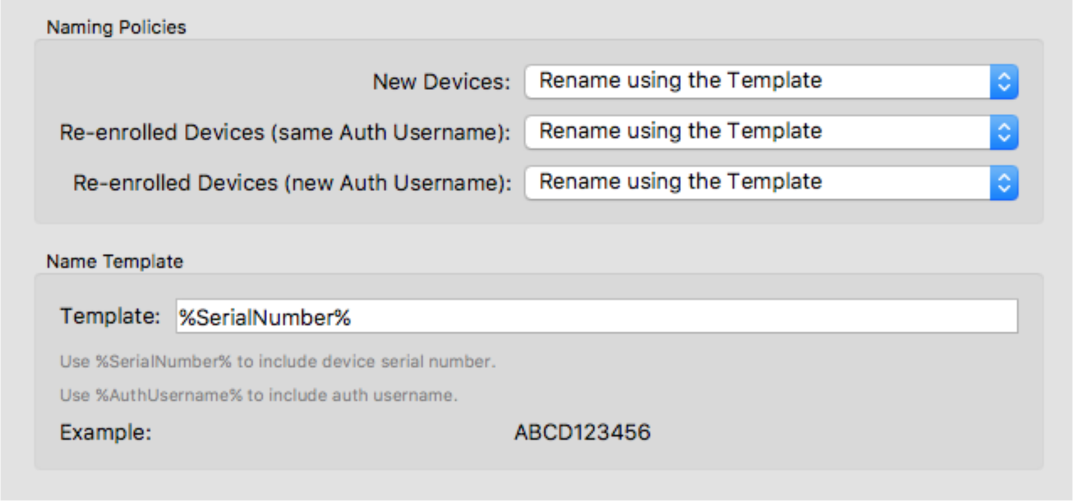


Supervising host certificates
If provided, the device will continue to pair with a host possessing one of these certificates even when "Allow pairing" is not checked.

Organization Nam	Common Name	Locality Name	Organizational Un	Country Name	State or Province	Effective Date	Expi

Device Naming

The devices being enrolled can have a rule-based name applied. In a 1:1 deployment with users authenticating with LDAP credentials, the device name can reflect an institutionally-derived naming convention punctuated by the user's name. This function is limited to supervised iOS devices running iOS 9+ and macOS computers running 10.11+.



Naming Policies

New Devices: Rename using the Template

Re-enrolled Devices (same Auth Username): Rename using the Template

Re-enrolled Devices (new Auth Username): Rename using the Template

Name Template

Template: %SerialNumber%

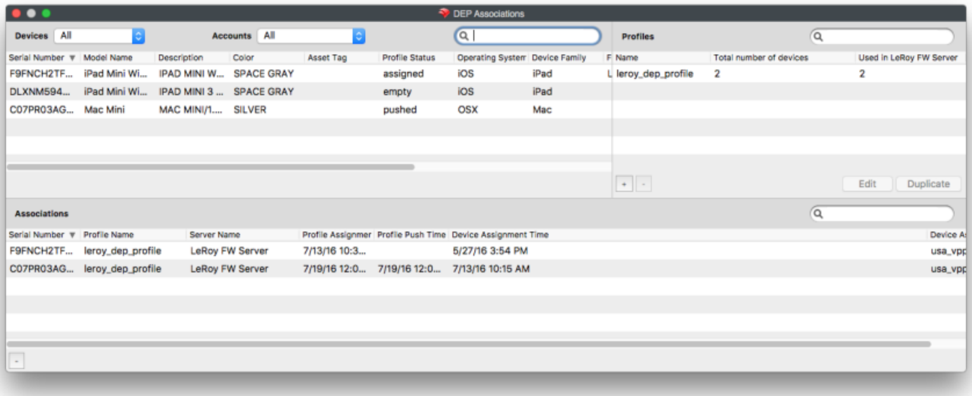
Use %SerialNumber% to include device serial number.

Use %AuthUsername% to include auth username.

Example: ABCD123456

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.



DEP Associations

Devices: All   Accounts: All

Serial Number ▼	Model Name	Description	Color	Asset Tag	Profile Status	Operating Systen	Device Family	F
F9FNCH2TF...	iPad Mini Wi...	IPAD MINI W...	SPACE GRAY		assigned	iOS	iPad	L
DLXNM594...	iPad Mini Wi...	IPAD MINI 3 ...	SPACE GRAY		empty	iOS	iPad	
C07PR03AG...	Mac Mini	MAC MINI/1....	SILVER		pushed	OSX	Mac	

Profiles

Name	Total number of devices	Used in LeRoy FW Server
leroy_dep_profile	2	2

Associations

Serial Number ▼	Profile Name	Server Name	Profile Assignmer	Profile Push Time	Device Assignment Time	Device A
F9FNCH2TF...	leroy_dep_profile	LeRoy FW Server	7/13/16 10:3...		5/27/16 3:54 PM	usa_vpp
C07PR03AG...	leroy_dep_profile	LeRoy FW Server	7/19/16 12:0...	7/19/16 12:0...	7/13/16 10:15 AM	usa_vpp

End Result of DEP associations

The end result of associating DEP profiles to devices is that upon activation, the device 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.
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 to perform 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; e.g., when the device is past its lease period and is going to sold to an end user.

4.9. Working with FileWave Clients

Once the various devices have 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

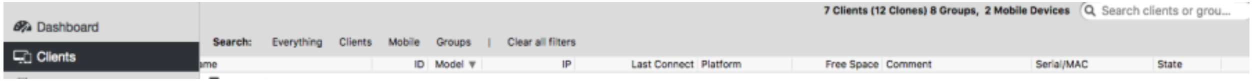
Within the **Clients** pane, you are presented with key information to help you track of the status of your devices:

- ***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
- ***State*** - shows the condition of the device (Normal, Missing, Not Tracked, Archived)
- ***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 in FileWave, you can start performing administrative and management tasks on them.

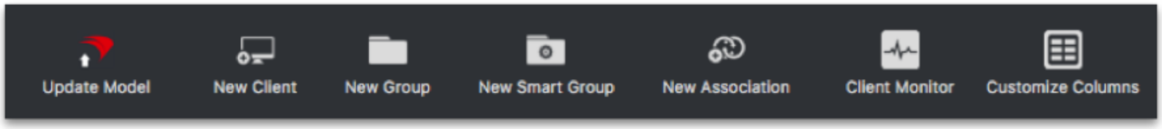
Search

At the top of the Clients view pane, you can see a **Search**: area that lets you quickly see one or four different views of all your devices (Everything, Clients, Mobile, and Groups) There is also a quick view of the total number of clients, Clones, Groups, and mobile devices. Finally, there is a global search field that allows you to type in a name or portion of a name, ID, database model number, or any other possible identifier to locate a specific device or Group. Any search you start can be cleared by clicking on the **Clear all filters** button just above the viewing window.



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, you should update the "Model." The *Model* is the current state of the FileWave database after changes have been committed by an administrator. 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.

New Client

This tool allows you to register with the database new clients for computers that have had the FileWave client installed and have checked-in initially, from mobile device that have enrolled with the FileWave MDM server, or by creating placeholders for devices or computers manually or using either text files or DEP.

New Group

The **New Group** tool allows you to create a named Group that will include individual Clients or Clones.

New Smart Group

This tool allows you to create a named Group of devices based upon inventory criteria.

New Association

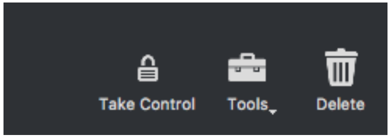
The focal point of FileWave is being able to create and distribute Filesets to devices. This tool provides one approach for you to associate a Fileset or Fileset Group with a Client or Group.

Client Monitor

The Client Monitor lets you view the current status of your Client after selecting that Client from the list. 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 Client to verify its status with the FileWave Server, and allows you to view the Client's FileWave log file.

Customize Columns

You can 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 resume managing their assigned clients.

Tools

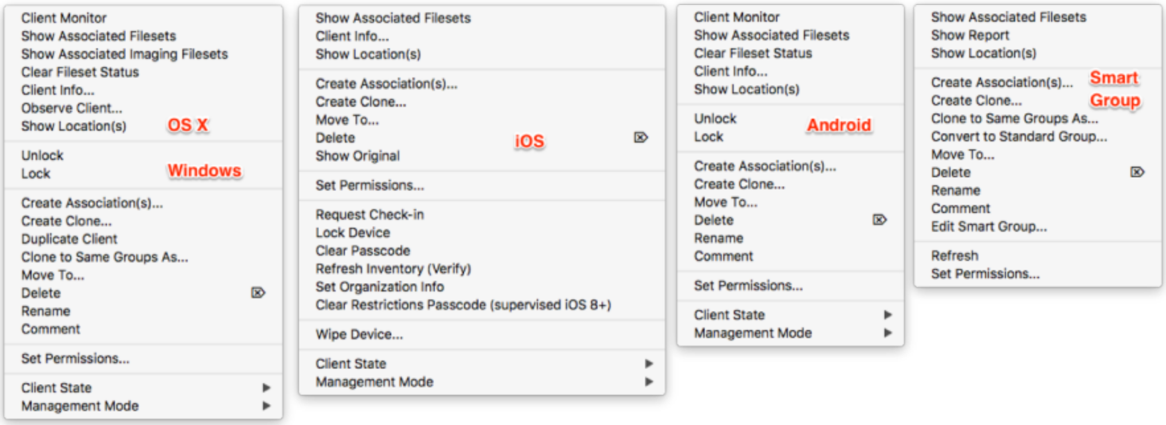
The Client tools are tasks that you can perform on a selected Client or Group. The specific tasks available vary between the different types of client devices or Groups. The next section will go into detail on each of the tools as they relate to the various types of clients and client Groups.

Delete

The Delete tool will remove the selected Client(s) or Group(s) from the database. If you delete a Group, then all nested items within that Group will also be deleted.

Client Tools

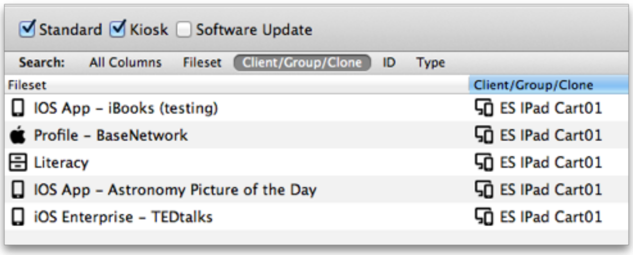
Here are the tools you have to directly impact a specific client. Depending on the client device, you will see differing settings.



When you right-click on a Client, or select a Client then select the **Tools** task bar item, you will see the listed tools that are available to interact with that type of 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.



☑ Standard ☑ Kiosk □ Software Update

Search: All Columns Fileset Client/Group/Clone ID Type

Fileset	Client/Group/Clone
IOS App - iBooks (testing)	ES IPad Cart01
Profile - BaseNetwork	ES IPad Cart01
Literacy	ES IPad Cart01
IOS App - Astronomy Picture of the Day	ES IPad Cart01
iOS Enterprise - TEDtalks	ES IPad Cart01

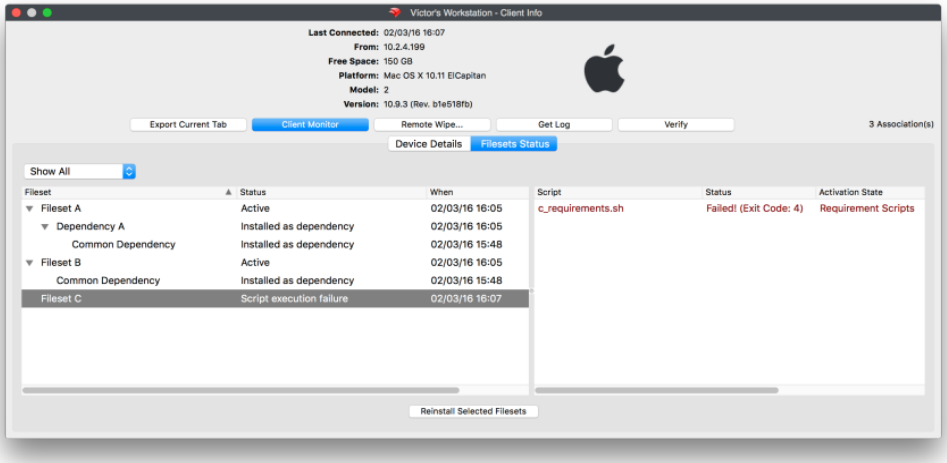
Client Info…

The Client Info window shows the current condition of a Client 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, which causes the Client to verify that it's current state matches what the current manifest says it should be. Depending on the device, you will get differing amounts of information.

As of FileWave 11, the list of Filesets is displayed as a tree, where dependencies appear as children of the Filesets that require them. When a dependency is required by more than one Fileset, the same dependency will appear more than once in the list, as a child of each of the Filesets that require it.

There is a selection box on the top-left corner that allows filtering Filesets. By default, it is set to "Show All. Other values are "Only successful" and "Only failed," that cause only Filesets without errors/with errors to be shown. "Filesets without errors" means any Fileset in any normal state, when nothing failed. Filesets that are associated but haven't been installed yet are considered "without errors

If the client version is 11.0 or later, it also supports reporting the results of the scripts that were executed. In this case, selecting a Fileset causes a list to appear on the right side, where the results of the last round of scripts is reported. Whenever a script fails, processing stops, and the exit code of the script can be seen in the Status column.



Victor's Workstation - Client Info

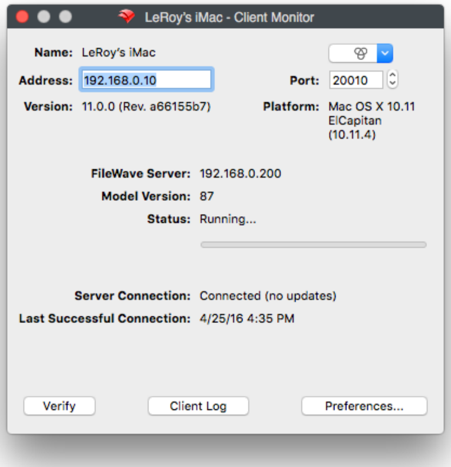
Last Connected: 02/03/16 16:07
From: 10.2.4.199
Free Space: 150 GB
Platform: Mac OS X 10.11 ElCapitan
Model: 2
Version: 10.9.3 (Rev. b1e518fb)

Fileset	Status	When
Fileset A	Active	02/03/16 16:05
Dependency A	Installed as dependency	02/03/16 16:05
Common Dependency	Installed as dependency	02/03/16 15:48
Fileset B	Active	02/03/16 16:05
Common Dependency	Installed as dependency	02/03/16 15:48
Fileset C	Script execution failure	02/03/16 16:07

Script	Status	Activation State
c_requirements.sh	Failed! (Exit Code: 4)	Requirement Scripts

Client Monitor

The Client Monitor lets you view the current status of your Client after selecting that Client from the list. 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 Client to verify its status with the FileWave Server, and allows you to view the Client's FileWave log file.



LeRoy's iMac - Client Monitor

Name: LeRoy's iMac

Address: 192.168.0.10

Port: 20010

Version: 11.0.0 (Rev. a66155b7)

Platform: Mac OS X 10.11 ElCapitan (10.11.4)

FileWave Server: 192.168.0.200

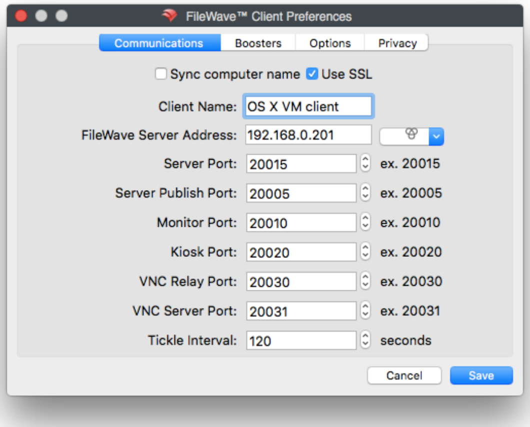
Model Version: 87

Status: Running...

Server Connection: Connected (no updates)

Last Successful Connection: 4/25/16 4:35 PM

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



FileWave™ Client Preferences

□ Sync computer name ☑ Use SSL

Client Name: OS X VM client

FileWave Server Address: 192.168.0.201

Server Port: 20015 ex. 20015

Server Publish Port: 20005 ex. 20005

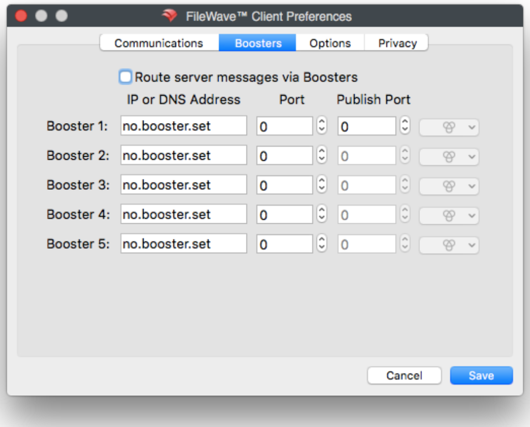
Monitor Port: 20010 ex. 20010

Kiosk Port: 20020 ex. 20020

VNC Relay Port: 20030 ex. 20030

VNC Server Port: 20031 ex. 20031

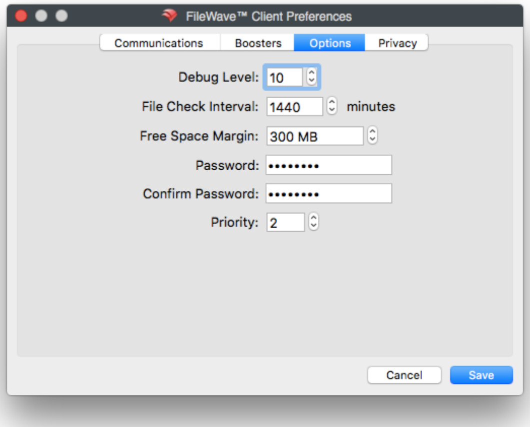
Tickle Interval: 120 seconds



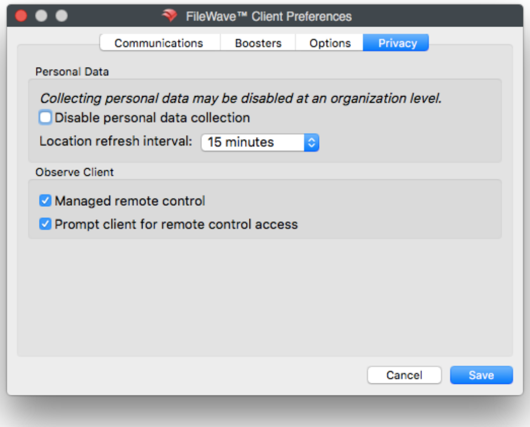
FileWave™ Client Preferences

□ Route server messages via Boosters

	IP or DNS Address	Port	Publish Port
Booster 1:	no.booster.set	0	0
Booster 2:	no.booster.set	0	0
Booster 3:	no.booster.set	0	0
Booster 4:	no.booster.set	0	0
Booster 5:	no.booster.set	0	0



Debug Level: 10
File Check Interval: 1440 minutes
Free Space Margin: 300 MB
Password: ••••••••
Confirm Password: ••••••••
Priority: 2



Personal Data

Collecting personal data may be disabled at an organization level.
☐ Disable personal data collection
Location refresh interval: 15 minutes

Observe Client

☑ Managed remote control
☑ Prompt client for remote control access

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.
Personal Data refers to device tracking (requires FW v10.1+). Tracking is covered in detail later in this Chapter.
Observe Client refers to the built-in VNC server introduced in the FW v10. If you select **Managed remote control,** you will have access to observe / control that computer. If you select **Prompt client for remote control access,** you will present the end user on the computer with a dialog requesting permission to remotely control the device. If this dialog is not responded to with permission granted, it will time out in about 30 seconds and default to permission denied.

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).

Edit Custom Fields(s) Values

This option will allow you to change the values of Custom Fields that have been associated to this device or group of devices. For example if you manually change the value of a Custom Field that is syncing with LDAP with this option, then your change will remain until LDAP scans again at which point your change will be over written with whatever data is synced from LDAP.

Edit Custom Field(s) Associations

Here is where association between Customs Fields and devices are made. If you select one or multiple devices you can set which Custom Field(s) you would like those devices to have. If you select a group (smart or standard) then you will select which custom Fields you would like to set for the devices under this group. If new devices enter this group after you have the Custom Field associated, you would need reassign that Custom Field to the group or those new devices specifically. Custom Fields do not auto-associate to new additions in a group.

Lock / Unlock

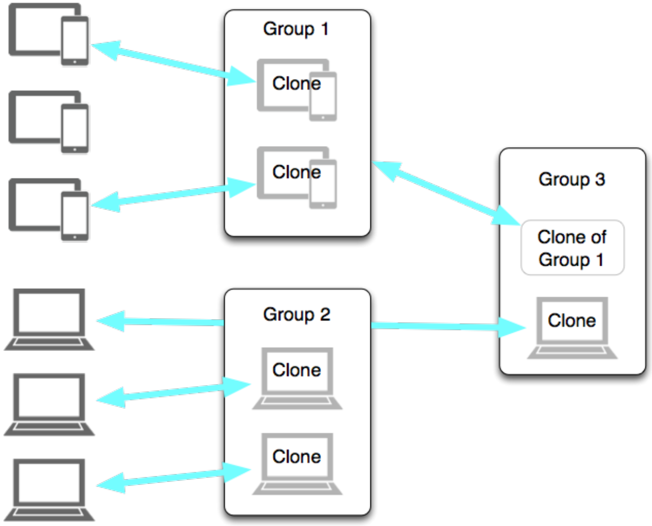
When a client device is locked, it can no longer receive model updates from the FileWave server. You might use this setting if a device is being used for some operation that would be interrupted during a Fileset activation.

Create Association(s)…

The primary function of FileWave Admin is to associate Clients 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 **5**.

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 Groups based on organizational needs, geographies, or even just for application usage. A Client 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 Client, you can leave the actual Client 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 into which you can place a Clone.

Clone to Same Groups As…

This task lets you choose another Client device as the template to create Clones of the selected Client. If the template device has Clones in several Groups, then your Client will end up with 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 will not be deleted, even if their Clones were inside the Group. Make sure you update the Model when you delete Clients or Groups.

Rename

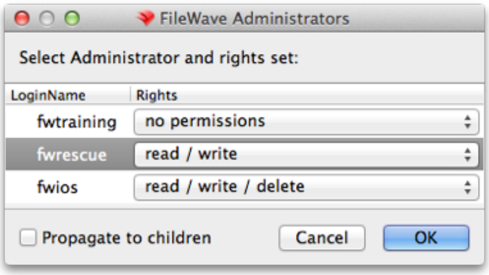
To rename your Client or Group, use this command. You can also click twice on your client (slower than a double-click) to edit the name.

Comment

This task allows you to add a comment to your Client or Group record.

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 computers and another to manage only the iPad cart in a classroom. Some administrators could be assigned only read permissions in order to create reports.



FileWave Administrators

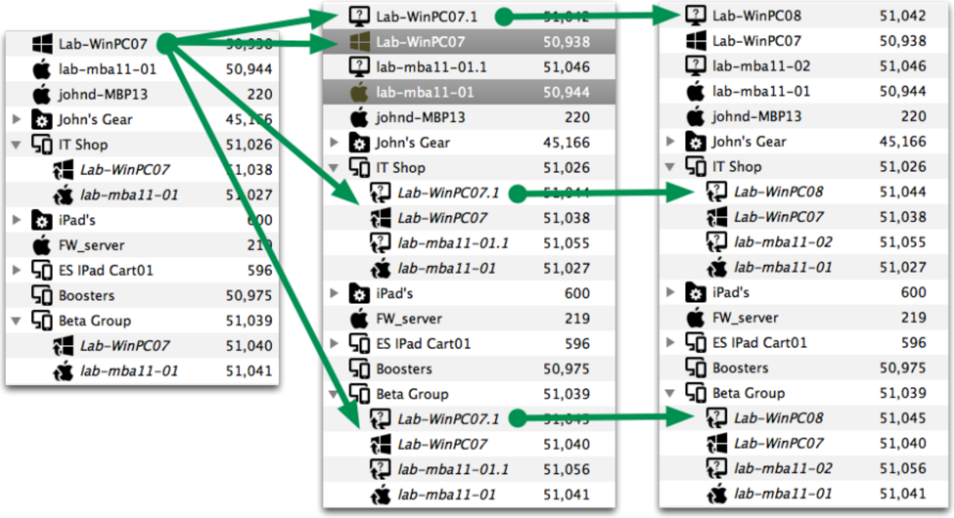
Select Administrator and rights set:

LoginName	Rights
fwtraining	no permissions
fwrescue	read / write
fwios	read / write / delete

□ Propagate to children

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 its new name is *Lab-WinPC07.1* Wh en 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.



Lab-WinPC07	50,938
lab-mba11-01	50,944
johnd-MBP13	220
▸ John's Gear	45,166
▾ IT Shop	51,026
Lab-WinPC07	51,038
lab-mba11-01	51,027
▸ iPad's	600
FW_server	219
▸ ES IPad Cart01	596
Boosters	50,975
▾ Beta Group	51,039
Lab-WinPC07	51,040
lab-mba11-01	51,041

Lab-WinPC07.1	51,042
Lab-WinPC07	50,938
lab-mba11-01.1	51,046
lab-mba11-01	50,944
johnd-MBP13	220
▸ John's Gear	45,166
▾ IT Shop	51,026
Lab-WinPC07.1	51,044
Lab-WinPC07	51,038
lab-mba11-01.1	51,055
lab-mba11-01	51,027
▸ iPad's	600
FW_server	219
▸ ES IPad Cart01	596
Boosters	50,975
▾ Beta Group	51,039
Lab-WinPC07.1	51,045
Lab-WinPC07	51,040
lab-mba11-01.1	51,056
lab-mba11-01	51,041

Lab-WinPC08	51,042
Lab-WinPC07	50,938
lab-mba11-02	51,046
lab-mba11-01	50,944
johnd-MBP13	220
▸ John's Gear	45,166
▾ IT Shop	51,026
Lab-WinPC08	51,044
Lab-WinPC07	51,038
lab-mba11-02	51,055
lab-mba11-01	51,027
▸ iPad's	600
FW_server	219
▸ ES IPad Cart01	596
Boosters	50,975
▾ Beta Group	51,039
Lab-WinPC08	51,045
Lab-WinPC07	51,040
lab-mba11-02	51,056
lab-mba11-01	51,041

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 Check-in

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). It sets a message on the screen to say that this device is "lost," along with an optional message and phone number to call if found. This is **not** the same as the **Lock** command for non-mobile devices.

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 report back to the FileWave Server an inventory report. 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 computers, it's located in the **Client Info…** window.
You must enter the FileWave "super administrator" (fwadmin) credentials 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 restrictions passcode set on a supervised iOS device.

Archive Client

This command allows an administrator to remove a Client from active use 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.
In order to re-add the client to the active FileWave database, you must fully remove it from FileWave, update the Model, 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 Groups at the same time, instead of having to match individual Clients with specific Filesets.
You can also have nested Groups.

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 (macOS), 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

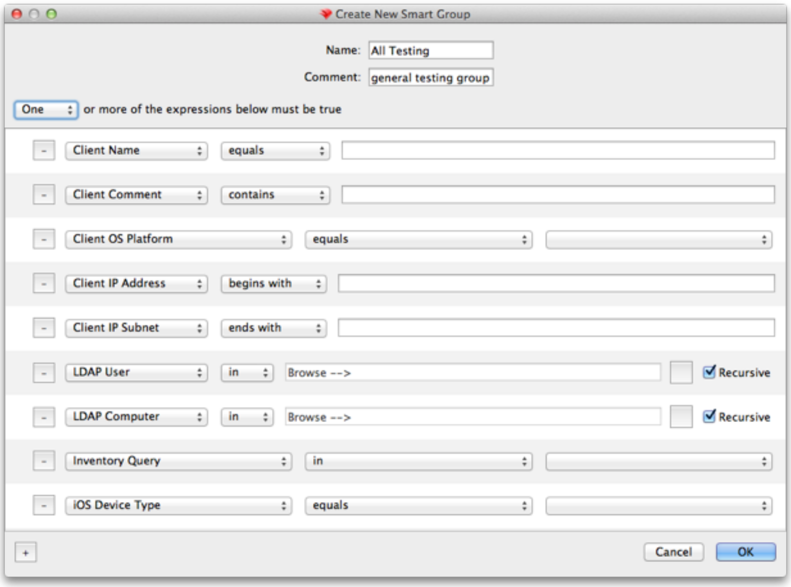
Once you have created one or more Groups, you might want to distribute overall management and maintenance of those Groups. The "Super Admin" account (fwadmin) will always be able to edit or delete any Client or Group in FileWave Admin. What you might want to have is one or more "sub-administrators" who can take over maintenance of one or more specific Groups. This is where the **permissions** come in; right-click on a 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:

- read/write/delete)
- read/write
- read
- no permissions, which equals no access.

The permissions can also be set to **Propagate to children,** which then assign the same permissions to any Group or Groups nested within in that Group.

Creating Smart Groups

The Smart Group is a collection of Clones based on specific criteria. The options you can choose are extensive:



Create New Smart Group

Name: All Testing
Comment: general testing group
One or more of the expressions below must be true

Client Name equals
Client Comment contains
Client OS Platform equals
Client IP Address begins with
Client IP Subnet ends with
LDAP User in Browse --> ☑ Recursive
LDAP Computer in Browse --> ☑ Recursive
Inventory Query in
iOS Device Type equals

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 Smart 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 computers that are bound to the directory. You can associate Filesets and set permissions for any of these Groups. Devices registered by users with their LDAP credentials show up under Users in the LDAP Smart Groups listing. This links the user to the device for tracking purposes. To set up LDAP for authentication, see Chapter **2.**

4.10. 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. 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 computers by installing the FileWave client and having at least one Fileset configured as a Kiosk item associated with that Client. The Kiosk is activated on a mobile device when that device enrolls with the FileWave MDM.
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 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. The computer Kiosk can be configured to always stay visible on a device by editing a file on the client.

The process is outlined and includes methods to customize the look and feel of the Kiosk.

Client Kiosk Customization (12.2+)

Client Kiosk Customization (5.5 - 12.1)

iOS Kiosk Customization

4.11. 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/control of Client computers. FileWave 10+ changes that by imbedding 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 computer and a VNC viewer that will be launched on the FW administrator's computer.

Features

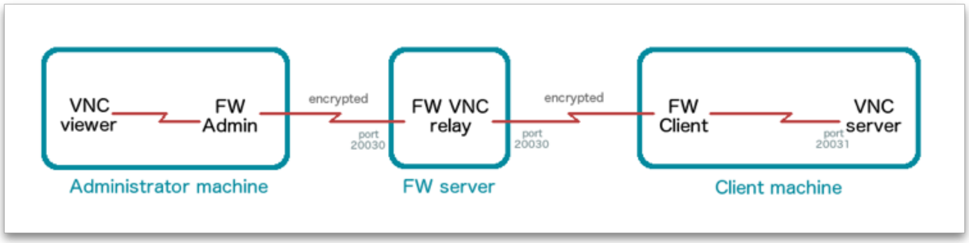
- Network Address Translation (NAT) issues solved using new VNC relay functionality built into the FileWave Server
- Deployment of an independent VNC server on Mac and Windows platforms, with integrated management to ensure existing VNC server deployments are not affected
- Native VNC viewer used on 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 to FileWave 10+.
- Clients must be upgraded to FileWave 10+ 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.

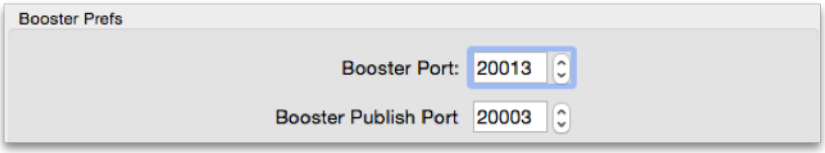
How it works

A FileWave administrator selects a Client computer and chooses to **Observe Client…** from either the **Tools** toolbar item or from the contextual menu for that Client. The VNC viewer will then be launched on the administrator's computer and, if all is well, a communication channel will be established to the client machine.
To avoid issues related to network address translation, 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 *fwcld* process) 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 communicate with the server, the Admin can reach the Client.



Configuration

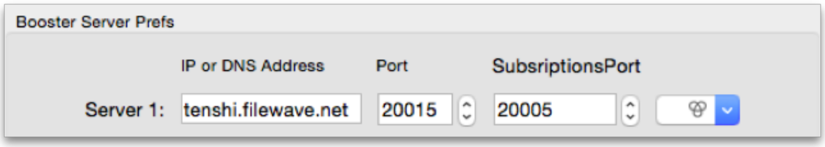
The communication can be from the FW Admin to the Client, or it can pass through a Booster. Any Boosters set up in this environment must be configured to listen for, and pass on, traffic as required using the Subscription and Publish ports. The Booster will "publish" any observe/control communication on its designated Publish port 20003. The Booster will also "subscribe" to any observe/control traffic from other Boosters and clients on port 20005.



Booster Prefs

Booster Port: 20013

Booster Publish Port 20003

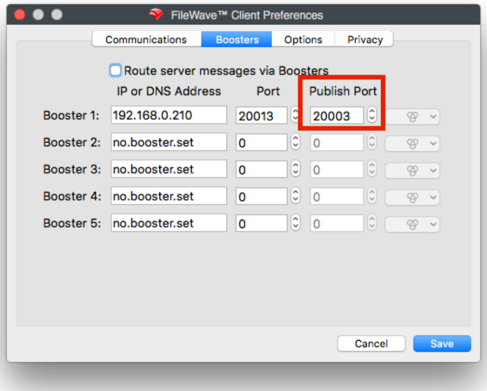


Booster Server Prefs

	IP or DNS Address	Port	SubsriptionsPort
Server 1:	tenshi.filewave.net	20015	20005

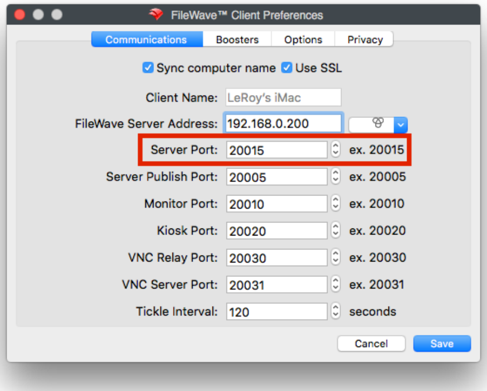
Client Configuration

There are only a few settings for your 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. Second, the user can have the ability to "opt-out" of the communication.



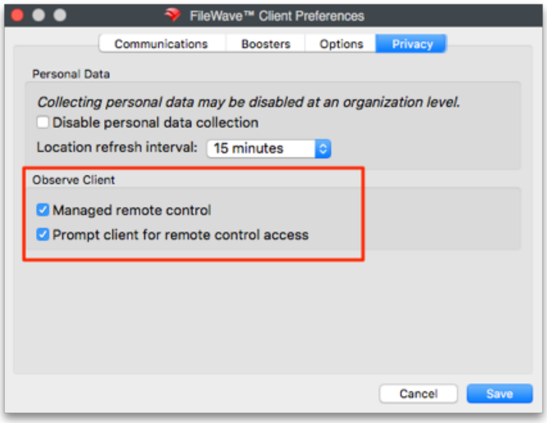
☐ Route server messages via Boosters

	IP or DNS Address	Port	Publish Port
Booster 1:	192.168.0.210	20013	20003
Booster 2:	no.booster.set	0	0
Booster 3:	no.booster.set	0	0
Booster 4:	no.booster.set	0	0
Booster 5:	no.booster.set	0	0



☑ Sync computer name ☑ Use SSL

Client Name:	LeRoy's iMac	
FileWave Server Address:	192.168.0.200	
Server Port:	20015	ex. 20015
Server Publish Port:	20005	ex. 20005
Monitor Port:	20010	ex. 20010
Kiosk Port:	20020	ex. 20020
VNC Relay Port:	20030	ex. 20030
VNC Server Port:	20031	ex. 20031
Tickle Interval:	120	seconds



Personal Data

Collecting personal data may be disabled at an organization level.

☐ Disable personal data collection

Location refresh interval: 15 minutes

Observe Client

☑ Managed remote control

☑ Prompt client for remote control access

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 this. If you select **Prompt client for remote control access**, the end user will have to approve permission in a dialog box at each instance of a remote control session.

4.12. Location Tracking (v10.1+)

FileWave Location Tracking (Version 10.1+)

The location reporting feature in FileWave is disabled by default. It is recommended that you; verify that this feature is in accordance with your organization’s policies and AUP (Acceptable Use Policy). Notify your end users before activating location reporting, as enabling the feature will prompt for permission to location information.

Set by Step Instructions for Enabling Location tracking on Windows, macOS, iOS, Android, and Chromebook

Global Location Reporting Disable

If there are any reasons, legal or otherwise, that you do not wish to enable tracking on a global level within your organization, your FileWave license can be adjusted to enable personal mode. This will disable devices from sending application usage as well as location information.
To have verify the current status of personal data collection. From FileWave Admin : Server Menu "Activation Code..." There you will see "Allow collection of personal data:" with Yes or No after it.

To have personal data enabled or disabled on your license, please submit a support ticket with "Personal data License" in the subject.

Only tickets from authorized support agents whose names are on the support contract will be accepted to adjust license personal data settings.

Requirements:

- FileWave version 10.1+
- Location Tracking Enabled - Server/Client
- All devices you want to track are already enrolled into FileWave and currently communicating properly

Supported Operating Systems:

- Android Jelly Bean, KitKat, Lollipop, Marshmallow, Nougat
- iOS 9+
- macOS 10.9+
- Windows 10
- ChromeOS 43+

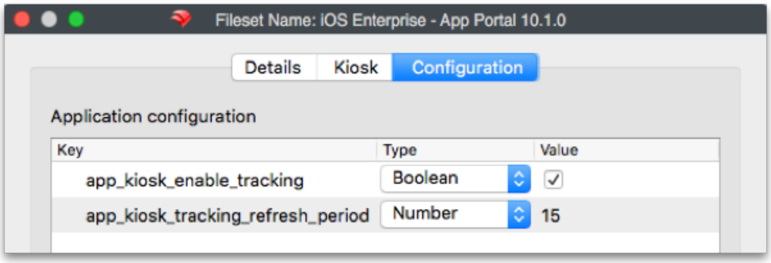
Things to consider:

- Different States of Tracking
  - Normal - Tracking is enabled and will update the location at different intervals
  - Missing - Tacking is enabled and will be update around every two minutes. The client also sends location immediately and does not wait for other scans to finish. For supervised iOS devices this option puts the device in Lost mode, has a message/footnote that can set in the FileWave Preferences under the Organization Info tab and locks the iOS device. The device will become usable again once the missing mode is switched off.
  - Not Tracked - No location is gathered at anytime.
- The FileWave IPA App Portal needs to be sent out and opened at least once before you will be prompted and allowed to gather location from the iOS device. Once it is sent out, the old FileWave App Portal that gets installed automatically with enrollment will be removed and the new one will be installed.
- For any updated location from your iOS devices the FileWave App Portal need to be open, whether that be in the background or the current active app.

There are two different types of location tracking in FileWave, Passive Tracking and Lost Mode. macOs, Windows, Chromebooks, and Android devices use the Passive tracking to gather the location of the device without locking it down. Supervised iOS devices set to Missing mode will put the device in Lost mode, which locks down the device making it unusable by the end user.

iOS custom configuration of tracking settings for App Portal

The iOS App Portal contains a *Preference Manifest* that holds a pair of custom keys and values for configuring the tracking settings. These values are **app_kiosk_enable_tracking** and **app_kiosk_tracking_refresh_period**. The first key enables location tracking when the App Portal is installed on the device (when it replaces the web clip). The second key sets the interval, in minutes, for the device to report its location to the FileWave server.
You manually enter these keys and settings into the **Configuration** tab of the App Portal's Fileset Properties:



Fileset Name: iOS Enterprise - App Portal 10.1.0

Application configuration

Key	Type	Value
app_kiosk_enable_tracking	Boolean	✓
app_kiosk_tracking_refresh_period	Number	15

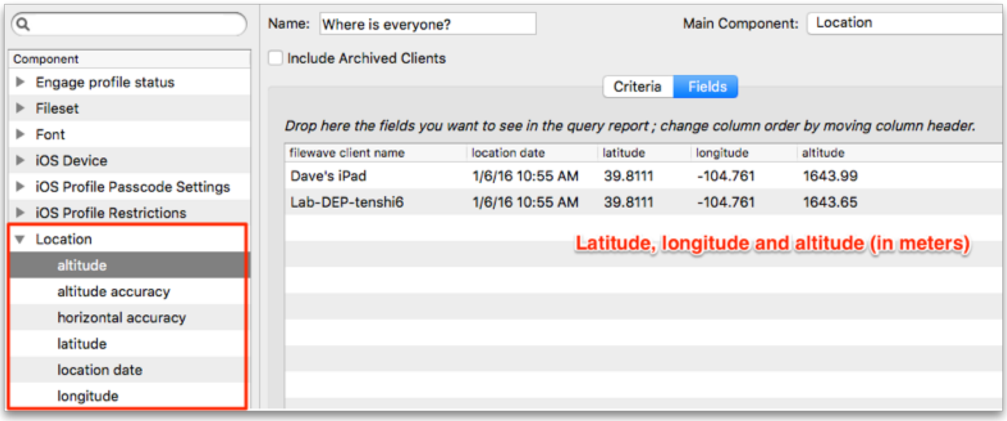
The settings do not override the dialog being presented for a user to approve tracking being enabled - that is a built-in requirement within iOS.

Location and Client Info

The device *Client Info* window also displays the location of a single device. Remember, a device must have Wi-Fi or cellular service enabled in order for it to report location.

Tracking and Inventory

FileWave Inventory now includes a new **Location** component that provides the last reported location data.



Name: Where is everyone?

Main Component: Location

☐ Include Archived Clients

Drop here the fields you want to see in the query report ; change column order by moving column header.

filewave client name	location date	latitude	longitude	altitude
Dave's iPad	1/6/16 10:55 AM	39.8111	-104.761	1643.99
Lab-DEP-tenshi6	1/6/16 10:55 AM	39.8111	-104.761	1643.65

4.13. MDM Lost Mode

Starting with iOS 9.3, supervised devices were able to be set to "MDM Lost Mode." Missing devices can be locked, displaying a message, phone number, and footnote. FileWave 11.1+ integrated this new feature with the "Missing" state. Changing device state to "Missing" will automatically send the new commands. You can configure text that will be displayed on the device in the Organizational Info portion of FileWave Admin Preferences. These strings are optional; however, we recommend that you specify a phone number or message. FileWave will display "Lost device" on an iOS device that is set to missing if nothing is provided in the settings. Now will the release of iOS 10.3 and FileWave 12.0+ you have the option to "Play Lost Mode Sound" on your devices. After you have set your device to missing, simply right click the it and select "Play Lost Mode Sound (iOS 10.3+)" the only way to turn that off will then to take the device out of "Missing".

4.14. Inventory-only Clients

Management Mode
A new flag has been added to computer Clients. It has two values: Managed (normal mode); and, Inventory only. To change Management Mode, right click on a client and select "Management Mode."
Inventory only
This setting allows you to have your client reporting data to FileWave, but will not be affected by any Filesets except for critical Filesets (for now, the only critical Filesets available are FileWave upgrade Filesets). Fileset status will report "Not installed, client is inventory only."

5. Working with Filesets
Core to the functionality of FileWave is our patented Fileset technology. Anything distributed from a FileWave Server to a FileWave Client is done using a Fileset. Except for Apple packages (.pkg) and Microsoft installers (.msi), which are run as normal installations, all content distributed by FileWave is done at the file level. 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.

5.1. 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 / 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 computer 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

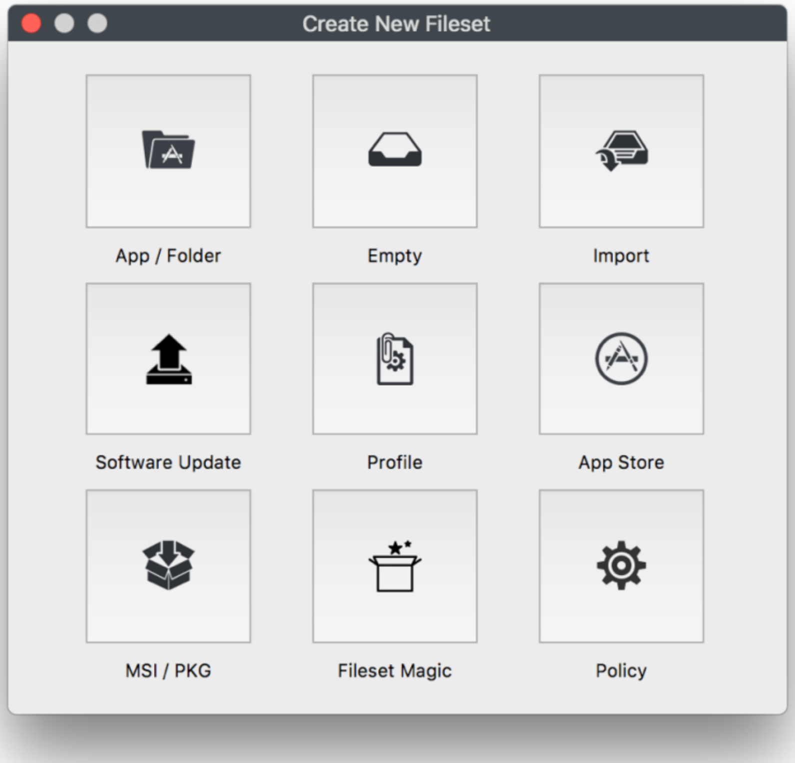
These settings are covered in detail in the next section on Associations.

- ***Specify a download time*** – You can choose to deploy this Fileset at another time other than immediately after the model is updated.
- ***Specify an activation time*** – You can choose to activate the payload at a later time rather than right after the download is complete.
- ***Specify a deactivation time*** – You can choose a time to make this payload inactive (but have it remain on the Client), 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; in other words, have it appear in the self-service Kiosk.
- ***Specify Fileset dependencies*** – You can specify that 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, 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 the file level, resulting in lower network loads, faster response times, and built-in self-healing of applications and content for your end users.

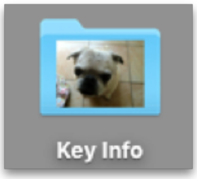
5.2. Desktop Filesets

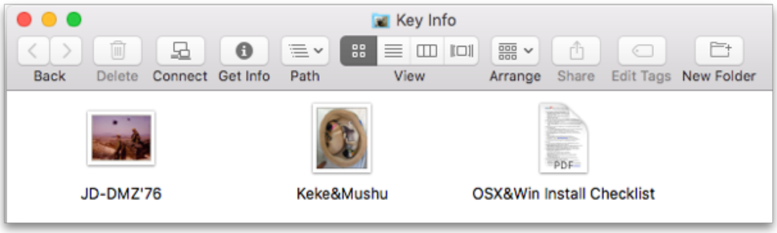
Desktop / laptops Filesets are designed for use on macOS and Windows computers. The Fileset types are shown below:



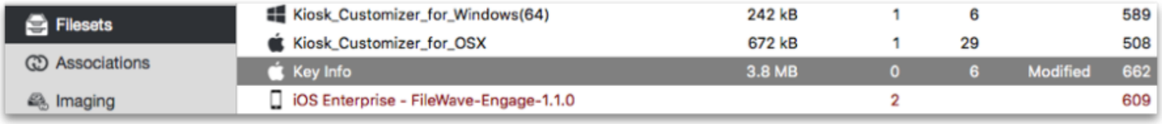
App / Folder Fileset

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 to every user who logs into a computer. First, you would select the files, in this case "Key Info":





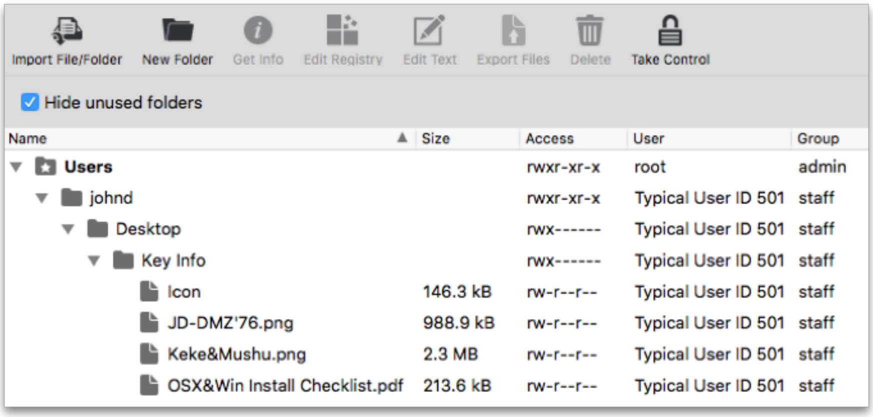
FileWave creates a Fileset from this folder and displays it in the **Fileset** pane in FileWave Admin.



Kiosk_Customizer_for_Windows(64)	242 kB	1	6		589
Kiosk_Customizer_for_OSX	672 kB	1	29		508
Key Info	3.8 MB	0	6	Modified	662
iOS Enterprise - FileWave-Engage-1.1.0		2			609

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 Fileset.

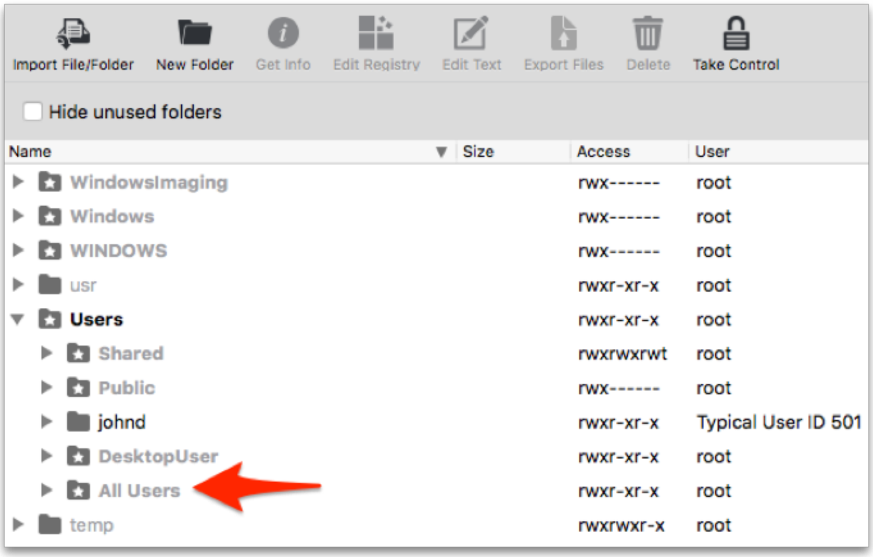
In order to prepare this Fileset for distribution, you double-click on it. This exposes the contents of the Fileset and allows you to specify the exact location for its distribution.



☑ Hide unused folders

Name	Size	Access	User	Group
▼ Users		rwxr-xr-x	root	admin
▼ johnd		rwxr-xr-x	Typical User ID 501	staff
▼ Desktop		rwx------	Typical User ID 501	staff
▼ Key Info		rwx------	Typical User ID 501	staff
Icon	146.3 kB	rw-r--r--	Typical User ID 501	staff
JD-DMZ'76.png	988.9 kB	rw-r--r--	Typical User ID 501	staff
Keke&Mushu.png	2.3 MB	rw-r--r--	Typical User ID 501	staff
OSX&Win Install Checklist.pdf	213.6 kB	rw-r--r--	Typical User ID 501	staff

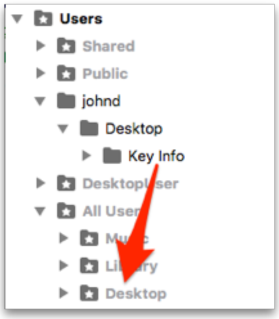
In order to make sure the files end up where you want them, you uncheck the box for **Hide unused** folders. FileWave allows you to send files not just to the exact same path you captured the files; but to a special location called **All Users**.



□ Hide unused folders

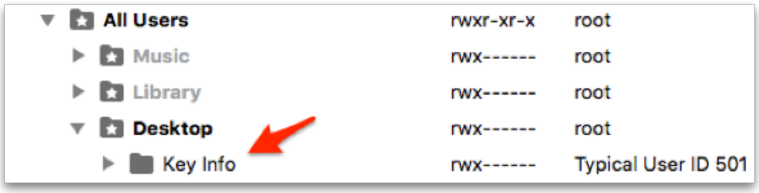
Name	Size	Access	User
▶ WindowsImaging		rwx------	root
▶ Windows		rwx------	root
▶ WINDOWS		rwx------	root
▶ usr		rwxr-xr-x	root
▼ Users		rwxr-xr-x	root
▶ Shared		rwxrwxrwt	root
▶ Public		rwx------	root
▶ johnd		rwxr-xr-x	Typical User ID 501
▶ DesktopUser		rwxr-xr-x	root
▶ All Users		rwxr-xr-x	root
▶ temp		rwxrwxr-x	root

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.
The **All Users** folder 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 into the home directory of every user account on a computer. In this case, we captured the folder item **Key Info** from the path **/Users/john d/Desktop** and we want it to be distributed into the Desktop folder of every user who access to a computer managed by FileWave. 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 on the next page:



```
▼ Users
  ▶ Shared
  ▶ Public
  ▼ johnd
    ▼ Desktop
      ▶ Key Info
  ▶ DesktopUser
  ▼ All Users
    ▶ Music
    ▶ Library
    ▶ Desktop
```

becomes…

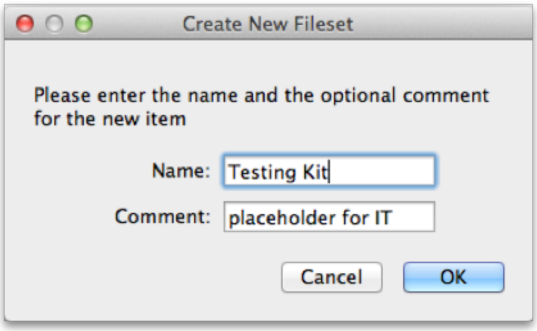


All Users	rwxr-xr-x	root
Music	rwx------	root
Library	rwx------	root
Desktop	rwx------	root
Key Info	rwx------	Typical User ID 501

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 'kickstart' the Kiosk on computers (the Kiosk shows up on a managed computer when at least one Fileset designated as a Kiosk item has been associated with that computer Client).



Create New Fileset

Please enter the name and the optional comment for the new item

Name: Testing Kit

Comment: placeholder for IT

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 Cient. 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/bin/**. 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. **Note: You do NOT put the "sudo" command into a script that is used in a Fileset; scripts run as root when executed by FileWave.**

Superprefs and Empty Filesets

One excellent use of the Empty Fileset is for Superprefs files. You can create a Superprefs file (see Section **5.8**) and just drop the file it creates (fwcld.newprefs.plist) into the Properties window. The settings will be activated upon arrival at the Client.

System Integrity Protection (FW 10+)

Apple introduced a security policy with OS X v10.11 (El Capitan) that restricts any non-Apple code from running in protected areas of the system. Make sure none of your scripts try to write to, or edit code, in these areas:
/System, /bin, /sbin, or **/usr**.
For more information on SIP, see this WikiPedia article: https://en.wikipedia.org/wiki/System_Integrity_Protection

Import Fileset

The *Import* Fileset is actually a dialog that allows you to import a previously created Fileset.

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 macOS (.pkg and .mpkg). When the Fileset is deployed to the Client, upon activation it will run as an installer with local administrator privileges.

Note: Under FileWave 10+, 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 (MSI). Customizations to MSI files can be made through Microsoft Transform (MST) files. FileWave supports MSI and MST through its Patch Installer feature. 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 *File Wave\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.*" 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's Windows Client 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. Sometimes 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.

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.

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 macOS computers and/or iOS devices, you should also plan to add one or more macOS servers running the Caching server process. This process caches all requests for Mac Store and iTunes Store content locally as devices request these items. See https://www.apple.com/support/osxserver/cachingservice/ for more information.

Deploying software updates

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, macOS, 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.

Once you create a Fileset from any of the updates, you can then select the Clients to associate with that update.

Be careful of manually associating Software Update Filesets with just any Client. You should associate the Filesets with requesting clients only. As always, test any updates on a non-production device before mass deployment. Finally, check all updates for dependency issues. Make sure an update is not going to break any existing software.

You can filter the selections by choosing a specific Group in the Groups window (upper right).

Starting with FileWave 10, is the ability to see iOS updates. The iOS updates will show up here. **Note: These updates do not include items from the iTunes or App Store; it shows iOS operating system updates only.**

Profile Fileset

The Profile Fileset contains all of the settings used for both computer and mobile device management on macOS and iOS. The Profile Editor in the Desktop Fileset window is identical to the one in the Mobile Fileset window.

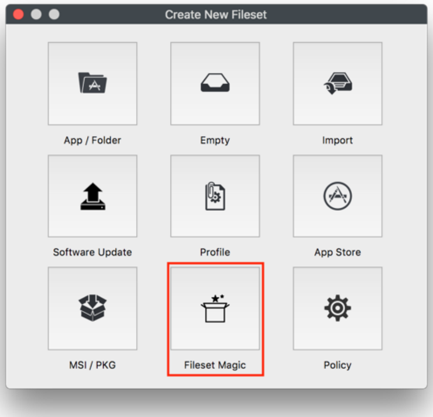
Details on creating and configuring Profile Filesets are in Chapter **7**.

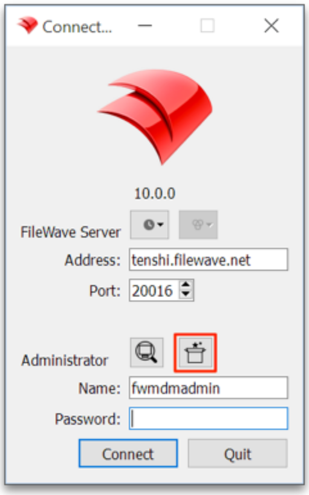
App Store Fileset

You can create Filesets for macOS 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 computer and require the user to enter their Apple ID 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 **6 (License Management)**.
With FileWave v10, you will have the ability to associate App Store content directly to a device, or to a user's Apple ID as part of a VPP distribution.

Fileset Magic

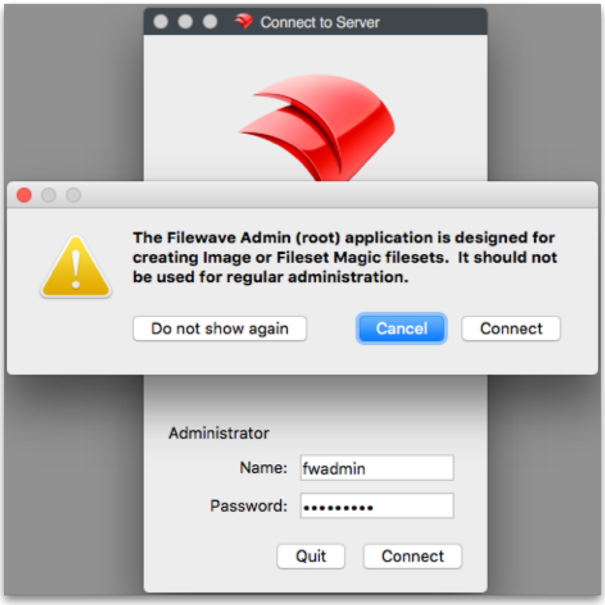
Sometimes, the content you want to distribute cannot be found in a completely deployable state. Fileset Magic allows you to build a Fileset from system snapshots taken before the installation/configuration of some software and after, resulting in a Fileset that contains the differences between the two snapshots.
Fileset Magic on macOS X is accessible from FileWave Admin, but you should use the special version of the Admin application - 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. This is in /Applications/FileWave/ and was installed as part of the administration software. 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.





FileWave Server
Address: tenshi.filewave.net
Port: 20016
Administrator
Name: fwmdmadmin
Password:

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

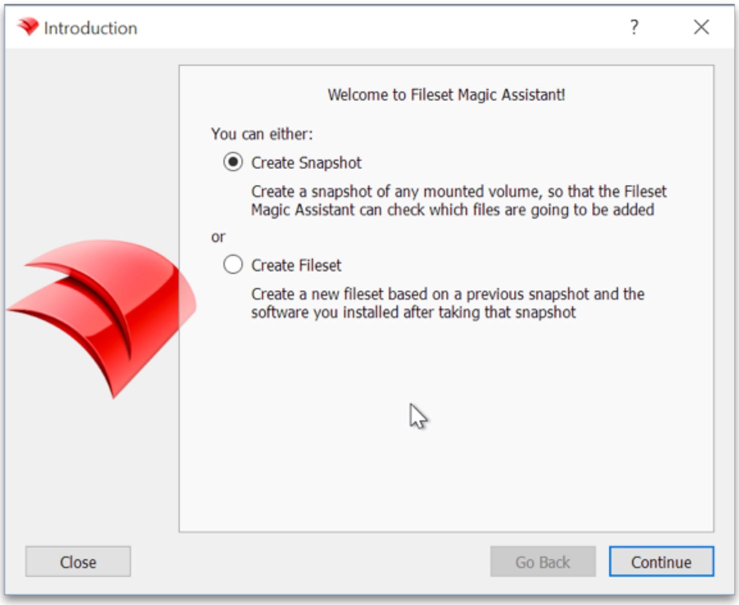


The Filewave Admin (root) application is designed for creating Image or Fileset Magic filesets. It should not be used for regular administration.

Administrator

Name: fwadmin

Password: •••••••••



Welcome to Fileset Magic Assistant!

You can either:

● Create Snapshot

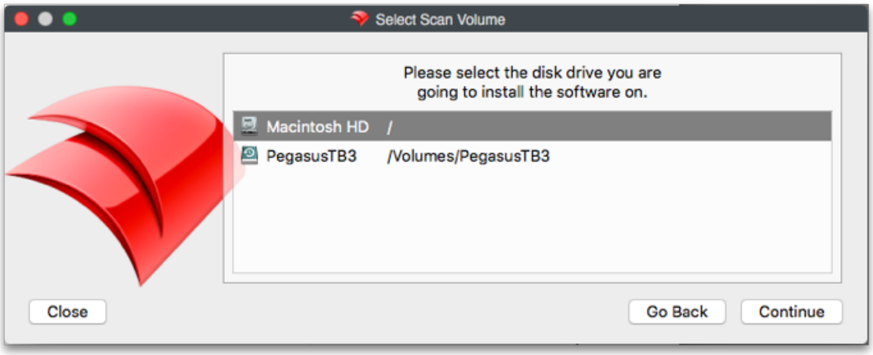
Create a snapshot of any mounted volume, so that the Fileset Magic Assistant can check which files are going to be added

or

○ Create Fileset

Create a new fileset based on a previous snapshot and the software you installed after taking that snapshot

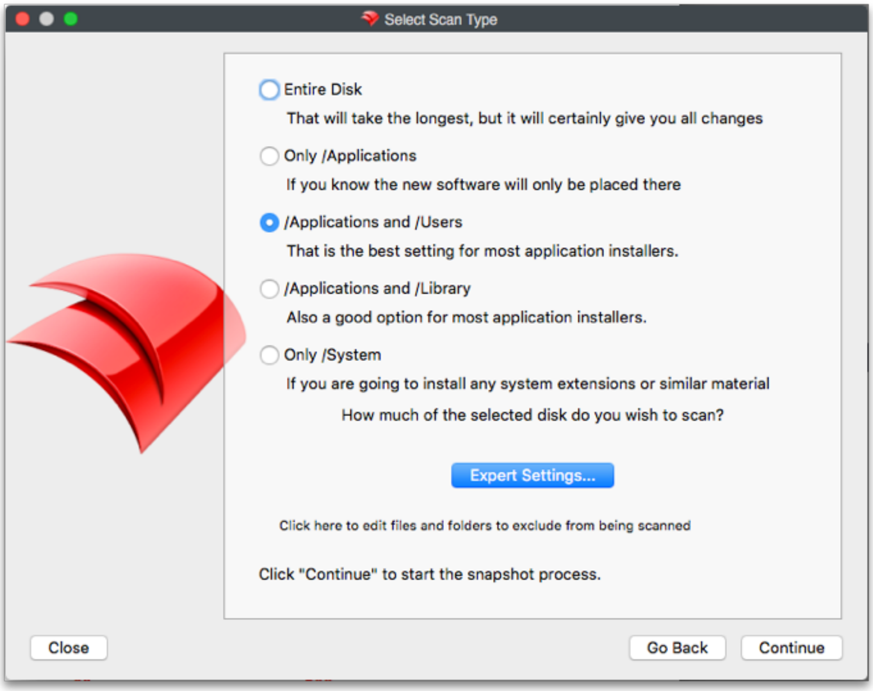
Once you have quit all unneeded applications, you create a snapshot of your system. It is a good practice to use a clean system for this process instead of your normal administrator machine. This will ensure that you are working with the files you want to add and avoiding dealing with all the additional files that get created on a production system from normal use. In other words, the snapshotting processes will run faster with a smaller number of files to scan.



Please select the disk drive you are going to install the software on.

Macintosh HD	/
PegasusTB3	/Volumes/PegasusTB3

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.



○ Entire Disk
That will take the longest, but it will certainly give you all changes

○ Only /Applications
If you know the new software will only be placed there

● /Applications and /Users
That is the best setting for most application installers.

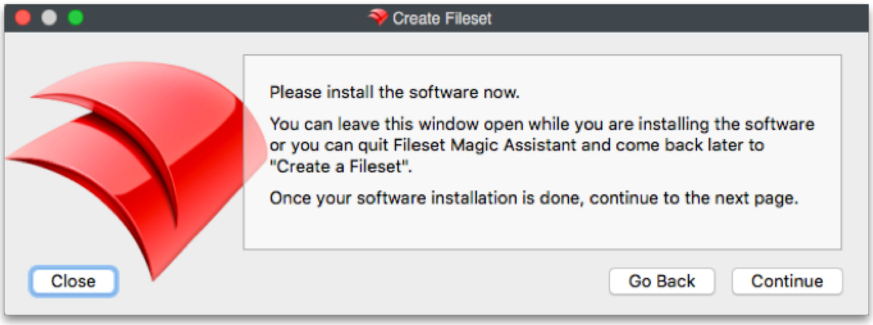
○ /Applications and /Library
Also a good option for most application installers.

○ Only /System
If you are going to install any system extensions or similar material

How much of the selected disk do you wish to scan?

Click here to edit files and folders to exclude from being scanned

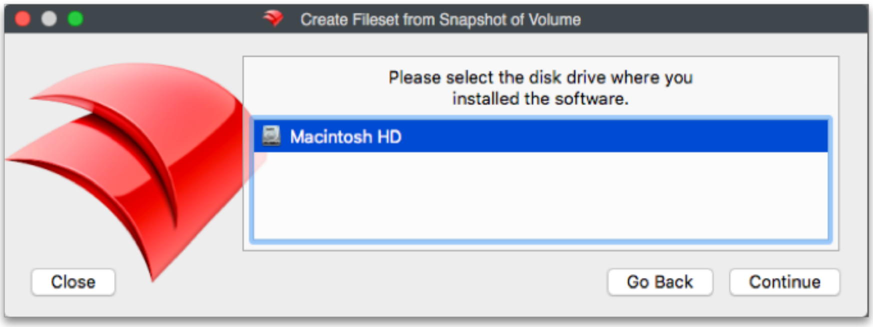
Click "Continue" to start the snapshot process.



Please install the software now.

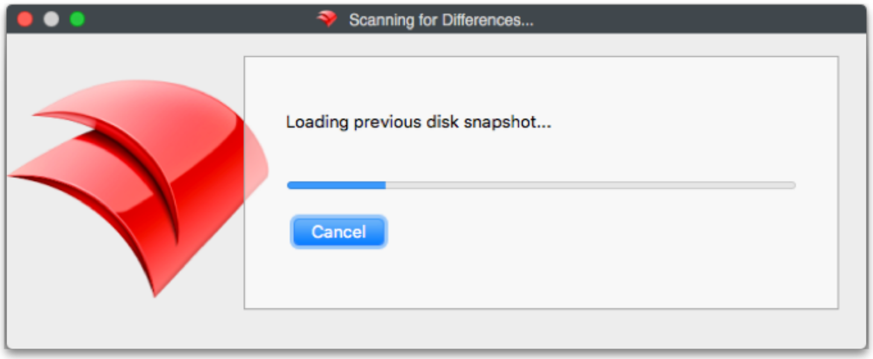
You can leave this window open while you are installing the software or you can quit Fileset Magic Assistant and come back later to "Create a Fileset".

Once your software installation is done, continue to the next page.



Please select the disk drive where you installed the software.

Macintosh HD



Loading previous disk snapshot...

Once the initial 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. Once you have picked the files you need, you will name the Fileset and save it.

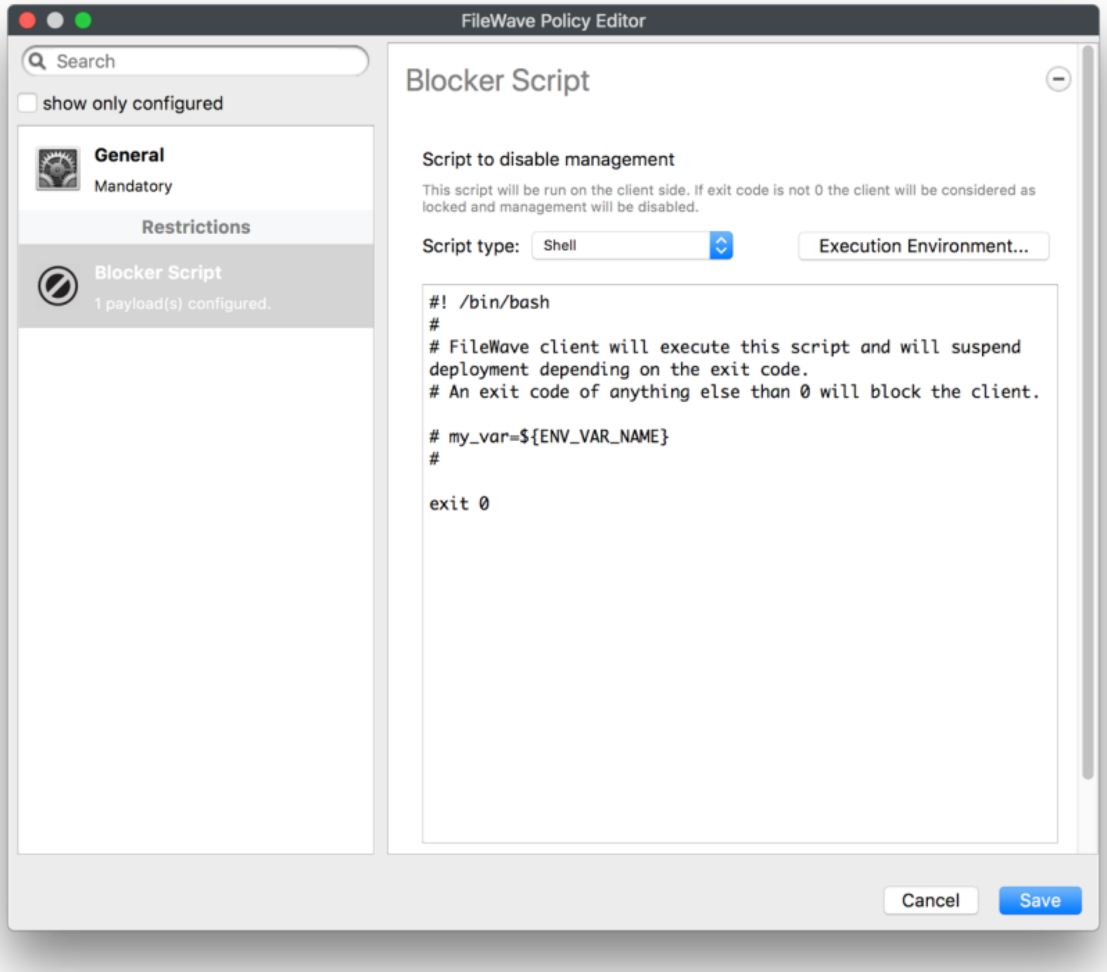
You can also choose to move any files that are needed by all users from the local account where they showed up into the **All Users** location in Fileset Contents. This would be general user-level application support files or specific settings for a local user. You can open the Fileset by double-clicking 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.

Policy

The Policy option contains different option to help configure many accepts of the FileWave Clients. The first policy introduced with 12.7.0 is *Block er Script.*

Blocker Script: This policy applies to desktop devices and allows you to suspend management via a script. The script will be ran every 5 minutes or at verify and if its exit code is different from 0 the client will suspend its management. If the script finishes with the exit code 0 then the device will continue/restore management. If management is suspended FileWave will reflect this in inventory under the new Component type "FileWave Policy" and also in the new tab "Policies" in the Client Info window for the clients.



Script to disable management

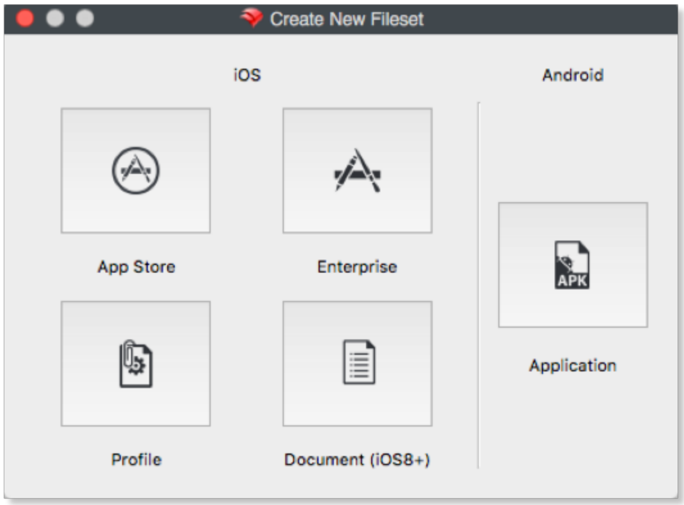
This script will be run on the client side. If exit code is not 0 the client will be considered as locked and management will be disabled.

Script type: Shell

```
#! /bin/bash
#
# FileWave client will execute this script and will suspend
deployment depending on the exit code.
# An exit code of anything else than 0 will block the client.

# my_var=${ENV_VAR_NAME}
#

exit 0
```

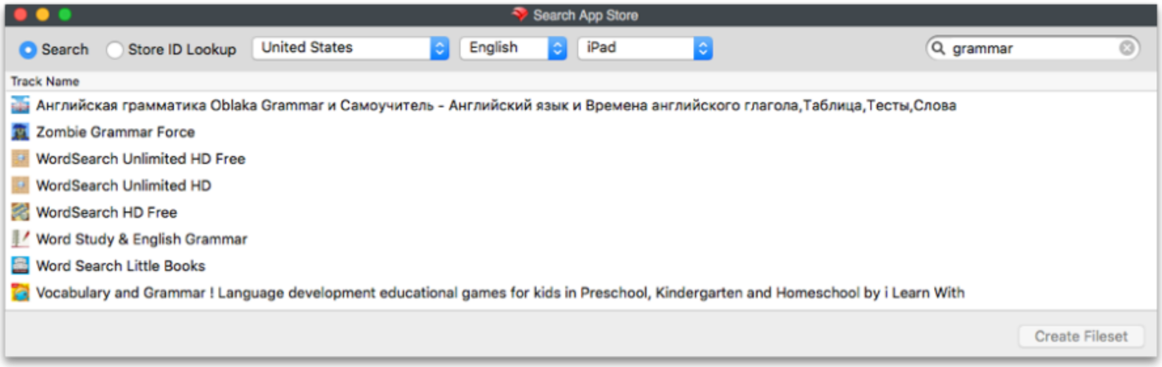
5.3. Mobile Filesets

For your mobile devices, the selection of possible Filesets is much smaller.



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. The user will then be required to enter his or her Apple ID 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 10+ supports the ability to associate VPP application Filesets either to an Apple ID, or directly to a device. More on the use of VPP for distributions in Chapter **6 (License Management)**.
You enter either a name or an iTunes ID code to search for the content to be deployed:



● Search ○ Store ID Lookup | United States | English | iPad | grammar

Track Name
Английская грамматика Oblaka Grammar и Самоучитель - Английский язык и Времена английского глагола,Таблица,Тесты,Слова
Zombie Grammar Force
WordSearch Unlimited HD Free
WordSearch Unlimited HD
WordSearch HD Free
Word Study & English Grammar
Word Search Little Books
Vocabulary and Grammar ! Language development educational games for kids in Preschool, Kindergarten and Homeschool by i Learn With

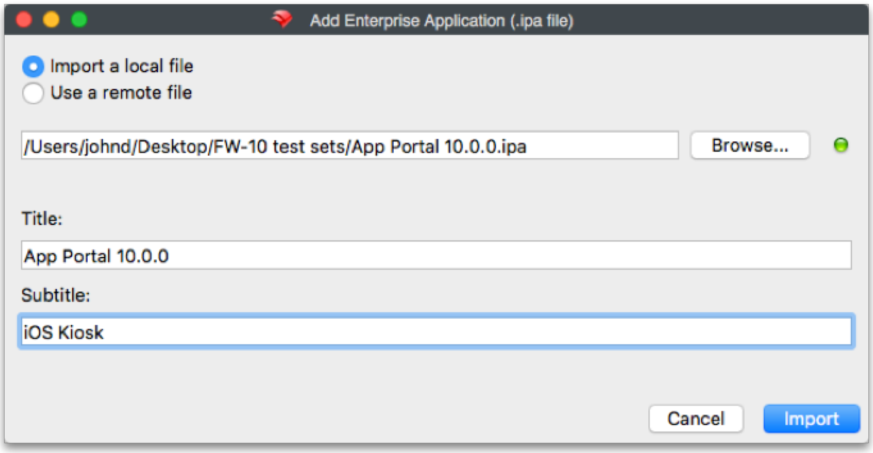
Once you have created the Fileset, you can double-click on it to view extra settings, such as setting Kiosk information. This Fileset does not download the item - application or eBook - but maintains a link to the iTunes Store for that item.

Enterprise Fileset

The Enterprise Fileset is designed for you to distribute an **internally-created** iOS application. Apple does not condone or support using this type of Fileset to distribute Apple App Store or iTunes Store content.
You can easily distribute software you have created with this Fileset by locating the **.ipa** file for 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.

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. This keeps all the traffic local and works well for small deployments. Remote distribution pulls the app from the FileWave Support servers. This is a best practice for large deployments over a wide geographic region. The local method looks like the first image on the next page:



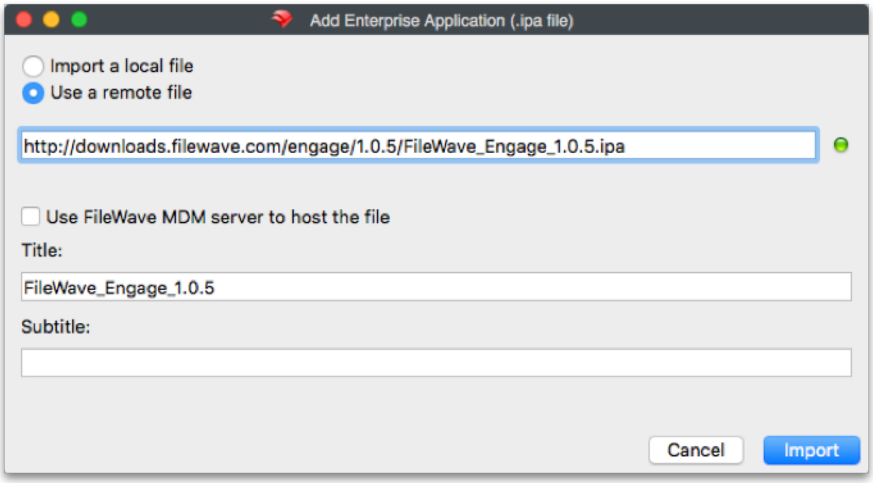
● Import a local file
○ Use a remote file

/Users/johnd/Desktop/FW-10 test sets/App Portal 10.0.0.ipa

Title: App Portal 10.0.0

Subtitle: iOS Kiosk

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



○ Import a local file
● Use a remote file

http://downloads.filewave.com/engage/1.0.5/FileWave_Engage_1.0.5.ipa

□ Use FileWave MDM server to host the file

Title:

FileWave_Engage_1.0.5

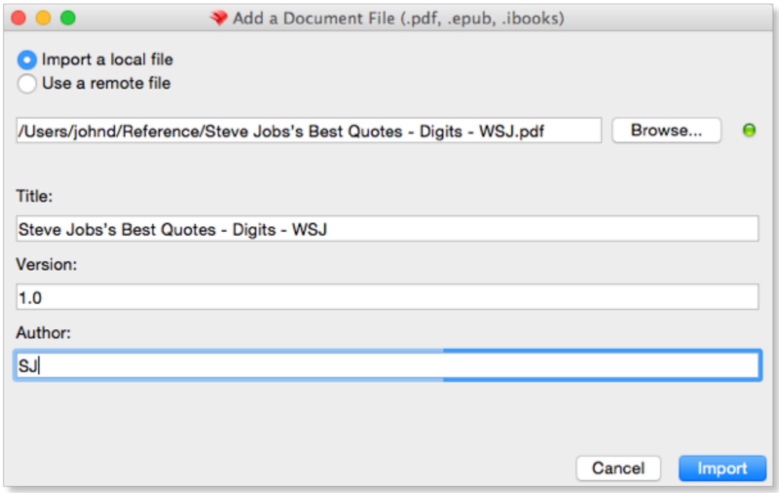
Subtitle:

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 starting with iOS 7. 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 **7** 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 non-Apple iBookstore **iBooks** formatted items (ones created with *iBooks Author*). They are delivered to the iBooks Library as a **managed document** which means it can be given, and taken away.



● Import a local file
○ Use a remote file

/Users/johnd/Reference/Steve Jobs's Best Quotes - Digits - WSJ.pdf

Title:

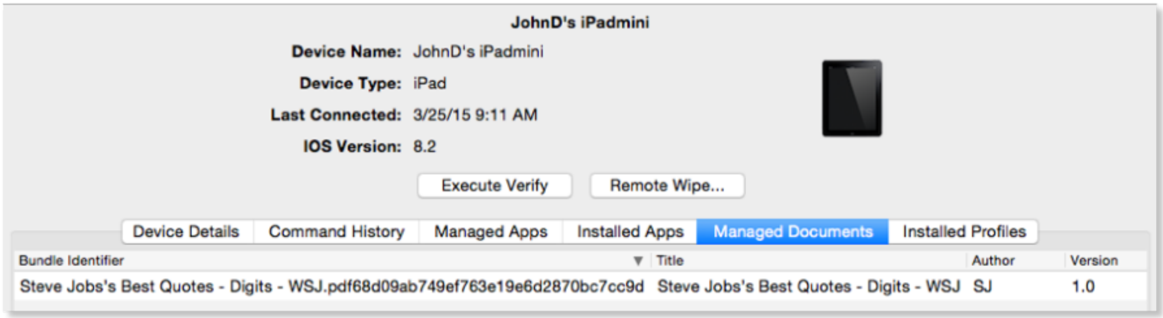
Steve Jobs's Best Quotes - Digits - WSJ

Version:

1.0

Author:

SJ



JohnD's iPadmini

Device Name: JohnD's iPadmini
Device Type: iPad
Last Connected: 3/25/15 9:11 AM
IOS Version: 8.2

Bundle Identifier	Title	Author	Version
Steve Jobs's Best Quotes - Digits - WSJ.pdf68d09ab749ef763e19e6d2870bc7cc9d	Steve Jobs's Best Quotes - Digits - WSJ	SJ	1.0

Android Fileset

You can add Android devices as Clients and deploy Filesets to them. The process for creating an Android Fileset resembles the Enterprise method. You must locate the application 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.

Imaging Filesets

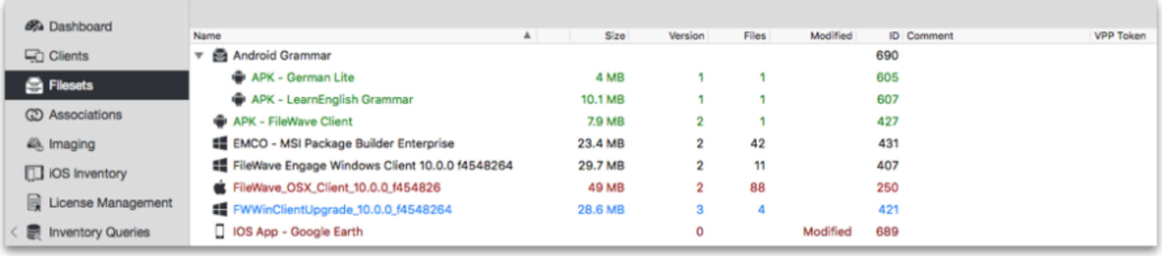
FileWave Imaging involves creating macOS X and Windows images that are used to image new computers or to re-image current computers. This workflow allows Boosters to act as imaging caches during the imaging process. More information on Imaging is in Chapter **9**.

5.4. Fileset Groups

You can arrange Filesets into Groups for easier deployment workflows. 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.

5.5. Advanced Editing - Contents, Properties, Settings, and Dependencies

While you can create a Fileset and associate it with a Client without doing any additional steps. However, 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 menu bar:



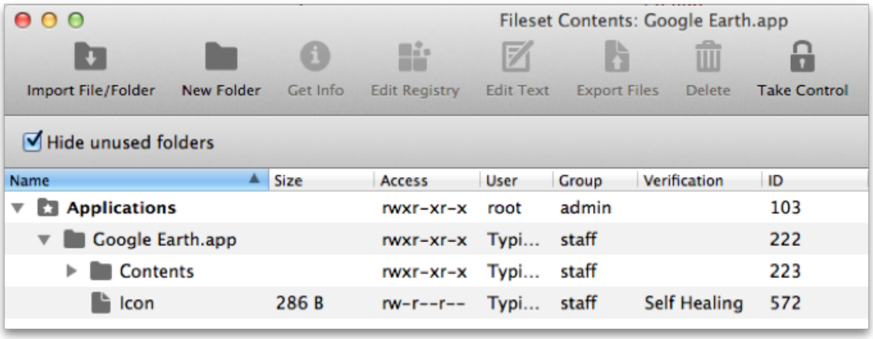
Name	Size	Version	Files	Modified	ID	Comment	VPP Token
Android Grammar					690		
APK - German Lite	4 MB	1	1		605		
APK - LearnEnglish Grammar	10.1 MB	1	1		607		
APK - FileWave Client	7.9 MB	2	1		427		
EMCO - MSI Package Builder Enterprise	23.4 MB	2	42		431		
FileWave Engage Windows Client 10.0.0 f4548264	29.7 MB	2	11		407		
FileWave_OSX_Client_10.0.0_f454826	49 MB	2	88		250		
FWWinClientUpgrade_10.0.0_f4548264	28.6 MB	3	4		421		
IOS App - Google Earth		0		Modified	689		

- ***Name*** – This is the title of the Fileset you created.
- ***Size*** – This is 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*** – This is the total number of files contained in the Fileset.
- ***ID*** – This is a unique identifier used by the FileWave server to keep track of your Filesets
- ***Comment*** – This is any optional text you enter to add information about the Fileset
- ***VPP Token*** – This designates which Apple Volume Purchase Program token is assigned to a particular 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 Fileset contents

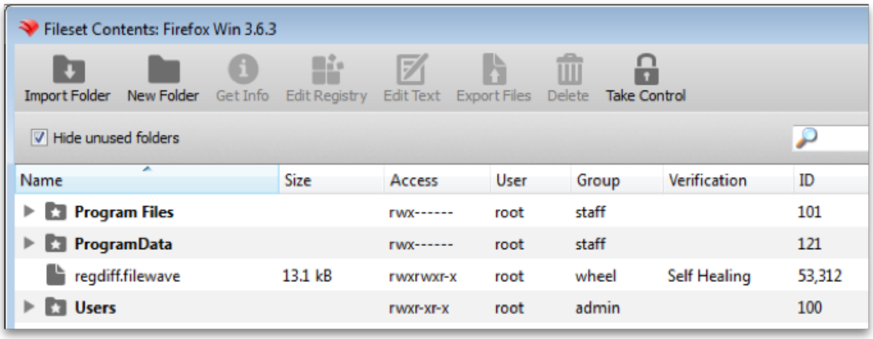
The Desktop Fileset contents are the specific items to be installed along with their designated paths. Examples are:



Fileset Contents: Google Earth.app

☑ Hide unused folders

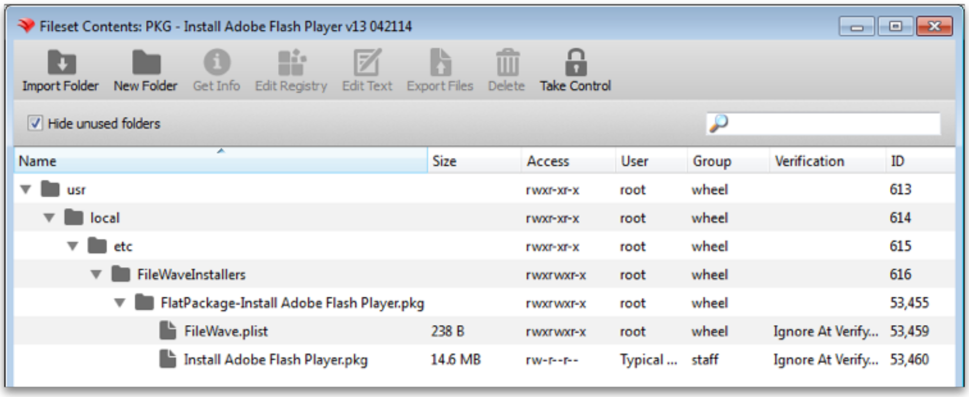
Name	Size	Access	User	Group	Verification	ID
Applications		rwxr-xr-x	root	admin		103
Google Earth.app		rwxr-xr-x	Typi...	staff		222
Contents		rwxr-xr-x	Typi...	staff		223
Icon	286 B	rw-r--r--	Typi...	staff	Self Healing	572



Fileset Contents: Firefox Win 3.6.3

☑ Hide unused folders

Name	Size	Access	User	Group	Verification	ID
Program Files		rwx------	root	staff		101
ProgramData		rwx------	root	staff		121
regdiff.filewave	13.1 kB	rwxrwxr-x	root	wheel	Self Healing	53,312
Users		rwxr-xr-x	root	admin		100



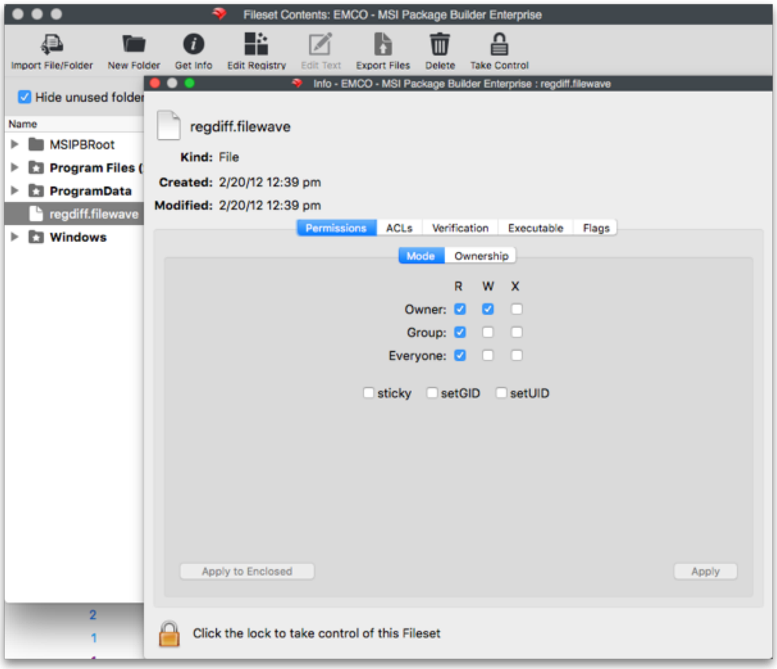
Fileset Contents: PKG - Install Adobe Flash Player v13 042114

☑ Hide unused folders

Name	Size	Access	User	Group	Verification	ID
usr		rwxr-xr-x	root	wheel		613
local		rwxr-xr-x	root	wheel		614
etc		rwxr-xr-x	root	wheel		615
FileWaveInstallers		rwxrwxr-x	root	wheel		616
FlatPackage-Install Adobe Flash Player.pkg		rwxrwxr-x	root	wheel		53,455
FileWave.plist	238 B	rwxrwxr-x	root	wheel	Ignore At Verify...	53,459
Install Adobe Flash Player.pkg	14.6 MB	rw-r--r--	Typical ...	staff	Ignore At Verify...	53,460

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.

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



☑ Hide unused folder

regdiff.filewave

Kind: File

Created: 2/20/12 12:39 pm

Modified: 2/20/12 12:39 pm

	R	W	X
Owner:	☑	☑	□
Group:	☑	□	□
Everyone:	☑	□	□

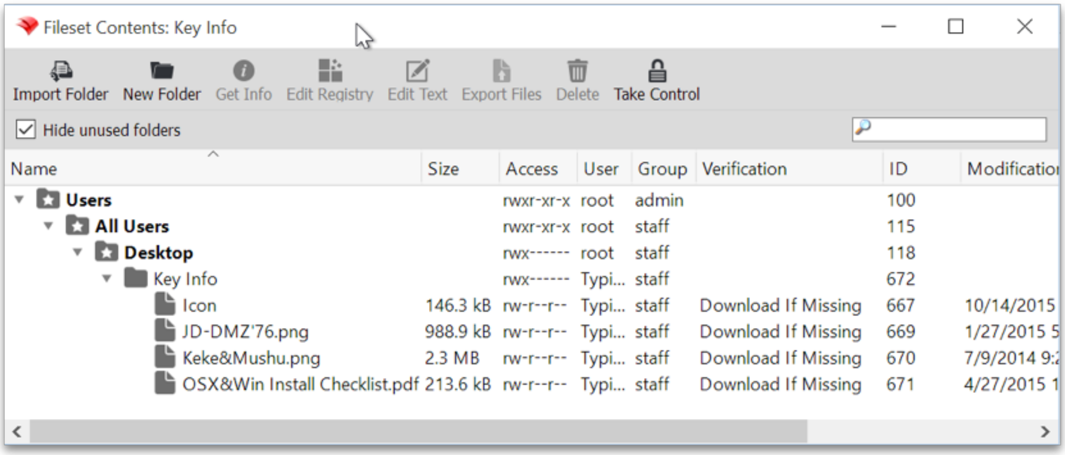
□ sticky □ setGID □ setUID

Click the lock to take control of this Fileset

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. Each of these settings causes the related file(s) to behave differently once deployed.



☑ Hide unused folders

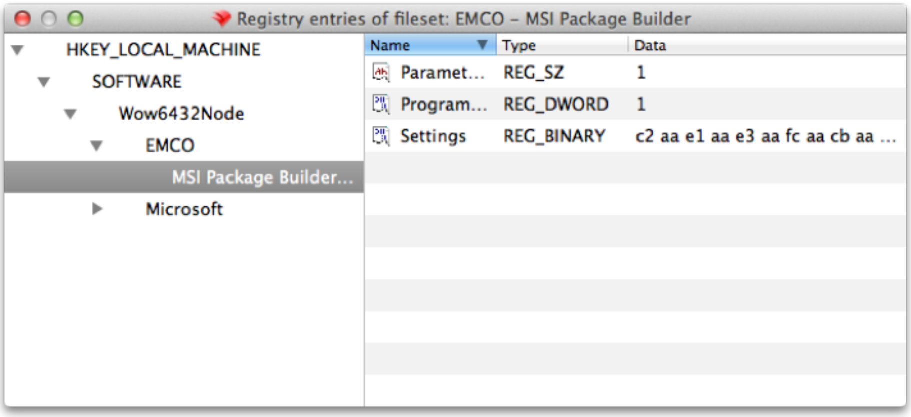
Name	Size	Access	User	Group	Verification	ID	Modificatio
Users		rwxr-xr-x	root	admin		100	
All Users		rwxr-xr-x	root	staff		115	
Desktop		rwx------	root	staff		118	
Key Info		rwx------	Typi...	staff		672	
Icon	146.3 kB	rw-r--r--	Typi...	staff	Download If Missing	667	10/14/2015
JD-DMZ'76.png	988.9 kB	rw-r--r--	Typi...	staff	Download If Missing	669	1/27/2015 5
Keke&Mushu.png	2.3 MB	rw-r--r--	Typi...	staff	Download If Missing	670	7/9/2014 9:
OSX&Win Install Checklist.pdf	213.6 kB	rw-r--r--	Typi...	staff	Download If Missing	671	4/27/2015 1

- ***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. 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.
- ***Don't overwrite existing files upon deployment*** – This setting can be chosen to go with either the *Download if Missing* or *Ignore At Verify (Left Behind)*. You can tell FileWave to not write over top of any files that already exist when the Fileset is activated.
- ***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. If you need to distribute a Registry file, you can add one to an empty Fileset.



Registry entries of fileset: EMCO – MSI Package Builder

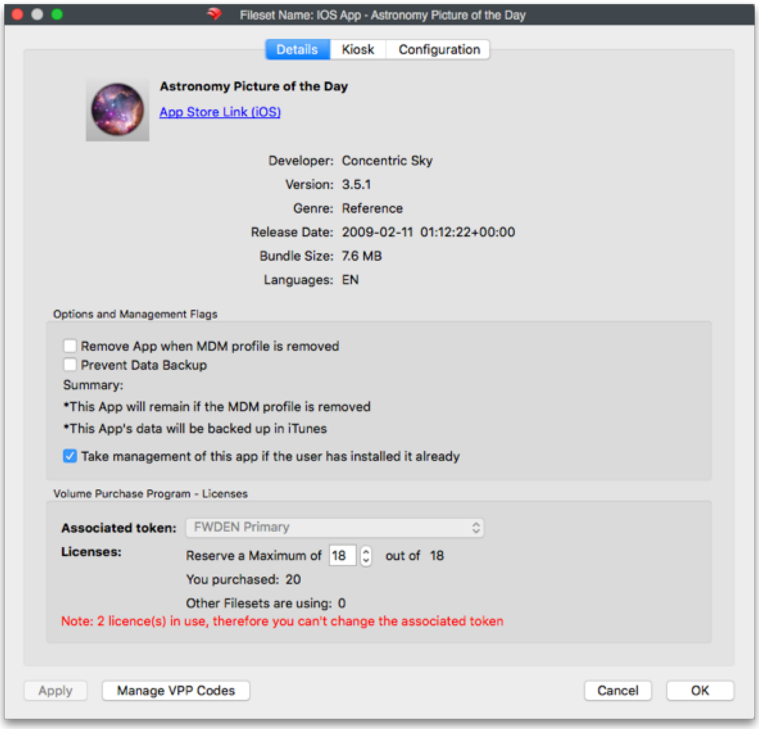
- HKEY_LOCAL_MACHINE
  - SOFTWARE
    - Wow6432Node
      - EMCO
        - MSI Package Builder...
      - Microsoft

Name	Type	Data
Paramet...	REG_SZ	1
Program...	REG_DWORD	1
Settings	REG_BINARY	c2 aa e1 aa e3 aa fc aa cb aa ...

- ***Edit Text*** – You can edit many of the text based files in a Fileset directly. In FileWave Admin's Preferences, you will see all of the various file type extensions that are supported.
- ***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 three panes: Details; Kiosk; and, Configuration.
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. A flag introduced in FW 10+ allows you to **take management** of an existing version of this application. If a user has installed an application that needs to be managed; because their device is managed, you can "take over" control of that application. This would allow you to control distribution and settings.
VPP shows the connection between a Fileset and a VPP account. A warning is shown (see screenshot on next page) if a VPP token is associated with the application noting that the Fileset cannot be attached to a different VPP account token.



Fileset Name: IOS App - Astronomy Picture of the Day

Astronomy Picture of the Day

App Store Link (iOS)

Developer: Concentric Sky
Version: 3.5.1
Genre: Reference
Release Date: 2009-02-11 01:12:22+00:00
Bundle Size: 7.6 MB
Languages: EN

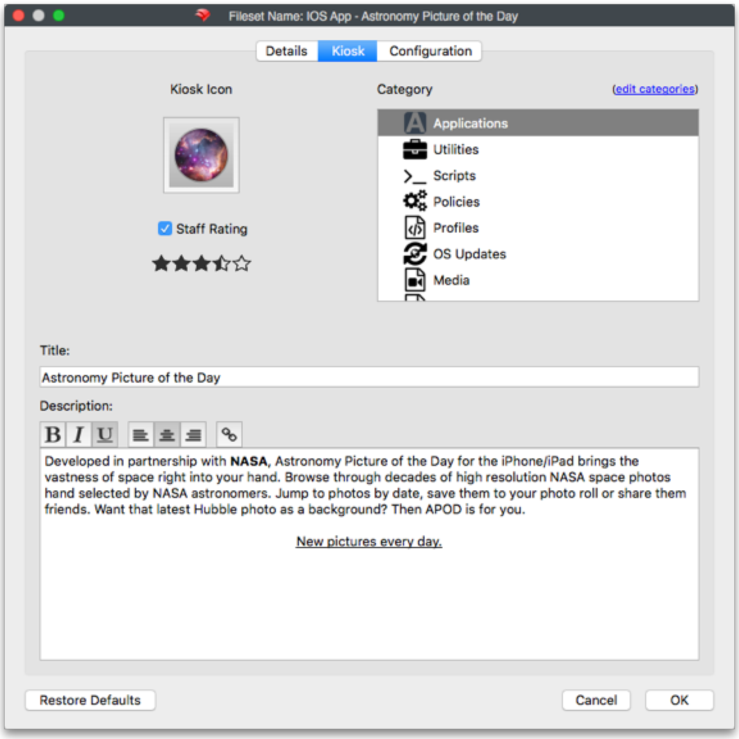
Options and Management Flags

□ Remove App when MDM profile is removed
□ Prevent Data Backup
Summary:
•This App will remain if the MDM profile is removed
•This App's data will be backed up in iTunes
☑ Take management of this app if the user has installed it already

Volume Purchase Program - Licenses

Associated token: FWDEN Primary
Licenses: Reserve a Maximum of 18 out of 18
You purchased: 20
Other Filesets are using: 0
Note: 2 licence(s) in use, therefore you can't change the associated 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. In FW 10+, you can customize the information with tags, such as **Bold**, and underlined, for readability; plus you can add URLs within the information pane.



☑ Staff Rating ★★★⯪☆

Title:

Astronomy Picture of the Day

Description:

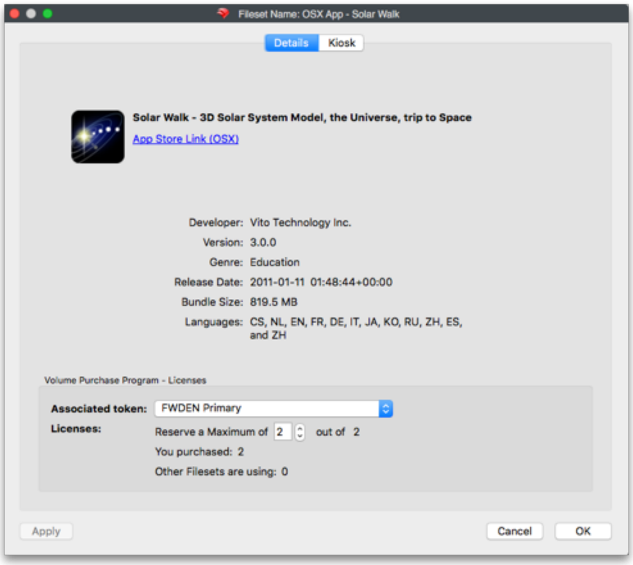
Developed in partnership with **NASA**, Astronomy Picture of the Day for the iPhone/iPad brings the vastness of space right into your hand. Browse through decades of high resolution NASA space photos hand selected by NASA astronomers. Jump to photos by date, save them to your photo roll or share them friends. Want that latest Hubble photo as a background? Then APOD is for you.

New pictures every day.

The **Configuration** pane allows you to add management settings for a specific application, if that application supports the use of a *preference manifest*. The settings must come from the application developer and will be in the form of a *property list* file (.plist). There is much more information on what these files are and how they are constructed in Apple's Developer site - https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

macOS App / iOS eBook Fileset contents

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

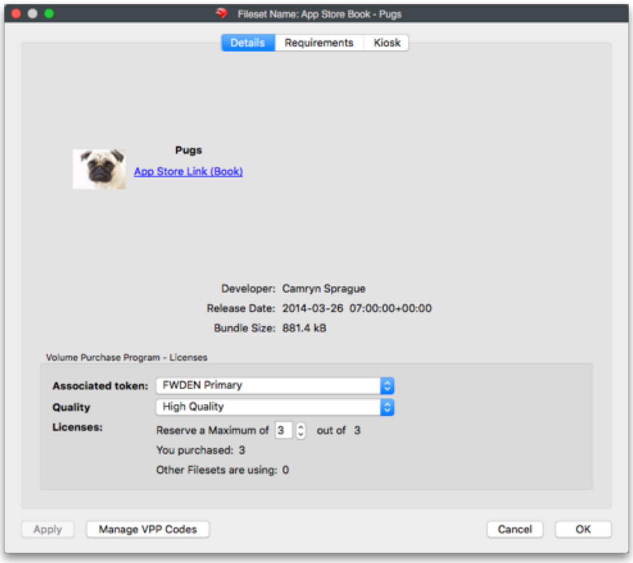


Solar Walk - 3D Solar System Model, the Universe, trip to Space

Developer: Vito Technology Inc.
Version: 3.0.0
Genre: Education
Release Date: 2011-01-11 01:48:44+00:00
Bundle Size: 819.5 MB
Languages: CS, NL, EN, FR, DE, IT, JA, KO, RU, ZH, ES, and ZH

Volume Purchase Program - Licenses

Associated token: FWDEN Primary
Licenses: Reserve a Maximum of 2 out of 2
You purchased: 2
Other Filesets are using: 0



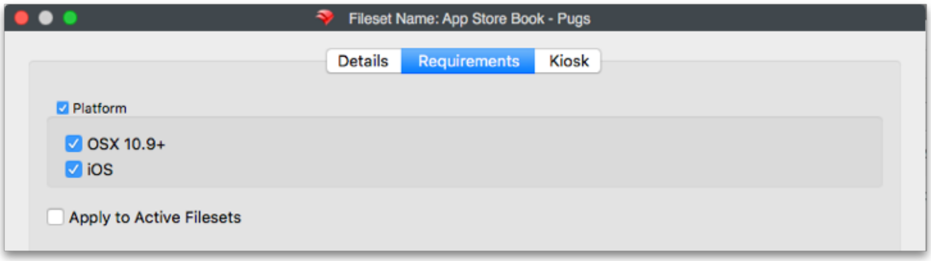
Pugs
App Store Link (Book)

Developer: Camryn Sprague
Release Date: 2014-03-26 07:00:00+00:00
Bundle Size: 881.4 kB

Volume Purchase Program - Licenses

Associated token: FWDEN Primary
Quality High Quality
Licenses: Reserve a Maximum of 3 out of 3
You purchased: 3
Other Filesets are using: 0

The **Requirements** pane specifies 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 change Filesets that have been deployed.



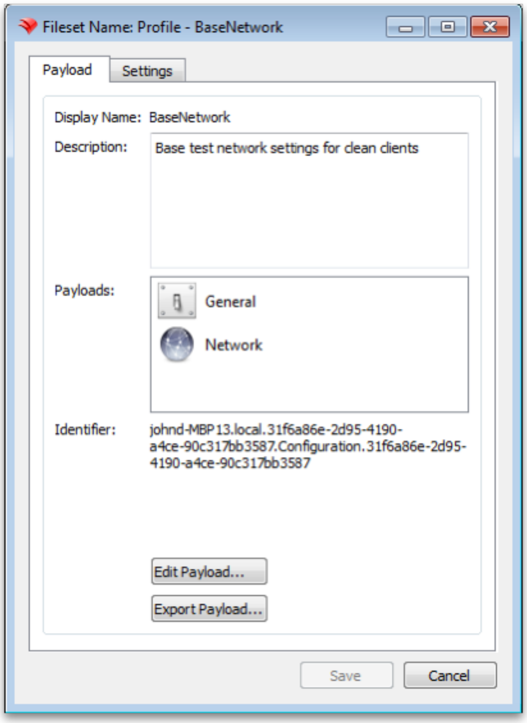
☑ Platform
☑ OSX 10.9+
☑ iOS
□ Apply to Active Filesets

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's title and description will revert to what is posted in the iTunes/App Store online.

Profile Fileset contents

Profile Filesets 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 include **Platform** choices which must match the categories in Profile Editor. The **Installation** c hoice determines whether the profile will be activated at system level (as a Daemon), which is prior to Login Window, or at user level (as a Launch Agent), which is at Finder launch. You can force the profile to reinstall if the user removes it. Devices that are running OS X 10.6 - 10.9 can have the **legacy install** flag set. This will force the settings that these devices get to be **MCX .plist** formatted, if the computers are running a FileWave Client earlier than version 9.

Starting wtih FW 10, there is a setting that makes the profile available to **Engage**, so that users logged in as teachers will have that profile available to apply to their class as needed. More on this capability in Chapter **10 (Engage)**.

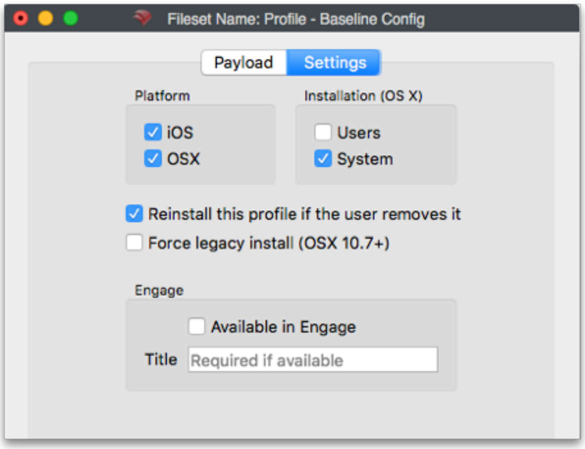


Display Name: BaseNetwork

Description: Base test network settings for clean clients

Payloads: General, Network

Identifier: johnd-MBP13.local.31f6a86e-2d95-4190-a4ce-90c317bb3587.Configuration.31f6a86e-2d95-4190-a4ce-90c317bb3587



Platform

☑ iOS
☑ OSX

Installation (OS X)

□ Users
☑ System

☑ Reinstall this profile if the user removes it

□ Force legacy install (OSX 10.7+)

Engage

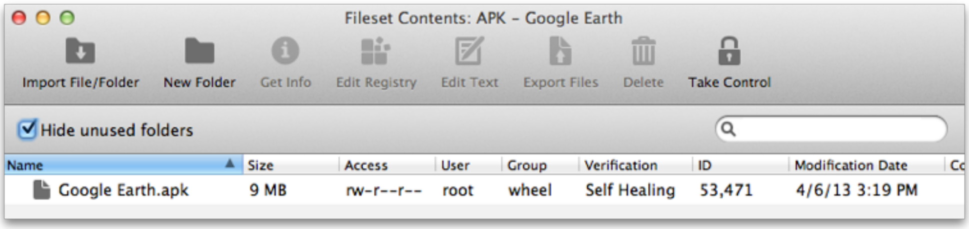
□ Available in Engage

Title: Required if available

Details on profiles and configuring them are in Chapter **7 (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.



☑ Hide unused folders

Name	Size	Access	User	Group	Verification	ID	Modification Date	Co
Google Earth.apk	9 MB	rw-r--r--	root	wheel	Self Healing	53,471	4/6/13 3:19 PM	

The Fileset will send the contents to the Android device's Kiosk. From there, the end user can select to install the item, which will place the contents in the Downloads folder for manual installation.

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:

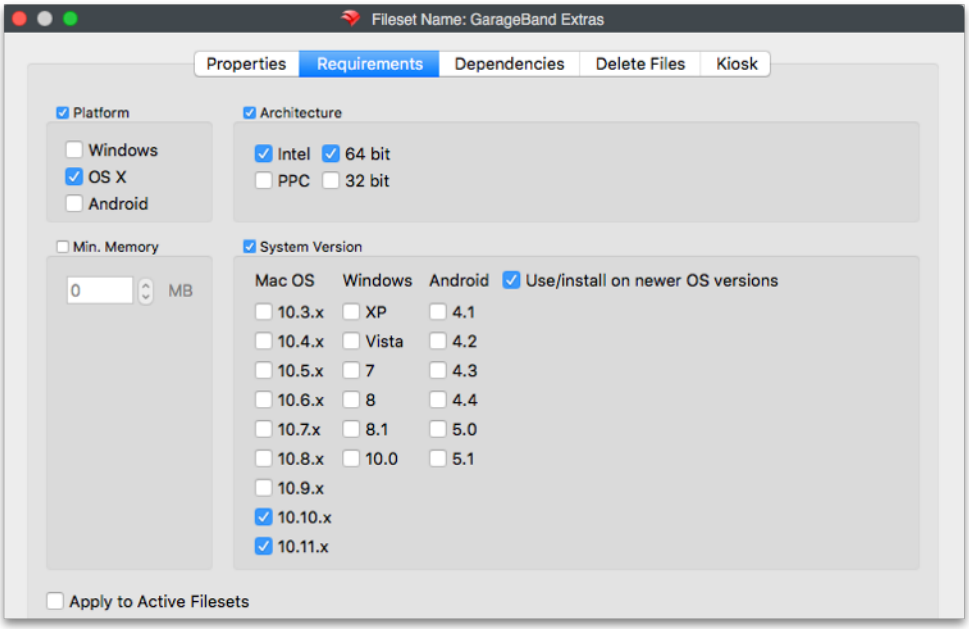
- ***Require Reboot (with Message)*** – In most cases, you won't need to require the computer to reboot; but software update Filesets usually do. You can provide a message to be displayed for the end user as a warning that software is being installed and a reboot will be required. Once you have configured a Fileset for **reboot**, you can also set a "Reboot deadline" to force the completion of the Fileset installation. This process is covered in the **Associations** section.
- ***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. 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 in 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*** – During verification, if a file is no longer present, it will be replaced from the master Fileset.
- ***Ignore At Verify (Left Behind)*** – 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.
- ***Don't Overwrite existing files upon deployment*** – This setting is a subset of the two settings above. 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*** – This setting is also a subset of *Download if Missing* and *Ignore At Verify (Left Behind)*, 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 the FileWave Client application (fwcld) to download and activate a Fileset. You can choose specific operating system platforms, architectures, memory, and system versions.
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.



☑ Platform

□ Windows
☑ OS X
□ Android

☑ Architecture

☑ Intel ☑ 64 bit
□ PPC □ 32 bit

□ Min. Memory

0 MB

☑ System Version

☑ Use/install on newer OS versions

Mac OS	Windows	Android
□ 10.3.x	□ XP	□ 4.1
□ 10.4.x	□ Vista	□ 4.2
□ 10.5.x	□ 7	□ 4.3
□ 10.6.x	□ 8	□ 4.4
□ 10.7.x	□ 8.1	□ 5.0
□ 10.8.x	□ 10.0	□ 5.1
□ 10.9.x		
☑ 10.10.x		
☑ 10.11.x		

□ Apply to Active Filesets

Properties - Delete Files

Use this tab to provide the paths to files that need to be deleted when this Fileset activates.

Properties - Kiosk

You 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 deployment needs. With FileWave 10+, you can use Rich Text formatting to improve the look and feel of the Description.

Properties - Details

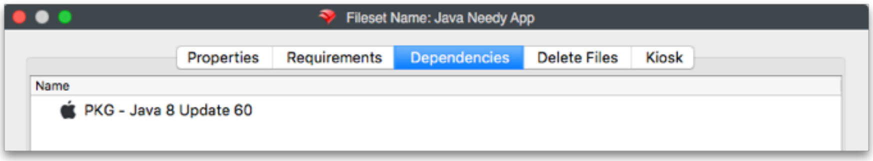
Details contains general application information, management flags, and VPP information. The management flags include the ability to force application removal when the MDM profile is removed, and the ability restrict application data from being backed up in iTunes. VPP shows the connection between Fileset and a VPP account (what VPP token was used for the item, if applicable). 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.

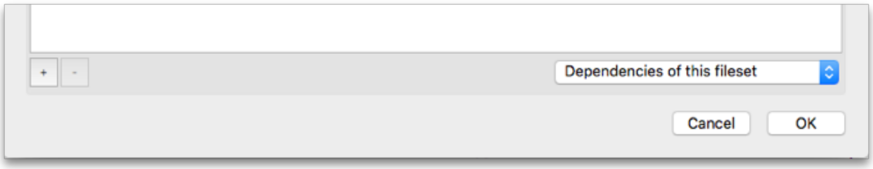
Exporting Filesets

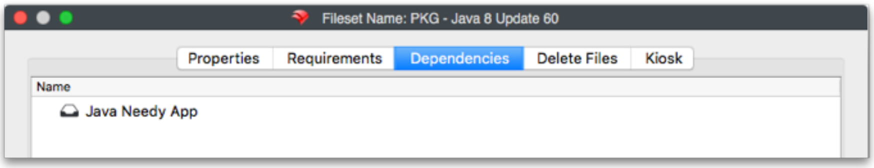
Filesets can be exported for transfer to another FileWave server. They can be compressed and stored for future use or archived. iOS Filesets, however, cannot be exported.

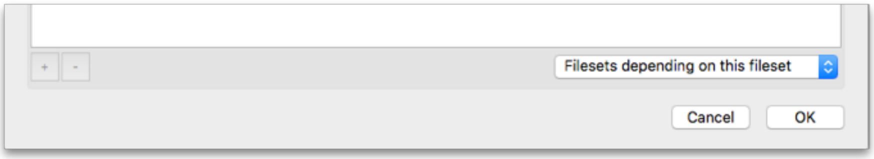
Dependencies (introduced in FW 10)

You can designate one of more Filesets that must be activated/installed before another can be activated. 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. The only Filesets that do not contain the ability to show dependency are the Apple App Store and iTunes Store Filesets.
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. There is also a toggle at the bottom to check and see if there are Filesets dependent upon the Fileset that you are examining.





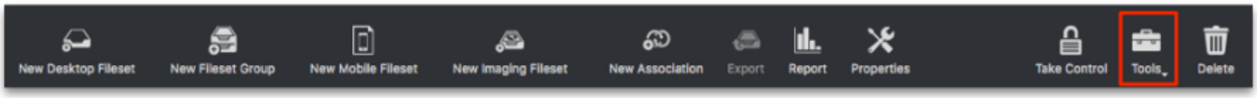


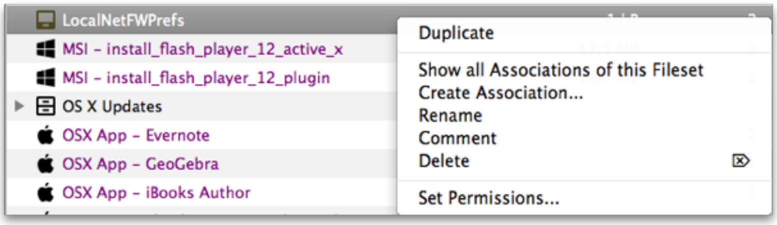


Starting with FileWave 11, is the ability to see a dependence chain when looking at the Fileset Status report in the Client Info dialog, where dependencies appear as children of the Filesets that require them.
Unable to render embedded object: File (worddav416f23a3d1561c0a3e9d6186b5480d74.png) not found.

5.6. 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.

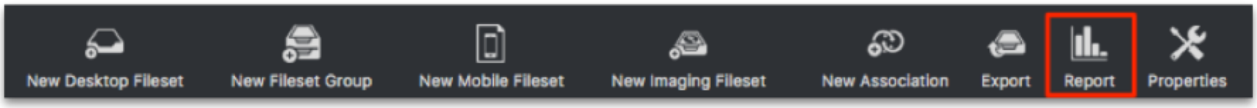




- ***Duplicate*** – You can take a fully-configured Fileset and create an exact Clone with the suffix "copy." This should be done whenever you want to assign a Fileset to more than one administrator for different deployment options, or when using VPP tokens that require different licenses assigned to 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.
- ***Create Association*** – This brings up a searchable list of Clients to associate with the Fileset.
- ***Rename*** – This allows you to change the name of the Fileset after it has been created.
- ***Comment*** – This allows you to add a comment that will show in the Fileset view to assist you in managing and keeping track of your Filesets.
- ***Delete*** – This deletes the selected Fileset from the database.
- ***Set Permissions*** – This allows you to specify the access level of your administrators to a given Fileset or Fileset Group.

5.7. Fileset Reports

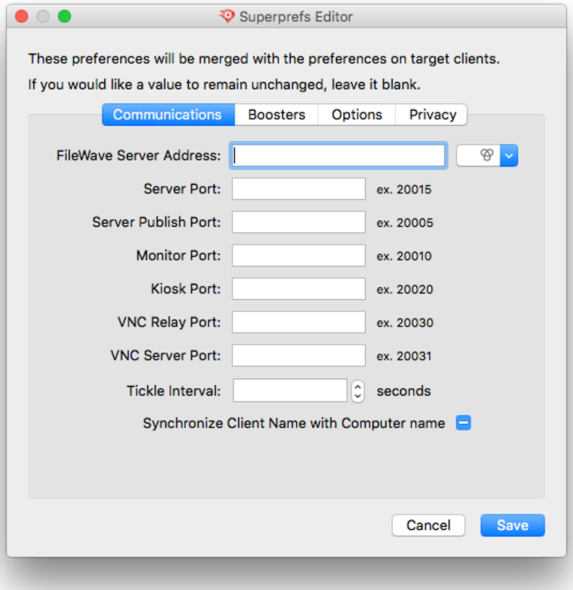
When you select a Fileset, Filesets, or Fileset Group, you can select the **Report** toolbar button to see the status of the selected item(s).



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.

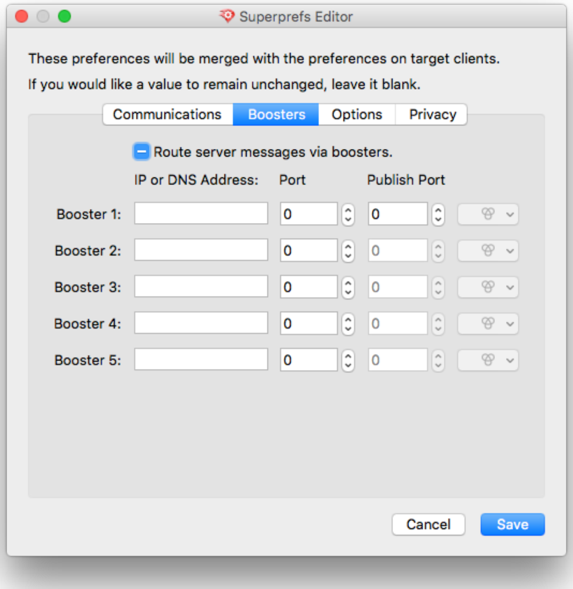
5.8. Using the Superprefs Editor

There are times when you may need to make significant changes to the Client settings (preferences stored on the Client). Instead of reinstalling the FileWave client software on all your Clients, you can use the *Superprefs Editor* to provide your Clients with a new configuration remotely.
The Superprefs Editor allows you to deploy updated Client preferences in a Fileset by delivering a file named "fwcld.newprefs.plist" to your Clients. This file may be delivered to any location on the Client, and will work with Android, Windows, and macOS 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 the 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, then click the OK button to save the file and exit the application.



These preferences will be merged with the preferences on target clients.
If you would like a value to remain unchanged, leave it blank.

FileWave Server Address:
Server Port: ex. 20015
Server Publish Port: ex. 20005
Monitor Port: ex. 20010
Kiosk Port: ex. 20020
VNC Relay Port: ex. 20030
VNC Server Port: ex. 20031
Tickle Interval: seconds
Synchronize Client Name with Computer name

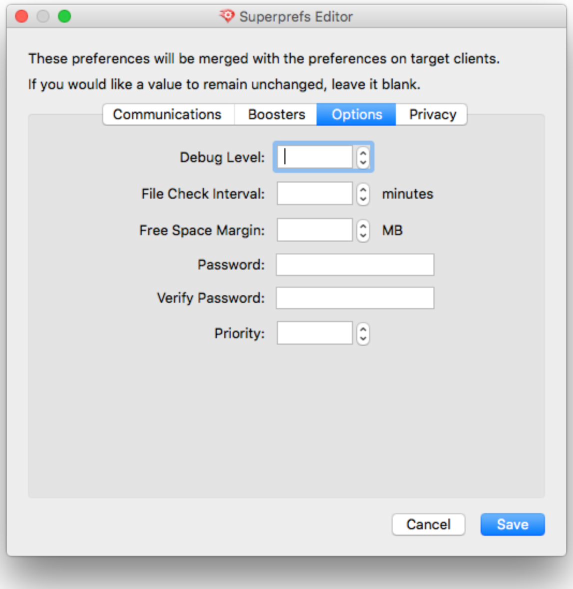


These preferences will be merged with the preferences on target clients.

If you would like a value to remain unchanged, leave it blank.

☐ Route server messages via boosters.

	IP or DNS Address:	Port	Publish Port
Booster 1:		0	0
Booster 2:		0	0
Booster 3:		0	0
Booster 4:		0	0
Booster 5:		0	0



These preferences will be merged with the preferences on target clients.

If you would like a value to remain unchanged, leave it blank.

Debug Level:

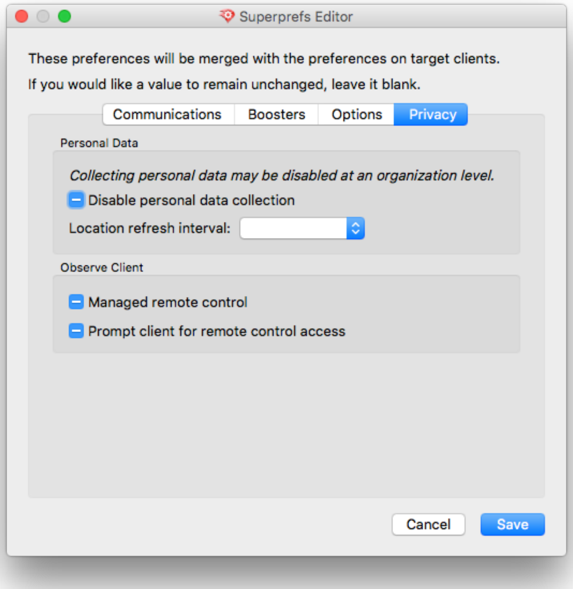
File Check Interval: minutes

Free Space Margin: MB

Password:

Verify Password:

Priority:



These preferences will be merged with the preferences on target clients.
If you would like a value to remain unchanged, leave it blank.

Personal Data

Collecting personal data may be disabled at an organization level.

⊟ Disable personal data collection

Location refresh interval:

Observe Client

⊟ Managed remote control

⊟ Prompt client for remote control access

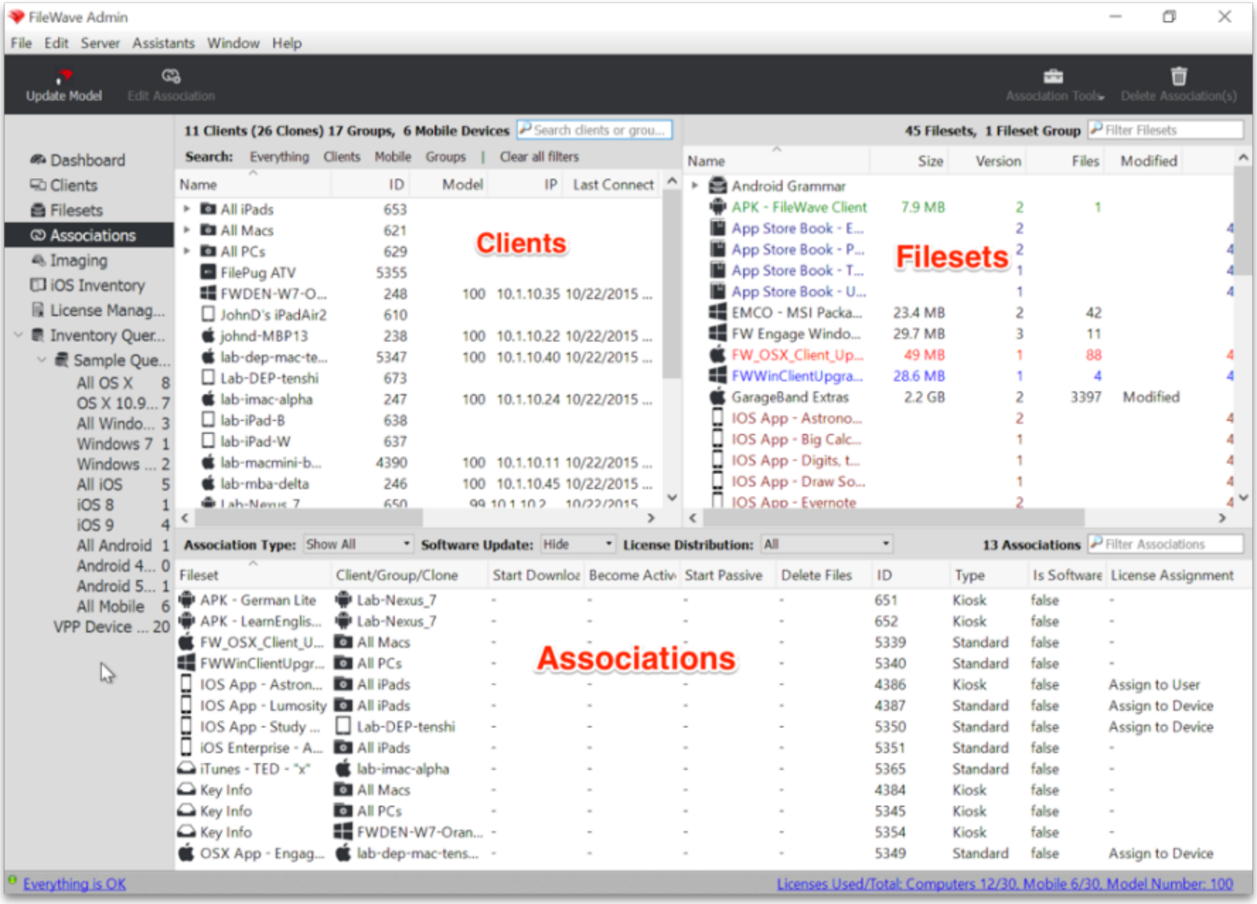
The file is automatically saved to your desktop on the computer running the FileWave Superprefs Editor. Open FileWave Admin and follow the next steps:

- 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.

5.9. Using Associations with Filesets

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



Clients

11 Clients (26 Clones) 17 Groups, 6 Mobile Devices

Name	ID	Model	IP	Last Connect
All iPads	653			
All Macs	621			
All PCs	629			
FilePug ATV	5355			
FWDEN-W7-O...	248	100	10.1.10.35	10/22/2015 ...
JohnD's iPadAir2	610			
johnd-MBP13	238	100	10.1.10.22	10/22/2015 ...
lab-dep-mac-te...	5347	100	10.1.10.40	10/22/2015 ...
Lab-DEP-tenshi	673			
lab-imac-alpha	247	100	10.1.10.24	10/22/2015 ...
lab-iPad-B	638			
lab-iPad-W	637			
lab-macmini-b...	4390	100	10.1.10.11	10/22/2015 ...
lab-mba-delta	246	100	10.1.10.45	10/22/2015 ...
Lab-Nexus 7	650	99	10.1.10.2	10/22/2015

Filesets

45 Filesets, 1 Fileset Group

Name	Size	Version	Files	Modified	
Android Grammar					
APK - FileWave Client	7.9 MB	2	1		
App Store Book - E...		2			4
App Store Book - P...		2			4
App Store Book - T...		1			4
App Store Book - U...		1			4
EMCO - MSI Packa...	23.4 MB	2	42		
FW Engage Windo...	29.7 MB	3	11		
FW_OSX_Client_Up...	49 MB	1	88		4
FWWinClientUpgra...	28.6 MB	1	4		4
GarageBand Extras	2.2 GB	2	3397	Modified	
IOS App - Astrono...		2			4
IOS App - Big Calc...		1			4
IOS App - Digits, t...		1			4
IOS App - Draw So...		1			4
IOS App - Evernote		2			4

Association Type: Show All Software Update: Hide License Distribution: All 13 Associations

Associations

Fileset	Client/Group/Clone	Start Downloa	Become Activ	Start Passive	Delete Files	ID	Type	Is Software	License Assignment
APK - German Lite	Lab-Nexus_7	-	-	-	-	651	Kiosk	false	-
APK - LearnEnglis...	Lab-Nexus_7	-	-	-	-	652	Kiosk	false	-
FW_OSX_Client_U...	All Macs	-	-	-	-	5339	Standard	false	-
FWWinClientUpgr...	All PCs	-			-	5340	Standard	false	-
IOS App - Astron...	All iPads	-	-	-	-	4386	Kiosk	false	Assign to User
IOS App - Lumosity	All iPads	-	-	-	-	4387	Standard	false	Assign to Device
IOS App - Study ...	Lab-DEP-tenshi	-	-	-	-	5350	Standard	false	Assign to Device
iOS Enterprise - A...	All iPads	-	-	-	-	5351	Standard	false	-
iTunes - TED - "x"	lab-imac-alpha	-	-	-	-	5365	Standard	false	-
Key Info	All Macs	-	-	-	-	4384	Kiosk	false	-
Key Info	All PCs	-	-	-	-	5345	Kiosk	false	-
Key Info	FWDEN-W7-Oran...	-	-	-	-	5354	Kiosk	false	-
OSX App - Engag...	lab-dep-mac-tens...	-	-	-	-	5349	Standard	false	Assign to Device

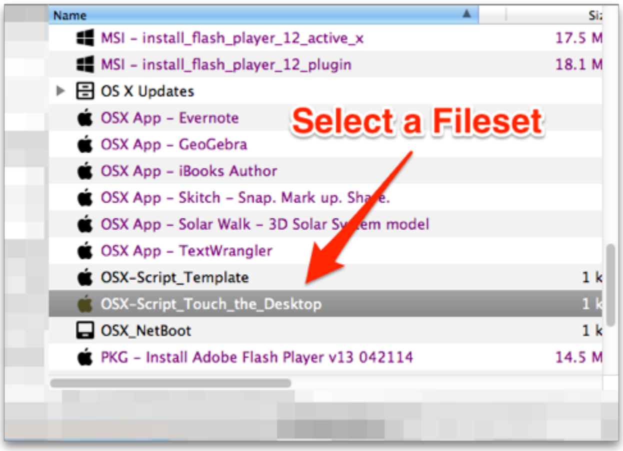
Licenses Used/Total: Computers 12/30, Mobile 6/30, Model Number: 100

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 select a Fileset, link it to a Client/Group, the update the server model.

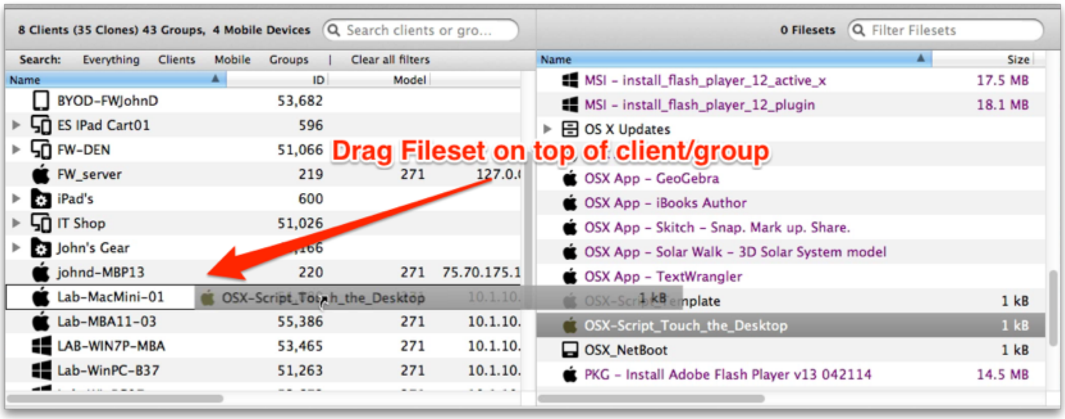
1. You choose a Fileset from the upper right pane:



Select a Fileset

Name	Si:
MSI – install_flash_player_12_active_x	17.5 M
MSI – install_flash_player_12_plugin	18.1 M
OS X Updates	
OSX App – Evernote	
OSX App – GeoGebra	
OSX App – iBooks Author	
OSX App – Skitch – Snap. Mark up. Share.	
OSX App – Solar Walk – 3D Solar System model	
OSX App – TextWrangler	
OSX-Script_Template	1 k
OSX-Script_Touch_the_Desktop	1 k
OSX_NetBoot	1 k
PKG – Install Adobe Flash Player v13 042114	14.5 M

1. 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.



Drag Fileset on top of client/group

8 Clients (35 Clones) 43 Groups, 4 Mobile Devices

Search clients or gro...
Search: Everything Clients Mobile Groups | Clear all filters

Name	ID	Model	
BYOD-FWJohnD	53,682		
ES IPad Cart01	596		
FW-DEN	51,066		
FW_server	219	271	127.0.(
iPad's	600		
IT Shop	51,026		
John's Gear	,166		
johnd-MBP13	220	271	75.70.175.1
Lab-MacMini-01			10.1.10.
Lab-MBA11-03	55,386	271	10.1.10.
LAB-WIN7P-MBA	53,465	271	10.1.10.
Lab-WinPC-B37	51,263	271	10.1.10.

0 Filesets

Filter Filesets
OSX-Script_Touch_the_Desktop
1 kB

Name	Size
MSI – install_flash_player_12_active_x	17.5 MB
MSI – install_flash_player_12_plugin	18.1 MB
OS X Updates	
OSX App – GeoGebra	
OSX App – iBooks Author	
OSX App – Skitch – Snap. Mark up. Share.	
OSX App – Solar Walk – 3D Solar System model	
OSX App – TextWrangler	
OSX-Script_Template	1 kB
OSX-Script_Touch_the_Desktop	1 kB
OSX_NetBoot	1 kB
PKG – Install Adobe Flash Player v13 042114	14.5 MB

1. Finally, click on **Update Model** in the main toolbar, or use *Cmd-U (macOS)* or *Ctrl-U (Win)*, to lock in the change.

Customizing the Association

The basic workflow will associate a Fileset with a Client. When the Client checks in following the server model update, the Client will get a new Manifest from the Server containing a list of any new Filesets to be associated or changes in existing Fileset associations. The Client compares the Manifest to its Catalog (current state after previous check-in) and build a work list if things have changed, which can include pulling down new Filesets, deactivating existing Filesets, etc
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

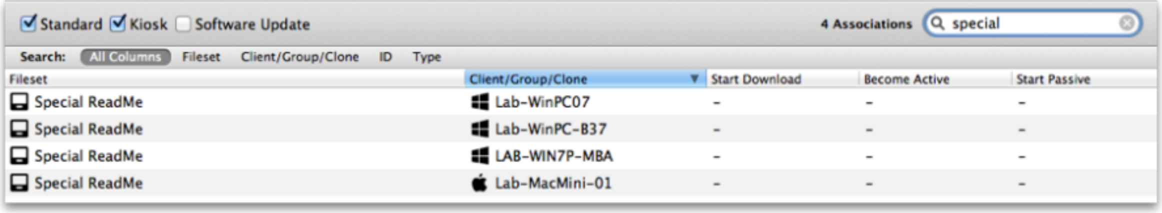
The first improvement over the basic workflow is being able to look at the Filesets that are associated with a specific Client or Group. You do this by right-clicking on the Client or Group in the Clients portion of the Associations window and selecting **Show Associated Fileset**. This will change the Associations view in the bottom part of the window to
show you all of the Filesets that have been **directly** associated with that specific Client. 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 and or to Clones in regular 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.

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.



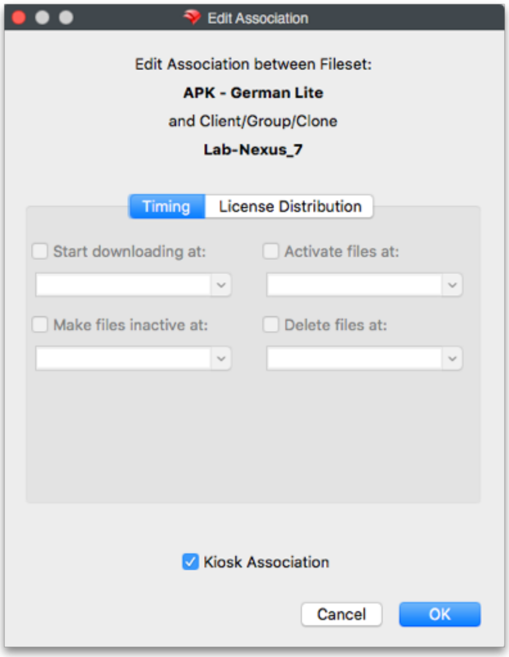
☑ Standard ☑ Kiosk ☐ Software Update

4 Associations

Fileset	Client/Group/Clone	Start Download	Become Active	Start Passive
Special ReadMe	Lab-WinPC07	-	-	-
Special ReadMe	Lab-WinPC-B37	-	-	-
Special ReadMe	LAB-WIN7P-MBA	-	-	-
Special ReadMe	Lab-MacMini-01	-	-	-

Editing the Association

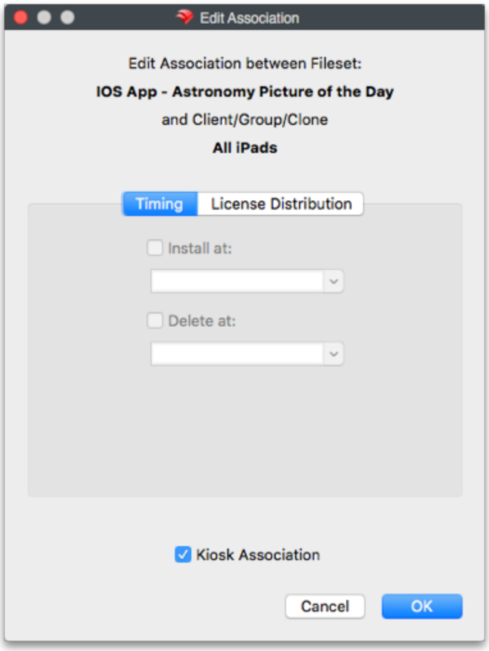
Another capability of the Associations window is the ability to edit Fileset associations. Within this functionality, you have the power to designate the deployment schedule, change the type of Fileset from standard to self-service Kiosk, and choose when the Fileset is deactivated and removed from the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



Edit Association between Fileset:
APK - German Lite
and Client/Group/Clone
Lab-Nexus_7

☐ Start downloading at:
☐ Activate files at:
☐ Make files inactive at:
☐ Delete files at:

☑ Kiosk Association



Edit Association between Fileset:
IOS App - Astronomy Picture of the Day
and Client/Group/Clone
All iPads

☐ Install at:
☐ Delete at:

☑ Kiosk Association

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

- ***Start downloading at*** – This tells the Client to start downloading the Fileset at a specific date and time. The Fileset will be downloaded and cached locally, but is inert; i.e., it will have no impact on the Client (other than storage space on the drive) until it is activated. 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 minimize network traffic bottlenecks when 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*** – This tells the Client when (date and time) 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*** – This tells the Client to locate and move all components of that Fileset back into the local cache, so that the

Fileset no longer has an affect on the operation of the Client computer or device.

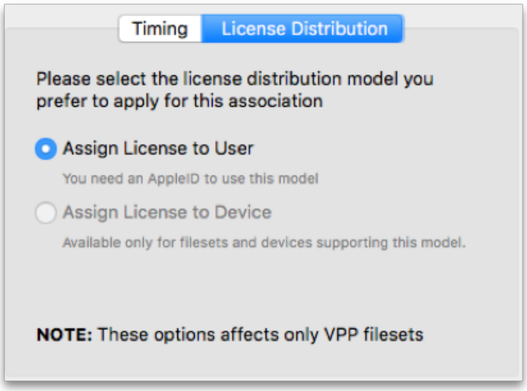
- ***Delete files at*** – This tells the Client to delete the Fileset at a specific data and time.
- ***Kiosk Association*** – This converts the Fileset from a standard distribution to a self-service Kiosk item. Filesets that have been distributed as standard items can be converted to Kiosk mode and vice versa.

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

License Distribution (FW 10+)

You have the ability to designate that an Apple Volume Purchase Program "Managed Distribution" license be applied to either an Apple ID that is associated with a macOS computer or iOS device or to the device directly. This applies only to applications controlled by Apple's VPP, with the additional requirement that the application developer configured the application to support **direct device** assignment. You can see if the application is device assignable in the App Store under the application

You can set a default value of User or Device assignment in FileWave Admin's Preferences, in the VPP & DEP tab, but can override the default settings on a per-Fileset basis, if both options are supported for the application in the Fileset. As you can see from the example below, one of the chosen applications has the *Assign License to Device* greyed out, meaning that this specific application must be assigned to a designated Apple ID, because it does not support direct device assignment.



Please select the license distribution model you prefer to apply for this association

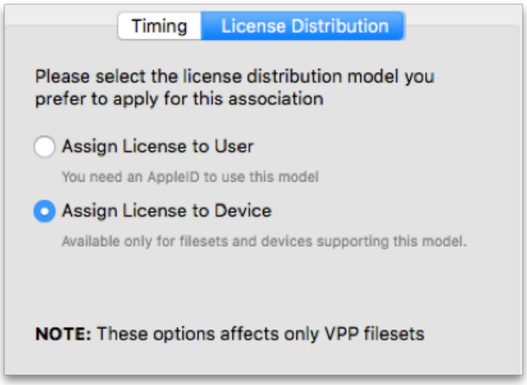
● Assign License to User

You need an AppleID to use this model

○ Assign License to Device

Available only for filesets and devices supporting this model.

NOTE: These options affects only VPP filesets



Please select the license distribution model you prefer to apply for this association

○ Assign License to User

You need an AppleID to use this model

● Assign License to Device

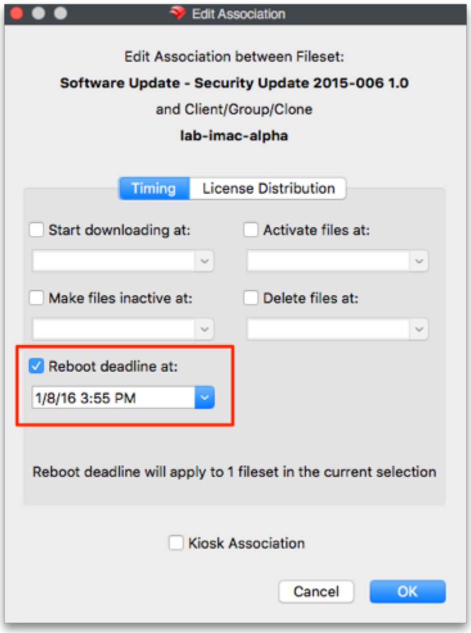
Available only for filesets and devices supporting this model.

NOTE: These options affects only VPP filesets

Note: 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. 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 for that Group.

Special setting for the Requires Reboot property

When you have a Fileset, such as a system software update, that requires a reboot of the client, the user may try to cancel that update to avoid the reboot. In FW 10.1+, a feature was added to the Fileset **Associations** editor window that allows you to set a deadline for the reboot. This editor property can be set for a Group of Filesets, or for a single Fileset. When the deadline comes, the device will reboot automatically in order to complete the installation of the designated Fileset.



Edit Association between Fileset:
Software Update - Security Update 2015-006 1.0
and Client/Group/Clone
lab-imac-alpha

□ Start downloading at:
□ Activate files at:
□ Make files inactive at:
□ Delete files at:
☑ Reboot deadline at: 1/8/16 3:55 PM

Reboot deadline will apply to 1 fileset in the current selection

□ Kiosk Association

Association Tools

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

- ***Reveal Client/Group/Clone*** – This displays and highlights the Client/Group/Clone related to this association in the upper-left portion of the window.
- ***Show all Associations of this Client/Group/Clone*** – This displays and highlights all associations related to the client/Group/Clone in the lower portion of window.
- ***Reveal Fileset*** – This displays and highlights the Fileset in the upper-right portion of window.
- ***Open Fileset*** – This displays the contents of the Fileset (same as double-clicking on Fileset in the Filesets view).
- ***Open Fileset Report Window*** – This displays the report showing the status of a Fileset, Filesets, or Fileset Group's distribution.
- ***Show all Associations of this Fileset*** – This displays all of the Clients associated with this Fileset
- ***Delete Association(s)*** – This removes 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 and added back to the list of available licenses.

Association Conflict Resolution

The algorithm for computing which Client 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 older 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 Client or Group. Associations made to a Smart Group will not show up when viewing the Client associations and vice versa.

Imaging associations

Imaging Filesets and their associations are covered in Chapter **9**.

5.10. FileWave and AutoPkg

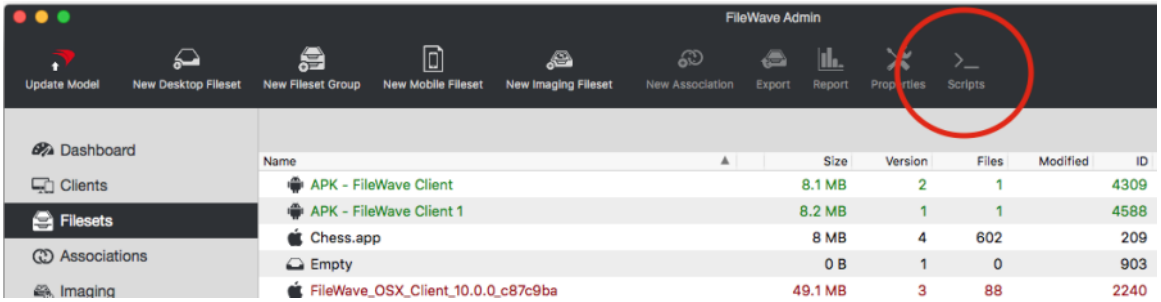
Software updates that come from Apple and Microsoft are sufficient for keeping operating systems up-to-date; but there is a need to maintain currency for 3rd party applications. **AutoPKG** is an automation framework for macOS software packaging and distribution, oriented toward the tasks one would normally perform manually to prepare third-party software for mass deployment to managed clients. It can be thought of as an automated version of **Fileset Magic** for software that runs on macOS.
FileWave administrators can merge the FileWave Admin and AutoPkg environments together through a series of **recipes.** Instructions for working with AutoPkg is here: https://github.com/autopkg/filewave
The primary site for AutoPkg is here: http://autopkg.github.io/autopkg with additional information here: https://github.com/autopkg/autopkg
Last, but not least, AutoPkgr is a free Mac app that makes it easy to install and configure AutoPkg. You can get that here: http://www.lindeGroup.com/autopkgr

5.11. Fileset Scripts

FileWave 11+ provides the ability to run a script at any of seven stages of Fileset deployment (called Activation States):

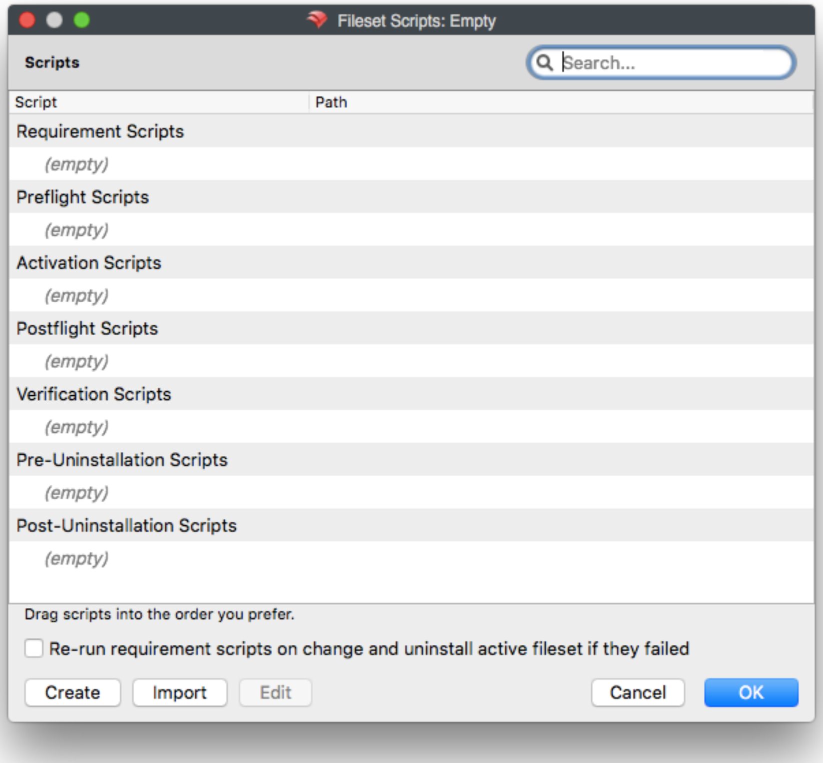
- Requirements
- Preflight
- Activation
- Postflight
- Verification
- Pre-Uninstallation
- Post-Uninstallation

In FileWave Admin, while in the Filesets view, the toolbar now contains a Scripts icon.



Name	Size	Version	Files	Modified	ID
APK - FileWave Client	8.1 MB	2	1		4309
APK - FileWave Client 1	8.2 MB	1	1		4588
Chess.app	8 MB	4	602		209
Empty	0 B	1	0		903
FileWave_OSX_Client_10.0.0_c87c9ba	49.1 MB	3	88		2240

When you select a given Fileset, then click on the Scripts icon, the Scripts dialog opens



Script	Path
Requirement Scripts	
(empty)	
Preflight Scripts	
(empty)	
Activation Scripts	
(empty)	
Postflight Scripts	
(empty)	
Verification Scripts	
(empty)	
Pre-Uninstallation Scripts	
(empty)	
Post-Uninstallation Scripts	
(empty)	

Drag scripts into the order you prefer.

☐ Re-run requirement scripts on change and uninstall active fileset if they failed

The dialog shows the scripts that will be executed for the given Fileset and the activation state in which they will be executed. The order in which scripts of the same activation state and Fileset are executed is the same as they appear in the list (i.e. from top to bottom). You can drag & drop scripts in order to change the execution order.
You can create and import scripts by clicking the corresponding buttons. Editing a script is also possible, so is dragging and dropping a script from Finder in order to import it.
Any changes to the Fileset will be applied when you click OK. If you click Cancel, the current changes will be lost and the Fileset will not be modified.
Scripts in the list can be double-clicked, which causes the file property dialog to appear. You can change most of the attributes of the script in the same way as in the open Fileset dialog. There are, however, certain attributes you cannot change. For instance, you cannot unset the Execute flag; therefore, it is disabled. For requirement scripts, it is not possible to change the interactive/non-interactive option, since the exit code of the script is required to decide whether the Fileset should be downloaded. Therefore, this field is also disabled.
The checkbox "Re-run requirement scripts on change and uninstall active Fileset if they failed" controls the same internal setting as the checkbox "Evaluate requirements on change and uninstall active Fileset if they failed" in the Requirements tab of the Fileset properties. If checked, when a Fileset needs to be updated, the Client checks the requirements of the Fileset again. This includes executing requirement scripts. If any of the requirements or requirement scripts fail, the Fileset will be uninstalled.

Fileset Scripts Types

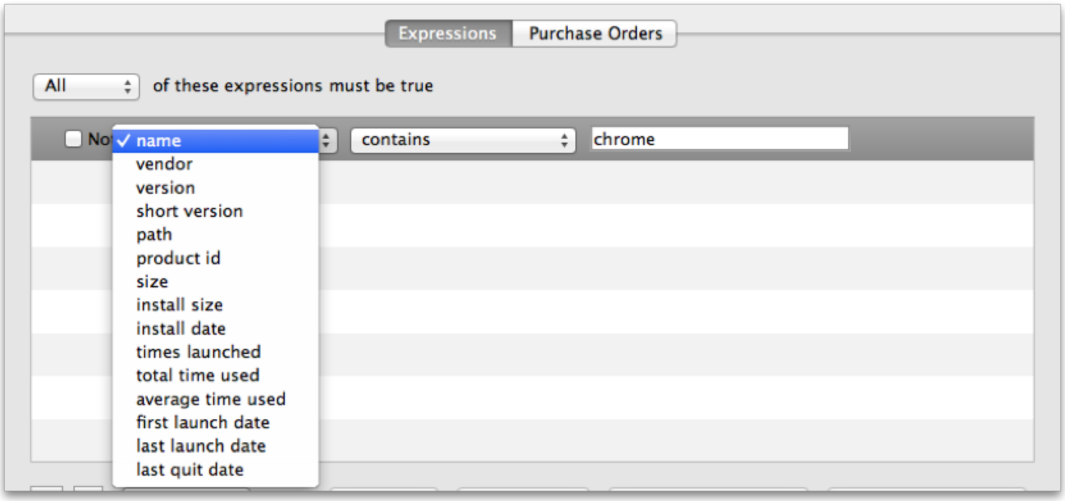
- ***Requirements Scripts*** – A requirements script checks the requirement on the Fileset before any dependencies are downloaded. If any requirement script fails (return non-zero), then the Fileset and its dependencies will not be downloaded nor installed.
- ***Preflight Scripts*** – A preflight script checks the needs of the Fileset before the Fileset downloads, but after dependencies have been installed. If any preflight script fails (returns non-zero), then the Fileset won't be downloaded or installed.
- ***Activation Scripts*** – An activation script is executed upon activation of the Fileset.
- ***Postflight Scripts*** – A postflight script is executed after the installation of the Fileset has completed.
- ***Verification Scripts*** – A verification script is executed after postflight scripts and upon every "verification of the Fileset."
- ***Pre-Uninstallation Scripts*** – A pre-uninstallation script is executed on inactivation of a Fileset and right before a Fileset is uninstalled.
- ***Post-Uninstallation Scripts*** – A post-uninstallation script is executed right after uninstalling/removing the Fileset from a client and its dependencies.

6. License Management and Apple's Volume Purchase Program (VPP)
FileWave supports a powerful license management module, allowing you to keep track of your software licenses, as reported to inventory,

manually using purchase orders, Apple's VPP managed distribution items, and licensed fonts. You can set triggers to let you know when you are running out of licenses.

6.1. Manual Licenses

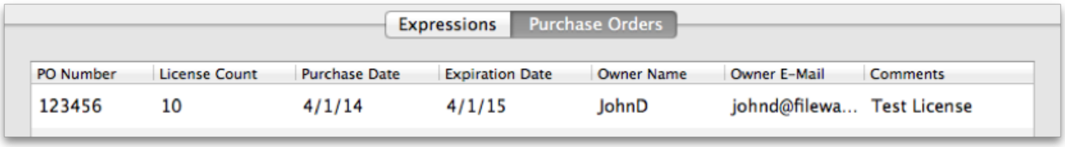
The first method for managing software licenses is to manually create the query to search inventory. You select **New License** from the toolbar and give it a name. Then you set the license expression to be based on managing an application or a font. You can choose to manage items installed in all three of the operating systems FileWave supports from a "computer" point of view. (Android, due to its FileWave client, is managed as a hybrid between computer and mobile. Next, you create the inventory search; e.g. the Chrome browser.



All of these expressions must be true

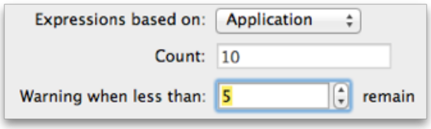
name contains chrome

Now, gather a count of the licenses you have. 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.



PO Number	License Count	Purchase Date	Expiration Date	Owner Name	Owner E-Mail	Comments
123456	10	4/1/14	4/1/15	JohnD	johnd@filewa...	Test License

Then add a trigger value to warn when you are running out of licenses.

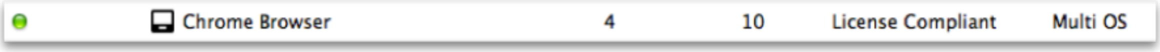


Expressions based on: Application

Count: 10

Warning when less than: 5 remain

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



● Chrome Browser 4 10 License Compliant Multi OS

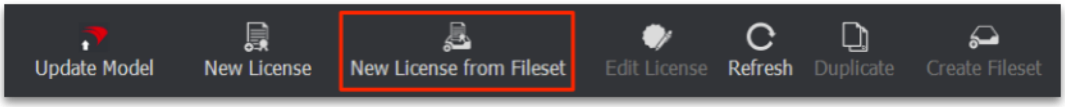
When you double-click on the license, you will see the details of the query displayed. The window will actually display a significant amount of information about your search results, including detailed device info.

6.2. 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 license fonts. The workflow for setting up a font license is roughly the same as that for applications. First, you create and name the license; but this time, designate the expressions based on "font."
As with application licenses, 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.

6.3. Creating Licenses from Filesets

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.



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, 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.

6.4. 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 macOS and iOS applications and books in bulk and provide these 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 available at the following two URLs:
http://help.apple.com/deployment/ios/
https://help.apple.com/deployment/macos/
VPP is supported in FileWave for both iOS and macOS. There are two mechanisms for assigning applications and books to clients - **redeemable codes** and **managed distribution licenses**. Redeemable codes provide a set of codes to be used for content distribution, but once given out, the content legally belongs to the owner of the Apple ID that redeemed the code. Managed Distribution provides licenses that can be associated and revoked, so the purchasing authority retains ownership of the license (with the exception of books, which always are owned by the person to whose Apple ID the license was distributed to). This allows you 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.

Differences between redeemable codes and managed distribution licenses

The original model for mass deployment of content was using **redeemable codes**. The VPP administrator purchased applications from the Apple VPP site. Apple provided a set of codes in a spreadsheet that could be downloaded. Those codes were then used to create an application Fileset for installation on managed devices, or were 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. This Apple Support article describes the process: https://support.apple.com/en-us/HT202863.
Apple's newer model for application license management allows you to assign licenses to users and revoke those licenses at a future date. This 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.
Note: This process is only valid for applications since Apple requires all book distributions to be permanently assigned to personal Apple IDs.

Managed Distribution - user versus device assignment

Initially, Managed Distribution required association to a unique Apple ID for any deployed content. With the release of iOS 9 and OS X 10.11, VPP managed distribution licenses acquired the ability to be assign applications directly to a device, provided the developer allows it. 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.

How FileWave works with VPP

There are several approaches to using FileWave with VPP. The deployment workflows relate to the overall control of the application(s) to be deployed. The actual workflows discussed are covered in detail later in this Chapter.
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 Apple ID. 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: 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 Apple ID and the FileWave MDM. Whether you use individual Apple IDs, in the case

of a BYOD or full 1:1 deployment, or institutional Apple IDs in the case of a managed lab or cart, the application licenses remain under your control.

If you assign the licenses to devices, there is no longer a requirement to match an Apple ID with the device. You can, for example, use a generic LDAP or fixed MDM authentication account to enroll the device(s), then just configure your Filesets to be assigned to the device.

When you assign or associate Apple Store content through a Fileset to a user's Apple ID, the end user will see that content in their Purchases in the App Store.

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 Apple ID. 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 users 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 VPP, you 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 customer, you 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 or Apple Configurator, active with your VPP token when you set up FileWave for VPP. This will 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. Use the instructions in Chapter **2** to configure your FileWave Admin Preferences for VPP.

Synchronize data with the VPP server for VPP

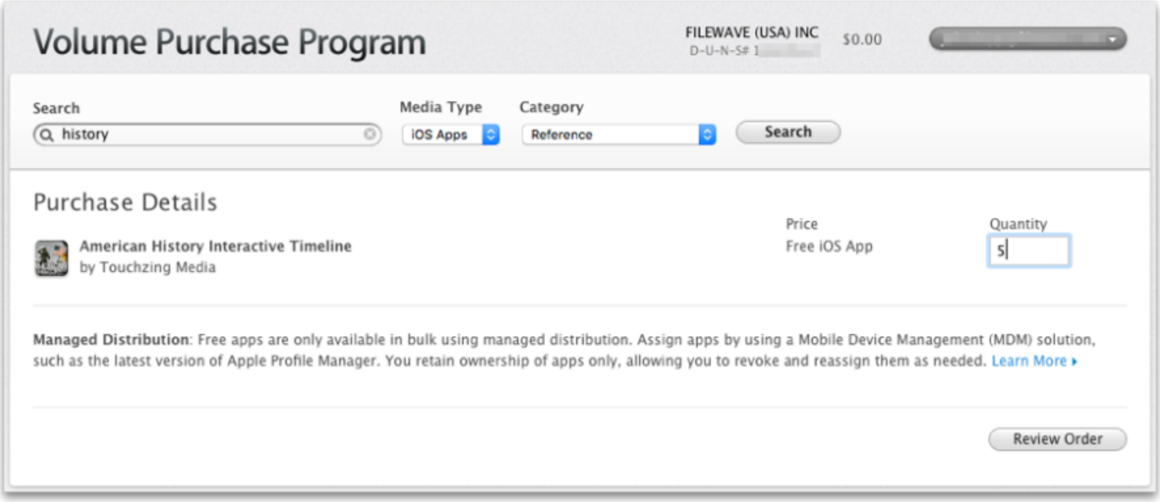
Once your token(s) are active, the FileWave Server will automatically synchronize with Apple's VPP service. Depending on how many items you have in your purchase list, this process may take a while. When you have synchronized your VPP data with your FileWave Server, you should see any VPP Managed Distribution purchases listed in the **License Management** section of FileWave Admin.

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. You should see entries in the License Management view that match your purchase history.

Note: Only VPP Managed Distribution licenses will be displayed here. The older VPP Redeemable Codes, if you have any, will still be located in the "VPP Code Management" assistant in FileWave Admin. When you purchase redeemable codes, you must download the spreadsheet and import it into FileWave using this assistant.

Adding licensed applications to your FileWave Server

The process of adding content for VPP code redemption or managed distribution is extremely simple. When you purchase any content in the VPP Store, upon a VPP sync with your FileWave server, the items will appear in your License Management pane. First, you make your purchase in the VPP Store:



Volume Purchase Program

FILEWAVE (USA) INC
D-U-N-S# 1[redacted]
$0.00
[redacted]

Search: history
Media Type: iOS Apps
Category: Reference

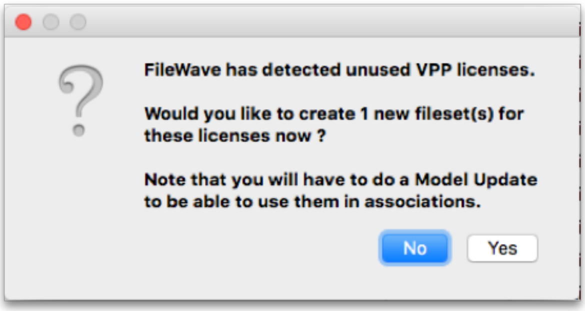
Purchase Details

American History Interactive Timeline
by Touchzing Media

Price: Free iOS App
Quantity: 5

Managed Distribution: Free apps are only available in bulk using managed distribution. Assign apps by using a Mobile Device Management (MDM) solution, such as the latest version of Apple Profile Manager. You retain ownership of apps only, allowing you to revoke and reassign them as needed. Learn More ▸

Once you receive confirmation that the purchase is completed, you can force a sync of VPP in your Preferences, or wait for the overnight sync. In FileWave Admin, go to the License Management pane and click the **Refresh** button in the toolbar. You will get the following dialog:

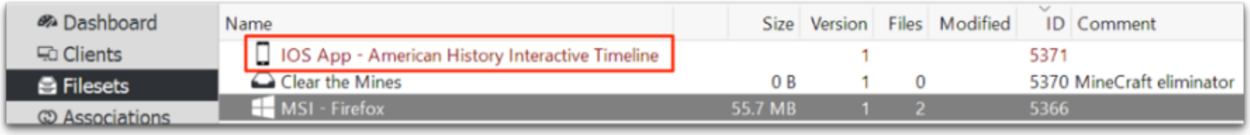


FileWave has detected unused VPP licenses.

Would you like to create 1 new fileset(s) for these licenses now ?

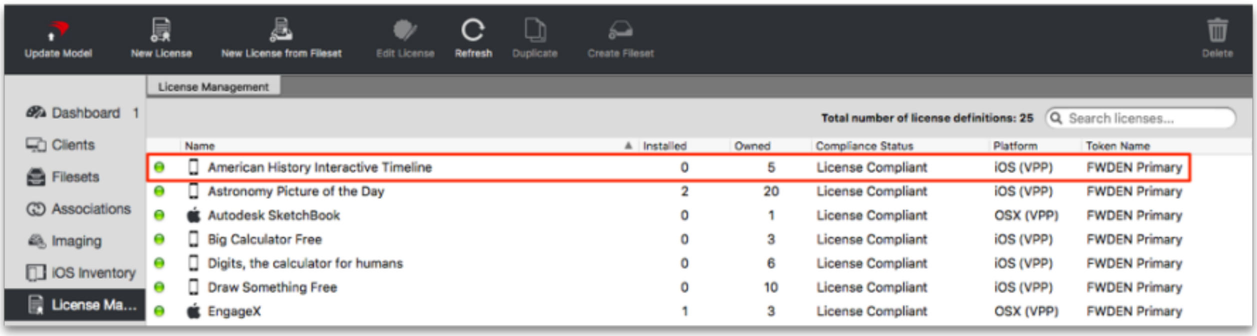
Note that you will have to do a Model Update to be able to use them in associations.

That dialog tells you that your purchase information has been loaded into FileWave; but there is no corresponding Fileset. At this point, you should click on *Yes* and follow up by updating the Model to refresh the database. You will be taken to the Filesets pane, and your new VPP application Fileset will be waiting:



Name	Size	Version	Files	Modified	ID	Comment
IOS App - American History Interactive Timeline		1			5371	
Clear the Mines	0 B	1	0		5370	MineCraft eliminator
MSI - Firefox	55.7 MB	1	2		5366	

Back at the License Management view, it will display the new license:



Total number of license definitions: 25

Name	Installed	Owned	Compliance Status	Platform	Token Name
American History Interactive Timeline	0	5	License Compliant	iOS (VPP)	FWDEN Primary
Astronomy Picture of the Day	2	20	License Compliant	iOS (VPP)	FWDEN Primary
Autodesk SketchBook	0	1	License Compliant	OSX (VPP)	FWDEN Primary
Big Calculator Free	0	3	License Compliant	iOS (VPP)	FWDEN Primary
Digits, the calculator for humans	0	6	License Compliant	iOS (VPP)	FWDEN Primary
Draw Something Free	0	10	License Compliant	iOS (VPP)	FWDEN Primary
EngageX	1	3	License Compliant	OSX (VPP)	FWDEN Primary

At this point, you can begin associating the new content with your enrolled devices.

VPP and iBooks

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. 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 Apple IDs; they are not allowed to be assigned to institutional Apple IDs per Apple's legal guidelines, nor can they be assigned to devices.

Manually creating Filesets from VPP managed distribution content

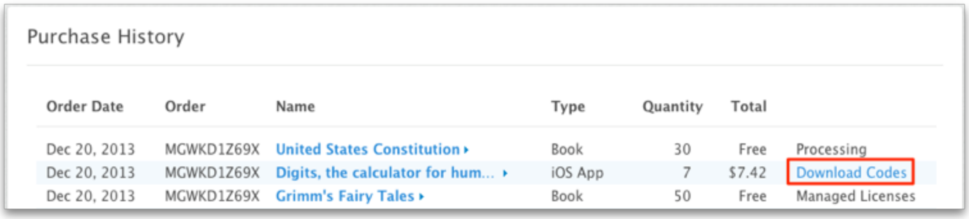
By default, your VPP managed distribution license purchases should automatically show up in License Management, and upon a ***Refresh*** of the pane, you should get a dialog asking you to create a Fileset for your purchases. If, however, you have items that are displayed in the License Management pane, and they do not have a corresponding Fileset, you can manually correct that problem.

Create a mobile Fileset for a managed content item.

All VPP purchases now appear in **License Management** as soon as the FileWave server syncs with the Apple VPP site. 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.

Redeemable codes

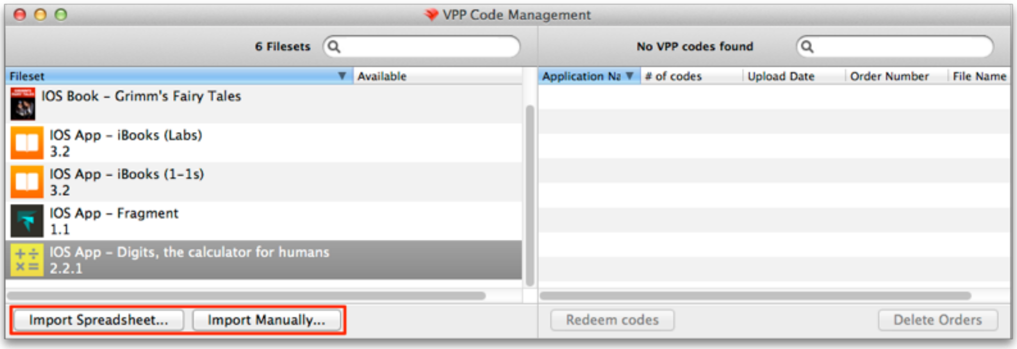
For redeemable codes, you will need to download the code spreadsheets. Log into your VPP account online, and select your *Purchase History*. For any content that you purchased using redeemable codes, you will see that you are able to download the codes in the form of an .xls spreadsheet. **Note: This 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.**



Purchase History

Order Date	Order	Name	Type	Quantity	Total	
Dec 20, 2013	MGWKD1Z69X	United States Constitution ▸	Book	30	Free	Processing
Dec 20, 2013	MGWKD1Z69X	Digits, the calculator for hum... ▸	iOS App	7	$7.42	Download Codes
Dec 20, 2013	MGWKD1Z69X	Grimm's Fairy Tales ▸	Book	50	Free	Managed Licenses

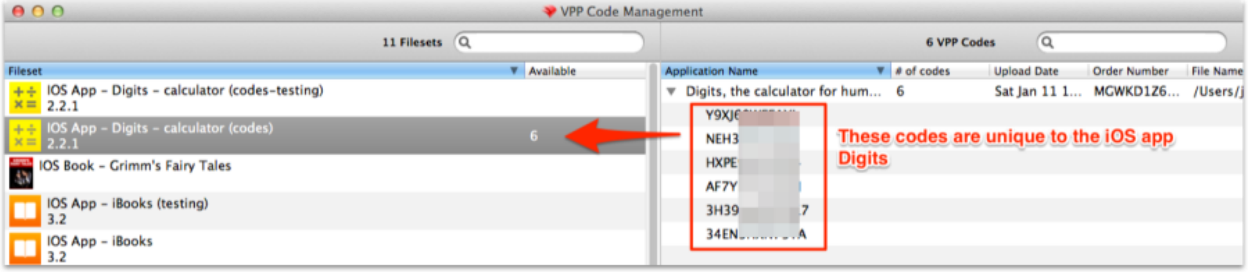
Once you have downloaded the spreadsheet(s) as needed, you will need to go to **Assistants / VPP Code Management**. This pane is used only for linking redeemable codes to Filesets. You have two methods for bringing codes into FileWave Admin, by importing the spreadsheet or manually entering the code information.



Fileset	Available
IOS Book - Grimm's Fairy Tales	
IOS App - iBooks (Labs) 3.2	
IOS App - iBooks (1-1s) 3.2	
IOS App - Fragment 1.1	
IOS App - Digits, the calculator for humans 2.2.1	

Application Na	# of codes	Upload Date	Order Number	File Name

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.

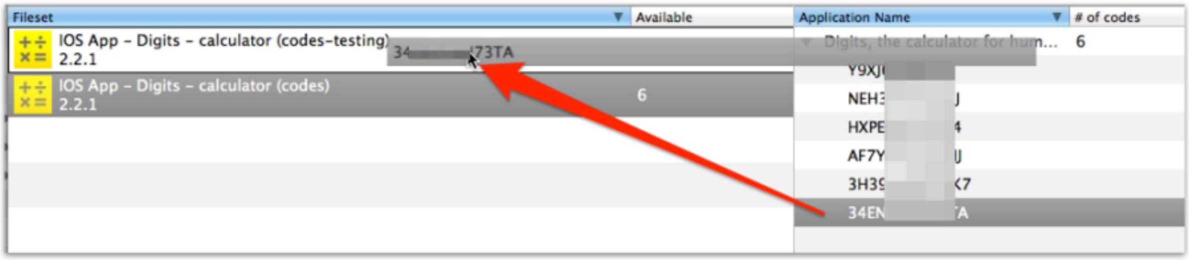


Fileset	Available
IOS App - Digits - calculator (codes-testing) 2.2.1	
IOS App - Digits - calculator (codes) 2.2.1	6
IOS Book - Grimm's Fairy Tales	
IOS App - iBooks (testing) 3.2	
IOS App - iBooks 3.2	

Application Name	# of codes	Upload Date	Order Number	File Name
▼ Digits, the calculator for hum...	6	Sat Jan 11 1...	MGWKD1Z6...	/Users/j
Y9XJ6[redacted]				
NEH3[redacted]				
HXPE[redacted]				
AF7Y[redacted]				
3H39[redacted]7				
34EN[redacted]A				

These codes are unique to the iOS app Digits

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
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 Fileset. This example shows dragging one code from the main Fileset for Digits onto the Fileset meant for the testing team.

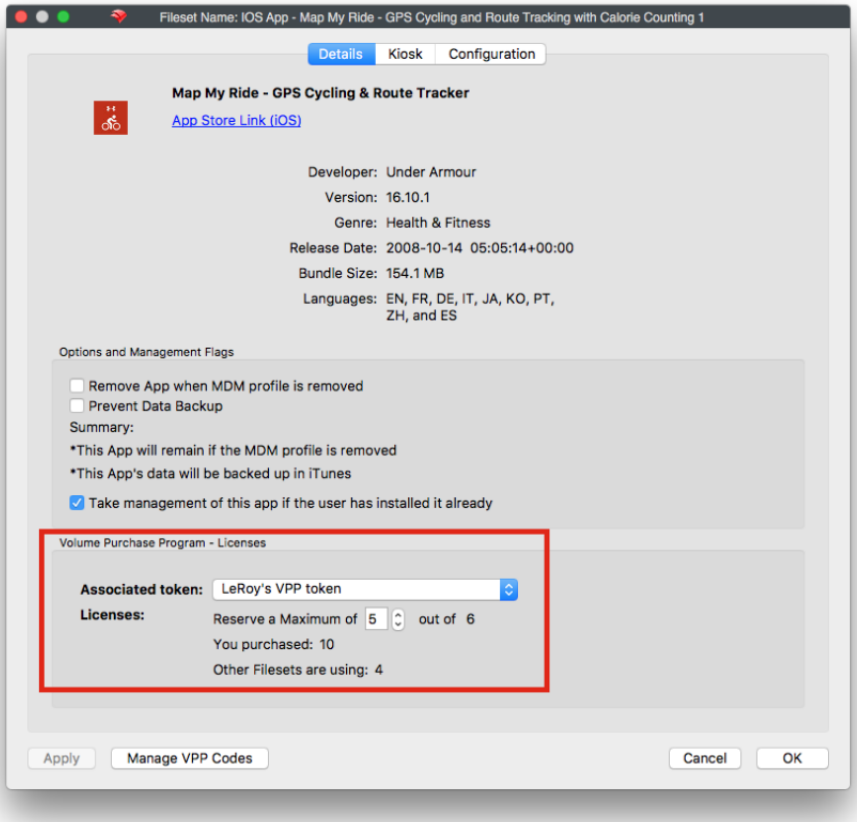


Fileset	Available
IOS App - Digits - calculator (codes-testing) 2.2.1	
IOS App - Digits - calculator (codes) 2.2.1	6

Application Name	# of codes
▼ Digits, the calculator for hum...	6
Y9XJ[redacted]	
NEH3[redacted]J	
HXPE[redacted]4	
AF7Y[redacted]J	
3H39[redacted]K7	
34EN[redacted]A	

Managed Distribution Licenses

The managed distribution content licenses are treated as part of a pool. When you look at each Fileset's details, you can see the status of your licenses:


Fileset Name: IOS App - Map My Ride - GPS Cycling and Route Tracking with Calorie Counting 1
Details
Kiosk
Configuration
Apply
Manage VPP Codes
Cancel
OK

Map My Ride - GPS Cycling & Route Tracker

App Store Link (iOS)

Developer: Under Armour
Version: 16.10.1
Genre: Health & Fitness
Release Date: 2008-10-14 05:05:14+00:00
Bundle Size: 154.1 MB
Languages: EN, FR, DE, IT, JA, KO, PT, ZH, and ES

Options and Management Flags

□ Remove App when MDM profile is removed
□ Prevent Data Backup

Summary:
•This App will remain if the MDM profile is removed
•This App's data will be backed up in iTunes

☑ Take management of this app if the user has installed it already

Volume Purchase Program - Licenses

Associated token: LeRoy's VPP token
Licenses: Reserve a Maximum of 5 out of 6
You purchased: 10
Other Filesets are using: 4

You will be required to track the usage of your licenses to avoid exceeding your allowed limit. If you distribute more copies of an item than you have licenses for, you will get installation errors.

VPP Managed Distribution User Management

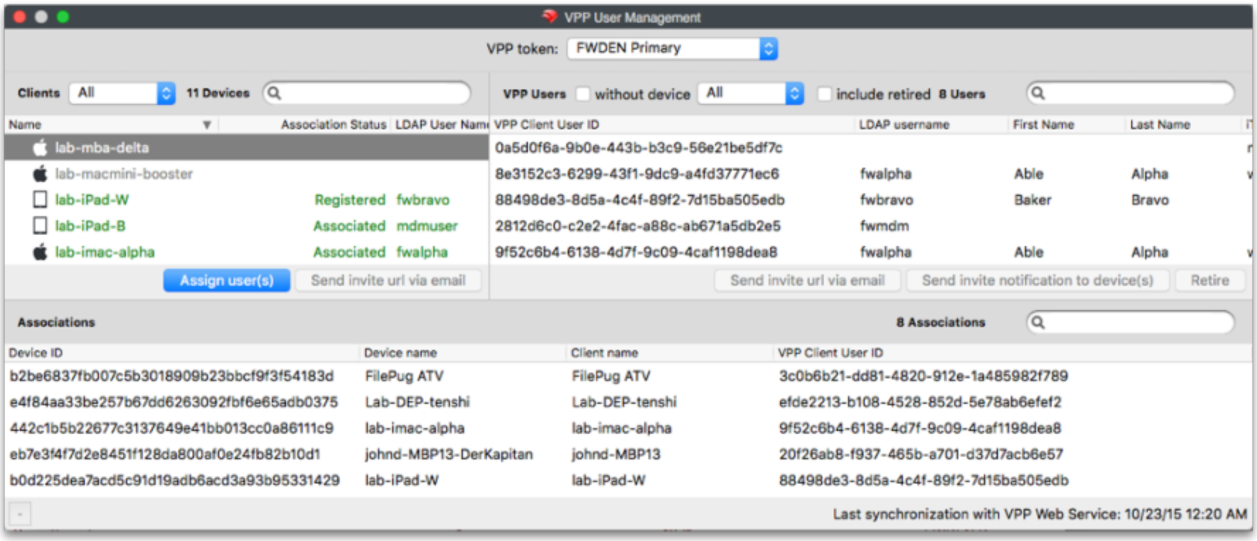
The most complex portion of the VPP Managed Distribution system is the interaction of the end user and the VPP license architecture. The process is as follows:

- User agrees to link their Apple ID with your VPP MDM server
- The MDM server associates managed distribution content licenses with a linked user
- The user sees all assigned content in their own Apple ID-based purchases in the iTunes/App Store
- If the user has auto-install enabled, the content automatically appears on the user's device(s)
- 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).

Note: Never use your VPP account Apple ID for personal purchases.

Creating users for your devices

Apple's VPP manages licenses that are either assigned to a device, or assigned to specific user's Apple ID. In the **Assistants / VPP User Management** pane, you can see all of your enrolled devices, and a list of VPP users.



VPP User Management

VPP token: FWDEN Primary

Clients All 11 Devices

Name	Association Status	LDAP User Name
lab-mba-delta		
lab-macmini-booster		
lab-iPad-W	Registered	fwbravo
lab-iPad-B	Associated	mdmuser
lab-imac-alpha	Associated	fwalpha

VPP Users □ without device All □ include retired 8 Users

VPP Client User ID	LDAP username	First Name	Last Name
0a5d0f6a-9b0e-443b-b3c9-56e21be5df7c			
8e3152c3-6299-43f1-9dc9-a4fd37771ec6	fwalpha	Able	Alpha
88498de3-8d5a-4c4f-89f2-7d15ba505edb	fwbravo	Baker	Bravo
2812d6c0-c2e2-4fac-a88c-ab671a5db2e5	fwmdm		
9f52c6b4-6138-4d7f-9c09-4caf1198dea8	fwalpha	Able	Alpha

Send invite url via email
Send invite notification to device(s)
Retire

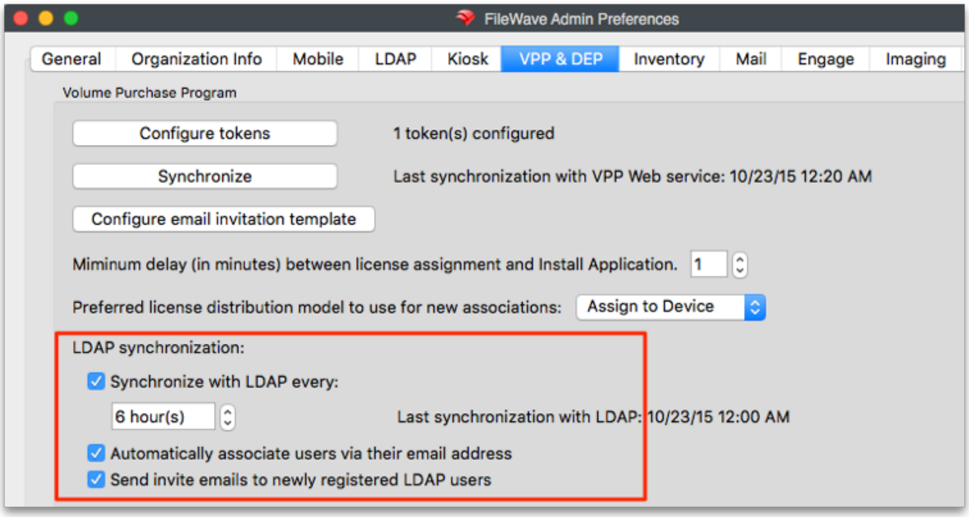
Associations 8 Associations

Device ID	Device name	Client name	VPP Client User ID
b2be6837fb007c5b3018909b23bbcf9f3f54183d	FilePug ATV	FilePug ATV	3c0b6b21-dd81-4820-912e-1a485982f789
e4f84aa33be257b67dd6263092fbf6e65adb0375	Lab-DEP-tenshi	Lab-DEP-tenshi	efde2213-b108-4528-852d-5e78ab6efef2
442c1b5b22677c3137649e41bb013cc0a86111c9	lab-imac-alpha	lab-imac-alpha	9f52c6b4-6138-4d7f-9c09-4caf1198dea8
eb7e3f4f7d2e8451f128da800af0e24fb82b10d1	johnd-MBP13-DerKapitan	johnd-MBP13	20f26ab8-f937-465b-a701-d37d7acb6e57
b0d225dea7acd5c91d19adb6acd3a93b95331429	lab-iPad-W	lab-iPad-W	88498de3-8d5a-4c4f-89f2-7d15ba505edb

Last synchronization with VPP Web Service: 10/23/15 12:20 AM

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.



FileWave Admin Preferences

Volume Purchase Program

1 token(s) configured

Last synchronization with VPP Web service: 10/23/15 12:20 AM

Miminum delay (in minutes) between license assignment and Install Application. 1

Preferred license distribution model to use for new associations: Assign to Device

LDAP synchronization:

☑ Synchronize with LDAP every:

6 hour(s) Last synchronization with LDAP: 10/23/15 12:00 AM

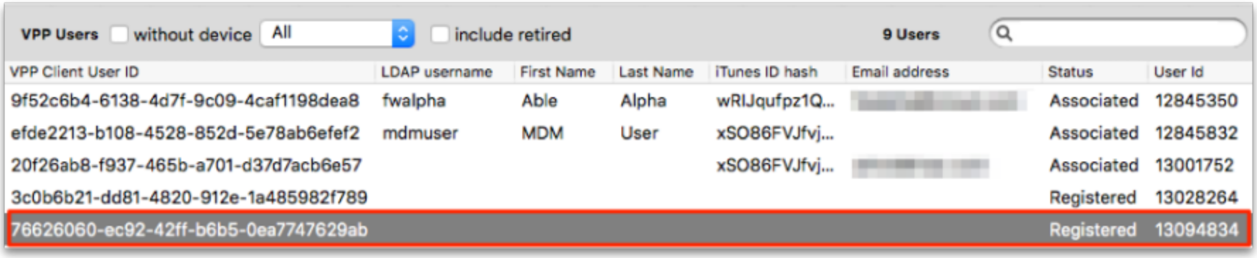
☑ Automatically associate users via their email address

☑ Send invite emails to newly registered LDAP users

The option 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.

Note: If you use only VPP device assignment, and do not assign licenses to any unique users, you will not need to work with the VPP User Management pane. FileWave assigns a "ghost" VPP user account to each device to handle device assignments. You cannot see these accounts and will not need to manage them.

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:



VPP Users □ without device All □ include retired 9 Users

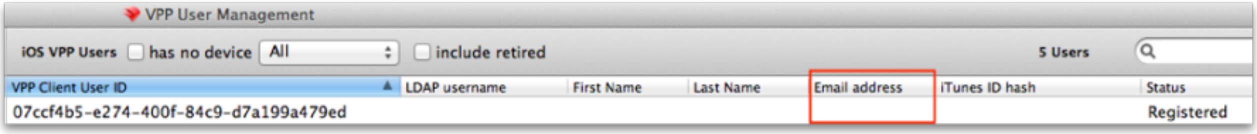
VPP Client User ID	LDAP username	First Name	Last Name	iTunes ID hash	Email address	Status	User Id
9f52c6b4-6138-4d7f-9c09-4caf1198dea8	fwalpha	Able	Alpha	wRIJqufpz1Q...	[redacted]	Associated	12845350
efde2213-b108-4528-852d-5e78ab6efef2	mdmuser	MDM	User	xSO86FVJfvj...		Associated	12845832
20f26ab8-f937-465b-a701-d37d7acb6e57				xSO86FVJfvj...	[redacted]	Associated	13001752
3c0b6b21-dd81-4820-912e-1a485982f789						Registered	13028264
76626060-ec92-42ff-b6b5-0ea7747629ab						Registered	13094834

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 Apple ID - 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 Apple ID 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 Apple ID 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/macOS devices to have a single VPP Client User ID associated with 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. LDAP authentication is covered in Chapter **3**.

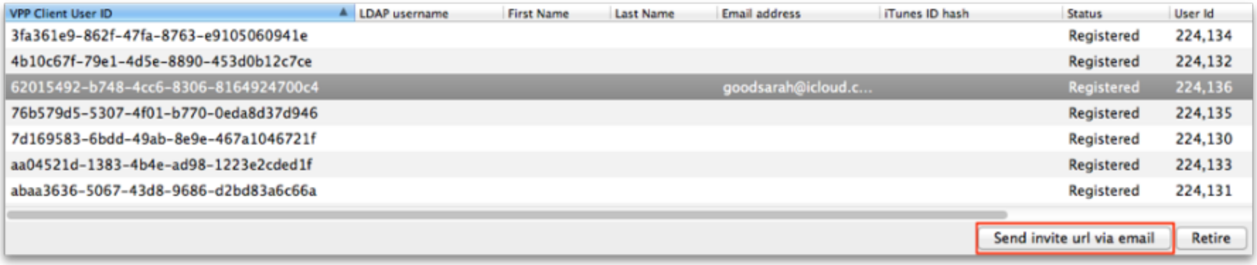
Inviting users to the FileWave MDM VPP

Apple requires the end user to actively link their Apple ID 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 Apple ID email address, just an address where the user can get a VPP MDM request.



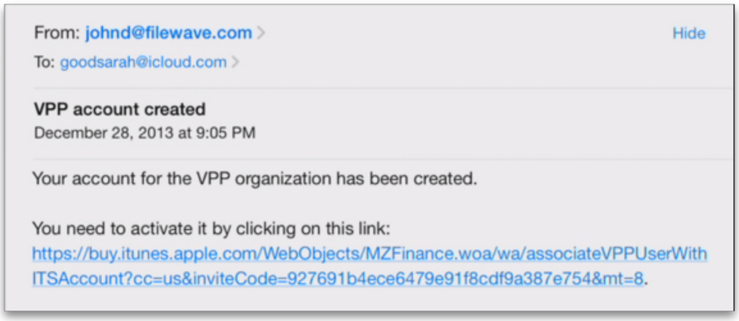
VPP Client User ID	LDAP username	First Name	Last Name	Email address	iTunes ID hash	Status
07ccf4b5-e274-400f-84c9-d7a199a479ed						Registered

Once you have entered a valid email address, the button to send an invite to the user will be active.



VPP Client User ID	LDAP username	First Name	Last Name	Email address	iTunes ID hash	Status	User Id
3fa361e9-862f-47fa-8763-e9105060941e						Registered	224,134
4b10c67f-79e1-4d5e-8890-453d0b12c7ce						Registered	224,132
62015492-b748-4cc6-8306-8164924700c4				goodsarah@icloud.c...		Registered	224,136
76b579d5-5307-4f01-b770-0eda8d37d946						Registered	224,135
7d169583-6bdd-49ab-8e9e-467a1046721f						Registered	224,130
aa04521d-1383-4b4e-ad98-1223e2cded1f						Registered	224,133
abaa3636-5067-43d8-9686-d2bd83a6c66a						Registered	224,131

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 Apple ID. It can be an internal email address used within your organization/institution, or any common email address the user may provide.



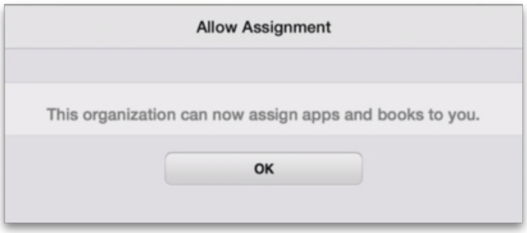
From: johnd@filewave.com
To: goodsarah@icloud.com

VPP account created
December 28, 2013 at 9:05 PM

Your account for the VPP organization has been created.

You need to activate it by clicking on this link:
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/associateVPPUserWithITSAccount?cc=us&inviteCode=927691b4ece6479e91f8cdf9a387e754&mt=8.

Once the user clicks on the link to the iTunes Store, authenticates with his or her Apple ID, and gives permission, the user will get notified that he/she can now be provided with content from your FileWave MDM.



Allow Assignment

This organization can now assign apps and books to you.

This process links that user's Apple ID to your FileWave MDM so that you can assign applications and content to them. You will never see the user's Apple ID (unless they give you the email account they use for their Apple ID as their contact email). What you will see, as proof that this has occurred, is an iTunes ID hash in the VPP User Management window.
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. When the user opens the App Portal he/she will be greeted with a dialog asking them to register their Apple ID: This is just like the above process; i.e., they authenticate to the iTunes Store and give permission for the linkage.

FileWave and macOS VPP users

The process for macOS computers and users is almost identical to that of iOS users. When you add an macOS computer as a FileWave Client, it

will show up in the **Manage VPP Users…** window.
Note: Direct device assignment is still an "in-progress" thing with OS X. Full functionality from Apple will be available in a future release.
You still have to go through the user assignment process 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

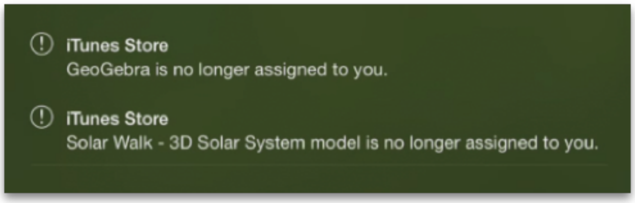
Note: If you retire a VPP user account, it <u>cannot</u> be used again. We suggest that you DO NOT test "retiring" VPP user accounts on actively enrolled users.

Where OS X VPP differs

One key difference between iOS and macOS 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 the installation manually.
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.

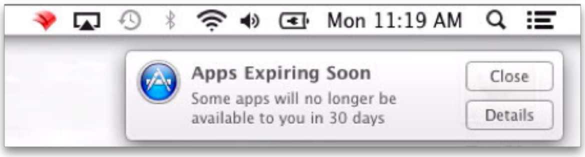
Revoking licenses using FileWave MDM with VPP managed distribution

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 that 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.
Note: macOS X computers 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 macOS device associated with your VPP system, you may see notifications pop up on the iOS device before the macOS computer gets the word.



iTunes Store
GeoGebra is no longer assigned to you.

iTunes Store
Solar Walk - 3D Solar System model is no longer assigned to you.

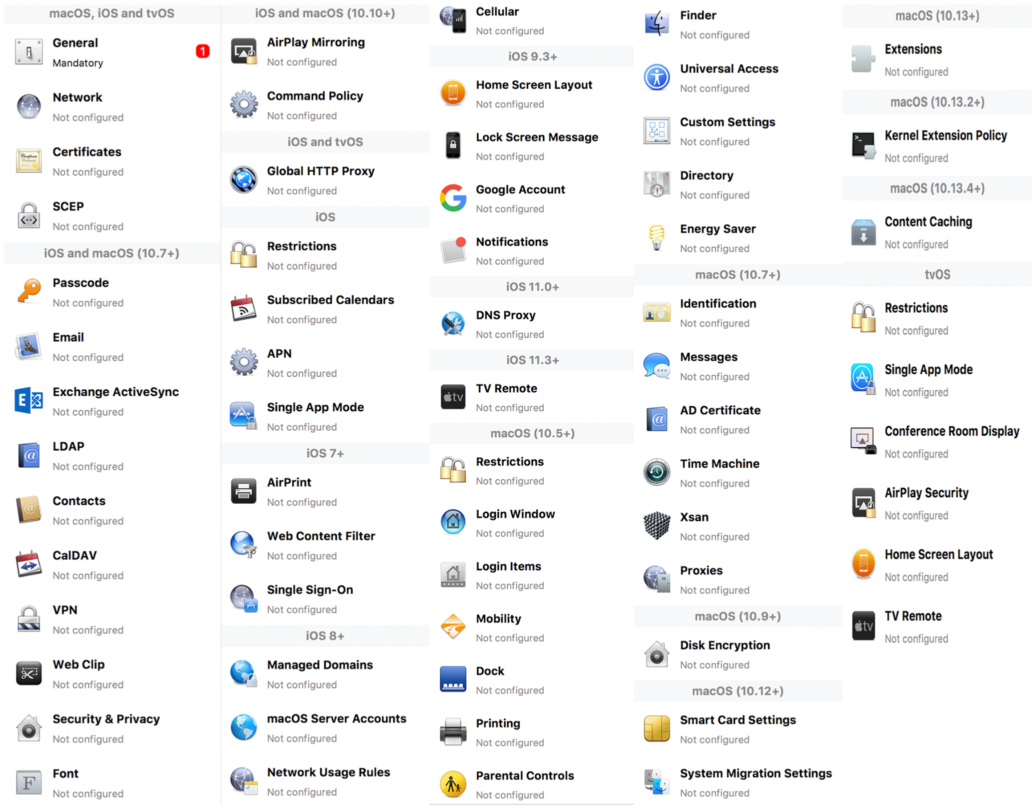


Apps Expiring Soon
Some apps will no longer be available to you in 30 days

7. Mobile Device Management (MDM)
FileWave supports both iOS and macOS management through its Profile Editor. Android and Windows management is handled through Filesets.

7.1. Profile Editor details

The primary management tool for client management / MDM on iOS and macOS X is the Profile Editor. It can be accessed through either the Desktop Fileset or Mobile Fileset tool.



macOS, iOS and tvOS

General 1

Mandatory

Network

Not configured

Certificates

Not configured

SCEP

Not configured

iOS and macOS (10.7+)

Passcode

Not configured

Email

Not configured

Exchange ActiveSync

Not configured

LDAP

Not configured

Contacts

Not configured

CalDAV

Not configured

VPN

Not configured

Web Clip

Not configured

Security & Privacy

Not configured

Font

Not configured

iOS and macOS (10.10+)

AirPlay Mirroring

Not configured

Command Policy

Not configured

iOS and tvOS

Global HTTP Proxy

Not configured

iOS

Restrictions

Not configured

Subscribed Calendars

Not configured

APN

Not configured

Single App Mode

Not configured

iOS 7+

AirPrint

Not configured

Web Content Filter

Not configured

Single Sign-On

Not configured

iOS 8+

Managed Domains

Not configured

macOS Server Accounts

Not configured

Network Usage Rules

Not configured

Cellular

Not configured

iOS 9.3+

Home Screen Layout

Not configured

Lock Screen Message

Not configured

Google Account

Not configured

Notifications

Not configured

iOS 11.0+

DNS Proxy

Not configured

iOS 11.3+

TV Remote

Not configured

macOS (10.5+)

Restrictions

Not configured

Login Window

Not configured

Login Items

Not configured

Mobility

Not configured

Dock

Not configured

Printing

Not configured

Parental Controls

Not configured

Finder

Not configured

Universal Access

Not configured

Custom Settings

Not configured

Directory

Not configured

Energy Saver

Not configured

macOS (10.7+)

Identification

Not configured

Messages

Not configured

AD Certificate

Not configured

Time Machine

Not configured

Xsan

Not configured

Proxies

Not configured

macOS (10.9+)

Disk Encryption

Not configured

macOS (10.12+)

Smart Card Settings

Not configured

System Migration Settings

Not configured

macOS (10.13+)

Extensions

Not configured

macOS (10.13.2+)

Kernel Extension Policy

Not configured

macOS (10.13.4+)

Content Caching

Not configured

tvOS

Restrictions

Not configured

Single App Mode

Not configured

Conference Room Display

Not configured

AirPlay Security

Not configured

Home Screen Layout

Not configured

TV Remote

Not configured

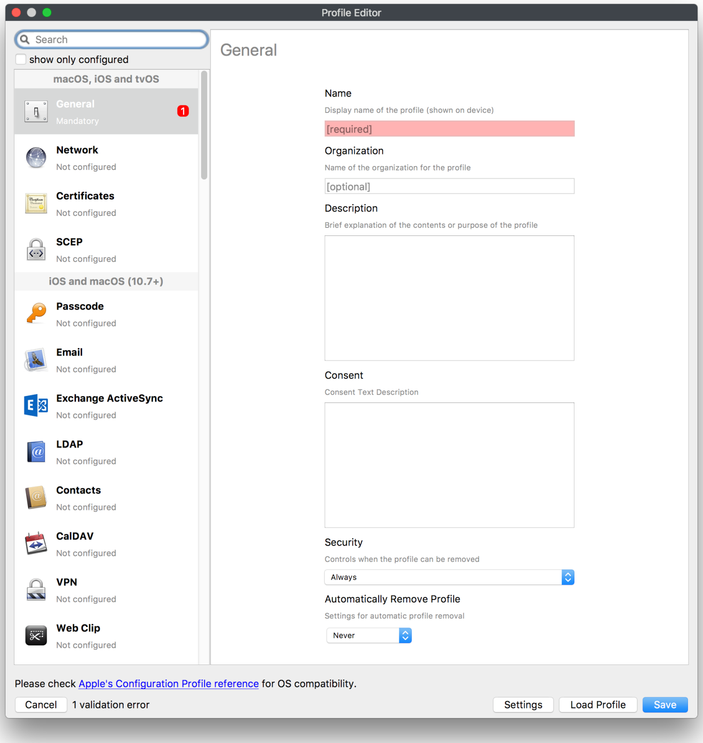
Search and Show only configured (FW 10+)

Two features introduced in FileWave 10 are a search field to locate specific settings and the ability to display only the configured payloads in a profile.

macOS, iOS and tvOS

General

The first item encountered in Profile Editor is the **General** settings. This is not a profile nor payload type; it's 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 descriptive name in the General settings. The key settings to note are the **Name, Security** and **Automatically Remove Profile**. All other General settings are optional. 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. Users on unsupervised iOS devices can remove profiles regardless of the settings here.



General

Name
Display name of the profile (shown on device)
[required]

Organization
Name of the organization for the profile
[optional]

Description
Brief explanation of the contents or purpose of the profile

Consent
Consent Text Description

Security
Controls when the profile can be removed
Always

Automatically Remove Profile
Settings for automatic profile removal
Never

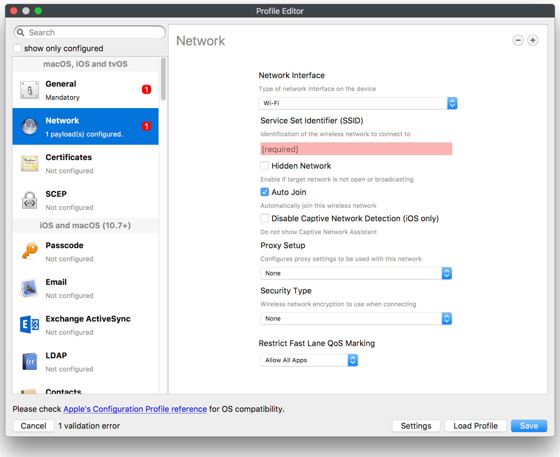
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Note: Due to changes in how profiles are installed on OS X 10.10+, if you install a profile with Security set to *Never,* FileWave will not be able to remove the profile and will ask for admin credentials on the client machines. The workaround is to use a password protected removal using the *With Authorization* option.

Automatically Remove Profile settings will disable the profile after a specific time interval or on a specific date. The recommendation is to leave this set to *Never* and use FileWave to remove the profile when necessary. The **Description** and **Consent** fields are 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, however.

Network



Network

Network Interface
Type of network interface on the device
Wi-Fi

Service Set Identifier (SSID)
Identification of the wireless network to connect to
[required]

□ Hidden Network
Enable if target network is not open or broadcasting

☑ Auto Join
Automatically join this wireless network

□ Disable Captive Network Detection (iOS only)
Do not show Captive Network Assistant

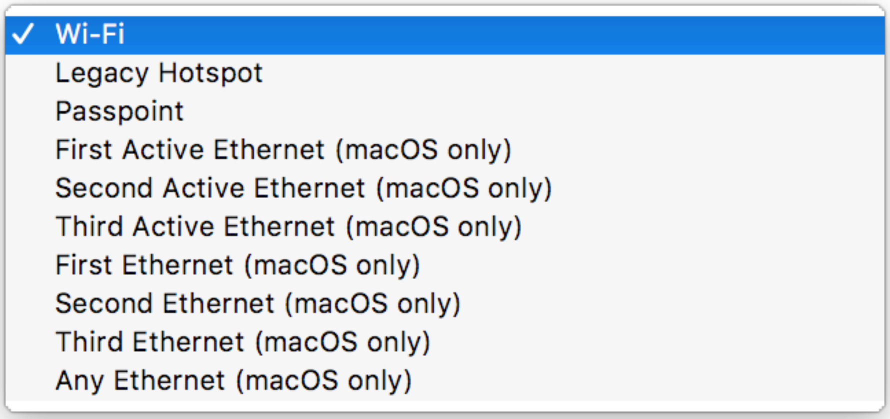
Proxy Setup
Configures proxy settings to be used with this network
None

Security Type
Wireless network encryption to use when connecting
None

Restrict Fast Lane QoS Marking
Allow All Apps

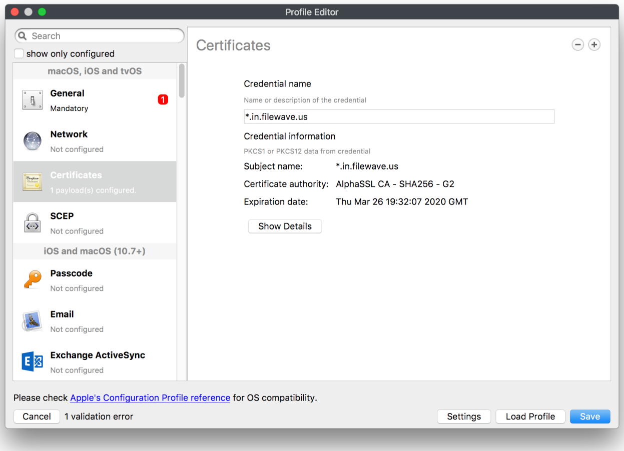
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error


✓ Wi-Fi
Legacy Hotspot
Passpoint
First Active Ethernet (macOS only)
Second Active Ethernet (macOS only)
Third Active Ethernet (macOS only)
First Ethernet (macOS only)
Second Ethernet (macOS only)
Third Ethernet (macOS only)
Any Ethernet (macOS only)

This payload allows you to preconfigure network settings for your devices. You can define Wi-Fi, Legacy Hotspot, Passpoint, or Ethernet (macOS only) settings, including Auto Join, Proxy, Wi-Fi Security, and 802.1x.

Certificates



Certificates

Credential name

Name or description of the credential

*.in.filewave.us

Credential information

PKCS1 or PKCS12 data from credential

Subject name: *.in.filewave.us

Certificate authority: AlphaSSL CA - SHA256 - G2

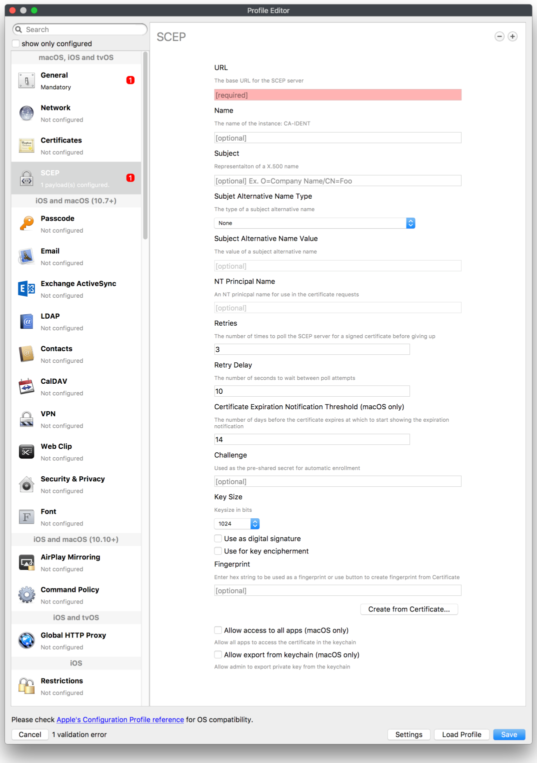
Expiration date: Thu Mar 26 19:32:07 2020 GMT

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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



SCEP

URL
The base URL for the SCEP server
[required]

Name
The name of the instance: CA-IDENT
[optional]

Subject
Representaiton of a X.500 name
[optional] Ex. O=Company Name/CN=Foo

Subjet Alternative Name Type
The type of a subject alternative name
None

Subject Alternative Name Value
The value of a subject alternative name
[optional]

NT Principal Name
An NT prinicpal name for use in the certificate requests
[optional]

Retries
The number of times to poll the SCEP server for a signed certificate before giving up
3

Retry Delay
The number of seconds to wait between poll attempts
10

Certificate Expiration Notification Threshold (macOS only)
The number of days before the certificate expires at which to start showing the expiration notification
14

Challenge
Used as the pre-shared secret for automatic enrollment
[optional]

Key Size
Keysize in bits
1024

☐ Use as digital signature
☐ Use for key encipherment

Fingerprint
Enter hex string to be used as a fingerprint or use button to create fingerprint from Certificate
[optional]

☐ Allow access to all apps (macOS only)
Allow all apps to access the certificate in the keychain

☐ Allow export from keychain (macOS only)
Allow admin to export private key from the keychain

Please check Apple's Configuration Profile reference for OS compatibility.

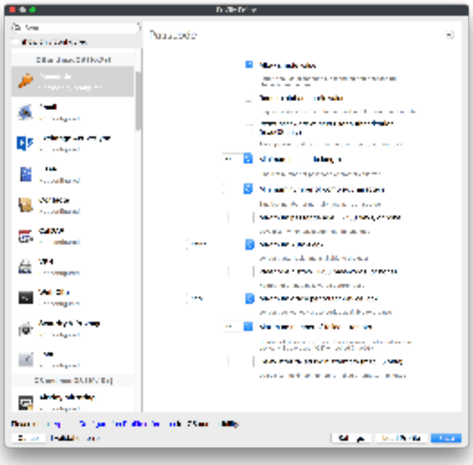
1 validation error

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.

iOS and macOS (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.

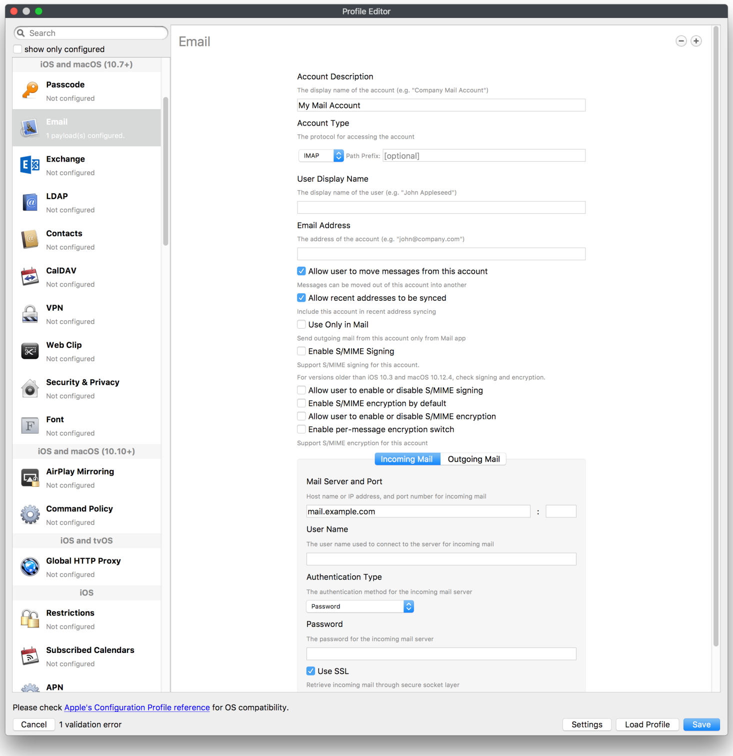
Passcode



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

Account Description

The display name of the account (e.g. "Company Mail Account")

My Mail Account

Account Type

The protocol for accessing the account

IMAP Path Prefix: [optional]

User Display Name

The display name of the user (e.g. "John Appleseed")

Email Address

The address of the account (e.g. "john@company.com")

☑ Allow user to move messages from this account

Messages can be moved out of this account into another

☑ Allow recent addresses to be synced

Include this account in recent address syncing

□ Use Only in Mail

Send outgoing mail from this account only from Mail app

□ Enable S/MIME Signing

Support S/MIME signing for this account.

For versions older than iOS 10.3 and macOS 10.12.4, check signing and encryption.

□ Allow user to enable or disable S/MIME signing

□ Enable S/MIME encryption by default

□ Allow user to enable or disable S/MIME encryption

□ Enable per-message encryption switch

Support S/MIME encryption for this account

Incoming Mail | Outgoing Mail

Mail Server and Port

Host name or IP address, and port number for incoming mail

mail.example.com :

User Name

The user name used to connect to the server for incoming mail

Authentication Type

The authentication method for the incoming mail server

Password

Password

The password for the incoming mail server

☑ Use SSL

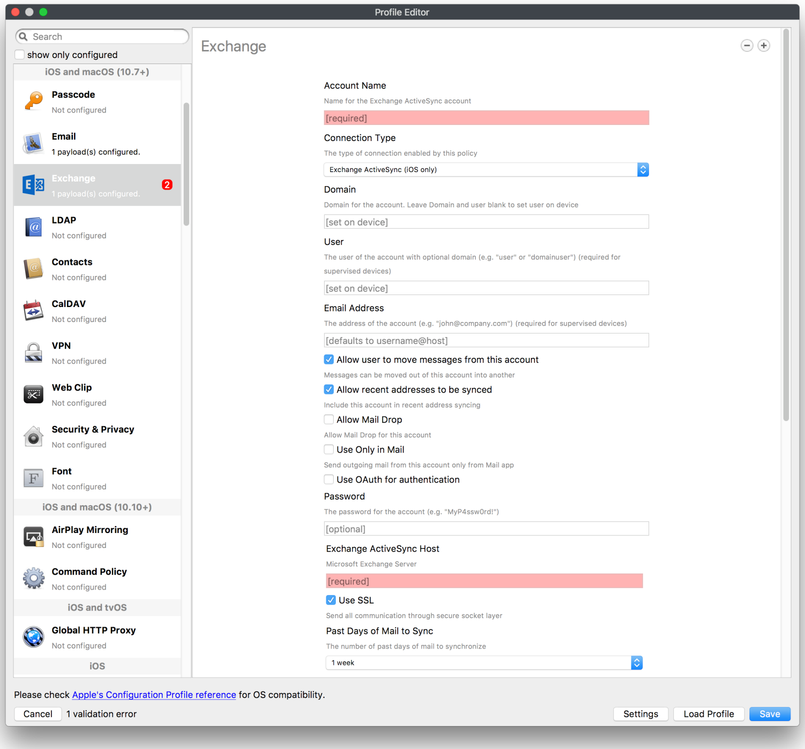
Retrieve incoming mail through secure socket layer

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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

Account Name
Name for the Exchange ActiveSync account
[required]

Connection Type
The type of connection enabled by this policy
Exchange ActiveSync (iOS only)

Domain
Domain for the account. Leave Domain and user blank to set user on device
[set on device]

User
The user of the account with optional domain (e.g. "user" or "domainuser") (required for supervised devices)
[set on device]

Email Address
The address of the account (e.g. "john@company.com") (required for supervised devices)
[defaults to username@host]

☑ Allow user to move messages from this account
Messages can be moved out of this account into another

☑ Allow recent addresses to be synced
Include this account in recent address syncing

□ Allow Mail Drop
Allow Mail Drop for this account

□ Use Only in Mail
Send outgoing mail from this account only from Mail app

□ Use OAuth for authentication

Password
The password for the account (e.g. "MyP4ssw0rd!")
[optional]

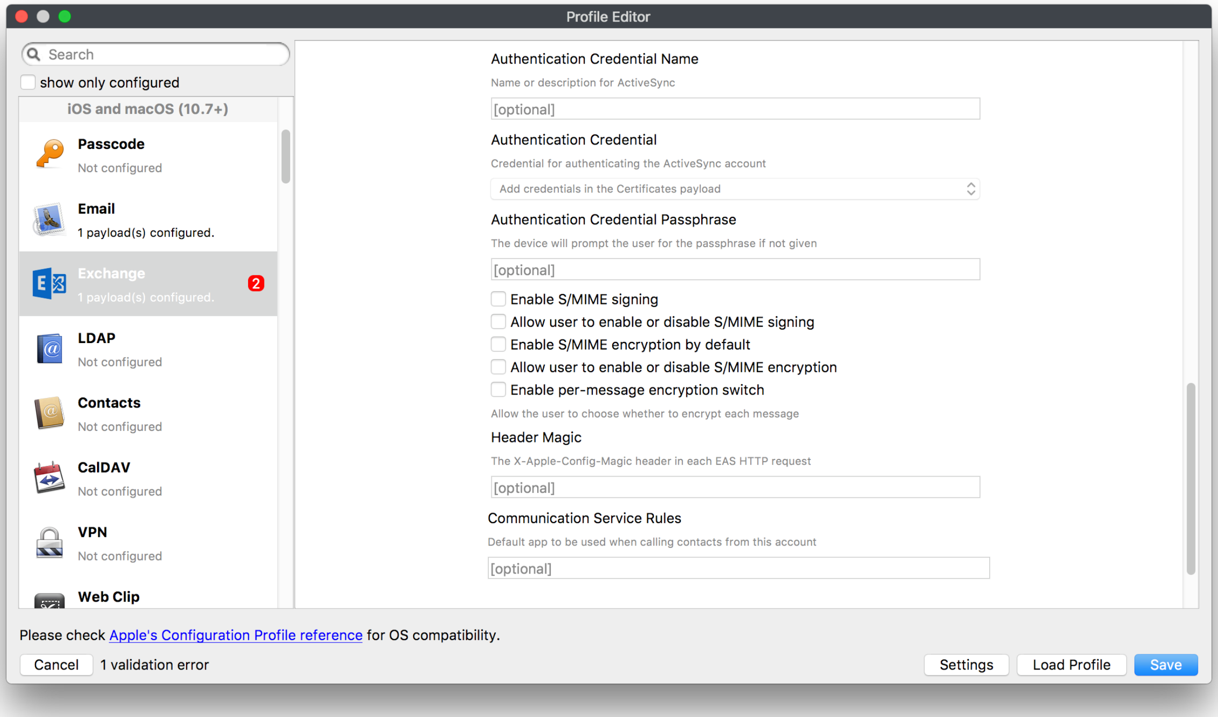
Exchange ActiveSync Host
Microsoft Exchange Server
[required]

☑ Use SSL
Send all communication through secure socket layer

Past Days of Mail to Sync
The number of past days of mail to synchronize
1 week

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Authentication Credential Name
Name or description for ActiveSync
[optional]

Authentication Credential
Credential for authenticating the ActiveSync account
Add credentials in the Certificates payload

Authentication Credential Passphrase
The device will prompt the user for the passphrase if not given
[optional]

□ Enable S/MIME signing
□ Allow user to enable or disable S/MIME signing
□ Enable S/MIME encryption by default
□ Allow user to enable or disable S/MIME encryption
□ Enable per-message encryption switch
Allow the user to choose whether to encrypt each message

Header Magic
The X-Apple-Config-Magic header in each EAS HTTP request
[optional]

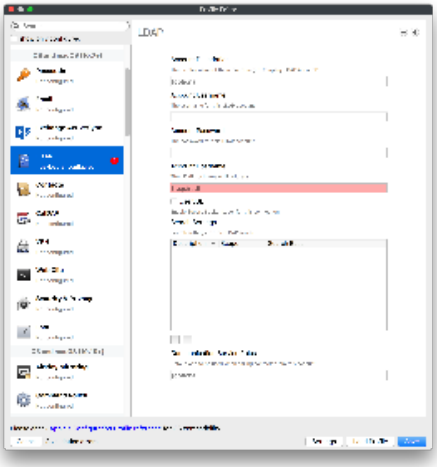
Communication Service Rules
Default app to be used when calling contacts from this account
[optional]

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

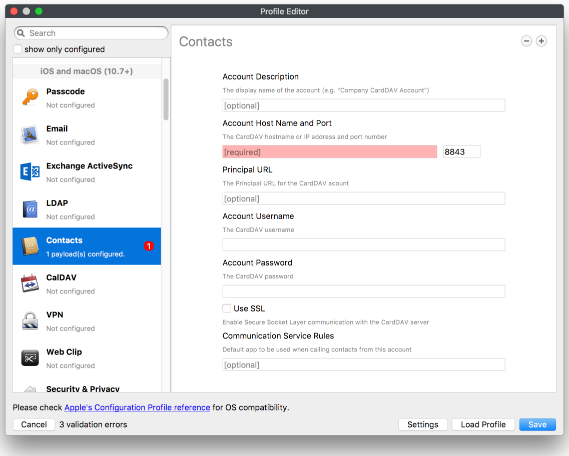
Exchange ActiveSync is a payload that lets you predefine settings for users' access to Microsoft Exchange services. New with FileWave 11's support for iOS 9.3 is an "Allow Mail Drop" option for the Exchange payload (Mail Drop lets you send large files like videos, presentations, and images through iCloud. For more info, see: https://support.apple.com/en-us/HT203093.

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 macOS computers, use the Directory payload for binding.

Contacts



Contacts

Account Description
The display name of the account (e.g. "Company CardDAV Account")
[optional]

Account Host Name and Port
The CardDAV hostname or IP address and port number
[required] 8843

Principal URL
The Principal URL for the CardDAV acount
[optional]

Account Username
The CardDAV username

Account Password
The CardDAV password

□ Use SSL
Enable Secure Socket Layer communication with the CardDAV server

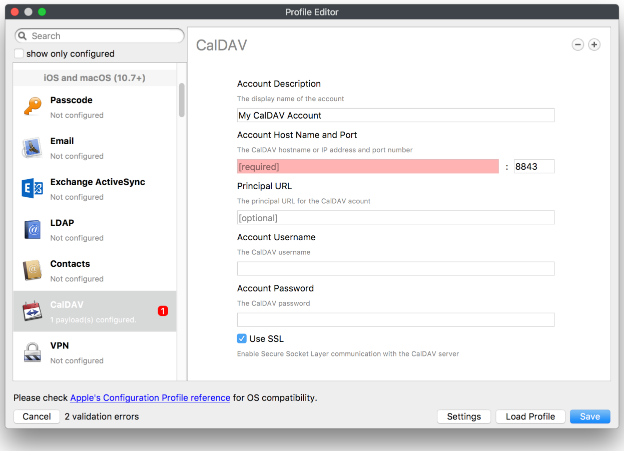
Communication Service Rules
Default app to be used when calling contacts from this account
[optional]

Please check Apple's Configuration Profile reference for OS compatibility.

3 validation errors

The Contacts payload provides settings to allow access to CardDAV servers. This payload supports parameterized profiles.

CalDAV



Account Description
The display name of the account
My CalDAV Account

Account Host Name and Port
The CalDAV hostname or IP address and port number
[required] : 8843

Principal URL
The principal URL for the CalDAV acount
[optional]

Account Username
The CalDAV username

Account Password
The CalDAV password

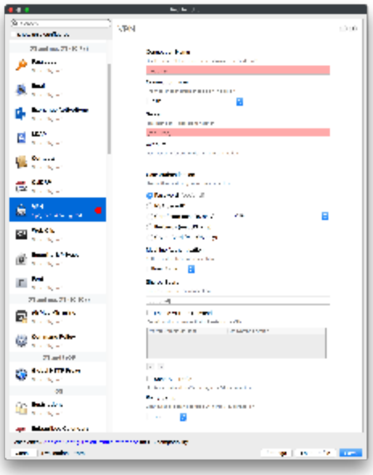
☑ Use SSL
Enable Secure Socket Layer communication with the CalDAV server

Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

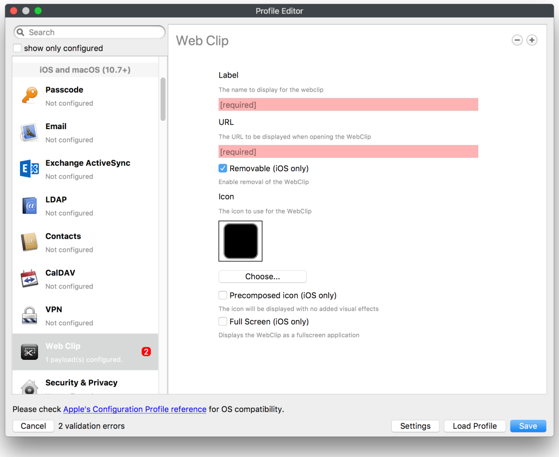
The CalDAV payload provides settings for access to CalDAV (Calendar) servers. This payload supports parameterized profiles.

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 VPN.

Web Clip



Label
The name to display for the webclip
[required]

URL
The URL to be displayed when opening the WebClip
[required]

☑ Removable (iOS only)
Enable removal of the WebClip

Icon
The icon to use for the WebClip

□ Precomposed icon (iOS only)
The icon will be displayed with no added visual effects

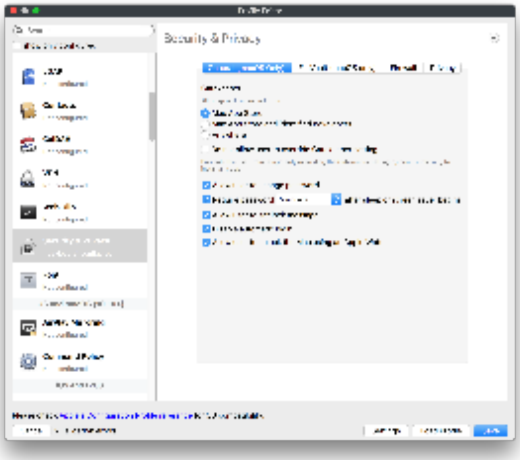
□ Full Screen (iOS only)
Displays the WebClip as a fullscreen application

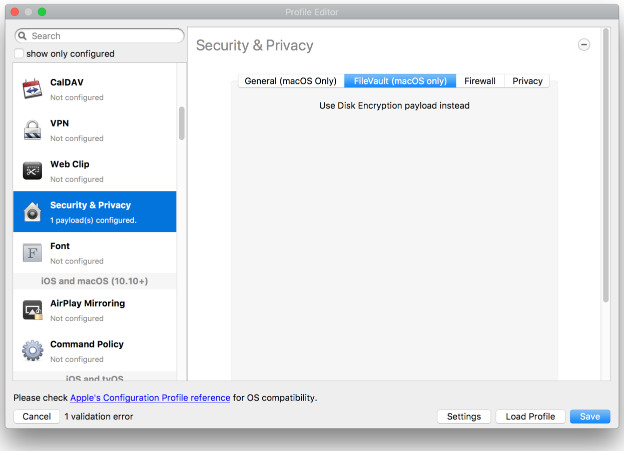
Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

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 macOS.

Security & Privacy

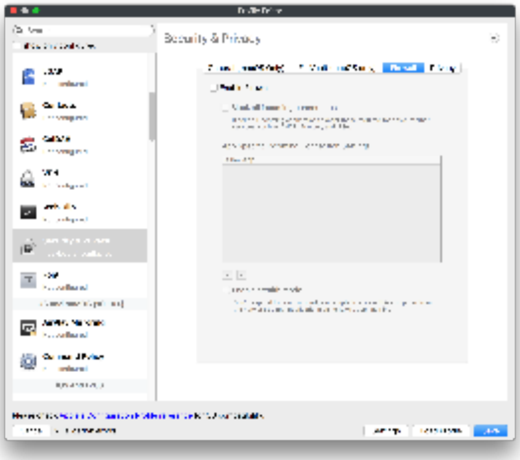


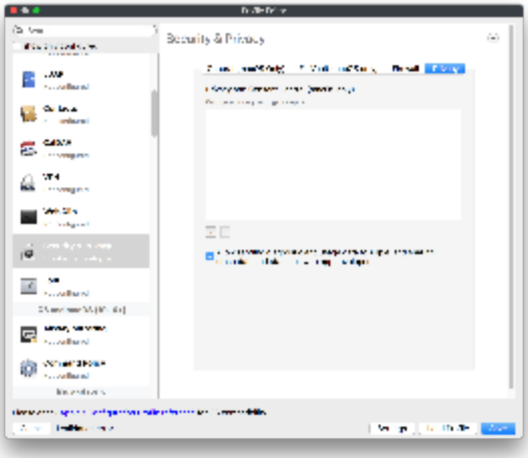


Use Disk Encryption payload instead

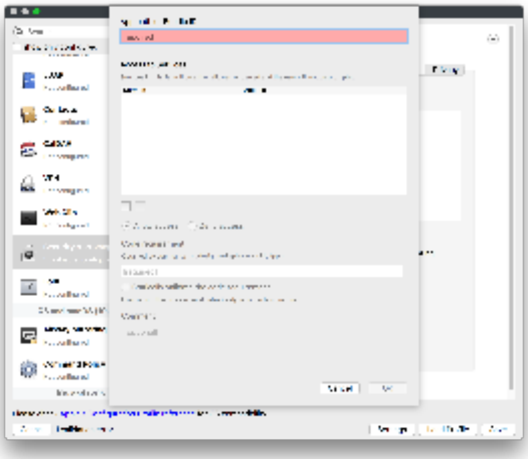
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



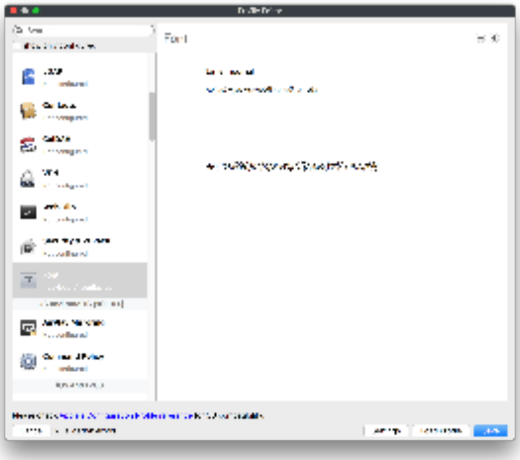


Security & Privacy



The Security & Privacy payload allows managed devices to be configured with access to specific sources for application downloads (macOS only Gatekeeper), Firewall settings, and specify if diagnostic information will be sent to Apple or not.
FileVault 2 settings are can be configured using the **Disk Encryption** payload.

Font



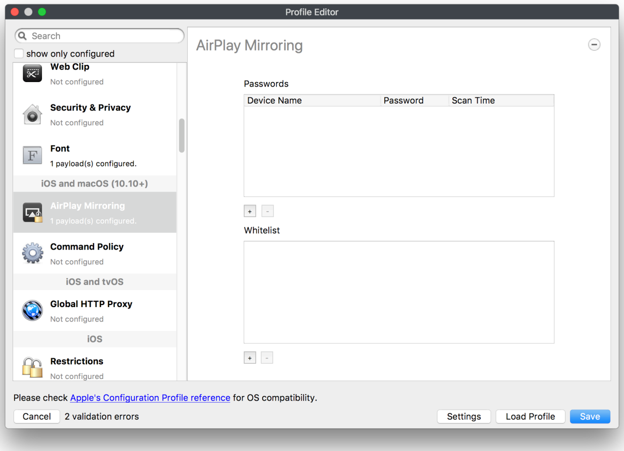
Font

The Font payload allows you send a specific font set to a device. This capability is very handy for insuring an iOS device has the same font installed for a document that is also being worked on with macOS computes.

iOS and macOS (10.10+)

This payload is for iOS and macOS

AirPlay Mirroring



AirPlay Mirroring

Passwords

Device Name	Password	Scan Time

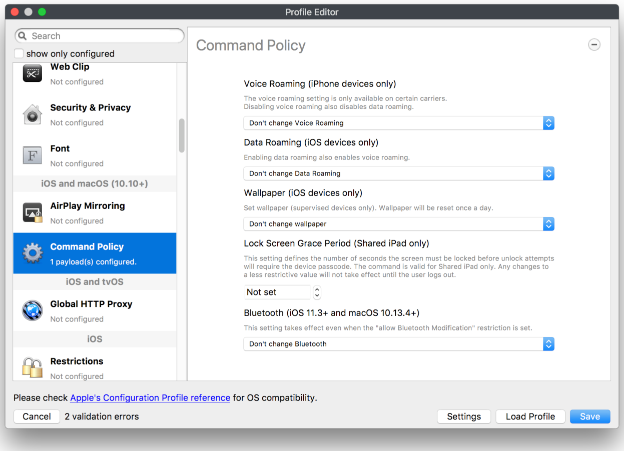
Whitelist

Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

AirPlay Mirroring payloads are for assignment of specific AirPlay devices to designated Apple TVs. A Group of iOS devices can be assigned to a certain Apple TV with the password imbedded in the profile. Other devices would not be able to connect to that Apple TV. You can also provide a set of whitelisted Apple TVs that the managed device can use for AirPlay.

Command Policy



Command Policy

Voice Roaming (iPhone devices only)

The voice roaming setting is only available on certain carriers.
Disabling voice roaming also disables data roaming.

Don't change Voice Roaming

Data Roaming (iOS devices only)

Enabling data roaming also enables voice roaming.

Don't change Data Roaming

Wallpaper (iOS devices only)

Set wallpaper (supervised devices only). Wallpaper will be reset once a day.

Don't change wallpaper

Lock Screen Grace Period (Shared iPad only)

This setting defines the number of seconds the screen must be locked before unlock attempts will require the device passcode. The command is valid for Shared iPad only. Any changes to a less restrictive value will not take effect until the user logs out.

Not set

Bluetooth (iOS 11.3+ and macOS 10.13.4+)

This setting takes effect even when the "allow Bluetooth Modification" restriction is set.

Don't change Bluetooth

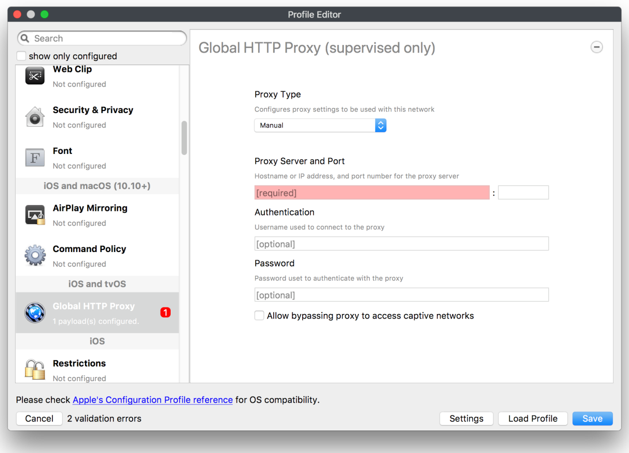
Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

These settings determine the voice and data roaming, Wallpaper, Lock Screen Grace Period, or Bluetooth. The commands are sent at each *Verify* from FileWave.

iOS and tvOS

Global HTTP Proxy



Global HTTP Proxy (supervised only)

Proxy Type
Configures proxy settings to be used with this network
Manual

Proxy Server and Port
Hostname or IP address, and port number for the proxy server
[required] :

Authentication
Username used to connect to the proxy
[optional]

Password
Password uset to authenticate with the proxy
[optional]

□ Allow bypassing proxy to access captive networks

Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

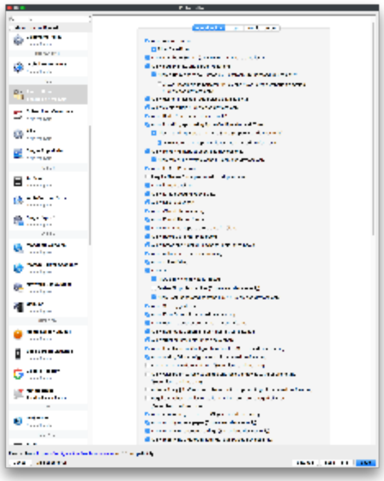
Global HTTP Proxy payload settings allow supervised iOS devices to be linked to a master network proxy for web content.

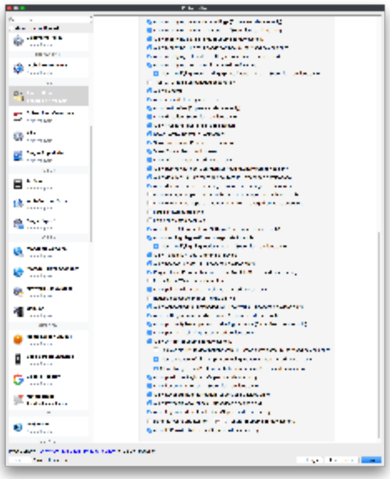
iOS

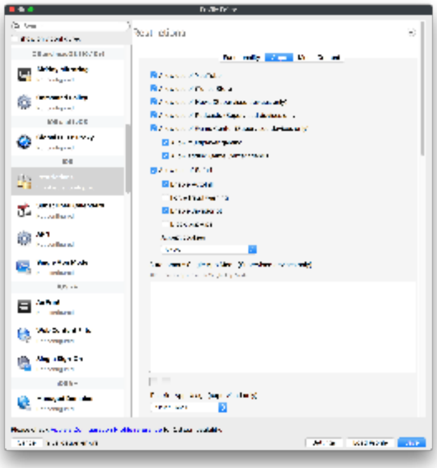
These payloads apply to all supported iOS devices.

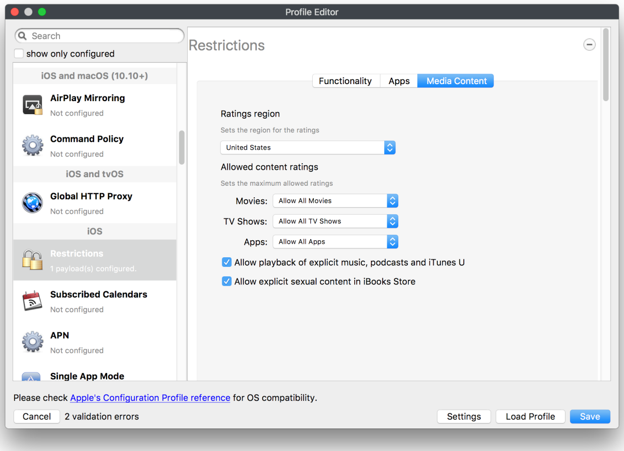
Restrictions

Restrictions allow for the establishment of tight controls over institutional iOS devices, and can be used for managing BYOD/1:1 devices. 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. Note that many of the settings require the device to be supervised. That means the device must be institutionally purchased and configured with either DEP, or with Apple Configurator.









Restrictions

Ratings region

Sets the region for the ratings

United States

Allowed content ratings

Sets the maximum allowed ratings

Movies: Allow All Movies

TV Shows: Allow All TV Shows

Apps: Allow All Apps

☑ Allow playback of explicit music, podcasts and iTunes U

☑ Allow explicit sexual content in iBooks Store

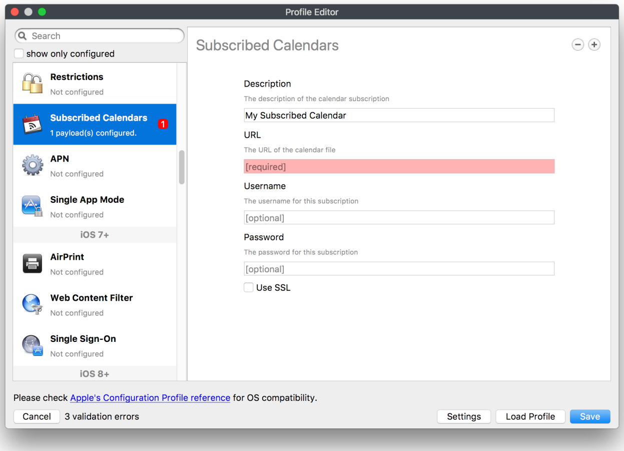
Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

New with FileWave 11's support for iOS 9.3 are the following restrictions, which apply to supervised devices:

- *Allow Apple Music* — If set to false, Music service is disabled and Music app reverts to classic mode. Defaults to true.
- *Allow Radio* — If set to false, iTunes Radio is disabled. Defaults to true.
- *Restrict App Usage*:
    - Allow All Apps
    - Allow Some Apps Only, where you can specify what apps are allowed
    - Don't Allow Some Apps, where you can specify what apps are not allowed

Subscribed Calendars



Subscribed Calendars

Description
The description of the calendar subscription
My Subscribed Calendar

URL
The URL of the calendar file
[required]

Username
The username for this subscription
[optional]

Password
The password for this subscription
[optional]

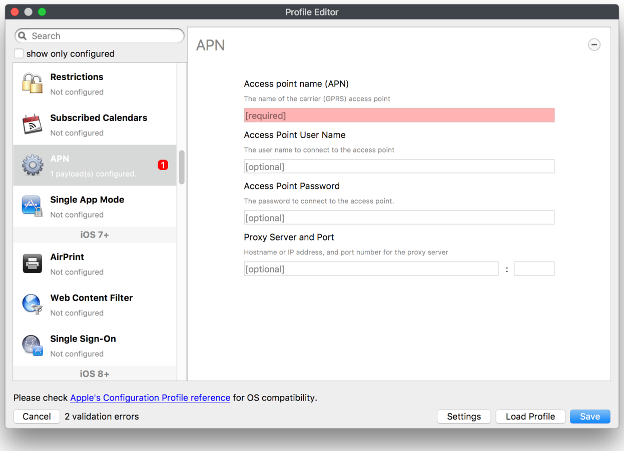
□ Use SSL

Please check Apple's Configuration Profile reference for OS compatibility.

3 validation errors

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



APN

Access point name (APN)
The name of the carrier (GPRS) access point
[required]

Access Point User Name
The user name to connect to the access point
[optional]

Access Point Password
The password to connect to the access point.
[optional]

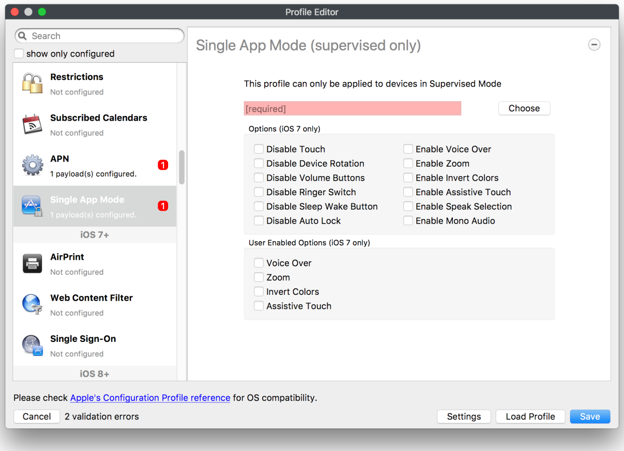
Proxy Server and Port
Hostname or IP address, and port number for the proxy server
[optional] :

Please check Apple's Configuration Profile reference for OS compatibility.

2 validation errors

The APN payload allows systems administrators the ability to manage Carrier Access Point Name configuration for iOS devices with cellular services enabled.

Single App Mode



Single App Mode (supervised only)

This profile can only be applied to devices in Supervised Mode

[required]

Options (iOS 7 only)

□ Disable Touch □ Enable Voice Over
□ Disable Device Rotation □ Enable Zoom
□ Disable Volume Buttons □ Enable Invert Colors
□ Disable Ringer Switch □ Enable Assistive Touch
□ Disable Sleep Wake Button □ Enable Speak Selection
□ Disable Auto Lock □ Enable Mono Audio

User Enabled Options (iOS 7 only)

□ Voice Over
□ Zoom
□ Invert Colors
□ Assistive Touch

Please check Apple's Configuration Profile reference for OS compatibility.

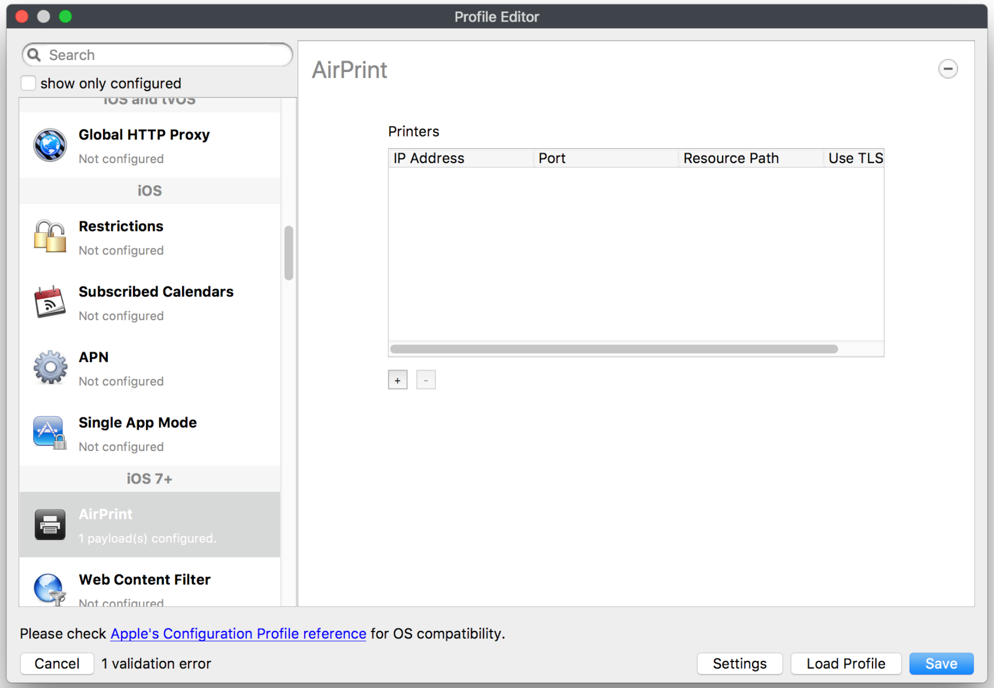
2 validation errors

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 in testing or kiosk environments. Setup requires the use of Apple Configurator to force the device into supervised mode. The payload also allows 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 iOS 7 and higher.

AirPrint



AirPrint

Printers

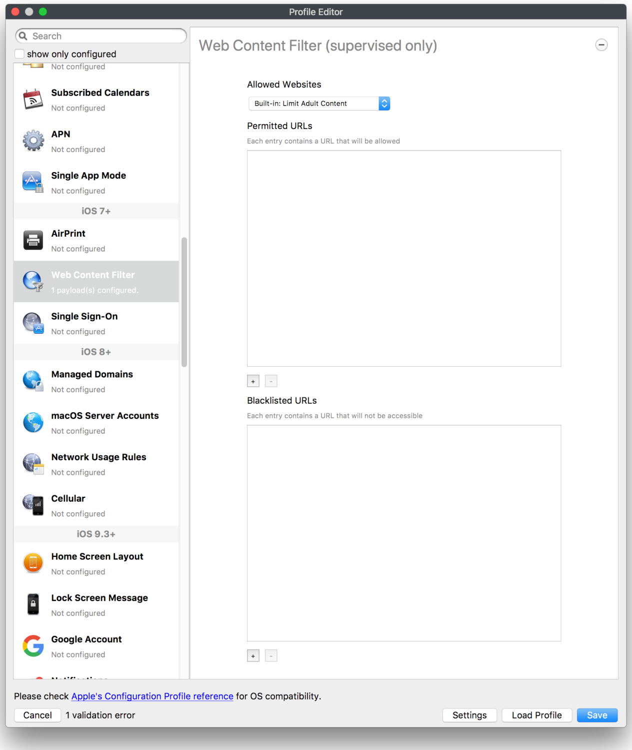
IP Address	Port	Resource Path	Use TLS

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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 (supervised only)



Web Content Filter (supervised only)

Allowed Websites

Built-in: Limit Adult Content

Permitted URLs

Each entry contains a URL that will be allowed

Blacklisted URLs

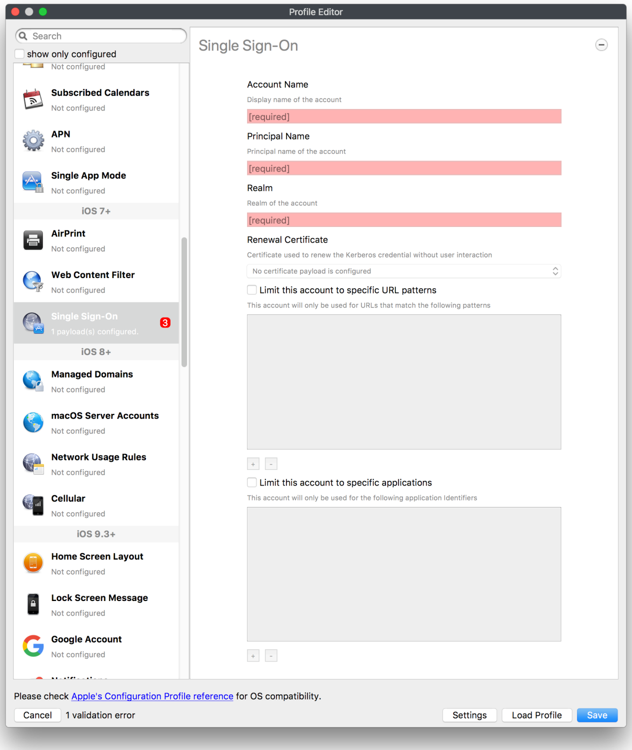
Each entry contains a URL that will not be accessible

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

The Web Content Filter payload supports whitelists and blacklists for web access, as well as setting a basic content filter to control access to adult content.

Single Sign-On



Single Sign-On

Account Name

Display name of the account

[required]

Principal Name

Principal name of the account

[required]

Realm

Realm of the account

[required]

Renewal Certificate

Certificate used to renew the Kerberos credential without user interaction

No certificate payload is configured

□ Limit this account to specific URL patterns

This account will only be used for URLs that match the following patterns

□ Limit this account to specific applications

This account will only be used for the following application identifiers

Please check Apple's Configuration Profile reference for OS compatibility.

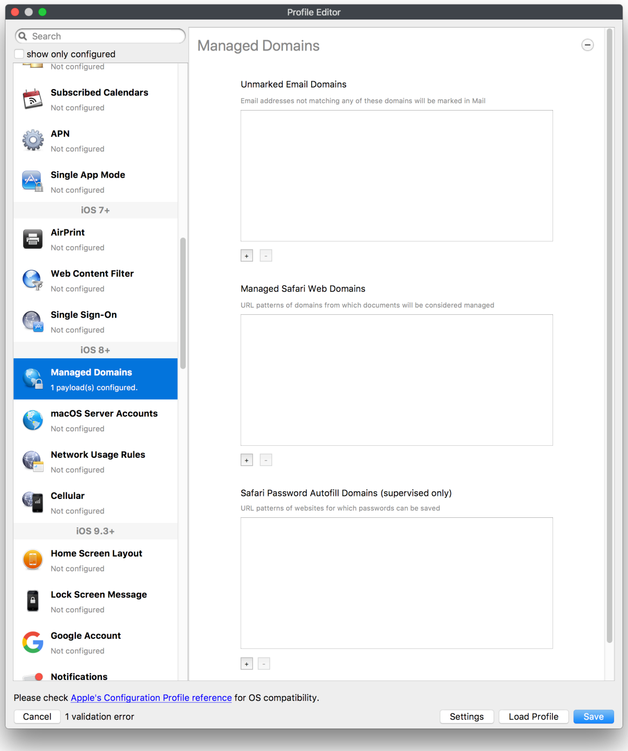
1 validation error

The Single Sign-On (SSO) payload allows you to configure Kerberos access for your managed device to specific services and applications.

iOS 8+

These settings are for iOS 8 or higher only.

Managed Domains



Unmarked Email Domains

Email addresses not matching any of these domains will be marked in Mail

Managed Safari Web Domains

URL patterns of domains from which documents will be considered managed

Safari Password Autofill Domains (supervised only)

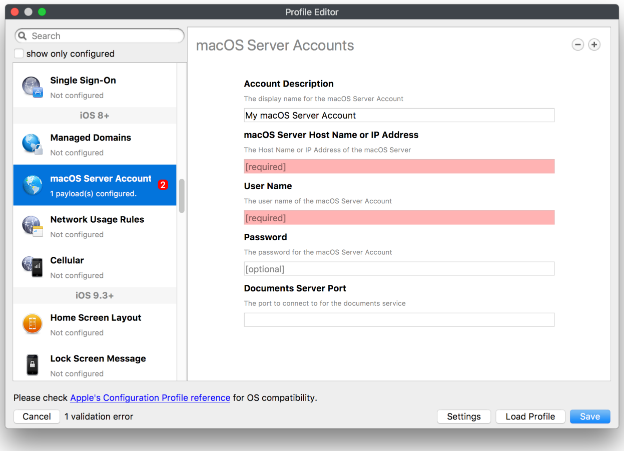
URL patterns of websites for which passwords can be saved

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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. New with FileWave 11 and iOS 9.3 is the ability to specify the URL patterns fro which passwords can be saved for supervised devices.

macOS Server Accounts



macOS Server Accounts

Account Description
The display name for the macOS Server Account
My macOS Server Account

macOS Server Host Name or IP Address
The Host Name or IP Address of the macOS Server
[required]

User Name
The user name of the macOS Server Account
[required]

Password
The password for the macOS Server Account
[optional]

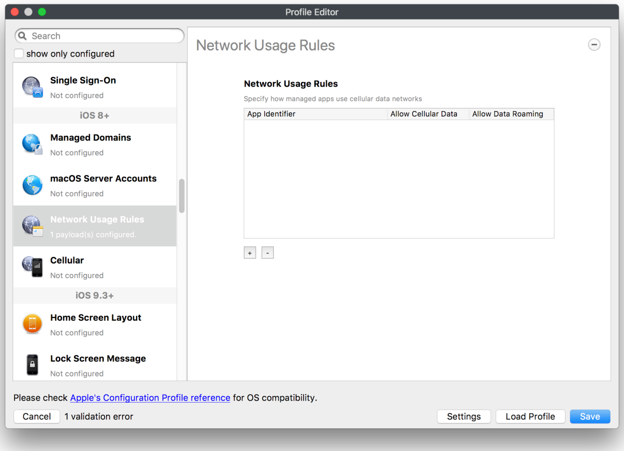
Documents Server Port
The port to connect to for the documents service

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

These settings allow you to pre-configure macOS file servers for access by managed users.

Network Usage Rules



Network Usage Rules

Network Usage Rules
Specify how managed apps use cellular data networks

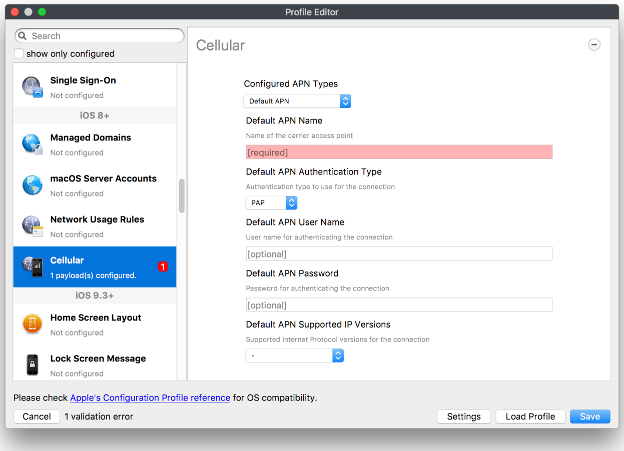
App Identifier	Allow Cellular Data	Allow Data Roaming

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

These setting specify how managed apps use cellular data networks.

Cellular



Cellular

Configured APN Types
Default APN

Default APN Name
Name of the carrier access point
[required]

Default APN Authentication Type
Authentication type to use for the connection
PAP

Default APN User Name
User name for authenticating the connection
[optional]

Default APN Password
Password for authenticating the connection
[optional]

Default APN Supported IP Versions
Supported Internet Protocol versions for the connection
-

Please check Apple's Configuration Profile reference for OS compatibility.

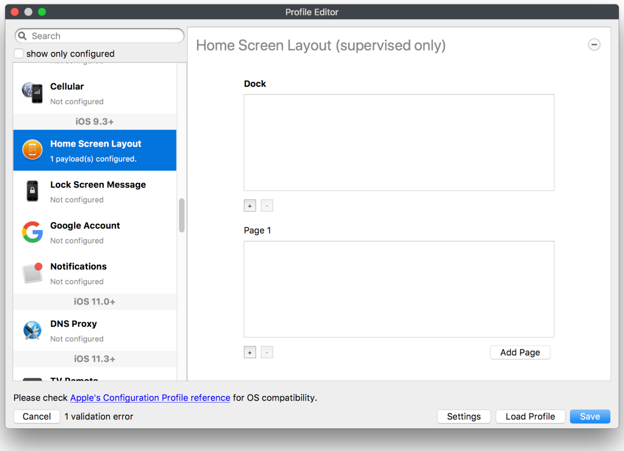
1 validation error

Use this payload for cellular settings. In iOS 7 or later, the APN payload is deprecated in favor of the Cellular payload.

iOS 9.3+

These settings apply to iOS devices running iOS 9.3 or higher.

Home Screen Layout (supervised only)



Home Screen Layout (supervised only)

Dock

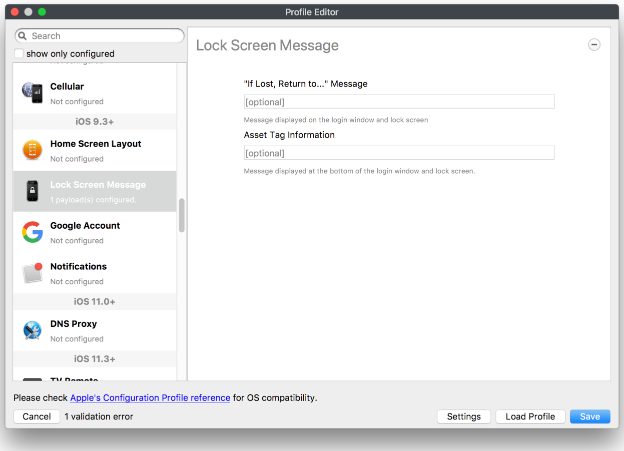
Page 1

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

With supervised devices, you can specify the home screen layout including which apps are in the Dock and which apps appear where on different pages of the home screen.

Lock Screen Message



Lock Screen Message

"If Lost, Return to..." Message

[optional]

Message displayed on the login window and lock screen

Asset Tag Information

[optional]

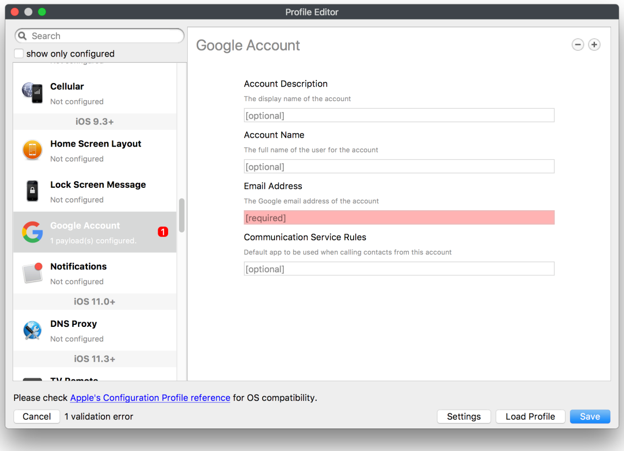
Message displayed at the bottom of the login window and lock screen.

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

This allows you to specify the text to be displayed in the login window and on the lock screen. Devices do not have to be supervised to use this payload type.

Google Account



Google Account

Account Description
The display name of the account
[optional]

Account Name
The full name of the user for the account
[optional]

Email Address
The Google email address of the account
[required]

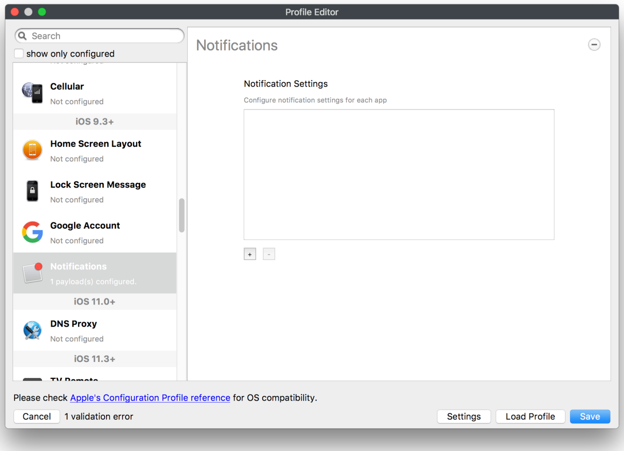
Communication Service Rules
Default app to be used when calling contacts from this account
[optional]

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

This payload type is used to configure Google accounts. The user will be prompted to sign in to the configured account(s).

Notifications

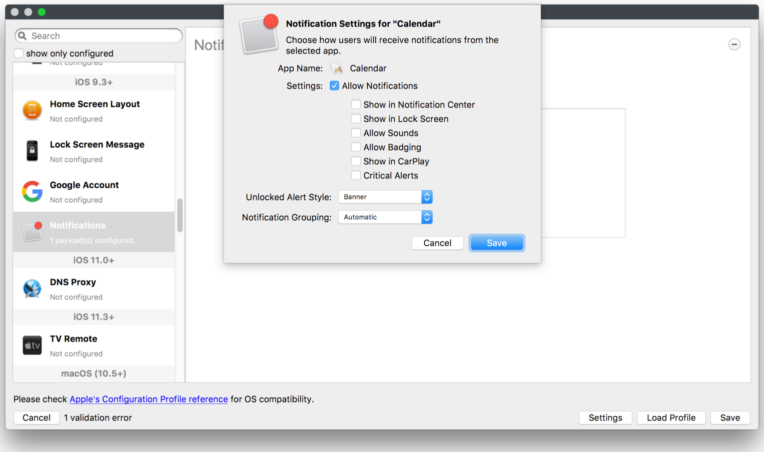


Notifications

Notification Settings
Configure notification settings for each app

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Notification Settings for "Calendar"

Choose how users will receive notifications from the selected app.

App Name: Calendar

Settings: ☑ Allow Notifications

☐ Show in Notification Center
☐ Show in Lock Screen
☐ Allow Sounds
☐ Allow Badging
☐ Show in CarPlay
☐ Critical Alerts

Unlocked Alert Style: Banner

Notification Grouping: Automatic

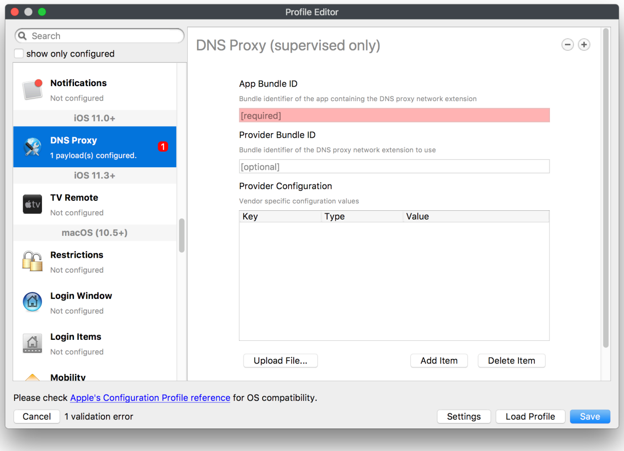
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

This payload type is used to enforce notification settings for each app. These settings only affect supervised devices.

iOS 11.0+

DNS Proxy (supervised only)



DNS Proxy (supervised only)

App Bundle ID

Bundle identifier of the app containing the DNS proxy network extension

[required]

Provider Bundle ID

Bundle identifier of the DNS proxy network extension to use

[optional]

Provider Configuration

Vendor specific configuration values

Key	Type	Value

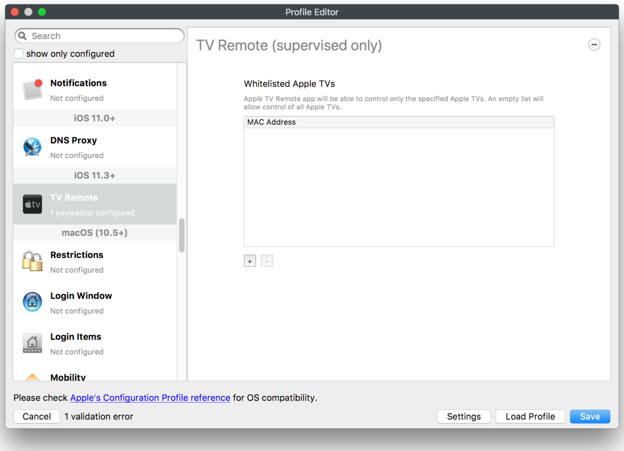
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure DNS procy settings. These settings will only affect supervised devices.

iOS 11.3+

TV Remote (supervised only)



TV Remote (supervised only)

Whitelisted Apple TVs

Apple TV Remote app will be able to control only the specified Apple TVs. An empty list will allow control of all Apple TVs.

MAC Address

Please check Apple's Configuration Profile reference for OS compatibility.

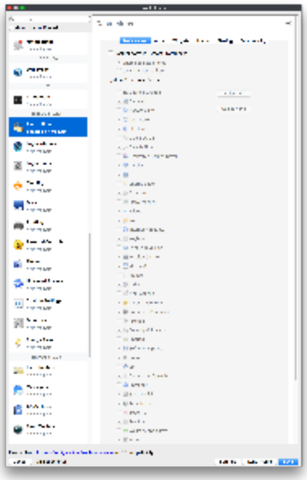
1 validation error

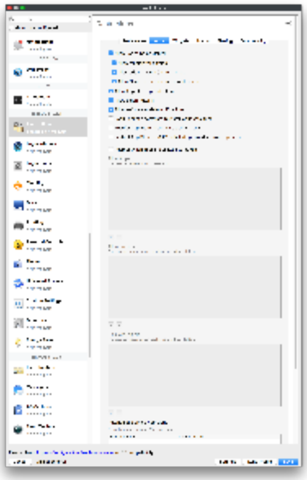
Use this section to configure the list of Apple TVs that can be controlled using the Remote app. these settings will only affect supervised devices.

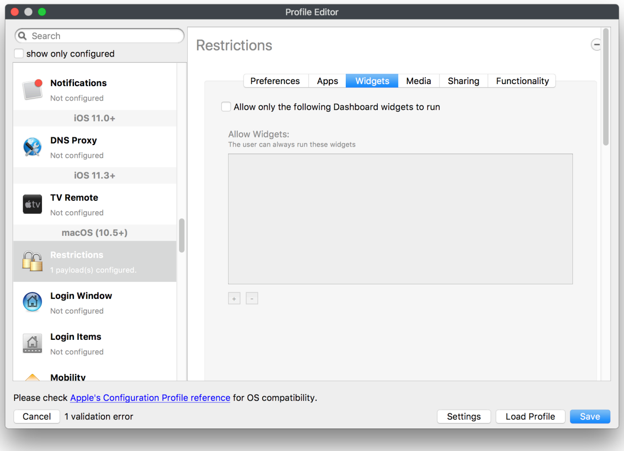
macOS (10.5+)

These settings are for macOS 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 – 10.11 and macOS Sierra (10.12) will be sent as managed profiles.
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







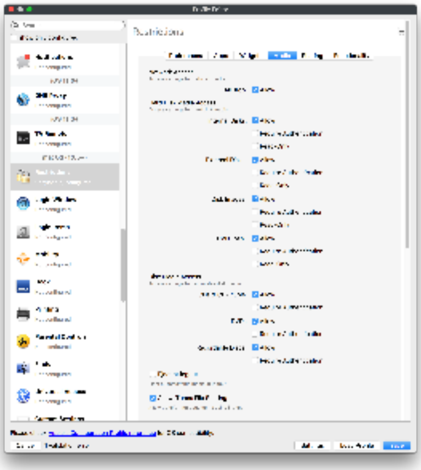
Restrictions

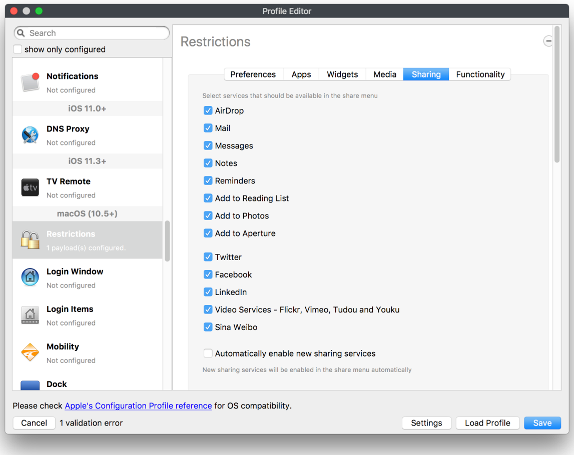
□ Allow only the following Dashboard widgets to run

Allow Widgets:
The user can always run these widgets

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error





Select services that should be available in the share menu

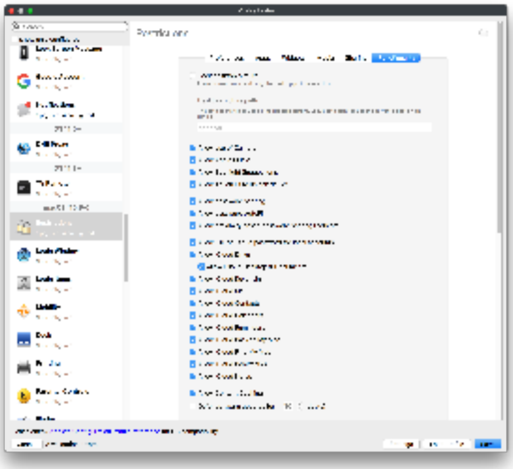
☑ AirDrop
☑ Mail
☑ Messages
☑ Notes
☑ Reminders
☑ Add to Reading List
☑ Add to Photos
☑ Add to Aperture

☑ Twitter
☑ Facebook
☑ LinkedIn
☑ Video Services - Flickr, Vimeo, Tudou and Youku
☑ Sina Weibo

☐ Automatically enable new sharing services

New sharing services will be enabled in the share menu automatically

Please check Apple's Configuration Profile reference for OS compatibility.

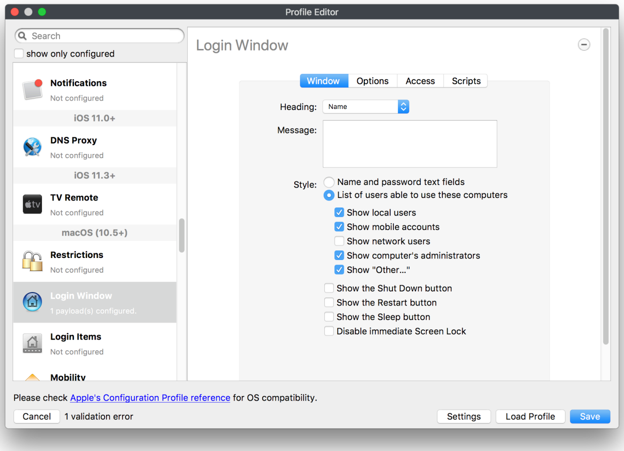


The restrictions payload contains settings to limit access to system preferences, applications, Widgets, media, and sharing services. Preferences now includes all Systems Preferences plus the 3rd party Preference panes that are installed on the FileWave Admin machine. If you want to control 3rd party Preference panes on client devices, you must have that same item installed on your administration machine in order to have it show up in the list for management.

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. Desktop settings allow control of the Desktop picture, Camera use, iCloud documents, data and passwords, and Spotlight suggestions.

Login Window



Login Window

Heading: Name

Message:

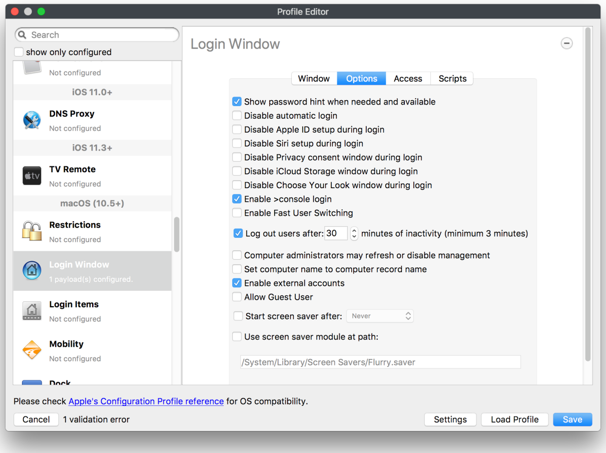
Style: ○ Name and password text fields
● List of users able to use these computers

☑ Show local users
☑ Show mobile accounts
□ Show network users
☑ Show computer's administrators
☑ Show "Other..."

□ Show the Shut Down button
□ Show the Restart button
□ Show the Sleep button
□ Disable immediate Screen Lock

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Login Window

☑ Show password hint when needed and available
□ Disable automatic login
□ Disable Apple ID setup during login
□ Disable Siri setup during login
□ Disable Privacy consent window during login
□ Disable iCloud Storage window during login
□ Disable Choose Your Look window during login
☑ Enable >console login
□ Enable Fast User Switching

☑ Log out users after: 30 minutes of inactivity (minimum 3 minutes)

□ Computer administrators may refresh or disable management
□ Set computer name to computer record name
☑ Enable external accounts
□ Allow Guest User

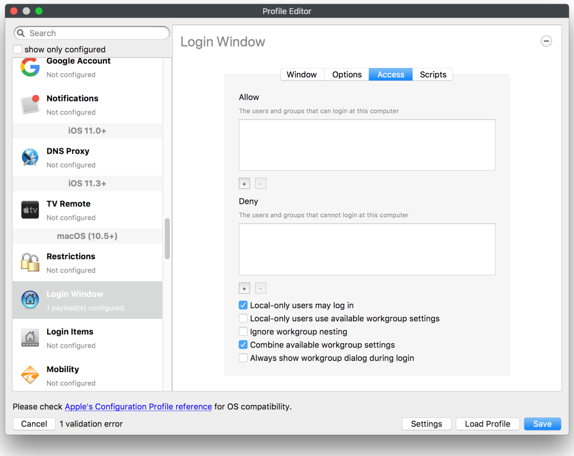
□ Start screen saver after: Never

□ Use screen saver module at path:

/System/Library/Screen Savers/Flurry.saver

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Login Window

Allow

The users and groups that can login at this computer

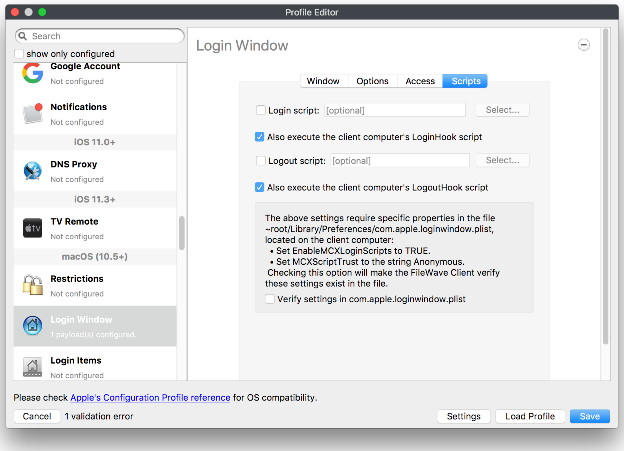
Deny

The users and groups that cannot login at this computer

☑ Local-only users may log in
□ Local-only users use available workgroup settings
□ Ignore workgroup nesting
☑ Combine available workgroup settings
□ Always show workgroup dialog during login

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Login Window

□ Login script: [optional]

☑ Also execute the client computer's LoginHook script

□ Logout script: [optional]

☑ Also execute the client computer's LogoutHook script

The above settings require specific properties in the file ~root/Library/Preferences/com.apple.loginwindow.plist, located on the client computer:

- Set EnableMCXLoginScripts to TRUE.
- Set MCXScriptTrust to the string Anonymous.

Checking this option will make the FileWave Client verify these settings exist in the file.

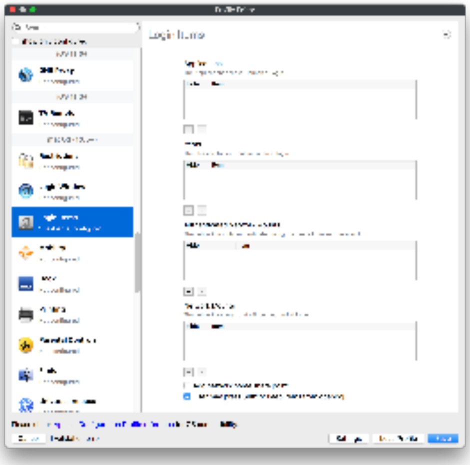
□ Verify settings in com.apple.loginwindow.plist

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

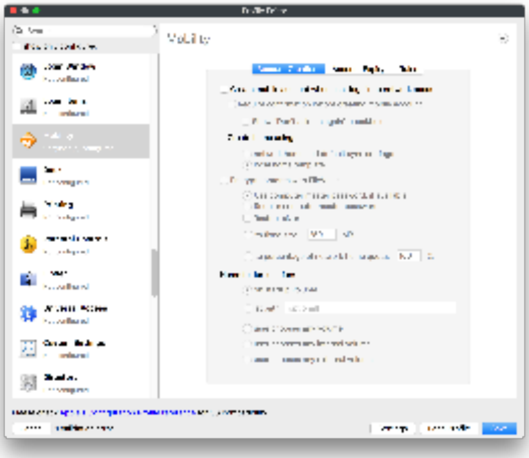
The Login Window payload lets you configure the login window with a message, designate the type of login display (name/pwd or list), allow local administrators to bypass management, allow the Guest account, configure a login window screen saver, limit device access to certain Groups, and imbed login/logout scripts.

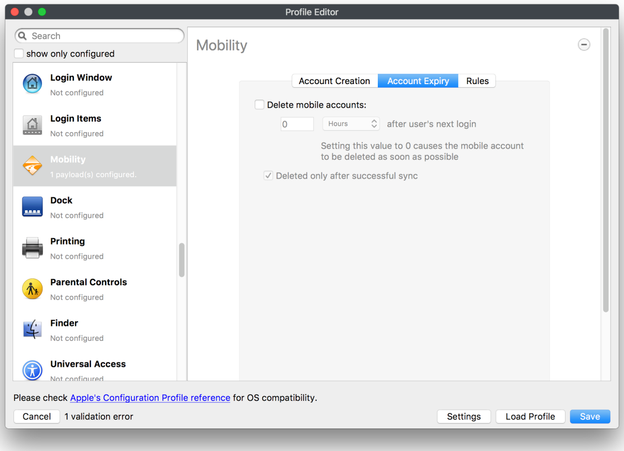
Login Items



Login Items is a payload that can contain specified applications and network 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

□ Delete mobile accounts:

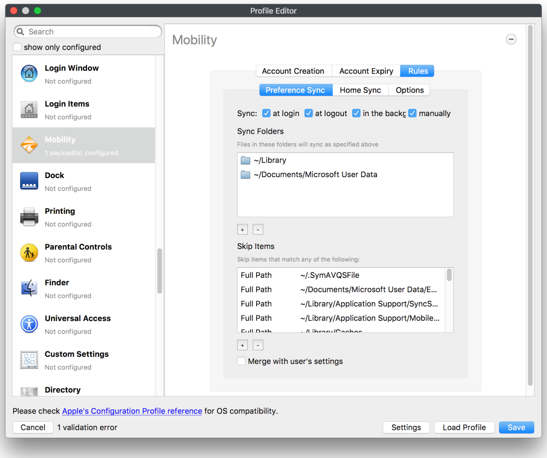
0 Hours after user's next login

Setting this value to 0 causes the mobile account to be deleted as soon as possible

☑ Deleted only after successful sync

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Mobility

Sync: ☑ at login ☑ at logout ☑ in the backg ☑ manually

Sync Folders

Files in these folders will sync as specified above

~/Library
~/Documents/Microsoft User Data

Skip Items

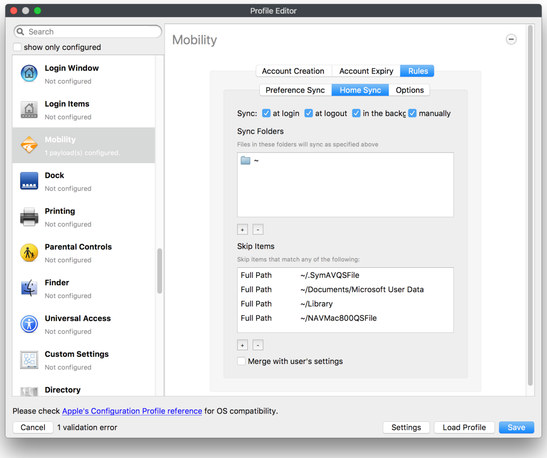
Skip items that match any of the following:

Full Path	~/.SymAVQSFile
Full Path	~/Documents/Microsoft User Data/E...
Full Path	~/Library/Application Support/SyncS...
Full Path	~/Library/Application Support/Mobile...
Full Path	~/Library/Caches

□ Merge with user's settings

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Sync: ☑ at login ☑ at logout ☑ in the backg ☑ manually

Sync Folders

Files in these folders will sync as specified above

~

Skip Items

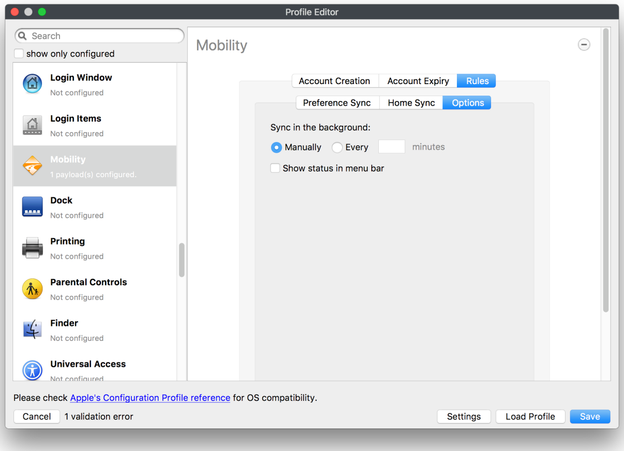
Skip items that match any of the following:

Full Path	~/.SymAVQSFile
Full Path	~/Documents/Microsoft User Data
Full Path	~/Library
Full Path	~/NAVMac800QSFile

□ Merge with user's settings

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Sync in the background:

● Manually ○ Every minutes

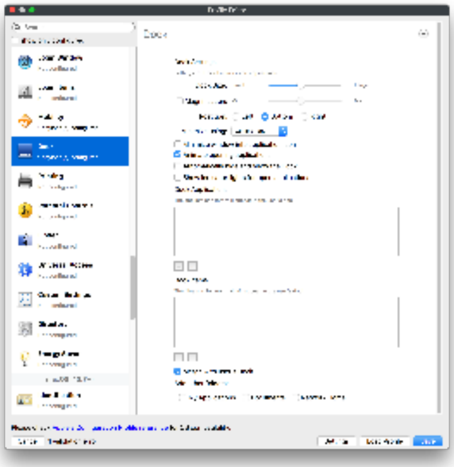
□ Show status in menu bar

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

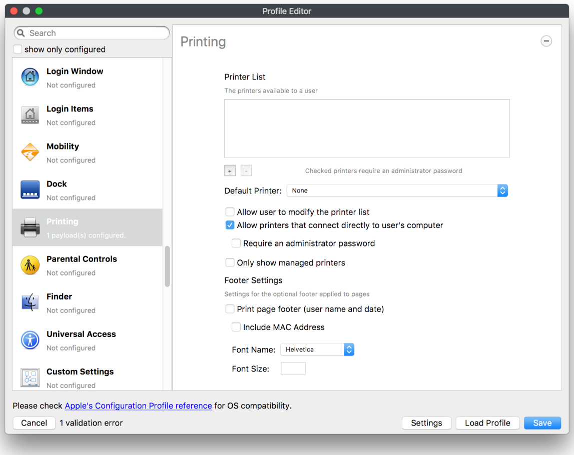
Mobility allows you to create mobile accounts - network user accounts with portable home directories. Used in conjunction with the Login Window payload, you can specify support for the External account, which is a mobile account with an externally attached home directory. The idea is to have managed systems, bound to a network directory, where the user carries their home directory (USB/Thunderbolt drive) from device to device; but still logs in as a network directory account.

Dock



The Dock payload can be configured for shared computers that need to have a consistent look and feel regardless of user.

Printing



Printing

Printer List

The printers available to a user

Checked printers require an administrator password

Default Printer: None

☐ Allow user to modify the printer list

☑ Allow printers that connect directly to user's computer

☐ Require an administrator password

☐ Only show managed printers

Footer Settings

Settings for the optional footer applied to pages

☐ Print page footer (user name and date)

☐ Include MAC Address

Font Name: Helvetica

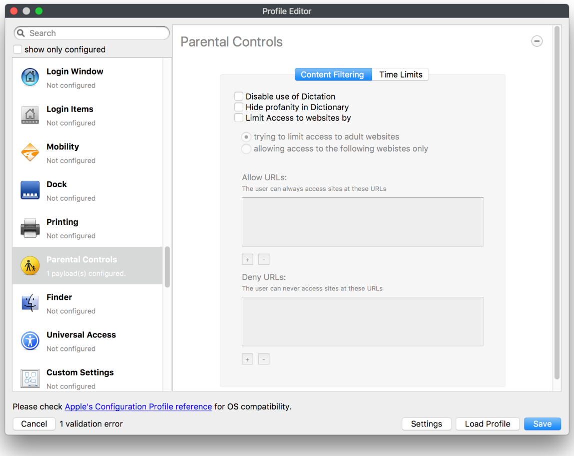
Font Size:

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Printing payloads allow the assignment of network printers to managed computers, as well as the ability to force all print jobs to contain the identity of the managed computer.

Parental Controls



Parental Controls

☐ Disable use of Dictation

☐ Hide profanity in Dictionary

☐ Limit Access to websites by

● trying to limit access to adult websites

○ allowing access to the following websites only

Allow URLs:

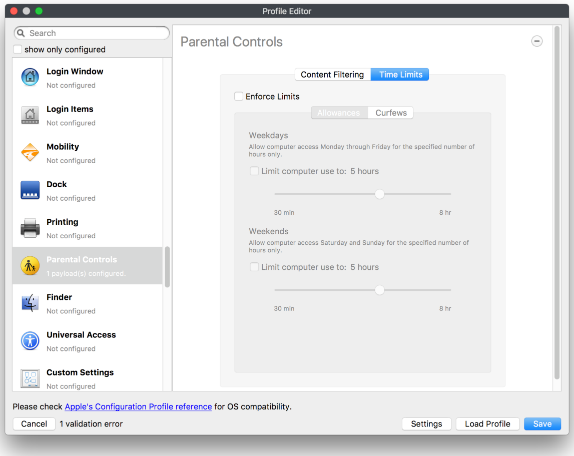
The user can always access sites at these URLs

Deny URLs:

The user can never access sites at these URLs

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Parental Controls

☐ Enforce Limits

Weekdays

Allow computer access Monday through Friday for the specified number of hours only.

☐ Limit computer use to: 5 hours

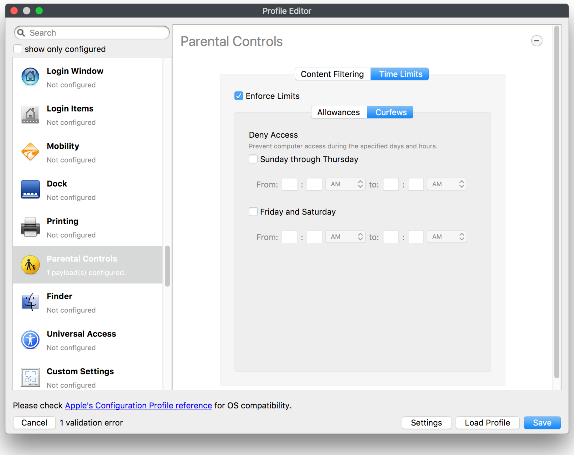
Weekends

Allow computer access Saturday and Sunday for the specified number of hours only.

☐ Limit computer use to: 5 hours

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Parental Controls

☑ Enforce Limits

Deny Access

Prevent computer access during the specified days and hours.

□ Sunday through Thursday

From: : AM to: : AM

□ Friday and Saturday

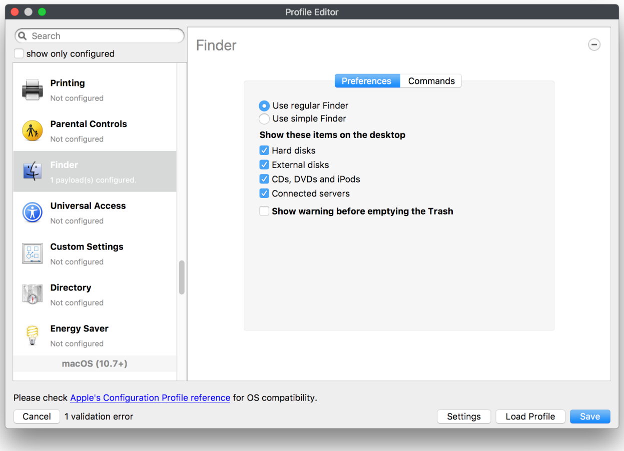
From: : AM to: : AM

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Parental Controls were designed to support 1:1's where policies required content filters for managed computers 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



Finder

● Use regular Finder
○ Use simple Finder

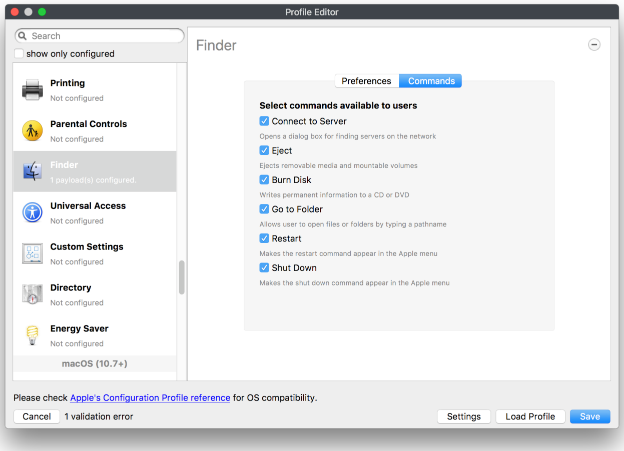
Show these items on the desktop

☑ Hard disks
☑ External disks
☑ CDs, DVDs and iPods
☑ Connected servers

□ **Show warning before emptying the Trash**

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Finder

Select commands available to users

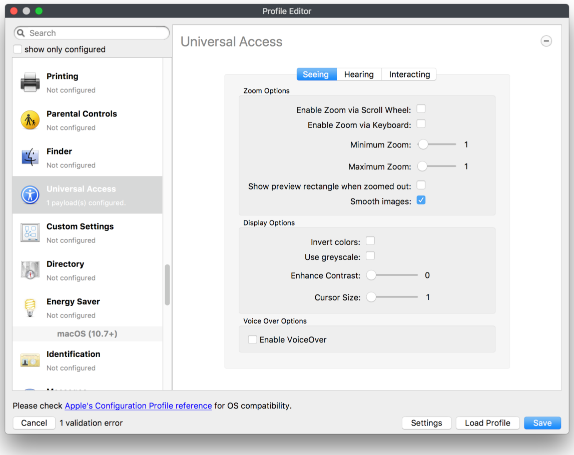
☑ Connect to Server
Opens a dialog box for finding servers on the network
☑ Eject
Ejects removable media and mountable volumes
☑ Burn Disk
Writes permanent information to a CD or DVD
☑ Go to Folder
Allows user to open files or folders by typing a pathname
☑ Restart
Makes the restart command appear in the Apple menu
☑ Shut Down
Makes the shut down command appear in the Apple menu

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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

Zoom Options

Enable Zoom via Scroll Wheel: □
Enable Zoom via Keyboard: □
Minimum Zoom: 1
Maximum Zoom: 1
Show preview rectangle when zoomed out: □
Smooth images: ☑

Display Options

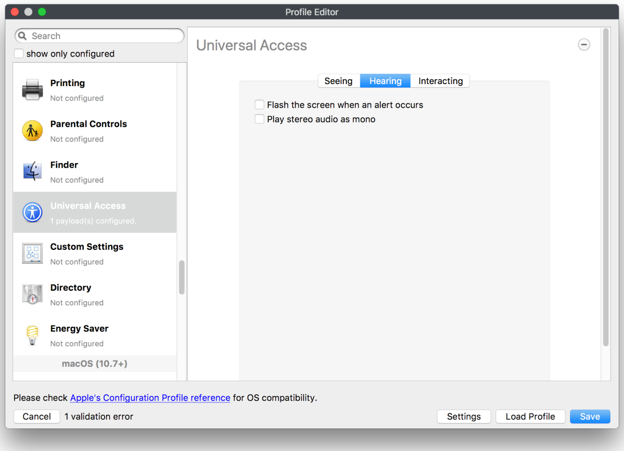
Invert colors: □
Use greyscale: □
Enhance Contrast: 0
Cursor Size: 1

Voice Over Options

□ Enable VoiceOver

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

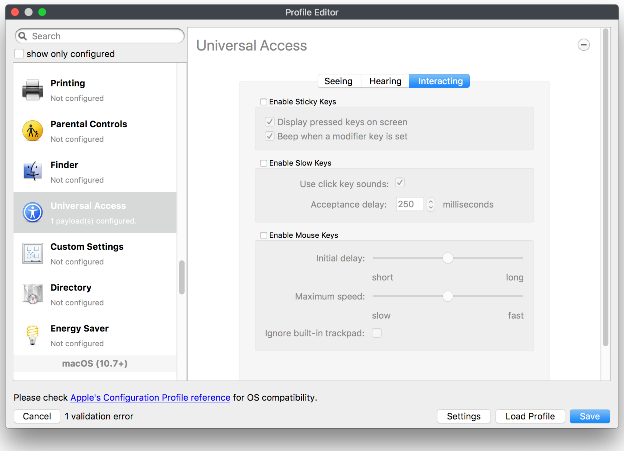


Universal Access

□ Flash the screen when an alert occurs
□ Play stereo audio as mono

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error



Universal Access

□ Enable Sticky Keys

☑ Display pressed keys on screen
☑ Beep when a modifier key is set

□ Enable Slow Keys

Use click key sounds: ☑
Acceptance delay: 250 milliseconds

□ Enable Mouse Keys

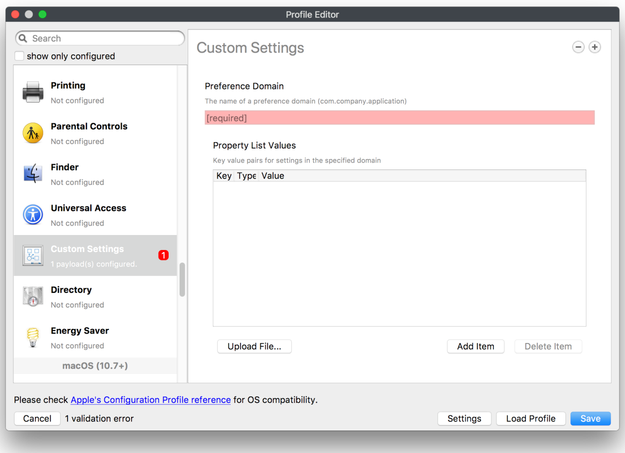
Initial delay: short long
Maximum speed: slow fast
Ignore built-in trackpad: □

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

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' computers to support zoom with the trackpad.

Custom Settings



Profile Editor

Search

□ show only configured

Printing
Not configured

Parental Controls
Not configured

Finder
Not configured

Universal Access
Not configured

Custom Settings
1 payload(s) configured. 1

Directory
Not configured

Energy Saver
Not configured

macOS (10.7+)

Custom Settings

Preference Domain
The name of a preference domain (com.company.application)
[required]

Property List Values
Key value pairs for settings in the specified domain

Key	Type	Value

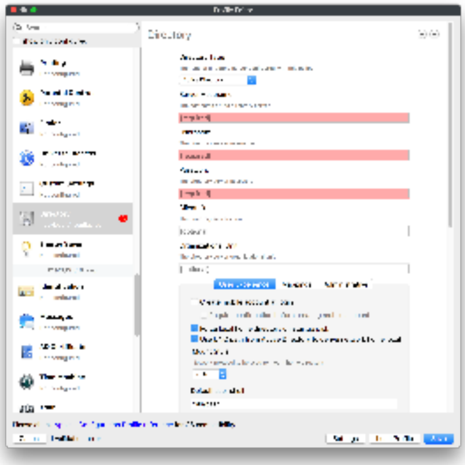
Upload File... Add Item Delete Item

Please check Apple's Configuration Profile reference for OS compatibility.

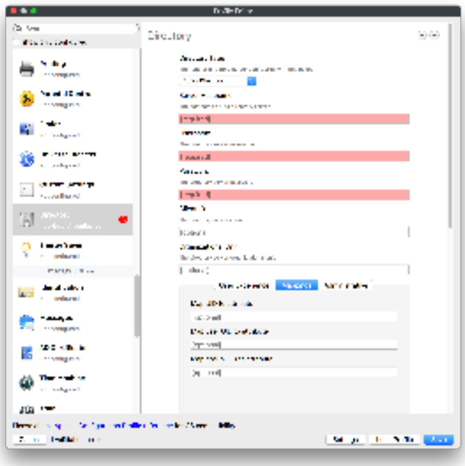
Cancel 1 validation error Settings Load Profile Save

Custom Settings payloads allow you to greatly expand your ability to provide templates and special settings for managed computers. 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 configuration settings to follow for that application.

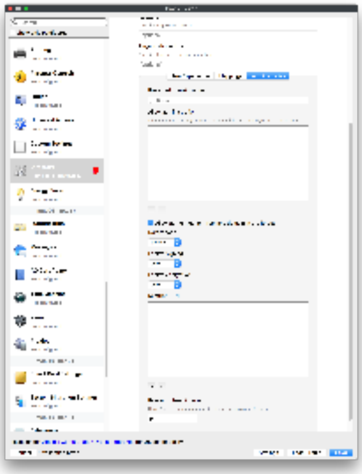
Directory



Directory

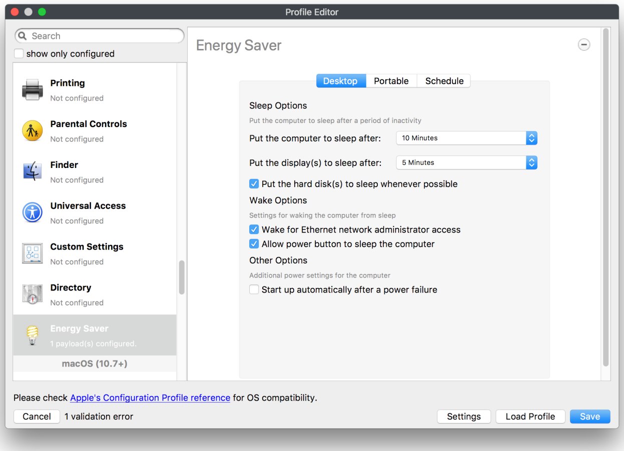


Directory



The Directory payload allows you to configure **binding** to LDAP directories for your macOS systems. You can set up anonymous or authenticated bindings.

Energy Saver



Energy Saver

Desktop | Portable | Schedule

Sleep Options

Put the computer to sleep after a period of inactivity

Put the computer to sleep after: 10 Minutes

Put the display(s) to sleep after: 5 Minutes

☑ Put the hard disk(s) to sleep whenever possible

Wake Options

Settings for waking the computer from sleep

☑ Wake for Ethernet network administrator access

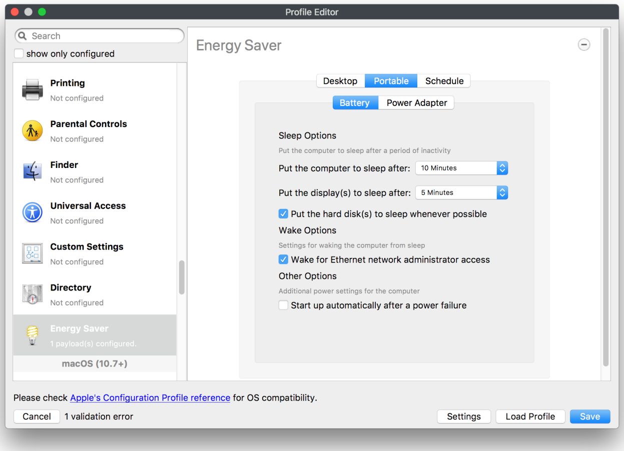
☑ Allow power button to sleep the computer

Other Options

Additional power settings for the computer

□ Start up automatically after a power failure

Please check Apple's Configuration Profile reference for OS compatibility.



Energy Saver

Desktop | Portable | Schedule

Battery | Power Adapter

Sleep Options

Put the computer to sleep after a period of inactivity

Put the computer to sleep after: 10 Minutes

Put the display(s) to sleep after: 5 Minutes

☑ Put the hard disk(s) to sleep whenever possible

Wake Options

Settings for waking the computer from sleep

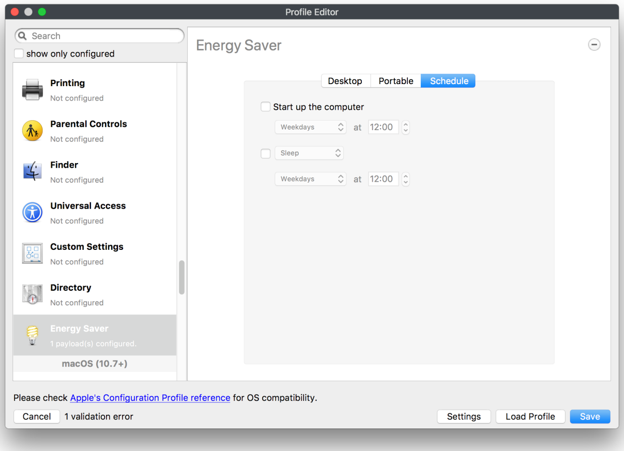
☑ Wake for Ethernet network administrator access

Other Options

Additional power settings for the computer

□ Start up automatically after a power failure

Please check Apple's Configuration Profile reference for OS compatibility.



Energy Saver

□ Start up the computer

Weekdays at 12:00

□ Sleep

Weekdays at 12:00

Please check Apple's Configuration Profile reference for OS compatibility.

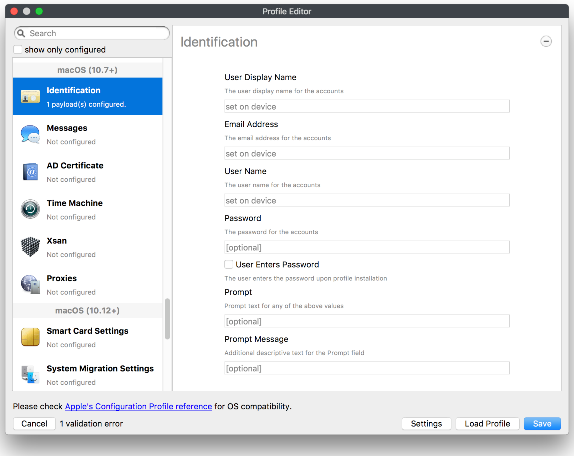
1 validation error

Energy Saver payload settings allow you to preconfigure managed computers 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.

macOS (10.7+) settings

These settings are OS X running v10.7 (Lion) or higher only.

Identification



Identification

User Display Name
The user display name for the accounts
set on device

Email Address
The email address for the accounts
set on device

User Name
The user name for the accounts
set on device

Password
The password for the accounts
[optional]

□ User Enters Password
The user enters the password upon profile installation

Prompt
Prompt text for any of the above values
[optional]

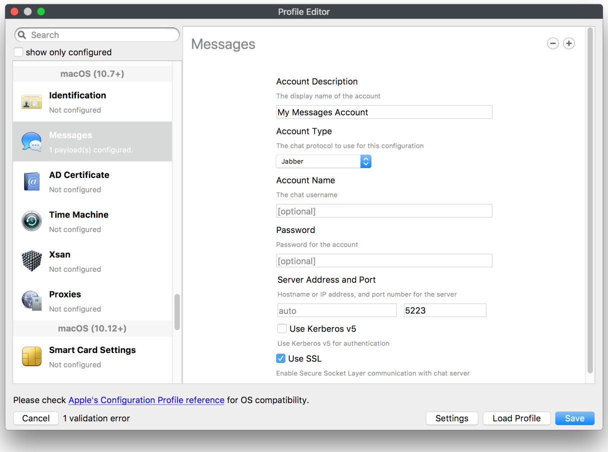
Prompt Message
Additional descriptive text for the Prompt field
[optional]

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

The Identification payload, using parameterized profile settings, can allow you to preconfigure user identity information for multiple users 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

Account Description
The display name of the account
My Messages Account

Account Type
The chat protocol to use for this configuration
Jabber

Account Name
The chat username
[optional]

Password
Password for the account
[optional]

Server Address and Port
Hostname or IP address, and port number for the server
auto 5223

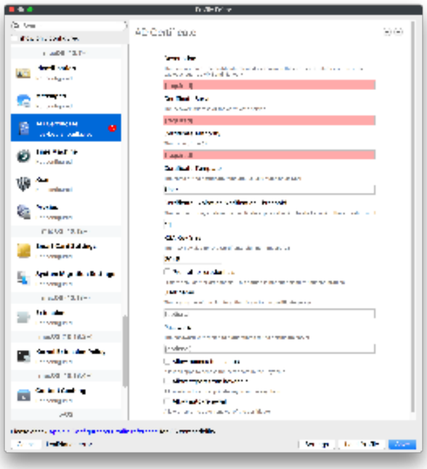
□ Use Kerberos v5
Use Kerberos v5 for authentication

☑ Use SSL
Enable Secure Socket Layer communication with chat server

Please check Apple's Configuration Profile reference for OS compatibility.

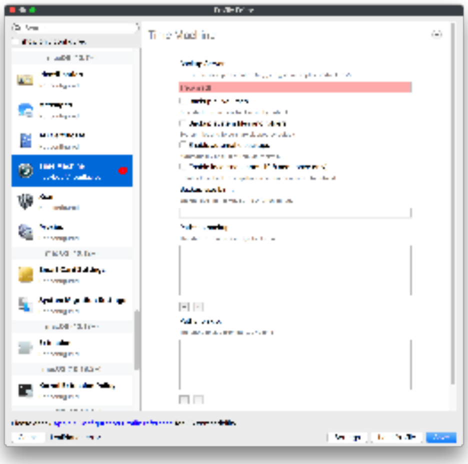
Messages allows you to preload the settings for user access to Jabber or AIM chat services. It can use parameterized profile settings for this payload.

AD Certificate



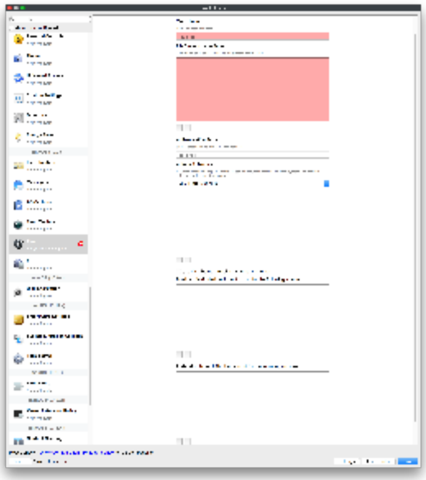
Configuring the AD Certificate payload lets you set up other payloads, such as VPN or Network, more easily. This payload provides the authentication data that will validate access to other services dependent on Active Directory certificates.

Time Machine



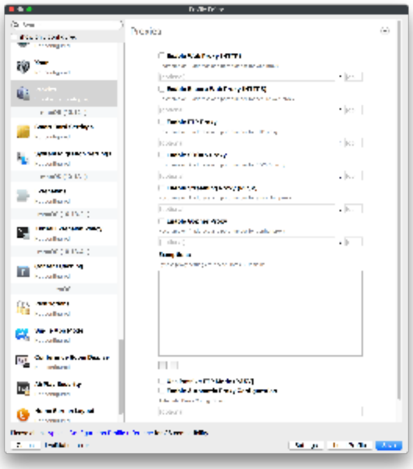
For environments using Time Machine servers or Time Capsules, this payload lets you set up the access information for backup of managed devices.

Xsan



This section is used to configure Xsan; specifically the name of the Xsan network, the name of the FS Name Server, and the authentication secret, if one is used.

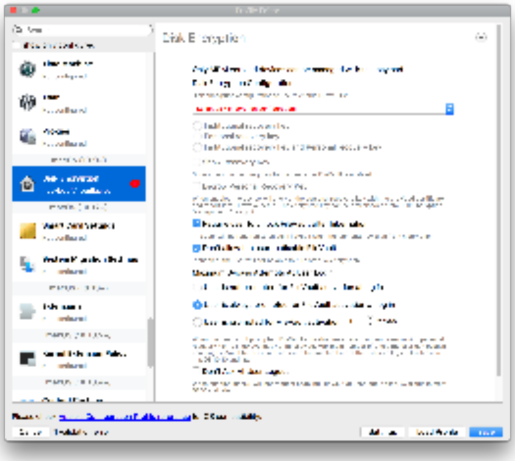
Proxies



This payload type is used to configure proxy settings, including exception for specified hosts and domains.

macOS (10.9+)

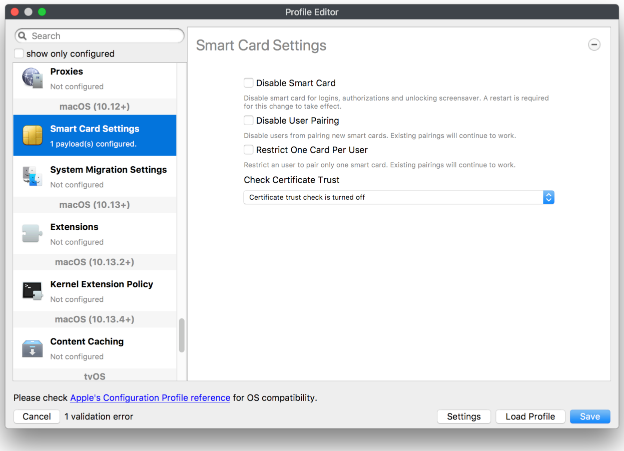
Disk Encryption



Use this section to define settings for Disk Encryption (FileVault 2). You can find more information about FileVault 2 on FileWave's Knowledge Base

macOS (10.12+)

Smart Card Settings



Smart Card Settings

□ Disable Smart Card

Disable smart card for logins, authorizations and unlocking screensaver. A restart is required for this change to take effect.

□ Disable User Pairing

Disable users from pairing new smart cards. Existing pairings will continue to work.

□ Restrict One Card Per User

Restrict an user to pair only one smart card. Existing pairings will continue to work.

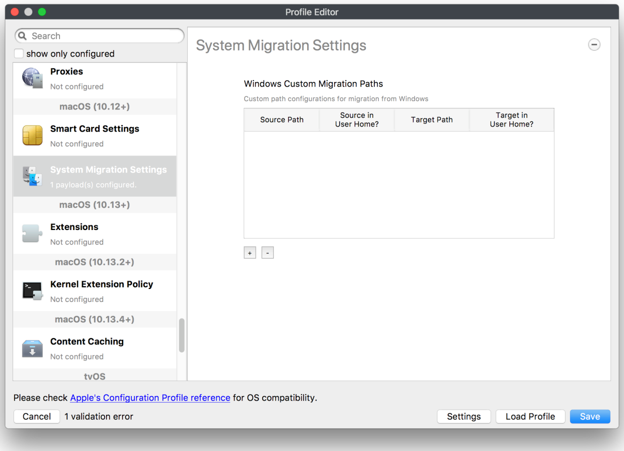
Check Certificate Trust: Certificate trust check is turned off

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use the section to configure smart card security settings for macOS

System Migration Settings



System Migration Settings

Windows Custom Migration Paths

Custom path configurations for migration from Windows

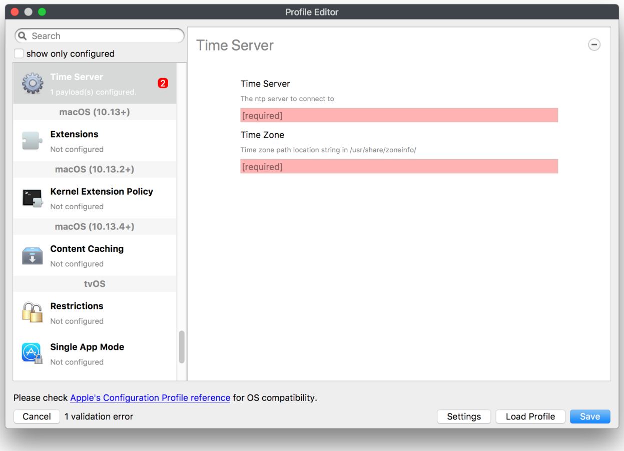
Source Path	Source in User Home?	Target Path	Target in User Home?

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure system migration settings

Time Server



Time Server

Time Server

The ntp server to connect to

[required]

Time Zone

Time zone path location string in /usr/share/zoneinfo/

[required]

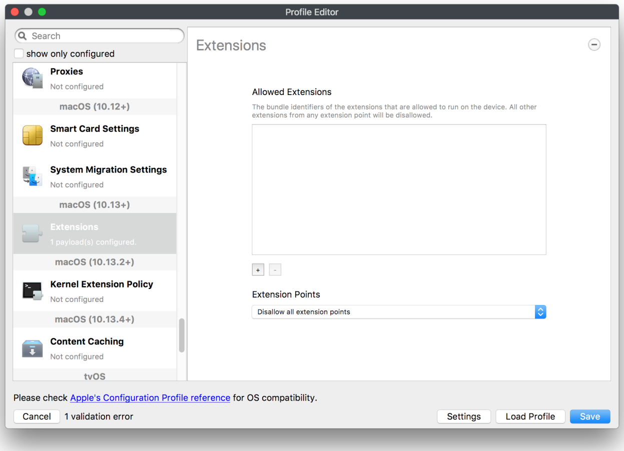
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

use this section to configure time server settings

macOS (10.13+)

Extensions



Extensions

Allowed Extensions

The bundle identifiers of the extensions that are allowed to run on the device. All other extensions from any extension point will be disallowed.

Extension Points

Disallow all extension points

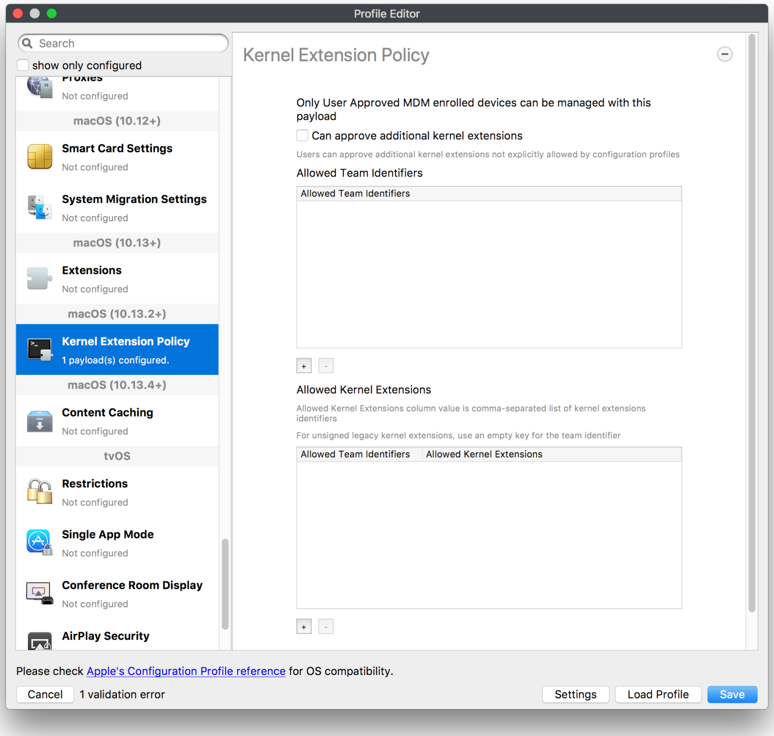
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure allowed extensions on macOS

macOS (10.13.2+)

Kernel Extension Policy



Kernel Extension Policy

Only User Approved MDM enrolled devices can be managed with this payload

□ Can approve additional kernel extensions

Users can approve additional kernel extensions not explicitly allowed by configuration profiles

Allowed Team Identifiers

Allowed Team Identifiers

Allowed Kernel Extensions

Allowed Kernel Extensions column value is comma-separated list of kernel extensions identifiers

For unsigned legacy kernel extensions, use an empty key for the team identifier

Allowed Team Identifiers	Allowed Kernel Extensions

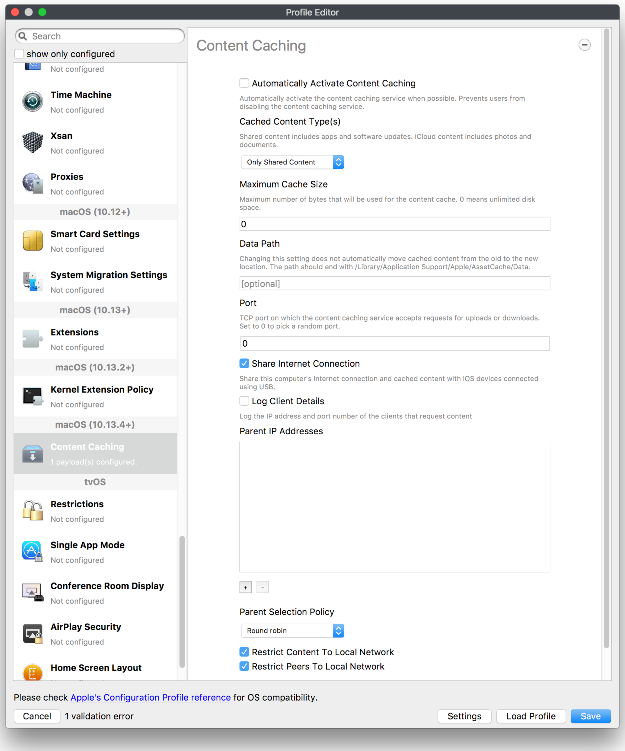
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure kernel extensions on macOS

macOS (10.13.3+)

Content Caching



Content Caching

□ Automatically Activate Content Caching

Automatically activate the content caching service when possible. Prevents users from disabling the content caching service.

Cached Content Type(s)

Shared content includes apps and software updates. iCloud content includes photos and documents.

Only Shared Content

Maximum Cache Size

Maximum number of bytes that will be used for the content cache. 0 means unlimited disk space.

0

Data Path

Changing this setting does not automatically move cached content from the old to the new location. The path should end with /Library/Application Support/Apple/AssetCache/Data.

[optional]

Port

TCP port on which the content caching service accepts requests for uploads or downloads. Set to 0 to pick a random port.

0

☑ Share Internet Connection

Share this computer's Internet connection and cached content with iOS devices connected using USB.

□ Log Client Details

Log the IP address and port number of the clients that request content

Parent IP Addresses

Parent Selection Policy

Round robin

☑ Restrict Content To Local Network

☑ Restrict Peers To Local Network

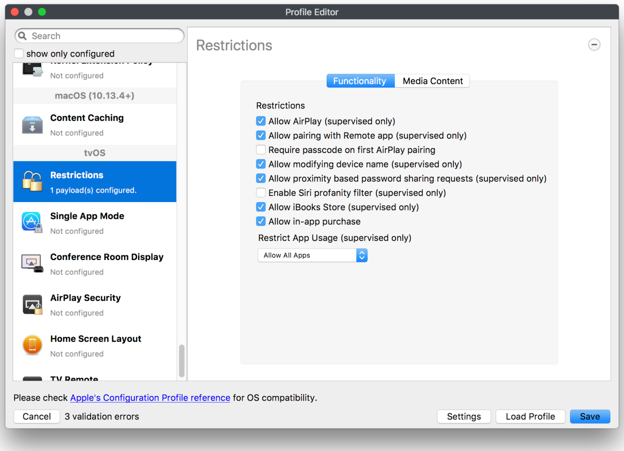
Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure content caching settings on macOS

tvOS

Restrictions



Restrictions

Restrictions

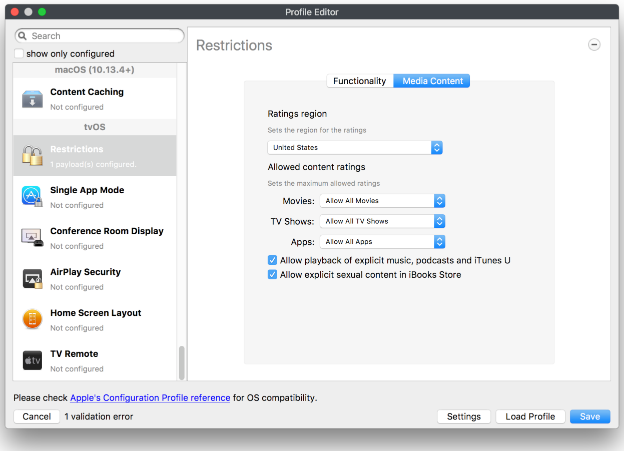
☑ Allow AirPlay (supervised only)
☑ Allow pairing with Remote app (supervised only)
□ Require passcode on first AirPlay pairing
☑ Allow modifying device name (supervised only)
☑ Allow proximity based password sharing requests (supervised only)
□ Enable Siri profanity filter (supervised only)
☑ Allow iBooks Store (supervised only)
☑ Allow in-app purchase

Restrict App Usage (supervised only)

Allow All Apps

Please check Apple's Configuration Profile reference for OS compatibility.

3 validation errors


Profile Editor

Search

□ show only configured

macOS (10.13.4+)

Content Caching
Not configured

tvOS

Restrictions
1 payload(s) configured.

Single App Mode
Not configured

Conference Room Display
Not configured

AirPlay Security
Not configured

Home Screen Layout
Not configured

TV Remote
Not configured

Restrictions

Functionality | Media Content

Ratings region
Sets the region for the ratings
United States

Allowed content ratings
Sets the maximum allowed ratings
Movies: Allow All Movies
TV Shows: Allow All TV Shows
Apps: Allow All Apps

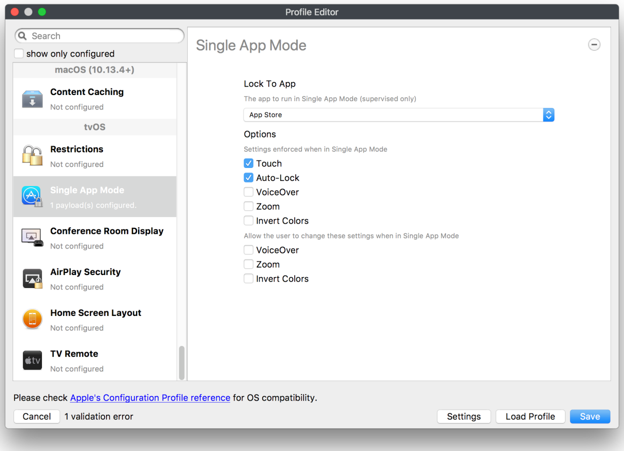
☑ Allow playback of explicit music, podcasts and iTunes U
☑ Allow explicit sexual content in iBooks Store

Please check Apple's Configuration Profile reference for OS compatibility.

Cancel 1 validation error Settings Load Profile Save

Restrictions allows you to push three different restrictions to your Apple TV. Disable Airplay (supervised only)Require passcode on first AirPlay pairingDisable control using Remote app (supervised only)

Single App Mode


Profile Editor

Search

□ show only configured

macOS (10.13.4+)

Content Caching
Not configured

tvOS

Restrictions
Not configured

Single App Mode
1 payload(s) configured.

Conference Room Display
Not configured

AirPlay Security
Not configured

Home Screen Layout
Not configured

TV Remote
Not configured

Single App Mode

Lock To App
The app to run in Single App Mode (supervised only)
App Store

Options
Settings enforced when in Single App Mode
☑ Touch
☑ Auto-Lock
□ VoiceOver
□ Zoom
□ Invert Colors

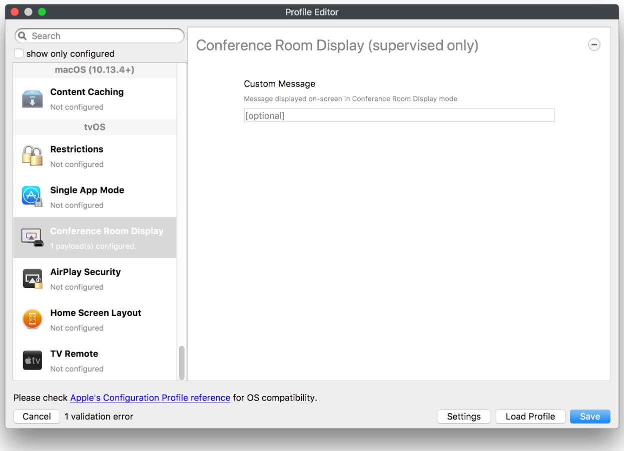
Allow the user to change these settings when in Single App Mode
□ VoiceOver
□ Zoom
□ Invert Colors

Please check Apple's Configuration Profile reference for OS compatibility.

Cancel 1 validation error Settings Load Profile Save

Use this section to specify the app to which the device should be locked to. These settings will only affect supervised devices.

Conference Room Display (supervised only)


Profile Editor

Search

□ show only configured

macOS (10.13.4+)

Content Caching
Not configured

tvOS

Restrictions
Not configured

Single App Mode
Not configured

Conference Room Display
1 payload(s) configured.

AirPlay Security
Not configured

Home Screen Layout
Not configured

TV Remote
Not configured

Conference Room Display (supervised only)

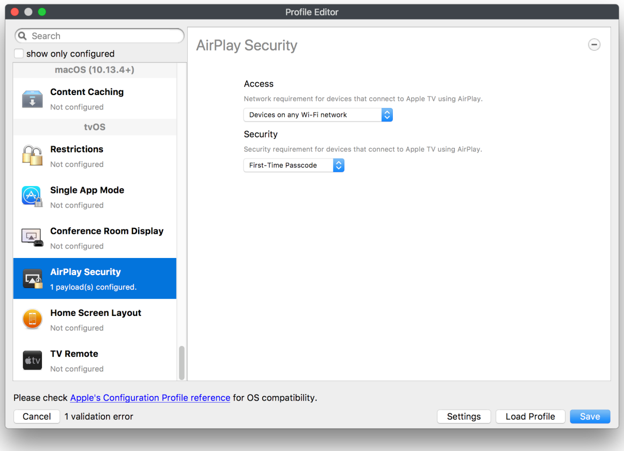
Custom Message
Message displayed on-screen in Conference Room Display mode
[optional]

Please check Apple's Configuration Profile reference for OS compatibility.

Cancel 1 validation error Settings Load Profile Save

Use this section to put a supervised Apple TV into Conference room Display mode.

AirPlay Security



AirPlay Security

Access

Network requirement for devices that connect to Apple TV using AirPlay.

Devices on any Wi-Fi network

Security

Security requirement for devices that connect to Apple TV using AirPlay.

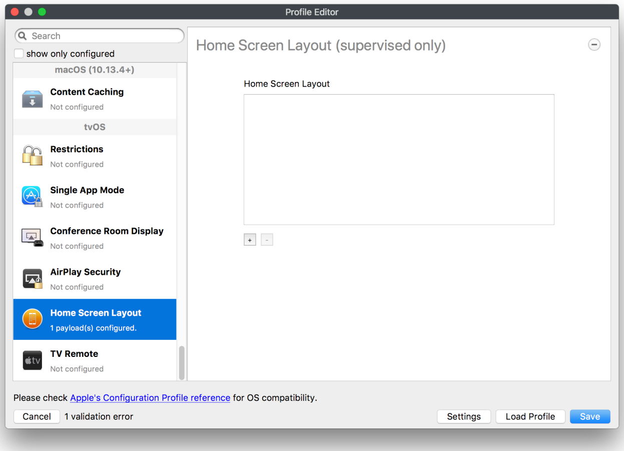
First-Time Passcode

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure settings for AirPlay security

Home Screen Layout (supervised only)



Home Screen Layout (supervised only)

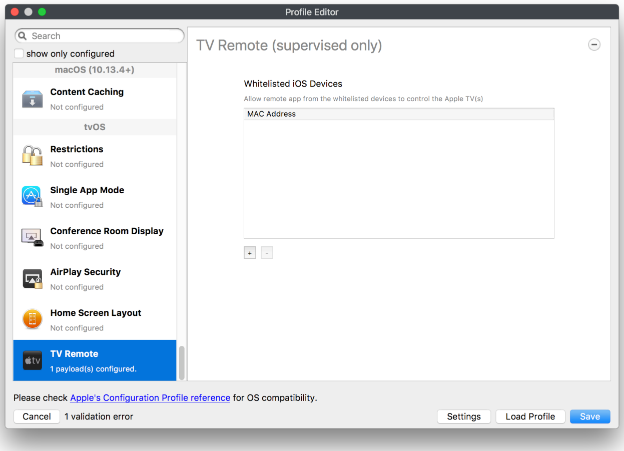
Home Screen Layout

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure tvOS home screen layout. These setttings will only affect supervised devices.

TV Remote (supervised only)



TV Remote (supervised only)

Whitelisted iOS Devices

Allow remote app from the whitelisted devices to control the Apple TV(s)

MAC Address

Please check Apple's Configuration Profile reference for OS compatibility.

1 validation error

Use this section to configure the list of iOS devices that can control the Apple TV(s). These settings will only affect supervised devices.

7.2. Parameterized profiles

FileWave allows you to use Directory based variables in your profile payloads. You can insert the following options into your profiles based on LDAP information for a particular user. Corresponding values in the user's LDAP record will replace the parameter variable in the actual profile placed on the device:
%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%
%WI-FIMAC% %ICCID% %IMEI%

Full List: Parameterized Profile

Setting Up LDAP for parameterized profiles

Setting up a directory server for use with Parameterized Profiles is easy. In FileWave Admin Preferences, fill out the appropriate information for your OpenDirectory, Active Directory, or E-Directory LDAP server. You must also be using LDAP authentication for iOS device enrollment. To add LDAP parameters to your profiles, simple replace the normal value with one from the list above.

7.3 Using FileWave Remote Control

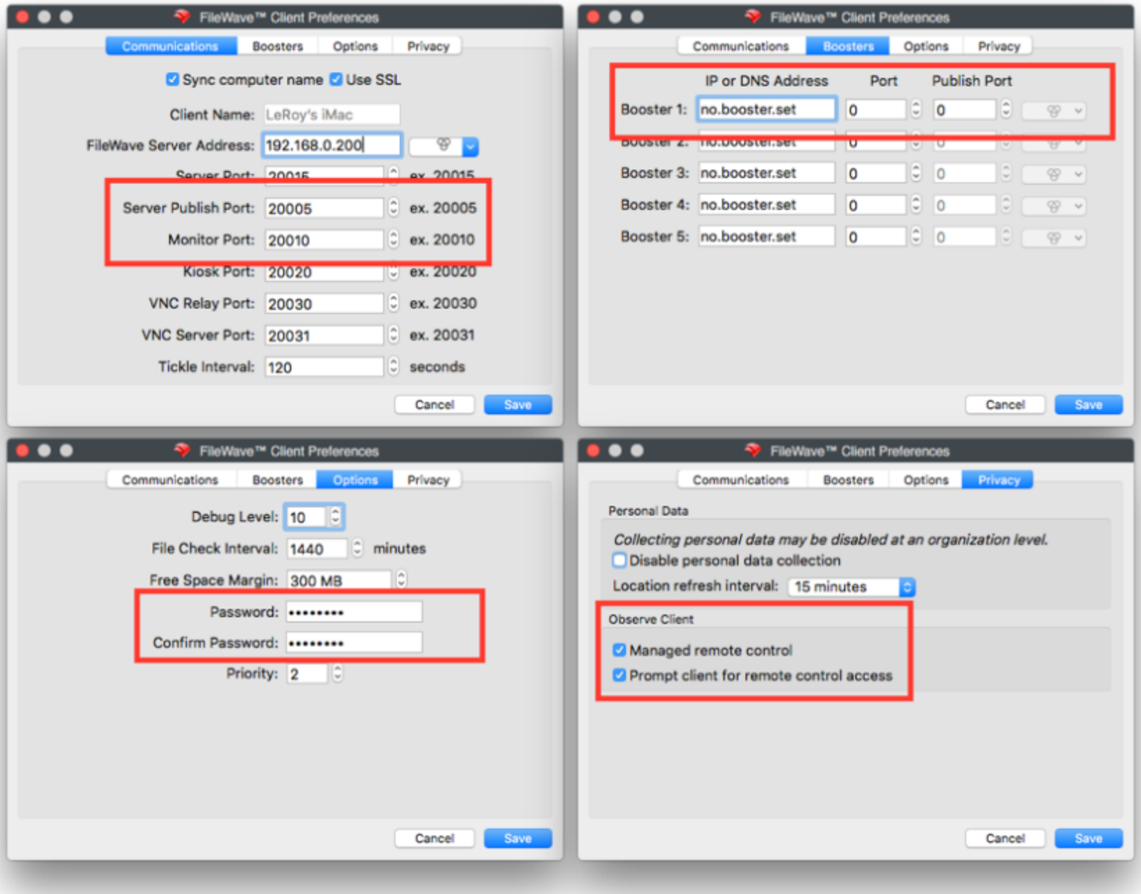
With FileWave 10+, administrators can view or control client devices across any network - as long as the FileWave Client and FileWave Admin can connect to the FileWave Server. All communications are tunneled through the FileWave Client, even through NAT'd networks. This is done by providing a secure VNC server built into the FileWave Client installer. The process even includes the ability to provide an "opt-in" for users.

Requirements

All FileWave Boosters must be upgraded to FW 10+ to support the ability for double-NAT traversal. All enrolled computers must be running FW 10+ client.

Configuration

The settings on the client are defaulted to the following (shown on the next page):



☑ Sync computer name ☑ Use SSL

Client Name:	LeRoy's iMac	
FileWave Server Address:	192.168.0.200	
Server Port:	20015	ex. 20015
Server Publish Port:	20005	ex. 20005
Monitor Port:	20010	ex. 20010
Kiosk Port:	20020	ex. 20020
VNC Relay Port:	20030	ex. 20030
VNC Server Port:	20031	ex. 20031
Tickle Interval:	120	seconds

	IP or DNS Address	Port	Publish Port
Booster 1:	no.booster.set	0	0
Booster 2:	no.booster.set	0	0
Booster 3:	no.booster.set	0	0
Booster 4:	no.booster.set	0	0
Booster 5:	no.booster.set	0	0

Debug Level:	10	
File Check Interval:	1440	minutes
Free Space Margin:	300 MB	
Password:	••••••••	
Confirm Password:	••••••••	
Priority:	2	

Personal Data

Collecting personal data may be disabled at an organization level.

☐ Disable personal data collection

Location refresh interval: 15 minutes

Observe Client

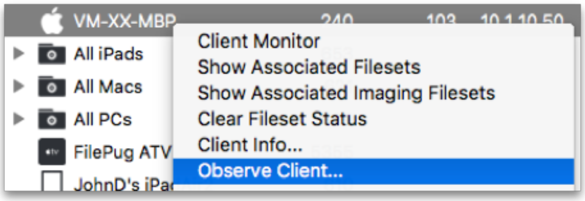
☑ Managed remote control

☑ Prompt client for remote control access

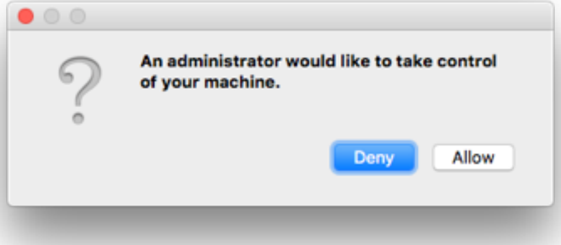
Note the **Managed remote control** and **Prompt for screen control**. These settings can be changed with a Superprefs Fileset, if necessary, or manually in the Client Monitor.
The Server and Booster settings are done as part of their initial configurations.

Operation

When you need to contact a client device, you use the **Observer Client…** command.

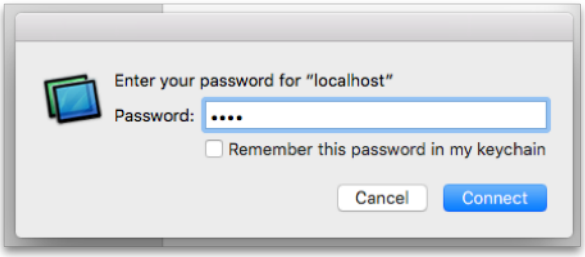


If the "Prompt client for remote control access" checkbox was checked in the Privacy pane of the Client Preference, then the Client will display a dialog asking for permission to connect. If permission is not granted by the user clicking on Allow, this dialog will time out and permission will be denied.



An administrator would like to take control of your machine.

Followed by the administrator getting a password request - the password will be the FileWave Client password you set in Client Monitor, or in the Installer.

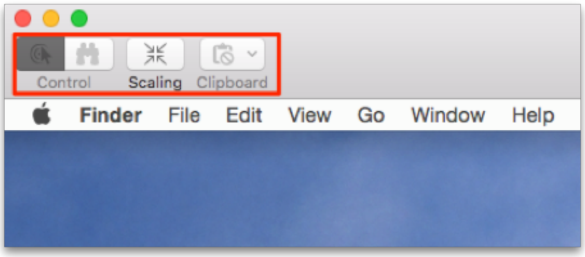


Enter your password for “localhost”

Password: ••••

☐ Remember this password in my keychain

Once the administrator has authenticated, he will see a full remote control window open with some basic tools in the upper corner:



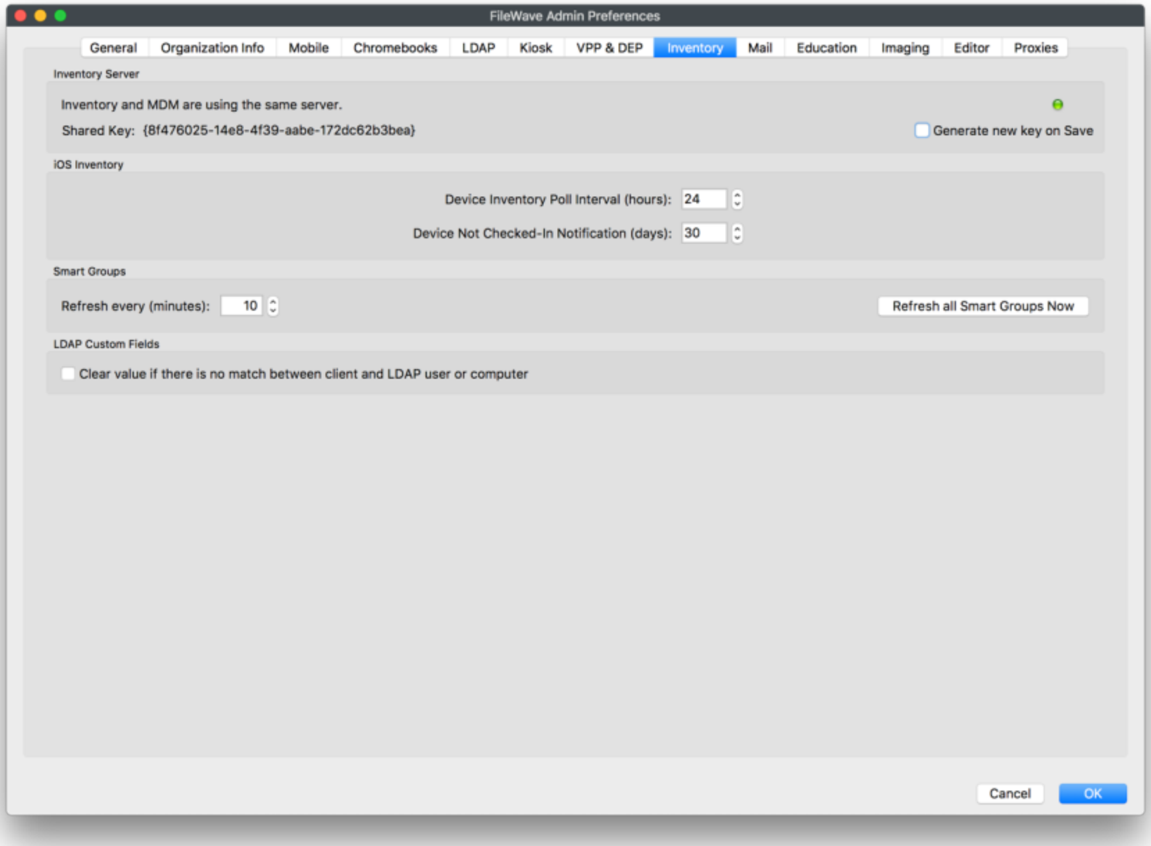
These tools allow changing between control and observe, scale the window between full screen and floating, and save Clipboard contents.
The key advantage of this workflow is its easy access to any FileWave computer Client you have, as long Client and your admin machine can communicate with the FileWave Server.
Note: You may have to adjust the firewall settings (making an allow rule for the publish and monitor ports) on Windows computers for this to work.

8. Working with Inventory and iOS Inventory

Integrated Inventory is a big part of the power of FileWave. 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 set schedule. With the ability to create your own datasets using custom fields, you can track more than just your devices, 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.
One of the strongest features 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 can 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.

8.1. 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 no longer contain a legacy connection to the EOL'd Inventory plus basic settings:



Inventory Server

Inventory and MDM are using the same server. ●

Shared Key: {8f476025-14e8-4f39-aabe-172dc62b3bea}

□ Generate new key on Save

iOS Inventory

Device Inventory Poll Interval (hours): 24

Device Not Checked-In Notification (days): 30

Smart Groups

Refresh every (minutes): 10

LDAP Custom Fields

□ Clear value if there is no match between client and LDAP user or computer

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

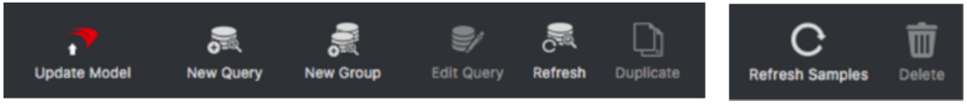
This checkbox is only selected if you are using a separate MDM server and your Inventory server is on this system.

Smart Groups

The button **Refresh all Smart Groups** forces a refresh of all the data requested by existing Smart Groups.
LDAP Custom Fields
If checked this option will clear the value of a LDAP Custom Field if there is no match between client and LDAP user or computer.

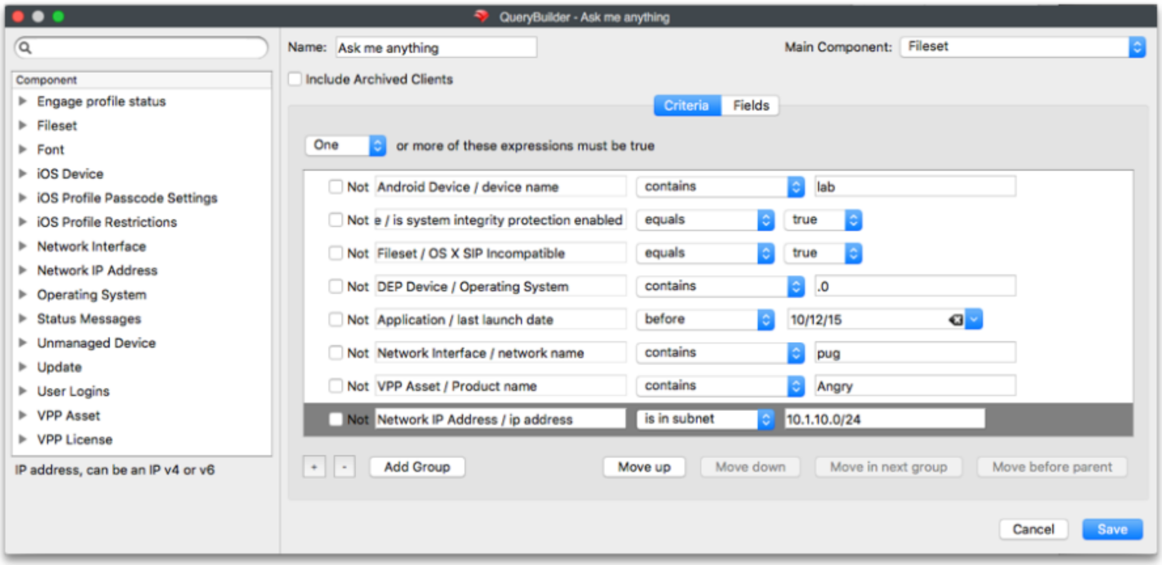
8.2. Inventory Toolbar

The Inventory toolbar consists of six simple tools plus the Delete item:



- ***New Query*** – Creates a new blank query
- ***New Group*** – Creates a new query Group to contain queries specific to any criteria you choose
- ***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 the copy and not the original
- ***Refresh Samples*** – Restores the default sample set we provide to their original state

8.3. Creating and Editing a query



Name: Ask me anything

Main Component: Fileset

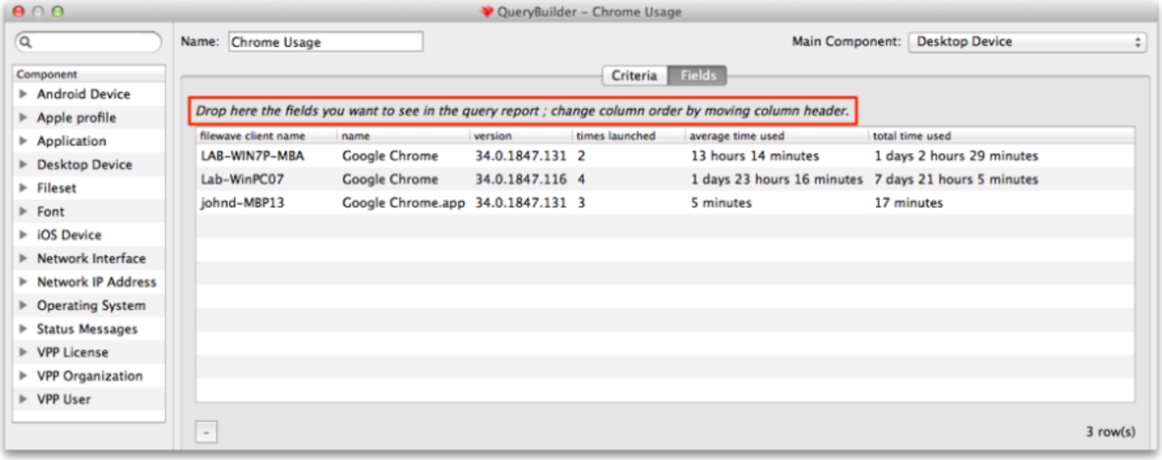
□ Include Archived Clients

One or more of these expressions must be true

□ Not	Android Device / device name	contains	lab
□ Not	e / is system integrity protection enabled	equals	true
□ Not	Fileset / OS X SIP Incompatible	equals	true
□ Not	DEP Device / Operating System	contains	.0
□ Not	Application / last launch date	before	10/12/15
□ Not	Network Interface / network name	contains	pug
□ Not	VPP Asset / Product name	contains	Angry
□ Not	Network IP Address / ip address	is in subnet	10.1.10.0/24

IP address, can be an IP v4 or v6

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.



Name: Chrome Usage

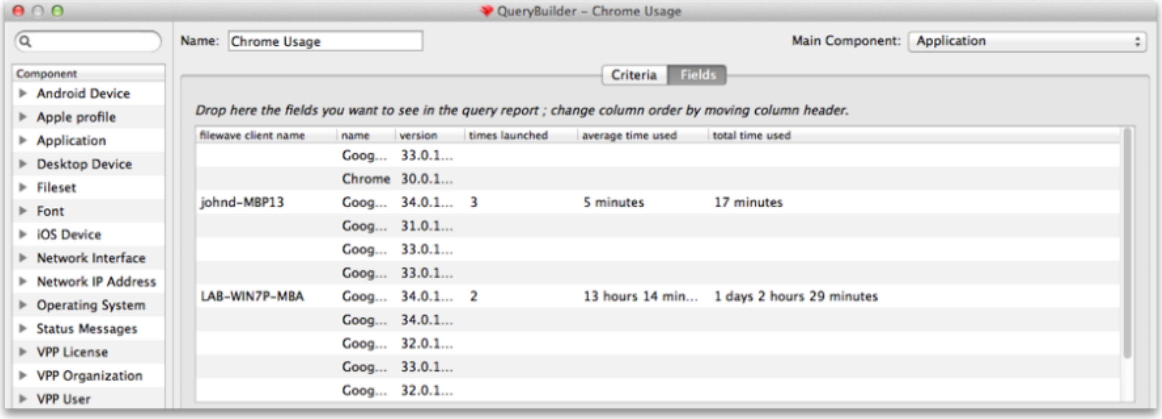
Main Component: Desktop Device

Drop here the fields you want to see in the query report ; change column order by moving column header.

filewave client name	name	version	times launched	average time used	total time used
LAB-WIN7P-MBA	Google Chrome	34.0.1847.131	2	13 hours 14 minutes	1 days 2 hours 29 minutes
Lab-WinPC07	Google Chrome	34.0.1847.116	4	1 days 23 hours 16 minutes	7 days 21 hours 5 minutes
johnd-MBP13	Google Chrome.app	34.0.1847.131	3	5 minutes	17 minutes

3 row(s)

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 should 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.



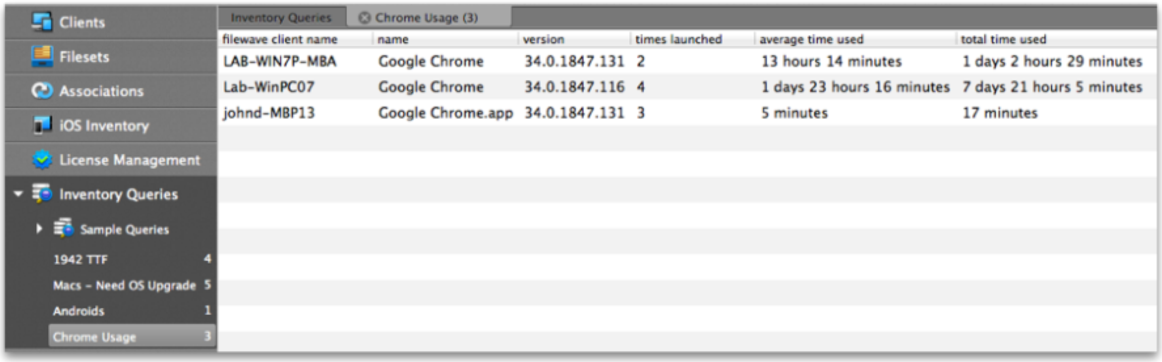
Name: Chrome Usage

Main Component: Application

Drop here the fields you want to see in the query report ; change column order by moving column header.

filewave client name	name	version	times launched	average time used	total time used
	Goog...	33.0.1...			
	Chrome	30.0.1...			
johnd-MBP13	Goog...	34.0.1...	3	5 minutes	17 minutes
	Goog...	31.0.1...			
	Goog...	33.0.1...			
	Goog...	33.0.1...			
LAB-WIN7P-MBA	Goog...	34.0.1...	2	13 hours 14 min...	1 days 2 hours 29 minutes
	Goog...	34.0.1...			
	Goog...	32.0.1...			
	Goog...	33.0.1...			
	Goog...	32.0.1...			

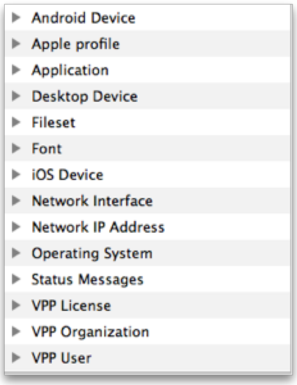
By choosing the correct component, and the right criteria, you can create queries that will tell you exactly what you want to know. In the main Inventory window, you can select your query so that it will display just by clicking on it.



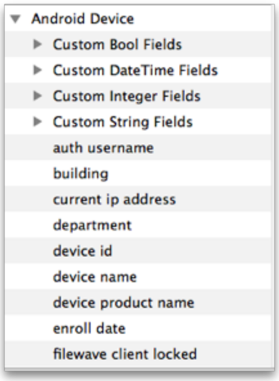
filewave client name	name	version	times launched	average time used	total time used
LAB-WIN7P-MBA	Google Chrome	34.0.1847.131	2	13 hours 14 minutes	1 days 2 hours 29 minutes
Lab-WinPC07	Google Chrome	34.0.1847.116	4	1 days 23 hours 16 minutes	7 days 21 hours 5 minutes
johnd-MBP13	Google Chrome.app	34.0.1847.131	3	5 minutes	17 minutes

Components

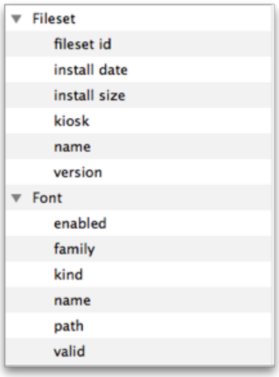
Key to being able to create a useful query is understanding the components you have access to. Here is a sampling of those items:



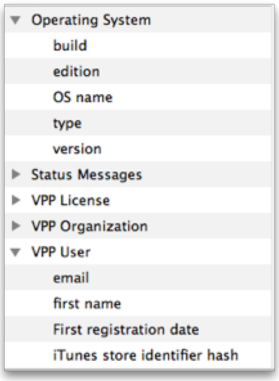
- Android Device
- Apple profile
- Application
- Desktop Device
- Fileset
- Font
- iOS Device
- Network Interface
- Network IP Address
- Operating System
- Status Messages
- VPP License
- VPP Organization
- VPP User



- Android Device
  - Custom Bool Fields
  - Custom DateTime Fields
  - Custom Integer Fields
  - Custom String Fields
  - auth username
  - building
  - current ip address
  - department
  - device id
  - device name
  - device product name
  - enroll date
  - filewave client locked



- Fileset
  - fileset id
  - install date
  - install size
  - kiosk
  - name
  - version
- Font
  - enabled
  - family
  - kind
  - name
  - path
  - valid



- Operating System
  - build
  - edition
  - OS name
  - type
  - version
- Status Messages
- VPP License
- VPP Organization
- VPP User
  - email
  - first name
  - First registration date
  - iTunes store identifier hash

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. You do this by passing arguments to the fwcld command.

The general format used to set any custom.ini value (including new keys) follows this format:

```
$ fwcld -custom_write -key <key_name> [-value <value_to_save] [-silent]
```

Examples

Setting "custom_bool_13" to a false:

```
$ fwcld -custom_write -key custom_bool_13 -value 0
$ fwcld -custom_write -key custom_bool_13 -value false
```

Setting "custom_bool_13" to true:

```
$ fwcld -custom_write -key custom_bool_13 -value 1
$ fwcld -custom_write -key custom_bool_13 -value true
$ fwcld -custom_write -key custom_bool_13 -value something
```

Setting "custom_date_02" to a date:

```
$ fwcld -custom_write -key custom_date_02 -value 2014-02-20T15:22:43
```

To remove any key value, just leave off the -value parameter - so to reset the "custom_date_02" value back to it's default.

```
$ fwcld -custom_write -key custom_date_02
```

Notes

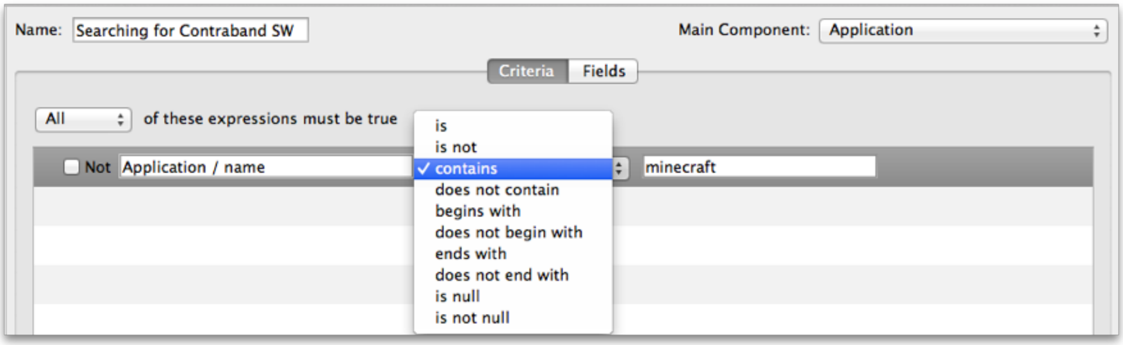
1. When a provided key name matches integer, date or boolean custom field names - the program will validate the provided input. If this validation fails, an error message is printed and the program will exit without setting the custom.ini value.
2. When any failure to set a custom.ini value occurs, the program will exit with code 1, if setting the value succeeds the exit code is 0.

Add FileWave Custom Inventory fields remotely using a Fileset

Expressions

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 this example, we are looking for any instance of an application where the name contains the text "minecraft" -



Name: Searching for Contraband SW

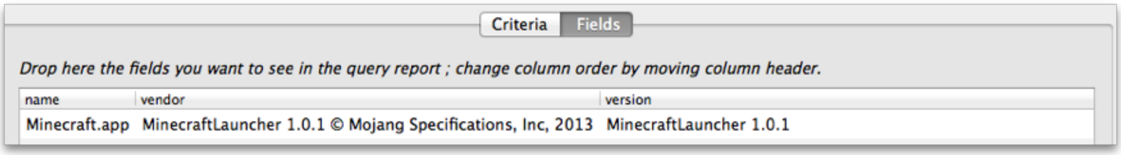
Main Component: Application

All of these expressions must be true

□ Not Application / name ✓ contains minecraft

Field values

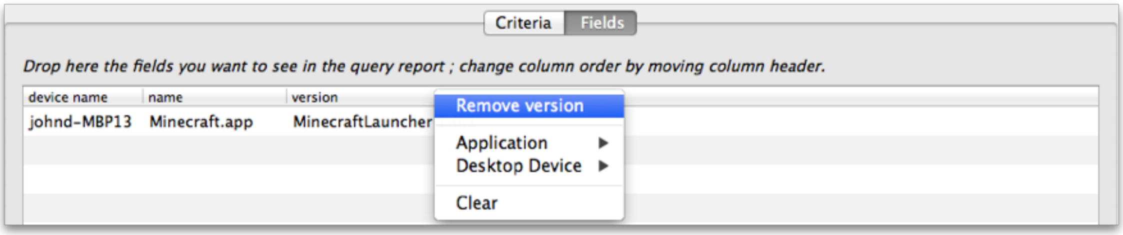
The whole purpose behind the query is to get useful information out of inventory. You do this by adding fields to display the results of answers to your query. In Inventory, you access the same components you use as criteria for the search as the display fields. In our example, we are looking for "minecraft" but if we left it at that, all we would get back from the FileWave database is "yup, I found it. Now what?"



Drop here the fields you want to see in the query report ; change column order by moving column header.

name	vendor	version
Minecraft.app	MinecraftLauncher 1.0.1 © Mojang Specifications, Inc, 2013	MinecraftLauncher 1.0.1

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.



Drop here the fields you want to see in the query report ; change column order by moving column header.

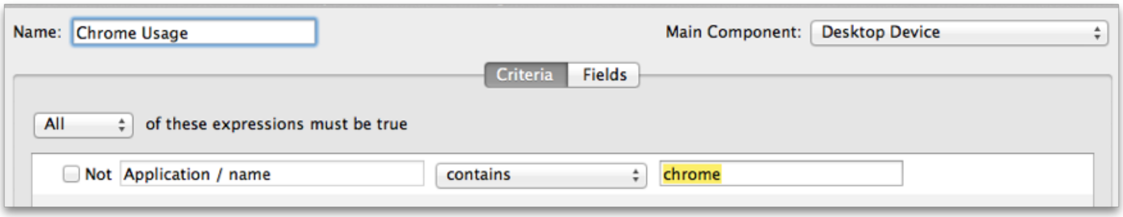
device name	name	version
johnd-MBP13	Minecraft.app	MinecraftLauncher

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

A powerful tool in the Inventory / License Management 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:

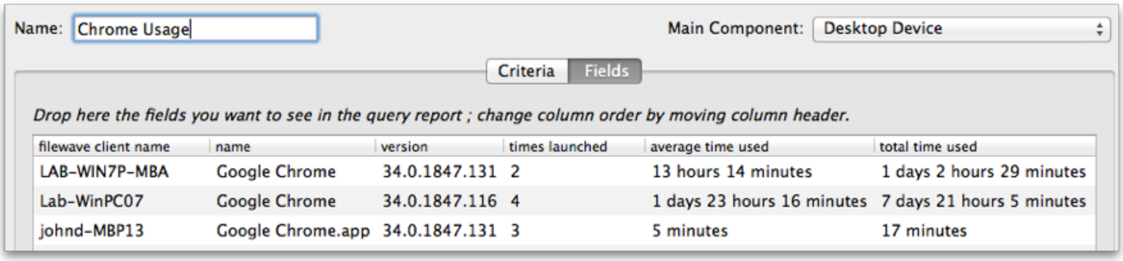


Name: Chrome Usage

Main Component: Desktop Device

All of these expressions must be true

□ Not Application / name contains chrome



Name: Chrome Usage

Main Component: Desktop Device

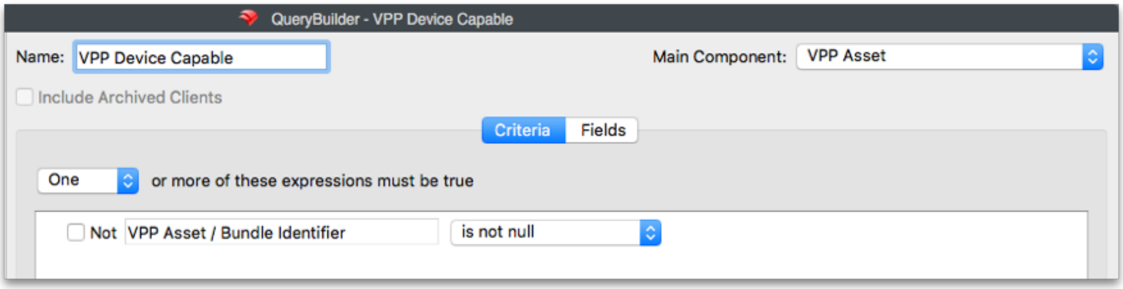
Drop here the fields you want to see in the query report ; change column order by moving column header.

filewave client name	name	version	times launched	average time used	total time used
LAB-WIN7P-MBA	Google Chrome	34.0.1847.131	2	13 hours 14 minutes	1 days 2 hours 29 minutes
Lab-WinPC07	Google Chrome	34.0.1847.116	4	1 days 23 hours 16 minutes	7 days 21 hours 5 minutes
johnd-MBP13	Google Chrome.app	34.0.1847.131	3	5 minutes	17 minutes

You can see that adding the proper fields, as well as choosing the proper index or Main Component for the display, you get a good bit of information from this query.

Example - Identifying VPP applications that support device assignment

With the functionality in Apple's VPP of directly assigning applications to FileWave client devices, you have the challenge of finding out which of your many applications support that feature. Here is a query you can set up to determine which of your deployed Filesets support device assignment.



QueryBuilder - VPP Device Capable

Name: VPP Device Capable

Main Component: VPP Asset

□ Include Archived Clients

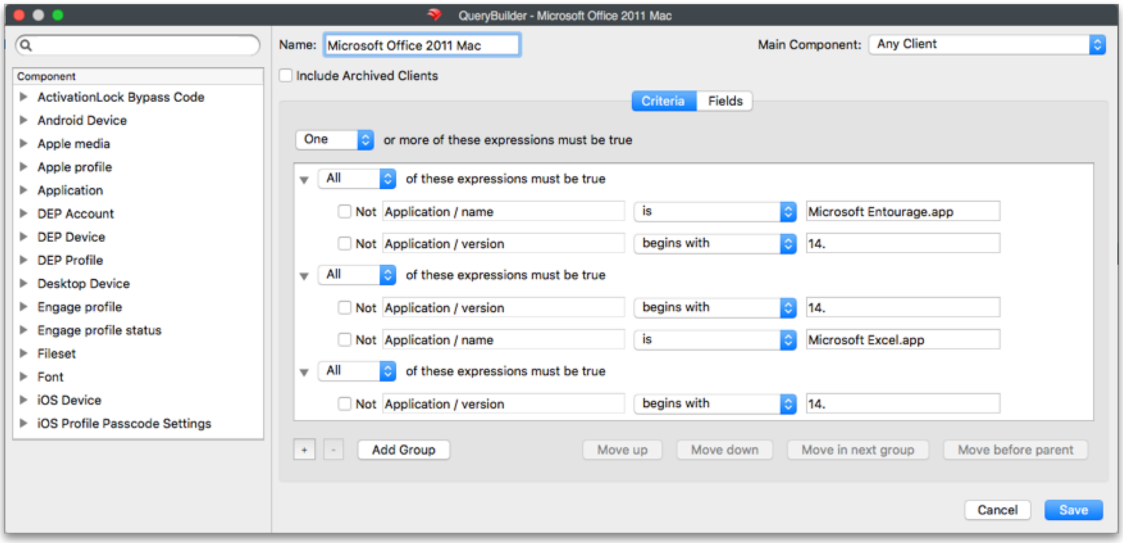
One or more of these expressions must be true

□ Not VPP Asset / Bundle Identifier is not null

The Fields include the *product name* and, most importantly, the *Device assignable flag*. The results don't show every VPP application and its status, only the ones that are already active.

8.4. 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.


QueryBuilder - Microsoft Office 2011 Mac

Component
- ActivationLock Bypass Code
- Android Device
- Apple media
- Apple profile
- Application
- DEP Account
- DEP Device
- DEP Profile
- Desktop Device
- Engage profile
- Engage profile status
- Fileset
- Font
- iOS Device
- iOS Profile Passcode Settings

Name: Microsoft Office 2011 Mac Main Component: Any Client

□ Include Archived Clients

Criteria | Fields

One or more of these expressions must be true

All of these expressions must be true
- □ Not Application / name is Microsoft Entourage.app
- □ Not Application / version begins with 14.

All of these expressions must be true
- □ Not Application / version begins with 14.
- □ Not Application / name is Microsoft Excel.app

All of these expressions must be true
- □ Not Application / version begins with 14.

8.5. Creating Query Groups

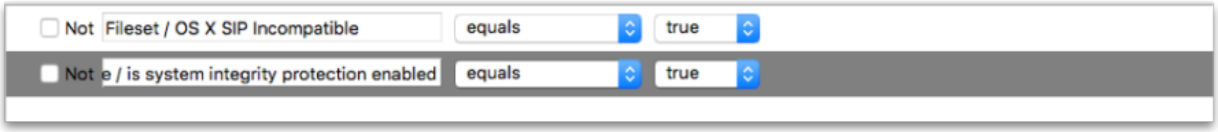
The idea behind *Query Groups* is that you might need to isolate queries into families of devices, operating systems, applications, or even based on results. Groups such as iOS Devices, Riverview Office, Campus ConfRms, etc. would all make sensible Inventory Groups. Just create the Group, name it, and drag the appropriate queries into it.

8.6. 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 certain 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.

Example - Locating Filesets that contain *SIP* violations

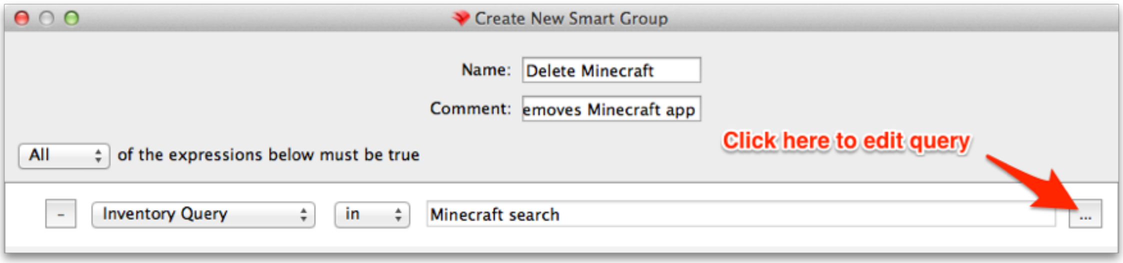
Apple has released a security policy with OS X 10.11 called **System Integrity Protection**. In a nutshell, it says that no process will be able to have write access to any area of the OS that is protected. FileWave administrators may have scripts that violate this policy, and need to find out which are affected other than just seeing their Fileset(s) 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:


- □ Not Fileset / OS X SIP Incompatible equals true
- □ Not e / is system integrity protection enabled equals true

If you use either one of these to create a Smart Group, you will be able to rapidly identify your Macs that have SIP active, or your Filesets that have incompatible code in them. As you repair the Filesets, they will drop from that Smart Group. If someone turns off the SIP settings (not an easy task), the affected Mac will drop off that Smart Group.

Example - 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:



Create New Smart Group

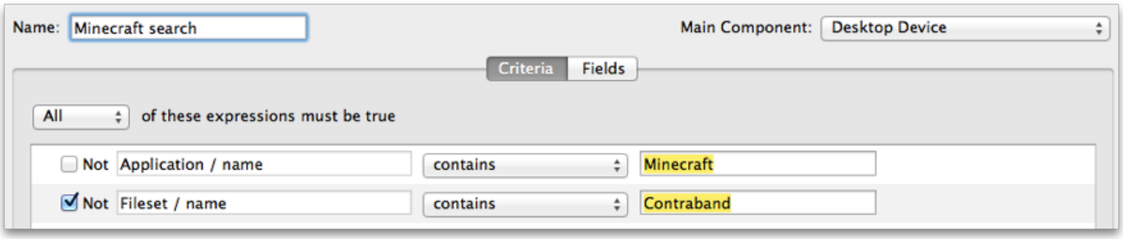
Name: Delete Minecraft

Comment: emoves Minecraft app

All of the expressions below must be true

Click here to edit query

- Inventory Query in Minecraft search ...

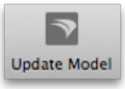


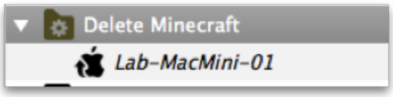
Name: Minecraft search

Main Component: Desktop Device

All of these expressions must be true

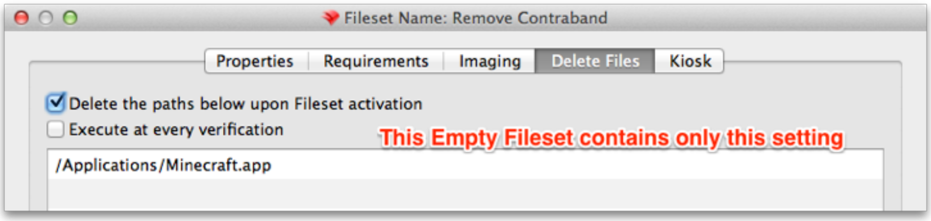
□ Not	Application / name	contains	Minecraft
☑ Not	Fileset / name	contains	Contraband





Delete Minecraft

Lab-MacMini-01



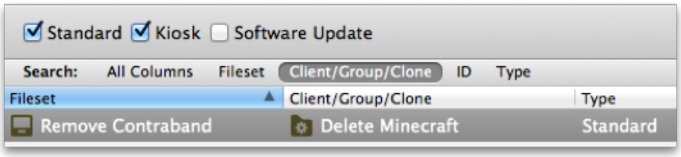
Fileset Name: Remove Contraband

☑ Delete the paths below upon Fileset activation

□ Execute at every verification

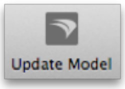
This Empty Fileset contains only this setting

/Applications/Minecraft.app



☑ Standard ☑ Kiosk □ Software Update

Fileset	Client/Group/Clone	Type
Remove Contraband	Delete Minecraft	Standard



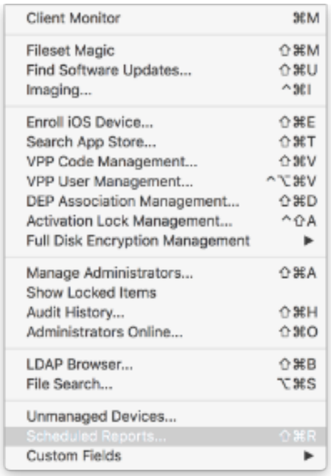
Once you have executed the **Update Model** command, the Fileset will execute and delete the software.

8.7. Generating scheduled reports

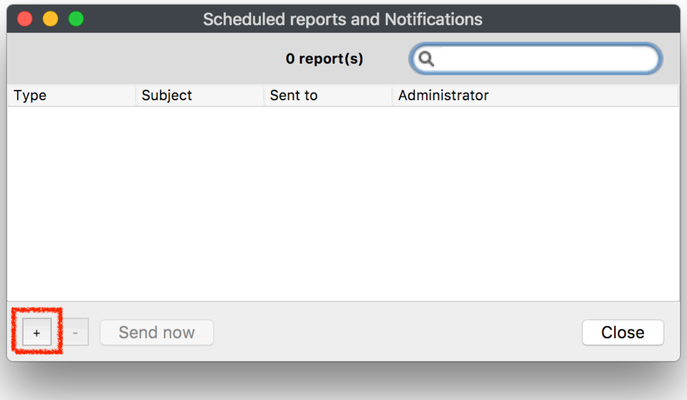
Being able to look at the various queries while logged in to the FileWave Admin is one thing. Being able to have the results of a query automatically sent to your or someone else's email inbox at the same time every week is much better. FileWave supports creating scheduled reports from queries and the process is very simple.

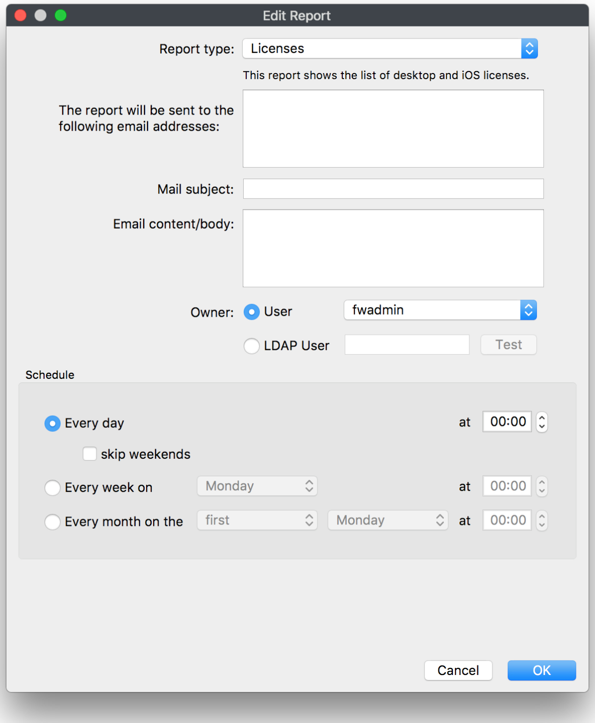
How to create Scheduled Reports

1. First, you select **Assistants Scheduled Reports…** from the FileWave Admin menubar.


Client Monitor ⌘M
Fileset Magic ⇧⌘M
Find Software Updates... ⇧⌘U
Imaging... ^⌘I
Enroll iOS Device... ⇧⌘E
Search App Store... ⇧⌘T
VPP Code Management... ⇧⌘V
VPP User Management... ^⌥⌘V
DEP Association Management... ⇧⌘D
Activation Lock Management... ^⇧A
Full Disk Encryption Management ▶
Manage Administrators... ⇧⌘A
Show Locked Items
Audit History... ⇧⌘H
Administrators Online... ⇧⌘O
LDAP Browser... ⇧⌘B
File Search... ⌥⌘S
Unmanaged Devices...
Scheduled Reports... ⇧⌘R
Custom Fields ▶

2. Then click the "+" in the lower left of the window to create a new report. If you had existing reports they would be visible here.





Report type: Licenses

This report shows the list of desktop and iOS licenses.

The report will be sent to the following email addresses:

Mail subject:

Email content/body:

Owner: ● User fwadmin

○ LDAP User

Schedule

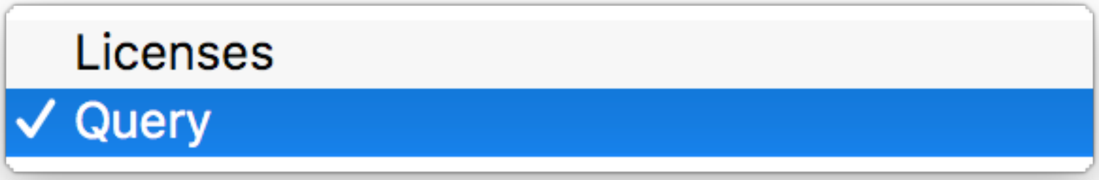
● Every day at 00:00

□ skip weekends

○ Every week on Monday at 00:00

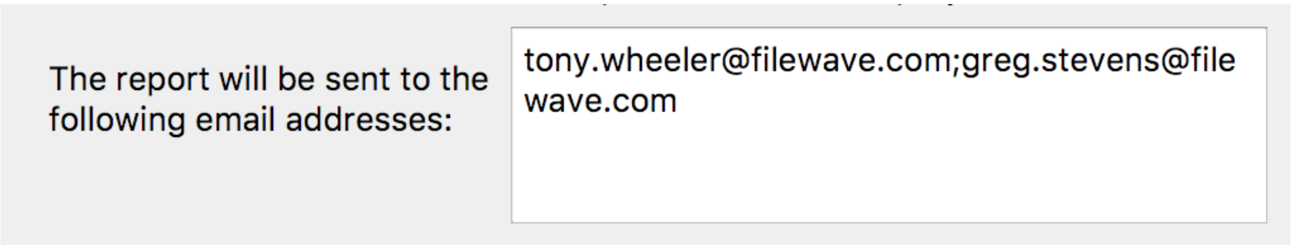
○ Every month on the first Monday at 00:00

3. You can now choose a **Report Type** which are a License or Query report.
    a. License: This will create a report of everything that is listed in your **License Management** section in FileWave. This includes all VPP licenses and manually created licenses from Filesets or inventory.
    b. Query: This option will send a report with the results of a specific inventory query that was created in the **Inventory Management** section in FileWave.



4. Next is to type in what email address you want to send these reports too.

Multiple Email Addresses
If you would like to send to multiple email addressrd you will need to separate the addresses by a semicolon.

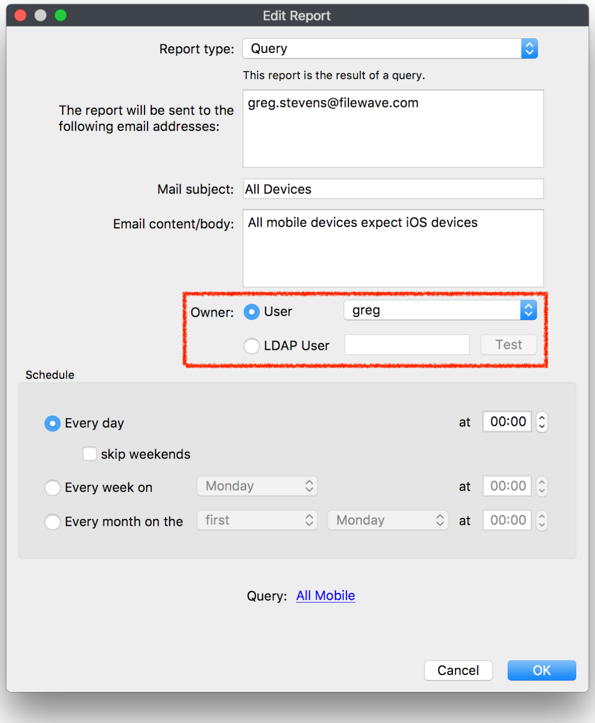


The report will be sent to the following email addresses: tony.wheeler@filewave.com;greg.stevens@filewave.com

5. Then add in a **Mail Subject** and the **Email content/body**, these will give some definition to the reports sent.
6. Next if you are signed into the FileWave Admin as the **Superuser** you will see a section for **Owner.** Whichever user account is selected will affect the results of the Scheduled Report based on that users permissions.

Example: If the user Greg Stevens was selected as the owner of this report for a query of all devices but Greg does not have access to see any iOS devices then the report will not show iOS.

> If you are not the Superuser you will NOT see the **Owner** section at all; as you can see in the screenshots below, only the Superuser can assign a user to reports.



Edit Report

Report type: Query

This report is the result of a query.

The report will be sent to the following email addresses: greg.stevens@filewave.com

Mail subject: All Devices

Email content/body: All mobile devices expect iOS devices

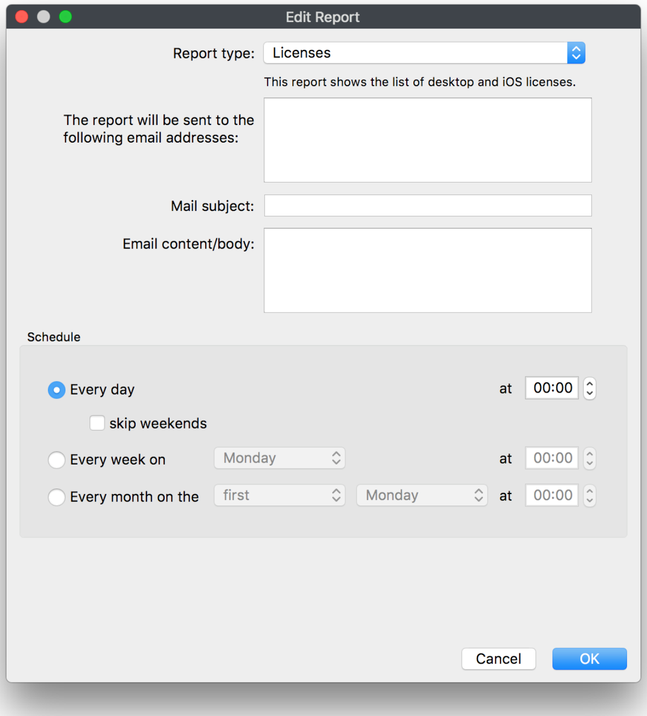
Owner: ● User greg
○ LDAP User Test

Schedule

● Every day at 00:00
□ skip weekends
○ Every week on Monday at 00:00
○ Every month on the first Monday at 00:00

Query: All Mobile

Cancel OK



Edit Report

Report type: Licenses

This report shows the list of desktop and iOS licenses.

The report will be sent to the following email addresses:

Mail subject:

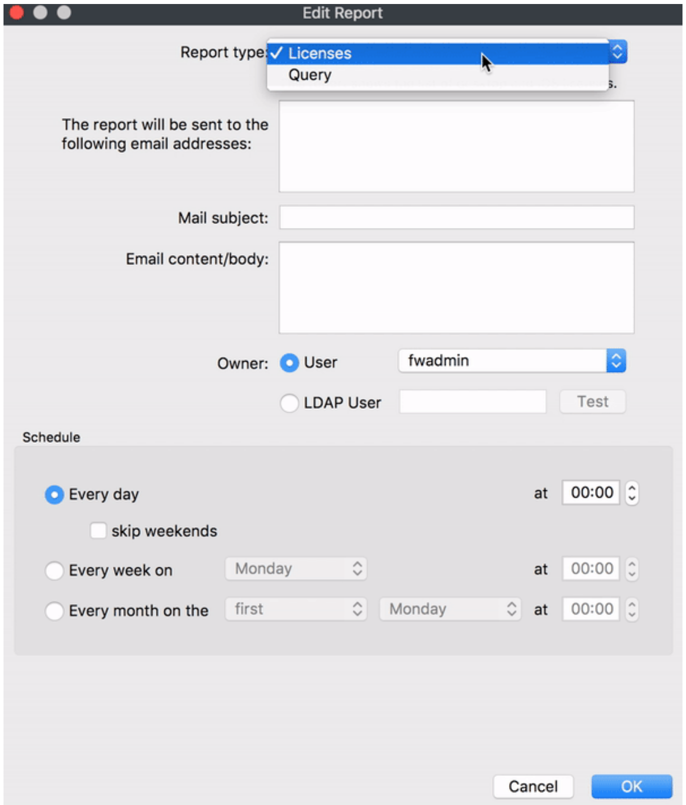
Email content/body:

Schedule

● Every day at 00:00
□ skip weekends
○ Every week on Monday at 00:00
○ Every month on the first Monday at 00:00

Cancel OK

7. After you have selected an **Owner** you will need to set when the report is going to be sent out
    a. Every day
        i. skip weekends
    b. Every week on
    c. Every month on
8. Optional - if the **Report Type** is set to **Query** you will need to select which query the report will send



Edit Report

Report type: ✓ Licenses
Query

The report will be sent to the following email addresses:

Mail subject:

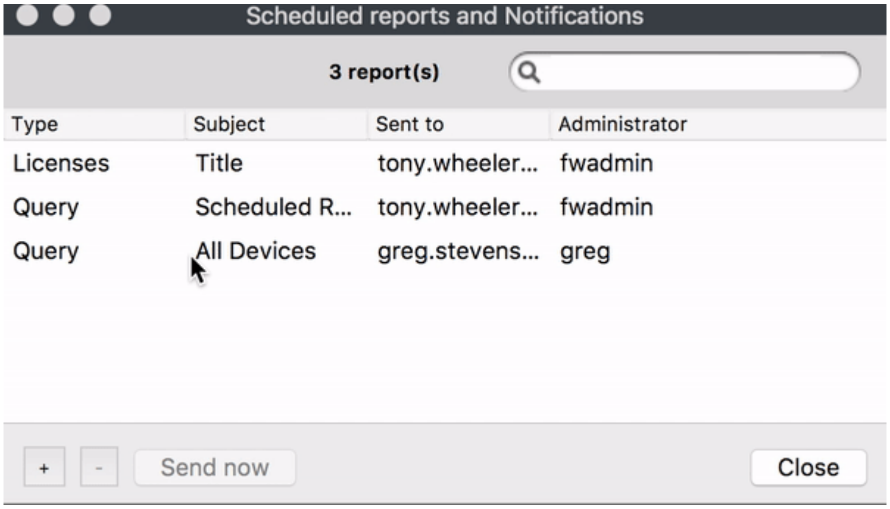
Email content/body:

Owner: ● User fwadmin
○ LDAP User

Schedule

● Every day at 00:00
□ skip weekends
○ Every week on Monday at 00:00
○ Every month on the first Monday at 00:00

9. Click **OK** to save this scheduled report, you will then be able to view any previously created reports as well as the option to send the report out immediately.



Scheduled reports and Notifications

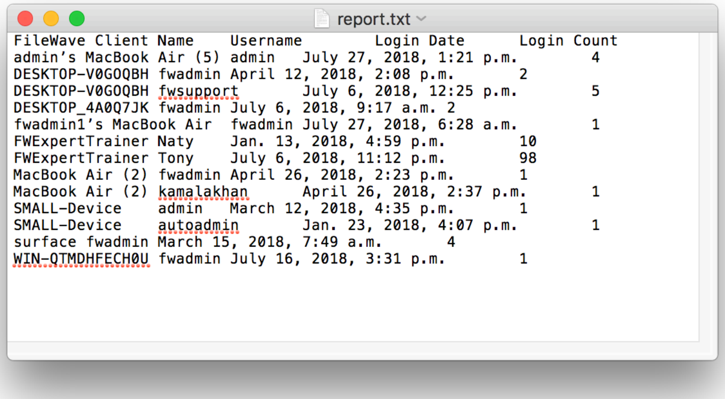
3 report(s)

Type	Subject	Sent to	Administrator
Licenses	Title	tony.wheeler...	fwadmin
Query	Scheduled R...	tony.wheeler...	fwadmin
Query	All Devices	greg.stevens...	greg

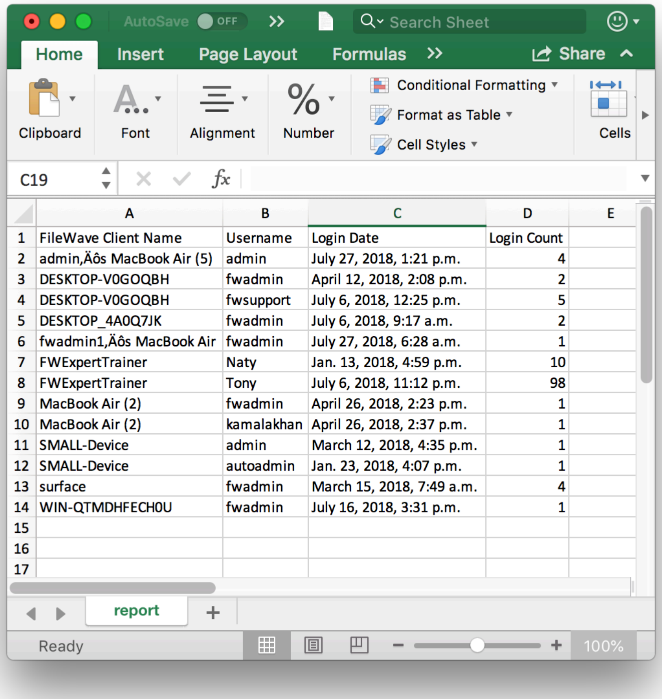
Scheduled Reports Results

The reports that get sent will be tab-delimited text files that you can easily convert or import into any editor you like to use.

1. Query Results

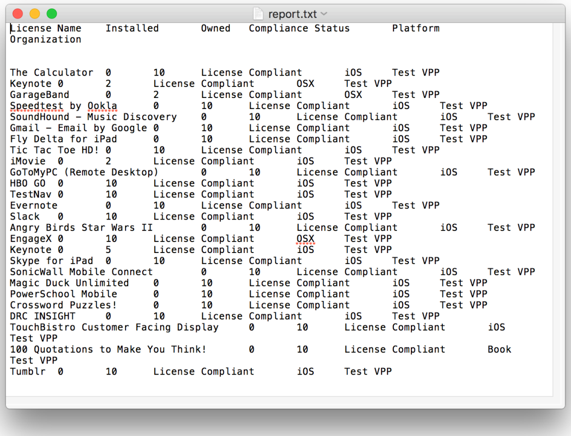


```
FileWave Client Name    Username        Login Date      Login Count
admin’s MacBook Air (5) admin   July 27, 2018, 1:21 p.m.        4
DESKTOP-V0GOQBH fwadmin April 12, 2018, 2:08 p.m.       2
DESKTOP-V0GOQBH fwsupport       July 6, 2018, 12:25 p.m.        5
DESKTOP_4A0Q7JK fwadmin July 6, 2018, 9:17 a.m. 2
fwadmin1’s MacBook Air  fwadmin July 27, 2018, 6:28 a.m.        1
FWExpertTrainer Naty    Jan. 13, 2018, 4:59 p.m.        10
FWExpertTrainer Tony    July 6, 2018, 11:12 p.m.        98
MacBook Air (2) fwadmin April 26, 2018, 2:23 p.m.       1
MacBook Air (2) kamalakhan      April 26, 2018, 2:37 p.m.       1
SMALL-Device    admin   March 12, 2018, 4:35 p.m.       1
SMALL-Device    autoadmin       Jan. 23, 2018, 4:07 p.m.        1
surface fwadmin March 15, 2018, 7:49 a.m.       4
WIN-QTMDHFECH0U fwadmin July 16, 2018, 3:31 p.m.        1
```

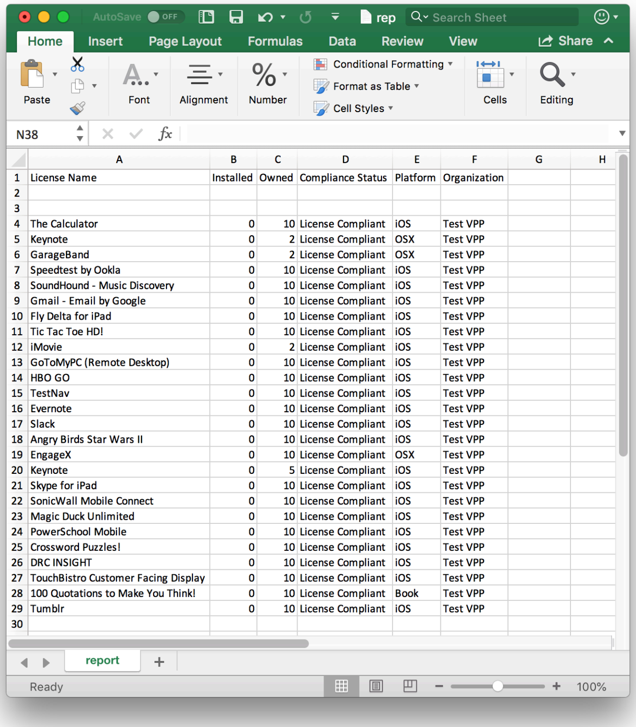


	A	B	C	D	E
1	FileWave Client Name	Username	Login Date	Login Count	
2	admin‚Äôs MacBook Air (5)	admin	July 27, 2018, 1:21 p.m.	4	
3	DESKTOP-V0GOQBH	fwadmin	April 12, 2018, 2:08 p.m.	2	
4	DESKTOP-V0GOQBH	fwsupport	July 6, 2018, 12:25 p.m.	5	
5	DESKTOP_4A0Q7JK	fwadmin	July 6, 2018, 9:17 a.m.	2	
6	fwadmin1‚Äôs MacBook Air	fwadmin	July 27, 2018, 6:28 a.m.	1	
7	FWExpertTrainer	Naty	Jan. 13, 2018, 4:59 p.m.	10	
8	FWExpertTrainer	Tony	July 6, 2018, 11:12 p.m.	98	
9	MacBook Air (2)	fwadmin	April 26, 2018, 2:23 p.m.	1	
10	MacBook Air (2)	kamalakhan	April 26, 2018, 2:37 p.m.	1	
11	SMALL-Device	admin	March 12, 2018, 4:35 p.m.	1	
12	SMALL-Device	autoadmin	Jan. 23, 2018, 4:07 p.m.	1	
13	surface	fwadmin	March 15, 2018, 7:49 a.m.	4	
14	WIN-QTMDHFECH0U	fwadmin	July 16, 2018, 3:31 p.m.	1	
15					
16					
17					

2. License Results



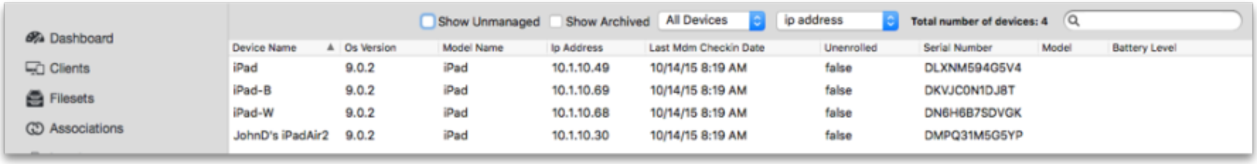
```
License Name    Installed       Owned   Compliance Status       Platform
Organization


The Calculator  0       10      License Compliant       iOS     Test VPP
Keynote 0       2       License Compliant       OSX     Test VPP
GarageBand      0       2       License Compliant       OSX     Test VPP
Speedtest by Ookla      0       10      License Compliant       iOS     Test VPP
SoundHound – Music Discovery    0       10      License Compliant       iOS     Test VPP
Gmail – Email by Google 0       10      License Compliant       iOS     Test VPP
Fly Delta for iPad      0       10      License Compliant       iOS     Test VPP
Tic Tac Toe HD! 0       10      License Compliant       iOS     Test VPP
iMovie  0       2       License Compliant       iOS     Test VPP
GoToMyPC (Remote Desktop)       0       10      License Compliant       iOS     Test VPP
HBO GO  0       10      License Compliant       iOS     Test VPP
TestNav 0       10      License Compliant       iOS     Test VPP
Evernote        0       10      License Compliant       iOS     Test VPP
Slack   0       10      License Compliant       iOS     Test VPP
Angry Birds Star Wars II        0       10      License Compliant       iOS     Test VPP
EngageX 0       10      License Compliant       OSX     Test VPP
Keynote 0       5       License Compliant       iOS     Test VPP
Skype for iPad  0       10      License Compliant       iOS     Test VPP
SonicWall Mobile Connect        0       10      License Compliant       iOS     Test VPP
Magic Duck Unlimited    0       10      License Compliant       iOS     Test VPP
PowerSchool Mobile      0       10      License Compliant       iOS     Test VPP
Crossword Puzzles!      0       10      License Compliant       iOS     Test VPP
DRC INSIGHT     0       10      License Compliant       iOS     Test VPP
TouchBistro Customer Facing Display     0       10      License Compliant       iOS
Test VPP
100 Quotations to Make You Think!       0       10      License Compliant       Book
Test VPP
Tumblr  0       10      License Compliant       iOS     Test VPP
```



	A	B	C	D	E	F	G	H
1	License Name	Installed	Owned	Compliance Status	Platform	Organization		
2								
3								
4	The Calculator	0	10	License Compliant	iOS	Test VPP		
5	Keynote	0	2	License Compliant	OSX	Test VPP		
6	GarageBand	0	2	License Compliant	OSX	Test VPP		
7	Speedtest by Ookla	0	10	License Compliant	iOS	Test VPP		
8	SoundHound - Music Discovery	0	10	License Compliant	iOS	Test VPP		
9	Gmail - Email by Google	0	10	License Compliant	iOS	Test VPP		
10	Fly Delta for iPad	0	10	License Compliant	iOS	Test VPP		
11	Tic Tac Toe HD!	0	10	License Compliant	iOS	Test VPP		
12	iMovie	0	2	License Compliant	iOS	Test VPP		
13	GoToMyPC (Remote Desktop)	0	10	License Compliant	iOS	Test VPP		
14	HBO GO	0	10	License Compliant	iOS	Test VPP		
15	TestNav	0	10	License Compliant	iOS	Test VPP		
16	Evernote	0	10	License Compliant	iOS	Test VPP		
17	Slack	0	10	License Compliant	iOS	Test VPP		
18	Angry Birds Star Wars II	0	10	License Compliant	iOS	Test VPP		
19	EngageX	0	10	License Compliant	OSX	Test VPP		
20	Keynote	0	5	License Compliant	iOS	Test VPP		
21	Skype for iPad	0	10	License Compliant	iOS	Test VPP		
22	SonicWall Mobile Connect	0	10	License Compliant	iOS	Test VPP		
23	Magic Duck Unlimited	0	10	License Compliant	iOS	Test VPP		
24	PowerSchool Mobile	0	10	License Compliant	iOS	Test VPP		
25	Crossword Puzzles!	0	10	License Compliant	iOS	Test VPP		
26	DRC INSIGHT	0	10	License Compliant	iOS	Test VPP		
27	TouchBistro Customer Facing Display	0	10	License Compliant	iOS	Test VPP		
28	100 Quotations to Make You Think!	0	10	License Compliant	Book	Test VPP		
29	Tumblr	0	10	License Compliant	iOS	Test VPP		
30								

8.8. 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.



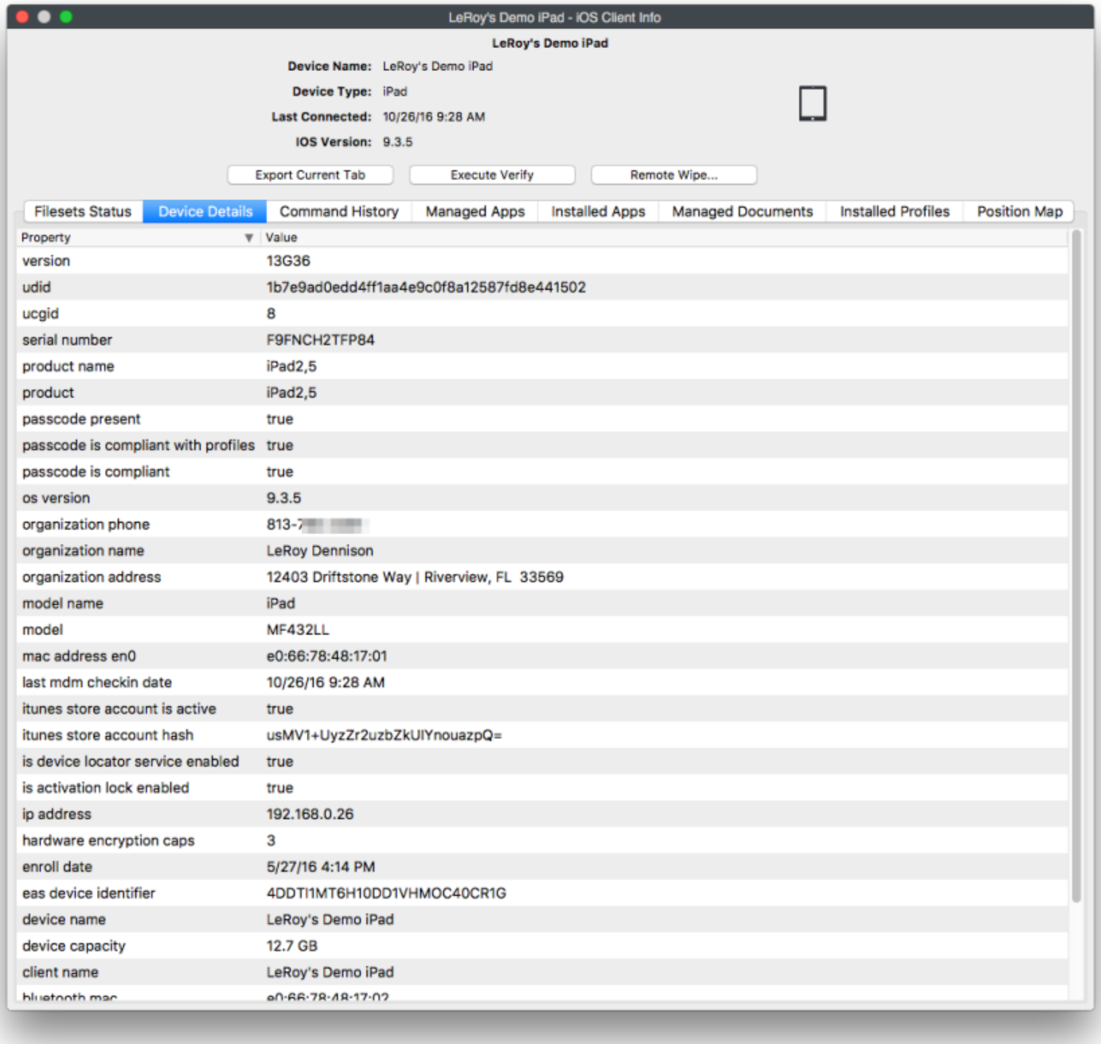
Total number of devices: 4

Device Name ▲	Os Version	Model Name	Ip Address	Last Mdm Checkin Date	Unenrolled	Serial Number	Model	Battery Level
iPad	9.0.2	iPad	10.1.10.49	10/14/15 8:19 AM	false	DLXNM594G5V4		
iPad-B	9.0.2	iPad	10.1.10.69	10/14/15 8:19 AM	false	DKVJC0N1DJ8T		
iPad-W	9.0.2	iPad	10.1.10.68	10/14/15 8:19 AM	false	DN6H6B7SDVGK		
JohnD's iPadAir2	9.0.2	iPad	10.1.10.30	10/14/15 8:19 AM	false	DMPQ31M5G5YP		

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.



LeRoy's Demo iPad

Device Name: LeRoy's Demo iPad
Device Type: iPad
Last Connected: 10/26/16 9:28 AM
iOS Version: 9.3.5

Property	Value
version	13G36
udid	1b7e9ad0edd4ff1aa4e9c0f8a12587fd8e441502
ucgid	8
serial number	F9FNCH2TFP84
product name	iPad2,5
product	iPad2,5
passcode present	true
passcode is compliant with profiles	true
passcode is compliant	true
os version	9.3.5
organization phone	813-7[redacted]
organization name	LeRoy Dennison
organization address	12403 Driftstone Way | Riverview, FL 33569
model name	iPad
model	MF432LL
mac address en0	e0:66:78:48:17:01
last mdm checkin date	10/26/16 9:28 AM
itunes store account is active	true
itunes store account hash	usMV1+UyzZr2uzbZkUlYnouazpQ=
is device locator service enabled	true
is activation lock enabled	true
ip address	192.168.0.26
hardware encryption caps	3
enroll date	5/27/16 4:14 PM
eas device identifier	4DDTI1MT6H10DD1VHMOC40CR1G
device name	LeRoy's Demo iPad
device capacity	12.7 GB
client name	LeRoy's Demo iPad
bluetooth mac	e0:66:78:48:17:02

The window also provides all of the key details about your iOS device:

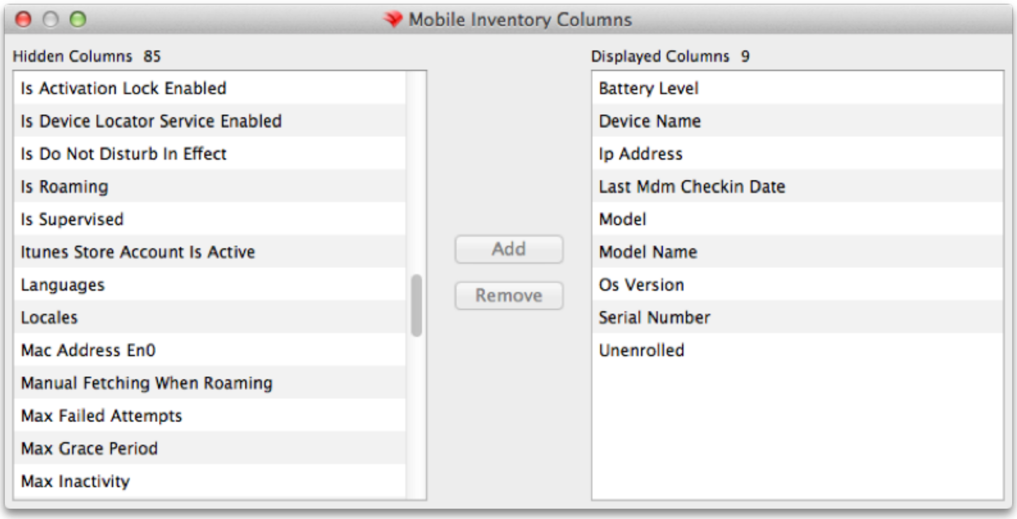
- ***Fileset Status*** – This shows the list of Filesets that have been installed on the device.
- ***Device Details*** – This displays technical information on the device to include UDID, serial number, etc.
- ***Command History*** – This displays the commands sent from FileWave server to the device with actions and results.
- ***Managed Apps*** – This shows the applications sent from FileWave as Filesets.
- *Installed Apps* – This displays all applications, other than the built-in one, that were not sent by FileWave. It shows the applications installed by the user.
- ***Managed Documents*** – This shows a list of any documents that have been installed using a Fileset.
- ***Installed Profiles*** – This displays the profiles on the device from the the FileWave MDM server.
- ***Position Map*** – This shows a map displaying the last reported position for devices in which tracking has been enabled.

Refresh

This toolbar command forces the devices listed to be refreshed from information in inventory. 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.



Mobile Inventory Columns

Hidden Columns 85

- Is Activation Lock Enabled
- Is Device Locator Service Enabled
- Is Do Not Disturb In Effect
- Is Roaming
- Is Supervised
- Itunes Store Account Is Active
- Languages
- Locales
- Mac Address En0
- Manual Fetching When Roaming
- Max Failed Attempts
- Max Grace Period
- Max Inactivity

Displayed Columns 9

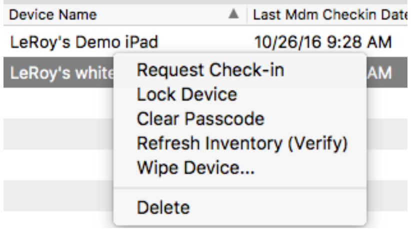
- Battery Level
- Device Name
- Ip Address
- Last Mdm Checkin Date
- Model
- Model Name
- Os Version
- Serial Number
- Unenrolled

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. You can also see a list of **Archived** iOS devices, if you have any that were previously enrolled, but have since been archived.

Contextual Menu

The contextual menu, from right-clicking a device, 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.



Device Name	Last Mdm Checkin Date
LeRoy's Demo iPad	10/26/16 9:28 AM
LeRoy's white	AM

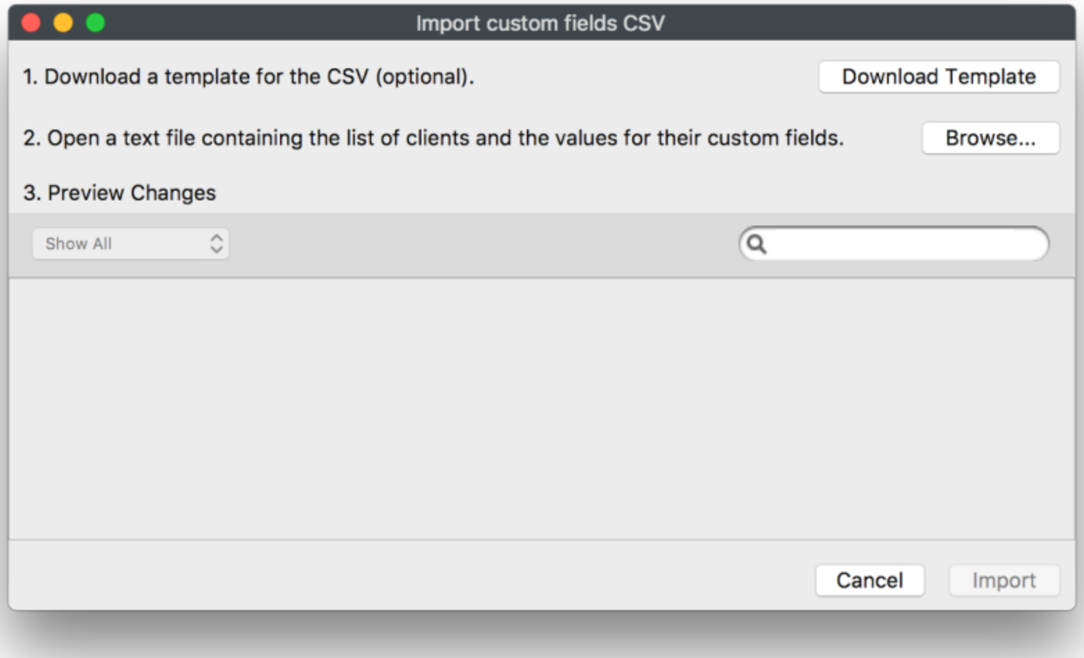
8.9. Custom Fields

Added in FileWave 12.7.0, Custom Fields will allow you to create custom inventory values and assign them to your devices in a 5 different ways. You will find this option under the **Assistants** menu called **Custom Fields**, from there you can either **Import CSV** or **Edit Custom Fields**. The Edit Custom Fields section has four different options you can chose from that will allow you to create custom fields and in turn assign those values to devices.

Important Note:
You cannot use special characters in the creation of Custom Fields!

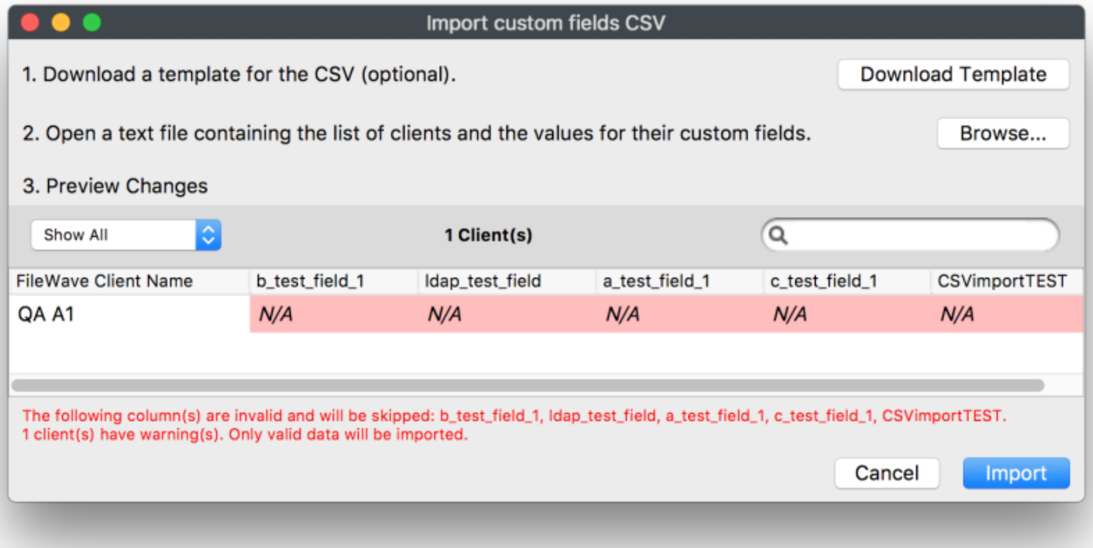
Importing from a CSV

This will allow you to change values of Custom Fields that have already been associated to devices in bulk. In the Import Custom Fields CSV window we provide a template that will let you choose not only which existing custom fields you would like in the template, but also how you would like to identify devices. Identifying devices in this section can be done with FileWave Client Name, Serial Number, Device ID, or FileWave ID. *Note*: It is important to remember that the only custom field values that will be changed are ones that have already been associated in FileWave to your devices. If you upload a CSV that specifies a value for a device that does not have the corresponding custom fields associate to it prior to upload, then you will see an error telling you those values were skipped.



Import custom fields CSV

1. Download a template for the CSV (optional).
2. Open a text file containing the list of clients and the values for their custom fields.
3. Preview Changes



Import custom fields CSV

1. Download a template for the CSV (optional).
2. Open a text file containing the list of clients and the values for their custom fields.
3. Preview Changes

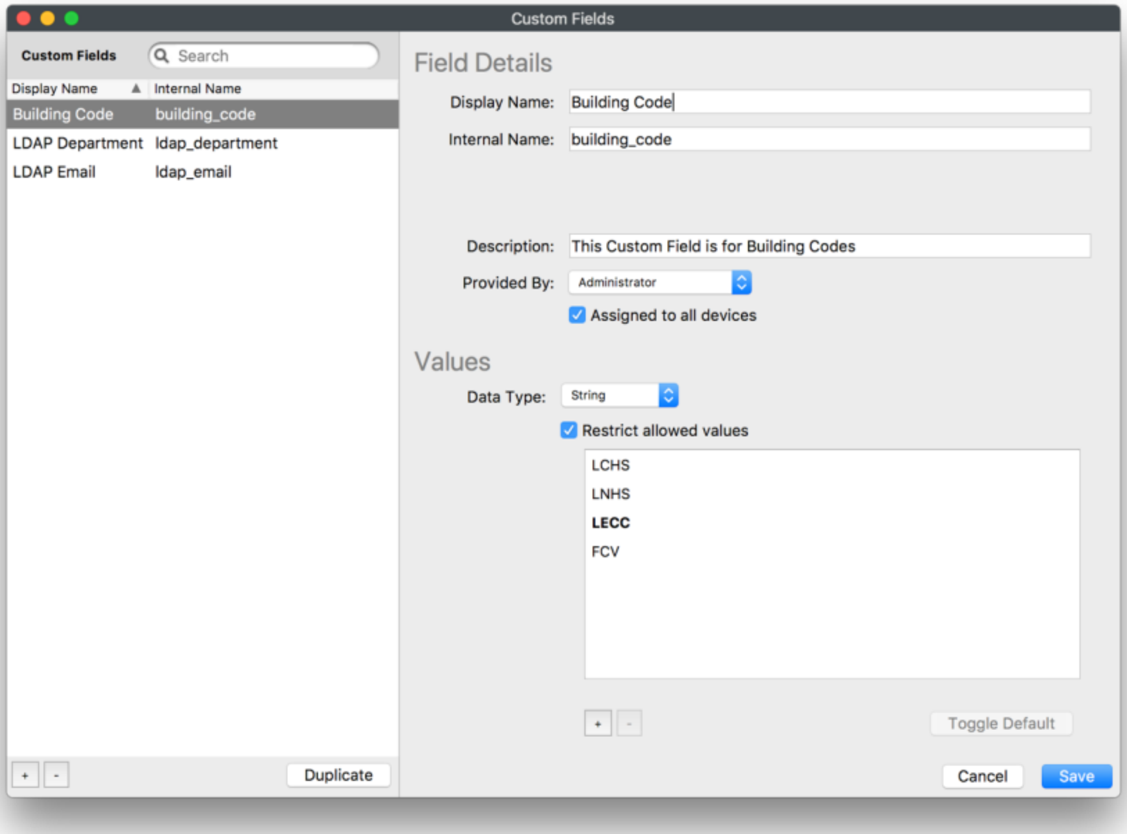
1 Client(s)

FileWave Client Name	b_test_field_1	ldap_test_field	a_test_field_1	c_test_field_1	CSVimportTEST
QA A1	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*

The following column(s) are invalid and will be skipped: b_test_field_1, ldap_test_field, a_test_field_1, c_test_field_1, CSVimportTEST.
1 client(s) have warning(s). Only valid data will be imported.

Administrator

This option will allow you to set a custom field to your selected device(s) with a single or multiple preset values. This will be admin data so nothing has to be sent out to the device themselves. The setting "Assigned to all devices " will auto-associate this custom field to all devices in FileWave and any new devices that become enrolled. After picking the **Data Type**, you can select either a **Default Value** or if you would like to **Restrict Allowed Values**. If "Restrict allowed values" is selected then you can enter as many values as you like and then select one as default. If no value is selected as default then the value will simply be empty for the device. To modify or add these values simply right click on your selected device, select **Edit Custom Field(s) Value**, in the **Field Value** column double click and select the value from your list.



Display Name ▲	Internal Name
Building Code	building_code
LDAP Department	ldap_department
LDAP Email	ldap_email

Field Details

Display Name: Building Code

Internal Name: building_code

Description: This Custom Field is for Building Codes

Provided By: Administrator

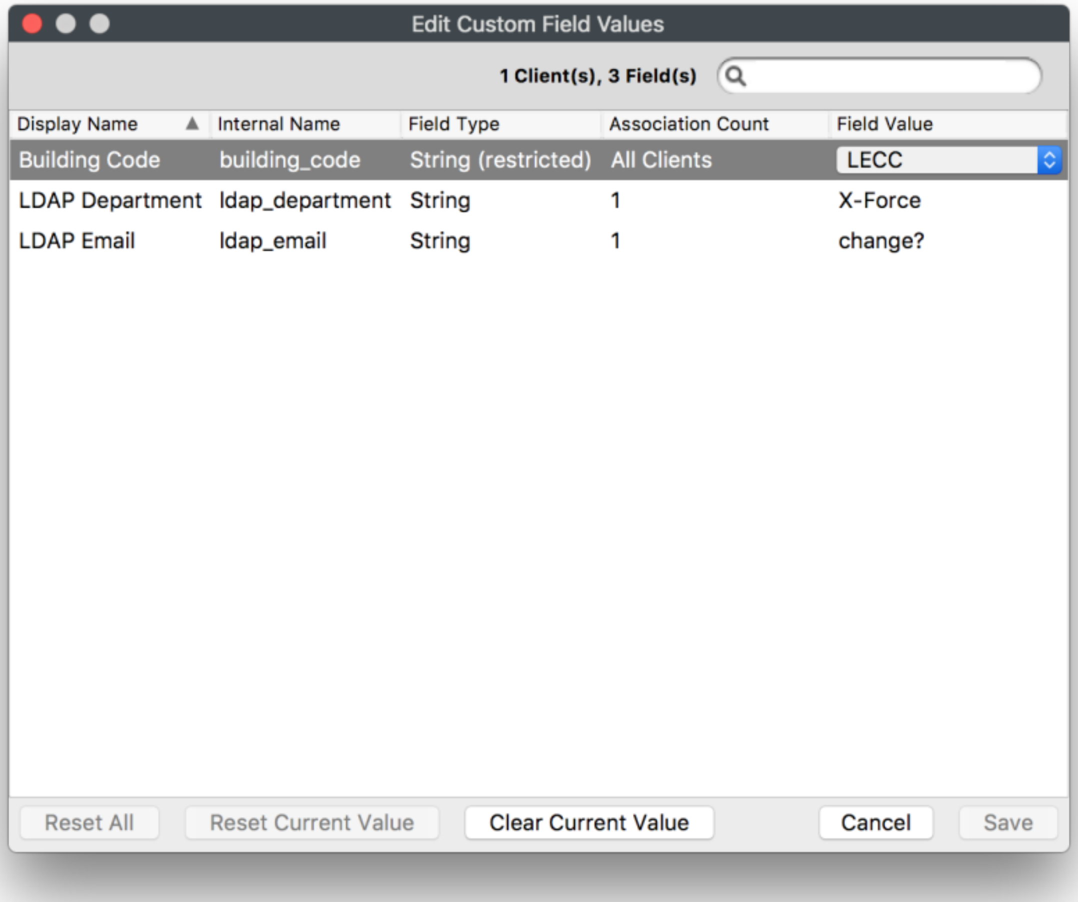
☑ Assigned to all devices

Values

Data Type: String

☑ Restrict allowed values

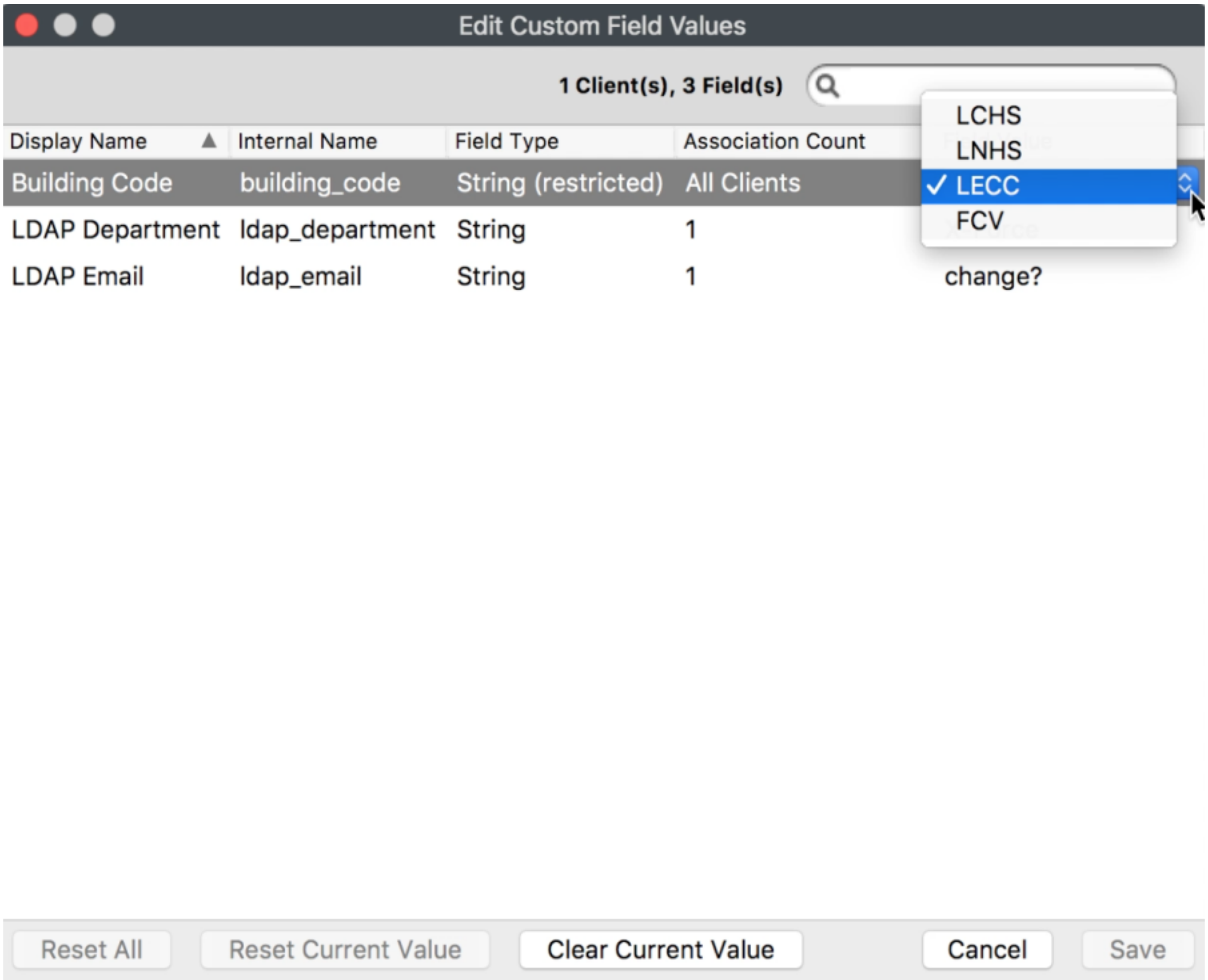
LCHS
LNHS
LECC
FCV



Edit Custom Field Values

1 Client(s), 3 Field(s)

Display Name	Internal Name	Field Type	Association Count	Field Value
Building Code	building_code	String (restricted)	All Clients	LECC
LDAP Department	ldap_department	String	1	X-Force
LDAP Email	ldap_email	String	1	change?



Display Name ▲	Internal Name	Field Type	Association Count	
Building Code	building_code	String (restricted)	All Clients	LECC
LDAP Department	ldap_department	String	1	
LDAP Email	ldap_email	String	1	change?

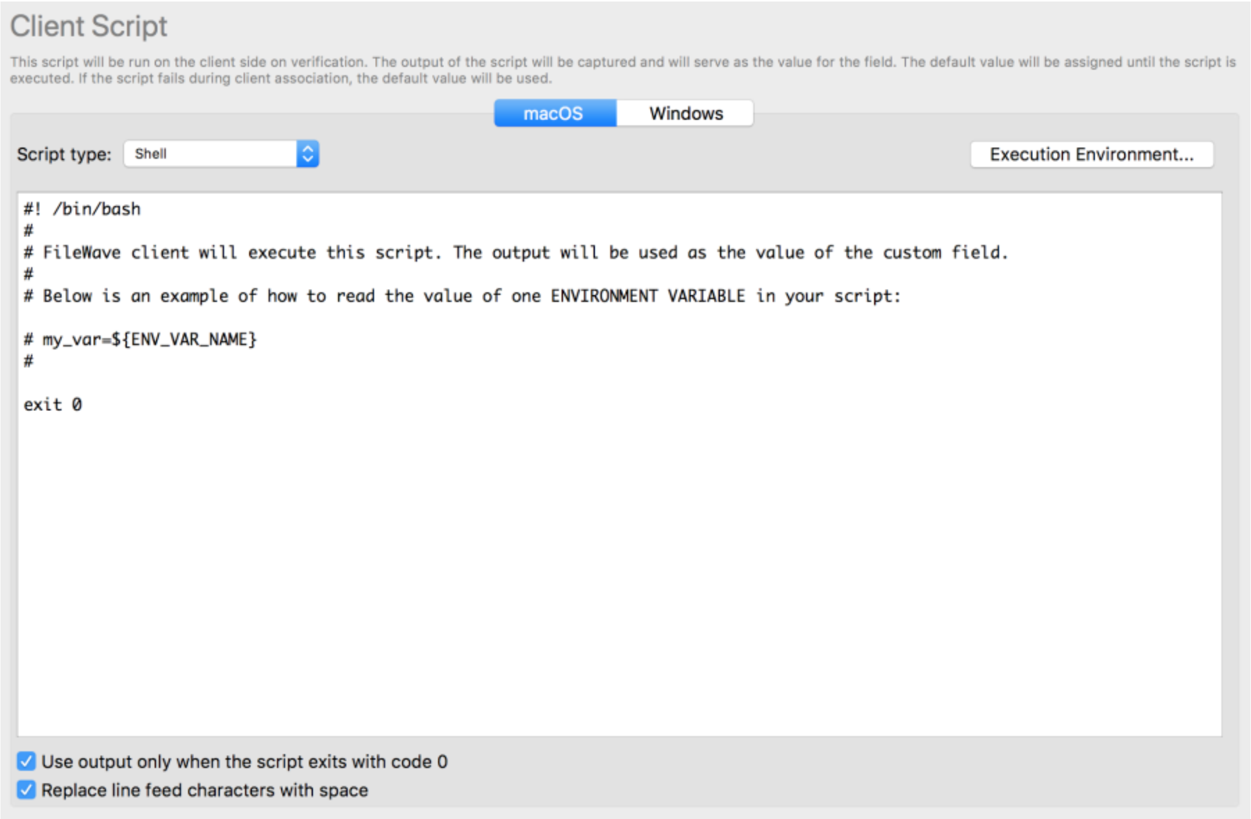
Client Script
Client Script will allow you to create and send out a script to associated devices. The output of this script will be what's written as the value for your custom field. You also have the option to set the output of the script as the custom field value only if the script has the exit code of 0. This option is for both macOS and Windows using the following script types:

- Shell
- Python
- Perl
- Bat
- PowerShell

Important: *Python and Perl will need to be installed on your Windows clients. When instlaling Python and Perl make sure a system path is added to enviroment variables during install.*

The Script will be executed after each verify, before sending inventory data.

Another option you have for script, is setting launch arguments and Environment Variables. (This option is also for any scripts you have in Desktop Filesets) So now any inventory field value can be plugged into a script.



Client Script

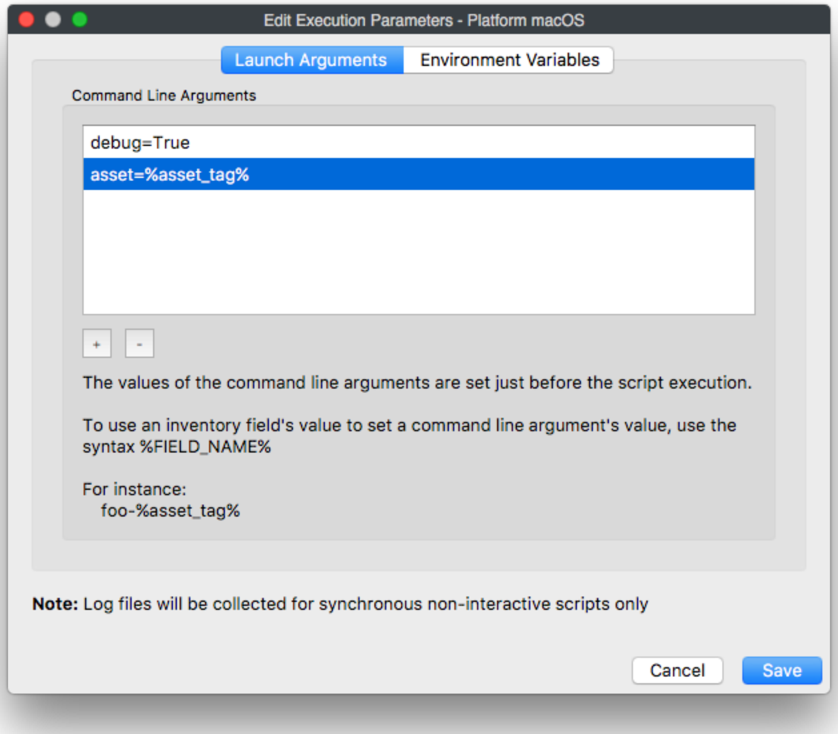
This script will be run on the client side on verification. The output of the script will be captured and will serve as the value for the field. The default value will be assigned until the script is executed. If the script fails during client association, the default value will be used.

Script type: Shell

```
#! /bin/bash
#
# FileWave client will execute this script. The output will be used as the value of the custom field.
#
# Below is an example of how to read the value of one ENVIRONMENT VARIABLE in your script:

# my_var=${ENV_VAR_NAME}
#

exit 0
```

☑ Use output only when the script exits with code 0

☑ Replace line feed characters with space



Edit Execution Parameters - Platform macOS

Command Line Arguments

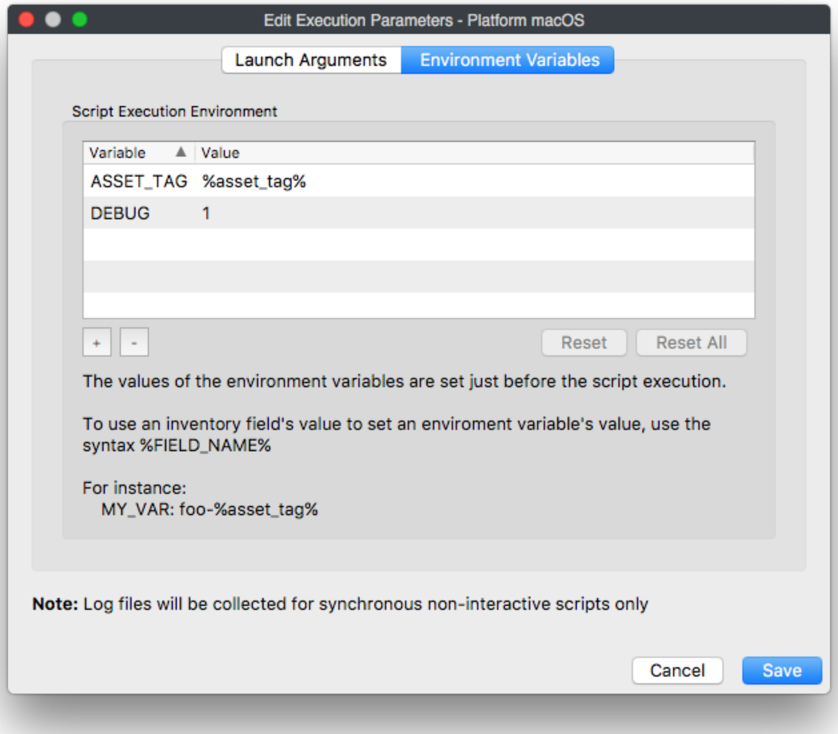
```
debug=True
asset=%asset_tag%
```

The values of the command line arguments are set just before the script execution.

To use an inventory field's value to set a command line argument's value, use the syntax %FIELD_NAME%

For instance:
  foo-%asset_tag%

Note: Log files will be collected for synchronous non-interactive scripts only



Edit Execution Parameters - Platform macOS
Launch Arguments
Environment Variables
Script Execution Environment
+
-
Reset
Reset All
Cancel
Save

Variable	Value
ASSET_TAG	%asset_tag%
DEBUG	1

The values of the environment variables are set just before the script execution.

To use an inventory field's value to set an enviroment variable's value, use the syntax %FIELD_NAME%

For instance:
MY_VAR: foo-%asset_tag%

Note: Log files will be collected for synchronous non-interactive scripts only

Note: Dates must be ISO-8601 format (for instance: 2011-08-27T23:22:37Z).
The last line feed will be ignored to ease conversion, as commands like "echo" (bash) or "print" (python) add a line feed at the end of standard output.
Scripts are stored encrypted on the disk and the FileWave client will automatically decrypt them when it needs to run. The encryption used is RSA 2048 bits, with no symmetric key exchange (only RSA).

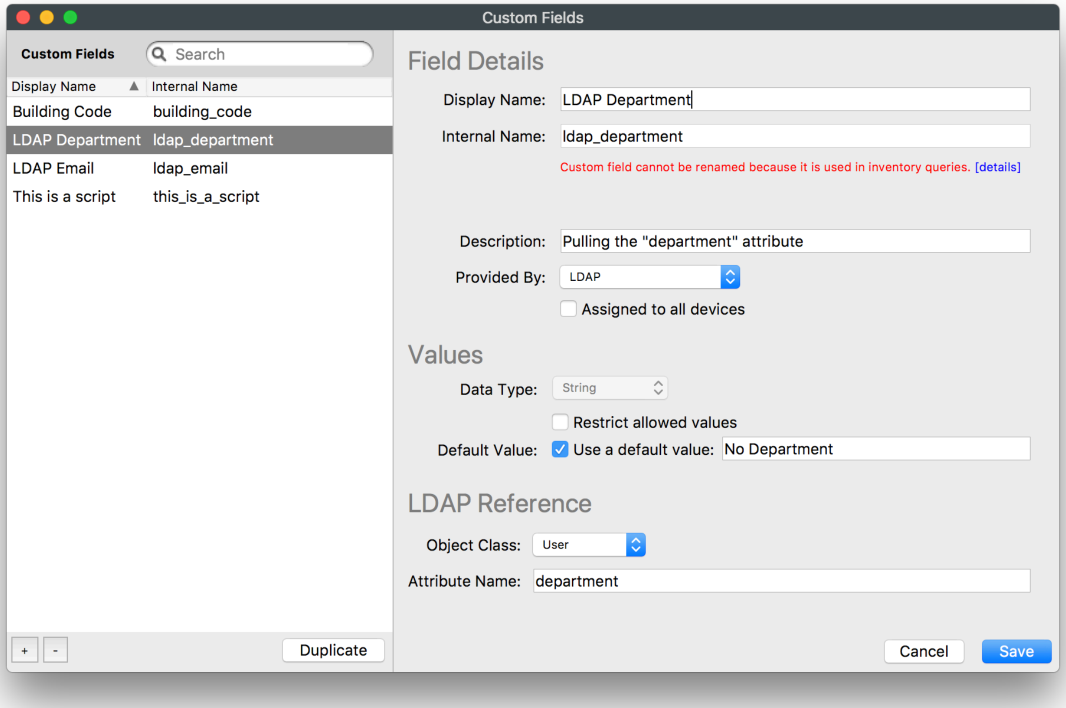
Client Command Line

This is used for existing Custom Fields that were made prior to FileWave 12.7.0 using a script to write to the custom.ini file on the client, this generally won't be used going forward for new custom fields. But if you have used custom queries with FileWave before, you will notice all of those are still present in the Custom Fields window. This will also allow you to now change the names from the deafult "custom_string_01" name for instance, to whatever you like.

LDAP

You will be able to pull attribute values from whichever directory service is being extracted in the LDAP tab in FileWave Preferences. These values are then assigned to your devices in FileWave so that you can query them at anytime. You will simply find the attribute you would like to query such as "department", which in this case is a String type. Your chooses are String, Integer, Boolean, Date/Time. If the value does not match the data type you will get a type conversion error flag when the value is pulled. Then the object class which is either user or computer:

- *User:* LDAP entry is matched using either Authusername for iPads or the last LDAP user to login for the macOS and Windows devices.
- *Computer:* LDAP entry is found using the device name in inventory against the computer name in the LDAP directory.



Custom Fields

Custom Fields | Search

Display Name	Internal Name
Building Code	building_code
LDAP Department	ldap_department
LDAP Email	ldap_email
This is a script	this_is_a_script

Field Details

Display Name: LDAP Department

Internal Name: ldap_department

Custom field cannot be renamed because it is used in inventory queries. [details]

Description: Pulling the "department" attribute

Provided By: LDAP

□ Assigned to all devices

Values

Data Type: String

□ Restrict allowed values

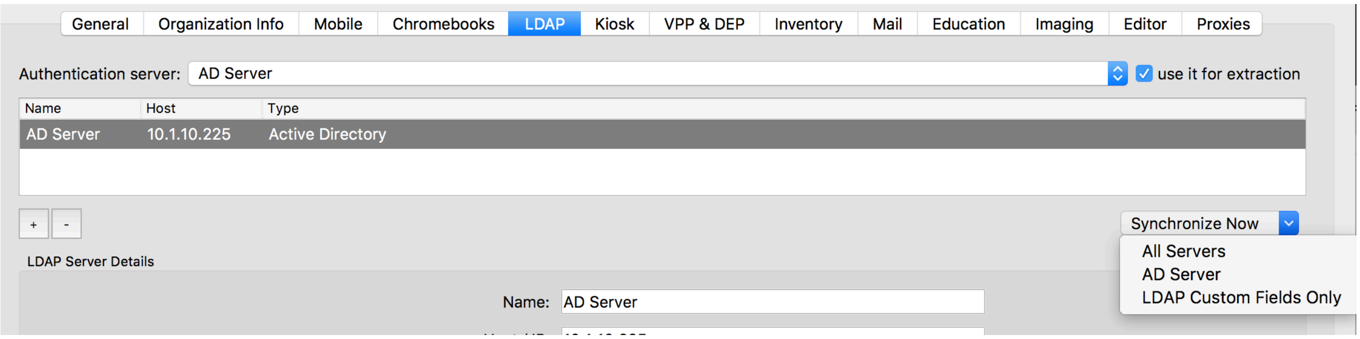
Default Value: ☑ Use a default value: No Department

LDAP Reference

Object Class: User

Attribute Name: department

How often does LDAP get scanned for updated values? Anytime a custom field is assigned to a device in FileWave or when the LDAP server is synced in the FileWave Preferences (this is either at the Refresh interval you can set or manually). However if a LDAP Custom Field is modified, your directory service will not be scanned right away, instead it will be scheduled to scan in 120 seconds; which is the minimum. (to change this time please contact FileWave support).



Authentication server: AD Server ☑ use it for extraction

Name	Host	Type
AD Server	10.1.10.225	Active Directory

LDAP Server Details

Name: AD Server

Other LDAP Considerations:
If the value of the attribute you specified is empty or the attribute is not found in LDAP, then the value of the Custom Field will simply be empty.

In the case of an attribute that has multiple entries, all entries will be returned as encoded JSON array for string custom fields. For other types of custom fields the value would contain the type conversion error flag instead. The order of entries in the JSON array is not specified.

It may happen where no matching LDAP user or computer is found for a given client associated with LDAP custom field(s). In this case, the appropriate status for custom fields values will be set upon extraction ("Matching LDAP User/Computer Not Found"). Administrator has a global option to clear current custom field(s) value when such situation occurs. The option can be found in Preferences, Inventory tab, "Clear value if there is no match between client and LDAP user or computer" checkbox.

9. FileWave Imaging

FileWave has two different types of imaging, one for direct imaging and one over the network.

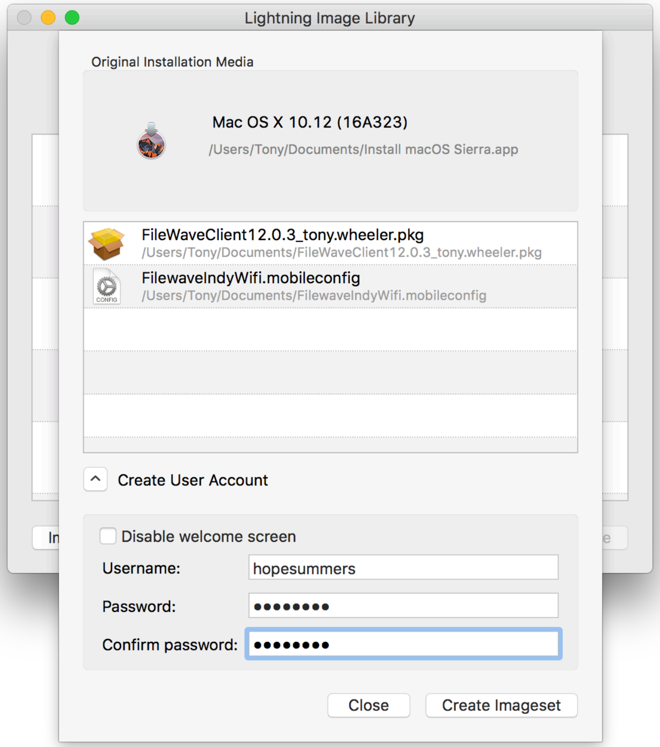
To see the newest features and supported hardware for your version of FileWave imaging visit the Imaging downloads page linked here.

Lightning

This method works over Firewire and Thunderbolt, using an application called Lighting which can be downloaded here. This method creates an image with the OS Installer app and any .moblieconfig or .pkg files you wish to install during the image deployment. You also have the option to set a user account and whether or not creating a new account is prompted during the welcome screen.

Remember you have to be on the exact same OS as the one you are trying to deploy.

Example: If you want to create a High Sierra APFS image you need be running the Lightning app on my a High Sierra APFS machine.



Lightning Image Library

Original Installation Media

Mac OS X 10.12 (16A323)
/Users/Tony/Documents/Install macOS Sierra.app

FileWaveClient12.0.3_tony.wheeler.pkg
/Users/Tony/Documents/FileWaveClient12.0.3_tony.wheeler.pkg

FilewaveIndyWifi.mobileconfig
/Users/Tony/Documents/FilewaveIndyWifi.mobileconfig

Create User Account

□ Disable welcome screen

Username: hopesummers

Password: ••••••••

Confirm password: ••••••••

This image process can take only a matter of seconds if the drive is an SSD and only slightly longer if it is a standard HDD.

To get the steps on how to create and push out an image with FileWave lightning follow this guide up to step 7: macOS Network Imaging - Netboot

- After you completed step 7 from the guide above, just connect a Thunderbolt cable from your machine to the target machine you would like to image, boot that device in Target disk mode (holding T while booting), select the image in Lightning, select Deploy, and finally restore the desired attached volume.

Network Imaging

Network imaging is supported over ethernet using the FileWave **Imaging Virtual Server (IVS).** It uses the **PXEboot** system for Windows computers and **NetBoot** for macOS computers.

For a complete guide on how to fully setup a FileWave Imaging Virtual Server (IVS):

- Network Imaging Guide

For more information about commands you can run on the IVS check out this article:

- Imaging Control Commands (IVS)

The imaging process has been greatly improved since FileWave 9. A new client process (*imaging-fwcld*) runs on the IVS, reporting back into the FileWave Server and Admin. Images are now Filesets and these Filesets can be delivered to the IVS directly from the Server or though a Booster. The imaging configuration is completely integrated into FileWave Admin.

As FileWave Imaging is unicast you can image on multiple subnets by adding an IVS on any desired subnet you like, at no additional cost. Alternatively you can also have more centralized imaging servers and just have IPhelpers to help point the traffic across subnets. The last option is to change options 66 and 67 in DHCP but keep in mind if you do this you will only be able to image Windows and not macOS.

- Option 66 - IP of the IVS
- Option 67 - pxelinux.0

How does it work?

The process for sending out an image with FileWave follows the same flow as if you would send out any other Fileset in FileWave. Before anything else you need to be sure you have the device(s) you would like to pull an image from or push an image out to in FileWave. So either having the device already enrolled and checking in, or as a place holder in FileWave. Either way, the device has to be in FileWave with a Serial number for macOS or MAC Address for Windows. Then the image Fileset is assigned to a device so that an association is made, you update the model, the IVS checks in to see new updates (just as a client would check in for new files) and then you PXE/Netboot.

When the devices are imaged FileWave names them automatically based on the name provided by the FileWave Client in FileWave. For Windows devices we also support driver injections so that you can have one base image sent out to different models with the drivers pushed out along side.

***Important Note**: If there are no associations between a device and an image in FileWave, and propagated to the IVS, then when that device PXE/Netboot's it will see no image assigned to it and then boot straight into the OS.

Upgrading an IVS

Instructions on how to upgrade a FileWave Imaging Virtual Server can be found on the downloads page for the IVS: Imaging Server downloads page

Which OS are you going to image?

Windows - PXE

Windows

For a complete walk through on how to create/deploy Windows images with FileWave and how to create/send out drivers please follow these guides:

- Windows Network Imaging - PXE
- Creating Windows Driver Filesets

Things to consider when imaging Windows devices with FileWave:

- Know whether your devices are Legacy or UEFI and make separate images accordingly
- At this time we do not support secure boot
- Your image can be smaller than the target drive but not larger
- Make sure the FileWave Custom Client is installed on the machine before the image is captured: Custom MSI

macOS - Netboot

macOS

For a complete walk through on how to create/deploy macOS images with FileWave follow this guide:

- macOS Network Imaging - Netboot

Things to consider when imaging macOS devices with FileWave:

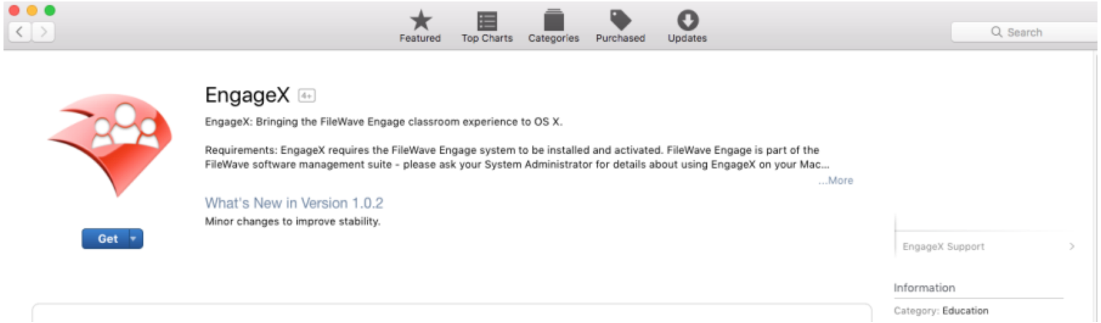
- macOS High Sierra 10.13.x APFS images can only be sent to devices that are already running High Sierra 10.13.x APFS
- An NBI has to be ran on every IVS if you have multiple
- Monolithic imaging is not supported by FileWave

10.1. Engage server

For caching the SIS information, as well as the polls and content links, Engage uses a virtual machine 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 initially boots, it will grab a DHCP address. See Section **2.3** for details on setting up and configuring the Engage Virtual Server (EVS).
The login and password for the Engage server, by default, is ***filewave / filewave.***

10.2. Engage applications

All interactions between teachers and students take place from within the Engage application. There is an iOS version of the Engage application provided to you as an **ipa** file download from the FileWave Support site. For macOS, the Engage application is available as a free download from the Mac App Store. The macOS 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.



EngageX 4+

EngageX: Bringing the FileWave Engage classroom experience to OS X.

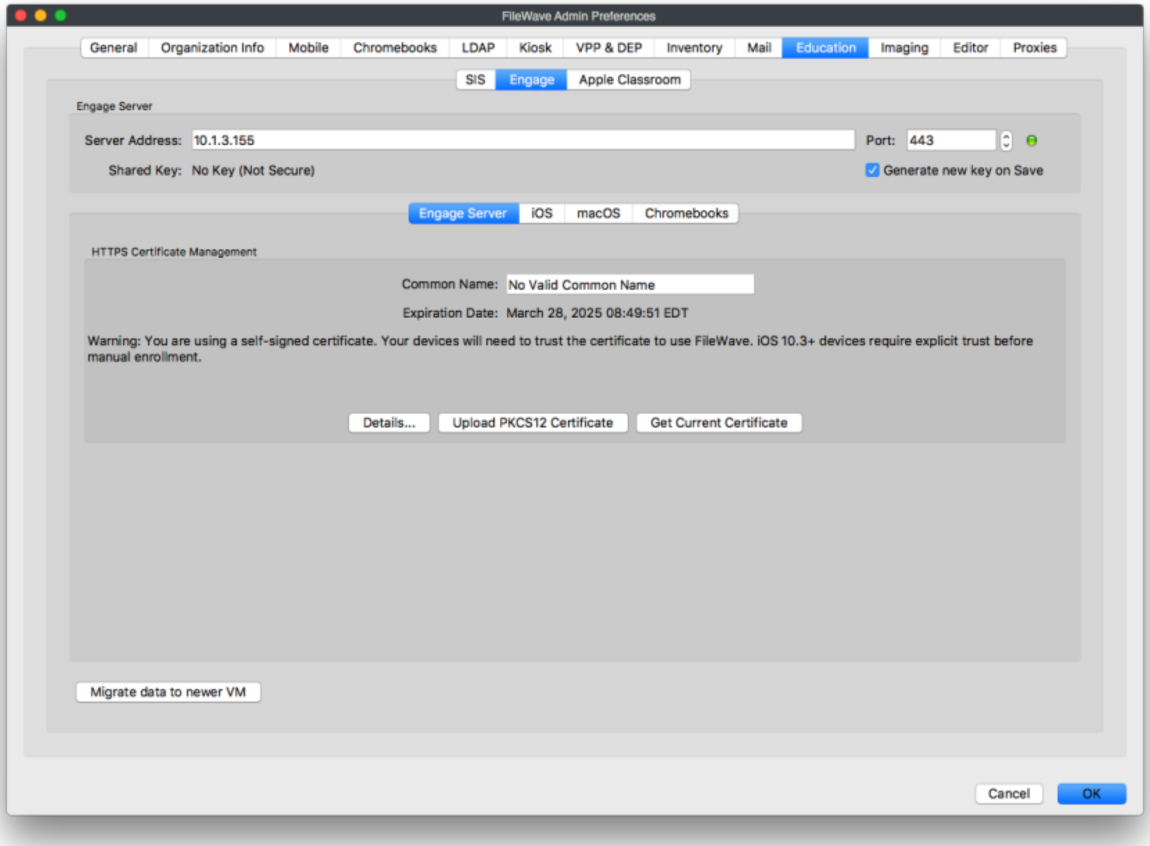
Requirements: EngageX requires the FileWave Engage system to be installed and activated. FileWave Engage is part of the FileWave software management suite - please ask your System Administrator for details about using EngageX on your Mac...
...More

What's New in Version 1.0.2
Minor changes to improve stability.

EngageX Support

Information
Category: Education

10.3. Engage preferences in FileWave Admin



Engage Server

Server Address: 10.1.3.155 Port: 443

Shared Key: No Key (Not Secure) ☑ Generate new key on Save

HTTPS Certificate Management

Common Name: No Valid Common Name

Expiration Date: March 28, 2025 08:49:51 EDT

Warning: You are using a self-signed certificate. Your devices will need to trust the certificate to use FileWave. iOS 10.3+ devices require explicit trust before manual enrollment.

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.

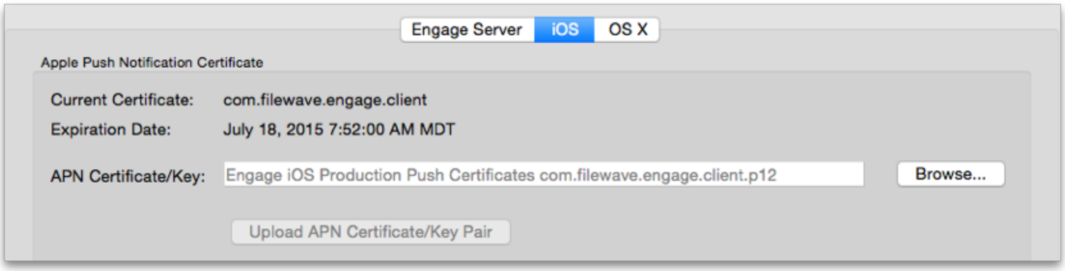
HTTPS Certificate Management

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

- *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. You will download the certificate and import it into FileWave Admin as part of a Certificate profile. See Chapter **7** for further information on profiles. **This certificate profile <u>must</u> 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.**

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***



Apple Push Notification Certificate

Current Certificate: com.filewave.engage.client

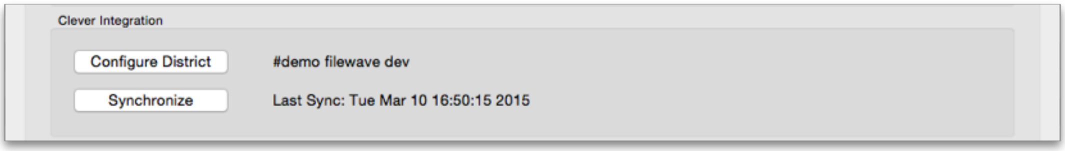
Expiration Date: July 18, 2015 7:52:00 AM MDT

APN Certificate/Key: Engage iOS Production Push Certificates com.filewave.engage.client.p12

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.



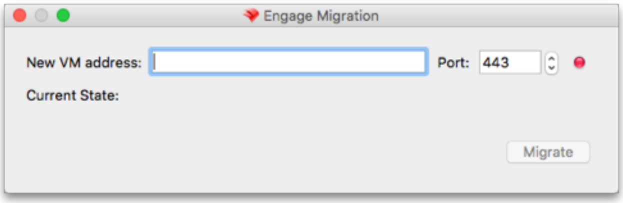
Clever Integration

#demo filewave dev

Last Sync: Tue Mar 10 16:50:15 2015

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.



Engage Migration

New VM address:

Port: 443

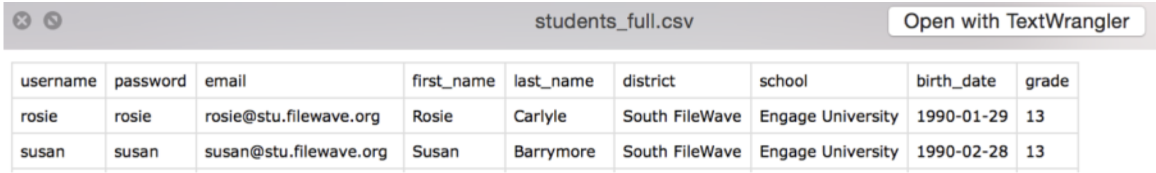
Current State:

10.4. 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 with very little effort.
Once your FileWave Server is linked to Clever, 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.

10.5. 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 class roster 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:
Each file is a CSV-formatted file with a header row. In the header, you have to specify which fields you want to insert/update for each of the records. The default for all values is an empty string.



username	password	email	first_name	last_name	district	school	birth_date	grade
rosie	rosie	rosie@stu.filewave.org	Rosie	Carlyle	South FileWave	Engage University	1990-01-29	13
susan	susan	susan@stu.filewave.org	Susan	Barrymore	South FileWave	Engage University	1990-02-28	13

You have three different entities for which you can import/update instances in the database. Below is the format for these:
Student Entity Fields
username (ID, required): username used for logging in
password: password used for authentication
email
first_name
last_name
district
school
birth_date (ISO encoded date)
grade

Teacher Entity Fields
username (ID, required): username used for logging in
password: password used for authentication
email
first_name
last_name
district
school
title

Classes Entity Fields
class_id (ID, required)
owner (required)
district
school
name
description
grade
start_date
end_date
students: a '|' (pipe) - separated list of student usernames

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:

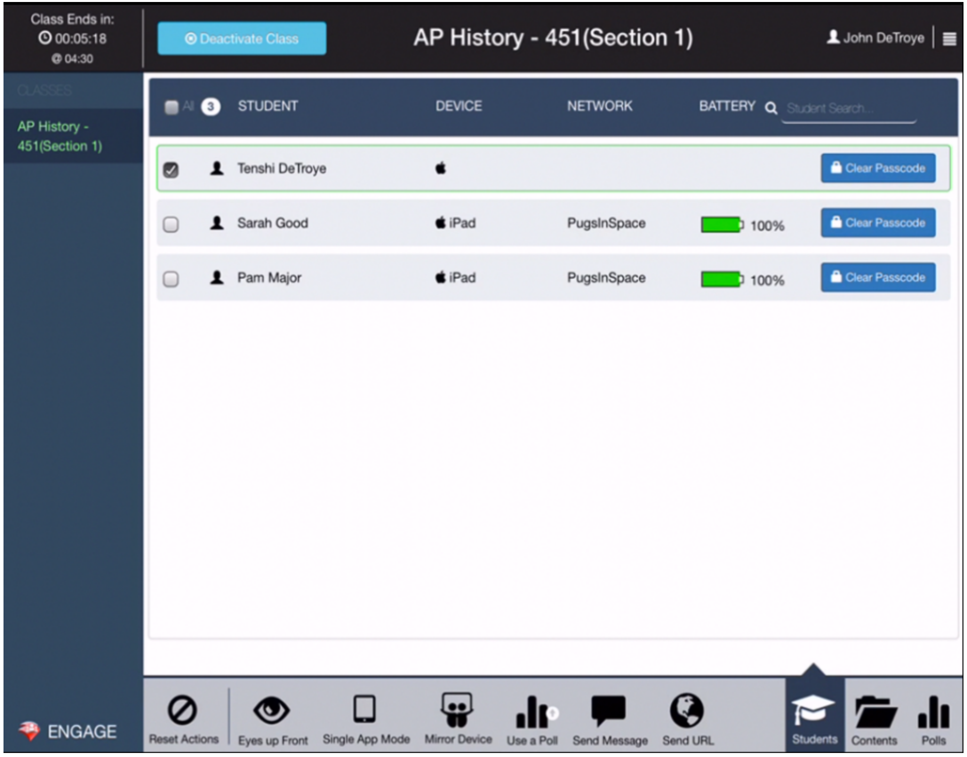
engage-control synchronize_engage -~~classes <classes.csv> --teachers <teachers.csv> --students <students.csv> [fulll~~ incremental]

Where:

- --<classes.csv> gives the path to the CSV file that defines the classes to import
- < teachers.csv> gives the path to the CSV file that defines the teachers to import
- < students.csv> gives the path to the CSV file that defines the students to import
- --full or --incremental (default is --full): 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.

10.6. Teacher Interface

The teacher interface in Engage shows three primary views: Students; Contents; and, Polls.



Class Ends in:
00:05:18
@ 04:30

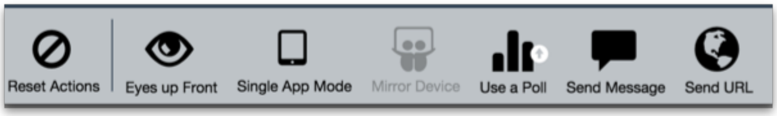
AP History - 451(Section 1)

John DeTroye

CLASSES
AP History - 451(Section 1)

□ All 3	STUDENT	DEVICE	NETWORK	BATTERY	
☑	Tenshi DeTroye				Clear Passcode
□	Sarah Good	iPad	PugsInSpace	100%	Clear Passcode
□	Pam Major	iPad	PugsInSpace	100%	Clear Passcode

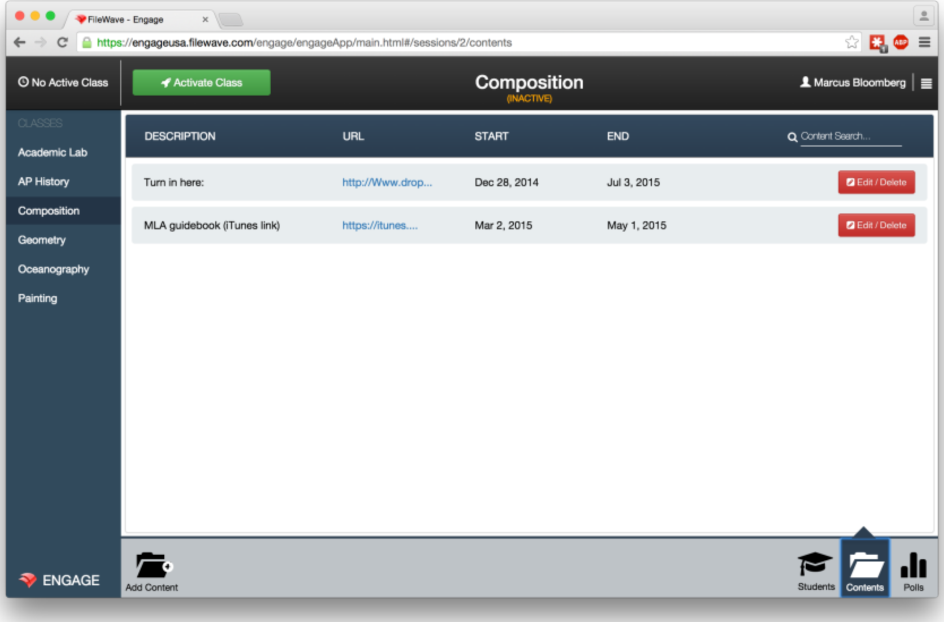
Teacher Interface: Students view
The Students view shows the currently active class, the students by name in that specific class, select status items, and some control buttons and actions. In this window, the teacher can select a class, activate/deactivate that class, send specific commands to some or all of the students, and clear the student's passcode on their device.
The commands the teacher can send are as shown:



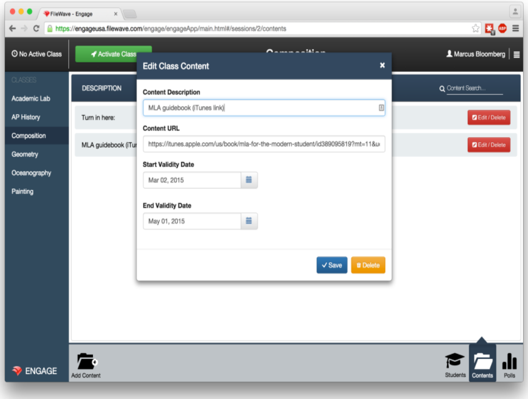
- ***Reset Actions*** – Returns all devices to a neutral state, clearing any locked screens, messages, and AirPlay
- ***Eyes Up Front*** – *Sends a message to all designated users to get their attention. Devices in Single App mode cannot dismiss the message.*
- ***Single App Mode*** – Forces supervised 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.

Teacher Interface: Contents view

This view allows the teacher add or edit content for use by the students. Contents allow a teacher to provide URLs to students. 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.



DESCRIPTION	URL	START	END	
Turn in here:	http://Www.drop...	Dec 28, 2014	Jul 3, 2015	Edit / Delete
MLA guidebook (iTunes link)	https://itunes....	Mar 2, 2015	May 1, 2015	Edit / Delete



Edit Class Content

Content Description: MLA guidebook (iTunes link)

Content URL: https://itunes.apple.com/us/book/mla-for-the-modern-student/id389095819?mt=11&u

Start Validity Date: Mar 02, 2015

End Validity Date: May 01, 2015

✓ Save Delete

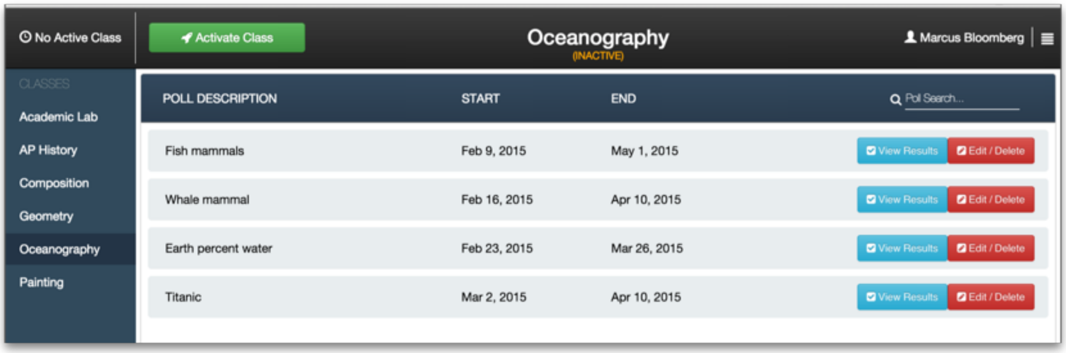
Teachers can also set availability of the content by setting start and end dates for access to the items.

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. Polls are single multiple choice questions.

The Polls View provides the following functions:

- Add Poll
- Edit Content
    - Edit Name/Description
    - Edit Question
    - Edit Start / End Date
- View Results: see all responses, correct and incorrect



POLL DESCRIPTION	START	END	
Fish mammals	Feb 9, 2015	May 1, 2015	View Results Edit / Delete
Whale mammal	Feb 16, 2015	Apr 10, 2015	View Results Edit / Delete
Earth percent water	Feb 23, 2015	Mar 26, 2015	View Results Edit / Delete
Titanic	Mar 2, 2015	Apr 10, 2015	View Results Edit / Delete

10.7. Student Interface

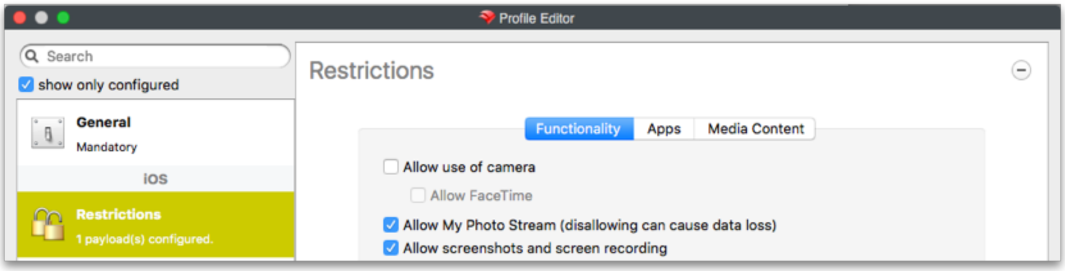
Using the same Engage application, the student interface contains a simpler set of data:

- *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

10.8. Session Profiles

Engage includes the ability to use 'tagged' FileWave profile Filesets for expanded classroom control. The teacher can coordinate with the FileWave administrator to have specific profiles made available for access during class. An example would be having the ability turn off the camera at certain times during class. The wrokflow to set this up would go like this:

Create Profile Fileset with needed controls



☐ Allow use of camera

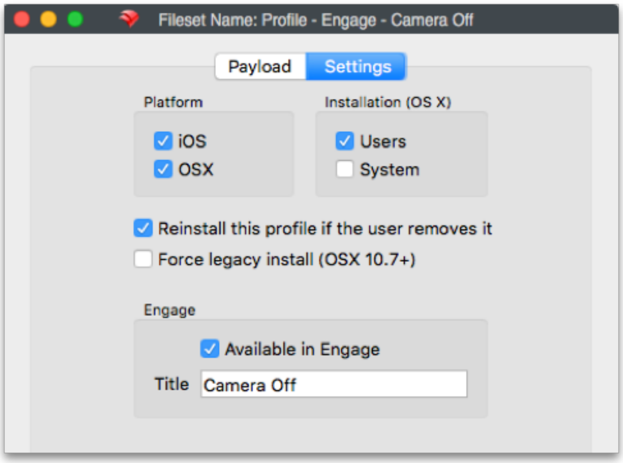
☐ Allow FaceTime

☑ Allow My Photo Stream (disallowing can cause data loss)

☑ Allow screenshots and screen recording

Be careful with restrictions - many of the payloads have a lot of default settings that may severely interfere with instructional flow; while other payloads have defaults that may allow too much leeway with younger students. Best practice is to keep the settings simple, and test them as much as possible before going live.

Configure the Fileset to support Engage



Fileset Name: Profile - Engage - Camera Off

Platform

☑ iOS
☑ OSX

Installation (OS X)

☑ Users
□ System

☑ Reinstall this profile if the user removes it
□ Force legacy install (OSX 10.7+)

Engage

☑ Available in Engage
Title: Camera Off

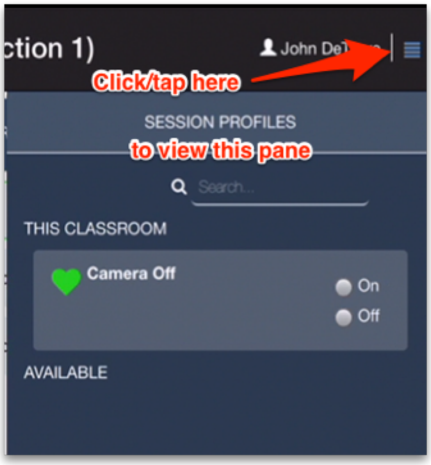
Profile Filesets support an **Engage** setting that allows you to 'tag' this Fileset to be used in Engage by any teacher. You must give the Profile a title that will allow the teachers to know what this profile will do when activated on student devices.

Update the Model to activate this Fileset

This allows the Engage server to recognize the new Profile Fileset and make it available to teachers.

Teacher logs into Engage and checks for profile

When a teacher logs into Engage and activates a class, they can tap/click on the icon next to their login name to see what **Session Profiles** are available.



Click/tap here

to view this pane

Activate profile as needed

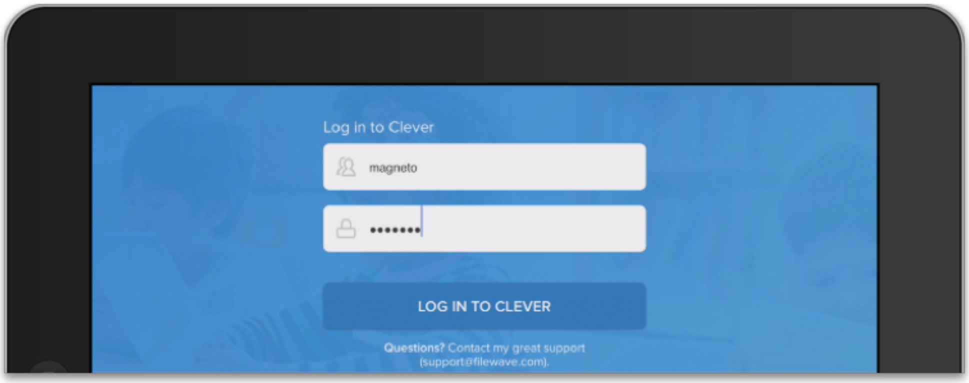
The teacher needs only to toggle the profile on/off to activate it during their class session. The impact at the student end will usually be close to instantaneous.

10.9. 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.



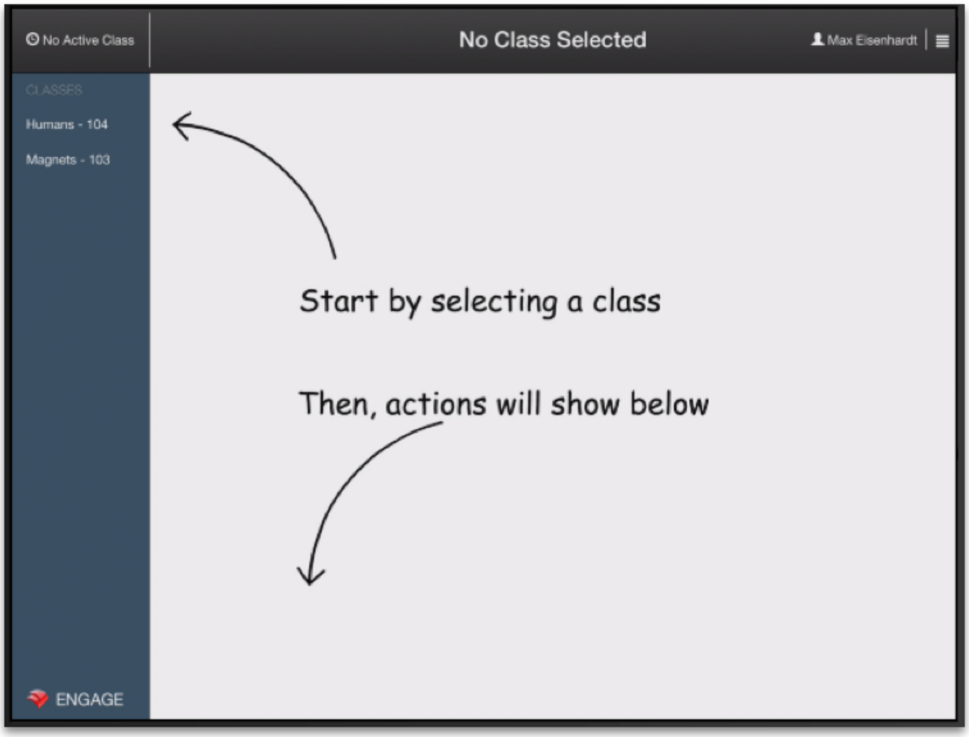
Log in to Clever

magneto

•••••••

Questions? Contact my great support (support@filewave.com).

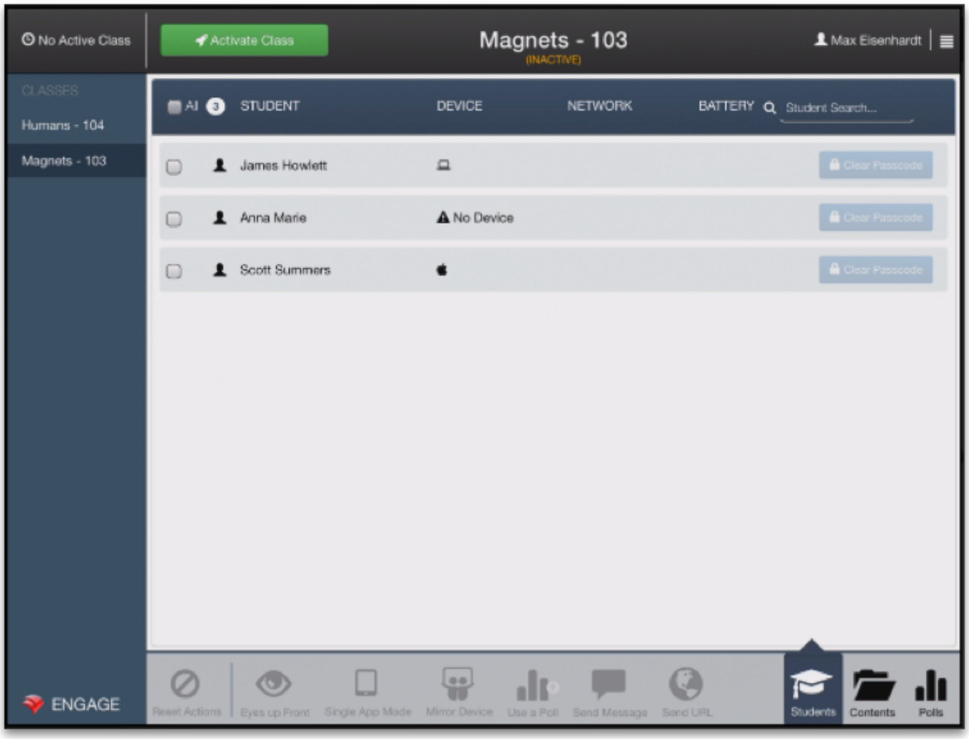
Once logged in, the teacher is presented with a view with helpers:



Start by selecting a class

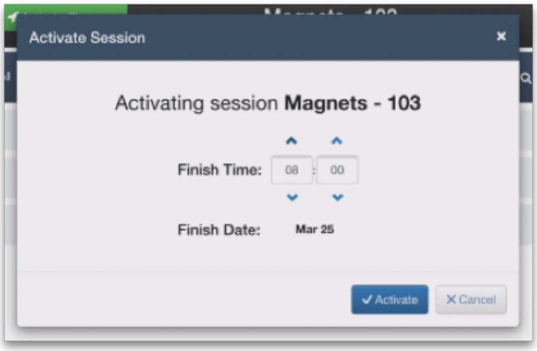
Then, actions will show below

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.



STUDENT	DEVICE	NETWORK	BATTERY
James Howlett	💻		
Anna Marie	⚠ No Device		
Scott Summers			

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.

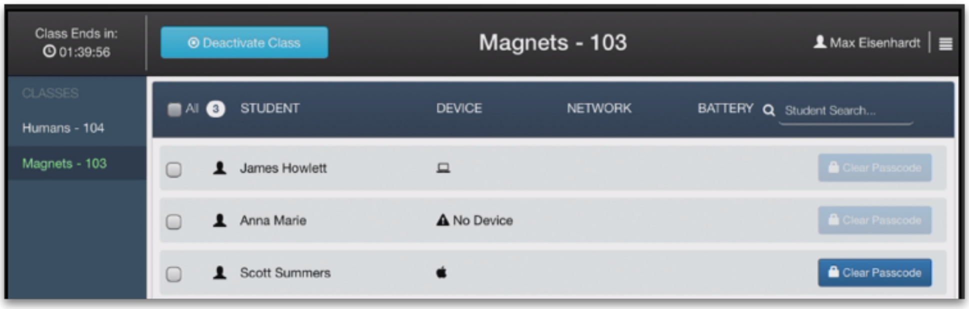


Activating session **Magnets - 103**

Finish Time: 08 : 00

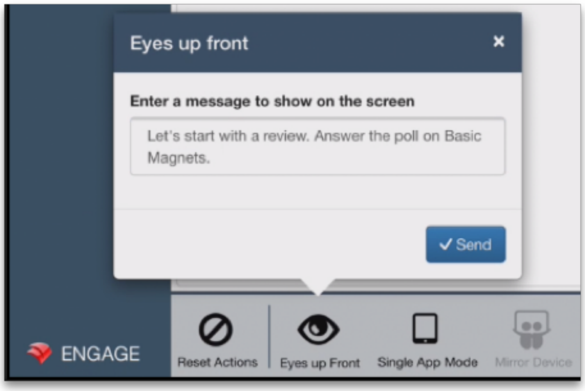
Finish Date: Mar 25

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.



STUDENT	DEVICE	NETWORK	BATTERY
James Howlett	💻		
Anna Marie	⚠ No Device		
Scott Summers			

Note some of the indicators on the teacher's view. Anna Marie is absent or hasn't checked in. James Howlett has checked into the class and is on a Mac. Scott Summers 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.

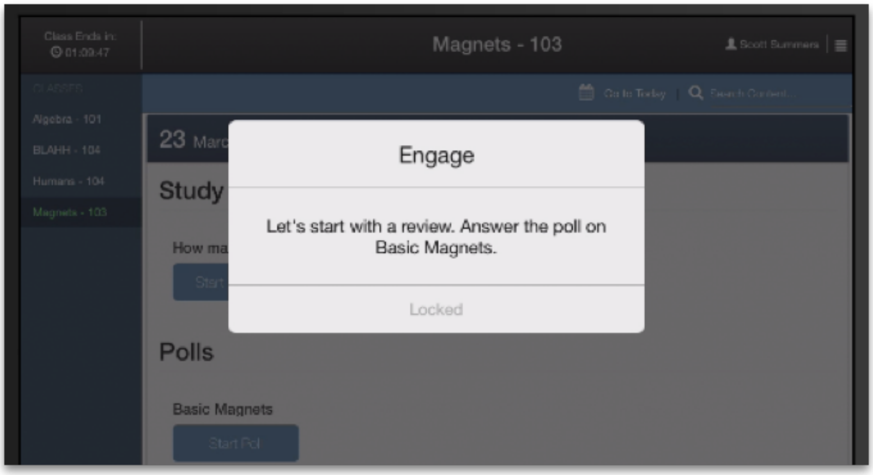


Eyes up front ×

Enter a message to show on the screen

Let's start with a review. Answer the poll on Basic Magnets.

What everyone sees is this:

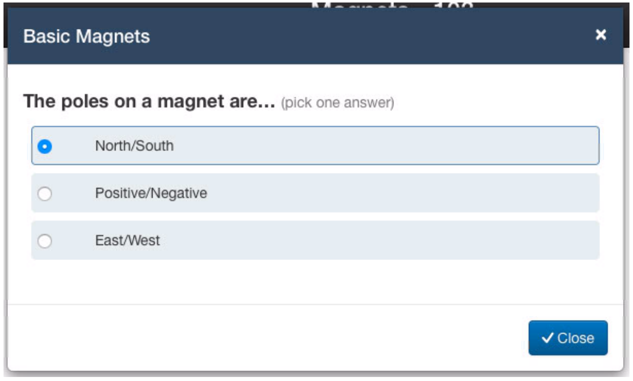


Engage

Let's start with a review. Answer the poll on Basic Magnets.

Locked

At this point, Max clicks on the **Reset Actions** button to clear the alert, and the students tackle the poll on magnets.



Basic Magnets ×

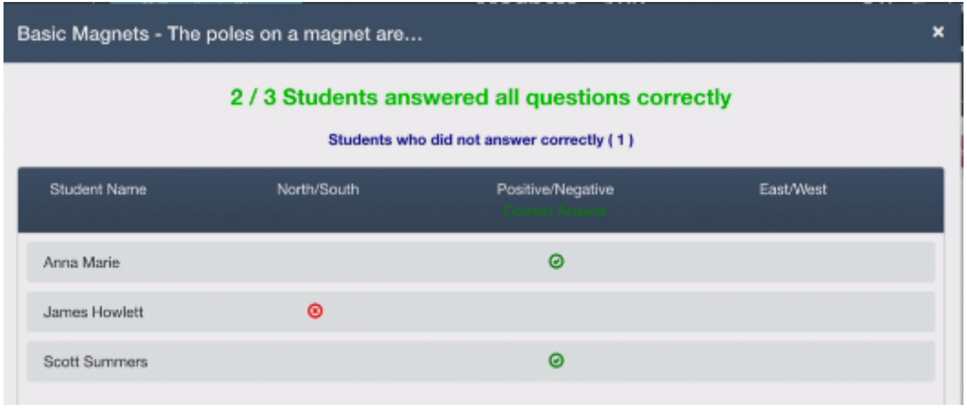
The poles on a magnet are... (pick one answer)

● North/South

○ Positive/Negative

○ East/West

Of course, someone gets the wrong answer, and our teacher sees that right away by checking the poll results.



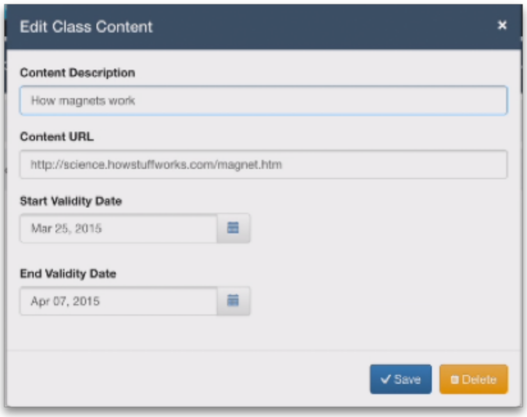
Basic Magnets - The poles on a magnet are... ×

2 / 3 Students answered all questions correctly

Students who did not answer correctly (1)

Student Name	North/South	Positive/Negative Correct Answer	East/West
Anna Marie		✓	
James Howlett	⊗		
Scott Summers		✓	

Since James was not paying attention, Max creates a special content item for him:



Edit Class Content

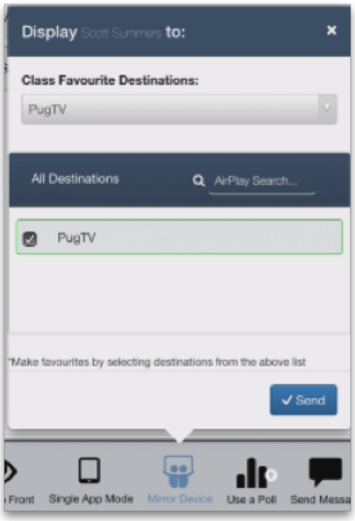
Content Description: How magnets work

Content URL: http://science.howstuffworks.com/magnet.htm

Start Validity Date: Mar 25, 2015

End Validity Date: Apr 07, 2015

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.



Display Scott Summers to:

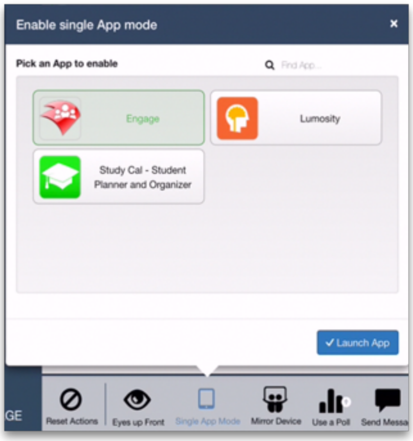
Class Favourite Destinations: PugTV

All Destinations

☑ PugTV

*Make favourites by selecting destinations from the above list

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 by sending everyone into **Single App Mode** by selecting the toolbar item, and choosing a specific application (the app must be installed on all student devices).



Enable single App mode

Pick an App to enable

Engage

Lumosity

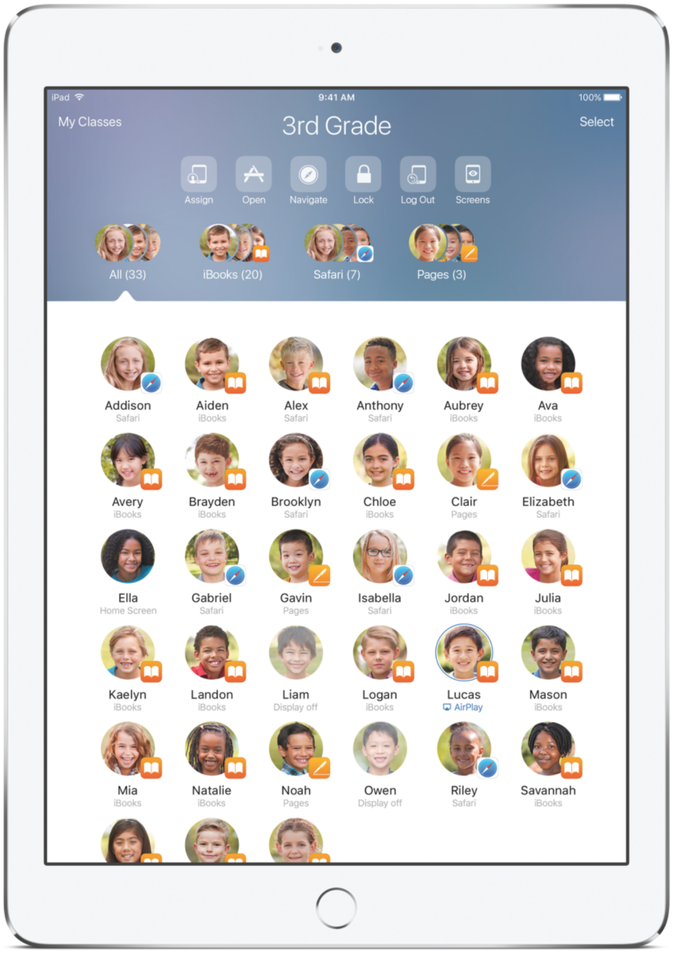
Study Cal - Student Planner and Organizer

When the teaching moment is over, Max can select the Engage application for Single App Mode, or select **Reset Actions** to allow the students to return to Engage as needed.

11. Apple Classroom and Shared iPad Support

11.1. Classroom – Feature Overview

This is Apple's application for teachers allowing them to manage a class of students using iPads. The application is available on the iTunes App Store and the Volume Purchase Program (VPP) App Store. Apple has a video about the application in the "Meet your new teaching assistant" section at this link: http://www.apple.com/education/products/



Main features:

-
  - Show, for each device, what the student is doing (which app is in the foreground)
  - Lock student devices (eyes up front)
  - Start application or Safari on a given web page on student devices (either in single app mode or not)
  - Observe (without interaction) student devices
  - Pre-assign shared iPad to student to ease login
  - Display student iPad screen on Apple TVs
  - Logout users
  - Change user passwords (with Managed Apple IDs)

Note: The *Classroom* app should only be installed on teacher iPads. Do not install it on a student device; it will only produce an error when launching…

Apple School Manager (ASM)

ASM can be thought of as a "Super Device Enrollment Program (DEP)" account, including VPP, DEP, Student Information System (SIS) data management, and Apple ID management. Existing customers will have to upgrade their DEP account to ASM. Customers are encouraged to read and follow this Apple knowledgebase article to prepare their setup for conversion: https://support.apple.com/en-us/HT206590.

ASM is only mandatory to create and manage Apple IDs. Which means that the only features requiring ASM are:

-
  - Shared iPad support
  - Reset student password

Everything else - *Classroom* included - works without an ASM account.

How FileWave supports it
FileWave helps with deploying the *Classroom* app to devices. After deployment, the app has to be configured, which requires:

- Client SSL certificates for each device
- A specific profile ("education payload") that will configure both the *Classroom* app and Shared iPad devices

FileWave will do all of this for you:

- Get information from your SIS provider
- Helps you associating devices and persons (1:1 context) or carts and classes (shared context)
- Support for both 1:1 and Shared iPad models
- Automatically generates and deploys the education payload, specific for each device
- Provide a way to import "place holders" for devices that you have not yet physically deployed, so you can prepare workflows for apps / payloads in advance

Unique FileWave benefits:

- Seamless integration with your usual FileWave deployment workflow
- Clever integration. FileWave allows school district's having an SIS supported by Clever to directly, and without any additional work, use the *Classroom* app.

11.2. Classroom – Shared iPad

Terms and Definitions
Classroom – this is this is Apple's application for teachers allowing them to manage a class of students using iPad devices. Main features:

-
    - Lock student devices
    - Start application or Safari on a given web page on student devices
    - Observe (without interaction) student devices
    - Pre-assign shared iPad to students
    - Display student iPad screen on Apple TVs

Shared iPad - this is a special mode in which iPad devices can be put, which allows multi-users on a single iPad.

-
    - Only one user is logged in at a time
    - Personal data are downloaded from iCloud on first login on the device and cached on the device
    - You can configure how many "user caches" can be stored on the device
    - Managed Apple IDs are required

Apple School Manager - this is Apple "Super DEP" portal for education.

-
    - Works as a normal DEP account (you can create multiple "virtual servers" and use them to deploy your devices)
    - Integrates VPP
    - Integrates Student Information System data
    - Integrates Managed Apple IDs management

One-to-One (1:1) context - this is a deployment model where a person is getting a device that is not shared with another person.
Cart - this is a Group of devices that usually stay in one classroom, and that are shared by students. They do not have to actually be stored in a cart; this is just a logical grouping that we chose to call a Cart.

While *Classroom* and Shared iPad share the same underlying concepts, it is not mandatory to use both together:

- *Classroom* only can be used in 1:1 context without Shared iPad
- Shared iPad can be used without a teacher running *Classroom*

Hardware Requirements
Apple has the hardware requirements listed here: https://help.apple.com/classroom/ipad/1.1/#/cadc1b9b4f8a (I know that it's an ugly URL, but it takes you where you need to go). On this page, you will see that the following applies:

- All devices require Bluetooth LE (Low Energy) support
- Nothing additional for teacher devices
- 1:1 student devices must be supervised
- Shared iPad requires more storage space

How it works: Classroom

- *Classroom* is configured using a special "education" payload (profile), which has to be sent via MDM.
- The profile has to contain data based on SIS data, indicating who is using what.

- From a communication point of view, Apple uses Bluetooth LE (hence the hardware limitation) to initiate the connection between devices and then establish a TCP/IP connection, using SSL certificates for security.

How it works: Shared iPad

- Devices have to be in an ASM account.
- There is a special option you have to enable in DEP profile before activating the device.
- Once the device is activated, it will be prepared for Shared iPad (it will reboot just after enrollment).
- Users can log into the device using a Managed Apple ID from the same ASM account.
- Device space will be shared:
    - iOS
    - Common apps, media
    - For each user, local cache of personal data
- When user logs in / out, data are synchronized via iCloud.

11.3. Classroom – SIS Data

SIS Support
To know how to configure devices, FileWave needs to import SIS data; mainly person details and class organization.
We currently support:

- Clever import - same as for Engage
- ASM import (AKA "roster API")
- CSV import - same as for Engage

ASM and Clever data will be synchronized once every day (at midnight). You can force a refresh in Education settings of FileWave Admin Preferences.

<span style="color: #333333"><strong>Engage and Classroom</strong></span>
Engage and *Classroom* share their import settings. Future versions of FileWave will go further and make Engage and *Classroom* share imported data (but, for now, if you have Clever, both FileWave and Engage will have to import data individually, because the Engage database is stored on the Engage Server not on the FileWave Server). The format for the CSV files is the same, but the syntax to import these is different (Engage syntax is covered in Section 10.5).
Importing CSV files for students, teachers, and classes for Classroom
SSH into the FileWave Server, then run the following commands as appropriate (note, the full path to python and django have to be specified):
/usr/local/filewave/python/bin/python /usr/local/filewave/django/manage.pyc sis_csv_data_import -~~teachers <full path to teachers.csv> [fulll~~-incremental]
/usr/local/filewave/python/bin/python /usr/local/filewave/django/manage.pyc sis_csv_data_import -~~students <full path to students.csv> [fulll~~-incremental]
/usr/local/filewave/python/bin/python /usr/local/filewave/django/manage.pyc sis_csv_data_import -~~classes <full path to classes.csv> [fulll~~-incremental]
<span style="color: #333333"><strong>Required Data</strong></span>
Classroom is an application that allows **teachers** to use their iPads to manage **student devices** during a class. *Classroom* requires the devices to be configured by MDM; with the configuration defining:
For **teacher** devices:

-
    - Which classes are lead by the teacher
    - Which students are in the classes
    - Which devices are used by those students

For **student** devices (1:1):

-
    - Which device(s) are used by the student
    - Which classes are attended by the student

For **cart** (shared) devices:

-
    - Which classes will use this cart (defined as a Group of devices used with Classroom, irrespective of whether they are in a physical cart).
    - Which students will use this cart (because they are in the class)

This means that in order to configure *Classroom*, you need to know:

1. Which devices you are managing
2. SIS data, which tells you which students are in a class lead by which teacher
3. A link between the device(s) and person(s):

a. Either a direct link for 1:1 (teachers or for 1:1 students deployment model); or
b. A link between a Group of devices ("a cart") to a Group of students ("a class")

Devices

Single devices

Any device already enrolled in FileWave can be used for *Classroom*. However, at times it may be useful to prepare your deployment system upfront, before devices are actually enrolled. This is more important in a 1:1 deployment model where you want to have your students unboxing and enrolling devices with their own usernames, but you don't want to wait hours (or days) until all VPP licenses finally land to the device. FileWave 11.1+ allows the creation of placeholders for iOS devices and preparation of your deployment workflow as well as your classroom settings before real enrollment occurs:

- Any iOS device in a DEP account can be imported as placeholder (if not enrolled yet)
- You can import a CSV file based on serial number for non-DEP devices.

Carts

Classroom support introduces concept of Carts, which are nothing more than a special Group of iOS devices. These apply to the term Cart:

- A Cart contains only Clones of iOS devices.
- A device can have a Clone in one and only one Cart.
- You can create a Cart by clicking on the toolbar icon.
- You can add a device to a cart by right-clicking on an iOS device and select "Add to Cart" or by drag-and-drop. Note: this will move any existing Clone currently in another Cart into the target Cart.

Define how persons are using devices

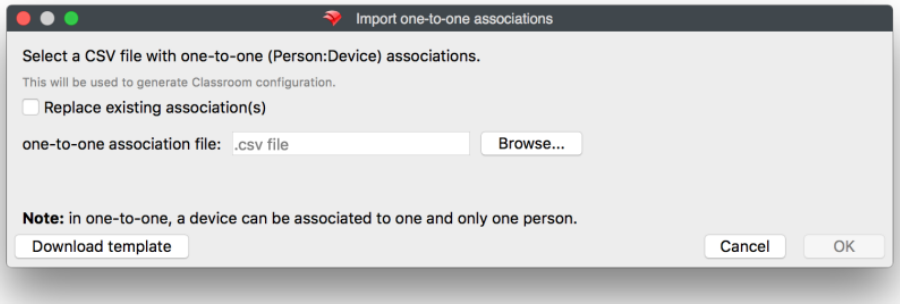
You need to tell FileWave who will be using which device. This can be:

- A direct 1:1 association for teachers
- A direct 1:1 association for students in a 1:1 deployment model
- An association between Group of devices (cart) and Group of students (class)

Note: Shared iPads can only be used with carts. If you make a 1:1 association between a shared iPad and a user, it will not work as part of a "Cart" Grouping of iPads.

FileWave offers you different ways of providing these mappings:

1. Import a CSV file for 1:1 associations



Import one-to-one associations

Select a CSV file with one-to-one (Person:Device) associations.

This will be used to generate Classroom configuration.

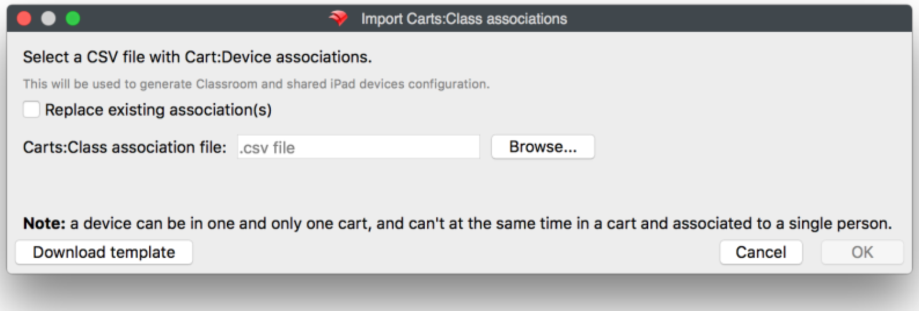
□ Replace existing association(s)

one-to-one association file: .csv file [Browse...]

Note: in one-to-one, a device can be associated to one and only one person.

[Download template] [Cancel] [OK]

1. Import a CSV file for cart:class associations



Import Carts:Class associations

Select a CSV file with Cart:Device associations.

This will be used to generate Classroom and shared iPad devices configuration.

□ Replace existing association(s)

Carts:Class association file: .csv file [Browse...]

Note: a device can be in one and only one cart, and can't at the same time in a cart and associated to a single person.

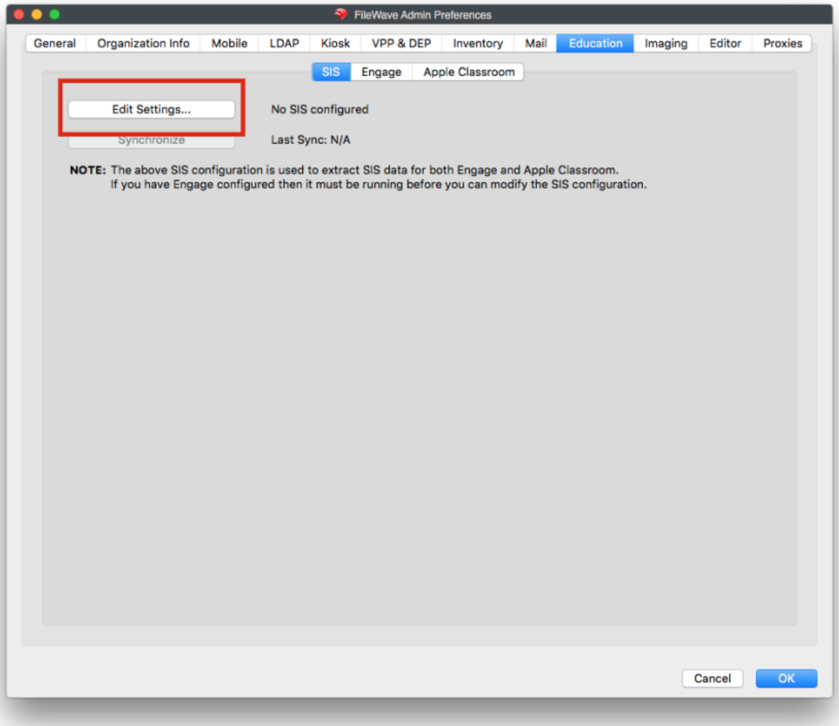
[Download template] [Cancel] [OK]

1. Authentication for 1:1 with LDAP

You can configure FileWave to automatically associate a device to a person using the enrollment auth username. Upon enrollment, FileWave can then look into SIS data and if there is a person having the same identifier in your SIS data, then the auth username link will be made. This can be enabled in *Classroom* preferences.

1. Manually via drag-and-drop

In order to import CSV files, you have to first specify that you will be using CSV files using the *SIS* pane of the Education settings of FileWave Admin Preferences, by clicking on the "Edit Settings…" button, authenticating as the super user (fwadmin), as shown on the next page.

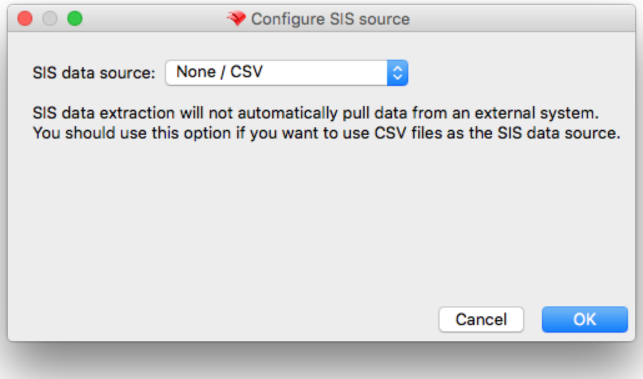


No SIS configured

Last Sync: N/A

NOTE: The above SIS configuration is used to extract SIS data for both Engage and Apple Classroom.
If you have Engage configured then it must be running before you can modify the SIS configuration.

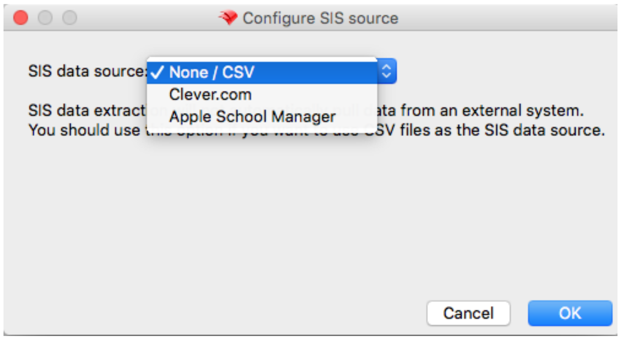
The import dialog should default to "None / CSV" in the selection box of "SIS data source."



SIS data source: None / CSV

SIS data extraction will not automatically pull data from an external system.
You should use this option if you want to use CSV files as the SIS data source.

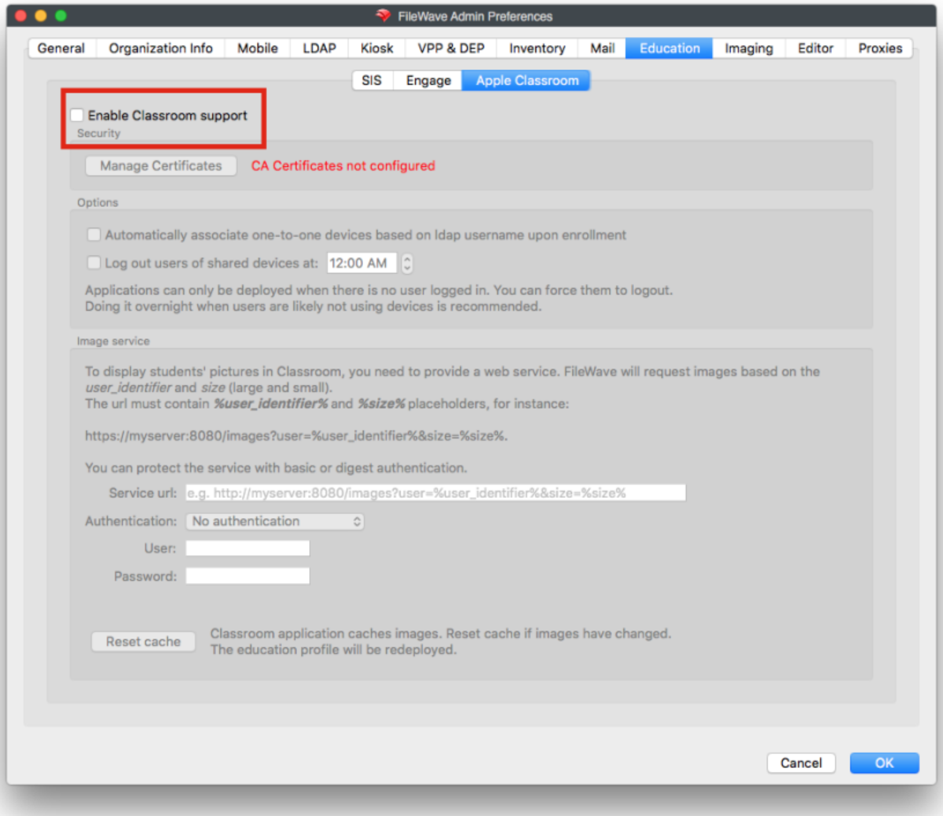
If not, select that option.



SIS data source: ✓ None / CSV
Clever.com
Apple School Manager

SIS data extract ata from an external system.
You should use SV files as the SIS data source.

You then need to enable Classroom support in FileWave Admin by selecting the following checkbox in the "Apple Classroom" pane the Education tab of FileWave Admin Preferences.



□ Enable Classroom support

Security

CA Certificates not configured

Options

□ Automatically associate one-to-one devices based on ldap username upon enrollment

□ Log out users of shared devices at: 12:00 AM

Applications can only be deployed when there is no user logged in. You can force them to logout.
Doing it overnight when users are likely not using devices is recommended.

Image service

To display students' pictures in Classroom, you need to provide a web service. FileWave will request images based on the *user_identifier* and *size* (large and small).
The url must contain ***%user_identifier%*** and ***%size%*** placeholders, for instance:

https://myserver:8080/images?user=%user_identifier%&size=%size%.

You can protect the service with basic or digest authentication.

Service url: e.g. http://myserver:8080/images?user=%user_identifier%&size=%size%

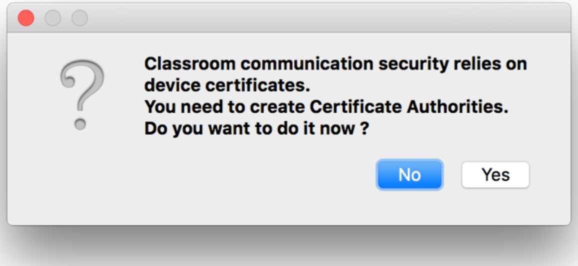
Authentication: No authentication

User:

Password:

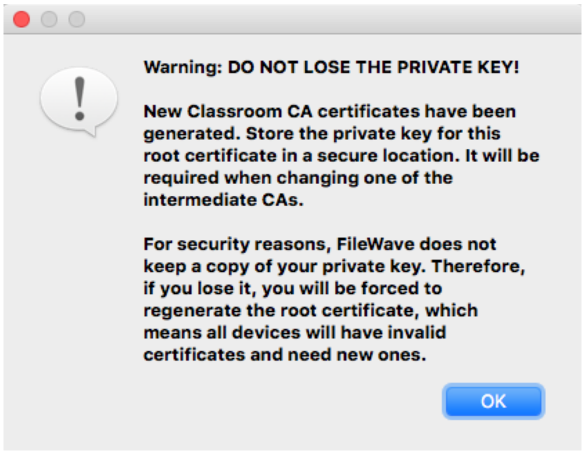
Classroom application caches images. Reset cache if images have changed.
The education profile will be redeployed.

Classroom security relies on SSL Certificates, which will be deployed on each device. FileWave has to create those certificates prior to configuring *Classroom*. The first time you enable *Classroom*, you'll then be prompted to generate those certificates:



Classroom communication security relies on device certificates.
You need to create Certificate Authorities.
Do you want to do it now ?

You'll then be able to save the main CA (certificate authority) private key - you'll need it if you want to revoke / renew certificates. (You also need super user credentials for that):



Warning: DO NOT LOSE THE PRIVATE KEY!

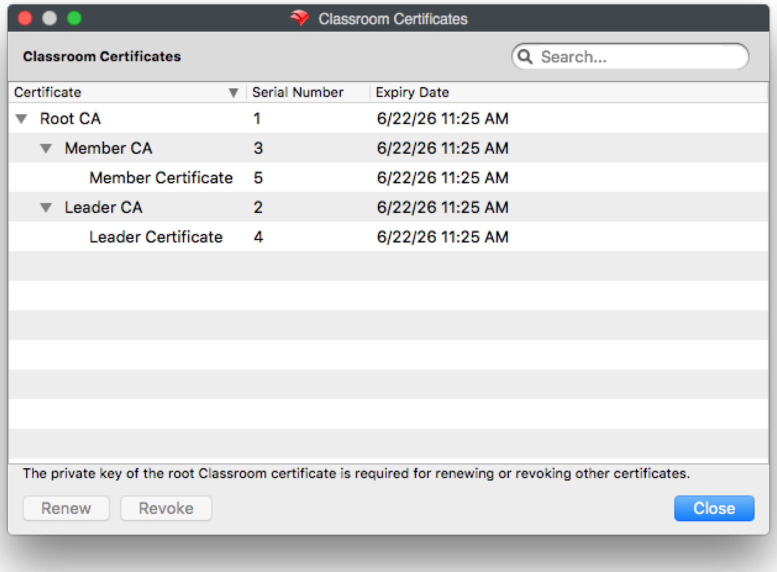
New Classroom CA certificates have been generated. Store the private key for this root certificate in a secure location. It will be required when changing one of the intermediate CAs.

For security reasons, FileWave does not keep a copy of your private key. Therefore, if you lose it, you will be forced to regenerate the root certificate, which means all devices will have invalid certificates and need new ones.

You will then be warned that the Private Key will not be stored within FileWave. It is your responsibility to maintain a copy of this in a safe location. Be sure to note where you are saving this so that you can put is somewhere safe. Also note that the file will be named "FileWave Classroom Private Key.key."

Note: If you have Keynote installed on your admin machine, the icon for this file will be a Keynote deck icon!

The dialog will display the certificates in a tree structure, where the root CA certificate is the top level item in the tree. The serial number and the expiry date of each certificate are also displayed. Certificates that will expire in less than one month are displayed with a yellow background, while expired certificates are displayed with red letters. You can sort by any column and filter certificates by typing some criteria in the search box and pressing Enter.



Certificate	Serial Number	Expiry Date
▼ Root CA	1	6/22/26 11:25 AM
▼ Member CA	3	6/22/26 11:25 AM
Member Certificate	5	6/22/26 11:25 AM
▼ Leader CA	2	6/22/26 11:25 AM
Leader Certificate	4	6/22/26 11:25 AM

The private key of the root Classroom certificate is required for renewing or revoking other certificates.

You can renew and revoke any certificates. In order to do so, select one or more certificates. The view supports multiple selection by holding the Ctrl key (Command or on Mac) and clicking entries. You can then either right-click to get a contextual menu or use the corresponding buttons on the lower left corner of the dialog. When revoking a certificate, all its child certificates will also be revoked. The certificate and its child certificates will be renewed automatically right after revocation.

You don't need the private key for renewing or revoking leader or member certificates. However, renewing/revoking any intermediate CAs requires the private key of the Root CA that was generated before. The first time you renew or revoke an intermediate CA certificate, you will be asked to open the private key. It will be remembered for the duration of the dialog, so you won't need to open it again for any subsequent operations on CA certificates, unless an operation fails. If you close the dialog and open it again later, you will need to provide the private key again for renewing/revoking CA certificates.

Although not recommended, it is possible to revoke the root CA without providing the private key by clicking "Cancel" in the file dialog to open the private key. This is useful for example in case you lose the private key. After revoking the root CA, the whole certificate tree will be regenerated automatically.

After getting the certificates taken care of and storing your Private Key, clicking OK in the Preferences will result in the main window of FileWave Admin having a new category listed in the left-hand column labeled "Classroom."

CSV File Formats

The Entities supported

Before importing your mappings for Person:Device and Cart:Class associations, you first have to get Teacher, Student, Class data into the

database, which you can do through the use of CSV files. Regardless of whether you are using Engage, you still have to get class/student/teacher data into FileWave for use with Classroom (Clever and FileWave use separate databases for class/student/teacher data). You can do that with CSV files. There are three different entities for which you can import/update instances in the DB. Here they are with the supported fields you can specify in the CSV files:
Students:

-
  - **username (ID, required)**: username used for logging in.
  - password: password used for authentication
  - email
  - first_name
  - last_name
  - district_id
  - school_id
  - birth_date (ISO encoded date)
  - grade
  - managed_apple_id

Teachers

-
  - **username (ID, required)**: username used for logging in.
  - password: password used for authentication
  - email
  - first_name
  - last_name
  - district_id
  - school_id
  - title
  - managed_apple_id

Classes:

-
  - **class_id (ID, required)**
  - teachers: a 'I' (pipe) - separated list of teachers' usernames
  - district_id
  - school_id
  - name
  - description
  - grade
  - start_date
  - end_date
  - students: a 'I' (pipe) - separated list of students' usernames

To import the CSV file, change your path to:
/usr/local/filewave/Django/ (on Mac or Linux), or
C:\Program Files (x86)\FileWave\ (on Windows)
then run this command:

macOS or Linux

```
/usr/local/filewave/python/bin/python manage.pyc sis_csv_data_import
-classes <path to classes.csv> --teachers <path to teachers.csv> --students
<path to students.csv> [-full|—incremental]
```

Windows

```
"C:\Program Files (x86)\FileWave\python\python.exe" "C:\Program Files
(x86)\FileWave\django\manage.pyc" sis_csv_data_import --classes <path to
classes.csv> --teachers <path to teachers.csv> --students <path to
students.csv> --full
```

Note: This is a single command without carriage returns at the end of the line.
Where:

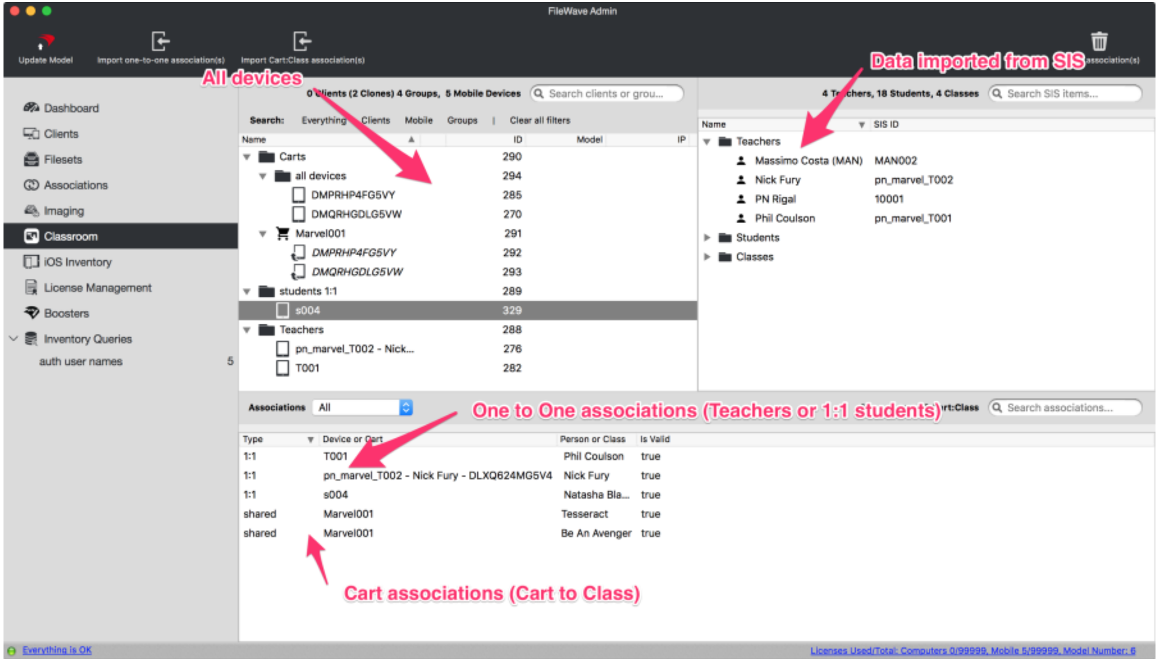
- *<path to classes.csv>* gives the path to the CSV file that defines the classes to import
- *<path to teachers.csv>* gives the path to the CSV file that defines the teachers to import

- *<path to students.csv>* gives the path to the CSV file that defines the students to import
- *--full or --incremental (default is --full):* 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 on the other hand is just updating or inserting records without touching the ones that are not referenced.

It's possible also to specify only one file

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 (see entity description for detailed info).
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 new "Classroom" view is not enabled by default. We do not want to have this showing for all customers unless they are using *Classroom*.



All devices

0 Clients (2 Clones) 4 Groups, 5 Mobile Devices

Name	ID	Model	IP
Carts	290		
all devices	294		
DMPRHP4FG5VY	285		
DMQRHGDLG5VW	270		
Marvel001	291		
DMPRHP4FG5VY	292		
DMQRHGDLG5VW	293		
students 1:1	289		
s004	329		
Teachers	288		
pn_marvel_T002 - Nick...	276		
T001	282		

Data imported from SIS

4 Teachers, 18 Students, 4 Classes

Name	SIS ID
Teachers	
Massimo Costa (MAN)	MAN002
Nick Fury	pn_marvel_T002
PN Rigal	10001
Phil Coulson	pn_marvel_T001
Students	
Classes	

One to One associations (Teachers or 1:1 students)

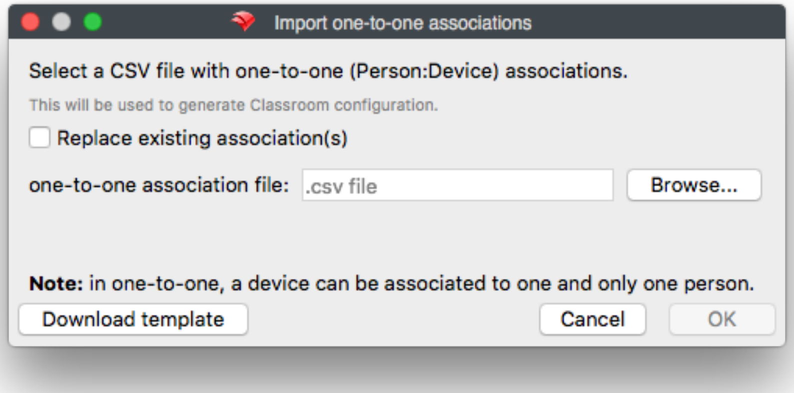
Type	Device or Cart	Person or Class	Is Valid
1:1	T001	Phil Coulson	true
1:1	pn_marvel_T002 - Nick Fury - DLXQ624MG5V4	Nick Fury	true
1:1	s004	Natasha Bla...	true
shared	Marvel001	Tesseract	true
shared	Marvel001	Be An Avenger	true

Cart associations (Cart to Class)

From the Classrrom view you can:

- Import One-to-One or Cart associations CSV files
- Change associations via drag and drop:
    - Drop one device to a single person for 1:1
    - Drop one person to a single device for 1:1
    - Drop a cart to a class for shared iPad model
    - Drop a class to a cart
- See the current association state

Clicking on "**Import one-to-one association(s)**" results in this dialog box:



Select a CSV file with one-to-one (Person:Device) associations.

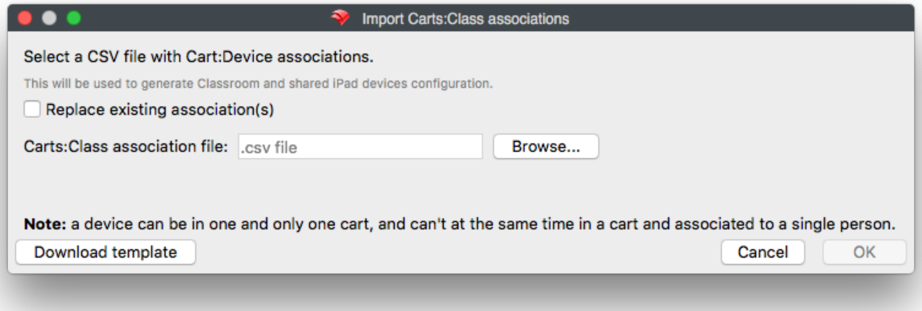
This will be used to generate Classroom configuration.

□ Replace existing association(s)

one-to-one association file: .csv file

Note: in one-to-one, a device can be associated to one and only one person.

Note the "Download template" button, which produces a CSV file that is commented to make it easy for you to produce files in the proper format. Clicking on the "**Import Cart:Class association(s)**" button results in this dialog box, which also has a "Download template" button:



Select a CSV file with Cart:Device associations.

This will be used to generate Classroom and shared iPad devices configuration.

□ Replace existing association(s)

Carts:Class association file: .csv file

Note: a device can be in one and only one cart, and can't at the same time in a cart and associated to a single person.

Once the import is successfully done, you will receive a prompt asking if you want to re-generate the Education Profiles. In cases where you are importing both 1:1 associations and carts mappings, the suggested workflow is to generate the Profiles only after the second import.

Cart CSV File

You can also produce the Cart:Device associations via CSV import. The file format needs to contain three columns:

- **cart_name**: identifier of the cart
- **devices**: list of serial_numbers separated by pipe "|"
- **classes**: list of class identifiers separated by pipe "|"

This is an example

```
cart_name,devices,classes
cart-1,SN-1|SN-2|SN-3,class-1|class-2
cart-2,SN-4|SN-5,class-2
```

Notes:

- In incremental mode is possible to omit the devices or the classes column.
- So this file updates only the list of the classes:

```
cart_name,classes
cart-1,class-1|class-2
cart-2,class-2
```

- And this file updates only the list of devices belonging to the carts

```
cart_name,devices
cart-1,SN-1|SN-2|SN-3
```

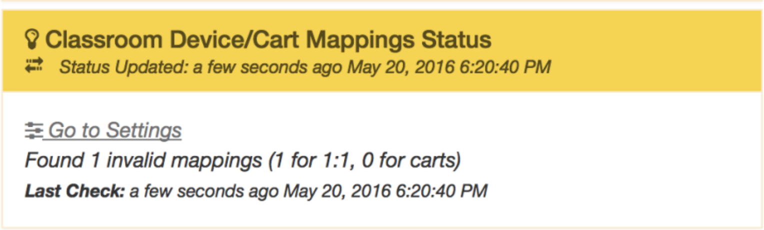
- A device can belong only to one cart. If the same serial number is listed multiple times, the last assignment will be the final one

Mappings Validity

To validate the mappings (1:1 or cart/class) the code applies the following rules:

- **Rule #0**: a mapping is invalid if the related item does not exist
- **Rule #1**: Devices in cart cannot have 1:1 mapping
- **Rule #2**: A 1:1 device can have only 1 mapping
- **Rule #3**: Teachers can have multiple 1:1 devices assigned
- **Rule #4**: Students can have only 1:1 mapping and use cart devices

Each time the check is performed a mapping is validated only if it is compliant with all the rules, otherwise it will be marked as invalid.
Invalid mappings are not taken in account for Education Profile generation
Information about invalid mappings are shown in the Dashboard



Classroom Device/Cart Mappings Status

Status Updated: a few seconds ago May 20, 2016 6:20:40 PM

Found 1 invalid mappings (1 for 1:1, 0 for carts)

***Last Check:** a few seconds ago May 20, 2016 6:20:40 PM*

11.4. Classroom – Image Service

The *Classroom* app is able to display pictures of students - by default, initials will be used. FileWave has to be configured regarding where to get images.
Classroom uses SSL for communication and will use the device certificate to authenticate itself to the imaging service. FileWave will receive the request from the device and check if the certificate is valid. If it is, then FileWave will request the image from the image (picture) hosting service and serve back the image to the device
People, in the *Classroom* environment, whether teachers or students, all have an identifier (sis_id) and images are stored on the referenced server in two sizes (large, small). Our recommendation regarding image size are 675x1024 pixels for the small image and 2700x4100 pixels for the large image. Test a few before deploying hundreds of images to ensure that these sizes work well with your student devices.
In FileWave Admin Preferences, Education Tab, Apple Classroom pane, you can specify where FileWave will request images from. We support http and https protocols, as well as basic and digest authentication.

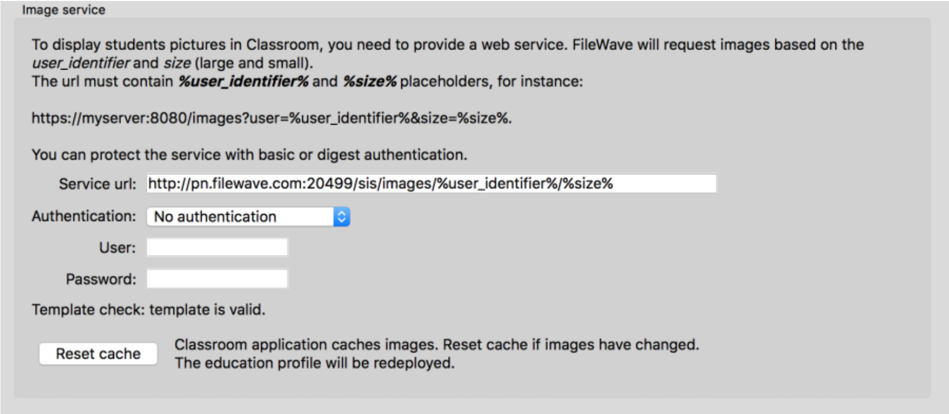


Image service

To display students pictures in Classroom, you need to provide a web service. FileWave will request images based on the *user_identifier* and *size* (large and small).
The url must contain ***%user_identifier%*** and ***%size%*** placeholders, for instance:

https://myserver:8080/images?user=%user_identifier%&size=%size%.

You can protect the service with basic or digest authentication.

Service url: http://pn.filewave.com:20499/sis/images/%user_identifier%/%size%

Authentication: No authentication

User:

Password:

Template check: template is valid.

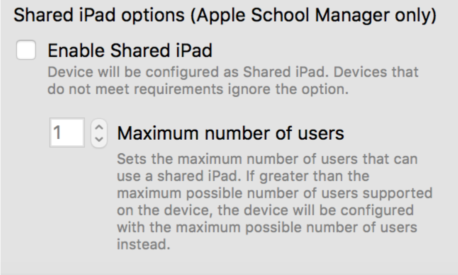
Classroom application caches images. Reset cache if images have changed.
The education profile will be redeployed.

Classroom app and shared iPad login screens have a long time cache based on the image URL. The cache can be "reset" by clicking the corresponding button above. Iit does not clear the cache (there is no way to do so), but it generates a new URL for each image, so devices will be forced to re-download them.
For more information regarding setting up your Classroom Image service, see this FileWave knowledgebase article: Getting student images into Classroom

11.5. Classroom – Shared iPad

Keep in mind that Shared iPad and *Classroom* are independent; they use the same configuration system (education profile), but they can be used separately.
Enable Shared iPad

- Devices have to be in an ASM DEP account; check also hardware requirements - they are pretty high.
- There is a new option in DEP profile



Shared iPad options (Apple School Manager only)

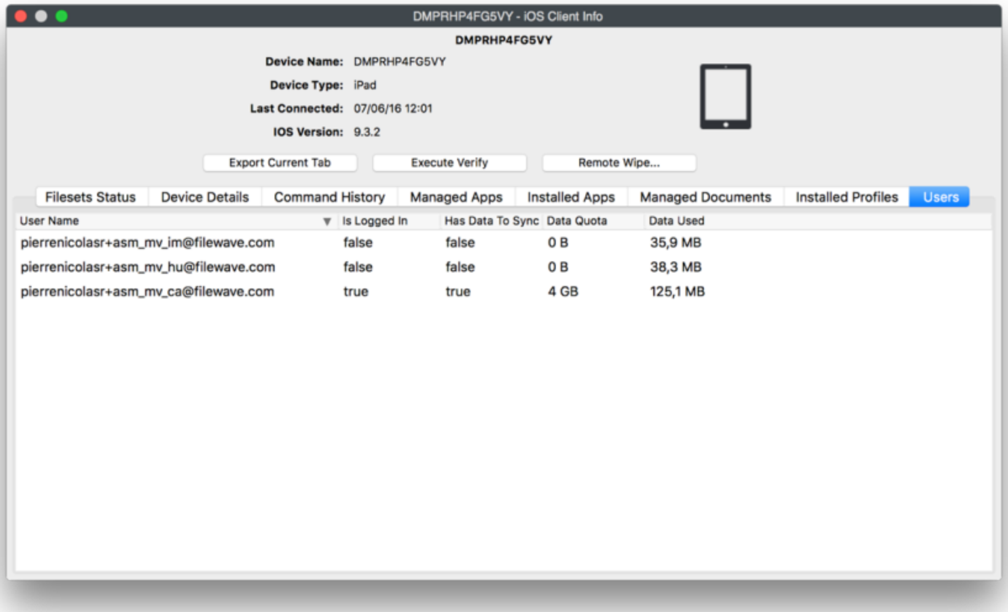
☐ Enable Shared iPad
Device will be configured as Shared iPad. Devices that do not meet requirements ignore the option.

1 Maximum number of users
Sets the maximum number of users that can use a shared iPad. If greater than the maximum possible number of users supported on the device, the device will be configured with the maximum possible number of users instead.

- Device must then be re-activated (wiped)

Shared iPad and multiple users
Shared iPad users are not "concurrent" users (as you could see with fast user switching on macOS); they just "share" iPad space and applications. Their personal data is stored in iCloud (this is why Managed Apple IDs are required) and will by synchronized on the device upon login.
Maximum resident users
You can define, in the DEP profile, the maximum number of users that can use a Shared iPad. Note: this only configures how many slices the user space will be divided into. For instance, on a 128 GB iPad, if you allocate 10 max users, each user will have an equal amount of storage space for personal data. Ten students can log into the device and will have a nearly instant login once their data is cached on the device. If an 11th student logs in, the oldest account will be deleted to free space for this user - so the login will be pretty long (sync user 1 data to iCloud, remove user 1 data from device, download user 11 data from iCloud).

User Management
There is a new entry in the Client Info dialog showing users on a shared device:


DMPRHP4FG5VY - iOS Client Info

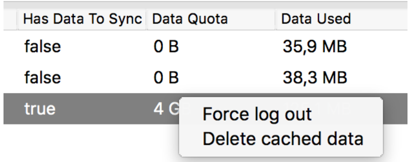
DMPRHP4FG5VY

Device Name: DMPRHP4FG5VY
Device Type: iPad
Last Connected: 07/06/16 12:01
iOS Version: 9.3.2

User Name	Is Logged In	Has Data To Sync	Data Quota	Data Used
pierrenicolasr+asm_mv_im@filewave.com	false	false	0 B	35,9 MB
pierrenicolasr+asm_mv_hu@filewave.com	false	false	0 B	38,3 MB
pierrenicolasr+asm_mv_ca@filewave.com	true	true	4 GB	125,1 MB

It returns data regarding who is logged in and the amount of space used by that user.
You can:

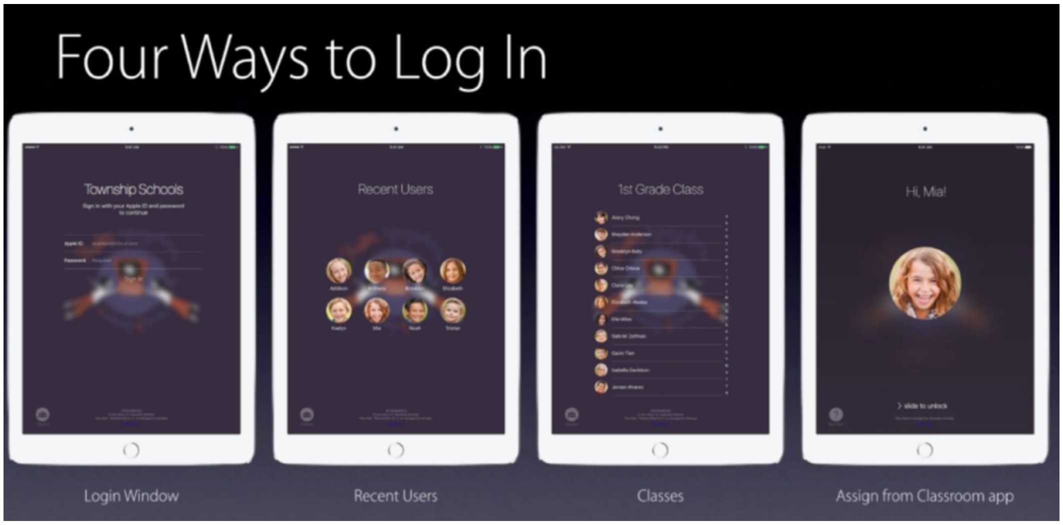
- Delete a user's current cache on a device: next login will be slower, but this will save a slot
- Log a user out



Has Data To Sync	Data Quota	Data Used
false	0 B	35,9 MB
false	0 B	38,3 MB
true	4 G	

Shared iPad and Login
To login to a Shared iPad, you need to enter a Managed Apple ID. To ease login, Apple provides different ways:

- Enter full Apple ID
- Select one of the recent users
- Select a class and then a user from the class
- Use "Assign" feature from Classroom app


Four Ways to Log In

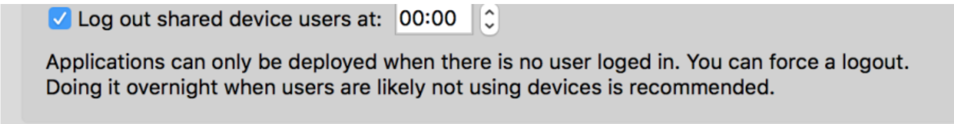
Passcode is still required; this is **pre-login** only.

By default, FileWave will use passcode type "four." This can be changed.

1. add this in settings_custom.py and restart apache
2. supported values are "four", "six", "complex"
   settings.CLASSROOM_DEFAULT_PASSCODE_TYPE = "six"
   Supported values are complex, four, or six
   This file is located at:
   on Mac OS X / Linux - /usr/local/filewave/django/filewave
   on Windows - C:\Program Files (x86)\FileWave\django\filewave
   Roster API currently only returns "Name" - no distinction between first and last name. In that case, FileWave will take the first word as first name and the rest as last name.

   Shared iPad restrictions
   Application installation
   Applications can only be installed when there is no logged in User - MDM will report invalid MDM command when it's done while a user is logged in on a shared iPad.
   The recommended workflow is:

- Pre-deploy all required apps before school starts
- If you need to deploy an app during school time, then:
  - FileWave can be configured to automatically log out users at a given time and proceed with Application self-healing. You can prepare app installation during the day and let FileWave log users out and then install apps overnight; or,
  - If urgent, you have to either force logout of all users or get them to manually log out.



☑ Log out shared device users at: 00:00

Applications can only be deployed when there is no user loged in. You can force a logout. Doing it overnight when users are likely not using devices is recommended.

11.6. Classroom – Different Deployment Scenarios

To have Classroom working, you need:

- All devices enrolled in FileWave
- Teacher devices identified, with *Classroom* app installed on them
- 1:1 devices identified (with identified Student)
- Cart Groups for shared devices
- Classes information (teachers, students, cart) loaded into the FileWave database

So you will have to:

- Enroll devices
- Import SIS data (classes, teachers, students)
- Associate devices to users (for 1:1 and teachers) and Carts-to-Classes (Shared model)
- Deploy *Classroom* app to teacher devices

FileWave does not require a specific order for these actions.
Some scenarios:

1. Enroll Cart devices and create carts
2. Import SIS data
3. Associate classes to carts
4. Create placeholders for teacher devices
5. Associate each teacher device to its teacher
6. Deploy *Classroom* to teacher devices
7. Have a 1:1 enrollment process (with auto enroll) where MDM auth username matches SIS identifier, so students can unbox their iPad and do the enrollment themselves

You can also prepare everything upfront:

1. Import SIS data
2. Import placeholders for 1:1 devices
3. Enroll cart devices
4. Associate classes to carts, devices to persons
5. Deploy Classroom to teacher devices
6. Enroll one-to-one devices

Changes can be incremental - so if, for instance, you have a new student, you can add the device:person association later without re-doing everything.

11.7. Classroom – What we don’t support

- Carts are always associated to a whole Class. There is no way to indicate to FileWave that this cart is for the 10 first students while the second cart is for the last 10 students.
- Passcode options - we can't get the passcode type from ASM for a person, so we can't prepare the right passcode keyboard.
- We don't Group classes by Department.
- Class-level deployment (i.e. make an association to a Class, all devices used by that class will get the app, users in that class will see the app, others won't. However, it is still possible to deploy apps outside of the *Classroom* use case, so you can't say that just because an iPad is in a Cart Group that only apps that have been deployed to the class(es) associated with the cart can be seen by students in a given class…).

11.8. Managed Apple IDs

Apple IDs has always been the central piece of Apple ecosystem - linked to an iTunes account, it was the only way to get software licenses until VPP device based licenses have been added. It was becoming more and more complicated for Education Organization to maintain, even after Apple introduced education / under-age Apple ids.

This is why Apple introduced, in conjunction with Apple School Manager, "Managed Apple Ids" - those Apple Ids behave like any other, but instead of being "owned" by a user, they are "managed" by an education organization.

Silent invite

It is now possible to assign licenses to Managed Apple IDs, via VPP Users. While most of the apps now support Device Based assignment, a few apps still require user based licenses, and books are still using User Based Licenses. On this level, Managed Apple IDs are like normal Apple IDs: they have to be associated to a VPP user for the corresponding VPP token so the token organization can assign licenses to the Apple ID.

To improve customers workflow, Apple introduced the ability for MDMs to automatically and silently link a VPP user and a Managed Apple IDs. This makes organization life easier as they don't have to rely on human interaction to link their Apple ID to your VPP organization.

With the release of FileWave 12.7 FileWave have implemented this feature for 1:1 devices. Whenever a change occurs in the "Classroom" panel, FileWave will link the VPP user to the device;

- from the same Organization as the DEP token used for SIS extraction
- used in a 1:1 association for SIS

When this happens a VPP user will be associated to the user Managed Apple ID - and therefore user based licenses, including those for books, can be deployed, without the need of manually joining the organization. You will no longer need to accept the Apple terms and conditions on each device you are managing.

How to implement Managed Apple IDs with user assignment with FileWave

The user will need to sign in to the App store on their device with their managed Apple ID. Without this there is no way to know what managed Apple ID should be on which device. To do this the user will need to go to Settings -> iTunes & App Store -> Sign in with the account. If you are already signing the devices in with the managed Apple ID for iCloud you still will need to sign them in to the iTunes App store settings on the device.

One tip with this setup would be to sign in with the Managed Apple ID on the device during DEP setup on the individual devices. This would allow you to skip a step of signing the devices in after Enrollment is finished. So for this you would want to Enable Apple ID setup in your DEP profile so that this is not skipped during initial activation.

12. Network Discovery

12.1. Network Discovery – Basic Networking Terms

Basic Network Terms

(Some information in this section came from http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html)

Address – The unique number ID assigned to one host or interface on a network.

Subnet – A portion of a network that shares a particular subnet address.

Subnet Mask (AKA Network Mask) – A 32-bit combination used to describe which part of an IPv4 address refers to the network/subnet and which part refers to the host/node.

Host/Node – A device on a network that has an address.

Interface – What a device uses to make a network connection, whether wired or wireless, whether it active and has link status or not (an interface does not always have link status with a switch or access point, and does not always have an IP address).

Router or Gateway Address – The address a device has to send packets to in order to have those packets go to another network or subnet.

IPv4 address – An IP address is used to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot); known as dotted-decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Here is how binary octets are converted to decimal: The right most bit, or least significant bit, of an octet holds a value of 2^0. The bit just to the left of that holds a value of 2^1. This continues until the left-most bit, or most significant bit, which holds a value of 2^7 for each octet. If all binary bits are a one, the decimal equivalent would be 255. This is covered in a little more detail on the next page.

Link-Local Address – A network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to. They are not guaranteed to be unique beyond a single network segment (routers do not forward packets with link-local addresses). Link-local address for IPv4 are defined in the block 169.254.0.0/16, using CIDR notation.

CIDR

Classless Inter-Domain Routing (CIDR) is a method for allocating IP address and routing IP packets. IP addresses are described as consisting of two Groups of bits in the address: The most significant bits are the *network address* (or *network prefix* or *network block*), which identifies a whole network or subnet. The least significant set forms the *host identifier*, which specifies a particular interface of a host on that network. This division is used as the basis of traffic routing between IP networks and for address allocation policies.
CIDR notation is a syntax for specifying an IP address and the associated routing prefix without specifying what the subnet mask is. For example 192.168.0.2/24 means a 24-bit subnet mask.
So, what is a subnet mask anyway and how does one (or a router) determine the actual network address portion (the most significant bits in the IP address)?

Binary Notation

As you know, computers, switches, routers, and anything to do with networking are really fast at doing math, but using numbers in binary notation, not decimal. With binary notation, the digits that are possible are 0 and 1. Let look at an example of converting from decimal to binary.
192 in decimal is 11000000 binary, 193 decimal is 11000001 binary
The least significant bit is in the right-hand position. This corresponds to 2^0 power. Anything to the zero power is 1, with the exception of zero, which is 0. The next digit moving to the left represents 2^1 power (and you can have one or not, so either a 0 or a 1 can be in this place), the digit to the left of that represents 2^2, etc.
Binary 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
Decimal 128 64 32 16 8 4 2 1
Add all of the above decimal numbers together and you get 255, which is the highest value allowed for an octet in an IPv4 address. If a whole IPv4 address where expressed in binary notation, there would be eight binary digits or bits in each Grouping; hence the term "octet."
So, these are equivalent:
Decimal notation 192 . 168 . 0 . 2
Binary notation 11000000 . 10101000 . 00000000 . 00000010

Network (or Subnet) Masks

A network/subnet mask is used to determine which portion of the address identifies the network/subnet and which portion identifies the node/endpoint/host. Class A, B, and C networks have default masks, also known as natural masks:

Network Class	Network (Subnet) Mask	Number of bits in the mask
Class A	255.0.0.0	8
Class B	255.255.0.0	16
Class C	255.255.255.0	24

An IPv4 address on a Class A network that has not been subnetted would have an address/mask pair similar to address 8.20.15.1 with an 8-bit network/subnet mask of 255.0.0.0.
In order to see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
Once you have the address and the mask represented in binary, identification of the network and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000

----

net ID | node ID
net ID = 00001000 = 8
host ID = 00010100.00001111.00000001 = 20.15.1

Understanding Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network.
Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks (subnets), it allows you to create a network of interconnecting subnetworks.
Each data link on this network would then have a unique network/subnetwork ID.
Any device, or gateway, that connects *n* networks / subnetworks has *n* distinct IP addresses, one for each network / subnetwork that it interconnects.
In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID.
For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:
204.17.5.1 - 11001100.00010001.00000101.00000001
255.255.255.224 - 11111111.11111111.11111111.11100000

--~~|sub|~~---
By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device *since host IDs of all zeroes or all ones are not allowed* (it is very important to remember this). So, with this in mind, these subnets have been created.
Network address 204.17.5.1 / Subnet mask 255.255.255.224 / host address range 1 to 30*
Network address 204.17.5.32 / Subnet mask 255.255.255.224 / host address range 33 to 62
Network address 204.17.5.64 / Subnet mask 255.255.255.224 / host address range 65 to 94
Network address 204.17.5.96 / Subnet mask 255.255.255.224 / host address range 97 to 126
Network address 204.17.5.128 / Subnet mask 255.255.255.224 / host address range 129 to 158
Network address 204.17.5.160 / Subnet mask 255.255.255.224 / host address range 161 to 190
Network address 204.17.5.192 / Subnet mask 255.255.255.224 / host address range 193 to 222
Network address 204.17.5.224 / Subnet mask 255.255.255.224 / host address range 225 to 254

- Each of these subnets has a broadcast address. For the first subnet, it would be 204.17.5.31 (adding 1 decimal to the highest host address in the subnet), for the second, 204.17.5.63, etc. The router address for the first subnet is 204.17.5.1 and for the 2nd is 204.17.5.32, etc.
  These network / subnet mask pairs can be denoted using CIDR's shorthand notation; e.g., 204.17.5.64 with a subnet mask of 255.255.255.224 can be written as 204.17.5.64/27, because it has a 27-bit subnet mask (the 24 bits from the Class "C" mask, plus the three additional ones, the most significant bits used in the right-most octet).

Determining the network address from an IP address and the subnet mask

In order to determine what the network or subnet address is, convert from decimal to binary, then do a logical AND between the mask and the address.
With a logical AND operation, you compare corresponding value binary digits (2^{x} power in each of the corresponding positions of all four octets).
1 –AND– 1 = 1
Any other combinations (1 –AND– 0, 0 –AND– 1, 0 –AND– 0) all = 0
So, only two 1s result in a 1.
10101010
11000111
--~~AND~~--
10000010
Here's an example with an address/subnet
172.16.17.30 - 10101100 . 00010000 . 00010001 . 00011110
255.255.240.0 - 11111111 . 11111111 . 11110000 . 00000000
----------~~|logical "AND' operation|~~-----------
subnet = 10101100 . 00010000 . 00010000 . 00000000 = 172.16.16.0
This is what routers do very well and very rapidly. Whenever a packet is received by a router, it has to determine which network to route it to. If you have a router from your ISP in your home that uses either a 192.168 or a 10. IPv4 addressing scheme, your router is pretty good at determining which packets need to be sent out on your internal network (your LAN) and which ones need to go out the WAN port so that the upstream router can continue routing them until they reach their destination somewhere on the Internet.

> **IP Calculator**
> http://www.subnet-calculator.com/

12.2. Network Discovery – Feature Overview

The Discovery feature gives administrators the ability to discover data regarding devices that are working on an organization's network.
FileWave's network scans are easily accessible in FileWave Admin.
The list of high-level Network Discovery features:

- Run network scanners using existing Booster infrastructure (scanning only runs from Boosters, not from the FileWave Server);
- Broad network scanner configuration options (using CIDR notation and IP range, timing templates, and advanced network scan scheduling);
- Options to immediately start and stop discovery scans;
- Reporting of discovery application and network scanner statuses;
- Reporting of network changes (number of devices, running operating system, device type, device vendor, device name if possible, FileWave management status, IP address, MAC address, time of first detection);
- Discovery results filtering and grouping (results found after given date, FileWave management status, grouping devices using operating system, device type, and Booster criteria);

- An easy way to add devices not capable of being managed by FileWave to an unmanaged devices Group;
- An easy way to navigate between Booster and devices found by a particular Booster and other way around;
- An easy way to get rid of unnecessary discovery results; and,
- A discovery results web report that can be saved to PDF file.

Besides the new Discovery features, FileWave Admin v11.2.0+ has an improved user interface for the Boosters view – a new "card layout" – that gives administrators clear information about the status of all running Boosters (Note: Card View requires OpenGL on the administrator machine running FileWave Admin). If an administrator is interested in a more detailed view of the Boosters, this is available as well.
The Booster status reporting has been improved. The status now reflects the "real" status of Boosters (running/not running). Additionally, a new Booster state measurement has been added – "Booster Overload." It informs an administrator if there are any clients' requests that could not be served by a given Booster.
You can assign a human readable name to the Booster as well as a location. These options are configured using preferences in Booster Monitor.

12.3. Network Discovery - Requirements

Technical requirements

The following components of the FileWave system need to be installed to be able to use the Discovery feature:

- FileWave Server
- FileWave Admin
- At least one FileWave Booster (on Windows make sure to enable discovery in the installer, you can check if discovery is installed in Boosters view in 'Discovery Installed' column).

The Administrator must ensure that:

- There are no firewalls blocking network scanners (between the Booster and devices on the network that is to be scanned);
- There is no intrusion detection or other systems that might block the network scanners (which are nmap); and,
- The Booster runs in the same subnet as the network (or CIDR) range being scanned.

Legal and performance requirements

IMPORTANT: FileWave Administrators should ensure that they have the legal rights to perform a scan on their network(s). On sophisticated networks, with network intrusion and security monitoring tools, running a network scan can and will be seen as an attack.
IMPORTANT: Any nmap-based network scanning might slow down or trigger DDOS protections within the network. Therefore, before starting scans, the FileWave Administrator must make sure that the network is capable of being scanned without interruption of service. In other words, do not use this feature without checking with the network manager first.

12.4. Network Discovery - Technical Feature Overview

Components

The Discovery feature spans multiple FileWave components. What follows is a brief description of the roles of each component.

Component	Purpose
Django	Serves as entry point and discovery data provider to other components.
ZeroMQ notification channels	Carries control information between Django and discovery applications.
Booster	Responsible for managing dedicated discovery application (fwdiscovery).
Discovery application	Responsible for running network scans and reporting data to Django.
FileWave Admin	Used to configure & control discovery and view discovery results.

Flow

This section explains the flow of control and data in the regular discovery use case, assuming that the system is configured and ready to work. This description doesn't include any screenshots, for more thorough instructions on how to use discovery please refer to section12.6.
The FileWave Administrator enables a Booster so it appears in FileWave Admin's Boosters view. Boosters that are eligible for discovery purposes can be configured using the Discovery Configuration dialog. Discovery configuration is saved in the Postgres database. From our MDM server (our MDM server is Apache server and Postgres database that are running Django, an open-source web framework written in Python), information about the configuration change is further propagated using ZeroMQ to discovery application(s) managed by each Booster for which a configuration has been modified (this happens via a new, built-in notification system within FileWave).

The Discovery application (on the Booster) reads its configuration on start up and every time it gets notified about configuration changes. Depending on the configuration, the discovery application launches network scans with the given configuration and at given schedule. As soon as a network scan is finished, the discovery application directly reports raw data (not processed output of network scanner) to the MDM server. The MDM server is responsible for processing this data and populating the database. Discovery results can be viewed in the FileWave Admin's Boosters view (in the "Discovery Results" tab).
The FileWave Administrator is able to directly control what happens with each discovery application (enable discovery, disable discovery, immediately start discovery using current configuration, immediately stop discovery). All control commands are sent to Django and then forwarded to the discovery applications using ZeroMQ communication channels.

nmap

FileWave has commercially licensed the nmap tool for use within any FileWave product.

Discovery results data processing – what, how, when, why?

FileWave uses an existing network scanner solution (https://nmap.org/). The nmap scanner returns this information in the form of XML. The output is captured from nmap's process, compressed, and sent to Django. In turn, Django is responsible for uncompressing data, validating, and processing it. Processing means loading XML data into an object model using a dedicated library (python-libnmap) and selecting specific information that is then stored in the database.

There are couple of subtleties that you need to be aware of:

- If for any reason, the MAC address for a device cannot be detected, such devices are ignored because they cannot be processed (MAC address is the unique key);
- Operating system detection is not 100% accurate;
- Usually, a device's fingerprint (fingerprint obtained by nmap) matches multiple operating systems, in this case processing logic takes the match with the highest probability (this indicator is also provided by nmap);
- nmap tries to obtain the device name using two custom scripts (nbstat and afp-serverinfo). If these scripts cannot find the device name, then this field remains empty; and,
- macOS / iOS detection mechanism is based only on our tests and observations. There is no guarantee that Apple will not change something that we currently rely on.

12.5. Network Discovery - Technical Limitations

This page describes the technical limitations of the Discovery feature that you may need to be aware of.

MAC address detection

It's not possible to get the MAC address of a computer that is running on a different network than the scanner. The FileWave Booster must be in the same subnet as devices that will be scanned. FileWave isn't able to clearly identify a device without a MAC address; hence a device whose MAC address cannot be determined is ignored and is not presented in our discovery results.

ZeroMQ communication doesn't work on fallback Boosters

This is due to how ZeroMQ communication was initially implemented. If you have tiered Boosters, then it's possible to switch to another Booster if the first Booster doesn't respond. After communication is switched to the another Booster, the ZeroMQ communication is not switched. It results in a broken chain of ZeroMQ communication and makes it impossible to deliver discovery command messages to this Booster (discovery application running on this Booster) and all Boosters connected to it.
The solution is to resolve the failover scenario and restart the affected Booster(s).

ZeroMQ communication strategy

Our ZeroMQ communication is based on the Pub/Sub architecture. This has implications for its reliability and permanence of messages.
Our current ZeroMQ communication strategy gives us great flexibility in sending messages to multiple receivers that can freely subscribe and unsubscribe to the different types of information. Unfortunately, this type of strategy gives us no guarantee that control messages sent by a notification service will ever be delivered to nodes that are subscribed to given topics. Taking into account the fact that our ZeroMQ communication infrastructure isn't overloaded, problems with delivering notifications should not occur in a properly-configured infrastructure.

Operating system detection is not 100% accurate

FileWave is using existing network scanning solution (nmap) to perform scans. At the moment, there is no available solution that gives you 100% accuracy in operating system detection just by scanning the network.

macOS / iOS detection

There is no documented and reliable way to detect if device is running OS X (macOS) or iOS. This is due to fact that network scanners identify the TCP stack of devices and for iOS and Mac, both operating systems are based on the same TCP stack; hence, identifying the difference between these two operating systems is extremely hard.
During our initial tests, we found that all iOS devices have a very specific port open, and on all OS X / macOS computers the very same port closed. Based on this data, we are using this particular port to detect what kind of operating system is running on the device. We are aware that this behavior might get changed. There is a switch in the Django configuration that allows this detection mechanism to be disabled.

iOS detection

Locked iOS devices connect to the network for short periods of time, which makes them difficult to detect and identify. This means that we cannot guarantee that all iOS devices on the network will be detected.

Devices with multiple network interfaces

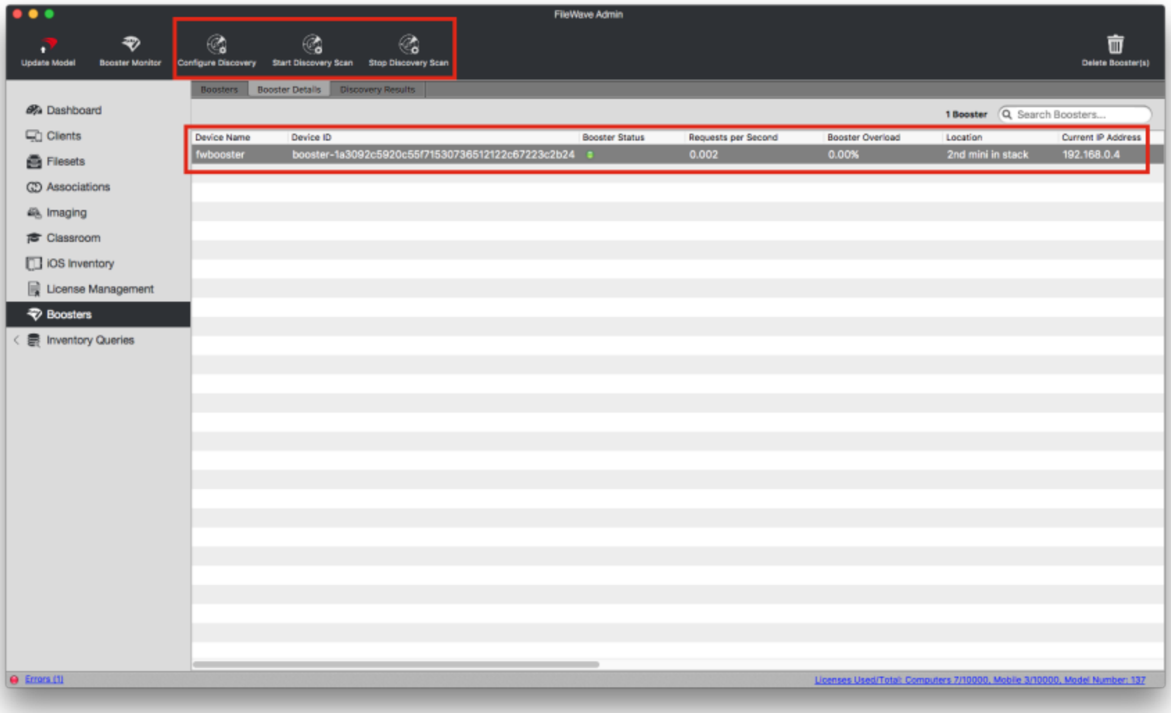
nmap is not able to detect whether a particular device operates using multiple network interfaces; hence, each network interface is shown in FileWave as a separate device. A computer with two IP addresses, one via Ethernet and the other via Wi-Fi, will be listed twice.

Nmap can't detect machines running as local virtual machines

If a Booster is running virtual machines, then those machines will not be correctly detected by nmap. This limitation applies only to local virtual machines that are running on the same host which is running Booster.

12.6. Network Discovery - Quick Starting Guide

Boosters view



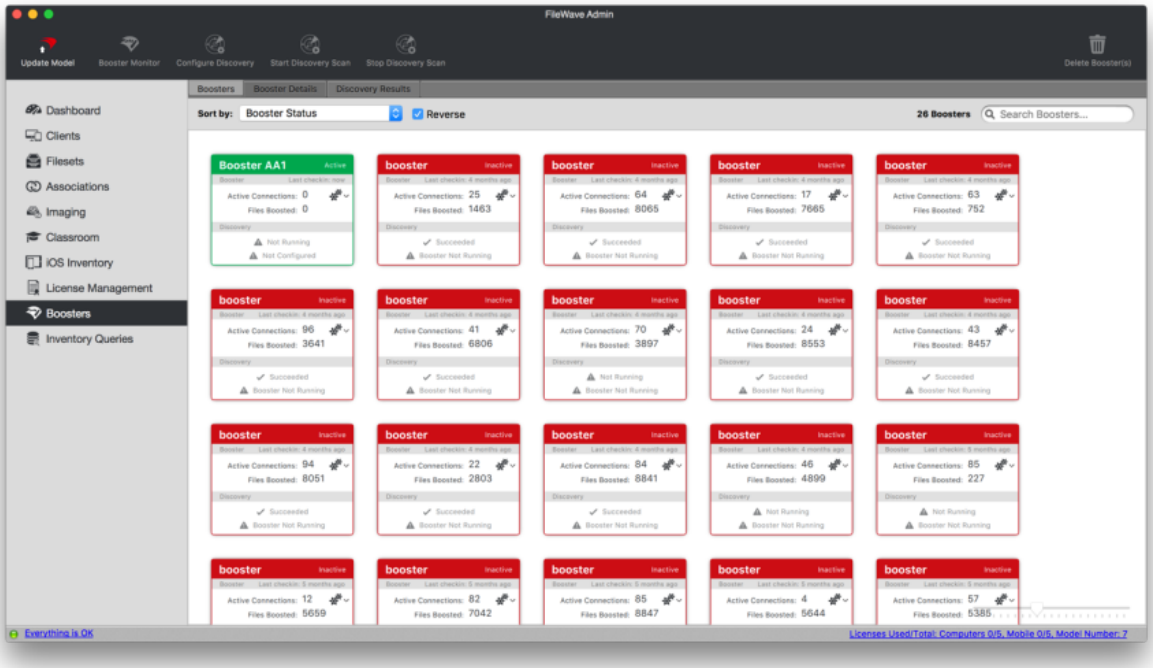
Device Name	Device ID	Booster Status	Requests per Second	Booster Overload	Location	Current IP Address
fwbooster	booster-1a3092c5920c55f71530736512122c67223c2b24	🟩	0.002	0.00%	2nd mini in stack	192.168.0.4

On the above screenshot, you can see the following new options in the Boosters tab in Boosters view:

- "**Configure Discovery**" button opens the Discovery Configuration dialog.
- "**Start Discovery Scan**" button immediately starts a scan using the existing configuration, if a scanner configuration is currently disabled then the configuration will be enabled at this point.
- "**Stop Discovery Scan**" button immediately stops the current scan, if the configuration is enabled then the configuration is also disabled.
- "**Device Name**" column contains the name of the Booster. This is configured in Booster preferences.
- "**Booster Status**" column indicates green/orange/red icon based on last check-in time:
    - green = check-in within last 5 minutes;
    - orange = check-in between last 5 and 10 minutes; and,
    - red = check-in more than 10 minutes ago).
- "**Next Scan Start Time**" column indicates start time of the next scan.
- "**Last Discovery Scan Status**" column shows the various statuses of a discovery scan and the discovery application (success, network scanner fail, network scanner crash, discovery application crash, discovery stop, generic failure).
- "**Requests per Second**" column indicates number of Booster requests per second within the last 15 minutes. Additionally, Booster statistics are sent by the Booster every 15 minutes at fixed times e.g. x:00, x:15, x:30, x:45.
- "**Booster Overload**" column indicates if there are any clients requests that could not be served by a Booster. This doesn't necessarily mean the Booster is failing; it simply implies that the client has been told to retry later.
- "**Location**" column contains location configured in Booster preferences.

View modes

The Boosters view offers two basic view modes: the Cards View (requires OpenGL on the administrator machine running FileWave Admin); and the Details View. Double-clicking on a single Booster in either view will open the Booster Monitor for that Booster.



Booster AA1 Active — Active Connections: 0, Files Boosted: 0 — Not Running, Not Configured

booster Inactive — Active Connections: 25, Files Boosted: 1463 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 64, Files Boosted: 8065 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 17, Files Boosted: 7665 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 63, Files Boosted: 752 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 96, Files Boosted: 3641 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 41, Files Boosted: 6806 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 70, Files Boosted: 3897 — Not Running, Booster Not Running

booster Inactive — Active Connections: 24, Files Boosted: 8553 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 43, Files Boosted: 8457 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 94, Files Boosted: 8051 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 22, Files Boosted: 2803 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 84, Files Boosted: 8841 — Succeeded, Booster Not Running

booster Inactive — Active Connections: 46, Files Boosted: 4899 — Not Running, Booster Not Running

booster Inactive — Active Connections: 85, Files Boosted: 227 — Not Running, Booster Not Running

booster Inactive — Active Connections: 12, Files Boosted: 5659

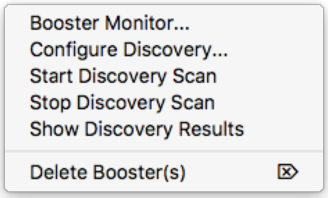
booster Inactive — Active Connections: 82, Files Boosted: 7042

booster Inactive — Active Connections: 85, Files Boosted: 8847

booster Inactive — Active Connections: 4, Files Boosted: 5644

booster Inactive — Active Connections: 57, Files Boosted: 5385

In the Cards View, each Booster is displayed as a card, with just an overview of its status. Besides using a right-click to open the contextual menu, on the top-right corner of each card there are two gears that you can click on to open the contextual menu for that Booster.

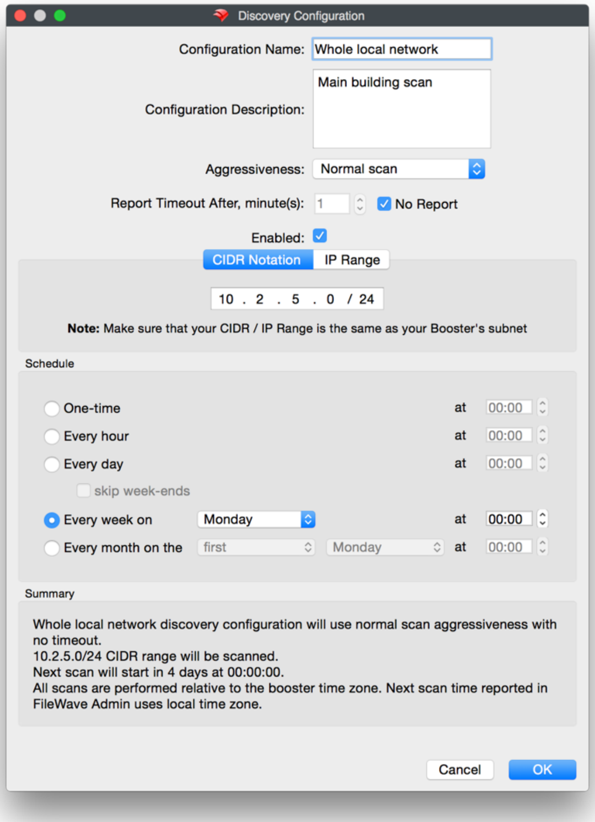


The Details View offers a lot more detail regarding the current state of your Boosters.

? Unknown Attachment

Discovery Configuration Dialog

To open this dialog, go to Boosters tab in Boosters view, select a Booster and click the "**Configure Discovery**" button in top pane, or select it from the contextual menu.



Discovery Configuration

Configuration Name: Whole local network

Configuration Description: Main building scan

Aggressiveness: Normal scan

Report Timeout After, minute(s): 1 ☑ No Report

Enabled: ☑

CIDR Notation | IP Range

10 . 2 . 5 . 0 / 24

Note: Make sure that your CIDR / IP Range is the same as your Booster's subnet

Schedule

- ○ One-time at 00:00
- ○ Every hour at 00:00
- ○ Every day at 00:00
  - □ skip week-ends
- ● Every week on Monday at 00:00
- ○ Every month on the first Monday at 00:00

Summary

Whole local network discovery configuration will use normal scan aggressiveness with no timeout.
10.2.5.0/24 CIDR range will be scanned.
Next scan will start in 4 days at 00:00:00.
All scans are performed relative to the booster time zone. Next scan time reported in FileWave Admin uses local time zone.

This dialog allows the user to configure the discovery behavior for the given Booster.

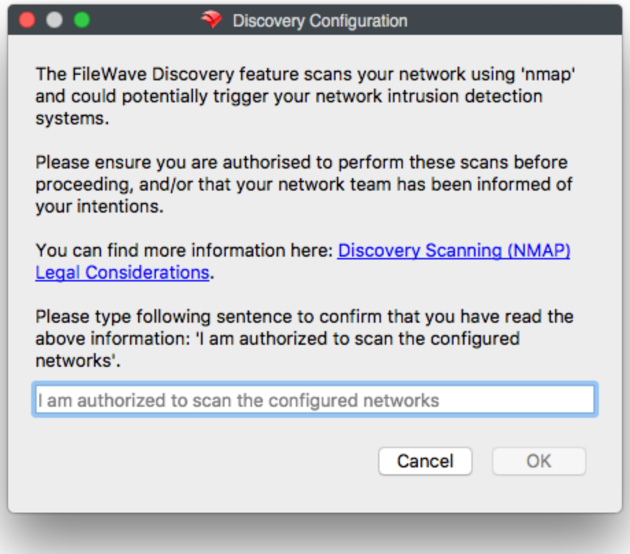
- "**Configuration Name**" and "**Configuration Description**" fields are only for informational purposes, but should be used to clearly describe where the scanner is and/or what its scanning for.
- "**Aggressiveness**" configures timing templates of the network scanner (nmap), which in turn allows the administrator to adjust load network scans put on the network. Scanning a small network could take hours if not days depending on which level you pick. The normal scan template used for OS detection scan of a network with 256 hosts, where around 20 are up, takes about 1h 30m. The polite timing template is said to be 10 times slower than normal. Remember, the more aggressive the scan, the more traffic on the network, which can impact normal network communications and be seen as a Denial of Services attack.

For more information about aggressiveness settings, see this article: https://nmap.org/book/man-performance.html

- "**Report Timeout After**" is the maximum duration interval a network scan can take without being reported visible in FileWave Admin. **Important:** Even if the timeout is exceeded, the network scan is **not cancelled**,
- "**CIDR Notation / IP Range**" widget is used to specify the subnet that will be scanned,
- "**Schedule**" widget is used to specify how often network scans will take place.

Discovery Configuration or Start Scan Configuration dialog

The first time an administrator changes the enabled configuration or manually starts a scan, he/she is asked for explicit confirmation about legal implications of running network scans.



The FileWave Discovery feature scans your network using 'nmap' and could potentially trigger your network intrusion detection systems.

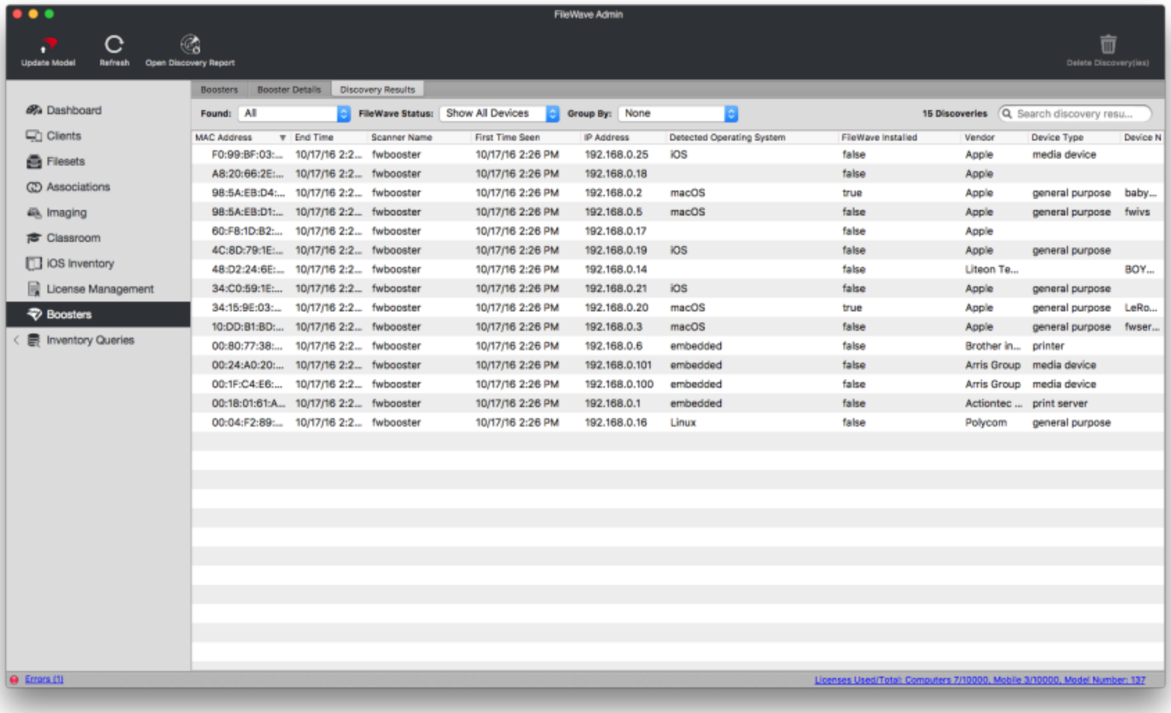
Please ensure you are authorised to perform these scans before proceeding, and/or that your network team has been informed of your intentions.

You can find more information here: Discovery Scanning (NMAP) Legal Considerations.

Please type following sentence to confirm that you have read the above information: 'I am authorized to scan the configured networks'.

I am authorized to scan the configured networks

Discovery Results tab in Boosters view



Found: All FileWave Status: Show All Devices Group By: None 15 Discoveries Search discovery resu...

MAC Address	End Time	Scanner Name	First Time Seen	IP Address	Detected Operating System	FileWave Installed	Vendor	Device Type	Device N
F0:99:BF:03:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.25	iOS	false	Apple	media device	
A8:20:66:2E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.18		false	Apple		
98:5A:EB:D4:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.2	macOS	true	Apple	general purpose	baby...
98:5A:EB:D1:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.5	macOS	false	Apple	general purpose	fwivs
60:F8:1D:B2:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.17		false	Apple		
4C:8D:79:1E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.19	iOS	false	Apple	general purpose	
48:D2:24:6E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.14		false	Liteon Te...		BOY...
34:C0:59:1E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.21	iOS	false	Apple	general purpose	
34:15:9E:03:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.20	macOS	true	Apple	general purpose	LeRo...
10:DD:B1:BD:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.3	macOS	false	Apple	general purpose	fwser...
00:80:77:38:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.6	embedded	false	Brother in...	printer	
00:24:A0:20:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.101	embedded	false	Arris Group	media device	
00:1F:C4:E6:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.100	embedded	false	Arris Group	media device	
00:18:01:61:A...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.1	embedded	false	Actiontec ...	print server	
00:04:F2:89:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.16	Linux	false	Polycom	general purpose	

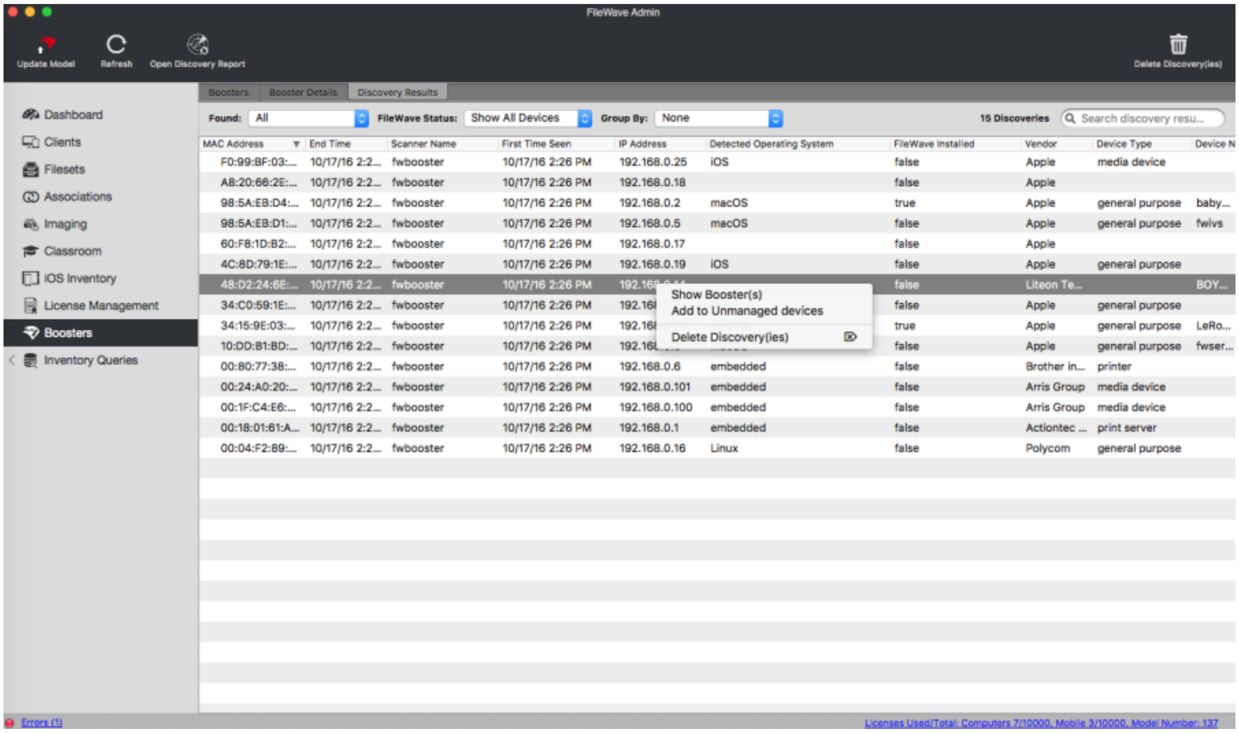
Errors (1) Licenses Used/Total: Computers 7/10000, Mobile 3/10000, Model Number: 137

In the screenshot on the previous page, you can see a view that presents all the discovery results. There are a few options to filter and group these results:

- The "**Found**" combo box allows an administrator to display devices that were found after given date. Options are: today; in last 1 day; in last 2 days, etc.
- The "**FileWave Status**" allows an administrator to filter devices based on whether they are managed or not.
- "**Group By**" widget allows an administrator to group devices based on: detected operating system; type; or Booster that performed the discovery (which should translate to a given subnet).

Right-clicking on a device or Group of devices gives the administrator the following options:

- "**Show Booster(s)**" switches back to the Booster tab and highlight the Booster(s) that found the selected results.
- "**Add to Unmanaged devices**" copies selected results to FileWave's unmanaged devices list.
- "**Delete Discovery(ies)**" removes selected discovery results from the database entirely.

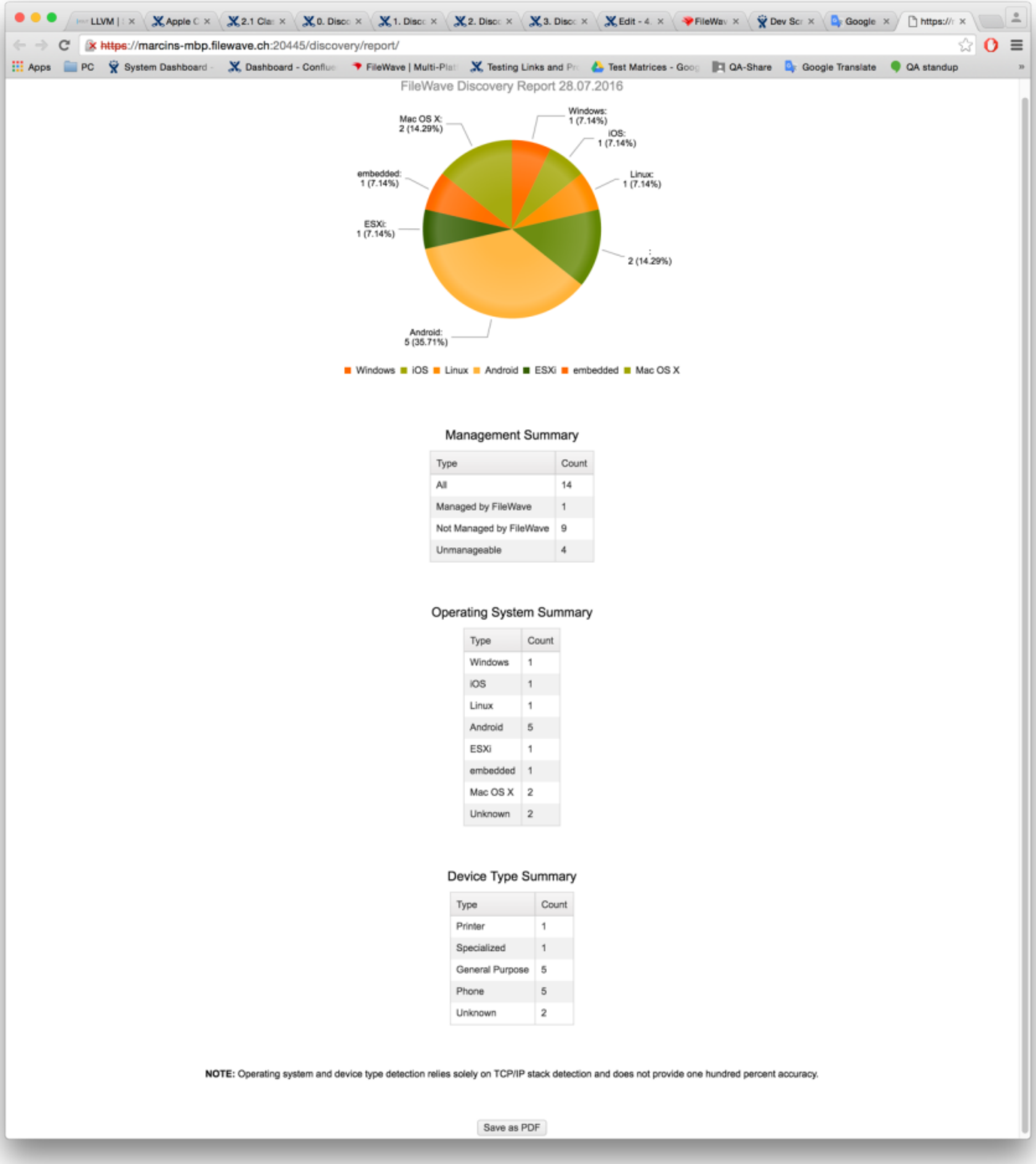


Found: All   FileWave Status: Show All Devices   Group By: None   15 Discoveries

MAC Address	End Time	Scanner Name	First Time Seen	IP Address	Detected Operating System	FileWave Installed	Vendor	Device Type	Device N
F0:99:BF:03:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.25	iOS	false	Apple	media device	
AB:20:66:2E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.18		false	Apple		
98:5A:EB:D4:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.2	macOS	true	Apple	general purpose	baby...
98:5A:EB:D1:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.5	macOS	false	Apple	general purpose	fwivs
60:F8:1D:B2:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.17		false	Apple		
4C:8D:79:1E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.19	iOS	false	Apple	general purpose	
48:D2:24:6E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168		false	Liteon Te...		BOY...
34:C0:59:1E:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168		false	Apple	general purpose	
34:15:9E:03:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168		true	Apple	general purpose	LeRo...
10:DD:B1:BD:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168		false	Apple	general purpose	fwser...
00:80:77:38:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.6	embedded	false	Brother in...	printer	
00:24:A0:20:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.101	embedded	false	Arris Group	media device	
00:1F:C4:E6:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.100	embedded	false	Arris Group	media device	
00:18:01:61:A...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.1	embedded	false	Actiontec ...	print server	
00:04:F2:89:...	10/17/16 2:2...	fwbooster	10/17/16 2:26 PM	192.168.0.16	Linux	false	Polycom	general purpose	

Discovery Report

In the top menu toolbar, there is "**Open Discovery Report**" button which opens the report in user's default web browser.
The Discovery report is used to visualize the entire set of devices that have been seen to date, it consists of the same information that is shown in the detailed list.



FileWave Discovery Report 28.07.2016

Management Summary

Type	Count
All	14
Managed by FileWave	1
Not Managed by FileWave	9
Unmanageable	4

Operating System Summary

Type	Count
Windows	1
iOS	1
Linux	1
Android	5
ESXi	1
embedded	1
Mac OS X	2
Unknown	2

Device Type Summary

Type	Count
Printer	1
Specialized	1
General Purpose	5
Phone	5
Unknown	2

NOTE: Operating system and device type detection relies solely on TCP/IP stack detection and does not provide one hundred percent accuracy.

The Discovery report can be saved as PDF file with button at the bottom of the screen.

How to configure your first Network Scan

1. Make sure that you have fulfilled all requirements described in section 12.3. Discovery - Requirements.
2. Make sure that your FileWave Server is correctly configured and working (Client can connect, shared keys are configured, etc.).
3. Make sure that your Booster is correctly configured and working (it must be connected to FileWave Server you prepared in previous step).
4. In FileWave Admin, go to the Boosters view, select your Booster and click the "**Configure Discovery**" icon in the top panel. In the configuration dialog that appears, enter all information required to perform a scan (if you want to get discovery results quicker, then change the aggressiveness to "aggressive" or "insane" scan, otherwise the timing template for network scanning results in a very, very slow scan (hours). Remember, however, more aggressive equals more network traffic that can affect normal network communications and can be seen as a Denial of Services attack.
5. The "**Enabled**" box must be checked for a scan to start. This protects the FileWave Administrator from configuring a scan and accidentally starting it. When you click on the "**OK**" button, you will be prompted with a warning regarding the implications of unauthorized

network scans. Depending on the configured schedule, you can wait until network scan is started by the scheduler or just start it immediately using the "**Start Discovery Scan**" button / contextual menu option.
6. You can monitor the status of the network scan using FileWave Admin Boosters view's "Last Discovery Scan Status" column. As soon as network scan data is reported to the database and FileWave Admin refreshes, the results should be visible in the Discovery Results tab in Boosters view.

You can tail the following file to see that a scan has been started, and is indeed running: /private/var/log/fwdiscovery.log

12.7. Network Discovery - Troubleshooting

If Discovery results aren't shown in FileWave Admin

If this occurs, re-enter the "**Discovery Results**" tab, switch to "**Boosters**" tab, then back. This will force a data refresh within the FileWave Admin UI.
Configure discovery options for given Booster again and start it manually. You should be able to see each action (configuration change, network scan starting) in the /var/log/fwdiscovery.log file. Depending on your configuration, eventually there will be message that the network scan has finished. If it finishes successfully and discovery results are still not shown in FileWave Admin, contact FileWave Support who will check your Django error log and verify that there were no database, exception, or other obvious errors.

Discovery application (*fwdiscovery*) doesn't start

Set Booster's log level to debug and restart it. You should be able to see whether the discovery application is started or not (in this case there will be a reason included). Don't forget to change the log level back to normal once troubleshooting is complete.

Discovery is not installed (Windows)

The "Discovery Installed" column in Boosters view reports that discovery is not installed. This is possible only for Windows platform. To install discovery, reinstall your Booster and make sure that you do not disable discovery during installation.

Discovery application seems to not react for configuration changes and/or manual start/stop scan requests from FileWave Admin

This shouldn't happen if the discovery application is working on tier-1 Booster (i.e., a Booster that communicates directly with the FileWave Server and with FileWave clients; not with another Booster). Things change when there are multi-tier Boosters deployed. If this is the case, make sure that all Boosters in the chain between the Booster having problems with discovery and FileWave Server are working correctly. Boosters in the chain are responsible for forwarding control messages for other Boosters and discovery applications. From our tests, it appears that notifications (control messages) chain starts working correctly after 30 seconds to two minutes after faulty Booster in the chain is brought back to life.
13. Chromebooks
The following processes and steps will walk you through getting your FileWave server setup to manage Chromebooks. Current functionality will allow you to pull/query inventory data and utilize our location tracking feature in FileWave. The 13.0 Chromebooks section will assume everything is being made from scratch. Some steps can be skipped if certain accounts and projects were made beforehand. Note that the extensions and application are only supported on Chrome 43 and greater.

13. Chromebook Management

FileWave has support for Chromebook management with the data that syncs from the Google Admin Console. Though this is not a total replacement for the Google Admin, FileWave does arm you with helpful tools and assets guaranteed to help your Chromebook deployment.

So what can we do?

With FileWave you will get all the same great inventory data you are used to with any other types of devices in FileWave. Maybe you would like to know how much disk space is left on those devices, or what user and at what time did they logged into any Chromebook? With FileWave all this data and more is available at your fingertips to run reports, scheduled email with this data, apply custom fields, or maybe you would like it easily exported out to a txt file.

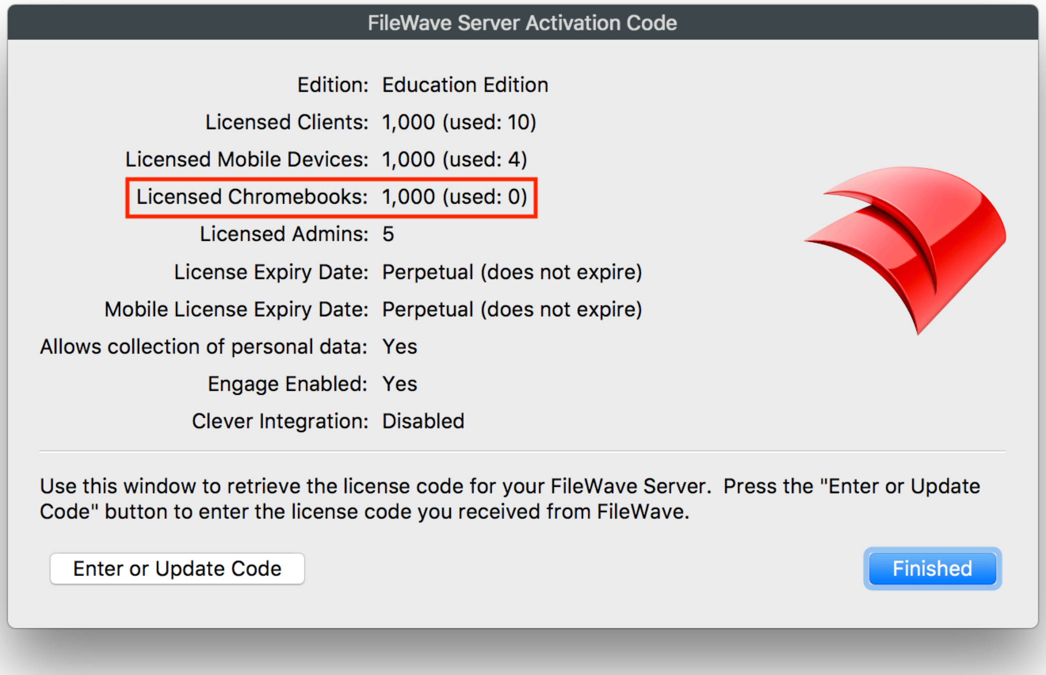
Inventory is just the beginning of what you can do with Chromebooks in FileWave, you also have the ability to gather a location and then view it right in the FileWave Admin on a map.

Using Engage? FileWave allows you to utilize Engage with your enrolled Chromebooks, so that teachers can have a more hands on approach with these devices in the classroom. They can send polls, launch extensions, see battery level, lock screen with a message, launch URL, send a message, and much more to come!

How do I set all this up?

To start managing your Chromebooks in FileWave there is some backend and prep work that needs to be done:

1. Make sure you have Chromebook Licenses in FileWave, you can check this by selecting **Activation Code** under the **Server menu** in the FileWave Admin:



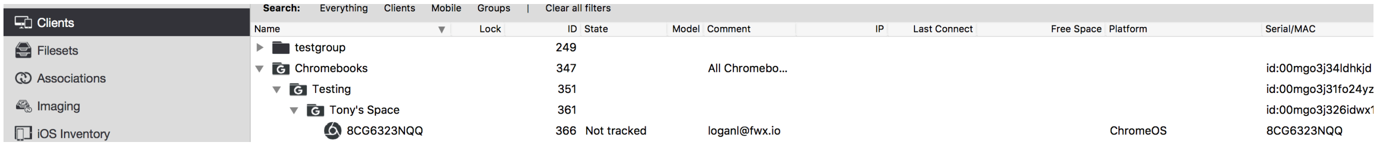
FileWave Server Activation Code

Edition: Education Edition
Licensed Clients: 1,000 (used: 10)
Licensed Mobile Devices: 1,000 (used: 4)
Licensed Chromebooks: 1,000 (used: 0)
Licensed Admins: 5
License Expiry Date: Perpetual (does not expire)
Mobile License Expiry Date: Perpetual (does not expire)
Allows collection of personal data: Yes
Engage Enabled: Yes
Clever Integration: Disabled

Use this window to retrieve the license code for your FileWave Server. Press the "Enter or Update Code" button to enter the license code you received from FileWave.

   *You will need to be sure you have enough Chromebook licenses in FileWave to match the number of Devices you are managing in the Google Admin. We will sync over the full list of devices, and you will not be able to update the model if FileWave does not have sufficient licenses.
2. You will need to follow the Guide linked here to setup GCM in FileWave: Google Cloud Messaging (GCM) Setup
3. Once GCM is fully setup you will need to follow the Quick Start Guide linked here to fully sync with Google Admin and get your Chromebooks talking to FileWave: Quick Start Guide for Chromebooks

With all that done you will notice there is now a new group structure in your Clients view that you can see all of your sync Chromebook devices:



Clients
Filesets
Associations
Imaging
iOS Inventory
Search: Everything Clients Mobile Groups | Clear all filters

Name	Lock	ID	State	Model	Comment	IP	Last Connect	Free Space	Platform	Serial/MAC
testgroup		249								
Chromebooks		347			All Chromebo...					id:00mgo3j34ldhkjd
Testing		351								id:00mgo3j31fo24yz
Tony's Space		361								id:00mgo3j326idwx1
8CG6323NQQ		366	Not tracked		loganl@fwx.io				ChromeOS	8CG6323NQQ

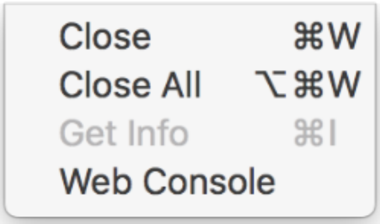
These devices and groups are synced with Google and therefore cannot be deleted directly out of FileWave.

14. Web Console

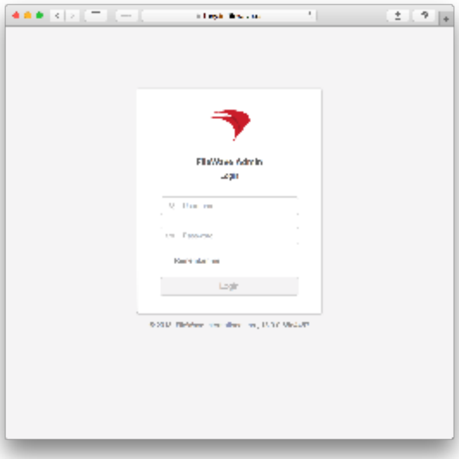
The FileWave Web Interface is an Inventory tool designed to help with quick FileWave inventory references for specific clients in your server. Within the Web console you will be able to view all devices currently enrolled, their Filesets, installed applications, users who have logged in, what groups they are apart of, and in the case of MDM enrolled Apple devices the command history.

To access this Web Console for the FileWave server you can use the following:

- Log into the FileWave Native Admin, select File at the top, then click Web Console



- Or Simply go to: https://FileWaveServerAddress
  If your server address is fw.initech.com
  https://tony.in.filewave.us



This Web Console utilizes port 443 and the FileWave server must be accessible to connect. So if your FileWave server is not accessible outside your internal network then you cannot expect to connect with the Web Console outside your network.

If you currently have a service running on the FileWave server that is already using port 443 the initial installation and an upgrade will fail. To resolve this, you will need to either shutdown that other 443 service or follow the instructions on the KB article linked here to change what port the FileWave Web Console is using.

> The error message in the macOS install log and Windows/CentOS terminal appears as follows:
>
> - 'FileWave requires port 443, but has noticed this port is already in use. To prevent a broken installation, FileWave has not installed/upgraded and your system has NOT been altered. Please contact Support for more information.'

The inventory information visible in the Web Console will be determined by the permissions of the admin account that logs in. For more information on setting permissions for FileWave administrators please visit the manual page linked here.

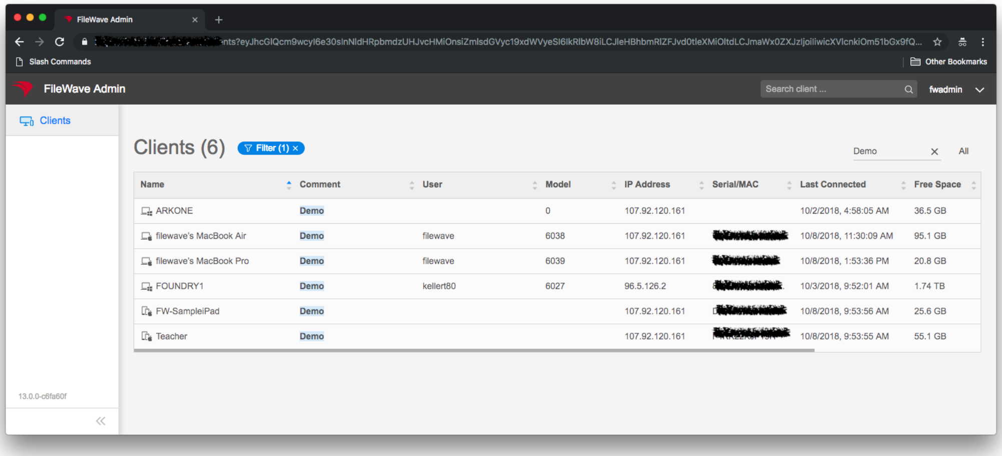
The information you have access to from inventory under the Details section for each client is the following:

- Applications
- Device
    - General
    - Hardware
    - Security Settings
- Engage Profiles
- Filesets
- Fonts
- FileWave Policies
- Groups
- Network Interfaces
- Operating System
- Profiles
- Users

- VPP Users

Below are some examples of the data you have access to in the Web Console and corresponding screenshots:

You will initially see the Clients dashboard that lists out every device currently being managed in your FileWave server:

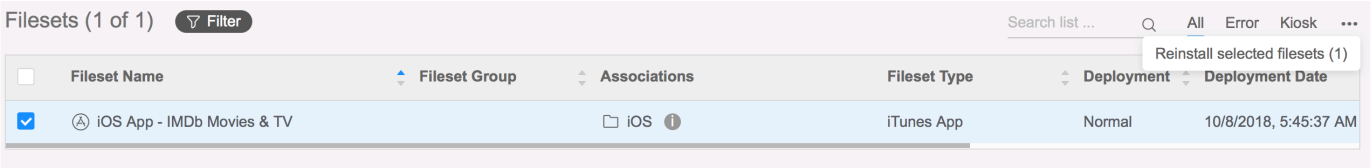


FileWave Admin
[redacted]nts?eyJhcGlQcm9wcyl6e30sInNldHRpbmdzUHJvcHMiOnsiZmlsdGVyc19xdWVyeSI6IkRlbW8iLCJleHBhbmRlZFJvd0tleXMiOltdLCJmaWx0ZXJzljoiliwicXVlcnkiOm51bGx9fQ...
Slash Commands
Other Bookmarks
FileWave Admin
Search client ...
fwadmin
Clients
Filter (1)
Demo
All
13.0.0-c6fa60f

Clients (6)

Name	Comment	User	Model	IP Address	Serial/MAC	Last Connected	Free Space
ARKONE	Demo		0	107.92.120.161		10/2/2018, 4:58:05 AM	36.5 GB
filewave's MacBook Air	Demo	filewave	6038	107.92.120.161	[redacted]	10/8/2018, 11:30:09 AM	95.1 GB
filewave's MacBook Pro	Demo	filewave	6039	107.92.120.161	[redacted]	10/8/2018, 1:53:36 PM	20.8 GB
FOUNDRY1	Demo	kellert80	6027	96.5.126.2	[redacted]	10/3/2018, 9:52:01 AM	1.74 TB
FW-SampleiPad	Demo			107.92.120.161	[redacted]	10/8/2018, 9:53:56 AM	25.6 GB
Teacher	Demo			107.92.120.161	[redacted]	10/8/2018, 9:53:55 AM	55.1 GB

From there you will be able to select a client and view inventory and Fileset status information including being able to reinstall selected Filesets:



Filesets (1 of 1)

	Fileset Name	Fileset Group	Associations	Fileset Type	Deployment	Deployment Date
☑	iOS App - IMDb Movies & TV		iOS	iTunes App	Normal	10/8/2018, 5:45:37 AM

Client Information tabs:

Your browser does not support the HTML5 video element

Client Details:

Your browser does not support the HTML5 video element