FileWave Client

Enrolling Devices

Articles about the process to enroll devices in to FileWave.

Enrolling Devices

Desktop / Laptop Client Install and Configure

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

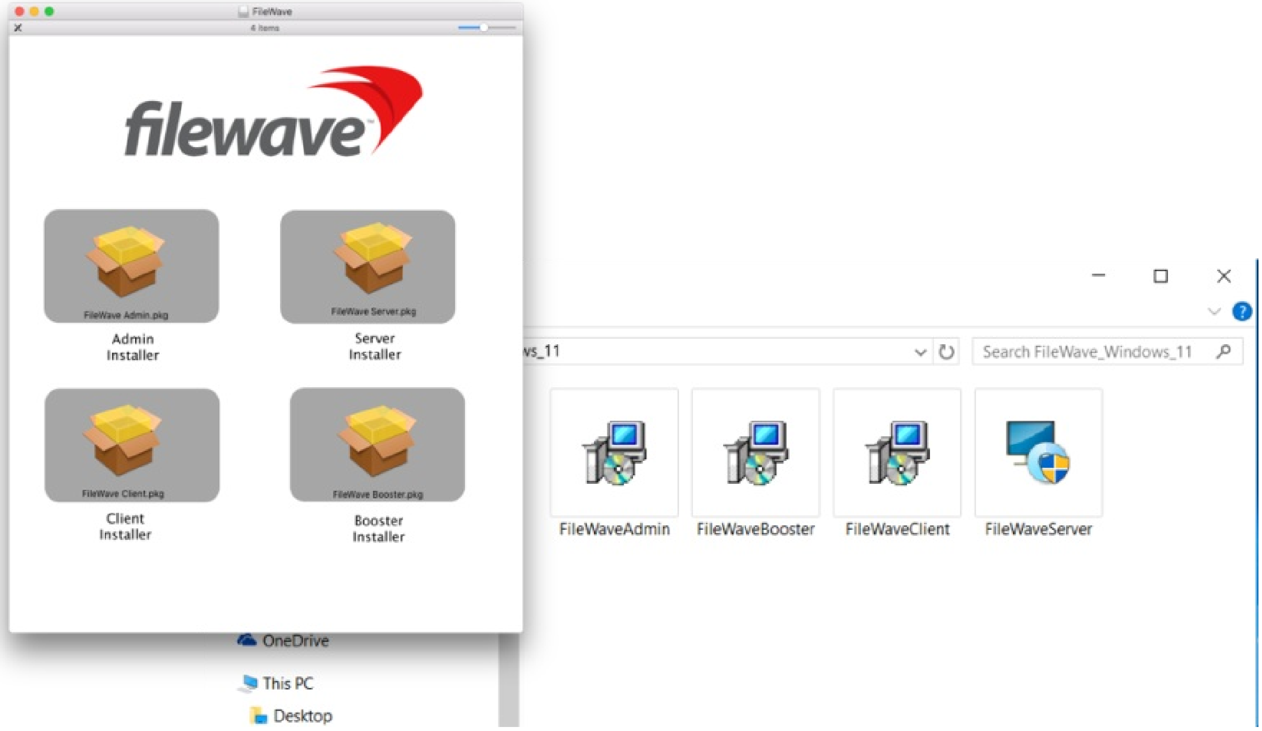
Operating Systems Supported

- macOS
- Windows 10 & 11

For specific versions look at the Downloads page to see what is required for that version.

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 KB in Downloads. For the computers mentioned under Legacy Support, you will need to install the most recent client supported on your OS.

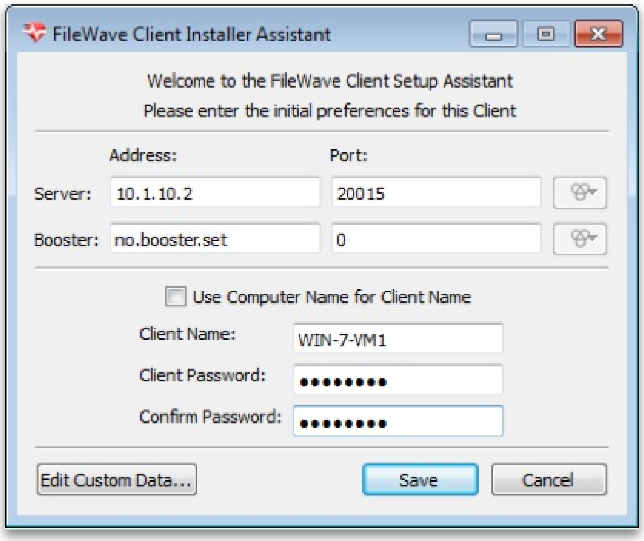


You should download all installers you will need for your deployment at the same time. They can be stored on a file server, or on a flash drive in Windows format for cross platform compatibility (OS X / macOS systems can read Windows-formatted drives without additional drivers).

> 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 in FileWave Server Installation. 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.



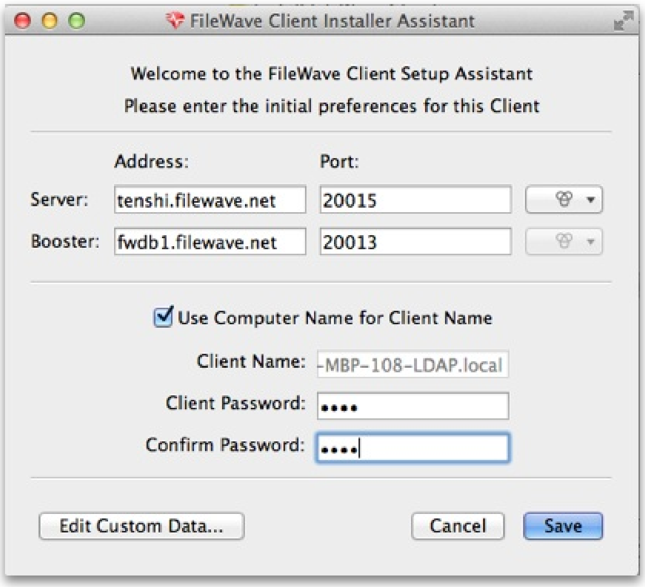
FileWave Client Installer Assistant

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: ••••••••



FileWave Client Installer Assistant

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: ••••

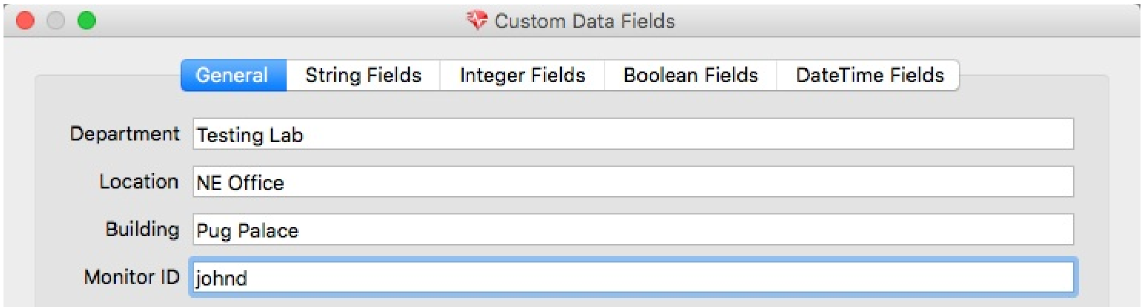
Installation Settings

- 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)
- 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 (20013)

Note: More on working with FileWave Boosters in Boosters.

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

Edit Custom Data...



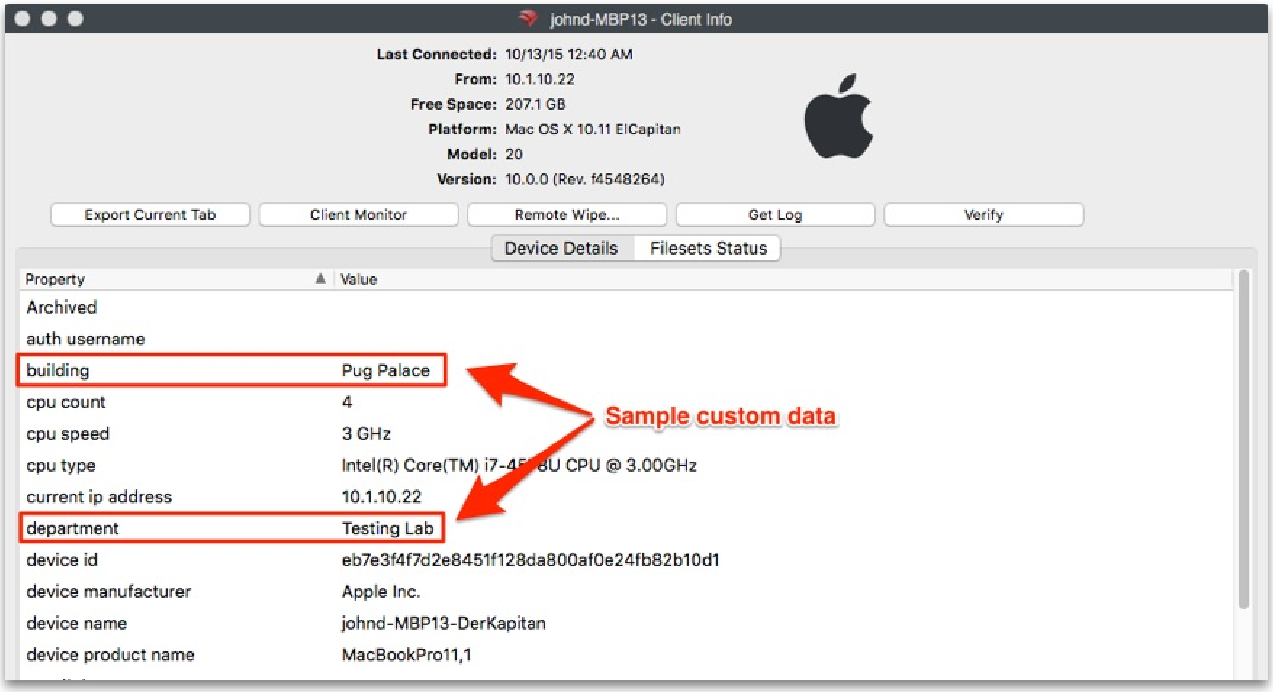
Department: Testing Lab

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) i7-4[illegible]8U 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

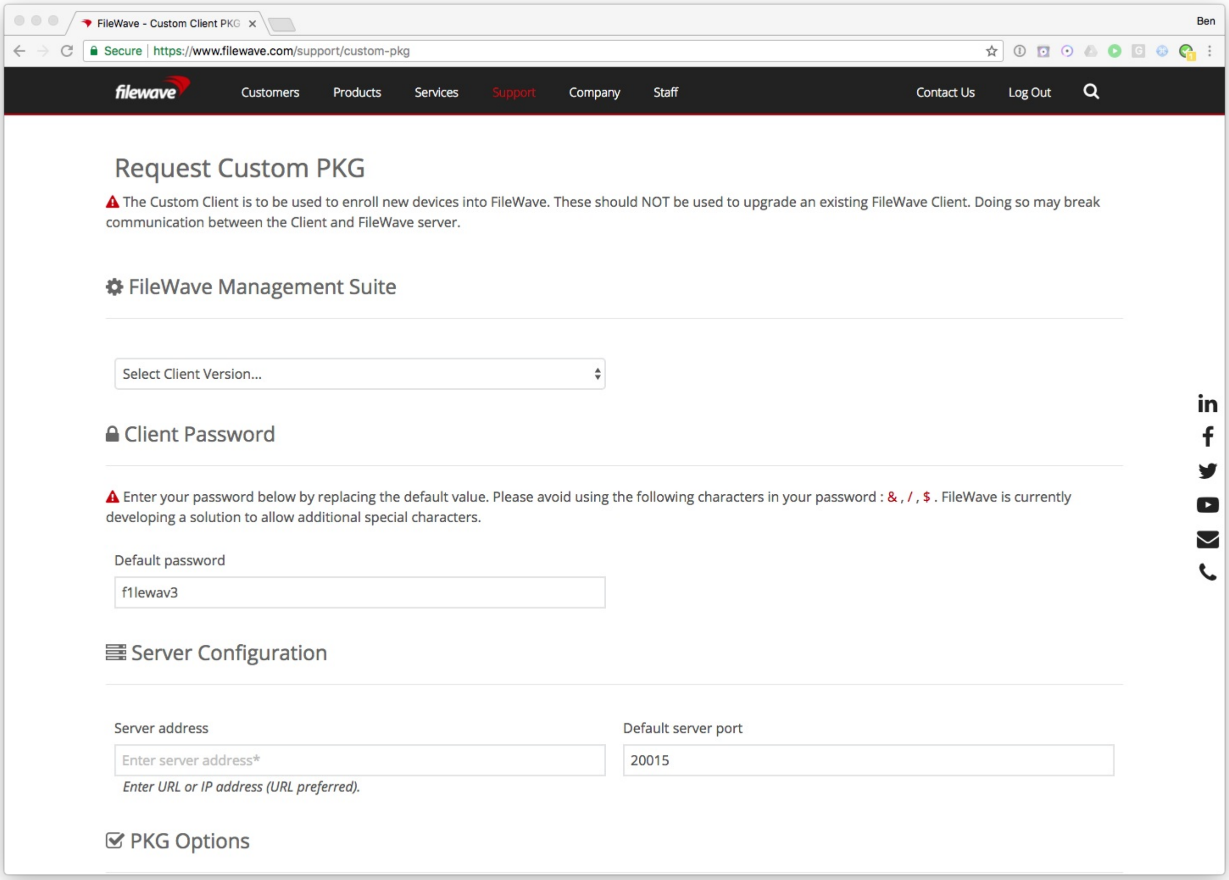
Automating installation with a custom client installer

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://custom.filewave.com/py/custom_client_mac.py
For Windows: https://custom.filewave.com/py/custom_client_win.py

> The customized client for macOS 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).

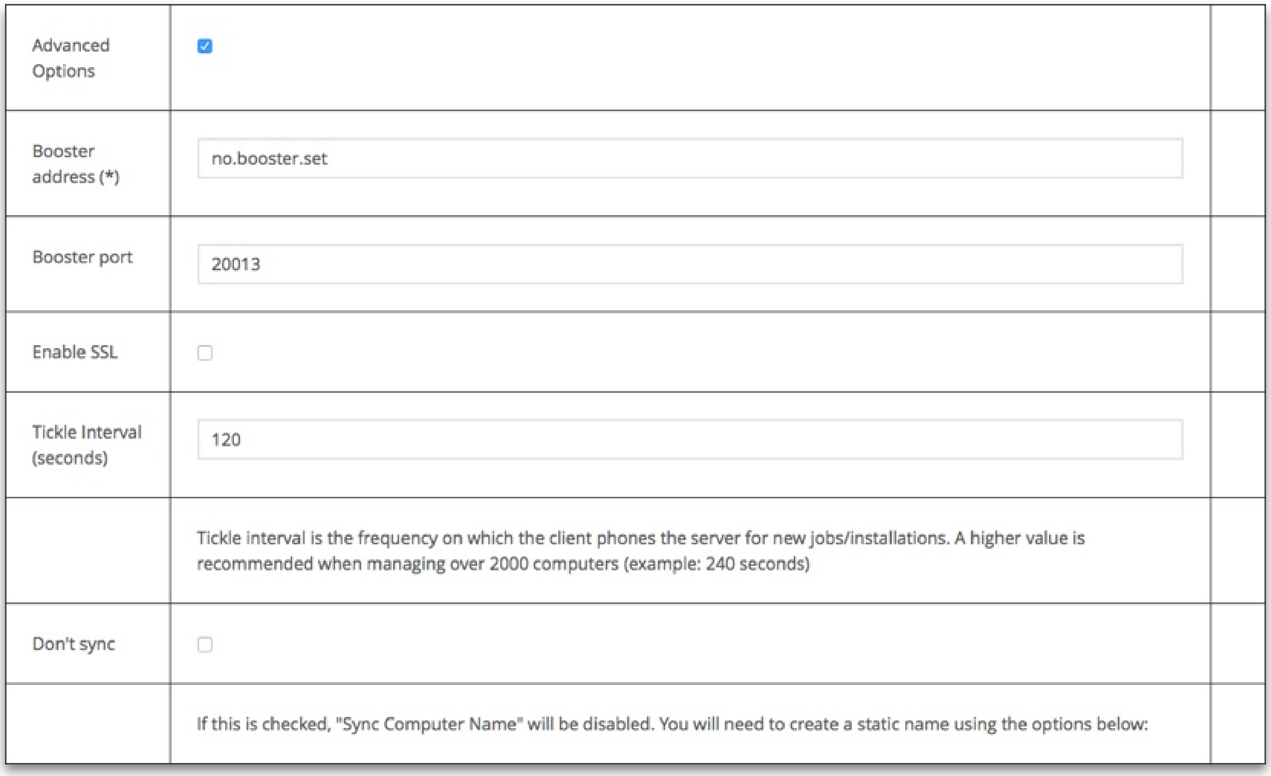
Default server port: 20015

PKG Options

Many fields are required.

> Note: The default port setting is 20015. However, SSL is now required, and the system will automatically use port 20017 instead when 20015 is entered. Do not manually set the port to 20017. Always enter 20015, and the system will handle the SSL port change for you.

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:

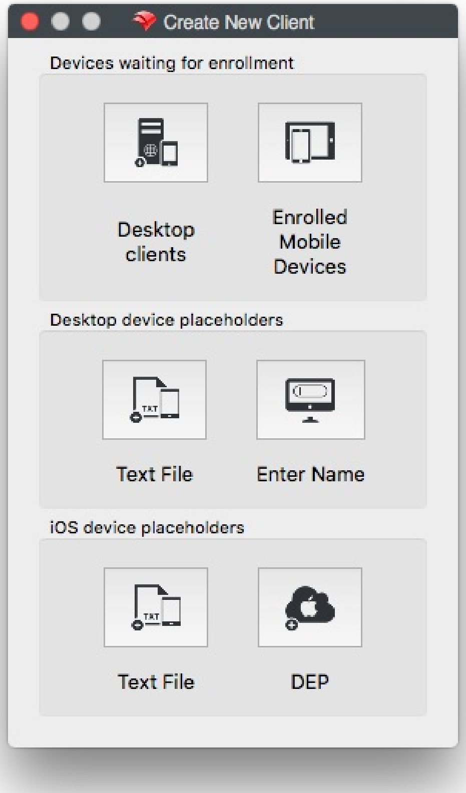
The custom installer does not ask the user for any device specific information, and can be distributed through several means:

- 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.

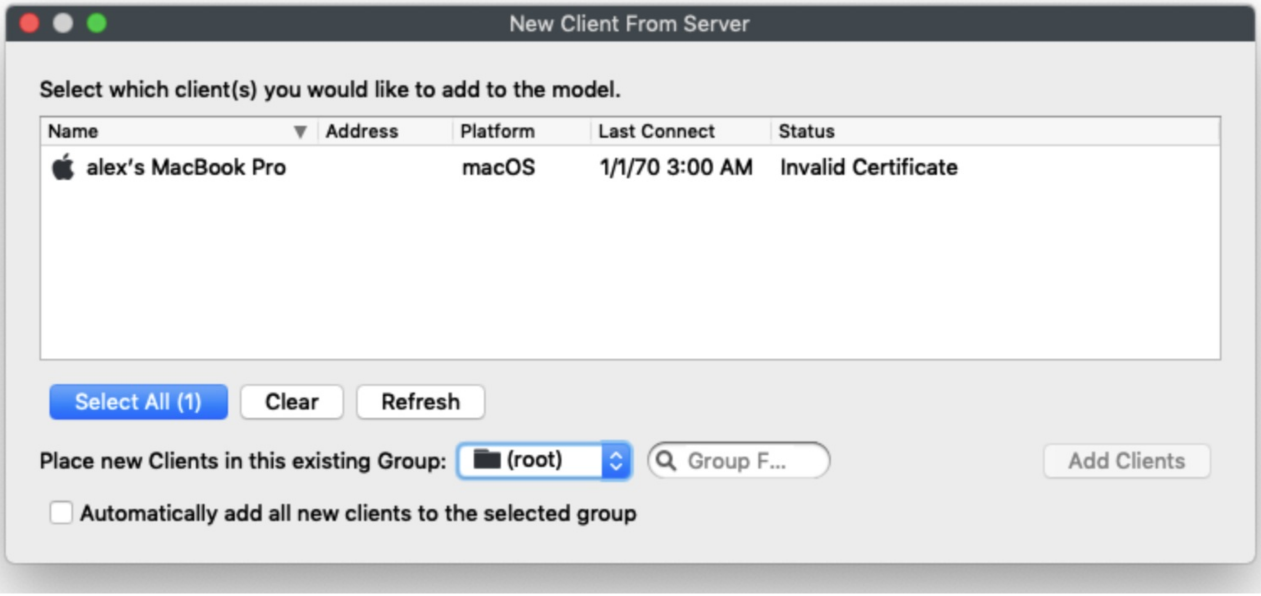
> ✓ Note: FileWave provides "recipes" of possible deployment workflows for the custom installer in the KB.

Enrolling Computer Clients in to FileWave

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.



For Text File see Importing Computer Clients from a File



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

Name	Address	Platform	Last Connect	Status
alex's MacBook Pro		macOS	1/1/70 3:00 AM	Invalid Certificate

Place new Clients in this existing Group: (root)

□ Automatically add all new clients to the selected group

Column Name	Notes

Name	The Client Name the computer is attempting to connect with (see Sync Computer Name)
Address	The IP Address the client is connecting from, this may be it's internal address, or NAT if the computer is connecting from somewhere on the internet
Platform	The OS of the client; macOS or Windows
Last Connect	The last time the FileWave Client attempted to check-in with the server (Default of every 2min)
Status	You will see one of three options: ● New Client - Brand new device with a valid certificate ● Invalid Certificate - The device either has no certificate (might be client older than 13.1), or the certificate is invalid or damaged on the client ● Valid Certificate but a new Enrollment happened - The certificate is OK, but the clients identification has changed All three status states can be approved by selecting then adding the client See: What is Compatibility Mode?

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.

Related Content

- Conflict Resolution
- Enrolling Mobile Devices

Mass Deploy Windows FileWave Client

Summary

One of the most irritating bumps in the road towards the administrative freedom of FileWave is installing the FileWave Client on your computers for the first time. Now that we've started using MSI-based installers, you can easily deploy the FileWave WinClient via a domain server or log-on script. This post provides materials to aid in WinClient Mass Deployment.

1. Download the latest Windows FileWave Client (it's an exe in version 5.7 and up) and WinClient Prefs Writer (link at bottom). To convert the exe into an msi installer check the conversion script

generatefwwinclientmsi.vbs.zip

This is an example on how you would run it:
cscript C:\path\generatefwwinclientmsi.vbs C:\path\FileWaveClient.exe

2. Edit the preferences script to include your settings. I have put in example settings -- you must put your own in and then save the file.

Before:

Code:

```
set serverName=no.server.set
set serverAddress="no.server.address"
set clientPassword="filewave"

set booster1="no.booster.set"
set booster1Port="0"

:::

set clientName=""
```

After:

Code:

```
set serverAddress="fwserver.filewave.us"
set clientPassword="jelly"

set booster1IP="fwbooster.filewave.us"
set booster1Port="20013"

:::

set clientName=""
```

3. Once the script is edited, these are both ready to execute on a computer, either by log-on script or some remote activation. Make sure that the MSI installs before the preferences script runs.

If you install the Client via the command line, add the "/quiet" argument to execute a silent installation. For a comprehensive list of the available arguments for MSI's, run the MSI using the "/?" argument.

FWClientPrefsWriter.zip	668 B

Apple Notarisation and Custom PKG Installers

Description

Apple has introduced notarisation as a requirement for installation of PKGs on macOS with macOS version 10.15. Notarisation status can be determined in two ways :

- Offline: cryptographically verifying a ticket stapled to the PKG at installer creation time
- Online: contacting apples servers to verify an app / installer has been notarised

Information

Custom installers for FileWave Client and Booster will be notarised starting from Version 13.2.2 and upwards, however, the notarisation ticket will not be stapled onto the PKG you download from https://custom.filewave.com at the current time, requiring 'Online' confirmation.

Provided your macOS machines can reach the required servers outlined in https://support.apple.com/en-us/HT210060 , you can expect everything to work as normal after 10-15 minutes of downloading the custom PKG.

Hosts	Ports	Protocol	OS	Description	Supports proxies
17.248.128.0/18	443	TCP	macOS only	Ticket delivery	—
17.250.64.0/18	443	TCP	macOS only	Ticket delivery	—
17.248.192.0/19	443	TCP	macOS only	Ticket delivery	—

> ⓘ Custom PKG Version 13.2.2
> Version 13.2.2 Custom PKGs created prior to 4th March 2020 will not be notarised and will require re-creating if notarisation is required

Confirmation

The PKG may be tested for notarisation. On macOS 10.15.x you may observe the following:

Before notarisation has been completed by Apple:

Unnotarised

```
% spctl -a -vvv -t install FileWaveClient_13.2.2-fw.filewave.com-20-Feb-2020.pkg
FileWaveClient_13.2.2-fw.filewave.com-20-Feb-2020.pkg: rejected
source=Unnotarized Developer ID
origin=Developer ID Installer: FileWave (Europe) Gmbh (83S2TRZ3CS)
```

After notarisation has been completed by Apple:

Notarised

```
% spctl -a -vvv -t install FileWaveClient_13.2.2-fw.filewave.com-20-Feb-2020.pkg
FileWaveClient_13.2.2-fw.filewave.com-20-Feb-2020.pkg: accepted
source=Notarized Developer ID
origin=Developer ID Installer: FileWave (Europe) Gmbh (83S2TRZ3CS)
```

User Approved MDM Enrollment (macOS)

Description

Apple has introduced a new concept with macOS High Sierra, User Approved MDM Enrolment. This will only affect the management of settings that Apple deemed to be considered ‘security-sensitive. All other non-sensitive settings will continue to work, as previously, without User Approved Enrolment. This does not affect devices enrolled through DEP.

There are two aspects to this.

- User Approved MDM Enrolment
- Configuration Profile payloads that will require User Approved MDM Enrolment.

The first payload Apple has announced that will use these features is the Kernel Extensions payload.

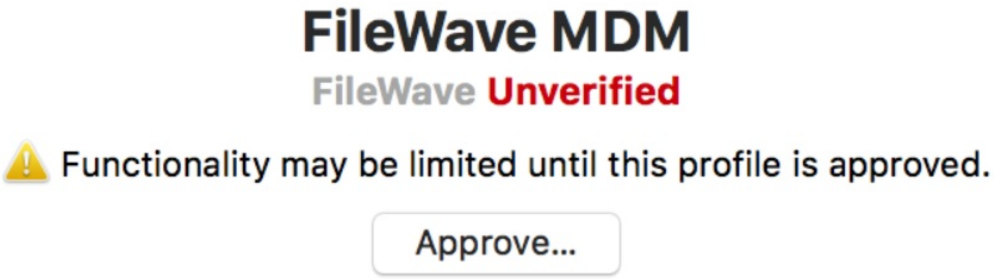
https://support.apple.com/en-us/HT208019

Unlike other payloads, any ‘security-sensitive’ payload will be deliverable only by MDM and will rely on the MDM enrolment being User Approved.

User Approved MDM Enrolment

Currently, User Approved MDM Enrolment relies on the device being enrolled; the method of enrolment does not matter yet but will do in future releases. At this point, the enrolment must be either:

- DEP enrolment (user approval not required)
- User installing the enrolment profile manually
- User accepts the enrolment profile through System Preferences > Profiles:



FileWave MDM

FileWave **Unverified**

⚠ Functionality may be limited until this profile is approved.

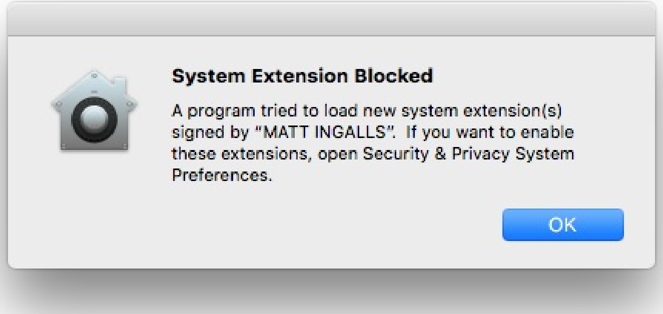
You will notice this approval box in 10.13.2, if the method of enrolment was hidden from the user, e.g. scripted. Devices enrolled on earlier versions and then upgraded will automatically be MDM enrolled as User Approved.

Kernel Extensions

Apple introduced a halfway house with the release of 10.13. Apple has now released version 10.13.4 which has full implementation of this feature.

How does this affect kernel extensions?

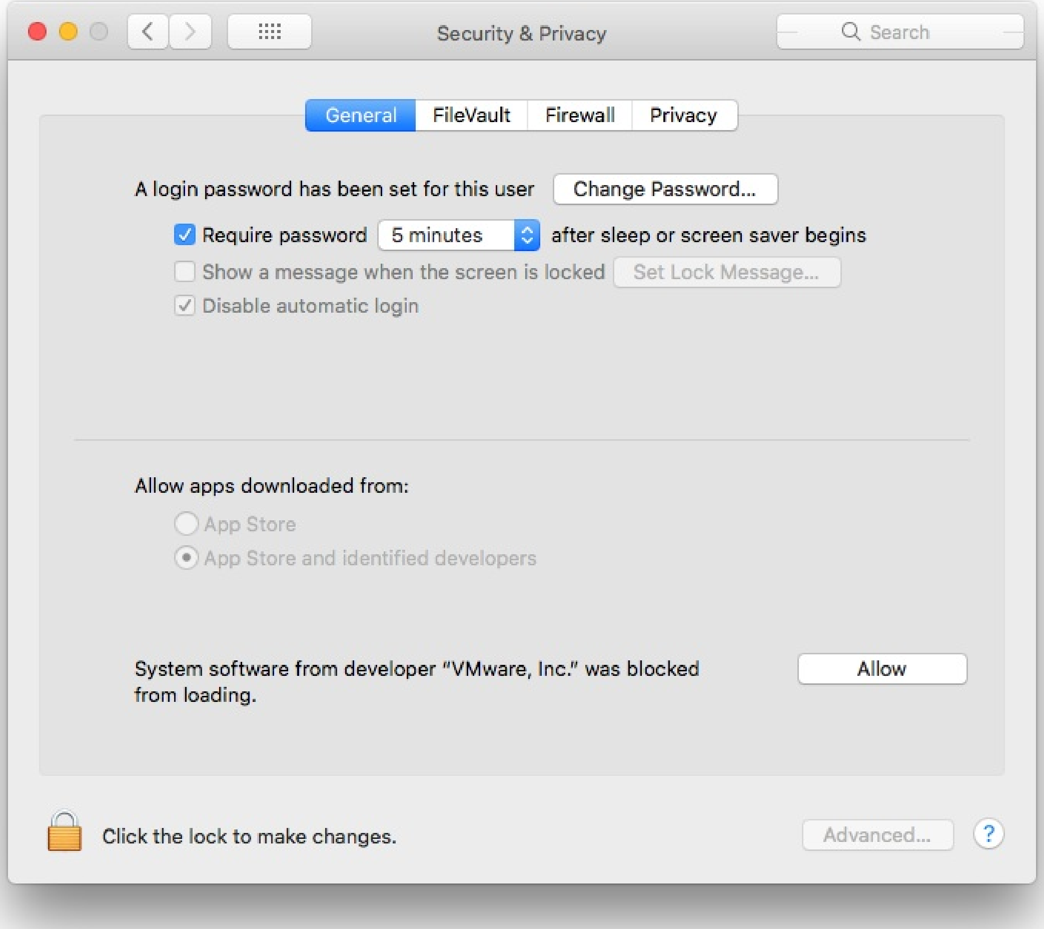
Attempts to install a Kernel Extension with a device that is not enrolled into MDM will be greeted with the following message:



System Extension Blocked

A program tried to load new system extension(s) signed by "MATT INGALLS". If you want to enable these extensions, open Security & Privacy System Preferences.

To approve the Kernel Extension will either require MDM enrolment or the user allowing the blocked Extension to run, via System Preferences > Security & Privacy > General:



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from developer "VMware, Inc." was blocked from loading.

What happens if I already have kernel extensions installed?

Any extension installed prior to upgrading to 10.13 High Sierra will continue to work, only newly installed kernel extensions will be affected.

Once a particular kernel extension is approved, subsequent upgrades to that kernel extension will automatically be user-approved.

Managing Kernel Extensions through MDM

Prior to version 10.13.4, there is no management beyond having the device enrolled into MDM. However, with 10.13.4, management is now available through the Kernel Extension Policy payload, allowing extension loading without user consent when enrolled appropriately; the payload can only be delivered with MDM, to devices that are User Approved MDM Enrolled. This could result in apps relying on kernel extensions to stop functioning properly (e.g. VPN clients, antivirus software).

As of FileWave version 12.7.0, the Kernel Extensions payload was introduced. To allow Kernel Extensions requires either:

1. 'Team Identifier'
2. Individually using the 'Kernel Extension bundle ID'.

These values are stored locally on a device after installation. Therefore, to find these values involves installing them on a device and then reading these values from a file, e.g., for a machine that has VMware Tools installed. One machine could have all Extensions installed prior to running the command to list all necessary Kernel Extensions.

```
$ sqlite3 /var/db/SystemPolicyConfiguration/KextPolicy 'select team_id,bundle_id from kext_policy;'
EG7KH642X6|com.vmware.kext.VMwareGfx
EG7KH642X6|com.vmware.kext.vmhgfs
```

This lists the Team Identifier followed by the Bundle ID for two Kernel Extensions that have been added with the installation of VMware Tools. Both have the same Team Identifier, but have differing Bundle IDs.

1. To just use Team Identifier, add the returned Team Identifier from the command for the Kernel Extensions you wish to approve, to the 'Allowed Team Identifiers' whtielist. All Kernel Extensions with this Team Identifier will be whitelisted.
2. To only allow certain Kernel Extensions, instead use the 'Allowed Kernel Extensions' whitelist and add both Team Identifier and Bundle ID. Note, legacy Extensions may not have a Team Identifier. For those that don't, just supply the Bundle ID and leave the Team Identifier empty.

There is also a community of users that are adding Identifiers and Bundle IDs which could save you having to instal in advance.

Community Kernel Extensions List

Data in this list is not checked in any way. As this is in place for security reasons and anyone can add information to this file, use with care:

Community Kernel Extensions List

Can I use User Approved Kernel Extension loading without MDM?

Yes. This however involves booting the computer into recovery mode and using the following command:

> $ spctl

See the man page for required options:

https://developer.apple.com/legacy/library/documentation/Darwin/Reference/ManPages/man8/spctl.8.html

N.B. This is stored in NVRAM. If you reset the NVRAM, you will lose the ability to use User Approved Kernel Extension loading with this method until the steps are retraced. A firmware password could be set to prevent unauthorized NVRAM resets.

Extensions Payload

The Extensions payload should not be confused with the Kernel Extensions payload.

https://help.apple.com/profilemanager/mac/5.4/#/apd58550e429

The Extensions payload controls those extensions visible through the Extensions System Preferences and will not affect Kernel Extensions

Enrolling Devices

macOS MDM Enrolment State

DESCRIPTION

macOS devices are unique, in as much as they may be managed by both the FileWave Client and Apple's MDM process. The MDM Enrolment State is an inventory item which shows the current state of MDM enrolment.

> FileWave requires the FileWave Client for basic management of macOS devices. MDM is an additional extra to expand the management options, as provided by Apple. There is no MDM only option for macOS devices.

INFORMATION

MDM Enrolment State

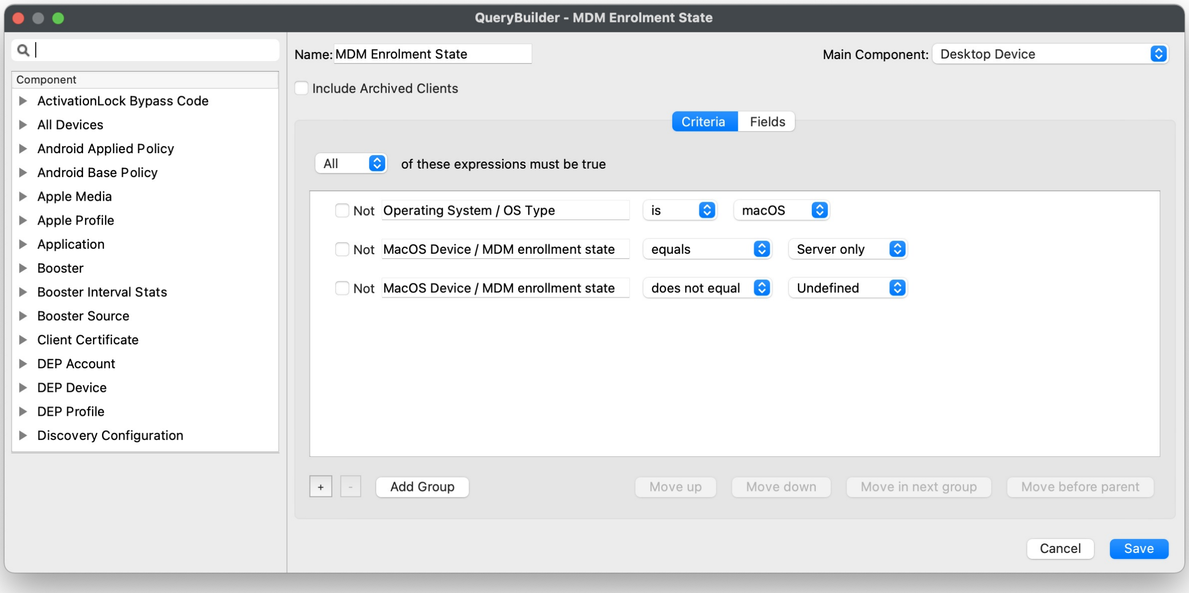
The state is a live report of the current status of the device's enrolment; imagine if a device was initially MDM enrolled, but the enrolment profile has been subsequently removed from the device. Status values include:

- Full Enrolled – Device was MDM enrolled and all is good. This would be usual for DEP or OTA
- Server only – Devices was MDM enrolled, but the device no longer has an enrolment profile installed
- Device only – Device has an MDM enrolment profile installed, yet the database has no reference of this
- Undefined – Device is running a version of FileWave older than 14.3.0 or has not yet reported back its state
- Not Enrolled – Device has never been MDM enrolled and is managed purely by the FileWave Client

DIRECTIONS

A query may be used to identify devices that are not in an expected state, for example, identify devices that no longer have an Enrolment Profile installed

An example query could look something like:



QueryBuilder - MDM Enrolment State

Name: MDM Enrolment State

Main Component: Desktop Device

□ Include Archived Clients

All of these expressions must be true

□ Not Operating System / OS Type is macOS

□ Not MacOS Device / MDM enrollment state equals Server only

□ Not MacOS Device / MDM enrollment state does not equal Undefined

Add, edit or remove criteria to meet desired reporting.

ADDITIONAL INFORMATION

To assist identifying why a device may show as 'Device Only', the following Custom Fields may be added, reporting the Server Root Cert Name and the APNs of the enrolment profile:

MDM Server Root Certificate Name

↓ macOS

Enrolment Profile APNs Topic

↓ macOS

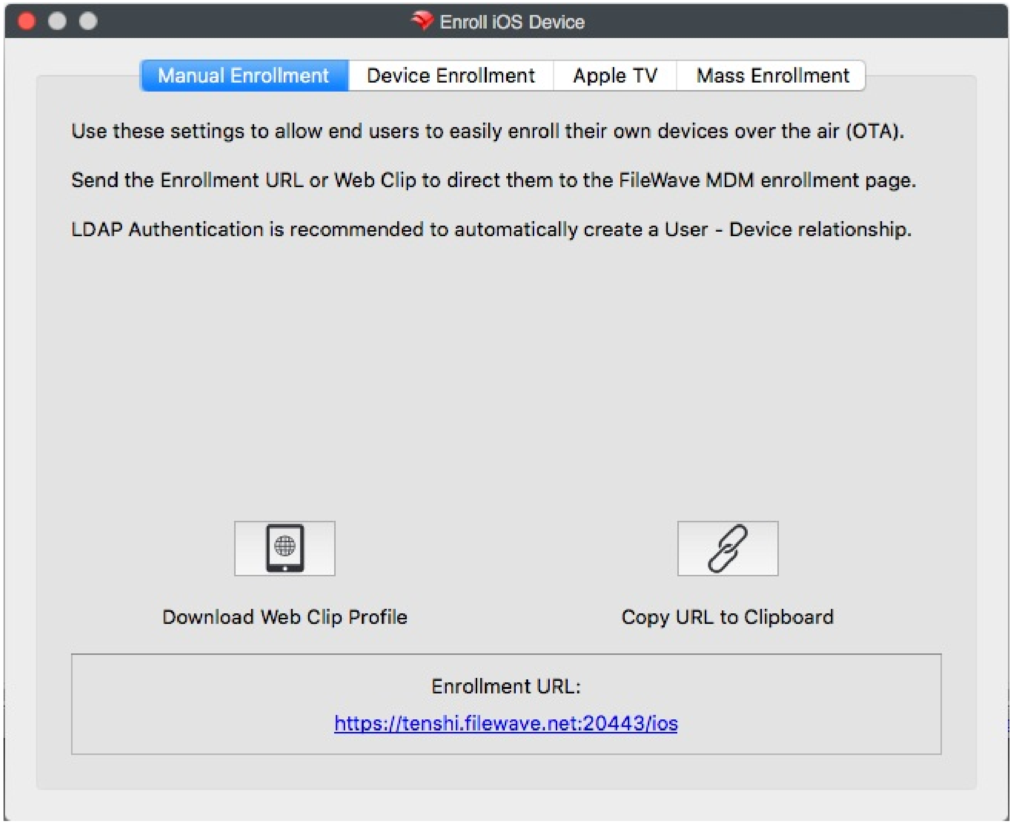
Enrolling Devices

Enrolling Mobile Devices into FileWave

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:



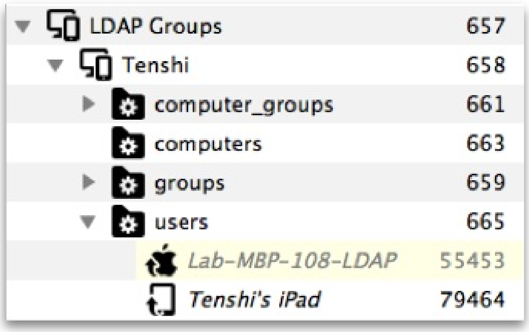
Use these settings to allow end users to easily enroll their own devices over the air (OTA).

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.

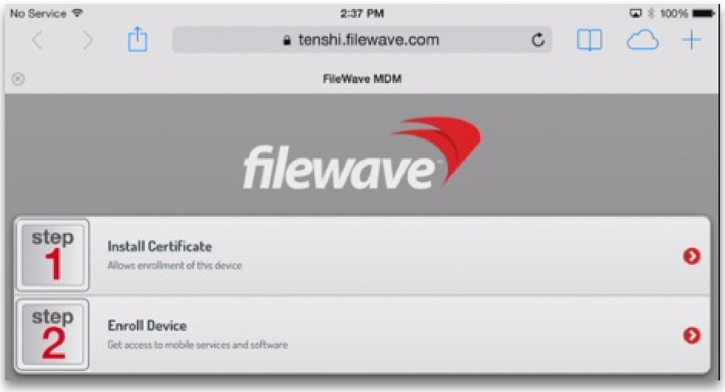
Enrollment URL:
https://tenshi.filewave.net:20443/ios

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.


No Service 2:37 PM 100%

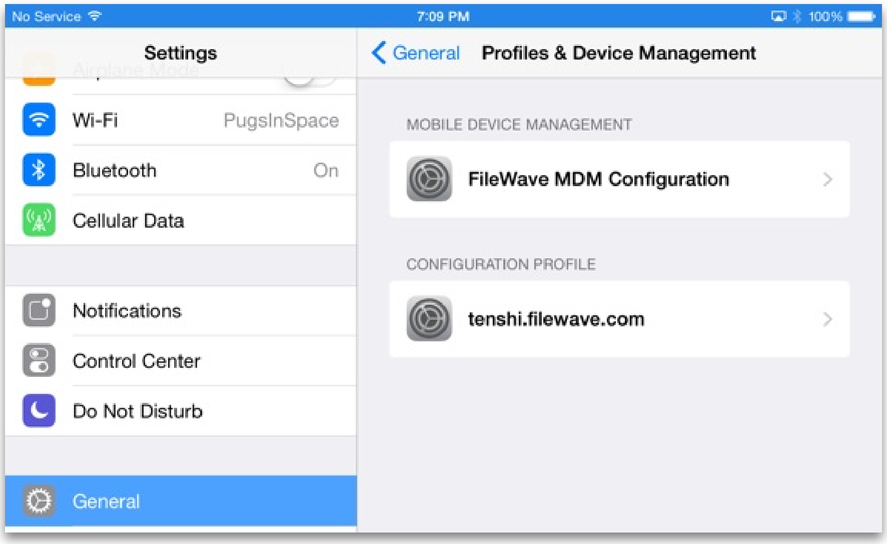
tenshi.filewave.com

FileWave MDM

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:


No Service 7:09 PM 100%

Settings

Wi-Fi PugsInSpace

Bluetooth On

Cellular Data

Notifications

Control Center

Do Not Disturb

General

General Profiles & Device Management

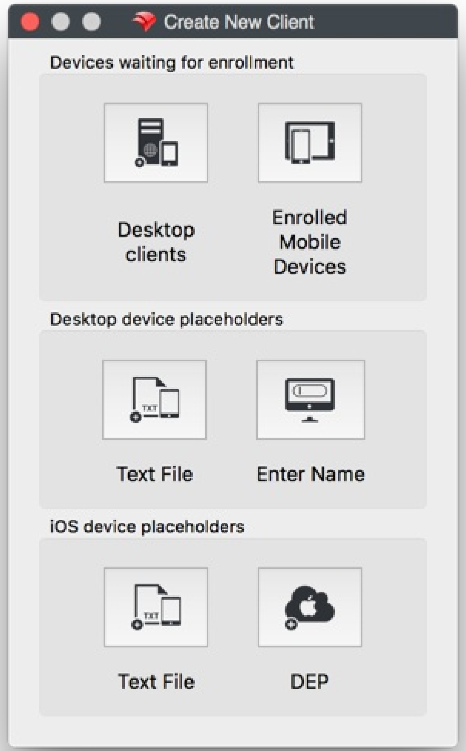
MOBILE DEVICE MANAGEMENT

FileWave MDM Configuration

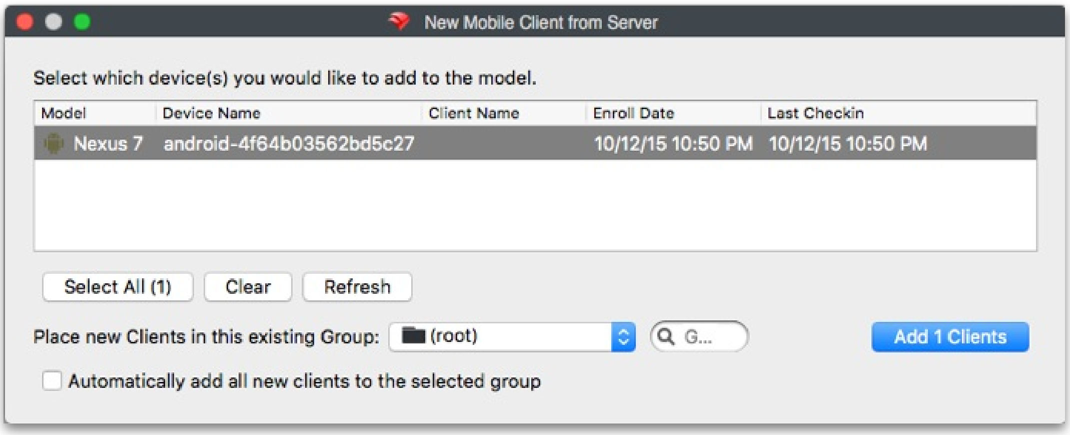
CONFIGURATION PROFILE

tenshi.filewave.com

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:



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.

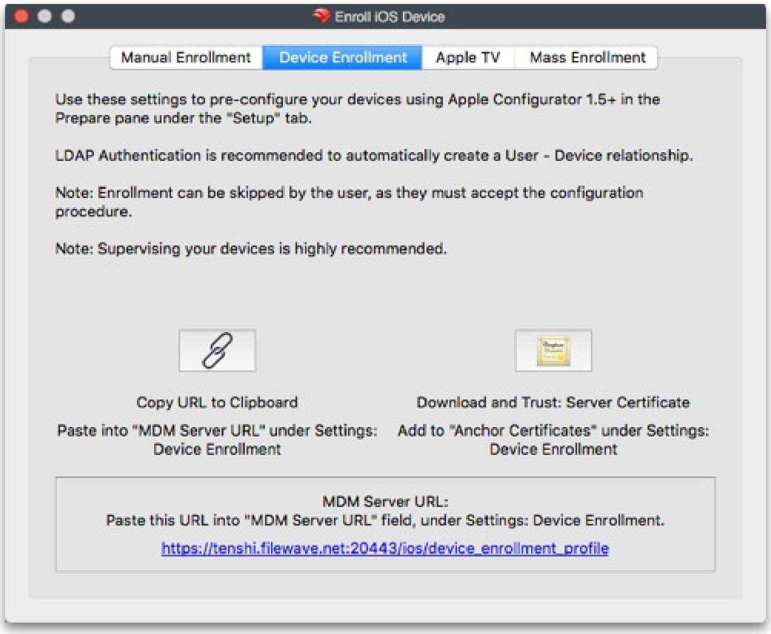
Automatic or Forced Enrollment - iOS

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

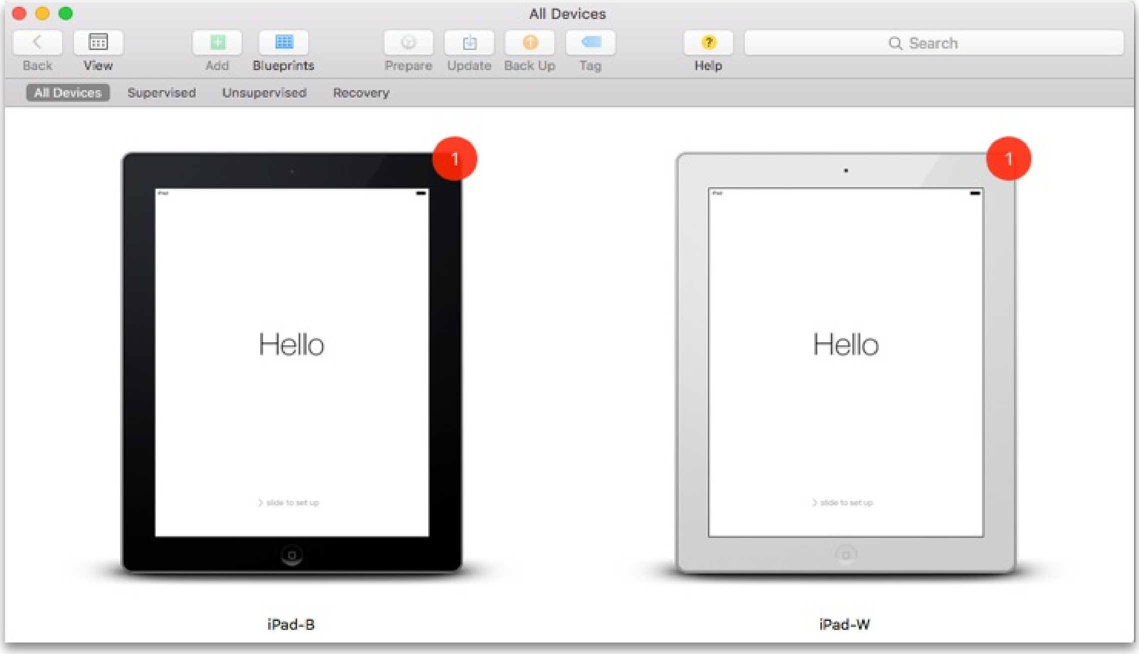
Add to "Anchor Certificates" under Settings: Device Enrollment

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

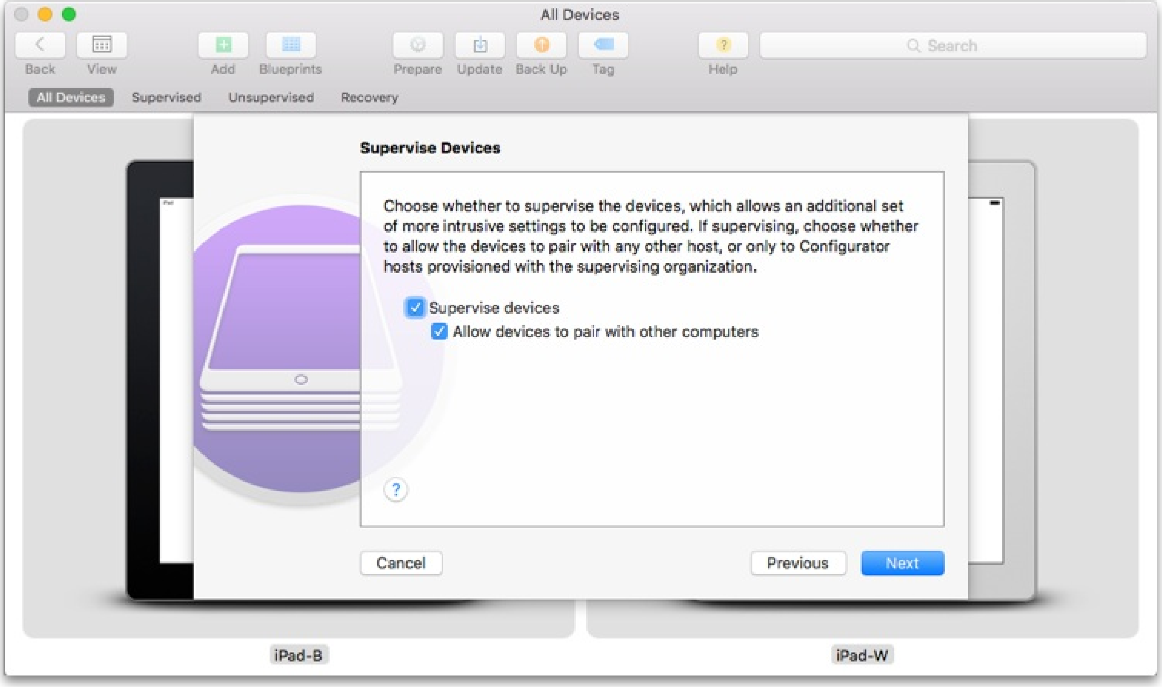
Apple Configurator v2.2.1

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.

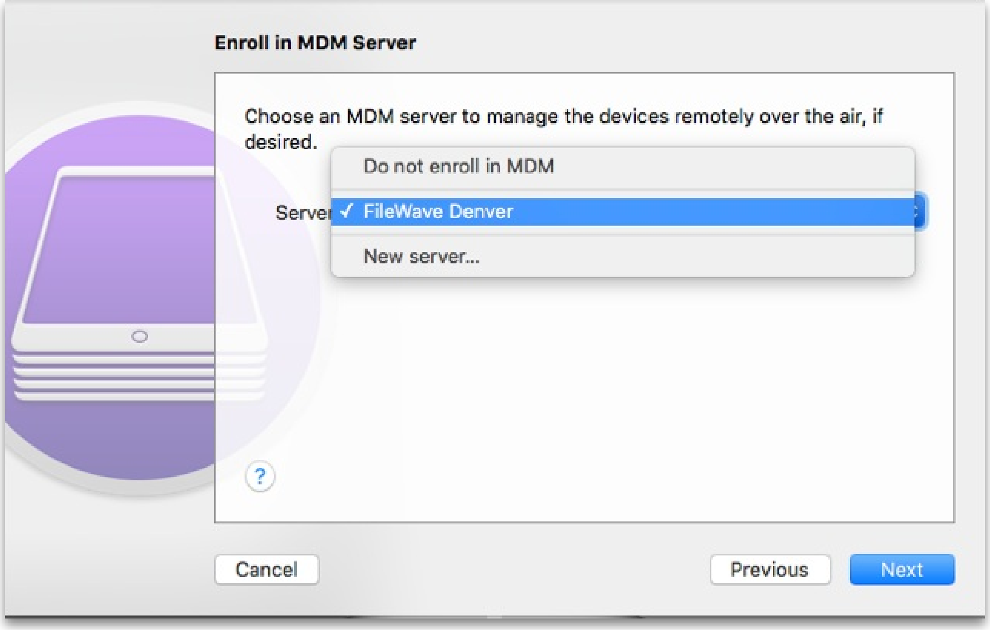


Supervise Devices

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

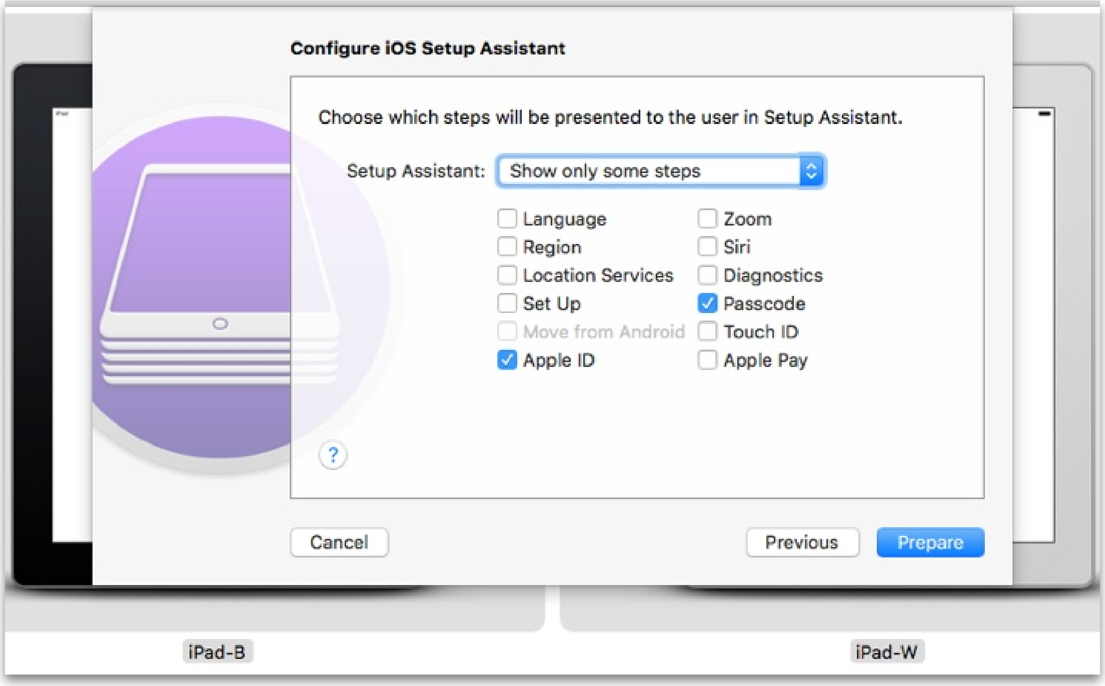
☑ Allow devices to pair with other computers



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.

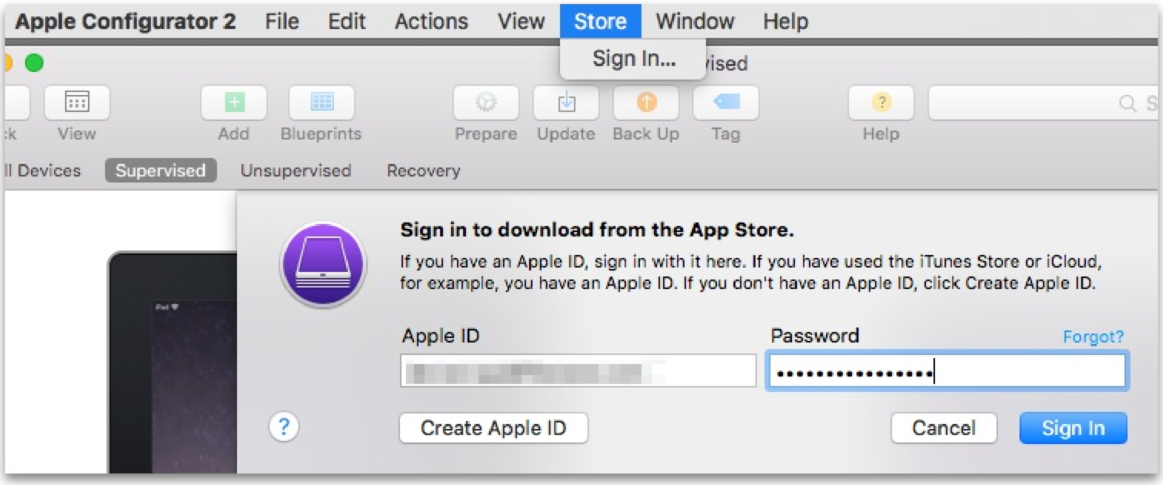
Setup Assistant: Show only some steps

- □ Language
- □ Region
- □ Location Services
- □ Set Up
- □ Move from Android
- ☑ Apple ID
- □ Zoom
- □ Siri
- □ Diagnostics
- ☑ Passcode
- □ Touch ID
- □ Apple Pay

Cancel | Previous | Prepare

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 cannot 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: ••••••••••••••••

Forgot?

Create Apple ID | Cancel | Sign In

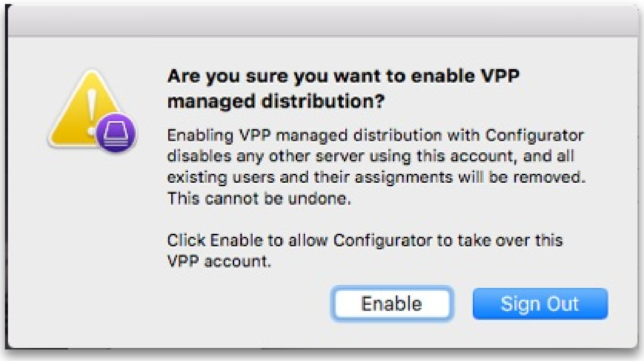
App Store account

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.

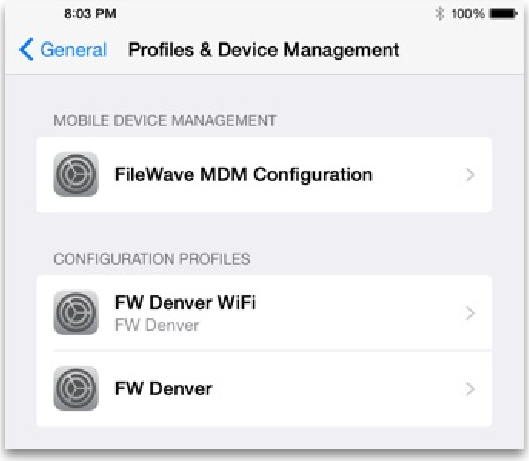


Are you sure you want to enable VPP managed distribution?

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.

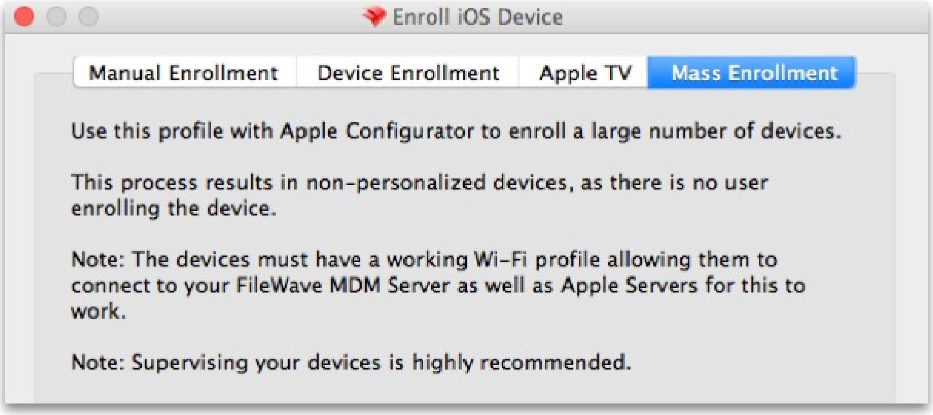
Once you have enrolled your mobile devices, and added them as clients in FileWave, you should see a set of installed profiles like the ones below.



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.

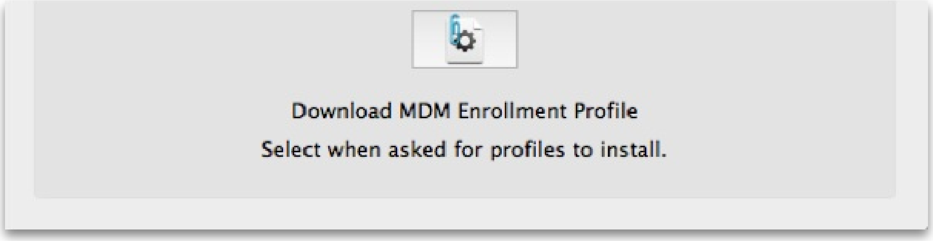


Use this profile with Apple Configurator to enroll a large number of devices.

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.



Download MDM Enrollment Profile

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.

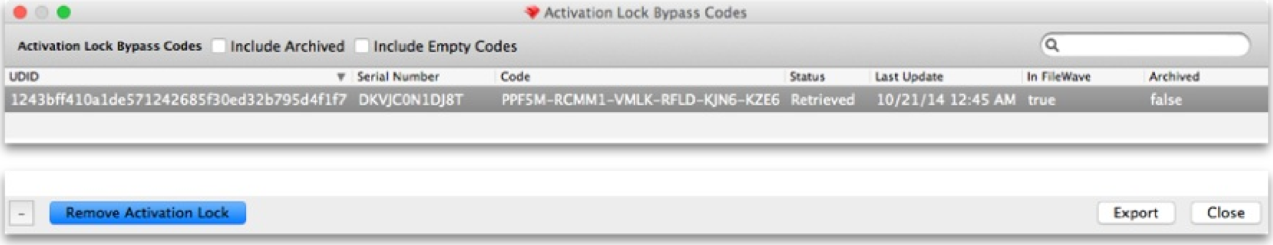
FileWave Enterprise App Portal for iOS

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.

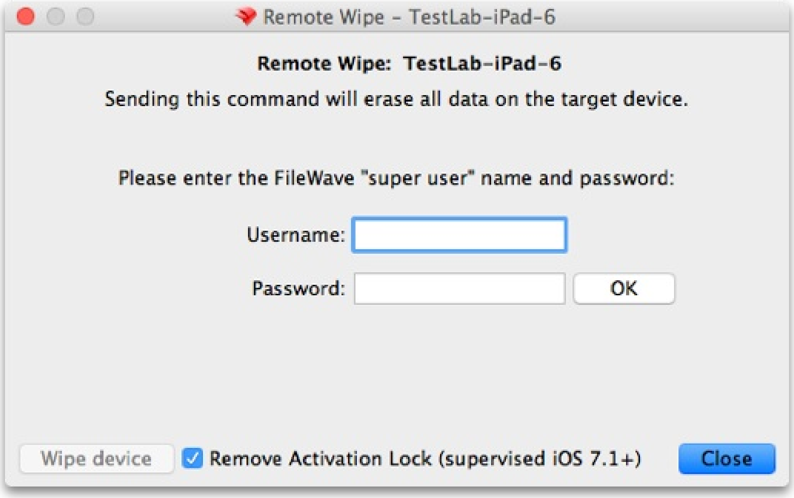


Activation Lock Bypass Codes

Activation Lock Bypass Codes □ Include Archived □ Include Empty Codes

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:

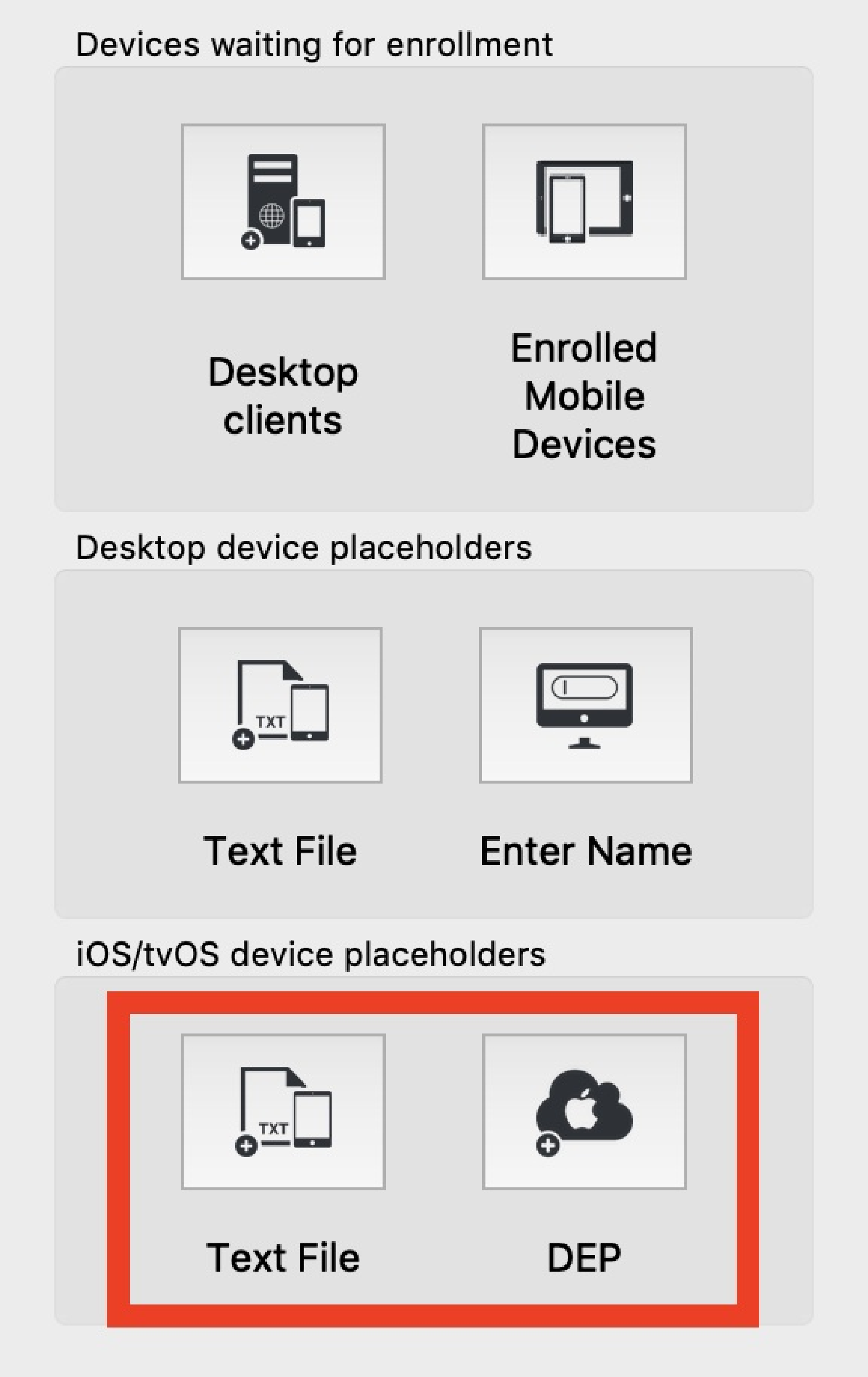
☑ Remove Activation Lock (supervised iOS 7.1+)

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).

You can also configure Activation lock in the DEP profile: Working with Apple’s Device Enrollment Program (DEP)

iOS/tvOS Device Placeholders

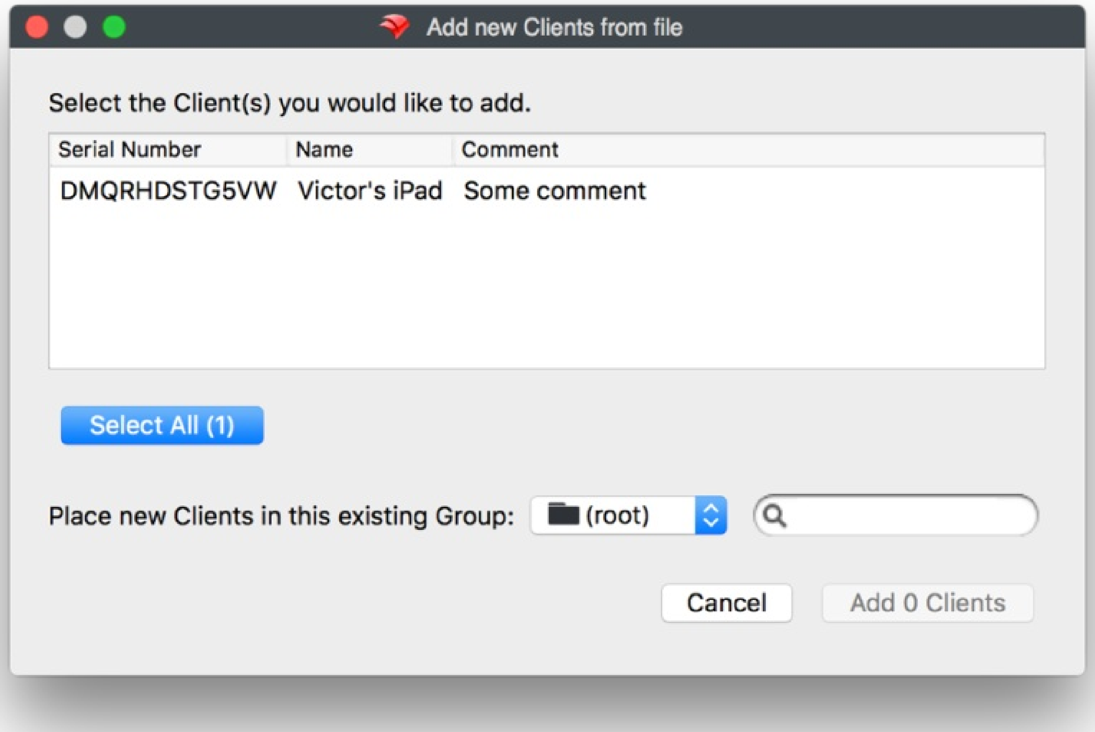

Devices waiting for enrollment
Desktop clients
Enrolled Mobile Devices
Desktop device placeholders
Text File
Enter Name
iOS/tvOS device placeholders
TXT
Text File
DEP

Text File (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

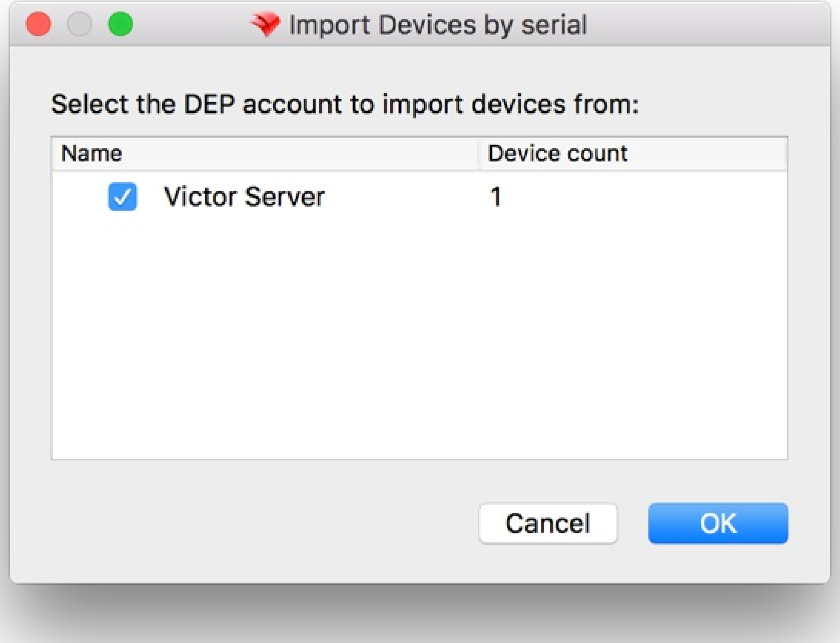
Place new Clients in this existing Group: (root)

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's 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.



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.

See Placeholders for what can be done with the imported devices

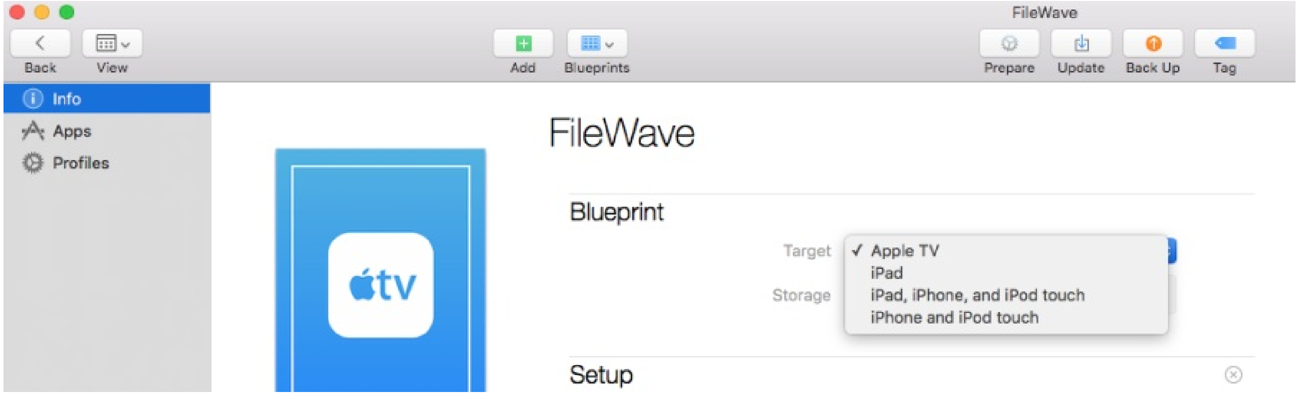
Related Content

- Conflict Resolution
- Enrolling Computer Clients

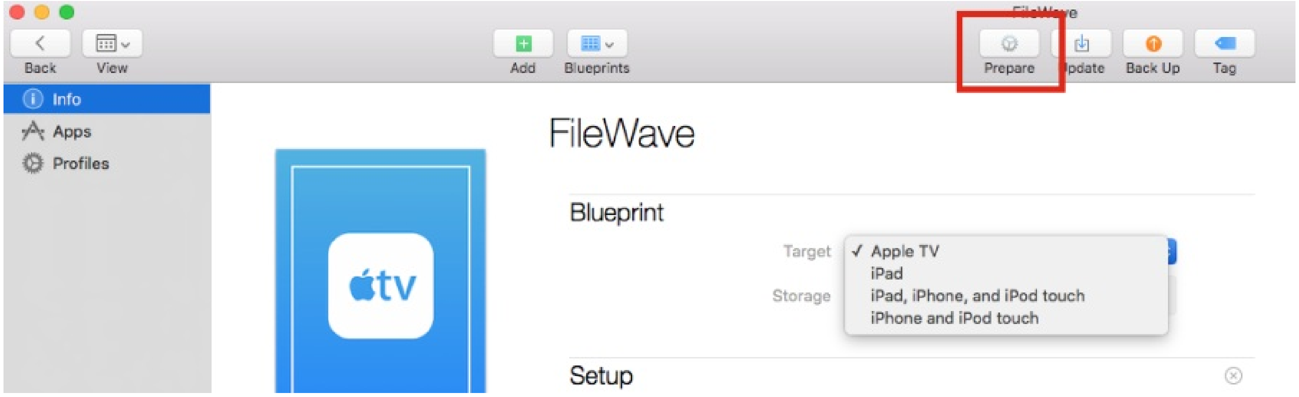
Enrolling AppleTV into FileWave

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.

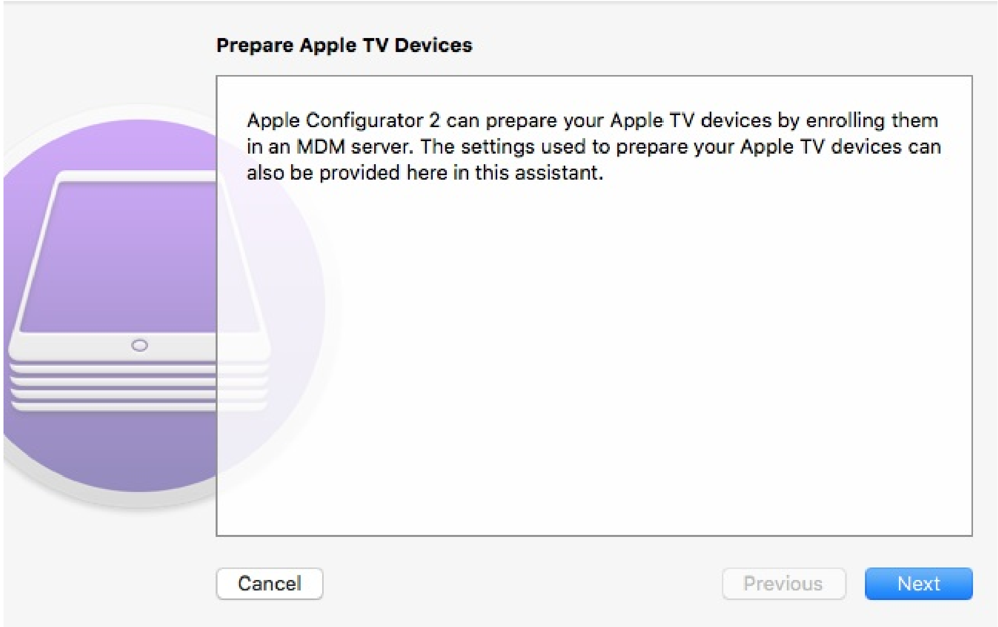
> Note that newer versions may change a dialog but the process should remain close to this.



Click on the Prepare icon



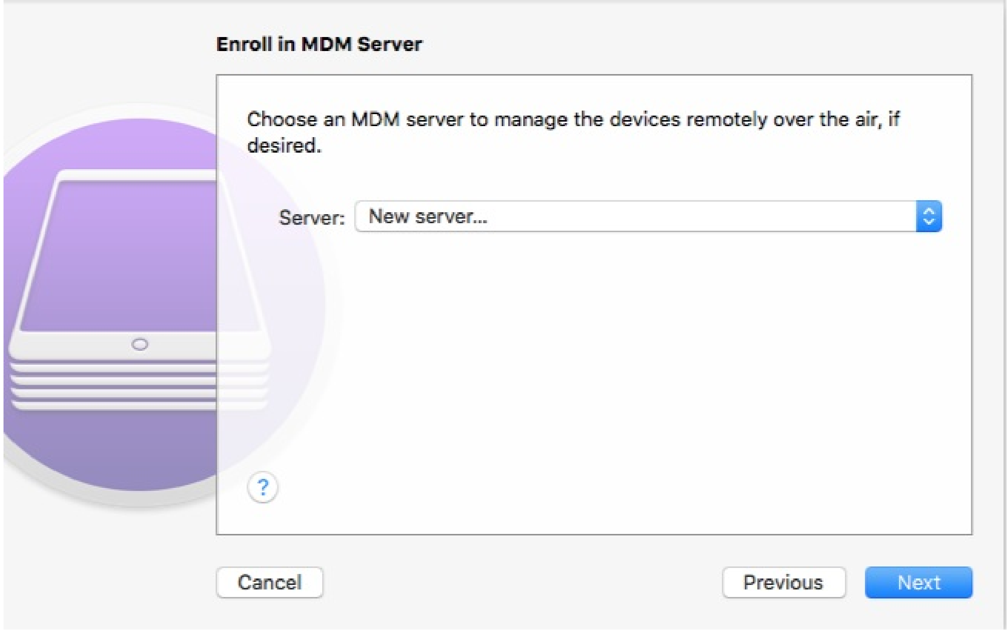
This opens the dialog box



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

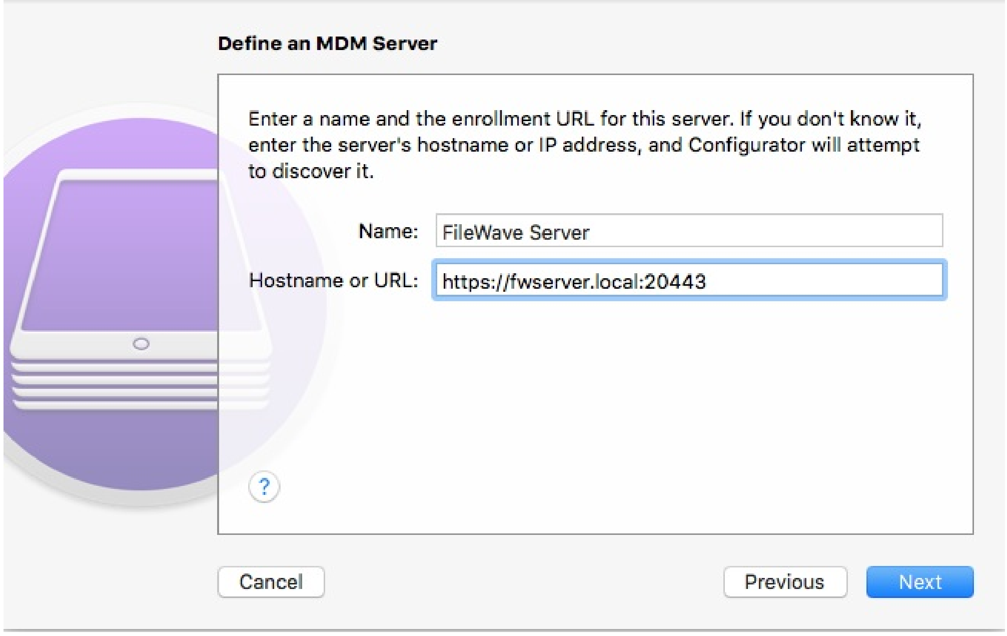


Enroll in MDM Server

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.



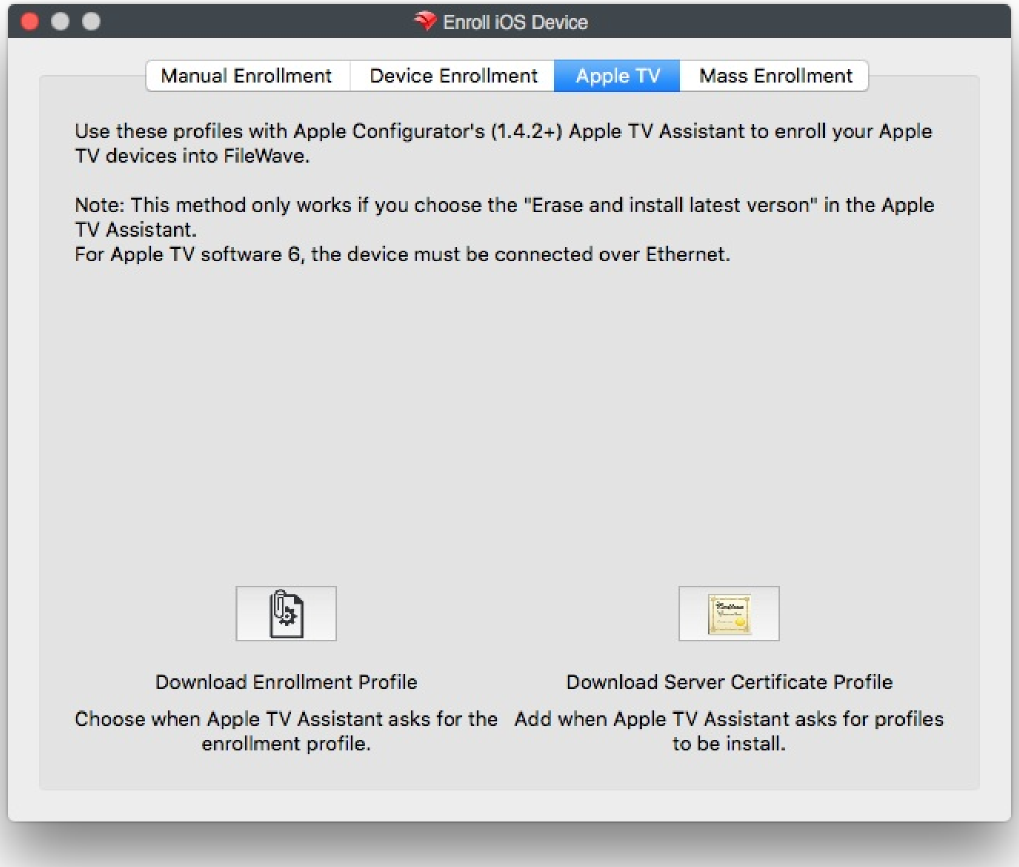
Define an MDM Server

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.



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.

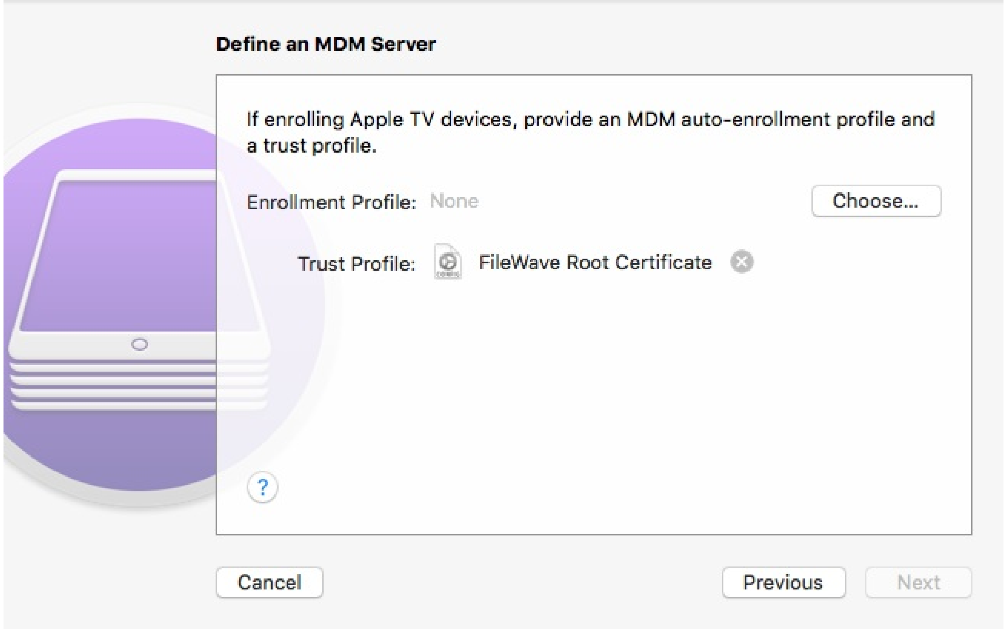
Download Enrollment Profile

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.

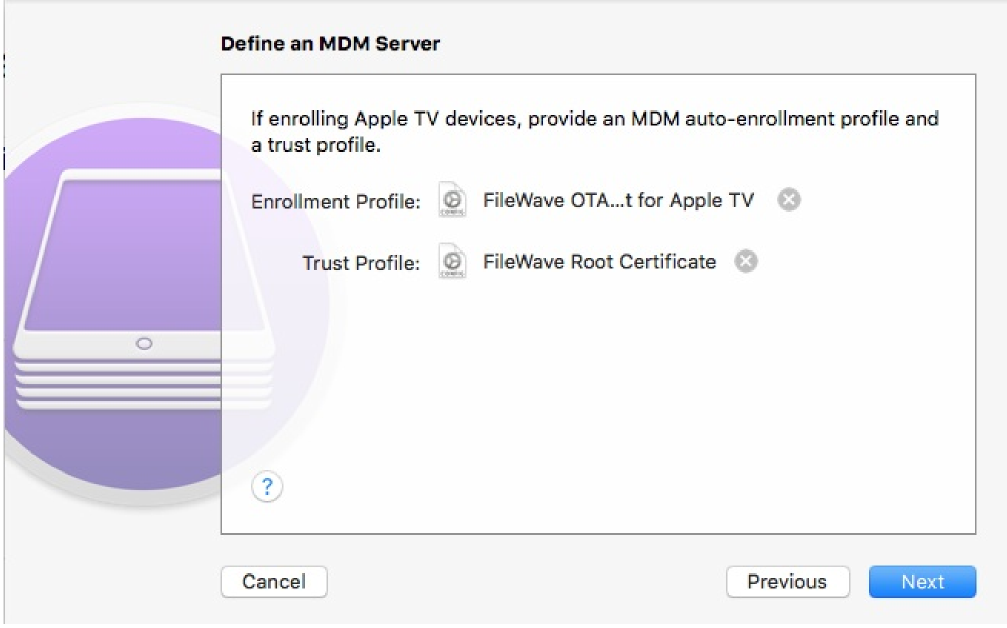


Define an MDM Server

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

Enrollment Profile: None

Trust Profile: FileWave Root Certificate



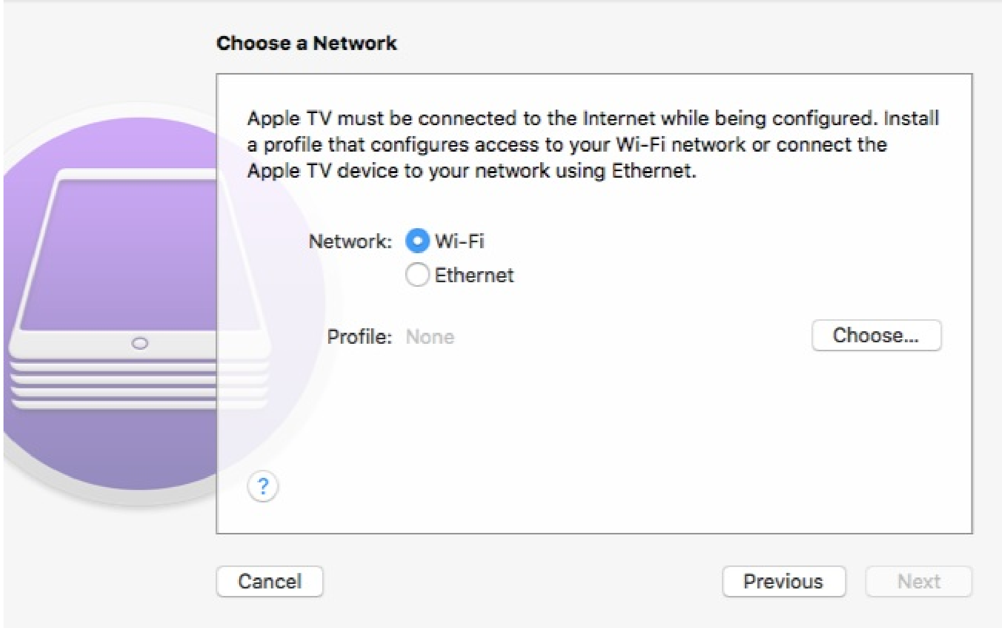
Define an MDM Server

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.



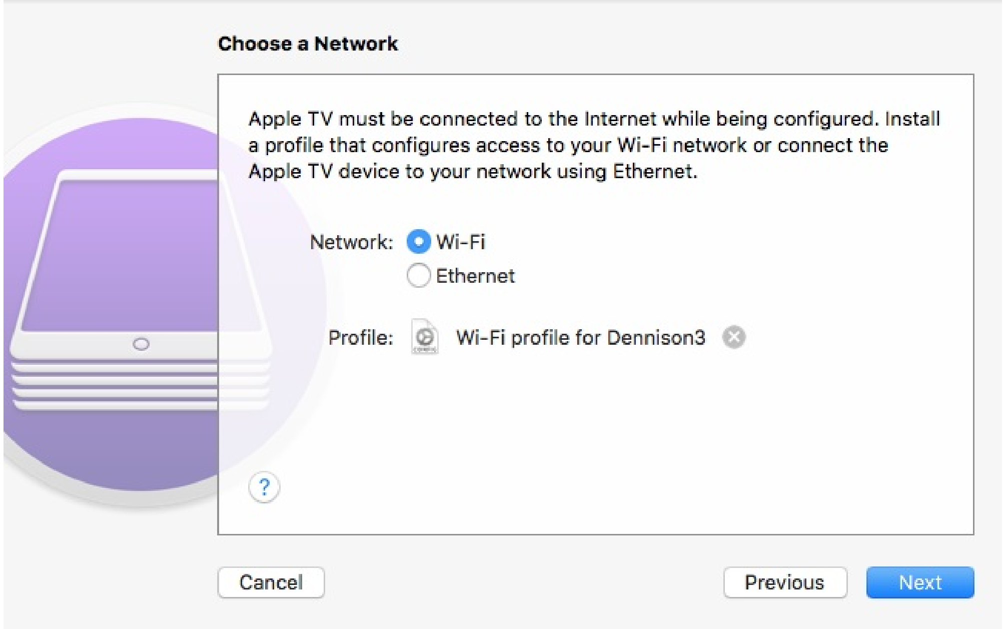
Choose a Network

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.



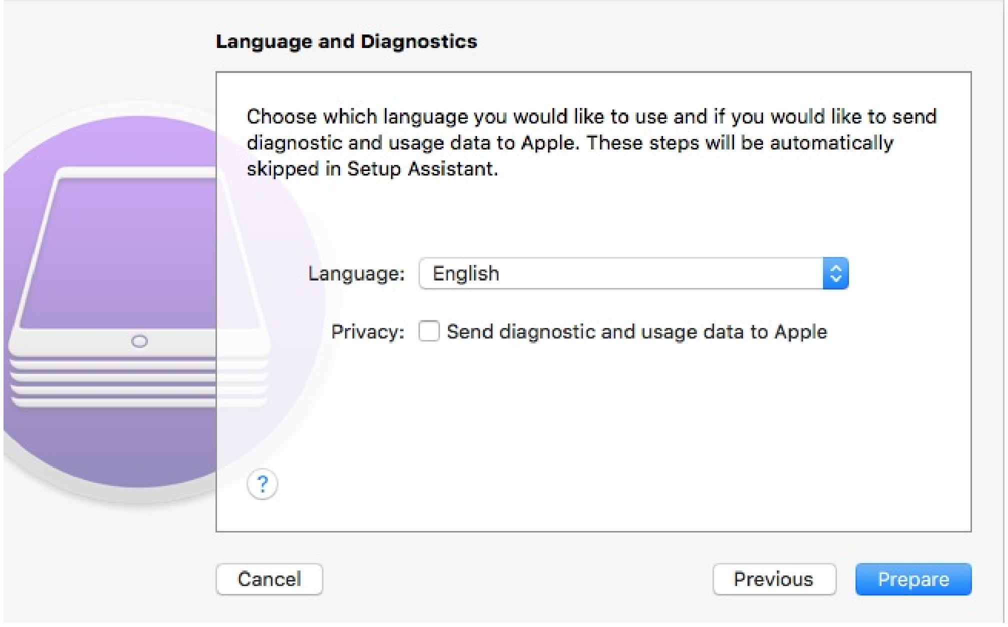
Choose a Network

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.



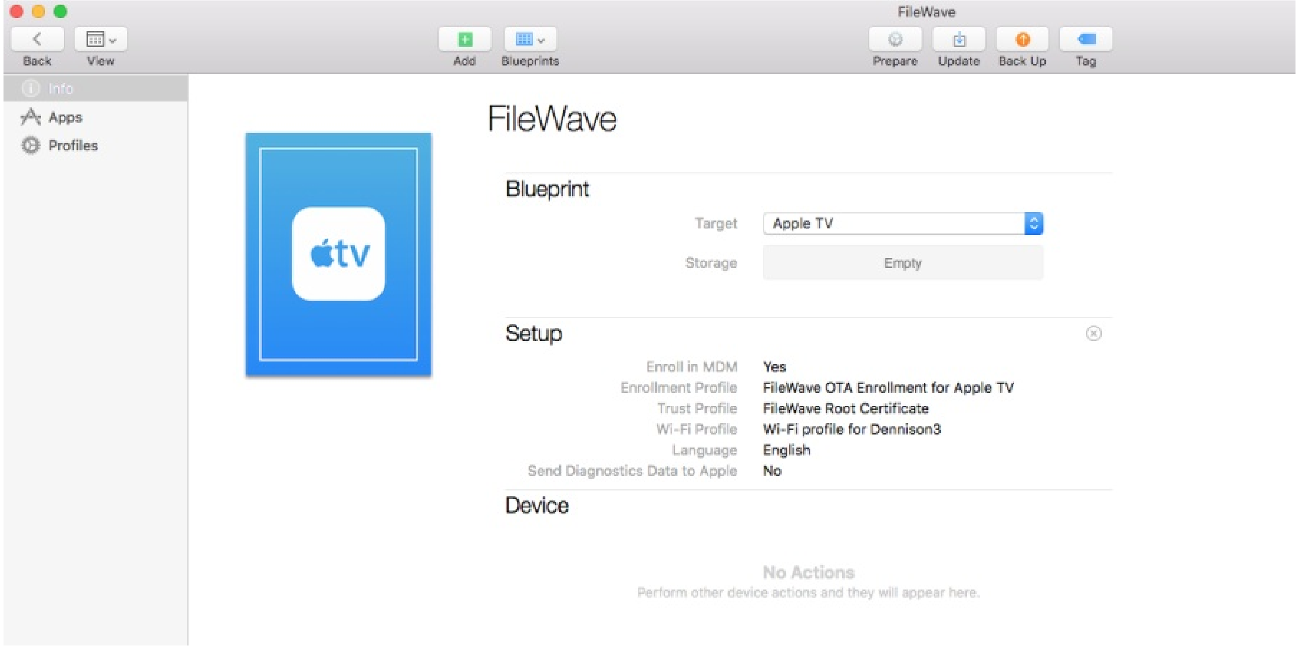
Language and Diagnostics

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.

Related Content

- Enrolling Devices
- Conflict Resolution

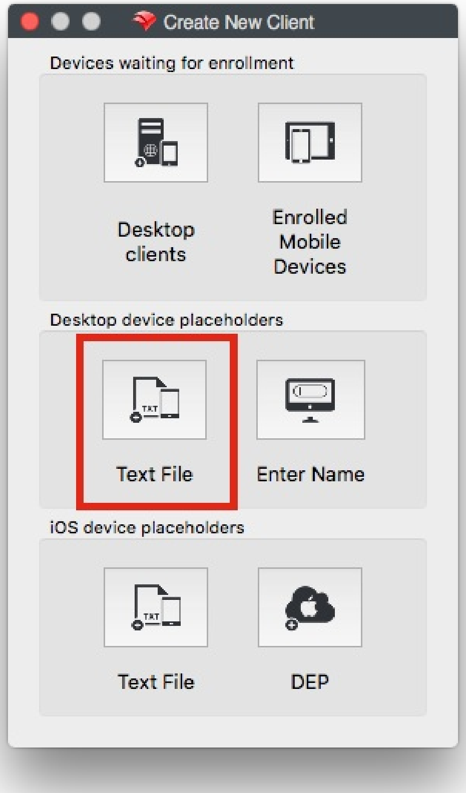
Importing Computer Clients from a File

You can import a "tab-delimited" text file (not a CSV file).

See Placeholders for more workflow information. Can be useful for

- Network Imaging Guide
- Device Enrollment Program (DEP)
- Enrolling Mobile Devices into FileWave
- Working with FileWave Clients

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.

FileWave Client Configuration Settings

FileWave Client Configuration Settings

Configuration Settings are found in the Windows registry or macOS plist:

- macOS: `/usr/local/etc/fwcld.plist`
- Windows: `HKLM\Software\FileWave\WinClient` (native), `HKLM\Software\FileWave\WOW6432\WinClient` (32bit install on 64bit OS)

Please refer to Creating a Superprefs Fileset to find out how to change these settings on any number of clients using a fileset.

The following list shows the default settings in the left row, describes the function and valid alternative settings (native)

Basic/Minimal Configuration

server = "no.server.set"	FileWave server IP or DNS
primaryPort = 20015	FileWave Server Port
fwPassword = ""	Encrypted FileWave Client Password - used for remote configuration through client monitor
fwUser = my.filewave.client.name	FileWave Client name (visible in FileWave Admin)

> Note: The default port setting above is 20015. However, SSL is now required, and the system will automatically use port 20017 instead when 20015 is entered. Do not manually set the port to 20017. Always enter 20015, and the system will handle the SSL port change for you.

Booster configuration

booster1 = "no.booster.set"	Booster 1 IP or DNS Address
booster1Port = 20013	Booster 1 Port
booster2 = "no.booster.set"	Booster 2 IP or DNS Address
booster2Port = 0	Booster 2 Port
booster3 = "no.booster.set"	Booster 3 IP or DNS Address
booster3Port = 0	Booster 3 Port
booster4 = "no.booster.set"	Booster 4 IP or DNS Address
booster4Port = 0	Booster 4 Port
booster5 = nobooster	Booster 5 IP or DNS Address
booster5Port = 0	Booster 5 Port
boosterRouting = 0	When set as 1, client connects to server through boosters, only for non HTTPS traffic (e.g. except for inventory / profile deployment)
connectorProbeAttemptDelay = 3	Number of Seconds the client waits between trying to reach boosters
connectorProbeAttempts = 10	Number of unsuccessful connections that lead to booster being marked "offline"

TeamViewer (was Observe Client)

vncManaged = 0	Controls whether remote connection is allowed: * Teamviewer – FileWave 14.7+ * FileWave Client (fwcld) prior to 14.8
vncPromptClient = 1	Controls whether end user is prompted to allow remote connection: * Teamviewer – FileWave 14.7+ * FileWave Client (fwcld) prior to 14.8

Ports the client listens on

monitorPort = 20010	Client Monitor connects here, over the network
kioskPort = 20020	Kiosk / Reboot Dialog connects here, from localhost

Client behaviour

debugLevel = 10	Controls fwcld log verbosity; 10(normal),99(debug),101(trace)
fileCheckInterval = 86400	Number of seconds between verification cycles (default once every 24 hours after launch)
freeSpaceMargin = 2147483648	Minimum Number of free bytes left on disk so filesets can be deployed
setUsersFilesOwner = 1	Set ownership of Users files/folders to appropriate user
syncComputerName = 0	If set to 1, fwcld will query OS to retrieve computer name at startup, and use that as fwUser value
tickleInterval = 120	Number of seconds between attempts to contact FileWave Server for new Commands

Location Related

locationRefreshInterval = 0	If set to >0, number of seconds between querying the OS for location data
deviceState = 3	Client State, e.g.: Missing, Tracked, Untracked
denyPersonalDataCollection = 0	If set to 1, disables Location Services

Obsolete / Unused keys

testMode	
desktopOwner	
currentFileWaveClientName	
niceTime	
priority	
useSSL	
srvPublishPort = 20005	ZeroMQ messaging port (Deprecated from FileWave 14.8+. Removed from FileWave server 15.0 and notifications from earlier clients (pre 14.8) will no longer work at this point)
vncRelayPort = 20030	Port used to connect towards the filewave server to forward VNC Data (Deprecated from FileWave 14.8+)
vncServerPort = 20031	Local Port VNC Data is relayed to/from (set to 5900 to use builtin VNC service) (Deprecated from FileWave 14.8+)
booster1PublishPort = 20003	Booster 1 ZeroMQ prior to 14.8
booster2PublishPort = 0	Booster 2 ZeroMQ prior to 14.8
booster3PublishPort = 0	Booster 3 ZeroMQ prior to 14.8
booster4PublishPort = 0	Booster 4 ZeroMQ prior to 14.8
booster5PublishPort = 0	Booster 5 ZeroMQ prior to 14.8

Filewave Firewall Scripts for Windows

Summary

FileWave Installers by default leave Windows Firewall settings untouched. This article provides scripts that opens the Windows Firewall so the Windows processes can accept connections from the outside.

Procedure

Use the attached .bat files to open the firewall for the respective executable at their standard install locations.
If you've installed a Filewave component to a nonstandard path, please adapt the path inside the .bat files.

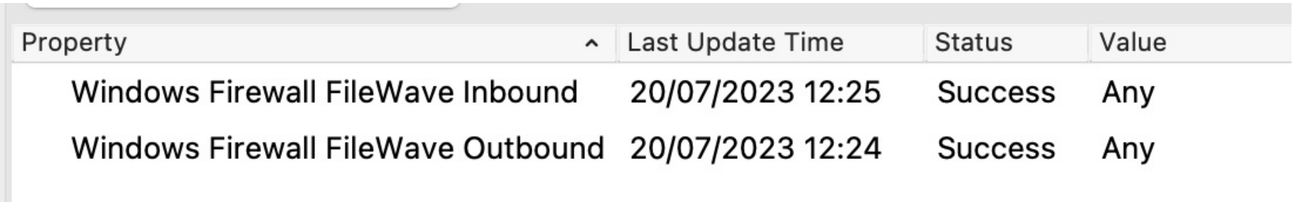
The Scripts allow both in- and outbound connections on all ports for the installed FileWave executables and follow the basic syntax :

Windows 10 and beyond:

```
netsh advfirewall firewall add rule name="FileWave Client" \
action=allow program="C:\Program Files\ (x86)\FileWave\fwcld.exe" \
enable=yes dir=in description="Filewave Client Inbound Access, usually only port 20010 is needed for client monitor connections"
```

Custom Fields

The following download contains two Custom Fields to report the firewall status of the FileWave Client, for example:



Property	Last Update Time	Status	Value
Windows Firewall FileWave Inbound	20/07/2023 12:25	Success	Any
Windows Firewall FileWave Outbound	20/07/2023 12:24	Success	Any

Creating a Superprefs Fileset

Description

A Superprefs Fileset will allow you to configure your FileWave Clients in mass. You need to create the Fileset and deploy it to your clients. In this recipe, we will take the Boosters configuration as an example. (More details...)

> Superprefs work the same way on both macOS and Windows.

Ingredients

- FileWave Superprefs Editor

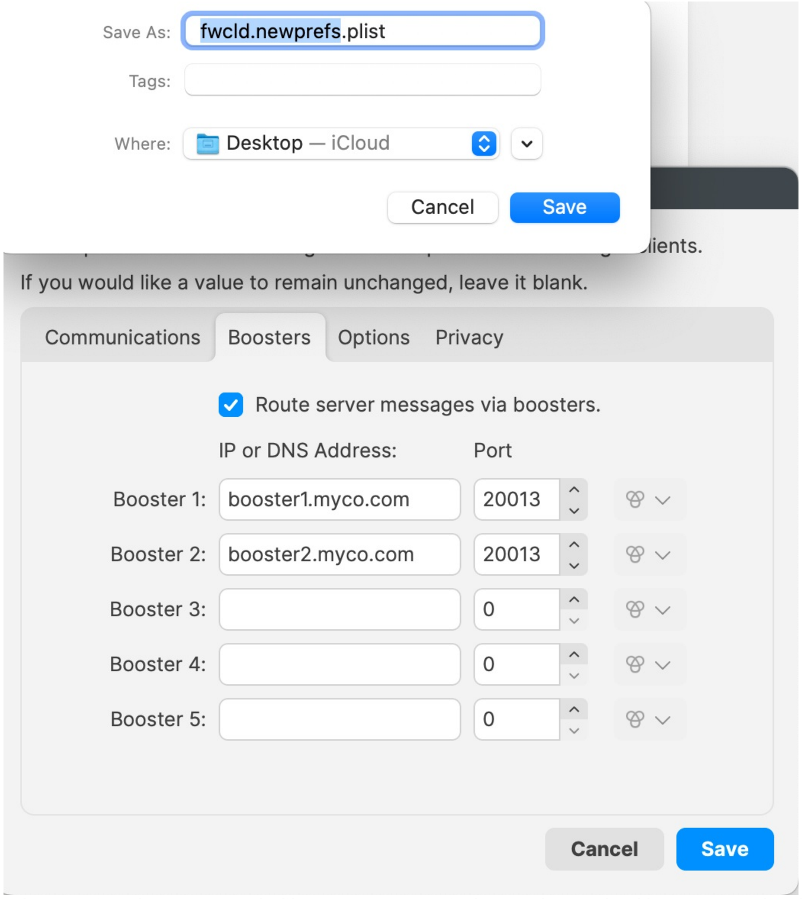
Directions

1. The process requires two main steps:
   - Create the SuperPrefs plist file using Superprefs Editor.
   - Create a Fileset and put the plist inside.

   Step 1:
   1. Open Superprefs Editor located in: /Applications/FileWave or C:\Program Files (x86)\FileWave\
   2. You will get prompted to select a file, click "Cancel"

      > The reason it prompts to open a file is so you can edit existing superprefs plist files.
      > Hitting cancel means you are making a new one.

   3. You will get the Editor Dialog. You have to type in only the fields that you want to change on the clients.
   4. Go to "Boosters" tab and add your boosters and ports (20013 and 20003 is the default port).



Save As: fwcld.newprefs.plist

Tags:

Where: Desktop — iCloud

...lients.

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

☑ Route server messages via boosters.

	IP or DNS Address:	Port
Booster 1:	booster1.myco.com	20013
Booster 2:	booster2.myco.com	20013
Booster 3:		0
Booster 4:		0
Booster 5:		0

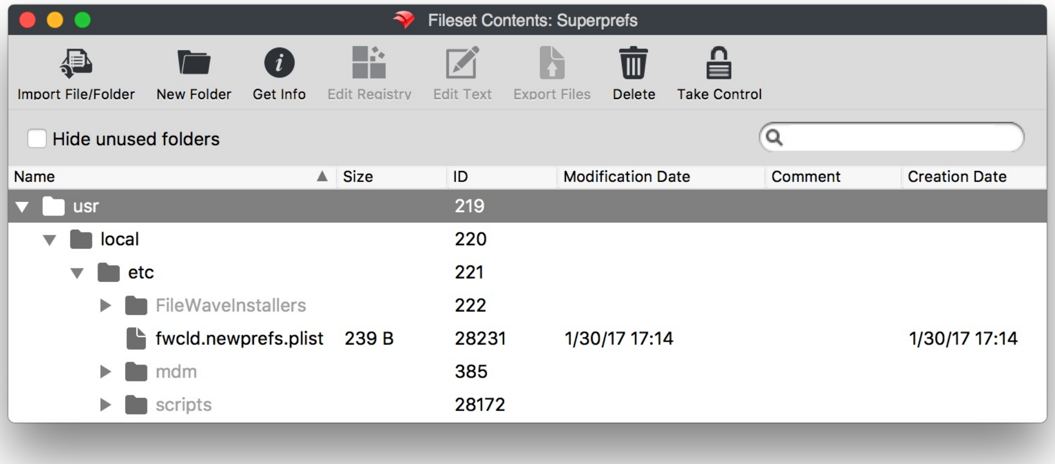
When saving the Superprefs file – macOS or Windows – leave the file name as the default "`fwcld.newprefs.plist`"
That file name is required for the settings to take effect
Step 2:
1. From Filesets view in FileWave Admin, click "New Desktop Fileset".
2. Click "Empty" and give your Fileset a name then click "Ok" to create it.
3. Double click on your Fileset to bring the contents up.
4. Uncheck "Hide Unused Folders" and browse to /usr/local/etc (see screenshot)
   Note: This plist you created can be placed anywhere and will still deploy properly. Good locations could be:
   Windows

   ```
   C:\ProgramData\FileWave\
   ```

macOS

```
/usr/local/etc/FileWaveInstallers/
```

5. Drag and drop your plist file in "etc".
6. Close the Fileset and test deploy.
7. From the Admin, go to the Client Monitor where you deployed the Fileset on and open its Preferences. Make sure the Boosters are set correctly.
8. Make sure you test your Fileset on a single computer first before deploy it out in mass.



☐ Hide unused folders

Name	Size	ID	Modification Date	Comment	Creation Date
usr		219			
local		220			
etc		221			
FileWaveInstallers		222			
fwcld.newprefs.plist	239 B	28231	1/30/17 17:14		1/30/17 17:14
mdm		385			
scripts		28172			

Use the Client Monitor to verify settings have been applied properly

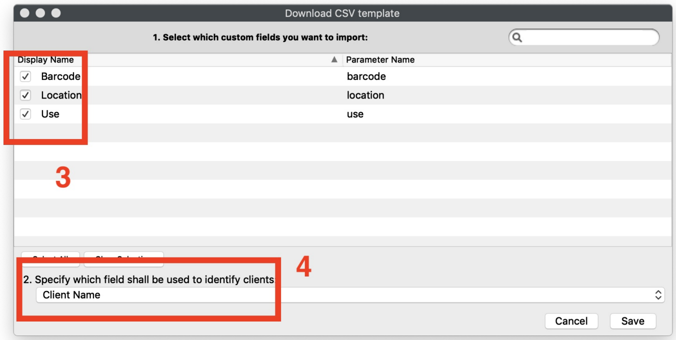
Digging Deeper

The following settings on a macOS or Windows FileWave client can be set by a Superpref;

- FileWave Server Address
- Server TCP Port
- Client Monitor Port
- Kiosk Port
- Tickle Interval
- Synchronize Client Name with Computer Name
- Define Booster configuration and Booster Routing
- Debug Level
- File Check Interval
- Free Space Margin
- Client Preferences Password / Client Monitor Password - Used to remotely configure FileWave Client options.
- Client process priority
- Disable Personal Data Collection
- Geolocation refresh interval
- Enable TeamViewer connections
- Prompt user when a TeamViewer connection is made

Placeholders

Placeholders



Download CSV template

1. Select which custom fields you want to import:

Display Name	Parameter Name
☑ Barcode	barcode
☑ Location	location
☑ Use	use

2. Specify which field shall be used to identify clients:

Client Name

Placeholders for computers and mobile devices are useful in many situations where you need to create a device FileWave has not seen yet, and pre-assign them varying content:

- Import new Windows computers and assign them what image you want to put on them (see: Windows Network Imaging - PXE)
- Import new devices (mac, Windows, iOS etc) and assign them custom names
- Import iOS or macOS devices and assign them custom fields so DEP can name with with variables (see: DEP Naming)
- Import devices (any OS) and assign them custom fields so that smart groups can deploy pre-assigned software immediately upon enrollment

This Article will focus on a situation where you need to import devices and give them custom field values before they are enrolled. This is great for fields like:

- Barcode / Asset tag
- Location
- Use
- Warranty information like expiration date

Preparing the Files

We typically start out with one large file; A CSV/excel that looks something like this:

Serial or MAC address	Name	Barcode	Location	Use
AS5D64AS65D4	Lab-A-comp1	321654987	North Campus	Student
Q32WE1WQ3E21	Lab-A-comp2	321654988	North Campus	Student
X9C87ZX9C87ZC	Front-Desk-1	321654989	Main Office	Admin
DF9H51DF95H1	BreakRoom-A	321654990	Break Room	Faculty

We will actually need to import this file two times

1. To create the placeholders
2. To Assign the custom fields to the placeholders

Creating the Placeholders

Use the "New Client" UI to import a tab delineated version of just serial number and name column

More detailed instructions:
Windows / macOS : Importing Computer Clients from a File
iOS / tvOS : Enrolling Mobile Devices into FileWave

Create the Custom Fields and import

You can can either import the custom fields file or follow the create step

Import Custom Fields

1. Download the custom field file: FileWave Custom Fields.customfields
2. Open your (Assistance → Custom Fields →) "Edit Custom Fields" UI
3. Press "import" Browse for file

> ✓ For more see: Importing and Exporting Custom Field Files

Create Custom Fields

Create any needed custom fields and assign them to all devices, or specific devices.

1. Open the custom field UI
2. Create Custom fields for Use, Location, barcode;
   1. Use: Provided: Admin, Type: string, Restricted: True, Values: None (DEFAULT), Faculty, Student, Administration
   2. Location: Provided: Admin, Type: string, Restricted: True, Values: None (Default), Site A, Site B
   3. Barcode: Provided: Admin, Type: string, Restricted: False, Use Default Values: True (Default: None)
   4. Take note of the "Internal Name" from the custom fields (I.E: barcode, location, use)

More detailed instructions:
Custom Fields

Import Custom Field Values

Once the fields are created and assigned to the proper devices we need to import your file again in the custom fields UI. This time with the serial, barcode, location, use column.

You can actually have FileWave to create a sample CSV file with the proper headings by going to

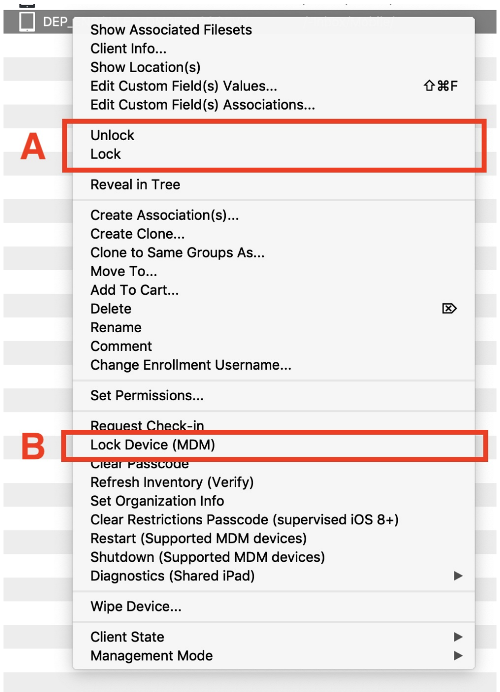
1. (Assistance → Custom Fields →) "Import Custom Fields" UI
2. Press "Download Template"
3. Select the values you want to import (barcode, location and use in our case)
4. Specify the field to identify clients (for example Serial Number or Client Name)
5. Save

Edit in a spreadsheet app (excel, numbers, etc) and add the needed vales and bring it back in

> ℹ Note that you can also set custom field values for placeholders manually by right-clicking if you have only a few to update

Locking Devices

What is it?



What are device locks? What is the difference between "Lock" and "Lock Devices"

> ℹ The locking behavior is the same for macOS, Windows, iOS, and non-EMM Android.

Answer

Lock / Unlock

Lock - Locking a client binds that client to the current model number. Meaning that if something unexpected should happen during a migration or update, a connecting client ignores any new manifests from the server (see: Upgrading your On-Premise FileWave Server).

Unlock - Allows a device to be updated to the latest model.

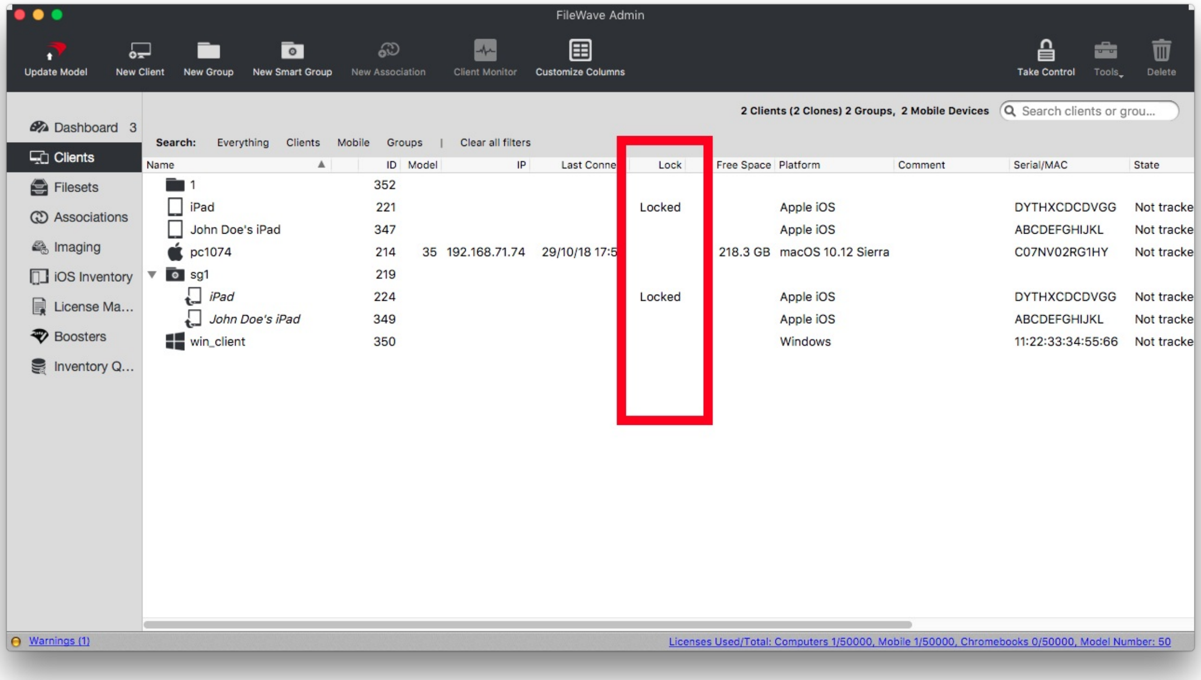
Lock Device

Lock the actual screen of the device. The user will be unable to use the device till a passcode (if present) is entered.

ADDITIONAL INFORMATION

When you lock a device the kiosk will not be available to the user. It will open, but display a message to the user they they are blocked.

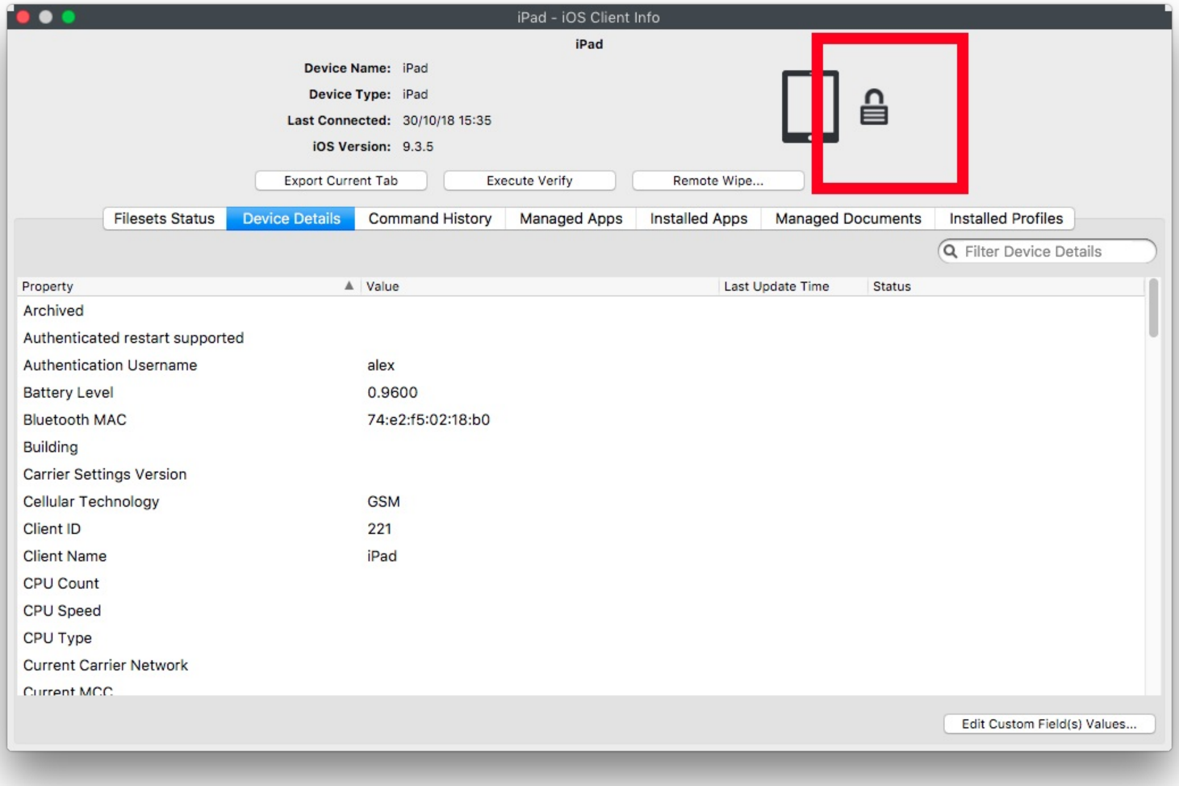
Locked device shows a lock icon or text in the client view, device info, and client monitor:



2 Clients (2 Clones) 2 Groups, 2 Mobile Devices

Name	ID	Model	IP	Last Conne	Lock	Free Space	Platform	Comment	Serial/MAC	State
1	352									
iPad	221				Locked		Apple iOS		DYTHXCDCDVGG	Not tracke
John Doe's iPad	347						Apple iOS		ABCDEFGHIJKL	Not tracke
pc1074	214	35	192.168.71.74	29/10/18 17:5		218.3 GB	macOS 10.12 Sierra		C07NV02RG1HY	Not tracke
sg1	219									
iPad	224				Locked		Apple iOS		DYTHXCDCDVGG	Not tracke
John Doe's iPad	349						Apple iOS		ABCDEFGHIJKL	Not tracke
win_client	350						Windows		11:22:33:34:55:66	Not tracke

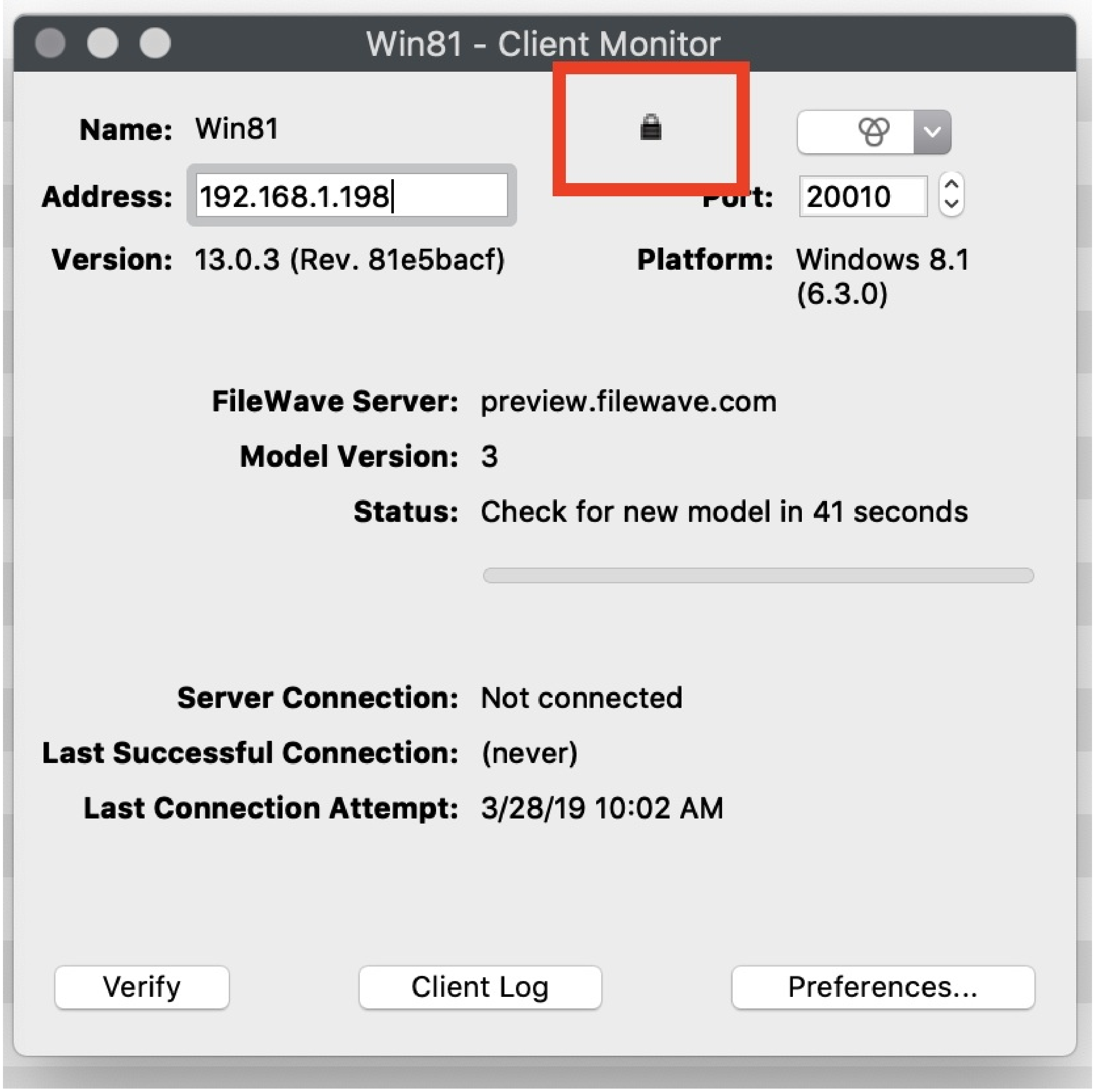
Licenses Used/Total: Computers 1/50000, Mobile 1/50000, Chromebooks 0/50000, Model Number: 50



iPad

Device Name: iPad
Device Type: iPad
Last Connected: 30/10/18 15:35
iOS Version: 9.3.5

Property	Value	Last Update Time	Status
Archived			
Authenticated restart supported			
Authentication Username	alex		
Battery Level	0.9600		
Bluetooth MAC	74:e2:f5:02:18:b0		
Building			
Carrier Settings Version			
Cellular Technology	GSM		
Client ID	221		
Client Name	iPad		
CPU Count			
CPU Speed			
CPU Type			
Current Carrier Network			
Current MCC			



Name: Win81

Address: 192.168.1.198

Port: 20010

Version: 13.0.3 (Rev. 81e5bacf)

Platform: Windows 8.1 (6.3.0)

FileWave Server: preview.filewave.com

Model Version: 3

Status: Check for new model in 41 seconds

Server Connection: Not connected

Last Successful Connection: (never)

Last Connection Attempt: 3/28/19 10:02 AM

Location Tracking

Location Tracking Technologies

FileWave Location Tracking

The location reporting feature in FileWave is disabled by default. It is recommended that you; verify that this feature is per 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 access location information. For details on how this works, look here: Location Tracking

Technologies used for Location Tracking

Location tracking technologies used will differ from client platform to client platform.

Maps used:

- ThunderForest - https://www.thunderforest.com/

Client location detection methods:

- On macOS/Windows - https://doc.qt.io/qt-5/location-positioning-cpp.html which tries different sources.
- On Windows specifically - https://learn.microsoft.com/en-gb/windows/win32/api/locationapi/nf-locationapi-ilocation-getreportstatus
- On iOS - The iOS API for location from Apple.
- On ChromeOS - The Google API for location from Google.

Related Content

- Location Tracking

Location Tracking Setup

FileWave Location Tracking

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 permission for access location information.

Requirements:

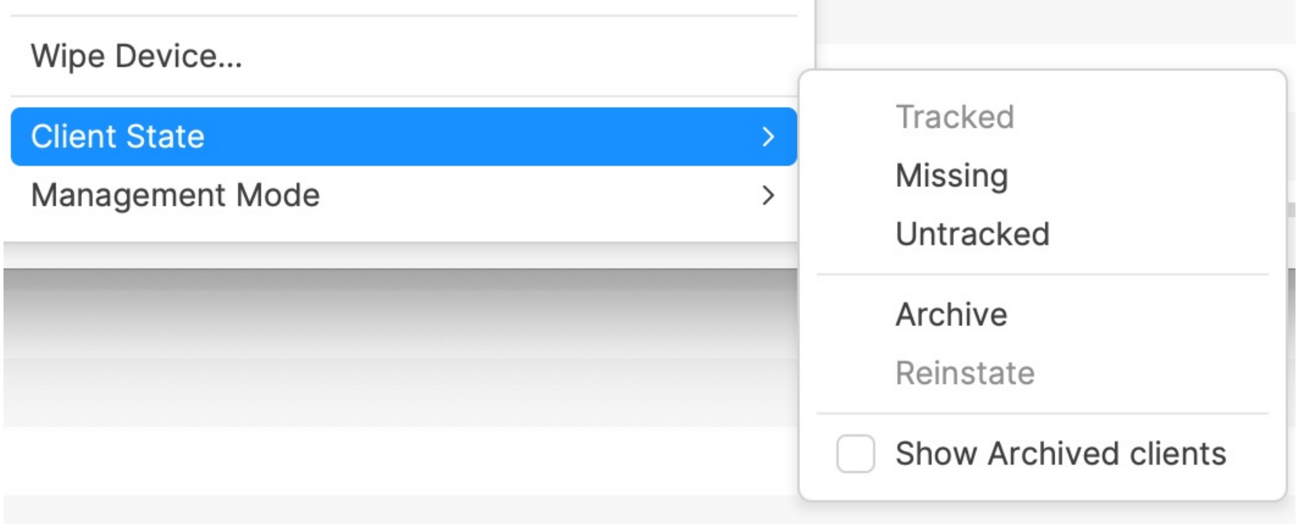
- FileWave version 10.1+
- Location Tracking Enabled - Server/Client
- iOS devices require the FileWave IPA App Portal for passive tracking
- All devices you want to track are already enrolled into FileWave and currently communicating properly

Supported Operating Systems:

- APK Android: 4.1+
- iOS 9+
- macOS 10.9+
- Windows 10+
- ChromeOS 43+

Things to consider:

Client State. For the items: Tracked, Missing and Untracked, the item greyed out is the active state:

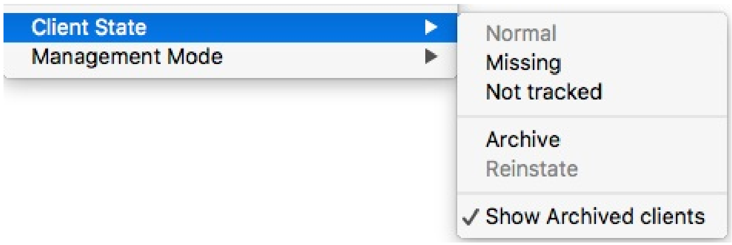


- Different States of Tracking
  - Tracked - Tracking is enabled and will update the location at different intervals
  - Missing - Tracking is enabled and will be updated around every two minutes. The client also sends the location immediately and does not wait for other scans to finish. For supervised 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 (DEFAULT)- No location is gathered at any time.
- 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 needs to be open, whether that be in the background or the currently active app.

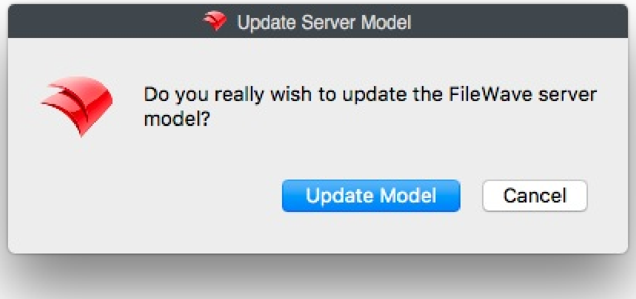
There are two types of location tracking in FileWave, Passive Tracking, and Lost Mode. macOS, Windows, Chromebooks, and Android devices use Passive tracking to gather the location of the device without locking it down. Supervised iOS devices set to Missing mode will put the device in Lost mode, which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

Lost Mode Setup (iOS macOS):

1. Right Click on your Supervised iOS or MDM-enrolled macOS device(s)
2. Select Missing from the Client State menu

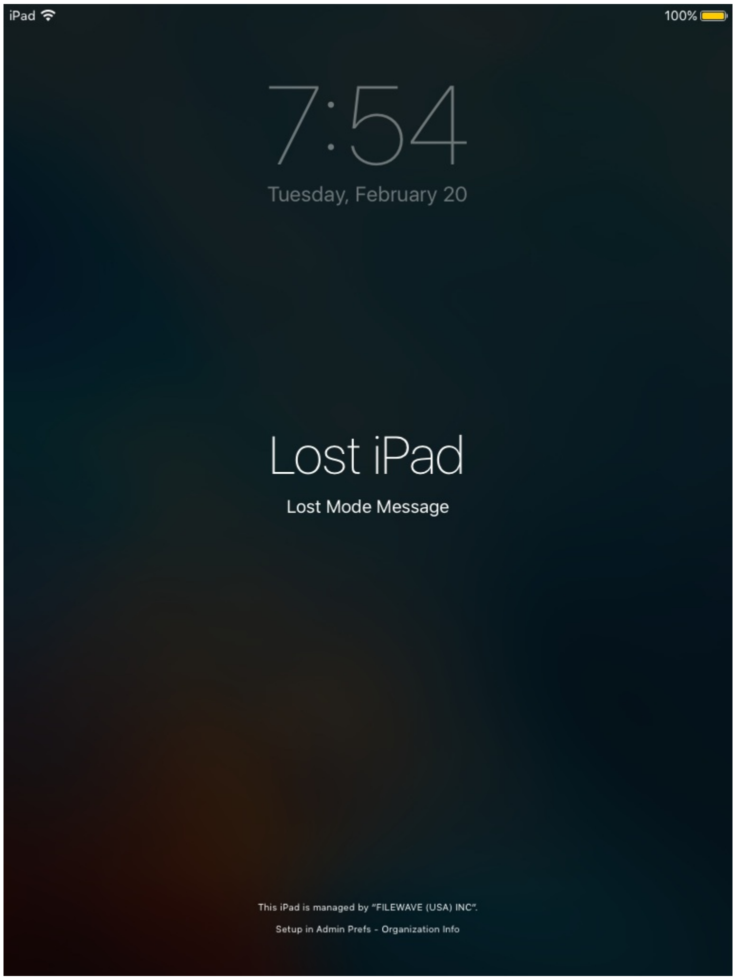


3. Update Model


Update Server Model

Do you really wish to update the FileWave server model?

4. Once the device checks in it will be in lost mode and report location.



Lost iPad

Lost Mode Message

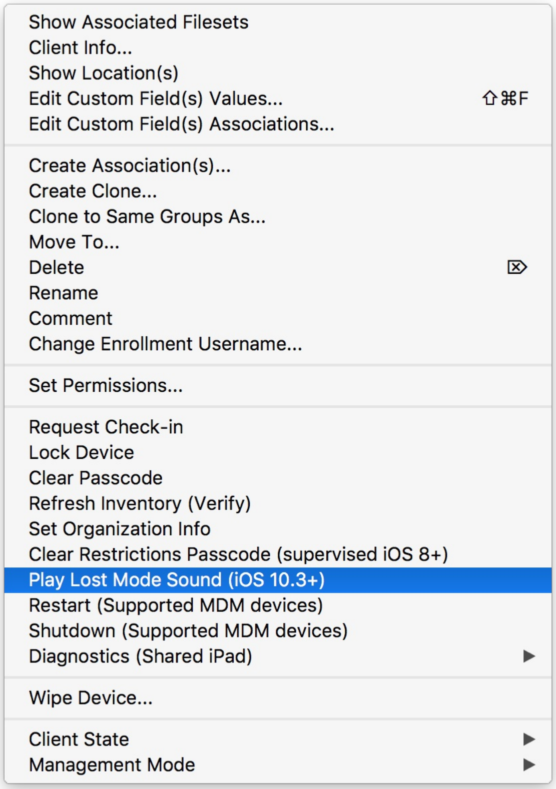
This iPad is managed by "FILEWAVE (USA) INC".

Setup in Admin Prefs - Organization Info

5. To take it out of lost mode, select "Not Tracked" in the Client State menu

> ✓ When the iOS device is in Lost Mode, do not reboot it. If the device losses Wifi, you will no longer be able to take the device out of Lost Mode since it will no longer be connecting to FileWave.

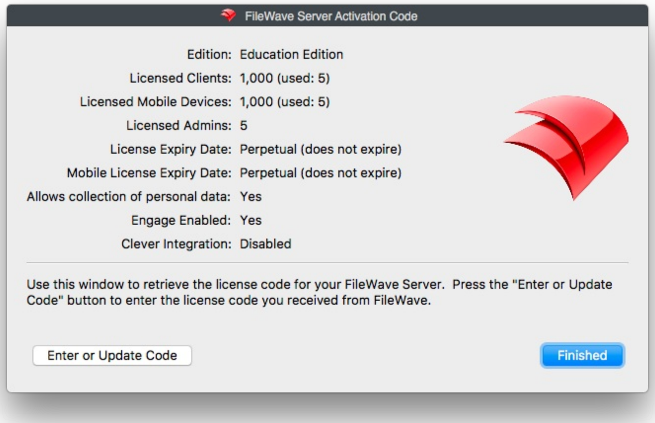
When the device is in Lost Mode, a new option in the tools menu is available, "Play Lost Mode Sound (iOS 10.3+)"


Show Associated Filesets
Client Info...
Show Location(s)
Edit Custom Field(s) Values... ⇧⌘F
Edit Custom Field(s) Associations...
Create Association(s)...
Create Clone...
Clone to Same Groups As...
Move To...
Delete ⌦
Rename
Comment
Change Enrollment Username...
Set Permissions...
Request Check-in
Lock Device
Clear Passcode
Refresh Inventory (Verify)
Set Organization Info
Clear Restrictions Passcode (supervised iOS 8+)
Play Lost Mode Sound (iOS 10.3+)
Restart (Supported MDM devices)
Shutdown (Supported MDM devices)
Diagnostics (Shared iPad) ▶
Wipe Device...
Client State ▶
Management Mode ▶

Passive Tracking Setup

This is receiving tracking data continuously.

1. Check your server license to be sure you have "Allows collection of personal data:" set to Yes.

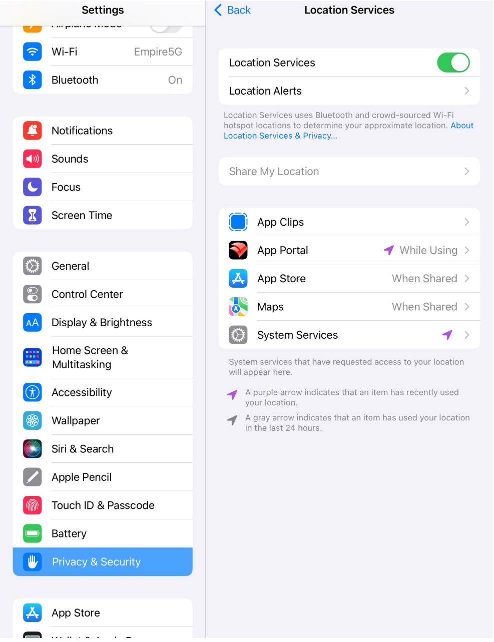


Edition: Education Edition
Licensed Clients: 1,000 (used: 5)
Licensed Mobile Devices: 1,000 (used: 5)
Licensed Admins: 5
License Expiry Date: Perpetual (does not expire)
Mobile License Expiry Date: Perpetual (does not expire)
Allows collection of personal data: Yes
Engage Enabled: Yes
Clever Integration: 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.

2. Make sure location services is enabled.

iOS	macOS



Settings

Airplane Mode

Wi-Fi Empire5G

Bluetooth On

Notifications

Sounds

Focus

Screen Time

General

Control Center

Display & Brightness

Home Screen & Multitasking

Accessibility

Wallpaper

Siri & Search

Apple Pencil

Touch ID & Passcode

Battery

Privacy & Security

App Store

Back

Location Services

Location Services

Location Alerts

Location Services uses Bluetooth and crowd-sourced Wi-Fi hotspot locations to determine your approximate location. About Location Services & Privacy...

Share My Location

App Clips

App Portal While Using

App Store When Shared

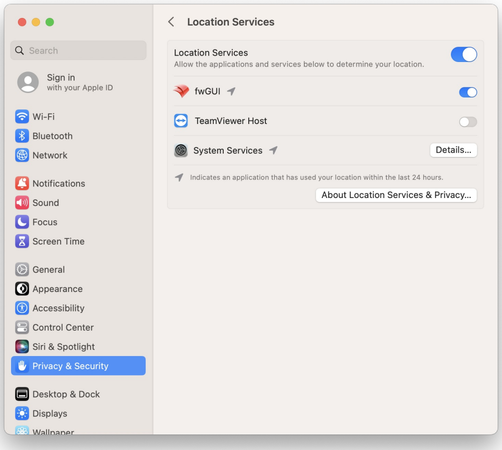
Maps When Shared

System Services

System services that have requested access to your location will appear here.

A purple arrow indicates that an item has recently used your location.

A gray arrow indicates that an item has used your location in the last 24 hours.



Search

Sign in
with your Apple ID

Wi-Fi

Bluetooth

Network

Notifications

Sound

Focus

Screen Time

General

Appearance

Accessibility

Control Center

Siri & Spotlight

Privacy & Security

Desktop & Dock

Displays

Wallpaper

Location Services

Location Services
Allow the applications and services below to determine your location.

fwGUI

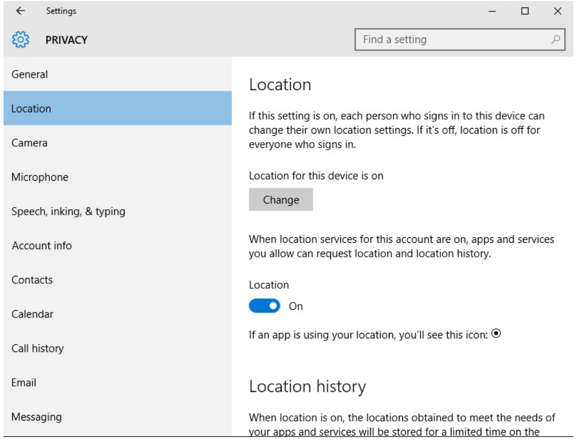
TeamViewer Host

System Services Details...

Indicates an application that has used your location within the last 24 hours.

About Location Services & Privacy...

Windows



Settings

PRIVACY

Find a setting

General

Location

Camera

Microphone

Speech, inking, & typing

Account info

Contacts

Calendar

Call history

Email

Messaging

Location

If this setting is on, each person who signs in to this device can change their own location settings. If it's off, location is off for everyone who signs in.

Location for this device is on

Change

When location services for this account are on, apps and services you allow can request location and location history.

Location

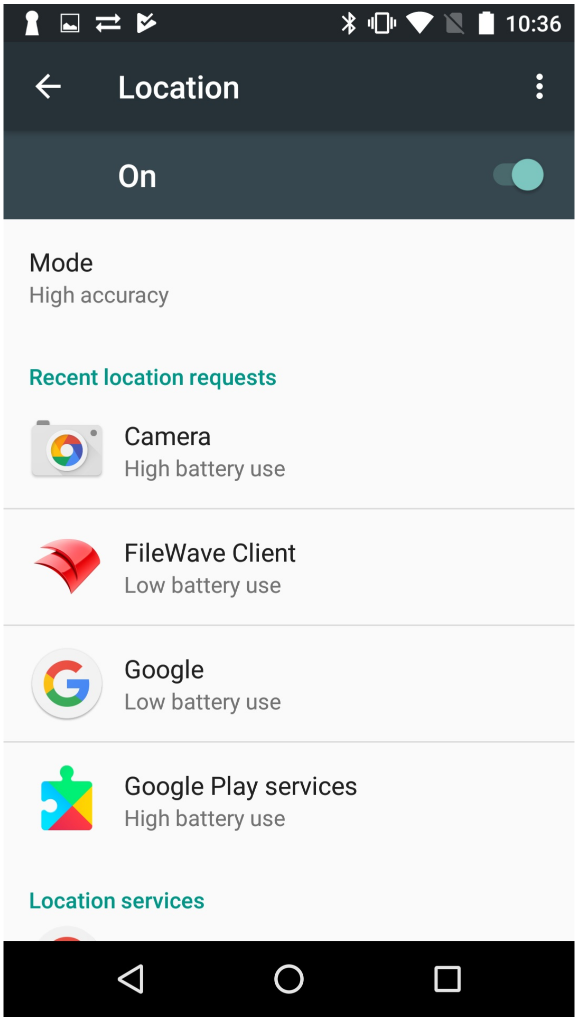
On

If an app is using your location, you'll see this icon: ⦿

Location history

When location is on, the locations obtained to meet the needs of your apps and services will be stored for a limited time on the

Android



10:36

Location

On

Mode
High accuracy

Recent location requests

Camera
High battery use

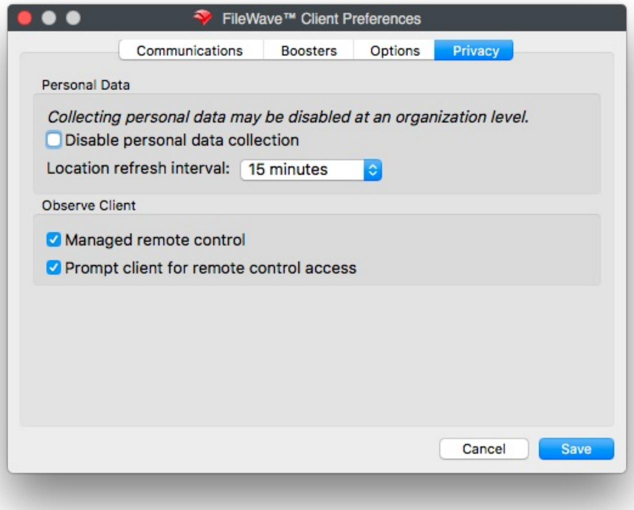
FileWave Client
Low battery use

Google
Low battery use

Google Play services
High battery use

Location services

3. Prepare the clients
    1. MacOS and Windows - Be sure that "Disable Personal Data Collection" option in the client preferences of your clients is not checked.



FileWave™ Client Preferences

Communications | Boosters | Options | Privacy

Personal Data

Collecting personal data may be disabled at an organization level.

☐ Disable personal data collection

Location refresh interval: 15 minutes

Observe Client

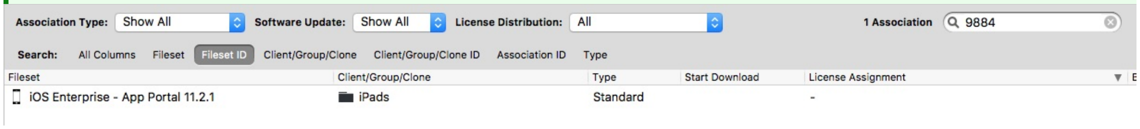
☑ Managed remote control

☑ Prompt client for remote control access

> You can set the "Disable personal data collection" one at a time with Client Monitor or Create a Superprefs (Creating a Superprefs Fileset) to change them in bulk.

2. iOS - Make sure the FileWave IPA App Portal has been sent out to all your iOS devices. Recommend to deploy latest version of IPA to ensure latest security certificates embedded. (Note: IPA does not need to match your server version.)

   > iOS devices: Can be downloaded from the FileWave Server download page near the bottom

   Association Type: Show All | Software Update: Show All | License Distribution: All | 1 Association | 9884

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

Fileset	Client/Group/Clone	Type	Start Download	License Assignment
iOS Enterprise - App Portal 11.2.1	iPads	Standard		-

   > FileWave 15.3+ will auto instal the latest App for you on qualifying devices. If the App is already open, when configuring the device for tracking, it may be necessary to close and re-open the App after the device has receive the subsequent MDM commands from the Model Update.

3. Chromebook - Be sure the Chrome Extension is installed and configured (See Quick Start Guide for Chromebooks)
4. Android (EMM)
   1. Force enable location tracking server side

      > By force enabling EMM tracking you are ignoring "Allows collection of personal data" in your license. Even is the license is set to false, this will collect data.

      1. Edit

         ```
         /usr/local/filewave/django/filewave/settings_custom.py
         ```

      2. add

         ```
         settings.EMM['FWCLIENT_FORCE_ALL_DEVICES_TRACKING_ENABLED'] = True
         ```

      3. Restart apache

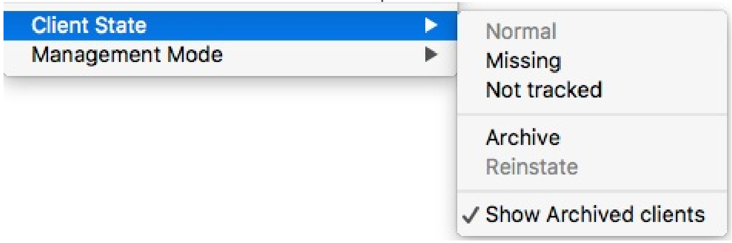
         ```
         /usr/local/filewave/apache/bin/apachectl restart
         ```

      4. Update Model
   2. Force enable location services on devices (See: Force Location for EMM Android Devices)

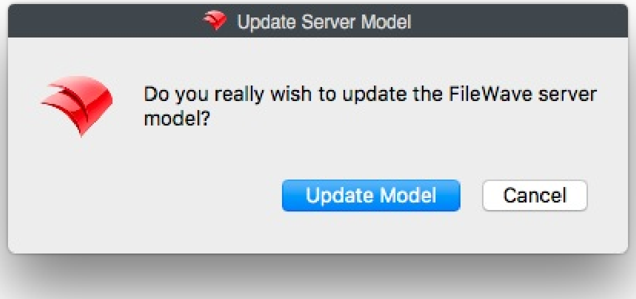
4. Change the state to Normal
   1. Right click on your macOS, Windows, Chromebook, and Android device(s)

      > For multiple devices use the filter options at the top of the client view, then select all

   2. Select Normal from the "Client State" option.

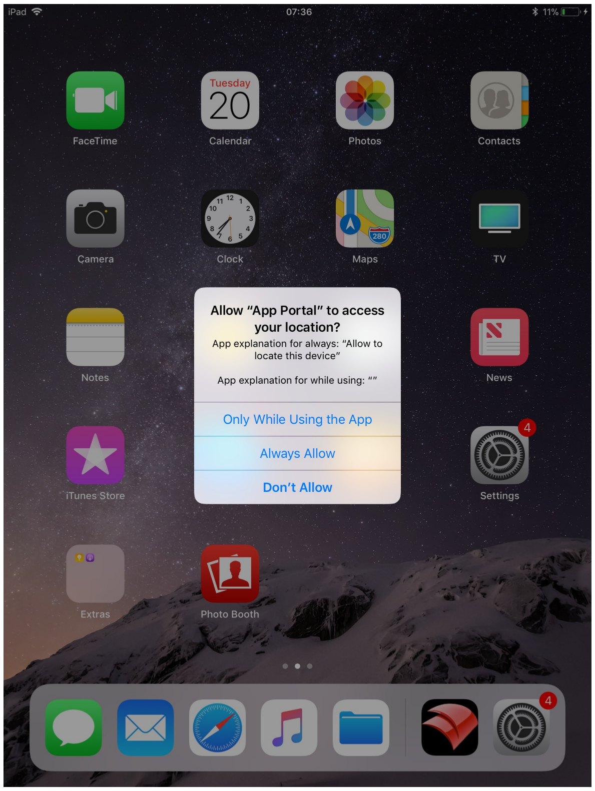
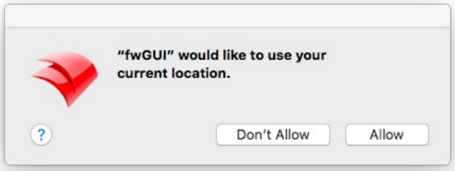
5. Update the model



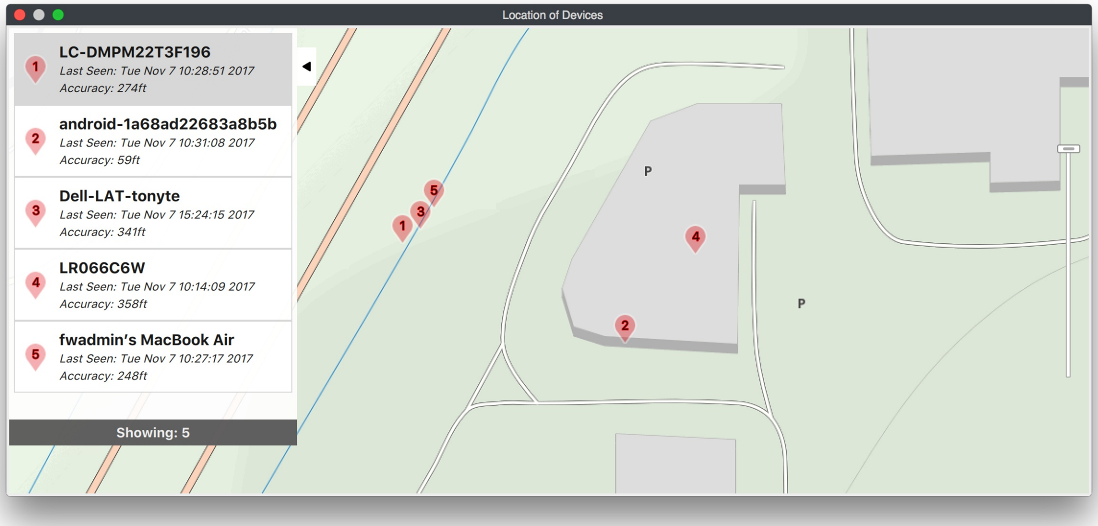
Update Server Model

Do you really wish to update the FileWave server model?

6. Accept any device prompts

iOS	macOS
 Allow “App Portal” to access your location? App explanation for always: “Allow to locate this device” App explanation for while using: “” 	 “fwGUI” would like to use your current location.

7. Wait a few minutes, can potentially take up to 15 minutes. Then simply right click on your device(s) and select the Show Location(s) option to see the map below. This will be accurate within a few hundred feet for most devices.



1 **LC-DMPM22T3F196**
Last Seen: Tue Nov 7 10:28:51 2017
Accuracy: 274ft

2 **android-1a68ad22683a8b5b**
Last Seen: Tue Nov 7 10:31:08 2017
Accuracy: 59ft

3 **Dell-LAT-tonyte**
Last Seen: Tue Nov 7 15:24:15 2017
Accuracy: 341ft

4 **LR066C6W**
Last Seen: Tue Nov 7 10:14:09 2017
Accuracy: 358ft

5 **fwadmin's MacBook Air**
Last Seen: Tue Nov 7 10:27:17 2017
Accuracy: 248ft

Showing: 5

> Warning: In order to avoid legal issues concerning user location tracking, it is highly recommended that you enable location tracking only on devices when a unique user may authorize the service.
> Privacy Policies: Apple/iOS and macOS – Microsoft/Windows – Google/Android

Additional OS Specific Considerations

macOS

Any user can agree to tracking, admin or not. Only an administrator can disable location services and/or FileWave's rights to location, as per Apple Inc. policy..

iOS

Any user can agree to tracking, can disable location services, and revoke FileWave's right to location, as per Apple Inc. policy.

Windows

The Windows operating system does not prompt the local user for access to location. Windows 10+ does have a location service that can be turned off.

Android (APK Client)

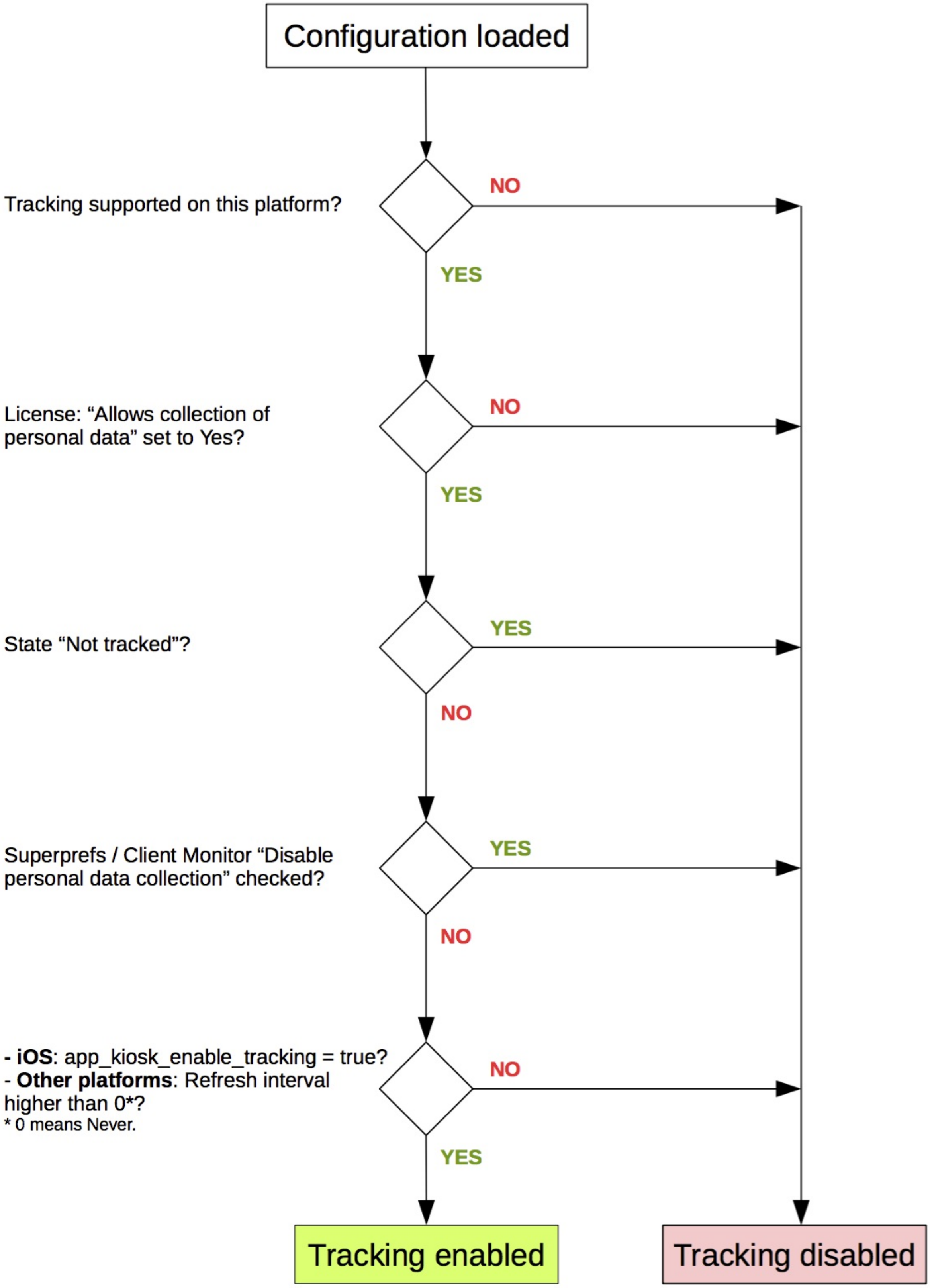
Upon installing or upgrading the Android FileWave Client to version 10.1 or greater, the user is requested to approve all rights an application needs. This includes location services, running in the background and several other rights.

Android (EMM Client)

A user can turn off their location tracking at anytime, but you can make a policy fileset that will Force Location for EMM Android Devices

Order of operation

It is important to note the way a client verifies it is able to ask the system for location information.
For example setting the state to "Missing" but it has a Superprefs file telling it the refresh interval is 0 See the flowchart for reference:


Configuration loaded
Tracking supported on this platform?
NO
YES
License: “Allows collection of personal data” set to Yes?
NO
YES
State “Not tracked”?
YES
NO
Superprefs / Client Monitor “Disable personal data collection” checked?
YES
NO
- **iOS**: app_kiosk_enable_tracking = true?
- **Other platforms**: Refresh interval higher than 0*?
* 0 means Never.
NO
YES
Tracking enabled
Tracking disabled

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 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.

How the FileWave Client Communicates

Enrollment

At this point you have either installed the FileWave client onto a computer, or the computer has gotten the client from DEP.

1. Client uses server field to make a connection to the server
2. Client downloads CA info from server
3. Client generates client ID
4. Client generates CSR (Certificate Signing Request), and saves key
5. Client sends client ID, name, CSR to server
   1. Client polls server (on tickle interval) until certificate is ready
   2. Server sends the client certificate
   3. Client verifies the certificate against the local key and the CA it downloaded
6. Client is added (and certificate is created)
   1. (Auto-add) Client is automatically approved and goes into the selected automatic add folder
   2. (upgraded client) Client is automatically approved, and continues normal operation
   3. (Vetting) Client sits in the new client UI (Client view → New client → Desktop Clients) till approved

If the client is older than 13.1 it will not connect if compatibility mode is disabled (see: What is Compatibility Mode?)

Daily Communication

FileWave server is updating manifests both when the model updates and when calculating smart group updates (see inventory preferences for time variable), so when a check-in happens the model may not have changed, but there may be new manifests for the client nonetheless.

macOS, Windows, Android APK

Tickle

1. Checkin (AKA Tickle) interval (Changeable with Superprefs, see: Creating a Superprefs Fileset) has passed
2. Client reaches out to server
3. Server verifies certificate
4. Server responds with model number
   1. If the model number on server matches client, then no model manifest is download
   2. If the model number does not match the server, client downloads manifest from server
5. Client processes manifest(s)
6. Client reaches out to either server or booster and downloads fileset(s)
   1. (if booster) Client reaches out to booster requesting fileset ID
   2. Client verifies the boosters certificate is valid against the same CA (Certificate Authority - AKA your FileWave server) that the client uses.
   3. Booster checks the client certificate against the CA it downloaded from the server and the CRL (Certificate Revocation List - Certs that have been made invalid)
   4. If the certificates (booster or client) are not valid, not signed by the CA or part of the CRL, the TLS handshake fails and the connection is dropped (with no data being transferred), the failure is reported to the server.

Verify

1. Additional check-in, by default every 24hrs. ('File Check Interval', changeable with Superprefs, see: Creating a Superprefs Fileset)
2. After Server/Client certificate confirmation, the client confirms status of all Filesets and Inventory and 'heals' any files as configured within Filesets.

> Verification also occurs when the client service commences (e.g. reboot) and can be triggered manually through Client Monitor/Info or command line on the device.

Android EMM

Review the topology on Default TCP and UDP Port Usage for a visual on how things connect.

At Model Update

1. A single manifest is created from all Android Policy Filesets (AKA Policy Fragments) associated to the device
2. Any App associated to the device (including app permissions) are added to the manifest
3. Manifest is sent to AMAPI (Android Management API)
4. EMM Android device reaches out to Google

Rest of the time

1. FileWave reaches out to Google every 5min to check for new devices and verify activity
2. If there are smart-groups update, a new manifest would be created and sent to AMAPI (see Android EMM Known Issues KB)

iOS

Review the topology on Default TCP and UDP Port Usage for a visual on how things connect.

At Model Update

1. At model update a push notification is send to the device asking it to verify
2. The iOS device connects with the FileWave server
3. The new changes in the manifest are sent

Rest of the time

1. Next inventory interval is hit
   Default is 24hrs. Configured in: Inventory preferences Meaning the last time we have talked to the device. So if you updated the model at 4pm on Friday, then 4pm Saturday would be the next interval
2. FileWave sends out a Push to Apple asking the device to talk to FileWave MDM server
3. The iOS device connects with the FileWave server
4. The new changes in the manifest are sent

Executing a Client-Side Script-Based Verification

What

The "verify" option of the fwGUI client application allows you to run a "verify" from the client programmatically.

When/Why

We are going to use this option whenever we want to get "immediate" feedback from a client. For instance, as a post-installation script, calling a verify would immediately make the client report updated inventory rather than waiting (up to 24 hours, default) for the next "regular" verify.

How

The verification is called as a command-line option to the fwGUI app on either a Windows or macOS client as follows:

	Windows Client	macOS Client
Path to fwGUI:	"C:\Program Files (x86)\FileWave"	/usr/local/sbin/FileWave.app/Contents/Resources/
App to call:	fwGUI.exe	fwGUI.app
Command Line options:	--verify Sends a verification (w/dialog by default...useful for troubleshooting)	--verify Sends a verification (w/dialog by default...useful for troubleshooting)
	--silent Used with --verify, sends verification without user dialog	--silent Used with --verify, sends verification without user dialog

Script examples:	Windows Batch Example
	`@echo off`
	`"C:\Program Files (x86)\FileWave\fwGUI.exe" --verify --silent`
	`exit 0`
		macOS Bash Example
		`#!/bin/bash`
		`/usr/local/sbin/FileWave.app/Contents/Resources/fwGUI.app/Contents/MacOS/fwGUI --verify --silent`
		`exit 0`

Related Content

- You can change the default 24h by adjusting the "File Check Interval" in a Superprefs - Creating a Superprefs Fileset

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."

Retiring a device from FileWave

In some cases, you may find yourself in a position where retiring a device is the wisest thing to do. Here are some steps to assist you in that process based on the operating system a device is running.

iOS

1. Log into ASM
2. Search for the device by serial number under Devices on the right-hand side of the screen
3. Click on the device to highlight it
4. Click Edit Device Management
5. Choose Unassign
6. Continue
7. OK
8. Go to FileWave Admin
9. Assistants
10. DEP Associations Mangement
11. Hold down Option
12. Click Full DEP Sync
13. Search for the device in
14. DEP Associations Mangement
15. Note that it should no longer appear here
16. Wipe the device
17. Search for the device in FileWave Admin > Clients
18. Single-click on the device
19. Click Delete at the top of the window
20. Update Model

macOS

1. Log into ASM
2. Search for the device by serial number under Devices on the right-hand side of the screen
3. Click on the device to highlight it
4. Click Edit Device Management
5. Choose Unassign
6. Continue
7. OK
8. Go to FileWave Admin
9. Assistants
10. DEP Associations Mangement
11. Hold down Option
12. Click Full DEP Sync
13. Search for the device in
14. DEP Associations Mangement
15. Note that it should no longer appear here
16. You can wipe the device if you would like, however, we have a KB article with a fileset that removes the FileWave Client: Uninstall the FileWave Client on macOS
17. Noe that the MDM Profile will still be on the device. It can be removed depending on the OS version. Starting in Catalina, if a profile is deployed via MDM it can only be removed via MDM. In those cases, we recommend wiping the device. Leaving it in place won't harm or change anything.
18. Search for the device in FileWave Admin > Clients
19. Single-click on the device
20. Click Delete at the top of the window
21. Update Model

Windows

1. Click on the Start Menu button
2. Type remove in the search bar
3. Choose Add/Remove Programs
4. Scroll down to find the FileWave Client
5. Click Remove
6. Allow the FileWave Client to uninstall
7. Search for the device in FileWave Admin > Clients
8. Single-click on the device
9. Click Delete at the top of the window
10. Update Model

We also have a Remove from System option for you to consider. You can read more about that here: Remove from System

Uninstall the FileWave Client on Windows

Description

The below Fileset can be used to uninstall the FileWave client on Windows machines.

Ingredients

- FW Admin
- FileWave Client uninstall Fileset

Directions

1. Download the attached Fileset from the recipe.
2. Drag and drop the unzipped Fileset in to your Filesets tab. Please make sure to drag it in your root level of your Filesets structure so it is not accidentally deployed to devices. This Fileset will uninstall the client and break communication to your FileWave server.
3. Associate the Fileset to machines that you want to remove from FileWave.
4. Once the Fileset is sent out the devices will not check back in and can be deleted from FileWave.

Windows-ClientUninstaller.fileset.zip

> ⓘ Last tested successfully November 10th, 2021.

Uninstall the FileWave Client on macOS

Description

The below methods can be used to uninstall the FileWave client on macOS machines.

> Updated with version 4.1. Version 4 did not allow for the removal of the FileWave VNC client and as such will cause devices to reboot and not uninstall the FileWave Client. Please update to version 4.1 to avoid this issue. Version 4.1 will still work with older version of FileWave Client.

Ingredients

- FileWave Uninstall, Fileset or Stanadalone

Directions

Fileset

1. Download the attached Fileset and unzip
2. Drag and drop the unzipped Fileset in to your Filesets tab. Please make sure to drag it in your root level of your Filesets structure so it is not accidentally deployed to devices. This Fileset will uninstall the client and break communication to your FileWave server.
3. Associate the Fileset to machines that you want to remove from FileWave.
4. Once the Fileset is sent out the devices will not check back in and can be deleted from FileWave.

↓ macOS

Standalone

1. Download the attached script
2. Use Terminal to run the script locally as root

↓ macOS

> This will uninstall the FileWave Client, but it will not remove an MDM enrolment profile if installed. As such, the device may still be able to connect back to the FileWave Server over MDM, but will be unmanageable. Additionally, if the Custom PKG is configured to instal beyond initial enrolment, MDM can reinstall the client onto the device again. Ensure the MDM profile is also removed if removing the client from FileWave.

Troubleshooting

Troubleshooting

Clearing FileWave Client Certs

In some situations, you may want to explicitly make the server clear and revoke a client certificate without deleting the client from FileWave, for instance if you are wiping a macOS client or reinstalling an IVS client.

From FileWave Central

For desktop clients, you can right-click the client and choose "Clear Certificate(s)".

Note that the current administrator needs to have write permissions on the clients, and will need to enter credentials.

From the Client

The first way is to use the client (13.1.1) certificate itself to authenticate, which is only possible if the certificate and its private key still exist on the client:

```
fwcld -clearCertificate [-serverHost <fwserver_address> -serverPort 20445]
```

This is the equivalent of the following command using curl (replace <fwserver_address> with the address of your FileWave server):

```
sudo curl --key /private/var/FileWave/client.key --cert /private/var/FileWave/client.crt -X POST
https://<fwserver_adress>:20445/auth/client/clear_certificate
```

The client will then be unable to communicate with the server (until a new CSR is created). This command can be used in the activation script of a macOS reinstall fileset to make the server properly clear the old client certificate.

Note that the command above uses the client certificate itself to identify the client. In case the certificate's private key is already lost, there is an alternative where you can authenticate with an administrator's token rather than with the client certificate:

```
fwcld -clearCertificate -token <application_token> [-serverHost <fwserver_address> -serverPort <fwserver_port>]
```

- <fwserver_address>: The FileWave server address (optional)
- <fwserver_port> : 20445 by default
- <application_token>: An administrator application token, with write permissions on this client. Can be found in the Application Tokens tab of the Manage Administrators dialog (example: {1ca3fe82-a41d-8866-bd4d-f83f9f1a8dd5}).

Alternatively, you can also clear certificates en masse using the inventory superadmin token. In this case, you are allowed to clear the certificate of any client (obviously use with caution):

```
curl -X POST https://<fwserver_address>:20445/auth/client/clear_certificates -H 'Authorization:
<application_token>' -H 'Content-Type: application/json' -d '["<serial_1>", "<serial_2>", ...]'
```

Included in 13.1.1 and above are the options to clear with 'MAC address' or 'Device ID':

```
curl -X POST https://<fwserver_address>:20445/auth/client/clear_certificates?identifier=mac -H 'Authorization:
<application_token_base64>' -H 'Content-Type: application/json' -d '["<mac_address_1>", "<mac_address_2>", ...]'
```

```
curl -X POST https://<fwserver_address>:20445/auth/client/clear_certificates?identifier=device_id -H
'Authorization: <application_token_base64>' -H 'Content-Type: application/json' -d '["<device_id_1>", "
<device_id_2>", ...]'
```

The identifier parameter is optional, its default value is serial_number.

- <fwserver_address>: The FileWave server address.
- <serial_1>, ...: serial numbers of clients to revoke. Must match the serial_number field from inventory.
- <mac_address_1>, ...: MAC addresses or clients to revoke.
- <device_id_1>, ...: device ids of clients to revoke.
- <application_token_base64>: base64-encoded value of an administrator application token, with write permission on this client. Can be found in the Application Tokens tab of the Manage Administrators dialog (example: ezFjYTNmZTgyLWE0MWQtODg2Ni1iZDRkLWY4M2Y5ZjFhOGRkNX0=_).

A dict of lists of clients for: SUCCESS, NOT_FOUND and ERROR statuses is returned.

- SUCCESS: the client certificate was successfully revoked.

- NOT_FOUND: no certificate was found on the server for this client, or no such client was found. Maybe the certificate was already revoked, or the client had no certificate yet, or the client had not reported its MAC address or serial number yet, if you passed a MAC address or a serial number.
- ERROR: an unexpected error occurred. Please check server logs for details.

Potential log entries

```
2019-06-12 7:12:02.481|main|FATAL|CLIENT|Unable to retrieve the contents of the cached custom field values: Error
decrypting data
2019-06-12 7:12:02.833|main|INFO|CLIENT|CRL updated
2019-06-12 7:12:02.834|main|INFO|CLIENT|No certificate private key yet. Sending a certificate signing request to
server my.FQDN.com.
2019-06-12 7:12:03.235|main|FATAL|CLIENT|Failed to send enrollment request (and CSR): error 400 a CSR for this
client was already sent.
2019-06-12 7:12:03.235|main|INFO|CLIENT|Falling back to no certificate.
```

Troubleshooting

FileWave Client notification for zsh running in the background

What

When I upgraded my FileWave Client to 15.3.0 or newer I saw a popup saying "zsh is now running in the background".

When/Why

This happens once when first going to version 15.3.0 or higher of the client on macOS. There is nothing to do. This popup is because the FileWave client needs permission to run zsh for scripting. It can be ignored and development is going to look at ways to suppress it so that in the future it should not show, but it should only happen 1 time on each machine and then even on newer versions of the clients you should not see it because it should already have the permission.

Related Content

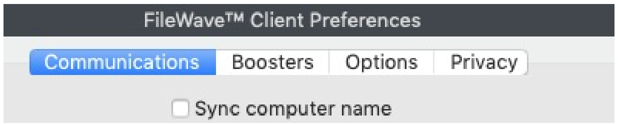
- FileWave Version 15.3.1

Troubleshooting

FileWave Client Rename Behavior

Renaming a desktop client in the admin console will now change the Client Name inventory field to match the new name entered and also change the client name "sync" setting in the client's preferences. This ensures that the device is able to connect properly with FileWave instance without duplicated entries. (The Device Name inventory filed is not modified)

So, when a client is renamed, the "Sync Computer Name" settings is turned off:



□ Sync computer name

Further Details

- The FileWave Client uses its name as part of the identity of the client (see: How the FileWave Client Communicates for more)
- The FileWave Client has a configuration (FileWave Client Configuration Settings) to "Sync Computer Name" that can be changed one at a time (Via Client Monitor) or en masse (Creating a Superprefs Fileset).
- Renaming devices in the FW Admin (r-click → rename) has a different behavior depending on the device (see below)

Behavior (Prior to FileWave v13.2)

- iOS - If you rename an iOS 9.3+ Supervised device in the admin, we send a rename command to the device. No disruption to communication
- macOS / Windows
  - If Sync Name is checked - Client name is new name, Device name is old name. Disruption to communication; Client is still checking in with the old name, and will appear as a new device.
  - if Sync Name is NOT checked - Client name is new name, Device name is old name. No disruption to communication, but there is a discrepancy between names.
- Android / Chromebook - Names in admin are for reference only, and has no effect on communications.

FileWave Client Status Check: How to ask the client what it is doing on macOS and Windows

What

The FileWave client, available for both macOS and Windows, allows administrators to verify its status and understand the tasks it's currently handling. This can be accomplished by executing a specific command in the Terminal application on macOS, or the Command Prompt on Windows. This article provides instructions on how to use this feature for troubleshooting purposes.

When/Why

This feature is especially useful when you have direct access to the device and need to determine what the FileWave client is currently working on. It enables you to view the current status of the FileWave client, the filesets in inventory, and other crucial information.

You might find this feature beneficial when:

- You're diagnosing issues related to the application of filesets or profiles.
- The FileWave client is behaving unpredictably and you want to determine its current state.

How

Follow the steps below to check the status of the FileWave client:

macOS

1. Open the Terminal application on the macOS device.
2. Execute the following command: `/usr/local/sbin/FileWave.app/Contents/MacOS/fwcld -s`

Windows

1. Open the Command Prompt on the Windows device.
2. Depending on the architecture of your Windows OS, execute the appropriate command:
   - For Windows 64bit or ARM, run: `"C:\Program Files (x86)\FileWave\fwcld.exe" -s`
   - For Windows 32bit, run: `"C:\Program Files\FileWave\fwcld.exe" -s`

After running the command, you will see output similar to the example below:

```
**************************
**FileWave Client Status**
**************************
User ID: 11354
Current Model Number: 660

Filesets in Inventory:

1. Fileset Mac MDM OS Update - macOS Monterey 12.6.3 12.6.3, revision ID 10148, ID 10148, revision ID 10148,
version 1 - Apple MDM OS Update is not supported (0)
2. Fileset Mac MDM OS Update - Safari 16.3, revision ID 10149, ID 10149, revision ID 10149, version 1 - Apple MDM
OS Update is not supported (0)
3. Fileset FileWave_macOS_Client_14.10.2_df52a47c77, revision ID 10169, ID 10169, revision ID 10169, version 1 -
Active (0)
4. Fileset Profile - TeamViewerHost Allow Standard User, revision ID 10173, ID 10173, revision ID 10173, version 1
- Handled via MDM (0)
5. Fileset Profile - Microsoft  Defender - Kernel Extension, revision ID 10190, ID 10190, revision ID 10190,
version 1 - Handled via MDM (0)
6. Fileset Profile - Microsoft Defender - Notifications, revision ID 10191, ID 10191, revision ID 10191, version 1
- Handled via MDM (0)
7. Fileset Profile - Microsoft Defender - Web Content Filter, revision ID 10192, ID 10192, revision ID 10192,
version 1 - Handled via MDM (0)
8. Fileset Profile - Microsoft Defender - TCC, revision ID 10193, ID 10193, revision ID 10193, version 1 - Handled
via MDM (0)
9. Fileset Profile - Microsoft Defender - Data Acceptance, revision ID 10194, ID 10194, revision ID 10194, version
1 - Handled via MDM (0)
```

```
10. Fileset Profile - Microsoft  Defender - System Extension, revision ID 10195, ID 10195, revision ID 10195,
version 1 - Handled via MDM (0)
11. Fileset Profile - Microsoft  - Background Service, revision ID 10196, ID 10196, revision ID 10196, version 1 -
Handled via MDM (0)
12. Fileset MS Defender macOS, revision ID 10197, ID 10197, revision ID 10197, version 1 - Active (0)
Filesets not meeting requirements:


Worklist:
```

The output provides the following information:

- User ID and Current Model Number where User ID is really the ID number of the device in FileWave
- Filesets currently in the device's inventory, along with their status
- Filesets not meeting requirements
- Current worklist

This information can assist you in understanding the tasks that the FileWave client is processing and aid in troubleshooting any issues.

Related Content

- FileWave Log File Locations
- Using PowerShell to Remotely Check the Windows FileWave Client Status

Using PsExec to Remotely Restart the FileWaveWinClient Service

What

Using PsExec to remotely restart the "FileWaveWinClient" Windows service allows you to remotely manage the FileWave client on Windows devices. This can be useful in situations where the client is not functioning properly and needs to be restarted in order to resolve the issue.

When/Why

There may be a variety of reasons why you would need to remotely restart the FileWaveWinClient service on a Windows device. Some common reasons include:

- The service has stopped functioning properly and needs to be restarted in order to resolve the issue
- The service needs to be restarted in order to apply a configuration change
- The service needs to be restarted as part of a troubleshooting process

How

To use PsExec to remotely restart the FileWaveWinClient service, you will first need to download and install PsExec on the device from which you will be initiating the restart. PsExec can be downloaded from the Microsoft TechNet website (https://docs.microsoft.com/en-us/sysinternals/downloads/psexec).

Once you have PsExec installed, you can use the following command to remotely restart the FileWaveWinClient service:

```
psexec \[remote device] -u [username] -p [password] net start "FileWaveWinClient"
```

Replace [remote device] with the hostname or IP address of the remote device, and [username] and [password] with the appropriate credentials for the remote device.

Related Content

- Microsoft TechNet: PsExec (https://docs.microsoft.com/en-us/sysinternals/downloads/psexec)

Digging Deeper

In addition to using PsExec to remotely restart the FileWaveWinClient service, you can also use the "net" and "sc" command-line tools to query and change Windows services.

To query a service using "net", you can use the following command:

```
net start [service name]
```

This will display the status of the specified service.

To start or stop a service using "net", you can use the following commands:

```
net start [service name] net stop [service name]
```

To change the startup type of a service using "net", you can use the following command:

```
net start [service name] [startup type]
```

Valid startup types include: boot, system, auto, demand, disabled

To query a service using "sc", you can use the following command:

```
sc query [service name]
```

This will display detailed information about the specified service, including its status, startup type, and binary path.

To start or stop a service using "sc", you can use the following commands:

```
sc start [service name] sc stop [service name]
```

To change the startup type of a service using "sc", you can use the following command:

```
sc config [service name] start=[startup type]
```

Valid startup types include: boot, system, auto, demand, disabled

Keep in mind that you will need to have the appropriate permissions on the remote device in order to use these commands. You can also use PsExec to execute these commands remotely, as described in the previous section.

Understanding and Resolving Proxy Communication Issues in FileWave

What

This article addresses the common communication issues encountered with FileWave, especially when using proxy servers like Lightspeed, Securly, and others. These issues often arise during periods of high network traffic, such as the re-deployment of devices within an organization. This article is meant to offer one possible reason for devices behind proxies could experience communication issues trying to talk to the FileWave Server.

When/Why

Communication problems with proxy servers tend to happen more frequently during peak network traffic times, such as the summer months when educational institutions are re-deploying devices for the new school year. The problem can manifest either through the proxy server being unable to handle the increased load or through port exhaustion if all network ports are in use. Understanding when and why this occurs will aid in prevention and troubleshooting.

How

To alleviate communication issues related to proxy servers, follow these steps:

1. Assess the Situation: Check if the proxy server is overwhelmed with traffic or experiencing port exhaustion. Look for signs such as slower response times or connection failures.
2. Bypass Filtering for Apple Devices: For organizations utilizing Apple devices, it is essential to bypass filtering for the IP range 17.0.0.0/8 as per Apple's guidance. This will prevent inspection of Apple traffic, which could otherwise lead to problems.
   For example, you may configure this in your proxy settings:
   ```
   # Bypass filtering for Apple IP range
   Allow 17.0.0.0/8
   ```
3. Consider Additional Public IPs: If port exhaustion is an issue, contemplate adding an additional public IP to expand the available network ports.
4. Monitor and Adjust: Continuously monitor the situation and adjust configurations as needed to ensure smooth operations during peak times.
5. Work with FileWave Support: Bring any issues to Customer Technical Support so that you don't have to investigate alone. There may also be the possibility of a FileWave Server issue that needs to be resolved.

Understanding the underlying architecture of the proxy server, along with FileWave's communication protocols, can be instrumental in troubleshooting and resolving these issues. Being proactive by preparing the network for expected traffic surges and adhering to recommended practices (like Apple's guidance for bypassing filtering) can prevent these challenges from occurring in the first place. Regular monitoring and adaptive strategies will ensure a resilient and responsive network environment.

Related Links

- Use Apple products on enterprise networks - Apple Support - Official instructions from Apple
- Default TCP and UDP Port Usage - A detailed guide on configuring network settings within FileWave

Troubleshooting

Using PowerShell to Remotely Check the Windows FileWave Client Status

What

The FileWave Client on Windows is like any other software service...the service can be impacted by computer uptime, user interference, crashes, etc. This article gives you a way to INDEPENDENTLY check that a list of devices has the FileWave Client, and it is in working order (or not).

When/Why

Will you need this frequently? Unlikely, but all the same, it is a great tool for sweeping a network to look for devices and confirm the FileWave client (for Windows only). The code here does make some assumptions about your environment, but those are called out below.

How

So, you think the FileWave client may be broken or missing on some endpoints? Wouldn't it be great if you could verify that remotely rather than having to confirm the devices by hand. The following allows you to do just that.

```
#import a list of computers
$mypath=$MyInvocation.MyCommand.Path
$mypath=Split-Path $mypath -Parent
try {
    $computers=Get-Content $mypath\computers.txt -ErrorAction Stop
} catch {
    #no computers.txt file found
    write-host "`nTo use this utility, a text file called computers.txt must exist in the same location as the script.  The file should contain one computer name or IP per line"
    break
}

foreach ($computer in $computers) {
    $online=$false
    try{
        #try to resolve the name
        $online = Resolve-DnsName $computer -quicktimeout -ErrorAction Stop
        $online = $true
    }catch{
        #Catching errors...machine offline
        $online= $false
    }

    if (!$online) {
        #device not online...show it in UI so that we see progress, but don't write it to the results file since it isn't actionable
        write-host "$computer, Not online"
    } else {
        #device online, so let's just see if the service is there
        $fw_service=""
        try{
            #Getting service ...sometimes device might not allow collection (if RPC is unavailable for instance)
            $fw_service = Get-Service -ComputerName $computer  -Name 'FilewaveWinClient' -ErrorAction Stop
            $fw_service=$fw_service.Status
        }catch{
            #Catching errors...no filewave service
            $fw_service="no"
        }

        if ($fw_service -eq "no") {
            #no need to look further since we either can't talk to RPC, or there is no FW service
            write-host "$computer, No FW Service or RPC unavailable"
            Add-Content -Path $mypath\output.txt -Value "$computer, FW Needs Installed or RPC Unavailable"

        } else {
            #fw is there as a service, so let's return status, version, and server address
            try {
                #using C$ share, which won't require winrm
                $TargetPath = "\\$computer\C$\Program Files (x86)\FileWave\fwcld.exe"
                $fw_version = [System.Diagnostics.FileVersionInfo]::GetVersionInfo($TargetPath)
                $fw_version = $fw_version.ProductVersion
            } catch {
                #Catching errors
                $fw_version="version not readable"
            }

            #get fw server address from registry
            try {
                #read server address from registry
                #we need remote registry turned on to read, but we'll turn it back off
                #note this does not account for an environment where remote-registry is on by default...if so, comment out the remote registry lines
                Get-Service -ComputerName $computer -Name RemoteRegistry | Set-Service -StartupType Manual -PassThru| Start-Service

                $Reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine', $computer)
                $RegKey= $Reg.OpenSubKey("SOFTWARE\\WOW6432Node\\FileWave\\WinClient")
                $fw_server = $RegKey.GetValue("Server")

                #turn remote registry back off
                Get-Service -ComputerName $computer -Name RemoteRegistry | Set-Service -StartupType Disabled -PassThru| Stop-Service

            } catch {
                #Catching errors...no registry
                $fw_server="server address not readable"
            }

            #write the output
            write-host "$computer, $fw_service, $fw_version, $fw_server"
            Add-Content -Path $mypath\output.txt -Value "$computer, $fw_service, $fw_version, $fw_server"

        }
    }
}
```

Assumptions made in the above code:

1. There is a text file called computers.txt in the same location as the Powershell script
2. That computers.txt file contains a computer name or IP per line (name is better if you have dynamic DNS)
3. That the Powershell itself is running from a Domain Admin account...this avoids any credential related issues
4. It is assumed that WinRM is not enabled in your environment (if it is this code could easily be made more elegant)

Note that this script could easily be modified to look at other services, to authenticate differently, and to take remediation. As provided, it simply provides a list of results of device name, FW service status, FW client version, and FW server address assigned. All very useful information for troubleshooting. PSEXEC is highly recommended for taking corrective action.

Related Content

- Script Best Practices
- Using PsExec to Remotely Restart the FileWaveWinClient Service
- FileWave Client Status Check: How to ask the client what it is doing on macOS and Windows

Digging Deeper

If you want a resource to pre-sweep the device list for devices that are online separately, you can use the following. A refined list will just make the above script run a bit faster.

```
#Let's just look for a list of devices online
```

```
#import a list of computers
$mypath=$MyInvocation.MyCommand.Path
$mypath=Split-Path $mypath -Parent
$computers=Get-Content $mypath\online_test.txt

foreach ($computer in $computers) {
    $online=$false
    try{
        #try to resolve
        $online = Resolve-DnsName $computer -quicktimeout -ErrorAction Stop
        $online = $true
        write-host $computer
    }catch{
        #Catching errors...machine offline
        $online= $false
    }
}
```

When does the inventory client run scans?

Inventory

The FileWave Client runs an inventory scan at startup, every time you execute a verify on the client, and every 24 hours.

Troubleshooting

PSExec as a Helper in Troubleshooting

What

The PS Tools from Microsoft (from SysInternals) are a terrifically powerful tool to help you troubleshoot when all else fails. In this article we'll look at how you can use PSExec to help troubleshoot an ill-behaving FileWave Client.

When/Why

From time to time, things don't work right. None of us would be employed if this weren't the case, so let's look on the bright-side of that! But what to do if a FileWave client on a Windows device is misbehaving, and you can't communicate through normal FileWave channels? PSEXEC to the rescue.

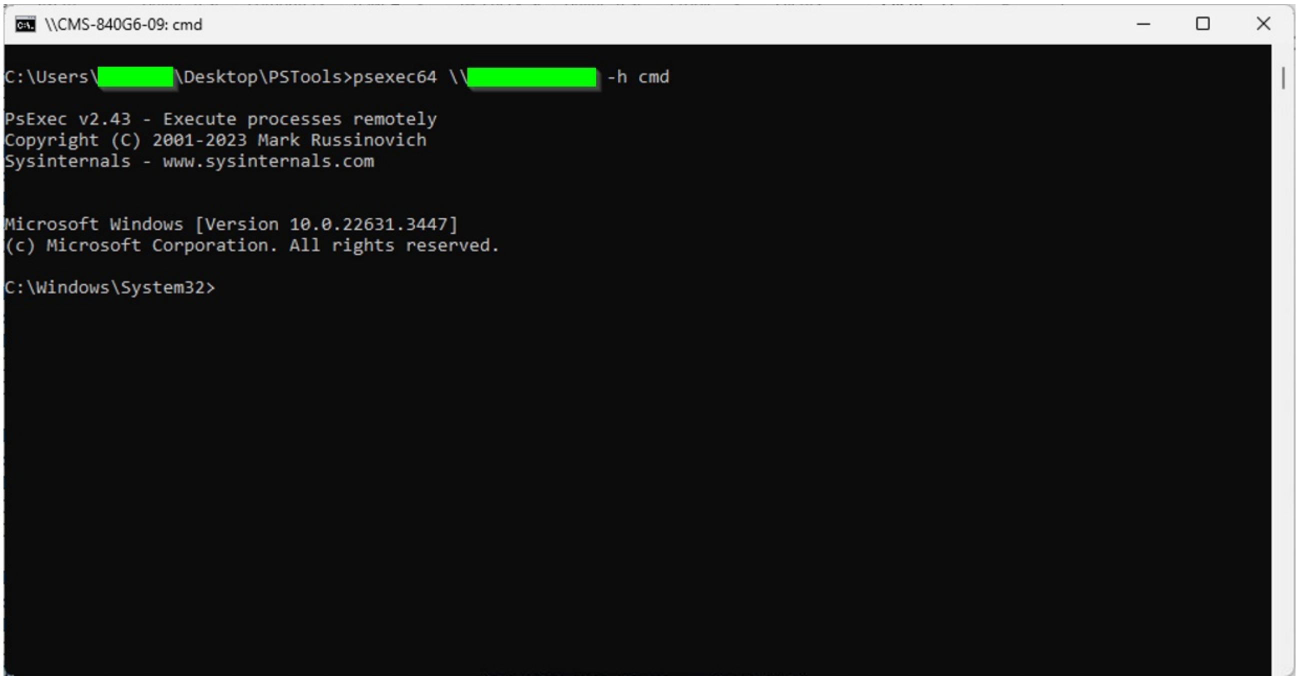
How

> Assumptions made in the following:
> 1) You have download PSTools, and unzipped
> 2) That you launched a cmd prompt as a domain admin user (makes credentials issue easier to deal with)
> 3) That you have changed directory into the directory where PSTools is located

We'll start by simply connecting to the remote computer by name in an interactive PSEXEC shell:

```
psexec64 \\computername -h cmd
```

You'll end up in a shell like the below ('exit' will allow you to leave that shell)

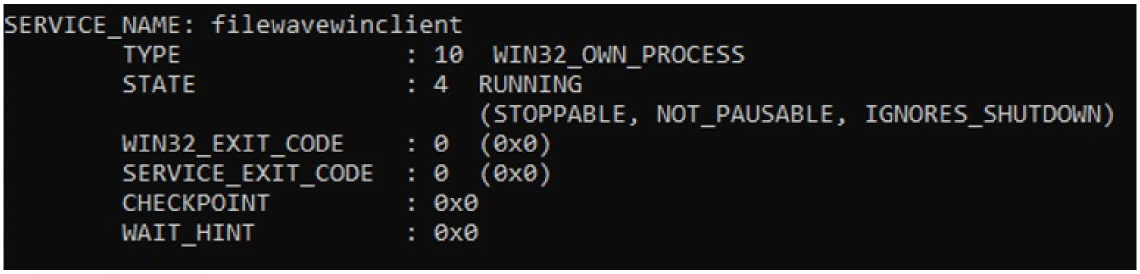


```
C:\Users\[redacted]\Desktop\PSTools>psexec64 \\[redacted] -h cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

Now, what's remarkable about this is that shell is running as your domain admin account, and you can do anything on it you can do from the command line. This article isn't meant to be a Windows CLI primer, but the following are some examples of things we could do if we assume we have a device that isn't reporting in correctly:

1. Check the FileWave Client Service:

   -
     ```
     sc query filewavewinclient
     ```



```
SERVICE_NAME: filewavewinclient
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

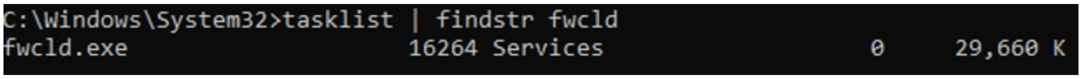
2. Stop the FW Client Service

   -
     ```
     sc stop filewavewinclient
     ```

3. Restart the FW Client Service

   -
     ```
     sc start filewavewinclient
     ```

4. If the service won't start or stop, maybe we need to kill it forcefully by:
   1. Looking for the client process

      -
        ```
        tasklist | findstr fwcld
        ```
      - 

        ```
        C:\Windows\System32>tasklist | findstr fwcld
        fwcld.exe                    16264 Services                   0     29,660 K
        ```
   2. And then killing it by PID

      -
        ```
        taskkill /PID 16264 /F
        ```

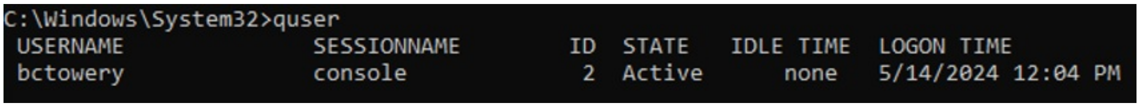
      > Note that this same procedure can be very helpful to clear up a misbehaving Windows Update agent. When Windows Update hangs, the service itself usually won't stop. Taskkill /SVC | find wuauserv will identify the proper task to stop to correct this. (A reboot is also corrective for this, but onviously impacts the use of the device)

5. Check the FW Client Log for entries from today

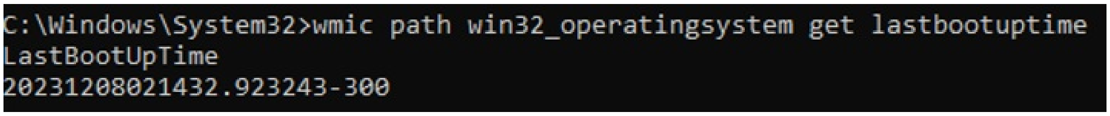
   -
     ```
     type c:\programdata\filewave\fwclient\fwcld.log | findstr mm-dd
     ```
   - (where mm-dd is today's date such as 05-16)
6. Get the IP of the workstation

   -
     ```
     ipconfig
     ```
7. Restart the device (which is obviously destructive to any existing user)

   -
     ```
     shutdown -r -t 0 -f
     ```
8. Determine if there are other users logged in

   -
     ```
     quser
     ```
   - 

     ```
     C:\Windows\System32>quser
      USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
      bctowery              console             2  Active       none   5/14/2024 12:04 PM
     ```
9. Get the last boot time

   -
     ```
     wmic path win32_operatingsystem get lastbootuptime
     ```
   - 

     ```
     C:\Windows\System32>wmic path win32_operatingsystem get lastbootuptime
     LastBootUpTime
     20231208021432.923243-300
     ```

Related Content

- PS Tools
- Great reference for Windows CLI commands (SS64)