Enrolling Devices

Articles about the process to enroll devices in to FileWave.

- Desktop / Laptop Client Install and Configure
- Enrolling Computer Clients in to FileWave
- Mass Deploy Windows FileWave Client
- Apple Notarisation and Custom PKG Installers
- Apple MDM Enrolment Methods
- User Approved MDM Enrollment (macOS)
- macOS MDM Enrolment State
- Enrolling Mobile Devices into FileWave
- Enrolling AppleTV into FileWave
- Importing Computer Clients from a File

Desktop / Laptop Client Install and Configure

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

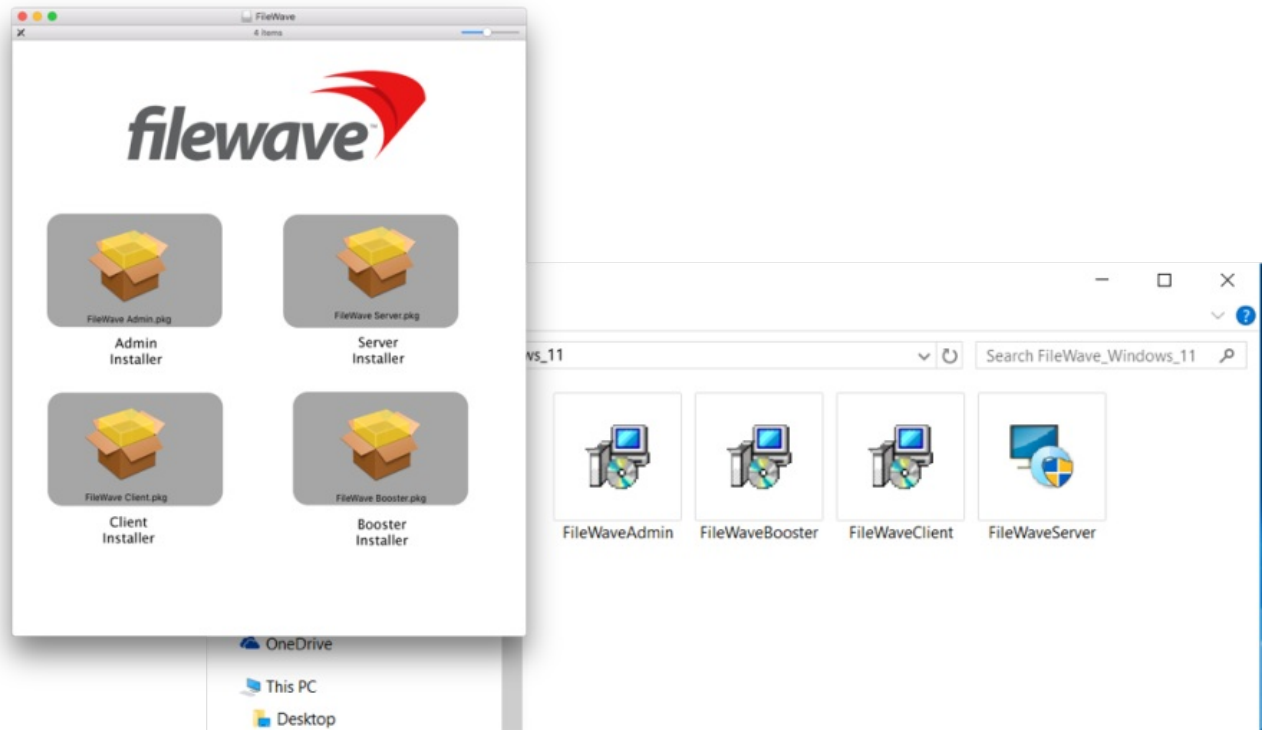
Operating Systems Supported

- 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.

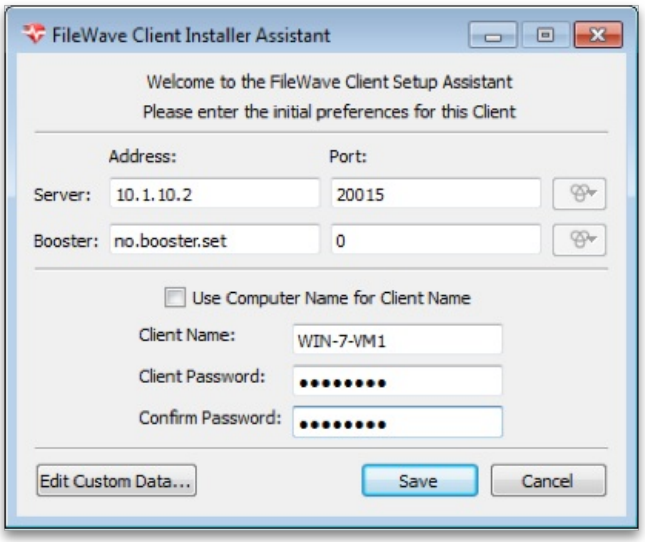


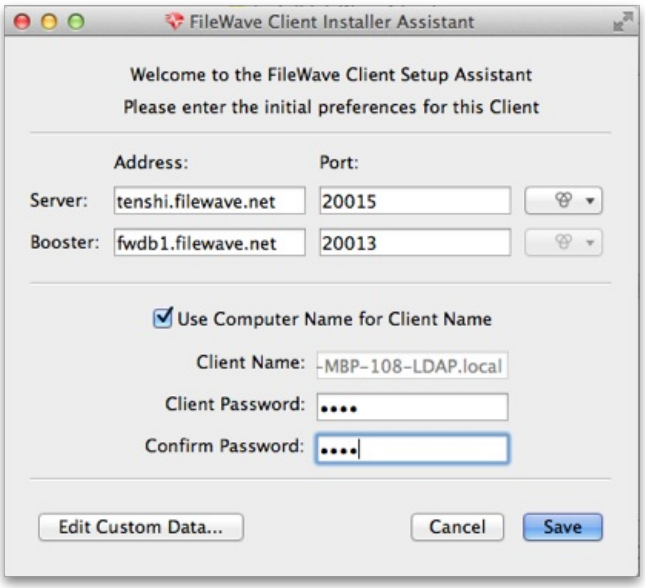
You should download all installers you will need for your deployment at the same time. They can be stored on a file server, or on a flash drive in Windows format for cross platform compatibility (OS X / macOS systems can read Windows-formatted drives without additional drivers).

> 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.





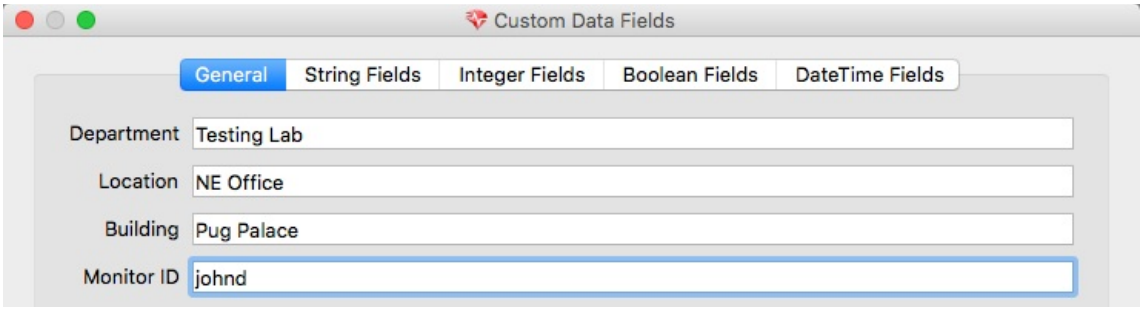
Installation Settings

- 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)

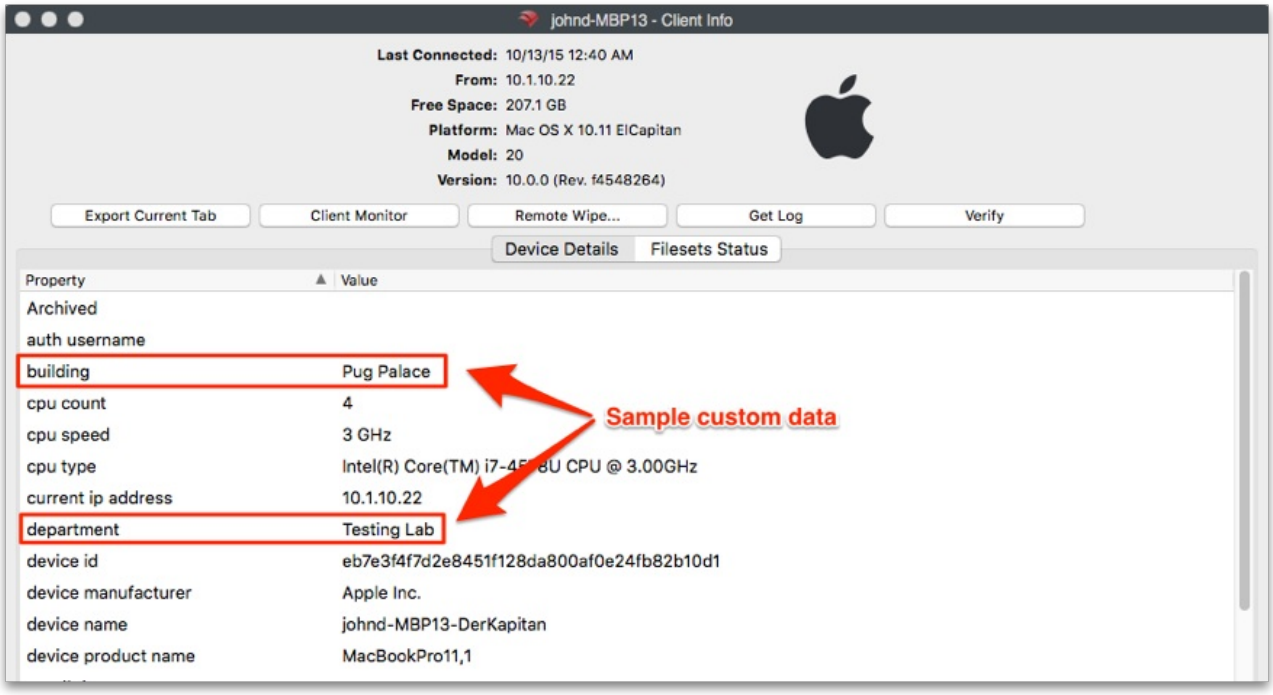
Note: More on working with FileWave Boosters in Boosters.

- 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...



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



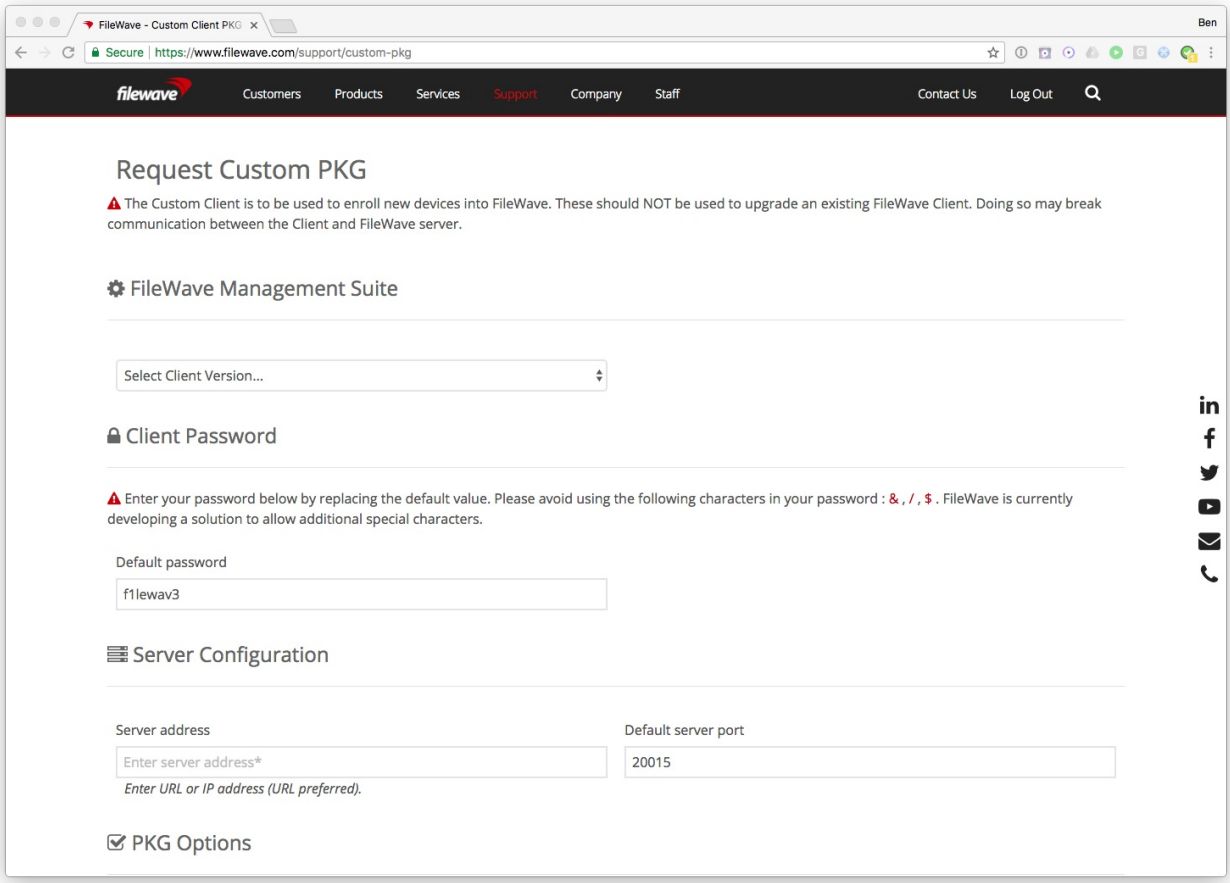
Automating installation with a custom client installer

While the manual method of running the installer and entering all of the connection information works fine for small deployments, FileWave provides you with the ability to perform larger scale installations. A customized client installer is available through the FileWave website:

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.

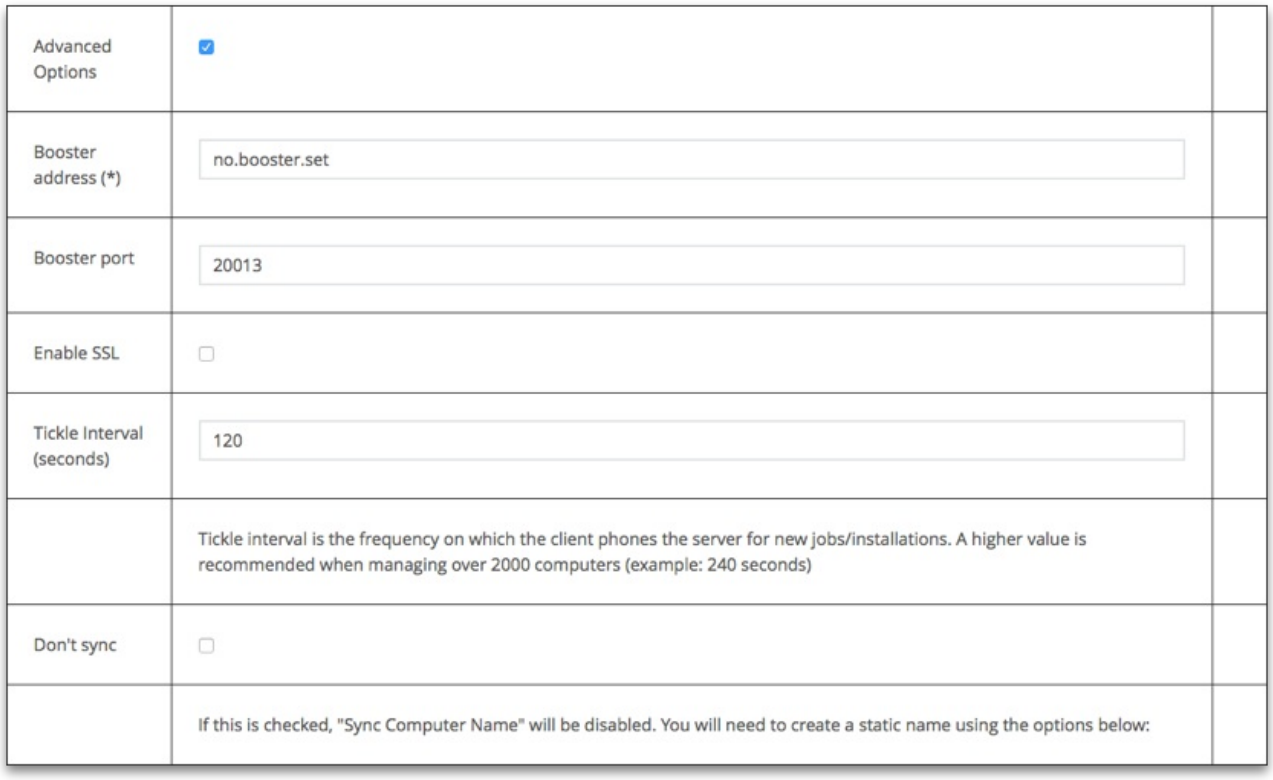
The form is shown on the next page.



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



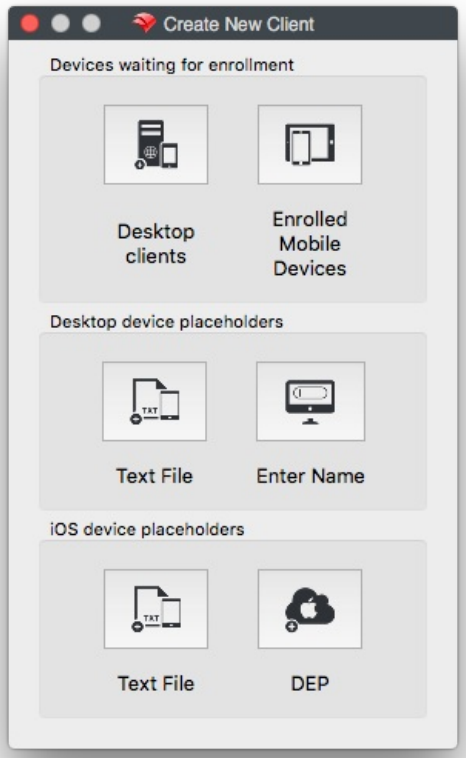
The custom installer does not ask the user for any device specific information, and can be distributed through several means:

- 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.

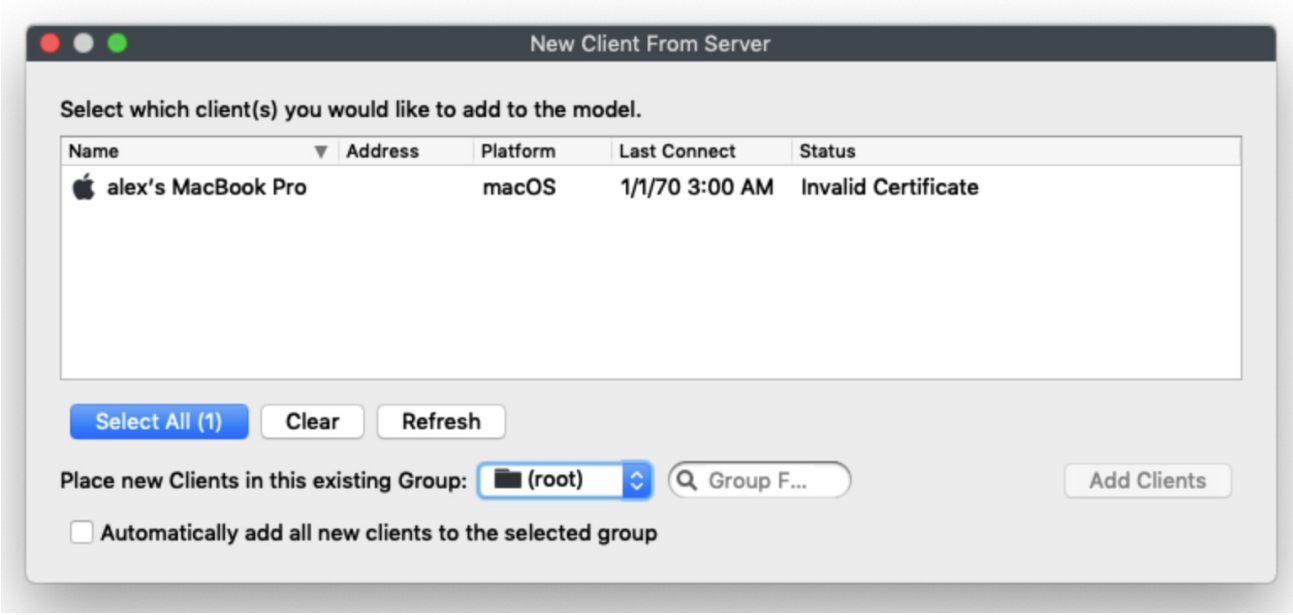
Note: FileWave provides "recipes" of possible deployment workflows for the custom installer in the KB.

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



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.

You can follow this method or possibly a more simple method is outlined here Deploying FileWave Client with Group Policy (GPO) from the eval guide.

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

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=""
```

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)
```

Apple MDM Enrolment Methods

Description

Enrolling Apple devices involves the installation of an MDM Enrolment Profile.

Installation may be initiated by either the user or the device. This same distinction also applies to the linking of the enrolment.

Initiating Enrolment

This refers to the driving force of enrolment.

Consider Automated Device Enrolment (ADE), delivering the Profile before authentication (if configured). This is an example of profile-based enrolment.

Account-driven enrolment relies on the authentication of a user in advance.

User vs Device Enrolment

Automated Device Enrolment links enrolment with the identity of the device; providing the maximum management options available. The extreme opposite is Bring Your Own Device (BYOD) enrolment. This is an example of the user's identity linking enrolment and provides the minimum amount of control.

User enrolment cryptographically separates organisational data from user data and limits many features of MDM. Further details explained in Apple's KB:

User Enrolment and MDM

Overview

Therefore, the key methods of enrolment can be categorised as:

- profile-based device enrolment
- account-driven device enrolment
- profile-based user enrolment
- account-driven user enrolment

Enrolment Methods

Automated Device Enrolment

On startup, the device reaches out to Apple and, where associated, the Enrolment Profile is delivered to the device and installed. The user is then prompted for authentication (if not configured for no authentication).

OTA Enrolment

This enrolment type potentially has two offerings:

- User authenticates to download the Enrolment Profile and then instals the Profile manually.
- An Enrolment Profile is provided to the user, for example by email, and the user manually instals the Profile.

BYOD

BYOD also could be described with two possible options:

- Enrolment Profile is downloaded and then the user authenticates (deprecated, see below note)
- User authenticates in Settings and then approves the subsequently downloaded Profile.

Deprecation

> ⚠ Although definitions exist for all enrolment methods above, as of iOS18 and macOS15 Apple will no longer support profile-based user enrolment. This impacts the first described BYOD enrolment method, meaning BYOD with personal devices must action account-driven user enrolment.

Account-Driven User Enrolment

Although these are personal devices, this enrolment method requires the user to add credentials into Settings which must be a Managed Apple ID. Federated Authentication links a supported IdP with Apple, matching Managed Apples IDs with IdP usernames

and passwords.

Federated Authentication

> Initial support for Account-driven user enrolment is currently targeted for FileWave 15.5. Confirmation of inclusion should be available closer to release.

Related Content

- Account-Driven User Enrolment for i(Pad)OS
- Apple Automated Device Enrolment
- Apple Manual Enrolment

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.

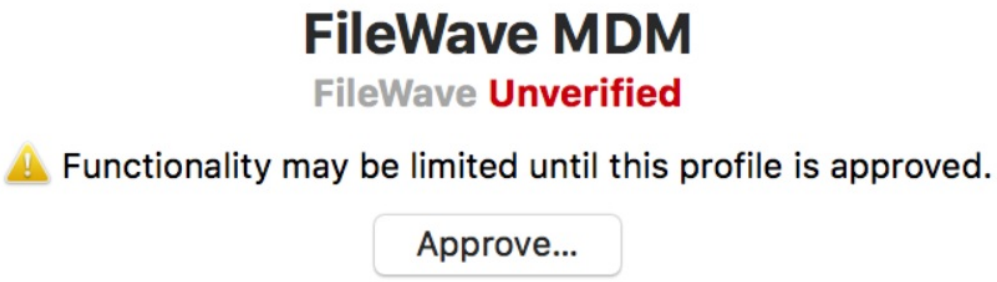
https://support.apple.com/en-us/HT208019

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:



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.

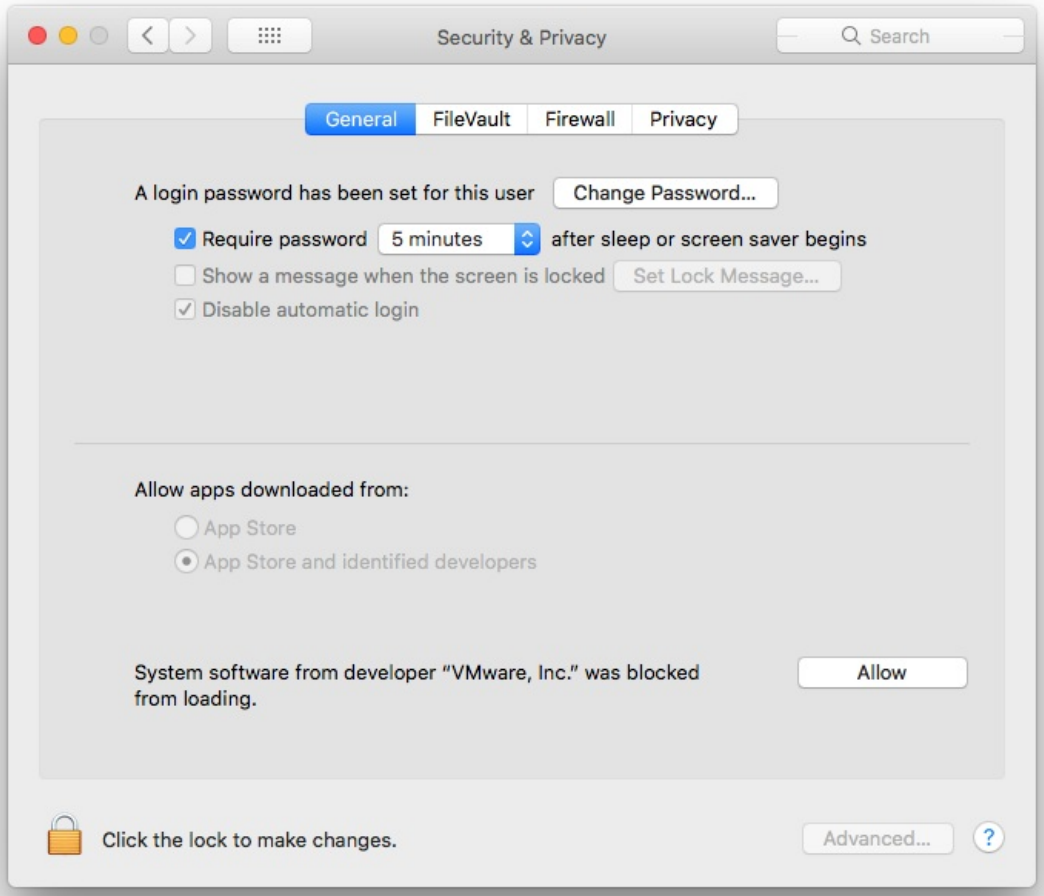
Kernel Extensions

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:

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:



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

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

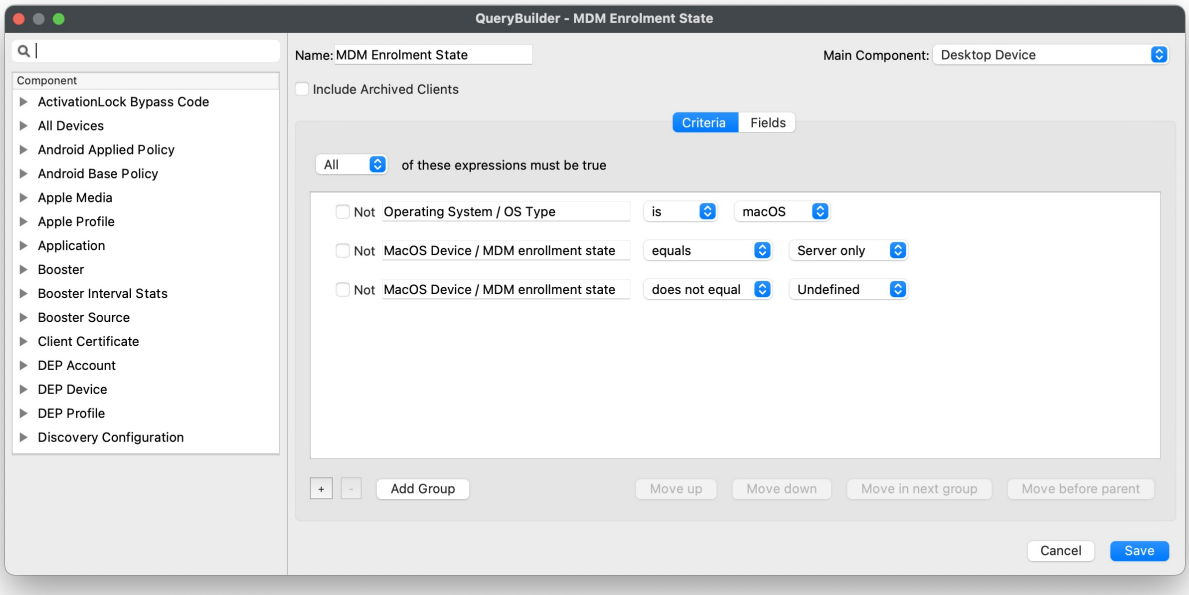
The state is a live report of the current status of the device's enrolment; imagine if a device was initially MDM enrolled, but the enrolment profile has been subsequently removed from the device. Status values include:

- 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:



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

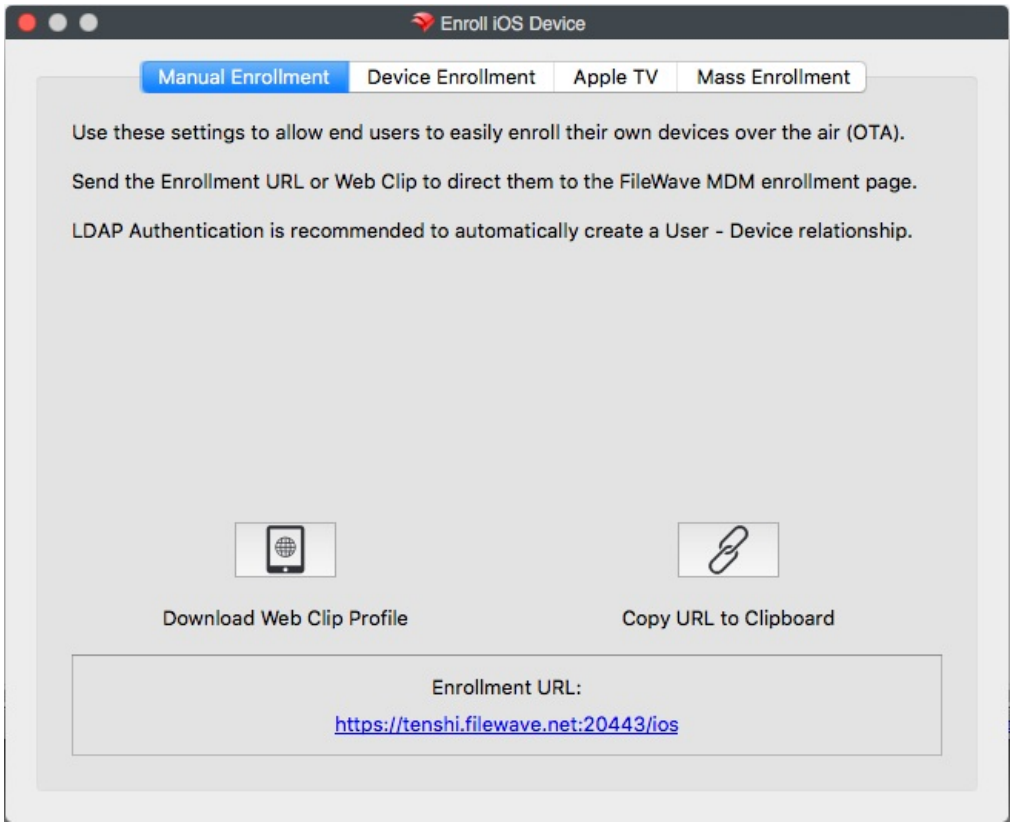
↓ macOS

Enrolling Mobile Devices into FileWave

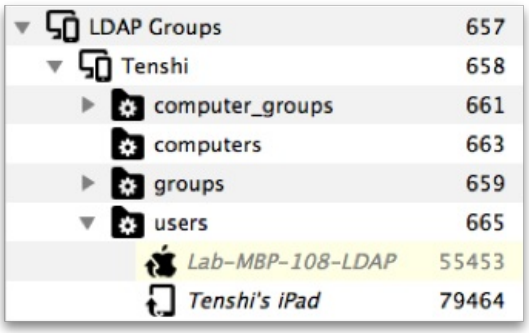
Before FileWave 11.1, iOS devices needed to enroll in MDM before they could be imported into FileWave Admin. Starting with FileWave 11.1, it's possible to pre-import iOS devices; i.e., make Placeholders for them in the database, before they enroll either using a CSV file containing serial numbers+Client 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:

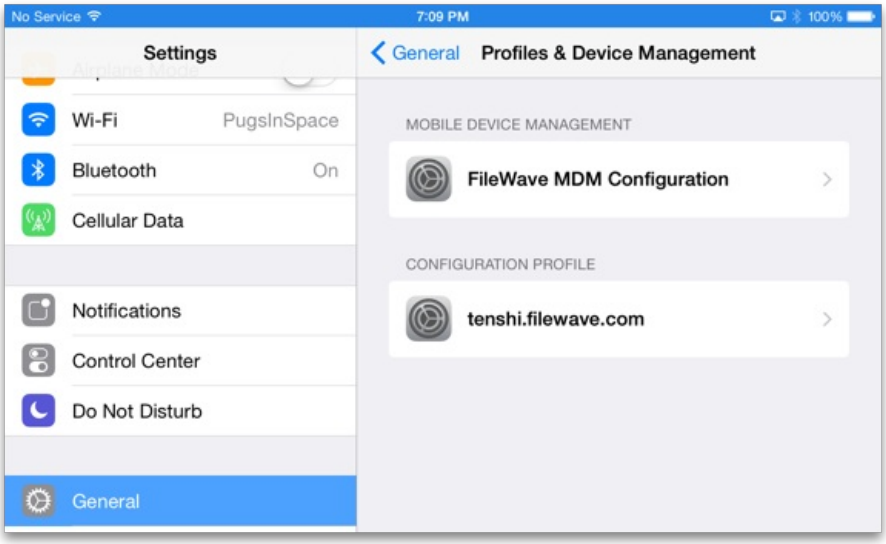


You can create a Web Clip with that URL embedded or copy the URL to the Clipboard and email it to your users. When they go to that URL on their mobile device, they will get instructions on how to properly enroll their device with your server. Having your FileWave server linked to your LDAP server allows 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.

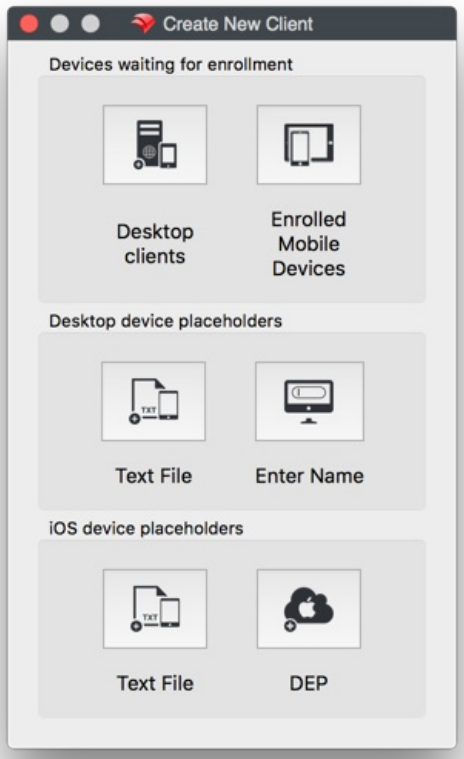


The user is presented with a dialog prompting to install a MDM server certificate, then enroll the device. The second step is when the user will be asked to authenticate - and this is where LDAP integration comes in handy. If not using LDAP, you need to inform users of the generic credential to use,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

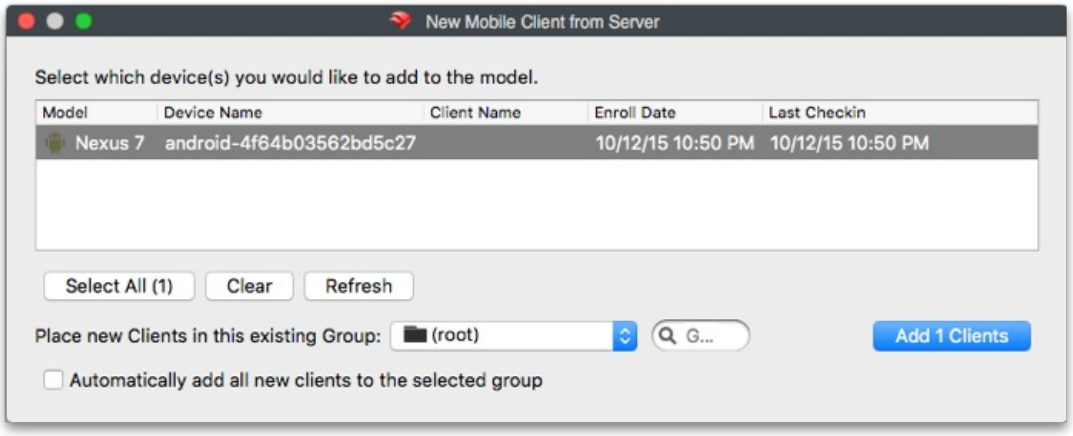
Once the user has completed these two steps, the device will display the new profiles that have been installed:



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



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



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.

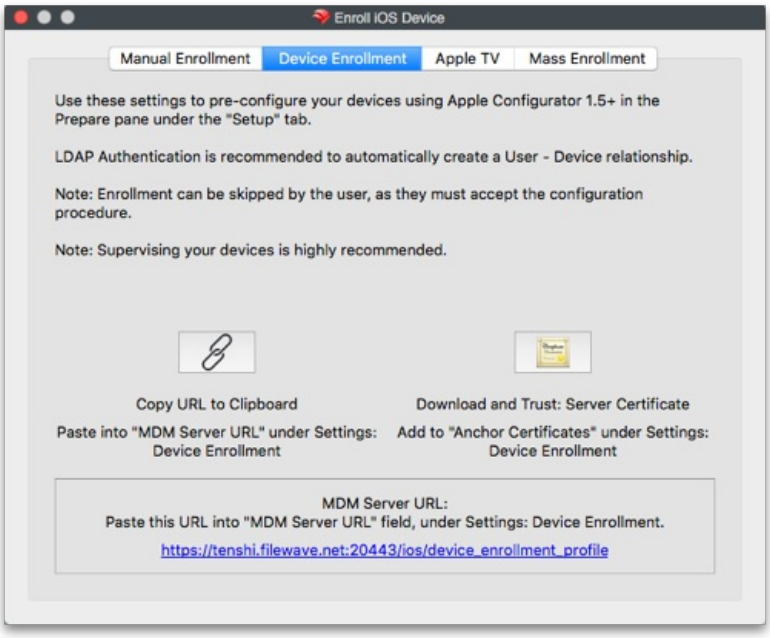
Automatic or Forced Enrollment - iOS

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

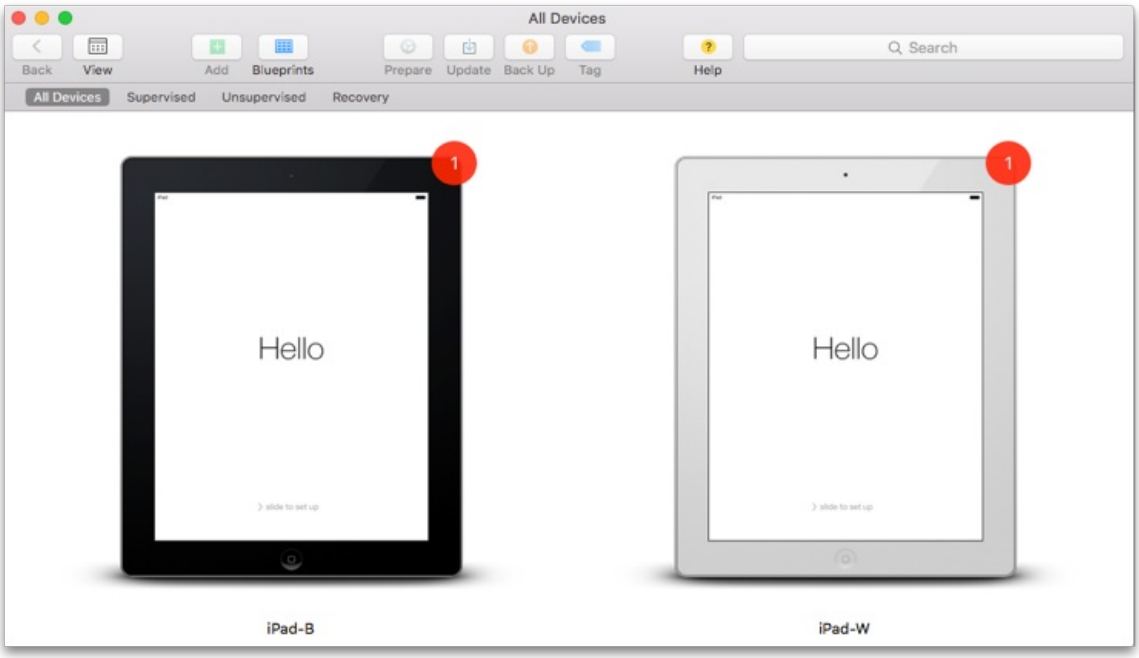
In FileWave Admin, under /Assistants/Enroll iOS Device, you select Device Enrollment:



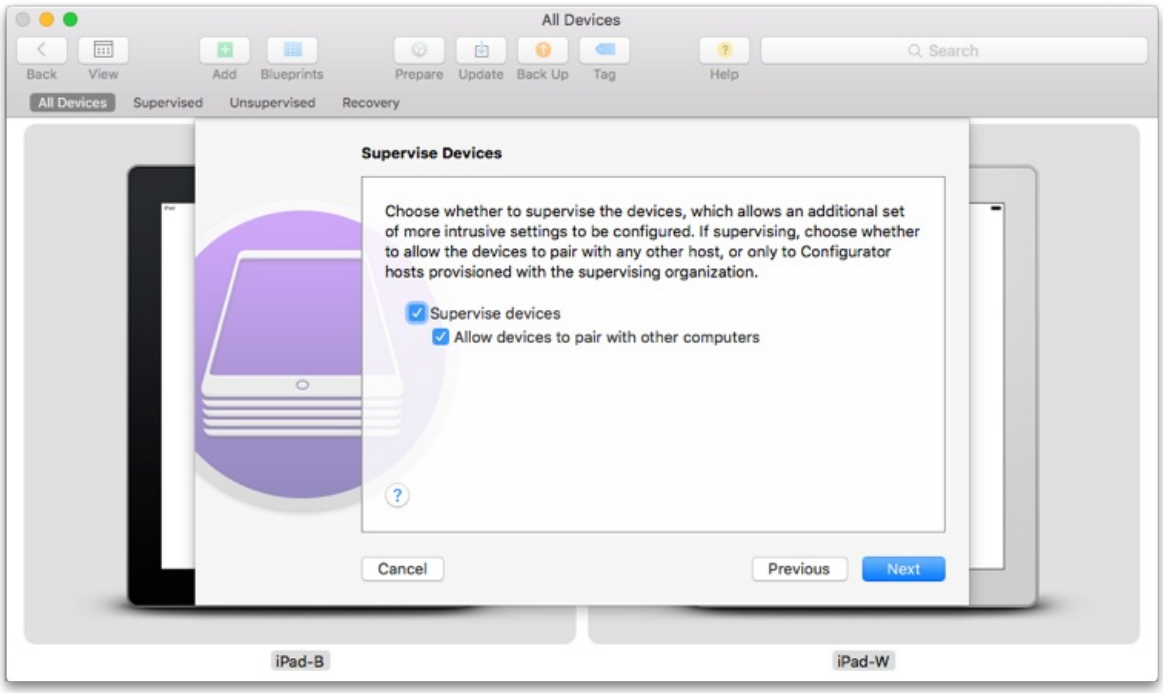
Apple Configurator v2.2.1

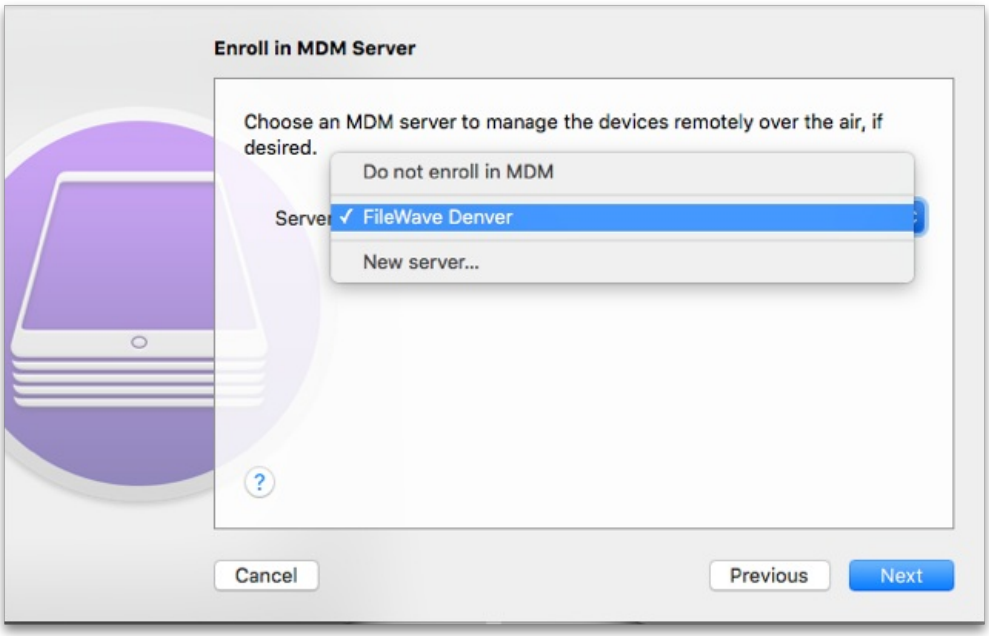
Apple Configurator 2's blueprints let you record actions that can be applied to devices. You add configuration profiles and apps to blueprints, just as you would add them to a physical device. You can prepare a blueprint so it has the MDM data and supervision identify attached. Once you have the blueprint 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/

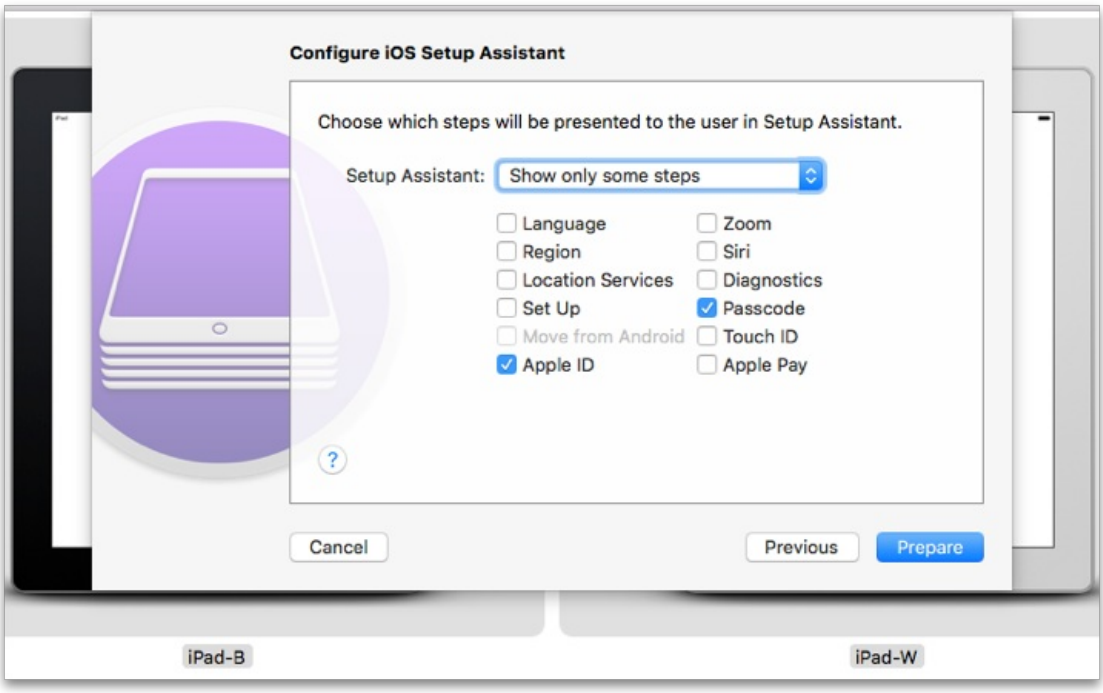
To create a blueprint, click  in the toolbar, select Edit Blueprints, then click on New in the bottom left corner to create a new blueprint. Perform your edits. When you finish, click Done.



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

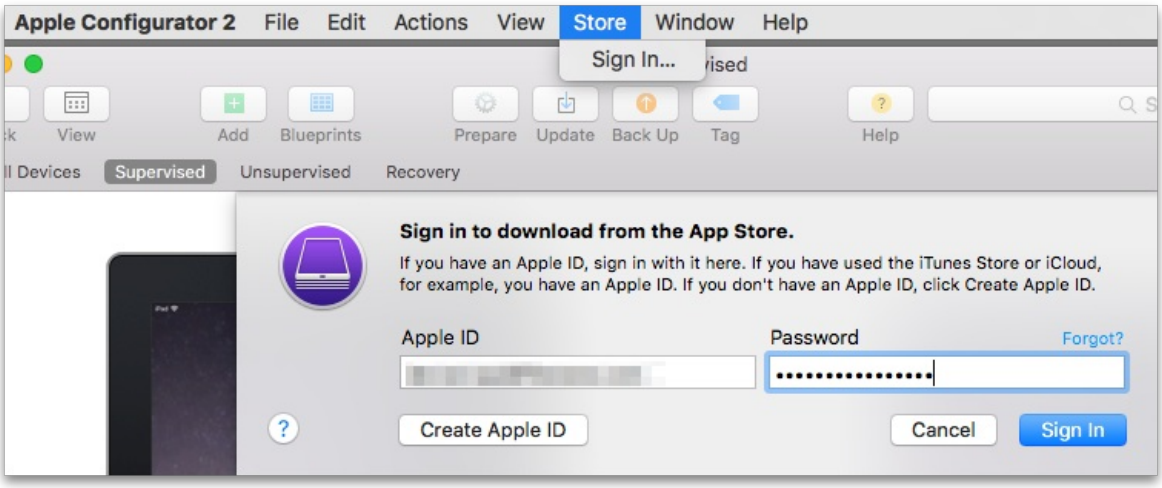

All Devices
Back
View
Add
Blueprints
Prepare
Update
Back Up
Tag
Help
Search
All Devices
Supervised
Unsupervised
Recovery
Supervise Devices
Choose whether to supervise the devices, which allows an additional set of more intrusive settings to be configured. If supervising, choose whether to allow the devices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


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



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!



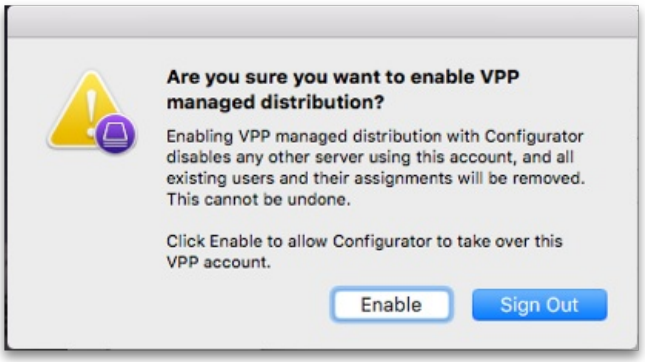
App Store account

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.



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.

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.

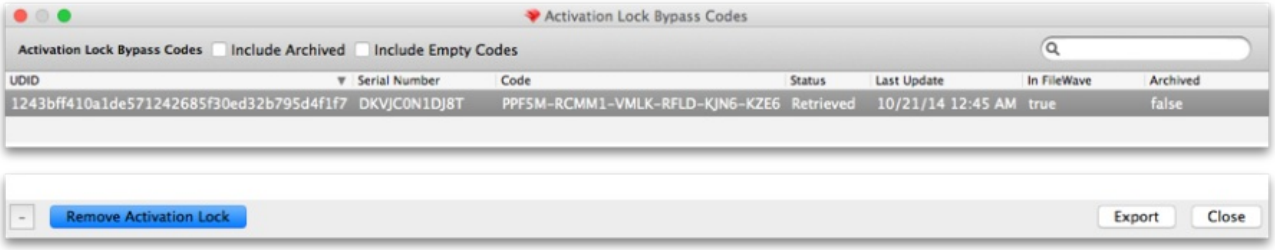
FileWave Enterprise App Portal for iOS

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.

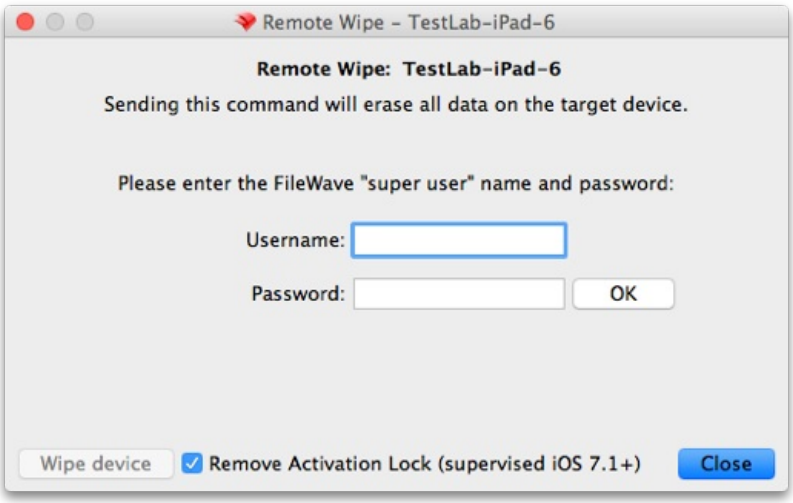
Activation Lock Bypass

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.



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

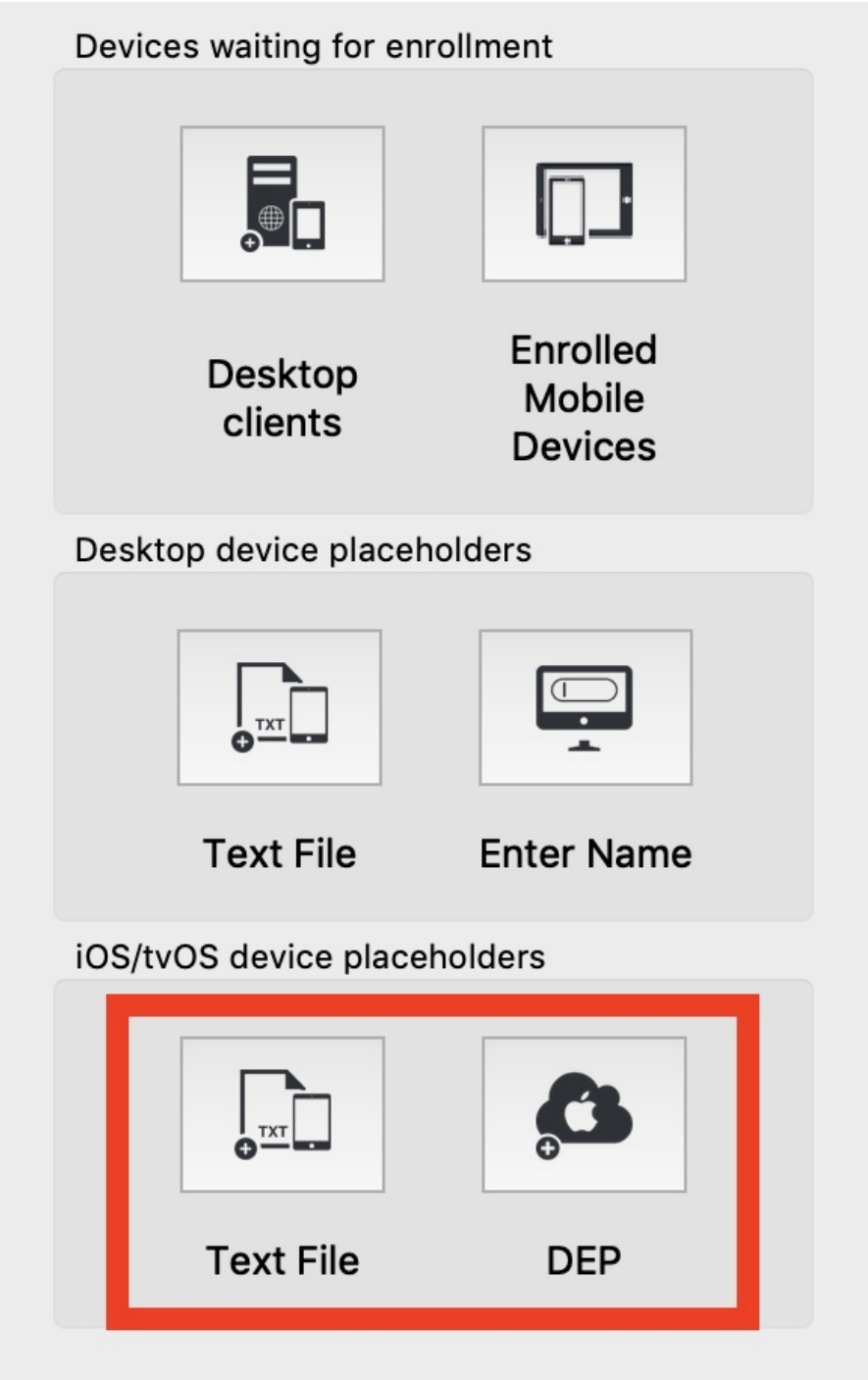


These lock bypass codes are stored in the FileWave server, and remain even when the device has been un-enrolled. The information concerning devices with bypass codes is even provided in Inventory queries. Best practice is to maintain the codes for institutional devices, regardless of the device's enrollment status, as a safety measure. If the device is no longer used, or taken offline, do NOT delete the device from your FileWave database, just archive the device. Once the device has been deleted, the activation lock information is deleted also.

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

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

iOS/tvOS Device Placeholders

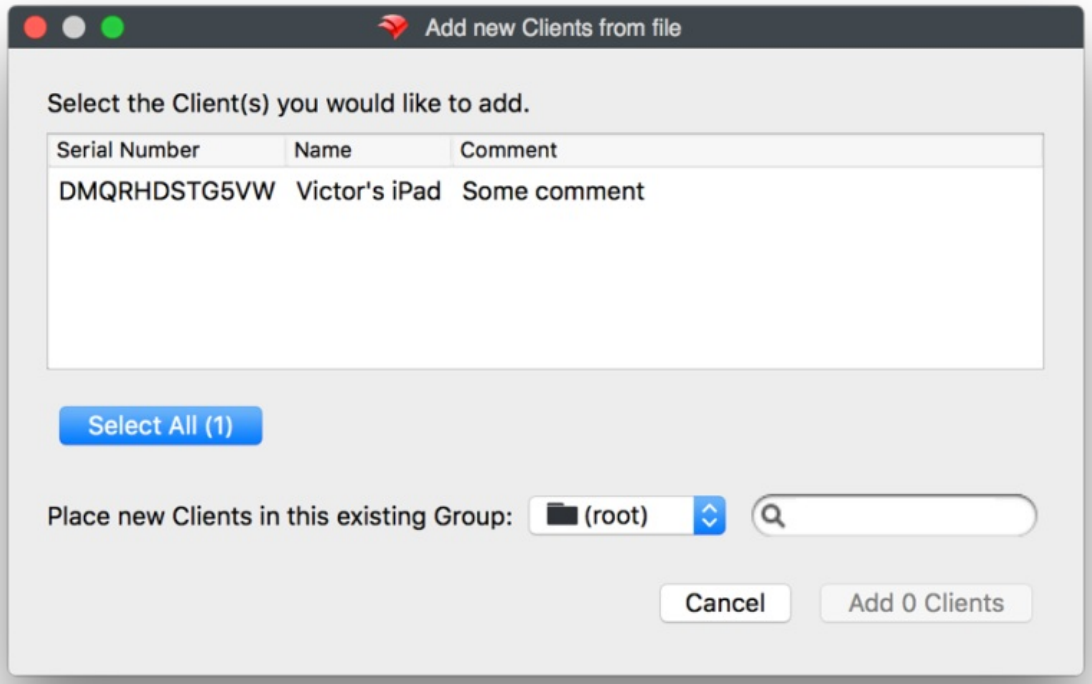


Text File (iOS Devices from CSV)

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.

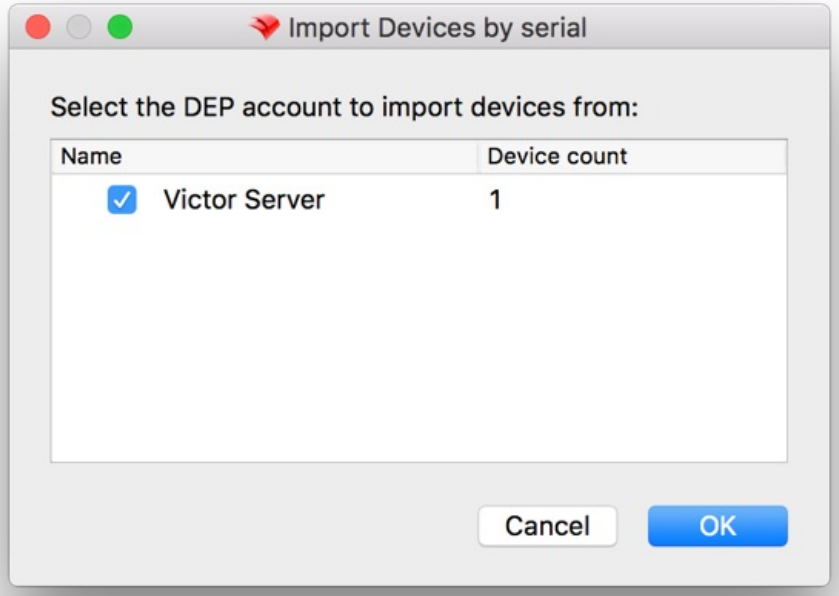


Just select any devices and click Add X Clients. After doing that, the new devices will appear in the Clients view. However, there's almost no information provided for them.

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.



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

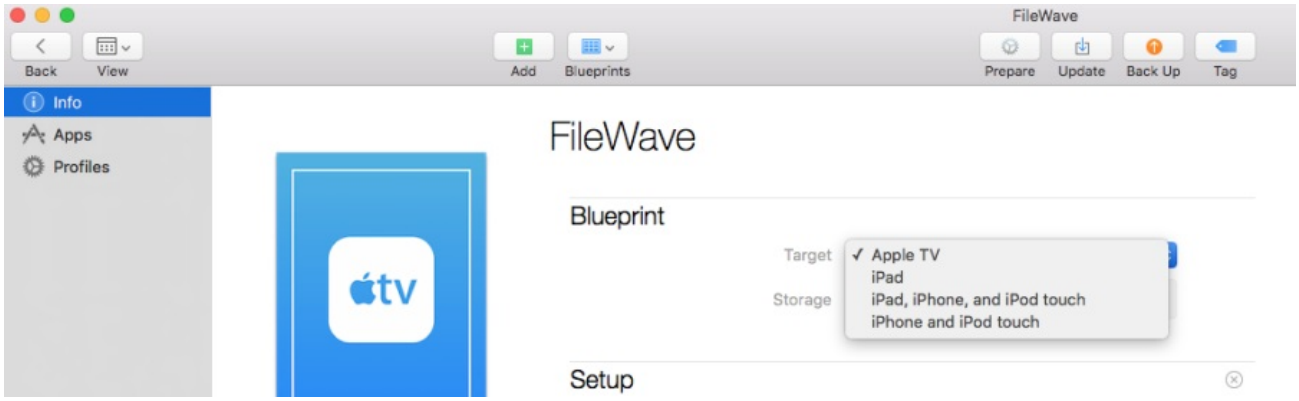
Related Content

- Conflict Resolution
- Enrolling Computer Clients

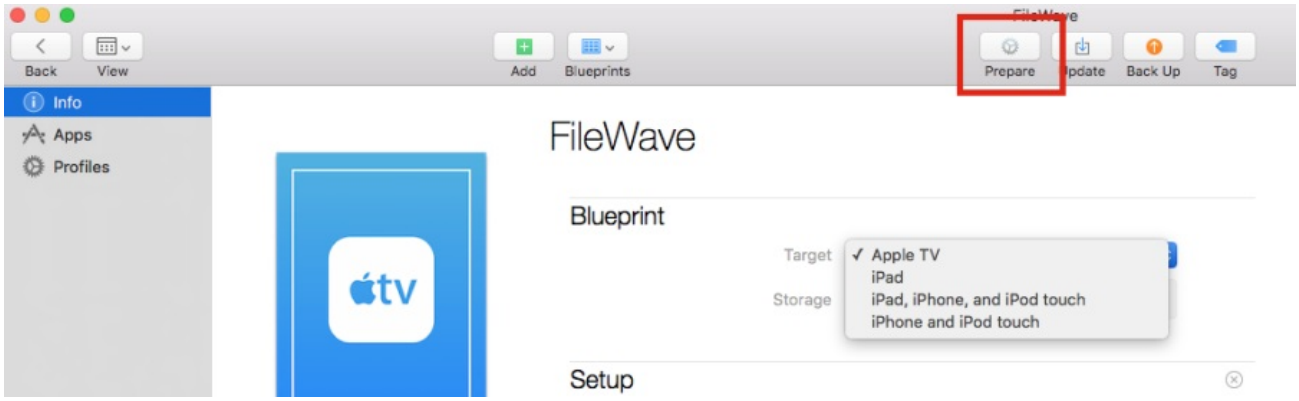
Enrolling AppleTV into FileWave

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.

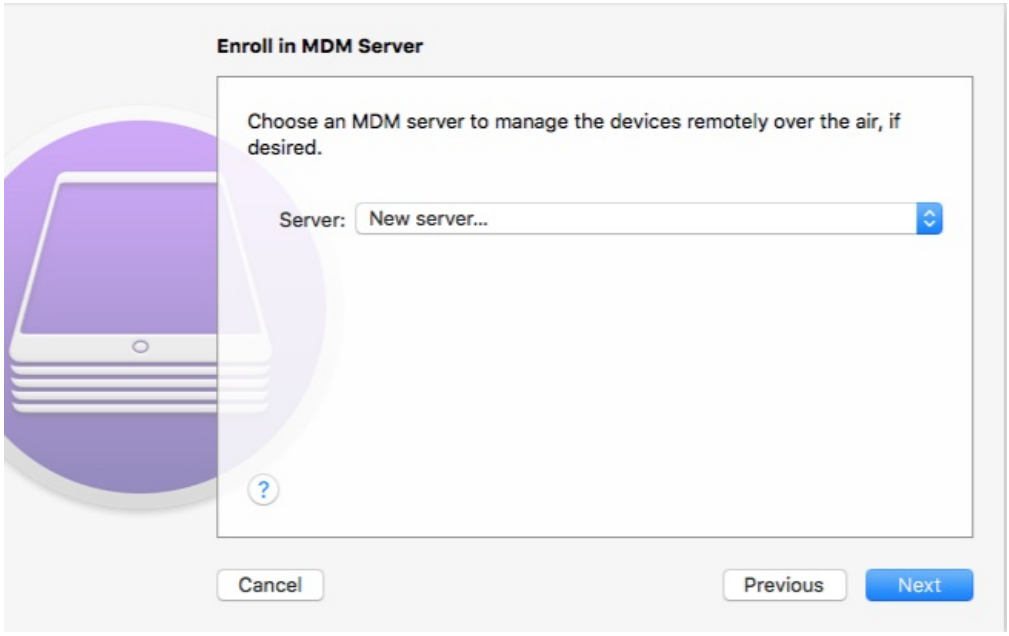


Click on the Prepare icon

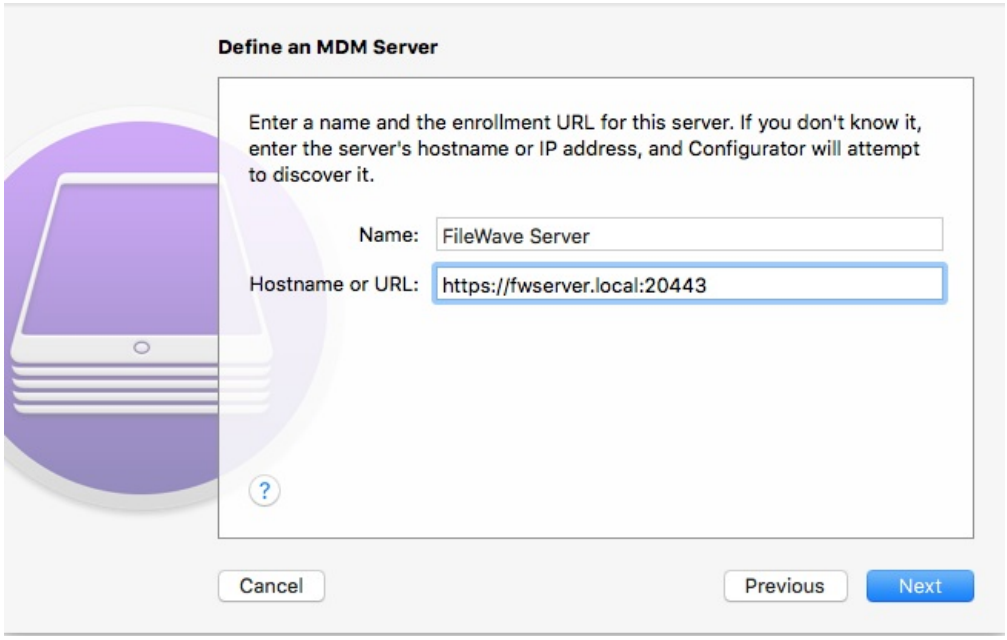


This opens the dialog box

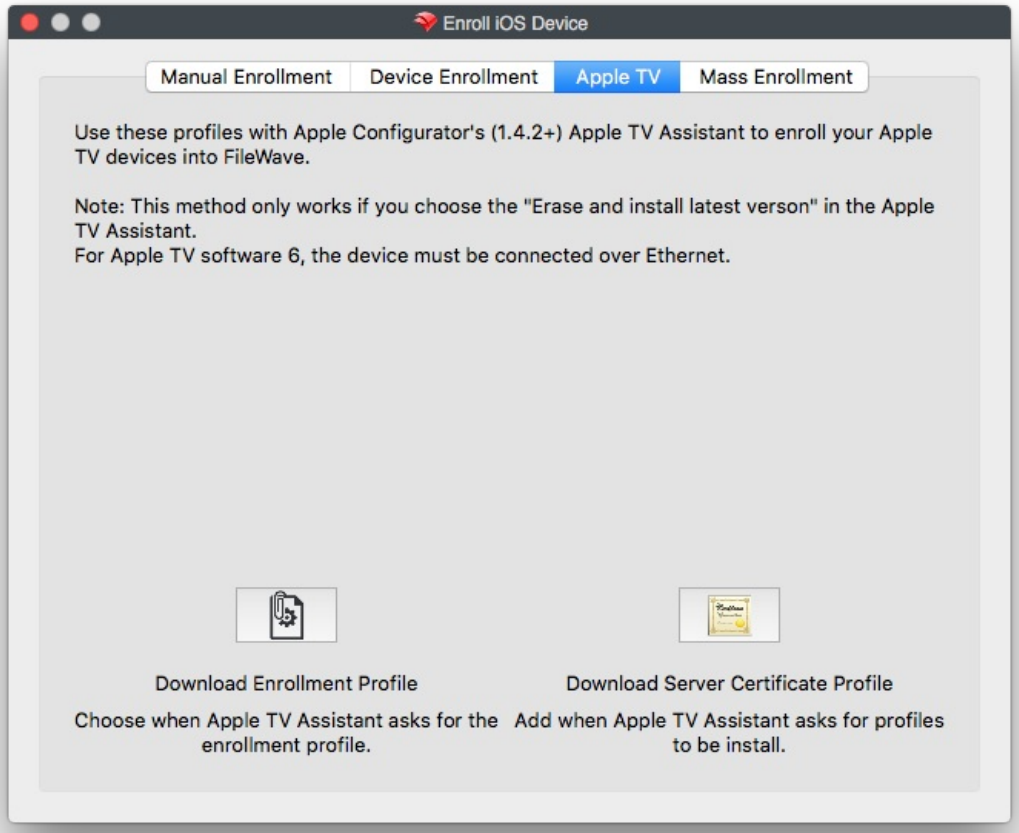
Click on Next.
Select New server... in the Server selection box, then click Next



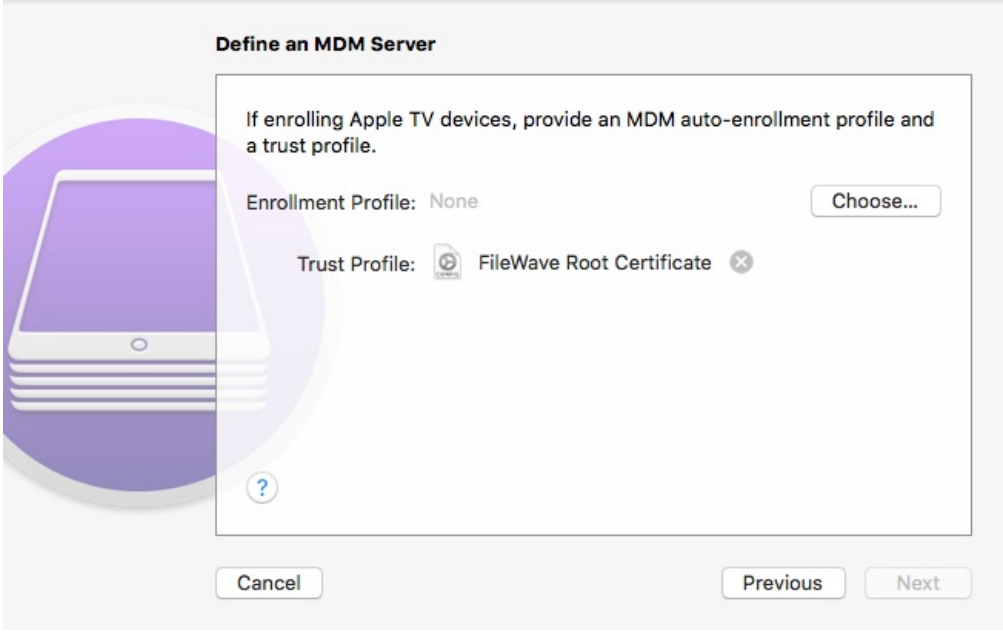
Enter your server name (does not have to be a host name and has no bearing on DNS records; this is for your identification purposes) and the URL for over-the-air enrollment (don't forget the port number at the end of the URL), then click Next.

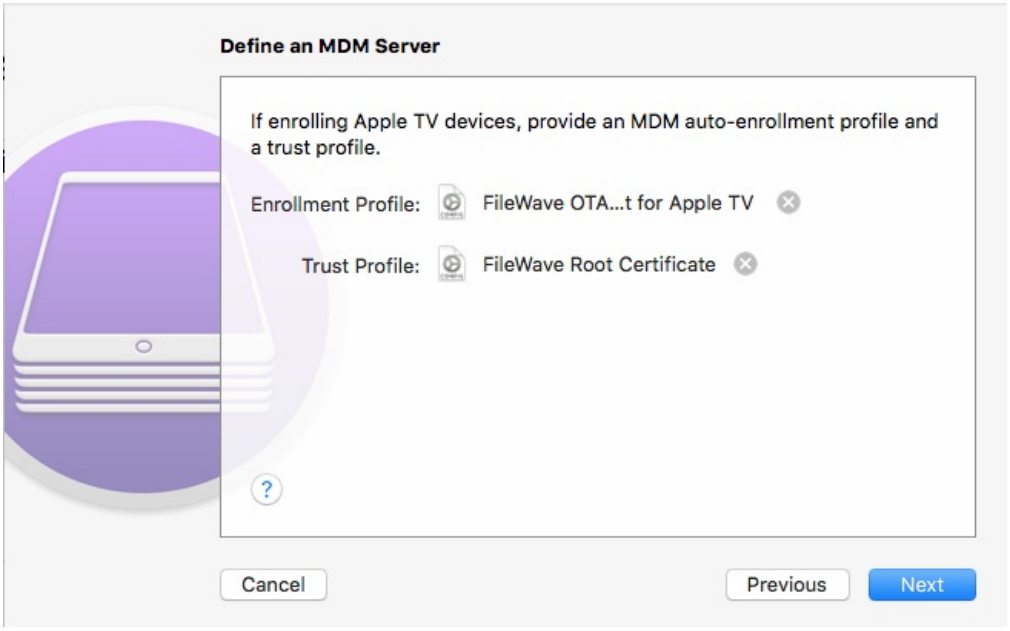


Provided AC2 is able to connect with your FileWave Server, it will show the trust profile and the FileWave Root Certificate. For the needed Enrollment Profile, you get that from the Enroll iOS Device assistant's Apple TV tab in the Enroll iOS Device windows (found under the Asistants pull-down menu)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

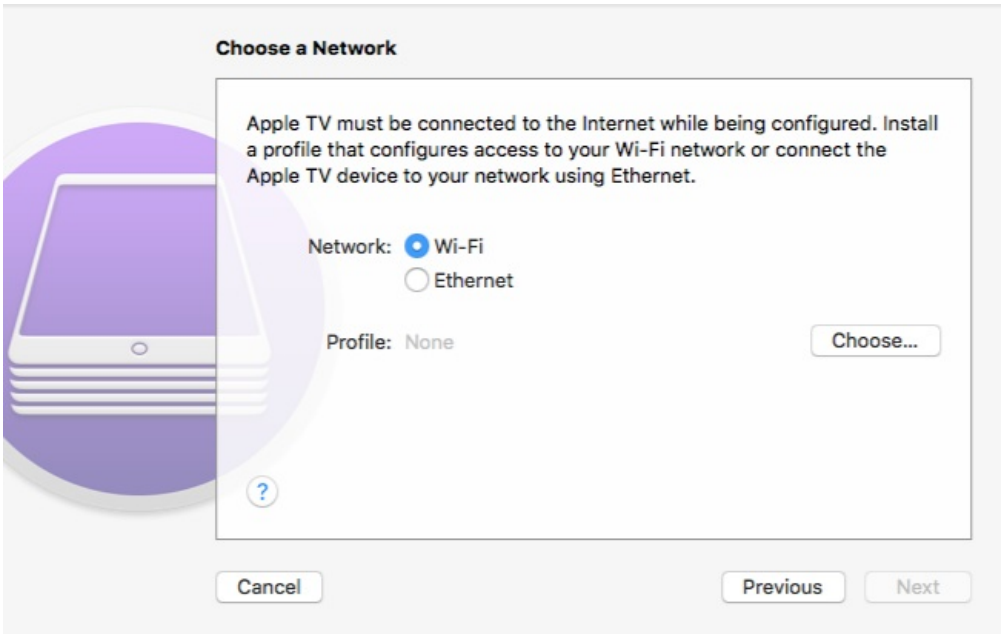


Click Choose... and navigate to where you saved the Enrollment Profile.

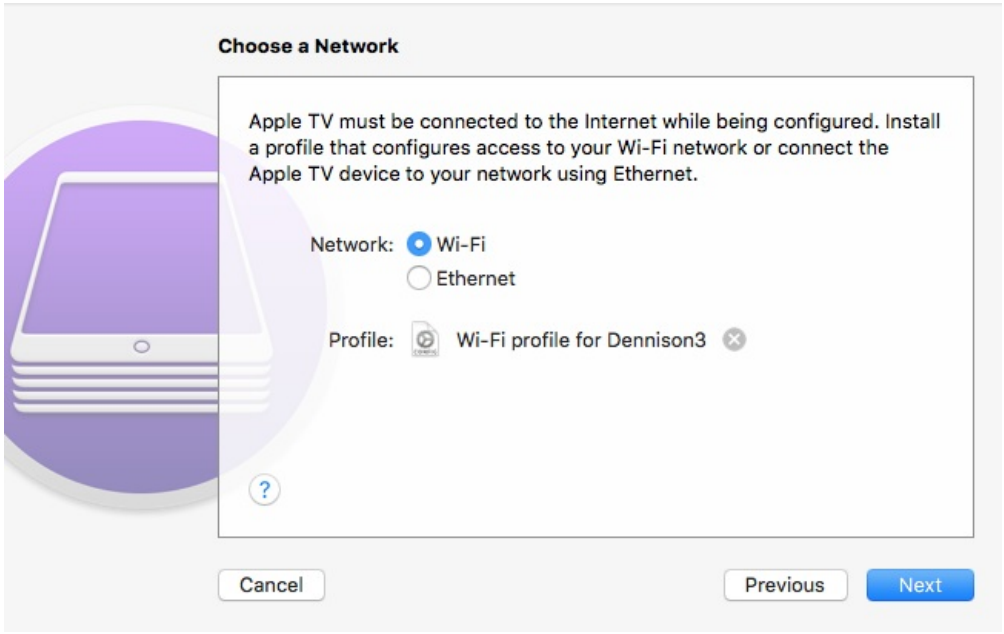




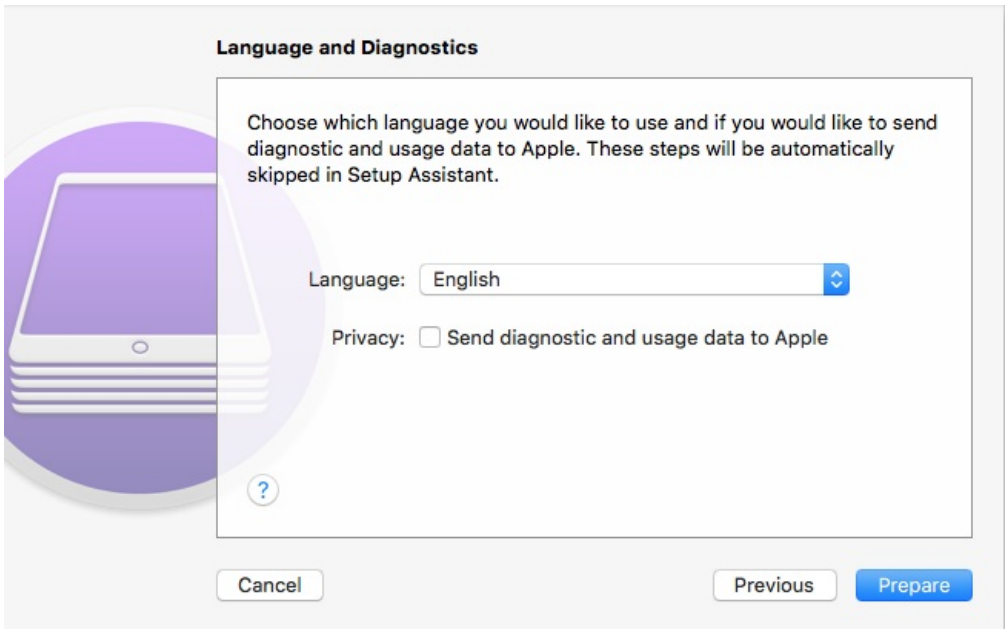
Now that you have all the needed items in this window, click Next. In FileWave, create a profile for Wi-Fi with the SSID and password necessary for the Apple TV to join the wireless network and import that using the Choose... button to navigate to its location to add it to the blueprint.



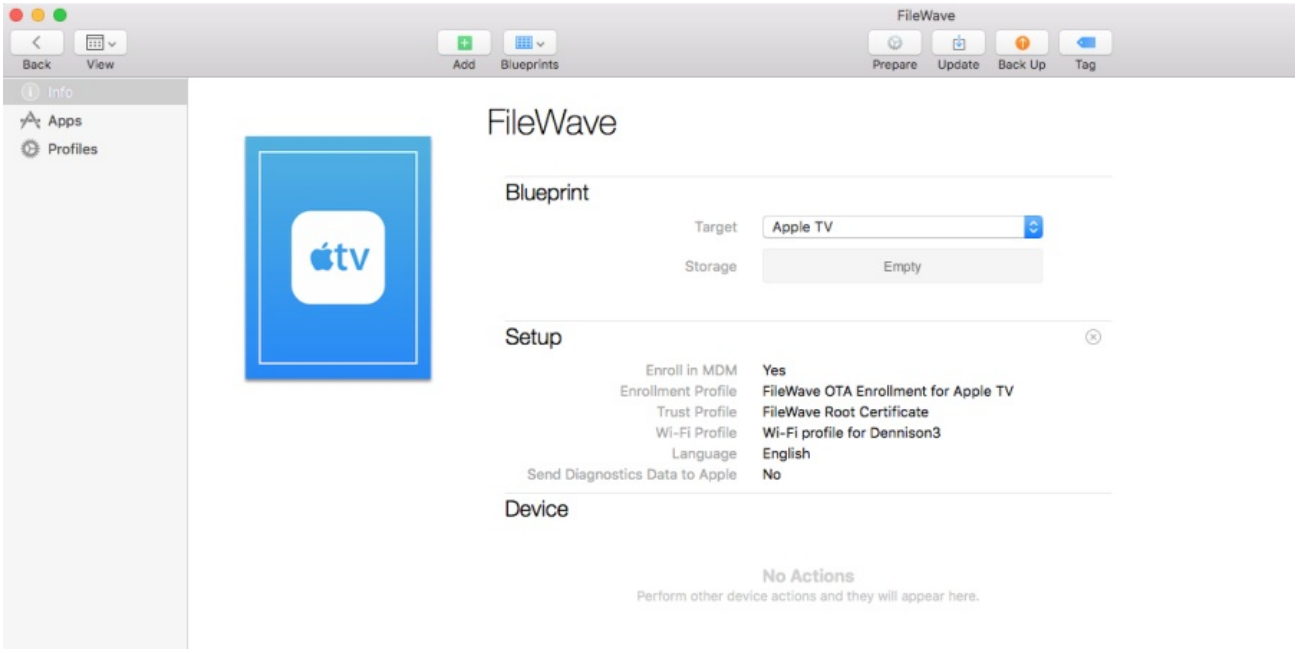
Now, click Next.



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



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



Related Content

- Enrolling Devices
- Conflict Resolution

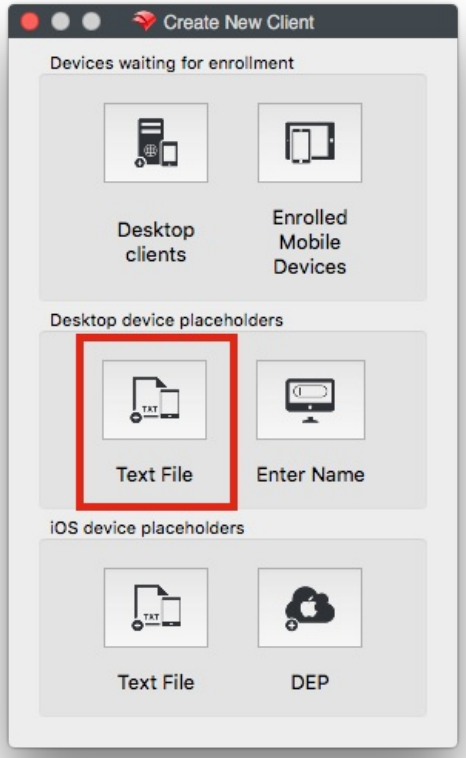
Importing Computer Clients from a File

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.