Working with Apple's Device Enrollment Program (DEP)

> This section is for FileWave version 9.1 and above only. DEP only works with devices purchased from Apple authorized sources. For information on approved devices in DEP, see the following reference: https://help.apple.com/deployment/business/

The features of DEP include:

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

DEP Workflow Overview

1. IT signs up for DEP account (or accounts)
2. Institution purchases devices via an authorized seller
3. IT doesn't see devices in the online DEP list until the shipping confirmation arrives from Apple (prior to that, Apple doesn't know what serial numbers are going to be shipped)
4. IT assigns the devices from the online DEP list to the FileWave MDM server by serial number (You can also assign defaults in ASM & ABM)
5. Wait for the DEP list and the FileWave MDM list to synchronize (24hr default sync, or triggered manually in the DEP UI
6. IT assigns DEP profiles to the serial numbers of the devices prior to arrival (Automatically Assign DEP profiles)
7. Devices arrive and, at first boot, are auto-enrolled and configured as managed devices (macOS computers will auto-enroll if connected to the Internet for push notification and the MDM server for enrollment.)

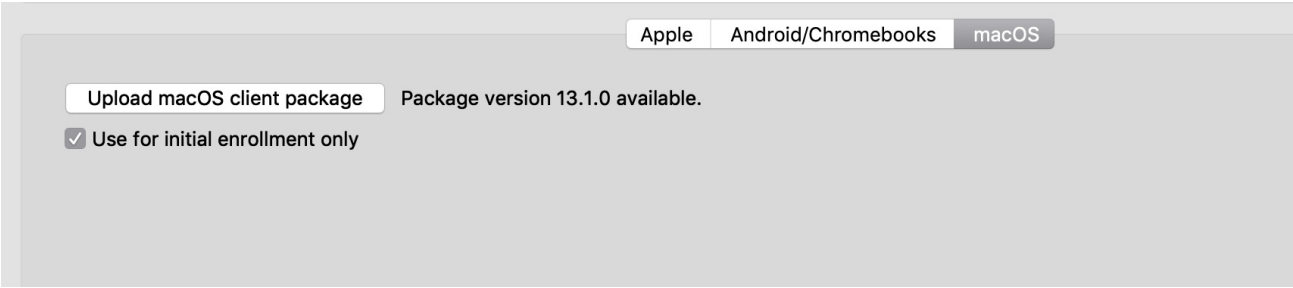
> For more information see: https://support.apple.com/en-us/HT204142

Configuring DEP with FileWave

This process is covered in VPP and DEP preferences

FileWave Client for OS X DEP

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



> "Use for initial enrollment only" is highly recommended. This means that FileWave will only attempt to install the PKG the first time a devices enrolls. If it is unchecked, and you upload a new PKG, FileWave will send this out via an APN immediately. This could cause existing devices to loose their configuration (like boosters)

Understanding devices and profiles for DEP

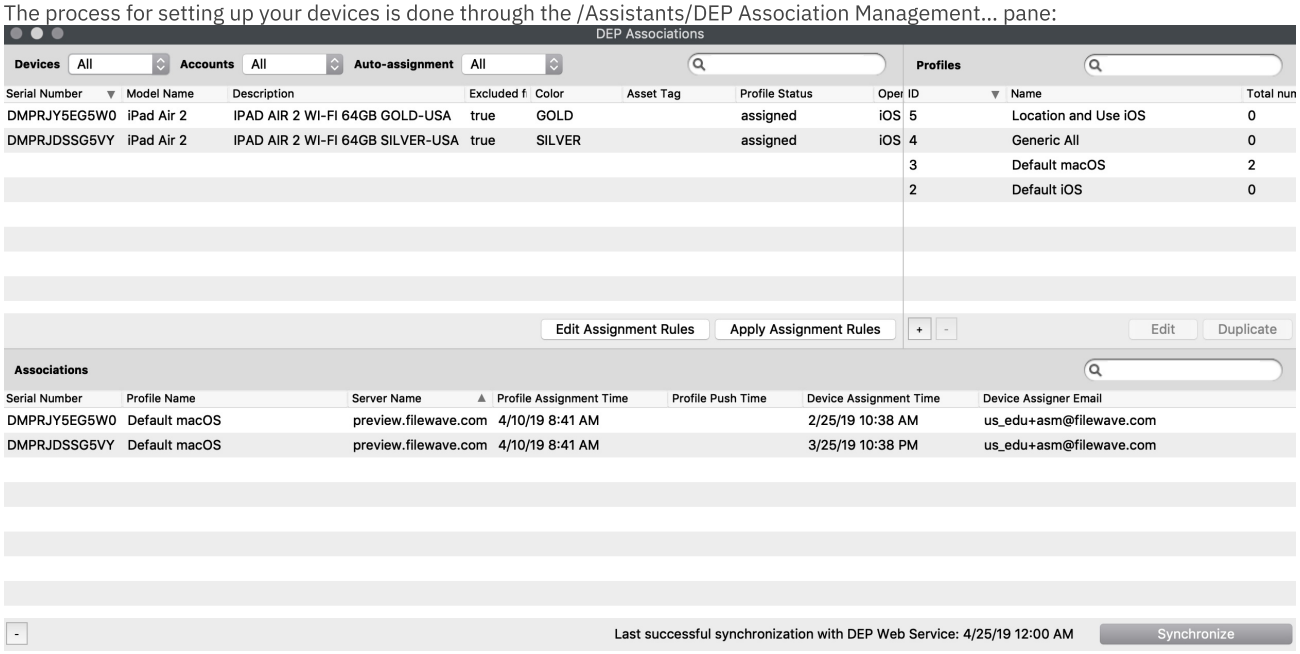
Once you have registered your FileWave Server with the DEP system, you can begin setting up your devices for automatic enrollment and management. You will be able to view a list of your devices along with certain characteristics of those devices, such as model number, color of the device, asset tag information,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

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

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

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

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



The DEP Associations pane looks similar to other FileWave windows with three sections. In this case, they are:

- The Device list in the upper left, which you can filter by the different accounts devices are purchased under;
- The Profiles list in the upper right, which lists all of the profiles available to associate to devices with the number of devices each is assigned to; and,
- The Associations list on the bottom, which displays the device by serial number, the name of the profile it is associated with, and various date-time Groups showing assignment dates and times.

Security prerequisites for DEP

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

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

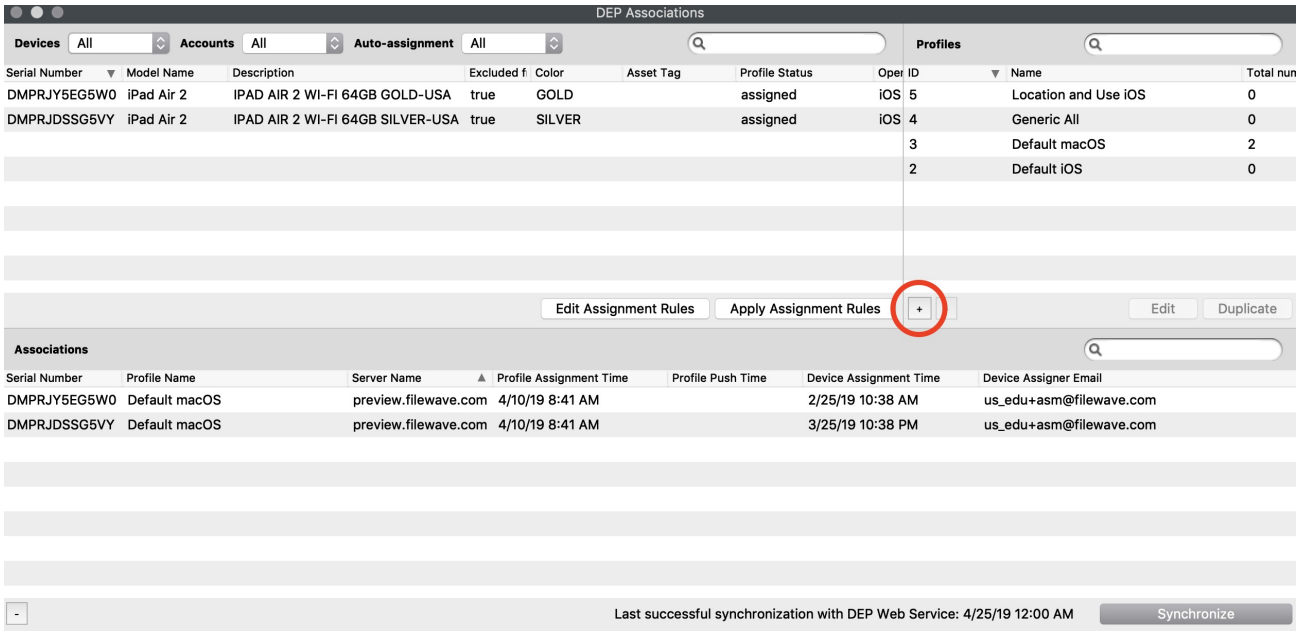
The adddepuser command requires you to provide a user name in the command, and respond to the prompt to add a password for that user, then to confirm the password. This user name and password will be requested by the device during DEP enrollment. These commands are issued on the FileWave MDM server either directly or remotely through terminal services.

Authentication with LDAP

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

Configuring DEP profiles

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

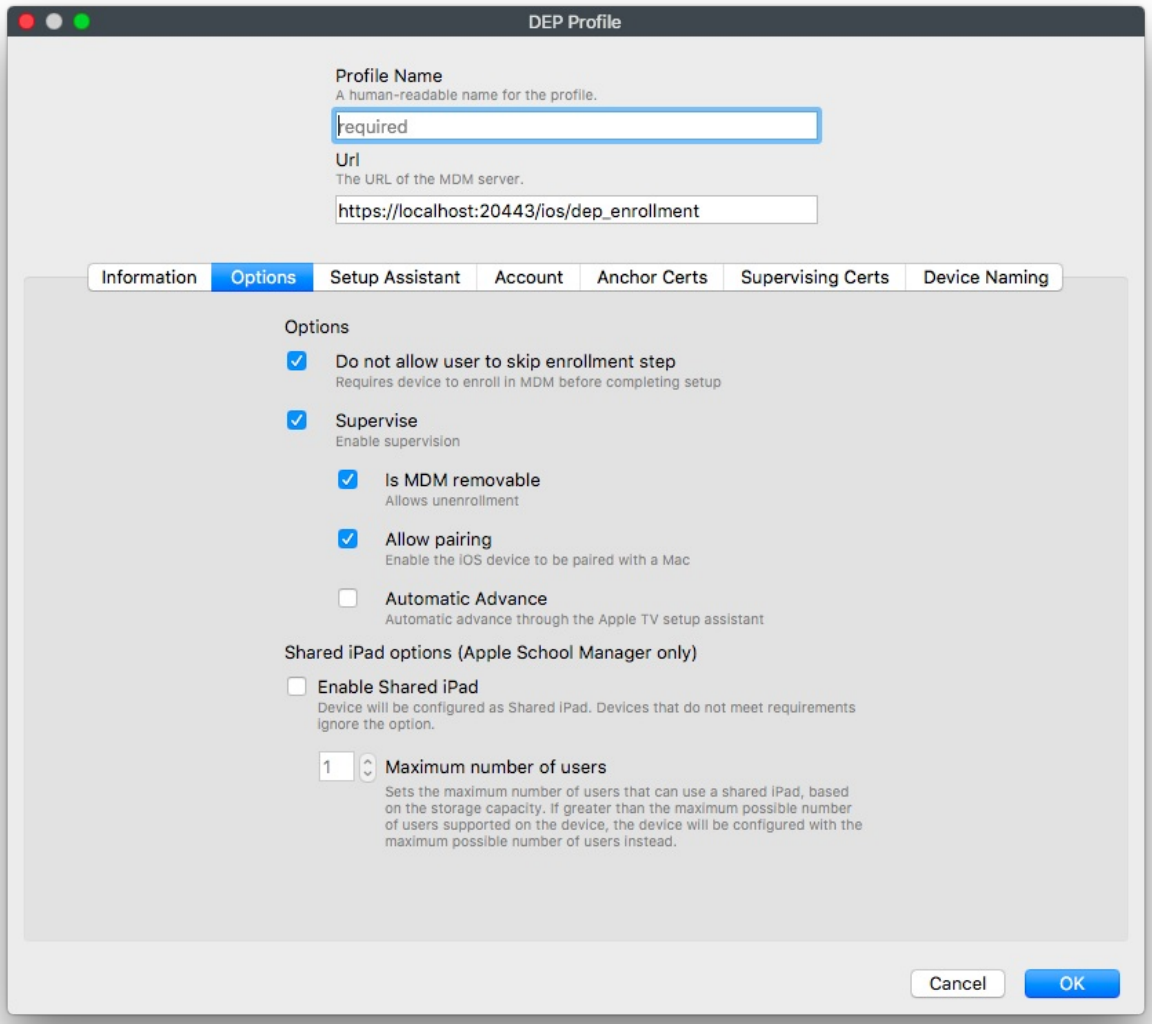


Here is a view of the DEP Profile creation window:

Information

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

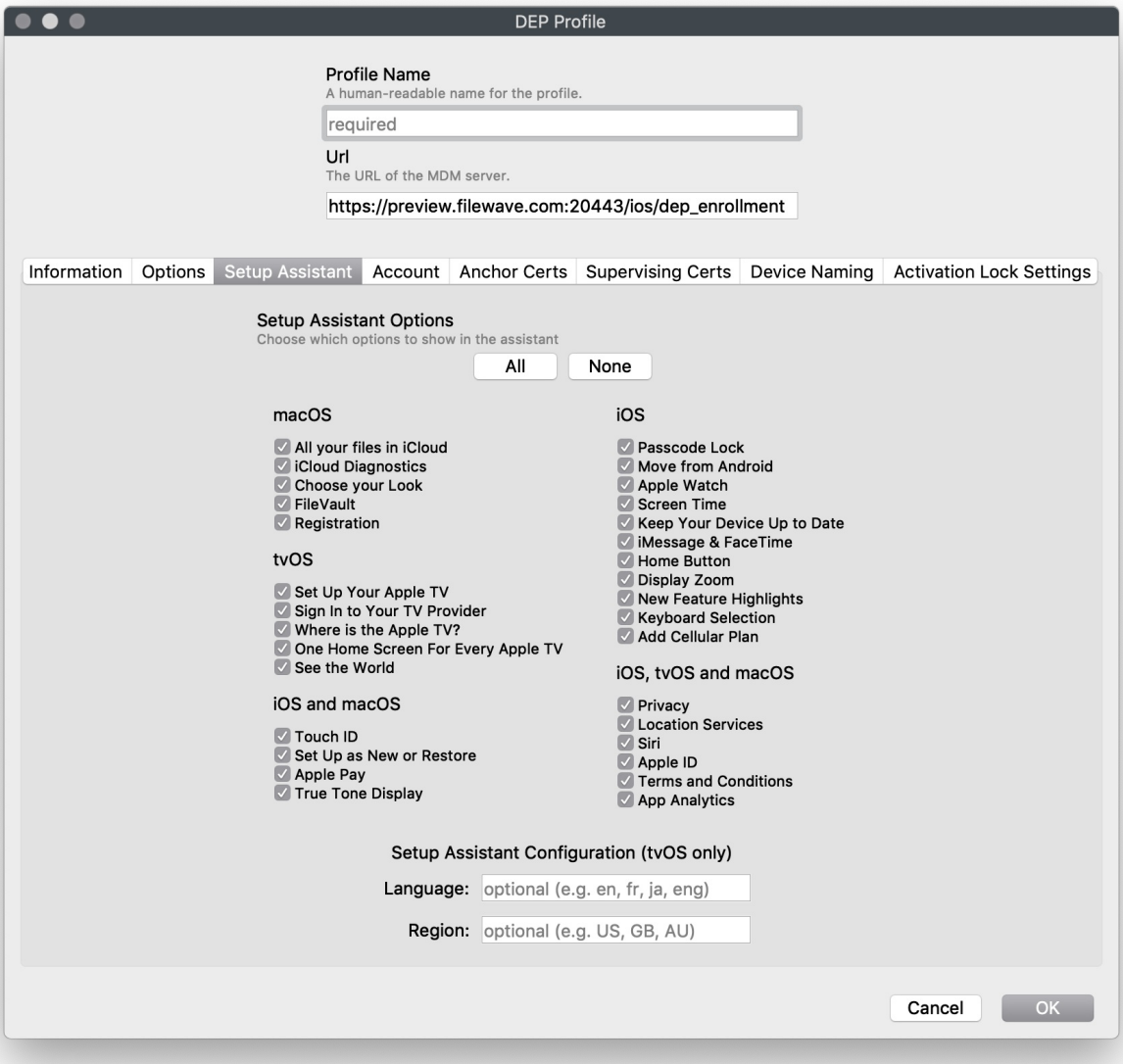
Options



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

- Do not allow user to skip enrollment step - the device must become enrolled in order to complete setup
- Supervise (iOS only) - the device will have supervision enabled
  - Is MDM removable - if unchecked, the MDM profile is locked to the device and cannot be removed by the user through the UI
  - Allow pairing - if checked, the user can pair the device with their own iTunes account to synchronize personal content
  - Automatic Advance - if checked, the Apple TV will automatically advance through setup assistant (If you use the remote on the Apple TV this option will be canceled)
- Enable Shared iPad - Device will be configured as a Shared iPad. Devices that do not meet requirements ignore the option.
  - Maximum number of users - Sets the maximum number of users that can use a shared iPad, based on the storage capacity. If greater than the maximum possible number of users supported on the device, the device will be configured with the maximum possible number of users instead.

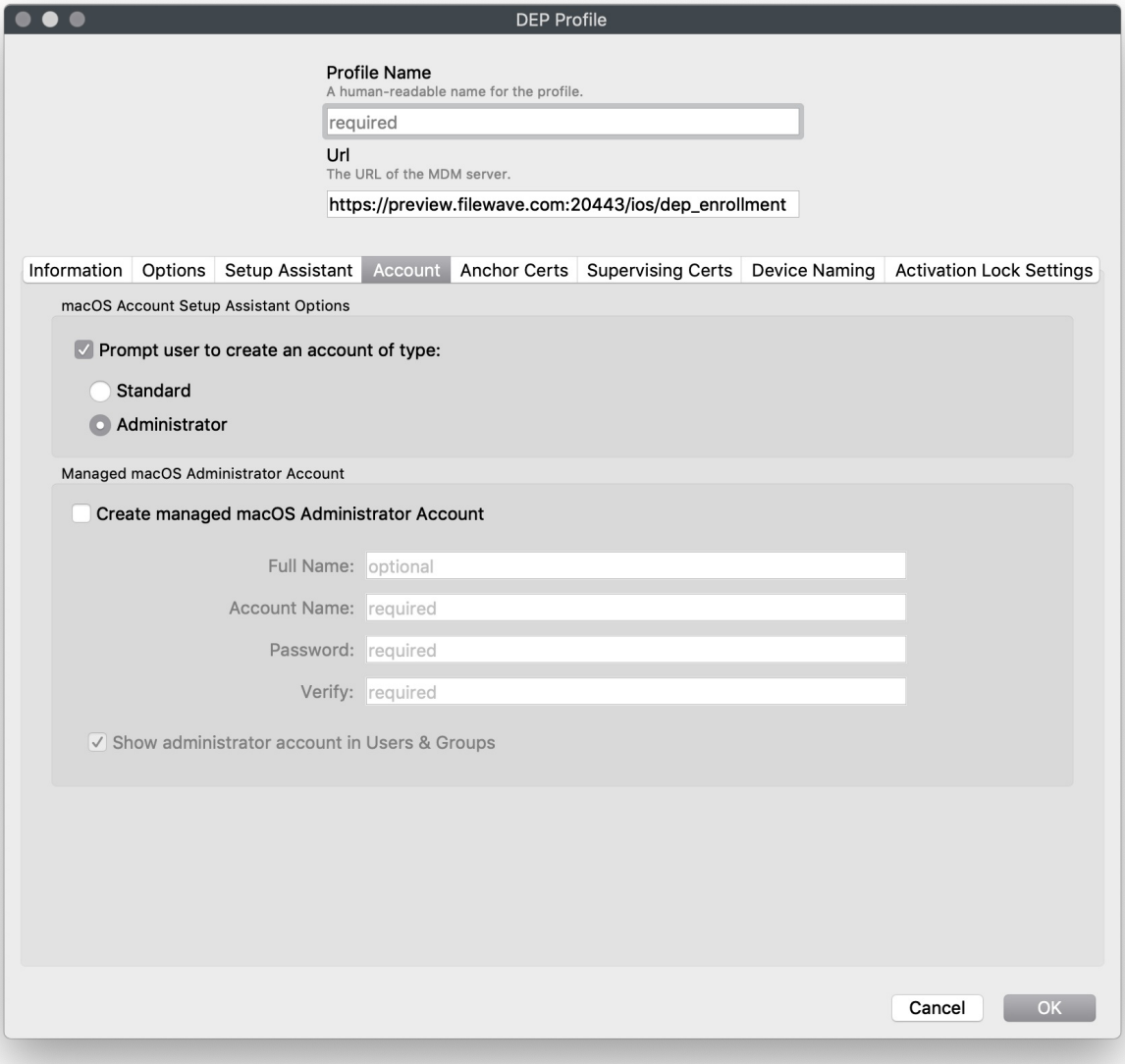
Setup Assistant



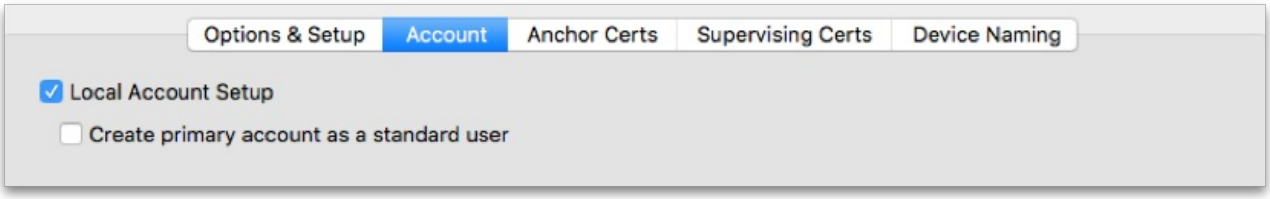
- Skip setup items - this allows the FileWave administrator the ability to configure which portions of the setup assistant are made available to the end user when they configure the device. If none of the items are allowed, then the device must be pre-configured using MDM profiles with all of the appropriate settings to ensure functionality.

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

A feature in DEP is the ability to create a local administrator account in advance of a user being guided through creating their own local account. If you configure this pane with a local administrator account, then the user will be allowed to create a local account of their own; but it will be a non-admin user. The local admin account can be somewhat hidden (the home directory will still be in /Users/ but it will not show up in the Users and Groups System Preference pane).



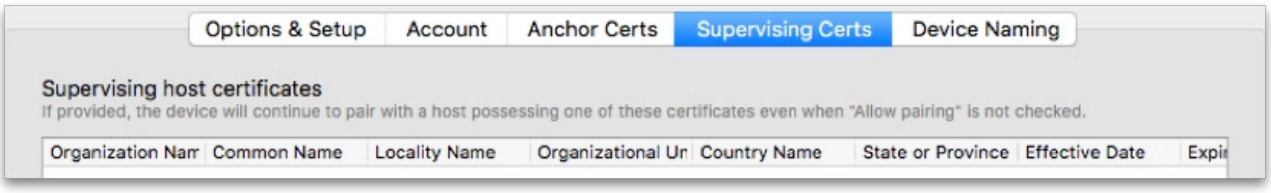
If this pane is configured with only the local account setup, the user setting up the device will be guided through setting up a local administrator account of their own.



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

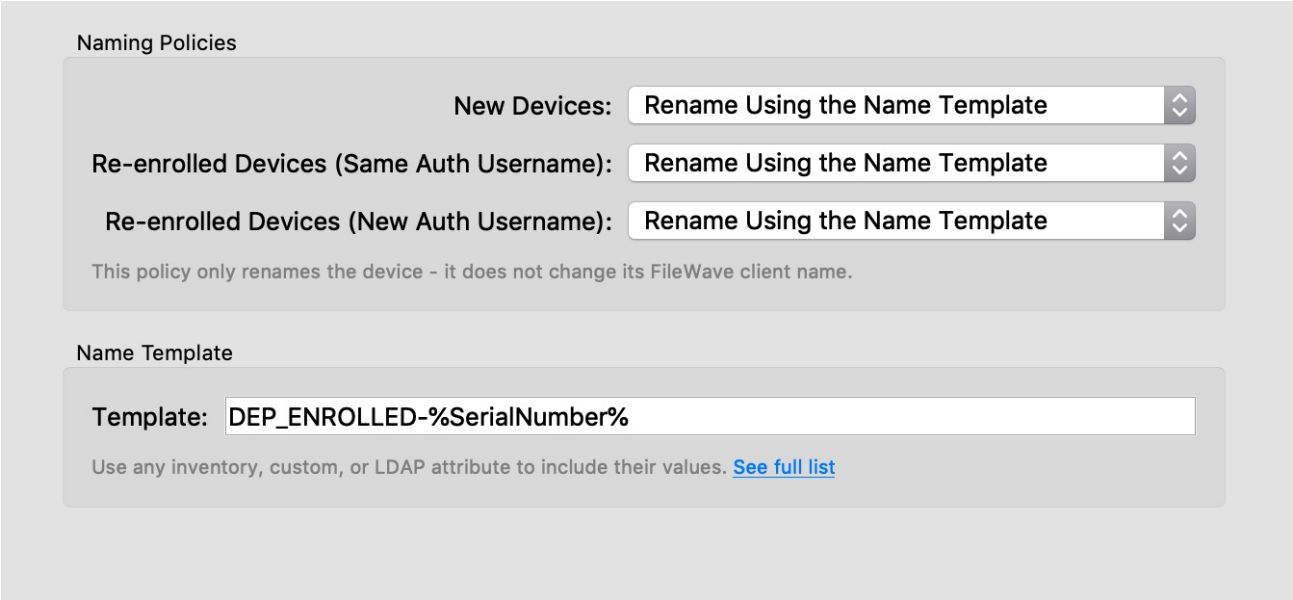
Anchor Certs & Supervising Certs

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



Device Naming

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



See: DEP Naming for more information

Activation Lock

Apple provides an anti-theft feature called Activation Lock. When wiped and activated again, the device is locked and will require an Apple ID credential to be unlocked. FileWave can ease the process by escrowing a bypass code which can be used to bypass iCloud credentials. The code can either be entered manually or automatically, typically just before refreshing the device.

Activation Lock can be against:

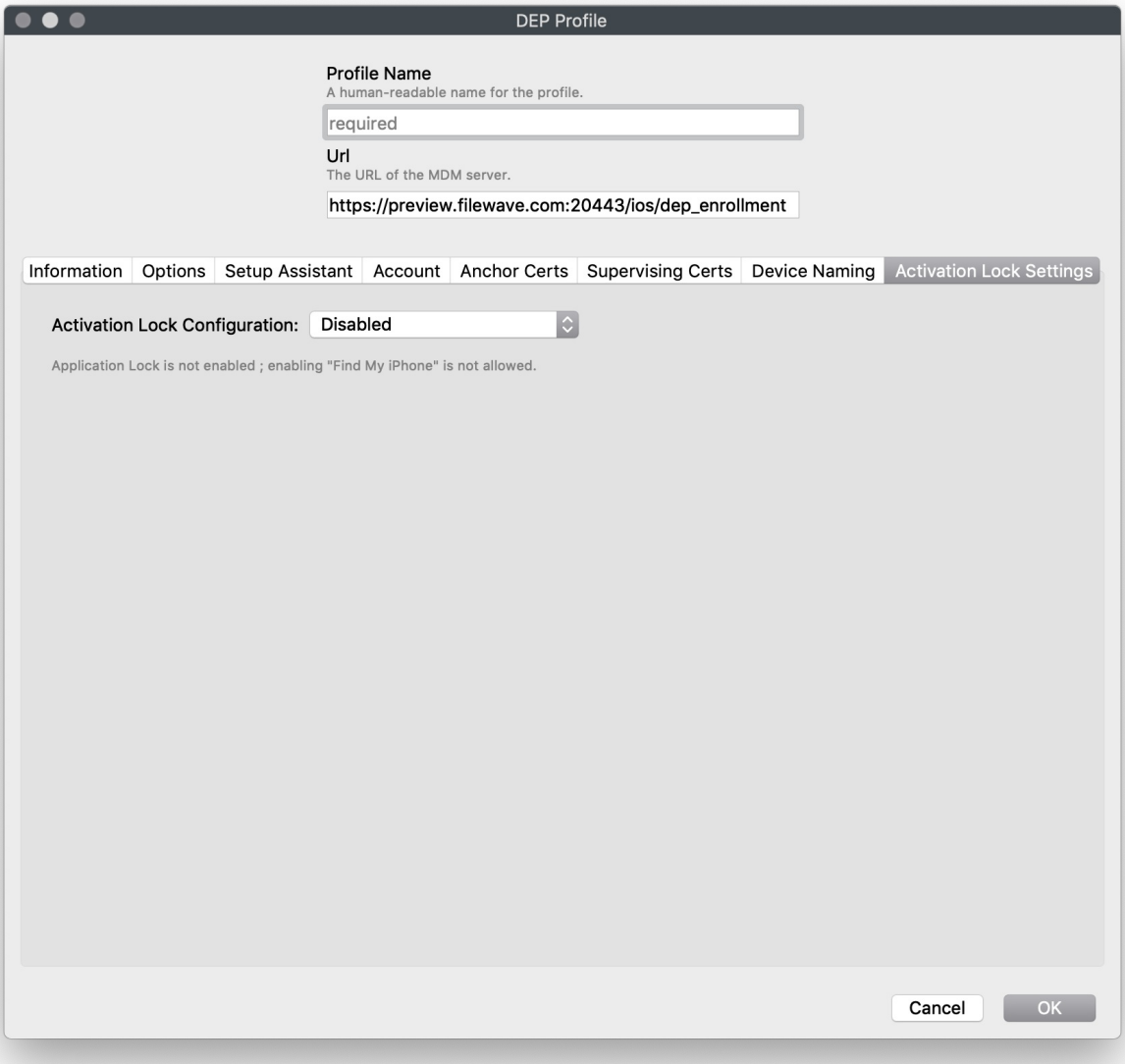
- a normal Apple ID - end user has to log in with iCloud on the device and enable Find My Phone
- a DEP (ASM or ABM) account ; in this case, the corresponding Apple ID is the Apple ID managing the DEP server.

In both cases, FileWave can escrow the key and use it to unlock the device during refresh. You can configure Activation Lock:

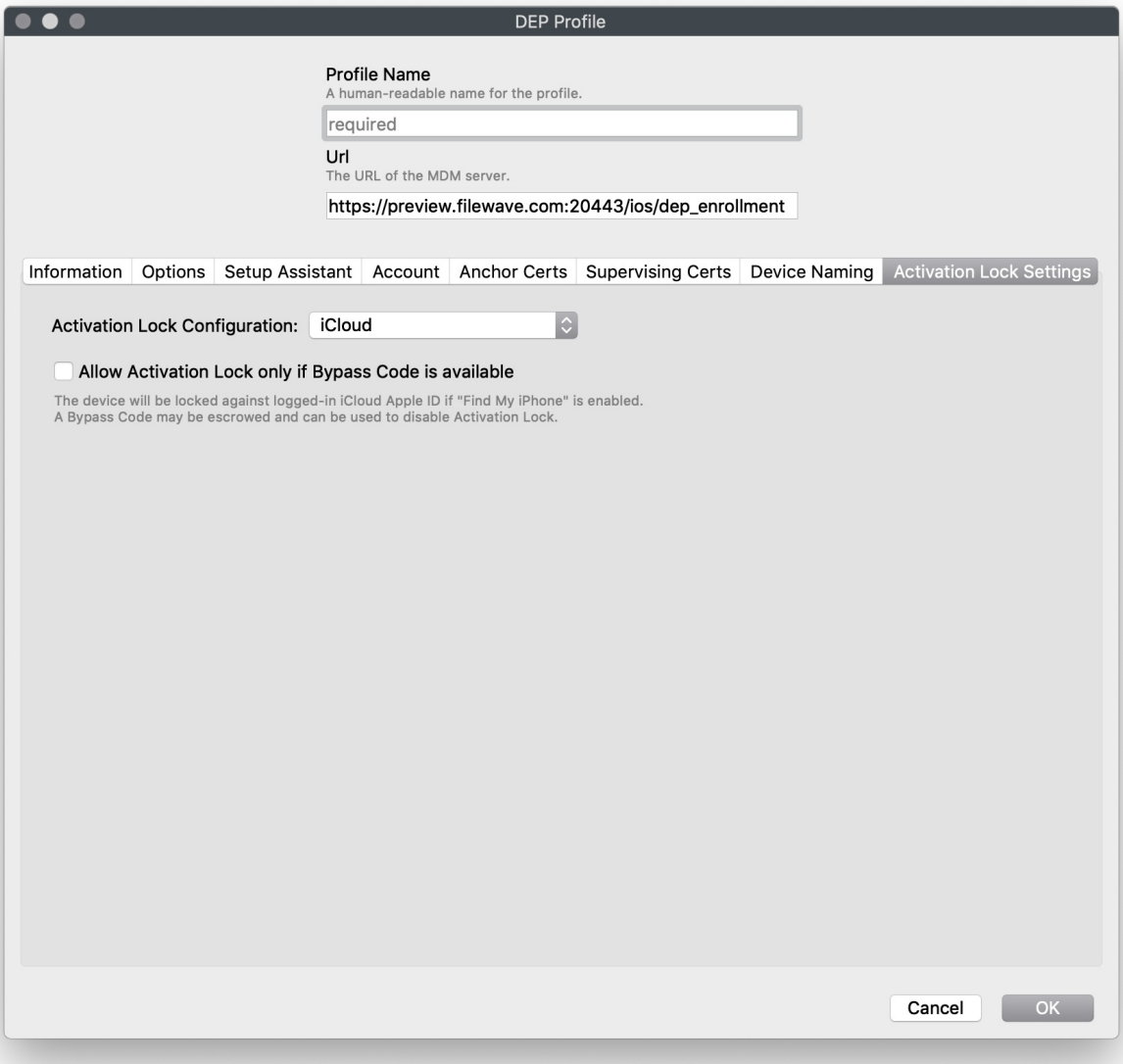
- for each DEP device, at the DEP profile level
- globally, for all non DEP devices

For DEP devices:

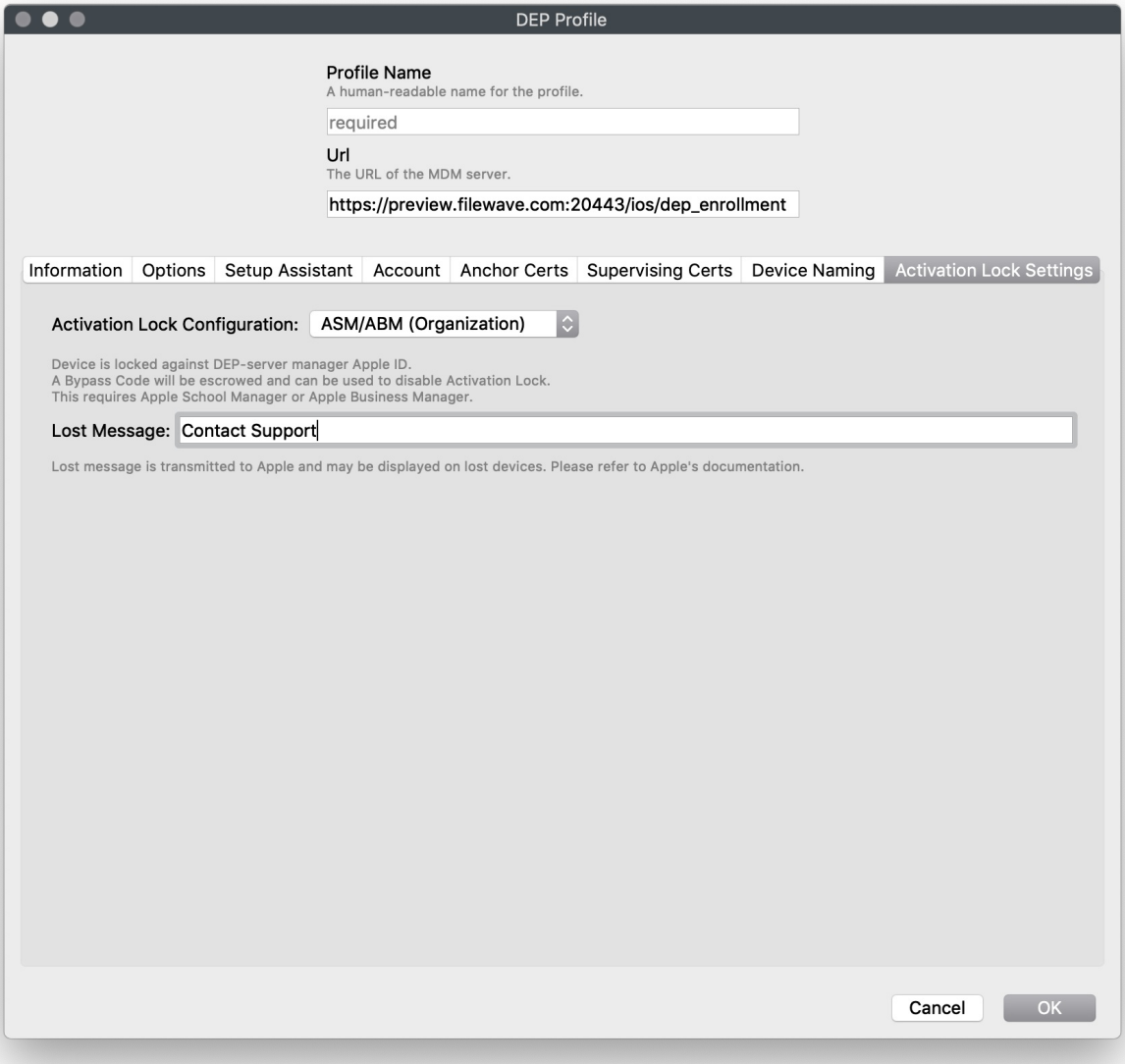
- No lock AKA Disabled


DEP Profile
Profile Name
A human-readable name for the profile.
required
Url
The URL of the MDM server.
https://preview.filewave.com:20443/ios/dep_enrollment
Information
Options
Setup Assistant
Account
Anchor Certs
Supervising Certs
Device Naming
Activation Lock Settings
Activation Lock Configuration:
Disabled
Application Lock is not enabled ; enabling "Find My iPhone" is not allowed.
Cancel
OK

Use iCloud

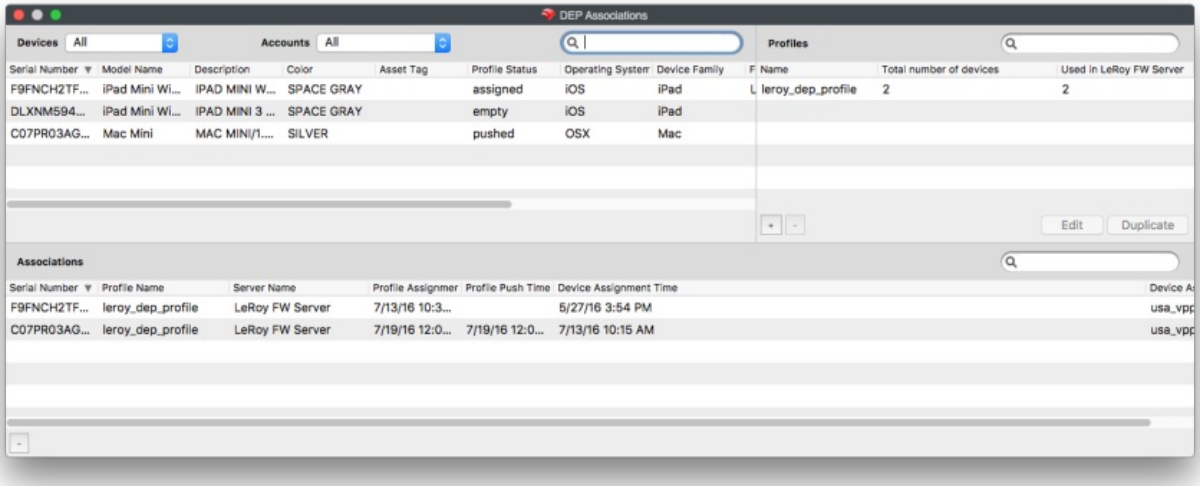


Use your AMS/ABM account



Associations

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



To automate see: Automatically Assign DEP profiles

End Result of DEP associations

The end result of associating DEP profiles to devices is that upon activation, the device will automatically become a FileWave Client with specific setup settings. You can have device Placeholders prepositioned in your FileWave Clients view, assigned to Groups, with Filesets ready to activate as soon as the device checks in.

Revision #5
★Created 12 July 2023 19:00:44 by Josh Levitsky
✎Updated 9 September 2024 09:25:39 by Josh Levitsky