Automated Device Enrollment (ADE)

This was formerly known as the Device Enrollment Program (DEP).

- Apple's Automated Device Enrolment
- Working with Apple’s Device Enrollment Program (DEP)
- Add or Renewing your ADE (DEP) Account Token
- DEP Naming
- Automatically Assign DEP profiles
- Control Await Configuration state (DEP enrolled devices)
- Apple TV Automatic Advance (DEP)
- DEP Notify - How to provide progress visibility during DEP activation (macOS)
- Minimum OS version for enrolling Apple devices via ADE
- Test macOS ADE (DEP) Enrolments with a Virtual Machine
- DEP Troubleshooting
- DEP Forbidden Error

Apple's Automated Device Enrolment

What

From inception known as Device Enrolment Programme (DEP), Apple's Automated Device Enrolment (ADE) is a zero touch enrolment method for Apple devices.

This article aims to cover the generic processes.

When/Why

Typically this process is used with new devices or those erased.

Registration

The basics:

- Devices, purchased from a supplier signed up to Apple's programme, are registered with Apple
- FileWave MDM server is registered with Apple
- Devices are assigned to the FileWave MDM server within the Apple Business or School account: ABM or ASM

Enrolment Profile

Enrolment Profile has options, e.g which Setup Assistant items are shown. When an Enrolment Profile is associated with one or more devices, the Enrolment Profile is sent to Apple; differing Enrolment Profiles may be configured and associated with different devices.

Working with Apple’s Device Enrollment Program (DEP)

How

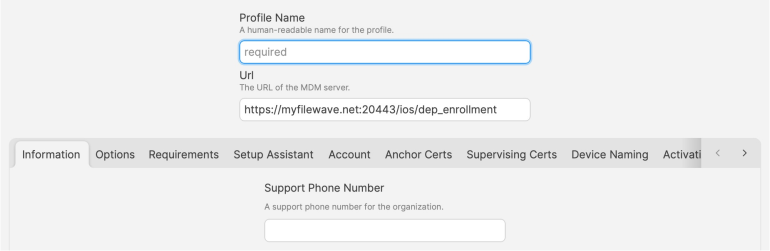
Enrolment Stages

Enrolment Profile delivery

When the device is first connected to a network, the device will initially communicate with Apple. Apple observe the identity of the device and if there is an associated Enrolment Profile with this device, the Profile is sent to the device.

> Once the Enrolment Profile is delivered, it will remain on the device, even if rebooted. Only a subsequent erase of the device will remove the Enrolment Profile and the process be re-triggered from scratch.

A key item in the Enrolment Profile is the MDM Server URL.



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

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

Support Phone Number
A support phone number for the organization.

Check-in

The device reads the MDM Server URL and the enrolment process can then begin.

Authentication

The next requirement from check-in is authentication.

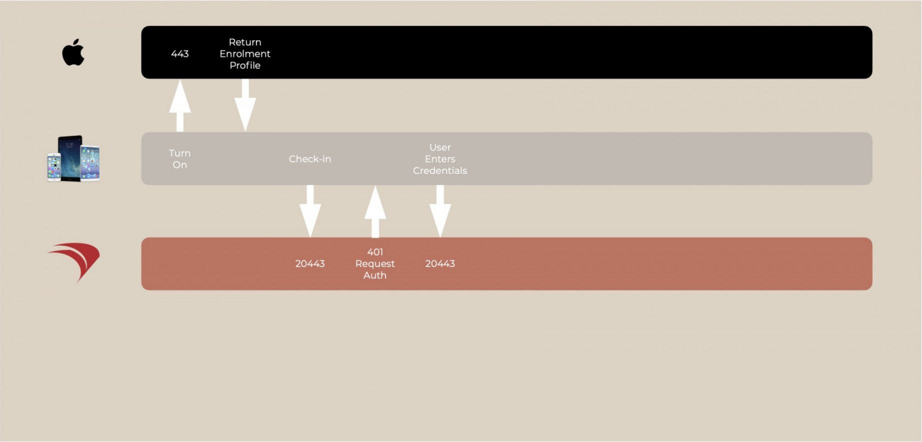
> On initial check-in, FileWave server returns a 401 due to no authentication and then informs the device how to authenticate.

Local Authentication	FileWave is configured with a local username and password encrypted on the FileWave Server (Default)
No Authentication	FileWave Server is configured to allow devices to enrol with no authentication required

No Authentication	FileWave Server is configured to allow devices to enrol with no authentication required
LDAP	An LDAP server, e.g. Active Directory, is configured, allowing directory users to authenticate enrolment
IdP	Okta, Google or Entra users may authenticate enrolment

Local and No authentication are configured through the server command line, LDAP may be configured through FileWave Central, whilst IdP is configured through FileWave Anywhere.

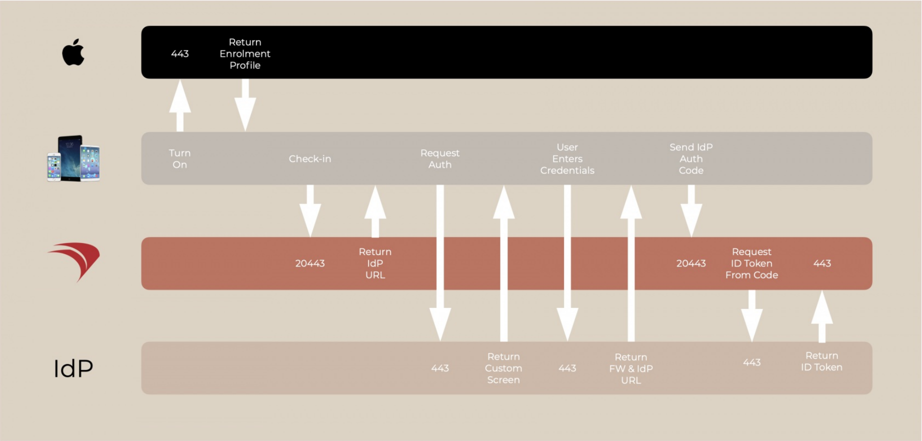
Basic Authentication



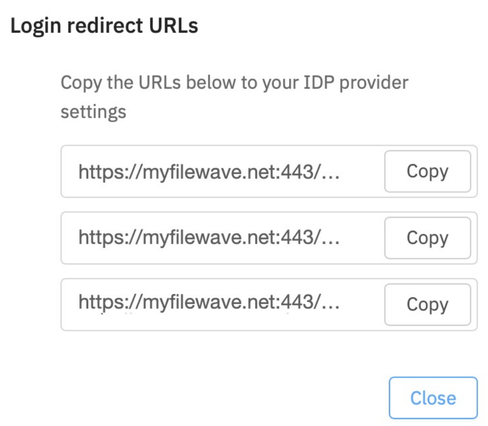
IdP Authentication

IdP requires a special mention here due to the additional steps involved.

FileWave server informs the device with a URL to direct the authentication; the IdP. The IdP custom authentication screen should be presented to the user and on entering details, if successful, the IdP uses the configured redirect, to contact the FileWave server to inform of success.



Redirects provided to IdP for connection with FileWave Server may be viewed from FileWave Anywhere, for example:



Login redirect URLs

Copy the URLs below to your IDP provider settings

https://myfilewave.net:443/…

https://myfilewave.net:443/…

https://myfilewave.net:443/…

FileWave Server informs the IDP where to respond to the FileWave Server once complete. The FileWave returned URL to send on the code from the device will be through port 20443 and includes the auth code as a parameter within the URL.

Federated Authentication

An extension of IdP, Federated Authentication is an offering from Apple, which allows Apple IDs/passwords to be synchronised with an IdP. This is configured within Apple's Management portal; FileWave is not involved with this configuration.

https://support.apple.com/en-gb/guide/apple-business-manager/axmb19317543/web

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.)

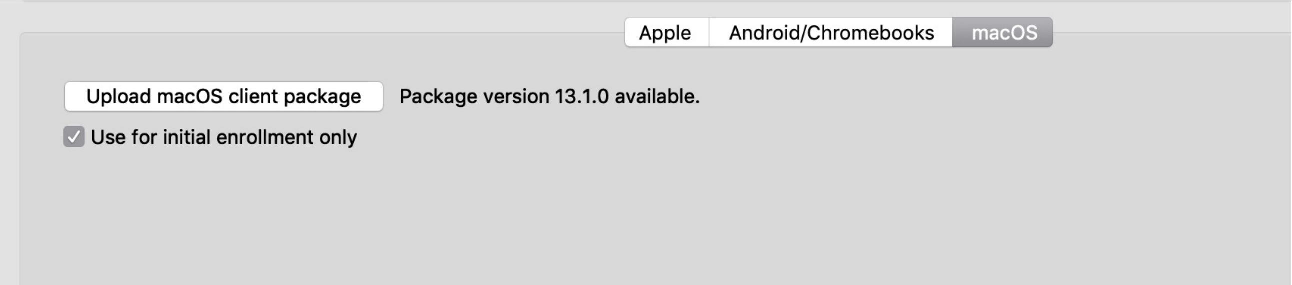
For more information see: https://support.apple.com/en-us/HT204142

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.



Package version 13.1.0 available.

☑ Use for initial enrollment only

"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

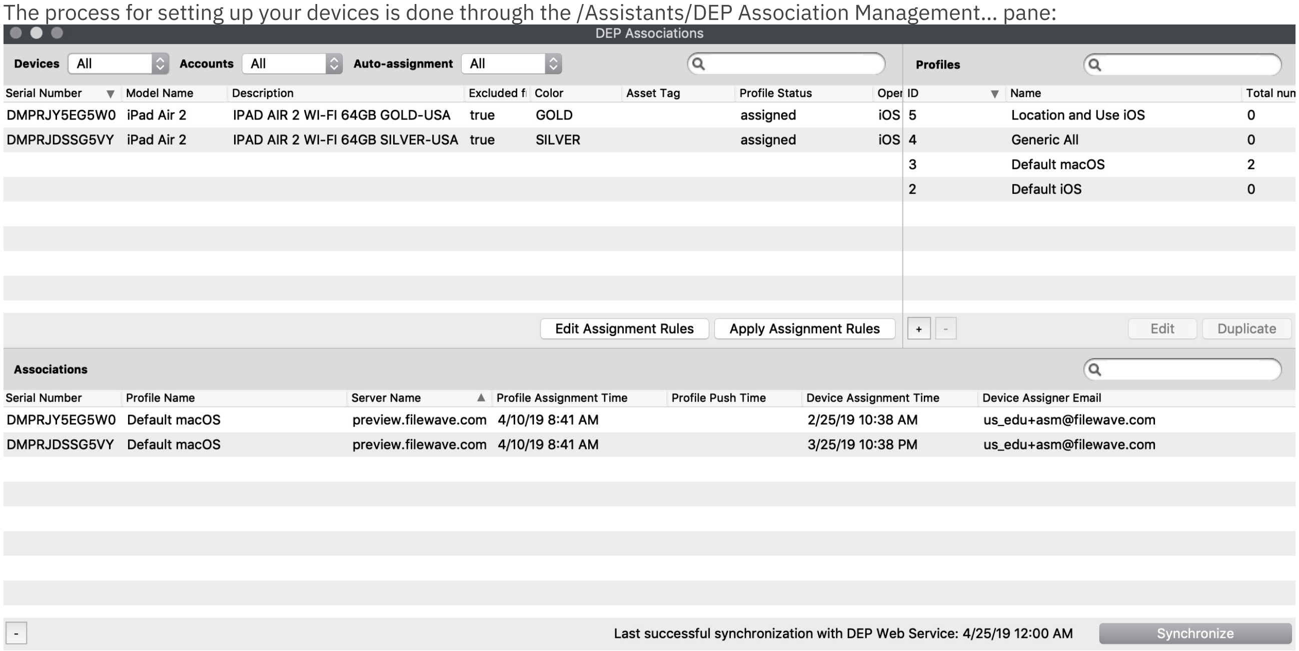
Once you have registered your FileWave Server with the DEP system, you can begin setting up your devices for automatic enrollment and management. You will be able to view a list of your devices along with certain characteristics of those devices, such as model number, color of the device, asset tag information,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



Devices: All
Accounts: All
Auto-assignment: All

Serial Number	Model Name	Description	Excluded f	Color	Asset Tag	Profile Status	Oper
DMPRJY5EG5W0	iPad Air 2	IPAD AIR 2 WI-FI 64GB GOLD-USA	true	GOLD		assigned	iOS
DMPRJDSSG5VY	iPad Air 2	IPAD AIR 2 WI-FI 64GB SILVER-USA	true	SILVER		assigned	iOS

ID	Name	Total nun
5	Location and Use iOS	0
4	Generic All	0
3	Default macOS	2
2	Default iOS	0

Serial Number	Profile Name	Server Name	Profile Assignment Time	Profile Push Time	Device Assignment Time	Device Assigner Email
DMPRJY5EG5W0	Default macOS	preview.filewave.com	4/10/19 8:41 AM		2/25/19 10:38 AM	us_edu+asm@filewave.com
DMPRJDSSG5VY	Default macOS	preview.filewave.com	4/10/19 8:41 AM		3/25/19 10:38 PM	us_edu+asm@filewave.com

Last successful synchronization with DEP Web Service: 4/25/19 12:00 AM

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>
```

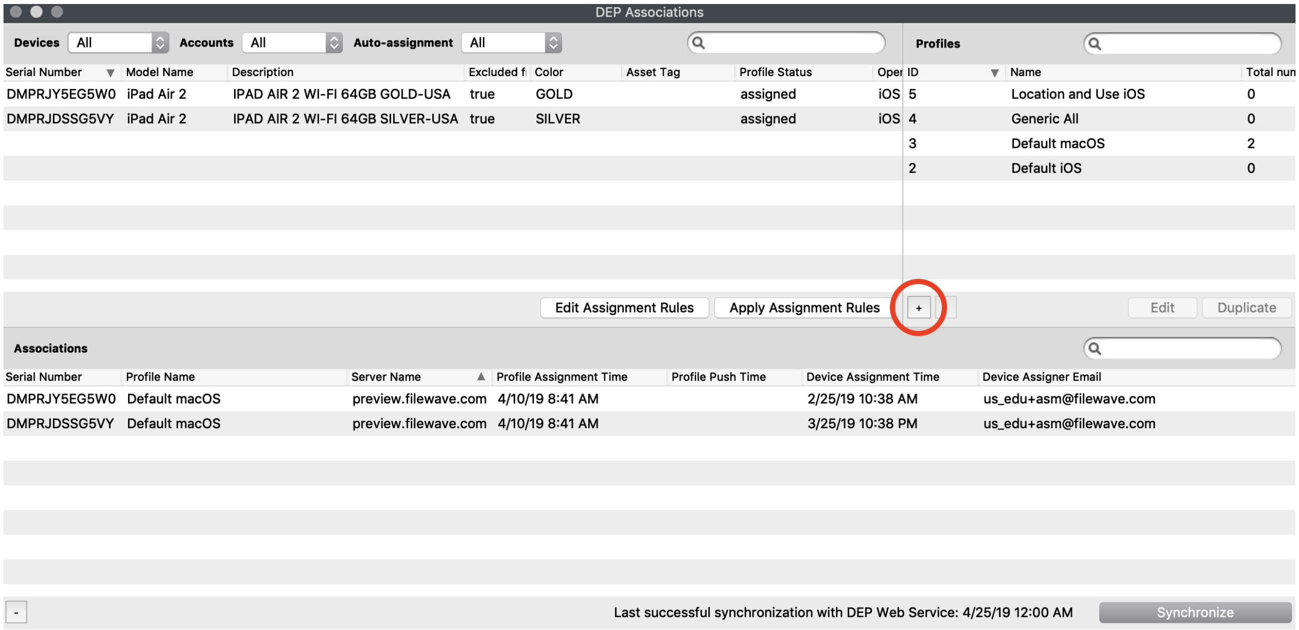
The adddepuser command requires you to provide a user name in the command, and respond to the prompt to add a password for that user, then to confirm the password. This user name and password will be requested by the device during DEP enrollment. These commands are issued on the FileWave MDM server either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



Devices All Accounts All Auto-assignment All

Serial Number	Model Name	Description	Excluded f	Color	Asset Tag	Profile Status	Oper
DMPRJY5EG5W0	iPad Air 2	IPAD AIR 2 WI-FI 64GB GOLD-USA	true	GOLD		assigned	iOS
DMPRJDSSG5VY	iPad Air 2	IPAD AIR 2 WI-FI 64GB SILVER-USA	true	SILVER		assigned	iOS

Profiles

ID	Name	Total num
5	Location and Use iOS	0
4	Generic All	0
3	Default macOS	2
2	Default iOS	0

Associations

Serial Number	Profile Name	Server Name	Profile Assignment Time	Profile Push Time	Device Assignment Time	Device Assigner Email
DMPRJY5EG5W0	Default macOS	preview.filewave.com	4/10/19 8:41 AM		2/25/19 10:38 AM	us_edu+asm@filewave.com
DMPRJDSSG5VY	Default macOS	preview.filewave.com	4/10/19 8:41 AM		3/25/19 10:38 PM	us_edu+asm@filewave.com

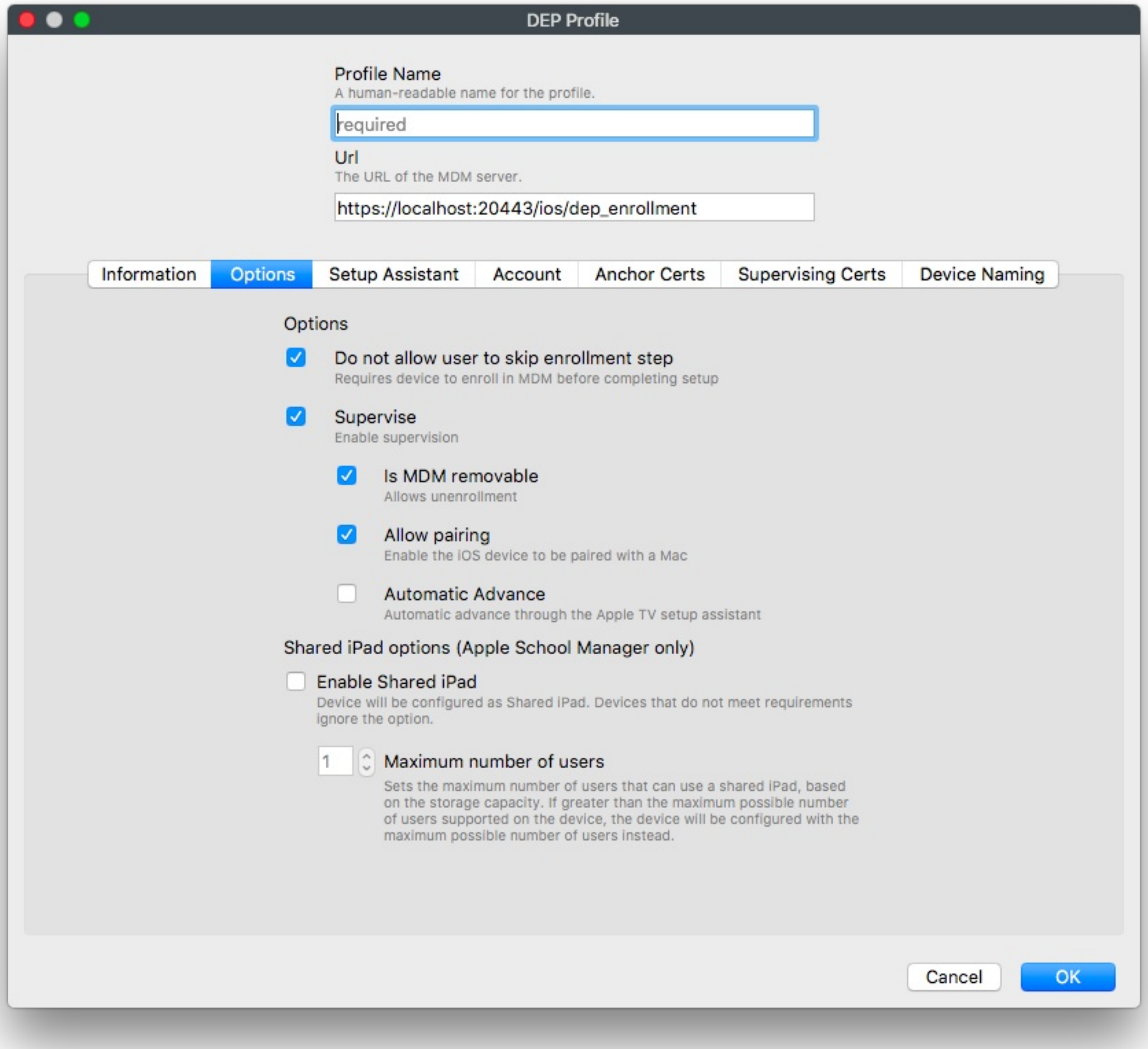
Last successful synchronization with DEP Web Service: 4/25/19 12:00 AM

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



DEP Profile

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

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

Options

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

☑ Supervise
Enable supervision

☑ Is MDM removable
Allows unenrollment

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

□ Automatic Advance
Automatic advance through the Apple TV setup assistant

Shared iPad options (Apple School Manager only)

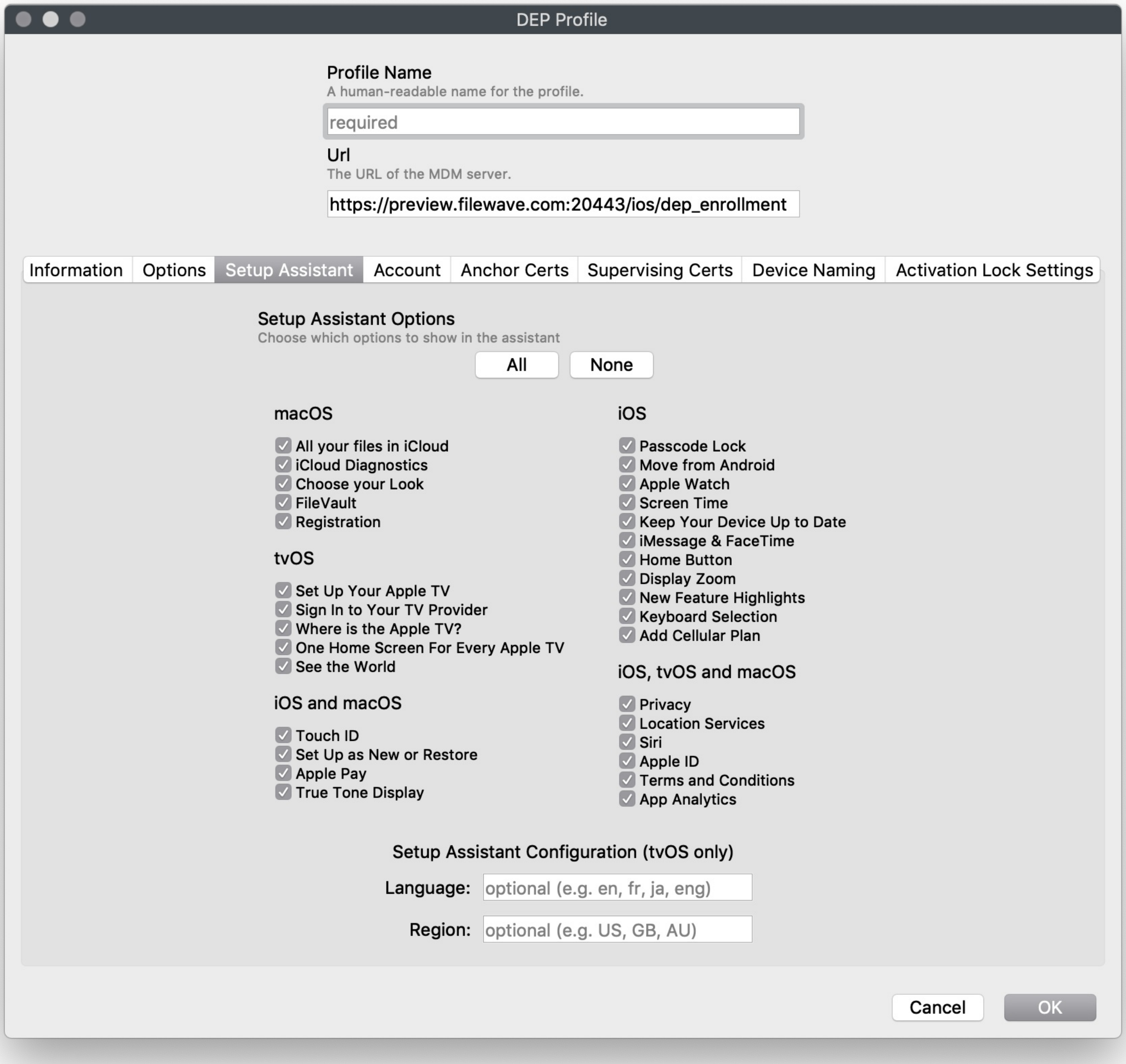
□ Enable Shared iPad
Device will be configured as Shared iPad. Devices that do not meet requirements ignore the option.

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

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

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



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

Setup Assistant Options
Choose which options to show in the assistant

macOS

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

tvOS

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

iOS and macOS

☑ Touch ID
☑ Set Up as New or Restore
☑ Apple Pay
☑ True Tone Display

iOS

☑ Passcode Lock
☑ Move from Android
☑ Apple Watch
☑ Screen Time
☑ Keep Your Device Up to Date
☑ iMessage & FaceTime
☑ Home Button
☑ Display Zoom
☑ New Feature Highlights
☑ Keyboard Selection
☑ Add Cellular Plan

iOS, tvOS and macOS

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

Setup Assistant Configuration (tvOS only)

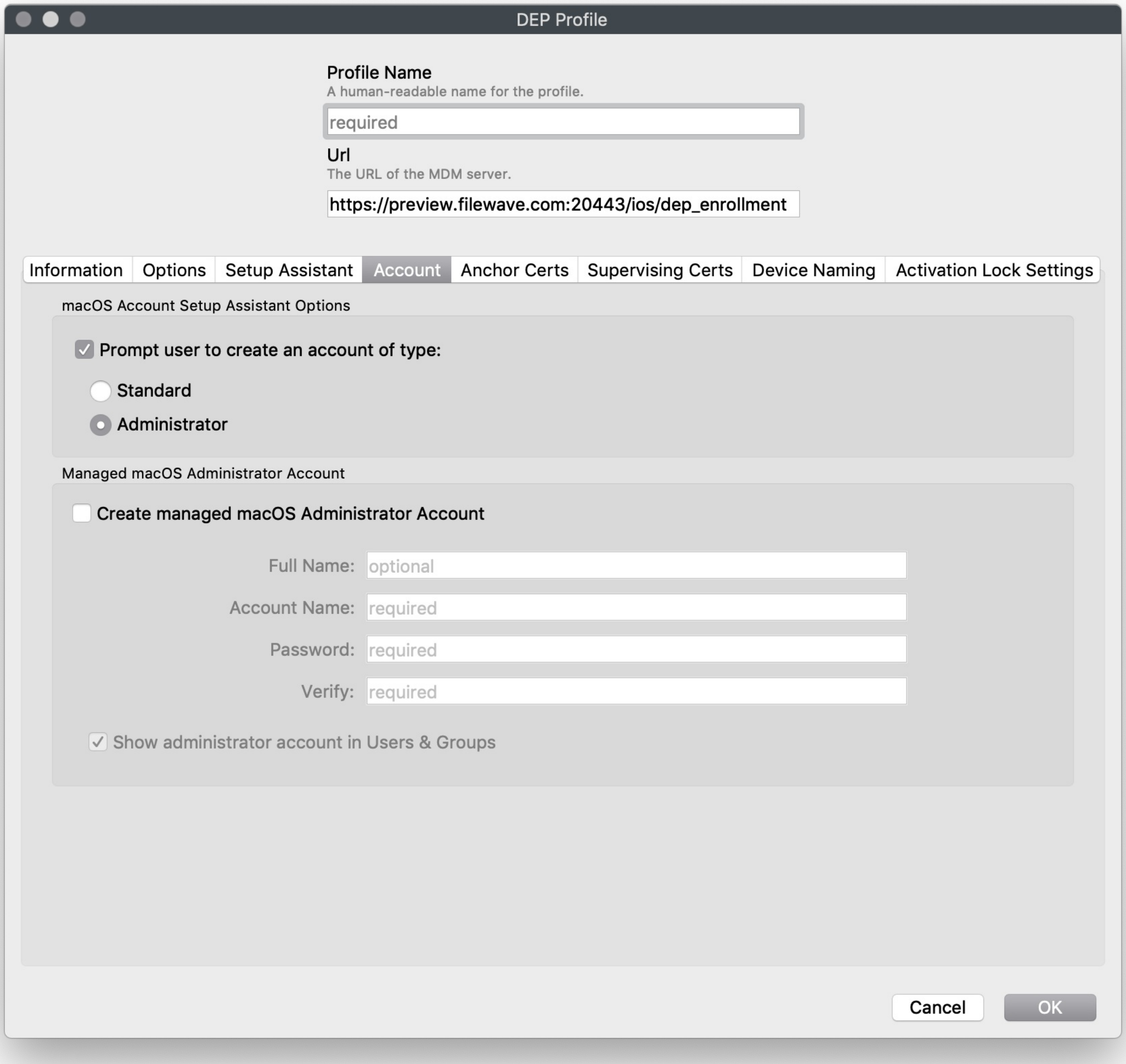
Language: optional (e.g. en, fr, ja, eng)

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

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

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

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



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

macOS Account Setup Assistant Options

☑ Prompt user to create an account of type:

○ Standard

● Administrator

Managed macOS Administrator Account

□ Create managed macOS Administrator Account

Full Name: optional

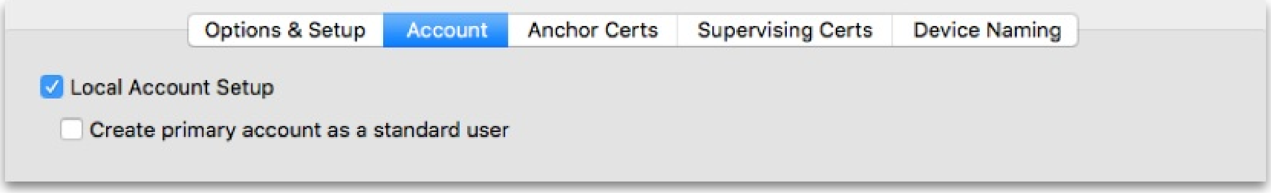
Account Name: required

Password: required

Verify: required

☑ Show administrator account in Users & Groups

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



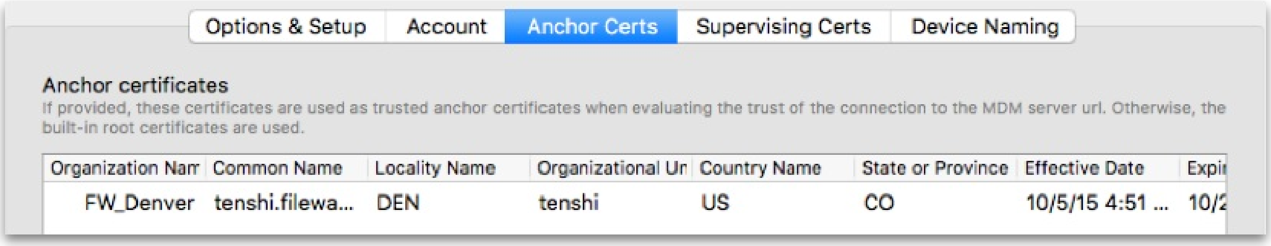
☑ Local Account Setup

□ Create primary account as a standard user

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

Anchor Certs & Supervising Certs

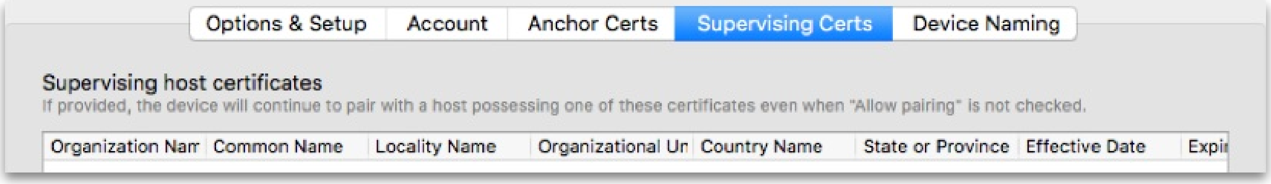
The "Certs" tabs are for adding the necessary certificates to the device to allow trusted connections and specialized pairing permissions. The FileWave MDM server certificate is automatically added to the Anchor Certs list.



Anchor certificates

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

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



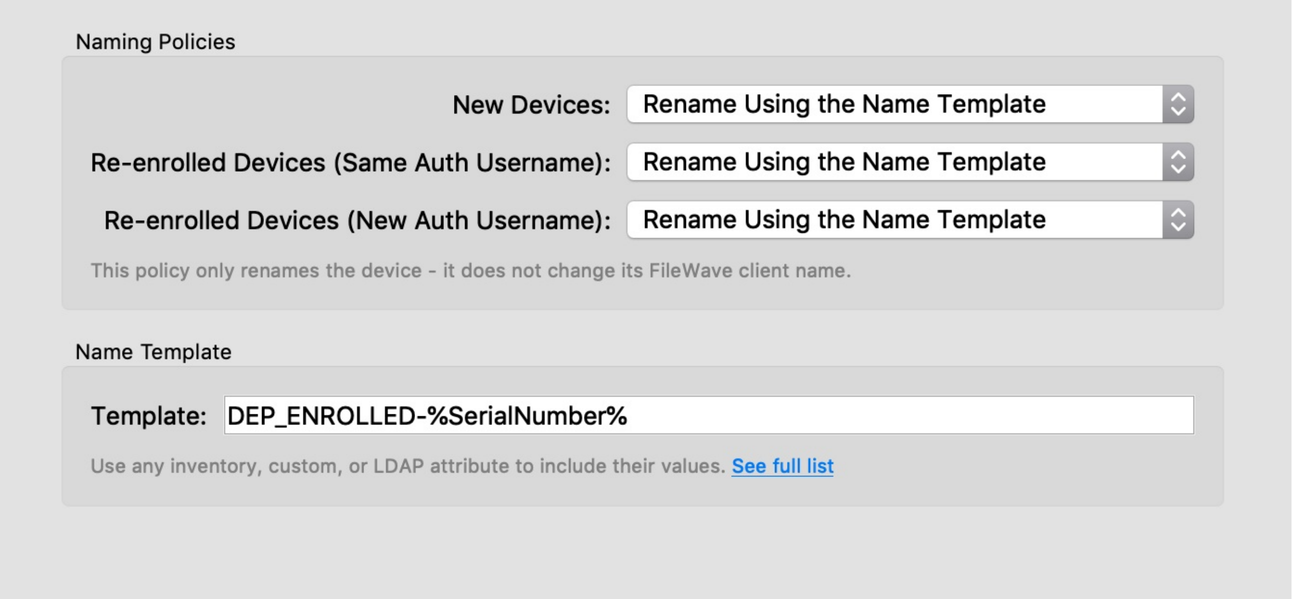
Supervising host certificates

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

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

Device Naming

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



Naming Policies

New Devices: Rename Using the Name Template

Re-enrolled Devices (Same Auth Username): Rename Using the Name Template

Re-enrolled Devices (New Auth Username): Rename Using the Name Template

This policy only renames the device - it does not change its FileWave client name.

Name Template

Template: DEP_ENROLLED-%SerialNumber%

Use any inventory, custom, or LDAP attribute to include their values. See full list

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:

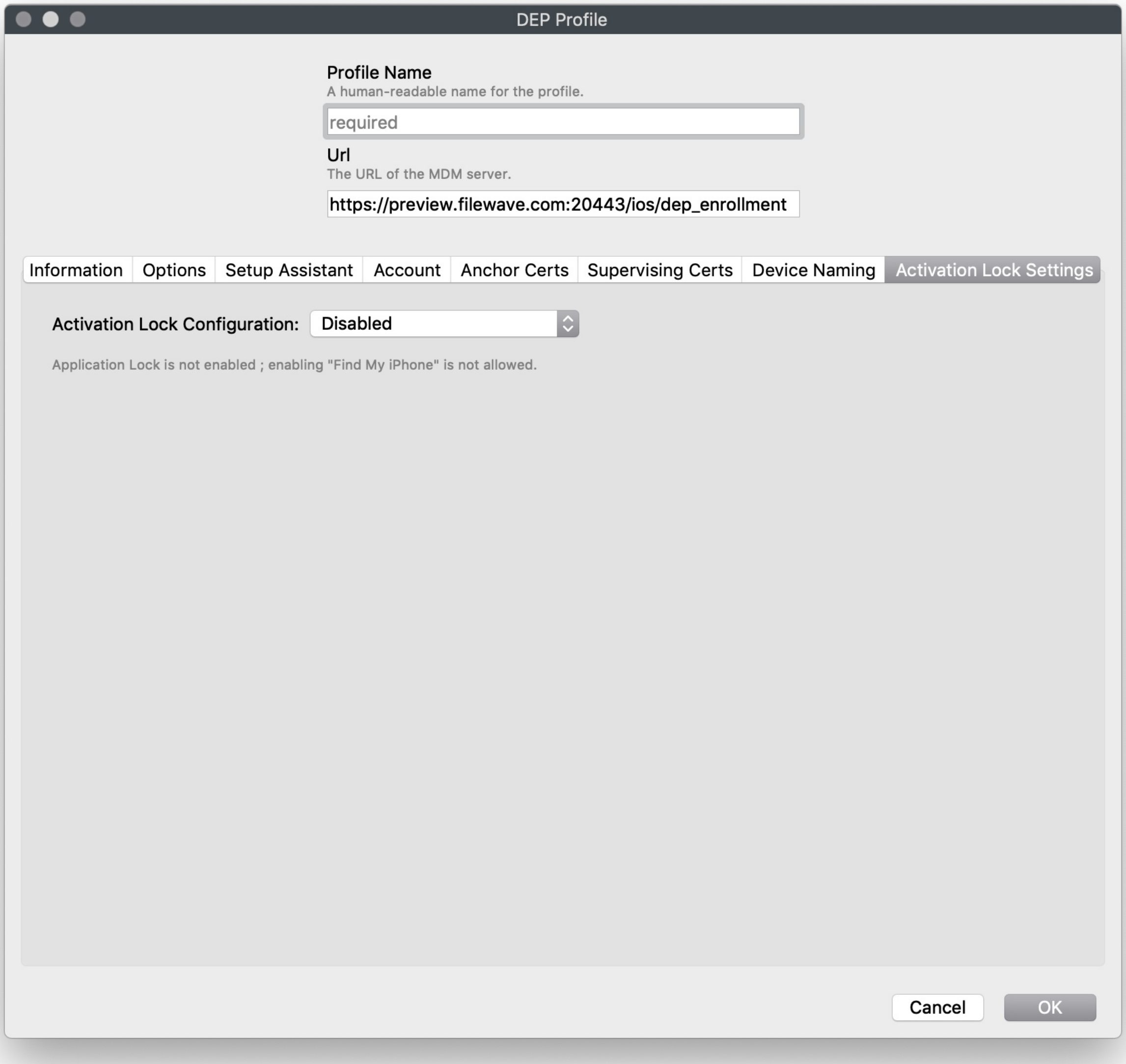
- a normal Apple ID - end user has to log in with iCloud on the device and enable Find My Phone
- a DEP (ASM or ABM) account ; in this case, the corresponding Apple ID is the Apple ID managing the DEP server.

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



Profile Name

A human-readable name for the profile.

required

Url

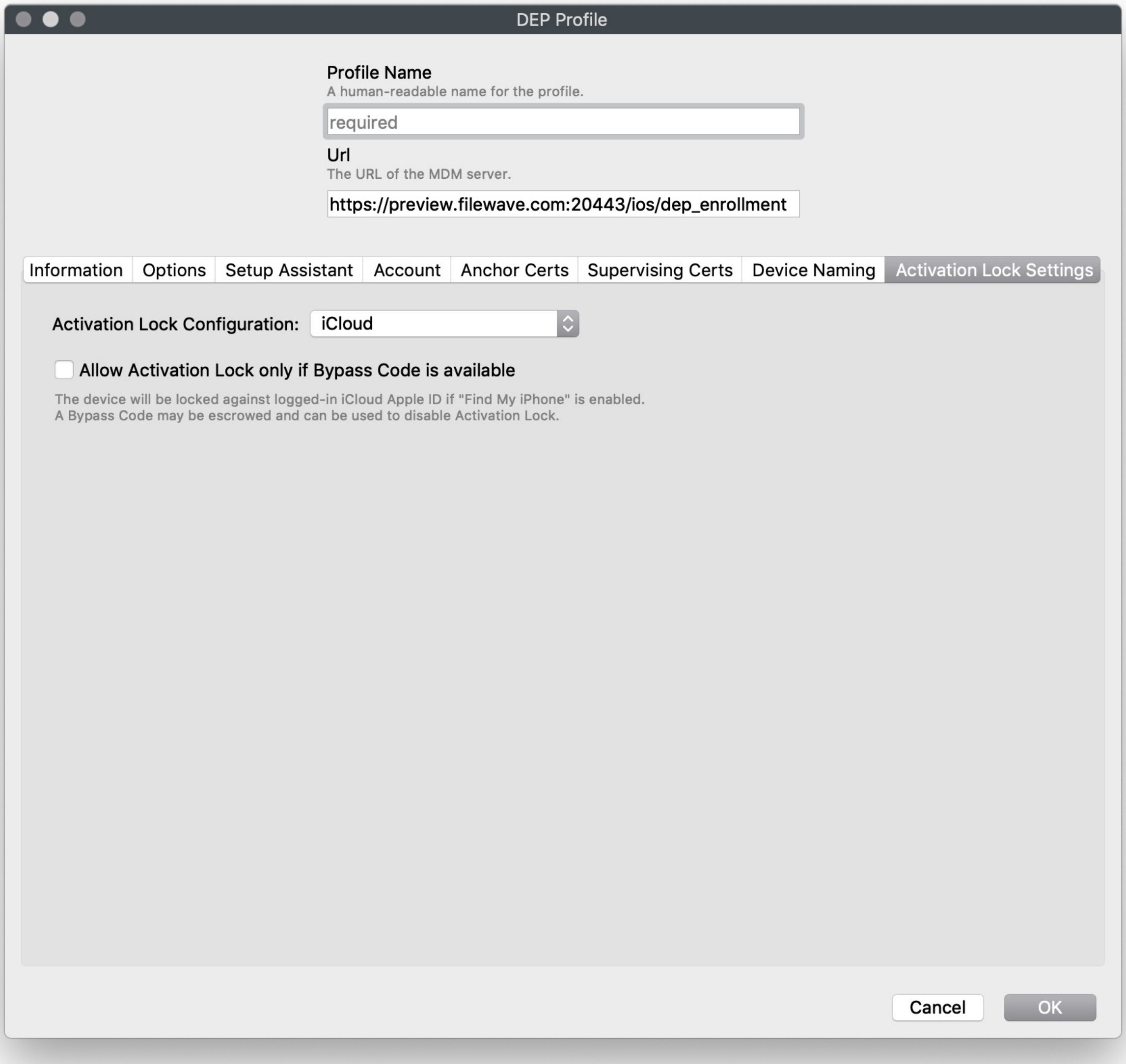
The URL of the MDM server.

https://preview.filewave.com:20443/ios/dep_enrollment

Activation Lock Configuration: Disabled

Application Lock is not enabled ; enabling "Find My iPhone" is not allowed.

Use iCloud



Profile Name

A human-readable name for the profile.

Url

The URL of the MDM server.

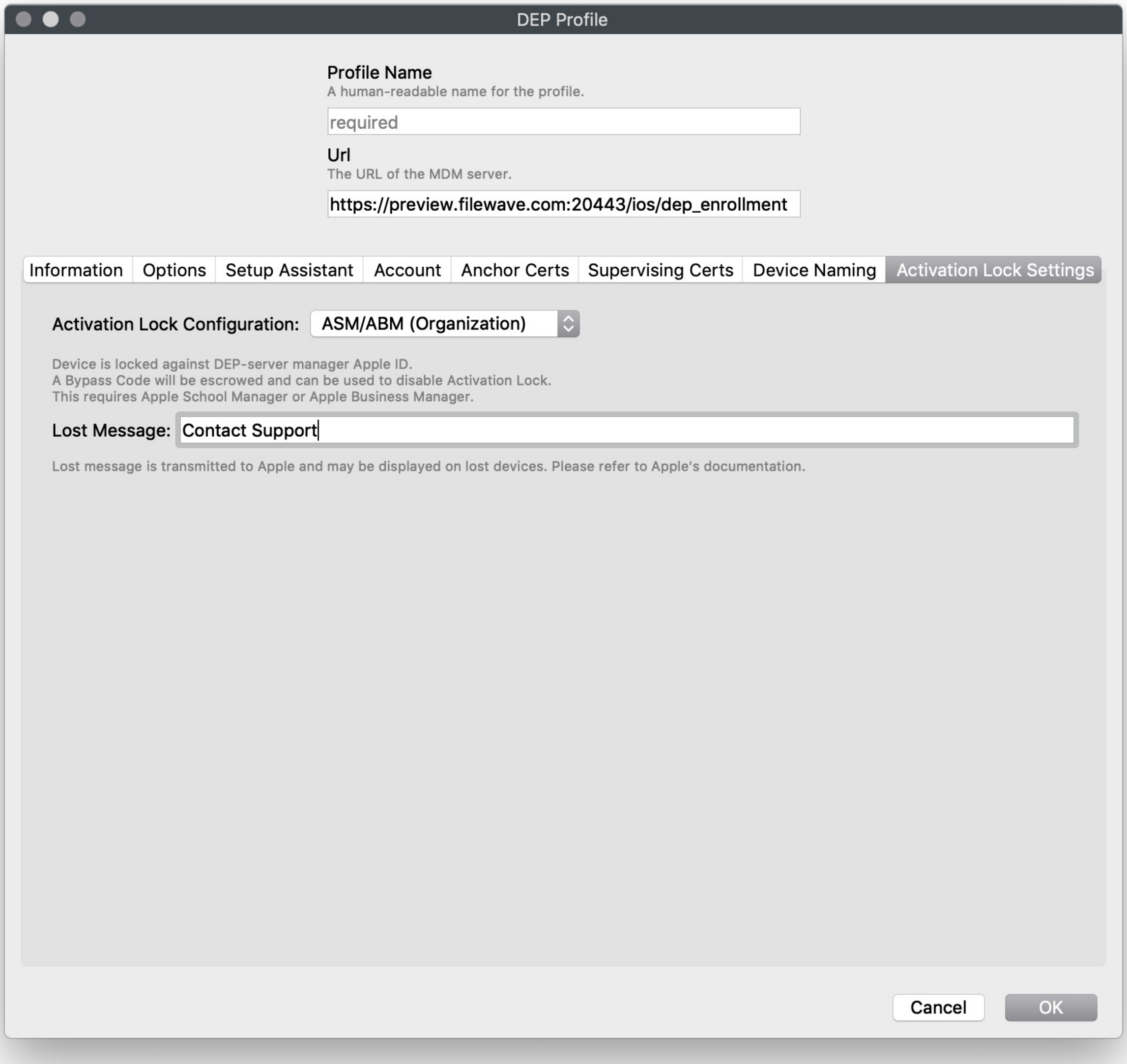
https://preview.filewave.com:20443/ios/dep_enrollment

Activation Lock Configuration: iCloud

□ Allow Activation Lock only if Bypass Code is available

The device will be locked against logged-in iCloud Apple ID if "Find My iPhone" is enabled.
A Bypass Code may be escrowed and can be used to disable Activation Lock.

Use your AMS/ABM account



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

Activation Lock Configuration: ASM/ABM (Organization)

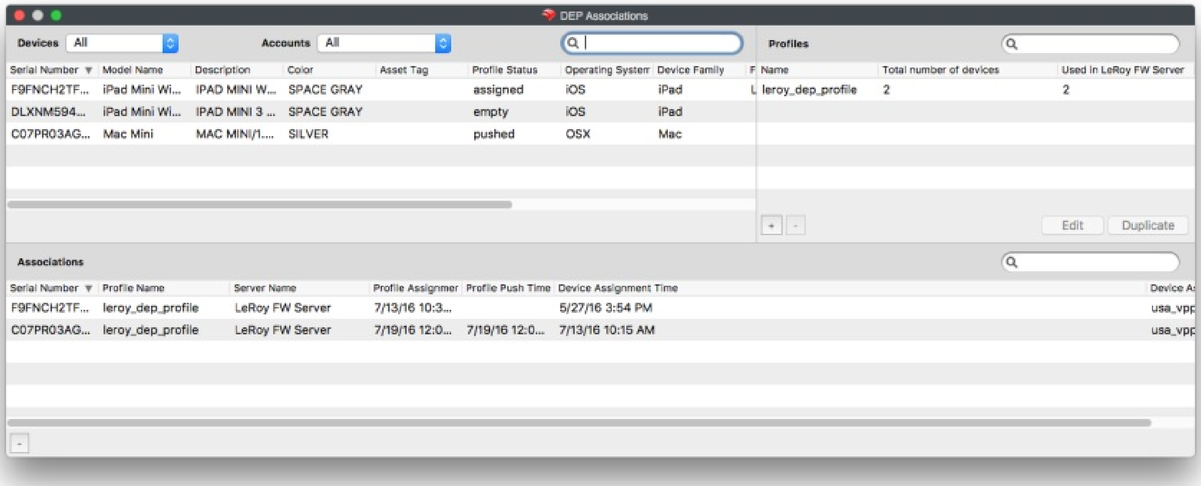
Device is locked against DEP-server manager Apple ID.
A Bypass Code will be escrowed and can be used to disable Activation Lock.
This requires Apple School Manager or Apple Business Manager.

Lost Message: Contact Support

Lost message is transmitted to Apple and may be displayed on lost devices. Please refer to Apple's documentation.

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.



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

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

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

ℹ 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.

Add or Renewing your ADE (DEP) Account Token

Description

DEP is the optimal way to enroll your Apple devices. DEP enrollment is required for countless features and management tools. Once added, you will need to renew your DEP token every year.

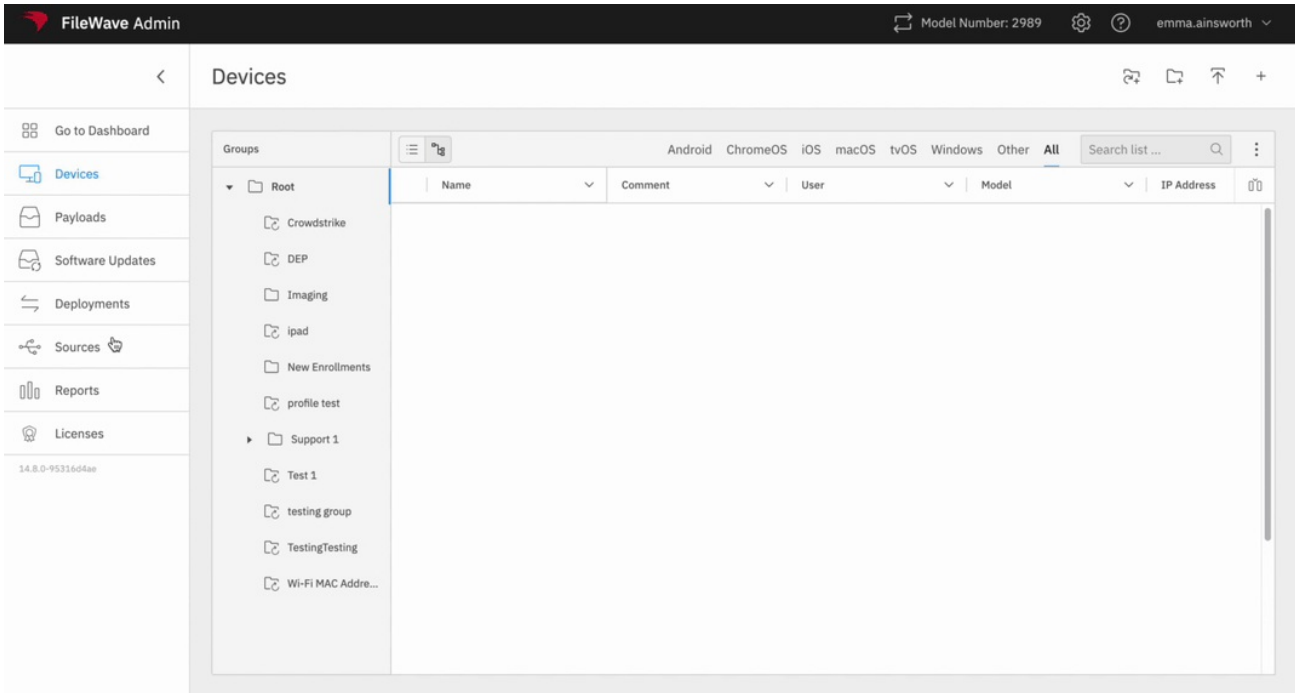
> If you're renewing your token, it's not necessary to re-upload the server certificate (steps 1, 2, 5 & 6) each time unless the cert has changed or you are receiving a FORBIDDEN error when syncing DEP.

Step-by-step guide

1. Download the DEP Certificate from FileWave Admin
2. Save the certificate "FileWave DEP" to your desktop.

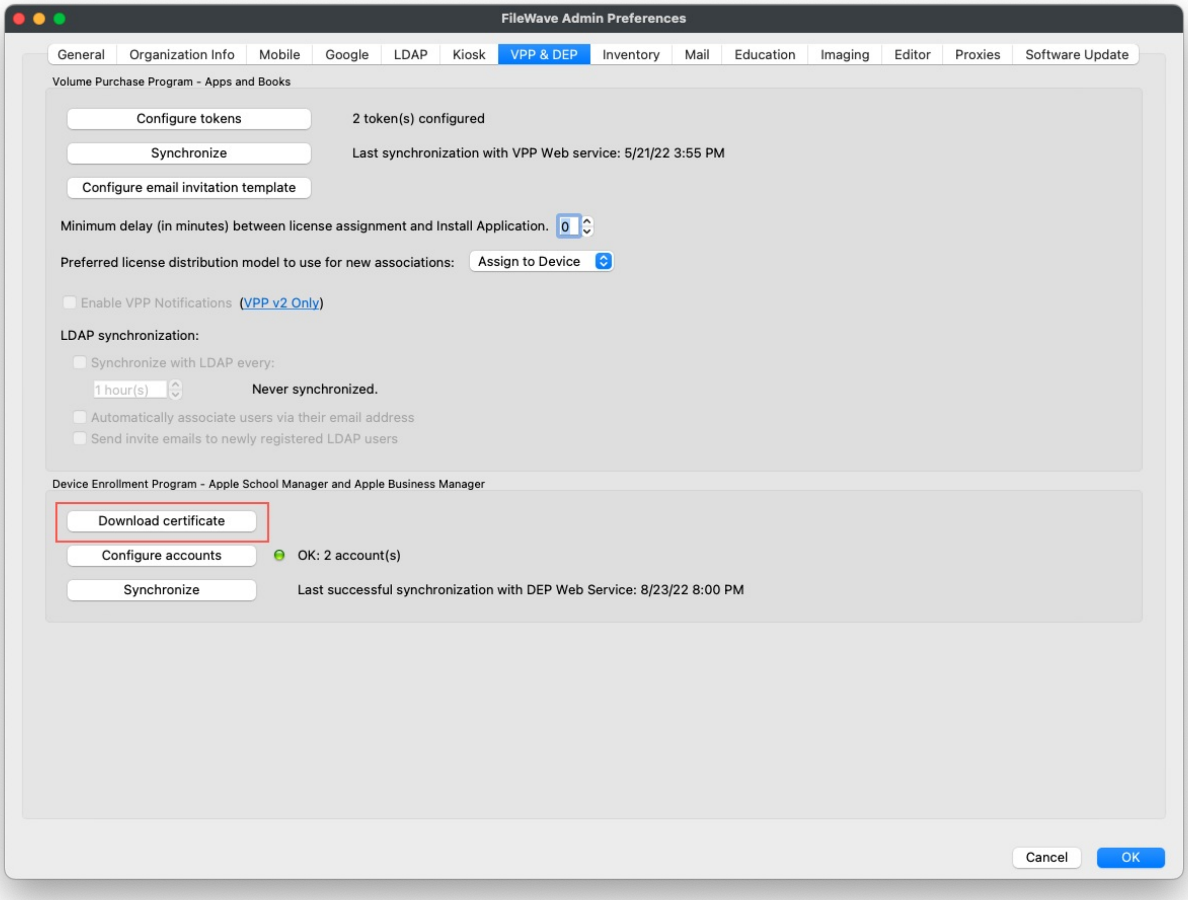
FileWave Anywhere

Sources > DEP Accounts > '+' > Download



FileWave Central

Preferences > VPP & DEP



Volume Purchase Program - Apps and Books

2 token(s) configured

Last synchronization with VPP Web service: 5/21/22 3:55 PM

Minimum delay (in minutes) between license assignment and Install Application. 0

Preferred license distribution model to use for new associations: Assign to Device

□ Enable VPP Notifications (VPP v2 Only)

LDAP synchronization:

□ Synchronize with LDAP every:

1 hour(s) Never synchronized.

□ Automatically associate users via their email address

□ Send invite emails to newly registered LDAP users

Device Enrollment Program - Apple School Manager and Apple Business Manager

● OK: 2 account(s)

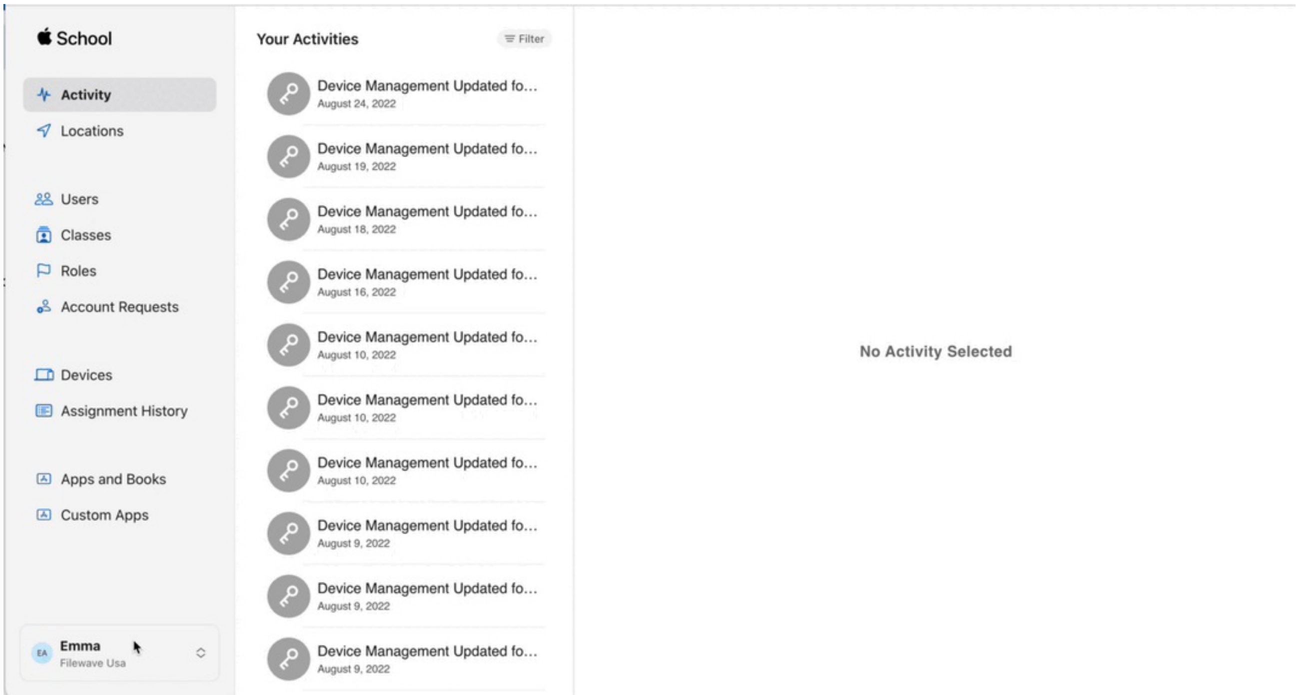
Last successful synchronization with DEP Web Service: 8/23/22 8:00 PM

3. Go to the relevant Apple DEP site, school.apple.com or business.apple.com

4. Once signed in, go to Preferences under your account name in the bottom left of ASM/ABM

5. Select the MDM Server that needs to be renewed and click edit

6. Under MDM Server settings, 'Upload New' MDM certificate



Device Management Updated fo...
August 24, 2022

Device Management Updated fo...
August 19, 2022

Device Management Updated fo...
August 18, 2022

Device Management Updated fo...
August 16, 2022

Device Management Updated fo...
August 10, 2022

Device Management Updated fo...
August 10, 2022

Device Management Updated fo...
August 10, 2022

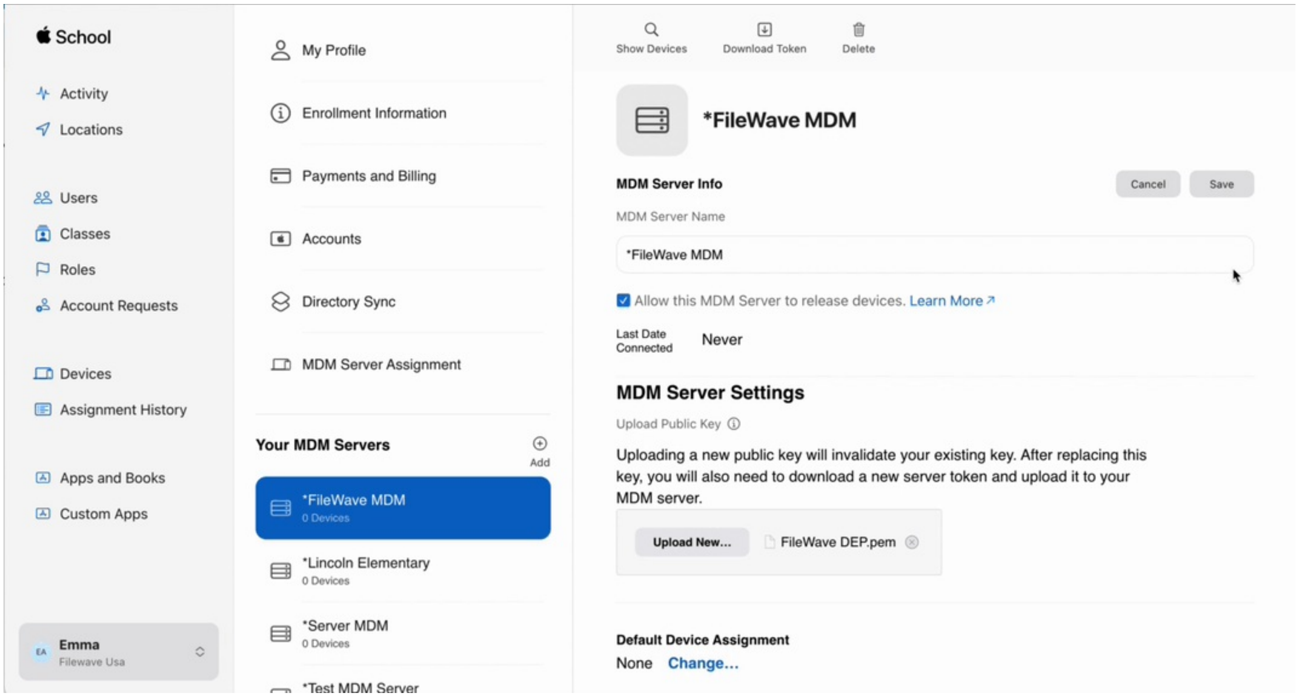
Device Management Updated fo...
August 9, 2022

Device Management Updated fo...
August 9, 2022

Device Management Updated fo...
August 9, 2022

No Activity Selected

7. Once saved, download the token from ASM/ABM



*FileWave MDM

MDM Server Info

MDM Server Name

*FileWave MDM

☑ Allow this MDM Server to release devices. Learn More ↗

Last Date Connected Never

MDM Server Settings

Upload Public Key ⓘ

Uploading a new public key will invalidate your existing key. After replacing this key, you will also need to download a new server token and upload it to your MDM server.

FileWave DEP.pem

Default Device Assignment

None

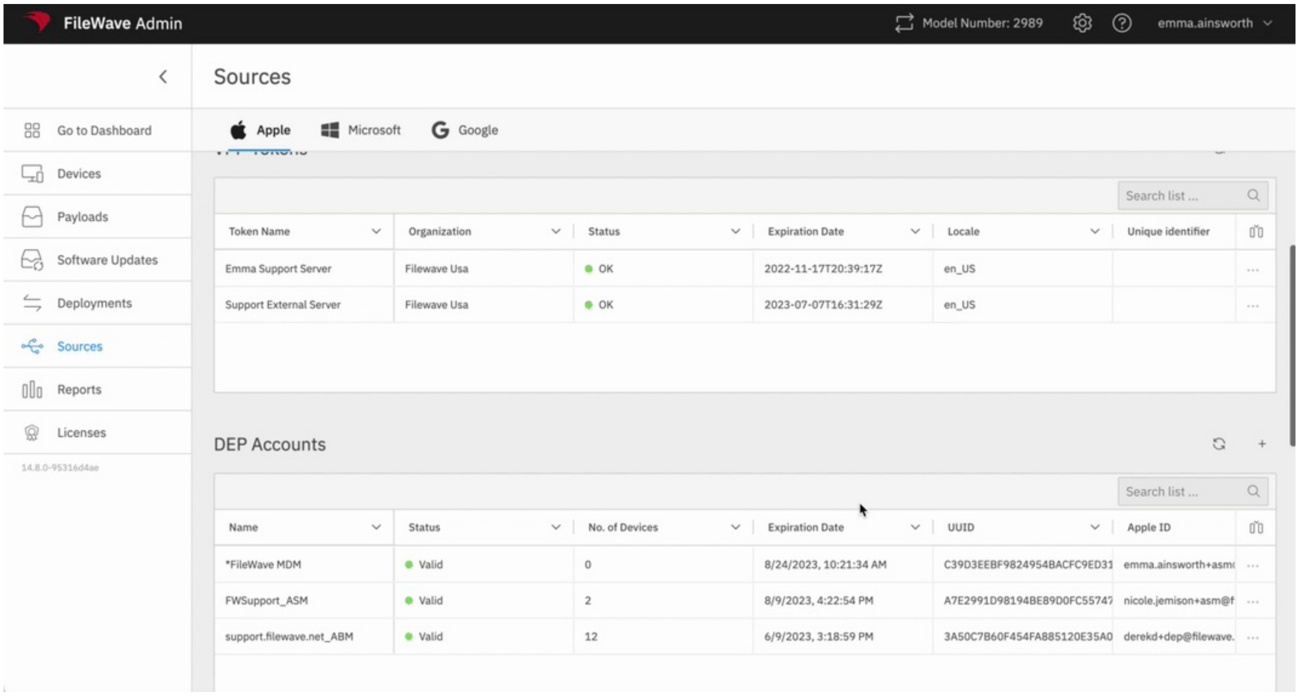
8. Go back to FileWave Central and upload the token

NOTE: At the end of this step, If any attributes have changed in the token, note that the dialog in FW may not reflect the new values for 10 - 30 minutes. (i.e. Server Name) and that is normal.

Renewing Token

FileWave Anywhere

In Sources, under DEP Accounts, select the ellipses next to the correct DEP account and choose ‘Edit’. Select Browse and upload the Apple Token downloaded in step 7 of this document. Click Save.



Sources

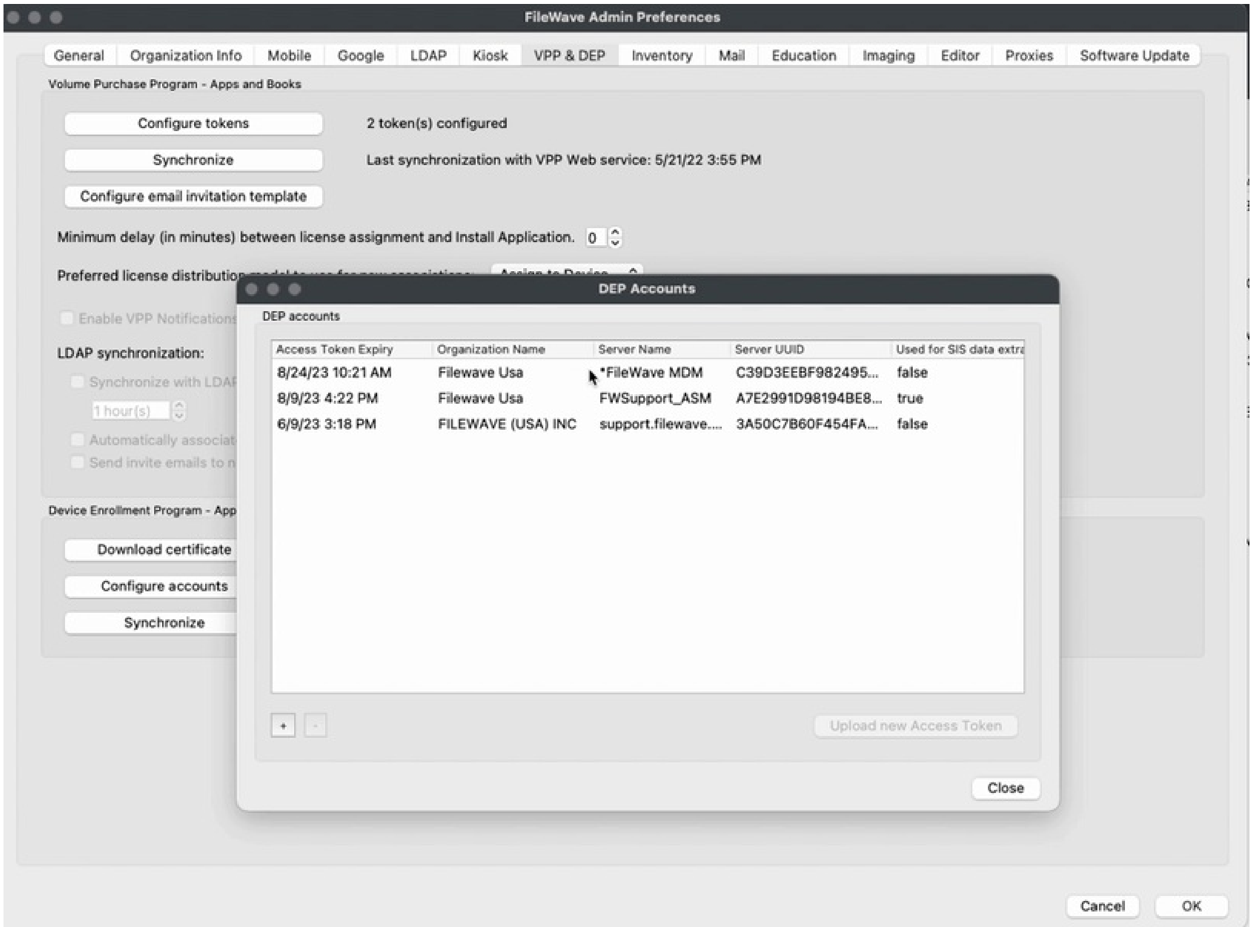
Token Name	Organization	Status	Expiration Date	Locale	Unique identifier
Emma Support Server	Filewave Usa	● OK	2022-11-17T20:39:17Z	en_US	
Support External Server	Filewave Usa	● OK	2023-07-07T16:31:29Z	en_US	

DEP Accounts

Name	Status	No. of Devices	Expiration Date	UUID	Apple ID
*FileWave MDM	● Valid	0	8/24/2023, 10:21:34 AM	C39D3EEBF9824954BACFC9ED31	emma.ainsworth+asm(
FWSupport_ASM	● Valid	2	8/9/2023, 4:22:54 PM	A7E2991D98194BE89D0FC55747	nicole.jemison+asm@f
support.filewave.net_ABM	● Valid	12	6/9/2023, 3:18:59 PM	3A50C7B60F454FA885120E35A0	derekd+dep@filewave.

FileWave Central

In Preferences > VPP & DEP, select Configure Accounts and enter your password. Select the correct DEP account and select ‘Upload new Access Token’. upload the Apple Token downloaded in step 7 of this document and click Open. Now you can close this window.



FileWave Admin Preferences
General | Organization Info | Mobile | Google | LDAP | Kiosk | VPP & DEP | Inventory | Mail | Education | Imaging | Editor | Proxies | Software Update

Volume Purchase Program - Apps and Books

2 token(s) configured

Last synchronization with VPP Web service: 5/21/22 3:55 PM

Configure email invitation template

Minimum delay (in minutes) between license assignment and Install Application. 0

Preferred license distributio

□ Enable VPP Notifications

LDAP synchronization:

□ Synchronize with LDAP

1 hour(s)

□ Automatically associat

□ Send invite emails to n

Device Enrollment Program - App

DEP Accounts

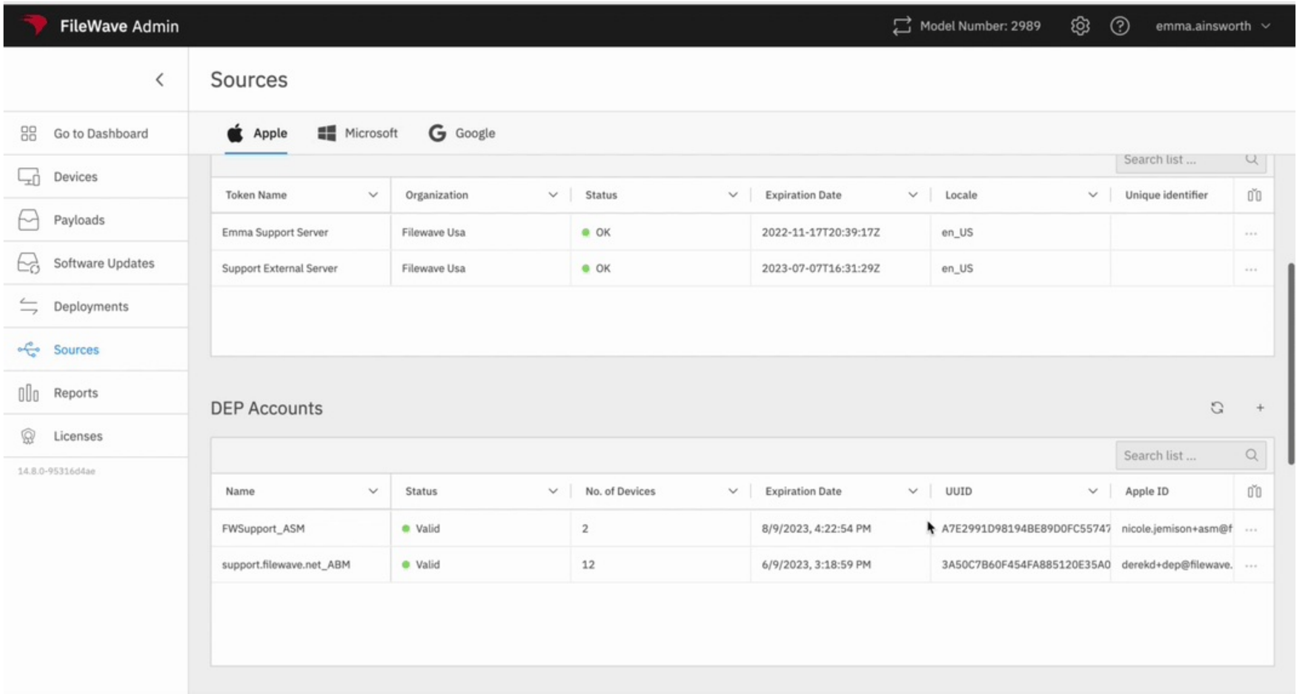
DEP accounts

Access Token Expiry	Organization Name	Server Name	Server UUID	Used for SIS data extra
8/24/23 10:21 AM	Fileware Usa	*FileWave MDM	C39D3EEBF982495...	false
8/9/23 4:22 PM	Filewave Usa	FWSupport_ASM	A7E2991D98194BE8...	true
6/9/23 3:18 PM	FILEWAVE (USA) INC	support.filewave....	3A50C7B60F454FA...	false

Adding New Token

FileWave Anywhere

In Sources, under DEP Accounts, select the '+' to the right. Steps 1 & 2 were completed earlier, so skip down to Step 3 and upload the Apple Token downloaded in step 7 of this document. Click Save.



Sources

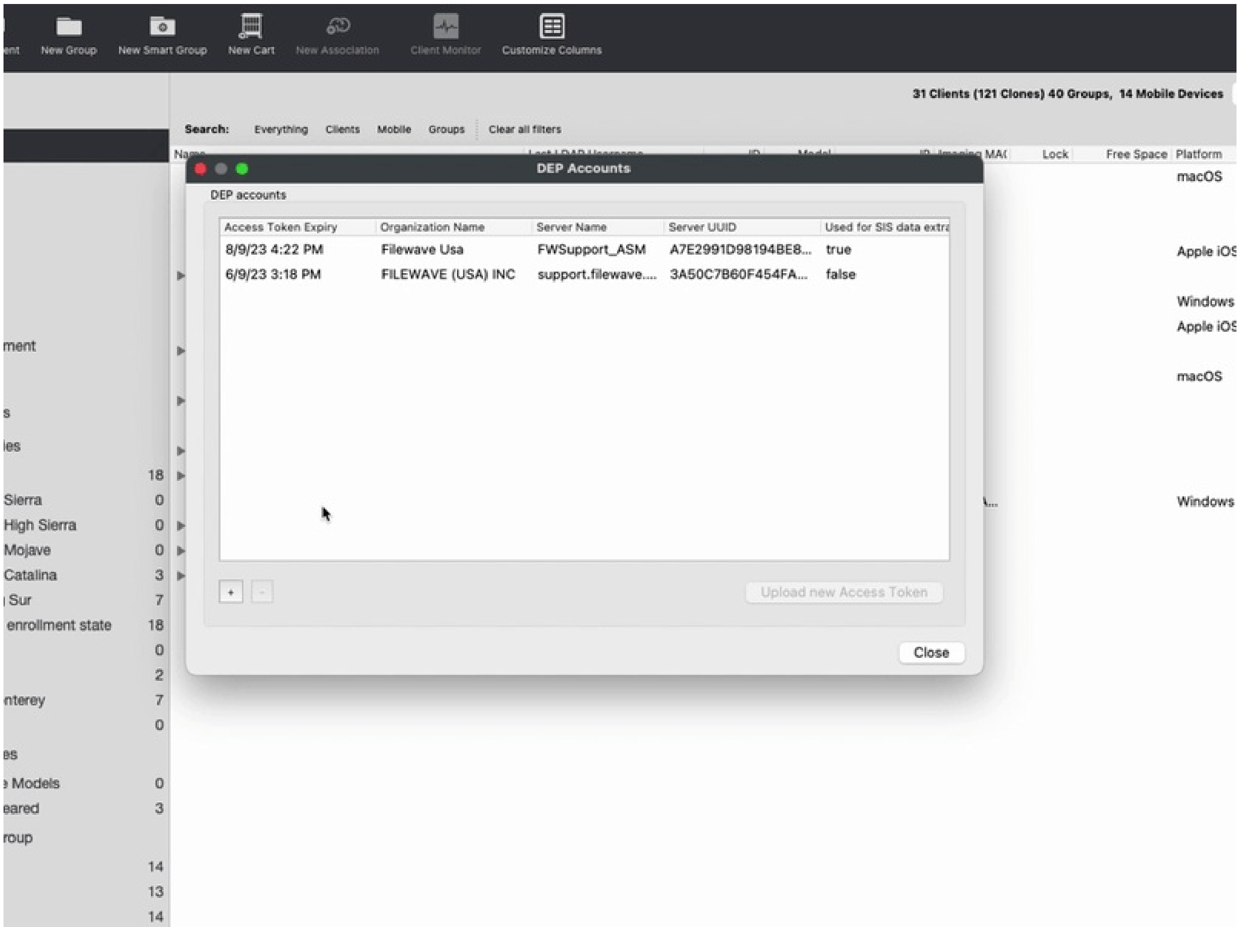
Token Name	Organization	Status	Expiration Date	Locale	Unique identifier
Emma Support Server	Filewave Usa	● OK	2022-11-17T20:39:17Z	en_US	
Support External Server	Filewave Usa	● OK	2023-07-07T16:31:29Z	en_US	

DEP Accounts

Name	Status	No. of Devices	Expiration Date	UUID	Apple ID
FWSupport_ASM	● Valid	2	8/9/2023, 4:22:54 PM	A7E2991D98194BE89D0FC55747	nicole.jemison+asm@f
support.filewave.net_ABM	● Valid	12	6/9/2023, 3:18:59 PM	3A50C7B60F454FA885120E35A0	derekd+dep@filewave.

FileWave Central

In Preferences > VPP & DEP, select Configure Accounts and enter your password. Select the '+' on the bottom left of the Configure Accounts window and select the token downloaded in step 7 of this document. Click Save and close the window.



DEP accounts

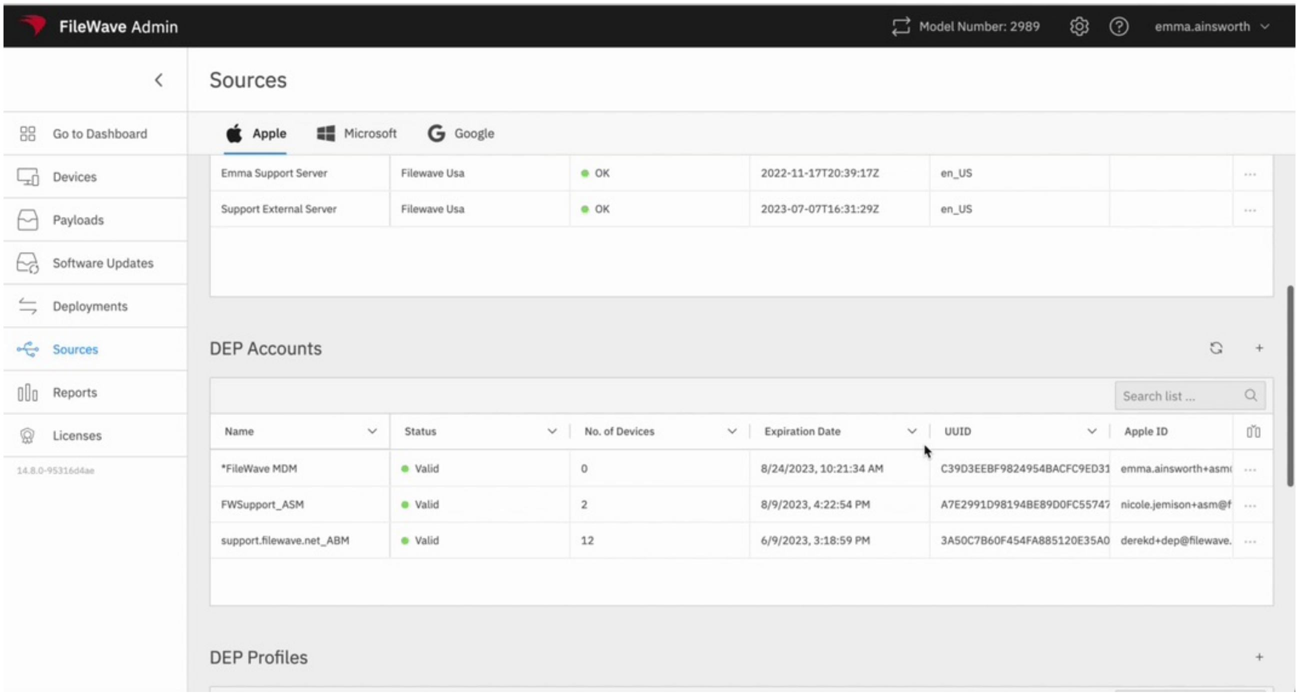
Access Token Expiry	Organization Name	Server Name	Server UUID	Used for SIS data extra
8/9/23 4:22 PM	Filewave Usa	FWSupport_ASM	A7E2991D98194BE8...	true
6/9/23 3:18 PM	FILEWAVE (USA) INC	support.filewave....	3A50C7B60F454FA...	false

9. After the token is uploaded, run a full DEP sync.

Perform full DEP sync

FileWave Anywhere

In the Sources tab, select the Sync icon next to DEP Account and choose Full Sync.



Sources

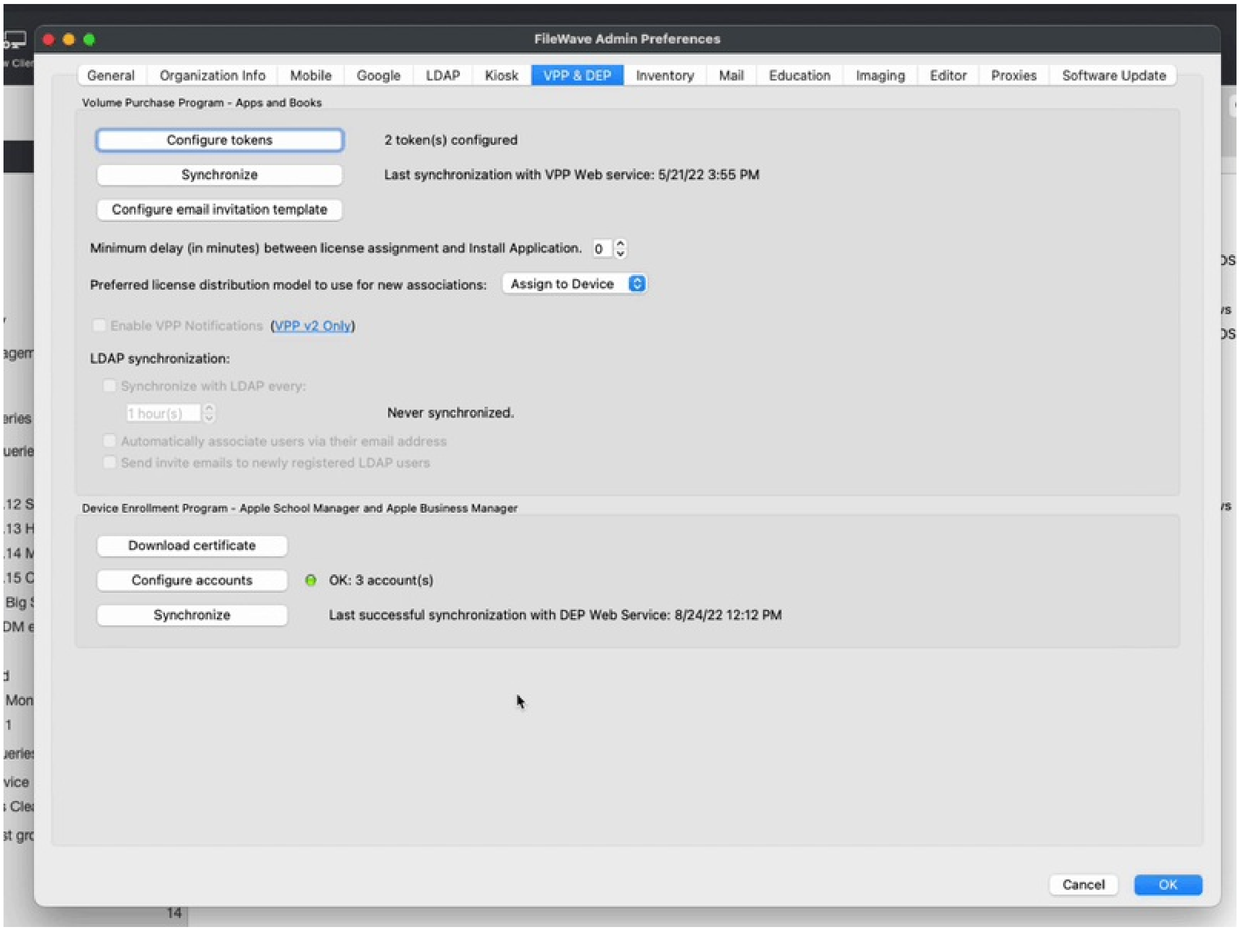
Emma Support Server	Filewave Usa	● OK	2022-11-17T20:39:17Z	en_US	···
Support External Server	Filewave Usa	● OK	2023-07-07T16:31:29Z	en_US	···

DEP Accounts

Name	Status	No. of Devices	Expiration Date	UUID	Apple ID
*FileWave MDM	● Valid	0	8/24/2023, 10:21:34 AM	C39D3EEBF9824954BACFC9ED31	emma.ainsworth+asm
FWSupport_ASM	● Valid	2	8/9/2023, 4:22:54 PM	A7E2991D98194BE89D0FC55747	nicole.jemison+asm@f
support.filewave.net_ABM	● Valid	12	6/9/2023, 3:18:59 PM	3A50C7B60F454FA885120E35A0	derekd+dep@filewave.

FileWave Central

Go to Preferences > VPP & DEP. While holding down the option/alt key, press ‘Synchronize (full sync)’.



Volume Purchase Program - Apps and Books

2 token(s) configured

Last synchronization with VPP Web service: 5/21/22 3:55 PM

Minimum delay (in minutes) between license assignment and Install Application. 0

Preferred license distribution model to use for new associations: Assign to Device

□ Enable VPP Notifications (VPP v2 Only)

LDAP synchronization:

□ Synchronize with LDAP every:

1 hour(s)

Never synchronized.

□ Automatically associate users via their email address

□ Send invite emails to newly registered LDAP users

Device Enrollment Program - Apple School Manager and Apple Business Manager

● OK: 3 account(s)

Last successful synchronization with DEP Web Service: 8/24/22 12:12 PM

You're all set! If you renewed your token, you should see a new expiration date. If you added a new token, you can learn more about managing your devices with DEP and FileWave here: Apple DEP Enrollment.

DEP Naming

This article is for individuals who want to customize naming of DEP devices. It will cover placeholders and their ability to accept name, as well as using custom and built-in strings in the DEP profile.

Placeholders are most useful for new incoming devices where the name is highly customized. And where you want to use additional attributes like custom fields.

Placeholders

Step-by-step guide

1. Generate a text file, ideally of serial numbers as one column and the custom name as the other.
   See Importing Computer Clients from a file and Enrolling Computer Clients
2. Import any custom field values if needed
   See Custom Fields: Importing CSV for more information

Variables in the DEP profile

Step-by-step guide

1. Generate a DEP profile
   See Working with Apple's Device Enrollment Program (DEP)
2. In the naming tab of the DEP profile you can use any:
   Built-in inventory variables (for a list of variables see Using variables in Apple iOS/macOS Profiles)
   Custom inventory variables, using the %custom_field.INTERNAL_NAME% (see more at Custom Fields)
3. It would also be recommended that you create an automatic DEP rule to only assign this profile to devices that have the variables set: see the example in Automatically Assign DEP profiles

FileWave Foundry Video

Sign into FileWave Foundry and watch a video here regarding DEP Naming.

Automatically Assign DEP profiles

Starting in FileWave version 13.1.0 you now have the ability to automatically assign DEP profiles to devices.

Step-by-step guide

Start by opening up the DEP Profiles UI (Assistant → DEP Association Management), and verify you have profiles created. It is recommended that you have a highly generic rule that will work with all iOS and macOS devices, and then profiles for your needed situations.

Assign Default Rule

1. Open the "Edit Assignment Rules" UI
2. Choose a Default DEP Profile (Figure 1.1)
3. Hit OK to save it

You can then choose between creating rules on simple things or advanced things:

Assign based on model/operating system (Simple)

1. Open the "Edit Assignment Rules" UI
2. Hit the [+] to create a new profile rule
3. Select your default profile for an OS (iOS in this example)
4. Drag the DEP Devices / Operating System component from the left into the Criteria
5. Set to "Contains" : "iOS" (See figure 2.1)
6. Save
7. Repeat again for "OS X" and "tv" as needed

Assign based on custom fields (Advanced)

1. Create Custom fields (in this example "usage" and "location")

   > See Custom Fields for more information

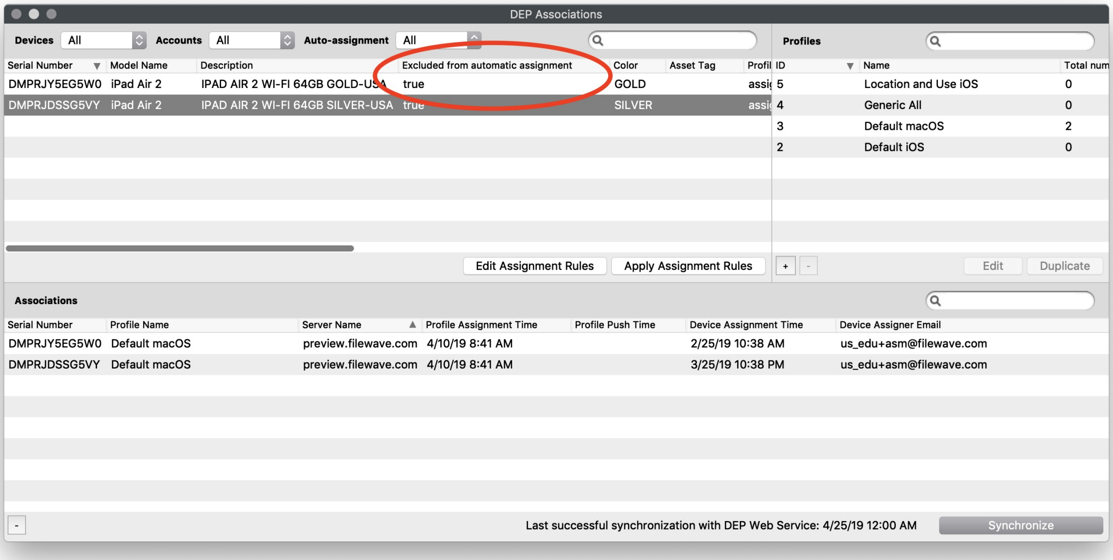
   1. Use: Provided: Admin, Type: string, Restricted: True, Values: None (DEFAULT), Faculty, Student, Administration (See Figure 3.1)
   2. Location: Provided: Admin, Type: string, Restricted: True, Values: None (Default), Site A, Site B... (Figure 3.2)
   3. Take note of the "Internal Name" from the custom fields
2. Open the DEP UI
3. Hit the [+] to create a new DEP profile
   1. Use the internal name in naming (see Figure 3.3)

      > See DEP Naming for more information

   2. Open the "Edit Assignment Rules" UI
   3. Hit the [+] to create a new profile rule
4. Select the profile you just created
   1. You will now see the Custom Fields component on the left Component list
   2. Open it and bring in location and use
   3. set them both to is not None (Figure 3.4)

Excluding serials from Auto Rules

You will notice a column named "Excluded from automatic assignment" with True or False (Figure 4.1)



DEP Associations

Serial Number	Model Name	Description	Excluded from automatic assignment	Color	Asset Tag	Profil
DMPRJY5EG5W0	iPad Air 2	IPAD AIR 2 WI-FI 64GB GOLD-USA	true	GOLD		assi
DMPRJDSSG5VY	iPad Air 2	IPAD AIR 2 WI-FI 64GB SILVER-USA	true	SILVER		assi

ID	Name	Total num
5	Location and Use iOS	0
4	Generic All	0
3	Default macOS	2
2	Default iOS	0

Serial Number	Profile Name	Server Name	Profile Assignment Time	Profile Push Time	Device Assignment Time	Device Assigner Email
DMPRJY5EG5W0	Default macOS	preview.filewave.com	4/10/19 8:41 AM		2/25/19 10:38 AM	us_edu+asm@filewave.com
DMPRJDSSG5VY	Default macOS	preview.filewave.com	4/10/19 8:41 AM		3/25/19 10:38 PM	us_edu+asm@filewave.com

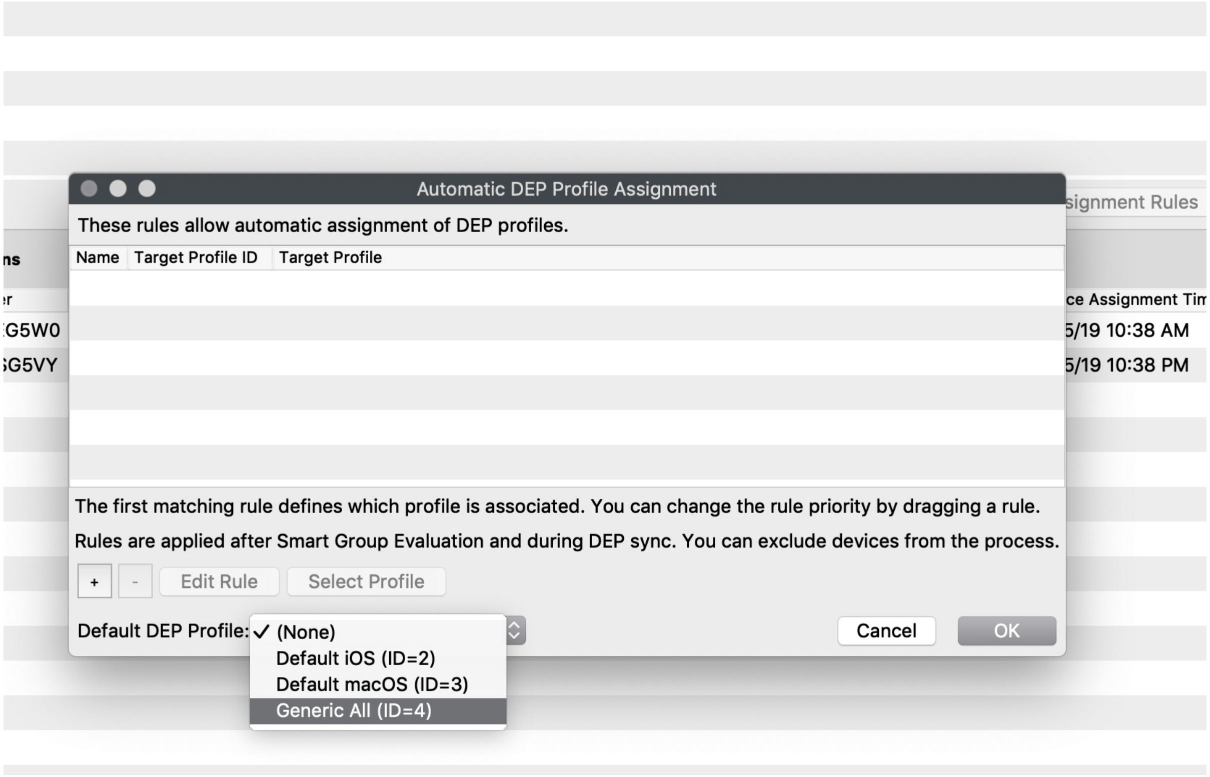
Last successful synchronization with DEP Web Service: 4/25/19 12:00 AM

Figure 4.1 - Exclude Column

true - Device will not be included in automatic rules. Note: "true" is NOT applicable when manually clicking the "Apply Assignment Rules" button...when that button is clicked all rules will be applied for any selected devices (after confirmation prompt). Selecting no devices infers ALL devices as selected.

false - Devices will be included in automatic rules, both automatically and when "Apply Assignment Rules" is triggered

true is the default for devices that were in your DEP list before an upgrade to 13.1 to protect those devices from changing before you have built new rules



Automatic DEP Profile Assignment

These rules allow automatic assignment of DEP profiles.

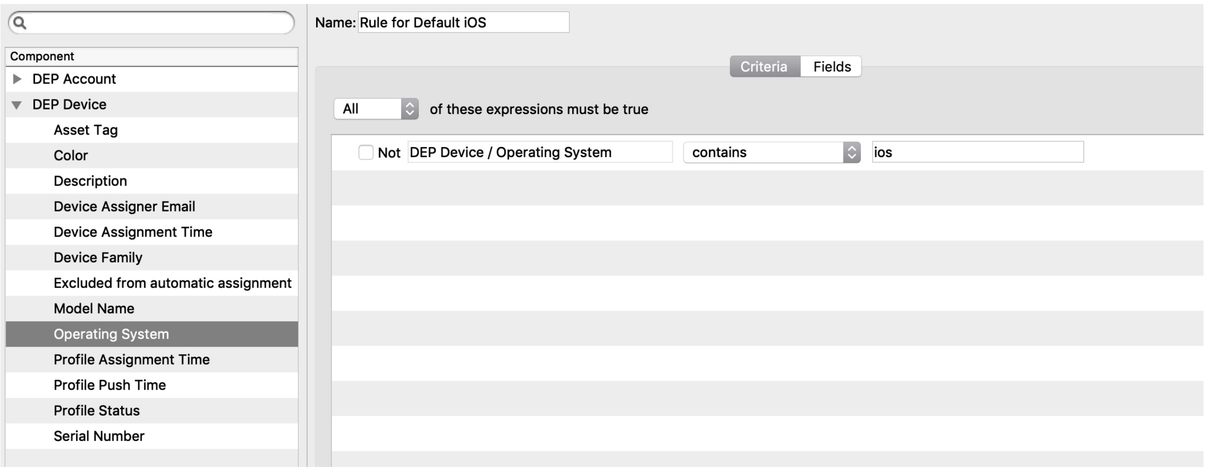
Name	Target Profile ID	Target Profile

The first matching rule defines which profile is associated. You can change the rule priority by dragging a rule.

Rules are applied after Smart Group Evaluation and during DEP sync. You can exclude devices from the process.

Default DEP Profile: ✓ (None)

Figure 1.1 - Default Rule



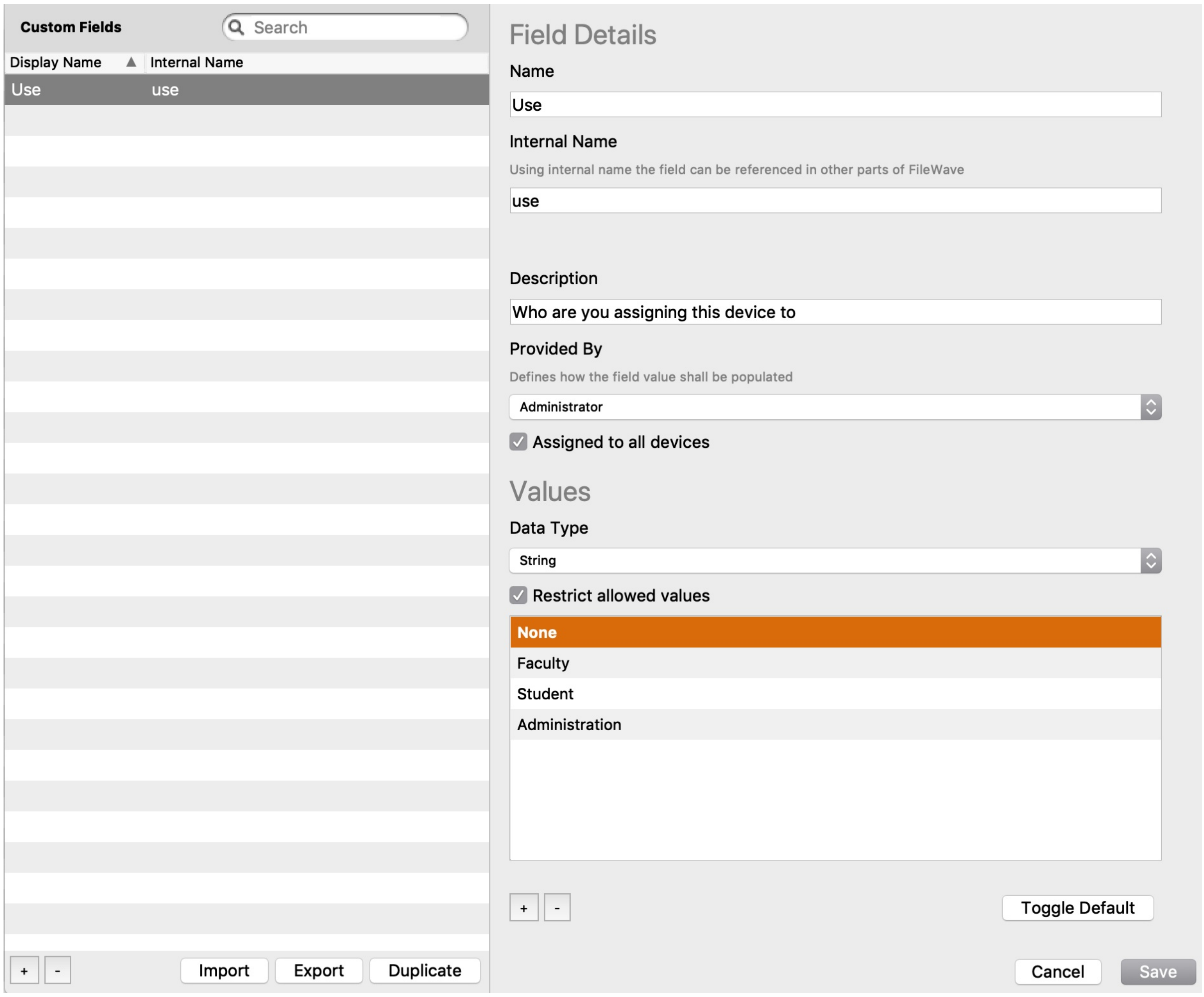
Component
- ▶ DEP Account
- ▼ DEP Device
  - Asset Tag
  - Color
  - Description
  - Device Assigner Email
  - Device Assignment Time
  - Device Family
  - Excluded from automatic assignment
  - Model Name
  - Operating System
  - Profile Assignment Time
  - Profile Push Time
  - Profile Status
  - Serial Number

Name: Rule for Default iOS

All of these expressions must be true

□ Not DEP Device / Operating System contains ios

Figure 2.1 - iOS Simple Rule



Custom Fields

Display Name ▲	Internal Name
Use	use

Field Details

Name: Use

Internal Name: use

Using internal name the field can be referenced in other parts of FileWave

Description: Who are you assigning this device to

Provided By: Administrator

Defines how the field value shall be populated

☑ Assigned to all devices

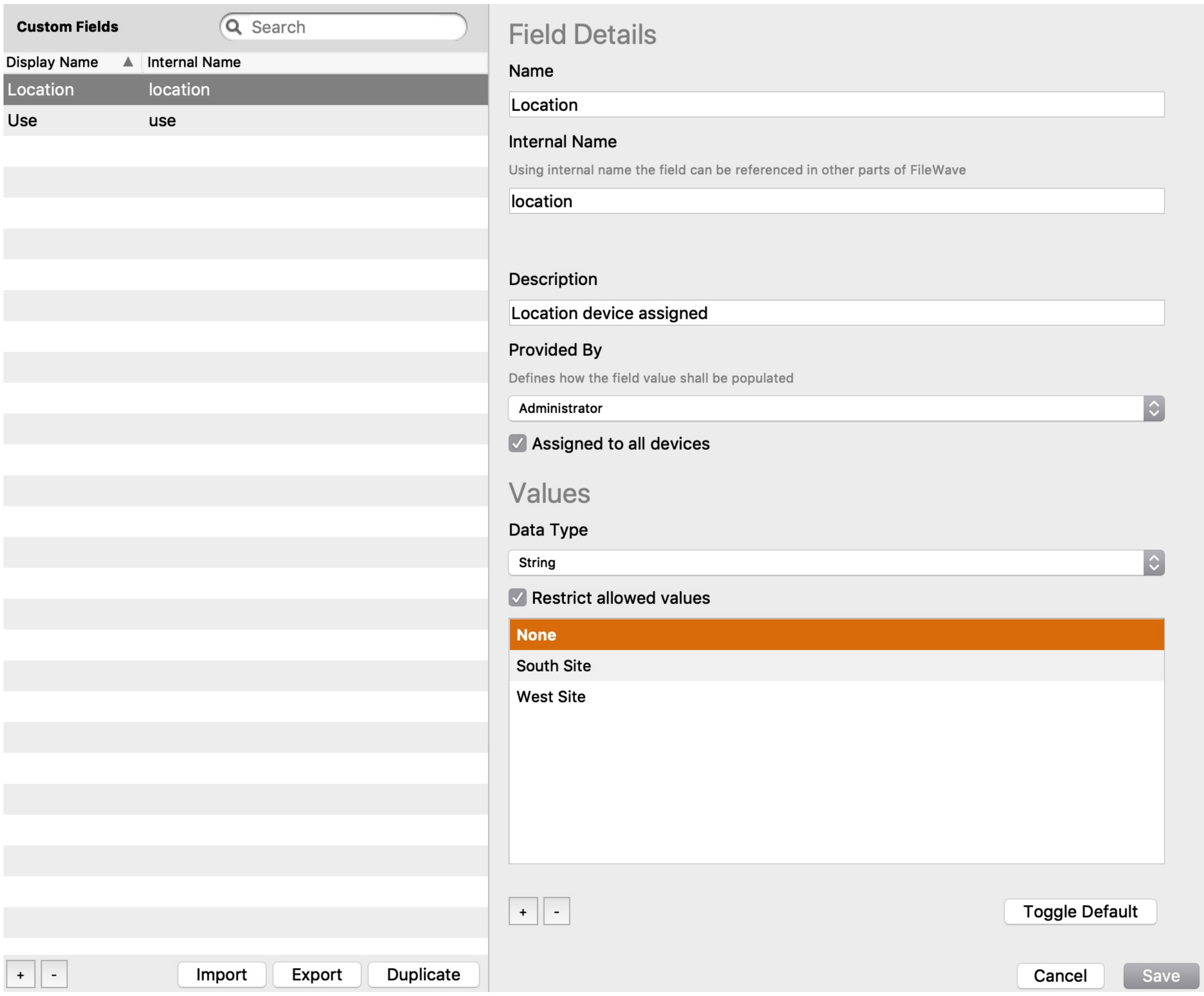
Values

Data Type: String

☑ Restrict allowed values

- None
- Faculty
- Student
- Administration

Figure 3.1 - Custom Use



Display Name	Internal Name
Location	location
Use	use

Field Details

Name: Location

Internal Name

Using internal name the field can be referenced in other parts of FileWave

location

Description: Location device assigned

Provided By

Defines how the field value shall be populated

Administrator

☑ Assigned to all devices

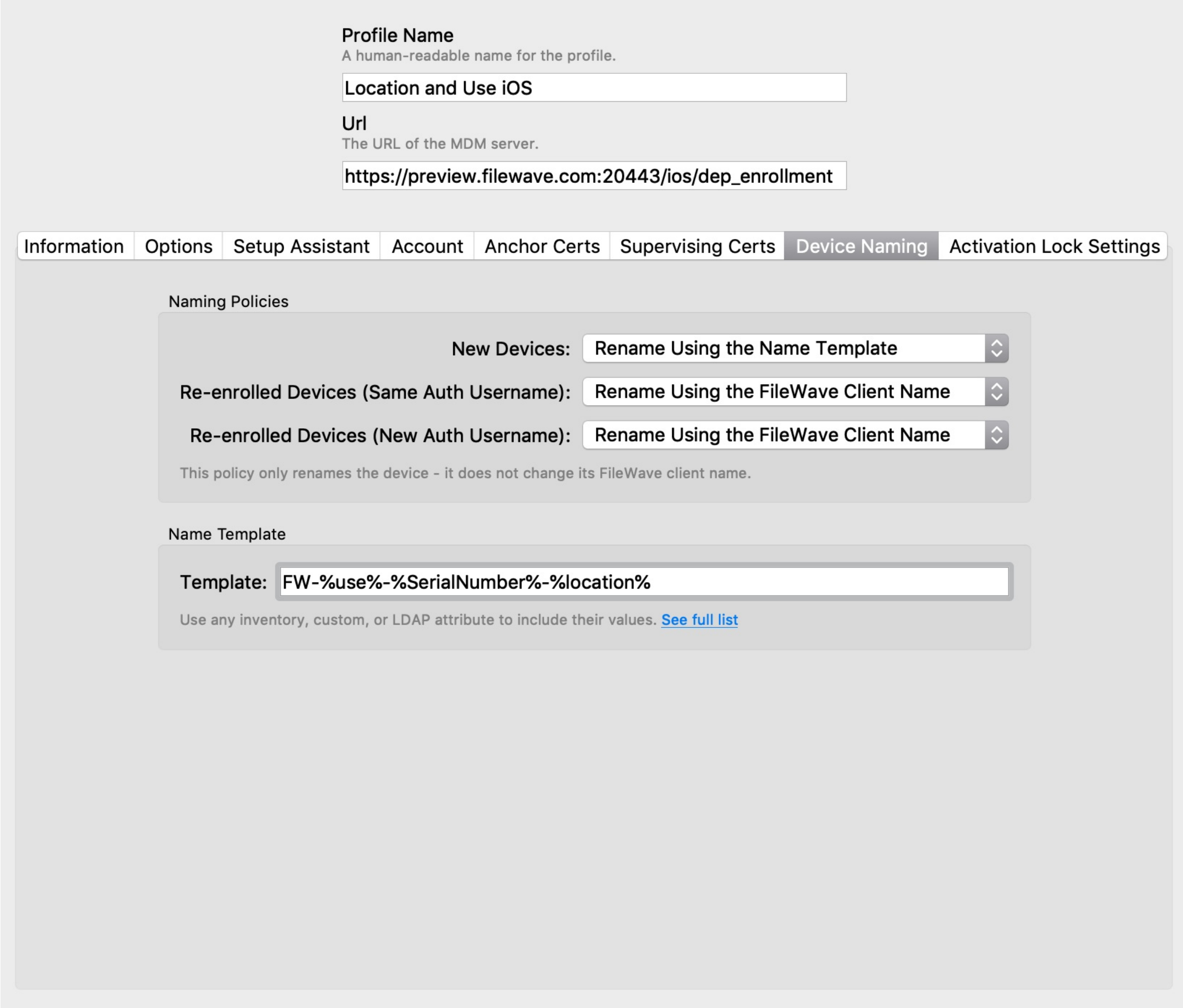
Values

Data Type: String

☑ Restrict allowed values

- None
- South Site
- West Site

Figure 3.2 - Custom Location



Profile Name
A human-readable name for the profile.
Location and Use iOS

Url
The URL of the MDM server.
https://preview.filewave.com:20443/ios/dep_enrollment

Naming Policies

New Devices: Rename Using the Name Template

Re-enrolled Devices (Same Auth Username): Rename Using the FileWave Client Name

Re-enrolled Devices (New Auth Username): Rename Using the FileWave Client Name

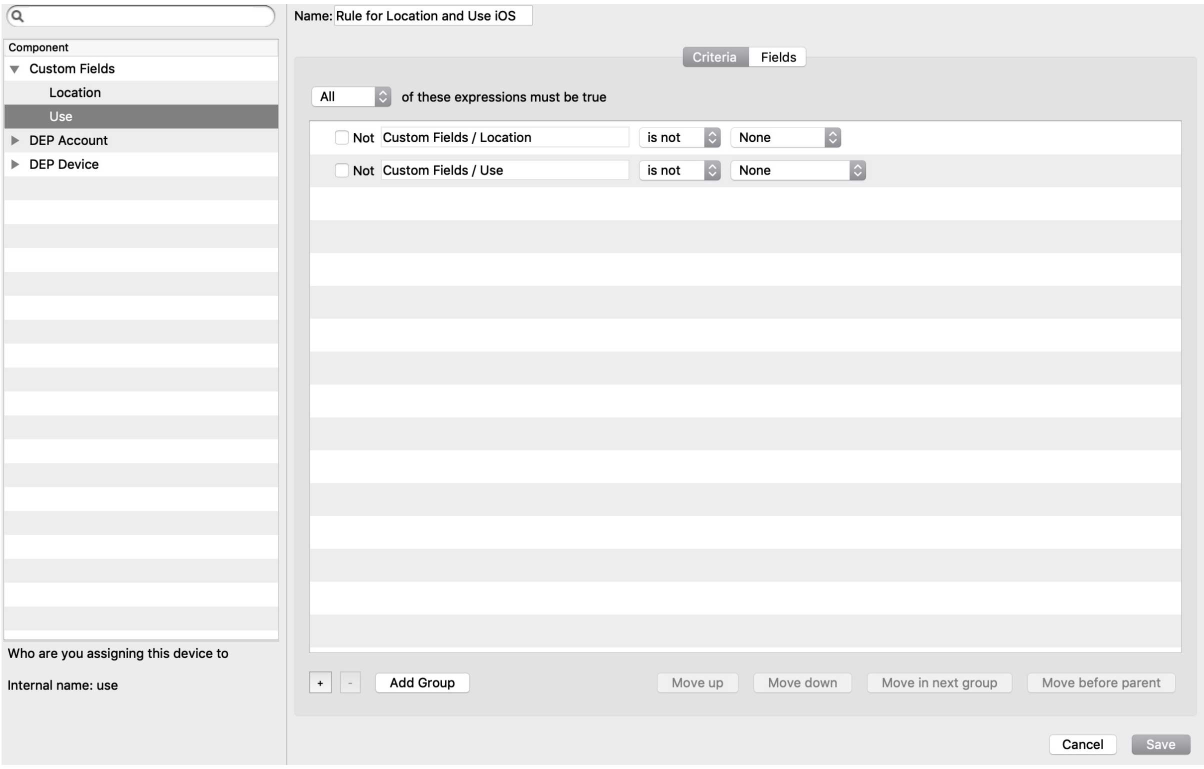
This policy only renames the device - it does not change its FileWave client name.

Name Template

Template: FW-%use%-%SerialNumber%-%location%

Use any inventory, custom, or LDAP attribute to include their values. See full list

Figure 3.3 - Custom Naming



Who are you assigning this device to

Internal name: use

Name: Rule for Location and Use iOS

All of these expressions must be true

□ Not Custom Fields / Location is not None

□ Not Custom Fields / Use is not None

Figure 3.4 - Custom Name Rule

Control Await Configuration state (DEP enrolled devices)

What

When Apple devices are enrolled via the Device Enrollment Program (DEP)—now known as Automated Device Enrollment (ADE)—they enter an “Await Configuration” state during the initial setup. In this mode, the user cannot interact with the device until the configuration process is complete, ensuring that devices are properly set up according to organizational policies before they are handed over to end-users.

Starting with FileWave 15.5.0, administrators have enhanced control over this process. You can now specify when a device is released from the “Await Configuration” state, rather than having FileWave automatically release it as soon as possible. This provides greater flexibility and control over the deployment and configuration of devices.

Supported Devices and OS Versions:

- iOS Devices:
  - iPhone and iPod touch running iOS 11 or later.
  - iPad running iOS 11 or later (before the introduction of iPadOS).
- iPadOS Devices:
  - iPad running iPadOS 13 or later.
- macOS Devices:
  - Mac computers running macOS 10.13 High Sierra or later.
- tvOS Devices:
  - Apple TV running tvOS 11 or later.

This feature is applicable to all the above device types enrolled via DEP/ADE and managed through FileWave 15.5.0 or later.

When/Why

Use this feature when you need devices to remain in the “Await Configuration” state until all necessary configurations, apps, and policies are fully deployed. This is particularly beneficial in scenarios where:

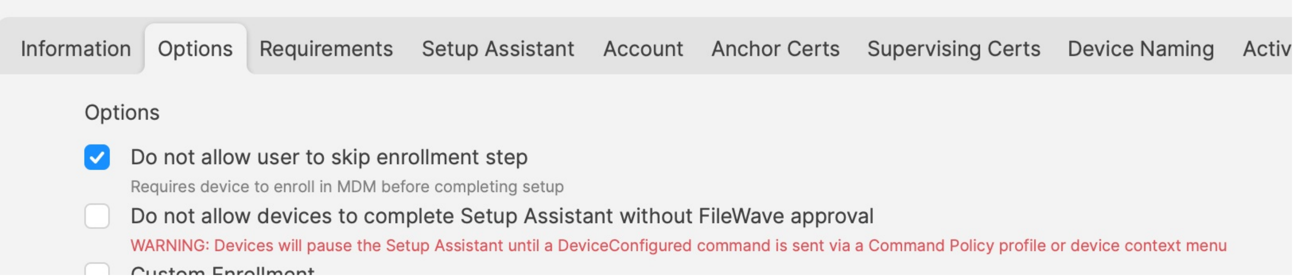
- Security Compliance: Ensuring that all security measures are in place before the device becomes operational.
- Standardization: Guaranteeing a consistent user experience by applying all organizational settings prior to device use.
- Controlled Deployment: Managing the timing of device readiness, especially in large-scale rollouts or staged deployments.

By controlling the release of the device, you enhance security, ensure compliance with organizational policies, and provide users with a fully configured device from the moment they begin using it.

How

When enrolled via DEP, devices are in a specific mode where the user is not allowed to interact with the device, which will stay in this state until configuration is over. By default, FileWave releases the device as soon as possible to shorten initial setup times. FileWave 15.5 now allows controlling when the device is released:

You can edit the DEP Profile used for enrolling your devices and go to the Options tab where you can check the "Do not allow devices to complete Setup Assistant without FileWave approval" which will make it so that devices will not finish setup until they are released.



Options

☑ Do not allow user to skip enrollment step

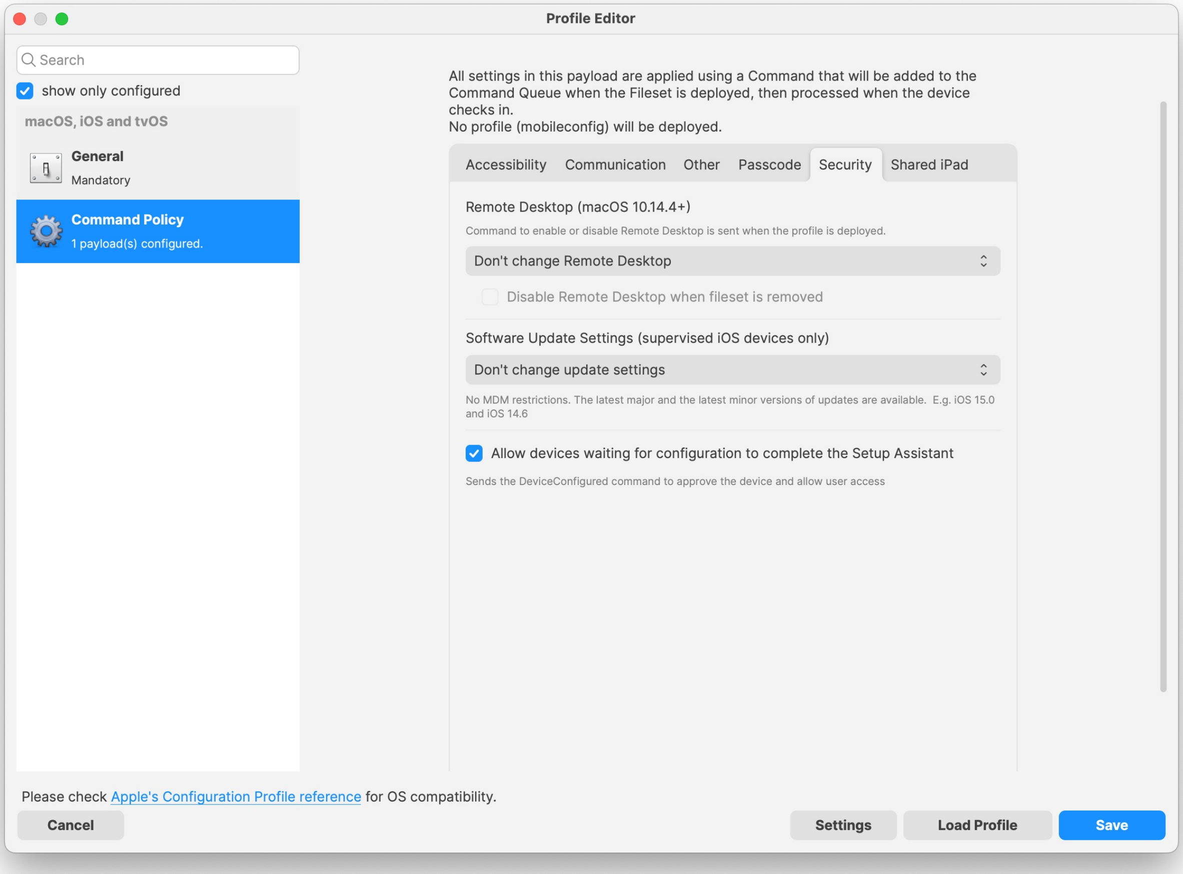
Requires device to enroll in MDM before completing setup

□ Do not allow devices to complete Setup Assistant without FileWave approval

WARNING: Devices will pause the Setup Assistant until a DeviceConfigured command is sent via a Command Policy profile or device context menu

□ Custom Enrollment

When creating a Profile to release devices you can see in the image below that there is a checkbox in Command Policy -> Security -> "Allow devices waiting for configuration to complete the Setup Assistant" and if a profile with this set is sent it will release the devices from setup to be able to be used.



Profile Editor

Search

☑ show only configured

macOS, iOS and tvOS

General
Mandatory

Command Policy
1 payload(s) configured.

All settings in this payload are applied using a Command that will be added to the Command Queue when the Fileset is deployed, then processed when the device checks in.
No profile (mobileconfig) will be deployed.

Accessibility | Communication | Other | Passcode | Security | Shared iPad

Remote Desktop (macOS 10.14.4+)

Command to enable or disable Remote Desktop is sent when the profile is deployed.

Don't change Remote Desktop

□ Disable Remote Desktop when fileset is removed

Software Update Settings (supervised iOS devices only)

Don't change update settings

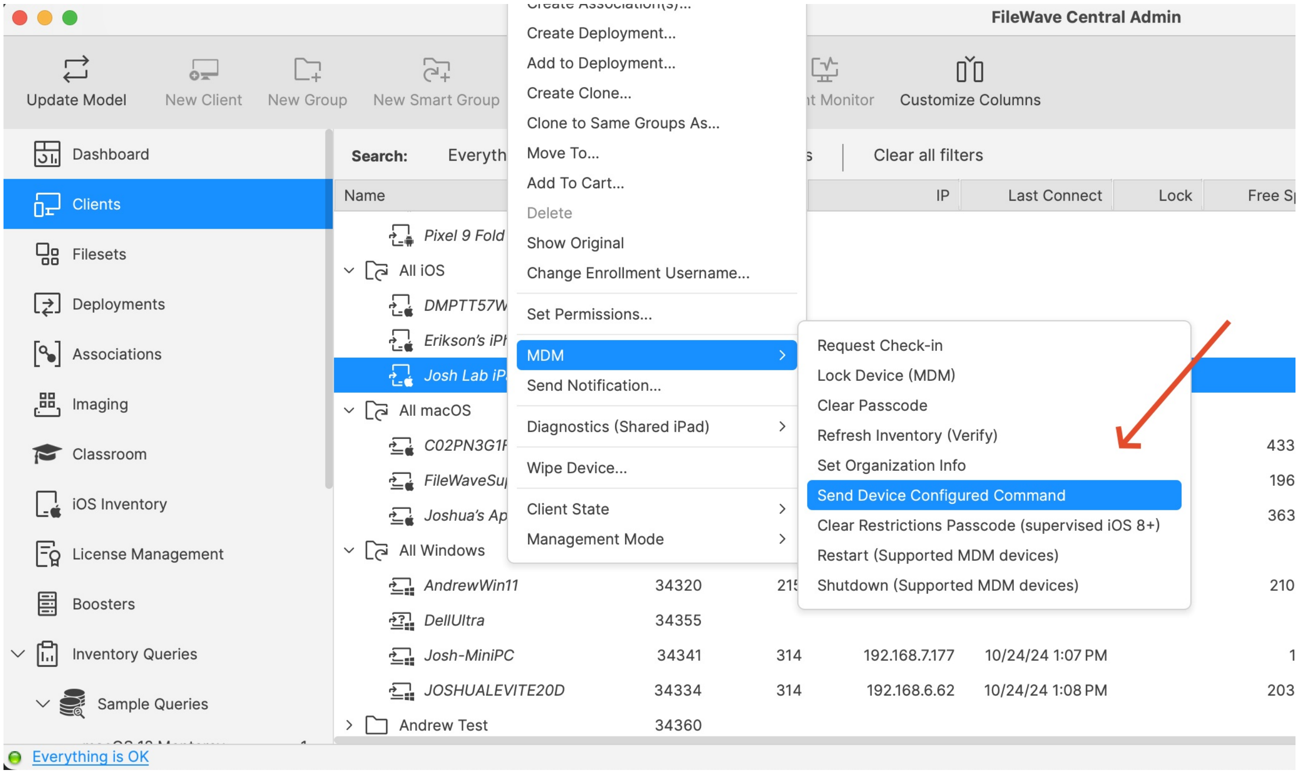
No MDM restrictions. The latest major and the latest minor versions of updates are available. E.g. iOS 15.0 and iOS 14.6

☑ Allow devices waiting for configuration to complete the Setup Assistant

Sends the DeviceConfigured command to approve the device and allow user access

Please check Apple's Configuration Profile reference for OS compatibility.

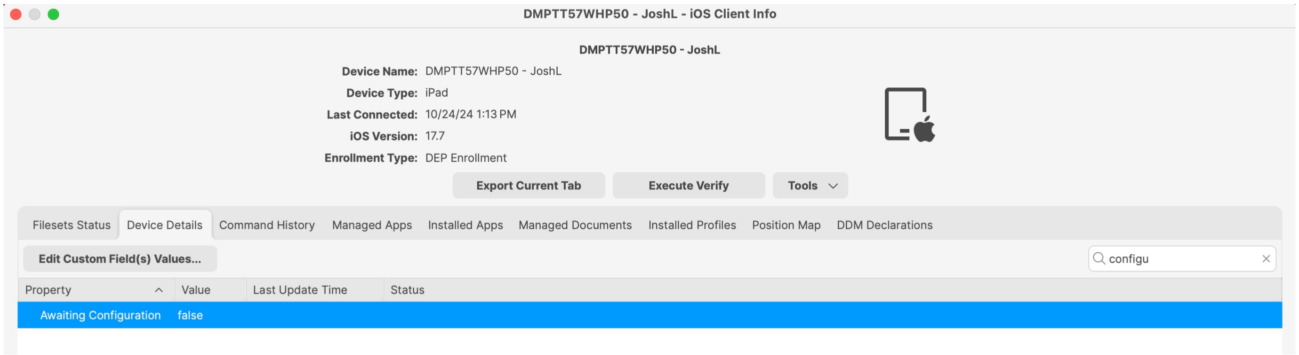
It is also possible to send the Device Configured command either manually (context menu) by right clicking one or more devices in FileWave Central and picking MDM -> Send Device Configured Command.



FileWave Central Admin

Name			IP	Last Connect	Lock	Free S
Pixel 9 Fold						
All iOS						
DMPTT57W						
Erikson's iPh						
Josh Lab iP						
All macOS						
C02PN3G1F						433
FileWaveSu						196
Joshua's Ap						363
All Windows						
AndrewWin11	34320	215				210
DellUltra	34355					
Josh-MiniPC	34341	314	192.168.7.177	10/24/24 1:07 PM		1
JOSHUALEVITE20D	34334	314	192.168.6.62	10/24/24 1:08 PM		203
Andrew Test	34360					

Devices will report their "Awaiting Configuration" state so that you can check on a device or make a Query to report on many devices to track if they are still in the setup process.



DMPTT57WHP50 - JoshL

Device Name: DMPTT57WHP50 - JoshL
Device Type: iPad
Last Connected: 10/24/24 1:13 PM
iOS Version: 17.7
Enrollment Type: DEP Enrollment

Property	Value	Last Update Time	Status
Awaiting Configuration	false		

Related Content

- Automated Device Enrollment (ADE)
- Apple DEP Enrollment

Digging Deeper

The introduction of this feature in FileWave 15.5.0 provides administrators with enhanced control over the device enrollment and configuration process. By keeping devices in the “Await Configuration” state, you can ensure that:

- All Required Configurations are Applied: Devices won’t be accessible to users until every necessary app, profile, and setting is installed.
- Improved Security: Prevents users from accessing the device with incomplete security policies, reducing potential vulnerabilities.
- Customized Deployment Workflow: Aligns device readiness with organizational schedules, training sessions, or specific events.

Automating the Release Process

Using Command Policy Filesets to send the Device Configured command allows for automation based on specific triggers or conditions, such as:

- Time-Based Triggers: Release devices at a specific time as set in the Association or Deployment properties.
- Configuration Completion: Automatically release once all deployments are confirmed as installed.
- Event-Based Triggers: Release devices in batches aligned with department needs or project phases.

Considerations

- User Experience: Communicate with end-users about the deployment timeline to manage expectations.
- Testing: Before wide-scale implementation, test the process with a small group to ensure configurations apply as intended.
- Monitoring: Utilize FileWave’s monitoring tools to track the status of devices in the “Await Configuration” state.

By leveraging this feature, organizations can enhance their deployment strategy, ensuring devices are secure, compliant, and fully configured right out of the box.

Apple TV Automatic Advance (DEP)

Description

This recipe will walk you through the steps of enrolling an Apple TV HD 4th gen into FileWave with DEP utilizing the Automatic Advance setting.

> ⓘ This setting is only available if you are using an Apple TV HD 4th gen and FileWave v12. Recommended to use wired connection for Automatic enrollment.

> ⓘ In the steps below please remember do not set up the Apple TV manually in anyway or the Automatic Advance feature will not work.
> This includes pairing the remote.
> Touching anything stops the process.

Ingredients

- DEP setup
- Ethernet Cable
- USB 3 Cable

Direction

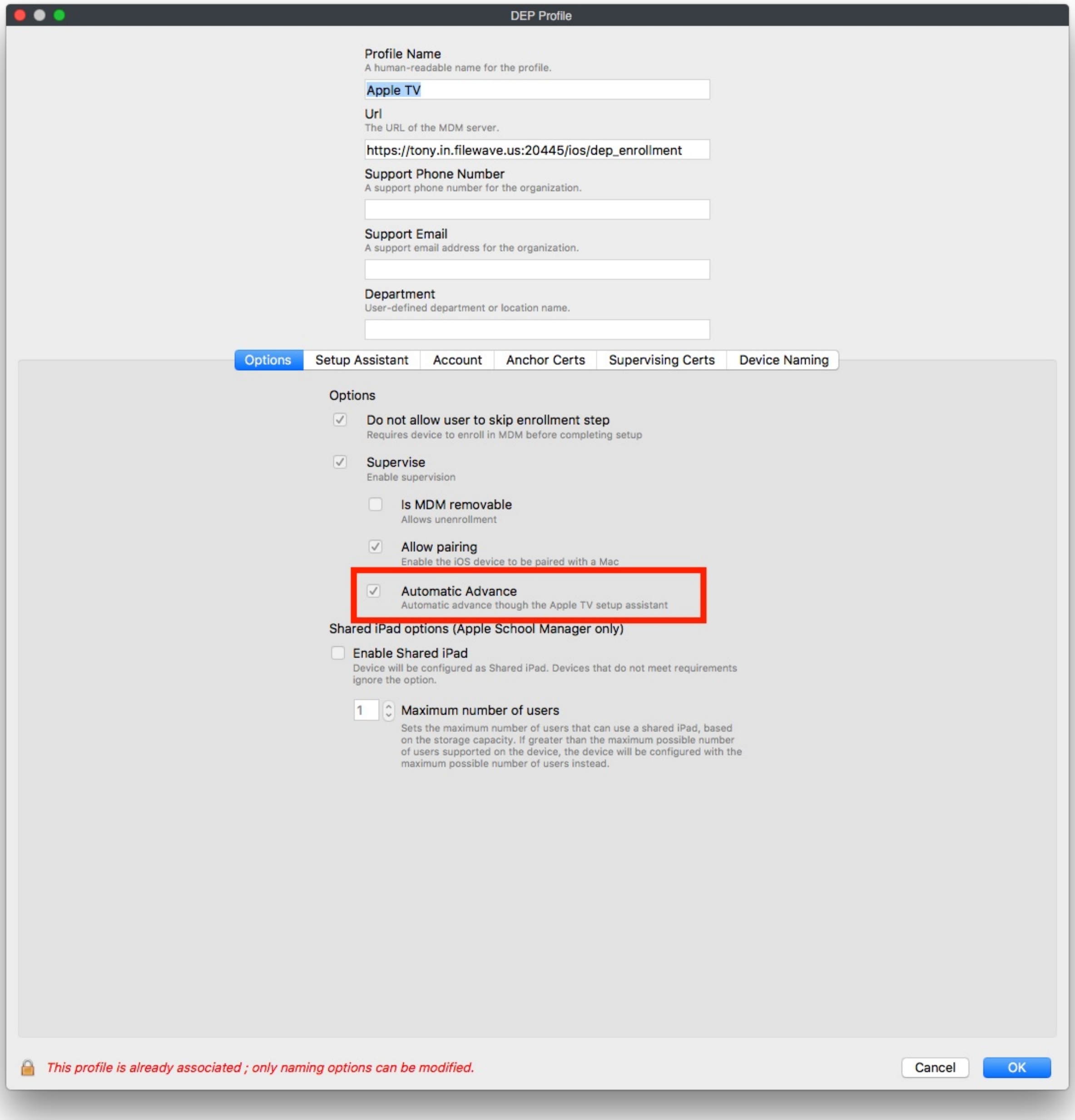
1. Go to the Assistants menu -> DEP Association Management

This opens the DEP Associations window

1. Fill out as much of the profile as you need in the Options, Setup Assistant, and the Device Naming tabs.

At the very least you will need to have the Automatic Advance option set.

Please Note: If you do not setup the Device Naming tab it will default as the serial number.



Profile Name
A human-readable name for the profile.
Apple TV

Url
The URL of the MDM server.
https://tony.in.filewave.us:20445/ios/dep_enrollment

Support Phone Number
A support phone number for the organization.

Support Email
A support email address for the organization.

Department
User-defined department or location name.

Options

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

☑ Supervise
Enable supervision

☐ Is MDM removable
Allows unenrollment

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

☑ Automatic Advance
Automatic advance though the Apple TV setup assistant

Shared iPad options (Apple School Manager only)

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

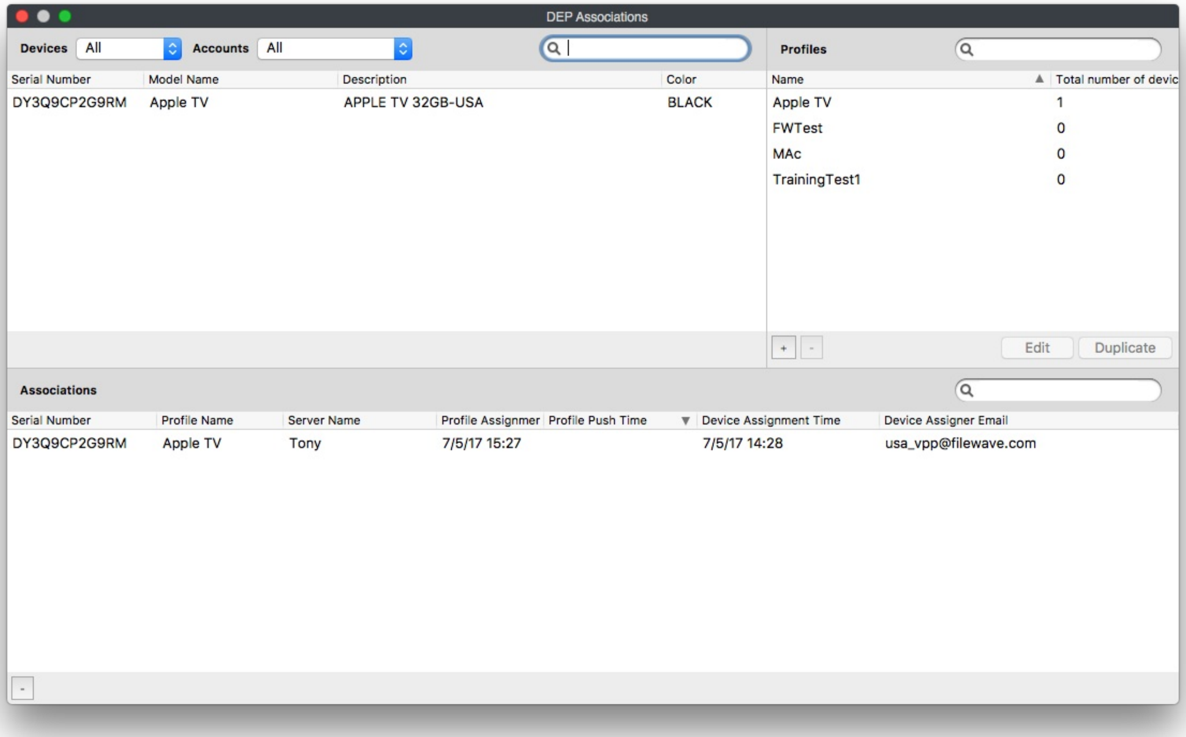
1 Maximum number of users
Sets the maximum number of users that can use a shared iPad, based on the storage capacity. If greater than the maximum possible number of users supported on the device, the device will be configured with the maximum possible number of users instead.

This profile is already associated ; only naming options can be modified.

1. Save the profile and assign it to your devices.

   All you have to do is find your Apple TV(s) on the left pane, find your profile on the right, then click, drag, and drop.

   You will see the association(s) in the bottom pane.



Devices: All Accounts: All

Serial Number	Model Name	Description	Color
DY3Q9CP2G9RM	Apple TV	APPLE TV 32GB-USA	BLACK

Profiles

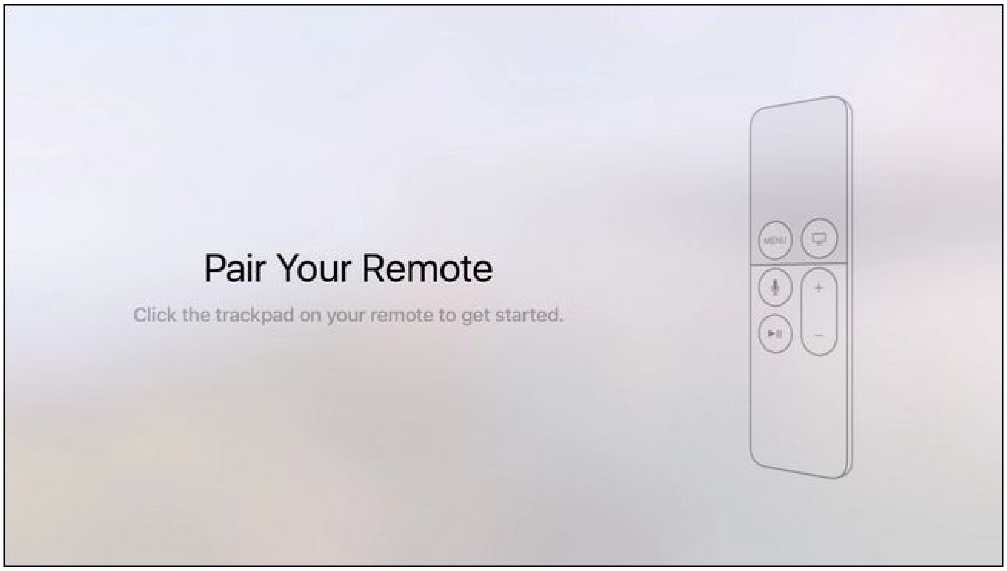
Name	Total number of devic
Apple TV	1
FWTest	0
MAc	0
TrainingTest1	0

Associations

Serial Number	Profile Name	Server Name	Profile Assignmer	Profile Push Time	Device Assignment Time	Device Assigner Email
DY3Q9CP2G9RM	Apple TV	Tony	7/5/17 15:27		7/5/17 14:28	usa_vpp@filewave.com

1. Now you will need to plug your Apple TV(s) into power and ethernet. If you are going to attach it to a TV/Monitor at this point remember do no pair the remote or go through any of the prompts. The settings you setup will automatically advance through all those for you but will not if you do any setup at this point.

   When the Apple TV(s) is at the Pair your Remote prompt if will wait 19 secs or so then the device will auto advance through all prompts.



Pair Your Remote

Click the trackpad on your remote to get started.

1. After the Apple TV(s) completed the setup you can now bring it into FileWave as you would any other Mobile device through the Admin.

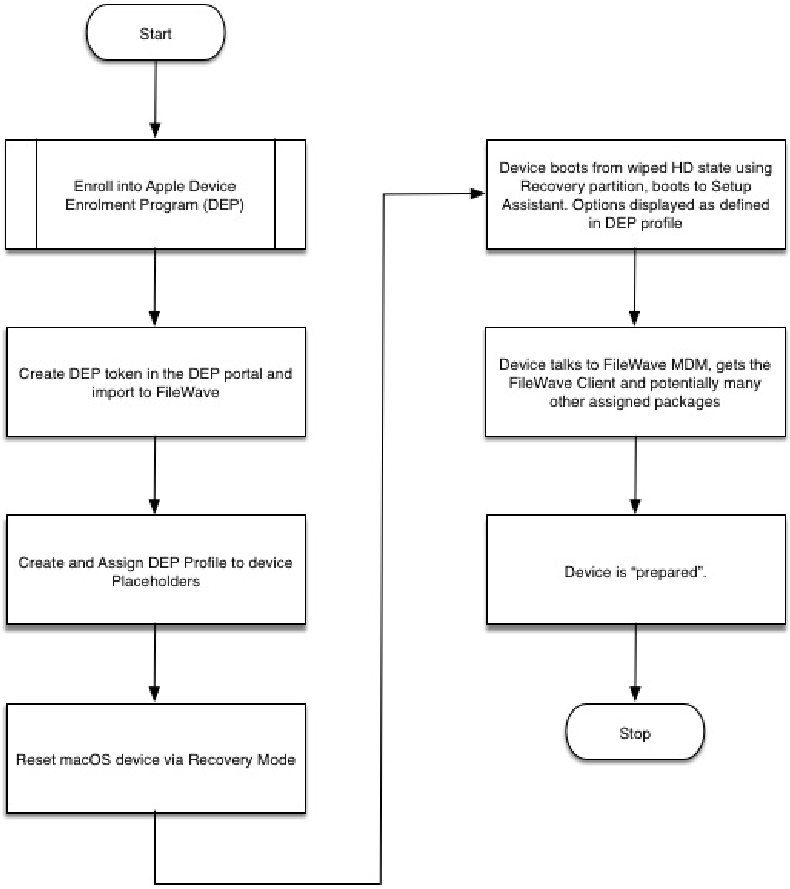
DEP Notify - How to provide progress visibility during DEP activation (macOS)

New to the Device Enrollment Program (DEP) process? Do you have a create full of macOS devices that need to be prepared and issued to end users? Did this need to happen yesterday?

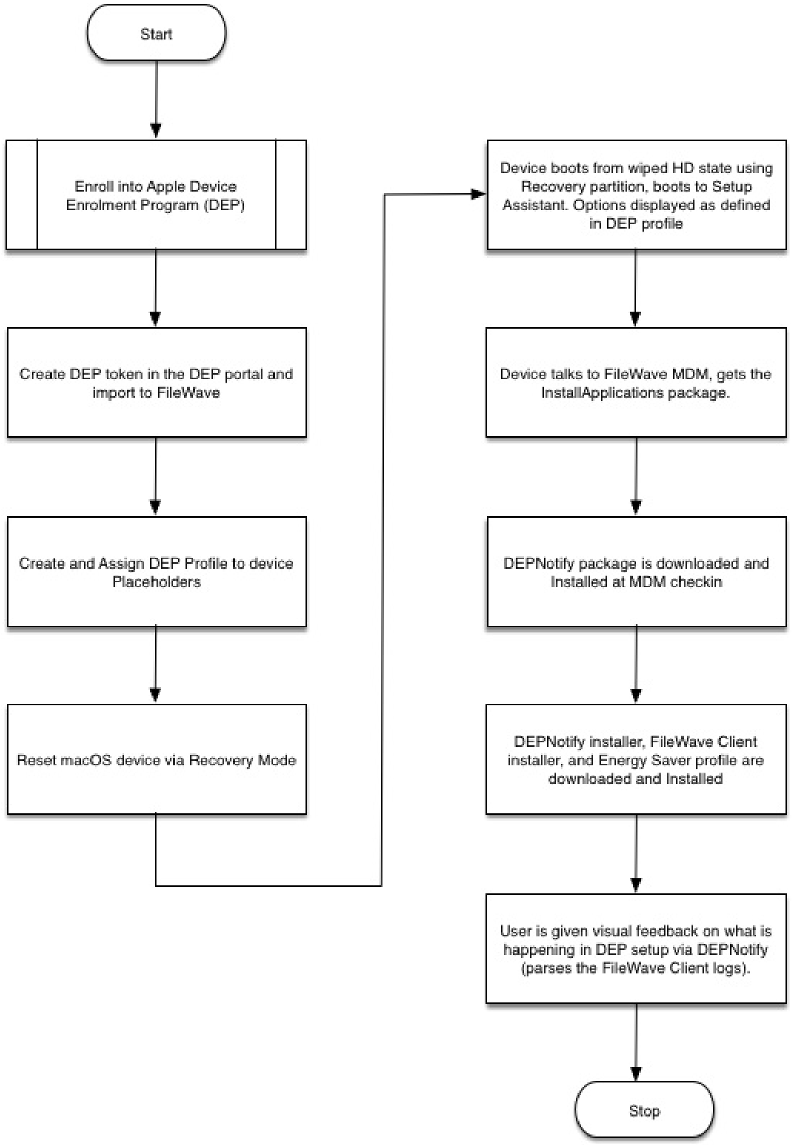
The world of DEP device provisioning has been a great help and has improved the speed at which devices can be issued to end users. Gone are the days of monolithic imaging! Long live DEP! But what is happening when a macOS device is going through the Setup Assistant process? Want to get some visibility on what is being installed during the device activation? Traditionally, when a device goes through the DEP assistant, any number of applications can be deployed to the device. The problem with this approach is that there is not any indication given to the end user as to what is happening during this time interval. To an end user, it could appear that there is a problem with the device, and they may create support tickets to your Help Desk on the subject.

In order to avoid that, we need to provide some visual indication of what is happening behind the scenes during this setup time. To do so, we will leverage two separate open source projects that are in use in the mac community, namely InstallApplications and DEPNotify.

FileWave, by default, will provision a DEP device, enroll it into the MDM server, then deploy the custom macOS client to the device. The process looks something like this:


Start
Enroll into Apple Device Enrolment Program (DEP)
Create DEP token in the DEP portal and import to FileWave
Create and Assign DEP Profile to device Placeholders
Reset macOS device via Recovery Mode
Device boots from wiped HD state using Recovery partition, boots to Setup Assistant. Options displayed as defined in DEP profile
Device talks to FileWave MDM, gets the FileWave Client and potentially many other assigned packages
Device is "prepared".
Stop

We need to instruct the FileWave server to deploy the open source package InstallApplications first so that we can set up the DEPNotify package and get feedback with all the great logging information that FileWave gives via its client log. The modified process looks something like this:


Start
Enroll into Apple Device Enrolment Program (DEP)
Create DEP token in the DEP portal and import to FileWave
Create and Assign DEP Profile to device Placeholders
Reset macOS device via Recovery Mode
Device boots from wiped HD state using Recovery partition, boots to Setup Assistant. Options displayed as defined in DEP profile
Device talks to FileWave MDM, gets the InstallApplications package.
DEPNotify package is downloaded and Installed at MDM checkin
DEPNotify installer, FileWave Client installer, and Energy Saver profile are downloaded and Installed
User is given visual feedback on what is happening in DEP setup via DEPNotify (parses the FileWave Client logs).
Stop

Step-by-step guide

Create, configure, and deploy the InstallApplications package

Create boostrap.json

1. Visit Erik Gomez's blog to get a practical example of configuring InstallApplications as well as some history and background on the project.
2. Visit Erik Gomez's github site and download the latest code. For the purposes of this document, I have used version 1.1.
3. Follow the instructions on the above site to configure your bootstrap.json file. Also, see the section below "Generating your bootstrap.json" for a simple example to get started with. To make troubleshooting easier, configure one or two packages defined in your bootstrap.json and ensure your packages are downloading correctly and your Install Application launch agent and launch daemon work successfully. If you have too many packages defined, it may be more difficult to determine where your configuration problem lies.
4. Generate your bootstrap.json with the generatejson.py script on Erik's site, which automatically generates the SHA256 hashes for you.
5. Once you have the bootstrap.json file generated (below is a sample boostrap.json), you will need to host it somewhere (like your filewave server) in order for the macOS client to download it during DEP activation.

bootstrap.json

```
{
"preflight": [],
"setupassistant": [
{
"file": "/some_path/DEPNotify_installer.pkg",
"url": "https://<your_filewave_server>:20443/some_folder/DEPNotify_installer.pkg",
"packageid": "com.package.depnotify",
"version": "1.0",
"hash": "some_long_hash",
"name": "DEPNotify",
"type": "package"
},
{
"file": "/some_path/FileWave_installer.pkg",
"url": "https://<your_filewave_server>:20443/some_folder/filewave_installer.pkg",
"packageid": "com.package.filewaveinstaller",
"version": "1.0",
"hash": "some_long_hash",
"name": "FileWave Client",
"type": "package"
}
],
"userland": [
{
"file": "/some_path/EnergySaver.py",
"url": "https://<your_filewave_server>:20443/some_folder/EnergySaver.py",
"hash": "some_long_hash",
"name": "Energy Saver Profile",
"type": "rootscript"
}
]
}
```

> Note: In the above bootstrap.json, the preflight stage is required, even if it is empty. If you don't have it defined, the script will error out (01/20/2018).

Hosting and Serving your packages via the FileWave Server (Linux)

To serve packages from FileWave, we will need to modify the httpd_custom.conf file for apache. To do this:

1. On the FileWave server, open "/usr/local/filewave/apache/conf/httpd_custom.conf" and add the following:

   ```
   Alias /custompkg /usr/local/filewave/custompkg
   <Directory "/usr/local/filewave/custompkg">
   Options Indexes FollowSymLinks
   AllowOverride All
   Order allow,deny
   Allow from all
   </Directory>
   ```

2. Restart apache with "fwcontrol apache restart"
3. Create the folder "custompkg" within /usr/local/filewave/. This will be the storage location for all of the packages that you defined in your boostrap.json file.

Testing the InstallApplications workflow outside of the DEP activation process

1. Testing the InstallApplications workflow outside of the DEP workflow will save you time.
2. To do this, execute the installapplications.py using the following command line on any macOS test device, such as a VM:

Launching installapplications.py manually

```
sudo python /Library/Application Support/installapplications/installapplications.py --jsonurl
https://<your_filewave_server>:20443/bootstrap.json
```

There is also an option to skip the validation of the bootstrap.json file. Use this option to include the bootstrap.json in the installapplications package rather than download it via url.

```
sudo python /Library/Application\ Support/installapplications/installapplications.py --jsonurl
https://<your_filewave_server>:20443/bootstrap.json --skip-validation
```

It turns out that the installapplications.py really doesn't like urls that have redirection. So, if you want to use some file hosting site like Dropbox, etc. think again. You may choose to host all the files on github, but then convert to raw links using rawgit.com; these links do not seem to redirect and worked fine to download installer packages via installapplications.py. Alternatively, you can choose to serve these files directly from your FileWave server.

Configure the InstallApplications LaunchDaemon and LaunchAgent

LaunchDaemon:

1. Edit payload/Library/LaunchDaemons/com.erikng.installapplications.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>Label</key>
<string>com.erikng.installapplications</string>
<key>ProgramArguments</key>
<array>
<string>/usr/bin/python</string>
<string>/Library/Application Support/installapplications/installapplications.py</string>
<string>--jsonurl</string>
<string>https://<your_filewave_server>:20443/custompkg/bootstrap.json</string>
<!-- <string>--iapath</string> -->
<!-- <string>/Library/Application Support/installapplications</string> -->
<!-- <string>--laidentifier</string> -->
<!-- <string>com.erikng.installapplications</string> -->
<!-- <string>--ldidentifier</string> -->
<!-- <string>com.erikng.installapplications</string> -->
<string>--depnotify</string>
<string>DEPNotifySkipStatus</string>
<string>Command: WindowTitle: Welcome to your Mac!</string>
<string>Command: NotificationOn:</string>
<string>Command: Quit: Thanks for your patience while we setup your new mac.</string>
<string>Command: WindowStyle: ActivateOnStep</string>
<string>DEPNotifyPath: /Applications/Utilities/DEPNotify.app</string>
<string>DEPNotifyArguments: -filewave</string>
<!-- <string>DEPNotifyArguments: -filewave -fullScreen</string> -->
<!-- <string>--reboot</string> -->
<string>--skip-validation</string>
</array>
<key>RunAtLoad</key>
<true/>
<key>StandardOutPath</key>
<string>/var/log/installapplications.log</string>
<key>StandardErrorPath</key>
<string>/var/log/installapplications.log</string>
</dict>
</plist>
```

In the above example, I left the reboot and fullscreen option disabled, but feel free to adjust this according to your needs.

LaunchAgent:

There was no need to adjust this, but if you wish to customize the install applications bundle ID, you will have to edit this file.

Signing your InstallApplications package

Prerequisite: Membership in Apple's Developer Program

1. Use a package creation utility to generate the .pkg for installapplications. One type of tool to use is Apple's command line pkgbuild, for example:

```
pkgbuild --identifier com.erikng.installapplications --root <path_to_root_of_installapplications_payload>
InstallApplications.pkg
```

1. Only distribution style packages are supported, so to convert from a flat package to a distribution package:

```
productbuild --package InstallApplications.pkg InstallApplicationsDistr.pkg
```

1. To sign the distribution package:

```
/usr/bin/productsign --sign "Developer ID Installer: <yourID> (XXXXXXXX)" InstallAppplicationsDist.pkg
FileWaveClientInstaller.pkg
```

1. To check your signing, you can issue:

```
pkgutil --check-signature FileWaveClientInstaller.pkg
```

The above command should return "Status: signed by a certificate trusted by Mac OS X".

Test the "InstallApplications.pkg" thoroughly on a test mac before attempting to deploy via the DEP Setup Assistant.

Steps for deploying your signed InstallApplications.pkg using FileWave

Instead of deploying the macOS custom pkg, you will be deploying the InstallApplications.pkg. If you are currently deploying the custom FileWave client in your DEP workflow as the starting point, I highly recommend testing this workflow out on a test server before deploying to production. The deployment scenario below considers that we are running FileWave on the linux appliance and have NEVER previously deployed the custom FileWave client before using the InstallApplication DEP workflow.

1. Open an ssh connection to your FileWave server

```
$ ssh root@<yourfilewaveserver.com>
```

2. Run a complete backup of your filewave server.
3. Backup the current DEP macOS installer package

```
$ cd /usr/local/filewave/fwcld
$ mv FileWaveClient.pkg FWClient_old.pkg
```

4. Copy your signed InstallApplications.pkg on your mac to the /usr/local/filewave/fwcld folder on your FileWave server and change its name at the same time

```
$ scp /InstallApplications.pkg root@yourfilewaveserver.com:/usr/local/filewave/fwcld/FileWaveClient.pkg
```

5. Remove the MD5 hash of the old FileWave macOS custom pkg from the database. You should see that the above query should affect one row only.

```
$ /usr/local/filewave/postgresql/bin/psql mdm django -c "DELETE from ios_preferences WHERE key =
'dep_osx_package_md5';"
```

6. Set the MD5 checksum and version of the "FileWaveClient.pkg" (really now the InstallApplications package disguised as the FileWave client package).

macOS FileWave Server:

```
# sudo /usr/local/filewave/python/bin/python /usr/local/filewave/django/manage.pyc shell
from ios.fwcld_utility import get_package_sha256;
get_package_sha256(force=True)
from ios.preferences_manager import PreferencesManager; PreferencesManager.set_dep_osx_package_version("14.0.3")
exit()
fwcontrol server stop
fwcontrol server start
```

Linux FileWave Server:

```
# sudo /usr/local/filewave/python/bin/python /usr/local/filewave/django/manage.pyc shell
from ios.fwcld_utility import get_package_sha256;
get_package_sha256(force=True)
from ios.preferences_manager import PreferencesManager; PreferencesManager.set_dep_osx_package_version("14.0.3")
exit()
fwcontrol server stop
fwcontrol server start
```

Command to execute to generate the new MD5 for the "fake" Custom Client (InstallApplications.pkg):

```
from ios.fwcld_utility import get_package_md5;
get_package_md5(force=True)
```

This will generate a result like:

['70c829ddd9bd2aeafbe07fdd35f91c03']

Command to set the new "version" of the package:

```
from ios.preferences_manager import PreferencesManager; PreferencesManager.set_dep_osx_package_version("12.7.1")
```

1. Exit the psql shell with "\q"
2. Restart the filewave server:

   ```
   fwcontrol server restart
   ```

Result

During setup assistant, you will no longer get the custom FileWave client delivered first. The FileWave client will be installed by the InstallApplications script, along with any other crucial application / setup file that is needed (such as the Energy Saver) during DEP provisioning. Once the FileWave client is on the device, all other associated filesets can be deployed according to the needs of the end user.

Minimum OS version for enrolling Apple devices via ADE

What

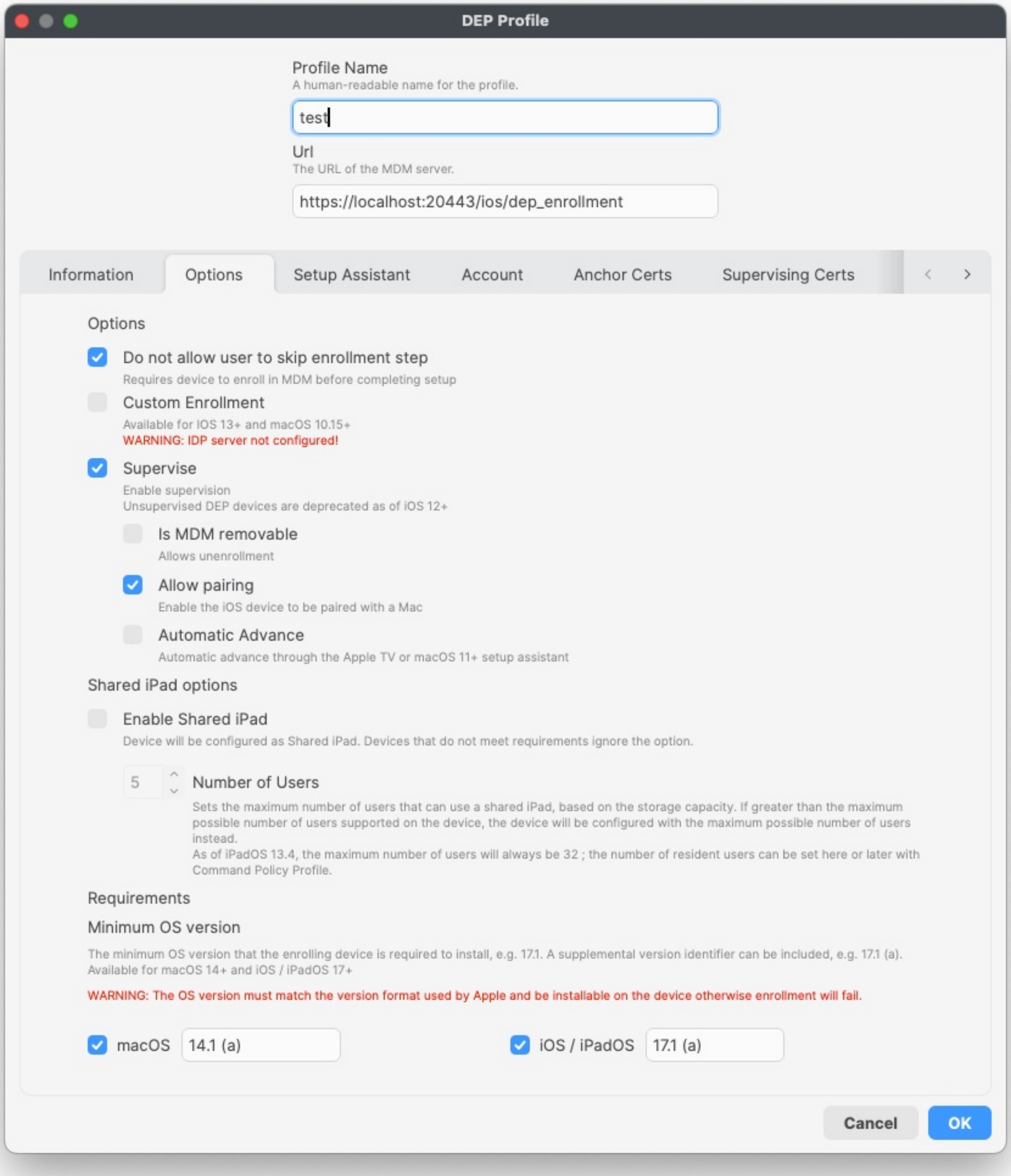
MDM servers have the ability to enforce a minimum operating system version on enrolling devices when using Automated Device Enrollment (ADE). This feature was added in FileWave version 15.1.0 for macOS 14.0 Sonoma and iOS/iPadOS 17.0. Apple does not support this feature on older versions of macOS or iOS/iPadOS.

When/Why

Minimum OS version allows to ensure that devices are on the necessary OS version before being put into production. The MDM will send a JSON 403 response when the device requests the enrollment profile. If the minimum operating system version is needed, the user will be guided through a process of updating the device. Restarts will be performed automatically. Once completed, the device returns to Setup Assistant and the user can finish the enrollment and setup process.

How

With FileWave 15.1.0 support of minimum OS version was added. To specify minimum OS versions open DEP profile and go to Options → Requirements section. There are separate fields for macOS and iOS / iPadOS minimum OS versions.



DEP Profile

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

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

Options

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

☐ Custom Enrollment
Available for iOS 13+ and macOS 10.15+
WARNING: IDP server not configured!

☑ Supervise
Enable supervision
Unsupervised DEP devices are deprecated as of iOS 12+

☐ Is MDM removable
Allows unenrollment

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

☐ Automatic Advance
Automatic advance through the Apple TV or macOS 11+ setup assistant

Shared iPad options

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

5 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.
As of iPadOS 13.4, the maximum number of users will always be 32 ; the number of resident users can be set here or later with Command Policy Profile.

Requirements

Minimum OS version

The minimum OS version that the enrolling device is required to install, e.g. 17.1. A supplemental version identifier can be included, e.g. 17.1 (a).
Available for macOS 14+ and iOS / iPadOS 17+

WARNING: The OS version must match the version format used by Apple and be installable on the device otherwise enrollment will fail.

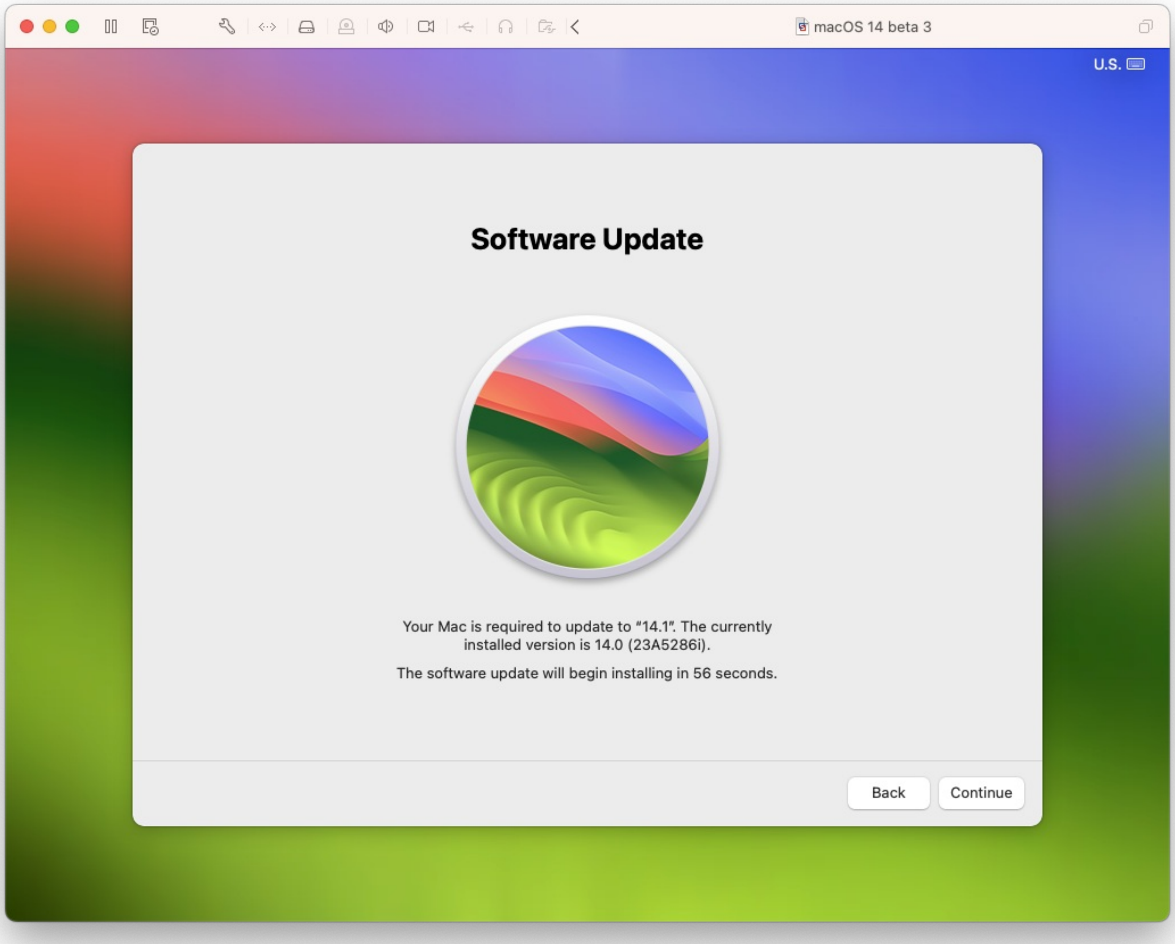
☑ macOS 14.1 (a)   ☑ iOS / iPadOS 17.1 (a)

The supplemental version identifiers can be specified in addition to standard MAJOR.MINOR.PATCH format (for example “17.1 (a)“).

What is displayed on the device?

When minimum OS version is requested by MDM server specific dialog appears on the device.

For macOS:

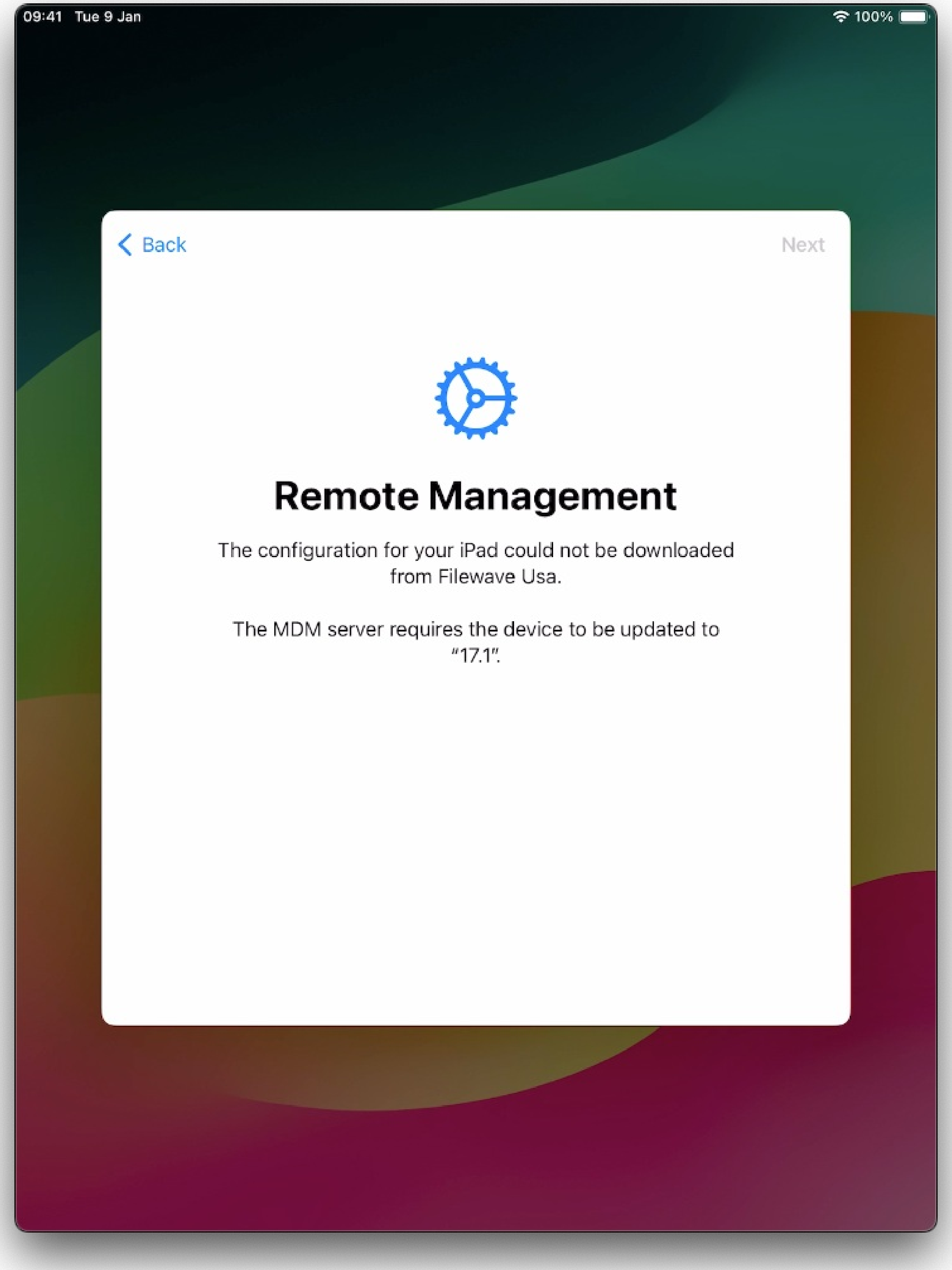


Software Update

Your Mac is required to update to "14.1". The currently installed version is 14.0 (23A5286i).

The software update will begin installing in 56 seconds.

For iPadOS:

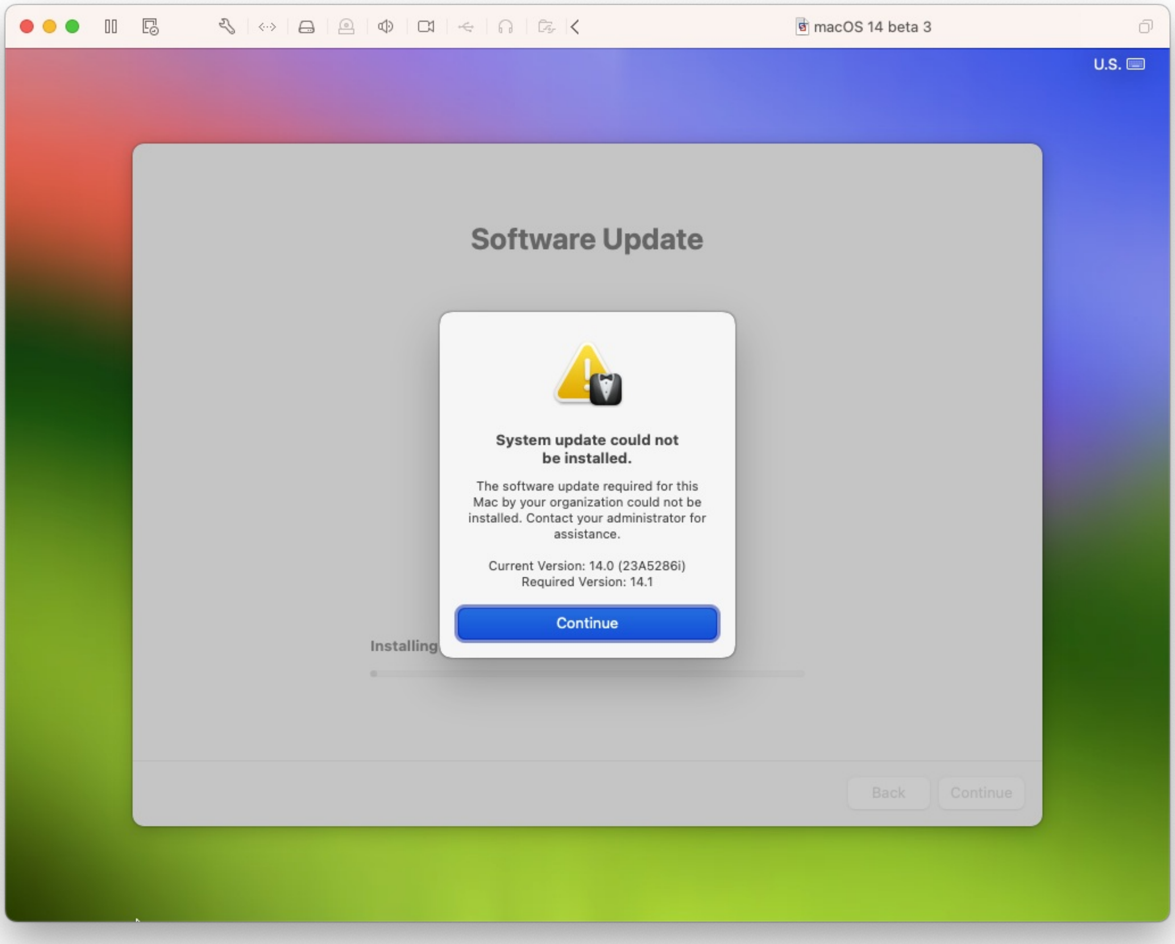


Remote Management

The configuration for your iPad could not be downloaded from Filewave Usa.

The MDM server requires the device to be updated to "17.1".

If macOS device cannot install requested OS version next dialog appears:



System update could not be installed.

The software update required for this Mac by your organization could not be installed. Contact your administrator for assistance.

Current Version: 14.0 (23A5286i)
Required Version: 14.1

On iPadOS there is no specific dialog in this case, just “Next“ button is grey and no way to pass.

Related Content

- Automated Device Enrollment (ADE)

Digging Deeper

`MachineInfo` from the device is parsed on server side during DEP profile handling. If it contains `MDM_CAN_REQUEST_SOFTWARE_UPDATE` flag and it’s True, the specified minimum OS version from DEP profile is compared with `OS_VERSION` from `MachineInfo` according to the device type (macOS or iOS/iPadOS). Software update request is sent to the device by MDM server in 2 cases:

1. If current OS version is less than minimum OS version
2. If current OS version equals minimum OS version but current supplemental version identifier is less than required supplemental version identifier.

The software update request from the server looks like 403 JSON response with next body:

```
{
    "code": "com.apple.softwareupdate.required",
    "details": {"OSVersion": <minimum OS version> }
}
```

In this case enrollment is interrupted by dialogs mentioned above.

Test macOS ADE (DEP) Enrolments with a Virtual Machine

Description

Testing macOS device enrolments can be very time consuming, since a device must be erased and OS reinstalled on each attempt. A Virtual Machine (VM) may be used to substantially reduce the amount of testing time. Although VMware has been used in this example, other Virtualisation software could be used, e.g Parallels.

Requirements

- Copy of VMware Fusion
- macOS installer, e.g. Install macOS High Sierra.app or a VMware Fusion installed on a relevant macOS device
- A registered macOS device serial number and optionally a Model Identifier, e.g. MacBookPro15,1

Obtain a serial number for a device that is registered in ABM or ASM.

> Any one serial number of a device should only occur once in FileWave. Therefore, if there is an old or broken device which is registered in ABM/ASM, consider using the serial number from this device otherwise a serial number from a usable, physical device will need to be taken, meaning that physical device cannot be used within FileWave otherwise.
>
> Mactracker may be used to show the Model Identifier of devices, since ASM/ABM only provides the Model Name

Directions

1. Use VMware Fusion to create a new image from disc and use the macOS installer app or choose to create an image from the recovery partition
2. Once completed, do no hit play. Instead, locate the virtual machine in Finder. If the VM starts, shut it down before continuing.
3. From Virtual Machine Library, right click and choose show in Finder.
4. From Finder, right click the highlighted VM and choose 'Show Package Contents' or use Terminal to navigate inside this VM
5. Locate the file with a .vmx extension and choose an editor to edit this .vmx file
6. Two lines need to be added as below. Replace Serial Number and Model Identifier as appropriate (remove brackets, but keep quotes):

```
serialNumber = "[Serial Number]"
hw.model = "[Model Identifier]"
```

1. Now Play the VM
2. Select language and once the option to re-instal the operating system is shown, choose utilities and Terminal
3. Type the following line to confirm that the VM has the appropriate serial number:

```
ioreg -l | grep "IOPlatformSerialNumber"
```

1. Quit Terminal and choose to re-instal the operating system
2. Have a cup of tea!
3. Disable network settings at the earliest, allowable moment, before the device comes back up and finalises the installation
4. Snapshot the VM when the Choose Language prompt is shown

> A device receives an associated DEP profile before the option to select the language appears after installing the operating system. Once in place, the device will maintain this profile across reboots. If the network is not disabled before receiving the Enrolment profile, then changes to the Enrolment profile associated or assigning a new DEP profile subsequently, will have zero impact on a fresh Enrolment; the original Enrolment settings will continue to apply.
>
> By disabling the network before the Enrolment profile is in place and then taking the snapshot, multiple Enrolment profiles or changes may be tested with each restore of the snapshot. On each restore, the network should require enabling.

Tested on VMware Fusion 10, 11 and 12

DEP Troubleshooting

Apple Device Enrollment Program (DEP) is a service provided by Apple that allows organizations to easily deploy and manage iOS, iPadOS, macOS, and tvOS devices. It streamlines the initial setup and configuration process for large-scale device deployments, making it easier for businesses, educational institutions, and other organizations to integrate Apple devices into their workflows.

Correct DEP Workflow

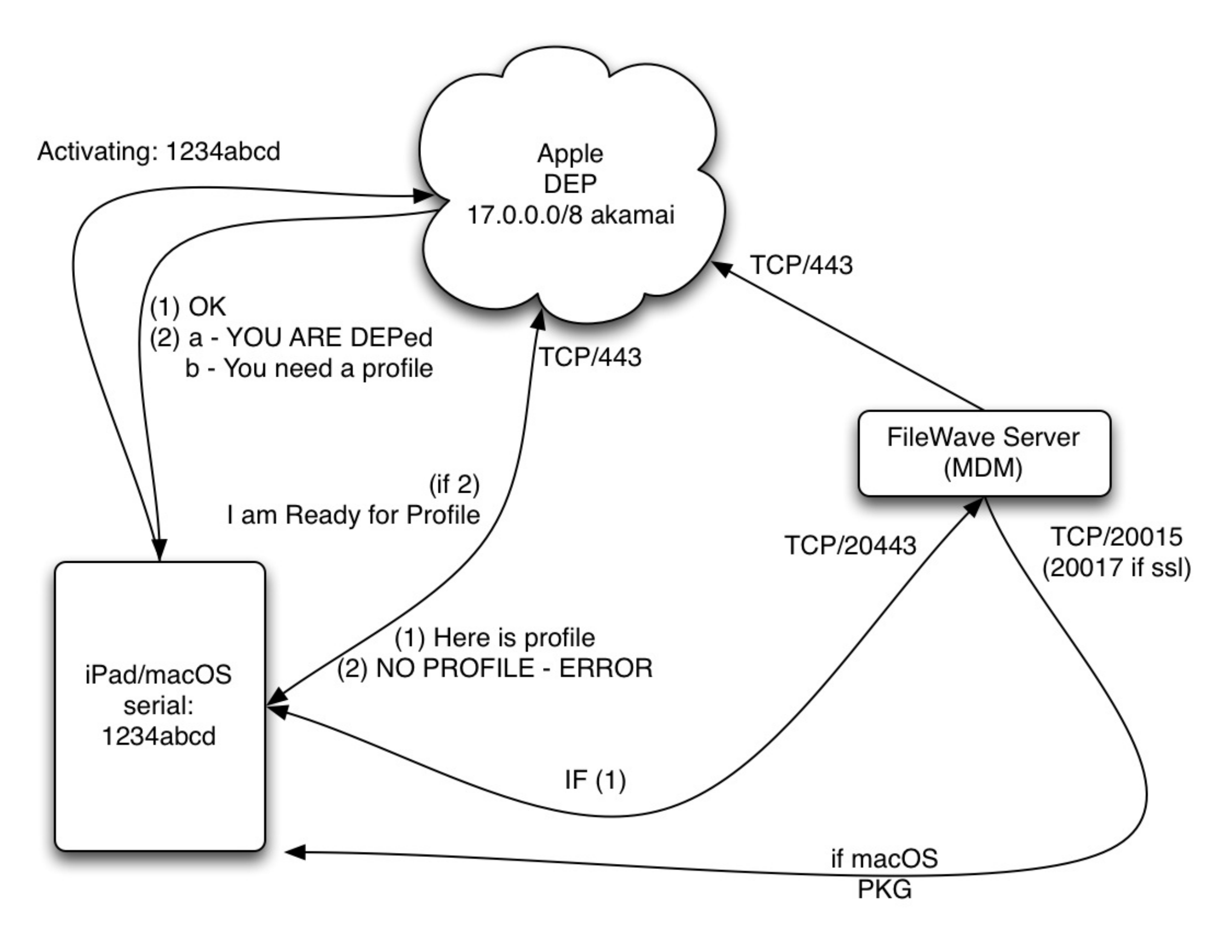


Figure 1.1 - DEP Workflow

1. Device activates to apple (see ports: Default TCP and UDP Port Usage)
   1. Devices is not in DEP - Apple responds with done - Setup Assistant skips enrollment
   2. Devices is in DEP - Apple responds with enrollment ownership info
2. Apple sends the DEP profiles to the device (See: Working with Apple's Device Enrollment Program (DEP))
3. Devices installs the DEP profile which makes it reach out to FileWave MDM server
4. Device MDM enrolls
5. (if macOS) Devices then installs the macOS PKG

Things to Test

Check the connectivity

- Check the Default TCP and UDP Port Usage KB article for the needed ports.

> You can download a FileWave port testing tool from https://supportresources.filewave.com/

- Get a devices (like a laptop) onto the same wifi devices enroll with
- Try enrolling iOS/iPadOS devices with ethernet or a mobile hotspot to see if the network restrictions are doing something to block traffic.

You can get devices to join ethernet by creating an adapter using

- Apple's "Lightning to USB 3 Camera Adapter" (the one with a female USB and another lightning port)
- Apple's "Apple USB Ethernet Adapter"
- A USB charger suppling 2+ amps of power

Plug in the device and make sure you get a link light.

Check the profile

Because these profiles are stored with Apple for the devices, when new options become available in DEP profiles FileWave can't just auto-update existing ones. If you have upgraded your FileWave instance recently you might want to create a new one and change your auto assignment rules (Automatically Assign DEP profiles). Do not duplicate an existing profile.

DEP Forbidden Error

Description

On creating a DEP Association or from any other DEP synchronisation action, the following error may be observed: DEP error: Forbidden

The most likely causes are:

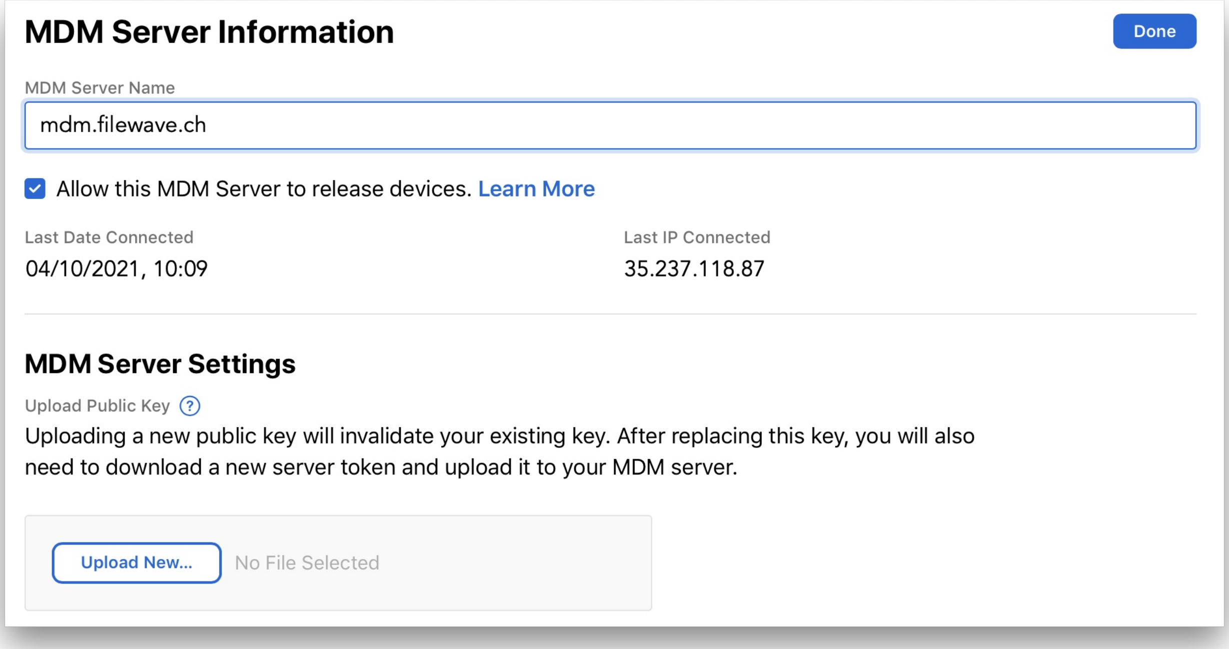
- Server SSL certificate change. Check Preferences > Mobile tab to ensure the server SSL certificate is not revoked or expired.
- A change to the external IP address of the FileWave Server.

Apple store the external IP of the FileWave Server from the last successful contact. If this differs at the time of a synchronisation , the action will fail and the DEP Server Token will need to be replaced.

The stored IP may be observed from the relevant DEP account:

- Apple Business Manager
- Apple School Manager

The Last Date and IP Connected may be seen from the Settings view; select the MDM Server and choose Edit.



MDM Server Information

MDM Server Name: mdm.filewave.ch

☑ Allow this MDM Server to release devices. Learn More

Last Date Connected: 04/10/2021, 10:09

Last IP Connected: 35.237.118.87

MDM Server Settings

Upload Public Key

Uploading a new public key will invalidate your existing key. After replacing this key, you will also need to download a new server token and upload it to your MDM server.

Requirements

- FileWave MDM DEP Certificate

Resolution

Forbidden error requires the token be replaced and not updated.

From FileWave Admin > Preferences > VPP & DEP:

1. Choose 'Download certificate' (requires fwadmin password) to save the certificate

From the relevant Apple DEP account Apple Business Manager or Apple School Manager:

1. Select 'Settings'
2. Highlight the MDM server from the list and choose Edit
3. Select 'Upload New...' and select the saved downloaded file from above
4. When prompted, select to download the DEP Server Token

From FileWave Admin > Preferences > VPP & DEP:

1. Click 'Configure Accounts' (requires fwadmin password)
2. Select the Forbidden token and use the '-' button to remove that token
3. Select the '+' button to select the DEP Server Token downloaded from Apple
4. Run a DEP Synchronisation Full Sync (Hold down ALT(macOS), Option(Windows)), then select to synchronise (the name of the button will change)

At this stage synchronisation should now be successful.

> ℹ If the DEP Server Token is currently configured in the Education tab of Preferences, this association will need to be removed prior to removing the DEP token, but may be re-added again afterwards.