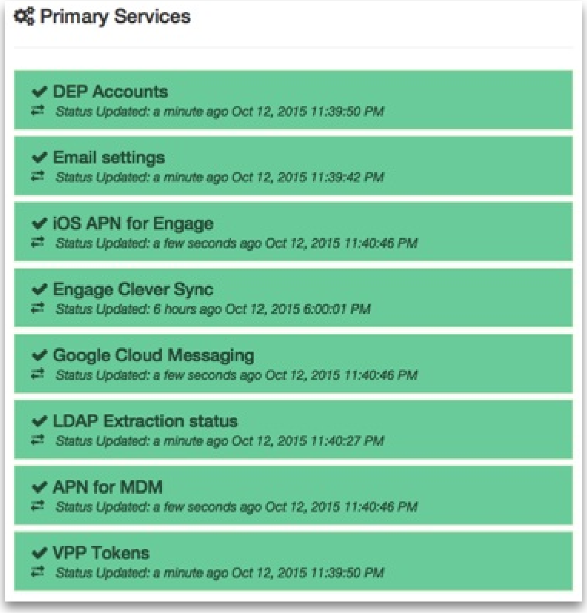
Settings

Configuring and using the Dashboard

In FileWave Central, the Dashboard is the first view an administrator gets of their FileWave environment. The Dashboard is designed to give the FileWave administrators a quick view of their server and be able to focus in on a missing setting, or a possible service interruption. There are seven major sections on the Dashboard.

Primary Services

This section shows the major services - DEP, VPP, Email, etc with last update and, if there is an error, a direct link to the settings that can address that error.



Primary Services

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

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

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

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

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

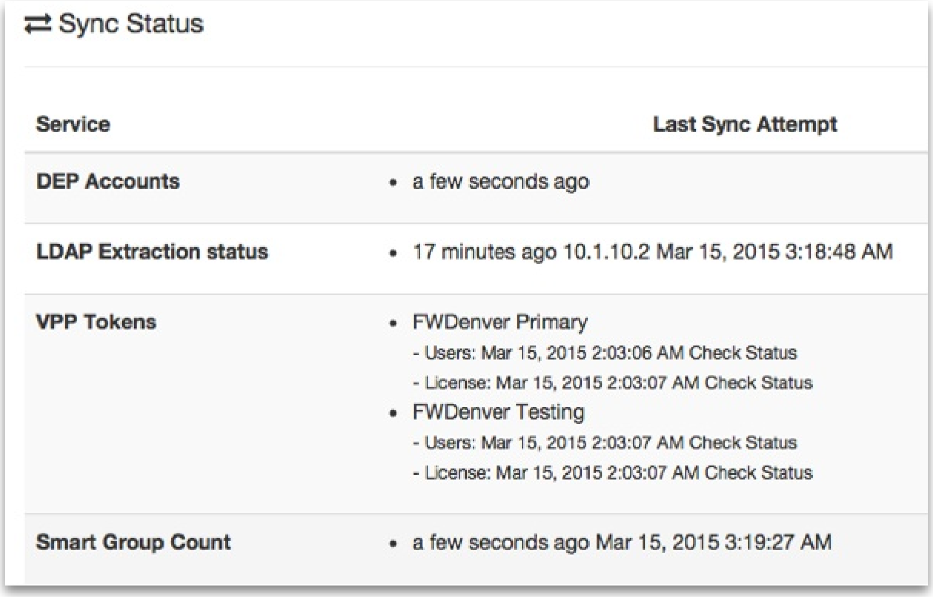
✓ LDAP Extraction status
⇄ *Status Updated: a minute ago Oct 12, 2015 11:40:27 PM*

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

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

Sync Status

This section shows the latest 'check-in' times for certain services, such as VPP, DEP, LDAP, and Smart Groups. These services all have preferences requiring synchronization between a remote service, for example your LDAP server, and the FileWave server.

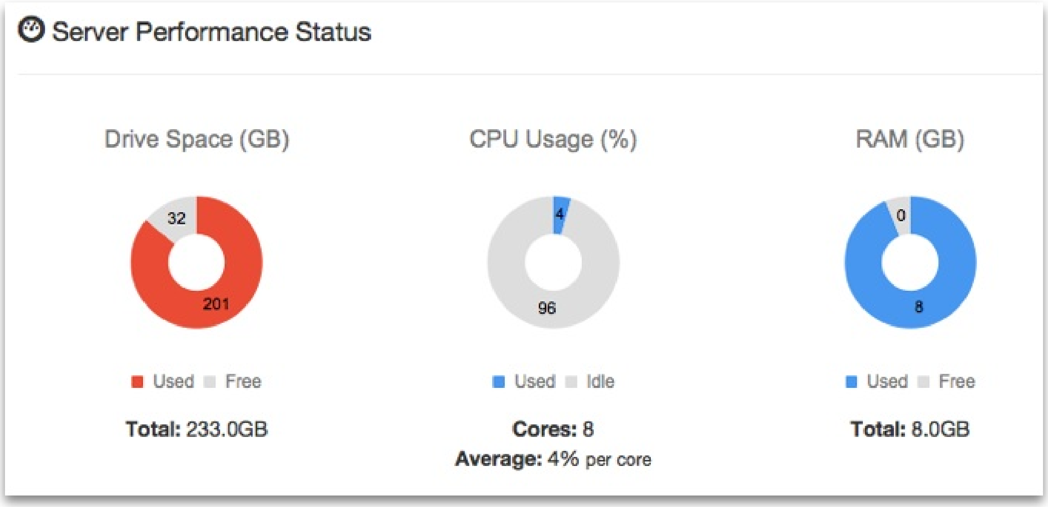


⇄ Sync Status

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

Server Performance Status

This section is an active chart of the status of the primary FileWave server's storage space, CPU usage, and RAM utilization.


Server Performance Status

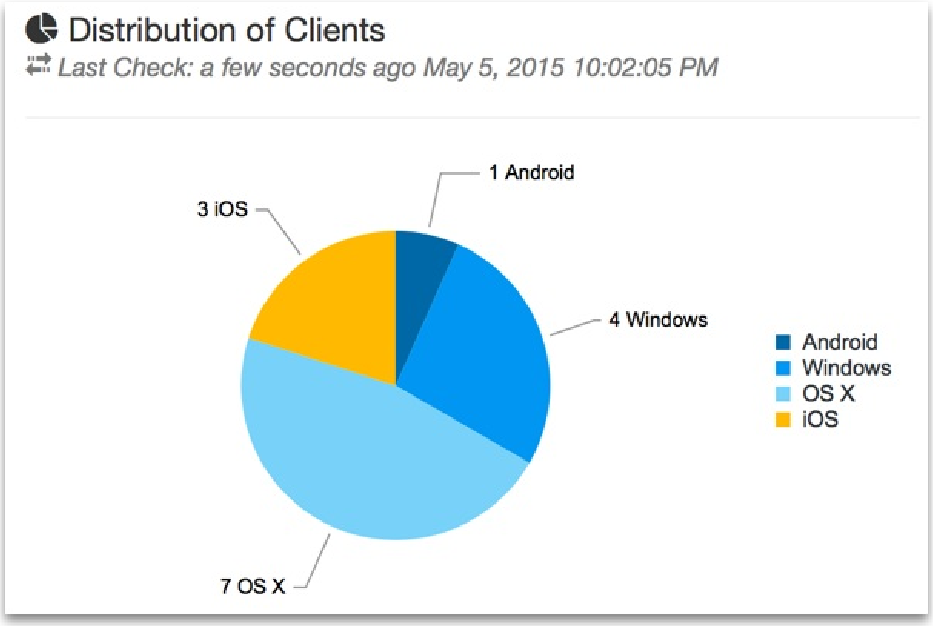
Total: 233.0GB

Cores: 8
Average: 4% per core

Total: 8.0GB

Distribution of clients

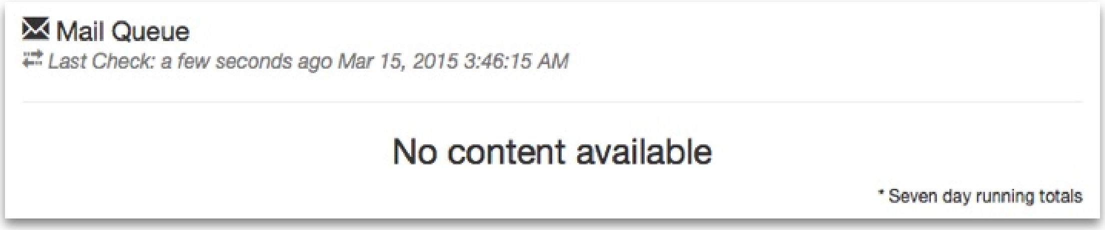
This section displays a graph showing the breakdown of FileWave clients based on operating system.


Distribution of Clients

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

Mail Queue

This section displays a running graph of the status of emails sent from the FileWave server. The focus will be on the VPP / MDM invitation emails. This will help you see situations where your local email server may be getting overwhelmed by the large number of MDM invitations going out at the same time.


Mail Queue

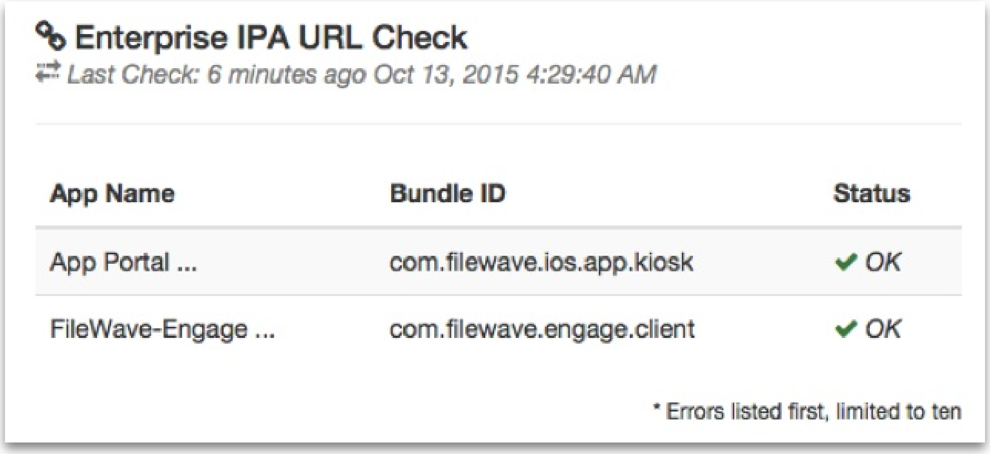
Last Check: a few seconds ago Mar 15, 2015 3:46:15 AM

No content available

* Seven day running totals

Enterprise IPA URL Check

This section shows the validity of your institutionally created iOS apps as well as the enterprise apps provided by FileWave (iOS App Portal / Kiosk and Engage).



Enterprise IPA URL Check

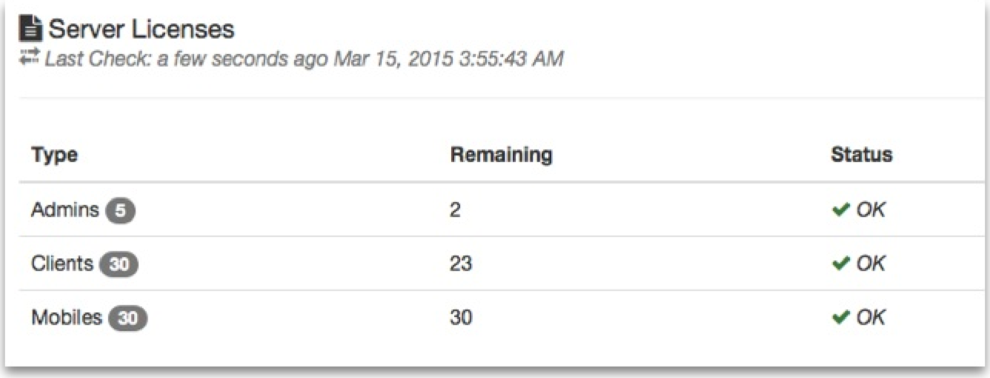
Last Check: 6 minutes ago Oct 13, 2015 4:29:40 AM

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

* Errors listed first, limited to ten

Server Licenses

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



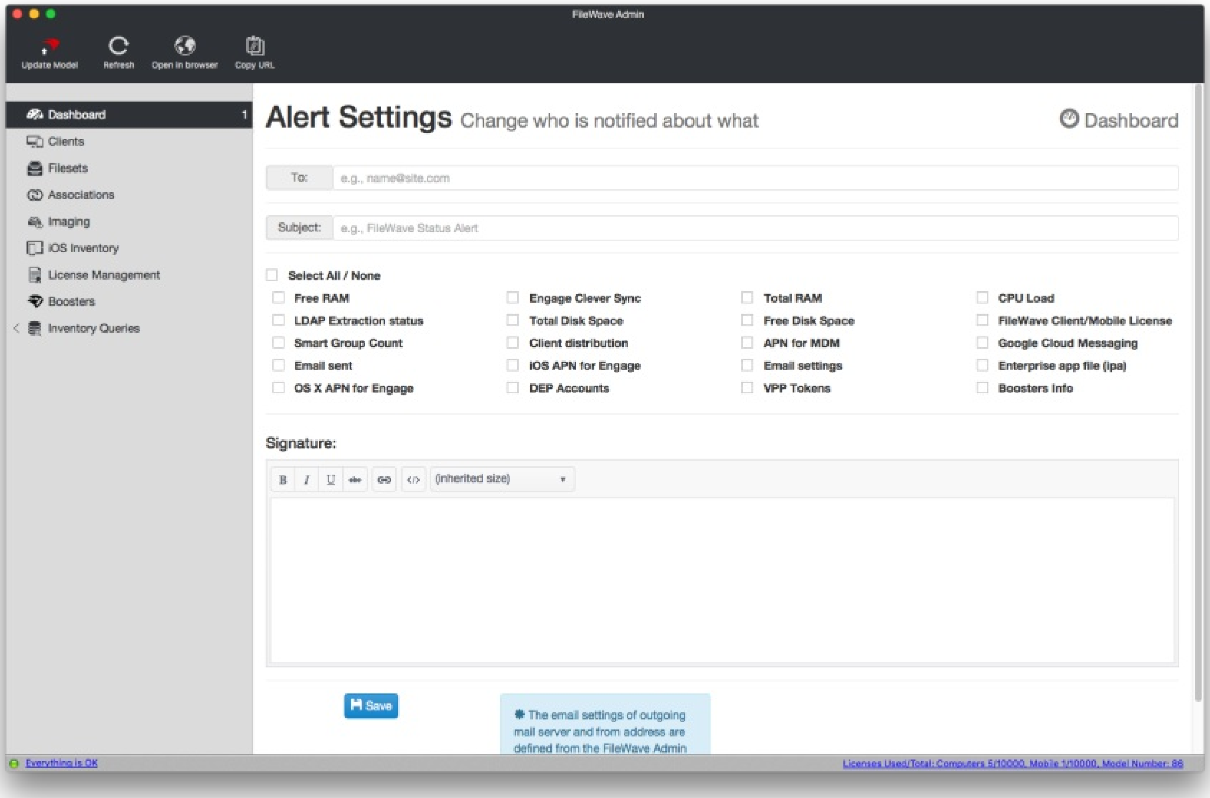
Server Licenses

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

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

Alert Settings

The Dashboard provides FileWave Central with the ability send notifications out to individuals at status changes on the server. You toggle between the Alert Settings and the Dashboard in order to configure the types of alerts sent out and who they are sent to.



Alert Settings Change who is notified about what

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

Subject: e.g., FileWave Status Alert

☐ Select All / None

☐ Free RAM
☐ LDAP Extraction status
☐ Smart Group Count
☐ Email sent
☐ OS X APN for Engage

☐ Engage Clever Sync
☐ Total Disk Space
☐ Client distribution
☐ iOS APN for Engage
☐ DEP Accounts

☐ Total RAM
☐ Free Disk Space
☐ APN for MDM
☐ Email settings
☐ VPP Tokens

☐ CPU Load
☐ FileWave Client/Mobile License
☐ Google Cloud Messaging
☐ Enterprise app file (ipa)
☐ Boosters Info

Signature:

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

Everything is OK

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

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

"Detachable" Dashboard

The Dashboard is part of the FileWave Central application; but it can also be dragged off to be viewed as a separate window on the administrator's computer, opened in a browser, or provided as a URL to other interested parties to view on their own computers or devices.

Dashboard Alert details

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

Related Content

- FileWave Server Mail test receives Bad Request with Google Accounts
- Dashboard Warning levels and Descriptions

Mobile Preferences - iOS / Android

The Mobile preferences are designed around Mobile Device Management for Apple's iOS/macOS and Google's Android/Chromebooks. This section discusses setting up the basic components in FileWave Central/Preferences.

Configure MDM Server

- MDM Server Address - Enter your MDM server's FQDN or routable IP address.
- Port - The default port for FileWave MDM is 20445.
- Shared Key - This is used to create a secure connection between the MDM Server and the FileWave Server. Generate a new key on Save only needs to be done once and is applied when the preferences are closed with the OK button.

Mobile Certificate Management (HTTPS Certificate Management)

This section shows the information used by FileWave to create a valid certificate that will be used to authenticate the FileWave MDM server with your clients and with Apple's Push Notification System.

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

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

Apple Push Notification Certificate (APN) for iOS

The APN certificate is required to allow the application developers to send notifications to their applications, such as the Weather app getting current storm alerts. In order to allow the applications you deploy to your mobile devices to get these notifications, you request a secure certificate from Apple. The process for getting the certificate is detailed in the Appendix for FileWave administrators running either OS X or Windows.

Once you have received your APN Certificate from Apple, you will add it by clicking on the Upload APN Certificate/Key Pair button. This will configure your FileWave MDM server to support secure communications with Apple's Push Notification service.

Android/Chromebooks MDM Configuration

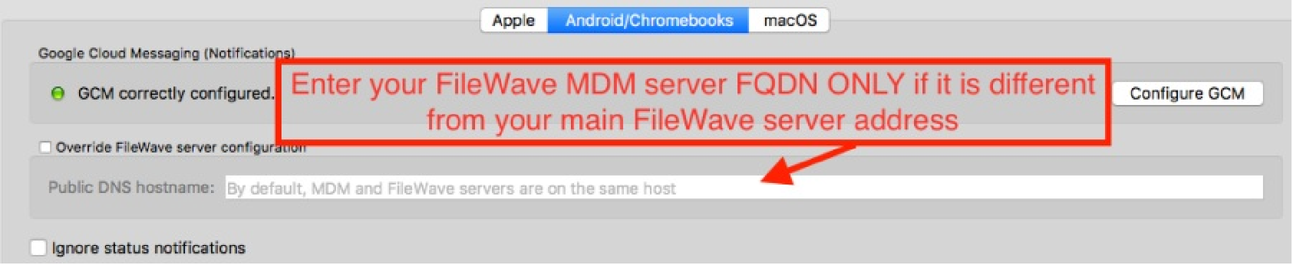
If you are deploying Android clients, then you will need to configure the Android/Chromebooks section of the Mobile preferences. You will need to get a Project Number and API key from Google. Instructions on how to accomplish that task are in the Appendix. Once you have those two items, go to the FileWave Preferences / Mobile pane and select the Android/Chromebooks tab.
Select the Configure GCM button, authenticate as the FileWave super administrator, then enter the Project Number and the Server API key you were given.

Click on Save and you should immediately see that GCM is correctly configured.

Override FileWave Server configuration

The Android client is a composite of the computer and iOS client. It must connect to both the FileWave Server and the FileWave MDM server. Enrollment is done the "iOS" way through the MDM portal; but the client must also connect to the main FileWave server for additional functionality. In most cases, this is not an issue because the FileWave Server and the FileWave MDM server are on the same system. However, it is possible for you to configure the two services to run on different systems with differing external IP addresses.

If you are hosting the MDM service on a different system, then you will need to check the Override FileWave server configuration checkbox and enter the FQDN name of your main FileWave server. Do not enter anything in this section if you are running your FileWave MDM services on the same system as your primary FileWave server.



Google Cloud Messaging (Notifications)

● GCM correctly configured.

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

□ Override FileWave server configuration

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

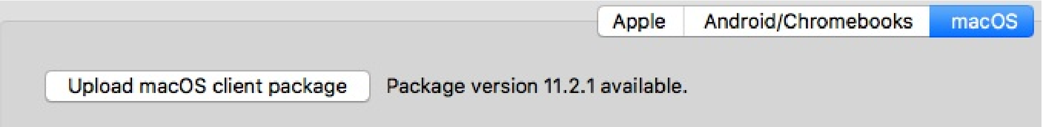
□ Ignore status notifications

macOS MDM configuration

For macOS devices, you will need to request a custom FileWave Client installation package (.pkg) and upload it to your FileWave server. This allows FileWave to provide the package for all MDM enrolled devices. When a MDM macOS device is added to your FileWave server, it will automatically receive the client installer package and will be configured as one of your client devices.

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

The first step is to go to the FileWave Support site and request a custom installer: https://custom.filewave.com
Download the zip file and then expand it to have the PKG. When you have the package, you will upload it to your FileWave Server using the button in the macOS MDM preferences pane:

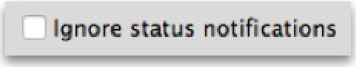


Package version 11.2.1 available.

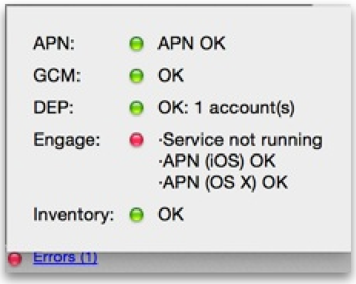
Authenticate as the FileWave Central superuser (fwadmin), then locate the newly downloaded package. Note: You must unpack/unzip the package before being able to upload it to your server!

Ignore status notifications

In the lower left corner of the main FileWave Central window is the status box for your key external services - Apple Push Notification (APN), Google Cloud Messaging (GCM), Apple Device Enrollment Program (DEP), Engage server (if used) and Inventory. You have the option of installing the MDM services on a different system, or not needing APN, DEP, or GCM at all - assuming you aren't using any iOS devices, macOS systems with VPP, or Android devices. If any of these services are not running, the status indicators will show that there is a problem. You can disable status notifications and FileWave Central will report only the services you are using.



□ Ignore status notifications



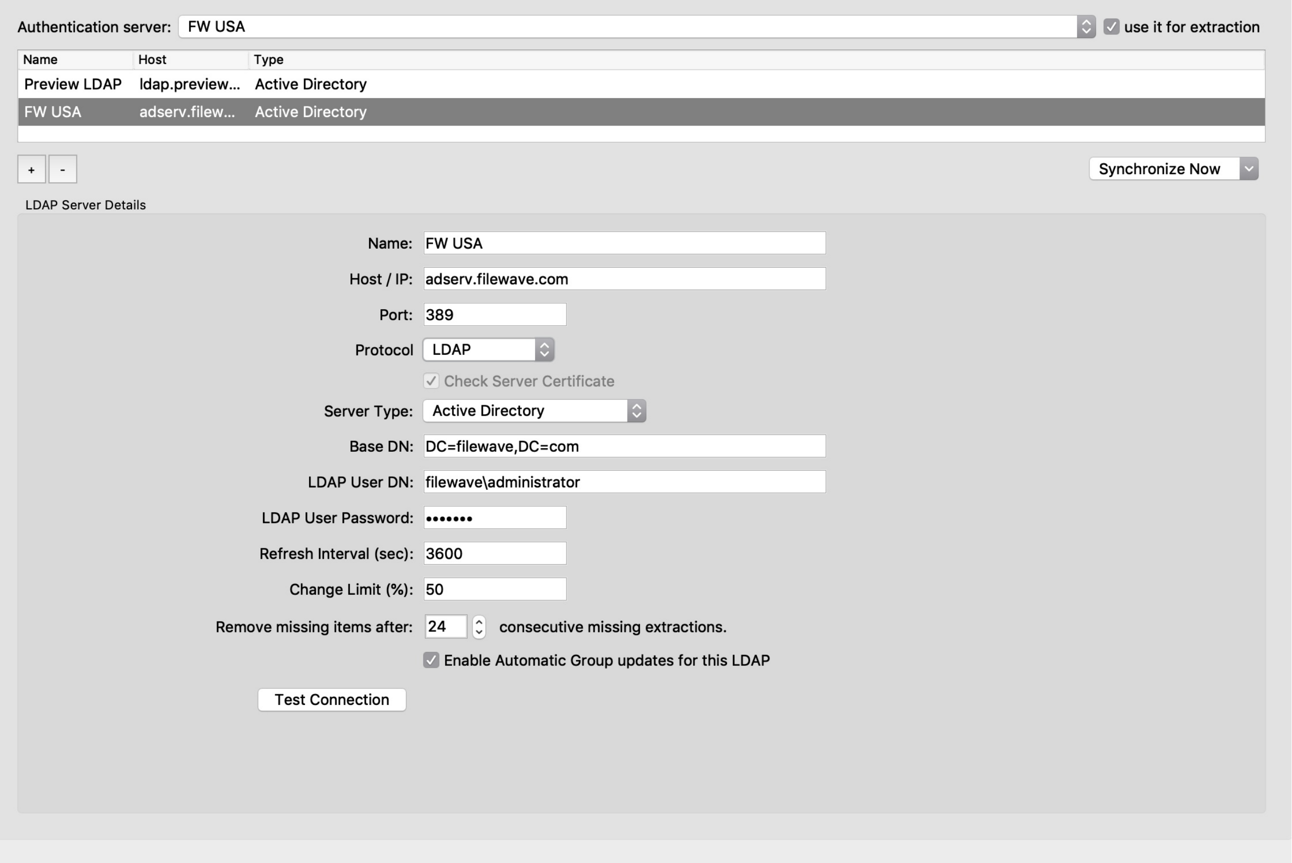
APN: 🟢 APN OK
GCM: 🟢 OK
DEP: 🟢 OK: 1 account(s)
Engage: 🔴 ·Service not running
·APN (iOS) OK
·APN (OS X) OK
Inventory: 🟢 OK

🔴 Errors (1)

LDAP Preferences

FileWave supports connecting your LDAP network directory – Active Directory, Open Directory, or eDirectory – to your FileWave Server. This capability provides access to directory information for use in Smart Groups and parameterized profiles. You can also use LDAP for enrollment authentication. Using LDAP to authenticate your devices gives you a way to know who (which LDAP user) enrolled what device.

Creating an LDAP server entry in Preferences



Authentication server: FW USA ☑ use it for extraction

Name	Host	Type
Preview LDAP	ldap.preview...	Active Directory
FW USA	adserv.filew...	Active Directory

Name: FW USA

Host / IP: adserv.filewave.com

Port: 389

Protocol: LDAP

☑ Check Server Certificate

Server Type: Active Directory

Base DN: DC=filewave,DC=com

LDAP User DN: filewave\administrator

LDAP User Password: •••••••

Refresh Interval (sec): 3600

Change Limit (%): 50

Remove missing items after: 24 consecutive missing extractions.

☑ Enable Automatic Group updates for this LDAP

Use the [+] button to create a new LDAP server entry and enter the needed connection information as described below:

- Name - a reference name used by you to differentiate your LDAP servers
- Host / IP - enter either a FQDN or IP address for your LDAP server
- Port - enter the TCP port required to access your LDAP server (you may need to check with your network support)
- Protocol – select LDAP, LDAPS, STARTSSL.
  - For LDAPS and STARTSSL you have a checkbox that you can potentially uncheck so that the server certificate is not checked against the machine's trust store.

> ⚠ IF LDAPS or STARTSSL it is recommended to be using a trusted LDAP cert.

- Server Type - choose Active Directory, Open Directory, or eDirectory
- Base DN - enter the primary distinguished names (DN) for your LDAP server using the domain components separated by commas. For example, if the LDAP server is running on the same box as the FileWave server, your base DN may be as simple as "dc=home,dc=local"; but if the LDAP server is running on a different system, the value of the base DN may be involve using a more extended value, such as "dc=tanner,dc=filewave,dc=net".
- LDAP User DN - if you are doing authenticated binds to your LDAP server, you will need to enter a valid user account that has been designated for binding. If you are doing anonymous binding, this entry is left blank.
- LDAP User Password - enter a password to complete the authenticated bind; not needed for anonymous binds
- Refresh Interval (sec) - enter a value in seconds for the FileWave Server to contact the LDAP server to refresh the available data. If you are just setting up a FileWave server on a network with an established LDAP server, you should set the interval relatively short (~120 seconds) while you are testing and making changes. Once you go into production mode, you should change the interval to 24 hr. (86,400 seconds).
- Change Limit (%) - LDAP related items will not be removed if more than the given percentage of the items disappear after a sync. This is to avoid loss of data if something goes wrong with the LDAP configuration.

> ⚠ If for example an entire OU is suddenly missing that makes up 25% of your LDAP directory, then the amount of change will be so large that FileWave will not initially accept the changes if you set Change Limit from 1% to 25%, but if you had it set to 26% it would accept that removal. When considering the next option in conjunction with this it can still take X amount of syncs for removals to occur.

- Remove Missing items after - 0 means that records not found in the LDAP server, but are still present in FileWave will be removed immediately.

> Setting it to a number that is equivalent to 24 hrs is recommended for safety.
>
> (Refresh Interval / 60(second to min) / 60(min to hrs)) * x = 24(hrs)
>
> So if I wanted an interval of 1800 seconds (30min), I would set my interval to 48

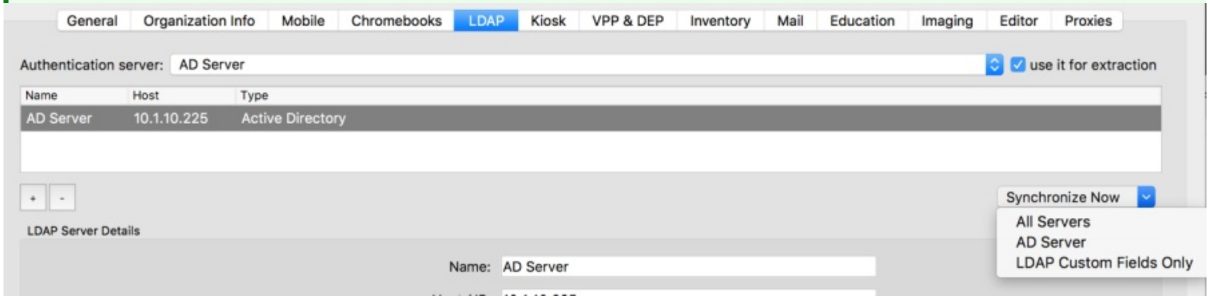
Enable Automatic Group updates for this LDAP creates a visible set of entries (Smart Groups) in the Clients pane under an LDAP designator. These Smart Groups will be updated by FileWave at the designated refresh interval
The information provided in the Clients pane for LDAP is a one-way view of your directory server. While changes made at the LDAP server are automatically reflected in FileWave; changes made in FileWave Admin do not affect the LDAP directory information.

> Choosing to enable the automatic Group updates creates a visible set of entries in the Clients pane of FileWave Admin, and keeps that information up to date; however, for an LDAP environment of over a few hundred records, the load on the LDAP server can get extremely heavy.

The Test Connection button pings the server to see if it is online; but does not verify all connection settings. You should always use an LDAP browser tool to verify the link to your server.
You can create entries for multiple LDAP servers, and an LDAP server can be running on the same device or VM as the FileWave Server.

An LDAP server can be chosen as the Authentication server which, in this case, means that the directory for that server will be used for profiles that support parameterized settings. Selecting the use it for extraction setting adds the directory information to the FileWave database. You can view the LDAP settings in the Assistants/LDAP Browser in FileWave Admin.

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



Authentication server: AD Server ☑ use it for extraction

Name	Host	Type
AD Server	10.1.10.225	Active Directory

Name: AD Server

VPP and DEP Preferences

FileWave supports both Apple's Volume Purchase Program (VPP) and Device Enrollment Program (DEP). In order to get these working within FileWave, you will need to configure certain preferences. This section just discusses the settings required in the Preferences.

Note: Instructions for joining and working with the Apple VPP and DEP programs from the Apple side are outlined in detail on these web sites:

https://help.apple.com/deployment/business/

https://help.apple.com/schoolmanager/

https://help.apple.com/deployment/ios/

https://help.apple.com/deployment/macos/

Warning: All of the configuration steps in this section must be done while signed in as fwadmin.

FileWave supports multiple tokens for the VPP service. This allows you to create multiple purchase authorities for your institution's App Store content. Content is automatically synchronized every 24 hours with the Apple VPP service. You may force a full synchronization when you are deploying a large number of App Store items, or any time that a delay may interfere with operational needs by holding down the Option key and clicking on the Synchronize button.

Volume Purchase Program preferences

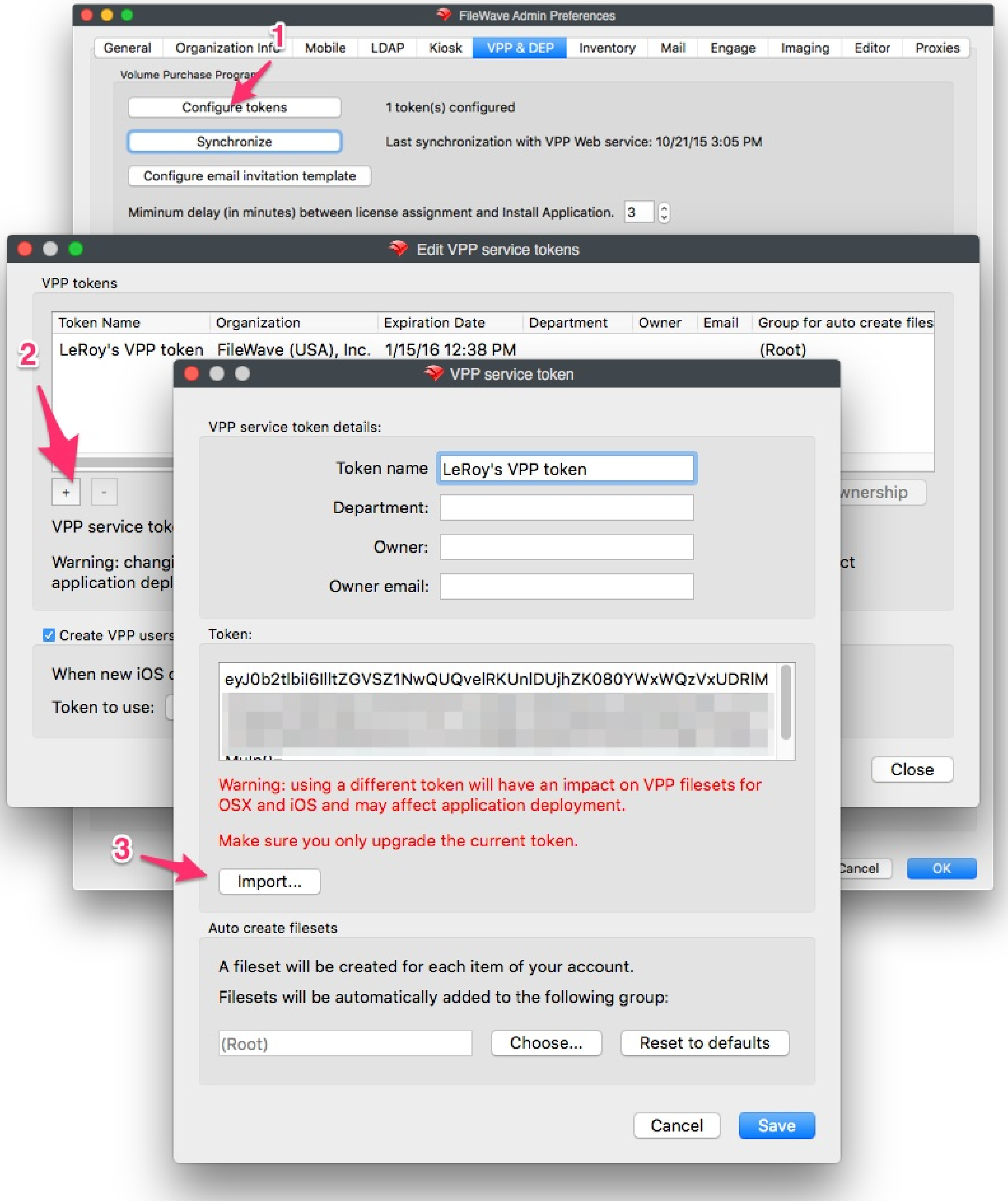
This pane contains the information for your VPP account with Apple. In order to proceed, you will have to have created a VPP for Education or VPP for Business account with Apple. Once you have a VPP account, you can download your VPP token for inclusion into FileWave. You may add as many tokens as you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

Configure VPP token(s)

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

Adding a VPP service token

Click on the [+] button (2) and import your downloaded VPP token (3). When you import the token into this pane, you will see a long alphanumeric hash as shown. Continue these actions until you have added all of the VPP tokens you plan to use for content distribution.



Volume Purchase Program

1 token(s) configured

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

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

VPP tokens

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

VPP service tok

Warning: changi ct
application depl

☑ Create VPP users

When new iOS d

Token to use:

VPP service token details:

Token name LeRoy's VPP token

Department:

Owner:

Owner email:

Token:

eyJ0b2tlbiI6IlltZGVSZ1NwQUQvelRKUnlDUjhZK080YWxWQzVxUDRlM
[redacted]

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

Make sure you only upgrade the current token.

Auto create filesets

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

Filesets will be automatically added to the following group:

(Root)

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

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

Auto-create Filesets

The first time you set up VPP, you will get Filesets automatically created for each of your existing VPP purchases. You can assign those Filesets to a designated FileWave Group for management. The default is the (Root) Group.

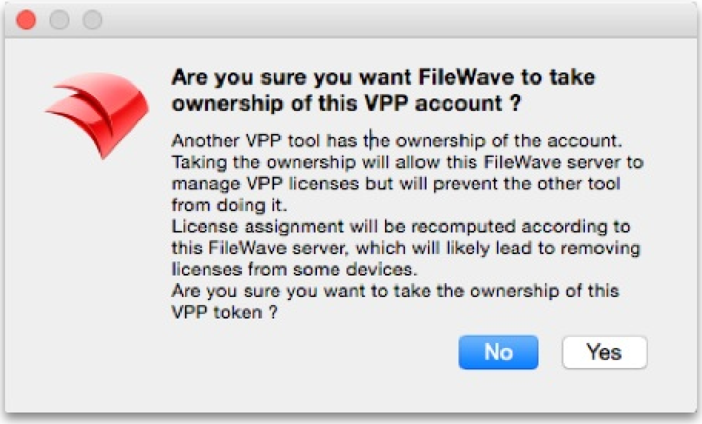
VPP account protection (aka "Take ownership")

One of the new features in FileWave v10 is protection of the VPP accounts and tokens that you use with your server. The concept is very simple: an identifier (called "client context") is sent to Apple for a given VPP account. When an MDM server has to use a VPP account, it will query this identifier and compare with its own; if they match, everything is fine. If they don't match, the server should not use the token.

As long as you are the confirmed owner of the token, the Is Owner flag says Yes;. If you have changed servers, or let another process, such as Apple Configurator, use that VPP token, then you will get an alert stating that the token is owned by another server.

If you have a mismatch, your VPP token entry will turn red, and you will not be able to use that token. Your first indication of an issue may be an alert in your Dashboard:

In order to regain control of the token, you will need to select the token entry and click on the Take ownership button in the lower right corner of the VPP tokens pane. Once you have done that, you will get a confirmation dialog:



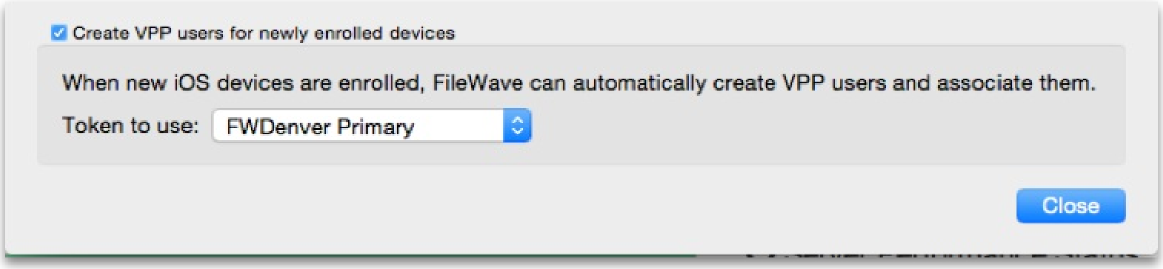
Are you sure you want FileWave to take ownership of this VPP account ?

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

The key to this process is making sure you do not apply any of your VPP tokens to a different server, tool, or application. If you are running a test/beta FileWave server or Apple Configurator, you should create a unique VPP account and token for that purpose.

Create VPP users for newly enrolled devices

Back in the Volume Purchase Program pane, you can elect to Create VPP users for newly enrolled devices. VPP users are internally created accounts that link your enrolled device to the FileWave VPP management process. It's not an actual "user" account; but more of a placeholder for the assignment of VPP apps and books. Each VPP user account may contain a link to an actual end user's Apple ID.



☑ Create VPP users for newly enrolled devices

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

Token to use: FWDenver Primary

If this checkbox is selected, then newly enrolled devices will automatically get a VPP user and that user account will be associated with the device. This can speed up mass deployments, as well as reduce the overhead on 1:1/BYOD deployments. Used in conjunction with settings in the VPP Assistant, your FileWave server can then automatically notify new user's to register their Apple ID with your FW MDM server. You can select a single VPP token to be the primary token related to those VPP users. Also, you can change which tokens are associated with specific VPP users as you need.

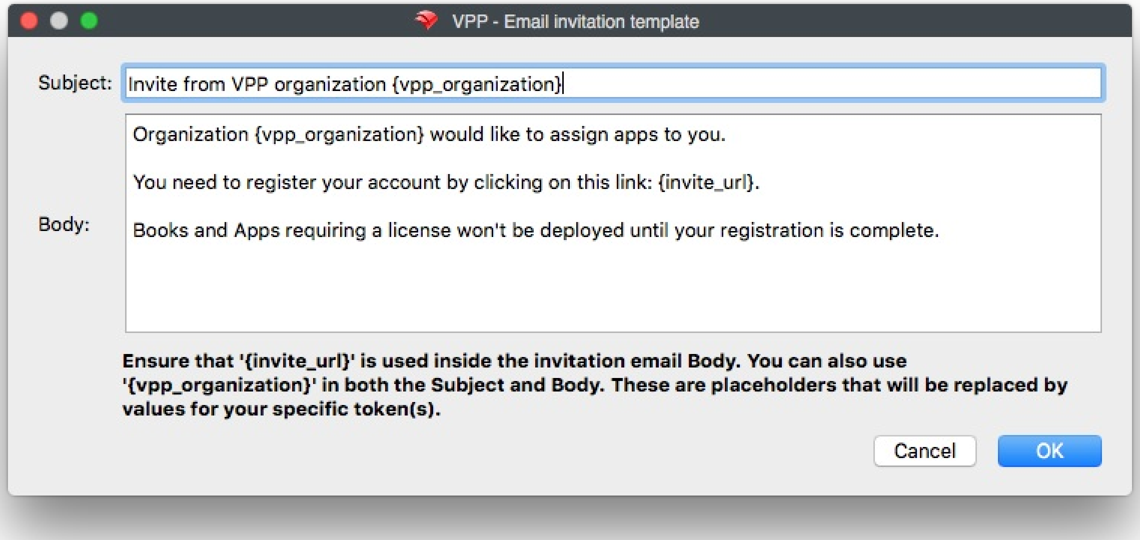
> Note: If you are using VPP device assignment for application distribution (versus assignment by user - Apple ID), a "ghost" or invisible VPP user account is created. This account is not visible within the VPP User Management pane.

Synchronization

The VPP Synchronization setting lets you determine how often the FW MDM server will match data with your assigned VPP token account. You can push an incremental synchronization by clicking on the Synchronize button; and you can force a full synchronization by holding down the Option key while pressing the Synchronize now button.

Configuring VPP email invitation template

This template will be used by your FileWave server to send an invite to users enrolling in your MDM from iOS devices and macOS computers. If you have configured your setup to use LDAP authentication for enrollment, then your users will get an email addressed to the mail account in their LDAP record. It will contain a custom URL pointing them to the Apple App Store where they will authenticate with their Apple ID to register that ID with your FileWave MDM.


VPP - Email invitation template

Subject: Invite from VPP organization {vpp_organization}

Body:

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

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

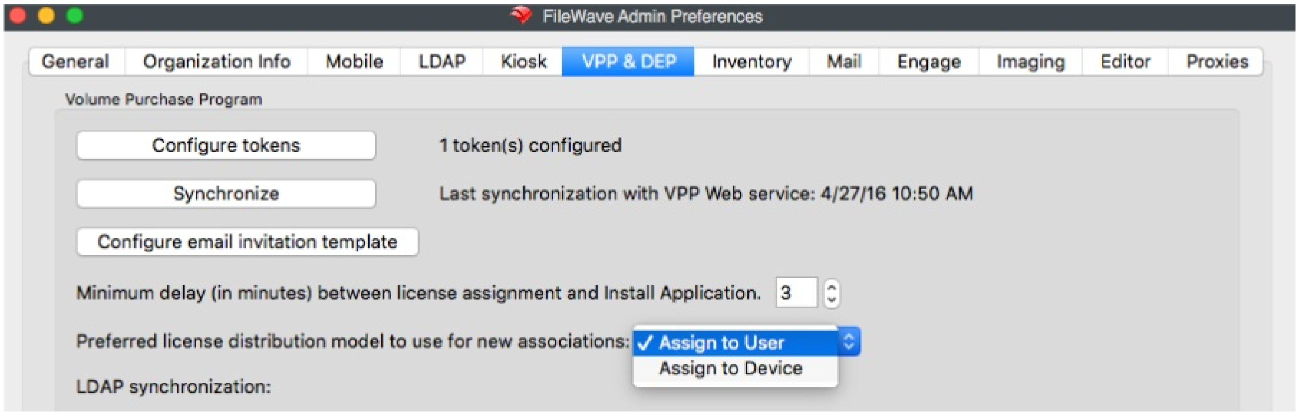
Books and Apps requiring a license won't be deployed until your registration is complete.

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

Minimum delay and Preferred Distribution

Starting with FileWave v10, you have the ability to establish a delay between the time you associate a VPP application with a license and when the application is made available to install at the client. This avoids issues during large scale deployments where clients are trying to install VPP applications; but haven't gotten their license assignment yet.

Preferred Distribution allows you to choose the method of deploying a VPP application. The original method has been to assign an application to a registered Apple ID (User). The license shows up in the user's Purchases, and the license can be managed by the FileWave MDM. The new method, supported in iOS 9+ and OS X v10.11+, allows you to assign VPP applications directly to an enrolled device (provided the app developer has coded the app to support this). This method applies only to VPP applications - iBooks are still required to be assigned to individual Apple IDs.


FileWave Admin Preferences

1 token(s) configured

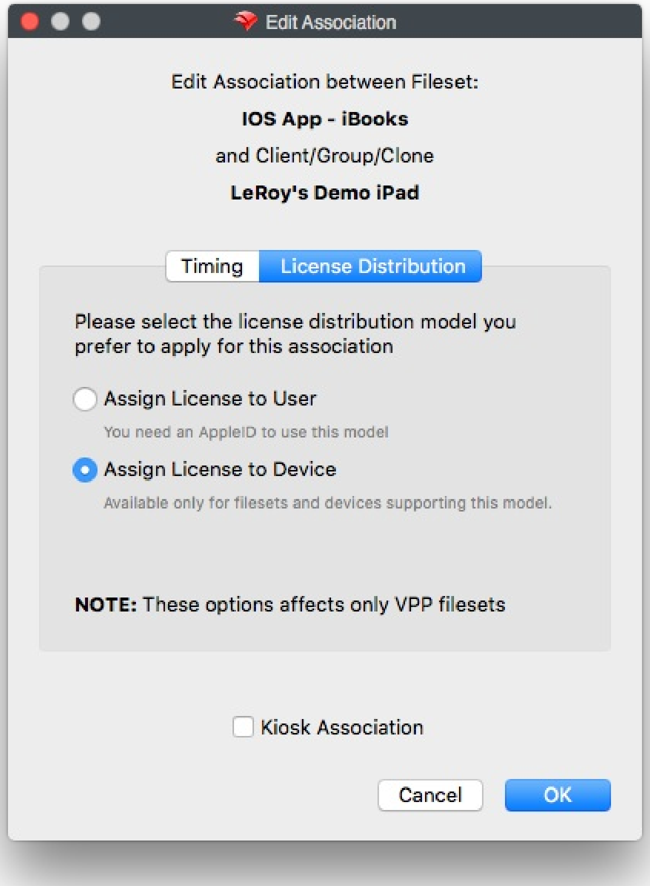
Last synchronization with VPP Web service: 4/27/16 10:50 AM

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

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

LDAP synchronization:

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



Edit Association

Edit Association between Fileset:

IOS App - iBooks

and Client/Group/Clone

LeRoy's Demo iPad

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

○ Assign License to User

You need an AppleID to use this model

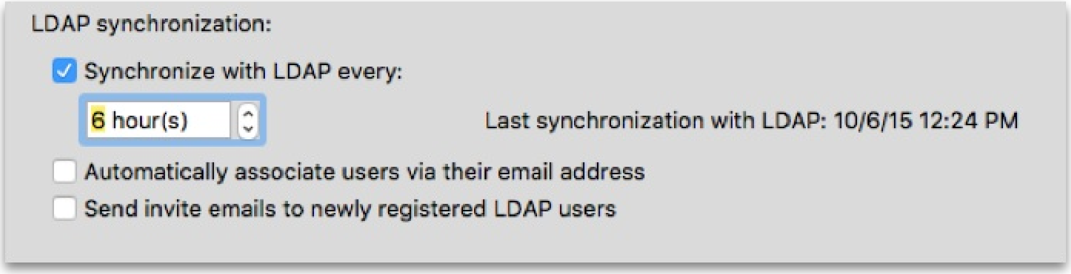
● Assign License to Device

Available only for filesets and devices supporting this model.

NOTE: These options affects only VPP filesets

□ Kiosk Association

Using LDAP synchronization allows you to link your LDAP users with VPP users, who can then be associated with their email addresses (if those exist in the LDAP directory). This allows you to have VPP/MDM emails automatically sent to those users. This process can be left off if you are going to use device assignment of all your distributed VPP applications.



LDAP synchronization:

☑ Synchronize with LDAP every:

6 hour(s)

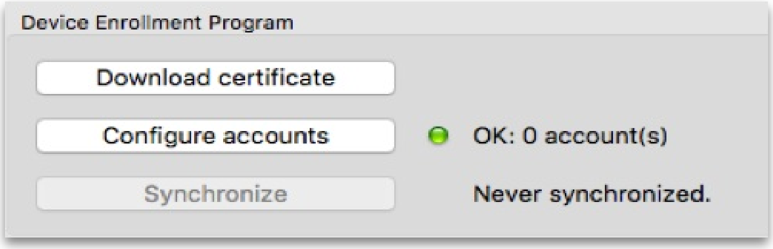
Last synchronization with LDAP: 10/6/15 12:24 PM

□ Automatically associate users via their email address

□ Send invite emails to newly registered LDAP users

Device Enrollment Program preferences

Apple's Device Enrollment Program is designed to support OTA (over the air - Wi-Fi) supervision of devices. FileWave supports iOS devices and macOS computers using DEP. Institutionally purchased devices are registered with Apple, and Apple provides a DEP token for you to link your FileWave MDM server to the DEP service. When a device comes up online, it is recognized by the Apple DEP service, matched to the downloaded token, and automatically configured for supervised management with your FileWave MDM. The preferences you set to get this process up and running are shown below.



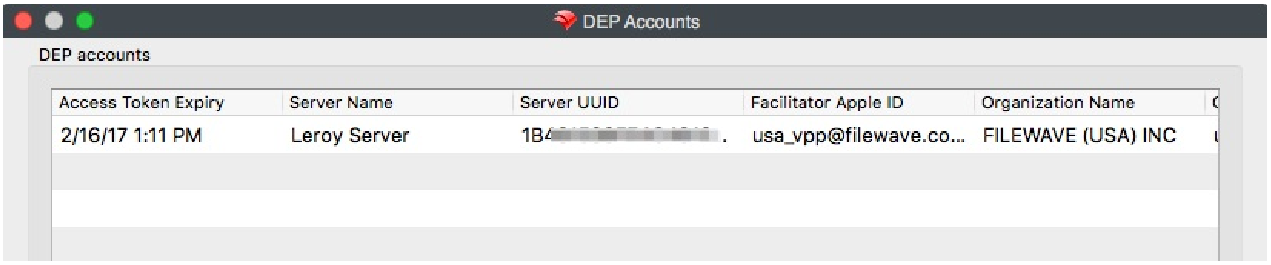
Device Enrollment Program

● OK: 0 account(s)

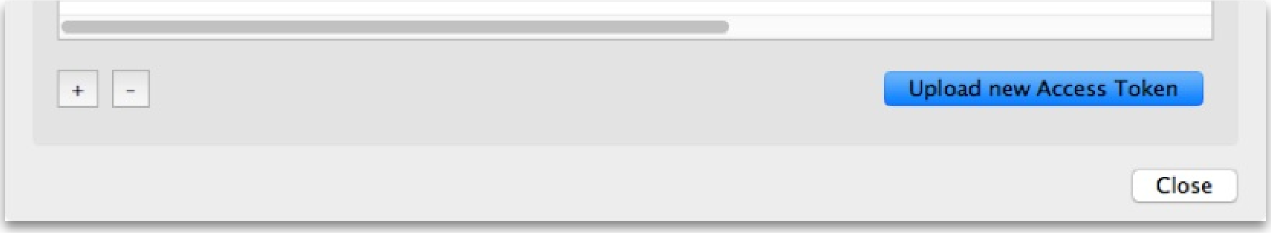
Never synchronized.

Using the "Download certificate" button, download a special "FileWave DEP" certificate to your administrator machine. You will be

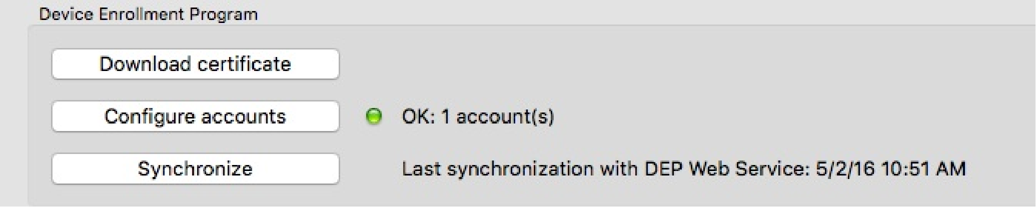
required to authenticate with the fwadmin FileWave Admin account. Use that certificate to get a DEP token from the Apple DEP site (https://deploy.apple.com or https://school.apple.com).
Select the "Configure accounts" button, and authenticate using the primary fwadmin account. You'll be presented with the option of uploading new tokens. You can have a token for each of the DEP facilitators you have.



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



The Synchronize button works the same as the VPP synchronize button. DEP will synchronize between Apple and your FileWave Server once a day. You can hold the alt/option key down to force a full, immediate synchronization. Use that sparingly, since it may take a long time to synchronize with lots of devices in the system.



● OK: 1 account(s)

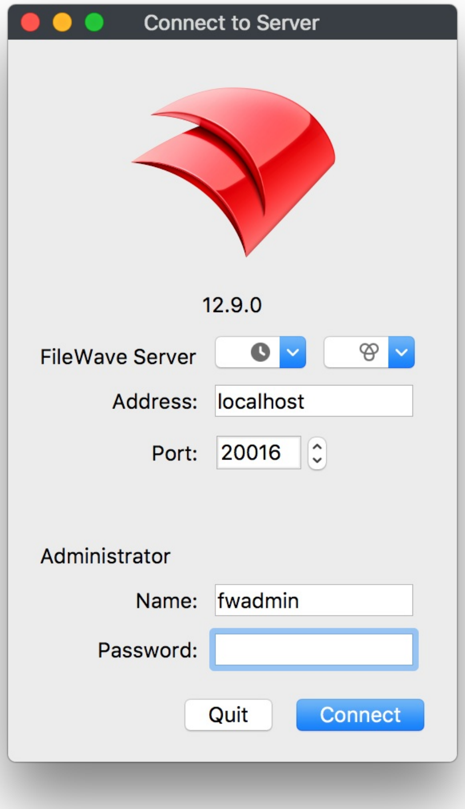
Last synchronization with DEP Web Service: 5/2/16 10:51 AM

Managing FileWave Administrators

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

How to log into FileWave Admin

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



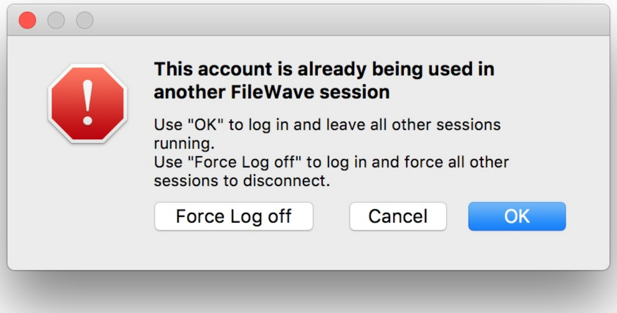
Address: localhost

Port: 20016

Name: fwadmin

Password:

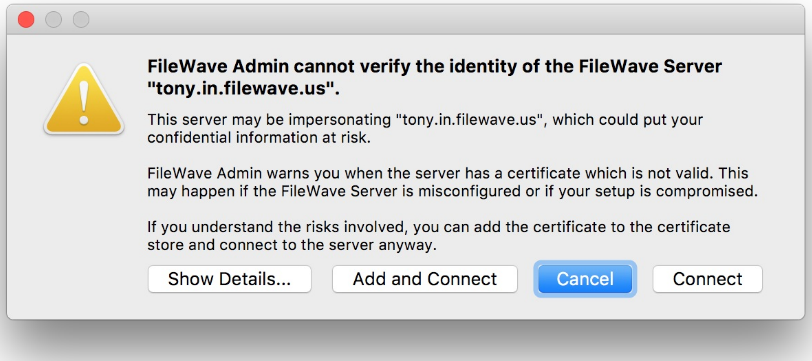
FileWave supports multiple admin connections from the same or separate admin accounts. If you try to log in with the same account that is already connected somewhere else you will get prompted to either end that first connection, start a second connection, or cancel.



This account is already being used in another FileWave session

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

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



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

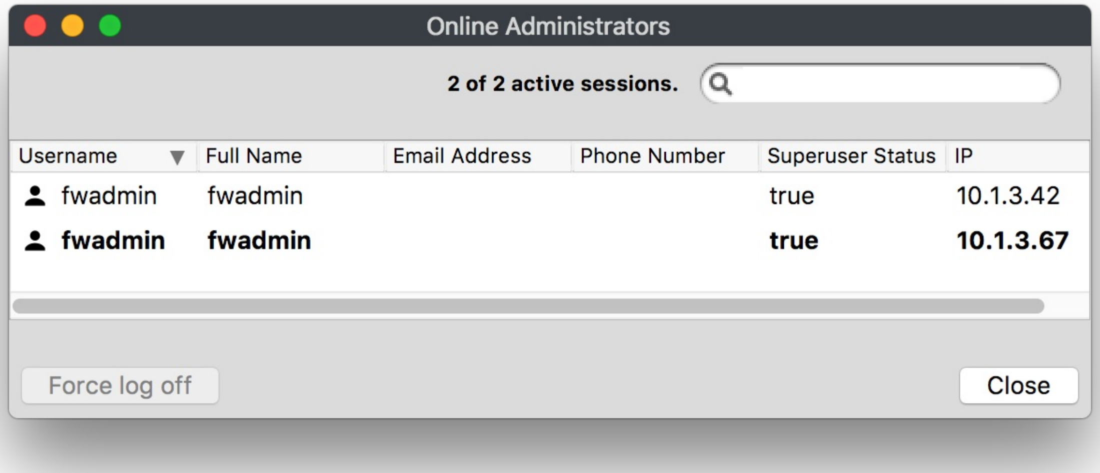
This server may be impersonating "tony.in.filewave.us", which could put your confidential information at risk.

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

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

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

The bolded entry is your current connection



Online Administrators

2 of 2 active sessions.

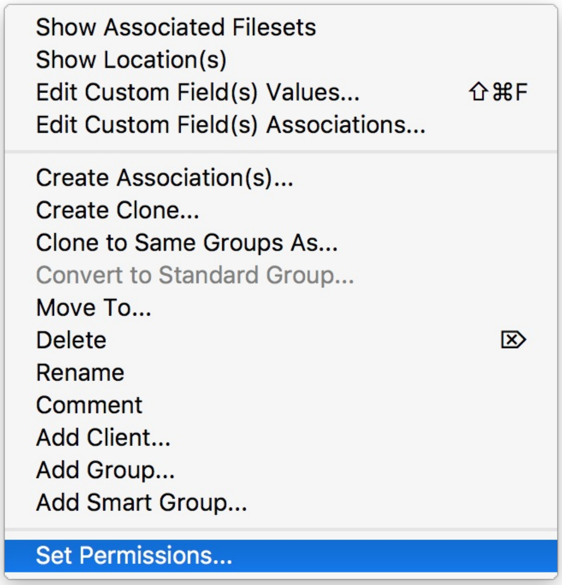
Username	Full Name	Email Address	Phone Number	Superuser Status	IP
fwadmin	fwadmin			true	10.1.3.42
fwadmin	**fwadmin**			**true**	**10.1.3.67**

FileWave Administrators and Inventory

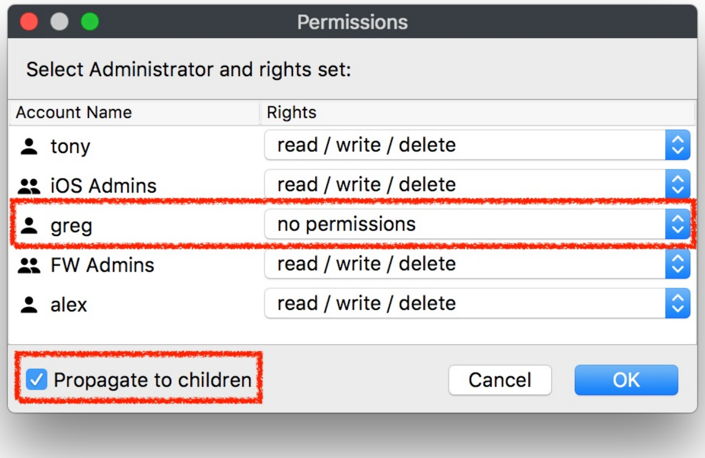
In the FileWave Admin console you have the ability to set read/write/delete permissions to specific objects which include devices, filesets, and groups. These permissions will follow the user all the way into inventory so that only what the current administrator has access too can be seen in the inventory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

Example:

- Right click on an object (user, group, fileset) and select Set Permissions



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



Select Administrator and rights set:

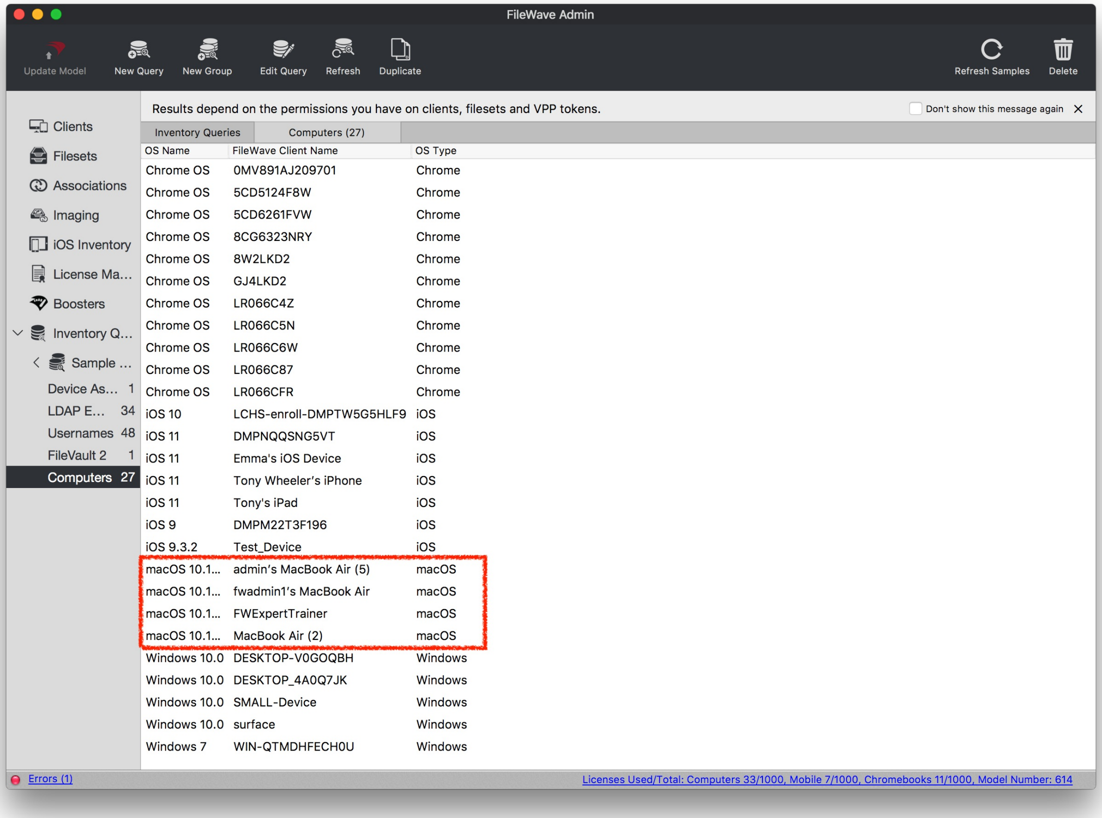
Account Name	Rights
tony	read / write / delete
iOS Admins	read / write / delete
greg	no permissions
FW Admins	read / write / delete
alex	read / write / delete

☑ Propagate to children

You have to select Propagate to children if you are setting permissions on a group and want those permissions to be added to sub-objects.

read/write/delete permissions are received from the original object and the clones will get the same permissions. If you modify these permissions on a clone, only this specific clone will get them not the original or other clones.

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



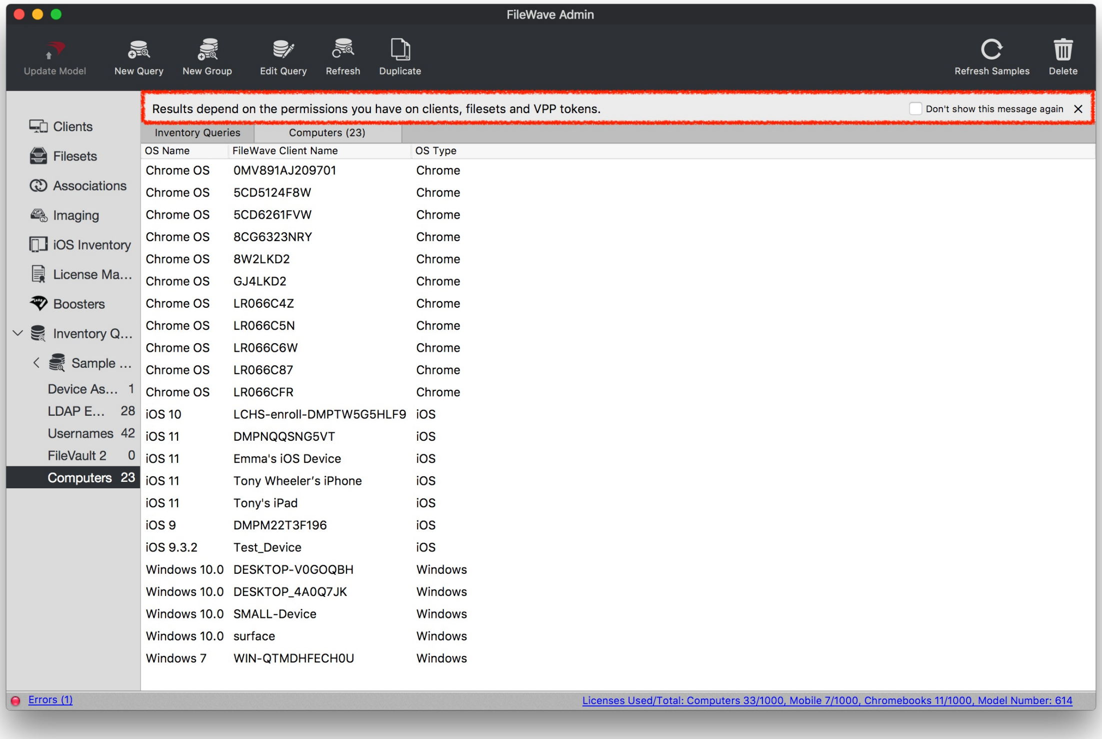
Results depend on the permissions you have on clients, filesets and VPP tokens.

□ Don't show this message again ✕

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

Errors (1)

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



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

□ Don't show this message again ✕

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

Errors (1)

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

Types of Administrator Accounts

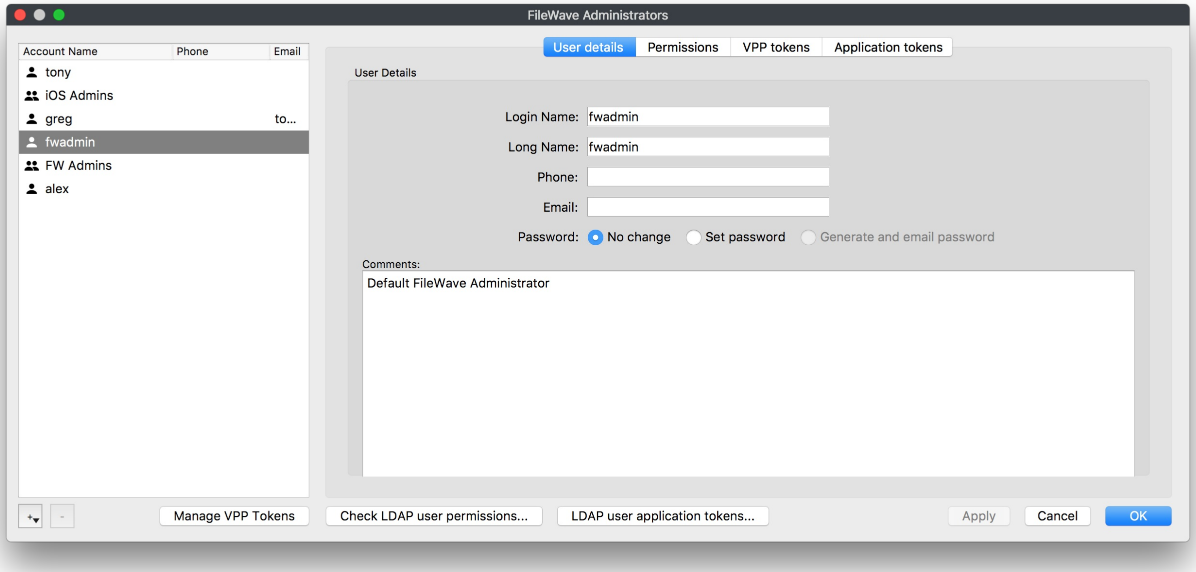
FileWave has three different account types;

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

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

Superuser

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



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

User Details

Login Name: fwadmin

Long Name: fwadmin

Phone:

Email:

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

Comments:

Default FileWave Administrator

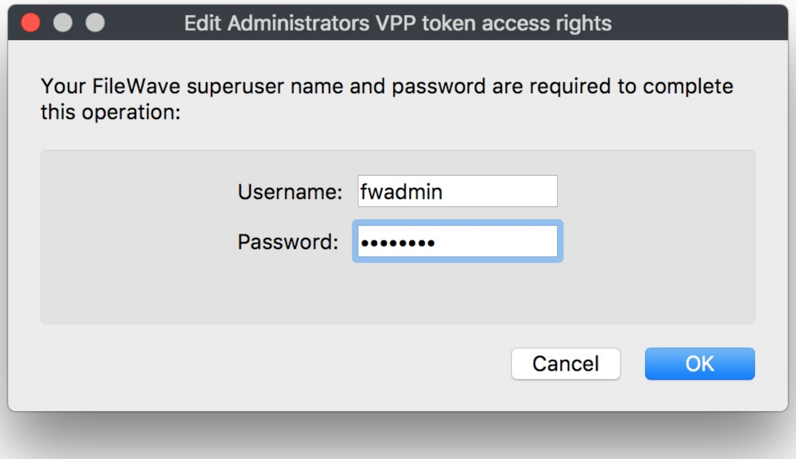
There are areas and features in FileWave that can only be accessed with the FileWave Superuser account. Three of these sections won't even be visible to any other Admin account, one (Software Update) is grayed out for all but the Superuser, and the other features will trigger a dialog window requesting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

Only Visible from the Superuser logged in:

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

All Admins will be prompted for Superuser credentials:

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



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

Username: fwadmin

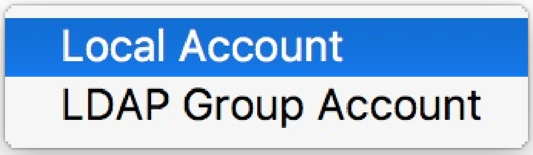
Password: ••••••••

Local Account

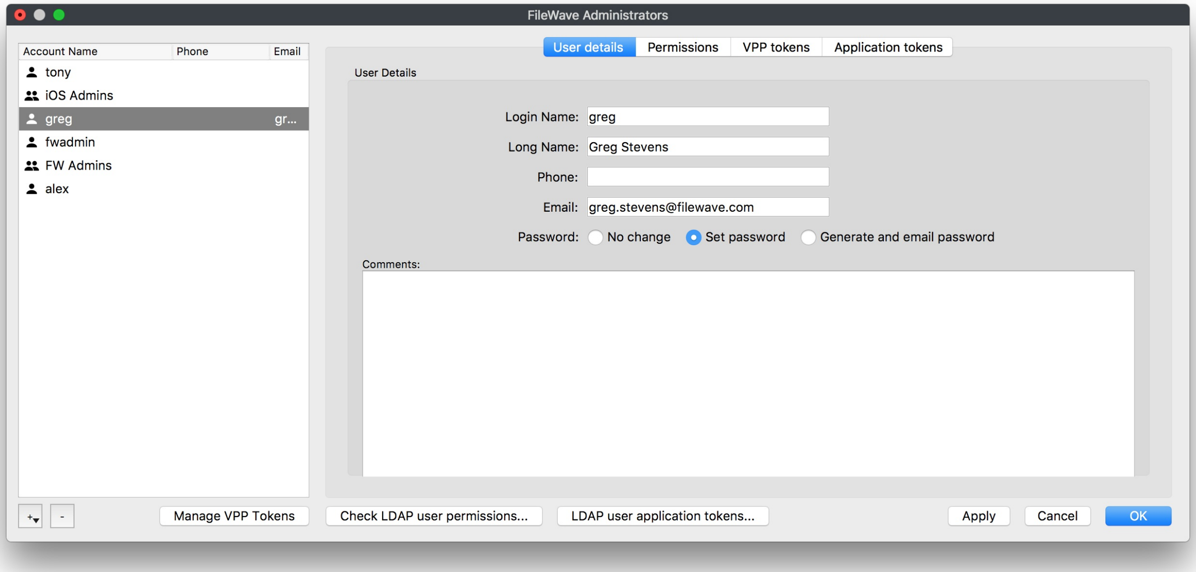
Local Accounts can be created very simply and then given whatever permissions you wish them to have. Keep in mind even if a Local Administrator Account is given full rights they will still be prompted for Superuser credentials in the areas listed in the Superuser section above.

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

- Go to Assistants→ Manage Administrators
- Click on the the "+" sign at the bottom left
- Then select Local Account



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



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

User Details

Login Name: greg

Long Name: Greg Stevens

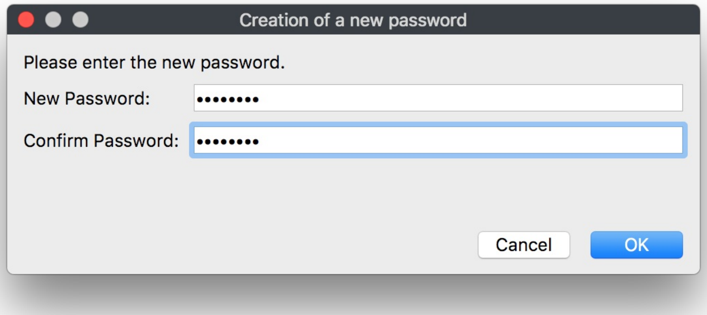
Phone:

Email: greg.stevens@filewave.com

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

Comments:

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



Please enter the new password.

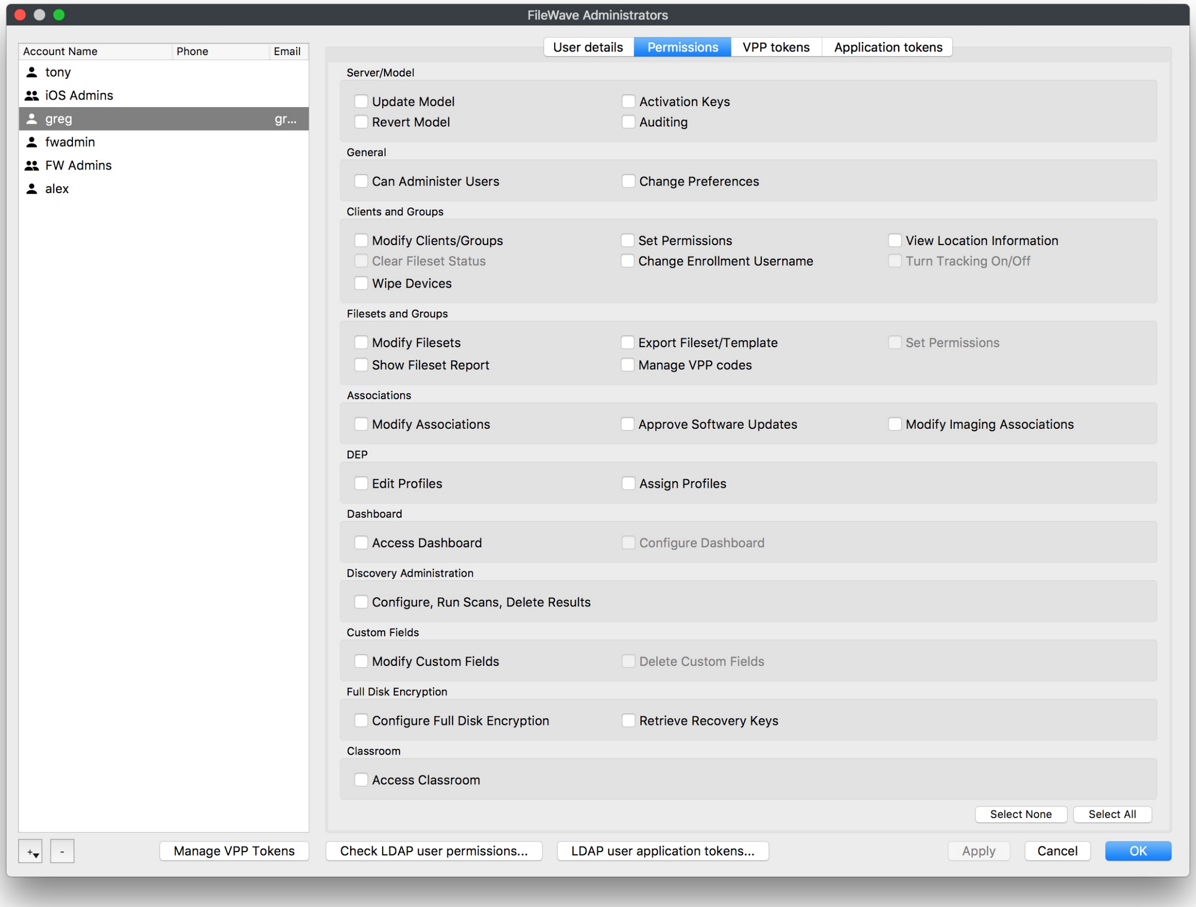
New Password: ••••••••

Confirm Password: ••••••••

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

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

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



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

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

General
☐ Can Administer Users
☐ Change Preferences

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

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

Associations
☐ Modify Associations
☐ Approve Software Updates
☐ Modify Imaging Associations

DEP
☐ Edit Profiles
☐ Assign Profiles

Dashboard
☐ Access Dashboard
☐ Configure Dashboard

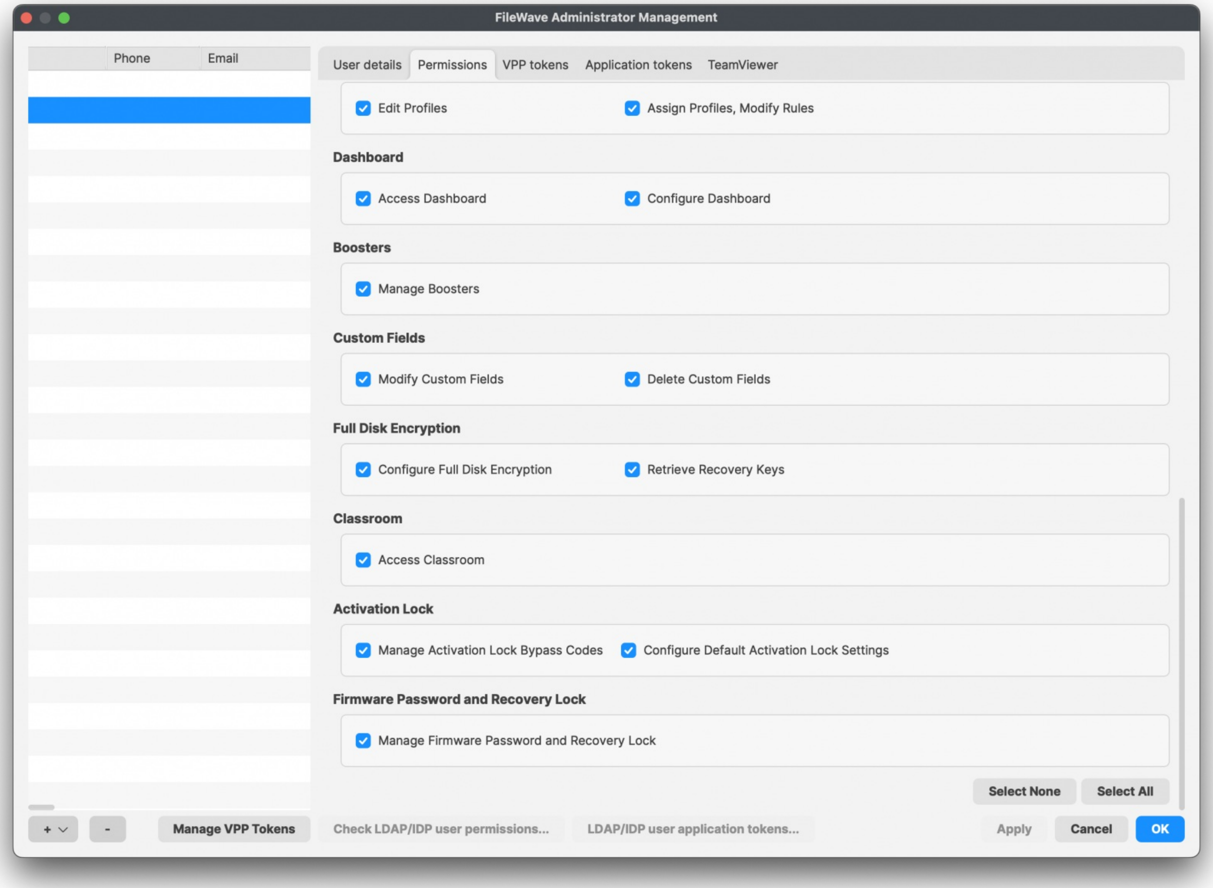
Discovery Administration
☐ Configure, Run Scans, Delete Results

Custom Fields
☐ Modify Custom Fields
☐ Delete Custom Fields

Full Disk Encryption
☐ Configure Full Disk Encryption
☐ Retrieve Recovery Keys

Classroom
☐ Access Classroom

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



☑ Edit Profiles ☑ Assign Profiles, Modify Rules

Dashboard

☑ Access Dashboard ☑ Configure Dashboard

Boosters

☑ Manage Boosters

Custom Fields

☑ Modify Custom Fields ☑ Delete Custom Fields

Full Disk Encryption

☑ Configure Full Disk Encryption ☑ Retrieve Recovery Keys

Classroom

☑ Access Classroom

Activation Lock

☑ Manage Activation Lock Bypass Codes ☑ Configure Default Activation Lock Settings

Firmware Password and Recovery Lock

☑ Manage Firmware Password and Recovery Lock

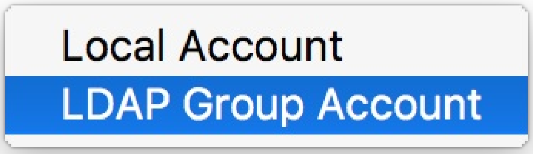
LDAP Group Account

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

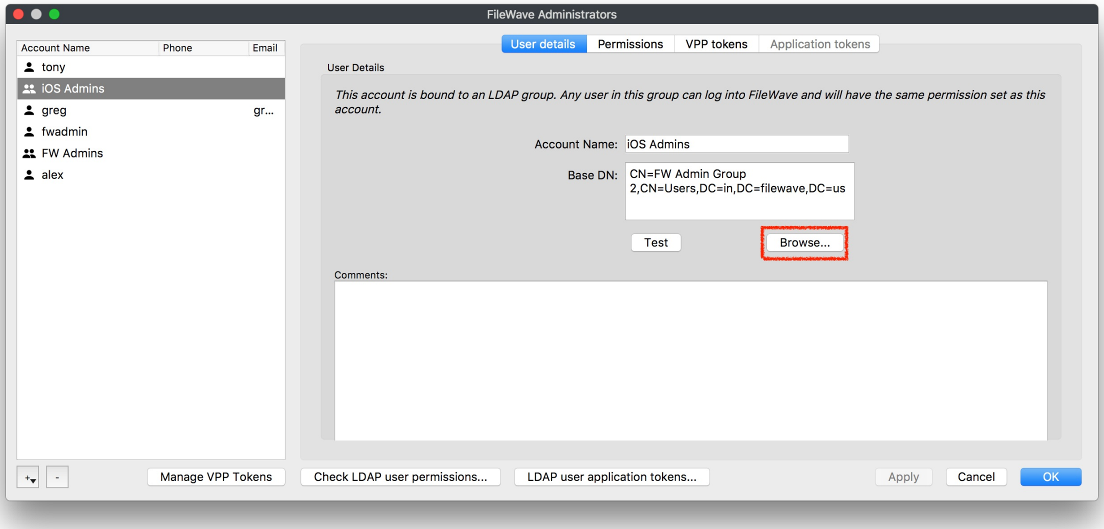
> To setup LDAP please see: LDAP Preferences

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

- Go to Assistants→ Manage Administrators
- Click on the the "+" sign at the bottom left
- Then select LDAP Group Account



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



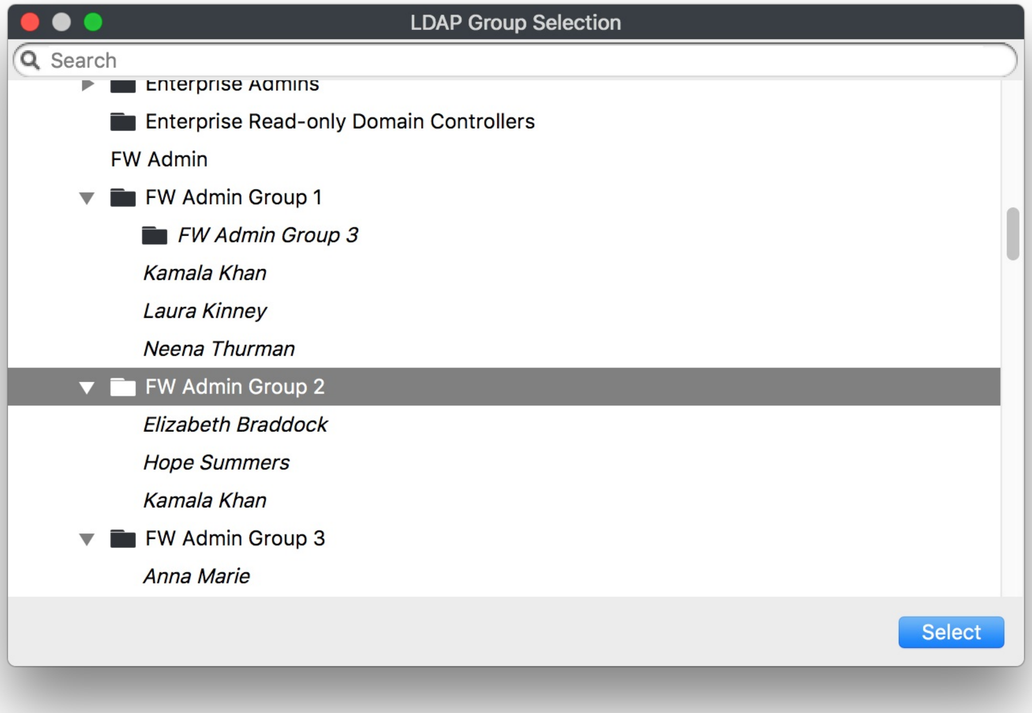
Account Name	Phone	Email
tony		
iOS Admins		
greg		gr...
fwadmin		
FW Admins		
alex		

User Details

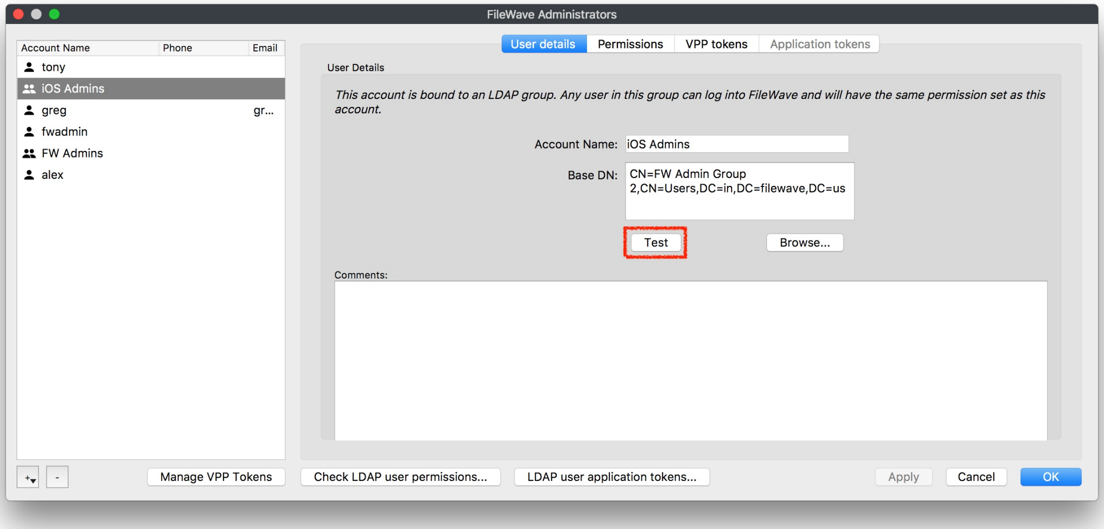
This account is bound to an LDAP group. Any user in this group can log into FileWave and will have the same permission set as this account.

Account Name: iOS Admins

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



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



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

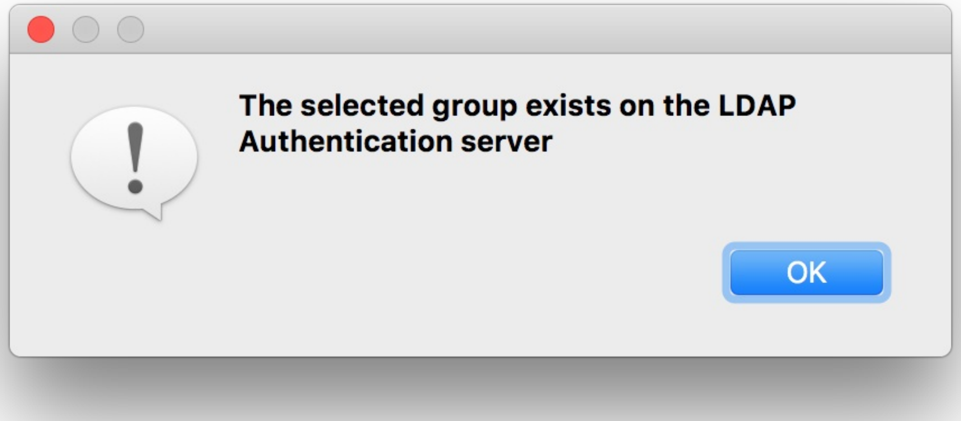
User Details

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

Account Name: iOS Admins

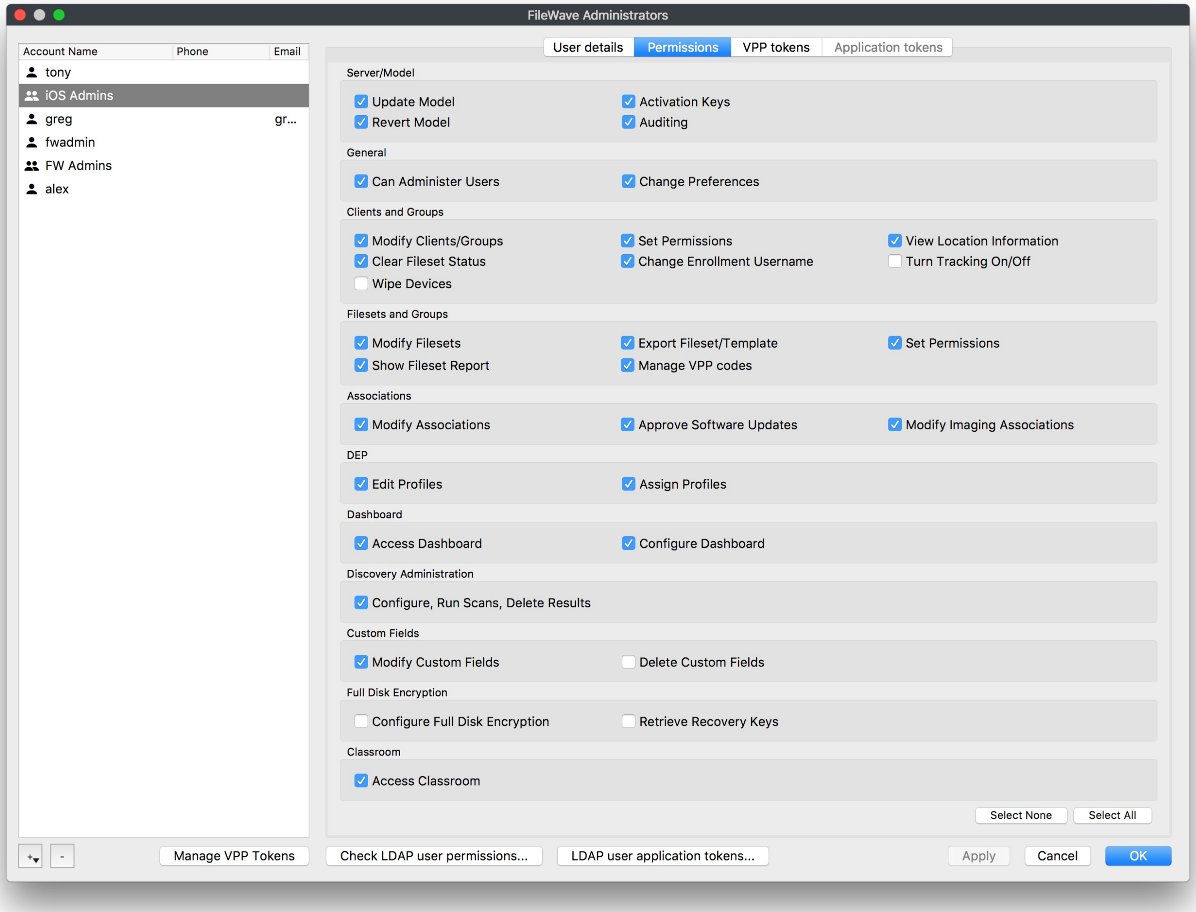
Base DN: CN=FW Admin Group 2,CN=Users,DC=in,DC=filewave,DC=us

Comments:



The selected group exists on the LDAP Authentication server

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



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

Server/Model

☑ Update Model ☑ Activation Keys
☑ Revert Model ☑ Auditing

General

☑ Can Administer Users ☑ Change Preferences

Clients and Groups

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

Filesets and Groups

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

Associations

☑ Modify Associations ☑ Approve Software Updates ☑ Modify Imaging Associations

DEP

☑ Edit Profiles ☑ Assign Profiles

Dashboard

☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration

☑ Configure, Run Scans, Delete Results

Custom Fields

☑ Modify Custom Fields □ Delete Custom Fields

Full Disk Encryption

□ Configure Full Disk Encryption □ Retrieve Recovery Keys

Classroom

☑ Access Classroom

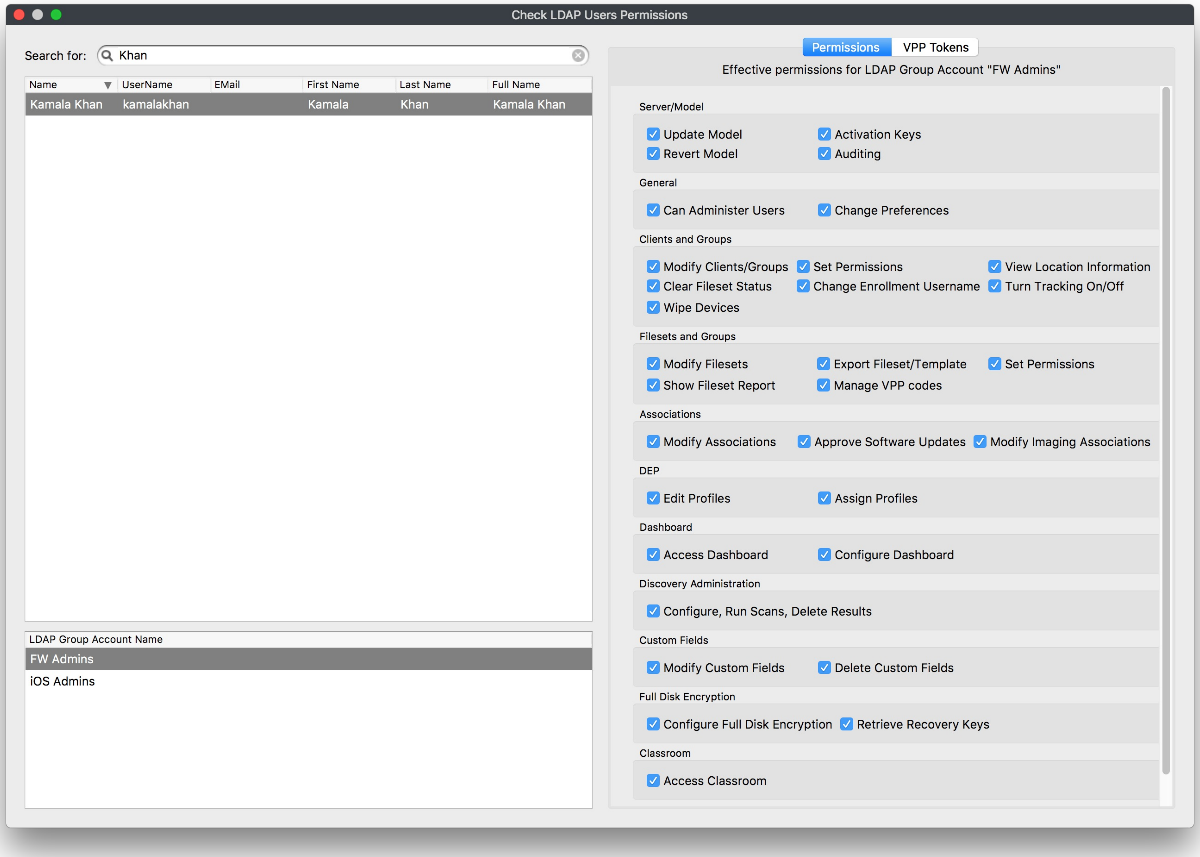
Permissions

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

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

LDAP Group Account Permissions

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



Search for: Khan

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

LDAP Group Account Name
FW Admins
iOS Admins

Effective permissions for LDAP Group Account "FW Admins"

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

General
☑ Can Administer Users ☑ Change Preferences

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

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

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

DEP
☑ Edit Profiles ☑ Assign Profiles

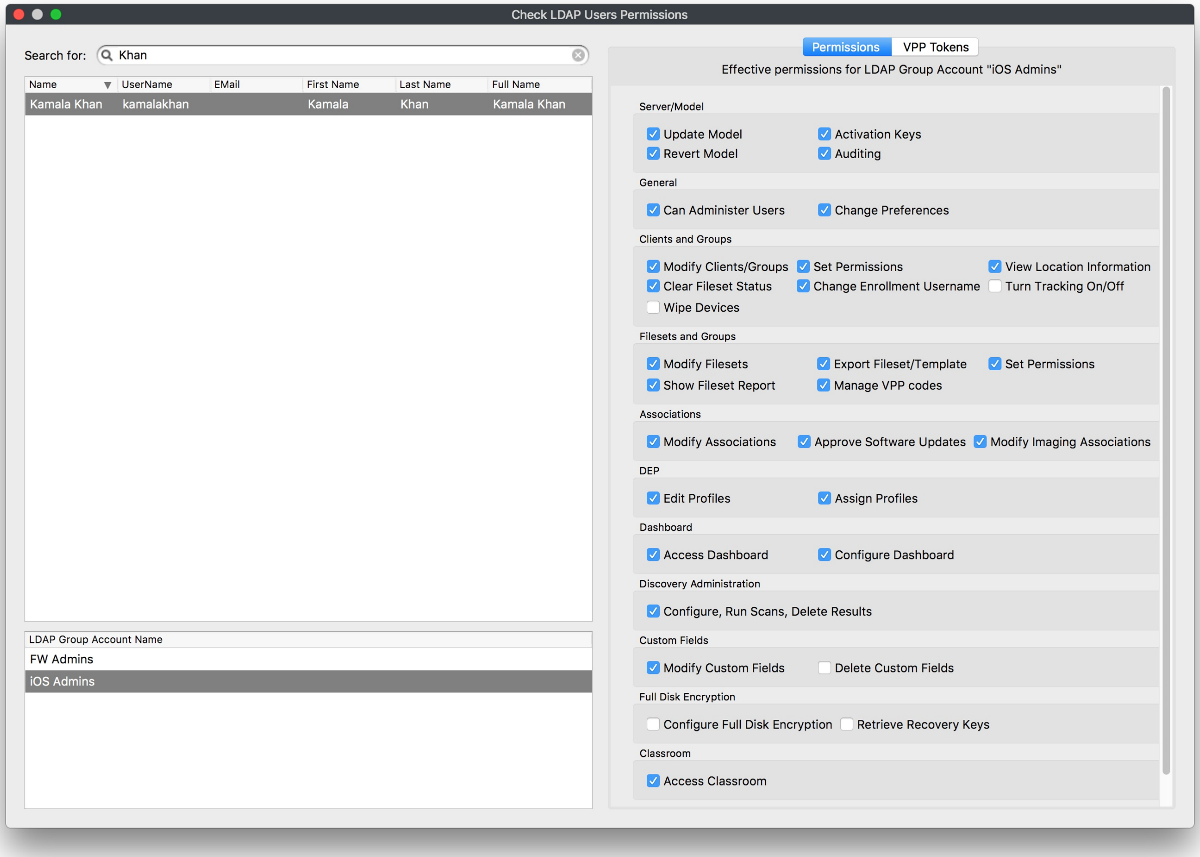
Dashboard
☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration
☑ Configure, Run Scans, Delete Results

Custom Fields
☑ Modify Custom Fields ☑ Delete Custom Fields

Full Disk Encryption
☑ Configure Full Disk Encryption ☑ Retrieve Recovery Keys

Classroom
☑ Access Classroom



Search for: Khan

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

LDAP Group Account Name
FW Admins
iOS Admins

Effective permissions for LDAP Group Account "iOS Admins"

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

General
☑ Can Administer Users ☑ Change Preferences

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

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

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

DEP
☑ Edit Profiles ☑ Assign Profiles

Dashboard
☑ Access Dashboard ☑ Configure Dashboard

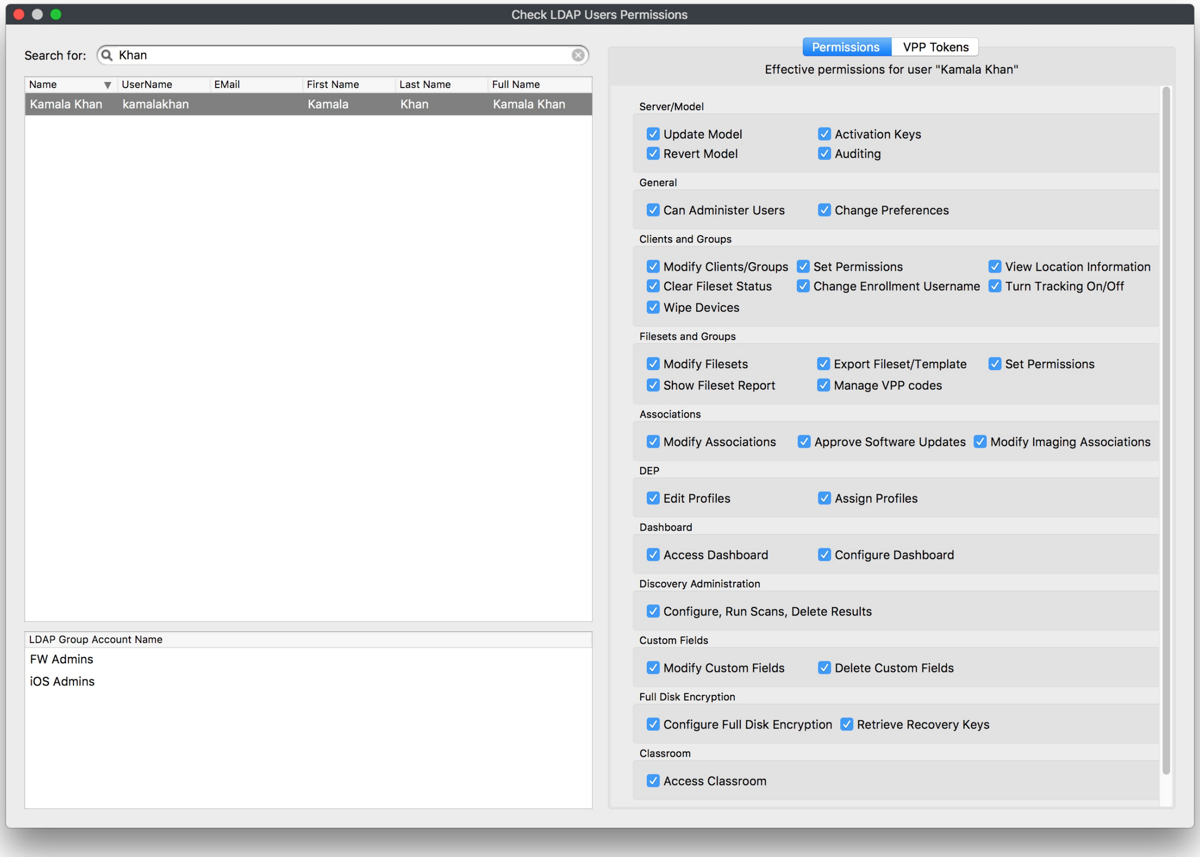
Discovery Administration
☑ Configure, Run Scans, Delete Results

Custom Fields
☑ Modify Custom Fields □ Delete Custom Fields

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

Classroom
☑ Access Classroom

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



Check LDAP Users Permissions

Search for: Khan

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

LDAP Group Account Name
FW Admins
iOS Admins

Permissions | VPP Tokens

Effective permissions for user "Kamala Khan"

Server/Model

☑ Update Model ☑ Activation Keys
☑ Revert Model ☑ Auditing

General

☑ Can Administer Users ☑ Change Preferences

Clients and Groups

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

Filesets and Groups

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

Associations

☑ Modify Associations ☑ Approve Software Updates ☑ Modify Imaging Associations

DEP

☑ Edit Profiles ☑ Assign Profiles

Dashboard

☑ Access Dashboard ☑ Configure Dashboard

Discovery Administration

☑ Configure, Run Scans, Delete Results

Custom Fields

☑ Modify Custom Fields ☑ Delete Custom Fields

Full Disk Encryption

☑ Configure Full Disk Encryption ☑ Retrieve Recovery Keys

Classroom

☑ Access Classroom

What are all the permissions you can choose from?

Server / Model

- Update Model - allows the administrator to approve changes to the server model. Updating the model sends notifications to all FW clients of any possible changes to any Filesets they have.
- Revert Model - allows the administrator to cancel changes made at the last model update and revert to the previous model version.
- Auditing - allows the administrator to view the Audit History of all actions logged by FileWave.
- Activation Keys - allows the administrator to enter, change, or update the activation keys for the FileWave server.

General

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

Clients and Groups

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

Filesets and Groups

- Modify Filesets - allows administrator to edit Filesets , add or delete content within a Fileset.
- Export Fileset / Template - allows the user to export a specific Fileset or a template for use on another FileWave server, or for archival purposes.
- Set Permissions - allows the administrator to change the permissions within a Fileset or Fileset Group.
- Show Fileset Report - allows administrator to view the Fileset report showing the status of that Fileset.
- Manage VPP codes - with this unchecked and disallowed this will prevents administrators from accessing all VPP settings and menus, will also prevents the admins access to setup DEP tokens.
  Note: If you do not allow an administrator to Manage VPP codes then they will not be able to see any of the VPP purchased applications or ebooks. This is especially important if you have multiple VPP token support.

Associations

- Modify Associations - allows the administrator to change the associations settings between a client or client Group and any Fileset or Fileset Group.
- Approve Software Updates - allows the administrator to designate specific software updates as pre-approved for association by other administrators.
- Modify Imaging Associations - allows the administrator to change which Imaging Filesets are associated with which devices

DEP

- Edit Profiles - allows the administrator to change the characteristics of DEP profiles, including naming conventions, setup assistant workflow, and certificate assignment.
- Assign Profiles - allows the administrator to designate specific client devices to be managed by certain DEP profiles.

Dashboard

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

Discovery Administration

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

Custom Fields

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

Full Disk Encryption

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

Classroom

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

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

Application tokens

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

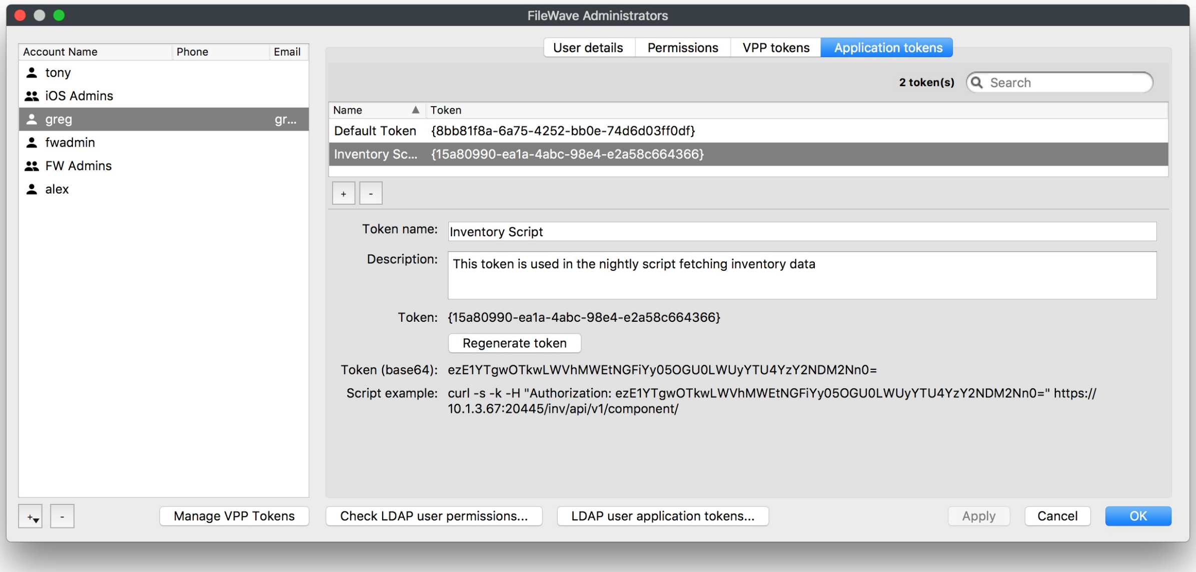
Any script or 3rd party component that needs access to FileWave Inventory will need to have this token that has been assigned to a user. These tokens can be revoked, re-generated, and a user can have multiple tokens assigned to it.

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

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

Local Account New Application Token Setup:

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



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

2 token(s)

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

Token name: Inventory Script

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

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

Token (base64): ezE1YTgwOTkwLWVhMWEtNGFiYy05OGU0LWUyYTU4YzY2NDM2Nn0=

Script example:

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

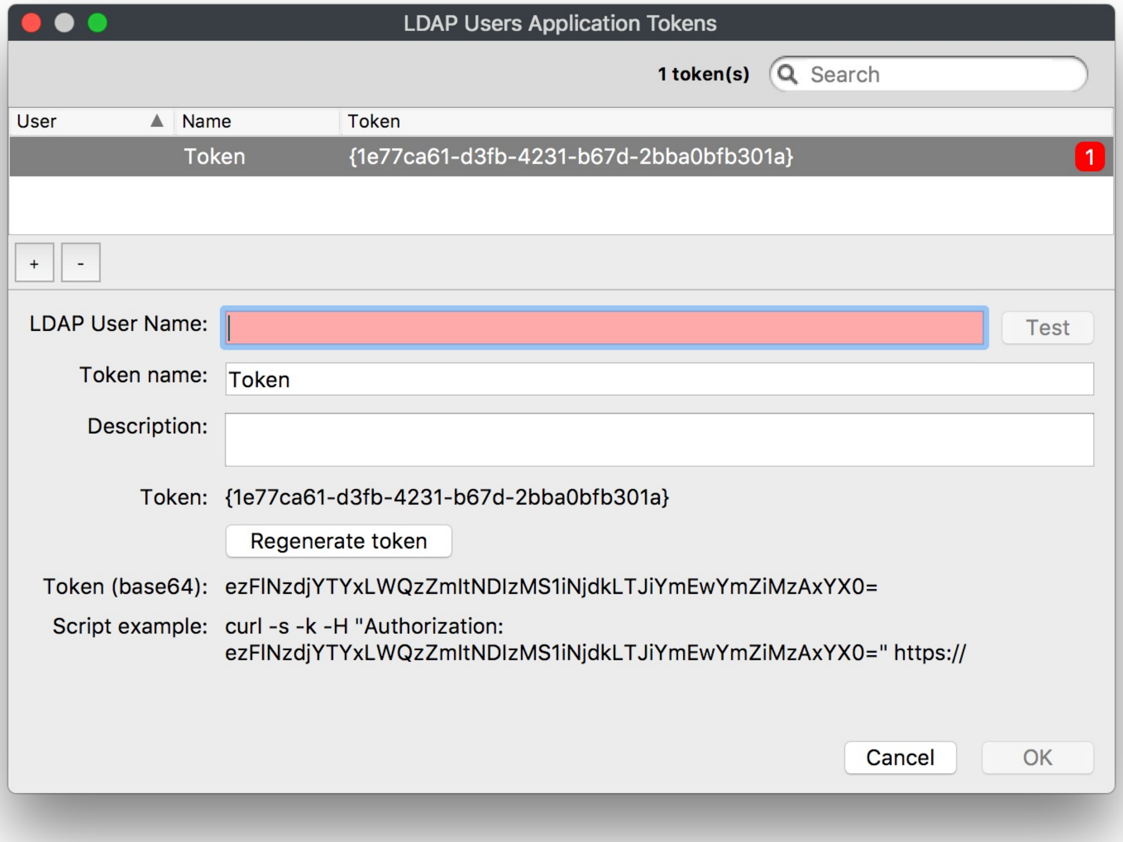
- This will show
  1. The raw token
  2. base64 encoded token
  3. An example script you can copy and paste to test with

LDAP user application tokens

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

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

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



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

LDAP User Name:

Token name: Token

Description:

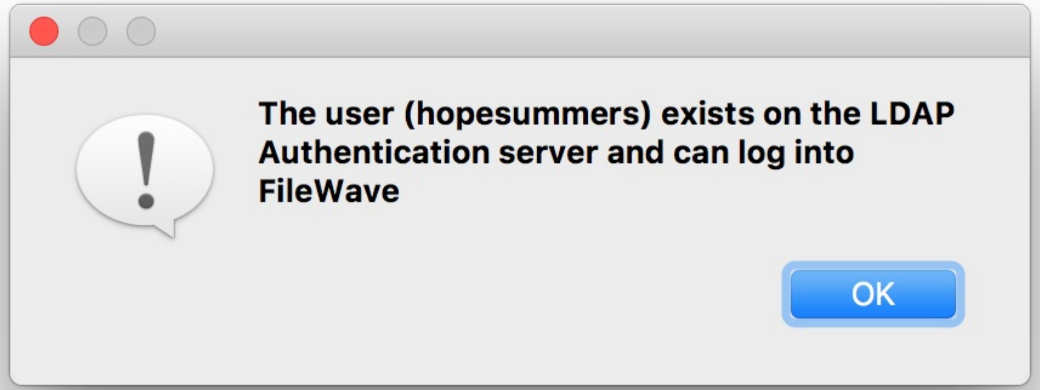
Token: {1e77ca61-d3fb-4231-b67d-2bba0bfb301a}

Token (base64): ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=

Script example:

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

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

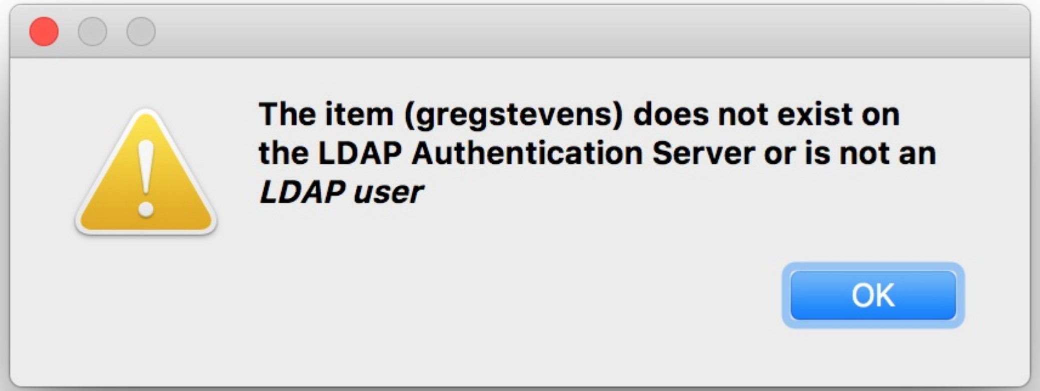


The user (hopesummers) exists on the LDAP Authentication server and can log into FileWave

LDAP User TEST
The test will make sure the user belongs to the LDAP server configured for authentication in the FileWave Preferences and will also make sure the user belongs to at least 1 LDAP group defined in the main FileWave Administrators window.

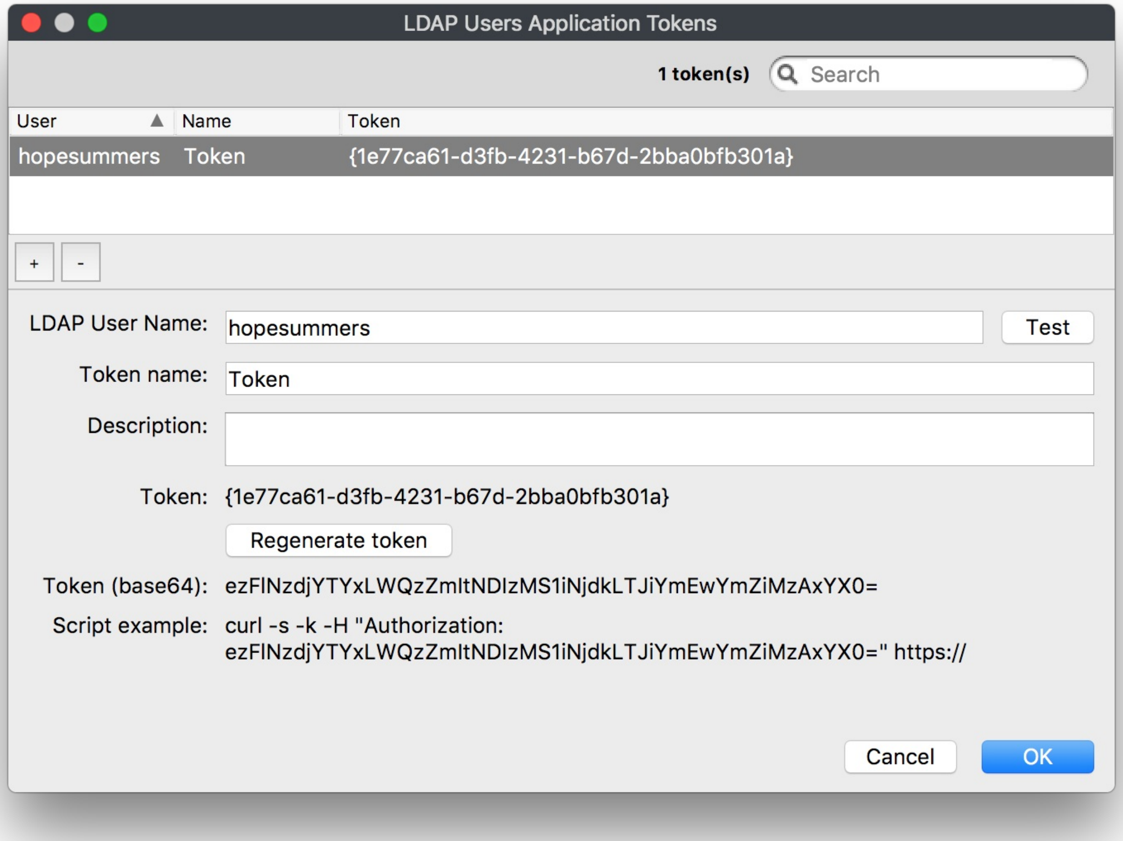
Note: The part of the test to check for the LDAP group in FileWave is cached for 1 hour. The cache is reset every time you save the user dialog, or change the LDAP server in preferences or if you do a LDAP "synchronize".

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



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

- Once it has confirmed you are ready to use the token



LDAP Users Application Tokens

1 token(s)

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

LDAP User Name: hopesummers

Token name: Token

Description:

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

Token (base64): ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=

Script example:

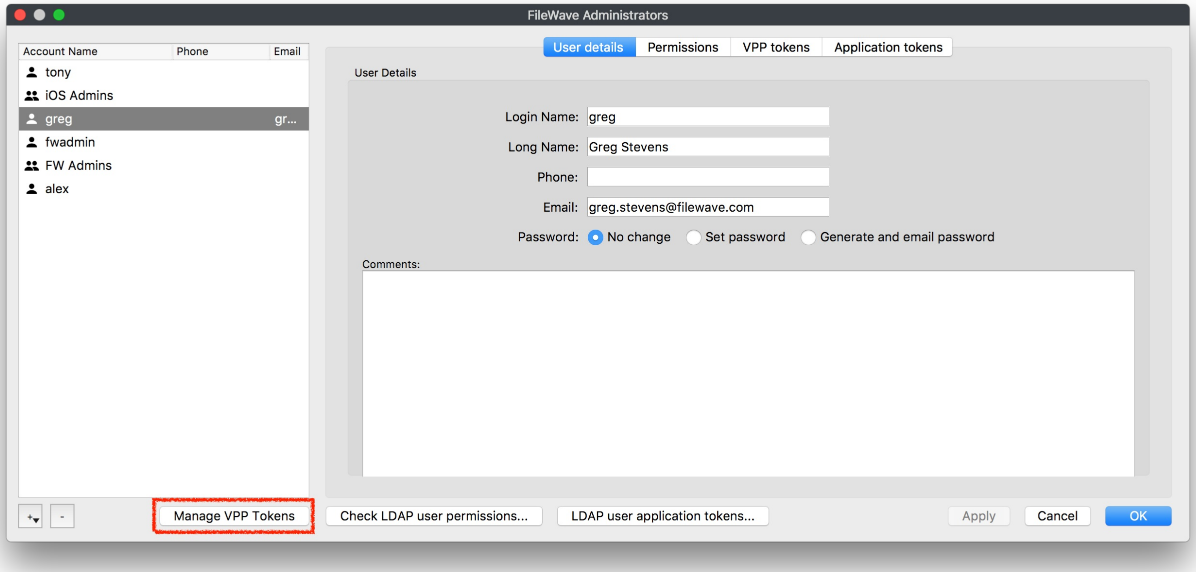
```
curl -s -k -H "Authorization:
ezFlNzdjYTYxLWQzZmItNDIzMS1iNjdkLTJiYmEwYmZiMzAxYX0=" https://
```

Manage VPP Tokens

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

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

- Click the Manage VPP Tokens button at the bottom



FileWave Administrators

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

User Details

Login Name: greg

Long Name: Greg Stevens

Phone:

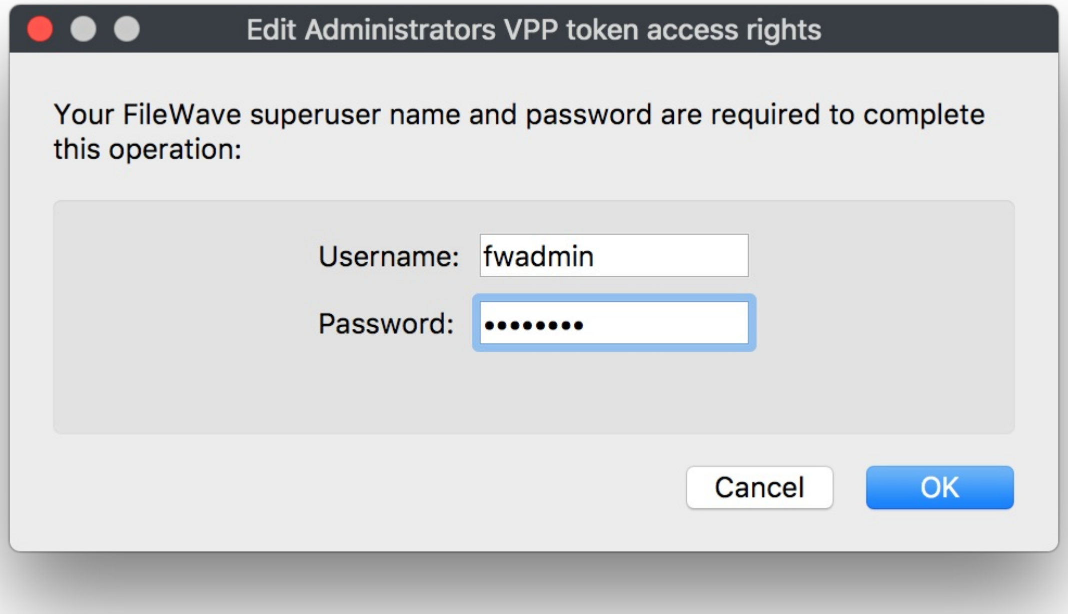
Email: greg.stevens@filewave.com

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

Comments:

+
-
Manage VPP Tokens
Check LDAP user permissions...
LDAP user application tokens...
Apply
Cancel
OK

- You need to authenticate with the Superuser



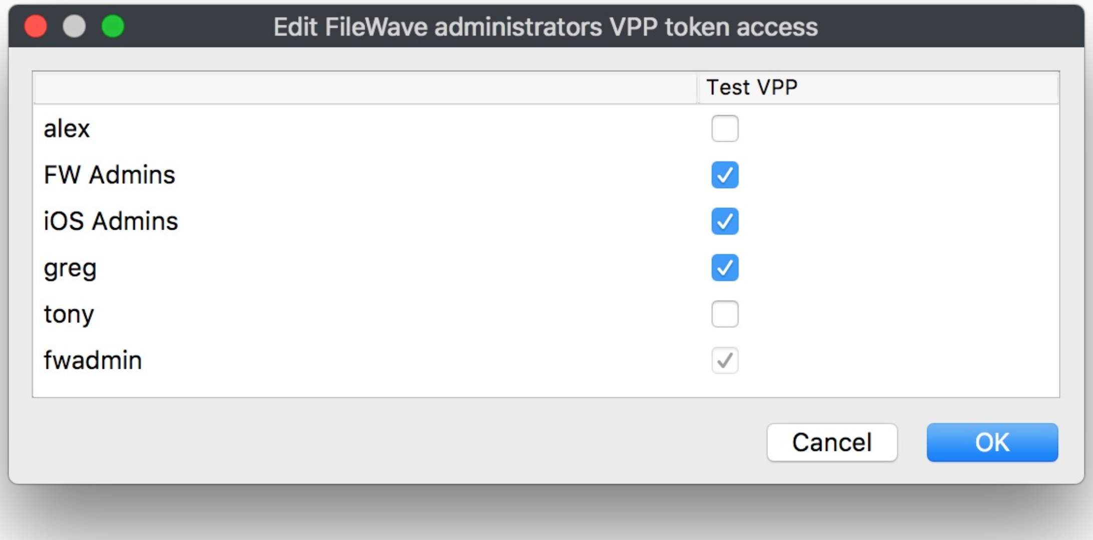
Edit Administrators VPP token access rights

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

Username: fwadmin

Password: ••••••••

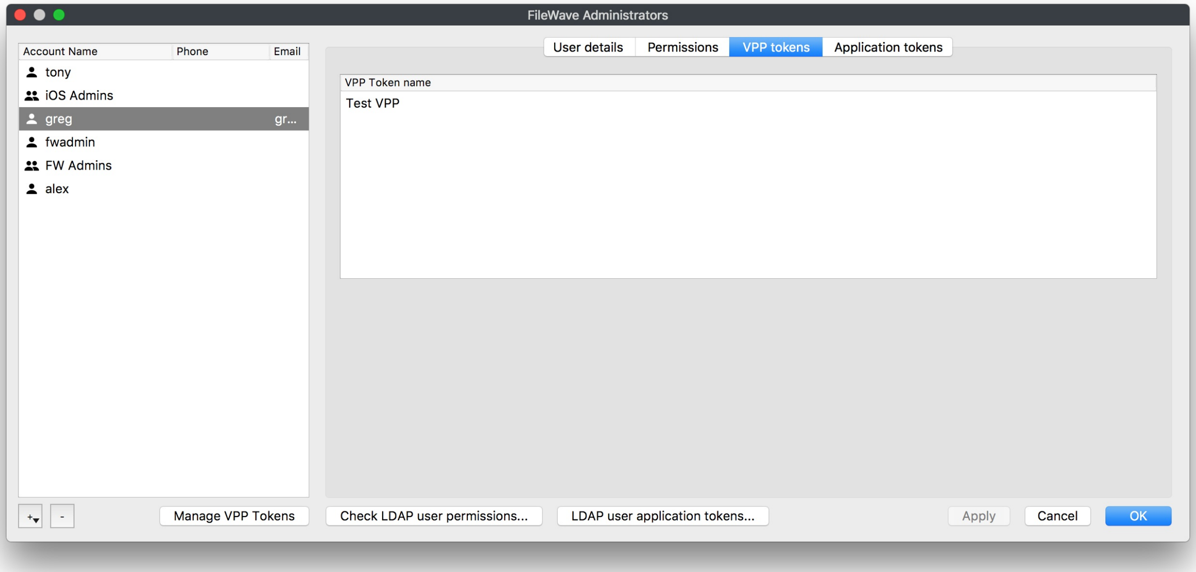
- Now you will check which users you would like to manage which VPP Token



Edit FileWave administrators VPP token access

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

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



FileWave Administrators

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

VPP Token name
Test VPP

Embracing the Dark Side: Dark Mode for FileWave Central (15.3+)

What

Once upon a time, in a brightly lit world of screens, a shadowy figure emerged, promising salvation to our eyes: Dark Mode. As legends of its comfort and sleekness spread across the realms of software applications, we at FileWave decided it was time to embrace the dark side. Here's the tale of how Dark Mode came to FileWave Central, turning night into a friendlier place for all administrators.

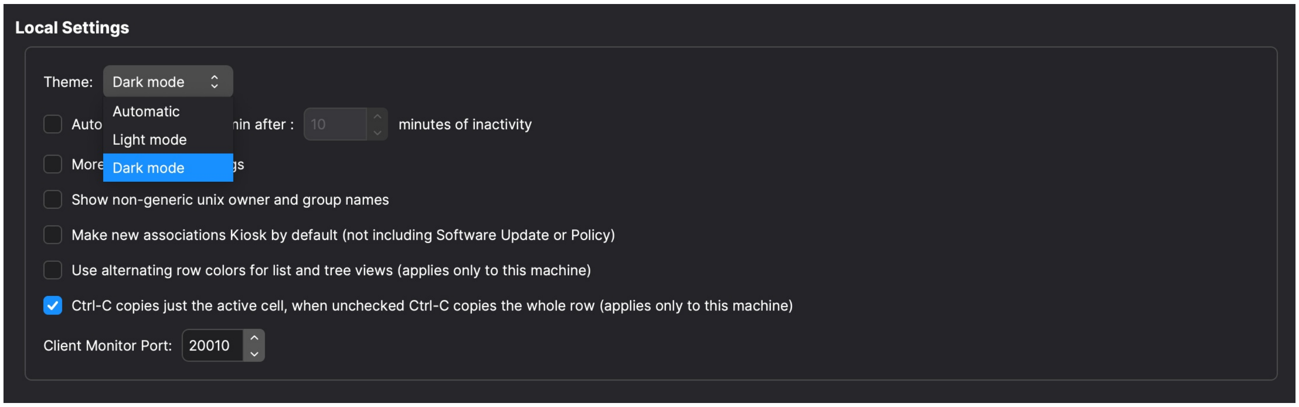
Dark Mode, the knight in shining armor (or should we say, 'shimmering darkness'?), transforms the blinding lights of your screen into a soothing, shadowy oasis. It’s not just a fashion statement; it’s a guardian of your eyesight, a curator of concentration, and a promoter of power saving. By inverting the bright white backgrounds into deep, dark hues, Dark Mode makes nighttime work less of a nightmare.

When/Why

As the clock struck midnight on yet another session of late-night device management, it dawned on us: our users deserved the option to go dark. Following a cascade of requests and after noticing the shift towards dark themes across the tech landscape, we knew the time was right. Our decision was fueled by the desire to not only keep up with modern UI trends but to also offer our hardworking administrators a visually comfortable and customizable working environment, proving our commitment to not just meeting but exceeding user expectations.

How

To embrace the dark side or bask in the light, journey to **Preferences -> General** in FileWave Central. There, under the Theme setting, select your allegiance: Automatic, Light Mode, or Dark Mode. Choose wisely, for each setting casts FileWave Central in a different aura, from the bright, welcoming light of day to the mysterious, serene shadows of night.



Local Settings

Theme: Dark mode

□ Auto nin after : 10 minutes of inactivity

□ More gs

□ Show non-generic unix owner and group names

□ Make new associations Kiosk by default (not including Software Update or Policy)

□ Use alternating row colors for list and tree views (applies only to this machine)

☑ Ctrl-C copies just the active cell, when unchecked Ctrl-C copies the whole row (applies only to this machine)

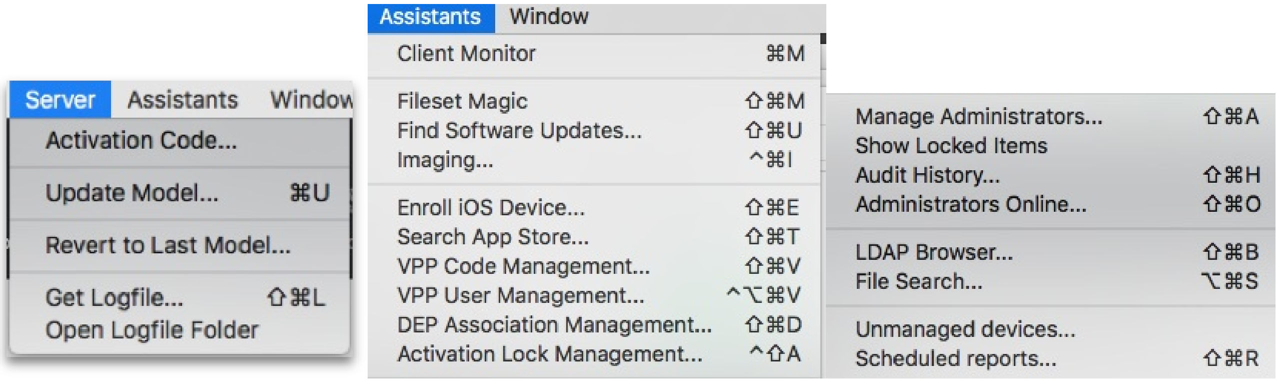
Client Monitor Port: 20010

Related Content

- FileWave Central / Anywhere

FileWave Central - Additional Settings Menu Items

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



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

Activation Code...

This is the access to the code you received when you purchased your FileWave license.

Update Model...

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

Revert to Last Model...

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

Get Logfile...

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

Open Logfile Folder

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

Client Monitor

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

Fileset Magic

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

Find Software Updates...

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

Imaging...

This item opens the Imaging pane that allows you to associate disk images with OS X and Windows devices for re-imaging. This is covered in detail in Network Imaging / IVS.

Enroll iOS Device...

This item opens the pane with the various settings for enrolling iOS devices, and AppleTV, either manually or automatically.

Search App Store...

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

VPP Code Management... / VPP User Management...

These two menu items relate to Apple's Volume Purchase Program within FileWave. They allow you to manage the distribution of institutionally purchased content.

DEP Association Management...

This menu item relates the Apple Device Enrollment Program within FileWave. You use this pane to configure DEP profiles, and associate them to institutionally purchased devices. .

Activation Lock Management...

This menu item displays the status of your supervised iOS devices with activation lock active. The bypass codes are stored on the FileWave server for your use when taking these devices out of service.

Manage Administrators...

This menu item opens the management pane for creating, editing, and managing the FileWave administrator account and sub-admin accounts.

Show Locked Items

This menu opens the window with a display of any and all aspects of the FileWave Admin UI that has been "taken control of" using the Take Control button, or that is in use by another FileWave administrator. For example, when an administrator needs to work on editing the sub-administrators, changing some settings in Clients, or editing a Fileset, they can Take Control of those specific items (and when they are finished, they can Release Control).

In the meantime, any administrator trying to work on those areas, can use the Show Locked Items menu to view areas they cannot control.

If an administrator has left items locked too long, or walked away from their system with items still locked, you can force quit that administrator (see Administrators Online... below). You should also make sure your sub-administrators set a reasonable auto-logout time in the General preferences of their FileWave Admin application.

Audit History...

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

Administrators Online...

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

LDAP Browser...

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

File Search...

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

Unmanaged Devices...

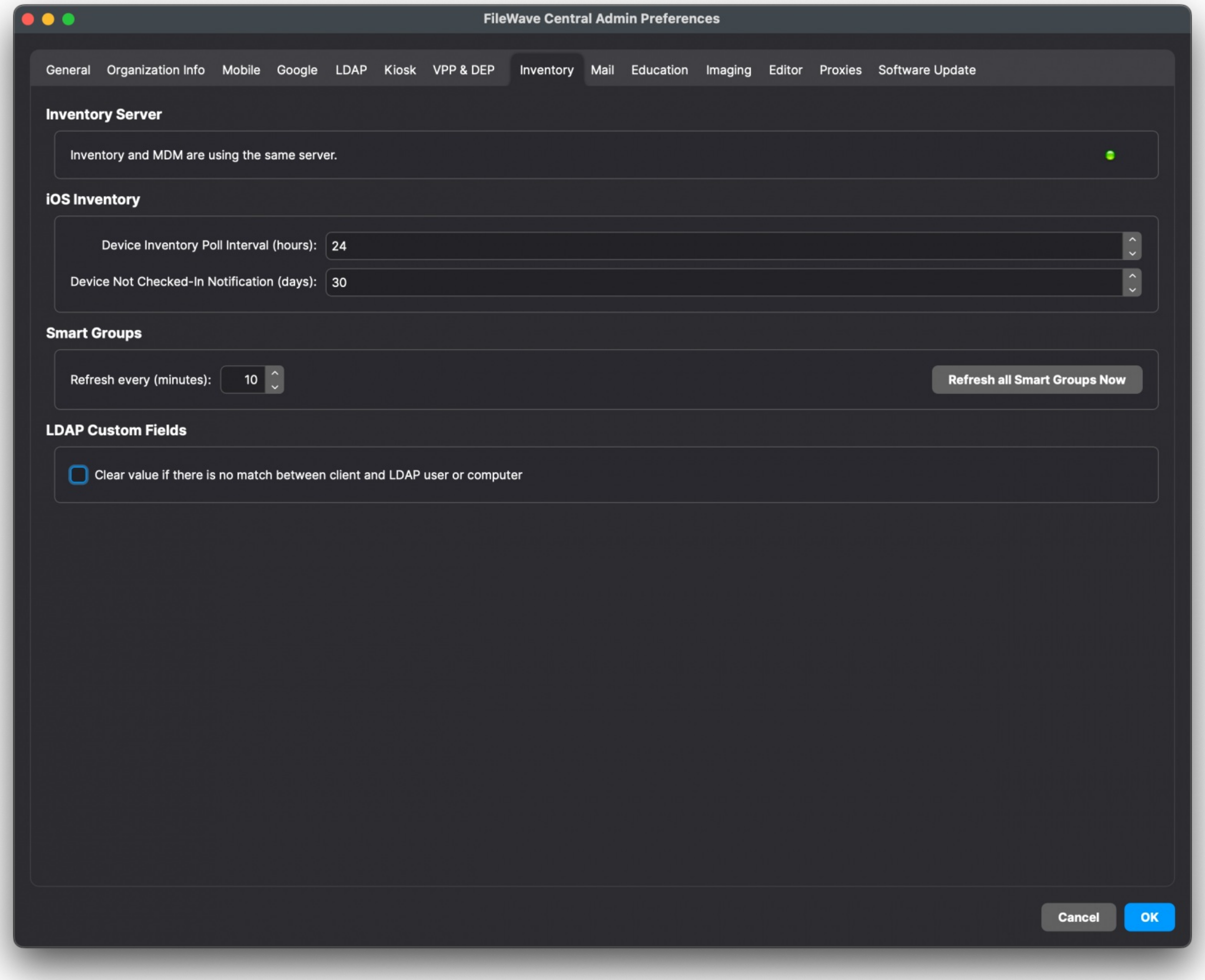
This menu item displays a pane with the "non-client" devices you are keeping track of. You can enter items such as printers, scanners, cameras, etc. to the set by clicking on [+] in the window.

Scheduled Reports...

This menu item allows you to create and generate Inventory reports that are automatically sent to designated email accounts.

Configuring Inventory preferences

With version 6 and higher, FileWave integrated Inventory into the main FileWave server. With version 8, FileWave introduced Smart Groups with Inventory queries:



Inventory Server

Inventory and MDM are using the same server. ●

iOS Inventory

Device Inventory Poll Interval (hours): 24

Device Not Checked-In Notification (days): 30

Smart Groups

Refresh every (minutes): 10

LDAP Custom Fields

□ Clear value if there is no match between client and LDAP user or computer

iOS Inventory

These settings only apply to the iOS/iPadOS/tvOS enrolled devices. These devices show up in the normal Clients section of FileWave Admin as well as in the iOS Inventory section.

- Device Inventory Poll Interval – Default is 24hrs. This setting is how often all iOS devices will report their profiles, application, security and device settings unless a Verify command is sent.
- Device Not Checked-In Notification – When an iOS device exceeds the timeframe set, the device color changes to alert the administrator that that device has not checked in with the MDM server.

Smart Groups

The button Refresh all Smart Groups forces a refresh of all the data requested by existing Smart Groups. Smart Groups normally update every 10 minutes, but this can be adjusted here as well. Do not make this much more frequent or you may make your server overly busy. If you have a very large environment you may want to increase this value to perhaps 20 minutes.

LDAP Custom Fields

If checked this option will clear the value of a LDAP Custom Field if there is no match between client and LDAP user or computer.

Related Content

- FileWave Client Configuration Settings

FileWave Anywhere persistent user preferences (14.8+)

What

As a user of FileWave Anywhere, I frequently have to resize columns when I’m using it.

When/Why

In v14.8.0 we have introduced the ability to store preferences about column width so that when you login columns will retain their size as appropriate.

How

User preferences in main views will be stored on the user account:

- Pinned columns
- Width of the columns
- Visibility of the columns
- Order of the columns

User preferences in main views will be stored in the active session:

- Filters
- Quick filters
- Search
- Applied sorting on a column

Profiles section error handling improvements:

- Error handling in the profiles is more user friendly and the mandatory fields are better highlighted