Classroom – Identity Certificate Management

Overview

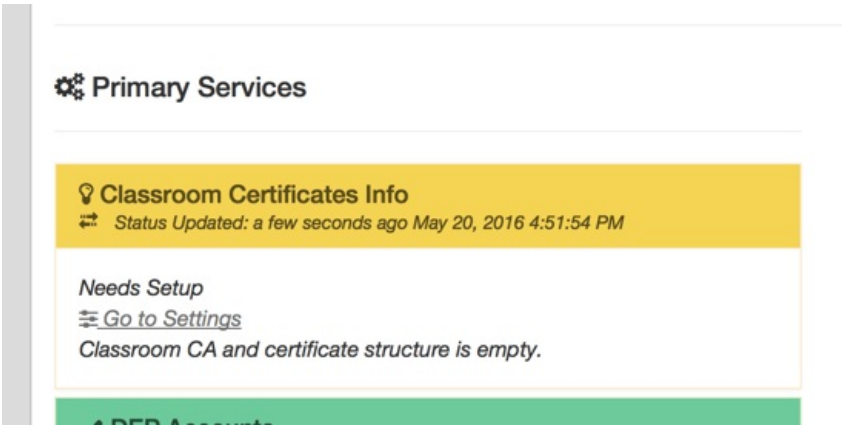
FileWave 11.1 includes support for Apple Classroom. The setup recommended by Apple for MDM providers is to have one root CA, intermediate CAs for leaders (teachers) and members (students) and one certificate per device. This means we need a UI where administrators are able to generate, view and manage those certificates, which allows renewing/revoking certificates, as well as creating the initial root CA and intermediate CAs.

In the Admin

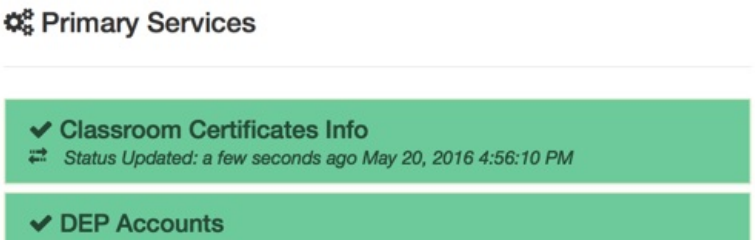
Dashboard

First place where you might see anything that is related to classroom is in the dashboard. By default we check if all the certificates are ok. It goes into warning state (yellow) if a certificate is about to expire (in less than 30 days) or if the whole classroom CA/certificate chain is absent. IT goes into error if at least on the the certificate is already expired.

In case of warning or error, you can click on "Go to settings" and it will ask you the super user credentials and if you want to create the defaut CA/Certificates (see following on how to proceed).

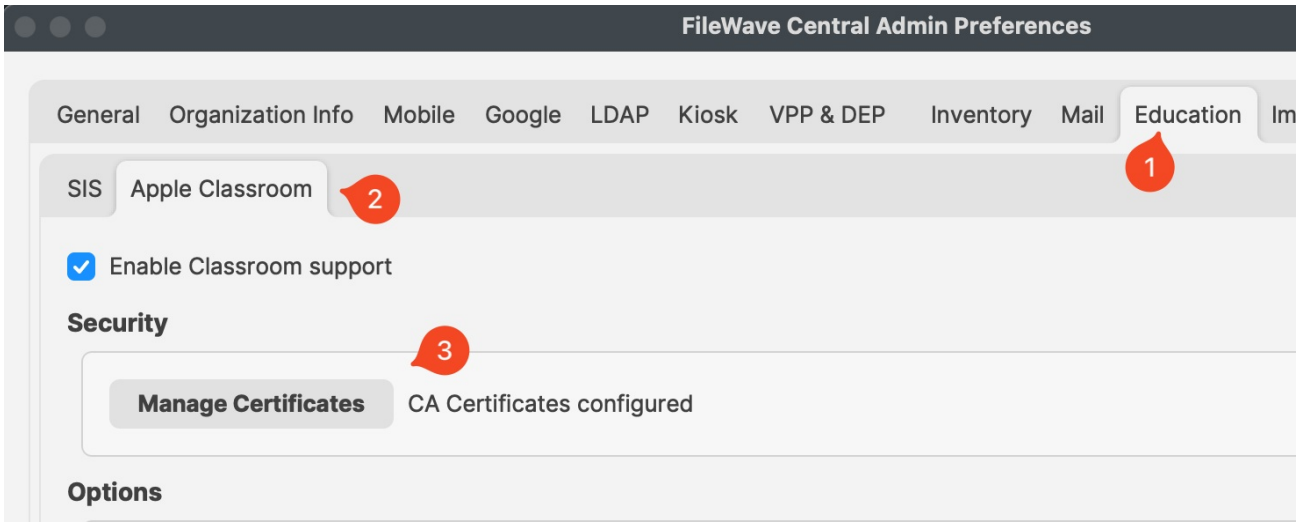


After it has refreshed (can take a few seconds), it will look like that:

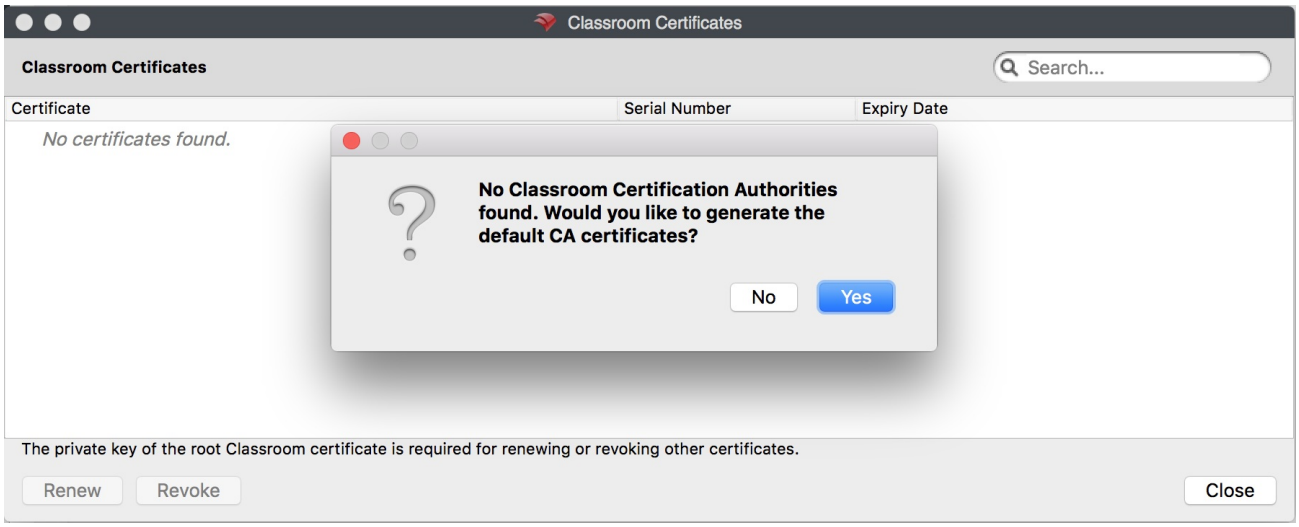


Preferences

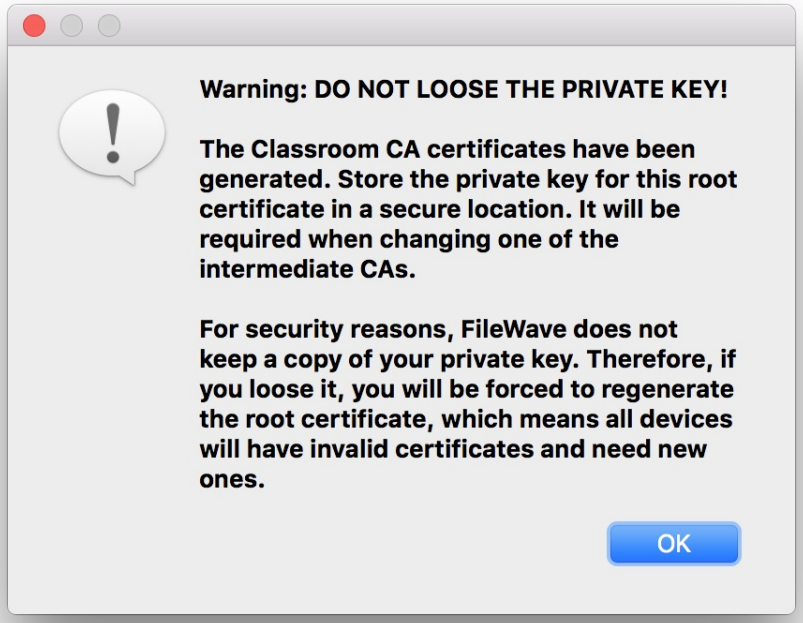
The certificate management UI is available in the Preferences, in the Education section, on the Apple Classroom tab. Click "Manage Certificates" to open the Classroom certificate management UI. You will need to enter fwadmin credentials.



The first time you open the Manage Certificates dialog, no certificates exist at all. Therefore, FileWave Admin asks you whether you want to generate the certificates:

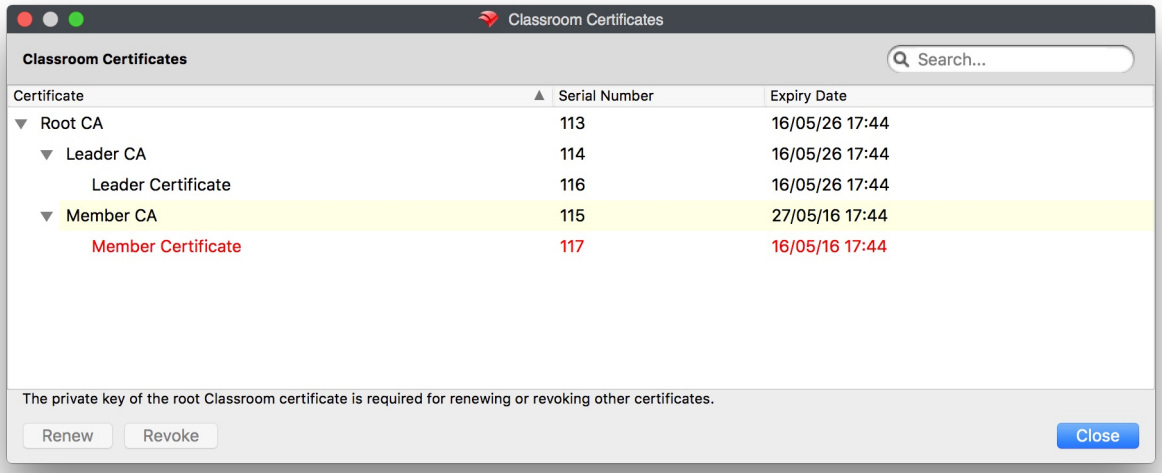


As part of the process, a private key for the root CA certificate is generated. FileWave does not store a copy of this private key. It is your responsibility to store this key in a secure location, as you can see in the warning that is displayed.



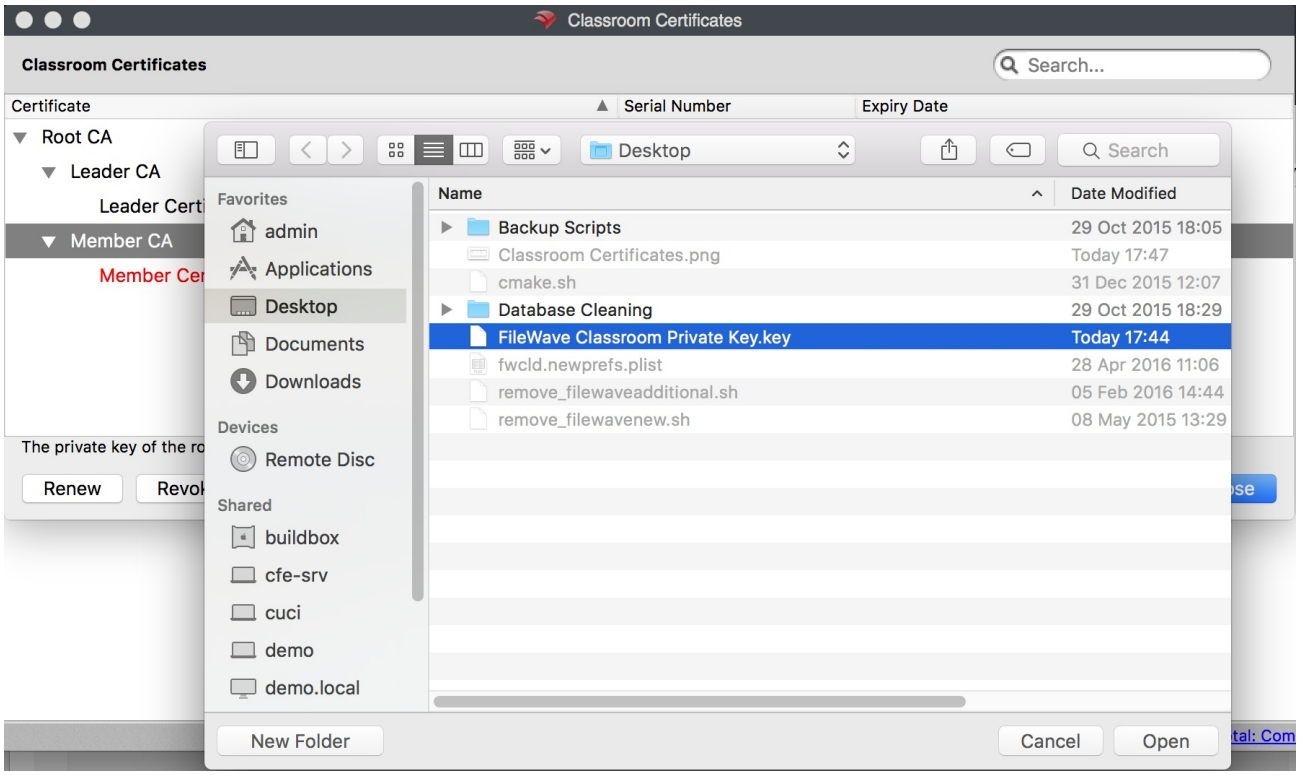
FileWave will ask you to store the private key as soon as the certificate generation is completed successfully. The private key is a PKCS #8 key stored in DER format. FileWave Admin saves this private key in the local disk of the computer where it is running and sets restrictive permissions on the file. You will need to provide this private key when renewing or revoking certificates. The default file name is "FileWave Classroom Private Key.key" and it is stored on the Desktop by default. If you press Cancel or the Esc key by mistake while on the save dialog, FileWave stores the private key on the default location anyway, so you won't need to regenerate the root CA.

The dialog displays the certificates in a tree structure, where the root CA certificate is the top level item in the tree and child certificates appear as child items. The serial number and the expiry date of each certificate are also displayed next to it. Certificates that will expire in less than one month are displayed with a yellow background, while expired certificates are displayed with red letters. You can sort by any column and filter certificates by typing some criteria in the search box and pressing Enter.



You can renew and revoke any certificates. In order to do so, select one or more certificates. The view supports multiple selection by holding the Ctrl key (⌘ on Mac) and clicking entries. You can then either right-click to get a context menu or use the corresponding buttons on the lower left corner of the dialog. When revoking a certificate, all its child certificates will also be revoked. The certificate and its child certificates will be renewed automatically right after revocation.

You don't need the private key for renewing or revoking leader or member certificates. However, renewing/revoking any intermediate CAs requires the private key of the Root CA that was generated before. The first time you renew or revoke an intermediate CA certificate, you will be asked to open the private key. It will be remembered for the duration of the dialog, so you won't need to open it again for any subsequent operations on CA certificates, unless any operation fails. If you close the dialog and open it again later, you will need to provide the private key again for renewing/revoking CA certificates.



Although not recommended, it is possible to revoke the root CA without providing the private key by clicking Cancel in the file dialog to open the private key. This is useful for example in case you loose the private key. Beware it will not be possible to revoke intermediate CAs before renewing the root CA certificate. However, after revoking the root CA, the whole certificate tree will be regenerated automatically, including intermediate CA certificates and their child certificates.

> What is the impact if I lost my private key? You can revoke and start a new one. On devices they will get the new keys when they check in. Shared iPads will need each user to logout and login again.

Under the Hood

Device certificates are valid for 10 years. FileWave takes care of renewing device certificates automatically when they are about to expire. This is done 30 days before the expiry date. On the other hand, CAs cannot be renewed automatically because the private key is required. For this reason, administrators should take care of renewing the CA certificates manually. When the CA certificates are about to expire, a warning is displayed in the Dashboard.

Revision #1
★Created 1 May 2024 15:45:30 by Josh Levitsky
Updated 1 May 2024 16:00:12 by Josh Levitsky