Self-signed SSL Certificates

Self-Signed SSL Certificates Going Forward

Using a self-signed certificate is not the recommended option and needs to be given a second thought before implementation. Having a certificate trusted by a Global Certificate Authority (CA) is not only the most recommended and most secure option but also becoming more of a requirement for a lot of processes in the tech world.

Having a certificate trusted from a CA will also make sure all of your FileWave communication is as secure and user experience as simplified as possible. If you’re FileWave server is going to be managing Chromebooks then a root trusted certificate is required, where as managing iOS devices were self-signed certs can work, you will have to manually trust the certificate during OTA enrollment for the device to communicate with FileWave.

Of course there are some use cases where a self-signed certificate makes sense such as a test or evaluation server.

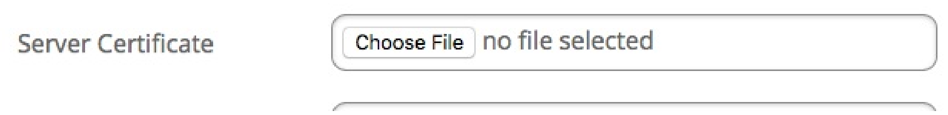
FileWave Clients

When using a self-signed certificate your client devices will need this certificate to trust for proper and secure communication with FileWave.

Initial Install

If the FileWave Client has never been installed on your macOS or Windows devices then you will need to create a custom PKG/MSI. This custom package will need to be filled out with your server address, booster info, and other important data to make sure your clients connect successfully to the FileWave Server. One of those options is Server Certificate, you will need to upload your self-signed certificate into this option so that your new client devices will be trusted by the FileWave server.

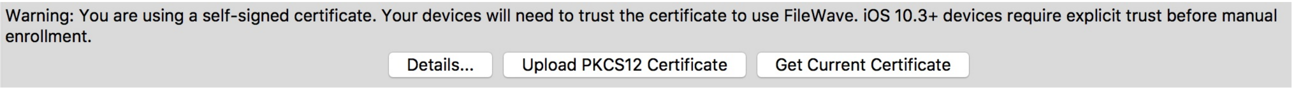
- macOS Custom PKG
- Windows Custom MSI



How do you get the self-signed certificate to upload?

To get the self-signed certificate that needs to be uploaded just follow the steps below:

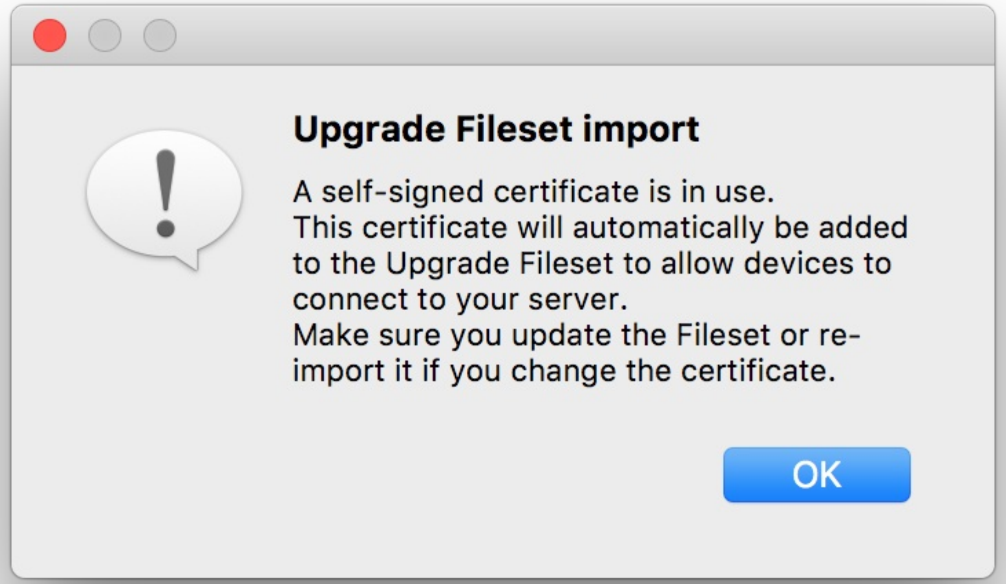
1. Log into the FileWave Admin
2. Go to FileWave Admin → Preferences
3. While in the General Tab find the SSL Certificate Management pane
4. Finally click the Get Current Certificate button, this will download the current SSL certificate you have in FileWave


Warning: You are using a self-signed certificate. Your devices will need to trust the certificate to use FileWave. iOS 10.3+ devices require explicit trust before manual enrollment.

iOS devices will enroll normally during DEP but, during OTA enrollment the FileWave certificate will need to be trusted manually. Please refer to the KB article linked here for more information.

Upgrade

All macOS and Windows clients on FW version 12.9.1 and below will still communicate with the FileWave server, but once upgraded to version 13 the self-signed certificate will need to be pushed to the devices. This will be done automatically when you upload the FileWave version 13 upgrade Fileset into the Filesets section the FileWave Admin.



Upgrade Fileset import

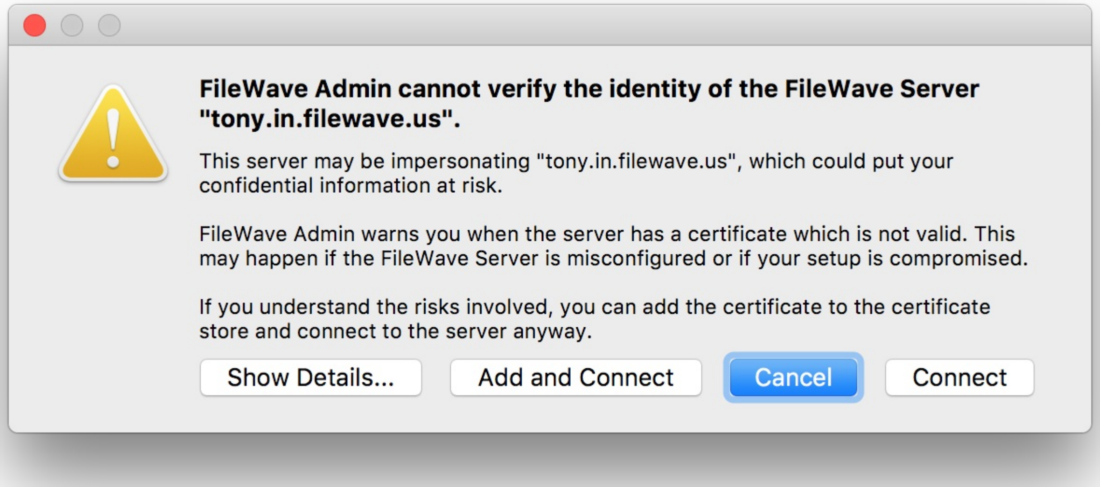
A self-signed certificate is in use.
This certificate will automatically be added to the Upgrade Fileset to allow devices to connect to your server.
Make sure you update the Fileset or re-import it if you change the certificate.

iOS devices will not need anything pushed out, when the FileWave server is updated. But keep in mind during OTA enrollment the FileWave certificate will need to be trusted manually. Please refer to the KB article linked here for more information.

If you need to renew your self-signed certificate please refer the KB article linked here for those steps.

FileWave Admin

If using a self-signed certificate the FileWave Admin won't be able to verify the identity of the server. When you log into the Admin you will be prompted that the server doesn't trust the certificate and you have the option to continue with the connection being untrusted or you can add the certificate to your trust store then connect. Also when you connect via the Web Console you will be warned that the connection is not private.

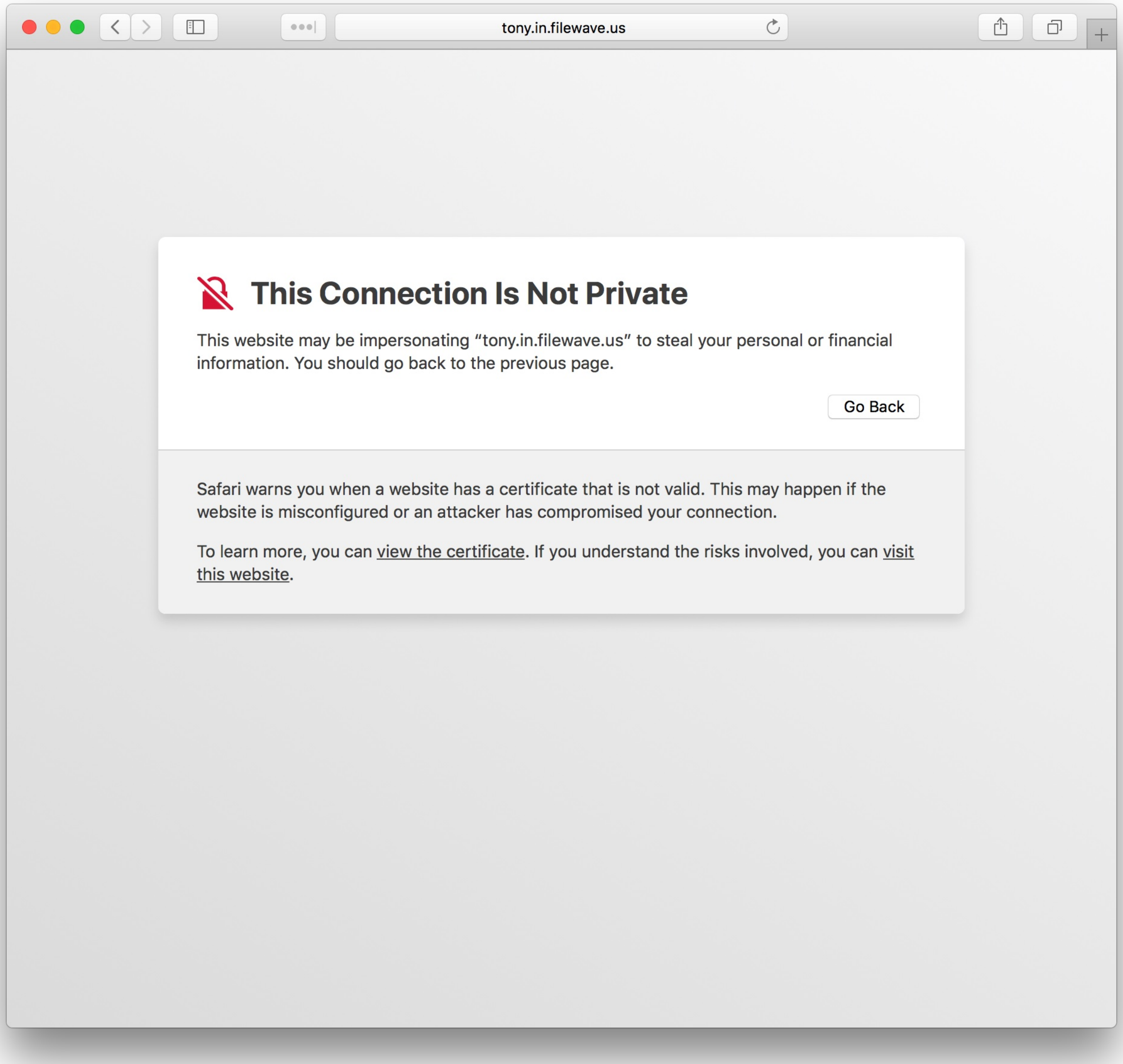


FileWave Admin cannot verify the identity of the FileWave Server "tony.in.filewave.us".

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.



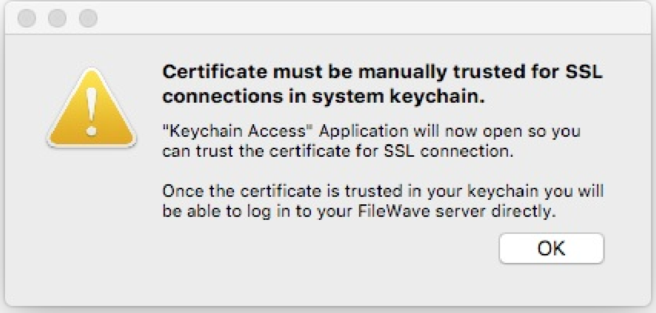
This Connection Is Not Private

This website may be impersonating “tony.in.filewave.us” to steal your personal or financial information. You should go back to the previous page.

Safari warns you when a website has a certificate that is not valid. This may happen if the website is misconfigured or an attacker has compromised your connection.

To learn more, you can view the certificate. If you understand the risks involved, you can visit this website.

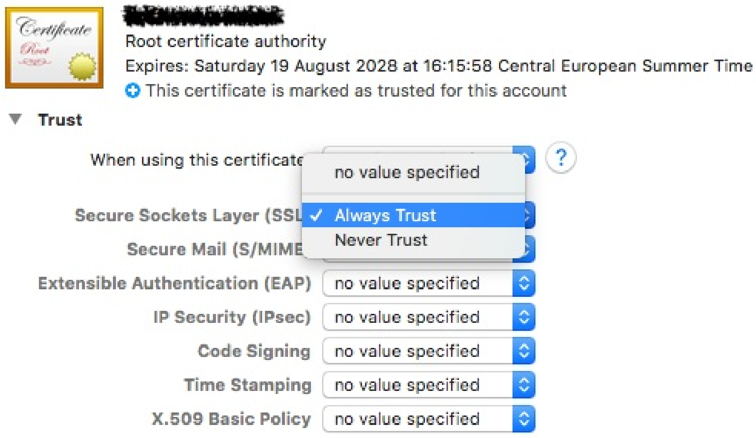
On macOS, certificates manually added to trust store require explicit "Trust for SSL" permission.



Certificate must be manually trusted for SSL connections in system keychain.

"Keychain Access" Application will now open so you can trust the certificate for SSL connection.

Once the certificate is trusted in your keychain you will be able to log in to your FileWave server directly.



[redacted]

Root certificate authority

Expires: Saturday 19 August 2028 at 16:15:58 Central European Summer Time

This certificate is marked as trusted for this account

▼ Trust

When using this certificate: no value specified

Secure Sockets Layer (SSL) ✓ Always Trust

Secure Mail (S/MIME)

Extensible Authentication (EAP) no value specified

IP Security (IPsec) no value specified

Code Signing no value specified

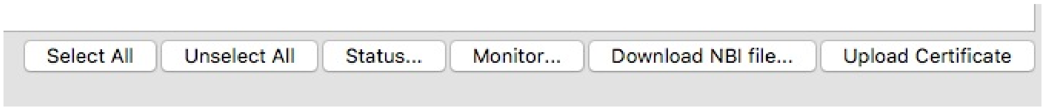
Time Stamping no value specified

X.509 Basic Policy no value specified

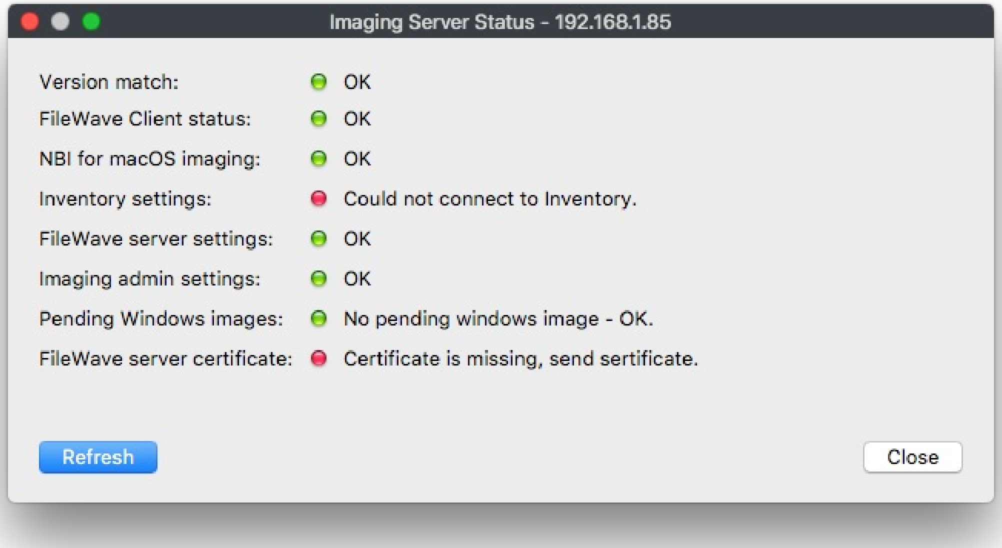
Imaging Virtual Server

When using self-signed certificates the FileWave server will automatically transfer the certificate to a newly created IVS, but existing imaging servers will need to be pushed the certificate.

1. Log into the FileWave Admin
2. Go to FileWave Admin → Preferences → Imaging
3. Select an imaging server then the Upload Certificate button at the bottom right of the pane



This will send the SSL certificate to the IVS, you have to do this for any existing IVS you have attached to your FileWave server. You can check the status of the IVS to see whether or not the certificate is uploaded, by selecting the IVS and clicking the Status... button.


Imaging Server Status - 192.168.1.85

Version match: ● OK

FileWave Client status: ● OK

NBI for macOS imaging: ● OK

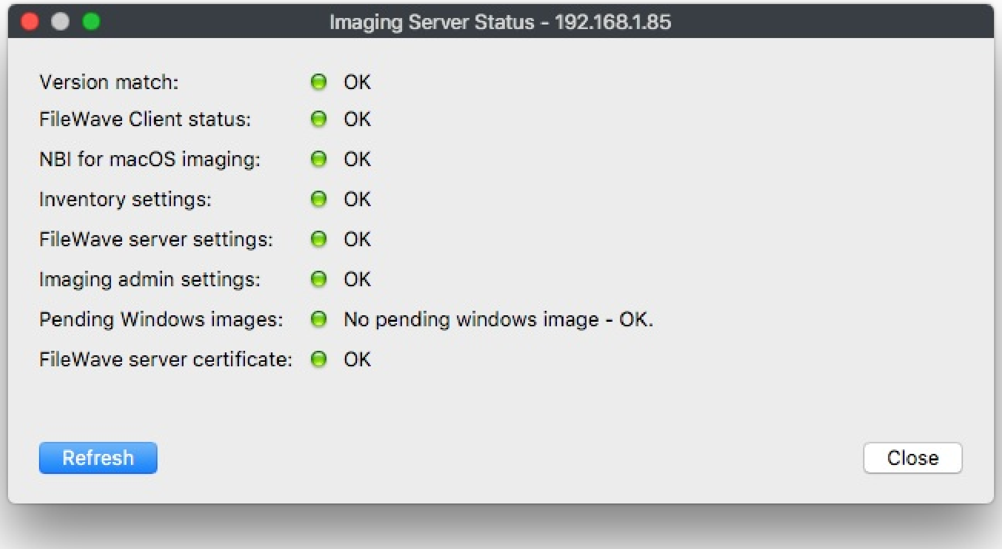
Inventory settings: ● Could not connect to Inventory.

FileWave server settings: ● OK

Imaging admin settings: ● OK

Pending Windows images: ● No pending windows image - OK.

FileWave server certificate: ● Certificate is missing, send sertificate.



Imaging Server Status - 192.168.1.85

Version match:	●	OK
FileWave Client status:	●	OK
NBI for macOS imaging:	●	OK
Inventory settings:	●	OK
FileWave server settings:	●	OK
Imaging admin settings:	●	OK
Pending Windows images:	●	No pending windows image - OK.
FileWave server certificate:	●	OK

Related Content

- Let's Encrypt Setup for FileWave Server (Debian)
- FileWave Server SSL Certificate from Windows

Renew FileWave Server Self-signed Certificate

Description

For simplicity, we should recommend Renewing with an Official SSL certificate or Let's Encrypt Setup for FileWave Server (Debian)

> Using a self-signed certificate is strongly discouraged for a production server.

Information

A self-signed certificate may not be trusted by devices out of the box. Instead, the device requires a local copy to be able to trust the certificate. Prior to FileWave 13, this has only affected Mobile devices: Renew MDM self signed SSL certificate on iOS

However, FileWave uses the certificate for additional security for non MDM communication and initial installation or upgrading to FileWave 13 from a release of 12 or lower.

> Renewal though requires additional steps to ensure device communication is not lost.

Directions

The 'fwcontrol' command for creating certificates is now a 2 step process, where 'fqdn' should be the Fully Qualified Domain Name of your FileWave Server, e.g. demo.filewave.ch:

```
sudo fwcontrol server generateSelfSignedCert --create --cn=fqdn [--country COUNTRY] [--state STATE] [--locality
LOCALITY] [--organization ORGANIZATION] [--ou ORGANIZATIONAL_UNIT] [--email EMAIL] [--ignore_name_mismatch]
sudo fwcontrol server generateSelfSignedCert --install
```

Bracketed options are not required, but may be specified.

Step 1

Certificate Generation

Using demo.filewave.ch as an example:

```
sudo fwcontrol server generateSelfSignedCert --create --cn=demo.filewave.ch. --country Switzerland
```

This first step generates a new certificate, but unlike before, it does not overwrite the current active certificate. Instead, this certificate is in a 'pending' state. You should see the following warning when creating the certificate:

```
WARNING: Self-signed certificates are NOT recommended! If you install one, clients in version 13 or greater will
no longer allow connections with the FileWave Server unless you put the new self-signed certificate in their trust
store.
A self-signed certificate has been successfully created and is now pending for later installation on the server.

IMPORTANT!
- Before installing it, you must deploy it to the trust store of any device whose FileWave Client is in version 13
or greater, otherwise these clients will no longer be able to connect to the server!
To do so, you can create a fileset with a copy of /usr/local/filewave/certs/server.crt.pending to be deployed in
the trust store folder.
- Once you are ready to install the new self-signed certificate and if you understand the risks, please run this
command again with option --install.
running restart apache command
```

Instead a new certificate key/crt pair of files may be seen in the following server folder and will show as 'pending', along with the original key/crt pair:

```
/usr/local/filewave/certs/server.crt
/usr/local/filewave/certs/server.crt.pending
/usr/local/filewave/certs/server.key
/usr/local/filewave/certs/server.key.pending
```

As indicated by the Important message, all clients will require a copy of this certificate to communicate with the server. During transition, it is important that both original and new certificate are installed on devices. Copy the server.crt.pending and rename appropriately for deployment. e.g. server.2019.04.30.crt

Mobile Devices

Installing the new certificate on Mobile devices is as before, except a profile needs to be made with this new certificate as well as the current certificate:

Renew MDM self signed SSL certificate with iOS devices

Computers

Installing the new certificate on Computers is the same as the process for Upgrading to FileWave 13, but this new certificate needs to be added to a Fileset manually. This could either be the current FileWave Upgrade Fileset or a new Fileset. Location of the file is either:

macOS:

macOS Client/Booster Trust Store

```
/private/var/FileWave/trust_store
```

Windows:

Windows Client/Booster Trust Store

```
C:\ProgramData\FileWave\FWClient\trust_store
```

⚠ Set the certificate 'Verification' to 'Ignore At Verify' to ensure it is never removed

⚠ If the new certificate should become live on the server prior to the clients receiving this Fileset, those devices will no longer be manageable through FileWave and a manual process will be required to locally instal the certificate.

Whichever option is chosen, a method should be designed to monitor the installation process. Only once all devices are updated, should the 'pending' certificate become the active server certificate.

Options for monitoring could include:

- Fileset Reports
- Custom Fields

A Custom Field could take the following form (assuming the example file name of 'server.2019.04.30.crt'):

macOS Example Custom Field

```
#!/bin/bash

server_cert=$(find /var/FileWave/trust_store -name "server.*.crt")

if [[ "$server_cert" != "" ]]
then
    echo Yes
else
    echo No
fi

exit 0
```

Step 2

This second step enables the 'pending' certificate as the active certificate, replacing the original server certificate file.

```
sudo fwcontrol server generateSelfSignedCert --install
```

Once all clients have the new certificate within their respective trust stores, the 'pending' server certificate may now become active. When this update of the certificate occurs, any other elements requiring the server certificate should also be updated as this time.

DEP

The server certificate is stored as an 'Anchor certificate' within any created DEP profile. As with any certificate change, once the certificate is renewed, new DEP profiles should be created; do not duplicate.

Custom PKG/MSI

The Custom Client Installer also needs to include the certificate. The following links allow for uploading the current server certificate within the 'Options'

- macOS Custom Client Builder
- Windows Custom Client Builder

Details highlighted on: Self-Signed Certificates Going Forward

Renew MDM self signed SSL certificate with iOS devices

Self Signed certificate renewal

Renewing MDM self-signed certificate can be done if the current certificate has to be changed:

- the certificate is or is about to expire
- the certificate is not or will not be trusted by devices anymore

The main issue with self-signed certificate is that, by definition, those certificates are not issued by a trusted Certificate Authority (CA), and are not trusted by default on devices. To have devices trust those certificates, the certificate must be added to the trust store. This can be achieved by:

- DEP enrollment, which can add the server certificate
- Deploying a profile
- manually installing and trusting the certificate

> In production environment, it is highly recommended to use trusted CA issued certificate ; self-signed certificates should only be used for testing and evaluation purpose. The best and most simple way to solve self-signed certificate renewal issues is to stop using self-signed certificate and use trusted CA certificates. There are free options like Let's Encrypt to have a trusted cert.

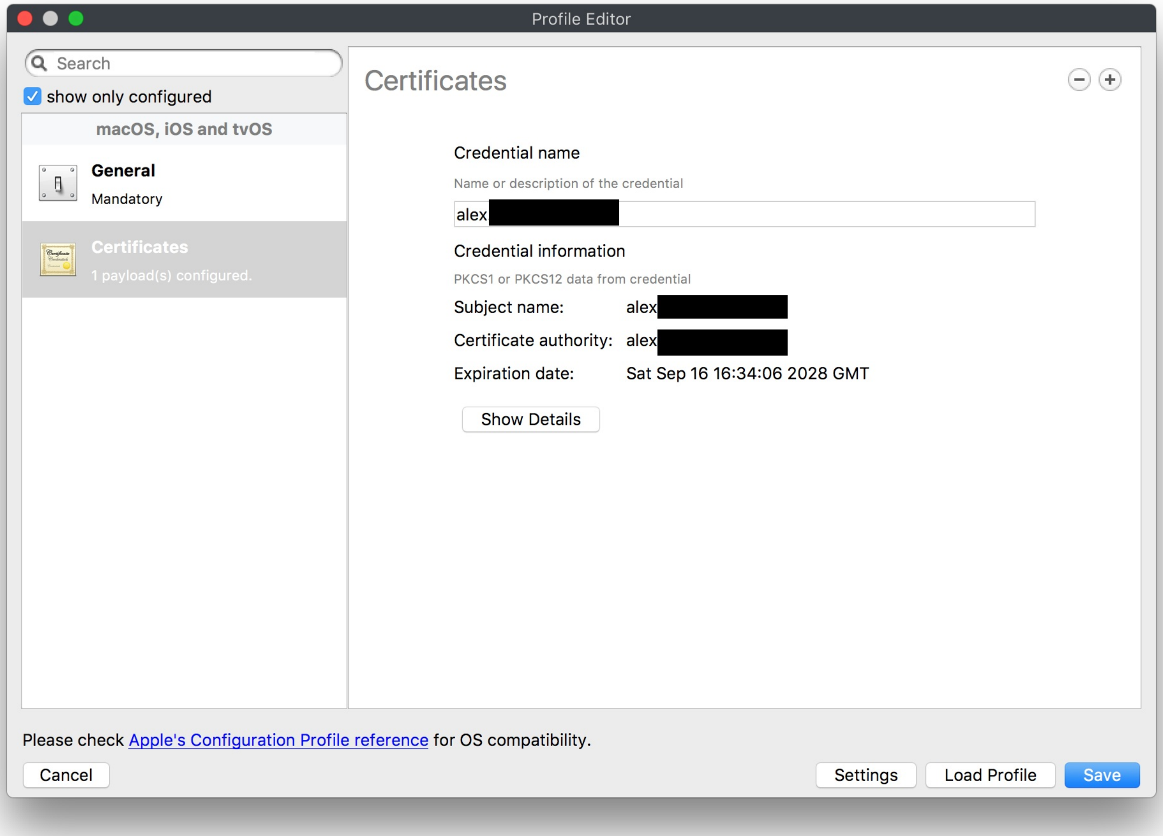
Planned renewal

In case you need to renew a self-signed certificate, you need to ensure all your devices will trust the new certificate before you renew it ; this implies the following steps:

1. Create a new private key and certificate

```
$ openssl req -x509 -nodes -sha256 -days 3650 -newkey rsa:2048 -keyout /tmp/server.key -out /tmp/server.crt
Generating a 2048 bit RSA private key
...........................................................+++
....................+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:filewave.acme.org
Email Address []:
```

2. Import server.crt file into a profile fileset



Certificates

Credential name

Name or description of the credential

alex[redacted]

Credential information

PKCS1 or PKCS12 data from credential

Subject name: alex[redacted]

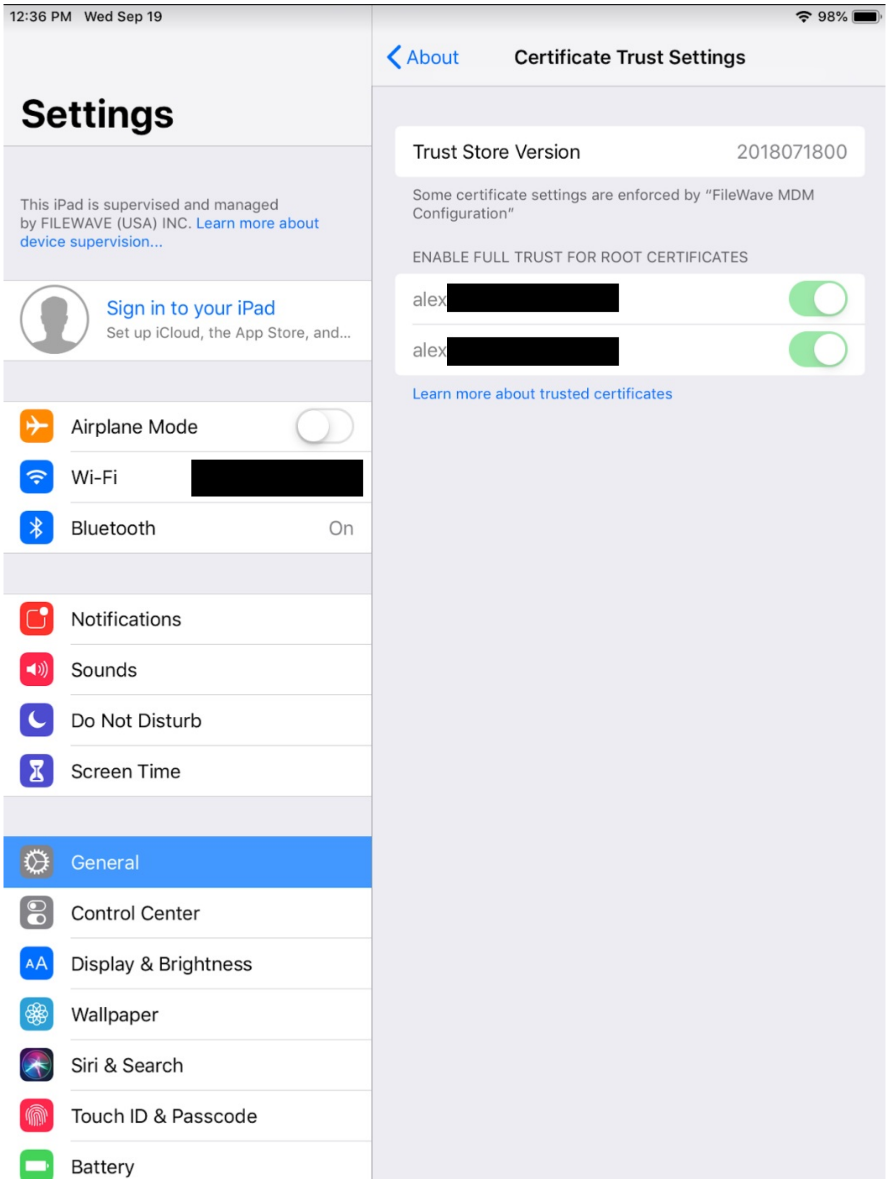
Certificate authority: alex[redacted]

Expiration date: Sat Sep 16 16:34:06 2028 GMT

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

3. Deploy the profile filest to all your devices

4. You are able to confirm that the profile was received and trusted by the device by going to Settings → General → About → Certificate Trust Settings, and should see your old as well as new self-signed certificate listed and trusted. The screen shot below shows what you will see with the device trusting both certificates.



12:36 PM Wed Sep 19 98%

Settings

This iPad is supervised and managed by FILEWAVE (USA) INC. Learn more about device supervision...

Sign in to your iPad
Set up iCloud, the App Store, and...

Airplane Mode

Wi-Fi [redacted]

Bluetooth On

Certificate Trust Settings

Trust Store Version 2018071800

Some certificate settings are enforced by “FileWave MDM Configuration”

ENABLE FULL TRUST FOR ROOT CERTIFICATES

alex[redacted]

alex[redacted]

Learn more about trusted certificates

5. Once all devices have the profile, you can switch the key and certificate. The path to your new "server.crt" and "server.key" may change depending on where the certificate is located on your FileWave server:

```
$ cd /usr/local/filewave/certs
$ mkdir old_certs
$ mv server.crt server.key old_certs
$ cp /tmp/server.*
$ fwcontrol apache restart
```

6. Re-create DEP profiles and associations as the DEP profile contains a copy of the certificate and is sent to Apple at association time ; a new certificate implies a new DEP profile.

⚠ Failure to update your DEP profiles to have the new profile will cause trust issues at enrollment

Unplanned or late renewal

❗ Worst case possibility using a self-signed cert that expires.

If the current certificate is not trusted by devices anymore (or because some devices did not get the new certificate before the switch), the renewal process remains the same, but with one exception: as devices will stop trusting the server certificate it's not possible to use FileWave to deploy the new certificate.

At this point, the best solution is to move forward with a trusted CA certificate ; your devices will start communicating immediately to your server as soon as the certificate is in place.

In case trusted CA is not possible, you will have to manually add the certificate to each impacted device:

1. deploy the new certificate to devices ; you can either send it via e-mail, or send your users to the usual enrollment page and ask them to install the cert via "step 1"
2. in the trust store, the newly installed certificate must be granted "use for SSL" permission

Related Content

- Renew FileWave Server Self-signed Certificate
- Let's Encrypt Setup for FileWave Server (Debian)