

Using Self-Signed Certificates with FileWave

Use a certificate issued by a publicly trusted certificate authority (CA) for production FileWave environments whenever possible. It reduces manual trust work, avoids certificate warnings, and gives FileWave components and managed devices a consistent chain of trust.

A publicly trusted certificate is required for Chromebook management. Self-signed certificates can still be used in some iOS enrollment and desktop-client workflows, but administrators must distribute or explicitly trust the certificate where the platform requires it. That trust requirement applies independently to FileWave Clients, FileWave Central, browsers opening the Web Console, and existing Imaging Virtual Servers.

Self-signed certificates remain useful for isolated test or evaluation servers where administrators control every device and trust store. The sections below explain the additional package configuration, manual trust prompts, certificate export, and IVS update steps.

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](#)

Server Certificate

Choose File no file selected

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. Open FileWave Central.
2. Go to FileWave Central → Preferences.
3. On the General tab, find SSL Certificate Management.
4. Click Get Current Certificate to download the certificate currently used by the FileWave Server.

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.

[Details...](#)

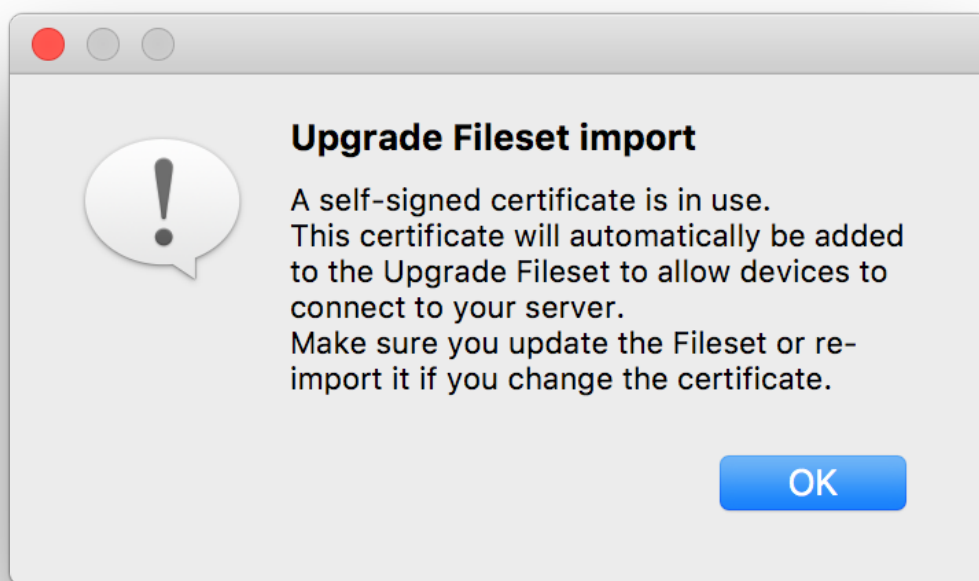
[Upload PKCS12 Certificate](#)

[Get Current Certificate](#)

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.

Historical FileWave 13 upgrade behavior

i Historical note. For migrations from FileWave 12.9.1 or earlier to FileWave 13, the version 13 upgrade Fileset automatically delivered the self-signed certificate to macOS and Windows clients. Current upgrades should follow the instructions for the target release.

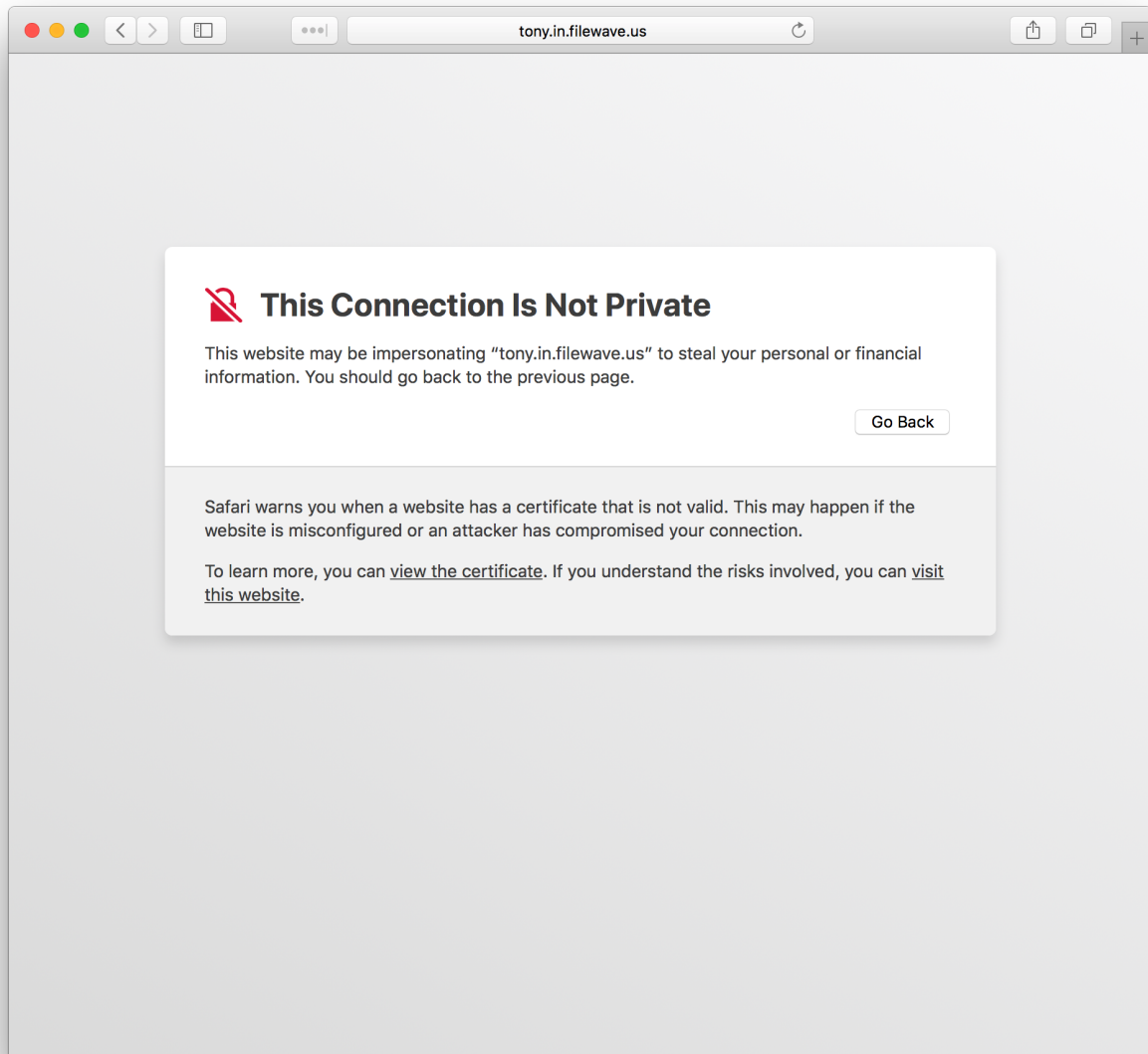
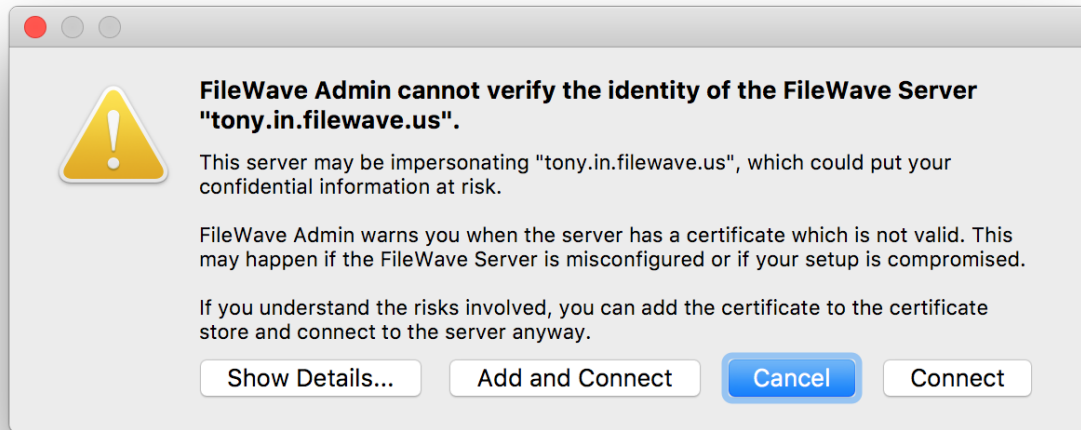


iOS devices will not need anything pushed out, when the FileWave server is updated. But keep in mind during OTA enrollment the FileWave certificate will need to be trusted manually. Please refer to the [KB article linked here](#) for more information.

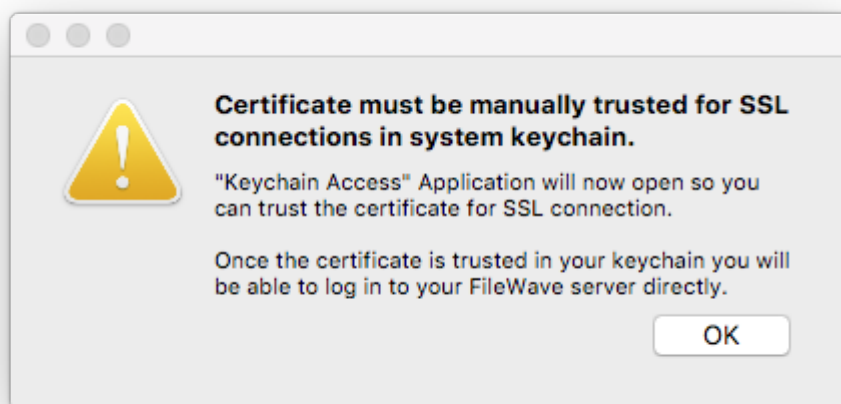
If you need to renew your self-signed certificate please refer the [KB article linked here](#) for those steps.

FileWave Central and the Web Console

With a self-signed certificate, FileWave Central cannot verify the server identity until the certificate is trusted locally. Central may offer either an untrusted connection or an option to add the certificate to the trust store. A browser opening the Web Console will also display a certificate warning until the certificate is trusted.



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



[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

Never 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. Open FileWave Central.
2. Go to FileWave Central → Preferences → Imaging.
3. Select an imaging server, then click Upload Certificate at the bottom right of the pane.

Select All

Unselect All

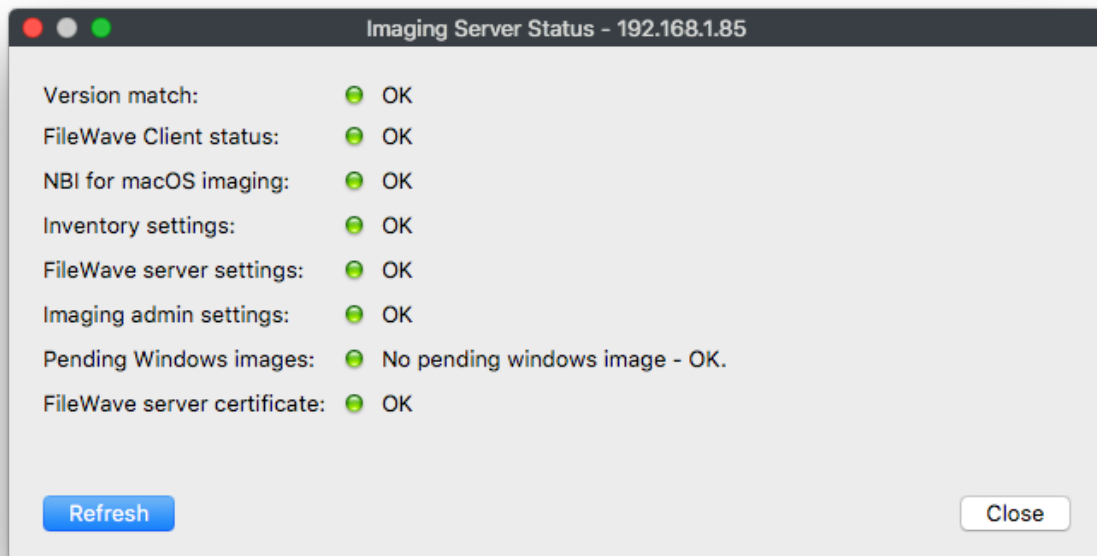
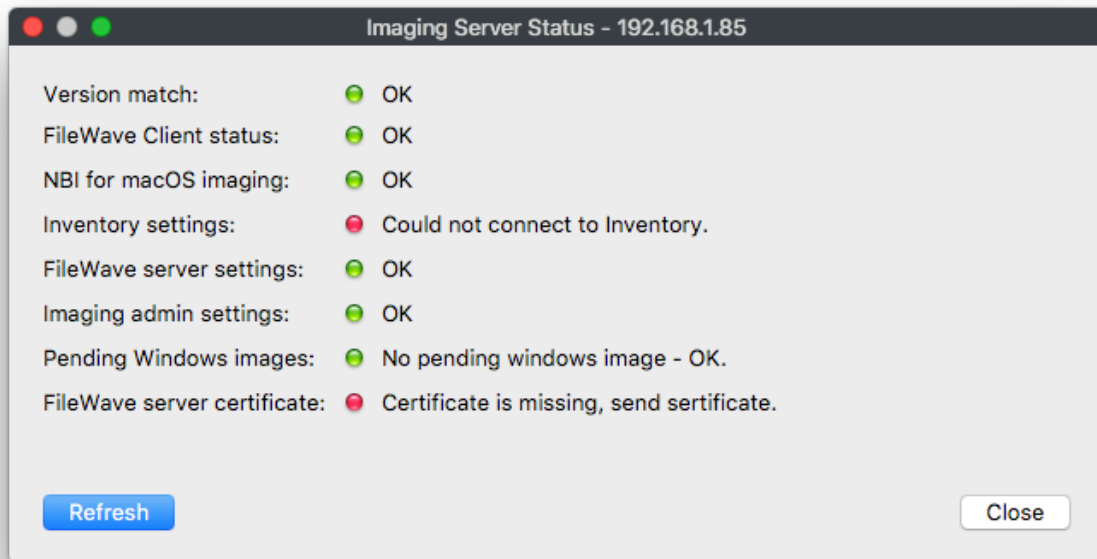
Status...

Monitor...

Download NBI file...

Upload Certificate

Repeat this for every existing IVS attached to the FileWave Server. To verify the certificate state, select the IVS and click Status....



Related Content

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

🕒 Revision #8

★ Created 2023-07-10 23:33:49 UTC by Josh Levitsky

✎ Updated 2026-08-07 12:55:50 UTC by Josh Levitsky