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.

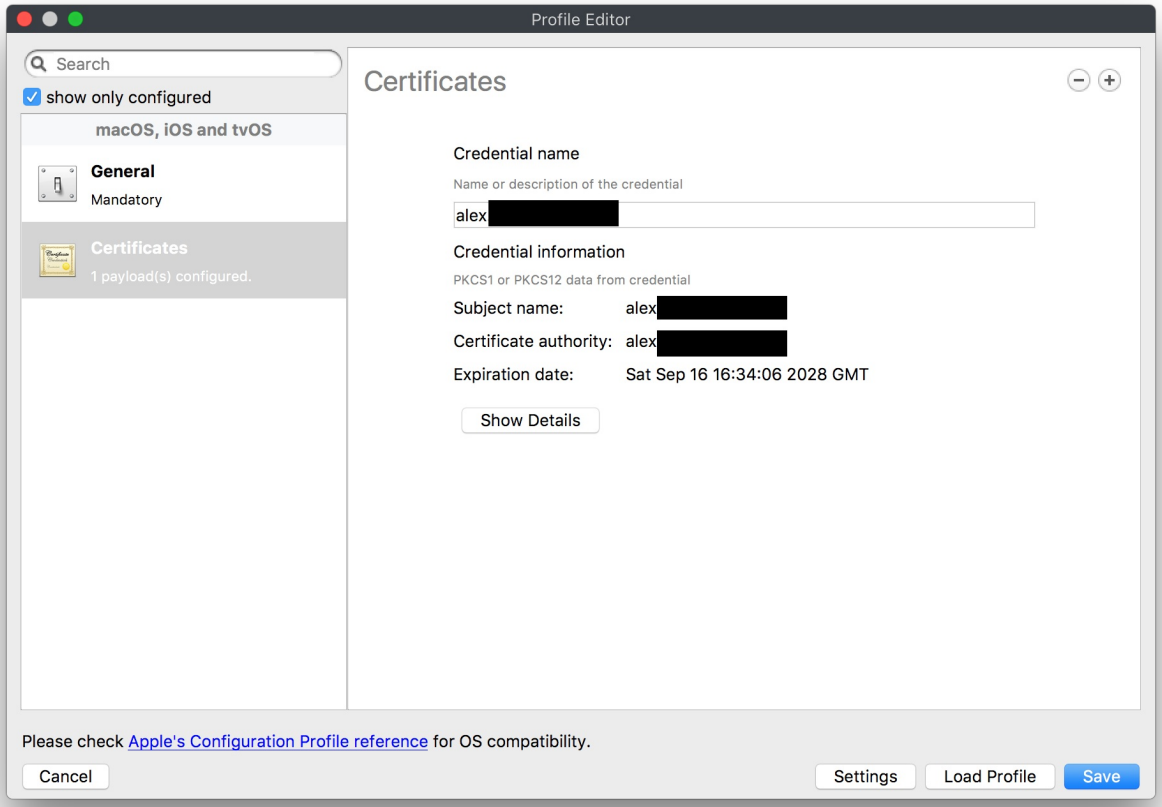
Planned renewal

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

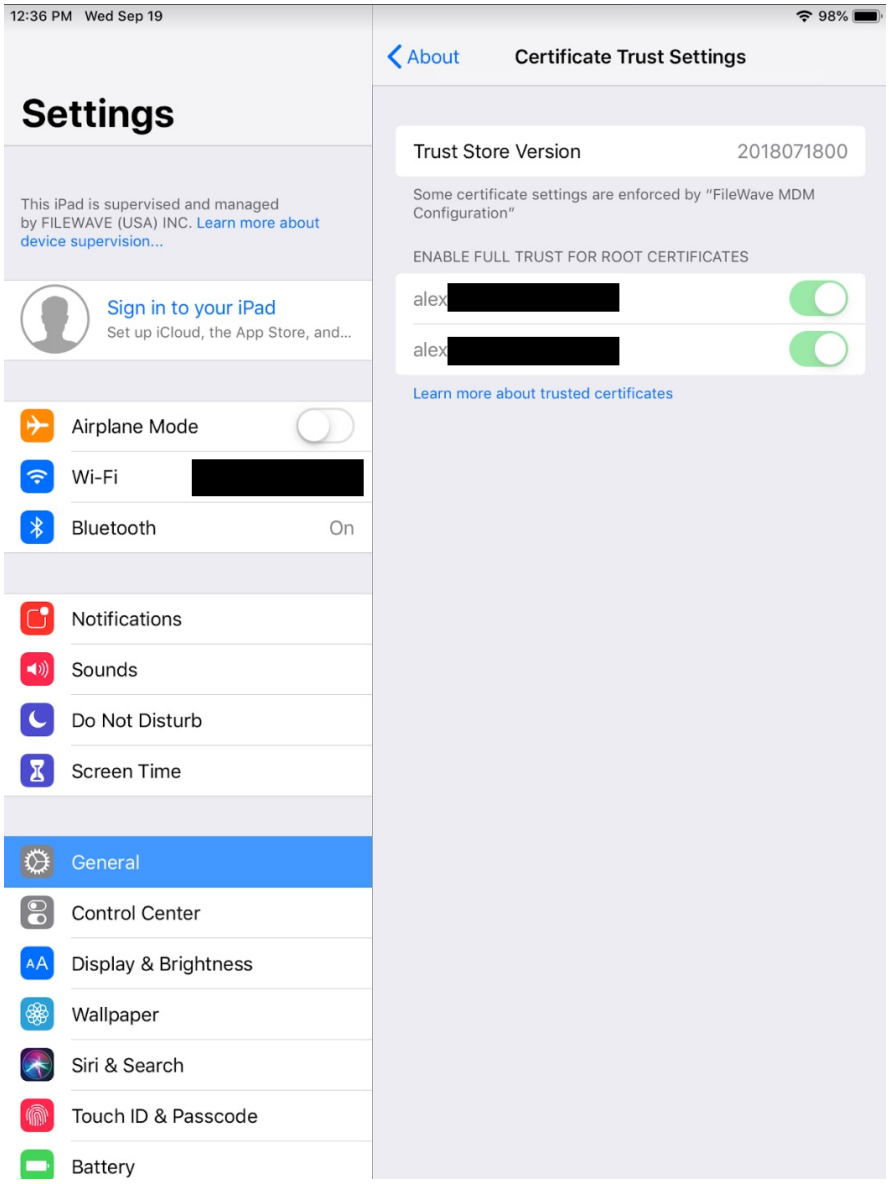
```
$ openssl req -x509 -nodes -sha256 -days 3650 -newkey rsa:2048 -keyout /tmp/server.key -out /tmp/server.crt
Generating a 2048 bit RSA private key
.....................................................+++
.................+++
writing new private key to 'server.key'
-----
You are about to be asked to 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



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.



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)

Revision #8
★Created 10 July 2023 23:10:07 by Josh Levitsky
Updated 23 April 2024 14:41:10 by Josh Levitsky