

# SSL Certificate



It is highly recommended to use a company-owned SSL certificate in order to run all features of ApplicationInsights properly!

The SSL certificate and key are stored in the folder `/opt/panagenda/appdata/volumes/nginx`. If you want to use your own certificate, just put your files **certfile.pem** and **keyfile.key** in this folder.

*use `winscp.exe` to establish an ssh session and to copy it into the folder*

**Note: Both files must not be encrypted** (no pass phrase required)!



**Please note that you have to keep the filenames!**

After completing this step, please reboot the ApplicationInsights virtual appliance after changing the SSL certificate.

## What can you do if you have only a PFX file available?

You can extract the required private key and public cert from your PFX file:

Run the following commands on the ApplicationInsights command-line level by using **putty.exe** in order to extract the private key and save it as a KEY file (after you have copied the pfx file over to the appliance **/tmp** folder):

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out keyfile.key -nodes
```

You will be asked to enter the certificate password.

Once this has been done, run the following command to also extract the public cert and save it as a PEM file:

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out certfile.pem -nodes
```

Finally copy both files (**pem and key**) in the `/opt/panagenda/appdata/volumes/nginx` folder by using the following command

```
cp certfile.pem /opt/panagenda/appdata/volumes/nginx/certfile.pem
cp keyfile.key /opt/panagenda/appdata/volumes/nginx/keyfile.key
```

Make sure to reboot the ApplicationInsights virtual appliance