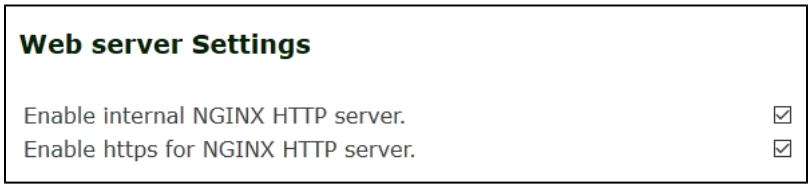
Update the SSL Certificate

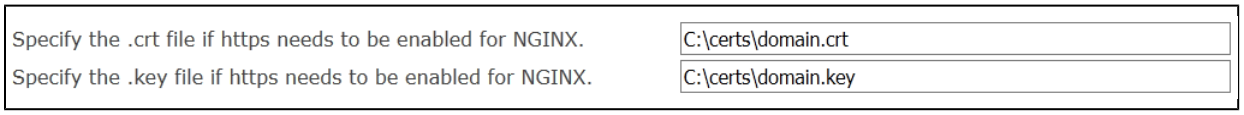
If you maintain Agiloft on your own server, you will need to update the SSL security certificate occasionally. The procedure to update the certificate on your server will depend on the type of web server you have integrated with Agiloft. We recommend Nginx as the front-end web server for stability and performance. If Agiloft is integrated with Nginx on your server, please follow these steps to upload a new certificate.

Follow these steps

1. Copy the SSL certificate and the private key for it to a directory on the server, for example: `C:\certs\`. Make sure the certificate and the private key are in PEM format.
2. Run the Setup.exe utility found under the Agiloft installation directory and access the server through HTTP on port 8888 with a web browser. The browser will show "Agiloft Setup Assistant".
3. Click the "Web Server" link to bring up the Web server settings page.
4. Select the checkboxes to enable Nginx HTTPS.



   Note: Nginx will reserve ports 80/443, so please set a different port for Jboss's internal web server - for example 8080/8443 - while enabling Nginx.
5. Scroll to the bottom of the page and specify the full path to the certificate and private key as shown in the screenshot below.



   Note: The certificates must be in the PEM format.
6. Click the "Change web server settings" button to apply and restart the application.
7. Test the new certificates by accessing the site via HTTPS through a browser, at https://www.<domain>.com/gui2/login.jsp.
   Note: If Agiloft is integrated with some other web server like IIS, please refer to the corresponding documentation from the vendor.