

REAL
INDUSTRIAL
TRANSFORMATION



OpenWebStart and Expired Certificates

OWS-expiredCert-10.1-V1.0-EN.pdf

Copyright

The dissemination and reproduction of this publication or parts or excerpts thereof, for whatever reason and in whichever form, are not permitted without the explicit written approval by iTAC Software AG. Photographs, diagrams and texts are subject to copyright and may only be used for other purposes with the approval of iTAC Software AG.

The iTAC products and services mentioned in the text and the respective logos and brand names are protected or registered brands of iTAC Software AG in Germany and other countries worldwide. The software products offered by iTAC Software AG may include software components of other software manufacturers.

All other logos, trademarks, brand names and names of products and services are registered and protected brands and trademarks of the relevant companies and their further use is subject to approval by these companies. We draw to your attention that it is not permitted to change or modify trademarks or brand names and that this may be legally prosecuted by the owner.

We accept no liability for references to third party suppliers, Internet links, and other source references, in any shape or form. The information and text included in this publication are intended only for informational purposes. Products may exhibit country-specific differences.

© 2024 - iTAC Software AG

All statements are subject to change and changes do not require notification.

Table of Contents

1. Scope of this document	3
2. How to configure OpenWebStart application to accept applications with expired code signing certificates	4
3. How to remove expired code signing certificates from OpenWebStart	6

1. Scope of this document

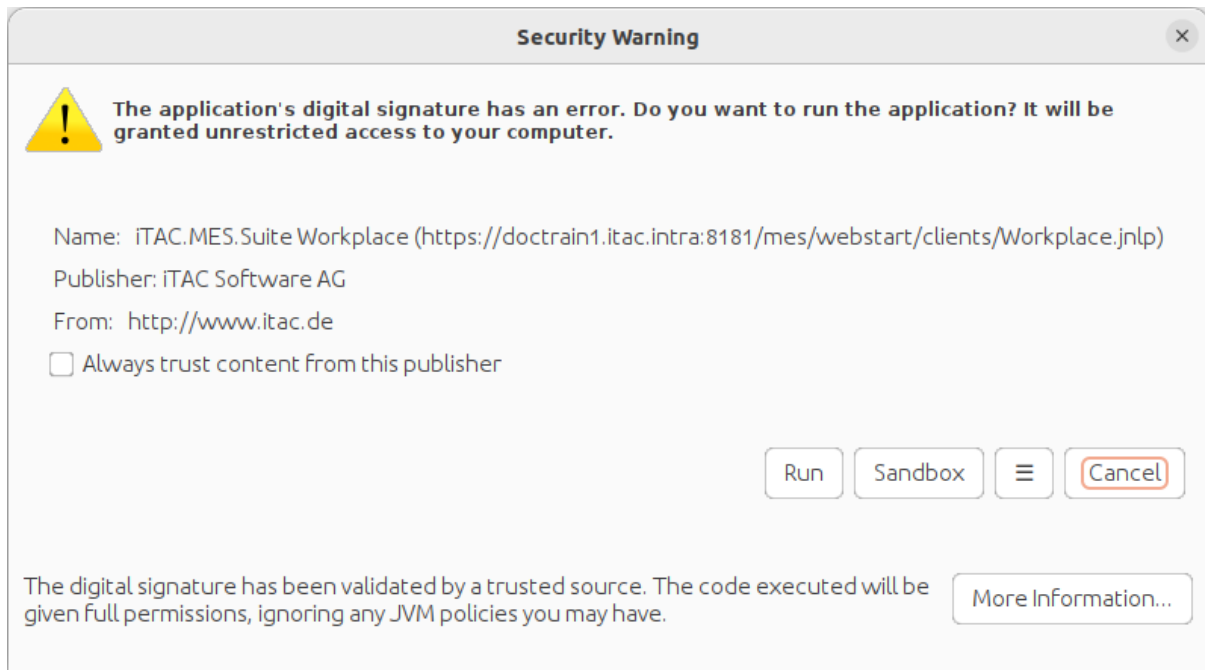
This document describes the necessary steps for configuring OpenWebStart to accept applications with expired code signing certificates. This only applies to systems using **OpenWebStart**.



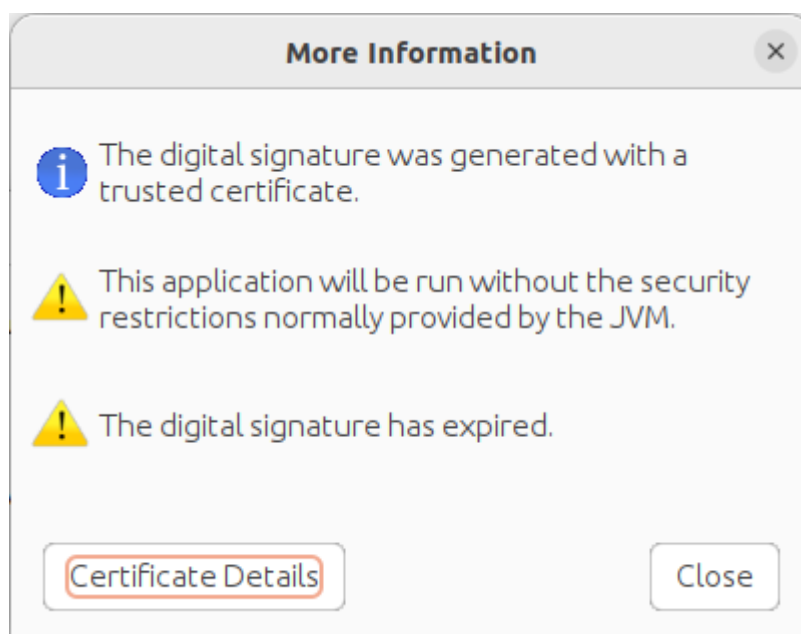
This document describes only a temporary workaround until the respective OpenWebStart applications with expired code signing certificates have been exchanged by applications with valid certificates!
Running applications with expired certificates as a general measure is not recommended due to security concerns!

2. How to configure OpenWebStart application to accept applications with expired code signing certificates

When starting an OpenWebStart application with an expired code signing certificate, a warning dialog similar to the following will be shown:

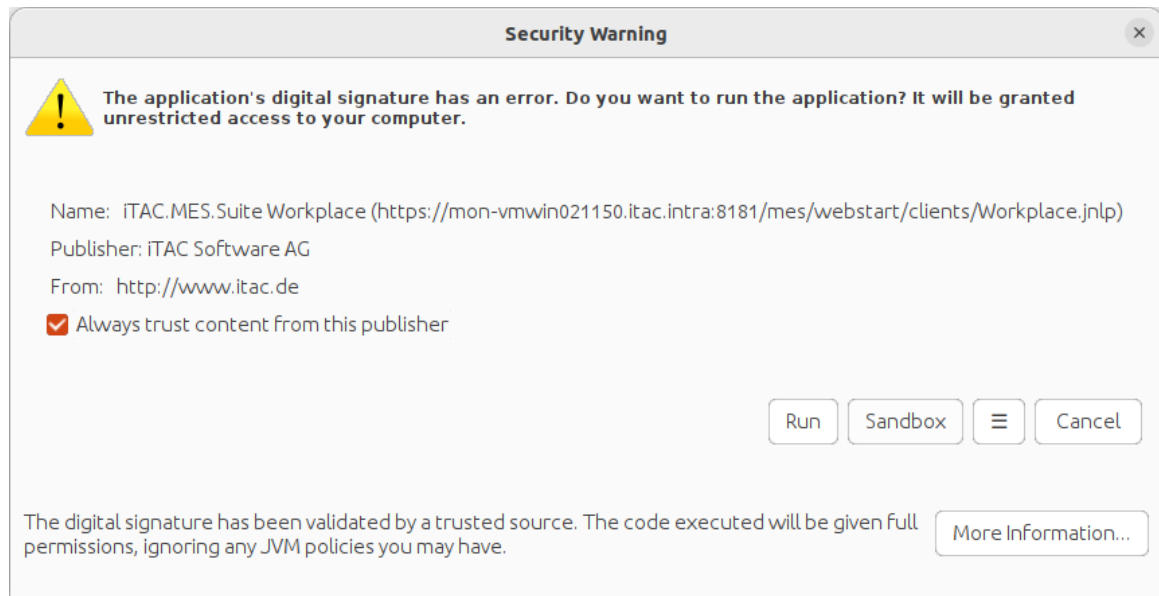


1. Click on [**More information**] to get more details on the warning.
2. See the third point:
The digital signature has expired.



In case of an expired code signing certificate, this the expected outcome. Click on [**Close**].

3. To avoid these **Security Warnings** showing up, activate the checkbox **Always trust content from this publisher** and click [**Run**].

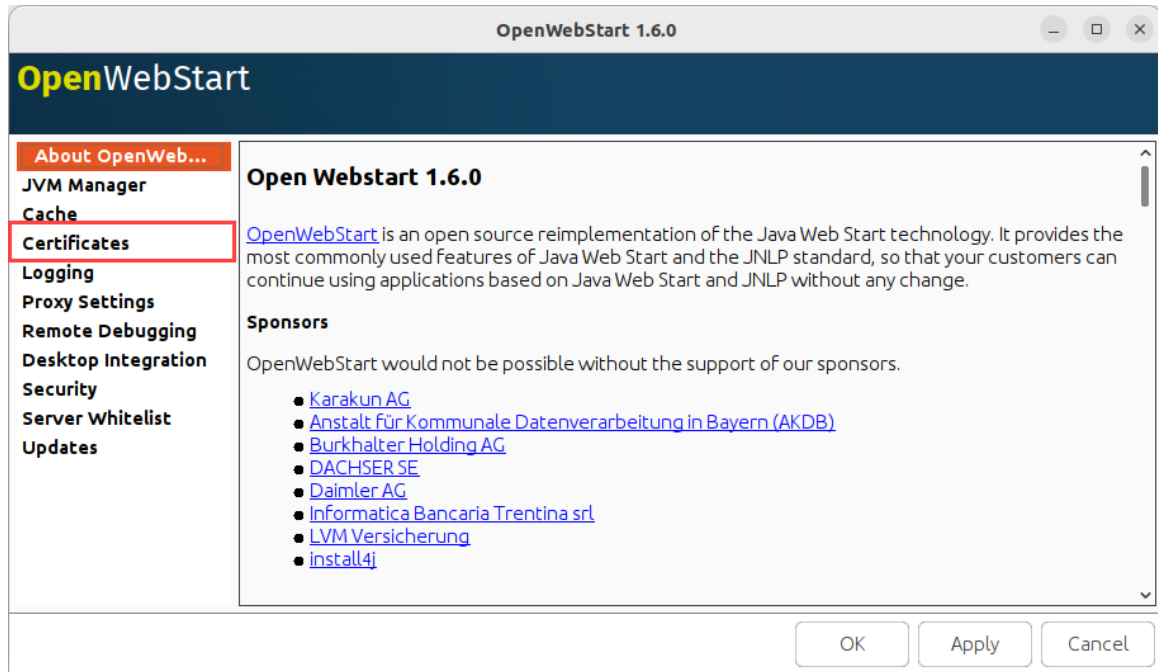


The application will start as usual. When starting the same or another application from the same publisher, this **Security Warning** dialog will not be shown.

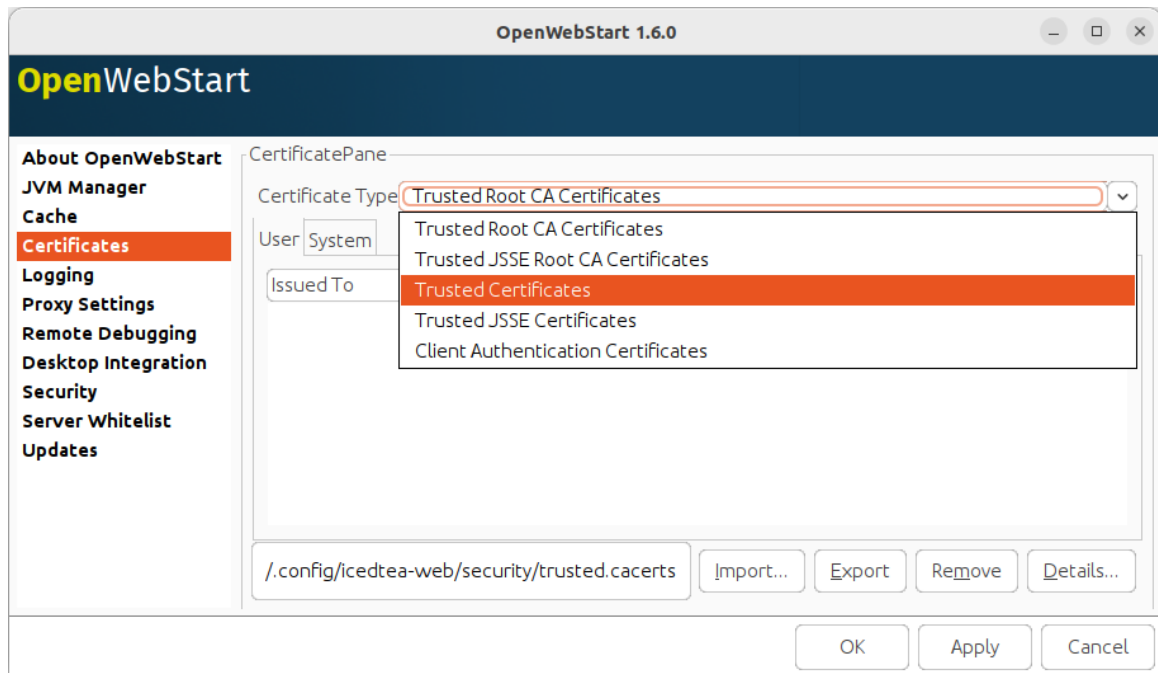
Once the respective OpenWebStart applications have been exchanged by applications with valid certificates, follow the steps in [How to remove expired code signing certificates from OpenWebStart](#).

3. How to remove expired code signing certificates from OpenWebStart

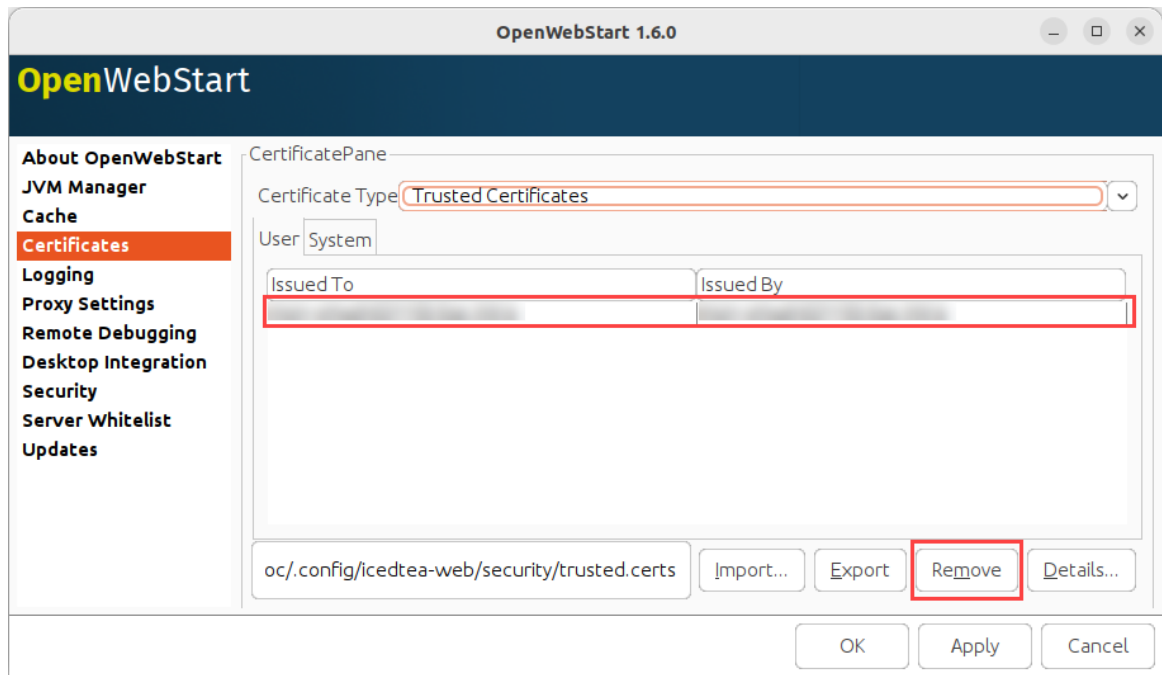
1. Start the application **OpenWebStart Settings** (e.g. search for it in the OS start/launcher menu).
2. Select **Certificates** from the main menu.



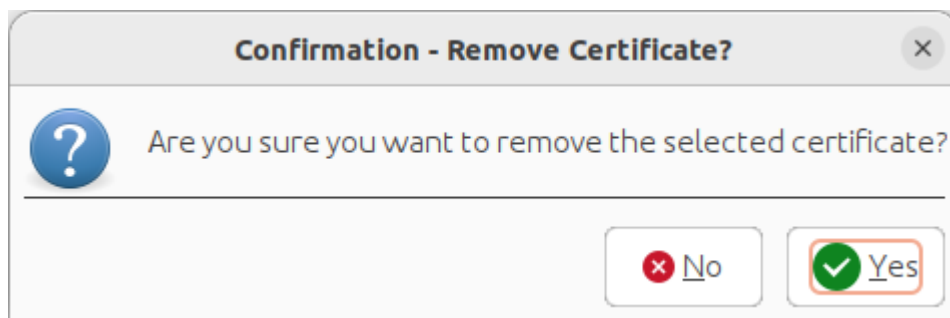
3. From the **Certificate Type** drop down menu select **Trusted Certificate**.



4. Select the certificate you would like to remove, then click **[Remove]**.



5. Click [**Yes**] to confirm.



The trusted certificate has been removed. In case of an expired code signing certificate when starting an OpenWebStart application, the respective warning dialog will be shown again.