

# Selbstsigniertes Zertifikat einrichten (SSL)

When connecting to a Kentix device via a browser, the browser warns that the device's certificate is invalid or untrusted.

This is because the device uses a "self-signed" certificate created by Kentix.

This has no effect on the security and/or encryption of the connection between the browser and the end device. It only warns that the certificate is unknown to the browser.

In order to suppress or bypass the security warning, it is possible to load your own certificate into the device.

You can find an example of how to create such a certificate in the respective device in the "Certificate" tab under "System".

The example shows the creation using "Ubuntu".

On a Windows server system, a certificate previously generated as "PFX" can be converted into a valid PEM format certificate with the following command sequence:

```
openssl.exe pkcs12 -to server.pfx -out server_withkey.pem -nodes
```

Please note that the command sequence for creating the certificate using "Openssl" can vary depending on the operating system.

However, due to the number of different operating systems and system stands, we cannot offer any technical support.