

Removing HTTPS Warnings with Device-Generated Certificates/



Contents

- [1 Summary](#)
- [2 Generating the certificates](#)
- [3 Applying certificates to the device](#)
- [4 Uploading CA on Windows PC](#)
- [5 Uploading certificate to the browser](#)
- [6 Testing](#)
- [7 See also](#)

Summary

One of the key benefits of HTTPS is that it enhances security and trust by protecting users from man-in-the-middle (MitM) attacks, which can be initiated through compromised or insecure networks. Hackers may exploit these vulnerabilities to steal sensitive information. By implementing SSL, data transmitted between the server and the browser during a user's interaction with your device is securely encrypted.

This page contains links with descriptions of all of the WebUI windows. If you're having trouble finding this page or some of the parameters described here on your device's WebUI, you should turn on "**Advanced WebUI**" **mode**. You can do that by clicking the "Advanced" button, located at the top of the WebUI.



To access the device WebUI using HTTPS, a certificate is required; otherwise, the browser will display the following error:



Generating the certificates

Certificates can be generated and signed directly on our device. To do this, navigate to **System** → **Administration** → **Certificates**. In the certificate generation tab, select the following settings:

1. File type - **Simple**
2. IP addresses - **192.168.14.1** (*the IP address of the device that is used for WebUI access*)

3. Click on the **Generate button**.



After the certificates are generated, you can find them by opening the **Certificates Manager** tab. In this tab, you will be able to find and download if necessary all of the available certificates in your device altogether with the ones we recently generated.



Applying certificates to the device

After the certificates are generated, navigate to **System → Administration → Access Control**. In the **WebUI** section make these selections:

1. Certificate files from device - **Enable**
2. Server certificate - **server.cert.pem**
3. Server key - **server.key.pem**

Note: make sure you are using previously generated certificates



Uploading CA on Windows PC

The CA certificate must be imported into either the computer's operating system or the web browser.

First, download the CA certificate from the **Certificates Manager section** on your Teltonika device.



To upload a CA certificate on a WindowsOS based PC follow these steps:
In the device search bar, enter **Manage User Certificates** and open the service.



Navigate to **Trusted Root Certification Authorities → Certificates** in the **Certificates - Current User** tab, then click on **Action** tab and import your certificate by selecting **All tasks → Import**.



Uploading certificate to the browser

Another option is to upload the recently generated certificates directly to your browser instead of your PC. In this example, I used **Google Chrome**.

Start by opening your browser settings by clicking the three vertical dots in the top right corner, then navigate to *Settings*.



In the opened settings window, click on **Privacy and Security** → **Security** → **Manage certificates** and a certificates pop-up window will appear.

Navigate to the **Trusted Root Certification Authorities** and import your generated CA certificate.



Once done, restart your browser.

Testing

Once all the steps are completed and the certificate is imported, the warning should no longer appear when accessing your device via **WebUI** using the HTTPS protocol.



See also

[HTTPS Warning Removal With Encrypted Certificate](#)