https://wiki.teltonika-networks.com/view/Removing_HTTPS_Warnings_with_Device-Generated_Certificates

Removing HTTPS Warnings with Device-Generated Certificates

□

Contents

Summary

One of the main benefits of HTTPS is that it adds security and trust. It protects users against man-in-the-middle (MitM) attacks that can be launched from compromised or insecure networks. Hackers can use such techniques to steal your sensitive information. Implementing SSL secures any data transmitted between server and browser during a user's session interacting with your device.

This page contains links with description all of WebUI windows. If you're having trouble seeing all the pages listed here on your WebUI, you may need to **turn on "Advanced WebUI" mode**. You can do that by clicking the "Basic" button under "Mode", which is located at the top-right corner 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 *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" 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 the PC. For 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 the 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
Noip.com DDNS configuration