Removing of HTTPS security warning

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 article will help you get a good idea about how to implement security into your network while using **Teltonika** devices.

This page contains links with description all 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.

For accessing the device WebaUI using HTTPS it requires a certificate, else it will show the below error:

In this example, we will be able to access the device webpage using HTTPS, with a free certificate from a free CA.

Certificate creation and trust

1. You must have a DNS record linked to the IP of the router; in my case, I’m using a Windows server to act as a DNS server.

```
As shown, I choose the hostname rut955.teltonika.uae and it's linked with
```

172.16.16.1 the LAN IP of the router.
This hostname will be used for creating the certificate later.

2. Go to: **GetAcert** website.

3. Fill in the information regarding your requirements:

NOTE: 1,2 and 3 are the names you will use in the browser.
Other information isn't mandatory. Click **Next Page**.

4. Check the data once again, if everything is okay click **Submit self-signed Certificate**:

5. The final page:

6. Click on (+) beside **Open Private Key**:

Copy the text to a new Notepad file, and rename it to **name.crt** in my case I used a simple name **cer.crt**

7. Click on (+) beside Open Public Key:

Copy the text to a new Notepad file, and rename it to **name.key** in my case I used a simple name **key.key**

8. Click on the [.p12] file, and it will be downloaded:

9. Go to the Microsoft search bar and type: **cer** then choose Manage user certificates:

10. Go to Trusted Root Certification Authorities:

11. Right-click and highlight **All Tasks**, click **Import...**

12. Choose the ".p12" file downloaded before:

Then **Next**, **Next**, then **Finish**.

Device configuration

`Go to` **`System → Access Control → WEBUI`**

1) Turn off **Certificate files from device**.

2) Click browse in **Server certificate** and choose the [.crt] file created.

3) Click browse in **Server key** and choose the [.key] file created.

4) Click **SAVE & APPLY**.

5) Open the WebUI again using the DNS record:

Now we can access the WebUI securely, and we can turn off the HTTP access.

See Also

- Remote WebUI Access
- Unblocking WebUI Access