

HTTPS Warning Removal With Encrypted Certificate



Contents

- [1 Introduction](#)
- [2 Certificate generation](#)
- [3 Applying Certificate](#)
 - [3.1 Testing](#)

Introduction

Using encrypted certificates is important for keeping online communication safe. They help protect data from being stolen or accessed by unauthorized people. Certificates also verify the identity of websites, so users know they're connecting to a legitimate site. In a time when online security is a big concern, these certificates play a key role in keeping personal information secure.

Certificate generation


In order to generate an encrypted certificates with a Teltonika device, you will need to create a *DDNS instance*. In this example, we are assuming that the DDNS is already set up. If you need information on how to create a DDNS instance on your device please refer to this article: [Noip.com DDNS configuration](#)

To generate an encrypted protocol, navigate to *System → Administration → Certificates* and select these settings:

1. File type - *Let's encrypt*
2. Domain - *Enter your created Dynamic DNS domain name*
3. Automatically renew - *On*



Applying Certificate

Navigate to *System → Administration → Access Control*. Make sure you click on **Certificates files from device** then select your recently generated encrypted **server certificate** and **server key** on the **WebUI** tab and click on save and apply. 

Testing

If all of the mentioned steps were made correctly, you should no longer be able to see the warning

sign while accessing the device WebUI via HTTPS protocol. 