# SSL Authentication

# 1 Introduction

## 1.1 About the Functionality

SSL (Secure Sockets Layer) is a security technology used for establishing encrypted connections between server and client, as well as authenticating the identity of the server/client. All data transmitted between server and client is encrypted. An **SSL certificate** is required to create an SSL connection. An SSL certificate is a file installed on the server side. An additional certificate can be installed on the client side for extra security. Ruptela devices use the **TLS v1.2** version of SSL.

## 1.2 Legal Information



## 1.3 Compatibility

This functionality is compatible with the following devices with the newest firmware version:

- Trace5
- FM-Tco4 HCV
- FM-Tco4 LCV
- FM-Pro4
- FM-Eco4 T

## 1.4 Contact Information


**General enquiries**

Website: ruptela.com

E-mail: info@ruptela.com

Phone: +370 5 2045188

**Technical support**

E-mail: support@ruptela.com

Phone: +370 5 2045030


## 1.5 Document Changelog

| Version | Date | Modification |
|---|---|---|
| **1.0** | 2017-12-22 | Initial draft. Description transferred from FM device user manuals. |
| **1.1** | 2018-10-24 | Added: Description of OCSP server certificate validation.<br>Added: Description of the *ssl status* SMS command. |
| **1.2** | 2019-07-12 | Functionality available for 3G devices. |
| **2.0** | 2019-09-11 | Added: Note regarding required modem version for OCSP validation.<br>Updated: Document structure and design. |
| **2.1** | 2020-04-07 | Updated: List of compatible devices. |

## 1.6 Notations

The following notations are used in this document to highlight important information:

**Bold text**

Used to indicate user interface elements or for emphasis.

*Italic text*

Used to indicate items that belong to a list and can be selected.

**Note**

Used to highlight important information or special conditions.

**Caution**

Used to mark actions that require caution when handling the product.

## 1.7 References

SMS commands list and user manuals: https://doc.ruptela.lt/display/AB/Tracking+devices

# 2 Configuration

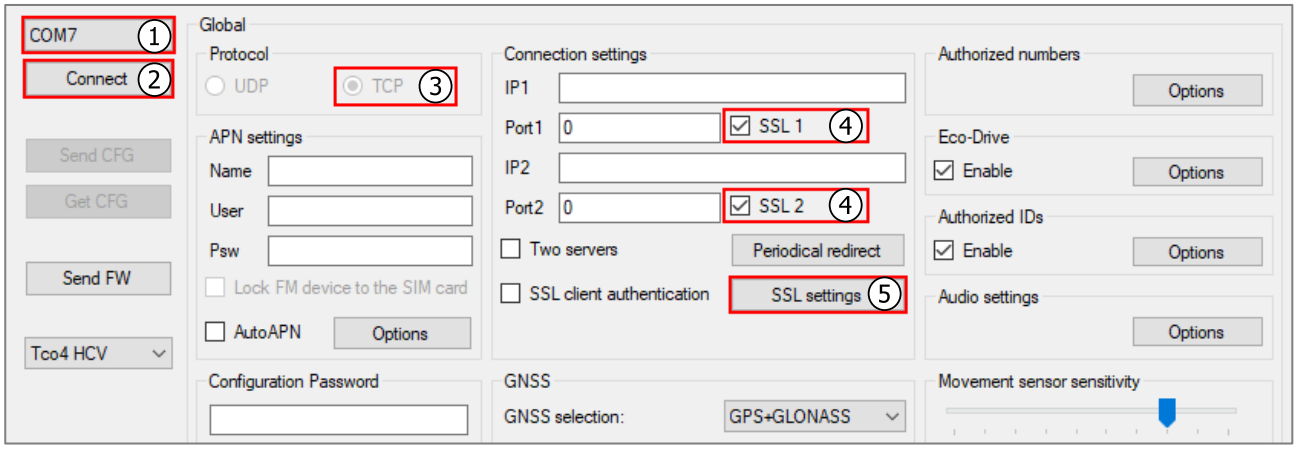
This functionality requires the use of the advanced configurator.

## 2.1 Starting the Configuration

Using SSL authentication may increase data consumption and may incur additional costs, according to your data plan.

To start the configuration, follow these steps:

1. Open the advanced configurator. Select the COM port to which your device is connected.
2. Click **Connect**.
3. Turn on the **TCP** protocol in **Protocol** settings.
4. Tick the **SSL 1**/**SSL 2** checkbox to enable SSL on the primary/secondary server. A pop-up warning window will appear, informing you that if SSL is enabled without uploading the certificates, the device will remain unprotected. The certificates uploaded to the servers are Root CA (certification authority) certificates, meaning that they are issued by a trusted certification authority.
5. Click **SSL settings** in the **Connection settings** section to open the **SSL Settings** window.




If SSL is enabled and the *econnect* or *connect* SMS commands are used, the device will **disable** SSL for that connection and use a regular insecure connection. In order to ensure that no unauthorized device sends SMS commands, it is highly recommended to use the authorized numbers functionality, described in the user manuals.

## 2.2 OCSP Server Certificate Validation

There may be cases when certificates in use are revoked by the CA and are no longer considered valid. Using revoked certificates makes the connection between client and server insecure. Because of this, OCSP (Online Certificate Status Protocol) server certificate validation can be used to determine, whether the certificates in use are valid.

OCSP functions as follows: the client requests the server certificate at the start of communication and forwards it to a CA server listed in the certificate. The CA then checks the status of the certificate and sends a response to the client. If the certificate is revoked, the client closes the connection with the server.

OCSP requires a dynamic identification string with an *OCSP status* parameter.

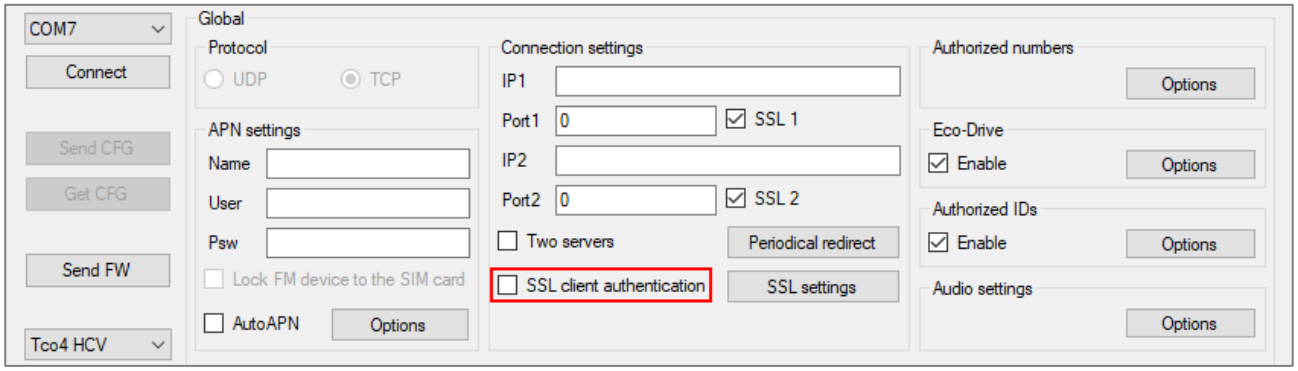
OCSP validation is performed after device boot and periodically once every 4 hours.

OCSP validation will not be performed if **Two servers** mode is enabled.

Trace5 devices and devices with the modem version M95EBXXXXXX do not support OCSP validation. Check your modem version using the *modrev* SMS command.

## 2.3 SSL Client Authentication

Ticking the **SSL client authentication** checkbox will enable SSL authentication on the client side. This checkbox is disabled by default and can only be ticked when SSL is enabled on at least one of the servers. For the functionality to work, you must upload a client certificate and private key in **SSL settings**.

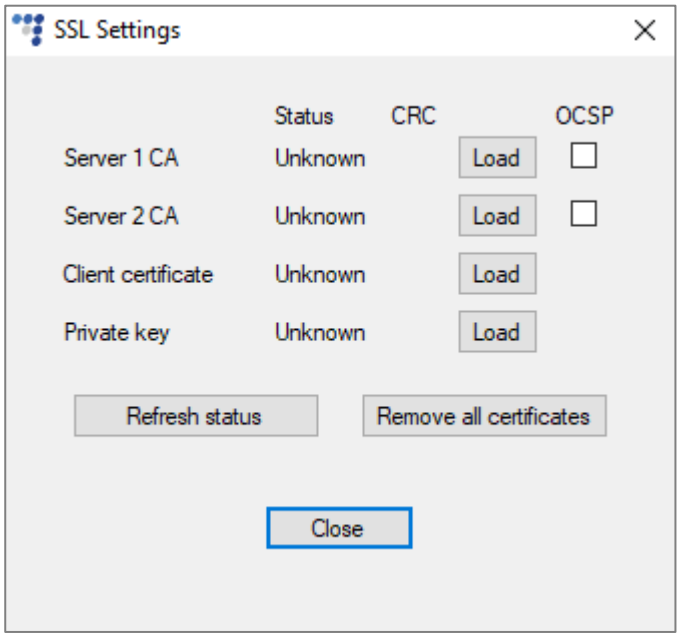


## 2.4 SSL Settings

Here you can upload certifications for both server and client to the device, as well as the client's private key (necessary for client authentication). The files are uploaded one by one by clicking the **Load** button and selecting the appropriate file in the file browser. Each file also has **Status** (Uploaded, Empty or Unknown) and **CRC** columns for additional information.

The files cannot be larger than 2025 bytes!

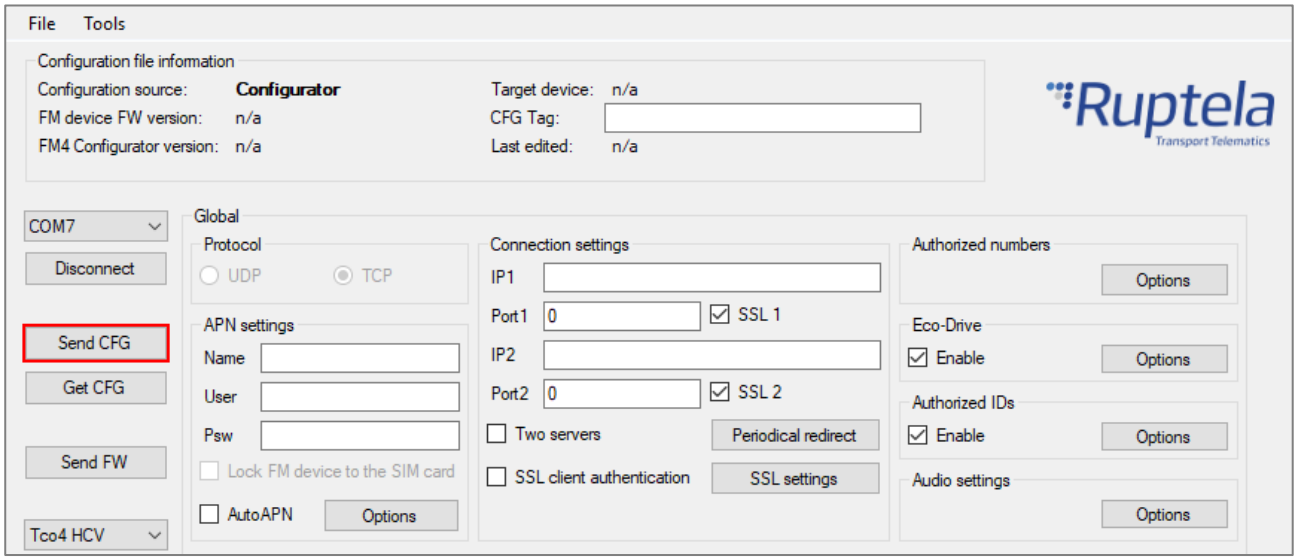
| | |
|---|---|
| **Server 1 CA/Server 2 CA** | Primary/secondary server certification files. |
| **Client certificate** | Client certification file, required if SSL client authentication is enabled. |
| **Private key** | Client private key file, required if SSL client authentication is enabled. |
| **OCSP** | If ticked, OSCP will be enabled on the primary/secondary server. A pop-up window will appear if a dynamic identification string with an *OCSP status* parameter is not enabled. Click **Yes** to enable it.<br>**Note:** Unavailable for Trace5 devices.<br>Default value: Disabled |
| **Refresh status** | Updates the status of all files. |
| **Remove all certificates** | Deletes all certificate and key files stored in the device. The file status is updated automatically. |




If SSL is configured incorrectly (e.g. the wrong certificates were uploaded), the device will not send any data to the server. The only way to restore data transmission is to reconfigure the device, thus SSL must be configured with caution.

## 2.5 Finishing the Configuration

To finish the configuration, close the **SSL settings** window. Click **Send CFG** to send the configuration to the device.



# 3 SSL Authentication Status via SMS

Use the *ssl status* SMS command to obtain the current SSL authentication status.

Command syntax: *password ssl status*

Response structure: *SSL status server1 <status>, server2 <status>*

*<status>* can have the following values:

- 0 – SSL authentication is disabled on this server
- 1 – SSL authentication is enabled on this server

If OCSP validation is enabled, *<status>* can have additional values:

- 2 – the certificate is valid
- 3 – OCSP lookup failed
- 4 – the certificate is revoked
- 5 – OCSP server URL not found
- 6 – unknown certificate
- 7 – validation request timeout
- 8 – modem firmware does not support OCSP validation