SSL authentication

Introduction

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. FM devices use the **TLS v1.2** version of SSL.

SSL authentication is compatible with the following FM devices with the latest firmware version:

- FM-Tco4 HCV
- FM-Tco4 LCV
- FM-Pro4

You can get the latest firmware and configurator from our documentation website: doc.ruptela.lt

Legal notice

Document change log

Date	Version	Change details
2017-12-22	1.0	Initial draft. Description transferred from FM device user manuals.
2018-10-24	1.1	Added description of OCSP server certificate validation. Added description of the *ssl status* SMS command.

Enabling SSL authentication

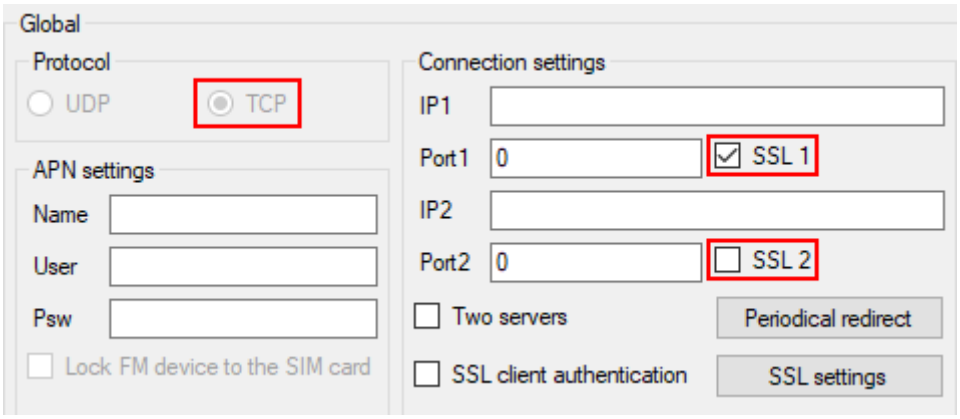
Note

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

Note

SSL will **not** work on devices with 3G modems.

SSL can be enabled on each server separately by ticking the **SSL 1**/**SSL 2** checkboxes in **Connection settings**. To do so, the **TCP** protocol must be enabled. The **SSL 1**/**SSL 2** checkboxes are disabled by default. After ticking any of the checkboxes, a pop-up warning window will always appear, informing the user that if SSL is enabled without uploading the certificates, the device will remain unprotected. The certificates uploaded for the servers are **Root CA** (certification authority) certificates, meaning that they are issued by a trusted certification authority.



Note

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.

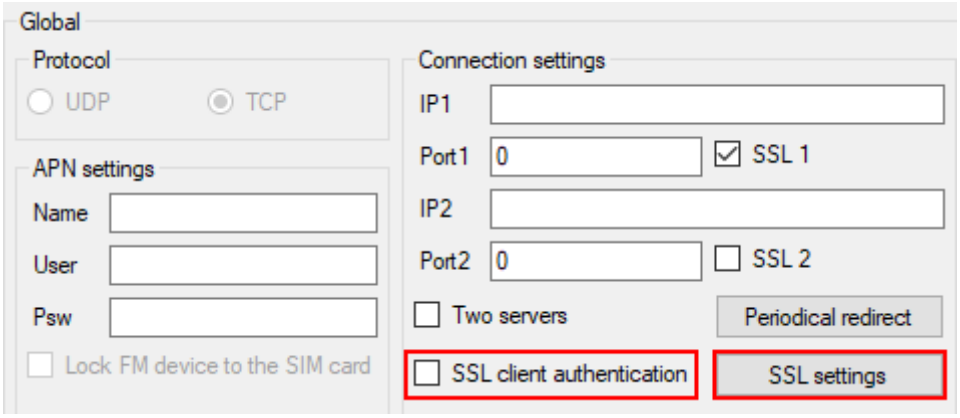
OCSP server certificate validation

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.

Configuration

After SSL is enabled, you can further configure SSL authentication by enabling **SSL client authentication** and configuring **SSL settings**. Both options are described below.

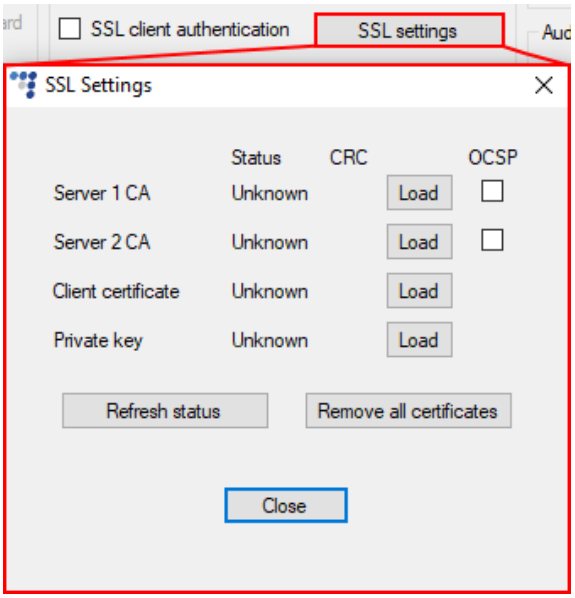


SSL client authentication

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**.

SSL settings

Clicking **SSL settings** will open a new **SSL Settings** window. Here you can upload certifications for both server and client to the FM 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. **The files cannot be larger than 2025 bytes!** Each file also has *Status* and *CRC* columns for additional information.



Ticking the **OCSP** checkbox will enable OCSP validation for that server. In order for OCSP validation to function correctly, a dynamic identification string must be enabled along with an *OCSP status* parameter. If the conditions are not met, a pop-up warning will appear after ticking the **OCSP** checkbox. Clicking **Yes** will automatically enable the needed parameters. OCSP validation is performed after device boot and periodically once every 4 hours.

Note

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

Refresh status – clicking this button will update the status of all files. The status can be one of the following: *Uploaded*, *Empty* or *Unknown;*

Remove all certificates – clicking this button will delete all certificate and key files stored in the FM device. The status information will be updated automatically.

Note

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.

SSL authentication status via SMS

SSL authentication status can be obtained using the *ssl status* SMS command, using the following structure:

password ssl status

After sending the SMS command, the FM device will send a response using the following 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.