Autenticación SSL

1 Introducción

1.1 Sobre la funcionalidad

SSL (Secure Sockets Layer – capa de puertos seguros) es una tecnología de seguridad usada para establecer conexiones cifradas entre servidor y cliente, también para autenticar la identidad del servidor/cliente. Todos los datos transmitidos entre el servidor y cliente están cifrados. Un **certificado de SSL** es obligatorio para establecer una conexión de SSL. Un certificado de SSL es un archivo, instalado en el servidor. También se puede instalar un certificado en el dispositivo del cliente para tener seguridad adicional. Los dispositivos de Ruptela usan la versión **TLS v1.2** de SSL.

1.2 Información legal

1.3 Compatibilidad

Esta funcionalidad está disponible para los siguientes dispositivos con la última versión de firmware:

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

1.4 Información de contacto

Consultas generales

Sitio web: ruptela.com

Correo electrónico: info@ruptela.com

Teléfono: +370 5 2045188

Soporte técnico

Correo electrónicol: support@ruptela.com

Teléfono: +370 5 2045030

1.5 Historial de cambios

Versión	Fecha	Modificación
1.0	2017-12-22	Borrador inicial. La descripción fue transferida desde los manuales de usuario de los dispositivos FM.
1.1	2018-10-24	Añadido: Descripción de validación OCSP de certificado de servidor. Añadido: Descripción del comando SMS *ssl status*.
1.2	2019-07-12	Funcionalidad disponible para los dispositivos con módems 3G.
2.0	2019-09-11	Añadido: Nota sobre la versión del módem requerida para la validación OCSP. Actualizado: Estructura y diseño del documento.

1.6 Notaciones

Las siguientes notaciones se usan en este documento para resaltar información importante:

Texto en negrita

Usado para indicar elementos de la interfaz de usuario o para énfasis.

Texto en cursiva

Usado para indicar elementos que pertenecen a una lista y se los pueden seleccionar.

Nota

Usado para resaltar información importante o condiciones especiales.

Precaución

Usado para marcar acciones que requieren precaución mientras usando el producto.

1.7 Referencias

Lista de comandos SMS y manuales de usuario: https://doc.ruptela.lt/display/AB/FM4

2 Configuración

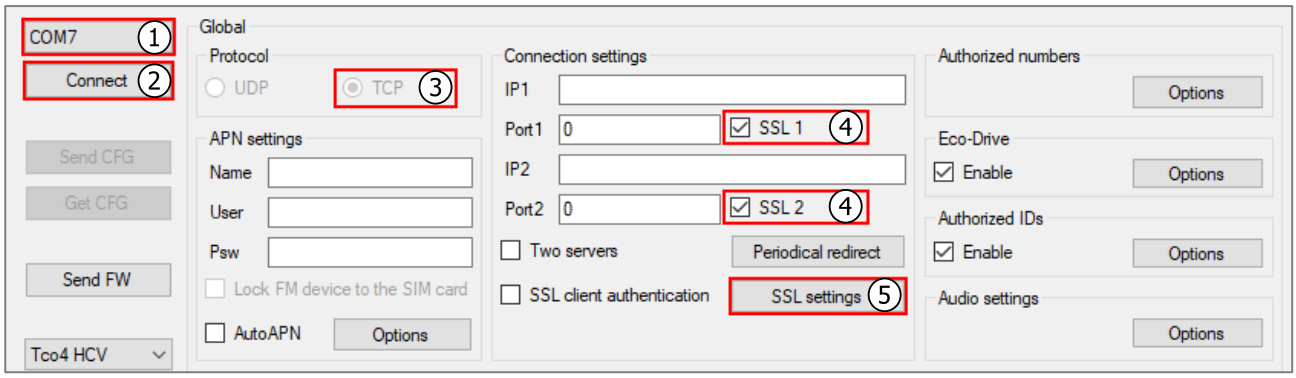
Esta funcionalidad requiere el uso del configurador avanzado.

2.1 Empezar la configuración

El uso de SSL puede aumentar el consumo de datos e incurrir gastos adicionales, según su plan de datos.

Para empezar la configuración, siga estos pasos:

1. Abra el configurador avanzado. Seleccione el puerto COM al cual ha conectado su dispositivo.
2. Haga clic en **Connect** (Conectar).
3. Encienda el protocolo **TCP** en los ajustes **Protocol** (Protocolo).
4. Marque la casilla **SSL 1**/**SSL 2** para habilitar SSL en el servidor principal/secundario. Se aparecerá una ventana emergente de advertencia, informándole que, si SSL está habilitado sin subir los certificados, el dispositivo no será protegido. Los certificados subidos al servidor son certificados **Root CA** (autoridad de certificación), esto significa que los certificados son emitidos por una autoridad de certificación de confianza.
5. Haga clic en **SSL settings** (Ajustes SSL) en **Connection settings** (Ajustes de conexión) para abrir la ventana **SSL Settings**.



Si SSL está habilitado y se usan los comandos SMS *econnect* y *connect*, el dispositivo **deshabilitará** SSL para esa conexión y usará una conexión regular insegura. Para asegurarse de que ningún dispositivo sin autorización envíe comandos SMS, es muy recomendable usar la funcionalidad de números autorizados, descrita en los manuales de usuario.

2.2 Validación OCSP de certificado de servidor

En algunos casos los certificados en uso hayan sido revocados por la CA y dejan de ser válidos. Si se usan certificados revocados, la conexión entre el cliente y servidor estará insegura. Debido a esto, se puede usar validación OCSP (Protocolo de comprobación del Estado de un Certificado En línea) de certificado de servidor para determinar, si los certificados en uso son válidos.

OCSP funciona como sigue: el cliente pide por el certificado del servidor al principio de la comunicación y lo transmite a un servidor de la CA, listado en el certificado. La CA entonces comprueba el estado del certificado y envía una respuesta al cliente. Si el certificado ha sido revocado, el cliente cierra la conexión con el servidor.

OCSP requiere una cadena de identificación dinámica junto con el parámetro *OCSP status* (estado OCSP).

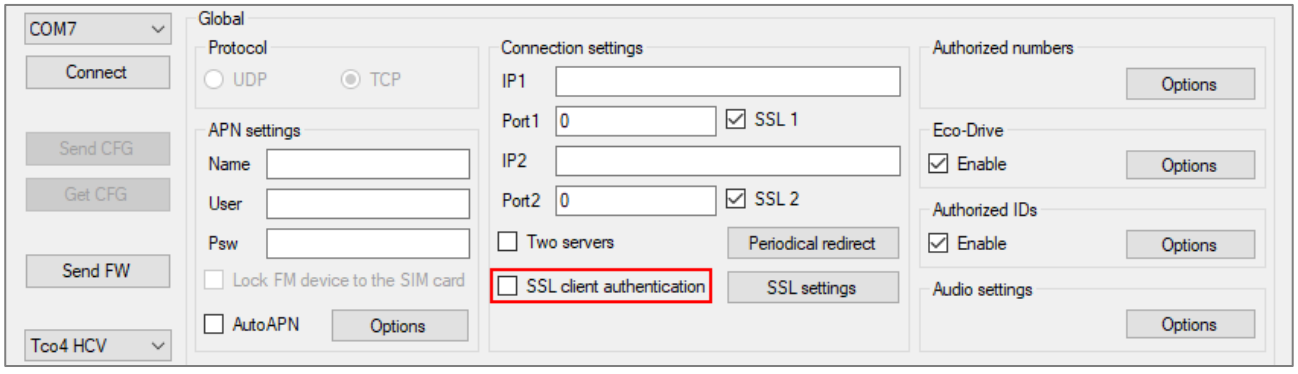
La validación OCSP se realiza tras iniciar el dispositivo y periódicamente una vez cada 4 horas.

La validación OCSP no se realizará si el modo **Two servers** (Dos servidores) está activo.

Los dispositivos con la versión del módem M95EBXXXXXX no admiten la validación OCSP. Compruebe la versión de su modem usando el comando SMS *modrev*.

2.3 Autenticación SSL del cliente

Marcando la casilla **SSL client authentication** (Autenticación SSL del cliente) activará la autenticación SSL al lado del cliente. La casilla está inactiva por defecto y sólo puede marcarse si SSL está habilitado en al menos uno de los servidores. Tiene que subir el certificado del cliente y la clave privada en **SSL settings** (Ajustes SSL) para que la funcionalidad funcione.

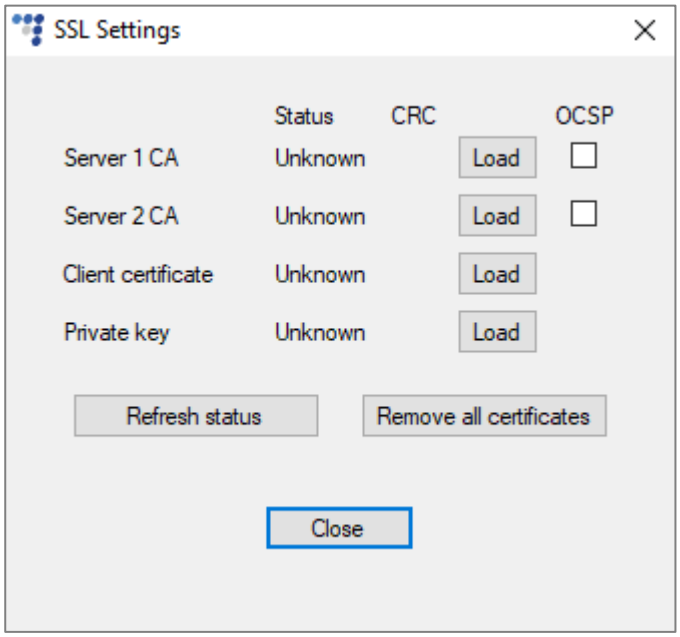


2.4 Ajustes SSL

Aquí puede subir los certificados para ambos servidor y cliente, también la clave privada del cliente (obligatoria para la autenticación SSL del cliente). Los archivos se suben uno por uno haciendo clic en el botón **Load** (Subir) y seleccionando el archivo respectivo en el navegador de archivos. Cada archivo también tiene columnas **Status** (Estado, puede ser Uploaded (Cargado), Empty (Vacío) o Unknown (Desconocido)) y **CRC** para información adicional.

¡El tamaño de los archivos no puede superar 2025 bytes!

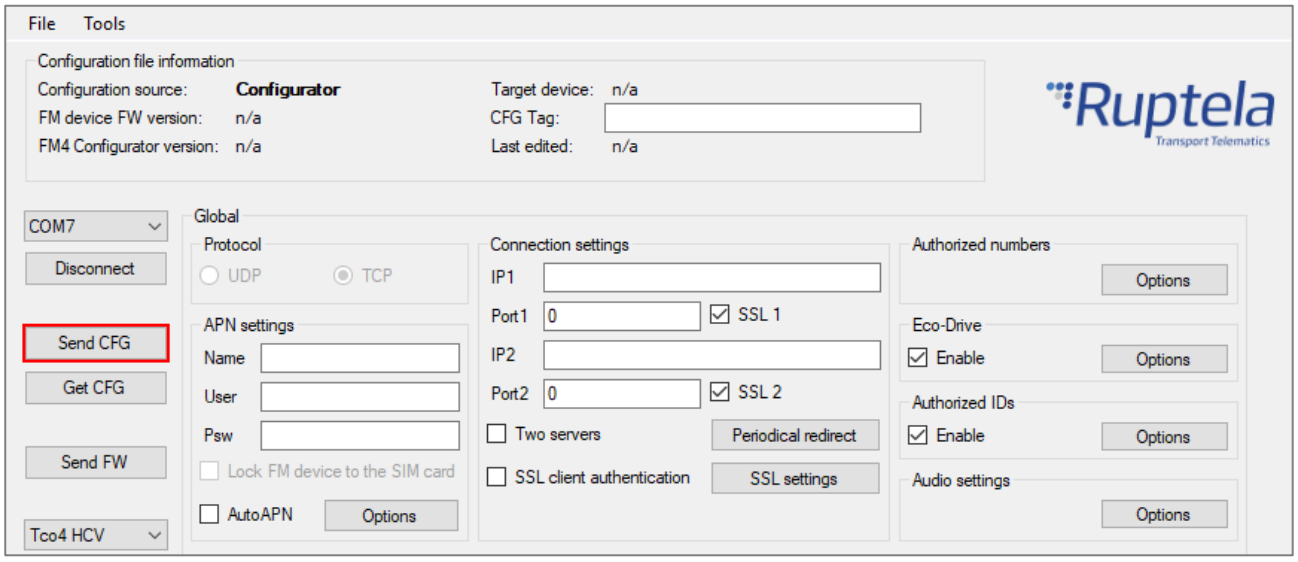
Server 1 CA/Server 2 CA CA del servidor 1/2	Los archivos del servidor principal/secundario.
Client certificate Certificado del cliente	El archivo del certificado del cliente, requerido si la autenticación SSL del cliente está habilitada.
Private key Llave privada	El archivo de la llave privada del cliente, requerido si la autenticación SSL del cliente está habilitada.
OCSP	Si está marcada, OCSP se habilitará en el servidor principal/secundario. Se aparecerá una ventana emergente si la cadena de identificación dinámica junto con el parámetro *OCSP status* no está habilitada. Haga clic en **Yes** (Sí) para habilitarla. Valor por defecto: Deshabilitada
Refresh status Actualizar los estados	Actualiza los estados de todos los archivos.
Remove all certificates Borrar todos los certificados	Borra todos los archivos de certificados y llaves almacenados en el dispositivo. Los estados de los archivos se actualizan automáticamente.



Si SSL fue configurado incorrectamente (por ejemplo, se ha subido certificados incorrectos), el dispositivo no enviará ningunos datos al servidor. La única manera de reiniciar el envío de datos es la reconfiguración del dispositivo, así que configure SSL con cuidado.

2.5 Terminando la configuración

Para terminar la configuración, cierre la ventana **SSL settings**. Haga clic en **Send CFG** (Enviar configuración) para enviar la configuración al dispositivo.



3 Estado de la autenticación SSL vía SMS

Use el comando SMS *ssl status* para obtener el estado actual de la autenticación SSL.

Estructura del comando: *contraseña ssl status*

Estructura de la respuesta: *SSL status server1 <estado>, server2 <estado>*

<estado> puede tener los siguientes valores:

- 0 – la autenticación SSL no está activa en este servidor
- 1 – la autenticación SSL está activa en este servidor

Si la validación OCSP está activa, *<estado>* puede tener valores adicionales:

- 2 – el certificado es válido
- 3 – la búsqueda OCSP no tuvo éxito
- 4 – el certificado ha sido revocado
- 5 – la dirección del servidor de OCSP no era encontrada
- 6 – el certificado es desconocido
- 7 – timeout de solicitud de validación
- 8 – el firmware del modem no admite la validación OCSP