Autenticación SSL

Introdución

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 FM usan la versión **TLS v1.2** de SSL.

La autenticación SSL está disponible para los siguientes dispositivos con la última versión de firmware:

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

Puede obtener el ultimo firmware y herramienta de configuración en nuestra web de documentación: doc.ruptela.lt

Información legal

Historial de cambios

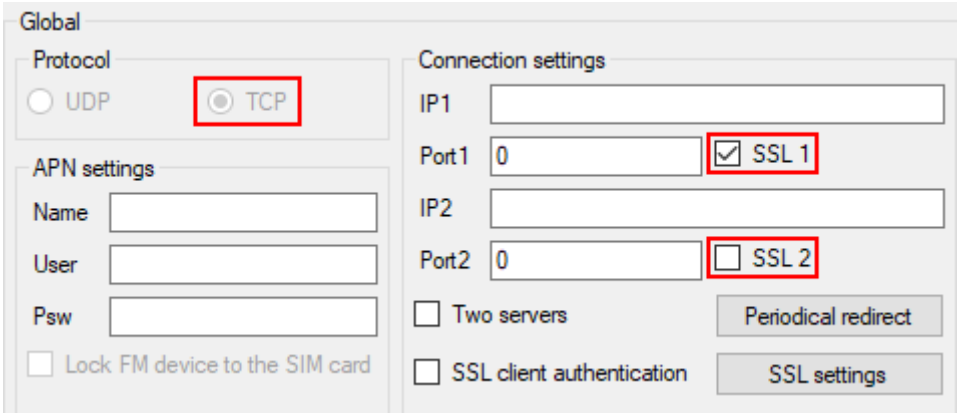
Fecha	Versión	Modificación
2017-12-22	1.0	Borrador inicial. La descripción fue transferida desde los manuales de usuario de los dispositivos FM.
2018-11-09	1.1	Descripción de validación OCSP de certificado de servidor añadida. Descripción del comando SMS *ssl status* añadida.

Activación de la autenticación SSL

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

Nota
SSL **no funcionará** en dispositivos con módems 3G.

SSL puede habilitarse en cada servidor de manera separada marcando las casillas **SSL 1/SSL 2**. El protocolo **TCP** debe estar seleccionado, para que las casillas estén activas. Las casillas **SSL 1/SSL 2** están desmarcadas por defecto. Después de marcar cualquier casilla, se aparecerá siempre una ventana emergente de advertencia, informando al usuario 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.



Nota
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 (Authorized numbers), descrita anteriormente en este documento.

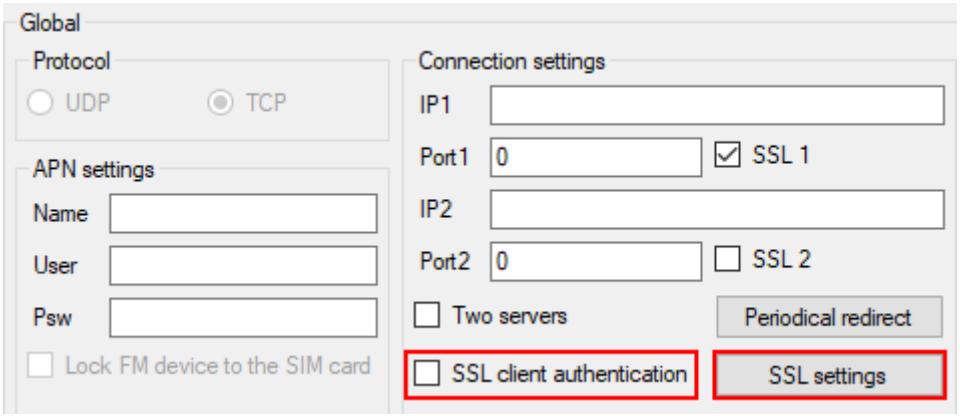
Validación OCSP de certificado de servidor

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.

Configuración

Después de habilitar la autenticación SSL, puede seguir configurándola, habilitando autenticación SSL del cliente (**SSL client authentication**) y configurando ajustes SSL (**SSL settings**). Ambas opciones se describen a continuación.

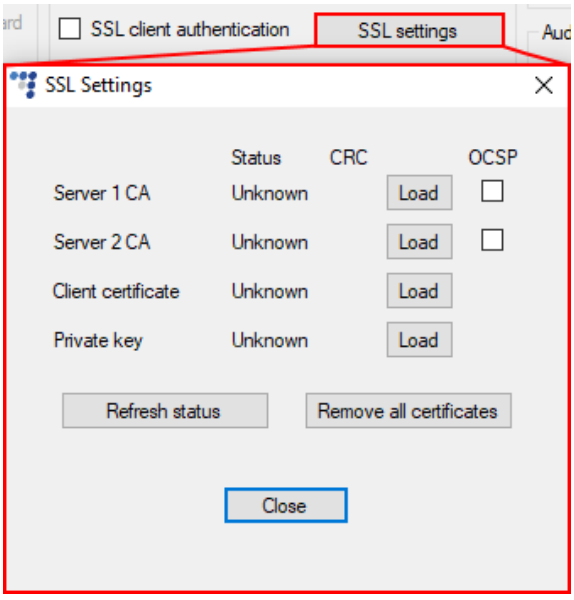


Autenticación SSL del cliente

Marcando la casilla **SSL client authentication** activará la autenticación SSL al lado del cliente. La casilla está inactiva por defecto y solo 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** para que la funcionalidad funcione.

Ajustes SSL

Haciendo clic en **SSL settings** abrirá una ventana nueva **SSL Settings**. Aquí puede subir los certificados para ambos servidor y cliente, también la clave privada del cliente (obligatoria para 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. **¡El tamaño de archivos no puede superar 2025 bytes!** Cada archivo también tiene columnas *Status* (Estado) y *CRC* para información adicional.



Marcando la casilla **OCSP** activará validación OCSP para ese servidor. Hay que habilitar una cadena de identificación dinámica junto con el parámetro *OCSP status* (estado OCSP) para que la validación OCSP funcione de una manera correcta. Si las condiciones no se cumplen, se aparecerá una ventana emergente de advertencia después de marcar la casilla **OCSP**. Haciendo clic en **Yes** automáticamente habilitará los parámetros necesarios. La validación OCSP se realiza tras iniciar el dispositivo y periódicamente una vez cada 4 horas.

Nota

La validación OCSP no se realizará si el modo **Two servers** está activo.

Refresh status – haciendo clic en este botón actualizará los estados de todos los archivos. Los estados posibles: *Uploaded* (Cargado), *Empty* (Vacío) o *Unknown* (Desconocido);

Remove all certificates – haciendo clic en este botón borrará todos los archivos de certificados y claves almacenados en el dispositivo FM. La información de estado se actualizará automáticamente.

Nota

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 reconfiguración del dispositivo, así que configure SSL con cuidado.

Estado de la autenticación SSL vía SMS

El estado de la autenticación SSL puede ser obtenido usando el comando SMS *ssl status* con la siguiente estructura:

contraseña ssl status

Después de enviar el comando SMS, el dispositivo FM enviará una respuesta con la siguiente estructura:

SSL status server1 <estado>, server2 <estado>

<estado> puede tener los siguientes valores:

- *0* – la autenticación SSL está desactiva 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.