How-To

Temat: CyberSecurity

Program version: 7.x

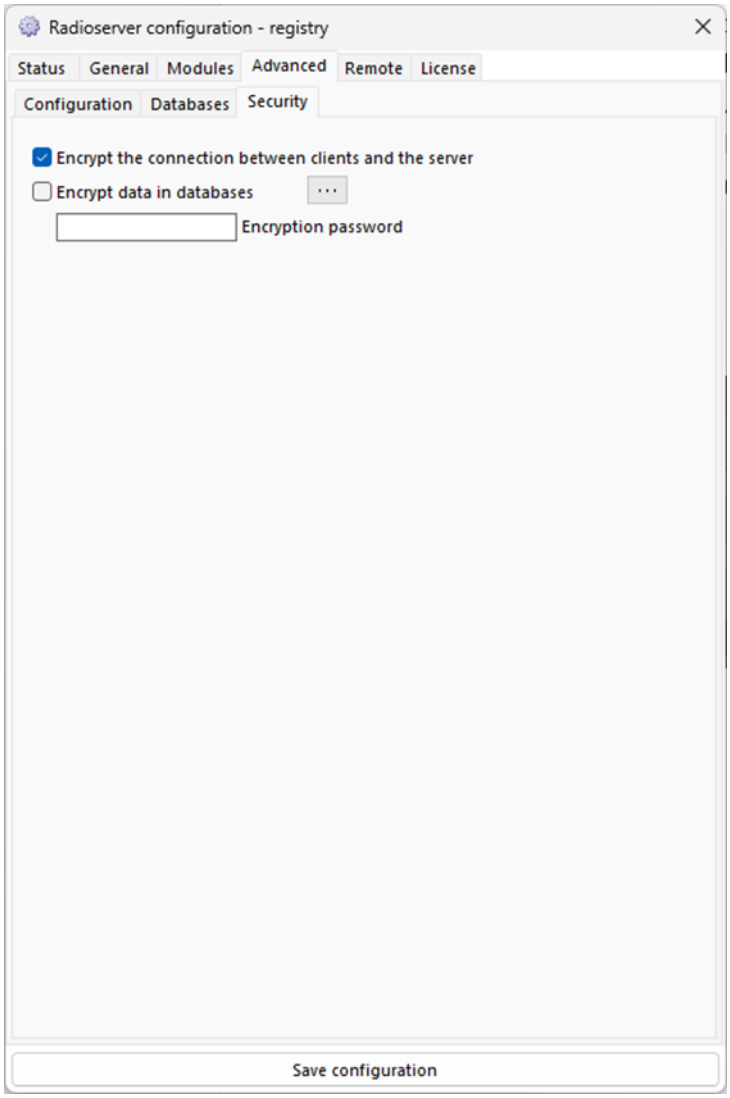
Document version: 1.0

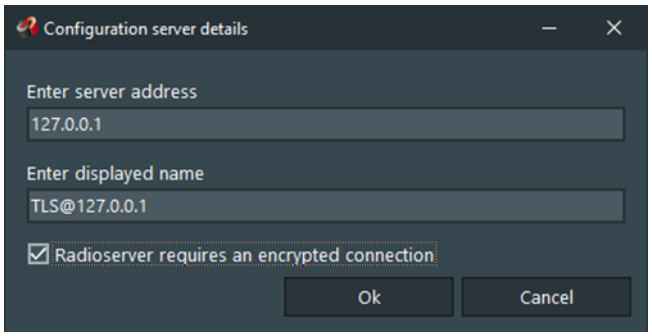
Author: Wiktor Śmieja

Contents

1 Encryption of connections to and from the radio server

To force encryption of connections between the console and the radio server, select the option „ Encrypt the connection between clients and the server” in the configuration of the radio server in the advanced tab -> security, and in the client, in the configuration server data window, in the administration tab -> configuration servers -> edit server.





2 Databases encryption

Database encryption can be configured in the security tab in the advanced settings of the radio server.

2.1 Starting data encryption in databases

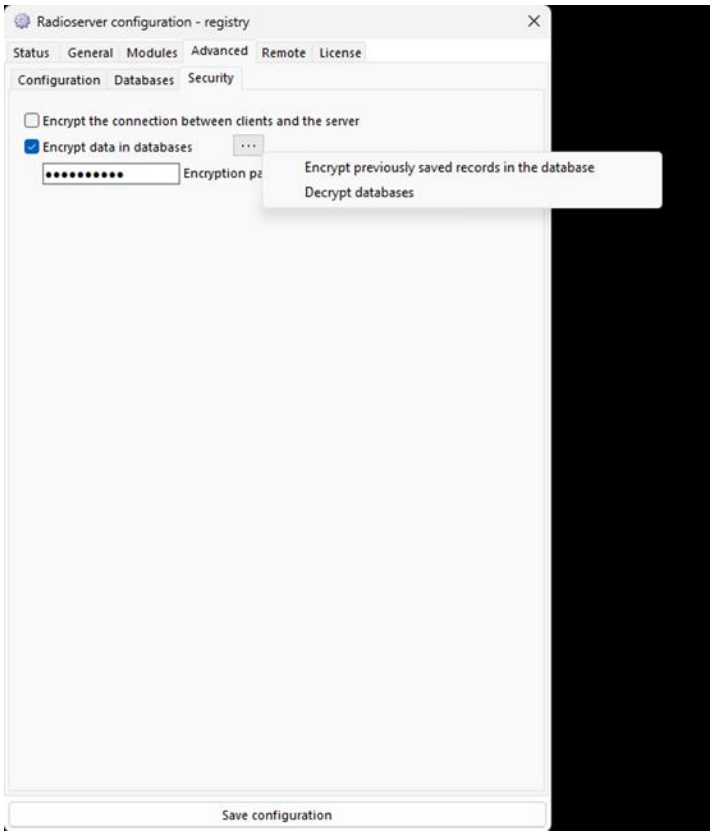
To start encrypting data in databases, select the option "Encrypt data in databases" and then enter the password in the field below and save.

2.2 Encryption of previously saved records in the database

Before encrypting existing records in databases, you must set and save an encryption password.

Then click on the button with three dots to the left of the inscription "Encrypt data in databases" and select the option "encrypt previously saved records in the database".

After reading the warning about the duration of database encryption, you will be asked to confirm the encryption passwordBefore encrypting existing records in databases, you must set and save an encryption password.



Then click on the button with three dots to the left of the inscription "Encrypt data in databases" and select the option "encrypt previously saved records in the database".

After reading the warning about the duration of database encryption, you will be asked to confirm the encryption password.

2.3 Decryption of databases

To decrypt the databases, proceed as in point 2.2, but instead of selecting the "Encrypt previously saved records in the database" option, select "Decrypt databases".

After reading the warning about the duration of decryption, we are asked to confirm the encryption password.

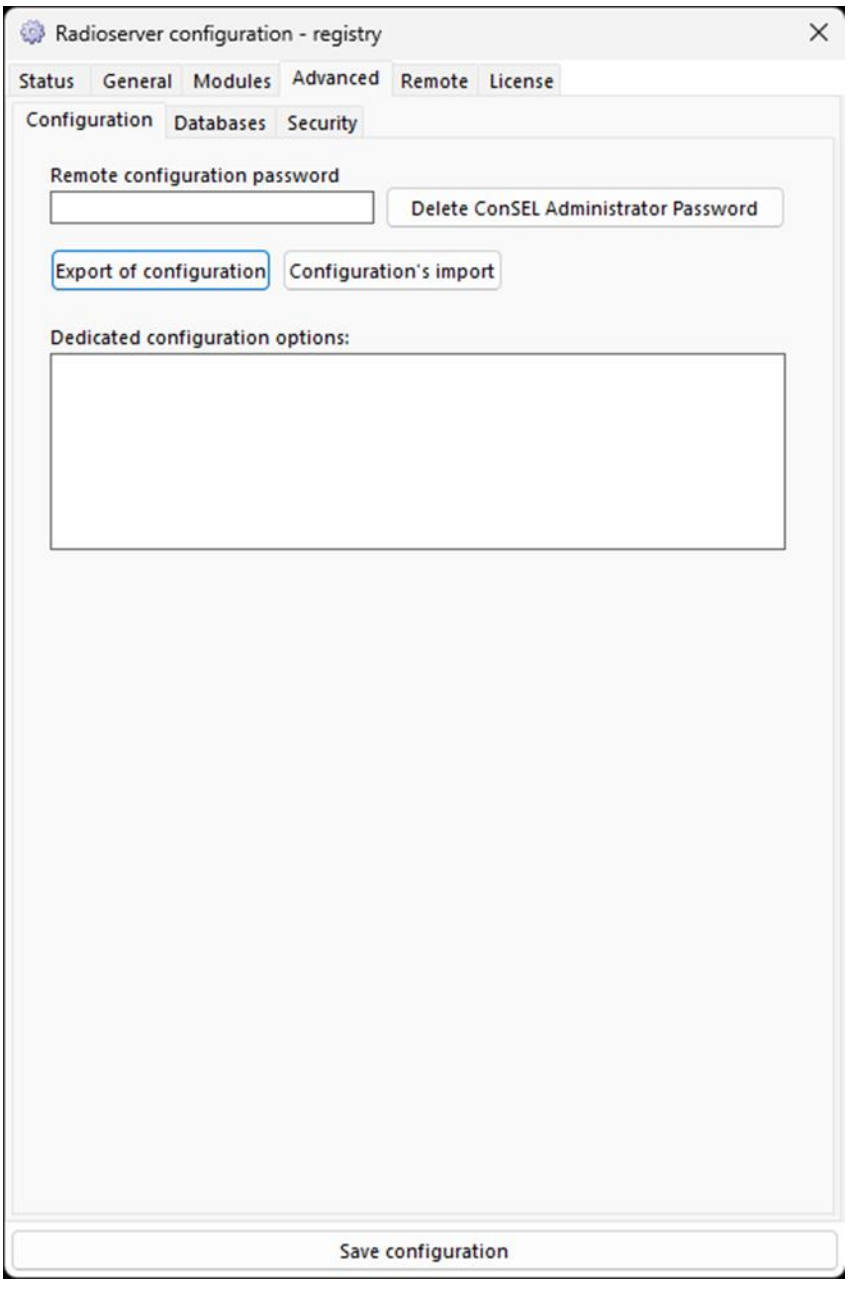
2.4 Backups

Backups created before the start of database encryption are not encrypted, as well as the backup that was created when the databases were encrypted.

these copies should be protected against data loss or leakage.

3 Client and server side verification of certificates for encrypted connections

3.1 Server side verification



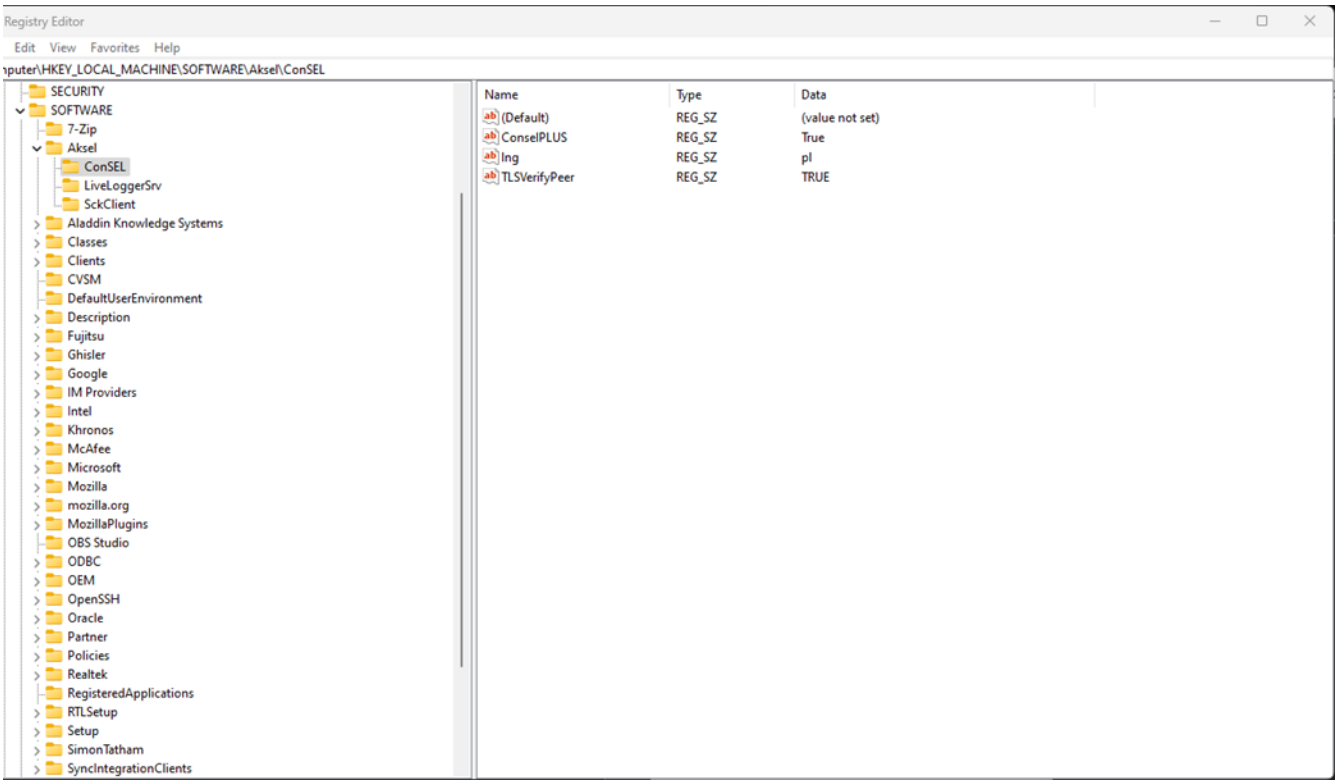
In order for the server to verify client certificates that connect to it, add TLSVerifyPeer=TRUE to the dedicated configuration options in the configuration options in the advanced options.

3.2 Client side verification

Adding validation of server certificates from the client side requires editing the Windows registry.

We head to the ConSEL folder which is located in HKEY_LOCAL_MACHINE\SOFTWARE\Aksel\

We add a string value:



3.3 Using your own certificates

The certificates used to verify the connection are in the folder Aksel/ConSEL/cert

The files in this folder are divided into 2 groups:

- ConSEL-client refers to ConSEL client,
- ConSEL-RS refers to radioserver.

In order to use your own certificates, replace the files in this folder with the names.

3.4 Signature generation for the encrypted certificate key

To use your own encrypted private key you need to create a signature for it.

To generate a signature for the certificate key, right-click on "encrypt the connection between the client and the server" (in the advanced option -> security) and select the option "Generate a signature file for the certificate key".