Important:
Using Microsoft SQL Server secure connections with Sage X3

From 2023 R2

Microsoft SQL Server "Forced encryption" flag is not supported with Sage X3 yet.

Microsoft SQL Server secure connections can be set up through the Sage X3 Management Console, from Sage X3 2023 R2. The Console documentation details how to secure Microsoft SQL Server connections for the Runtime (Application).

Microsoft SQL Server implements connection security for incoming connections through TLS encryption and the use of certificates. Microsoft proposes two options:

- ***Optional SSL connections***: Clients can choose whether they wish to encrypt the connection, and whether they trust the server's certificate or not.
- ***Forced SSL connections***: Clients must use encrypted communications. Non-encrypted connections will be refused by SQL Server.

Some components of the Sage X3 technology stack do not support encrypted communications yet. As a consequence, the 2023 R2 implementation *only supports optional SSL connections*. In other words, it is not possible to **force** encrypted communications in the Microsoft SQL Server settings with 2023 R2:

> The Microsoft SQL Server database flag **Force Encryption** should be set to **No** for databases used by Sage X3, in all cases.

Components of the Sage X3 technology stack that are clients of the database will specify how they connect to Microsoft SQL Server through two different flags:

- **Connection encryption** (**Yes** for encrypted connections, **No** otherwise)
- **Trust server certificate** (**Yes** to skip certificate chain validation, **No** otherwise)

If those two parameters are not specified, the communication is *not encrypted* by default.

> **NOTE:** Sage recommends using encrypted connections with a certificate chain whenever possible to secure your architecture, as specified in the security guidelines. Our recommended settings are:
>
> - Connection encryption: **Yes**
> - Trust server certificate: **No**

The following describes the behavior of each of the components of the Sage X3 stack that are clients of the database:

Sage X3 Runtime:

To enable the Sage X3 Runtime to connect to a secured SQL Server database, you must use the Console to carry out the following steps:

- Set the two parameters (**Connection encryption** and **Trust server certificate**) for the Runtime(s). Please review the Console documentation for details.
- Reconfigure the Runtime(s) and follow instructions to set up the certificate chain.
- **In architectures where the Runtime is not located in the same server as the Database, if SQL Server is using a root CA**:
  In addition to reconfiguring the Runtime, you must export the Certificate Authority (CA) public key (.pem) from the Certificate store of the database server and import it into the Microsoft Management Console (MMC) of each server where a Sage X3 Runtime exists.

X3 Services:

- Specify the two values for the **Connection encryption** and **Trust server certificate** options in the relevant solution settings in Sage X3 (Administration > Endpoints > MS SQL services).
  NOTE: The values will be defaulted from those used for the Sage X3 Runtime when you install the Syracuse server. Those defaults can be retrieved at any time later on.
  Please review the relevant technical documentation for more details.
- **If Connection encryption = true and SQL Server is using a root CA (not a self-signed CA)**, then you need to indicate the root CA .pem Key to use in the X3 Services configuration, whether X3 Services is installed on the same machine or not:
  - Export the CA public key from the Certificate store of the database server as a .pem file, and import it into the X3 Services server, in a repository that is accessible to X3 Services.
  - Change the X3 Services security configuration (**xtrem-security.yml**) to refer to that public CA key, in the **tls** section. Please review the technical documentation for more details.

Sage X3 Print Server:

The Sage X3 Print Server does not support encrypted connections yet. Support for encrypted Print Server connections will be released in the future. Until then, Print Server database connections are *not encrypted*.

In summary:

- Make sure you secure your database connection through encryption and a root CA certificate.
- However, do not set the Microsoft SQL Server flag **Force encryption** to true with Sage X3, until further notice.
- Set up your Sage X3 components accordingly, with the two MS SQL flags, and the certificate keys when necessary.