SYSPRO and SQL Server Encryption Overview

SYSPRO 8 Technical Article

Last Published: March 2021

Contents

SYSPRO and SQL Server Data Encryption

INTRODUCTION

This document focuses on data encryption relating to SYSPRO and Microsoft SQL Server. It should be considered as part of your company's overall security and privacy policies.

The focus is on securing data from the SYSPRO ERP application when using Microsoft SQL Server and securing the communication *between* SYSPRO and SQL Server.

Note: The remainder of this document includes some content from external sources. For clarity, we have highlighted the relevant content in *italicized* orange text preceded by the original URL. As these web sites are out of our control the text may have changed subsequently, or the URL may no longer be valid.

AUDIENCE

This document provides an overview of two technologies known as **Data Encryption at Rest (TDE)** and **Data Encryption in Motion (TLS)**.

If you require a more detailed explanation about how to configure SYSPRO, SQL Server and Windows to work with these technologies, then see the companion document: **SYSPRO and SQL Server Encryption Configuration**.

WHY DATA ENCRYPTION?

In today's highly regulated world, most companies operate in an environment where they must comply with one or more security and/or privacy regulations or government acts.

Examples include:

- EU citizens (GDPR - General Data Protection Regulation)
- Australia (OAIC - Privacy Act)
- Canada (PIPA, PIPEDA - Privacy Act)
- South Africa (POPI - Protection of Personal Information Act)
- USA (When this document was created (September 2019) the United States did not have any centralized, formal legislation at the federal level regarding this issue. However, it does ensure the privacy and protection of data through the United States Privacy Act, the Safe Harbor Act and the Health Insurance Portability and Accountability Act. Individual states may also have relevant acts that apply).

For additional information see the topic: Security and Privacy Links

Failure to comply with these regulations can often incur heavy penalties and even criminal prosecution.

In the event of a data breach, there are typically prescribed reporting considerations to a regulatory body. In most cases the penalties for a breach can be largely mitigated if it can be shown that reasonable attempts were taken to protect your data.

For example, if you can show that you have encrypted the database then any network or other security breach will limit the damage and, consequently, penalties can be mitigated.

In addition, by encrypting data passed between SYSPRO and SQL Server you effectively remove the chance of eavesdroppers and hackers being able to gather or even change data.

Owing to these considerations, many companies should consider data encryption as part of their security and privacy data compliance strategy.

The following topics will be introduced, together with some information relating to the available technologies and some performance considerations:

- Data Encryption at Rest
- Data Encryption in Motion

Data Encryption at Rest

Data Encryption at Rest describes the technique of configuring SQL Server so that the physical database files stored on the Windows file system are encrypted.

This ensures that, in the event of a network or other security breach, even if someone can access the physical database data or log files (or a backup of these files) the information remains secure.

The technique described here is known as **TDE - Transparent Data Encryption**.

Extract from: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017

Transparent Data Encryption (TDE) encrypts SQL Server, Azure SQL Database, and Azure SQL Data Warehouse data files, known as encrypting data at rest. You can take several precautions to help secure the database such as designing a secure system, encrypting confidential assets, and building a firewall around the database servers. However, in a scenario where the physical media (such as drives or backup tapes) are stolen, a malicious party can just restore or attach the database and browse the data. One solution is to encrypt the sensitive data in the database and protect the keys that are used to encrypt the data with a certificate. This prevents anyone without the keys from using the data, but this kind of protection must be planned in advance.

TDE performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data "at rest", meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries. This enables software developers to encrypt data by using AES and 3DES encryption algorithms without changing existing applications.

Relevant SYSPRO version – All versions

Data Encryption at Rest using TDE requires SQL Server configuration and does NOT require any additional configuration from within the SYSPRO application.

Therefore, Data Encryption at Rest using TDE is applicable to any SYSPRO version.

Note: SYSPRO software prior to SYSPRO 8 stores some configuration and auditing data in the file system, and therefore is not encrypted using this technique. This is one of the many benefits of organizations migrating from earlier versions to SYSPRO 8.

The technical details of how to setup and configure SQL Server with TDE is available in a separate technical guide available from within the SYSPRO 8 Help (see: *SYSPRO Help* > *Resources* > *Technical Guides* > *SYSPRO and SQL Server Encryption Configuration*).

PERFORMANCE RUNNING SYSPRO AND SQL SERVER USING TDE

The SYSPRO development team have a set of benchmarks to test the software under load. Although these are run in a Microsoft Azure environment, an equivalently configured on premise environment would also be expected to yield the same results.

During 2019 the SYSPRO development team ran the benchmarking application using SYSPRO 8 2019 R2 software connecting to SQL Server 2017 with TDE enabled. Results were compared with the same environment, the same SYSPRO software and the same database not using TDE (i.e. a direct comparison between encrypted and unencrypted databases).

All the tests ran successfully, even under load, and the comparison showed that the average performance throughput was only degraded by about 1%.

Some additional information about the benchmarks and the resulting data and graphical output can be seen in the topic: SYSPRO and SQL Server Benchmark Results

Data Encryption in Motion

Data Encryption in Motion describes the technique of configuring SYSPRO and SQL Server so that all communication between SYSPRO and SQL is encrypted. This includes initial connection information, SQL statements issued, and the actual data passed to-and-from SQL Server.

Data Encryption in Motion ensures that eavesdroppers and hackers can't see what is transmitted. This is particularly useful for private and sensitive information, but also for all information sent between SYSPRO and SQL Server.

It should be mentioned that if the SYSPRO Application server and SQL Server are running on the same server, then Data Encryption in Motion may add an unnecessary overhead with little or no benefit.

The technology described here is known as **TLS – Transport Layer Security**.

Extract from: https://blog.coeo.com/securing-connections-to-sql-server-with-tls

Fundamentally, TLS provides you with the ability to encrypt connections between SQL Server and calling client applications. When a client requests an encrypted connection to a SQL Server configured for TLS, an initial handshake takes place to negotiate the cipher suite from which further communication should take place. Once agreed, SQL Server then sends its TLS certificate to the client, which the client must then validate and trust against its copy of the Certification Authority (CA) certificate. Finally, providing the TLS certificate is trusted and it meets certain other requirements, a secure connection is established.

Warning: You must use TLS 1.2 (or higher) as earlier versions had known vulnerabilities. For your information, TLS supersedes its now deprecated predecessor – SSL - Secure Sockets Layer.

RELEVANT SYSPRO VERSION – SYSPRO 8 2020 R1

SYSPRO 8 2020 R1 (release February 2020) has been enhanced to allow an administrator to configure SYSPRO and SQL Server using TLS, thus providing Data Encryption in Motion.

ODBC DRIVER INFORMATION

SYSPRO communicates with SQL Server using ODBC drivers provided by Microsoft. These provide standardized, robust, and high-performance interfaces to SQL Server.

SYSPRO 8 2020 R1 supports three different ODBC Drivers:

- SQL Server
- ODBC Driver 13 for SQL Server
- ODBC Driver 17 for SQL Server

The first driver (simply named **SQL Server**) ships as part of Windows and is known as a Windows Data Access Component (WDAC) – it has provided ODBC access to SQL Server for applications such as SYSPRO for many years. However, Microsoft have recently indicated that new software should no longer use this driver, partly because some features (e.g. relating to encryption) are not fully available with the **SQL Server** (WDAC) driver.

For this reason, SYSPRO 8 2020 R1 has been enhanced to allow more recent ODBC drivers to be specified in the **System Setup**.

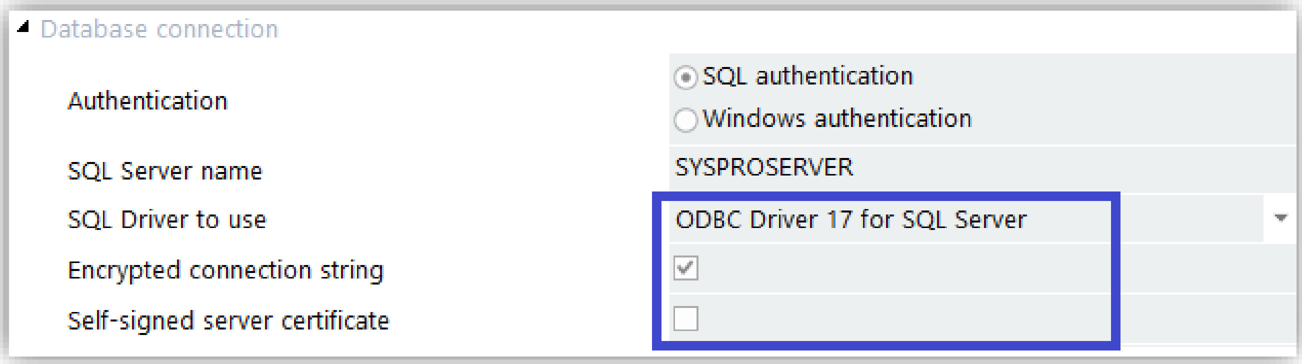
The remainder of this topic assumes that **ODBC Driver 17 for SQL Server** is selected. If you use the older driver (ODBC Driver 13 for SQL Server) then substitute the driver name when appropriate.

Note: You may have to download and install the required ODBC driver if it is not currently installed on your SYSPRO application server.

ENCRYPTED CONNECTION STRING

Once you have chosen **ODBC Driver 17 for SQL Server** in the **System Setup**, you can select the **Encrypted connection string** checkbox and indicate whether you want a **Self-signed server certificate**.

These options are available in the *System Setup* > *Database Tab*:



Database connection

Authentication	● SQL authentication ○ Windows authentication
SQL Server name	SYSPROSERVER
SQL Driver to use	ODBC Driver 17 for SQL Server
Encrypted connection string	☑
Self-signed server certificate	□

Warning: Self-signed server certificates are, by their nature, less secure. The encrypted handshake is based on NT LAN Manager (NTLM). It is recommended that you provision a verifiable certificate on SQL Server for secure connectivity. Transport Layer Security (TLS) can only be secured with certificate validation.

Once you have saved these settings you should immediately configure SQL Server to work with TLS security. Alternatively, if you had already set up SQL Server to support TLS security then just login and the new Encryption in Motion technology is applied.

The technical details of how to set up and configure SQL Server with TLS is available in a separate technical guide available from within the SYSPRO 8 Help (*see: SYSPRO Help* > *Resources* > *Technical Guides* > *SYSPRO and SQL Server Encryption Configuration*).

Performance running SYSPRO and SQL Server using TLS

The SYSPRO development team have a set of benchmarks to test the software under load. Although these are run in a Microsoft Azure environment, an equivalently configured on premise environment would also be expected to yield the same results.

During 2019 the SYSPRO development team ran the benchmarking application using SYSPRO 8 2020 R1 software connecting to SQL Server 2017 with TLS enabled. Results were compared with the same environment, the same SYSPRO software and the same database not using TLS (i.e. a direct comparison between encrypted and unencrypted communication between SYSPRO and SQL Server).

All the tests ran successfully, even under load, and the comparison showed that the average performance throughput was only degraded by about 1%.

Some additional information about the benchmarks and the resulting data and graphical output can be seen in the topic: SYSPRO and SQL Server Benchmark Results.

SYSPRO and SQL Server Benchmark Results

This topic provides a summary of the benchmark results described earlier in this document.

There are four benchmark results presented:

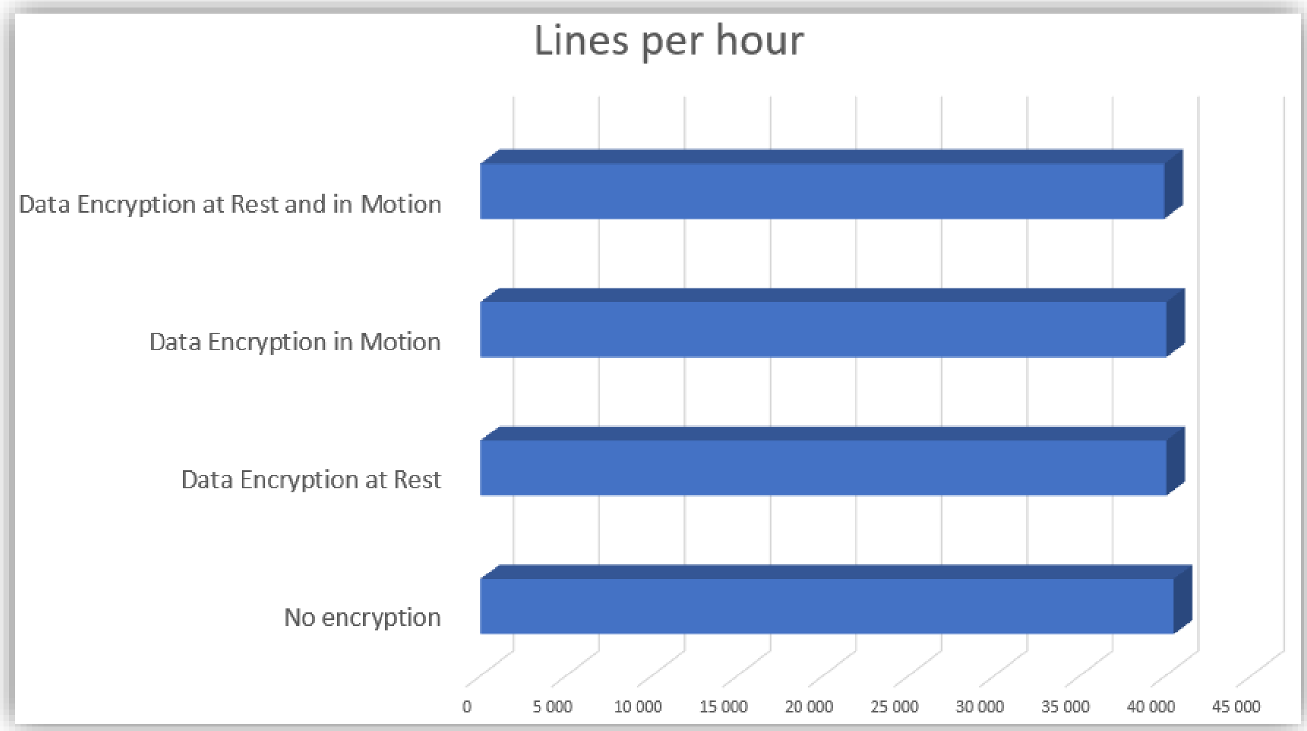
- SYSPRO running with no encryption - data or communication
- Data Encryption at Rest using TDE
- Data Encryption in Motion using TLS
- Both Data Encryption at Rest (TDE) and in Motion (TLS)

The benchmarks compared otherwise identical environments (such as hardware, software, operating system, SQL Server etc.) data and configuration, simply varying the applicable encryption.

The results compare the number of Sales Order **lines per hour** processed through our standard benchmark tool. This includes creating a sales order, querying a sales order, creating an invoice, and printing an invoice (although no physical printing is included).

The benchmark results shown below approximate the throughput of a 250-concurrent user system working with the sales order process.

Benchmark Results Graph



From this graph you can see that the throughput is nearly identical in all scenarios. Approximately 40 000 sales order lines per hour.

Benchmark Results Data

The data from which this graph was generated is provided below:

Encryption level	Lines per hour	Degradation
No encryption	40 480	-
Data Encryption at Rest	40 040	1.1%
Data Encryption in Motion	40 040	1.1%
Data Encryption at Rest and In Motion	39 920	1.4%

References

SECURITY AND PRIVACY LINKS

The following links provide some introductory information relating to the privacy and security regulations in various territories.

Important: The links below are provided for information only – you should always consult with the authorities under which your company operates and take appropriate advice.

- GDPR data protection: https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection
- OAIC privacy Act: https://www.oaic.gov.au/privacy/the-privacy-act/
- PIPA and PIPEDA Information: https://iclg.com/practice-areas/data-protection-laws-and-regulations/canada
- POPI Act information: https://www.michalsons.com/blog/popi-act-summary-in-plain-language/18618
- USA data protection: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

SQL SERVER SECURITY AND ENCRYPTION

- The following link provides a set of resources from Microsoft relating to various security topics:
  https://docs.microsoft.com/en-us/sql/relational-databases/security/security-center-for-sql-server-database-engine-and-azure-sql-database?view=sql-server-2017
- The following link provides a Microsoft introduction to SQL Server encryption:
  https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/sql-server-encryption?view=sql-server-2017
- The following link provides a Microsoft introduction to TDE:
  https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017
- The following link provides a Microsoft introduction to encrypted connections to the database engine:
  https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017
- The following link provides information relating to TLS 1.2 support for Microsoft SQL Server:
  https://support.microsoft.com/en-za/help/3135244/tls-1-2-support-for-microsoft-sql-server

SYSPRO™

www.syspro.com