Installation Instructions
Original Instructions

Allen-Bradley
by ROCKWELL AUTOMATION

FactoryTalk AssetCentre Installation Guide

Version 13.00.00

Rockwell Automation

Table of Contents

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT: Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.

Tip: Identifies information that is useful and can help to make a process easier to do or easier to understand.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Summary of changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Reason for change
About FactoryTalk AssetCentre Web Client on page 80	Add descriptions for new features.
Install Microsoft SQL Server on page 14	Update the steps of installing the Microsoft SQL Server.
Steps to install the FactoryTalk AssetCentre Server on page 19	Update the sequence of installation process.
Steps to install the FactoryTalk AssetCentre Agent software on page 24	Add steps for selecting the directory types and third-party controllers.
Configure for security-enabled RSLogix family software	Manual configuration of security-enabled RSLogix family software is no longer needed.
Command-line parameters for silent or unattended installation on page 62	Update command-line parameters.
Troubleshoot FactoryTalk AssetCentre on page 84	Update workarounds for connection issues of FactoryTalk AssetCentre Web Client.
Create a self-signed TLS certificate on the SQL Server or FactoryTalk Network Directory computer on page 109	Add steps of creating a self-signed TLS certificate on the SQL Server or FactoryTalk Network Directory computer.

Introduction

About FactoryTalk AssetCentre

FactoryTalk® AssetCentre monitors your factory automation system and provides centralized tools to minimize downtime due to unauthorized actions or failing devices. It does this by:

- Providing version control and archiving of program files and documents.
- Providing a disaster recovery system that verifies your devices' program and configuration files against protected master files, ensuring quick and accurate recovery if a problem should occur (optional Disaster Recovery capability).
- Monitoring FactoryTalk-enabled software products and logging system events and user actions (recorded in the Event log and Audit log respectively).
- Assets Lifecycle, which provides the lifecycle status of hardware devices by synchronizing lifecycle information in the FactoryTalk AssetCentre server and client with the data on the Rockwell Automation lifecycle website.
- Managing device configuration files.

FactoryTalk Services Platform

FactoryTalk AssetCentre uses the FactoryTalk® Services Platform to provide seamless connectivity with other FactoryTalk-enabled software. Customers and computers are defined in the FactoryTalk® Directory; access to user actions within the FactoryTalk AssetCentre system is controlled within FactoryTalk® Security.

About the documentation set

The documentation set includes:

- **FactoryTalk AssetCentre Installation Guide** (Document ID FTAC-IN005). Use this manual to install the FactoryTalk AssetCentre system. This manual is also available in the FactoryTalk AssetCentre installation package in 13.00.00-FTAssetCentre\Docs. The file name is FactoryTalk AssetCentre Installation Guide.pdf. You can find it in Rockwell Automation Literature Library.
- **Help**. Use the comprehensive Help for assistance while using the FactoryTalk AssetCentre system.
- **FactoryTalk AssetCentre Getting Results Guide** (Document ID FTAC-GR002). Use this manual to get started with the FactoryTalk AssetCentre system. You can find it in Rockwell Automation Literature Library.
- **FactoryTalk AssetCentre Utilities User Manual** (Document ID FTAC-UM001). Use this manual for assistance while using an array of utilities whose capabilities are not present in the FactoryTalk AssetCentre system. You can find it in Rockwell Automation Literature Library.

About this book

This book is written for FactoryTalk AssetCentre administrators and IT professionals. To perform many of the tasks described in this book, you need to log on to the computers onto which you are installing software as an Administrator, or log on using an account that has administrative privileges.

We assume you are familiar with:

- Microsoft® Windows® operating systems including basic Windows networking and administration tasks
- Microsoft SQL Server
- RSLinx® Classic and FactoryTalk® Linx communication software
- Rockwell Automation programming tools for programmable logic controllers
- Control networks such as DeviceNet and programmable logic controllers such as ControlLogix® processors

The components of FactoryTalk AssetCentre

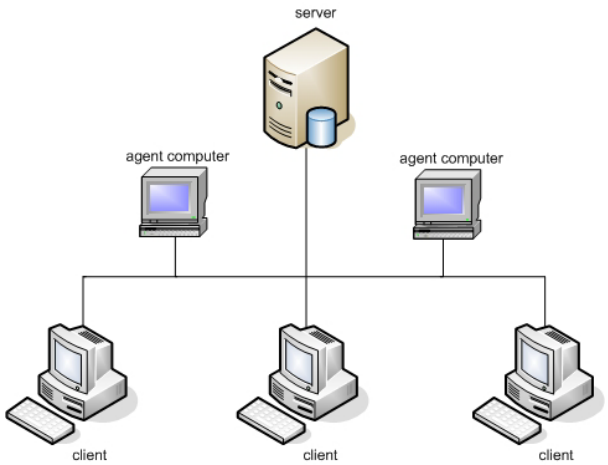
There are four primary components of a FactoryTalk AssetCentre system:

- **FactoryTalk AssetCentre server**, which controls the rest of the system and governs its operations. The server requires Microsoft SQL Server to function (see Server computer requirements on page 8). The SQL Server is typically on the same computer as the FactoryTalk AssetCentre server. The instructions in this manual are written for that case, although the SQL Server could be installed on a different computer.
- **FactoryTalk AssetCentre agents**, which are programs that perform certain scheduled operations, such as Disaster Recovery and searches. Agents run independently of the server and independently from each other—users schedule operations and the agents perform them at the scheduled time. By spreading the processing load over multiple computers, FactoryTalk AssetCentre agents speed up operations. When a server needs a scheduled operation to begin, it tries to locate an available computer running the appropriate agent to perform that task. When it locates an agent to perform the task, it assigns the task to that agent. When the agent has completed the task, the agent reports back to the server that the task is done.
  Agents can be installed on any computer that:
  - Is capable of running the agent software (see Agent computer requirements on page 10).
  - Is connected to the FactoryTalk AssetCentre server.
- **FactoryTalk AssetCentre desktop clients**, which permit users to configure and use the server, view logged events, and perform other tasks associated with the software. The desktop client can be installed on any computer that:
  - Is capable of running the desktop client software (see Client computer requirements on page 9).
  - Is connected to the FactoryTalk AssetCentre server.
- **FactoryTalk AssetCentre Web Client**, which allows users to access a FactoryTalk AssetCentre client through a web interface on computers. FactoryTalk AssetCentre Web Client supports several FactoryTalk AssetCentre desktop client functions. FactoryTalk AssetCentre Web Client can be accessed on any computer device that:
  - Is capable of running the Web Client software (See Web Client computer or device requirements on page 11).
  - Is connected to the FactoryTalk AssetCentre server.

The number of clients, agents, and agent groups qualified within one FactoryTalk AssetCentre system

The following is the number of clients, agents, and agent groups qualified within one FactoryTalk AssetCentre system at the same time. More clients, agents, or agent groups running will impact the system performance. The system cannot exceed 50 agents total. For example, a system could have 50 agent groups each with one agent member.

- Desktop client: 150
- Web client: 200
- Agent: 50
- Agent groups: 50



System requirements

FactoryTalk AssetCentre works within the system requirements of all Rockwell Automation software products.

Hardware requirements

- For the optimal performance of the FactoryTalk AssetCentre system, we recommend that computers running FactoryTalk AssetCentre Server, FactoryTalk AssetCentre Desktop Client, or FactoryTalk AssetCentre Agent meet or exceed the following hardware requirements.

Type	Description	CPU	Core Processors	RAM
Operator Workstation	FactoryTalk AssetCentre Desktop Client	Intel® Core™ i5 Standard Power processor	2	8 GB
Engineering Workstation	FactoryTalk AssetCentre Desktop Client FactoryTalk AssetCentre Agent	Intel Core i5 Standard Power processor	2	8 GB
System Agent	FactoryTalk AssetCentre Agent	Intel Core i5 Standard Power processor	2	8 GB
Application Server	FactoryTalk AssetCentre Server	**Small systems:** Intel Core i5 Standard Power processor	2	8 GB
		Medium to large systems: Intel® Xeon® quad-core family processor	4	16 GB

- For the optimal performance of the FactoryTalk AssetCentre system, we recommend that virtual machines running FactoryTalk AssetCentre Server, FactoryTalk AssetCentre Desktop Client, or FactoryTalk AssetCentre Agent meet or exceed the following hardware requirements.

Type	Description	CPU	Core Processors	RAM
Operator Workstation	FactoryTalk AssetCentre Desktop Client	Intel Xeon quad-core family processor	2	8 GB
Engineering Workstation	FactoryTalk AssetCentre Desktop Client FactoryTalk AssetCentre Agent	Intel Xeon quad-core family processor	2	8 GB
System Agent	FactoryTalk AssetCentre Agent	Intel Xeon quad-core family processor	2	8 GB
Application Server	FactoryTalk AssetCentre Server	**Small systems:** Intel Xeon quad-core family processor	2	8 GB
		Medium to large systems: Intel Xeon quad-core family processor	4	16 GB

- For display resolution, 1024x768 or higher resolution is required.

System size

FactoryTalk AssetCentre is tested based on these system sizes.

Types	Components	System architecture
Small systems	Server	AssetCentre Server, MicrosoftSQL Server©SQL Server, and FactoryTalk Directory Server are co-located.
	Agent	1-5
	Desktop Client	10
	Web Client	25
Medium systems	Server	AssetCentre Server and Microsoft SQL Server are co-located. FactoryTalk Directory Server is on a separate computer.
	Agent	6-25
	Desktop Client	60
	Web Client	100
Large systems	Server	AssetCentre Server, Microsoft SQL Server, and FactoryTalk Directory Server are hosted on separate computers.
	Agent	26-50
	Desktop Client	100-150
	Web Client	200

Product compatibility

FactoryTalk AssetCentre version 13.00.00 is compatible with the following Rockwell Automation products. For the latest information regarding software platform support, refer to the Rockwell Automation Product Compatibility and Download Center.

FactoryTalk AssetCentre Desktop Client

- To edit the file and data settings for a compare operation, you must have associated software installed on the client computer. To perform archive to archive version compare, you must install the programming software on the client computer.

Asset	Compatible Software	Version
Allen-Bradley® PLC-5® Controller	RSLogix™ 5	10.00 or later
Allen-Bradley SLC™ 500 Controller and Allen-Bradley MicroLogix™ Controller	RSLogix 500®	12.00 or later
ControlLogix® and CompactLogix™	RSLogix 5000®	17.00 or later
	Studio 5000 Logix Designer®	21.00 or later
	RSLogix 5000 Compare Utility or Logix Designer Compare Tool	10.00 or later
FactoryTalk® View Site Edition (SE)	FactoryTalk View Studio Enterprise	14.00 or later
Rockwell Automation drives	DriveExecutive™ Lite	5.02 or later

For more information about the specific drives that FactoryTalk AssetCentre is compatible with, see Knowledgebase Document ID: QA47141 - FactoryTalk AssetCentre RA Motor Control or PowerFlex Drive Device Support.

- FactoryTalk View ME Transfer Utility version 13.00 or later if your system includes Allen-Bradley PanelView Plus and MobileView™ operator interfaces.
- STEP7 version 5.6 sp1 or later if your system includes Siemens® S7 project.

FactoryTalk AssetCentre Agent

- For Disaster Recovery functions, the programming software for your devices MUST be installed on the agent computer.

Asset	Compatible Software	Version
Allen-Bradley PLC-5 Controller	RSLogix 5	10.00 or later
Allen-Bradley SLC 500 Controller and Allen-Bradley MicroLogix Controller	RSLogix 500	12.00 or later
ControlLogix and CompactLogix	RSLogix 5000	17.00 or later
	Studio 5000 Logix Designer	21.00 or later
	RSLogix 5000 Compare Utility or Logix Designer Compare Tool	10.00 or later
Allen-Bradley PanelView Plus Controller and Allen-Bradley MobileView Controller	FactoryTalk View ME Transfer Utility	14.00 or later
	FactoryTalk Linx (formerly known as RSLinx Enterprise)	6.40 or later
FactoryTalk View Site Edition	FactoryTalk View Studio Enterprise	14.00 or later
Rockwell Automation drives	DriveExecutive Lite	5.02 or later
Allen-Bradley PowerFlex® Drive	UDC	15.02 or later
Mitsubishi® Controller	GX Works2™	1.615R
	GX Works3™	1.095Z
Siemens S7 Controller	TIA Portal	15.1, 16, 17, and 18
	STEP7	5.6 sp1 or later

Operating systems

FactoryTalk AssetCentre is tested and supported on the operating systems installed from original Microsoft media only. FactoryTalk AssetCentre runs on 64-bit versions of the following operating systems.

IMPORTANT:

- Turn off the Windows updates on production computers. Installing Microsoft Service Pack release or Windows operating system updates may affect the operation of Rockwell Automation software installed on the computer. To avoid this problem, see Knowledgebase Document ID: QA2151 - Microsoft Patch Qualifications.
- Before you install FactoryTalk AssetCentre on the computer running Windows Server 2012 R2, it is required that you install the following Windows update: Windows Server 2012 R2 update: April 2014.

FactoryTalk AssetCentre Server

This version of FactoryTalk AssetCentre Server was tested on these 64-bit operating systems:

- Windows Server® 2022
- Windows Server 2019
- Windows Server 2016

FactoryTalk AssetCentre Desktop Client, Web Client, and Agent

This version of FactoryTalk AssetCentre Desktop Client, Web Client, and Agent were tested on these 64-bit operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows® 11 (v21H2 and v22H2)
- Windows 10 IoT Enterprise 2021 Long-Term Servicing Channel (LTSC)
- Windows 10 IoT Enterprise 2019 Long-Term Servicing Channel (LTSC)
- Windows 10 (v21H2 and v22H2)
  FactoryTalk AssetCentre adopts .NET 4.8, which is only supported on Windows 10 v1803 and later.

Software requirements

SQL Server databases

The following are SQL Servers supported by FactoryTalk AssetCentre.

- Microsoft SQL Server 2019
- Microsoft SQL Server 2022

FactoryTalk AssetCentre Desktop Client

The following are minimum software requirements for FactoryTalk AssetCentre Desktop Client.

- (optional) Editing software for Siemens S7 Controller (STEP7), such as SIMATIC Manager
  It is only required when using Archive to Archive comparison for Siemens S7 (S7-300/400 with STEP7 software).

FactoryTalk AssetCentre Agent

The following are minimum software requirements for FactoryTalk AssetCentre Agent.

- (optional) SIMATIC NET if you want to connect to Siemens S7 Controller (STEP7) via MPI (Multi Point Interface) or PROFIBUS protocol
  It is only required when using Disaster Recovery for Siemens S7 (S7-300/400 with STEP7 software).
- (optional) Siemens TIA Portal software if you want to use Disaster Recovery for Siemens controllers (S7-1200, S71500, and ET200 with TIA Portal software).
- (optional) Mitsubishi GX Works3 software if you want to use Disaster Recovery for Mitsubishi controllers (iQ-F and iQ-R series with GX Works3 software).
- (optional) Mitsubishi GX Works2 software if you want to use Disaster Recovery for Mitsubishi controllers (L, F, and Q series with GX Works2 software).

FactoryTalk AssetCentre Web Client

The following are minimum software requirements for FactoryTalk AssetCentre Web Client.

- Microsoft® Edge™
- Google® Chrome™ browser
- Mozilla® Firefox®

Network requirements

Your Microsoft Windows network must use the TCP/IP protocol.

If you use a firewall, you must configure the firewall to permit traffic on the following ports.

Port type and name	Comments
TCP port 25	Standard SMTP email port
TCP port 80	Standard WWW port
TCP port 135	RPC/DCOM endpoint mapper DCOM uses TCP Port 135 to establish communication and randomly assign ports from 1000 through 65535.
TCP port 443	HTTPS connection when SSL/TLS is enabled.
TCP port 445	File and printer sharing
TCP port 1433	Communications to SQL Server
TCP port 2222	Source port for connections
TCP port 4241	FactoryTalk Live Data Message for FactoryTalk Linx (RSLinxNG.exe)
TCP port 5241	FactoryTalk Application Services
TCP ports 7002 - 7004	FactoryTalk AssetCentre
UDP port 137	File and printer sharing
UDP port 138	File and printer sharing
UDP port 1434	Browsing for SQL Servers
UDP port 21060	Rockwell Automation Trace Diagnostics
UDP port 21061	Rockwell Automation Trace Diagnostics
TCP/UDP 44818	Ethernet/IP, messaging, data transfer, or peer messaging

Some of these ports may vary on your network. Work with your network administrators to determine the correct port numbers to open.

IMPORTANT: TCP port 445 can be turned off in the computers with FactoryTalk AssetCentre system or its components. If using Disaster Recovery for Remote Computer, the remote computer with the shared folder must have TCP port 445 turned on for file sharing.

You may need to open ports for other Rockwell Automation products as well. See Knowledgebase Document ID: BF7490 - TCP/UDP Ports Used by Rockwell Automation Products.

About the installation process

FactoryTalk AssetCentre supports two installation methods:

- Setup wizard installation
- Unattended or silent installation

The Setup wizard installs the software through the installation interface step by step. If you choose the standard Setup wizard to install FactoryTalk AssetCentre software, Chapter 2 through Chapter 5 guides you through the following tasks:

1. Install the prerequisite software for the FactoryTalk AssetCentre server.
2. Install the FactoryTalk AssetCentre server.
3. Install FactoryTalk AssetCentre agents.
4. Install FactoryTalk AssetCentre desktop clients.

The unattended or silent installation uses command lines to specify installation properties so that the software is installed without user intervention. Unattended or silent installation doesn't omit any installation components against the standard method. It allows you to specify all installation properties before the installation starts, and then installs the software automatically. To install FactoryTalk AssetCentre software with silent or unattended installation, see Chapter 8 for detailed instructions.

Install the FactoryTalk AssetCentre Server software

This chapter describes:

Before you install the FactoryTalk AssetCentre Server

The following tasks are required before installing FactoryTalk AssetCentre Server.

- Ensure that the user performing installation has administrative rights in Windows.
- Ensure that a Microsoft SQL Server is available, and it is already installed on the same computer as the intended FactoryTalk AssetCentre Server, or on a separate Microsoft Windows server.
- Ensure that the Windows account of the user performing the installation, or a Windows group of which the user performing the installation is a member, is assigned the Microsoft SQL Server System Administrator role before attempting the installation.
- If you will configure the FactoryTalk AssetCentre Server to use a remote SQL database, ensure that a standalone managed service account or a group managed service account has been created in your Windows Active Directory.

Ensure that the current Windows user has administrative rights

As part of the installation process, FactoryTalk AssetCentre creates program folders and modifies entries, which requires administrative rights in Windows. For example, the Windows domain Administrator account has these rights and will be able to successfully install the software.

Install Microsoft SQL Server

FactoryTalk AssetCentre uses a Microsoft SQL Server database to store project files and user data. You may install SQL Server on the FactoryTalk AssetCentre server computer or on another computer across a network. Microsoft SQL Server is not included in FactoryTalk AssetCentre installation package. We recommend you to acquire Microsoft SQL Server with its latest Service Pack separately.

Tip: Before you install Microsoft SQL Server, you need to turn off Windows Firewall from Windows Control Panel.

If a supported edition of SQL Server is installed, you can skip these steps, however, you may need to reconfigure the SQL Server.

To install Microsoft SQL Server

1. Log on to the server computer as an administrator or as a user with administrative rights.

   Tip: It is possible to install the SQL Server on a different computer from the one on which you install the FactoryTalk AssetCentre Server software as long as they are on the network.

2. Start the SQL Server installation from the SQL Server media.
3. Follow the on-screen instructions for installation until you get to the **Feature Selection** screen.
4. On the **Feature Selection** screen, choose the SQL Server features that you want to install. If you like, or if your business requires you to do so, you may install the complete SQL Server installation.

If you want to install only those features necessary to run the FactoryTalk AssetCentre server:

a. On the **Feature Selection** screen, make sure the following features are selected:
   - Database Engine Services
   - Full-Text and Semantic Extractions for Search
   - Client Tools Connectivity (not applicable for Microsoft SQL Server 2022 or later)
   - Client Tools Backwards Compatibility (not applicable for Microsoft SQL Server 2022 or later)
   - Management Tools - Basic (not applicable for Microsoft SQL Server 2016 or later)

b. Click **Next**.

5. Follow the on-screen instructions for installation until you get to the **Server Configuration** screen.
6. In the **Server Configuration** screen, keep the default settings for the **Services Accounts** tab.
7. In the **Server Configuration** screen, click the **Collation** tab.
8. Under **Database Engine**, make sure that **SQL_Latin1_General_CP1_CI_AS** is selected.
   If it isn't, click **Customize**, and then, in the **Customize the SQL Server Version Database Engine Collation** dialog box (where version is your SQL Server version), select **SQL collation, used for backwards compatibility** and **SQL_Latin1_General_CP1_CI_AS**.

IMPORTANT: The collation settings must be case-insensitive! If the settings are case-sensitive, the FactoryTalk AssetCentre database installation will fail.

---

9. In the **Database Engine Configuration** window, click the **Server Configuration** tab.
10. Under **Authentication Mode**, select **Windows authentication mode**.
    If you want to access the database with SQL Server Authentication in the future, select **Mixed Mode (SQL Server authentication and Windows authentication)**.
    If you use a SQL user account to connect the database, you have to pay attention to the disadvantages of SQL Server Authentication.

WARNING:

- A number of failed sign-in attempts from attackers will cause a user account to be locked.
- The encrypted SQL Server Authentication login password must be passed over the network at the time of the connection. Some applications that connect automatically will store the password at the client. These are additional attack points.
- Windows offers additional password policies that are not available for SQL Server logins.
  When you select **Mixed Mode**, fields open for entering the password for the sa (SQL Server system administrator) account password. Do not forget the password. You may need this password when you install the FactoryTalk AssetCentre server.

IMPORTANT: Do not leave the password blank. Doing so leaves your SQL Server and your computer open to attack.

---

11. Under **Specify SQL Server administrators**, add a Windows account to provision as a SQL Server system administrator, and then select **Next**.

NOTE: You must add the user account that is going to perform the FactoryTalk AssetCentre installation.

---

12. Follow the on-screen instructions to complete the installation.

After you install a Microsoft SQL Server, you must install an appropriate service pack, which is necessary for the software to run properly and protects your SQL Server from certain types of attacks.

Tip: We recommend that you install Microsoft SQL Servers with their latest Service Pack.

Minimum Microsoft SQL Server permissions

The permissions discussed here are set automatically during the FactoryTalk AssetCentre Database installation. The information is provided for reference for the SQL administrator.

The Microsoft service accounts (virtual service account, standalone managed service account, and group managed service account) user's default database value can be **master** or **AssetCentre**. By default, the database value is set to **AssetCentre**. The Microsoft service accounts (virtual service account, standalone managed service account, and group managed service account) user needs to belong to the following AssetCentre database roles:

- db_dataexecute
- db_datareader
- db_datawriter
- public

The db_dataexecute database role was added to the FactoryTalk AssetCentre database during the FactoryTalk AssetCentre server installation. All of the user stored procedures and user functions in the FactoryTalk AssetCentre database need to have the **Execute** permission granted to the db_dataexecute database role.

Configure the certificate for encrypted connection to the database

SQL Server can use Transport Layer Security (TLS) to encrypt data that is transmitted across a network between an instance of SQL Server and an application. TLS can be used for server validation when a client connection requests encryption.

We recommend using certificates signed by a certificate authority (CA). Encryption with a self-signed certificate is possible, but a self-signed certificate offers only limited protection. For more information about creating a self-signed certificate, please see Create a self-signed TLS certificate on the SQL Server computer on page 108.

For encrypted connection to the database with a CA issued certificate, besides configuring a certificate on the SQL Server computer, you also need to:

- Configure a certificate on the SQL Server computer
- Configure a certificate on the FTAC server computer

IMPORTANT: There will be an exception during the FactoryTalk AssetCentre installation if you don't configure the SQL Server certificate.

Configure a certificate on the SQL Server computer

To establish encrypted connections to the database, first install the certificate on the SQL Server computer.

To configure a certificate on the SQL Server computer

1. Add the snap-in.
   a. On the **Start** menu, select **Run**, enter **MMC** in the **Open** box, and then select **OK**.
   b. In the Microsoft Management Console, select **File > Add/Remove Snap-in**.
   c. In the **Add or Remove Snap-ins** dialog box, select **Certificates**, and then select **Add**.
   d. In the **Certificates snap-in** dialog box, select **Computer account**, and then select **Next**.
   e. In the **Select Computer** dialog box, keep the default **Local computer** selection, and then select **Finish**.
   f. In the **Add or Remove Snap-ins** dialog box, select **OK**.
2. Import the certificate.
   a. In the Microsoft Management Console, expand **Certificates > Personal**, right-click **Certificates**, and then select **All Tasks > Import**.
   b. In the Certificate Import Wizard, specify the certificate file's full path, and then select **Next**.
   c. Enter the password, and then select **Next**.

d. Specify the certificate store as **Personal**, and then select **Next**.

e. Select **Finish**.

3. Add the SQL Server service account permission.

a. In the Microsoft Management Console, right-click the imported certificate, and then select **All Tasks > Manage Private Keys**.

b. In the **Security** dialog box, add read permission for the user account used by the SQL Server service account. Note that the location should be your local computer name.

Tip: To find the SQL Server service account:

i. Open Windows **Services**.

ii. Double-click **SQL Server (InstanceName)**.

iii. Select the **Log On** tab, and then find the SQL Server service account in the **This account** box.

4. Add the certificate to the SQL Server instance.

a. Open SQL Server Configuration Manager.

b. Expand **SQL Server Network Configuration**, right-click **Protocols for InstanceName**, and then select **Properties**.

c. In the **Protocols for InstanceName Properties** dialog box, select the **Certificate** tab, and then select the certificate from the **Certificate** list.

d. Select **OK**.

5. Restart SQL Server.

a. In SQL Server Configuration Manager, select **SQL Server Services**.

b. Right-click **SQL Server (InstanceName)**, and then select **Restart**.

Configure a certificate on the FactoryTalk AssetCentre server computer

To establish encrypted connections to the database, after assigning a certificate to the SQL Server computer, set up the FactoryTalk AssetCentre server to trust the certificate's root authority.

To configure a certificate on the FactoryTalk AssetCentre server computer

1. Add the snap-in.

a. On the **Start** menu, select **Run**, enter **MMC** in the **Open** box, and then select **OK**.

b. In the Microsoft Management Console, select **File > Add/Remove Snap-in**.

c. In the **Add or Remove Snap-ins** dialog box, select **Certificates**, and then select **Add**.

d. In the **Certificates snap-in** dialog box, select **Computer account**, and then select **Next**.

e. In the **Select Computer** dialog box, keep the default **Local computer** selection, and then select **Finish**.

f. In the **Add or Remove Snap-ins** dialog box, select **OK**.

2. Import the certificate.

a. In the Microsoft Management Console, expand **Certificates > Trusted Root Certification Authorities**, right-click **Certificates**, and then select **All Tasks > Import**.

b. In the Certificate Import Wizard, specify the certificate file's full path, and then select **Next**.

c. Enter the password, and then select **Next**.

d. Specify the certificate store as **Trusted Root Certification Authorities**, and then select **Next**.

e. Select **Finish**.

Create and install a standalone managed service account or group managed service account

FactoryTalk AssetCentre version 11.00.00 and later support standalone managed service accounts (sMSA) and group managed service accounts (gMSA) that provide automatic password management, simplified service principal name (SPN) management, and the ability to delegate the management to other administrators.

Prerequisites

Make sure that:

- Your operating system is Windows Server 2012 R2 (patched with KB2998082) or later.
- Your SQL server is SQL Server 2014 or later.
- You have Active Directory module for Windows PowerShell installed on your computer.

To create and install a gMSA

1. On the domain controller computer, open the **Windows PowerShell** window.
2. To verify that the Key Distribution Service (KDS) Root Key for your domain controller is installed on your computer, enter *Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId*.
   If the returned value is *True*, it means that KDS Root Key is already installed.
   If the returned value is *False*, it means that there is no valid KDS Root Key. To add a KDS Root Key, enter *Add-KdsRootKey -EffectiveImmediately*.

   NOTE: It may take up to 10 hours to implement the function of the KDS Root Key.

3. To create an Active Directory (AD) Security Group, enter *New-ADGroup -Name <gsg_gmsa01> -Description "Security group for <gmsa01> computers" -GroupCategory Security -GroupScope Global*.

   Tip:
   - The "<>" means it is a variable. You can customize the name as needed.
   - Quotes are required for the name with space. For example, "gmsa 01".

4. To add computer objects to the AD Security group, enter *Add-ADGroupMember -Identity <gsg_gmsa01> -Members <winsql-0$>, <winsql-01$>*.

   NOTE: When adding the computer objects, it is required to add "$" after the computer account name and restart the computer.

5. To create a gMSA, enter *New-ADServiceAccount -Name <gmsa01> -PrincipalsAllowedToRetrieveManagedPassword <gsg_gmsa01> -Enabled:$true -DNSHostName ServerD.astest.com*.
6. On the FactoryTalk AssetCentre server computer, enter *Test-ADServiceAccount -Identity <gmsa01>* to test the gMSA. For some operating system, you need to restart the computer before entering the code.

To create and install an sMSA

1. On the domain controller computer, open the **Windows PowerShell** window.
2. To verify that the Key Distribution Service (KDS) Root Key for your domain controller is installed on your computer, enter *Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId*.
   If the returned value is *True*, it means that KDS Root Key is already installed.
   If the returned value is *False*, it means that there is no valid KDS Root Key. To add a KDS Root Key, enter *Add-KdsRootKey -EffectiveImmediately*.

   NOTE: It may take up to 10 hours to implement the function of the KDS Root Key.

3. To create an sMSA, enter *New-ADServiceAccount -Name <msa01> -Enabled:$true -Description "Manage Service Account for FTAC" -DisplayName <msa01> -RestrictToSingleComputer*

Tip:

- The "<>" means it is a variable. You can customize the name as needed.
- Quotes are required for the name with space. For example, "msa 01".
- Please pay attention to the space between the syntax.

4. On the FactoryTalk AssetCentre server computer, open the **Windows PowerShell** window, and then enter *Install-WindowsFeature RSAT-AD-PowerShell -ComputerName <winsql-01>* to install the Active Directory PowerShell module.

NOTE: The "<>" means it is a variable. That is the name of FactoryTalk AssetCentre server computer on which you will install the sMSA.

5. To install the sMSA, enter *Install-ADServiceAccount -Identity <msa01>*.
6. To test the sMSA, enter *Test-ADServiceAccount -Identity <msa01>*.
   An sMSA is only allowed for using on one computer. If you want to use it on another computer, enter *UnInstall-ADServiceAccount -Identity <msa01>*, and then install it on the computer as needed.

Steps to install the FactoryTalk AssetCentre Server

The Setup wizard installation process includes the following steps:

Step 1: Launch the Setup wizard and select what to install

Before starting the installation of FactoryTalk AssetCentre server, you should ensure:

- A standalone managed service account (sMSA) or group managed service account (gMSA) is required when the SQL Server is remote from the FactoryTalk AssetCentre sever.

NOTE: When SQL Server and FactoryTalk AssetCentre server are co-located, the system will automatically use a Windows virtual service account.

- Select **Windows Authentication**, when you install Microsoft SQL Server.

IMPORTANT:

- If you select **Mixed Mode** when installing Microsoft SQL Server, you can use SQL Server Authentication to access remote database.
- When using SQL Server Authentication, you must use silent or unattended setup to install FactoryTalk AssetCentre version 11.00.00 or later.

- A local Windows user account, a Windows Active Directory (AD) user account or a Windows AD group where your user account is a member has been assigned SQL Server system administrator role.

When installing FactoryTalk AssetCentre server, you can follow the steps as below:

NOTE: When installing FactoryTalk AssetCentre server and SQL Server database on the same computer, you can use a local Windows user account or an AD user account.

When you install FactoryTalk AssetCentre server and SQL Server database on different computers, only an AD user account can be used.

1. Log on to your computer as an administrator, or as a user with administrative privileges.
2. If necessary, close all open Windows programs, and then place the FactoryTalk AssetCentre Installation DVD in the computer's DVD drive.

   Tip: You can also select FactoryTalk AssetCentre Server to download the software from the Rockwell Automation Product Compatibility and Download Center.

3. Run **D:\setup.exe**, where **D:** is the drive containing the DVD.
4. Select **AssetCentre Server**.

   Tip: To install **AssetCentre Server**, **AssetCentre Desktop Client**, and **AssetCentre Agent** at the same time, select **AssetCentre Custom Installation**. Custom installation allows you to install more than one or all of the installation components.

5. Select **Customize**.
6. On the Customize page, the required software and components for FactoryTalk AssetCentre Server installation include:
   - **FactoryTalk Services Platform**
     - **FactoryTalk Directory Server Services**

       The FactoryTalk Directory Server Services include the FactoryTalk Reverse Proxy, the FactoryTalk Web Authentication Server, and the FactoryTalk Web Event Server. When selecting **AssetCentre Server** during installation, the FactoryTalk Directory Server Services will be selected by default. You can enable the FactoryTalk Directory Server Services as needed.
       - **FactoryTalk Reverse Proxy**

         The computer acting as the FactoryTalk AssetCentre server must also host FactoryTalk Reverse Proxy. You can install the FactoryTalk Reverse Proxy without installing the FactoryTalk Web Authentication Server and the FactoryTalk Web Event Server; the converse is not allowed.
       - **FactoryTalk Web Authentication Server**

         If your system requires the FactoryTalk Web Authentication Server, for example, to enable the use of the FactoryTalk AssetCentre version 13.00.00 Web Client, the computer acting as the FactoryTalk Directory server must also host the FactoryTalk Web Authentication Server. When selecting **FactoryTalk Web Authentication Server** during installation, the FactoryTalk Reverse Proxy will also be installed. There is no option to not install the FactoryTalk Reverse Proxy when installing the FactoryTalk Web Authentication Server.
       - **FactoryTalk Web Event Server**

         The FactoryTalk Web Event Server provides a FactoryTalk eventing subsystem based on Socket.IO rather than DCOM. There is no option to not install the FactoryTalk Reverse Proxy when installing the FactoryTalk Web Event Server.
   - **FactoryTalk Linx**
   - **FactoryTalk Alarms and Events**
   - **FactoryTalk Activation Manager**
   - **AssetCentre Server**

   The recommended software and components for FactoryTalk AssetCentre Server installation include:
   - **Register EDS Files**

     Register EDS Files will be installed to support devices browse.

- **FactoryTalk Updater Agent**

  To install the FactoryTalk Updater utility, expand **Tools** and then select **FactoryTalk Updater Agent**. It assists management of installed Rockwell Automation software by announcing new versions and patch roll-ups. Registering for updates is not required to receive announcements from the FactoryTalk Updater.

The optional software and components include:

- **FactoryTalk System Status Portal**
- **HistorianME Security Web Service**
- **Activation Websocket Service**

7. Select the location for the software. The default location is **C:**.
8. Select **Next**.
9. Select the directory type and then select **Next**.
   - **Standard**: Create an empty directory with unrestricted access.
   - **Secure**: Create a directory that contains the pre-configured access control lists which limit user access.

NOTE:

- If you select **Secure**, Step 2: Configure TLS setting on page 21 will be skipped and the **IIS Server Communication port** is set as 443 by default for HTTPS.
- This option is only presented during the setup of a new or greenfield FactoryTalk AssetCentre installation.

Step 2: Configure TLS setting

We recommend that you turn on HTTPS to secure the network. To use HTTPS, you must configure TLS certificate after installing FactoryTalk AssetCentre.

To configure TLS setting

1. On the **Configure AssetCentre Server** page, make sure the **Secure communication with TLS** check box is selected.
2. (optional) The **IIS Server Communication port** is set as 443 by default for HTTPS. If you don't want to use the default port, enter an unused port from 1025 through 49151 in the **IIS Server Communication port** box. Make sure to configure a Windows firewall rule for the modified port. For more information, see Configure a firewall rule if the default port is modified on page 69.

   If the HTTPS port was previously configured using FactoryTalk Services Platform, such as port 4356, then the existing HTTPS port setting is retained.

   If you need to change the **IIS Server Communication port** after installation, on the FactoryTalk AssetCentre server computer, select **Start** > **Rockwell Software** > **FactoryTalk AssetCentre Server Settings**.

Tip: If the specified port is blocked by the FactoryTalk AssetCentre Web Client supported browsers, you cannot access FactoryTalk AssetCentre Web Client. For more information about the browser blocked ports, see the following:

- Google Chrome: ChromeBlcokedPorts
- Microsoft Edge: EdgeBlockedPorts
- Mozilla Firefox: FirefoxBlockedPorts

If the **Secure communication with TLS** checkbox is not selected, the port number is set as 80 by default for HTTP, and you cannot configure the HTTP port.

WARNING: The potential risks of turning off HTTPS are as below:

- The data is transmitted without encryption across a network, which will cause leakage of information, if other solutions, such as IPSEC, are not used.
- The system may be vulnerable to a Remote Code Execution (RCE) attack.

3. Select **Next**.

Step 3: Configure the FactoryTalk AssetCentre Server

You can configure the FactoryTalk AssetCentre Server with a local or a remote database.

To configure the FactoryTalk AssetCentre Server

1. In the **Database Server** box, enter the name of the database server.
   - For the local database server
     If you selected the default instance during the Microsoft SQL Server installation, keep the default name of the database server as **(local)**.
     If you customized the instance during the Microsoft SQL Server installation, you need to enter the Fully Qualified Domain Name (FQDN) of the server. For example, *WIN-2B92QFPB9CO\SQLSERVERTEST*. *SQLSERVERTEST* is the customized instance name.
   - For the remote database server
     Enter the name of a remote database server, or in the Location list, choose the location of the remote database server you ever used.

     IMPORTANT: The default port used for SQL Server communication is 1433. If you want to change the SQL Server port, you must add the port number after the SQL Server name during installation. For example, *mySQLServer,1526*. The comma (,) is required.
     You must ensure that the port is not in use by any other application, service, or process in your system.

2. Select **Next**.
3. On the Configure AssetCentre Server database page, select **Install**.
   When the SQL Server is remote from the FactoryTalk AssetCentre Server, do the following:
   a. On the Configure AssetCentre Server database page, select **Browse**.
   b. In the **Select Service Account** dialog box, select **Advanced**, and then select **Find Now**.
   c. In the **Search results** box, select the sMSA or gMSA created, and then select **OK**.
   d. On the Configure AssetCentre Server database page, select **Install**.

   NOTE: If you turn on TLS for secure communication within the FactoryTalk AssetCentre system and use a self-signed certificate, you need to enter the Fully Qualified Domain Name (FQDN) of the Database Server.

Step 4: Read and accept license agreements

End-user license agreements (EULA) spell out your rights and responsibilities. Depending on the components being installed, there may be more than one license agreement on this page. The individual license agreements are listed above the text box.

Some software products may be delivered or made available only after you agree to the terms and conditions of each of the license agreements.

1. On the **End User License Agreements** page, select each agreement and read the agreement carefully.
2. When all license agreements have been read, select **Accept All**.

Step 5: Start the installation

After accepting the license agreements, the Setup wizard automatically installs all the Rockwell Software applications selected previously. No further user input is required.

Step 6: Finish the installation

After the installation completes, you need to activate the software for its full feature capabilities. You can activate the software now or later.

- To activate the installed software, select **Activate your software,** and then select **Next**.

  The **Software Activation** dialog box opens.

  a. In the **Serial number** box, enter the serial number.
  b. In the **Product key** box, enter the product key.
  c. Select the earliest version you will use.
  d. Select **Activate locally** or **Activate using a dongle**.
  e. Click **Continue**.

     You will be prompted to restart the computer after the activation.
- To finish the installation without activation, select **Skip activation**, and then select **Next**.
  - To view the installation details, select **Installation Summary**.
  - To receive the latest product updates and patch notification, select **Register for updates**.
  - To install the latest version of Adobe® Acrobat® Reader®, select **Download it free** and follow the on-screen instructions.

    Restart the computer to complete the installation.

After installation of FactoryTalk AssetCentre Server software

Select FactoryTalk Directory Server

If the FactoryTalk AssetCentre Server is not also the system's FactoryTalk Directory Server, you must change the FactoryTalk AssetCentre Server to use the computer that hosts the FactoryTalk Directory use the **Specify FactoryTalk Directory location** utility. After changing the FactoryTalk Directory Server to the remote computer, you must perform the following steps:

a. On the FactoryTalk AssetCentre Server computer, select **Start** > **Rockwell Software** > **FactoryTalk AssetCentre Server Settings** to launch the server configuration utility.

   From FactoryTalk AssetCentre v13.00.00, the Server Settings utility is renamed to FactoryTalk AssetCentre Server Settings.
b. Use the **Specify FactoryTalk Directory location** utility to verify if the AssetCentre Server fully qualified domain name (FQDN) is entered in the **Server Location**.
c. Configure **Use the secure communication channel**, that is, perform encryption of communication between the server, agent(s), and client(s) using TLS.
   - When **Use the secure communication channel** is selected, the IIS Server is configured to use port 443.
   - When **Use the secure communication channel** is not selected, the IIS Server is configured to use port 80.

HTTPS configuration

If you have HTTPS turned on during the installation of FactoryTalk AssetCentre, you must Configure the TLS protocol for FactoryTalk AssetCentre on page 68. We recommend that you use a TLS certificate signed by a certificate authority (CA) to secure the communication.

Install the latest FactoryTalk AssetCentre patches

For more information about the latest FactoryTalk AssetCentre patches, see Knowledgebase Document ID: QA15600 - FactoryTalk AssetCentre Patch Roll-up for 3.0 and later.

Install the FactoryTalk AssetCentre Agent software

This chapter describes:

Before you install the FactoryTalk AssetCentre Agent software

Agents are programs that communicate with the FactoryTalk AssetCentre Server and perform scheduled tasks on behalf of the FactoryTalk AssetCentre Server. Agents allow work to be distributed and shared among multiple computers to spread processing load and speed up operations. When a server needs an agent to perform a task, it locates the computer running the operation and assigns the task to that agent. The agent then reports the task's completion to the server. The Search feature, as well as purchased capabilities, such as Disaster Recovery capabilities, require the use of agents to perform scheduled operations.

Where to install the FactoryTalk AssetCentre Agent software

We recommend that you install FactoryTalk AssetCentre Agent software on the workstation:

- Being capable of running the Agent software (see Agent computer requirements on page 10).
- In the same network as the FactoryTalk AssetCentre Server.
- Running the FactoryTalk AssetCentre Server.

If scheduled operations are taking longer than desired to complete, you may need install more Disaster Recovery agents. To estimate the number of necessary FactoryTalk AssetCentre agents in your system, see Knowledgebase Document ID: IN29429 - Determining the Necessary Number of FactoryTalk AssetCentre Agents.

You can use the FactoryTalk AssetCentre Agent Controller Launch Control Panel to start the agent controller application automatically following a restart of the computer.

The agent computer MUST have the appropriate RSLogix family software for your devices to perform Disaster Recovery functions.

Steps to install the FactoryTalk AssetCentre Agent software

The Setup wizard installation process includes the following steps:

Step 1: Launch the Setup wizard and select what to install

You must have the appropriate Rockwell Automation software for your devices installed on the agent computer to run Disaster Recovery schedules.

You can install the agent using either the installation package or the FactoryTalk AssetCentre server website.

To install a FactoryTalk AssetCentre agent using the installation package

1. Log on to your computer as an administrator, or as a user with administrative privileges.
2. If necessary, close all open Windows programs, and then place the FactoryTalk AssetCentre Installation DVD in the computer's DVD drive.

Tip: You can also select FactoryTalk AssetCentre Server to download the software from the Rockwell Automation Product Compatibility and Download Center.

3. Run **D:\setup.exe**, where **D:** is the drive containing the DVD.
4. Select **AssetCentre Agent**.

Tip: To install **AssetCentre Server**, **AssetCentre Desktop Client**, and **AssetCentre Agent** at the same time, select **AssetCentre Custom Installation**. Custom installation allows you to install more than one or all of the installation components.

5. To install all components available in the selected software using the recommended settings, select **Install now** and skip to Step 2: Read and accept license agreements on page 26.
6. To select which components to install, select **Customize**.
7. On the **Customize** page, the required software and components for FactoryTalk AssetCentre Agent installation include:
   - **FactoryTalk Services Platform**
   - **FactoryTalk Linx**
   - **FactoryTalk Alarms and Events**
   - **FactoryTalk Activation Manager**
   - **AssetCentre Agent**
     - **Siemens Connector**

       By default, the checkbox is not selected. If you need to manage the Siemens controllers in your system, select this checkbox.
     - **Mitsubishi Connector**

       By default, the checkbox is not selected. If you need to manage the Mitsubishi controllers in your system, select this checkbox.

       IMPORTANT:
       - It is recommended that you install the Siemens S7 Controller (TIA Portal) before installing the FactoryTalk AssetCentre Agent. If you install the Siemens S7 Controller (TIA Portal) after installing the FactoryTalk AssetCentre Agent, further configurations are required to make them work correctly, see FactoryTalk AssetCentre Agent Controller Launch Control Panel in *FactoryTalk AssetCentre Client Help*.
       - When selecting either the Siemens or Mitsubishi connector, the FactoryTalk AssetCentre AgentController *must* run as an Application and you have to provide a Windows user later during the installation process.
       - If you select the checkbox for Mitsubishi Connector or Siemens Connector, FIPS *must* be disabled for communication to work properly.
   - **RSLinx Classic**

   The recommended software and components for FactoryTalk AssetCentre Agent installation include:
   - **Register EDS Files**

     Register EDS Files will be installed to support devices browse.
   - **Logix Designer Compare Tool**
   - **RSLogix 5**
   - **RSLogix 500**
   - **FactoryTalk View ME Transfer Utility**
   - **FactoryTalk Updater Agent**

     To install the FactoryTalk Updater utility, expand **Tools** and then select **FactoryTalk Updater Agent**. It assists management of installed Rockwell Automation software by announcing new versions and patch roll-ups. Registering for updates is not required to receive announcements from the FactoryTalk Updater.

The optional software and components include:

- **FactoryTalk Directory Server Services**

  The FactoryTalk Directory Server Services include the FactoryTalk Reverse Proxy, the FactoryTalk Web Authentication Server, and the FactoryTalk Web Event Server. When selecting **AssetCentre Server** during installation, the FactoryTalk Directory Server Services will be selected by default. You can enable the FactoryTalk Directory Server Services as needed.

  - **FactoryTalk Reverse Proxy**

    The computer acting as the FactoryTalk AssetCentre server must also host FactoryTalk Reverse Proxy. You can install the FactoryTalk Reverse Proxy without installing the FactoryTalk Web Authentication Server and the FactoryTalk Web Event Server; the converse is not allowed.
  - **FactoryTalk Web Authentication Server**

    If your system requires the FactoryTalk Web Authentication Server, for example, to enable the use of the FactoryTalk AssetCentre version 13.00.00 Web Client, the computer acting as the FactoryTalk Directory server must also host the FactoryTalk Web Authentication Server. When selecting **FactoryTalk Web Authentication Server** during installation, the FactoryTalk Reverse Proxy will also be installed. There is no option to not install the FactoryTalk Reverse Proxy when installing the FactoryTalk Web Authentication Server.
  - **FactoryTalk Web Event Server**

    The FactoryTalk Web Event Server provides a FactoryTalk eventing subsystem based on Socket.IO rather than DCOM. There is no option to not install the FactoryTalk Reverse Proxy when installing the FactoryTalk Web Event Server.
  - **FactoryTalk System Status Portal**
- **HistorianME Security Web Service**
- **Activation Websocket Service**
- **Enable Security**

  When using FactoryTalk AssetCentre to work with RSLogix 5 or RSLogix 500 to do Disaster Recovery schedule and the RSLogix editors have been secured, you have to select the **Enable Security** check box.
- **SmartGuardUSB - KernelDrivers**

8. Select the location for the software. The default location is **C:**.
9. Select **Next**.
10. (optional) If you have selected Siemens Connector or Mitsubishi Connector in **Step 7**, enter a Windows user account with standard user permission or select **Browse** to select the user that you want to use to run the Agent Controller. Select **OK**, and then select **Next**.
11. In the **Security options** box, select the options for RSLogix 5 as needed. If you do not want to use FactoryTalk Security, clear the **Enable FactoryTalk® Security** check box.

    NOTE: For more information about the RSLogix 5 installation, refer to *RSLogix 5 Getting Results Guid*e.
12. Select **Next**.
13. In the **Security options** box, select the options for RSLogix 500 as needed. If you do not want to use FactoryTalk Security, clear the **Enable FactoryTalk® Security** check box.

    NOTE: For more information about the RSLogix 500 installation, refer to *RSLogix 500 Getting Results Guide*.
14. Select **Install**.

Step 2: Read and accept license agreements

End-user license agreements (EULA) spell out your rights and responsibilities. Depending on the components being installed, there may be more than one license agreement on this page. The individual license agreements are listed above the text box.

Some software products may be delivered or made available only after you agree to the terms and conditions of each of the license agreements.

1. On the **End User License Agreements** page, select each agreement and read the agreement carefully.
2. When all license agreements have been read, select **Accept All**.

Step 3: Start the installation

After accepting the license agreements, the Setup wizard automatically installs all the Rockwell Software applications selected previously. No further user input is required.

Step 4: Finish the installation

To make sure the settings are fully configured, you must restart the computer by selecting the **Restart now** or **Restart later** button that appears on the complete page.

IMPORTANT:

- If you don't select the **Restart now** or **Restart later** button during the installation and close the installation dialog or manually restart your computer, the Agent Controller will run as a service and log on as "Local System". However, automatic permission changes that occur when you click **Restart now** or **Restart later** are not executed, preventing the Agent's proper operation. You must configure these permissions by running the **FactoryTalk AssetCentre Agent Controller Launch Control Panel** from **Start** > **Rockwell Software**.
  By default, the Agent Controller runs as a service. On **Agent Controller Launch Control Panel**:
  - If you want Agent Controller to keep running as a service, select **Repair**.
  - If you selected either the Siemens or Mitsubishi connector during **Step 1**, the Agent Controller mode must be run as an application:
    a. Switch to start agent as an application.
    b. Specify a Windows user account with standard user permissions to run the Agent Controller.
    c. Select **Save**.
- It will take several seconds for the system to restart after clicking **Restart Now**. During this time, do not manually shut down or restart your computer.

After installation of FactoryTalk AssetCentre Agent software

HTTPS configuration

If you have HTTPS turned on during the installation of FactoryTalk AssetCentre, you must Configure the TLS protocol for FactoryTalk AssetCentre on page 68. We recommend that you use a TLS certificate signed by a certificate authority (CA) to secure the communication.

Install the latest FactoryTalk AssetCentre patches

For more information about the latest FactoryTalk AssetCentre patches, see Knowledgebase Document ID: QA15600 - FactoryTalk AssetCentre Patch Roll-up for 3.0 and later.

Install the FactoryTalk AssetCentre Desktop Client software

This chapter describes:

Before you install FactoryTalk AssetCentre Desktop Client software

The FactoryTalk AssetCentre Desktop Client software provides the user interface for FactoryTalk AssetCentre. It is through the client that you perform tasks such as checking files in and out, creating and running scheduled events, and viewing logs. For more information on what you can do with FactoryTalk AssetCentre Desktop Client software, see the *FactoryTalk AssetCentre Help* after the desktop client is installed.

Install the FactoryTalk AssetCentre Desktop Client software on all computers on which you want to use FactoryTalk AssetCentre.

The desktop client is not required on the FactoryTalk AssetCentre server computer, but you can install it on the server if desired.

Where to install FactoryTalk AssetCentre Desktop Client software

NOTE:

For current information on the system requirements for the FactoryTalk AssetCentre software, see FactoryTalk AssetCentre Release Notes and the Product Compatibility and Download Center.

Install the desktop client on any computer

- From which you want to access the FactoryTalk AssetCentre Desktop Client software (to edit the representation of your assets, to view logs, to create schedules, to search the logs, and so on).
- That is capable of running the FactoryTalk AssetCentre Desktop Client software (see Client computer requirements on page 9).
- That is connected to the FactoryTalk AssetCentre Server.
- From which FactoryTalk audits are desired.

NOTE: The Disaster Recovery capability provides the ability to schedule a comparison between master files, and processor program and data files. To edit the file and data settings for a compare operation for Allen-Bradley PLC-5, SLC 500, or MicroLogix controllers, you must have RSLogix 5, or RSLogix 500 software installed on the client computer.

Steps to install FactoryTalk AssetCentre Desktop Client software

The Setup wizard installation process includes the following steps:

Step 1: Launch the Setup wizard and select what to install

You can install the desktop client using either the installation package.

To install a FactoryTalk AssetCentre Desktop Client software using the installation package

1. Log on to your computer as an administrator, or as a user with administrative privileges.
2. If necessary, close all open Windows programs, and then place the FactoryTalk AssetCentre Installation DVD in the computer's DVD drive.

   Tip: You can also select FactoryTalk AssetCentre Server to download the software from the Rockwell Automation Product Compatibility and Download Center.

3. Run **D:\setup.exe**, where **D:** is the drive containing the DVD.
4. Select **AssetCentre Desktop Client**.

   Tip: To install **AssetCentre Server**, **AssetCentre Desktop Client**, and **AssetCentre Agent** at the same time, select **AssetCentre Custom Installation**. Custom installation allows you to install more than one or all of the installation components.

5. To install all components available in the selected software using the recommended settings, click **Install now** and skip to Step 2: Read and accept license agreements on page 30.
6. To select which components to install, click **Customize**.
7. On the **Customize** page:

   The required software and components for FactoryTalk AssetCentre Desktop Client installation include:

   - **FactoryTalk Services Platform**
   - **FactoryTalk Linx**
   - **FactoryTalk Alarms and Events**
   - **FactoryTalk Activation Manager**
   - **AssetCentre Client**
   - **RSLinx Classic**

   The recommended software and components for FactoryTalk AssetCentre Desktop Client installation include:

   - **3rd party editor integration**

     Step7 Version 5.6 sp1

     If the installation detects the Step7 editor file (S7tgtopx.exe) at either of the following paths, you can choose to select **Step7 Version 5.6 sp1** and install the feature. If you have the Step7 editor file installed, make sure they are located at either of the following paths for the installation to detect.

     - C:\Siemens\Step7\s7bin
     - C:\Program Files\Siemens\Step7\s7bin or C:\Program Files (x86)\Siemens\Step7\s7bin

     Tip: If you have Siemens S7 Controllers (STEP7), you may also need to install the Step7 feature. This step is not required for Disaster Recovery actions, it merely associates project files with the appropriate editor.

     You can install the Step7 feature at this point or install it after the installation. To install it after installing FactoryTalk AssetCentre Desktop Client:

     a. Run **setup.exe** in the installation package.
     b. Select **AssetCentre Desktop Client** and click **Modify**.
     c. Expand **AssetCentre Client** and select **Step7 Version 5.6 sp1**.
     d. Click **Modify**.

   - **Register EDS Files**

     Register EDS Files will be installed to support devices browse.

- **FactoryTalk Updater Agent**

  To install the FactoryTalk Updater utility, expand **Tools** and then select **FactoryTalk Updater Agent**. It assists management of installed Rockwell Automation software by announcing new versions and patch roll-ups. Registering for updates is not required to receive announcements from the FactoryTalk Updater.

The optional software and components include:

- **FactoryTalk Directory Server Services**

  The FactoryTalk Directory Server Services include the FactoryTalk Reverse Proxy, the FactoryTalk Web Authentication Server, and the FactoryTalk Web Event Server. When selecting **AssetCentre Server** during installation, the FactoryTalk Directory Server Services will be selected by default. You can enable the FactoryTalk Directory Server Services as needed.

  - **FactoryTalk Reverse Proxy**

    The computer acting as the FactoryTalk AssetCentre server must also host FactoryTalk Reverse Proxy. You can install the FactoryTalk Reverse Proxy without installing the FactoryTalk Web Authentication Server and the FactoryTalk Web Event Server; the converse is not allowed.
  - **FactoryTalk Web Authentication Server**

    If your system requires the FactoryTalk Web Authentication Server, for example, to enable the use of the FactoryTalk AssetCentre version 13.00.00 Web Client, the computer acting as the FactoryTalk Directory server must also host the FactoryTalk Web Authentication Server. When selecting **FactoryTalk Web Authentication Server** during installation, the FactoryTalk Reverse Proxy will also be installed. There is no option to not install the FactoryTalk Reverse Proxy when installing the FactoryTalk Web Authentication Server.
  - **FactoryTalk Web Event Server**

    The FactoryTalk Web Event Server provides a FactoryTalk eventing subsystem based on Socket.IO rather than DCOM. There is no option to not install the FactoryTalk Reverse Proxy when installing the FactoryTalk Web Event Server.
  - **FactoryTalk System Status Portal**
- **HistorianME Security Web Service**
- **Activation Websocket Service**
- **Enable Security**

  When using FactoryTalk AssetCentre to work with RSLogix 5 or RSLogix 500 to do Disaster Recovery schedule and the RSLogix editors have been secured, you have to select the **Enable Security** check box.
- **SmartGuardUSB - KernelDrivers**

8. Select the location for the software. The default location is **C:**.
9. Select **Install**.

Step 2: Read and accept license agreements

End-user license agreements (EULA) spell out your rights and responsibilities. Depending on the components being installed, there may be more than one license agreement on this page. The individual license agreements are listed above the text box.

Some software products may be delivered or made available only after you agree to the terms and conditions of each of the license agreements.

1. On the **End User License Agreements** page, select each agreement and read the agreement carefully.
2. When all license agreements have been read, select **Accept All**.

Step 3: Start the installation

After accepting the license agreements, the Setup wizard automatically installs all the Rockwell Software applications selected previously. No further user input is required.

Step 4: Finish the installation

Restart the computer to complete the installation.

After installation of FactoryTalk AssetCentre Desktop Client software

HTTPS configuration

If you have HTTPS turned on during the installation of FactoryTalk AssetCentre, you must Configure the TLS protocol for FactoryTalk AssetCentre on page 68. We recommend that you use a TLS certificate signed by a certificate authority (CA) to secure the communication.

Install the latest FactoryTalk AssetCentre patches

For more information about the latest FactoryTalk AssetCentre patches, see Knowledgebase Document ID: QA15600 - FactoryTalk AssetCentre Patch Roll-up for 3.0 and later.

Custom install the FactoryTalk AssetCentre software

FactoryTalk AssetCentre supports custom installation of the FactoryTalk AssetCentre software. Custom installation allows you to install more than one or all of the installation components, including **AssetCentre Server**, **AssetCentre Desktop Client**, and **AssetCentre Agent**.

Before starting the installation of FactoryTalk AssetCentre system, you should ensure that:

FactoryTalk AssetCentre Server

- Select **Windows Authentication**, when you install Microsoft SQL Server.

  IMPORTANT:
  - If you select **Mixed Mode** when installing Microsoft SQL Server, you can use SQL Server Authentication to access remote database.
  - When using SQL Server Authentication, you must use silent or unattended setup to install FactoryTalk AssetCentre version 11.00.00 or later.

- If you will configure the FactoryTalk AssetCentre Server to use a remote SQL database, ensure that a standalone managed service account or a group managed service account has been created in your Windows Active Directory.
- Ensure that the Windows account of the user performing the installation, or a Windows group of which the user performing the installation is a member, is assigned the Microsoft SQL Server System Administrator role before attempting the installation.

FactoryTalk AssetCentre Agent

- You must have the appropriate Rockwell Automation software for your devices installed on the agent computer to run Disaster Recovery schedules.

To perform a custom installation of FactoryTalk AssetCentre

1. Log on to your computer as an administrator, or as a user with administrative privileges.
2. If necessary, close all open Windows programs, and then place the FactoryTalk AssetCentre Installation DVD in the computer's DVD drive.

   Tip: You can also select FactoryTalk AssetCentre Server to download the software from the Rockwell Automation Product Compatibility and Download Center.

3. Run **D:\setup.exe**, where **D:** is the drive containing the DVD.
4. Select **AssetCentre Custom Installation**.
5. Select **Customize**.
6. On the **Customize** page, select the components. There may be three options shown:
   - **Mandatory** (grayed-out and selected check box) indicates software that will be automatically installed as part of the selected application.
   - **Recommended** (selected check box) indicates software that Rockwell recommends for the application. You may decide to clear the check box, so the software does not install.
   - **Optional** (clear check box) indicates software that you may wish to include depending on your system. Select the box to include the software during installation.

     For more information about the components' installation, refer to
   - Steps to install the FactoryTalk AssetCentre Server software on page 19
   - Steps to install the FactoryTalk AssetCentre Agent software on page 24
   - Steps to install the FactoryTalk AssetCentre Desktop Client software on page 28
7. Select the location for the software. The default location is **C:**.
8. Select **Next**.
9. Follow the on-screen instructions to complete the installation.

When configuring FactoryTalk AssetCentre Server database, you need to pay attention to the potential security risks of turning off HTTPS.

WARNING: We recommend that you turn on HTTPS. The potential security risks of turning off HTTPS are as below:

- The data is transmitted without encryption across a network, which will cause leakage of information, if other solutions, such as IPSEC, are not used.
- The system may be vulnerable to a Remote Code Execution (RCE) attack.

  For more information on the installation of theFactoryTalk AssetCentre Server, refer to Install the FactoryTalk AssetCentre Sever software on page 14.

  For more information on the installation of the FactoryTalk AssetCentre Agent, refer to Install the FactoryTalk AssetCentre Agent software on page 24.

  For more information on the installation of the FactoryTalk AssetCentre Desktop Client, refer to Install the FactoryTalk AssetCentre Desktop Client software on page 28.

After the installation of FactoryTalk AssetCentre software

- **HTTPS configuration**

  If you have HTTPS turned on during the installation of FactoryTalk AssetCentre, you must Configure the TLS protocol for FactoryTalk AssetCentre on page 68. We recommend that you use a TLS certificate signed by a certificate authority (CA) to secure the communication.
- **Install the latest FactoryTalk AssetCentre patches**

  For more information about the latest FactoryTalk AssetCentre patches, see Knowledgebase Document ID: QA15600 - FactoryTalk AssetCentre Patch Roll-up for 3.0 and later.

Install the AssetCentre Diagnostics Connector

If you want the Event and Audit information generated by other Rockwell Automation software products in the same FactoryTalk Directory to be recorded in the FactoryTalk AssetCentre database without installing the full FactoryTalk AssetCentre Desktop Client, install the AssetCentre Diagnostics Connector. The AssetCentre Diagnostics Connector includes only those FactoryTalk AssetCentre components that are necessary to send the Event and Audit log the AssetCentre database.

A typical use of this feature is to send audit records from a FactoryTalk View Site Edition client to the Factory Talk AssetCentre database without installing the full FactoryTalk AssetCentre Desktop Client.

Steps to install the AssetCentre Diagnostics Connector

The Setup wizard installation process includes the following steps:

- Step 1: Launch the Setup wizard and select what to install on page 34
- Step 2: Read and accept license agreements on page 34
- Step 3: Start the installation on page 35
- Step 4: Finish the installation on page 35

Step 1: Launch the Setup wizard and select what to install

1. Log on to your computer as an administrator, or as a user with administrative privileges.
2. If necessary, close all open Windows programs, and then place the FactoryTalk AssetCentre Installation DVD in the computer's DVD drive.

Tip: You can also select FactoryTalk AssetCentre Server to download the software from the Rockwell Automation Product Compatibility and Download Center.

3. Run **D:\setup.exe**, where **D:** is the drive containing the DVD.
4. Select **AssetCentre Diagnostics Connector (Optional)**.
5. To install all components available in the selected component using the recommended settings, click **Install now** and skip to Step 2: Read and accept license agreements on page 34.
6. To select which components to install, select **Customize**.
7. On the **Customize** page:
   - **AssetCentre Common Components** are what you need to install as the diagnostics connector.
8. Select the location for the software. The default location is **C:**.
9. Select **Install**.

Step 2: Read and accept license agreements

End-user license agreements (EULA) spell out your rights and responsibilities. Depending on the components being installed, there may be more than one license agreement on this page. The individual license agreements are listed above the text box.

Some software products may be delivered or made available only after you agree to the terms and conditions of each of the license agreements.

1. On the **End User License Agreements** page, select each agreement and read the agreement carefully.
2. When all license agreements have been read, select **Accept All**.

Step 3: Start the installation

After accepting the license agreements, the Setup wizard automatically installs all the Rockwell Software applications selected previously. No further user input is required.

Step 4: Finish the installation

Restart the computer to complete the installation.

Upgrade FactoryTalk AssetCentre

If you upgrade from a previous version of FactoryTalk AssetCentre, use the following steps to upgrade from FactoryTalk AssetCentre versions 7.00.00 and later to version 13.00.00.

- To upgrade an RSMACC system to FactoryTalk AssetCentre, follow the instructions in Knowledgebase Document ID: IN3311 - Upgrade an existing RSMACC system to FactoryTalk AssetCentre.
- To upgrade FactoryTalk AssetCentre version 7.00.00 or earlier, you have to first upgrade to version 7.00.00, and then use the following steps to upgrade from version 7.00 to version 13.00.00.

Important information related to upgrading

Please take note of these considerations when upgrading a FactoryTalk AssetCentre system:

- To ensure a successful FactoryTalk AssetCentre Server installation, you must make sure the FactoryTalk Directory Server is running the correct software version and is available before attempting the FactoryTalk AssetCentre Server installation. Otherwise, the upgrading of FactoryTalk AssetCentre Server will fail.
- When upgrading FactoryTalk AssetCentre to version 10.00.00 and later, the **FactoryTalk AssetCentre VerificationAgent** service is forcibly set to operate using the LocalSystem service account. If the previous service configuration was using a Windows user account, such as AssetCentre_DR, then use the **FactoryTalk AssetCentre Agent Controller Launch Control Panel** to re-configure the **FactoryTalk AssetCentre Agent** services.
- After upgrading from a previous version of FactoryTalk AssetCentre to version 13.00.00, you *must* manually clear your browser's cache to successfully use the FactoryTalk AssetCentre Web Client.
- When upgrading from a previous version of FactoryTalk AssetCentre, your customized settings will be kept.
  When repairing a FactoryTalk AssetCentre installation, your customized settings will be restored to the default.
- In rare situations, especially on low-performance computers, a dialog box may open during the installation when upgrading FactoryTalk AssetCentre. The dialog box indicates that the FactoryTalk AssetCentre server service needs to be stopped. If you use the unattended setup to upgrade FactoryTalk AssetCentre, you need to click **Yes** to stop the service or click **No** to cancel the installation.

The following information is very important for users upgrading to FactoryTalk AssetCentre version 10.00.00 and later. Starting from FactoryTalk AssetCentre version 10.00.00, process device capabilities are not supported.

IMPORTANT: After upgrading to FactoryTalk AssetCentre version 10.00.00 and later from earlier versions, you will no longer be able to use Process Device Configuration and Calibration Management functionality.

After upgrading from FactoryTalk AssetCentre version 9.00.00 or earlier to version 10.00.00 and later, General DTM Device, Equipment, Instrument, Loop, System, and Test Instrument process devices are not available in the asset catalog. The Process Device Configuration Field Edition, ProcalV5 Data Source Configuration, and Procal DB Connector Installer will be removed.

If Process Device Configuration is required for your system, Rockwell Automation recommends you consider Endress+Hauser FieldCare. Endress+Hauser FieldCare SFE500 is a comprehensive tool for managing process instruments from Device Setup to Plant Asset Management. FieldCare can be used with instruments communicating via Profibus-PA, Foundation Fieldbus, and HART.

All calibration records and information are retained in ProCalV5, thus the previously existing process device assets will be displayed in the asset tree. You can still cut, copy, and paste the existing process devices in the asset tree. However, their hardware and asset properties will be disabled. The ProCalV5 Company and ProCalV5 Linked Item properties of Instrument, Equipment, Loop, System, and Test Instrument are removed from the asset properties dialog box. Process devices will still consume the capacity activation. If you are still owning FactoryTalk AssetCentre Calibration Management, we recommend you contacting the following vendors for more solutions:

- Prime Technologies (https://www.primetechpa.com/)
- CompuCal (https://compucalcalibrations.com/)

Upgrade to a new version of FactoryTalk AssetCentre retaining existing database server

To upgrade FactoryTalk AssetCentre to version 11.00.00 or later with a new database server, AssetCentre server will be configured with Windows service accounts (virtual accounts, standalone managed service accounts, and group managed service accounts), or SQL Server accounts.

IMPORTANT: To upgrade FactoryTalk AssetCentre to version 11.00.00 or later with SQL Server Authentication, FactoryTalk AssetCentre installer will create AssetCentreUser and AsseCentreDBMaintenance forupgrading.

You must use silent or unattended setup to install it and know the risks of SQL Server Authentication:

- The number of failed sign-in attempts from attackers will cause a user account to be locked.
- The encrypted SQL Server Authentication login password, must be passed over the network at the time of the connection. Some applications that connect automatically will store the password at the client. These are additional attack points.
- Windows offers additional password policies that are not available for SQL Server logins.

If you turn on TLS for secure communication within the FactoryTalk AssetCentre system, you must also configure a certificate for encrypted connection between the SQL Server and the FactoryTalk AssetCentre Server computer when the SQL Server is not installed on the FactoryTalk AssetCentre Server computer. For more information, see Configure the certificate for encrypted connection to the database on page 16.

To configure TLS setting

1. On the **Configure AssetCentre Server** page, make sure the **Secure communication with TLS** check box is selected.
2. (optional) The **IIS Server Communication port** is set as 443 by default for HTTPS. If you don't want to use the default port, enter an unused port from 1025 through 49151 in the **IIS Server Communication port** box. Make sure to configure a Windows firewall rule for the modified port. For more information, see Configure a firewall rule if the default port is modified on page 69.
   If the HTTPS port was previously configured using FactoryTalk Services Platform, such as port 4356, then the existing HTTPS port setting is retained.
   If you need to change the **IIS Server Communication port** after installation, on the FactoryTalk AssetCentre server computer, select **Start** > **Rockwell Software** > **FactoryTalk AssetCentre Server Settings**.

   Tip: If the specified port is blocked by the FactoryTalk AssetCentre Web Client supported browsers, you cannot access FactoryTalk AssetCentre Web Client. For more information about the browser blocked ports, see the following:
   - Google Chrome: ChromeBlcokedPorts
   - Microsoft Edge: EdgeBlockedPorts
   - Mozilla Firefox: FirefoxBlockedPorts

   If the **Secure communication with TLS** checkbox is not selected, the port number is set as 80 by default for HTTP, and you cannot configure the HTTP port.

   WARNING: The potential risks of turning off HTTPS are as below:
   - The data is transmitted without encryption across a network, which will cause leakage of information, if other solutions, such as IPSEC, are not used.
   - The system may be vulnerable to a Remote Code Execution (RCE) attack.
3. Select **Next**.

To configure the FactoryTalk AssetCentre Server

1. In the **Database Server** box, enter the name of the database server.
   - For the local database server

     If you selected the default instance during the Microsoft SQL Server installation, keep the default name of the database server as **(local)**.

     If you customized the instance during the Microsoft SQL Server installation, you need to enter the Fully Qualified Domain Name (FQDN) of the server. For example, *WIN-2B92QFPB9CO\SQLSERVERTEST*. *SQLSERVERTEST* is the customized instance name.
   - For the remote database server

     Enter the name of a remote database server, or in the Location list, choose the location of the remote database server you ever used.

     IMPORTANT: The default port used for SQL Server communication is 1433. If you want to change the SQL Server port, you must add the port number after the SQL Server name during installation. For example, *mySQLServer,1526*. The comma (,) is required.

     You must ensure that the port is not in use by any other application, service, or process in your system.
2. Select **Next**.
3. On the Configure AssetCentre Server database page, select **Install**.

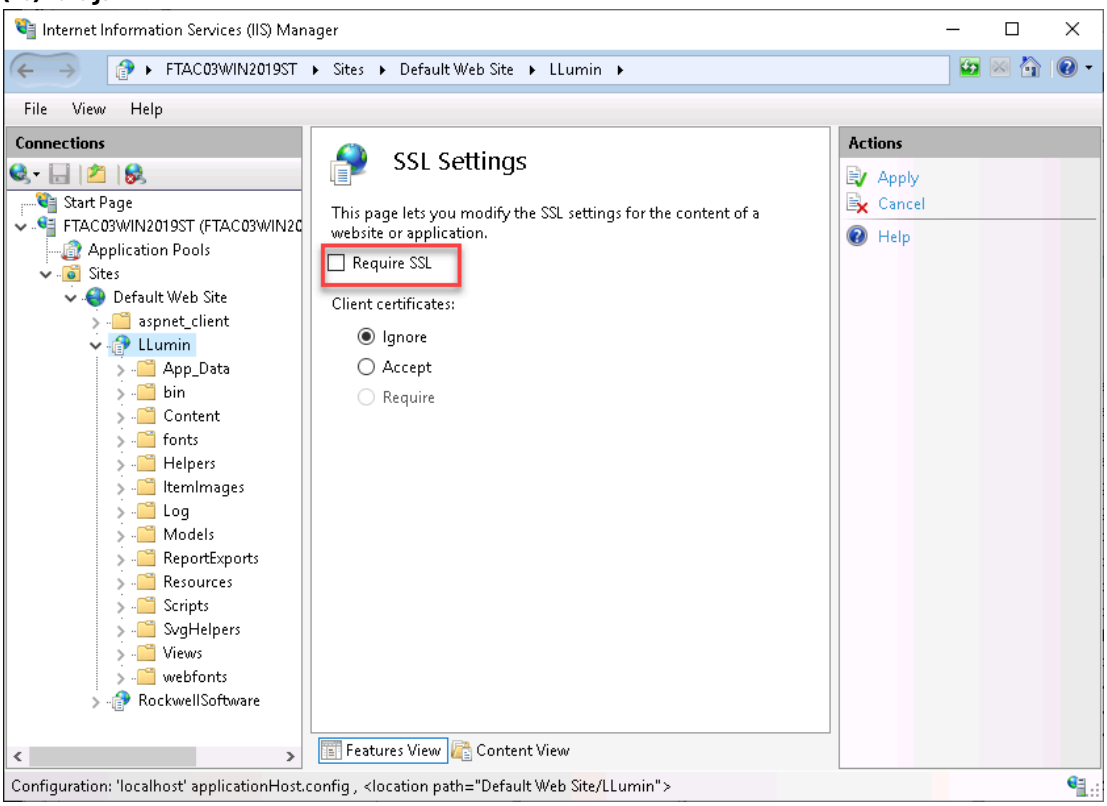
   When the SQL Server is remote from the FactoryTalk AssetCentre Server, do the following:
   a. On the Configure AssetCentre Server database page, select **Browse**.
   b. In the **Select Service Account** dialog box, select **Advanced**, and then select **Find Now**.
   c. In the **Search results** box, select the sMSA or gMSA created, and then select **OK**.
   d. On the Configure AssetCentre Server database page, select **Install**.

   NOTE: If you turn on TLS for secure communication within the FactoryTalk AssetCentre system and use a self-signed certificate, you need to enter the Fully Qualified Domain Name (FQDN) of the Database Server.

For more information, see Step 3: Configure the FactoryTalk AssetCentre Server on page 22.

After upgrading to FactoryTalk AssetCentre to version 11.00.00 or later and the HTTPS is turned on, you can do the following:

- If the TLS certificate is already configured on your computer, it is recommended to select the **Require SSL** check box through **Internet Information Services (IIS) Manager**.



- If the TLS certificate is not configured, you must Configure the TLS protocol for FactoryTalk AssetCentre on page 68. We recommend that you select the **Require SSL** check box through **Internet Information Services (IIS) Manager**.

IMPORTANT: After configuring the TLS certificate, you must manually restart **FactoryTalk AssetCentre Server** service through **Control Panel** > **System and Security** > **Administrative Tools** > **Services**, or restart your computer.

Back up FactoryTalk AssetCentre with Microsoft SQL Server

Proper retention of data is a mission critical task in any industry. For FactoryTalk AssetCentre, this means backing up the data stored in the FactoryTalk AssetCentre database and LLumin database. The information in FactoryTalk AssetCentre, from audits and events, to the asset tree itself, is stored in the **AssetCentre database** within the Microsoft SQL (MSSQL) server. The information of Management of Change is stored in **LLumin database** within the Microsoft SQL (MSSQL) server. The following instructions use FactoryTalk AssetCentre database as an example. The instructions also apply to LLumin database.

Planning an AssetCentre Maintenance Window

When backing up any production system, such as FactoryTalk AssetCentre, it is critical to plan the event as a scheduled maintenance window. A maintenance window is a period of time that is planned to make a production system unavailable to its users, thus allowing for proper maintenance to that system to ensure continued system health. During the backup of the FactoryTalk AssetCentre system, user access should be limited. While users can continue to query the system during the backup, it is not recommended to have any user activity occur during this time. Fortunately, the Microsoft SQL server is capable of handling user queries of a database it is currently backing up, meaning that the FactoryTalk AssetCentre system does not need to be stopped in order to proceed with a backup.

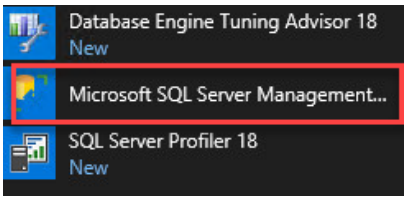
Backing Up FactoryTalk AssetCentre in Microsoft SQL Server 2019

The following set of instructions is intended for use on systems using Microsoft SQL Server 2019. Proper steps for manual backup of the AssetCentre database and the accompanying transaction log will be shown. A backup operation will essentially create a copy of the current database contents, and store them in a user-defined location. It should be noted that this process can also be automated, which is covered at the end of this section.

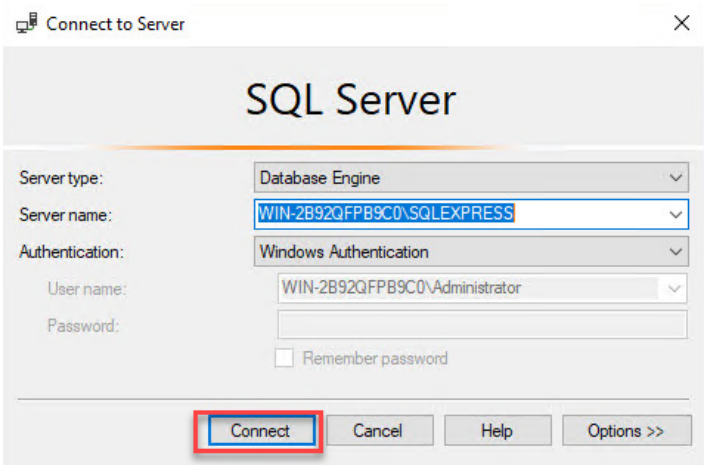
AssetCentre Database Backup

During the backup of the FactoryTalk AssetCentre system, user access should be limited. While users can continue to query the system during the backup, it is not recommended to have any user activity occur during this time. Additionally, it is advisable to run the Database Cleanup Wizard from the FactoryTalk AssetCentre desktop client prior to backing up the system to clean out any aged data that no longer needs to be retained (see online help in FactoryTalk AssetCentre desktop client for this procedure).

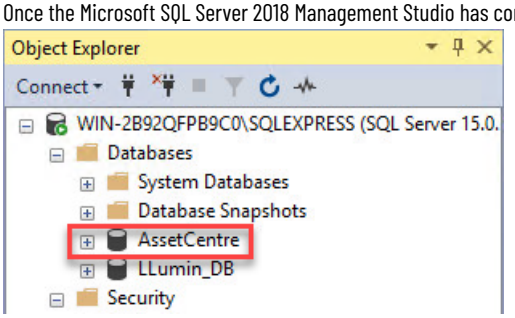
1. From the **Start** menu, select **SQL Server 2018 Management Studio**.



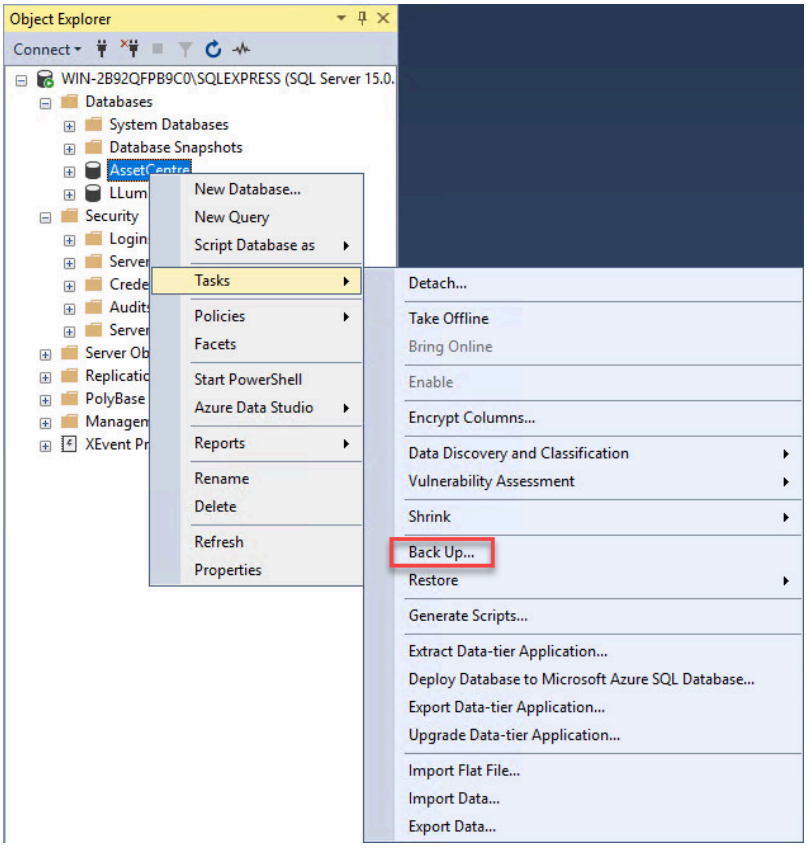
2. Click **Connect**.



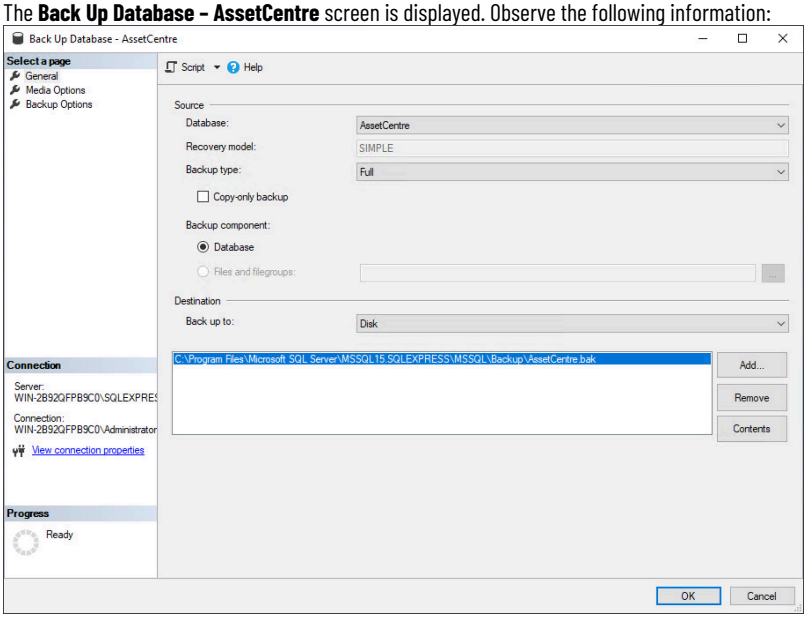
3. Once the Microsoft SQL Server 2018 Management Studio has connected to the database server, navigate to the **AssetCentre** database.



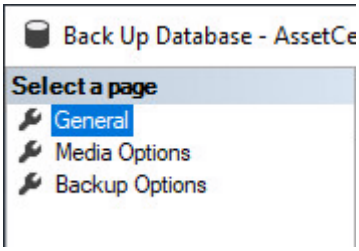
4. Right-click on the **AssetCentre database** and then select **Tasks > Back Up...**.



5. The **Back Up Database – AssetCentre** screen is displayed. Observe the following information:

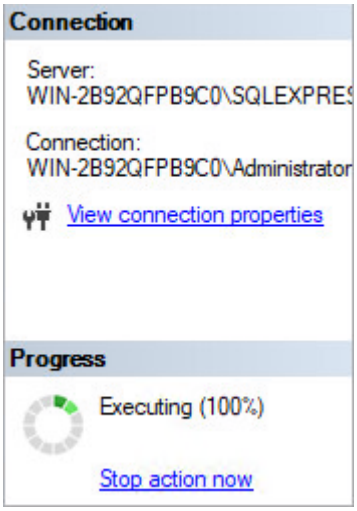


6. Note the **Media Options** and **Backup Options** from the tree on the left of the screen. In this example, all options are left at default.

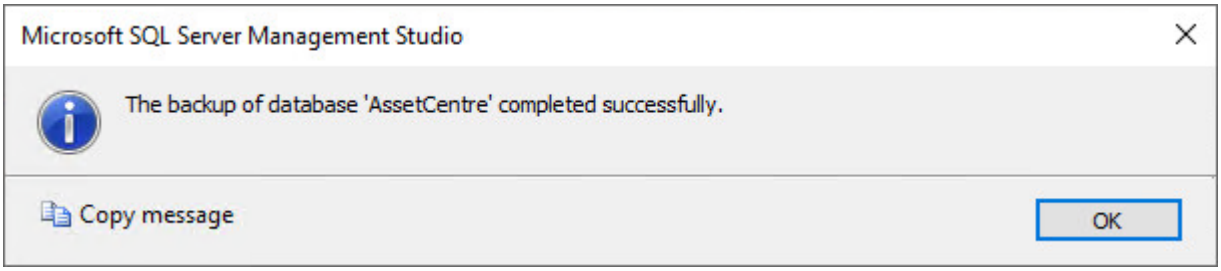


7. Click **OK** to initiate the backup.

8. Note the **Progress** panel in the bottom left of the screen.



9. Upon successful completion of the backup, the following window will be displayed.



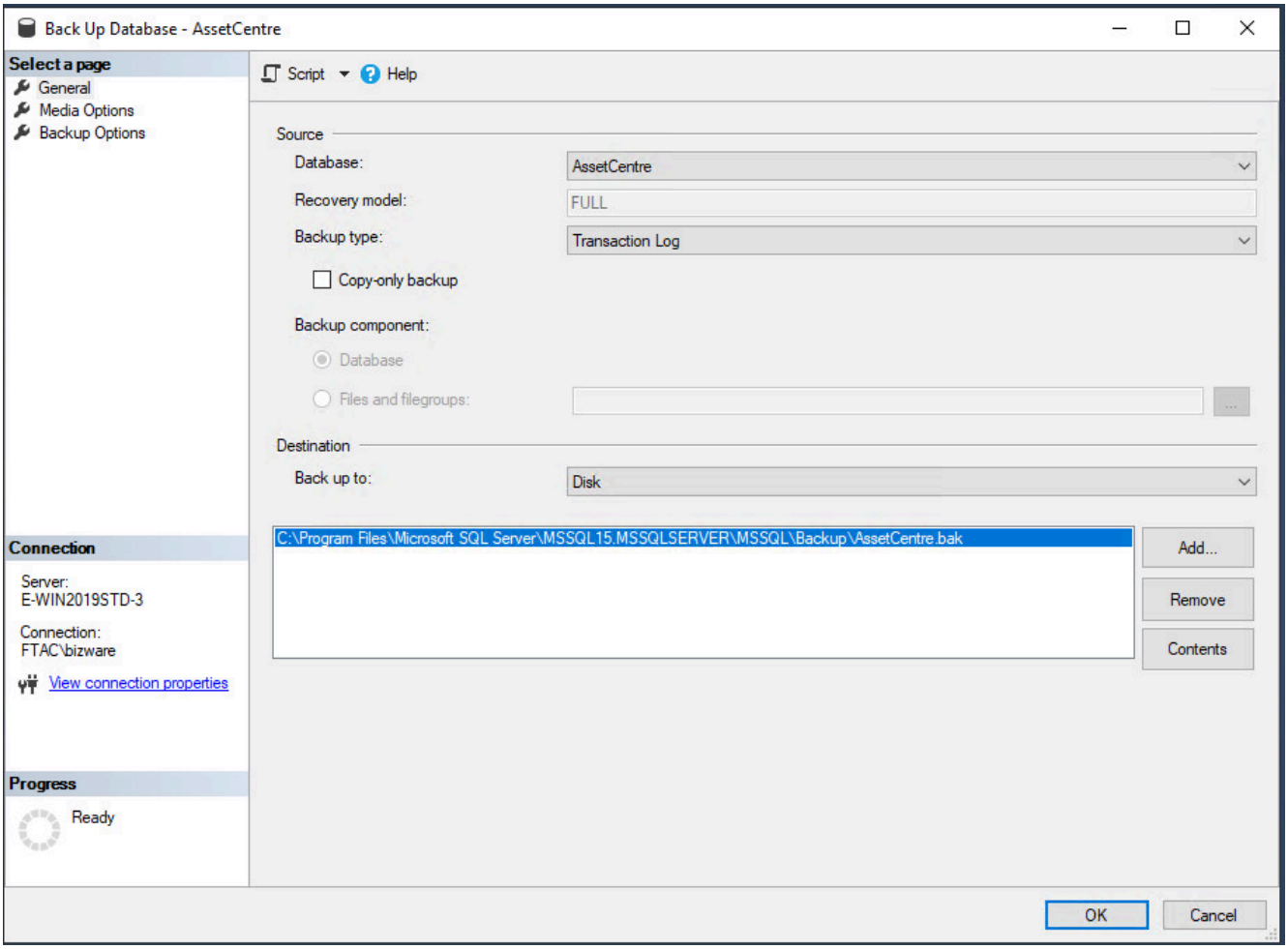
The AssetCentre database is now backed up.

AssetCentre Database Transaction Logs Backup

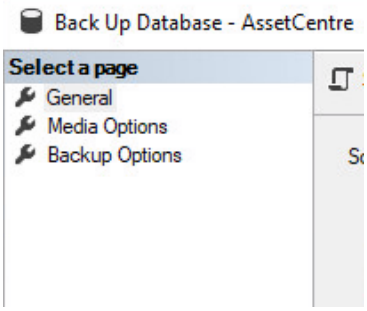
It is strongly recommended to backup the database transaction logs in addition to the database itself. The transaction logs essentially keep audits of the database, recording actions performed upon it. Both the transaction logs and database can be stored in the same file, specified in the section above on how to back up the database.

1. Right-click on the **AssetCentre database**, and then select **Tasks > Back Up...**.

   The following screen will be displayed:



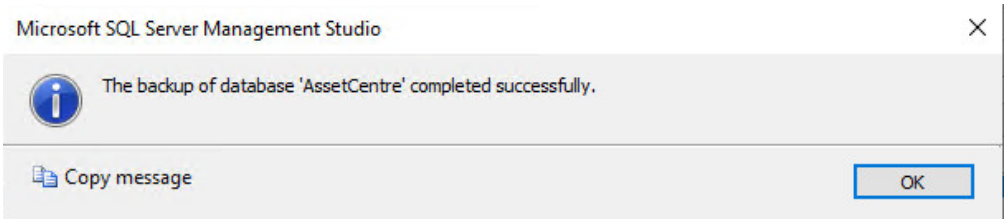
2. Note the **Media Options** and **Backup Options** from the tree on the left of the screen. In this example, all options are left at default.



3. Click **OK** to initiate the backup.

   Note the **Progress** panel in the bottom left of the screen.

4. Upon successful completion of the backup, the following window will be displayed, click **OK**.



   The AssetCentre database's transaction logs have now been backed up successfully.

   Repeat step 1-4 to backup the LLumin database transaction logs.

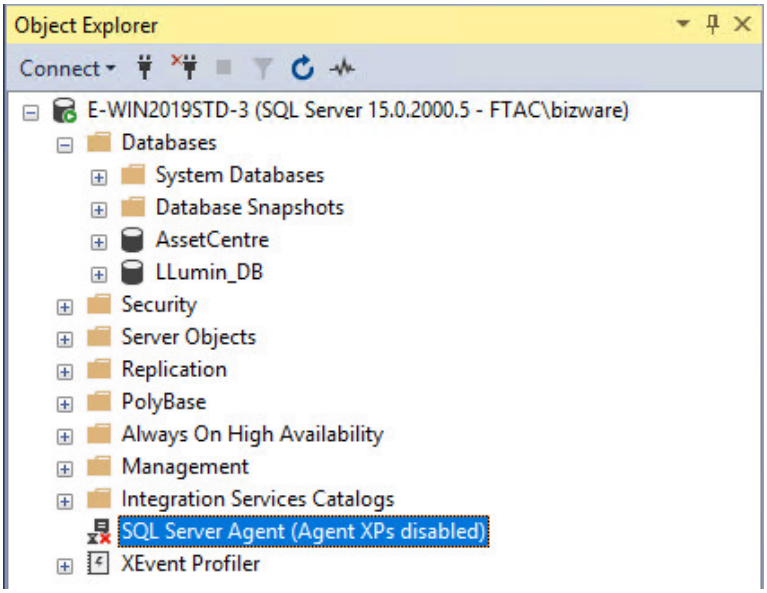
Scheduling Backups

Using the Microsoft SQL Server Agent, it is possible to schedule backups of the AssetCentre database and transaction logs on a user defined schedule. Typically, an entire database backup is scheduled less often than the transaction log backup (for example, the database might be backed up weekly, whereas the transaction logs are backed up daily).

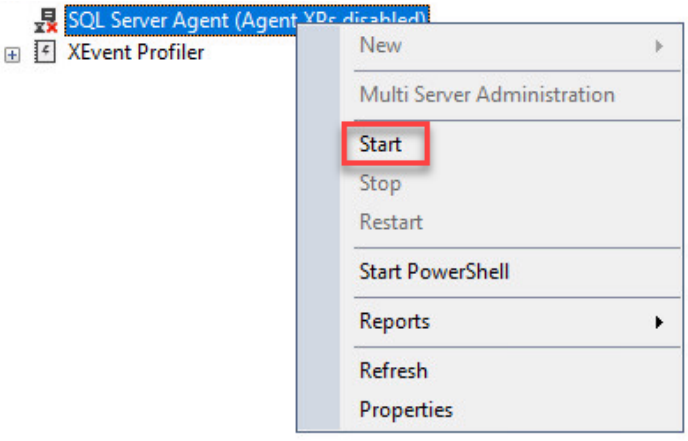
Since the Microsoft SQL Server Agent is performing the operation, its service must be running. It is recommended to set this service to automatic, such that the service will start on reboots without user intervention.

NOTE: The steps below assume a configuration of two separate maintenance plans: one for the transaction log and one for the database itself. It is possible to configure both in the same plan.

1. Ensure that the SQL Server Agent is started. This can be accomplished directly from the Microsoft SQL ServerManagement Studio, at the bottom of the navigation tree.

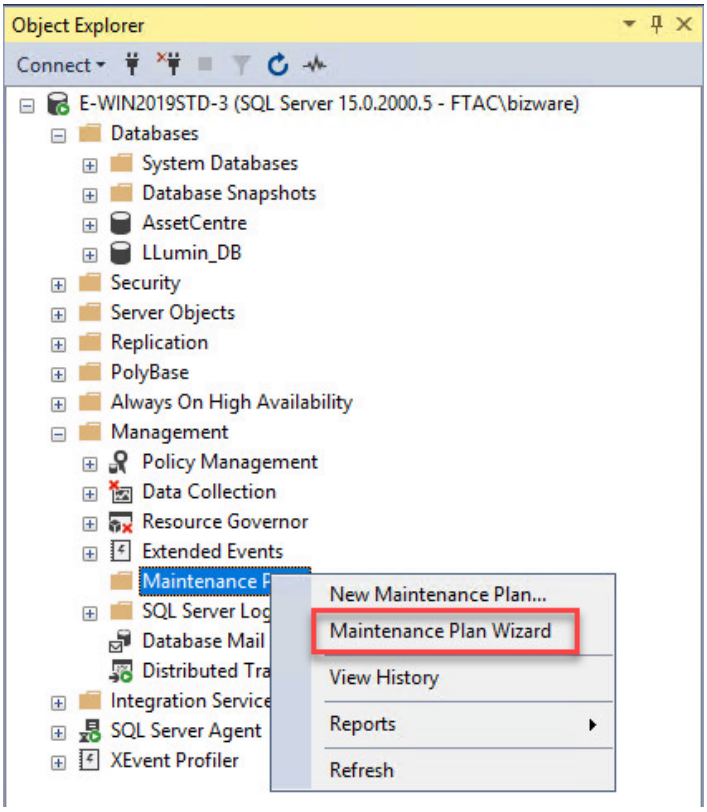


2. If the Agent is not started, right-click on it, and then select **Start**.

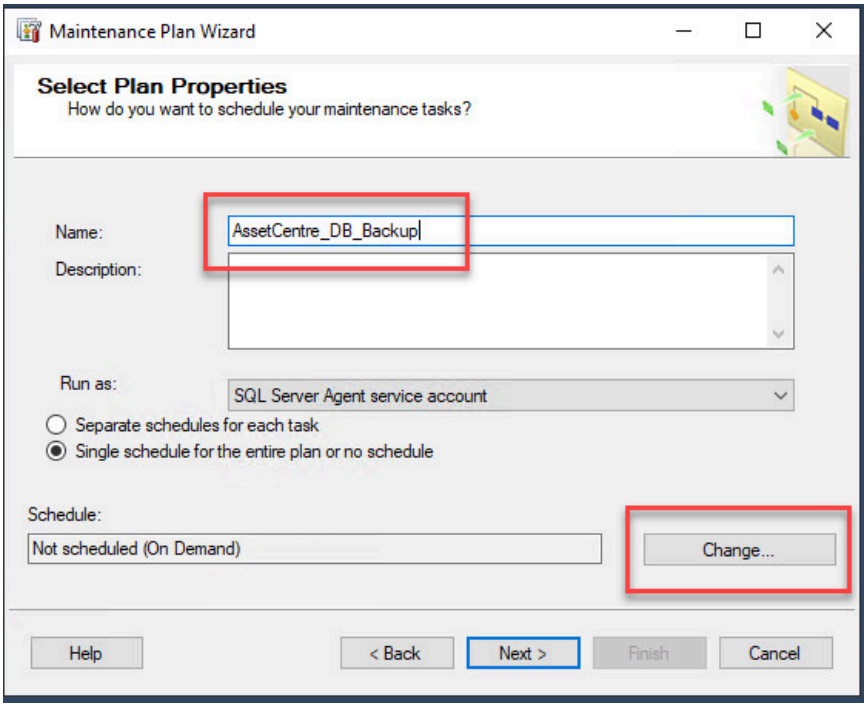


3. Click **Yes** when prompted to start the service.

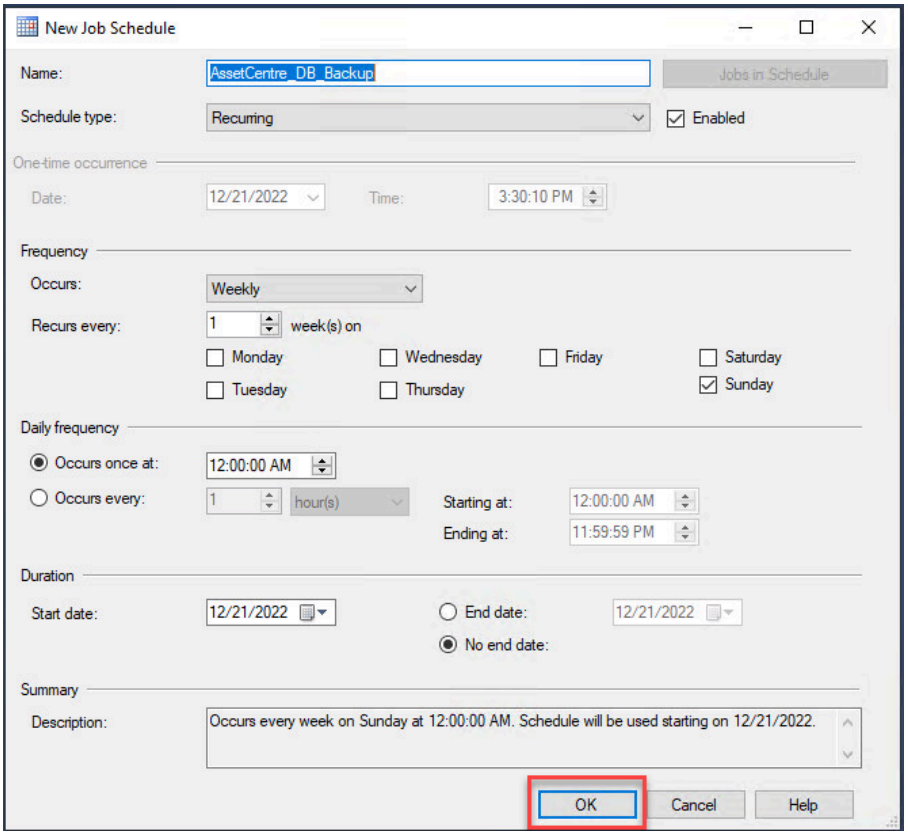
4. Once the SQL Server Agent is started, right-click on **Management > Maintenance Plans**, and then select **Maintenance Plan Wizard**.



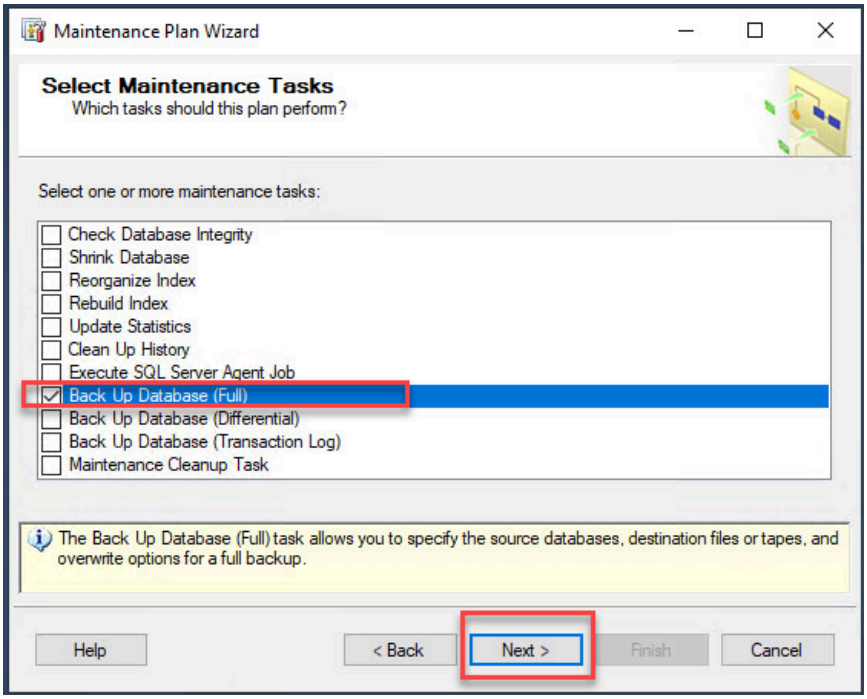
5. Enter **AssetCentre_DB_Backup** as the name for the maintenance plan, and then click the **Change** button to schedule the plan.



6. Use the following screen to configure the schedule for the operation, then click **OK** to continue.

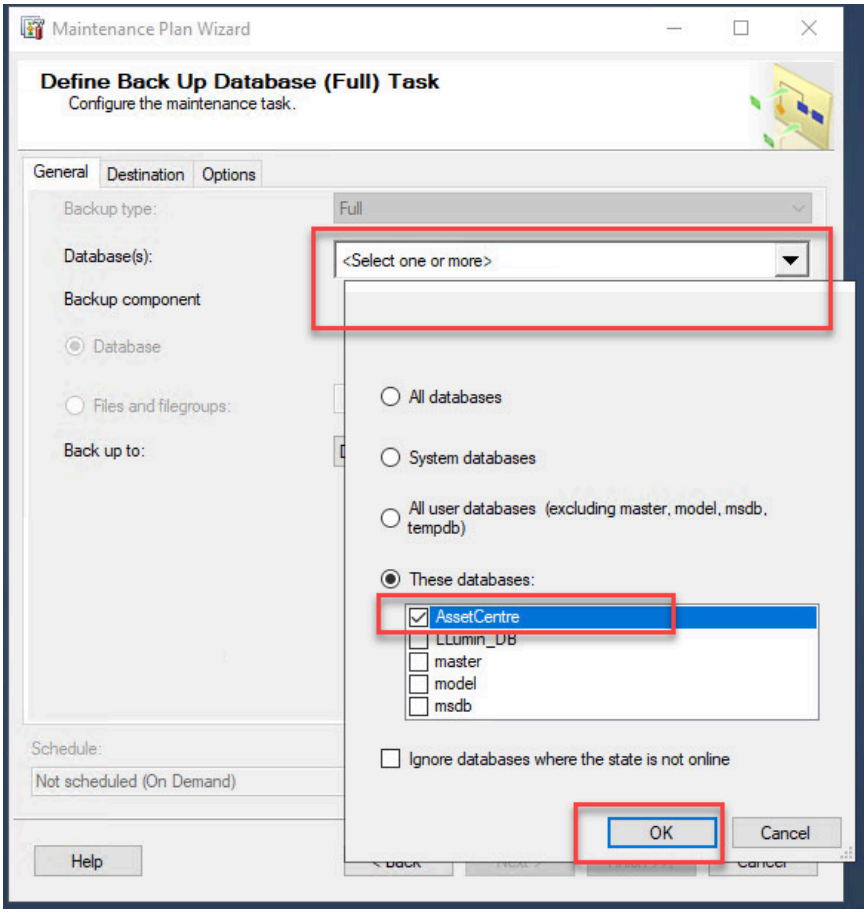


7. Click **Next** to progress past this screen now that the schedule is configured.
8. Select **Back Up Database (Full)** to configure this maintenance task to back up the database itself. Click **Next** to continue.



9. Click **Next** again.

10. Select the **AssetCentre** database from the drop down menu and click **OK**.



11. Under **Create a backup file for every database**, specify the location to store the backup file.

NOTE: A preferred location would be a separate hard drive from the one on which the database resides (thus saving the backup location if the database's hard drive fails).

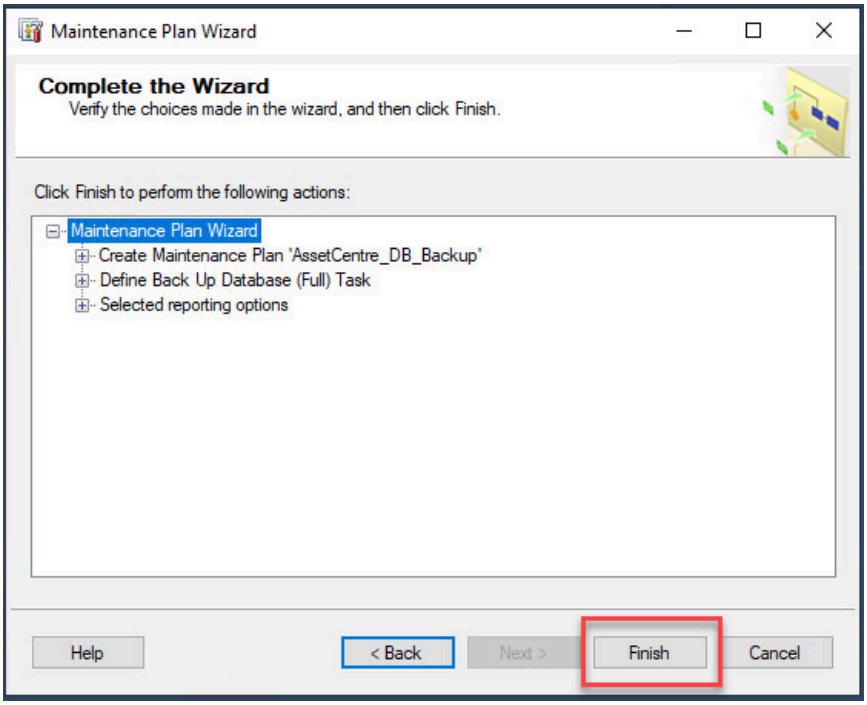
---

12. Click **Next**.
13. Enter the location to save the log files of the backup.
14. Click **Next**.

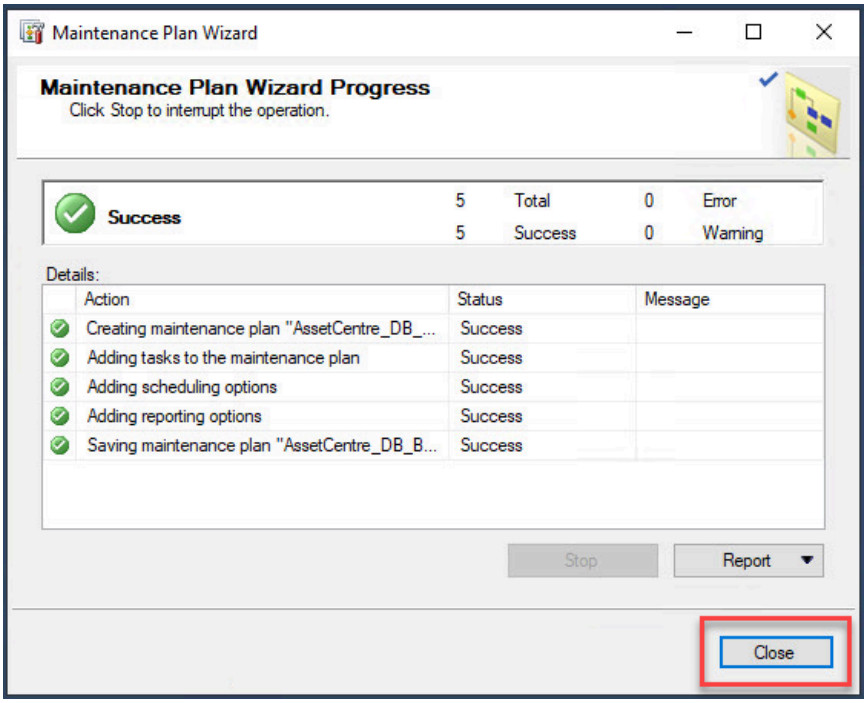
NOTE: It is possible to configure email reporting from this screen.

---

15. Click **Finish** to finalize the maintenance plan.



16. When complete, the following screen will be displayed:



17. Once the success of the operation is reported, click **Close**.
18. A database backup has now been scheduled.

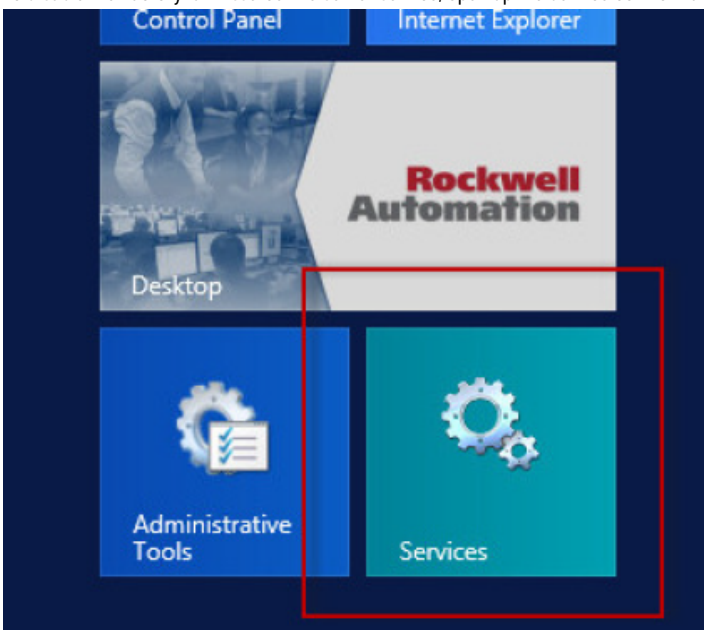
NOTE: If a maintenance plan for the transaction log is also desired, simply follow these steps again and select Back Up Database (Transaction Log) instead of Back Up Database (Full).

Restore FactoryTalk AssetCentre in Microsoft SQL Server 2019

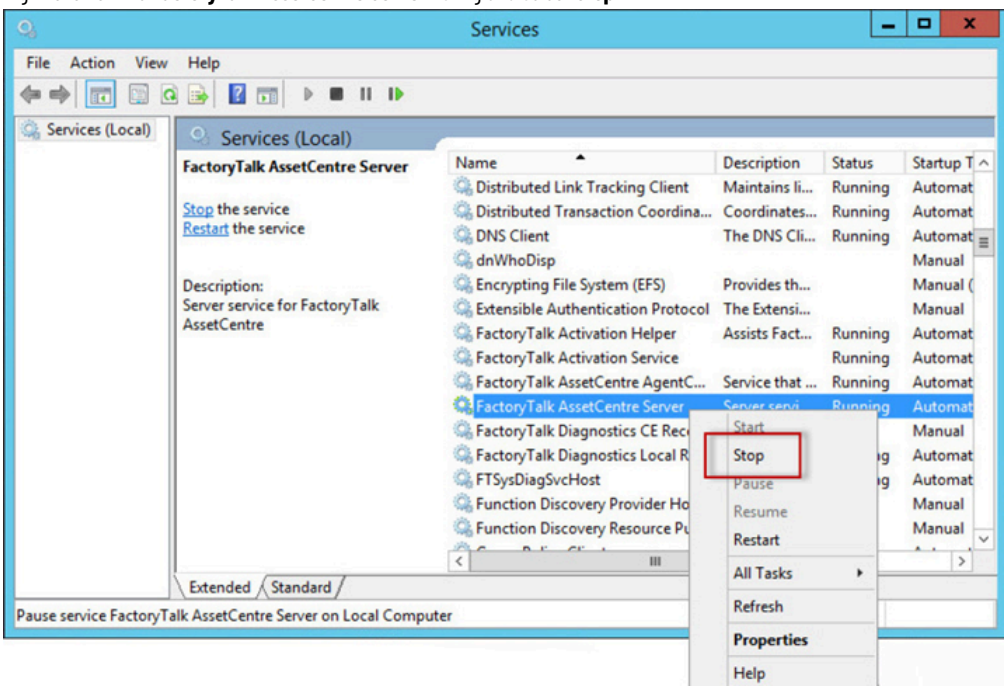
Before beginning the process of restoring the database, all users of the FactoryTalk AssetCentre system should be disconnected. It is advisable to simply stop the FactoryTalk AssetCentre server service until the Microsoft SQL database restore and subsequent re-connecting of the FactoryTalk AssetCentre server is complete. Additionally, the World Wide Web Publishing service should be stopped until the entire procedure is complete.

IMPORTANT: We recommend that you back up the database whether moving the database or not.

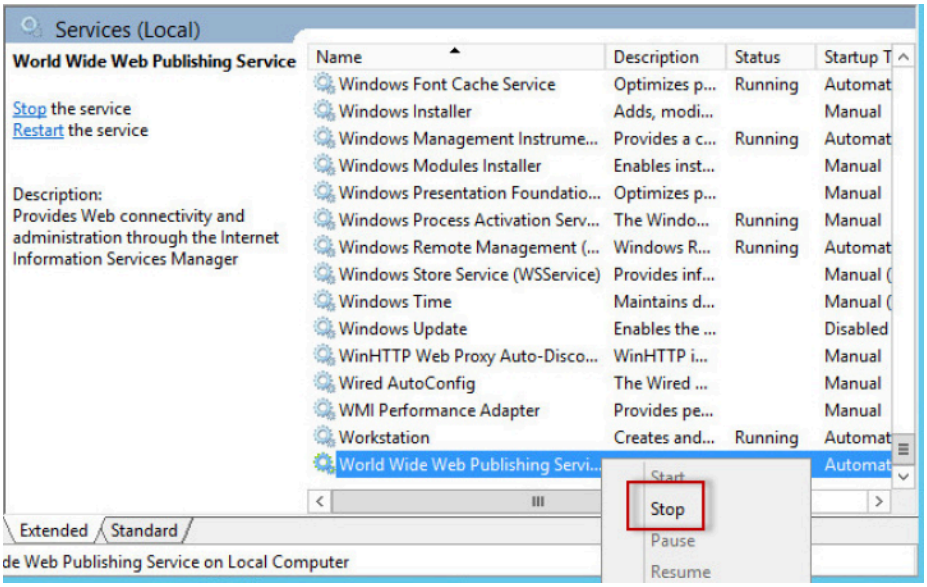
1. To disable the FactoryTalk AssetCentre server service, open up the Service Control Manager (**Start > Services**).



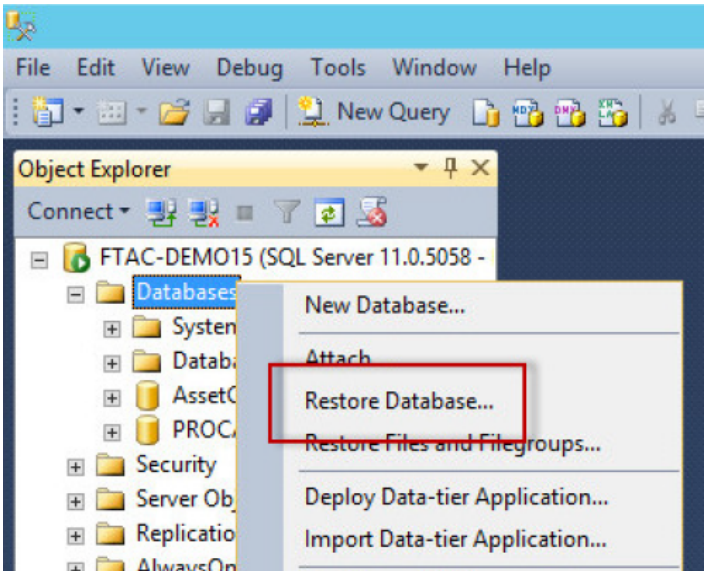
2. Right-click on the **FactoryTalk AssetCentre Server** listing and select **Stop**.



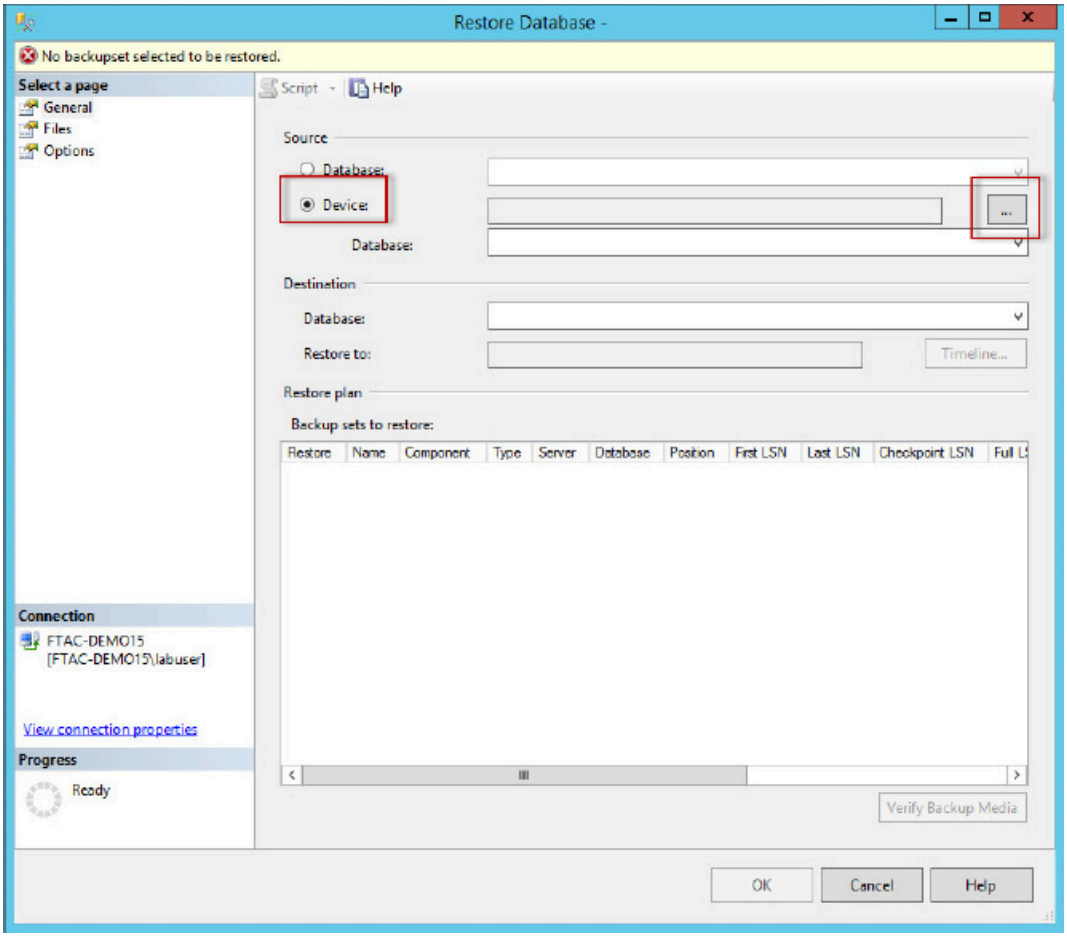
3. Stop the World Wide Web Publishing service in the same way.



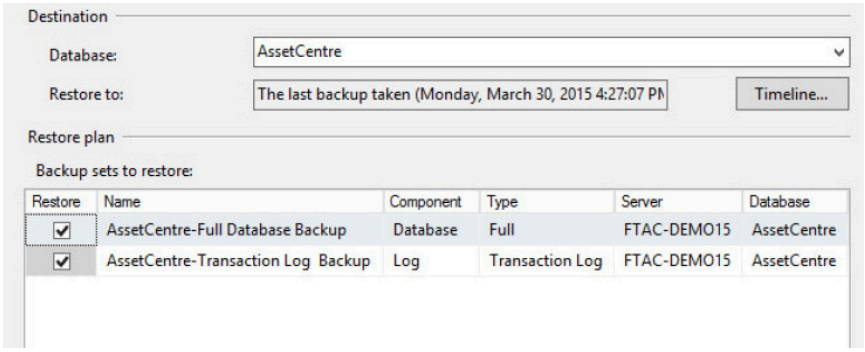
4. Return to the SQL Server Management Studio.
5. Right-click on **Databases**, then select **Restore Database**.



6. Select **Device**, and then click the **Browse** button.

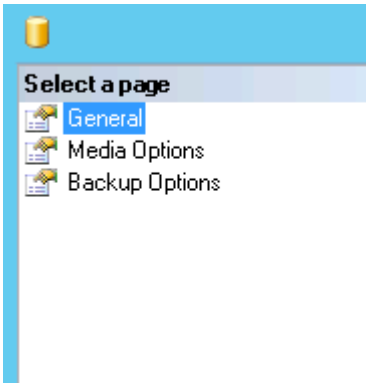


7. Click **Add**.
8. Browse to the location where you store the backup file, and then select it, then press **OK** twice to continue.
9. The backup list below the browse button will populate. Check all check boxes.

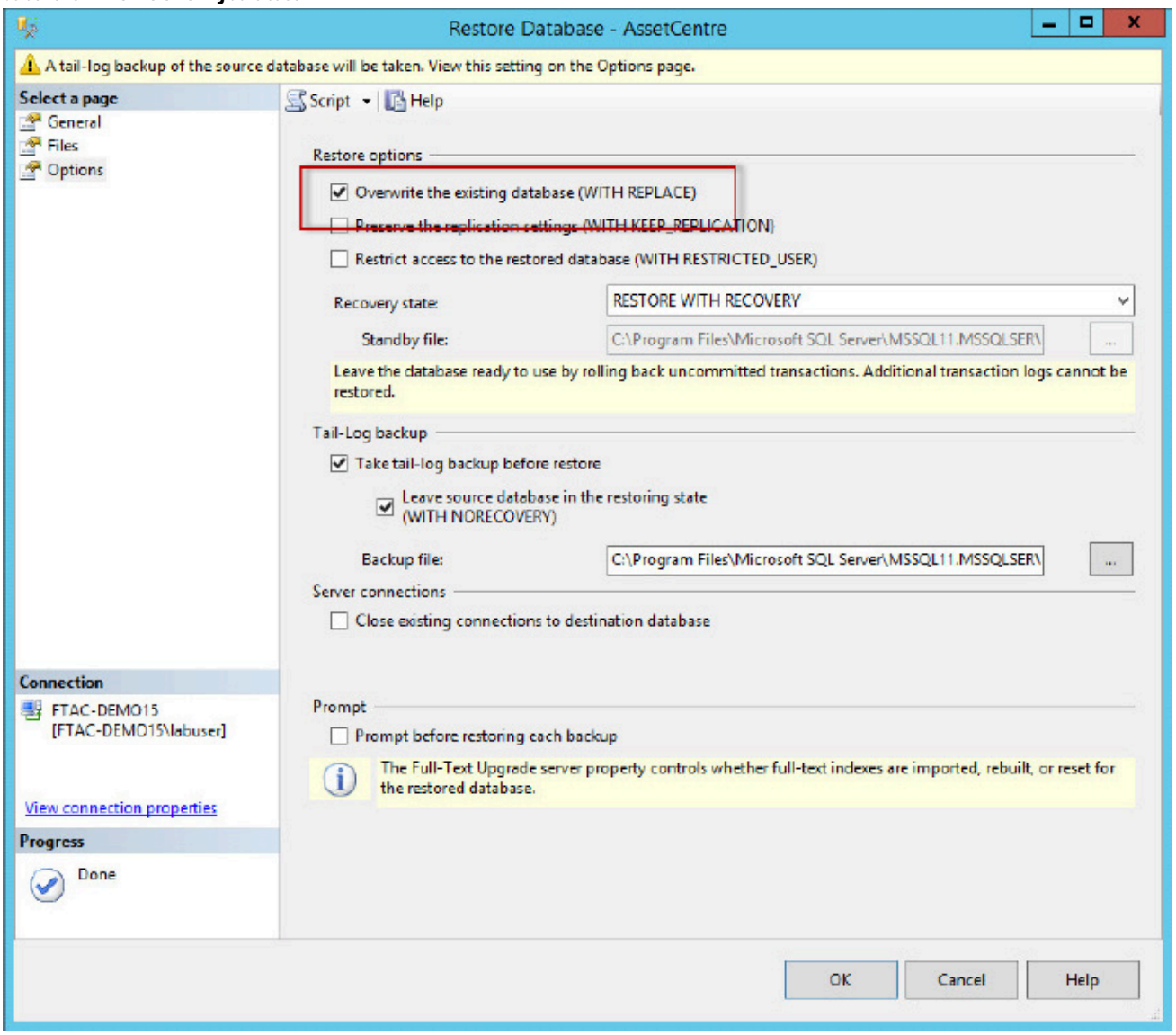


NOTE: If different options are selected, such as overwriting on each backup, or if a previous backup file is used, there will be a different number of rows to select from. Additionally, if no transaction logs were backed up, there may only be one checkbox available, corresponding to the AssetCentre database itself. It is also possible to perform restores of just the transaction log or database, depending on the checkbox selections. These steps show the process for restoring both at the same time.

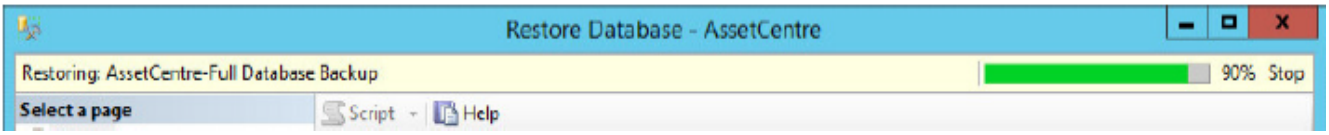
10. Click **Media Options**.



11. Select **Overwrite the existing database**.



12. Click **OK**. SQL will now restore the AssetCentre database. Progress is reported at the top of the window:

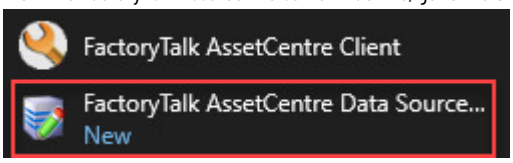


Use Data Source Configuration Wizard to update a SQL user account

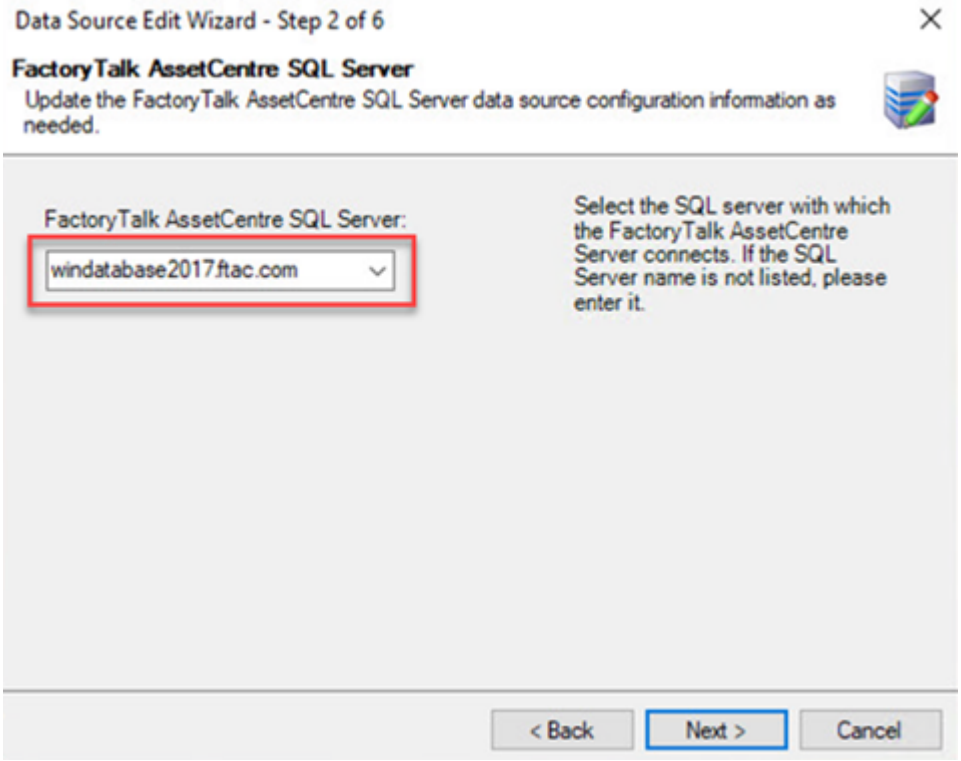
If the AssetCentre database has been moved or restored on a Microsoft SQL Server, it is important to reconnect the FactoryTalk AssetCentre server to this new database. The steps below will walk through the FactoryTalk AssetCentre Data Source Configuration Wizard, installed by default along with the FactoryTalk AssetCentre server.

NOTE: The FactoryTalk AssetCentre server and World Wide Web Publishing services should still be stopped at this point, following the restoration of the database. If this is not so, stop them now.

1. From the FactoryTalk AssetCentre server machine, go to the **Start** menu and select **FactoryTalk AssetCentre Data Source Configuration**.



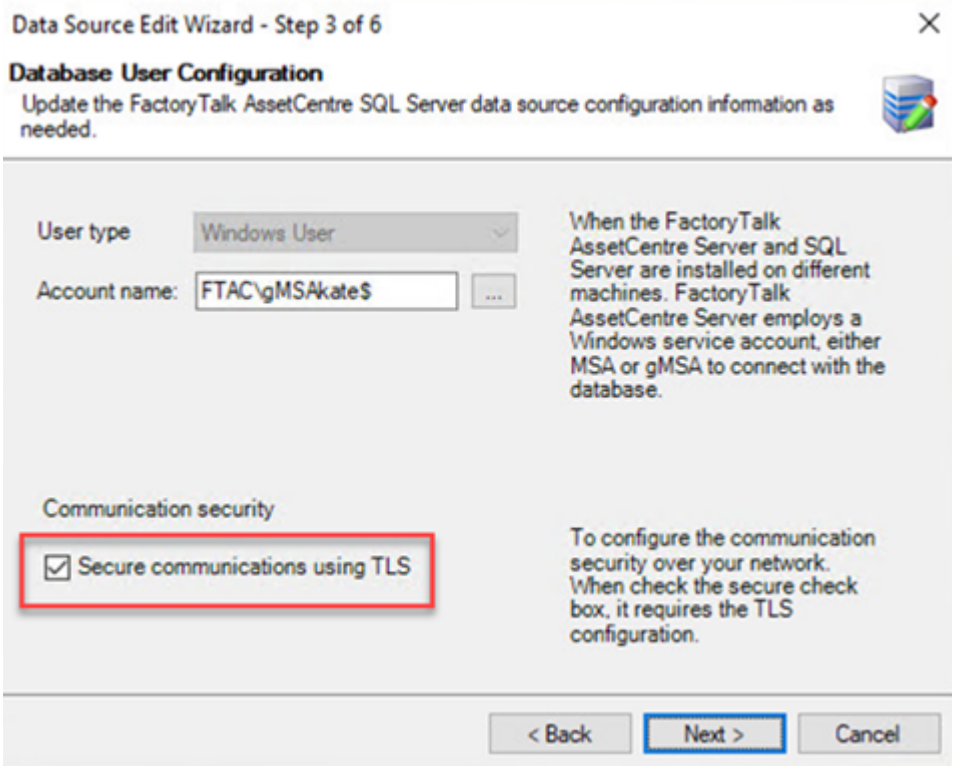
2. Click **Next** on the first screen.
3. Enter the name of the Microsoft SQL Server in the **FactoryTalk AssetCentre SQL Server** dropdown menu, and then click **Next**.



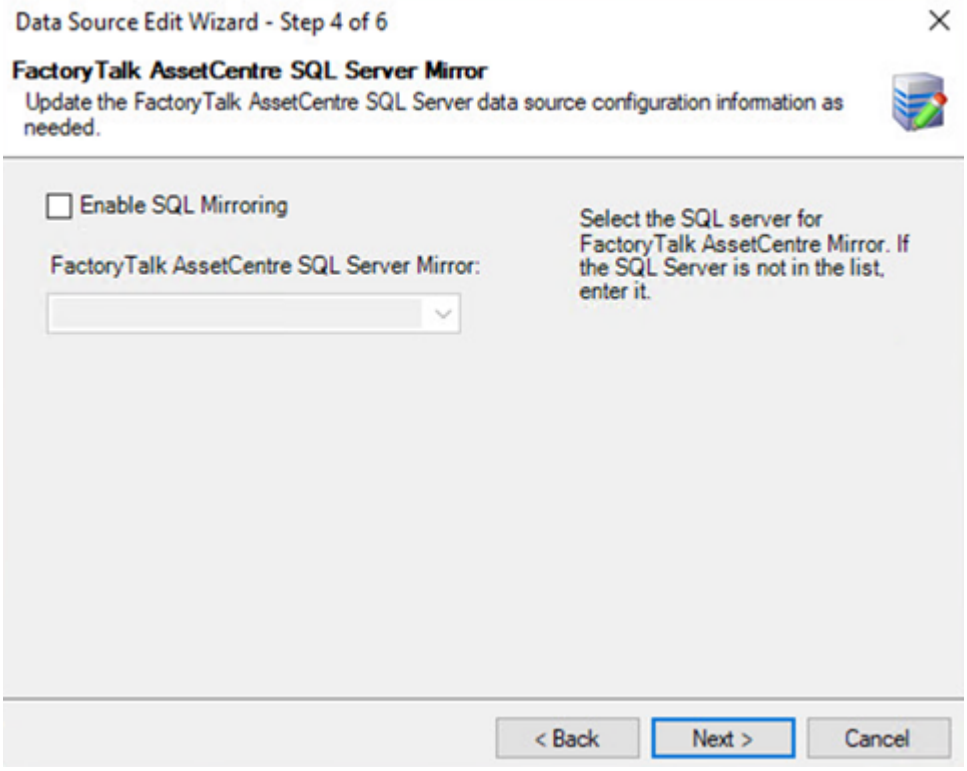
NOTE:

- If you want to turn on the TLS for the database, the fully qualified domain name (FQDN) computer name is required when you specify the FactoryTalk AssetCentre SQL server.
- The default port used for SQL Server communication is 1433. If you want to change the SQL Server port, you must add the port number after the FQDN SQL Server name. For example, *mySQLServer.myDomain.com,1526*. The comma (,) is required.
  You must ensure that the port is not in use by any other application, service, or process in your system.

4. Configure the **Account name** and communication security options as needed, and then click **Next**.

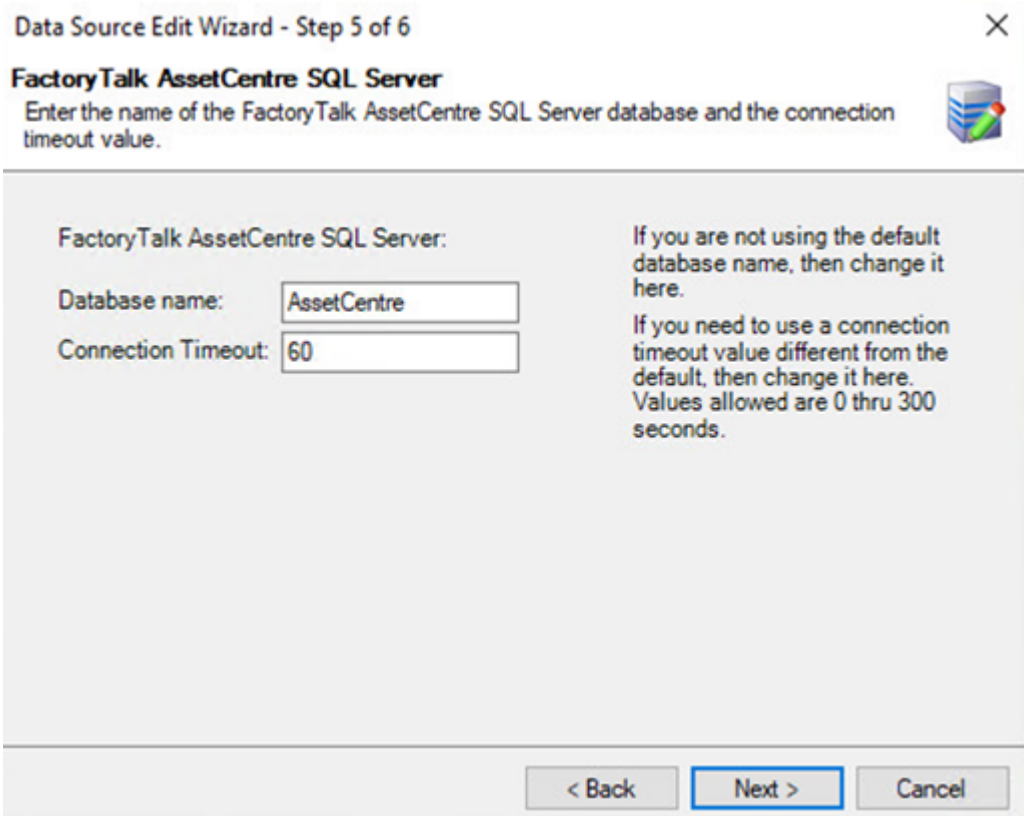


5. Configure the FactoryTalk AssetCentre SQL Server Mirror properties if applicable, and then click **Next**.

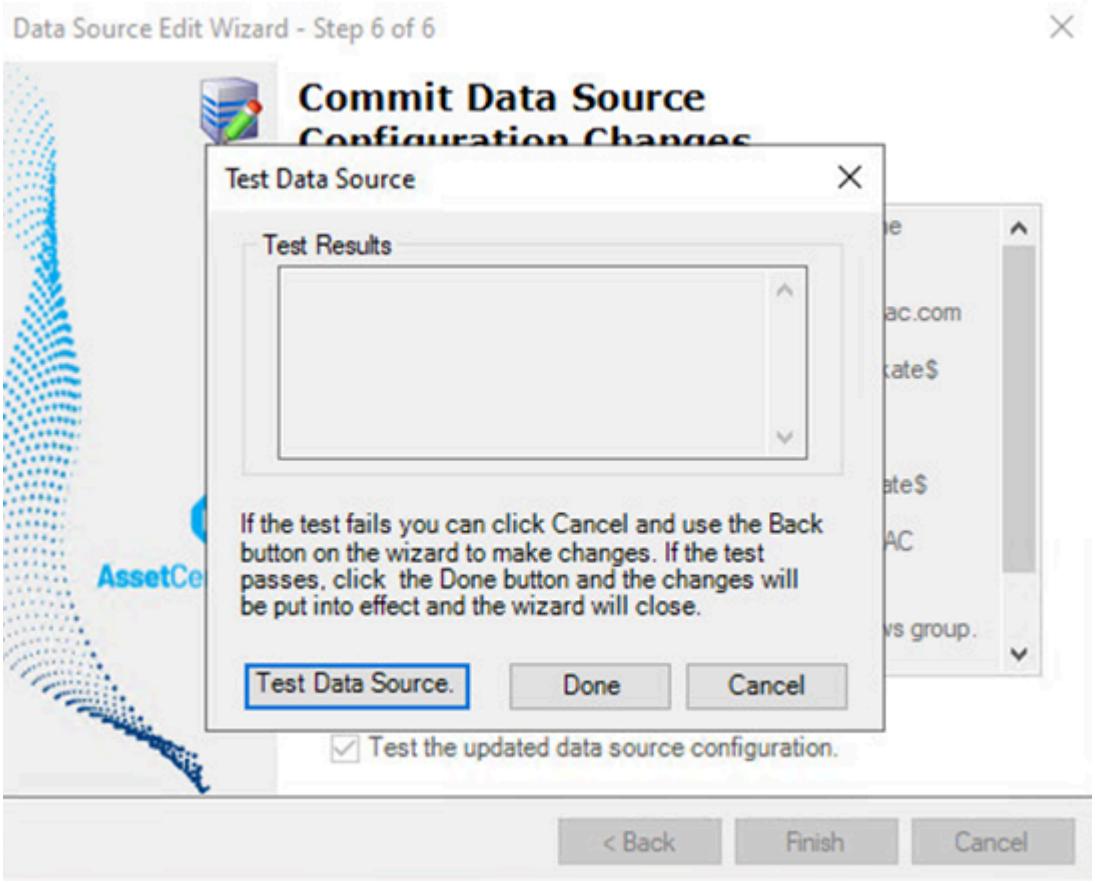


NOTE: If the **Enable SQL Mirroring** check box is selected, in the **FactoryTalk AssetCentre SQL Server Mirror** box, you can enter a name of Mirror Database Server or SQL Server Mirror that hosts the mirrored FactoryTalk AssetCentre Database.

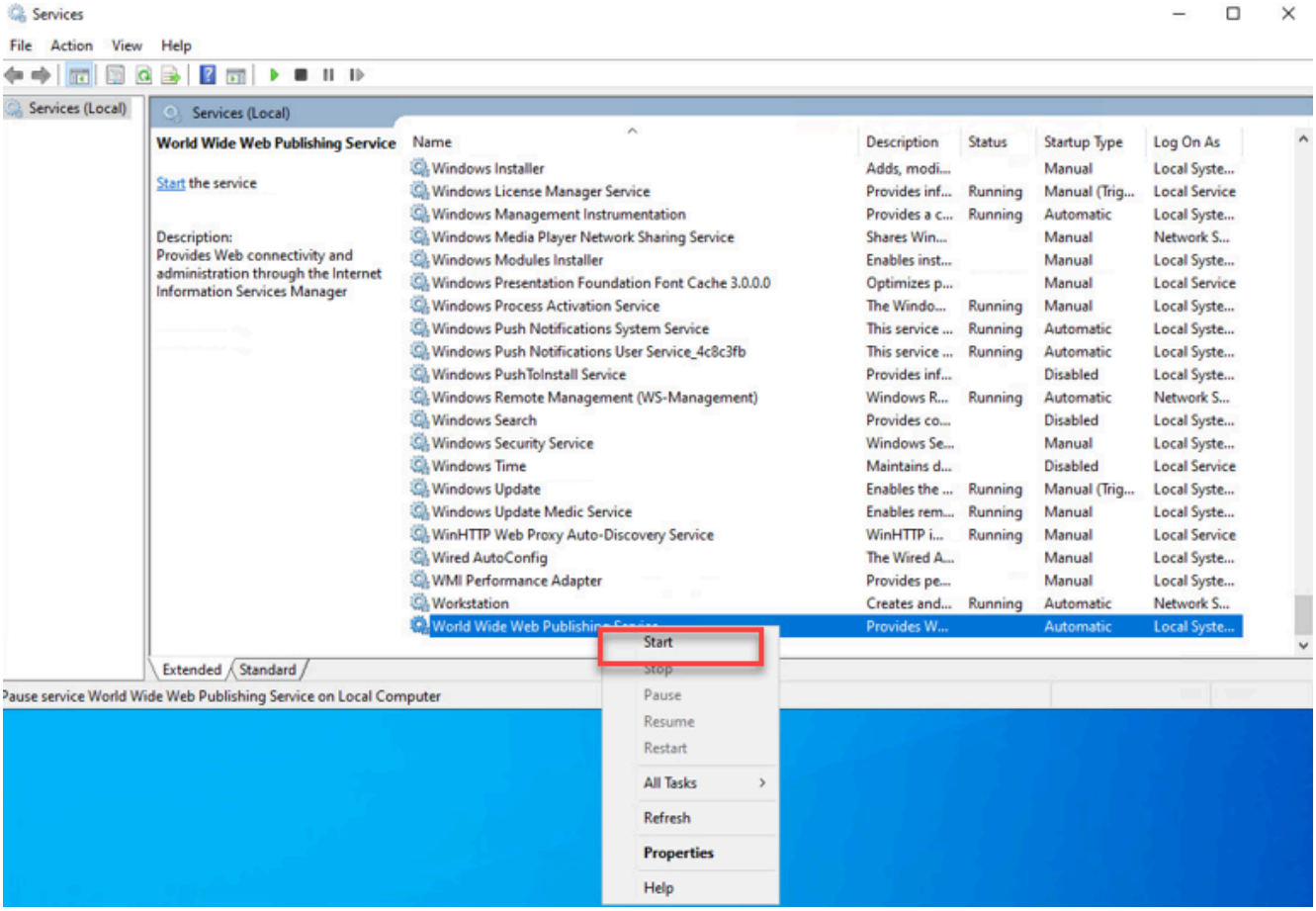
6. Confirm the **Database name** and **Connection Timeout** values in the FactoryTalk AssetCentre SQL Server window, and then click **Next**.



7. Click **Finish**, and a data source test window will appear.
8. Press **Test Data Source** to test the connection that you've just configured and verify that the test completes successfully.



9. Click **Done** to close the wizard.
10. Finally, start the FactoryTalk AssetCentre and World Wide Web Publishing services. From the **Start** menu, open the **Services** program. Start the World Wide Web Publishing service first Right-click on the World Wide Web Publishing listing and select **Start**.



11. Start the FactoryTalk AssetCentre Server service in the same way.

    The FactoryTalk AssetCentre Server is now connected to the newly restored database.

Command-line parameters for Data Source Configuration Wizard

Use command-line parameters to configure Data Source Configuration Wizard.

Parameter	Description
/m	Specifies the password for the FactoryTalk AssetCentre user and FactoryTalk AssetCentre database maintenance user, or generates a random password.
/SqlAdmin	Specifies the Microsoft SQL Server administrator account name. The Windows authentication is used by default to start Data Source Configuration Wizard.
/SqlAdminPwd	Specifies the Microsoft SQL Server administrator account password.
/SqlUserPwd	Specifies the password for the FactoryTalk AssetCentre user.
/SqlMaintainPwd	Specifies the password for the FactoryTalk AssetCentre database maintenance user.

Example:

- Generate a random password for the FactoryTalk AssetCentre user and FactoryTalk AssetCentre database maintenance user and start Data Source Configuration Wizard with Windows or SQL Server authentication.
  - For Windows authentication

    `RockwellAutomation.FTAssetCentre.DataSourceEditWizard.exe /m`
  - For SQL Server authentication

    `RockwellAutomation.FTAssetCentre.DataSourceEditWizard.exe /m /SqlAdmin=sa /SqlAdminPwd=rockwell123@RA`
- Specify a password for the FactoryTalk AssetCentre user and start Data Source Configuration Wizard with Windows authentication.

  `RockwellAutomation.FTAssetCentre.DataSourceEditWizard.exe /m /SqlUserPwd=rockwell123@RA`
- Specify a password for the FactoryTalk AssetCentre database maintenance user and start Data Source Configuration Wizard with SQL authentication.

  `RockwellAutomation.FTAssetCentre.DataSourceEditWizard.exe /m /SqlAdmin=sa /SqlAdminPwd=rockwell123@RA /SqlMaintainPwd=rockwell123@RA`

Move existing database to new server

Backup the FactoryTalk AssetCentre database and LLumin database before making any changes to your system configuration.

Ensure that the following components are installed on the new server computer before installing the FactoryTalk AssetCentre server components:

- Microsoft Internet Information Services (IIS)
- Microsoft SQL Server

NOTE: If you are upgrading your system to a new version of Microsoft SQL Server you will need to include the Integration Tools of the Microsoft SQL server installation to ensure SQL can successfully migrate a database to the new version.

The following instructions use FactoryTalk AssetCentre database as an example. The instructions also apply to LLumin database.

To update FactoryTalk AssetCentre database to new version on a new server

1. Move the FactoryTalk AssetCentre database backup (BAK) file from the old server to the new server.
2. Use the Microsoft SQL Server Management Studio on the new server to restore the .bak file to this server, for more information on how to backup and restore a Microsoft SQL database, see Backing up and Restoring FactoryTalk AssetCentre with Microsoft SQL Server on page 39.
3. On the new server from the SQL Management Studio expand the **AssetCentre Database > Security** folder.
4. Find the **AssetCentreUser** user and delete this user from the newly restored database.
5. Click **Yes** when asked to delete the associated schema with this user.

NOTE: This user must be deleted as the installation of the AssetCentre server installation will re-create a new AssetCentreUser tied to the AssetCentre Server instance running on this system.

When the **AssetCentreUser** has been removed from the AssetCentre database, the AssetCentreUser SQL login user is also deleted.

6. Proceed with the AssetCentre Server installation, see Install the FactoryTalk AssetCentre Server software on page 14.

NOTE: After upgrading FactoryTalk AssetCentre from previous version to version 10.00.00 and later, and restarting your computer, you can check the SDF file to confirm whether the migration from SDF to MDF succeeded. If the size of the SDF file is still large (for example, more than 1GB), in the **Control Panel**, you can repair FactoryTalk AssetCentre Common Components to restart the migration.

Optional software upgrades

If earlier versions of the following software are installed on your computer, and they are lower than the minimum versions required to install FactoryTalk AssetCentre, the FactoryTalk AssetCentre Setup wizard will upgrade the software automatically.

- RSLinx Classic Lite
- Logix Designer Compare Tool
- FactoryTalk View ME Transfer Utility
- RSLogix 5
- RSLogix 500

If the software versions are equal to or higher than the minimum versions required to install FactoryTalk AssetCentre, but lower than the versions included in the FactoryTalk AssetCentre installation package, the installation process will not upgrade the software automatically. If you want to use the latest versions instead, you must select the software check boxes during the installation of FactoryTalk AssetCentre.

Tip: If you use FactoryTalk Services Platform CPR 9 SR 14, be sure to use the CPR 9 SR 14 versions of RSLinx Enterprise and RSLinx Classic Lite.

If you want to upgrade the optional software products, we recommend that you upgrade them before installing FactoryTalk AssetCentre.

Use silent or unattended setup to install the FactoryTalk AssetCentre software

FactoryTalk AssetCentre supports silent or unattended installation. Silent installation runs in a quiet mode without any user interface, while unattended installation runs in a quiet simple mode and shows progress through the UI. Unattended installation does not accept any input, but still shows error or restart messages.

IMPORTANT: Before starting silent or unattended setup to install the FactoryTalk AssetCentre software, ensure that your Windows Active Directory (AD) user account has been assigned the SQL Server system administrator (SA) role.

Use command lines to specify properties to install FactoryTalk AssetCentre software automatically with little interaction. The silent or unattended installation supports the following installation modes:

- FactoryTalk AssetCentre Server
- FactoryTalk AssetCentre Agent
- FactoryTalk AssetCentre Desktop Client
- FactoryTalk AssetCentre Custom Installation

Tip: Unlike custom installation using the standard Setup wizard that allows you to select software products to install, the custom installation mode in silent or unattended setup automatically installs all FactoryTalk AssetCentre software, including FactoryTalk AssetCentre server, desktop client, and agent.

During the silent or unattended installation, all associated Rockwell Automation software processes will be forcibly ended automatically. Make sure to shut down all associated Rockwell Automation software products before installation.

This chapter describes how to use silent or unattended setup to install the FactoryTalk AssetCentre software. If you want to use the standard Setup wizard to install the software step by step, see Chapter 4 through Chapter 7 for detailed instructions.

IMPORTANT: When using the silent or unattended setup to upgrade FactoryTalk AssetCentre version 8.00.00 or later, the upgrade will fail if any of the following additional software components version' on the computer is equal to or higher than the version you will upgrade to.

- Logix Designer Compare Tool
- RSLogix 5
- RSLogix 500
- FactoryTalk View ME Transfer Utility
- FactoryTalk Updater Agent

To avoid this problem, do one of the following:

- Upgrade FactoryTalk AssetCentre version 8.00.00 or later using the Setup wizard.
- Enter `/IgnoreWarning` when upgrading FactoryTalk AssetCentre version 8.00.00 or later using the silent or unattended setup.
  Example:
  ```
  D:\12.00.00-FTAssetCentre-DVDD\Setup.exe /Q /IAcceptAllLicenseTerms /SetupLanguage=ENU /
  Product="AssetCentre Server" /InstallDrive=D: /SqlServer="RemoteInstance" /MSA="RA\FTACgMSA$" /
  FTSPWebAuth=yes /ReverseProxy=yes /FTSPWebEventServer=yes /DirectoryServer=FTDIRECTORY /IgnoreWarning /
  AutoRestart
  ```

Before performing the silent or unattended installation

This section describes things you need to know:

- Before you install the FactoryTalk AssetCentre Server software using silent or unattended setup on page 60
- Before you install FactoryTalk AssetCentre Agent software using unattended silent or setup on page 60
- Before you install the FactoryTalk AssetCentre Desktop Client software using silent or unattended setup on page 60

For current information on the system requirements for the FactoryTalk AssetCentre software, see FactoryTalk AssetCentre Release Notes and the Product Compatibility and Download Center.

Before you install the FactoryTalk AssetCentre Server software using silent or unattended setup

The following checklist summarizes the basic tasks involved in the unattended installation of FactoryTalk AssetCentre Server software along with supporting software.

- Ensure that the user performing installation has administrative rights in Windows.
- Ensure that a Microsoft SQL Server is available, and it is already installed on the same computer as the intended FactoryTalk AssetCentre Server, or on a separate Microsoft Windows server.
- Ensure that the Windows account of the user performing the installation, or a Windows group of which the user performing the installation is a member, is assigned the Microsoft SQL Server System Administrator role before attempting the installation.
- If you will configure the FactoryTalk AssetCentre Server to use a remote SQL database, ensure that a standalone managed service account or a group managed service account has been created in your Windows Active Directory.

Before you install FactoryTalk AssetCentre Agent software using silent or unattended setup

Agents are programs that communicate with the FactoryTalk AssetCentre server and perform scheduled tasks on behalf of the FactoryTalk AssetCentre server. Agents allow work to be distributed and shared among multiple computers to spread processing load and speed up operations. When a server needs an agent to perform a task, it locates the computer running the operation and assigns the task to that agent. The agent then reports the task's completion to the server. The Search feature, as well as purchased capabilities, such as Disaster Recovery capabilities, require the use of agents to perform scheduled operations.

Where to install the FactoryTalk AssetCentre Agent software

Agents can be installed on any computer that:

- Is capable of running the FactoryTalk AssetCentre Agent software (see Agent computer requirements on page 10).
- Is connected to the FactoryTalk AssetCentre server.
- Runs the FactoryTalk AssetCentre server, or the FactoryTalk AssetCentre desktop client.

See Before you install the FactoryTalk AssetCentre Agent software on page 24 for more information about FactoryTalk AssetCentre Agent software.

Before you install the FactoryTalk AssetCentre Desktop Client software using silent or unattended setup

The FactoryTalk AssetCentre Desktop Client software provides the user interface for FactoryTalk AssetCentre. It is through the client that you perform tasks such as checking files in and out, creating and running scheduled events, and viewing logs. For more information on what you can do with FactoryTalk AssetCentre Desktop Client software, see the *FactoryTalk AssetCentre Help* (once the desktop client is installed).

Install the FactoryTalk AssetCentre Desktop Client software on all computers on which you want to use FactoryTalk AssetCentre.

The desktop client is not required on the FactoryTalk AssetCentre server computer, but you can install it on the server if desired.

Install the desktop client on any computer

- From which you want to access the FactoryTalk AssetCentre Desktop Client software (to edit the representation of your assets, to view logs, to create schedules, to search the logs, and so on).
- That is capable of running the FactoryTalk AssetCentre Desktop Client software (see Client computer requirements on page 9).
- That is connected to the FactoryTalk AssetCentre Server.
- From which FactoryTalk audits are desired.

The Disaster Recovery capability provides the ability to schedule a comparison between master files, and processor program and data files. To edit the file and data settings for a compare operation for Allen-Bradley PLC-5, SLC 500, or MicroLogix controllers, you must have RSLogix 5, or RSLogix 500 software installed on the client computer.

Perform silent or unattended installation

Use command-line parameters to perform a silent or unattended installation of the software.

The command-line installation requires the administrator permission. The steps may vary slightly depending on your operating system.

WARNING: HTTPS is turned on by default during silent or unattended installation. If you don't want to use it, you can turn it off with `/NoHTTPS`. The potential security risks of turning off HTTPS are as below:

- The data is transmitted without encryption across a network, which will cause leakage of information, if other solutions, such as IPSEC, are not used.
- The system may be vulnerable to a Remote Code Execution (RCE) attack.

To perform silent or unattended installation

1. Close all Windows programs.
2. Open the **Command Prompt** window.
3. In the **Command Prompt** window, navigate to the drive containing the FactoryTalk AssetCentre installation package.
   In this example, type *D:*, where *D:* is the logical drive or volume, and press **Enter**.

   Tip: If **User Account Control** dialog box shows, click **Yes.**

4. Type a command with the following syntax:
   - Perform silent or unattended installation and access database with Windows Authentication.

     ```
     Setup.exe {/Q | /QS} /IAcceptAllLicenseTerms [/SetupLanguage=language] [/Record] [/Playback] [/Product=product_name] [/InstallDrive=drive] [/SqlServer=SQL_location] [/MSA=MSA or gMSA] [/FTSPWebAuth=Yes or No] [/ReverseProxy=Yes or No] [/FTSPWebEventServer=Yes or No ] [/DirectoryServer=FTD_server_location] [/AutoRestart]
     ```

     Example:

     ```
     D:\12.00.00-FTAssetCentre-DVDD\Setup.exe /Q /IAcceptAllLicenseTerms /SetupLanguage=ENU /Product="AssetCentre Server" /InstallDrive=D: /SqlServer="RemoteInstance" /MSA="RA\FTACgMSA$" /FTSPWebAuth=yes /ReverseProxy=yes /FTSPWebEventServer=yes /DirectoryServer=FTDIRECTORY /AutoRestart
     ```

   - Perform silent or unattended installation with Windows Authentication and access database with SQL Authentication.

     ```
     Setup.exe {/Q | /QS} /IAcceptAllLicenseTerms [/SetupLanguage=language] [/Record] [/Playback] [/Product=product_name] [/InstallDrive=drive] [/SqlServer=SQL_location] [sql] [/FTSPWebAuth=Yes or No] [/ReverseProxy=Yes or No] [/FTSPWebEventServer=Yes or No ] [/DirectoryServer=FTD_server_location] [/AutoRestart]
     ```

Example:

```
D:\12.00.00-FTAssetCentre-DVDD\Setup.exe /Q /IAcceptAllLicenseTerms /SetupLanguage=ENU /Product="AssetCentre Server" /InstallDrive=D: /SqlServer="RemoteInstance" /sql /FTSPWebAuth=yes /ReverseProxy=yes /FTSPWebEventServer=yes /DirectoryServer=FTDIRECTORY /AutoRestart
```

- Perform silent or unattended installation with SQL Authentication and access database with Windows Authentication.

  ```
  Setup.exe {/Q | /QS} /IAcceptAllLicenseTerms [/SetupLanguage=language] [/Record] [/Playback] [/Product=product_name] [/InstallDrive=drive] [/SqlServer=SQL_location] [/sa] [/SqlAdmin=SQL_administrator] [/SqlAdminPwd=SQL_admin_password] [MSA=MSA or gMSA] [/FTSPWebAuth=Yes or No] [/ReverseProxy=Yes or No] [/FTSPWebEventServer=Yes or No ] [/DirectoryServer=FTD_server_location] [/AutoRestart]
  ```

  Example:

  ```
  D:\12.00.00-FTAssetCentre-DVDD\Setup.exe /Q /IAcceptAllLicenseTerms /SetupLanguage=ENU /Product="AssetCentre Server" /InstallDrive=D: /SqlServer="RemoteInstance" /sa /SqlAdmin="sa" /SqlAdminPwd="SqlAdminPwd" /MSA="RA\FTACgMSA$" /FTSPWebAuth=yes /ReverseProxy=yes /FTSPWebEventServer=yes /DirectoryServer=FTDIRECTORY /AutoRestart
  ```

- Perform silent or unattended installation and access database with SQL Authentication.

  ```
  Setup.exe {/Q | /QS} /IAcceptAllLicenseTerms [/SetupLanguage=language] [/Record] [/Playback] [/Product=product_name] [/InstallDrive=drive] [/SqlServer=SQL_location] [/sa] [/SqlAdmin=SQL_administrator] [/SqlAdminPwd=SQL_admin_password] [/sql] [/FTSPWebAuth=Yes or No] [/ReverseProxy=Yes or No] [/FTSPWebEventServer=Yes or No ] [/DirectoryServer=FTD_server_location] [/AutoRestart]
  ```

  Example:

  ```
  D:\12.00.00-FTAssetCentre-DVDD\Setup.exe /Q /IAcceptAllLicenseTerms /SetupLanguage=ENU /Product="AssetCentre Server" /InstallDrive=D: /SqlServer="RemoteInstance" /sa /SqlAdmin="sa" /SqlAdminPwd="SqlAdminPwd" /sql /FTSPWebAuth=yes /ReverseProxy=yes /FTSPWebEventServer=yes /DirectoryServer=FTDIRECTORY /AutoRestart
  ```

IMPORTANT:

- When installing FactoryTalk AssetCentre through silent or unattended installation, quotes are required for the parameters with space (for example, `/Product="AssetCentre Server"`).

5. Press **Enter**.

   For more information about parameters, type **Setup.exe /?** or see Command-line parameters for silent or unattended installation on page 62.

Command-line parameters for silent or unattended installation

Unattended or silent install

Use command-line parameters to perform an unattended or silent installation of the software.

IMPORTANT: When installing or upgrading FactoryTalk AssetCentre to version 11.00.00 or later with SQL Server Authentication, you must use silent or unattended setup to install it.

Command-line parameters

The following table identifies the installation command-line parameters. Command-line parameters are case-insensitive. However, if a specified value includes a space, be sure to enclose the value in quotation marks (for example, "value with spaces").

Parameter	Description
/?	Displays the usage options for installation parameters.
/Q	Silent Install, install runs in a quiet mode without any user interface. This parameter is recommended if you are deploying the software installation using an IT tool or script, and don't expect to see any error or restart messages. When using this parameter, your IT tool or script should check the error codes and respond as needed. For example, if the installation returns error code 1641, then the IT tool or script should restart the computer and relaunch the installation after restart. This parameter is required if /QS or /Record is not specified.
/QS	Unattended Install, install runs in a quiet simple mode and shows progress through the UI, it does not accept any input but still shows error or restart messages. When using this parameter, you will not have to check the error codes, and the installation will stop and display a prompt if there are error or restart messages. For example, if an immediate restart is required to complete the install, a restart message will be displayed for you to confirm the restart. Installation resumes automatically from the point of interruption after restart. This parameter is required if /Q or /Record is not specified.
/IAcceptAllLicenseTerms	Acknowledges acceptance of the license terms. This parameter is required for /Q or /QS parameters.
/AutoRestart	Automatically restarts the computer after the installation is complete. Used when a restart is required to complete the installation. This parameter is optional. If this parameter is not used silent install (/Q) will return either error code 1641 or 3010 if a restart is required, and unattended install (/QS) will result in a confirmation prompt that must be agreed to before the installation is completed.
/SetupLanguage="value"	Specifies which language will be displayed during install process. The value must be the one of the following: • ENU • CHS • DEU • ESP • FRA • ITA • JPN • KOR • PTB This parameter is optional. If this parameter is not used, the default language is the current user or operating system user interface language.
/Record	Records the installation options chosen to a recording file. This parameter is optional.
/Playback	Plays back a recording file to specify the installation options. This parameter is optional.
/IgnoreWarning	Specifies that the setup ignores warnings and continues. This parameter is optional. If it is not specified, the setup exits when a warning occurs.

Parameter	Description
/Product="value"	Specifies which sub-products will be installed. The product name must be one of followings: • AssetCentre Server • AssetCentre Client • AssetCentre Agent • AssetCentre Custom Installation
/Uninstall	Uninstalls the product. This parameter is optional.
/ProductLanguage="value"	Specifies the language version of the software being installed. The value must be the one of the following: • ENU • CHS • DEU • ESP • FRA • ITA • JPN • KOR • PTB This parameter is optional. If this parameter is not used, the default language is the same as the setup language. If the software does not support multiple languages this parameter is not available.
/SerialNumber="value"	Specifies the serial number of the software being installed. This is used to activate the software during installation. This parameter is optional. If it is not specified the software must be activated manually after installation if activation is required. Some software does not require activation. If activation is not required this parameter is not available.
/ProductKey="value"	Specifies the product key used to get activation keys during installation. This parameter is optional. If it is not specified the software must be activated manually after installation if activation is required. Some software does not require activation. If activation is not required this parameter is not available.
/Version="value"	Specifies the version of the software to activate which corresponds to the product version associated with the SerialNumber and ProductKey. This parameter is optional. If it is not specified the installer will use the most recent product version available. Some software does not require activation. If activation is not required this parameter is not available.
/InstallDrive="value"	Specifies the install drive. This parameter is optional. If this parameter is not used, the default install location is "C:\Program Files (x86)\Rockwell Software".

Parameter	Description
	Some software restricts the installer to only change the drive the software is installed on. Use /? to determine which parameter is supported.
/ftsp-value="value"	Specifies the FactoryTalk security policy value. This parameter is optional. Use the **enable** or **disable** value to change the state of RequireComputerAccounts during installation.
/IISCommPort	Specifies the IIS server communication port for HTTPS. The default port for HTTPS is 443. If the HTTPS port was previously configured using FactoryTalk Services Platform, like port 4356, then the existing HTTPS port setting is retained. This parameter is optional.
/ftsp-s	Specifies the FactoryTalk Directory scope for restore. Only "Global" and "Local" scopes are supported. The SECURE.BAK backup file provided by Rockwell Automation is only supported for the "Global" scope. This parameter is optional.
/ftsp-bak	Restores the backup file and specifies where the restore file can be found. Rockwell Automation provides a SECURE.BAK backup file containing pre-configured access control lists which limit user access. The pre-configured access control lists follow Rockwell Automation recommended best practice. The SECURE.BAK backup file is located in the FactoryTalk Services Platform installation package, Redist\FTSPSecureBak. This parameter is optional.
/ftsp-pp	Specifies the plain text used to decrypt the backup file. This parameter is optional.
/FTSPWebAuth="value"	Specifies that the installation includes the FactoryTalk Web Authentication Server. This parameter is optional. The value must be one of the following: • **Yes** If the value is **Yes**, the FactoryTalk Web Authentication Server will be installed. The FactoryTalk Reverse Proxy will also be installed as it is required for operation of the FactoryTalk Web Authentication Server. • **No** If the value is **No**, the FactoryTalk Web Authentication Server will not be installed.
/ReverseProxy="value"	Specifies that the installation includes the FactoryTalk Reverse Proxy. This parameter is optional. The value must be one of the following: • **Yes** If the value is **Yes**, the FactoryTalk Reverse Proxy will be installed. • **No** If the value is **No**, the FactoryTalk Reverse Proxy will not be installed.
/FTSPWebEventServer="value"	Specifies that the installation includes the FactoryTalk Web Event Server. This parameter is optional.

Parameter	Description
	The value must be one of the following: • **Yes** If the value is **Yes**, the FactoryTalk Web Event Server will be installed. • **No** If the value is **No**, the FactoryTalk Web Event Server will not be installed.
/SystemStatusPortal="value"	Specifies that the installation includes the FactoryTalk System Status Portal. This parameter is optional. The value must be one of the following: • **Yes** If the value is **Yes**, the FactoryTalk System Status Portal will be installed. The FactoryTalk Reverse Proxy and FactoryTalk Web Authentication Server will also be installed as it is required for operation of the FactoryTalk System Status Portal. • **No** If the value is **No**, the FactoryTalk System Status Portal will not be installed.
/noHTTPS	Specifies that the setup turns off HTTPS and continues. This parameter is optional.
/SqlServer="value"	Specifies FactoryTalk AssetCentre database server (Microsoft SQL Server) location. This parameter is required when installing the FactoryTalk AssetCentre server software.
/MSA="value"	Specifies the Group Managed Service Account (gMSA) or Managed Service Account (MSA) that will be used by FactoryTalk AssetCentre Server to access the Microsoft SQL Server database when using Windows Authentication. • The parameter is required when the Microsoft SQL Server is hosted on a different computer than the FactoryTalk AssetCentre Server. • The parameter is optional when the Microsoft SQL and FactoryTalk AssetCentre Servers are hosted o the same computer.
/sql	Uses SQL Authentication between the FactoryTalk AssetCentre and Microsoft SQL Servers. The use of SQL Authentication is discouraged due to security concerns. This parameter is required if SQL authentication will be used over MSA.
/sa="value"	Uses SQL Authentication for SQL Server Logins. If you use SQL Server Authentication to perform silent or unattended installation, the parameters /SqlAdmin, and /SqlAdminPwd are required.
/SqlAdmin="value"	Specifies the Microsoft SQL Server administrator account name.
/SqlAdminPwd="value"	Specifies the Microsoft SQL Server administrator account password.
/DirectoryServer="value"	Specifies the FactoryTalk network directory if you are using a distributed system. This parameter is optional. If it is not specified, the software will use its current computer as the FactoryTalk Directory server. The value must be the host name of the FactoryTalk Directory server.
/ThirdPartyConnectorAccount="value"	Specifies a Windows user account with standard user permissions that you want to use to run the Agent Controller. This parameter is required if you want to use Siemens or Mitsubishi connectors in your system. The format for the "value" is domain\username.

Parameter	Description
	Note: After you specify the username, the Agent Controller mode will be run as an application.

Error codes

The following table identifies the error codes that can be returned by an installation.

Error Code	Value	Description
ERROR_SUCCESS	0	The installation completed successfully.
ERROR_INVALID_PARAMETER	87	One of the parameters was invalid.
ERROR_INSTALL_USEREXIT	1602	The installation was cancelled by the user.
ERROR_INSTALL_FAILURE	1603	A fatal error occurred during installation or the software component to be installed already exists on the computer.
ERROR_BAD_CONFIGURATION	1610	The configuration data for this product is corrupt. Contact your support personnel.
ERROR_REBOOT_CONTINUE	1641	A reboot is required to continue to installation.
ERROR_SUCCESS_REBOOT_REQUIRED	3010	A restart is required to complete the installation. After restart the product is successfully installed.
ERROR_REBOOT_PENDING	3012	A restart is pending and is required before the installation can continue.
ERROR_SUCCESS_NOT_APPLICABLE	3013	The installation cannot proceed because the products are already installed.
ERROR_SUCCESS_WARNING_REBOOT	3014	Install succeed with warnings. Check installation logs for details. A restart is required to complete the installation.

After the installation using the unattended setup

You can find the installation logs and view the installation status in the following path:

- On 64-bit operating systems:
  C:\Program Files (x86)\Common Files\Rockwell\Install Logs

Once the installation is complete, you need to activate FactoryTalk AssetCentre. For more information, see Step 6: Finish the installation on page 23.

After the installation using the unattended setup, you can configure FactoryTalk AssetCentre.

For details, see:

- Configure the TLS protocol for FactoryTalk AssetCentre on page 68
- Configure FactoryTalk AssetCentre on page 75

Configure the TLS protocol for FactoryTalk AssetCentre

Beginning with FactoryTalk AssetCentre version 13.00.00, it is required to turn on TLS 1.2 for secure communications within the FactoryTalk AssetCentre system. We recommend that you disable TLS 1.0 and TLS 1.1 in the system and we strongly recommend that you use a TLS certificate signed by a certificate authority (CA).

For more information about TLS protocol version support, see Protocols in TLS/SSL. For more information about the compatible operating system, see Software requirements on page 8.

IMPORTANT:

- When the installation environment is targeted to use TLS 1.3, note that FactoryTalk AssetCentre requires both TLS 1.2 and TLS 1.3 to be enabled. FactoryTalk AssetCentre will not work if only TLS 1.3 is enabled.
- Using the TLS protocol is an essential part for the communication security over your network.
- If you want to configure the protocols as needed, you should use the same protocol for all computers deployed in your network.

The configuration including these steps:

- Install a TLS Certificate on page 68
- Configure the HTTPS site binding on page 68
- Configure a firewall rule if the default port is modified on page 69

Install a TLS certificate

The steps to install a TLS certificate may depends on the certificate types and operating systems. The following instruction describes how to install a PFX or CER file on Windows Server 2022.

To install a PFX file containing the TLS certificate

1. On the Management of Change,FactoryTalk AssetCentre Server, Agent, Desktop Client, and Web Client computers, open Internet Information Services (IIS) Manager.
2. Under **IIS**, double-click **Server Certificates**.
3. In the **Actions** pane, select **Import**.
4. In the **Import Certificate** dialog box, select the **Browse** button.
5. Select the PFX file, and then select **Open**.
6. Enter the password.
7. Select **OK**.

To install a CER file containing the TLS certificate

1. On the Management of Change,FactoryTalk AssetCentre Server, Agent, Desktop Client, and Web Client computers, open Internet Information Services (IIS) Manager.
2. Under **IIS**, double-click **Server Certificates**.
3. In the **Actions** pane, select **Complete Certificate Request**.
4. On the **Specify Certificate Authority Response** page, click the **Browse** button.
5. Select the certificate file, and then select **Open**.
6. In the **Friendly name** box, enter a name for the certificate.
7. Select **OK**.

Configure the HTTPS site binding

After installing the certificate, ensure that the TLS certificate is selected for the HTTPS site binding.

To select a TLS certificate for the HTTPS site binding

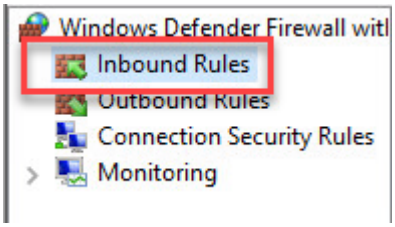
1. On the Management of Change, FactoryTalk AssetCentre Server, Agent, Desktop Client, and Web Client computers, go to **Site Bindings** in the Internet Information Services (IIS) **Default Web Site**.
2. In the **Actions** pane, select **Bindings**.
3. In the **Site Bindings** dialog box, select the HTTPS site binding, and then select **Edit**.
4. From the **SSL certificate** list, select the desired certificate.
5. Select **OK**.

Configure a firewall rule if the default port is modified

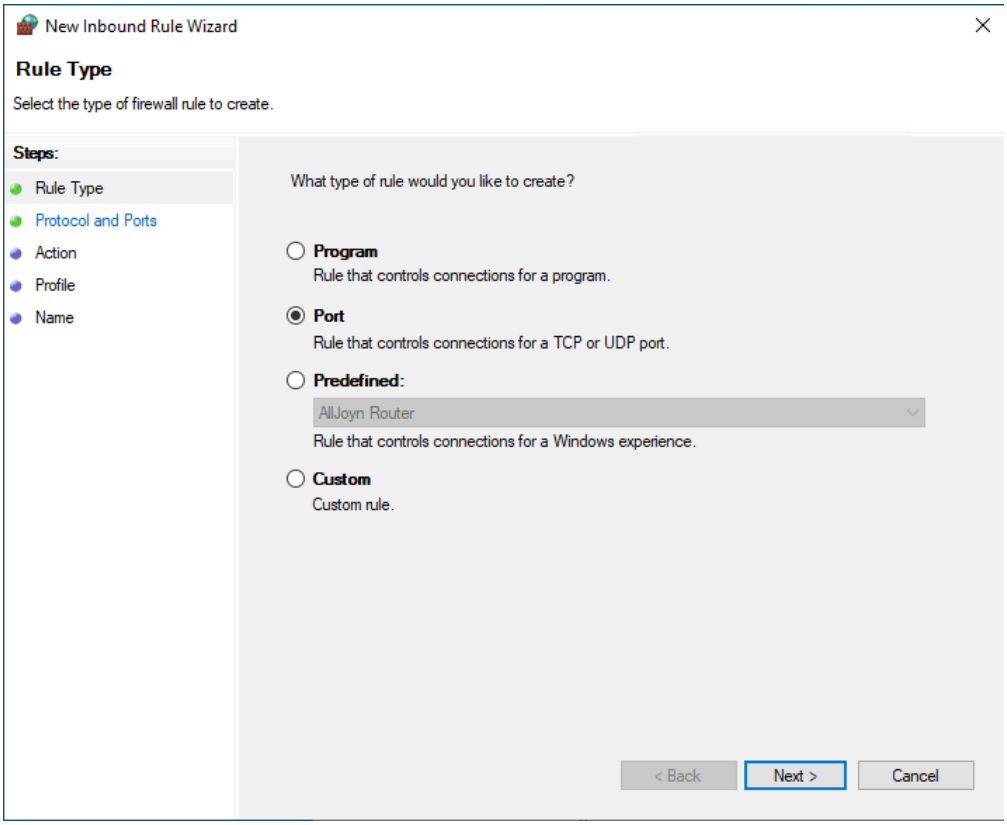
If the default port 443 is modified during the site binding configuration, you need to configure a Windows firewall rule for the self-defined port.

To configure a Windows firewall rule

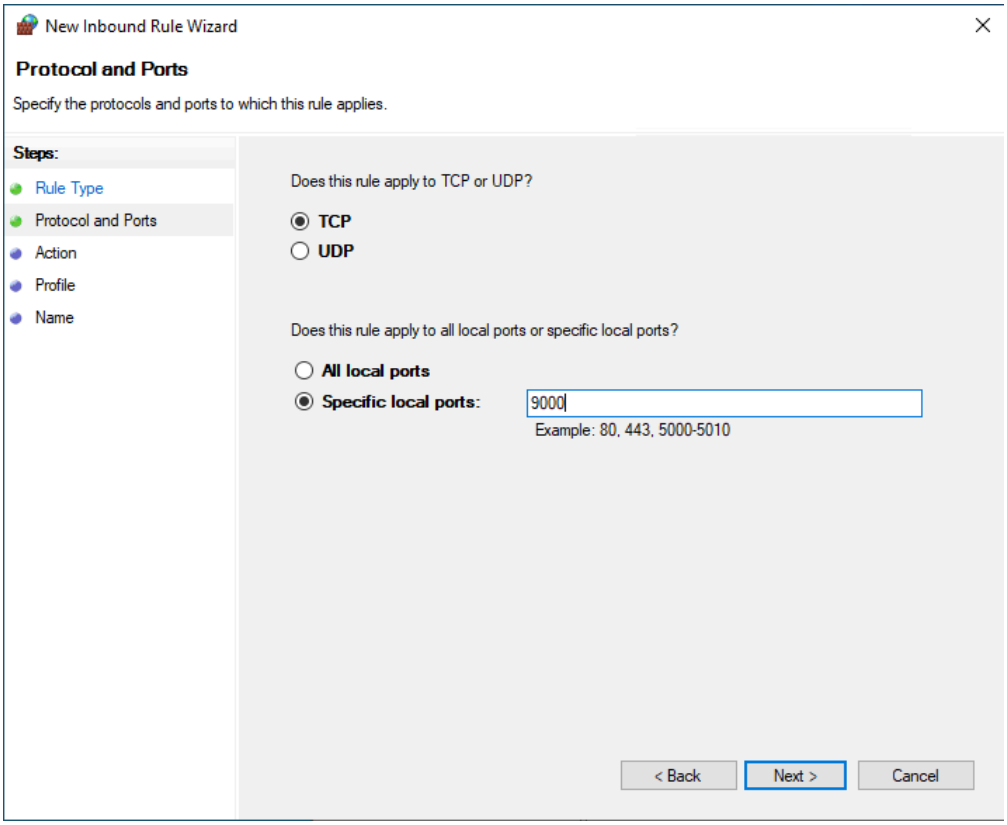
1. On the FactoryTalk AssetCentre server computer, click **Start**, type *firewall*, and then click **Windows Defender Firewall with Advanced Security**.
2. Click **Inbound Rules**.



3. Click **Action > New Rule**.
4. In the **New Inbound Rule Wizard**, select **Port**, and then click **Next**.

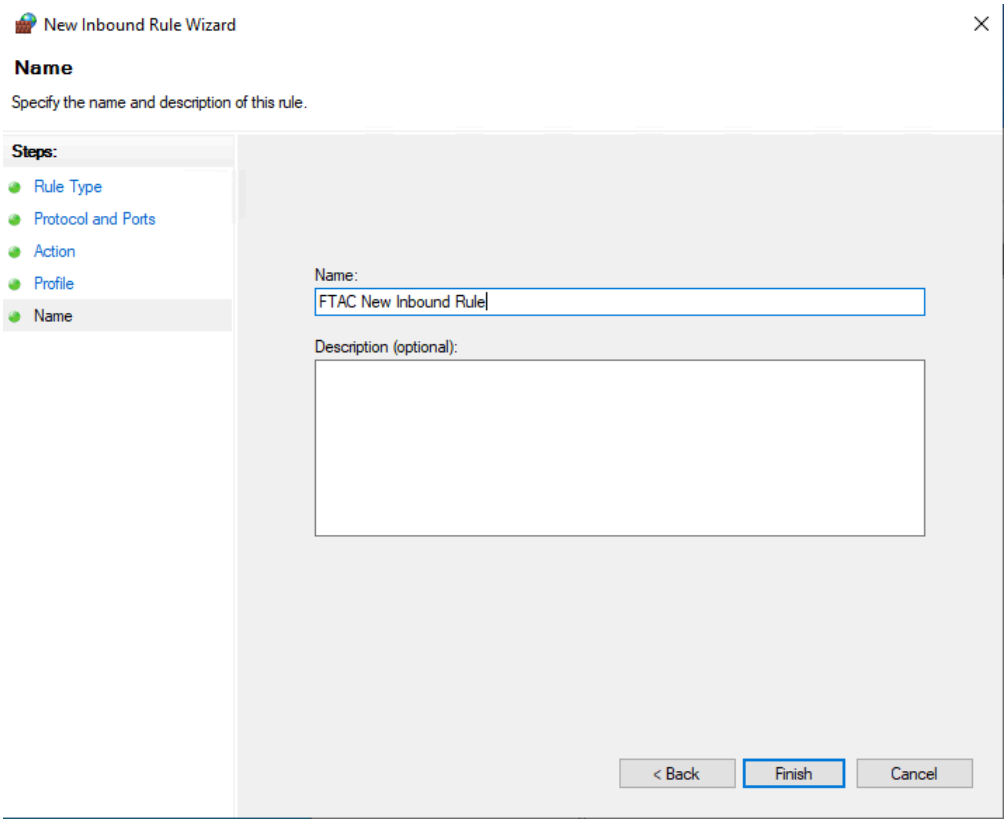


5. In the **Specific local ports** box, enter the self-defined port as set during the site binding configuration, for example *9000*, and then click **Next**.

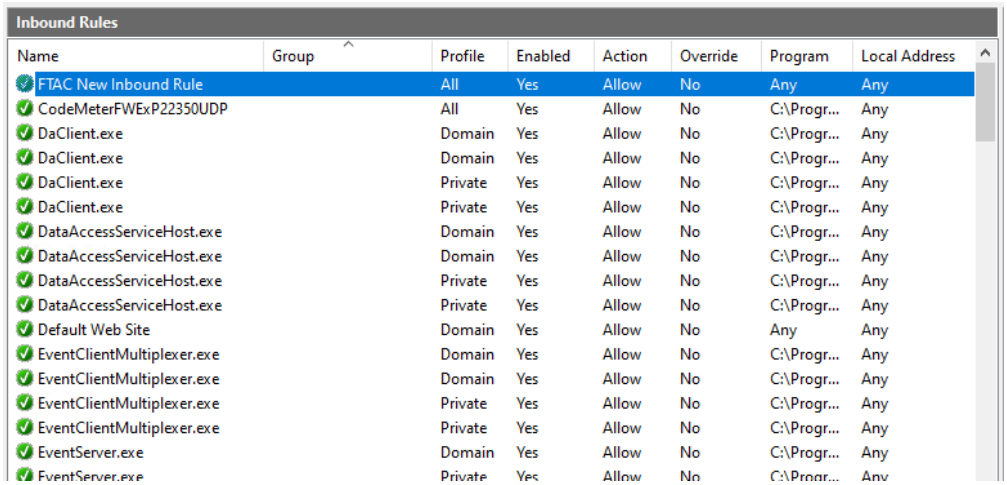


6. Follow the on-screen instructions until you get to the **Name** page.

7. In the **Name** box, enter the name for the new inbound rule, and then click **Finish**.



The new rule is shown in the list.



Configure Windows Authentication

Windows Authentication is a secure way of authentication that uses the username and the password of the user logged on to the operating system. In the communication secured with Windows Authentication mode, the username and the password are sent between the client and the server in a strongly hashed form.

Windows Authentication may be enabled in corporate networks that use Microsoft Active Directory services as well as other ways to identify users.

By turning on Windows Authentication mode you increase the security of the communication between the FactoryTalk AssetCentre server, client(s) and agent(s) and prevent unauthorized users from accessing the FactoryTalk AssetCentre server.

IMPORTANT: For the purposes of FactoryTalk AssetCentre, Windows Authentication mode should be enabled only in corporate networks that use Microsoft Active Directory services.

After you turn on Windows Authentication mode, the access to the page:

http(s)://assetcentre_server_full_name/rockwellsoftware/assetcentre

...will be secured from being accessed by anonymous users.

In order to access the page, the users will need to log on using their Windows username and password.

This chapter describes:

Turn on Windows Authentication mode in Internet Information Services (IIS)

To turn on Windows Authentication mode in Internet Information Services (IIS)

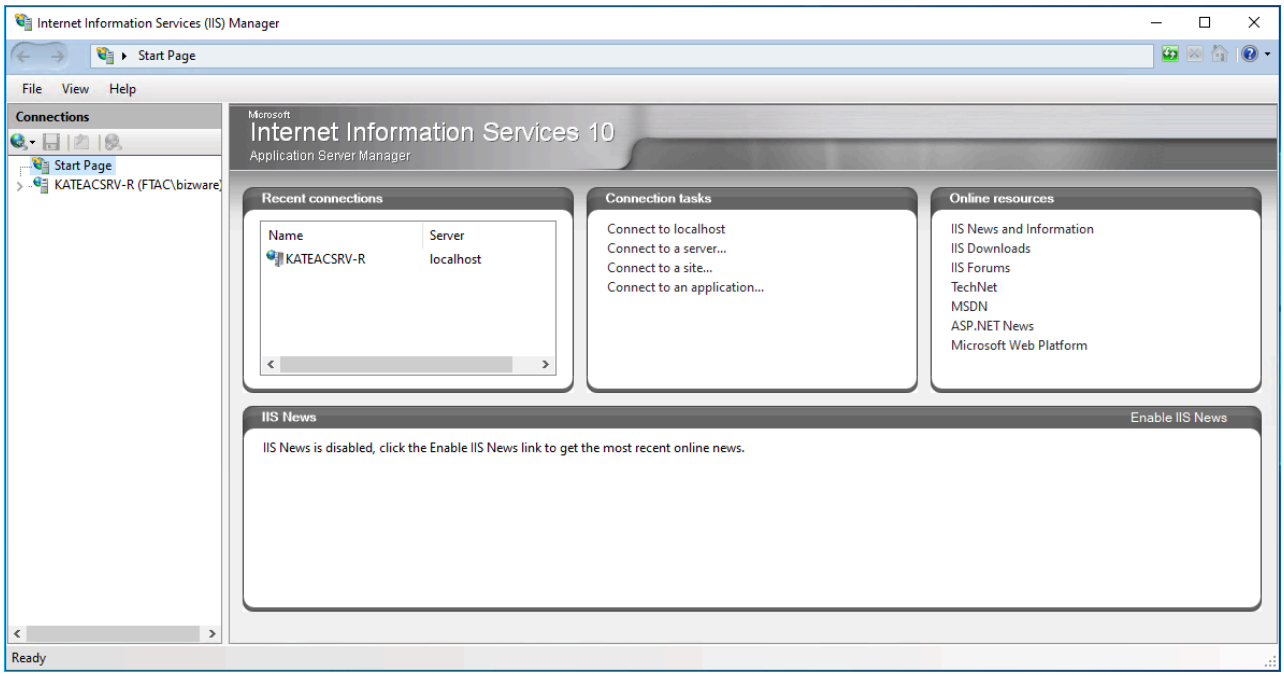
1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer.

   On Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2:

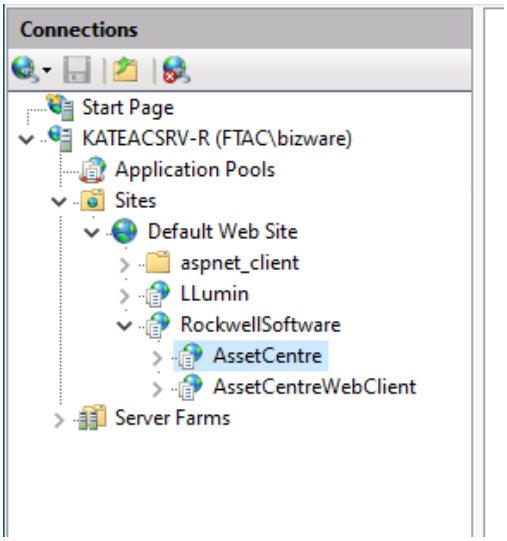
   a. On the taskbar click 

   b. In the search box, type *inetmgr*, and then press **Enter**.

   c. Click the best match result.



2. Under **Connections**, expand the tree, and then click **AssetCentre**.

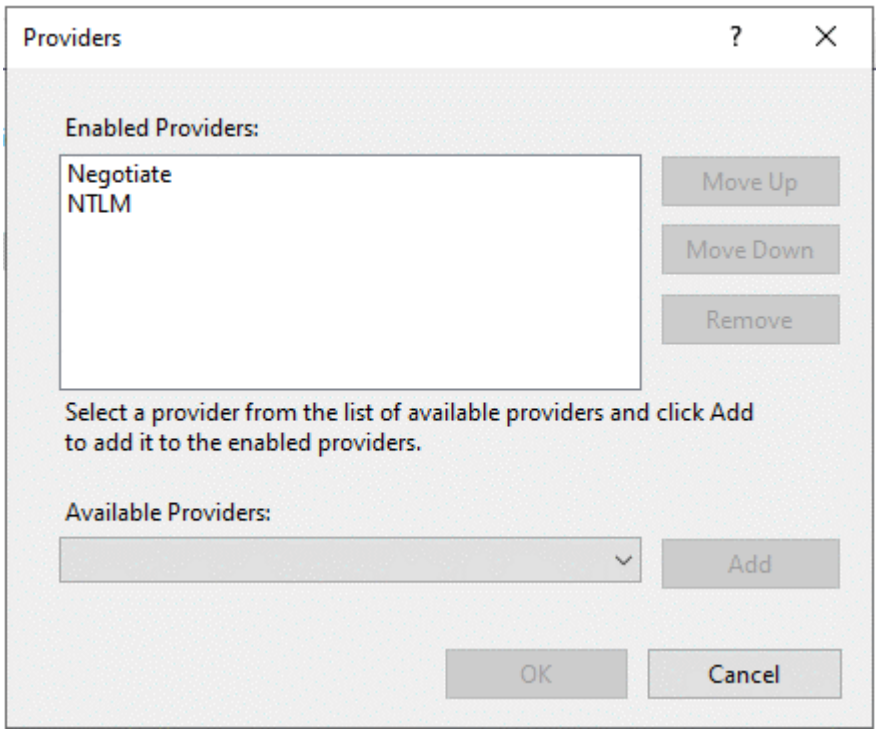


3. In **Features View**, double-click **Authentication**.
4. Under **Authentication**, click **Windows Authentication**.
5. Under **Actions**, click **Providers**.

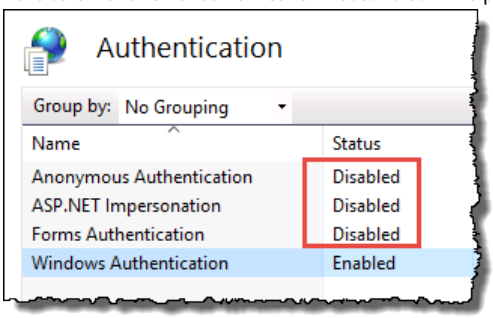
   The **Providers** dialog box appears.

6. Make sure that you have the following providers selected in the order presented in the figure below.

If these providers are not listed, select each of them in the list under **Available Providers**, and then click **Add**.



7. Make sure that all other authentication modes listed in the pane under **Authentication** are disabled.



IMPORTANT: When running FactoryTalk AssetCentre in a workgroup environment, Internet Information Services (IIS) **Anonymous Authentication** is enabled by default. **Anonymous Authentication** is required for proper operation of the system. To mitigate any security-related concerns, you must run FactoryTalk AssetCentre in a domain environment.

Configure FactoryTalk AssetCentre

This chapter describes:

Configure for client access to the server

For clients to be able to access the FactoryTalk AssetCentre server, the FactoryTalk Directory and FactoryTalk Security must be configured to give clients access. To configure access, you will need to use the FactoryTalk Administration Console.

The FactoryTalk Directory uses two factors to determine who should have access to any given function:

- **The user's account,** which can either be a FactoryTalk Directory account or a Windows domain account. This identifies the user.
- **The computer from which the user is accessing the FactoryTalk Directory.**
  This allows you to limit which computers can access the directory, and also allows you to determine whether certain functions can or cannot be performed from a given computer. For example, you can configure the FactoryTalk Directory to give access to a user from her or his own computer but not from another computer.

At a minimum, you must add the FactoryTalk AssetCentre users and their computers to the FactoryTalk Directory, and you must configure access privileges for FactoryTalk AssetCentre in the FactoryTalk Directory.

Add users to the FactoryTalk Directory

A user must be able to authenticate with the FactoryTalk Directory in order to be authorized to use FactoryTalk AssetCentre.

Tip: This section contains only basic instructions for using the FactoryTalk Directory and FactoryTalk Security. For background information and information regarding more advanced procedures, see the Help section in FactoryTalk Administration Console.

By default, all members of the Administrators group on the computers on which you installed the FactoryTalk Services Platform were added to the Administrators group in the FactoryTalk Directory. Also, any rights that you assign to a Windows User Group are assigned to all members of that group.

We recommend that you use a native FactoryTalk Group with Windows AD linked Group. This practice simplifies the process of confirming the security configuration as testing is performed on the native FactoryTalk Group, and policy is written about which Windows user and groups are added to the native FactoryTalk group.

To add a user to the FactoryTalk Directory

1. Start the FactoryTalk Administration Console:
   a. Click **Start**, and then use search to search for *FactoryTalk Administration Console*.
   b. Click **FactoryTalk Administration Console**.
   FactoryTalk Administration Console appears.
2. Log on to the Network directory using a FactoryTalk Administrator account.
3. Open the **Users and Groups** folder.
4. Under the **Users and Groups** folder, right-click the **Users** folder, and then select **New**.

5. Determine how you want to add user accounts to the system. You can add users indirectly by adding Windows-linked Groups or Azure AD Groups. Or, directly add users using Windows-linked User or native FactoryTalk User accounts. For more information, see "Accounts and groups" in *FactoryTalk Services Platform Help*. Consider the following:
   - Adding user accounts indirectly, using groups, is a best practice. Adding user accounts indirectly moves group management, that is, who is a member of which group, from the FactoryTalk system administrator to IT.
     This technique also simplifies commissioning as a group's permissions are validated in the system, but group membership is determined by policy or standard operating procedures. Further abstracting the security design by adding Windows-linked or Azure AD groups to a native FactoryTalk Groups that are used within the system's access-control lists results in a security system that is more maintainable and sustainable.
   - Windows-linked groups and Windows-linked users can be part of either a Microsoft Active Directory domain or local to a specific computer.
     The Microsoft Windows operating system is used to authenticate user credentials and determine Windows group membership. When disconnected from the network, the system can use valid cached Windows user credentials to perform authentication.
   - Azure AD groups requires the FactoryTalk Directory server has access to the Microsoft Azure. The system utilizes Microsoft Azure to authenticate user credentials and determine Azure AD group membership. When disconnected from the network, a user that is a member of an Azure AD group cannot be authenticated.
   - Native FactoryTalk User accounts are managed solely by the FactoryTalk system. Their access is independent of the Windows operating system. The FactoryTalk system authenticates the user and determines group member ship. When disconnected from the network, a user is authenticated using local valid FactoryTalk Directory cache. If the local FactoryTalk Directory cache has expired, the user cannot be authenticated.
6. Enter the information for the user.

Add computers to the FactoryTalk Directory

When FactoryTalk Services Platform is installed on a computer, that computer is automatically added to the FactoryTalk Network Directory. FactoryTalk Services Platform is included in the FactoryTalk AssetCentre installation, so your client computers should already be in the FactoryTalk Network Directory.

By default, for a user to be able to use FactoryTalk AssetCentre, the user's computer must be in the FactoryTalk Directory. If you want to pre-add user's computers to the system, refer to the FactoryTalk Help in the FactoryTalk Administration Console.

Tip: If you have a significant number of computers for which you need to permit or restrict access, consider grouping them to make assigning security privileges easier. For example, you can group all of the computers used in offices away from the plant floor and restrict access to features that should be used only from computers stationed where the user can see the automation system directly. For information about grouping computers, see the Help for the FactoryTalk Administration Console.

Configure feature security for FactoryTalk AssetCentre users

By default, all users and the Administrators group in FactoryTalk Directory can perform any task in the FactoryTalk AssetCentre software. To deny specific users the right to perform tasks in FactoryTalk AssetCentre, you must edit the **Feature Security** settings in the FactoryTalk Administration Console.

IMPORTANT: Never explicitly deny rights to the All Users or Administrators group in FactoryTalk. Rather, set up specific user groups of your own and deny rights to those groups. Denying rights to All Users or Administrators could lock everyone out of the system and would deny rights in all FactoryTalk-enabled products using any FactoryTalk CPR 9 version.

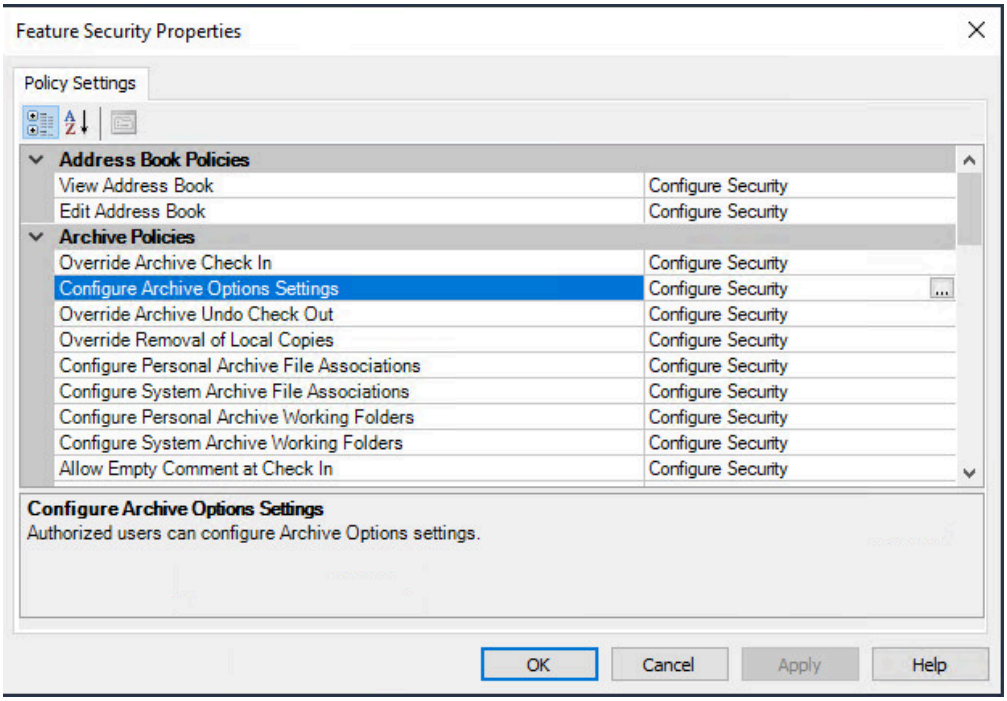
To change which users can perform tasks in FactoryTalk AssetCentre

1. Start the FactoryTalk Administration Console:
   a. Click **Start**, and then use search to search for *FactoryTalk Administration Console*.
   b. Click **FactoryTalk Administration Console**.
   FactoryTalk Administration Console appears.
2. Log on to the Network directory using a FactoryTalk Administrator account.
3. In the **Explorer** pane of the FactoryTalk Administration Console, navigate to **System > Policies > Product Policies > FactoryTalk AssetCentre**.
4. Double-click **Feature Security**.

IMPORTANT: There is also a Server Settings object in the FactoryTalk AssetCentre folder. Do NOT attempt to change any of the settings in this object. Doing so may render your FactoryTalk AssetCentre system inoperative. If you need to change server settings (to use a different mail server, for example), from **Windows Start** menu, select **Rockwell Software > FactoryTalk AssetCentre Server Settings**.

---

5. In the **Feature Security Properties** window, click the policy you want to change, and then click the browse button for the policy.
See Policy settings and their meanings on page 77.



6. In the **Configure Securable Action** dialog box, select the user or group for whom you want to assign permissions. If the user or group does not appear in the list, click **Add**, click **Show all**, select the user or group, and then click **OK**.
7. Click the appropriate box to allow or deny the user permission to the selected feature.
8. Click **OK**.

Policy settings and their functions

The following table shows the policy settings and their functions.

This policy setting	Controls whether users can
View Address Book	View the Address Book (which contains addresses for the purpose of sending automatic e-mail notifications).

This policy setting	Controls whether users can
Edit Address Book	Edit or add contacts and groups in the Address Book (which contains addresses for the purpose of sending automatic e-mail notifications).
Override Archive Check In	Check in a file regardless of who checked it out or from where it was checked out.
Configure Archive Options Settings	Turn on or off the function that allows Logix Designer to perform archive activities, such as file check-in, without direct interaction with the FactoryTalk AssetCentre Desktop Client and Web Client. FactoryTalk AssetCentre Diagnostics Connector installation is mandatory if only FactoryTalk AssetCentre Web Client is used.
Override Archive Undo Check Out	Undo a check out even if a different user checked the file out.
Override Removal of Local Copies	Choose to keep local copies of checked-in files on their computer. If this right is allowed, the user can keep local copies. If this right is denied, the user is not given this option.
Configure Personal Archive File Associations	Configure which software product launches when opening a particular type of file. If a personal file association is set, it will take precedence over the system file association.
Configure System Archive File Associations	Configure which software product launches when opening a particular type of file. This setting applies unless the user has specified a personal file association.
Configure Personal Archive Working Folders	Set a personal working folder for checking out files.
Configure System Archive Working Folders	Set the system working folder to which all users check out files unless they have a personal working folder.
Allow Empty Comment at Check In	Leave the comment field empty as they check in an asset.
Allow Empty Comment at Check Out	Leave the comment field empty as they check out an asset.
Clear the Get Writable Copy check box by default	Enable or clear the Get Writable Copy check box during get. Denying this permission enables the Get Writable Copy check box; a Get retrieves a writable copy of an Archive object. Allowing this permission (by default) clears the Get Writable Copy check box; a Get retrieves a read-only copy of an Archive object.
Store Latest Version Only	Choose to store only the latest version in the Archive.
Set Maximum Versions	Configure the total maximum number of versions stored in the Archive.
Configure Asset Inventory Settings	Configure the settings in the Asset Inventory window.
Configure Assets Lifecycle Sync	Synchronize lifecycle information in the FactoryTalk AssetCentre Server, Desktop Client, and Web Client with the Rockwell Automation lifecycle website.
Display Calibration Management Data*	View Calibration Management data in FactoryTalk AssetCentre.
Perform Calibration Management*	Access Calibration Management functionality in ProCalV5 software.
Administer Calibration Users*	Administer users, groups, and permissions in ProCalV5 software. Note that this policy only determines if the user is automatically added to the Administrator group in the ProCalV5 software. Once the user is added to ProCalV5, changing this policy for an AssetCentre user does not change the user's ProCalV5 security permissions.
Configure Database Limitations	Configure the total maximum size of the AssetCentre database, the size warning levels, the maximum number of versions per archive asset, the maximum size of Event, Audit, and Diagnostics logs, and the database capacity status refresh rate.
Configure Database Maintenance	Configure automatic database maintenance, manually analyze, or rebuild index fragmentation.
Run Archive Database Cleanup Wizard	Run the Archive Database Cleanup Wizard to delete unused versions of files.

This policy setting	Controls whether users can
Run Log Database Cleanup Wizard	Run the Log Database Cleanup Wizard to remove old records from the logs. Data can be exported and saved in a separate file.
Switch to Design mode	Enter Design mode, in which the user can edit the asset tree.
Use Web Client	Authorized users can use FactoryTalk AssetCentre Web Client.
Change Server Settings	Authorized users can run the Server Settings Utility and change system settings.
Configure Options	Authorized users can configure the system and client options.
View Event Log	Show the Event Log and run a search on the Event Log.
View Audit Log	Show the Audit Log and run a search on the Audit Log.
View Diagnostics and Health Log	Show the Diagnostics and Health Log and run a search on the Diagnostics and Health Log.
Change Diagnostics and Health Log Message	Change the status of or add a comment to a Diagnostics and Health Log record.
View Diagnostics and Health Log Status	View a status history for a Diagnostics and Health Log record.
Enable or Disable DTMs*	Enable and disable DTMs in the DTM Catalog.
Edit DTM Network*	Show the DTM Networks dialog box to edit the DTM network.
Run PDC Field Edition*	Use the Process Device Configuration Field Edition software.
Create a new schedule	Create a schedule.
Edit a schedule	Change existing schedules.
Delete a schedule	Delete schedules.
View a schedule	Show the Schedules tab.
Command a schedule	Issue commands to a schedule, such as making the schedule active or running the schedule immediately.
Create a Search	Set up a new search to find entries matching specified criteria in one of the logs, in the Archive History, or in Archive Check Out Status information.

* Starting from FactoryTalk AssetCentre version 10.00, process device capabilities are not supported. The policies marked with asterisk are only kept for viewing purposes if you have upgraded FactoryTalk AssetCentre from version 9.00 or earlier.

About FactoryTalk AssetCentre Web Client

FactoryTalk AssetCentre Web Client is a web application that provides access to the FactoryTalk AssetCentre system from a web browser. As opposed to the FactoryTalk AssetCentre Desktop Client with full read-and-write functions, the web client allows you to do the following to monitor your factory automation system:

- View the asset tree and archive workspace.
- Check in and check out files or binders, undo a check-out, unblock a workflow, pin, unpin, label, and promote files and binders, view and remove labels, and copy a version from backup data to configuration data.
- View, update, refresh, report lifecycle information, view, filter, and sort report.
- View, filter, and sort logs.
- Create, edit, delete, activate or deactivate, run, stop, filter, and sort schedules.
- Run, filter, and sort searches.
- View database information, set database limitations, analyze index fragmentation, and rebuild fragmented indexes.
- Create a log cleanup schedule.

We recommend that you use the TLS protocol with FactoryTalk AssetCentre Web Client. See Configure the TLS protocol for FactoryTalk AssetCentre on page 68.

Access FactoryTalk AssetCentre Web Client

You must sign in every time you try to open the web client with a browser.

To sign in to FactoryTalk AssetCentre Web Client

1. From the **Start** menu, select **FactoryTalk AssetCentre Web Client**, or open the browser, and then enter the URL address http://<FQDN>/RockwellSoftware/AssetCentreWebClient.

   Tip: FQDN is the fully qualified domain name of the FactoryTalk AssetCentre Server computer.
   If you are changed the default port in site binding, you need to include the self-defined port number in the computer name part in the form as *MYSERVER:PortNumber*.

2. On the AssetCentre Web Client page, enter the user name and the password.

   IMPORTANT: You can sign in to FactoryTalk AssetCentre Web Client using a FactoryTalk user or Windows-linked user.

3. Select **Sign in**.

Configure Idle Time-out property in Internet Information Services (IIS) Manager

When no interaction with the web client has occurred for 20 minutes, you will be automatically signed out. You can adjust the Idle Time-out property using the Internet Information Services (IIS) Manager.

To configure Idle Time-out property in Internet Information Services (IIS) Manager

1. Open **Internet Information Services (IIS) Manager** on the FactoryTalk AssetCentre server computer.
2. In the **Connections** pane, select **Application Pools**.
3. Under Application Pools, right-click **AssetCentreWebClient**, and then select **Advanced Settings**.
4. Do the following to configure Idle Time-out property:
   - To adjust the length of time before the user is automatically signed out:
     Adjust **Idle Time-out (minutes)** as desired. The default length of time is 20 minutes.

- To prevent the user from being automatically signed out:

  Change **Idle Time-out Action** by selecting **Suspend** from the dropdown menu. The default selection is Terminate.

Uninstall FactoryTalk AssetCentre

Uninstall FactoryTalk AssetCentre software version 8.00 or later from Programs and Features in Windows Control Panel or using a command.

Tip: To uninstall FactoryTalk AssetCentre version 7.10 or earlier, use Windows Control Panel.

Uninstall from the Control Panel

To uninstall FactoryTalk AssetCentre from the Control Panel

1. Depending on how the software component was installed with the Setup wizard, the uninstallation varies.
   - If only installed with **AssetCentre Server**, double-click **FactoryTalk AssetCentre Server 13.00.00**.
   - If only installed with **AssetCentre Agent**, double-click **FactoryTalk AssetCentre Agent 13.00.00**.
   - If only installed with **AssetCentre Desktop Client**, double-click **FactoryTalk AssetCentre Client 13.00.00**.
   - If installed with **AssetCentre Custom Installation**, double-click **FactoryTalk AssetCentre 13.00.00**.
2. Select **Uninstall**.
3. Select **Close** or restart the computer.

Uninstall using a command

When uninstalling with a command, it uninstalls components that are already installed with the product specified. It does not uninstall components, such as FactoryTalk Activation Manager, that are shared with other products. You need to manually uninstall them in Control Panel.

To uninstall FactoryTalk AssetCentre using a command

1. Close all Windows programs.
2. Open the **Command Prompt** window.
3. In the **Command Prompt** window, navigate to *D:*, where *D:* is the drive containing the FactoryTalk View installation package.
   In this example, type *D:* and press **Enter**.

   Tip: If **User Account Control** dialog box shows, click **Yes.**

4. Type a command with the following syntax and press **Enter**.

```
Setup.exe /Q /Uninstall /Product=product_name
```

For example, to uninstall FactoryTalk AssetCentre Desktop Client, use the following command:

```
Setup.exe /Q /Uninstall /Product="AssetCentre Client"
```

The following table shows command-line parameters for this mode:

Parameter	Description
/Q	Required if /QS is not specified. Uninstalls the product in the silent mode without any user interface during uninstallation.

Parameter	Description
/QS	Required if /Q is not specified. Uninstalls the product in the unattended mode during uninstallation, and shows the progress, errors, or complete messages on the user interface.
/Uninstall	Required. Uninstalls components that are already installed with the product specified.
/Product= *product_name*	Required. Specifies which product will be uninstalled. The parameter value must be the one of following: • AssetCentre Server • AssetCentre Client • AssetCentre Agent • AssetCentre Custom Installation

Troubleshoot FactoryTalk AssetCentre

This chapter describes:

General installation

A red x appears next to an item to be installed

The initial window in each installation (server, desktop client, and agent) shows a list of all necessary components, whether they were found on the computer, and whether they will be installed. If the installer could not determine whether the correct version already exists on that computer, a red x is shown next to a component .

Contact Technical Support using the contact information provided on the copyright page at the beginning of this guide.

A Program Maintenance window appears

This indicates that the component of the software you are installing is already installed. You do not need to install it again. If you suspect your installation is damaged, you can choose to repair the installation.

Server installation

SQL collation error encountered during database installation

The SQL Server collation must be case-insensitive for use with FactoryTalk AssetCentre software. If your SQL Server collation is case-sensitive, the FactoryTalk AssetCentre database installation will fail. If your SQL Server collation is case-sensitive, see Install Microsoft SQL Server on page 14 for detailed directions.

Change the FactoryTalk AssetCentre SQL server instance

For FactoryTalk AssetCentre version 8.00 and earlier, the repair function executes the same workflow which PlantPax team uses. Since version 9.00, FactoryTalk AssetCentre starts to use the silent repair of the common install. You cannot change the FactoryTalk AssetCentre SQL server instance during repair progress. If you need to change the FactoryTalk AssetCentre SQL server instance after installing the FactoryTalk AssetCentre server software, you can follow the steps as below:

1. Install FactoryTalk AssetCentre server, desktop client, agent, and SQL Express on a single Server 2016 instance.
2. Install SQL Server 2016 on a separated computer.
3. On the FactoryTalk AssetCentre server computer, run the utility **FTAssetCentre.DbInstaller.exe** in C:\Program Files (x86)\Rockwell Software\AssetCentre Server \Bin\RockwellAutomation, and then enter their SQL information which is on the separated computer.
4. Then run **FTAssetCentre.AosCatalogImport.exe** in C:\Program Files (x86)\Rockwell Software\AssetCentre Server\Bin\ RockwellAutomation.
5. Restart FactoryTalk AssetCentre server computer. At this time, the FactoryTalk AssetCentre server has pointed to the new SQL DB server. The FactoryTalk AssetCentre server, agent, and desktop client are working normally with new FactoryTalk AssetCentre SQL server instance.

Unable to log on to SQL Server during server installation

In FactoryTalk AssetCentre Server version 10.00.00 and later, SQL Server sa (system administrator) account is only available for silent or unattended installation.

- If you configured your SQL Server to use mixed (both SQL Server and Windows domain) authentication, the sa account is available. Use the password you created for the sa account when the installation program prompts you for it.
- If your SQL Server installation is not configured for mixed authentication, you will need to change the authentication method. See the documentation for SQL Server for more information.

Tip: New installations of FactoryTalk AssetCentre Server installation require that the Windows account of the user performing the installation, or a Windows group of which the user performing the installation is a member, is assigned the Microsoft SQL Server System Administrator role before attempting the installation. This change is optional for Upgrade installations.

- If you have forgotten your sa account password, you will need to change it. See the Microsoft SQL Server documentation for more information.

The application failed to initialize properly

This is a known issue with Symantec Endpoint Protection. When installing the FactoryTalk AssetCentre server on a computer that has Symantec Endpoint Protection version 11.0.5002.333, you may receive an error message indicating that the application you are installing fails to initialize properly.

To fix this issue

- Use a different Symantec Endpoint Protection version.
- Disable the Symantec Application and Device Controller service by following the steps below:
  a. From **Windows Start** menu, select **All Programs > Accessories > Command Prompt**.
  b. In the **Command Prompt** window, enter *sc config sysplant start=disabled* and press **Enter**.
  c. Restart the computer and try to install the server again.

Desktop client and agent installation

Check whether the desktop client is installed correctly

To check whether the desktop client is correctly installed and connected to the FactoryTalk AssetCentre server

1. Click **Start**, and then use search to search for FactoryTalk AssetCentre Client.
2. Click **FactoryTalk AssetCentre Client**.
   FactoryTalk AssetCentre Client appears.
   When the client runs, it checks the server for the latest version of the client software. If the client software is not the latest version, the following message is displayed:
   The client and server versions are incompatible.
   To update the client software, follow the Steps to install the FactoryTalk AssetCentre Desktop Client software on page 28 at the start of Chapter 4.
   For information on getting started with the software, see the *FactoryTalk AssetCentre Getting Results Guide*.

Check whether the agent software is current

Unlike the FactoryTalk AssetCentre desktop client, the FactoryTalk AssetCentre agent does not show a message if the agent does not have the latest version of the software. Instead, the agent does not start, and logs a message in the **System Event** log and the **AssetCentre Event** log.

To check whether the FactoryTalk AssetCentre software on the agent is up to date

1. Click **Start**, and then use search to search for FactoryTalk AssetCentre Client.
2. Click **FactoryTalk AssetCentre Client**.
   FactoryTalk AssetCentre desktop client appears.
3. Check the number of running agent computers.
   It is displayed in the bottom right corner of the window on the status bar. If one or more agents are not running, and the desktop client software has been recently updated, then the agent software may need to be updated as well.
   To update the agent software, follow the Steps to install the FactoryTalk AssetCentre Agent software on page 24.

Error reading Primary Server Name from FactoryTalk Directory

This error occurs when the computer on which you are installing the desktop client is not using the same FactoryTalk Directory as the computer running the FactoryTalk AssetCentre server, or there was an error in the FactoryTalk Services Platform.

To solve this problem

1. On the FactoryTalk AssetCentre server computer, set the FactoryTalk Directory location.
   From **Windows Start** menu, select **Rockwell Software** > **Specify FactoryTalk Directory Location**.
2. Log in if prompted to do so, and then specify the location of the FactoryTalk Directory.
3. Close any clients that are connected to the server.
4. Restart the FactoryTalk Directory Server.

Logged in user is not part of the Administrators group

Currently logged in Windows user is not part of the Administrators group.

To resolve this problem, make sure you are installing the software as an administrator, or a user with administrative privileges.

Start the desktop client

Error initializing FactoryTalk AssetCentre

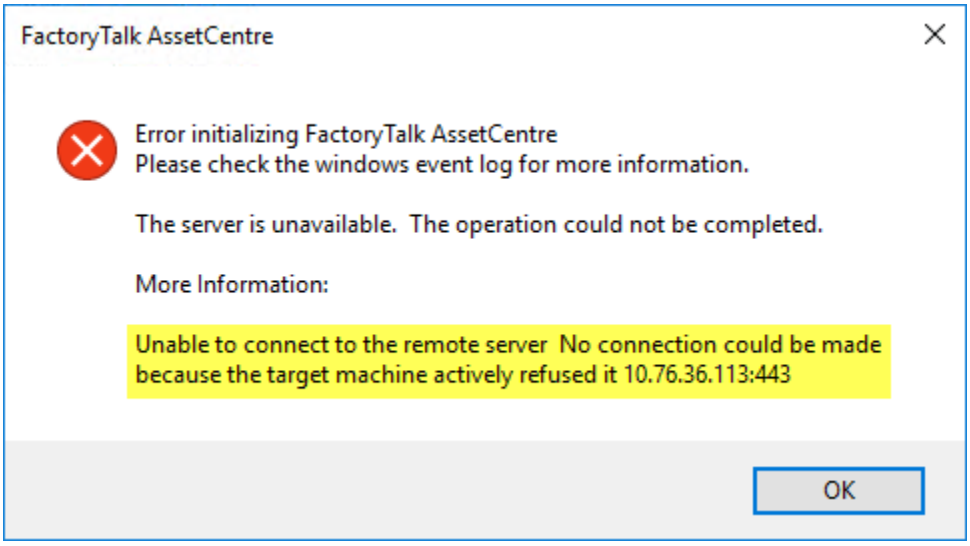
The FactoryTalk AssetCentre server may have failed (or you may have lost your network connection to the server), or the computer on which you installed the desktop client may not be part of the FactoryTalk Directory.

To solve the problem

- Check the server (see Other errors starting the desktop client on page 91).
- Try adding the client computer to the FactoryTalk Network Directory. From another computer that has access to the FactoryTalk Directory (the FactoryTalk AssetCentre server, for example), use the FactoryTalk Administration Console to add the computer to the FactoryTalk Directory. See Add computers to the FactoryTalk Directory on page 76.
- See If the FactoryTalk AssetCentre server is installed to a drive other than C on page 90.

Error initializing FactoryTalk AssetCentre: unable to connect to the remote server

When starting the FactoryTalk AssetCentre Desktop Client, you may get the following error:



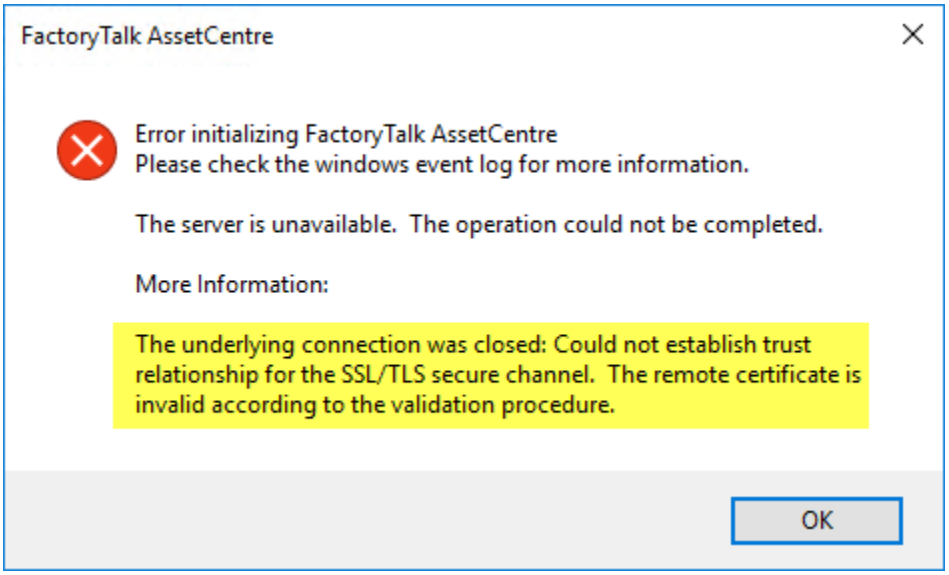
The error message may appear when you have checked the **Use the secure communication channel** option in the **Configure Server Settings Utility** window, but you haven't configured the SSL protocol.

To solve the problem

- Configure the SSL protocol.
  See Configure the SSL protocol for FactoryTalk AssetCentre on page 68.
- Clear the **Use the secure communication channel** check box in the **Configure Server Settings Utility** window, if you don't want to use the SSL protocol.

Error initializing FactoryTalk AssetCentre: the underlying connection was closed

When starting the FactoryTalk AssetCentre Desktop Client, you may get the following error:



The error message may appear in the following cases:

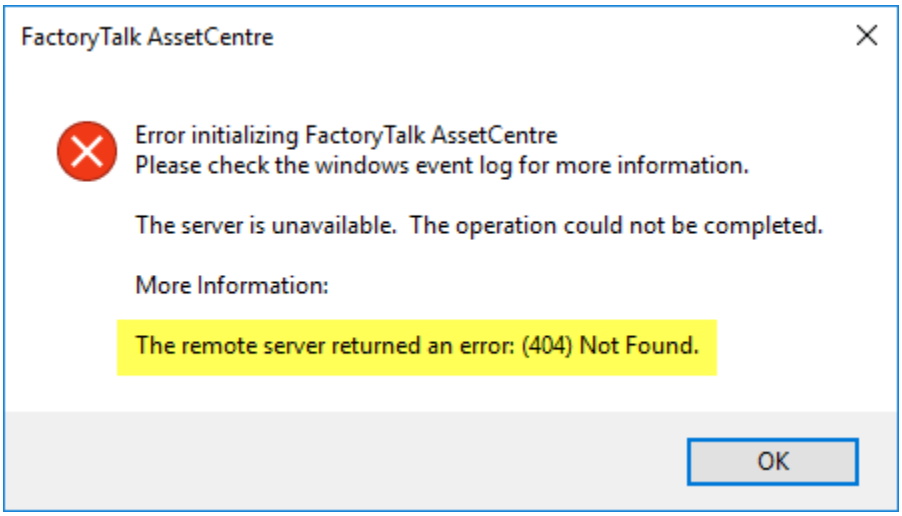
- You have provided an incomplete fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server computer in the **Configure Server Settings Utility** window for the SSL configuration.
- You haven't added the certificate authority that issued the SSL certificate to the Trusted Root Certification Authorities certificate store for the SSL configuration.

To solve the problem

- Make sure that the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server computer in the Configure Server Settings Utility window is complete.
  See Turn on secure communication between the server, client(s) and agent(s) on page 102.
- Add the certificate authority that issued the SSL certificate to the Trusted Root Certification Authorities certificate store for the SSL configuration.
- See Import the SSL certificate to client and agent computers on page 103.

Error initializing FactoryTalk AssetCentre: the remote server returned error (404) Not Found

When starting the FactoryTalk AssetCentre Desktop Client, you may get the following error:



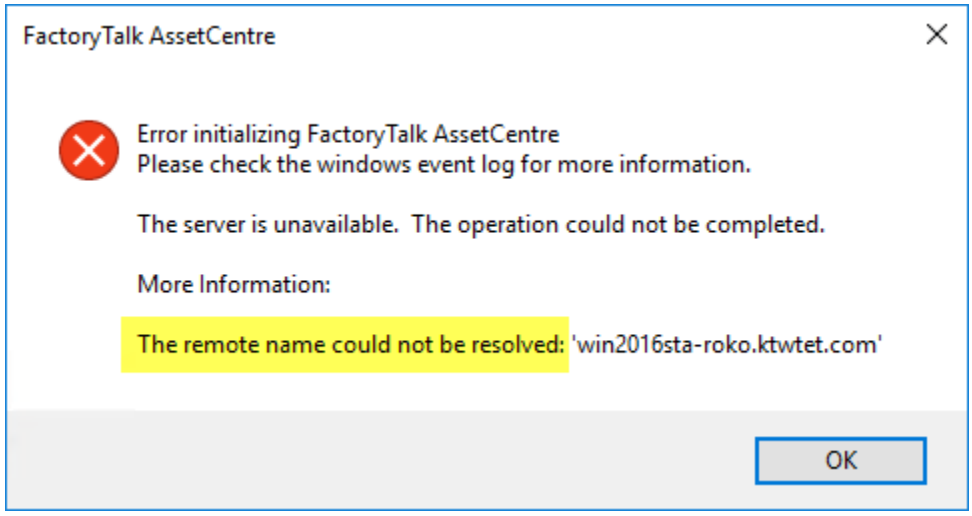
The error message may appear when you have misspelled the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server computer in the site binding for the SSL configuration in the Internet Information Services (IIS) Manager.

To solve the problem

- Correct the spelling of the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server computer in the site binding.
  See Configure a site binding on page 98.

Error initializing FactoryTalk AssetCentre: the remote name could not be resolved

When starting the FactoryTalk AssetCentre Desktop Client, you may get the following error:



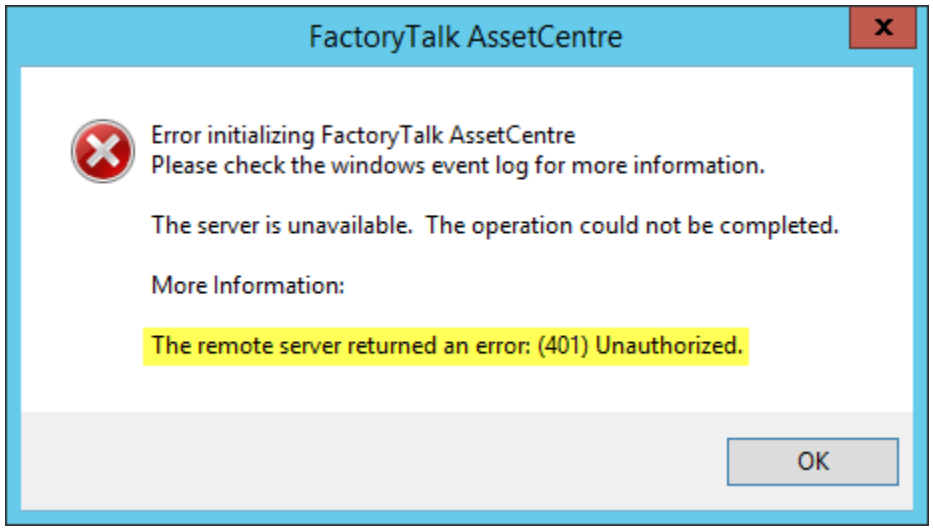
The error message may appear when you have misspelled the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server computer in the Configure Server Settings Utility window for the SSL configuration.

To solve the problem

- Correct the spelling of the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server computer in the **Configure Server Settings Utility** window. See Turn on secure communication between the server, client(s) and agent(s) on page 102

Error initializing FactoryTalk AssetCentre: the remote server returned an error (401) Unauthorized

When starting the FactoryTalk AssetCentre Desktop Client, you may get the following error:



The error message may appear when you have enabled Windows Authentication for FactoryTalk AssetCentre computers that are not added to a Microsoft Active Directory, and the local account with which you are starting the desktop client doesn't exist on the remote FactoryTalk AssetCentre server computer to which the desktop client is trying to connect.

To solve the problem

- On the remote FactoryTalk AssetCentre server computer, add an account that has the username and the password identical with the local account credentials that were used to start the FactoryTalk AssetCentre Desktop Client.
  See Configure Windows Authentication on page 72

The desktop client and server versions are incompatible

The FactoryTalk AssetCentre software installed on the server has been updated, and the software on the desktop client needs to be updated. See Check whether the desktop client is installed correctly on page 85.

Cannot initialize application eventing subsystem or No connection could be made because the target machine actively refused it

If you see the error *Cannot initialize application eventing subsystem*, or an error indicating that the target machine actively refused the connection, then:

- Make sure the FactoryTalk AssetCentre Server service is started on the server computer.
- Restart the client computer.
- If you still see the error, stop and disable all schedules. Restart the FactoryTalk AssetCentre server computer.

  IMPORTANT: While the server is restarting other users will not be able to edit the asset tree, create or edit schedules and searches, view information in the logs, and so on. Also, most data will not be logged during the reboot. The exception is audit data generated by other software products such as RSLogix software, which is cached and will appear in the audit log when the server comes back online.

- See If the FactoryTalk AssetCentre server is installed to a drive other than C: on page 90.

At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details

This message may appear when launching RSLinx Classic on a system that has both RSLinx Classic and FactoryTalk Linx, formerly known as RSLinx Enterprise, installed. The System Event log contains the message, *The A-B Virtual Backplane service failed to start due to the following error: The system cannot find the file specified*.

In some cases, the Virtual Backplane driver does not get installed correctly. For more information, see the Knowledgebase Document ID: BF16472 - AB Virtual Backplane Failed to Start Message.

If the FactoryTalk AssetCentre server is installed to a drive other than C:

If the server was installed to a drive other than **C:**, and necessary permissions to the Users group were removed on that drive, you may encounter error messages when starting the desktop client. The FactoryTalk AssetCentre Server service will be stopped and, if you attempt to manually start it, will fail to start.

To rectify this problem, you must set permissions for the Users group on that drive as follows:

1. On the server computer in Windows Explorer, or My Computer, navigate to the **Program Files** folder on the drive, on which the FactoryTalk AssetCentre server was installed.
2. Right-click the **Rockwell Software** folder and select **Properties**.
3. Select the **Security** tab.
4. Add the group **Users (***computername***\Users)** if it is not in the list. If it is in the list, skip to step 5.
   To add the Users group:
   a. Click **Add**.
   b. Make sure the local computer name appears in the **From this location** field.

c. In the **Enter the object names to select** field, type:

Users

d. Click **Check Names**, then **OK**.

5. Select the group **Users (***computername***\Users)**.
6. Set the **Read & Execute**, **List Folder Contents**, and **Read** permissions to **Allow**.

Other errors starting the desktop client

If the desktop client won't start or you see other error messages not specifically mentioned above, try the following:

- Make sure the client computer is connected to the network, and the network is operational.
- Make sure the FactoryTalk AssetCentre server computer is running.
- Make sure the FactoryTalk AssetCentre Server service, IIS, and SQL Server are all running on the server computer (and the database computer if separate).
- Make sure the correct FactoryTalk Directory is specified. On the machine running the desktop client, from **Windows Start** menu, select **Rockwell Software** > **Specify FactoryTalk Directory Location**.
- If you are running in an environment without a domain controller (in a workgroup), you may need to turn off the single sign-on feature of FactoryTalk. See the FactoryTalk Help for more information.
- Make sure the server location setting is correct. On the server computer, from **Windows Start** menu, select **Rockwell Software** > **FactoryTalk AssetCentre Server Settings**. The server location must be set in this utility, NOT in the FactoryTalk Administration Console.
- Make sure the SQL Connection is set properly. On the server computer, from **Windows Start** menu, select **Rockwell Software** > **FactoryTalk AssetCentre Data Source Configuration**.
- If you are using a firewall, make sure your firewall is configured properly to permit access to the FactoryTalk AssetCentre Server. See Network requirements on page 12, and Knowledgebase Document ID: BF7490 - TCP/UDP Ports Used by Rockwell Automation Products .

Start the agent

If the FactoryTalk AssetCentre software installed on the server has been updated, the agent will not start until the software on the agent is updated. See Check whether the agent software is current on page 85.

FactoryTalk AssetCentre Web Client

Cannot connect to FactoryTalk Web Authentication Server

If you cannot sign in to FactoryTalk AssetCentre Web Client because of the FactoryTalk Web Authentication Server connection, take these steps to check the FactoryTalk Authentication Server connection:

Step 1: To check whether the FactoryTalk Web Authentication Server is running

1. From **Start** menu, in the Search box, enter **Services**, and then select **Services**.
2. Check whether **FactoryTalk Web Server** is running.

Step 2: To check whether the Reverse Proxy works on the FactoryTalk Directory Server computer

1. Open the browser, and then enter the URL address **https://localhost/FTSecurity/api/v1/jwks**.
2. When the data appears as the following, FactoryTalk Web Authentication Server works.


```
{"keys":[{"kty":"RSA","use":"sig","kid":"iiTcv92IAABa4DXyvxRw838z_OkQrw8cI-
ifC2TW0Vs","e":"AQAB","n":"5OLCbfdDCqZIxPM-
j2Z4MqcY34Ud0T1JJKQVZtLH_HYYL596Wy9kmWWUFU9pnT6vHA7jgpUZpdcs9ZdSd4nD21SKqgl_cfabk_
plget-zITPR7-B9_rEs2RT3nzBAI49cxjSoq6LSa1KSZUUmFoCEuvssU5Vrzf8F_IwVo1d-
qfknGi3YF3q8qWhGKwLrB1oDgpopKninWV_0_41nRDJCdZLZafQOjpBY4AnhCGhHVtvMEPJLZ7etKj64xP
MRAb96jLocUnRa7rrcvMGy5dracXriRbmJELJkdJDoky1iBUucIwl2kQml7D-nmloD-
sRaUWqZzV0LxOb8qNHdpCOgQ"}]}
```


NOTE: The data in Step 2 is an example. It differs for each FactoryTalk Directory.

Step 3: To check whether the Reverse Proxy port or FactoryTalk Web Authentication port is changed

1. In FactoryTalk Administration Console **Explorer**, expand **System** > **Policies** > **System Policies**.
2. Right-click **Security Policy**, and then select **Properties**.
3. Check whether these properties are changed:
   - FactoryTalk Web Authentication port: 7110 by default
   - Reverse Proxy port: 443 for HTTPS and 80 for HTTP by default
   - Reverse Proxy protocol: HTTP or HTTPS
4. Open the browser, and then enter the URL address **<Reverse Proxy protocol>://localhost:<Reverse Proxy port>/FTSecurity/api/v1/jwks**. For example: https://localhost:443/FTSecurity/api/v1/jwks
5. When the data appears as the following, FactoryTalk Web Authentication Server works.


```
{"keys":[{"kty":"RSA","use":"sig","kid":"iiTcv92IAABa4DXyvxRw838z_OkQrw8cI-
ifC2TW0Vs","e":"AQAB","n":"5OLCbfdDCqZIxPM-
j2Z4MqcY34Ud0T1JJKQVZtLH_HYYL596Wy9kmWWUFU9pnT6vHA7jgpUZpdcs9ZdSd4nD21SKqgl_cfabk_
plget-zITPR7-B9_rEs2RT3nzBAI49cxjSoq6LSa1KSZUUmFoCEuvssU5Vrzf8F_IwVo1d-
qfknGi3YF3q8qWhGKwLrB1oDgpopKninWV_0_41nRDJCdZLZafQOjpBY4AnhCGhHVtvMEPJLZ7etKj64xP
MRAb96jLocUnRa7rrcvMGy5dracXriRbmJELJkdJDoky1iBUucIwl2kQml7D-nmloD-
sRaUWqZzV0LxOb8qNHdpCOgQ"}]}
```


NOTE: The data in Step 5 is an example. It differs for each FactoryTalk Directory.

6. If no data appears, enter the URL address **http://localhost:<FactoryTalk Web Authentication port>/FTSecurity/api/v1/jwks**.
7. If data as shown in Step 5 appears, there may be a Reverse Proxy problem.
8. If no data appears, in the Command Prompt window, enter **netstat -ano | findstr <FactoryTalk Web Authentication port>**, and then press **Enter**.

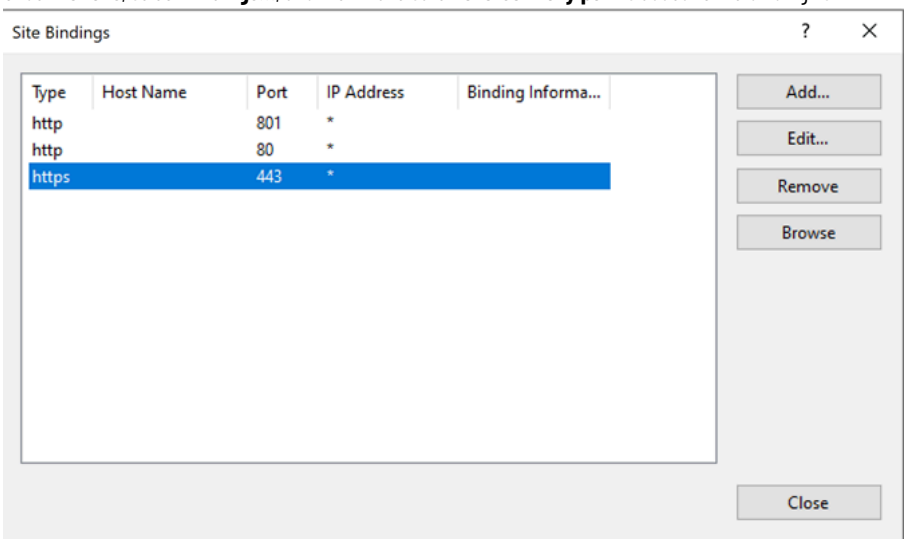
```
C:\Users\n0048153>netstat -ano | findstr 7110
  TCP    127.0.0.1:7110         0.0.0.0:0              LISTENING       38364
```

9. If there is no response to the netstat command or the system returns a process using the port that is not ftsp-web-server.exe, there may be a port conflict problem. You can change the port using FactoryTalk Administration Console.

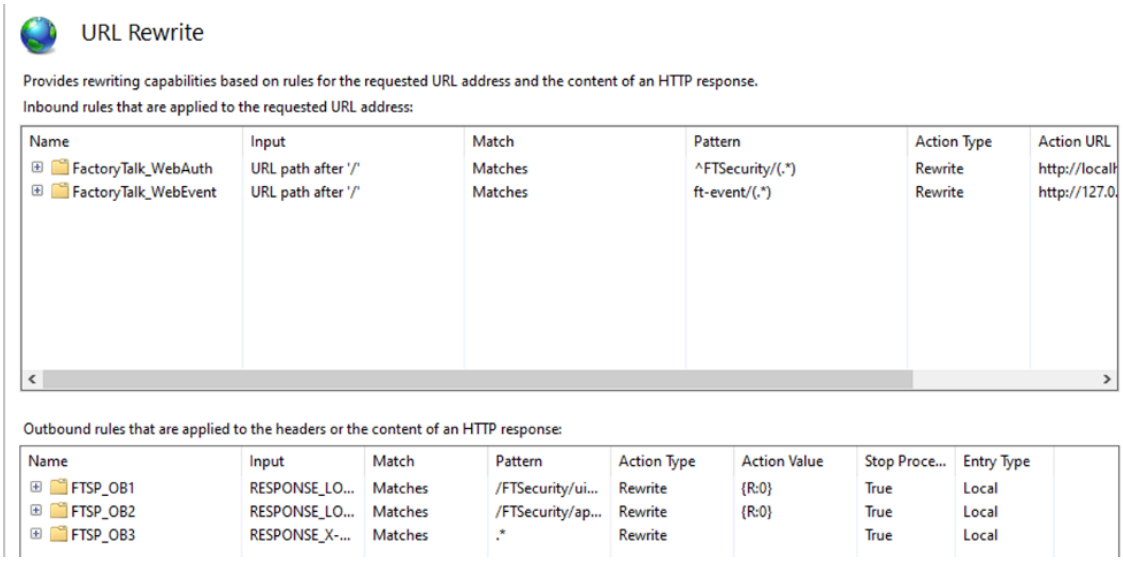
Tip: As the graphic shown in Step 8, you can identify port conflicts with the process identifier (PID) and use PID to determine which process listens on a given port.

Step 4: To check whether the service listened to the right port

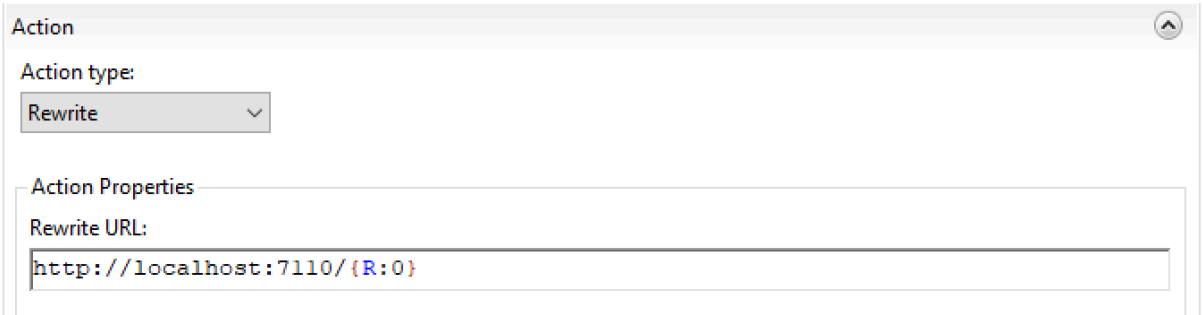
1. Open **Internet Information Services (IIS) Manager**, select **Default Web Site**.
2. Under **Manage Website**, make sure it is running.
3. Under **Actions**, select **Bindings...**, and then make sure **Reverse Proxy port** is added to the binding list.



4. In **Default Web Site Home**, select **URL Rewrite**, and then make sure **FactoryTalk_WebAuth** is in the inbound rule list and **FTSP_OB1**, **FTSP_OB2**, and **FTSP_OB3** are in the outbound rule list.



5. In inbound rule list, double-click **FactoryTalk_WebAuth**, and then make sure that the port number in **Rewrite URL** is the same as **FactoryTalk Web Authentication port**.



Configure the TLS protocol using a self-signed certificate

If you don't have a TLS certificate signed by certificate authority (CA), you need to create a self-signed TLS certificate on the FactoryTalk AssetCentre Server computer. After importing the TLS certificate to the Management of Change, FactoryTalk AssetCentre Server, Agent, Desktop Client, and Web Client computers, you must configure a firewall rule and web services URL if the default port is modified on page 69.

The configuration including these steps:

Create a self-signed TLS certificate

Follow these steps to create a self-signed TLS certificate on the FactoryTalk AssetCentre Server computer.

To create an TLS certificate

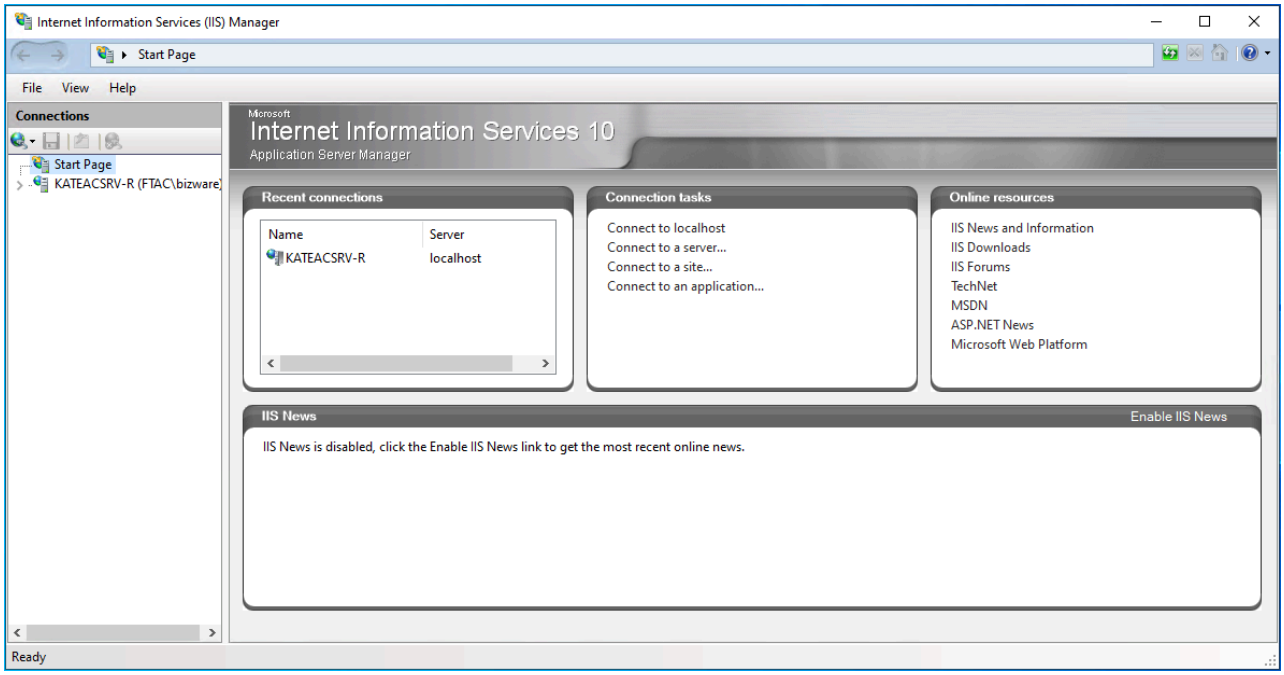
1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer.

   On Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2:

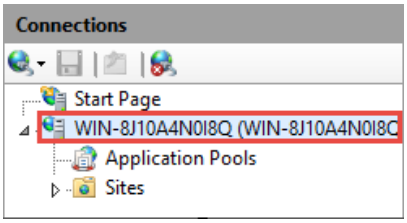
   a. On the taskbar, click  .

   b. In the search box, type *inetmgr*, and then press **Enter**.

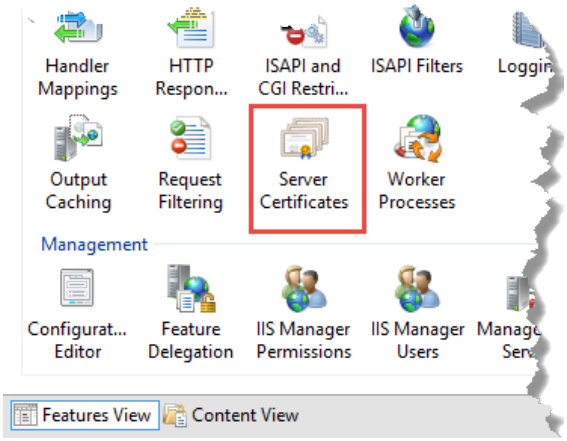
   c. Click the best match result.



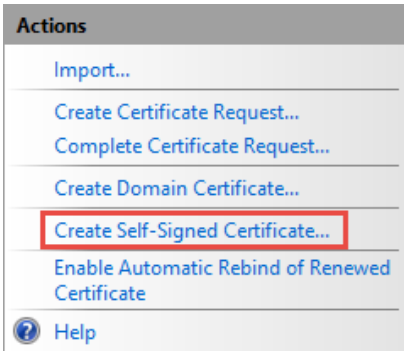
2. Under **Connections**, click the FactoryTalk AssetCentre server.



3. In **Features View**, double-click **Server Certificates**.



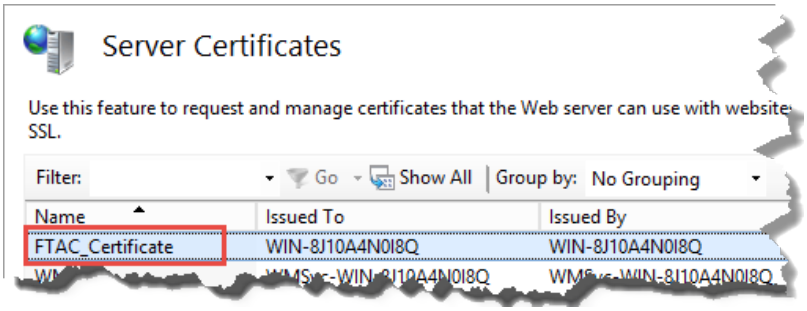
4. Under **Actions**, click **Create Self-Signed Certificate**.



5. In the **Create Self-Signed Certificate** dialog box:
   - Specify a name for the certificate.
   - Select **Web Hosting** as the certificate store.

6. Click **OK**.

   The created TLS certificate is listed.



Export the created TLS certificate for FactoryTalk AssetCentre client and agent computers

After creating an TLS certificate on the FactoryTalk AssetCentre server computer, export the certificate which will need to be imported on the FactoryTalk AssetCentre client and agent computers.

To export the created TLS certificate

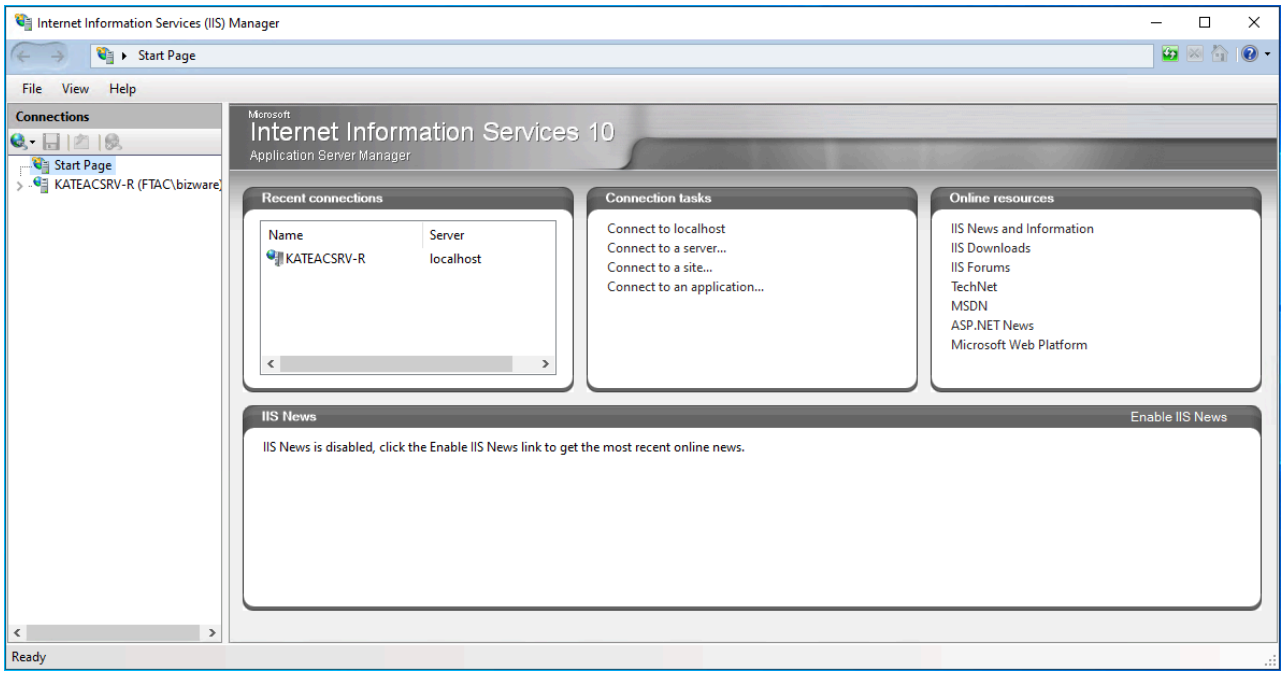
1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer.

   On Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2:

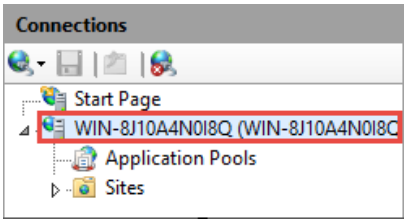
   a. On the taskbar, click  .

   b. In the search box, type *inetmgr*, and then press **Enter**.

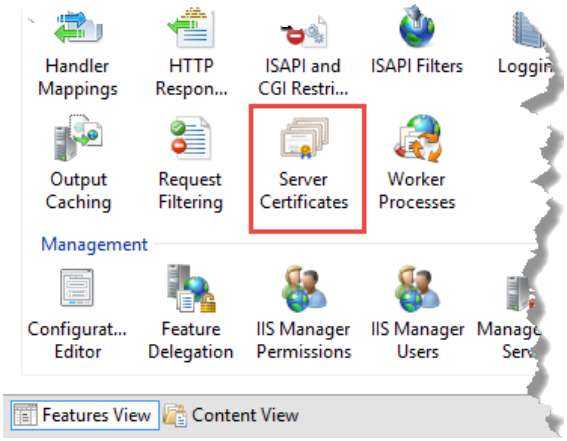
   c. Click the best match result.



2. Under **Connections**, click the FactoryTalk AssetCentre server.

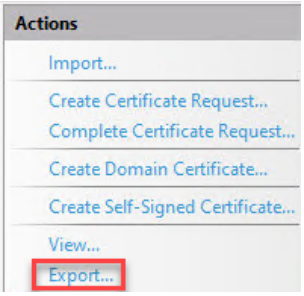


3. In **Features View**, double-click **Server Certificates**.



4. Select the TLS certificate that you have created.

5. Under **Actions**, click **Export**.



6. In the **Export Certificate** dialog box:
   - Under **Export to**, click ..., and then specify the location and name to save the certificate.
   - Specify the password for the certificate.
7. Click **OK**.

Configure a site binding

Before you begin

- Create a self-signed TLS certificate on page 94.

To configure a site binding

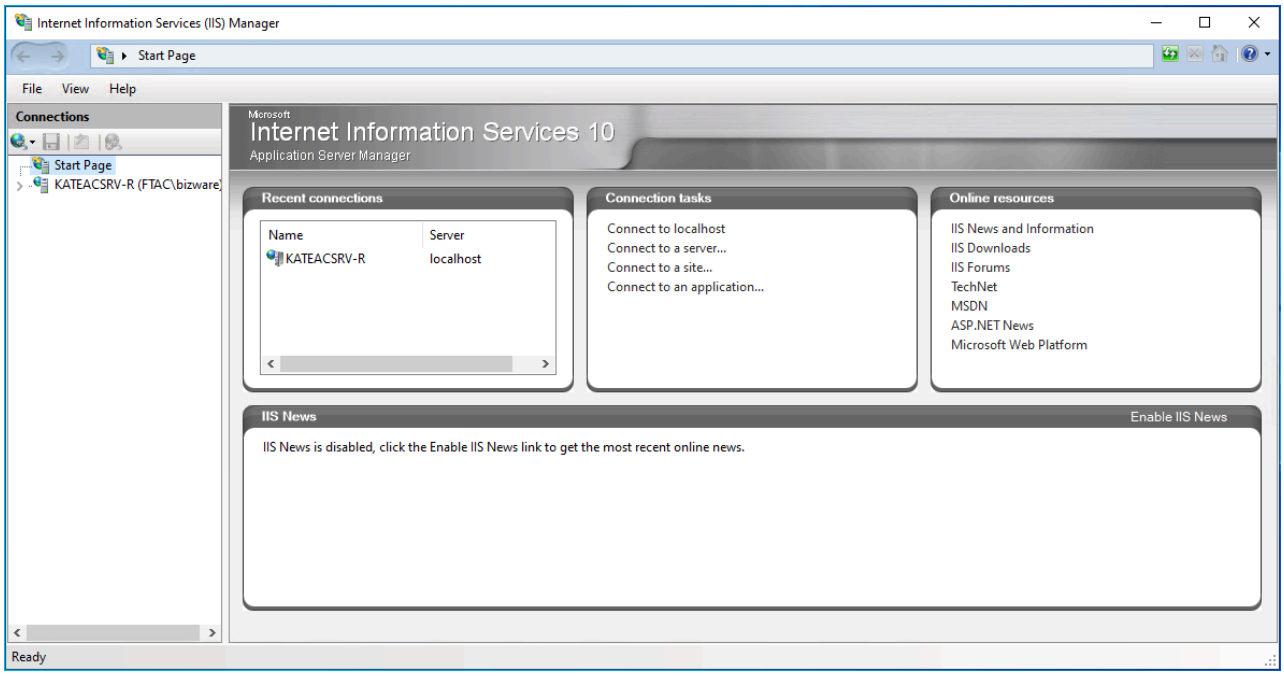
1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer.

   On Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2:

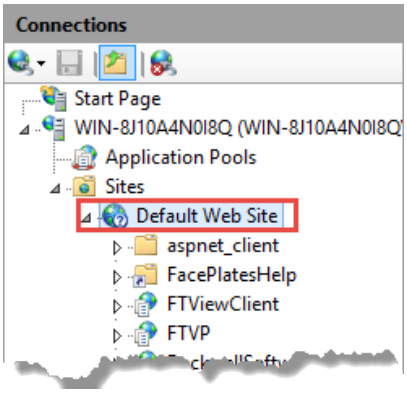
   a. On the taskbar, click .

   b. In the search box, type *inetmgr*, and then press **Enter**.

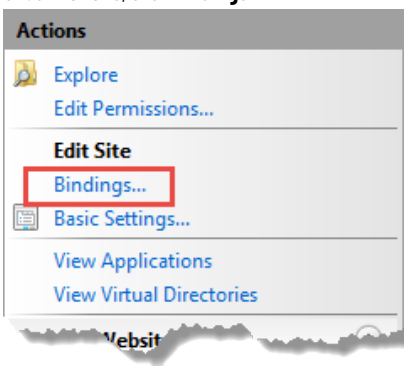
   c. Click the best match result.



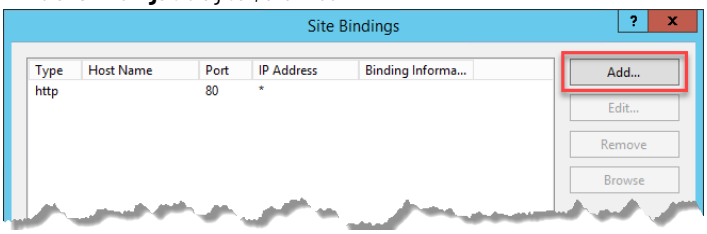
2. Navigate to **localhost > Sites > Default Web Site**.



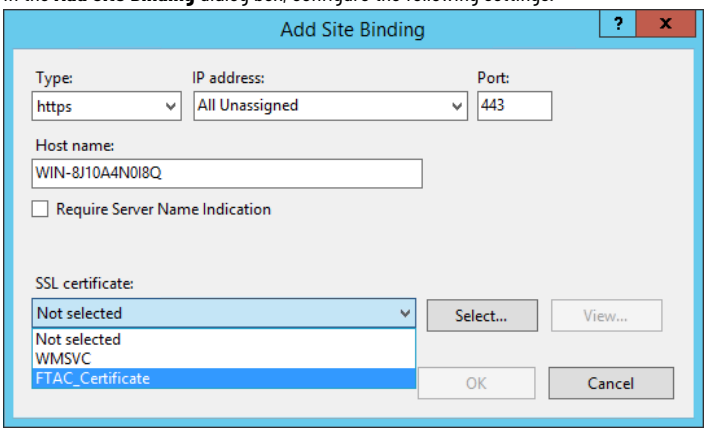
3. Under **Actions**, click **Bindings**.



4. In the **Site Bindings** dialog box, click **Add**.



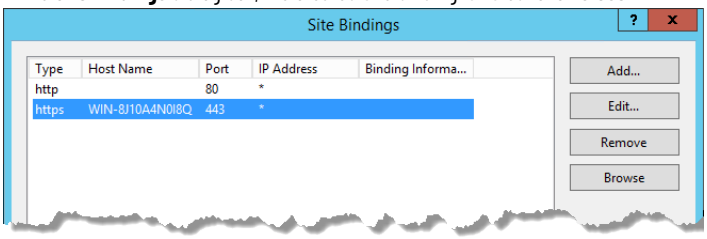
5. In the **Add Site Binding** dialog box, configure the following settings.



For this option...	Do this...
Type	Select **https**.
IP address	Select **All Unassigned**.
Port	Keep the default port number 443 or if you needed, you may change it to a self-defined port.

For this option...	Do this...
	If you use a self-defined port, you need to configure a firewall rule and web services URL on page 69.
Host name	Type the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server.
SSL certificate	Select your TLS certificate. See Create a self-signed TLS certificate on page 94.

6. Click **OK**.
7. In the **Site Bindings** dialog box, the created site binding is listed. Click **Close**.



Tip: You can remove the default HTTP site binding and only keep the created HTTPS site binding.

Configure SSL settings for Management of Change, FactoryTalk AssetCentre Desktop Client and Agent, and FactoryTalk AssetCentre Web Client

Before you begin

- Create a self-signed TLS certificate on page 94.
- Configure a site binding on page 98.

To configure SSL settings for Management of Change, FactoryTalk AssetCentre Desktop Client and Agent, and FactoryTalk AssetCentre Web Client

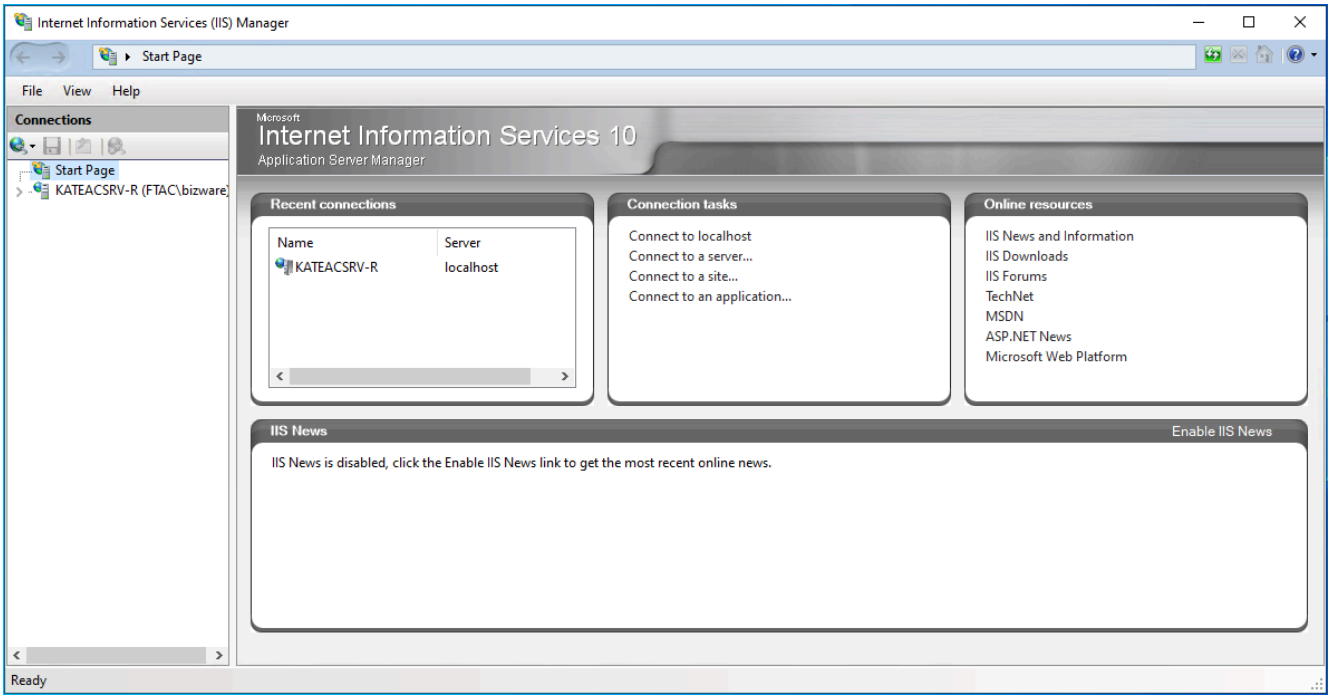
1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer.

   On Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2:

   a. On the taskbar, click .

   b. In the search box, type *inetmgr*, and then press **Enter**.

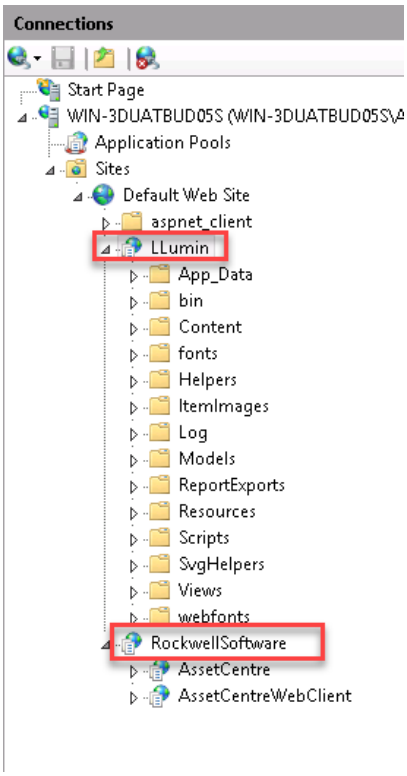
c. Click the best match result.



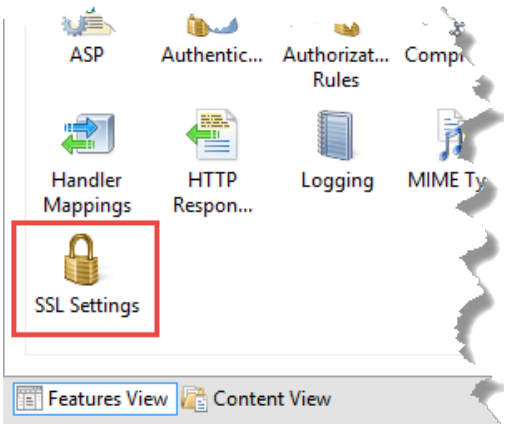
2. Navigate to **localhost > Sites > Default Web Site**.

   To configure the SSL settings for Management of Change, select **LLumin**.

   To configure the SSL settings for FactoryTalk AssetCentre Desktop Client and Agent, and FactoryTalk AssetCentre Web Client, select **AssetCentre** and **AssetCentreWebClient** under **RockwellSoftware**.



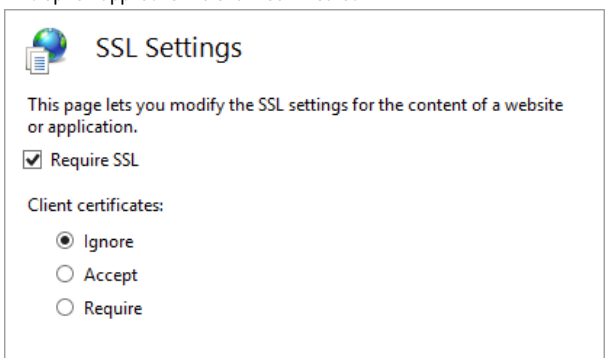
3. In **Features View**, double-click **SSL Settings**.



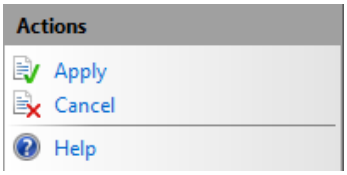
4. Make sure the following options are selected:
   - **Require SSL**

     (FactoryTalk AssetCentre Web Client only) Selecting this option will result in deactivating the HTTP protocol (with the default port 80). When you type *http://* in the web browser, it will be automatically redirected to *https://*.
   - **Ignore**

     This option applies to the client certificates.



5. Under **Actions**, click **Apply**.



6. Restart the computer.

Turn on secure communication between the server, client(s), and agent(s)

Once you configured the TLS protocol, turn on secure communication between the server, client(s), and agent(s) in the **Configure Server Settings Utility** window.

To enable secure communication

1. Open the **Configure Server Settings Utility** window.

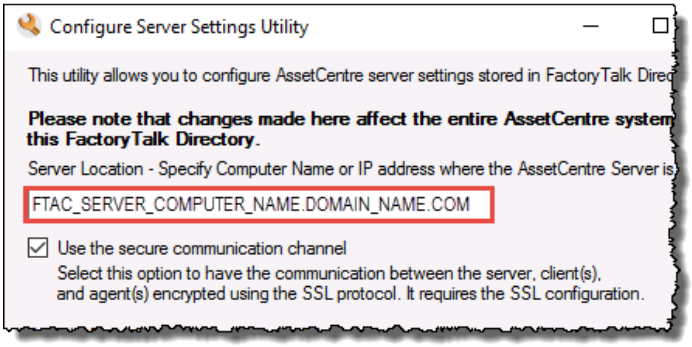
   On Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2:

   a. On the taskbar, click .

   b. In the search box, type *Server Settings*.

   c. Click **FactoryTalk AssetCentre Server Settings**.
2. Enter the user name and password to log on to FactoryTalk, and then click **OK**.

In the **Configure Server Settings Utility** window, under **Server Location**, the domain name (FQDN) of the FactoryTalk AssetCentre server computer will be detected automatically.



3. Select the **Use the secure communication channel** option.
4. Click **OK**.

Import the self-signed TLS certificate to client and agent computers

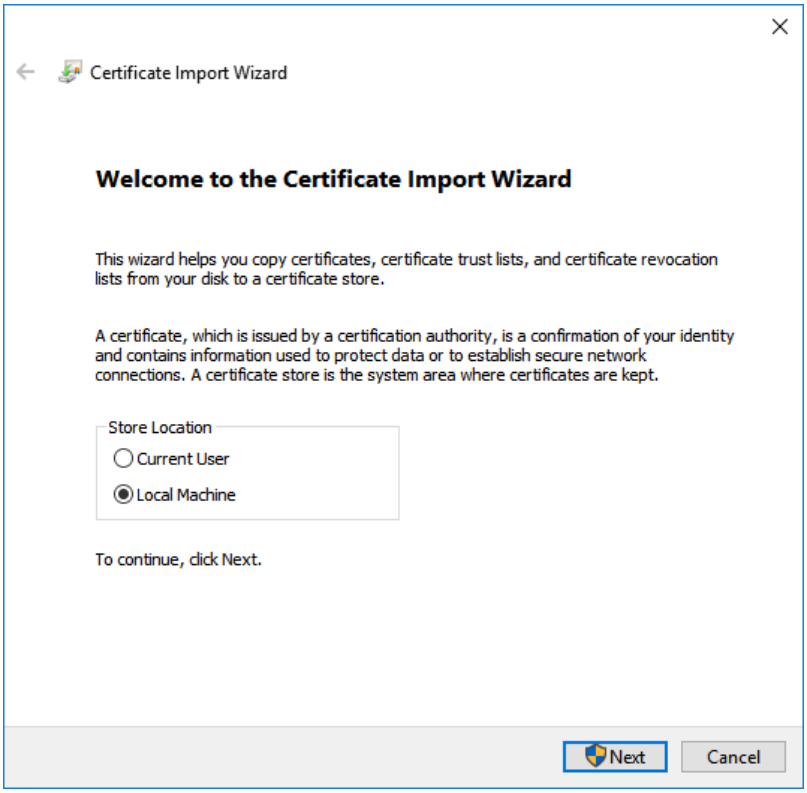
On the client and agent computers, add the self-signed TLS certificate to the Trusted Root Certification Authorities certificate store.

Before you begin

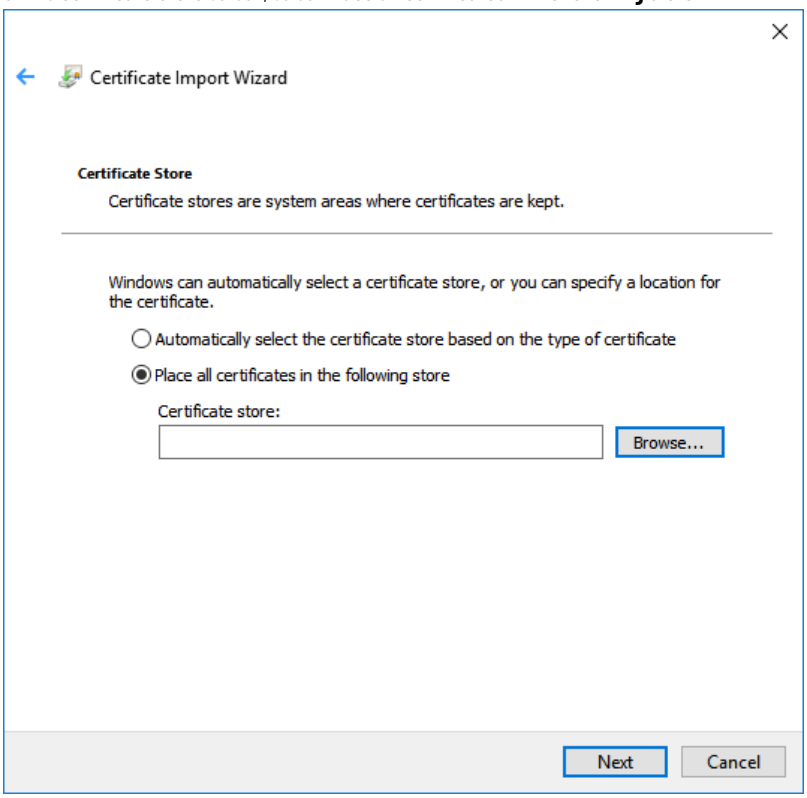
- Create a self-signed TLS certificate on page 94.
- Export the created TLS certificate on page 96.

To import the self-signed TLS certificate on operating systems

1. Copy the created TLS certificate on the computer.
2. Double-click the TLS certificate.
3. Select **Local Machine**, and then click **Next**.

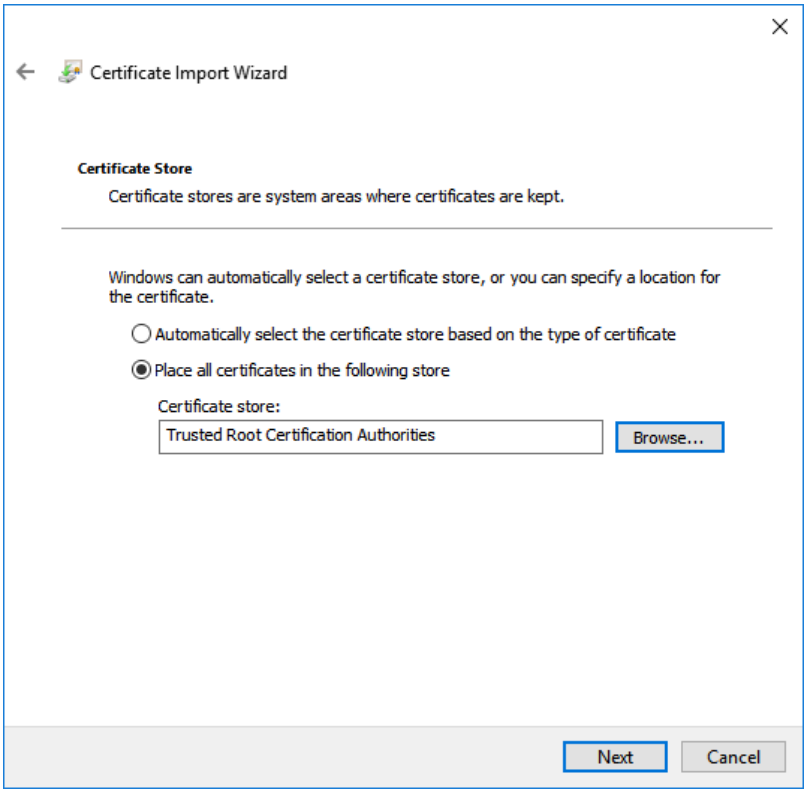


4. When prompted to confirm the operation, click **Yes**.
5. Follow the on-screen instructions until you get to the **Certificate Store** screen.
6. On the **Certificate Store** screen, select **Place all certificates in the following store**.



7. Click **Browse**, select **Trusted Root Certification Authorities**, and then click **OK**.

8. Click **Next**.



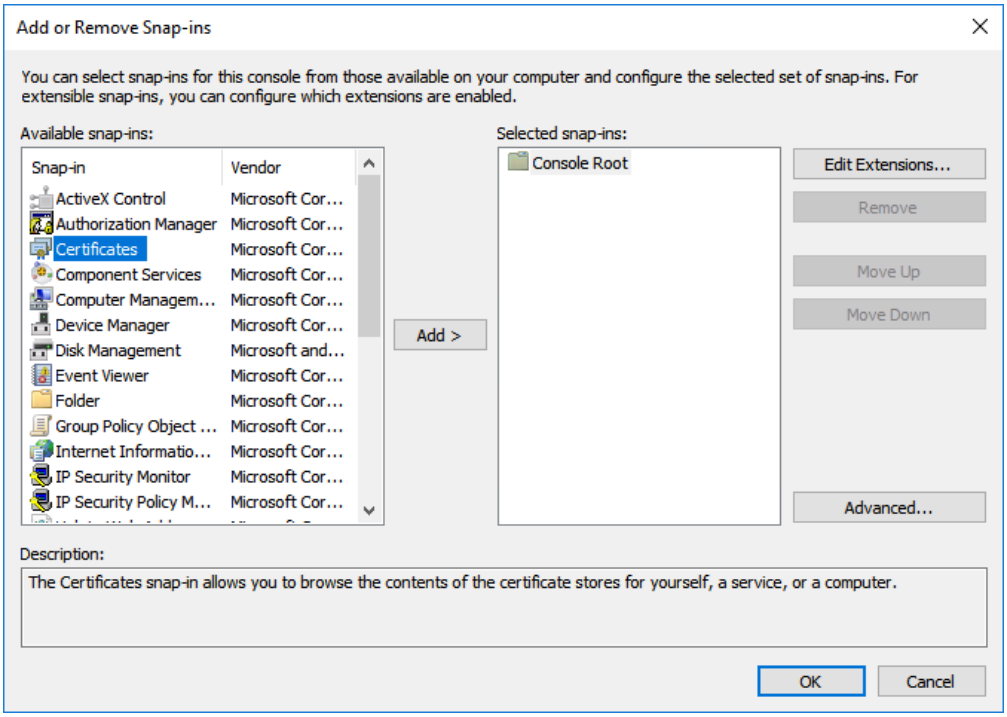
9. Follow the on-screen instructions to complete the import.

To verify the import operation

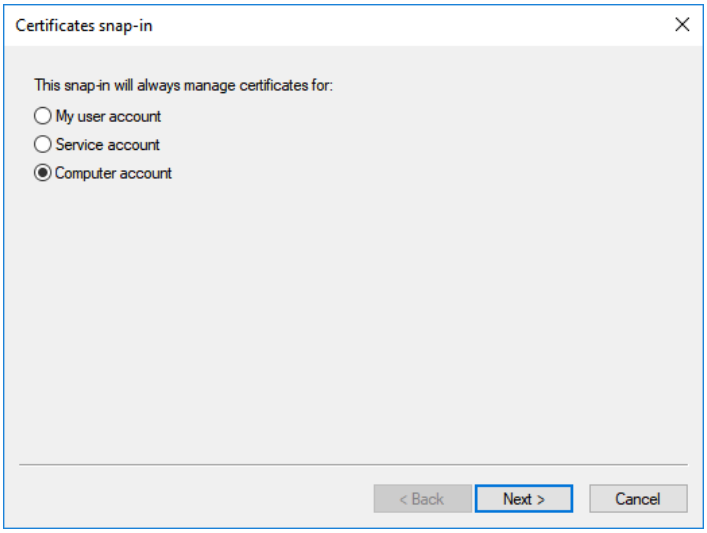
1. Click **Start**, type *mmc*, and then press **Enter**.

   The Microsoft Management Console opens.

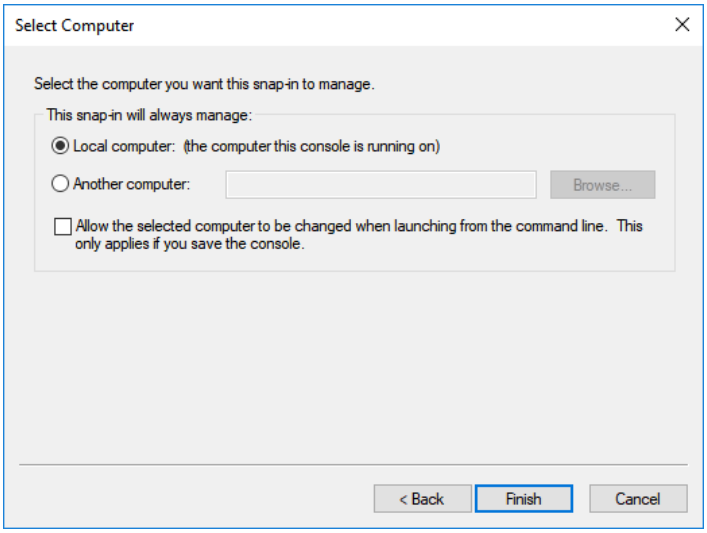
2. Click **File > Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, select **Certificates**, and then click **Add**.



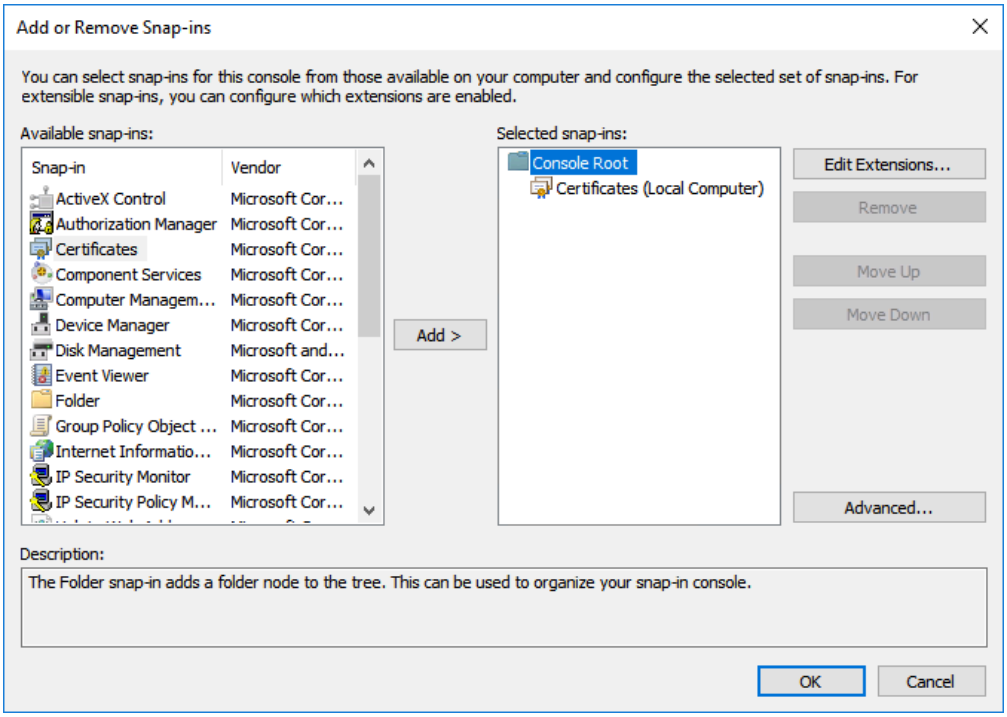
4. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.



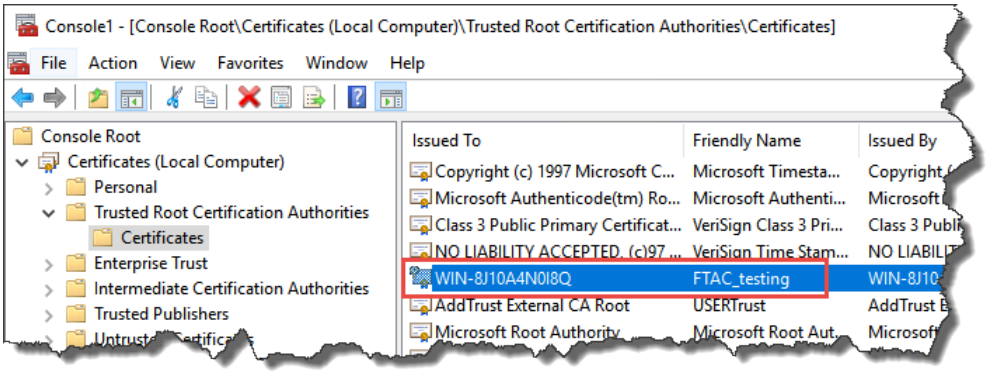
5. Click **Finish**.



6. In the **Add or Remove Snap-ins** dialog box, click **OK**.



7. In the Microsoft Management Console, navigate to **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**, and verify that the TLS certificate is listed.



8. If the TLS certificate is not listed, make sure to select **Certificates** under **Trusted Root Certification Authorities > Certificates**, and then click **Action > All Tasks > Import**.
9. Follow the on-screen instructions to complete the import.

Create a self-signed TLS certificate on the SQL Server computer

Follow these steps to create a self-signed TLS certificate on the SQL Server computer. The certificate must be issued for server authentication. The certificate should contain the computer name (fully qualified domain name) of SQL Server.

IMPORTANT: For encrypted connection to the database with a self-signed certificate, you need to create the certificate before installing.

To create a self-signed TLS certificate on the SQL Server computer

1. Open Internet Information Services (IIS) Manager on the SQL Server computer, and then double-click **Server Certificates**.
2. Under **Actions**, click **Create Self-Signed Certificate**.
3. In the **Create Self-Signed Certificate** dialog box:
   a. Specify a name for the certificate.
   b. Select **Web Hosting** as the certificate store.
4. Click **OK**.

Create a self-signed TLS certificate on the SQL Server or FactoryTalk Network Directory computer

Follow these steps to create a self-signed TLS certificate on the SQL Server or FactoryTalk Network Directory computer. The certificate must be issued for server authentication and contain the computer name (fully qualified domain name) of SQL Server or FactoryTalk Network Directory.

NOTE: Creating a self-signed TLS certificate for the FactoryTalk Network Directory computer is necessary only when the FactoryTalk Network Directory is on a separate computer system than the FactoryTalk AssetCentre Server, SSL/TLS is enabled, and users are using the web client.

To create a self-signed TLS certificate on the SQL Server or FactoryTalk Network Directory computer

- On the SQL Server or FactoryTalk Network Directory computer:

1. Open the Internet Information Services (IIS) Manager on the SQL Server or FactoryTalk Network Directory computer.
2. Under **Connections**, select the localhost server and then double-click **Server Certificates**.
3. Under **Actions**, select **Create Self-Signed Certificate**.
4. In the **Create Self-Signed Certificate** dialog box:
    a. Specify a name for the certificate.
    b. Select **Web Hosting** as the certificate store.
5. Select **OK**.

For larger systems, the SQL Server and FactoryTalk AssetCentre Server might be on separate computer systems. If the servers are on different computer systems, the self-signed TLS certificate must be exported from the SQL Server computer system, copied to the FactoryTalk AssetCentre Server computer system, and imported.

To export the newly created self-signed TLS certificate on the SQL Server or FactoryTalk Network Directory computer

- On the SQL Server or FactoryTalk Network Directory computer:

1. Add the snap-in.
    a. On the **Start** menu, select **Run**, enter **MMC** in the **Open** box, and then select **OK**.
    b. In the Microsoft Management Console, select **File > Add/Remove Snap-in**.
    c. In the **Add or Remove Snap-ins** dialog box, select **Certificates**, and then select **Add**.
    d. In the **Certificates snap-in** dialog box, select **Computer account**, and then select **Next**.
    e. In the **Select Computer** dialog box, keep the default **Local computer** selection, and then select **Finish**.
    f. In the **Add or Remove Snap-ins** dialog box, select **OK**.
2. Export the certificate.
    a. Expand **Certificates** > **Trusted Root Certification Authorities**, select **Certificates**.
    b. Right-click on the certificate that you created and select **All Tasks** > **Export**.
    The self-signed certificate gets created within the Trusted Root Certificate Authorities folder without having to import in.
    c. In the Certificate Export Wizard, select **Next**.
    d. Select **Yes, export the private key,** and then select **Next**.
    e. Select the following under **Personal Information Exchange – PKCS #12 (.PFX)**, and then select **Next**.
        - **Include all certificates in the certification path if possible**.
        - **Export all extended properties**.
    f. Select the check box to enable using a password. Enter and confirm the desired password for the certificate and select **Next**.
    g. Browse the location and specify the file name of the exported certificate. Select **Save** and then select **Next**.

h. Verify the information in the specified settings, and then select **Finish**.

NOTE:

- For exporting the self-signed certificate from the SQL server, proceed to the next step.
- For exporting the self-signed TLS certificate from the FactoryTalk Network Directory computer, proceed to **step 7.**

3. Import the certificate. Back at the main screen of the MMC, navigate to **Console Root** > **Certificates (Local Computer)** > **Personal** > **Certificates**.
   a. In the Microsoft Management Console, expand **Certificates > Personal**, right-click **Certificates**, and then select **All Tasks > Import**.
   b. In the Certificate Import Wizard, select **Next** and specify the file name and path.
   c. Enter the password, and then select **Next**.
   d. Specify the certificate store as **Personal**, and then select **Next**.
   e. Select **Finish**.
4. Add the SQL Server service account permission.
   a. In the Microsoft Management Console, right-click the imported certificate, and then select **All Tasks** > **Manage Private Keys**.
   b. In the **Security** dialog box, add read permission for the user account used by the SQL Server service account. The location should be your local computer name.

Tip:

To find the SQL Server service account:

i. Open Windows **Services**
ii. Double-click **SQL Server (InstanceName)**
iii. Select the **Log on** tab, and then find the SQL Server service account in the **This account** box.

5. Add the certificate to the SQL Server instance.
   a. Open SQL Server Configuration Manager.
   b. Expand **SQL Server Network Configuration**, right-click **Protocols for InstanceName**, and then select **Properties**.
   c. In the **Protocols for InstanceName Properties** dialog box, select the **Certificate** tab, and then select the certificate from the **Certificate** list.
   d. Select **OK**.
6. Restart the SQL Server.
   a. In SQL Server Configuration Manager, select **SQL Server Services**.
   b. Right-click **SQL Server (InstanceName)**, and then select **Restart**.
7. Copy the exported self-signed certificate to a location where the FactoryTalk AssetCentre Server computer system can access.

- On the FactoryTalk AssetCentre Server computer:

1. Copy and paste the exported self-signed certificate from the SQL server into the desired location on the FactoryTalk AssetCentre Server computer's hard drive.
2. Follow the steps in **Configure a certificate on the FactoryTalk AssetCentre server computer on page 17**.

Legal Notices

Rockwell Automation publishes legal notices, such as privacy policies, license agreements, trademark disclosures, and other terms and conditions on the Legal Notices page of the Rockwell Automation website.

Software and Cloud Services Agreement

Review and accept the Rockwell Automation Software and Cloud Services Agreement here.

Open Source Software Licenses

The software included in this product contains copyrighted software that is licensed under one or more open source licenses.

You can view a full list of all open source software used in this product and their corresponding licenses by opening the oss_license.txt file located in your product's OPENSOURCE folder on your hard drive. This file is divided into these sections:

- Components
  Includes the name of the open source component, its version number, and the type of license.
- Copyright Text
  Includes the name of the open source component, its version number, and the copyright declaration.
- Licenses
  Includes the name of the license, the list of open source components citing the license, and the terms of the license.

The default location of this file is:

C:\Program Files (x86)\Common Files\Rockwell\AssetCentre\ReleaseNotes\OPENSOURCE\oss_license.txt

You may obtain Corresponding Source code for open source packages included in this product from their respective project web site(s). Alternatively, you may obtain complete Corresponding Source code by contacting Rockwell Automation via the **Contact** form on the Rockwell Automation website: http://www.rockwellautomation.com/global/about-us/contact/contact.page. Please include "Open Source" as part of the request text.

Rockwell Automation support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

FTAC-IN005L-EN-E - January 2024
Supersedes Publication FTAC-IN005K-EN-E - March 2023