



Micro Focus File Reporter 4.0 Installation Guide

January 8, 2021

Legal Notices

Condrey Corporation makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2021 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion without the express written consent of the publisher.

Condrey Corporation
122 North Laurens St.
Greenville, SC, 29601
U.S.A.
<http://condrey.co>

For information about Micro Focus legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Third Party Systems

The software is designed to run in an environment containing third party elements meeting certain prerequisites. These may include operating systems, directory services, databases, and other components or technologies. See the accompanying prerequisites list for details.

The software may require a minimum version of these elements in order to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth in order for the software to be able to perform in a way that meets the customer requirements. The download, installation, performance, upgrade, backup, troubleshooting, and management of these elements is the responsibility of the customer using the third party vendor's documentation and guidance.

Third party systems emulating any these elements must fully adhere to and support the appropriate APIs, standards, and protocols in order for the software to function. Support of the software in conjunction with such emulating third party elements is determined on a case-by-case basis and may change at any time.

Contents

About This Guide	7
1 Upgrading from a Previous Version	9
1.1 Database	9
1.1.1 Upgrading the Existing Database	9
1.2 License	9
1.3 Engine, Scan Processor, and Web Application	10
1.4 File Content Scanning	10
1.5 Microsoft 365 Reporting	10
1.6 Agents	10
1.6.1 File System Agents	10
1.6.2 Content Agent	10
1.6.3 Microsoft 365 Cloud Agent	11
2 Deployment Planning	13
2.1 Understand the Technologies and Expertise You Need	13
2.2 Decide Where to Host the Engine	14
2.3 Decide Which Database to Utilize	14
2.4 Determine Whether to Scan File Content	15
2.5 Determine Whether to Scan Microsoft 365	15
2.6 Develop a Plan for Deploying the Agents for Scanning	15
2.7 Database Deployment Recommendations	16
2.7.1 Use a Dedicated Server	16
2.7.2 Use a Dedicated Database Instance	16
2.7.3 Provide Sufficient I/O Bandwidth	16
3 Licensing the Product	19
3.1 Obtaining a Product Activation Key	19
3.2 Obtaining a License File	19
4 Installing and Configuring the PostgreSQL Database	23
4.1 Installing and Configuring the PostgreSQL Database on a Linux Server	23
4.1.1 Minimum Requirements	23
4.1.2 Installing and Configuring the PostgreSQL Database	24
5 Installing an SQL Server Instance that Supports File Reporter	25
5.1 Minimum Requirements	25
5.2 Prerequisites	25
5.3 Install a New Instance of SQL Server	26
5.4 Post Configuration Considerations	31

6	Installing and Configuring RabbitMQ	33
6.1	Upgrading from an Earlier Version of RabbitMQ	33
6.2	Extracting RabbitMQ	34
6.3	Creating Certificates for RabbitMQ	34
6.4	Installing Rabbit MQ	38
6.5	Changing the Default Password	39
7	Installing and Configuring the Engine, Database, Message Broker, and Web Application	43
7.1	Minimum Requirements	43
7.2	Prerequisites	43
7.3	Installing the Engine	44
7.4	Configuring the Database	46
7.5	Installing the License	51
7.6	Configuring the Engine	53
7.7	Configuring the Message Broker	59
7.8	Configuring the Web Application	62
8	Installing and Configuring Windows AgentFS	71
8.1	Minimum Requirements	71
8.2	Active Directory Requirements	71
8.3	Installing and Configuring AgentFS	71
9	Install ManagerFC	79
9.1	Minimum Requirements	79
9.2	Installing ManagerFC	79
10	Installing AgentFC	85
10.1	Minimum Requirements	85
10.2	Active Directory Requirements	85
10.3	Installing and Configuring AgentFC	86
11	Enabling Microsoft 365 Reporting and Installing Agent365	91
11.1	Preparing the Microsoft 365 Cloud Tenant	91
11.2	Installing Agent365	97
11.2.1	Prerequisites	97
11.2.2	Minimum Requirements	97
11.2.3	Installing and Configuring Agent365	97
12	Installing the Report Viewer and Client Tools	105
12.1	Minimum Requirements	105
12.2	Install the Report Viewer	106
12.3	Install the Client Tools	106

A	Replace a License File	107
A.1	Replacing a License	107

About This Guide

This installation guide is written to provide network administrators the conceptual and procedural information for installing and configuring Micro Focus File Reporter 4.0.

- ♦ Chapter 1, “Upgrading from a Previous Version,” on page 9
- ♦ Chapter 2, “Deployment Planning,” on page 13
- ♦ Chapter 3, “Licensing the Product,” on page 19
- ♦ Chapter 4, “Installing and Configuring the PostgreSQL Database,” on page 23
- ♦ Chapter 5, “Installing an SQL Server Instance that Supports File Reporter,” on page 25
- ♦ Chapter 6, “Installing and Configuring RabbitMQ,” on page 33
- ♦ Chapter 7, “Installing and Configuring the Engine, Database, Message Broker, and Web Application,” on page 43
- ♦ Chapter 8, “Installing and Configuring Windows AgentFS,” on page 71
- ♦ Chapter 9, “Install ManagerFC,” on page 79
- ♦ Chapter 10, “Installing AgentFC,” on page 85
- ♦ Chapter 11, “Enabling Microsoft 365 Reporting and Installing Agent365,” on page 91
- ♦ Chapter 12, “Installing the Report Viewer and Client Tools,” on page 105
- ♦ Appendix A, “Replace a License File,” on page 107

Audience

This guide is intended for network administrators who manage network storage resources.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Micro Focus File Reporter 4.0 Installation Guide*, visit the [Micro Focus File Reporter Documentation Web site \(http://www.novell.com/documentation/filereporter3\)](http://www.novell.com/documentation/filereporter3).

Additional Documentation

For additional Micro Focus File Reporter 4.0 documentation, see the following guides at the [Micro Focus File Reporter Documentation Web site](#)

- ◆ *[Micro Focus File Reporter 4.0 Administration Guide](#)*
- ◆ *[Micro Focus File Reporter 4.0 Database Schema and Custom Queries Guide](#)*

1 Upgrading from a Previous Version

You can upgrade from any version of File Reporter 3.5 or greater by installing the updated software on top of the existing software. Depending on the version from which you are upgrading, there might be new optional file content scanning components to be installed. These include The RabbitMQ messaging broker, ManagerFC, AgentFC, and Agent365.

- ♦ [Section 1.1, “Database,” on page 9](#)
- ♦ [Section 1.2, “License,” on page 9](#)
- ♦ [Section 1.3, “Engine, Scan Processor, and Web Application,” on page 10](#)
- ♦ [Section 1.4, “File Content Scanning,” on page 10](#)
- ♦ [Section 1.5, “Microsoft 365 Reporting,” on page 10](#)
- ♦ [Section 1.6, “Agents,” on page 10](#)

1.1 Database

File Reporter 4.0 supports only versions of PostgreSQL and Microsoft SQL Server that are supported by The PostgreSQL Global Development Group, and Microsoft, respectively. If you are using a non-supported database, you will need to first upgrade it.

For information on File Reporter supported versions of PostgreSQL, see [Section 4.1.1, “Minimum Requirements,” on page 23](#).

For information on File Reporter supported versions of SQL Server, see [Section 5.1, “Minimum Requirements,” on page 25](#).

1.1.1 Upgrading the Existing Database

For information on upgrading PostgreSQL, see <https://www.postgresql.org/docs/current/static/upgrading.html>.

For information on upgrading SQL Server, see <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server>.

1.2 License

Upgrading from a previous version of File Reporter will require a version 4.0 license. For procedures on updating the license, see [Appendix A, “Replace a License File,” on page 107](#).

1.3 Engine, Scan Processor, and Web Application

Upgrade the Engine, Web Application, and Scan Processor by installing the updated Engine installation package on top of the existing software by following the procedures in [Chapter 7, “Installing and Configuring the Engine, Database, Message Broker, and Web Application,”](#) on page 43.

1.4 File Content Scanning

Introduced with the release of File Reporter 3.5, file content scanning enables you to scan and classify file content. If you plan to utilize this capability, there will be new components to install as part of the upgrade process. For more information, see [Section 2.4, “Determine Whether to Scan File Content,”](#) on page 15.

1.5 Microsoft 365 Reporting

Introduced with the release of File Reporter 4.0, this enables you to scan and report on unstructured data, including metadata and permissions stored in the cloud repositories of OneDrive for Business, SharePoint Online document libraries, and Teams document libraries. If you plan to utilize this capability, you will need to install RabbitMQ, the Message Broker, and Agent365.

1.6 Agents

File Reporter 4.0 includes three Agent types:

- ◆ File System
- ◆ File Content
- ◆ Microsoft 365 Cloud

1.6.1 File System Agents

Formerly known simply as Agents, these are now referred to as File System Agents to distinguish them from the Content Agents introduced in File Reporter 3.5. File System Agents examine and report on NTFS file systems. Additionally, File System Agents examine and report on file system security and permissions.

File Reporter includes a single File System Agent:

- ◆ **AgentFS:** The Agent for scanning Windows network storage devices.

1.6.2 Content Agent

File Reporter currently includes a single Content Agent:

- ◆ **AgentFC:** Agent that performs file content scanning on files stored on Windows storage devices.

If you plan to utilize file content scanning you will need to install Content Agents as part of the upgrade process. For more information, see [Section 2.4, “Determine Whether to Scan File Content,”](#) on page 15.

1.6.3 Microsoft 365 Cloud Agent

- ♦ **Agent365:** Responsible for scanning the metadata and permissions of the files stored in OneDrive for Business, SharePoint Online document libraries, and Teams document libraries.

2 Deployment Planning

File Reporter can be installed to work in a variety of configurations. Before proceeding with the installation, you should understand how to deploy File Reporter to best meet the needs of your organization.

- ◆ [Section 2.1, “Understand the Technologies and Expertise You Need,” on page 13](#)
- ◆ [Section 2.2, “Decide Where to Host the Engine,” on page 14](#)
- ◆ [Section 2.3, “Decide Which Database to Utilize,” on page 14](#)
- ◆ [Section 2.4, “Determine Whether to Scan File Content,” on page 15](#)
- ◆ [Section 2.5, “Determine Whether to Scan Microsoft 365,” on page 15](#)
- ◆ [Section 2.6, “Develop a Plan for Deploying the Agents for Scanning,” on page 15](#)
- ◆ [Section 2.7, “Database Deployment Recommendations,” on page 16](#)

2.1 Understand the Technologies and Expertise You Need

Before you install File Reporter, review the following table to understand how different technologies might affect how you proceed.

Technology	Notes
Windows and Windows Networking	The Engine runs on a Windows operating system and uses basic TCP/IP networking inherent to the operating system.
Microsoft Internet Information Server (IIS)	File Reporter is accessed and managed via a Web browser. The Web service is an ASP.NET application that runs in conjunction with IIS. The installer and configuration utilities automatically configure IIS and manage most aspects of the installation for you. The Engine and Web service must run on the same system in this release of the software.
DNS	In order to access the File Reporter Web service with a browser, the Web site name as registered with IIS must be used. In other words, the raw IP address does not work. You need to create a DNS entry for the name in the environment, or the entry needs to be added to the hosts file on every machine accessing the File Reporter system.
Database	File Reporter utilizes a Microsoft SQL Server or PostgreSQL database as the back end data store. The database must be accessible from the server running the Engine.

Technology	Notes
Active Directory and Windows Server	<p>For reporting on Active Directory and Windows file systems, File Reporter makes use of a proxy object and group in Active Directory that is used by the system as part of day-to-day operations.</p> <p>You should be familiar with the Windows network that you will be reporting against with File Reporter as well as with basic Windows file system and Active Directory terminology and operations.</p>
Messaging Broker	To enable messaging between File Reporter components that are needed for file content scanning (ManagerFC and AgentFC), File Reporter utilizes the RabbitMQ messaging broker.

2.2 Decide Where to Host the Engine

- ◆ The Engine server host should have significant CPU, disk, and memory for all but the smallest installations.
- ◆ The Engine runs on any of the following Windows Servers:
 - ◆ Windows Server 2019
 - ◆ Windows Server 2016
- ◆ The Engine host must be joined to the domain

NOTE: Micro Focus strongly recommends that you install the Engine on a member server and not on a domain controller. This recommendation might be a requirement in a future release.

2.3 Decide Which Database to Utilize

IMPORTANT: Database deployment recommendations are detailed in [Section 2.7, “Database Deployment Recommendations,”](#) on page 16.

You can utilize either a PostgreSQL database or a Microsoft SQL Server database. Here are some considerations for choosing one over the other:

- ◆ You might prefer to utilize Microsoft SQL Server if you have a Microsoft Licensing Agreement that entitles you to Microsoft SQL Server.

File Reporter supports the Standard and Enterprise versions of SQL Server. It does not support the Web or Express editions.
- ◆ You might prefer to utilize the PostgreSQL database if you are proficient with Linux.

2.4 Determine Whether to Scan File Content

Among the capabilities of File Reporter is the ability to scan and classify file content. For example, you can scan for files containing U.S. Social Security numbers and then classify these documents as restricted documents whose access permissions and storage locations might need to be corrected.

If you plan to scan Windows network storage devices for file content, you will need to install the following additional components:

- ◆ RabbitMQ messaging broker
- ◆ ManagerFC
- ◆ AgentFC

For more details on File Content Scanning, see [File Content Scanning](#) in the *Micro Focus File Reporter 4.0 Administration Guide*.

2.5 Determine Whether to Scan Microsoft 365

With the release of File Reporter 4.0, File Reporter can scan and report on the metadata and permissions of files stored in OneDrive for Business, SharePoint Online, and Teams. If you plan to scan and report on these Microsoft 365 cloud-stored files, you will need to install the following components:

- ◆ RabbitMQ messaging broker
- ◆ Agent365

2.6 Develop a Plan for Deploying the Agents for Scanning

Target System to be Scanned	Agent can be Installed Locally?	Potential Proxy Agents
Windows	Yes	AgentFS
Network Attached Storage (NAS) Device (CIFS-based)	No	AgentFS
Microsoft 365 cloud	Yes	Not applicable

When you decide whether to install the Agent locally on a Windows server, or to have the Agent service run through a proxy, be aware of the following:

- ◆ Locally installed Agents perform scans faster than proxy-based Agents.
- ◆ Locally installed Agents share CPU and memory resources with other software running on the system. If a server is already constrained for resources, consider using a proxy instead of installing the Agent locally.

2.7 Database Deployment Recommendations

You should consider the following guidelines before installing and configuring any database system for File Reporter.

- ◆ [Section 2.7.1, “Use a Dedicated Server,” on page 16](#)
- ◆ [Section 2.7.2, “Use a Dedicated Database Instance,” on page 16](#)
- ◆ [Section 2.7.3, “Provide Sufficient I/O Bandwidth,” on page 16](#)

2.7.1 Use a Dedicated Server

Due to the potential size of the collected scan data and the I/O processing needed for large database installations, we strongly recommend that you install the database on a dedicated server.

- ◆ For minimum requirements for PostgreSQL, see [Section 4.1.1, “Minimum Requirements,” on page 23](#).
- ◆ For minimum requirements for a SQL Server host, see [Section 5.1, “Minimum Requirements,” on page 25](#).

2.7.2 Use a Dedicated Database Instance

In addition to sizing requirements, we recommend that you use a dedicated SQL Server instance or PostgreSQL cluster to prevent conflicts with other vendor software. File Reporter needs access to manage the database security principals and roles, which requires access at the instance level. In addition, File Reporter now ships with optional CLR extensions for SQL Server, which requires enablement at the instance level.

In short, do not install the File Reporter database in an instance or cluster that shares databases with other software.

2.7.3 Provide Sufficient I/O Bandwidth

Relational Database Management Systems are by nature very I/O intensive, especially when it comes to persisted storage on disk. For best performance, consider the following:

- ◆ Provide SSD-backed storage if possible for the database tablespaces or filegroups*.
- ◆ Alternatively, provide RAID-10 spindle storage for database tablespaces or filegroups*.
- ◆ Do not use RAID-5 storage for database storage.
- ◆ Do not use Network Attached Storage for database storage.
- ◆ If using a SAN, be sure to provide at least 10 GB or more throughput (ideally, the SAN link should be faster than the I/O capacity of the backend storage system, so that it is not the bottleneck).
- ◆ Be sure to enable battery-backed cache for RAID and SAN controllers.
- ◆ For SQL Server, optionally place tempdb on a separate RAID-1 or SSD.
- ◆ Optionally, place the transaction logs on a separate RAID-1 or SSD.

This can be done either during the installation of the SQL Server instance or afterwards.

For procedures on moving database files after the installation of an SQL Server instance, see <https://msdn.microsoft.com/en-us/library/ms189133.aspx>.

For PostgreSQL, moving database files is a simple process of stopping the database server, relocating the `pg_xlog` folder, and then creating a symbolic link to the new path.

The need for separate disks for transaction logs is minimized if the main storage is already on RAID-10 or SSD, and the I/O channel is not already saturated.

*For basic information on SQL Server filegroups, see <https://msdn.microsoft.com/en-us/library/ms189563.aspx>.

*For basic information on PostgreSQL tablespaces, see <https://www.postgresql.org/docs/current/static/manage-ag-tablespaces.html>.

3 Licensing the Product

This section provides procedures for obtaining a Micro Focus product activation key and obtaining a production license.

For procedures on replacing a license file, see [Appendix A, “Replace a License File,”](#) on page 107.

- ♦ [Section 3.1, “Obtaining a Product Activation Key,”](#) on page 19
- ♦ [Section 3.2, “Obtaining a License File,”](#) on page 19

3.1 Obtaining a Product Activation Key

- 1 In a Web browser, go to <https://www.microfocus.com/customercenter>.
- 2 Enter your username and password, then click **Login**.
- 3 Click **Software**.
- 4 In the page, locate **File Reporter**.
- 5 Click **Keys**.
- 6 Highlight and copy the alphanumeric characters in the displayed activation key.
You will be required to paste the activation key into a form to obtain a production license.

3.2 Obtaining a License File

Micro Focus File Reporter requires a production license file or evaluation license file that you obtain from Micro Focus.

- 1 In a Web browser, go to <https://www.filereportersupport.com>.
- 2 On the top banner of the Web page, click **License**.
A new Web page appears with options for obtaining the license.

License

Enter the required information below and click 'Submit' to generate your license file.
After verification, a link to the license file will be sent to the e-mail address entered below.

Customer Contact Information

First Name*	<input type="text"/>
Last Name*	<input type="text"/>
Email*	<input type="text"/>
Telephone*	<input type="text"/>
Address Line 1*	<input type="text"/>
Address Line 2:	<input type="text"/>
City*	<input type="text"/>
State / Province*	<input type="text"/>
Zip / Postal Code*	<input type="text"/>
Country*	<input type="text"/>

License Registration

Organization Name*	<input type="text"/>
Product:	File Reporter
Version*	4.0
Directory Service:	<input checked="" type="radio"/> Active Directory
Forest Root Name*	ad.example.com

The license keys are based on the distinguished name of the forest root domain in Active Directory.

[ADForestRootName Utility](#)

For help in determining the correct domain name to use, download and run.

Microsoft 365 (optional): Enable Microsoft 365 capabilities.

License Type: Evaluation Activation

Notice: Evaluation licenses are for the express purpose of product evaluation and testing. All features of the software may not be active or available when using evaluation licenses. Any use of the product using this license in a production network for production purposes or work is expressly prohibited.

Acceptance* I certify acceptance of this policy on behalf of my company, school, or organization.

I'm not a robot



Submit

3 Complete the fields.

3a In the **License Type** region, select **Activation** and in the **Activation Code** field, paste the activation key that you received from Micro Focus.

4 Click **Submit**.

An e-mail from File Reporter Support is automatically sent to you with an embedded link for accessing the license.

5 In the email, click **Download License File**.

A new Access Web page is opened.

6 From the Access page, select the listed license file and click the arrow icon to download the license.

7 Note where the license file is saved.

You need the license file to complete Engine setup wizard.

4 Installing and Configuring the PostgreSQL Database

This section provides links to procedures for installing and configuring the PostgreSQL database on a Linux server host.

4.1 Installing and Configuring the PostgreSQL Database on a Linux Server

- ♦ [Section 4.1.1, “Minimum Requirements,” on page 23](#)
- ♦ [Section 4.1.2, “Installing and Configuring the PostgreSQL Database,” on page 24](#)

4.1.1 Minimum Requirements

- ♦ Any major 64-bit Linux distribution supported by PostgreSQL.

PostgreSQL itself is supported on many host systems including UNIX, Linux and Windows variants. However, support in troubleshooting PostgreSQL itself is limited to the following major Linux distributions:

- ♦ SUSE Linux (SUSE Linux Enterprise Server, openSUSE)
- ♦ Red Hat
- ♦ CentOS
- ♦ Ubuntu

These major Linux distributions include PostgreSQL in their repositories.

For PostgreSQL installations on other hosts, support is limited to the data and schema in the database itself, not performance tuning or configuration.

Due to performance limitations, installing PostgreSQL on Windows is discouraged, especially for large deployments.

- ♦ Minimum of 16 GB of RAM

Depending on size and frequency of your scans, this amount might need to be significantly increased.

- ♦ Minimum of 100 GB of disk space

Depending on the size and frequency of your scans, this amount might need to be significantly increased.

4.1.2 Installing and Configuring the PostgreSQL Database

For procedures on installing and configuring PostgreSQL, see the following:

- ♦ <https://www.postgresql.org/docs/current/static/creating-cluster.html>
- ♦ <https://www.postgresql.org/docs/current/static/runtime.html>
- ♦ <https://www.postgresql.org/docs/current/static/runtime-config.html>

You will need to follow the references that are specific to the version of PostgreSQL that is installed in your environment.

5 Installing an SQL Server Instance that Supports File Reporter

This section provides procedures for installing a Microsoft SQL Server instance with the settings needed to support File Reporter.

- ◆ [Section 5.1, “Minimum Requirements,” on page 25](#)
- ◆ [Section 5.2, “Prerequisites,” on page 25](#)
- ◆ [Section 5.3, “Install a New Instance of SQL Server,” on page 26](#)
- ◆ [Section 5.4, “Post Configuration Considerations,” on page 31](#)

IMPORTANT: For best performance, Micro Focus strongly recommends that the database and Engine be installed on separate hosts.

5.1 Minimum Requirements

File Reporter supports the Standard and Enterprise versions of SQL Server. It does not support the Web or Express editions.

Microsoft SQL Server Software

- ◆ SQL Server 2019 (Windows Server or Linux)
- ◆ SQL Server 2017 (Windows Server or Linux)
- ◆ SQL Server 2016 SP2

Server Host

- ◆ Any Microsoft supported version of SQL Server running on a 64-bit multi-core processor machine
- ◆ Minimum 16 GB RAM
Depending on the size and frequency of your scans, you might need significantly more RAM.

For procedures on installing SQL Server, see <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server>.

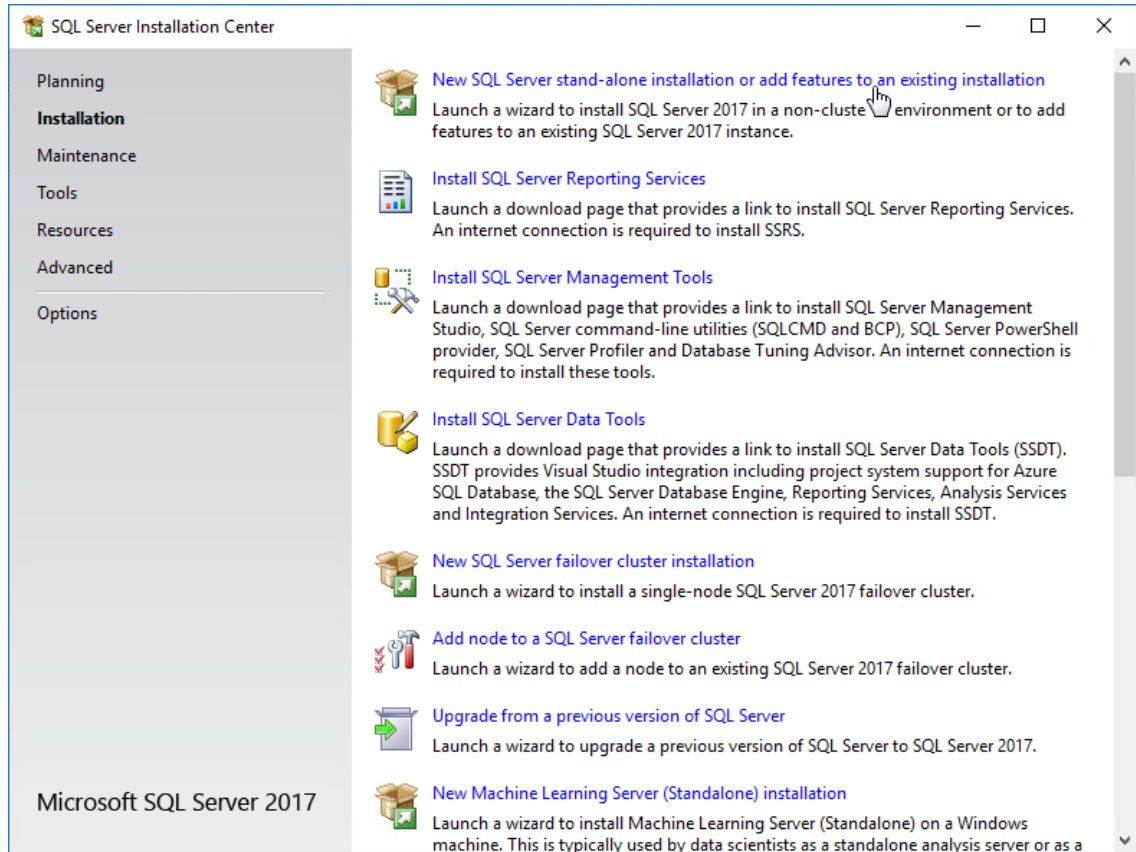
5.2 Prerequisites

- ◆ Verify that you have installed the latest SQL Server updates.

5.3 Install a New Instance of SQL Server

The following procedures are specific to Microsoft SQL Server 2017. Procedures will vary based on your version of SQL Server.

- 1 From the Microsoft SQL Server ISO, double-click `setup.exe`.
- 2 On the SQL Server Installation Center page, click **Installation**.
- 3 Select **New SQL Server stand-alone installation or add features to an existing installation**.

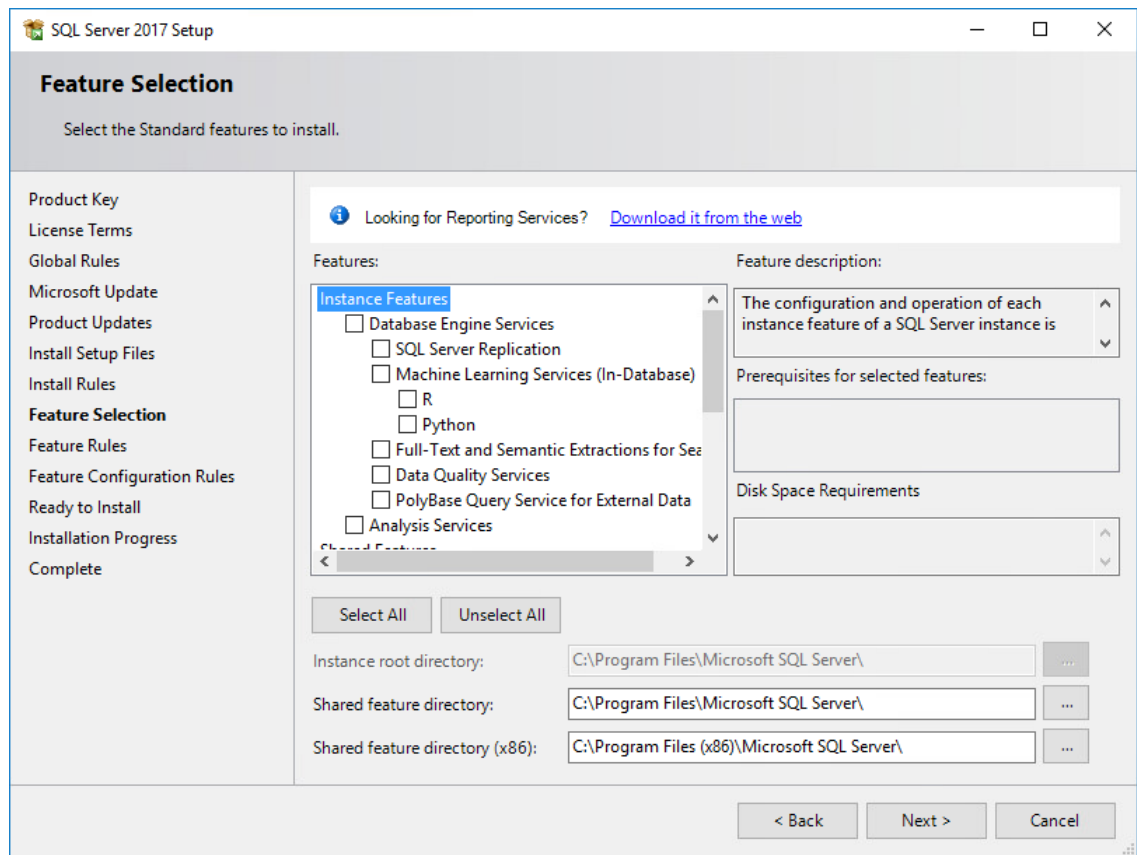


The Setup Support Rules operation is run.

- 4 When the operation has completed, click **OK**.
- 5 When prompted, enter your product key, then click **Next**.
- 6 Accept the license terms, then click **Next**.
- 7 Include all Microsoft SQL Server product updates, then click **Next**.

The Setup Support Rules operation is run again.

- 8 When the operation has completed, click **Next**.



- 9 On the Feature Selection page, select **Database Engine Services**.
- 10 In the **Instance root directory**, **Shared feature directory**, and **Shared feature directory (x86)** fields, specify the path where you want to SQL instance to reside, then click **Next**.
- 11 In the Instance Configuration page, click the **Named instance** option and specify a descriptive name for the instance such as SRSDB and click **Next**.
- 12 On the Server Configuration page, click the **Collation** tab.
- 13 Click **Customize**.
- 14 Click the **Windows collation designator and sort order** option.
- 15 From the **Collation designator** drop-down menu, select an acceptable collation and settings for your locale.

For example, in North America, an acceptable collation would be **Latin1_General_100** with the **Accent-sensitive** check box selected.

We recommend that you select a collation that aligns with the Windows locale of the server where the Engine is installed.

For more information on collation and locales, refer to [this Microsoft document \(http://technet.microsoft.com/en-us/library/ms175194%28v=sql.105%29.aspx\)](http://technet.microsoft.com/en-us/library/ms175194%28v=sql.105%29.aspx).

Customize the SQL Server 2017 Database Engine Collation

Select the collation you would like to use:

Windows collation designator and sort order

Collation designator:

Binary Binary-code point

Case-sensitive Kana-sensitive

Accent-sensitive Width-sensitive

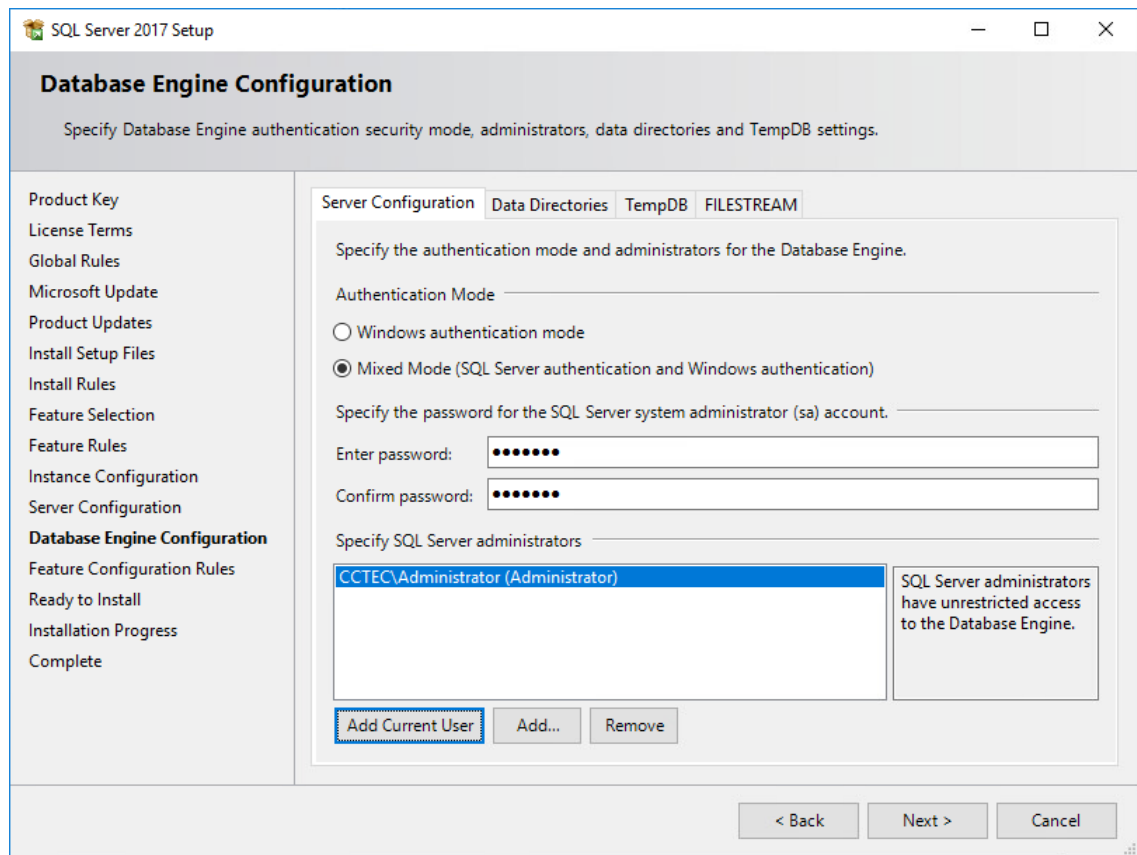
Supplementary characters Variation selector-sensitive

SQL collation, used for backwards compatibility

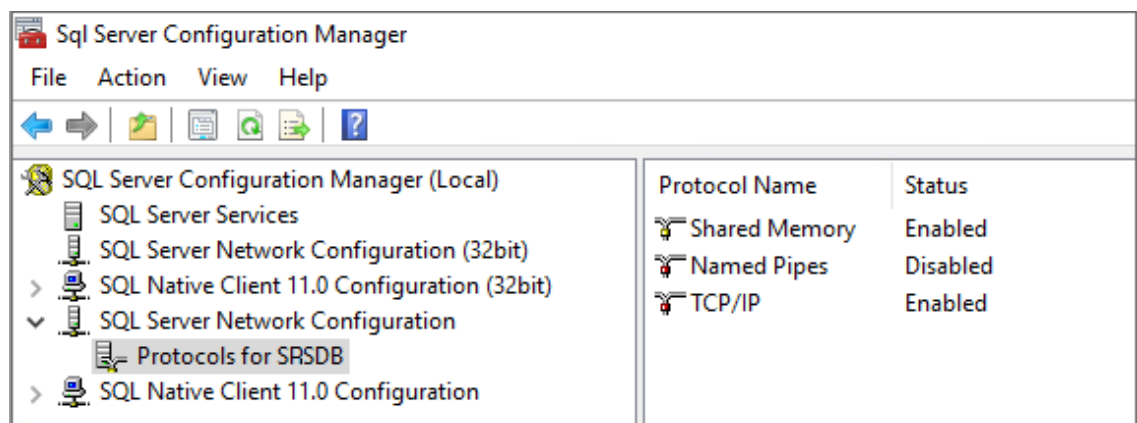
SQL_Hungarian_CP1250_CI_AS
 SQL_Hungarian_CP1250_CS_AS
 SQL_Icelandic_Pref_CP1_CI_AS
 SQL_Latin1_General_CP1_CI_AI
 SQL_Latin1_General_CP1_CI_AS

Collation description:
 Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data

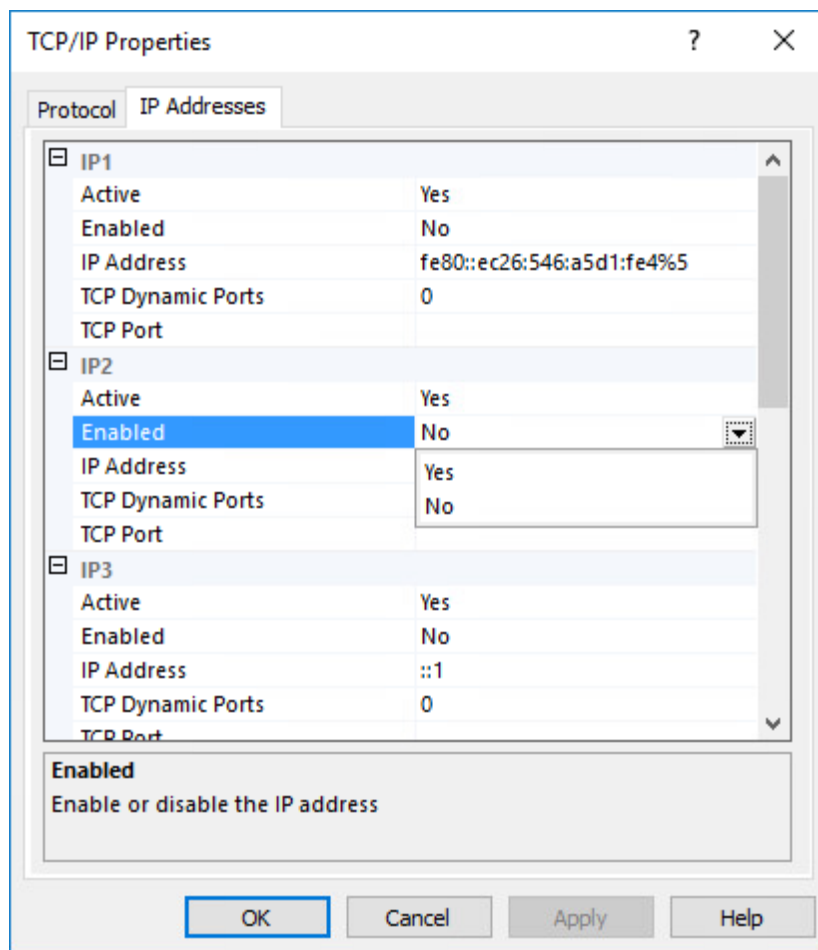
- 16 Click **OK**.
- 17 Click **Next**.
- 18 On the Database Engine Configuration page, select the **Mixed Mode (SQL Server authentication and Windows authentication)** option, enter and confirm the SQL Server administrator password, then click **Add Current User**.
- 19 Click **Next**.



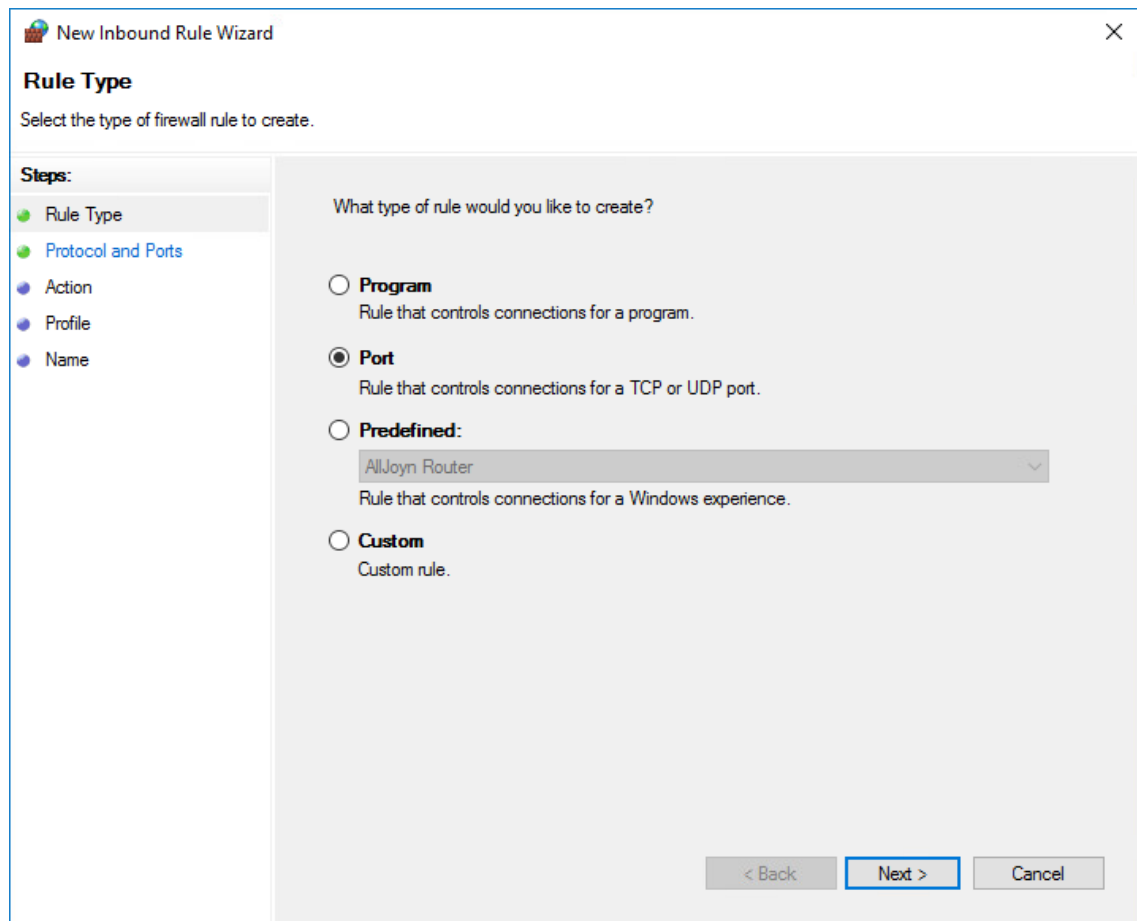
- 20 Click **Install**.
- 21 When the installation has completed, click **Close** to close the wizard.
- 22 Launch SQL Server Configuration Manager.
- 23 In the left pane, expand **SQL Server Network Configuration**.
- 24 Click **Protocols for SRSDB** (or the name of the database instance you chose earlier).



- 25 Right-click **TCP/IP** and select **Properties**.
- 26 Click the **IP Addresses** tab.
- 27 Under the **IP2** heading, for the **Enabled** field, right-click to select the drop-down menu and change the setting to **Yes**.



- 28 Select **TCP Dynamic Ports** and clear the field so there is no number associated to it.
- 29 Scroll down to the **IPALL** heading and for the **TCP Dynamic Ports** field, clear the field so there is no number associated to it.
- 30 In the **TCP Port** field, and enter 1433.
- 31 Click **Apply**.
- 32 When the warning dialog box appears, click **OK**.
- 33 Click **OK** to close the TCP/IP Properties page.
- 34 Close the SQL Server Configuration Manager.
- 35 Launch Windows Firewall with Advanced Security.
- 36 From the left column, click **Inbound Rules**.
- 37 From the **Actions** column, click **New Rule**.
- 38 In the Rule Type page, select **Port**.



- 39 Click **Next**.
- 40 In the Protocol and Ports page, enter 1433 in the **Specific local ports** field, then click **Next**.
- 41 In the Action page, accept the default setting by clicking **Next**.
- 42 In the Profile page, accept the default settings by clicking **Next**.
- 43 In the Name page, specify a name for the new inbound rule in the **Name** field.
For example SQL Server.
- 44 Click **Finish**.

5.4 Post Configuration Considerations

Review these points and make any needed adjustments to your SQL database settings before installing and configuring the File Reporter Engine and Web Application:

- ◆ The SQL Server service must be listening via TCP/IP v4, because the Engine and Web Service requires that for access.
- ◆ Some editions of SQL Server do not have TCP/IP enabled by default. If there are multiple instances, the instance that you just installed and configured might not be listening on the default port of 1433.
- ◆ Firewall rules might need to be modified.

6 Installing and Configuring RabbitMQ

- ◆ Section 6.1, “Upgrading from an Earlier Version of RabbitMQ,” on page 33
- ◆ Section 6.2, “Extracting RabbitMQ,” on page 34
- ◆ Section 6.3, “Creating Certificates for RabbitMQ,” on page 34
- ◆ Section 6.4, “Installing Rabbit MQ,” on page 38
- ◆ Section 6.5, “Changing the Default Password,” on page 39

RabbitMQ is an open source message broker that enables messaging between File Reporter components that are needed for file content scanning or for reporting on Microsoft 365 cloud applications including OneDrive, SharePoint Online, and Teams. Components include ManagerFC and AgentFC for content scanning and reporting, and Agent365 for Microsoft 365 cloud reporting. If you will not be performing file content scanning or reporting on Microsoft 365 cloud applications, you do not need to install RabbitMQ.

RabbitMQ can be installed using any of the supported distributions found here: <http://www.rabbitmq.com/download.html>.

In order to assist with the introduction of RabbitMQ into the File Reporter framework, a simplified, supported distribution for Windows has been included with this release. This distribution is meant solely for use in basic scenarios where clustering, containerization, or automated upgrades are not required. The installation steps in this chapter pertain solely to this included distribution. For other RabbitMQ distributions or installers, please follow the accompanying documentation included with them.

6.1 Upgrading from an Earlier Version of RabbitMQ

File Reporter introduced file content scanning in version 3.5 and subsequently introduced the RabbitMQ message broker as a File Reporter component. If you installed RabbitMQ previously, you are encouraged to upgrade to the updated version that is provided. Before doing so, you should do the following:

- 1 Verify all scans are completed or canceled.
- 2 Uninstall the service.
 - 2a Stop the RabbitMQ service.

The console command is `sc stop rabbitmq`
 - 2b Within the existing RabbitMQ folder, run `remove-rabbitmq-service.bat`
- 3 Delete the existing RabbitMQ folder.
- 4 Follow the installation steps in the remainder of this chapter to install and set up the new version.

6.2 Extracting RabbitMQ

- 1 Install the Visual C++ Redistributable Packages for Visual Studio 2013.

The Erlang runtime for RabbitMQ requires the Visual C++ Redistributable Package for Visual Studio 2013. This is a common dependency for many applications, so it might already be present on the machine where RabbitMQ is to be installed.

If this package is not currently installed, it may be found at: <https://www.microsoft.com/en-us/download/details.aspx?id=40784>.

- 2 At the root of the `FileReporter_4.0.iso` image, unzip the `RabbitMQ-3.8.x.zip` file to the your desired path.

NOTE: The path cannot contain spaces. The zipped file contains the `rabbitmq` folder.

- 3 Proceed with [Section 6.3, “Creating Certificates for RabbitMQ,”](#) on page 34.

6.3 Creating Certificates for RabbitMQ

Certificates are needed to enable TLS for secure messaging between RabbitMQ, ManagerFC, AgentFC, and the Web Application.

- 1 At the root of the `FileReporter_4.0.iso` image, double-click `CertificateGenerator.exe`.

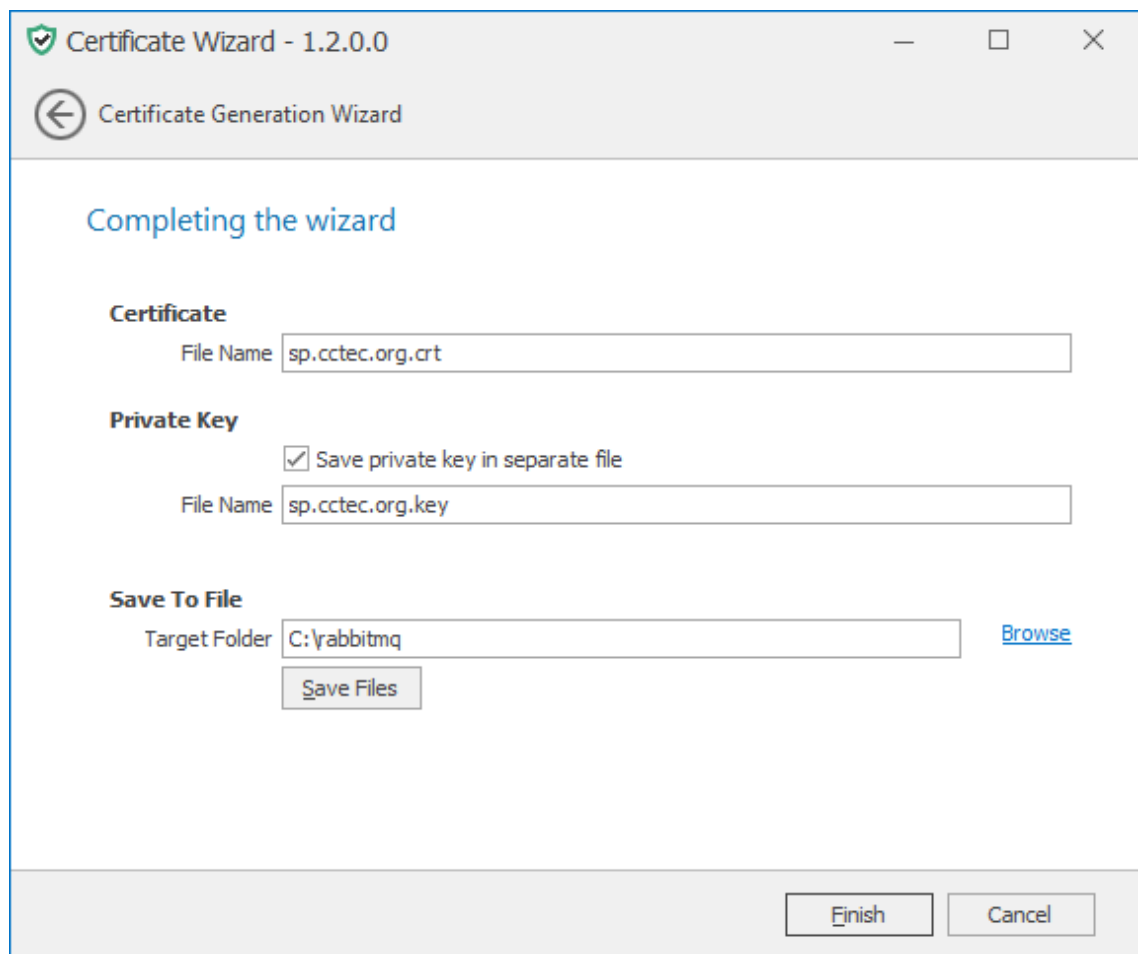
The image shows a Windows-style dialog box titled "Certificate Wizard" with a sub-header "Certificate Generation Wizard". The main content area is titled "Certificate Parameters" and contains a section for "Basic Parameters".

Basic Parameters

- Subject Name:** A text input field containing the text "Hostname".
- Expiration:** A numeric spinner box set to "5" followed by the text "years".
- Key Length:** A dropdown menu currently showing "4096".

At the bottom right of the dialog, there are two buttons: "Generate" and "Cancel".

- 2 In the **Subject Name** field, enter the DNS for the RabbitMQ service.
- 3 (Optional) Modify the settings in the other fields.
- 4 Click **Generate**.



Certificate: Information pertaining to the certificate that is to be generated.

File Name: The default name and path of the certificate to be generated. If you choose, you can modify the name and path.

Private Key: Information and settings pertaining to the private key.

Save private key in separate file: When selected, this option saves the private key as a separate file from the certificate.

For use with RabbitMQ, having a separate key file might be less confusing.

File Name: The default name and path of the private key to be generated. If you choose, you can modify the name and path.

Save To File: Information and the means of saving the certificate and private key.

Target Folder: The default file path for the certificate and if specified, the private key. If you choose, you can modify the path.

Browse: Click to specify a new location for the certificate and if specified, the private key.

5 Make any needed modifications to the settings and click **Save Files**.

If one of the files already exists, you are prompted to overwrite it.

6 When notified that the files have been saved, click **OK**.

7 Click **Finish**.

You will be notified if you have not yet saved your certificate files.

- 8 From the location where the files were generated, copy them to a folder on the RabbitMQ system.

For example, copy them to the RabbitMQ folder that is created when you extract the RabbitMQ-3.8.xx.zip file.

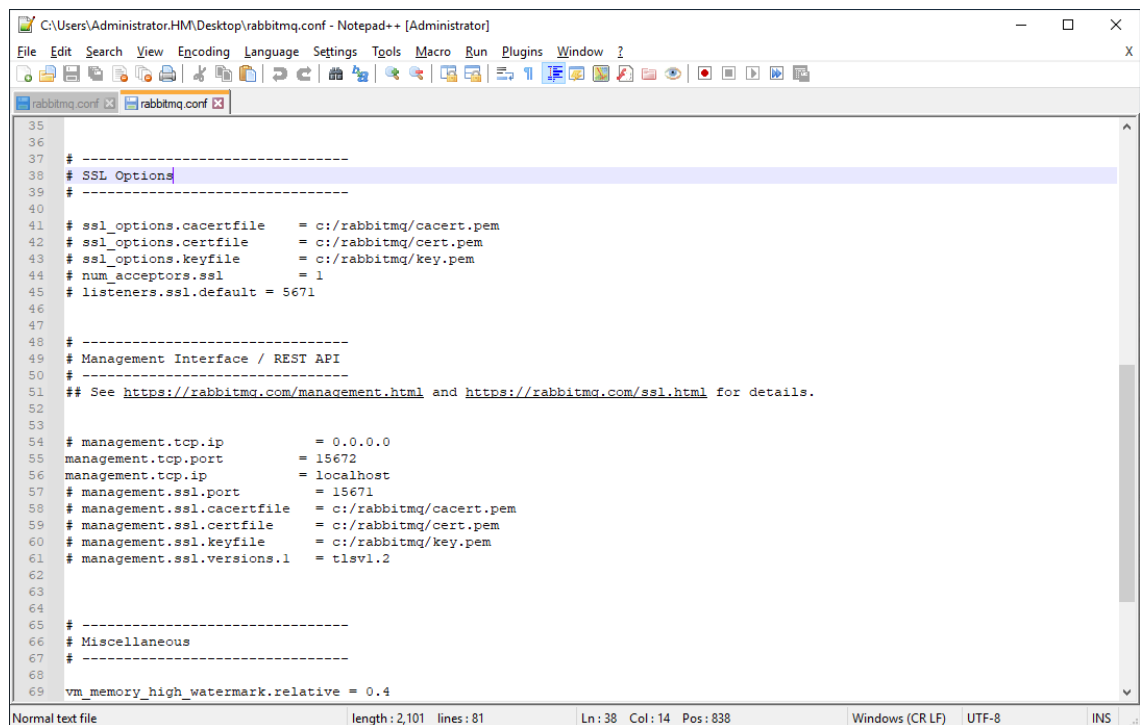
- 9 Edit the `rabbitmq.conf` file located in the `rabbitmq\base` folder where RabbitMQ was extracted (if using the provided archive).

- 10 Modify the entries for `ssl_options.*`

Note that paths are absolute and use forward slashes.

Uncomment the following lines:

```
ssl_options.cacertfile
ssl_options.certfile
ssl_options.keyfile
num_acceptors.ssl
listeners.ssl.default
```



```
C:\Users\Administrator.HM\Desktop\rabbitmq.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
rabbitmq.conf x rabbitmq.conf x
35
36
37 # -----
38 # SSL Options
39 # -----
40
41 # ssl_options.cacertfile = c:/rabbitmq/cacert.pem
42 # ssl_options.certfile = c:/rabbitmq/cert.pem
43 # ssl_options.keyfile = c:/rabbitmq/key.pem
44 # num_acceptors.ssl = 1
45 # listeners.ssl.default = 5671
46
47 # -----
48 # Management Interface / REST API
49 # -----
50 #
51 ## See https://rabbitmq.com/management.html and https://rabbitmq.com/ssl.html for details.
52
53
54 # management.tcp.ip = 0.0.0.0
55 management.tcp.port = 15672
56 management.tcp.ip = localhost
57 # management.ssl.port = 15671
58 # management.ssl.cacertfile = c:/rabbitmq/cacert.pem
59 # management.ssl.certfile = c:/rabbitmq/cert.pem
60 # management.ssl.keyfile = c:/rabbitmq/key.pem
61 # management.ssl.versions.1 = tlsv1.2
62
63
64 # -----
65 # Miscellaneous
66 # -----
67 #
68
69 vm_memory_high_watermark.relative = 0.4
Normal text file length: 2,101 lines: 81 Ln: 38 Col: 14 Pos: 838 Windows (CR LF) UTF-8 INS
```

- 11 Modify the entries for `management.*` interface.

Note that paths are absolute and use forward slashes.

Comment the following lines:

```
management.tcp.port
management.tcp.ip
```

Uncomment the following lines:

```
management.ssl.port
management.ssl.cacertfile
```

```
management.ssl.certfile
management.ssl.keyfile
management.ssl.versions.1
```

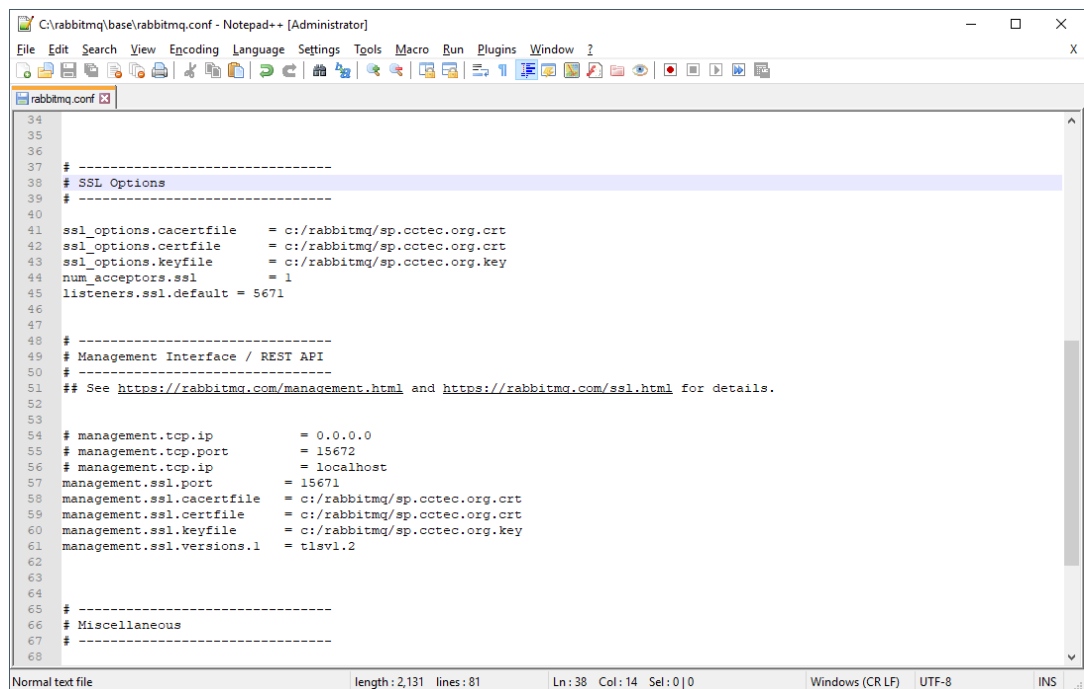
12 Specify the certificate and private key.

12a In the SSL Options section, modify the paths pertaining to `ssl_options.cacertfile` and `ssl_options.certfile` with the path to the certificate you created in Step 5.

12b While still in the SSL Options section, modify the path pertaining to `ssl_options.keyfile` to the private key that you created in Step 5.

12c In the Management Interface / REST API section, modify the paths pertaining to `management.ssl.cacertfile` and `management.ssl.certfile` with the path to the certificate you created in Step 5.

12d While still in the Management Interface / REST API section, modify the path pertaining to `management.ssl.keyfile` with the path of the private key you created in Step 5.



```
C:\rabbitmq\base\rabbitmq.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
rabbitmq.conf
34
35
36
37 # -----
38 # SSL Options
39 # -----
40
41 ssl_options.cacertfile = c:/rabbitmq/sp.ctec.org.crt
42 ssl_options.certfile  = c:/rabbitmq/sp.ctec.org.crt
43 ssl_options.keyfile   = c:/rabbitmq/sp.ctec.org.key
44 num_acceptors.ssl    = 1
45 listeners.ssl.default = 5671
46
47
48 # -----
49 # Management Interface / REST API
50 # -----
51 ## See https://rabbitmq.com/management.html and https://rabbitmq.com/ssl.html for details.
52
53
54 # management.tcp.ip      = 0.0.0.0
55 # management.tcp.port   = 15672
56 # management.tcp.ip     = localhost
57 management.ssl.port     = 15671
58 management.ssl.cacertfile = c:/rabbitmq/sp.ctec.org.crt
59 management.ssl.certfile  = c:/rabbitmq/sp.ctec.org.crt
60 management.ssl.keyfile   = c:/rabbitmq/sp.ctec.org.key
61 management.ssl.versions.1 = tlsv1.2
62
63
64
65 # -----
66 # Miscellaneous
67 # -----
68
```

13 Save any modifications you have made to the configuration file.

14 Close the editor.

15 Proceed with [Section 6.4, “Installing Rabbit MQ,”](#) on page 38.

6.4 Installing Rabbit MQ

1 From the extracted RabbitMQ files, double-click the `rabbitmq` folder.

2 Double-click `install-rabbitmq-service.bat`.

RabbitMQ is installed.

```

Administrator: C:\Windows\system32\cmd.exe
E:\RabbitMQ>install-rabbitmq-service.bat
ERLANG_HOME: E:\RabbitMQ\otp-20.3
RABBITMQ_BASE: E:\RabbitMQ\base
RABBITMQ_HOME: E:\RabbitMQ\3.7.4
ERLINI: [erlang]
Bindir=E:\RabbitMQ\otp-20.3\erts-9.3\bin
Progamme=erl
Rootdir=E:\RabbitMQ\otp-20.3

E:\RabbitMQ\otp-20.3\erts-9.3\bin\erlsrv: Unable to remove service (not enough privileges?
Error: The handle is invalid.
E:\RabbitMQ\otp-20.3\erts-9.3\bin\erlsrv: Service RabbitMQ added to system.

SERVICE_NAME: rabbitmq
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                  : 3920
        FLAGS                 :

```

Successfully installed/updated RabbitMQ service.

```

E:\RabbitMQ>

```

In the graphic above, the error: The handle is invalid is normal during an installation and can be ignored.

- 3 From a Web browser, access the management interface for RabbitMQ by typing: `https://dns_name:15671`

This port might need to be opened in the firewall.

- 4 Proceed with [Section 6.5, “Changing the Default Password,”](#) on page 39.

6.5 Changing the Default Password

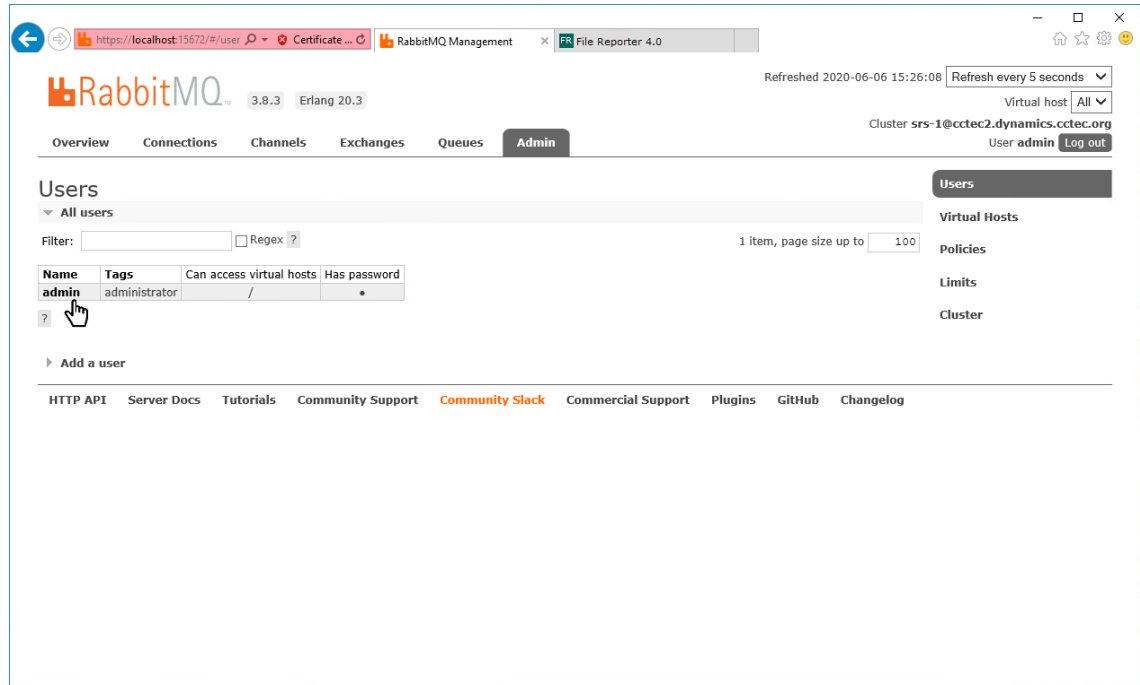
As a best practice, you should change the default password for RabbitMQ before performing any administrative work.

- 1 From a Web browser access the RabbitMQ management interface by typing: `https://server:15671` where *server* is the address of the server where RabbitMQ is installed.

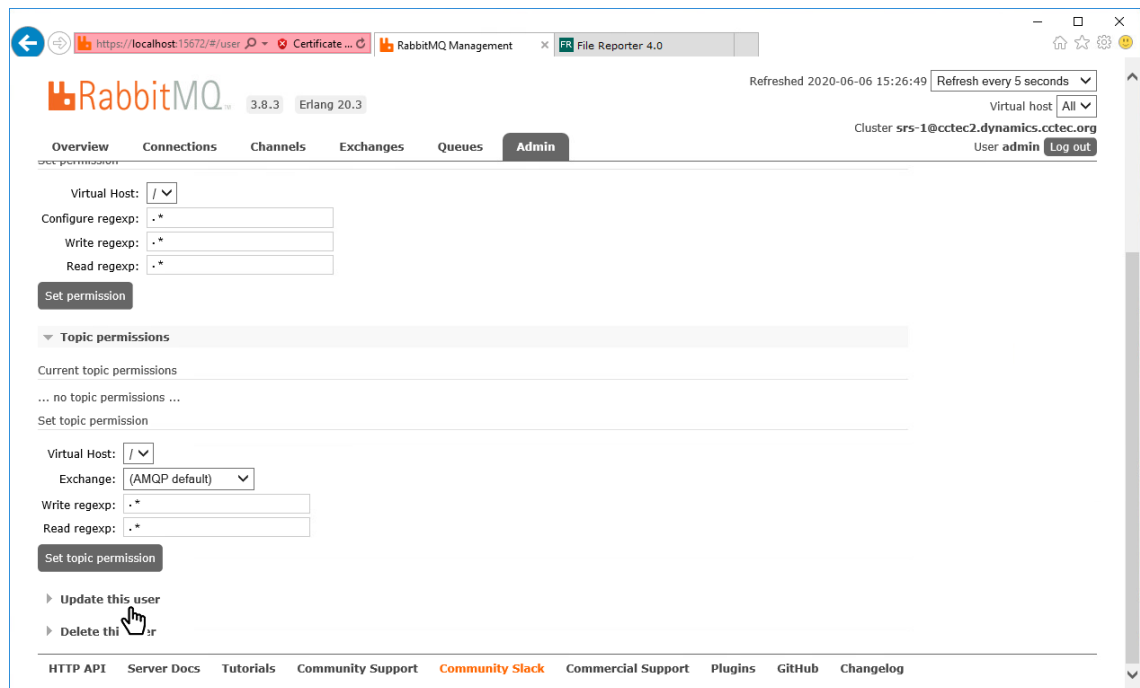


- 2 In the **Username** field, enter `admin`, in the **Password** field, enter `srsadmin`, then click **Login**.
- 3 Click the **Admin** tab.

4 Under the **Name** column, click **admin**.



5 In the new page, scroll down and select **Update this user**.



6 Enter and confirm the new password and click **Update user**.

The screenshot shows the RabbitMQ Management interface in a browser window. The address bar shows `https://localhost:15672/#/user`. The page title is "RabbitMQ" with version "3.8.3" and "Erlang 20.3". The page is refreshed every 5 seconds. The user is logged in as "admin" and the cluster is "srs-1@cctec2.dynamics.cctec.org".

The "Admin" tab is active, and the "Update this user" section is expanded. The "Password" field is set to "*****" and the "Confirm" field is also "*****". The "Tags" field is set to "administrator".

Below the "Update this user" section, there is a "Delete this user" section.

At the bottom of the page, there is a navigation bar with links: [HTTP API](#), [Server Docs](#), [Tutorials](#), [Community Support](#), [Community Slack](#), [Commercial Support](#), [Plugins](#), [GitHub](#), and [Changelog](#).

7 Installing and Configuring the Engine, Database, Message Broker, and Web Application

- ◆ [Section 7.1, “Minimum Requirements,” on page 43](#)
- ◆ [Section 7.2, “Prerequisites,” on page 43](#)
- ◆ [Section 7.3, “Installing the Engine,” on page 44](#)
- ◆ [Section 7.4, “Configuring the Database,” on page 46](#)
- ◆ [Section 7.5, “Installing the License,” on page 51](#)
- ◆ [Section 7.6, “Configuring the Engine,” on page 53](#)
- ◆ [Section 7.7, “Configuring the Message Broker,” on page 59](#)
- ◆ [Section 7.8, “Configuring the Web Application,” on page 62](#)

Procedures in this section include those needed for installing and configuring the Engine, configuring the database, and configuring the Web Application.

If not already installed, .NET 4.8 will be installed during the installation of the Engine.

7.1 Minimum Requirements

- ◆ Quad core 64-bit processor or better
- ◆ Minimum 16 GB RAM
 - Depending on the size and frequency of your reports, you might need significantly more RAM.
- ◆ Minimum 20 GB free space for installation files and scan processing space
- ◆ Supported operating systems:
 - ◆ Windows Server 2019
 - ◆ Windows Server 2016
- ◆ Active Directory requirements:
 - ◆ The server must be joined to Active Directory
 - ◆ Minimum forest functional level of Windows 2003

7.2 Prerequisites

- ◆ Create a new host record in DNS for use with the Web Application.

For example: fr.cctec.org

- ♦ If you will be scanning for file content or on Microsoft 365, you should first install the RabbitMQ messaging broker. For procedures, see [Chapter 6, “Installing and Configuring RabbitMQ,”](#) on [page 33](#).

7.3 Installing the Engine

IMPORTANT: In order to successfully install the Engine, you must be logged in as a domain administrator for the domain the computer is a member of. If you are not, the rights are not sufficient.

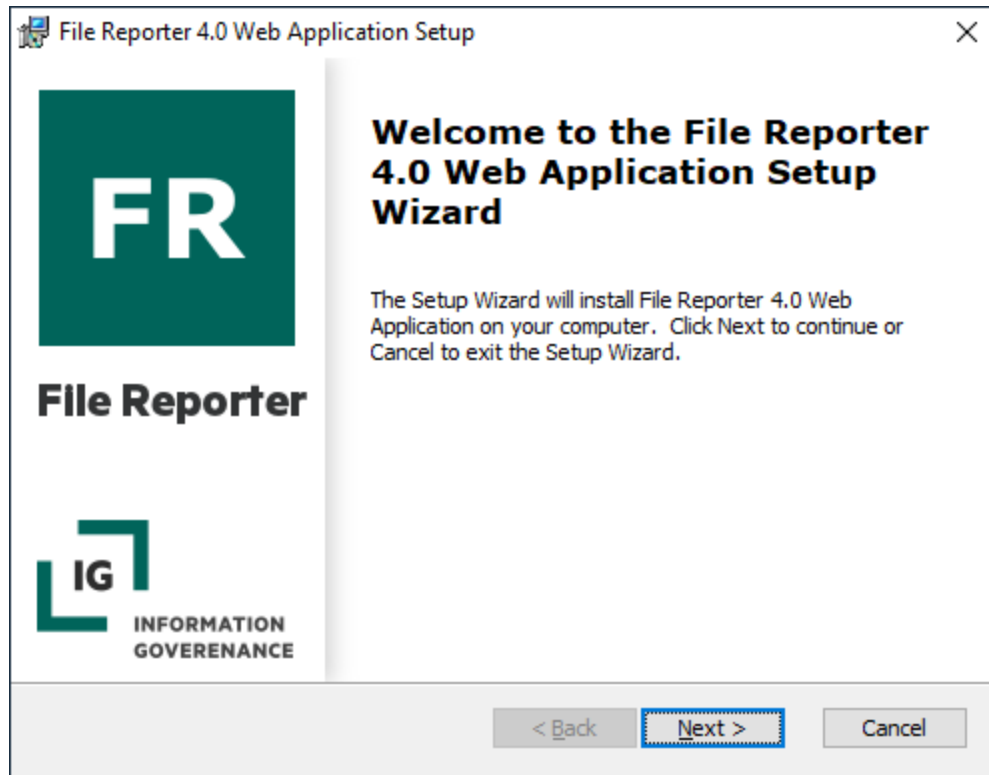
- 1 At the root of the `FileReporter_4.0.iso` image, double-click `FileReporter-Engine-4.0-x64-xxx.exe`.
- 2 When you are asked if you want to run this file, click **Run**.
- 3 Agree to the license terms and conditions and click **Install**.

If your File Reporter deployment will utilize Microsoft SQL Server as the database, a dialog box appears informing you of the need to update your OLE DB driver for SQL Server.

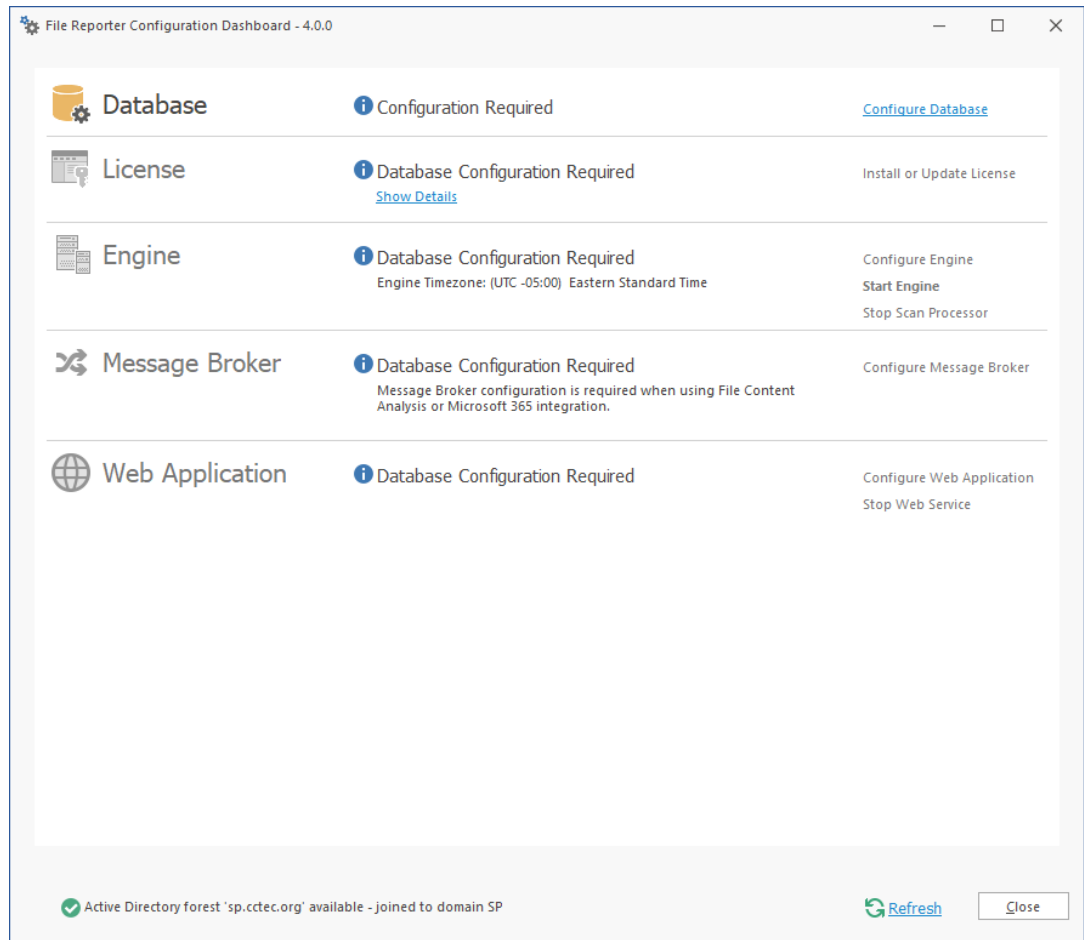
- 4 (Conditional) Update the OLE DB driver.
 - 4a In the dialog box, click **Yes** to begin the process of updating the driver.

This launches the installation wizard.
 - 4b Click **Next**.
 - 4c Accept the license terms and click **Next**.
 - 4d Accept the default feature selections by clicking **Next**.
 - 4e Click **Install**.

- 4f (Conditional) If you are notified that you have applications running that are preventing the driver from being updated, close the listed applications and then click **Retry**.



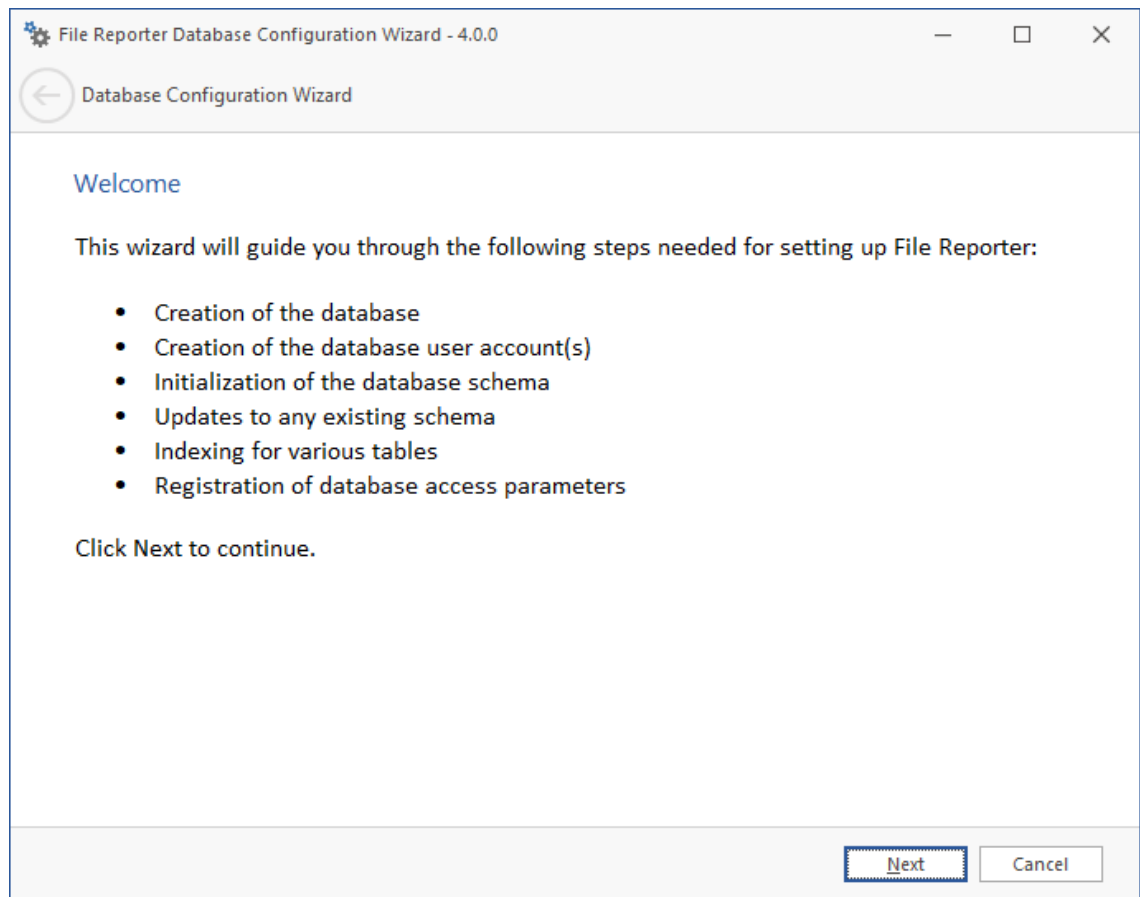
- 5 Click **Next**.
- 6 Accept the installation path or indicate a new path by using the **Browse** button. and click **Next**.
- 7 Click **Install**.
- 8 Click **Finish**.
- 9 Do one of the following:
 - ♦ If prompted to restart the server, do so to activate the updated OLE DB driver. Then from the **Start** menu, select **File Reporter > File Reporter Configuration Dashboard**.
 - ♦ Click **Run Config Utility**.The File Reporter Configuration Dashboard appears.



NOTE: Each step in the Configuration Utility should be run in sequential order from top to bottom. If you chose not to install RabbitMQ, you can skip the Message Broker section.

7.4 Configuring the Database

- 1 Click [Configure Database](#).



The page indicates what database configuration tasks are to be completed in this wizard.

- 2 From the wizard page, read the overview of what will be configured and click **Next**.

This page lets you establish the settings needed for the Engine and IIS to communicate with the database.

Database Properties: Displays information on the database name and version.

Type: Depending on the database you are using, select either **PostgreSQL** or **SQL Server**.

Communication: Specifies address, port number, and name of the database.

Database Host Address: Specify the host address of the server where the database is installed.

Port: Enter the port that the database listens on. The default PostgreSQL database port setting is 5432. The default SQL Server port setting is 1433.

Initial Database: The default name of the File Reporter database.

Database Service Accounts: Use this region to set authentication information for the Database Service User and Database Report User.

IMPORTANT: Retain the user and password information as this will be needed again during the component configuration processes.

Database Service User: This field specifies the database account name that is used by File Reporter to manage data in the database. This account has both read and write access to the database.

Set Password: Click **Set Password** to establish the password for the Database Service User.

Database Report User: This field specifies the database account name that File Reporter uses to read data in the database while reporting.

Set Password: Click **Set Password** to establish the password for the Database Report User.

Database Report Role: This field specifies the account name of the role used to manage access for Report Users.

Database Admin Credentials: Use this region to establish the database administrator name and credentials.

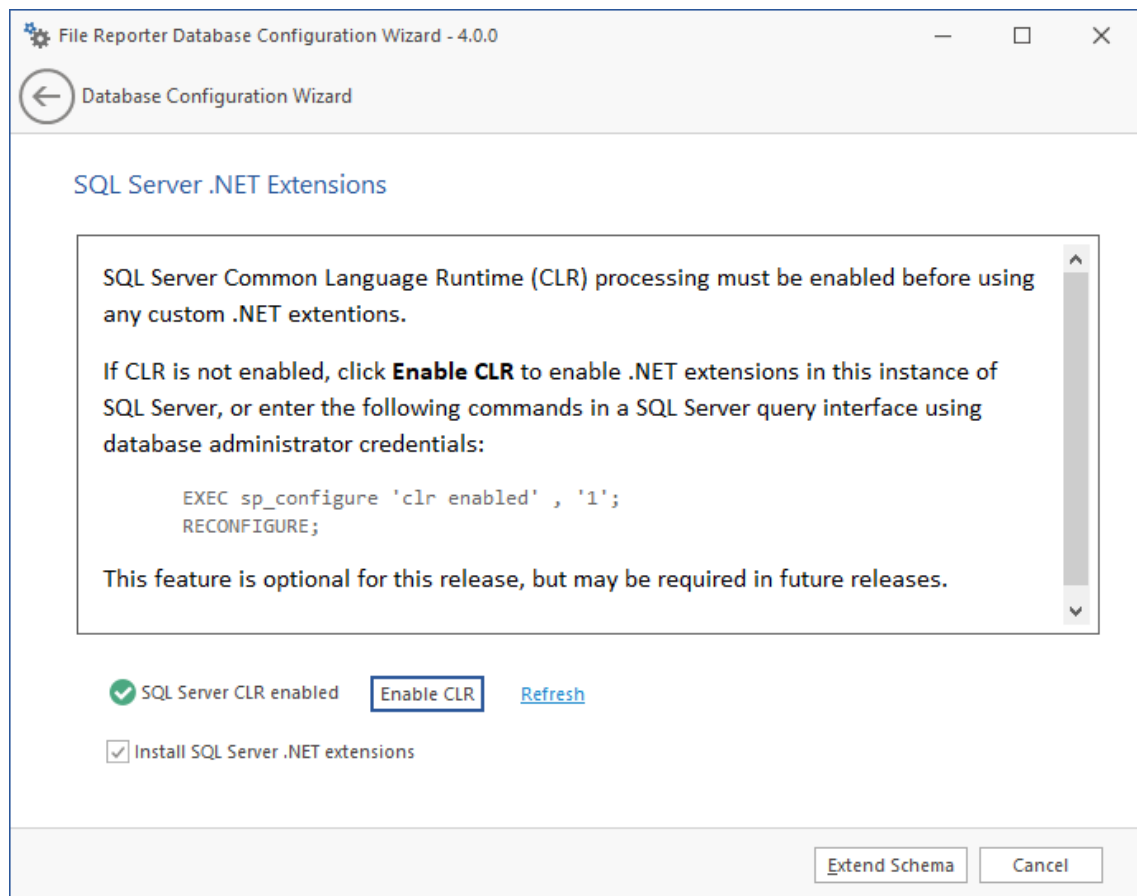
Database Administrator: If you are using a PostgreSQL database, specify the superuser name. If you are using an SQL Server, specify the administrator name.

Password: If you are using a PostgreSQL database, specify the superuser password. If you are using an SQL Server, specify the database administrator password.

Test Credentials: Clicking this lets you quickly confirm that the entries in the **Database Service Accounts** region are accurate before advancing in the wizard.

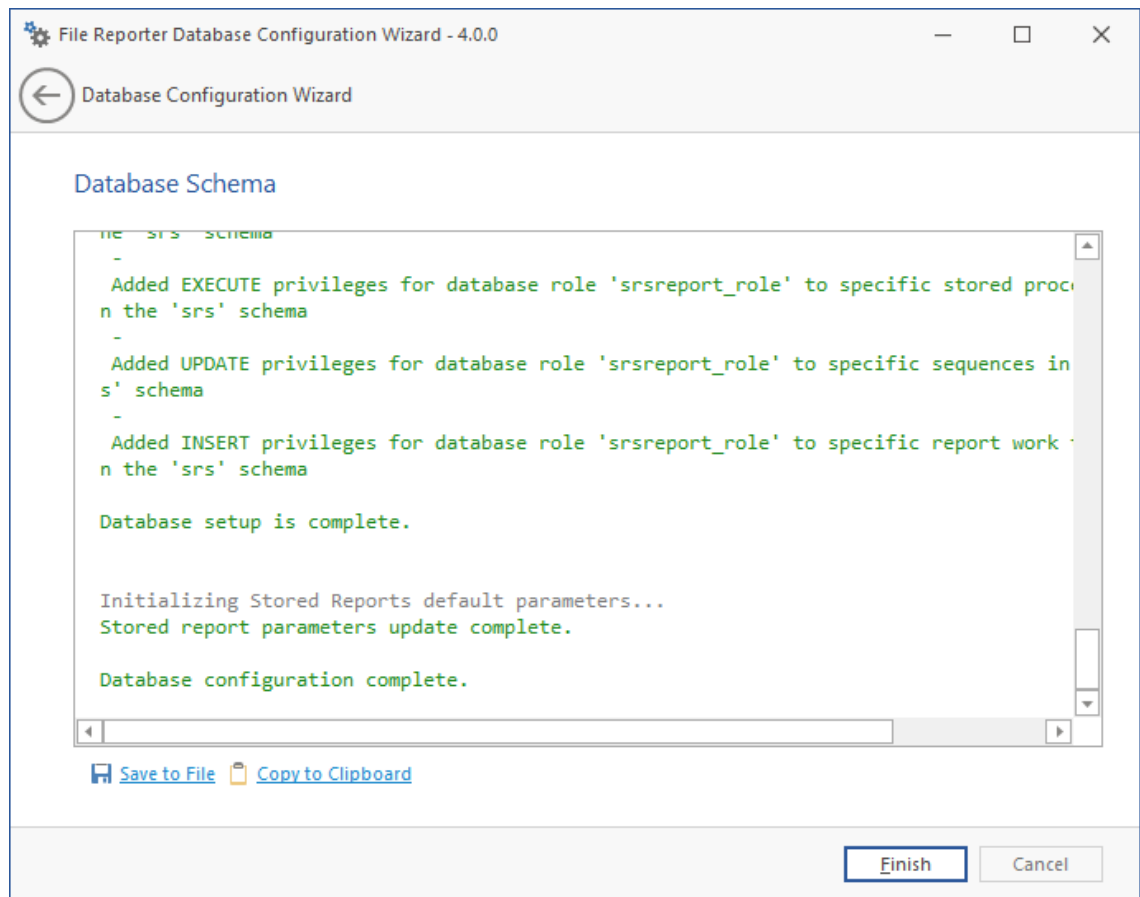
- 3 Complete the fields and click **Next**.

If you are using a Microsoft SQL Server database, the following page appears, indicating that File Reporter will add custom extensions for SQL Server that help File Reporter with advanced reporting queries.

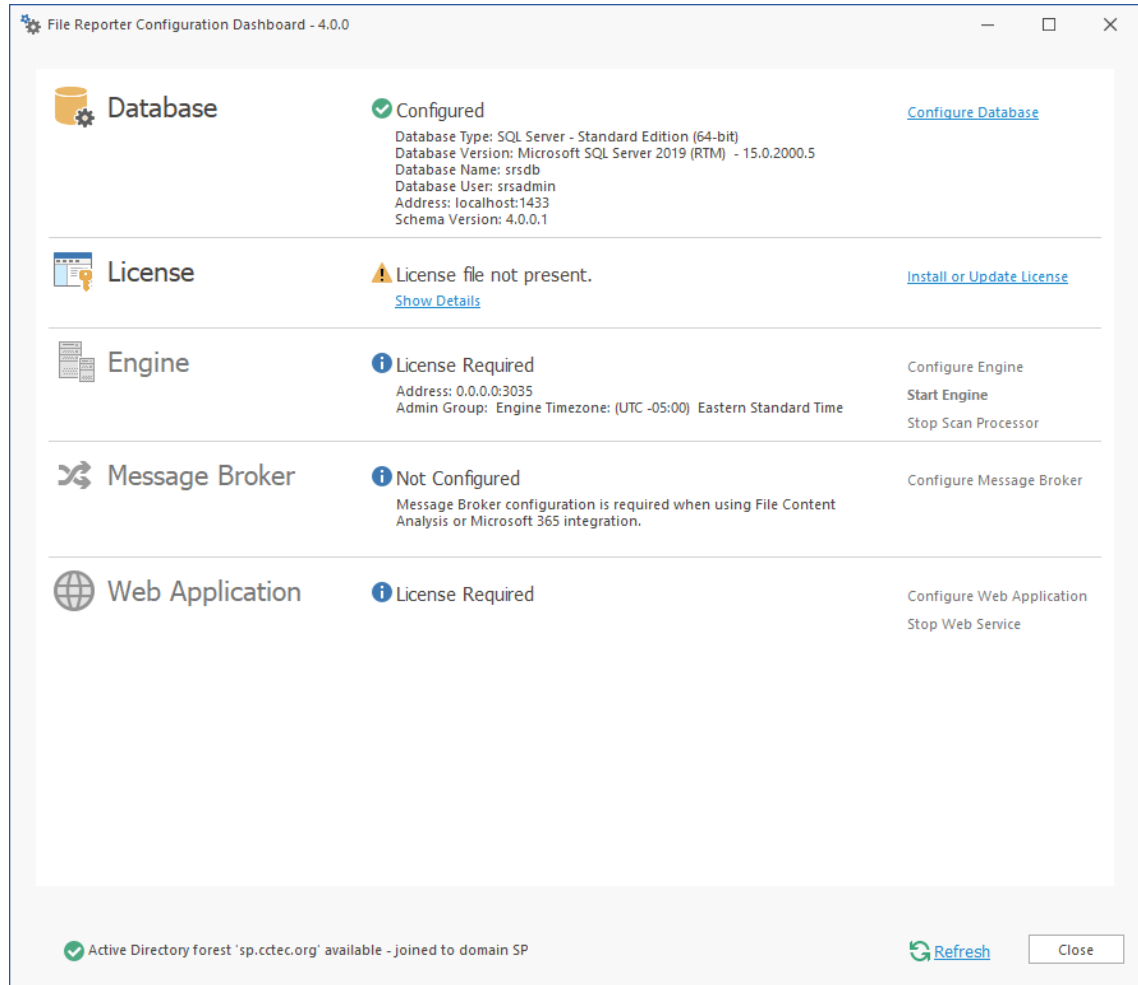


- 4 (Conditional) Click **Enable CLR**.

- 5 (Conditional) Click **Extend Schema**.

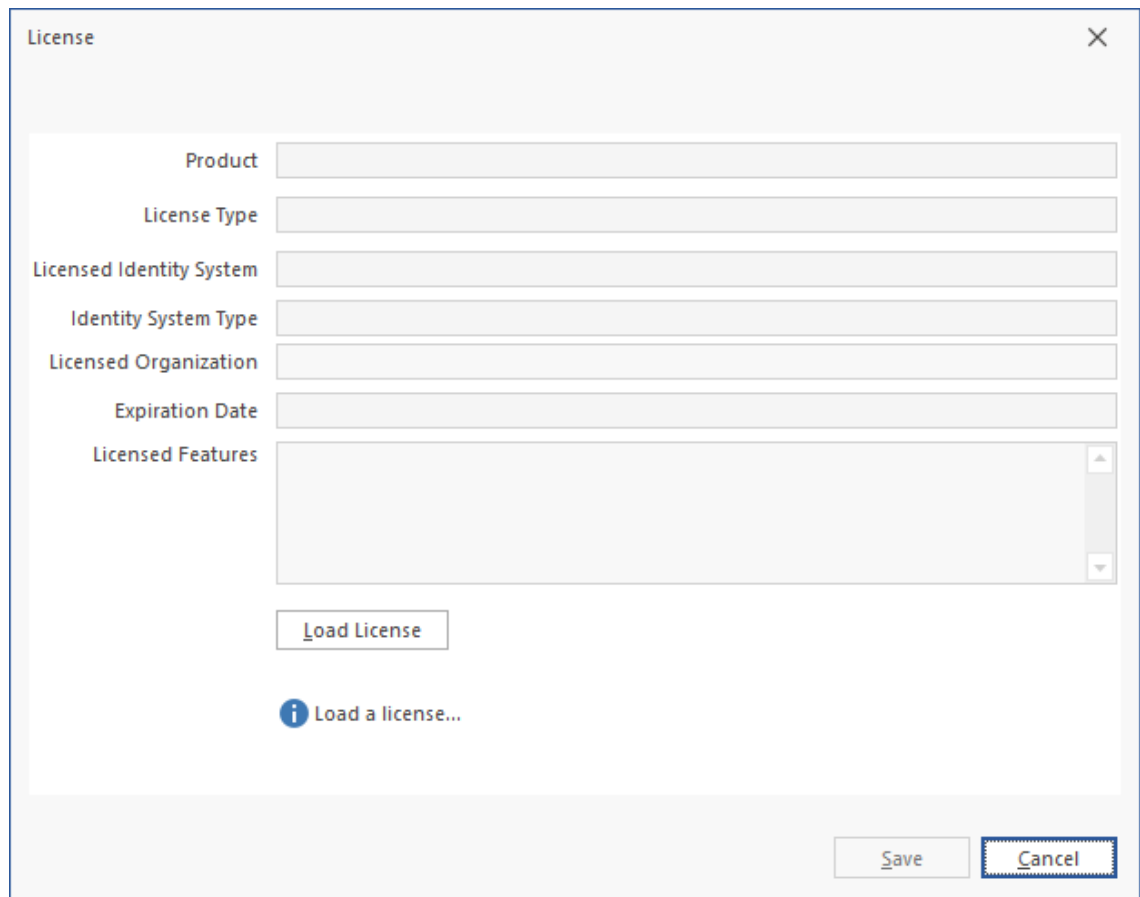


6 Review the configuration log and click **Finish**.



7.5 Installing the License

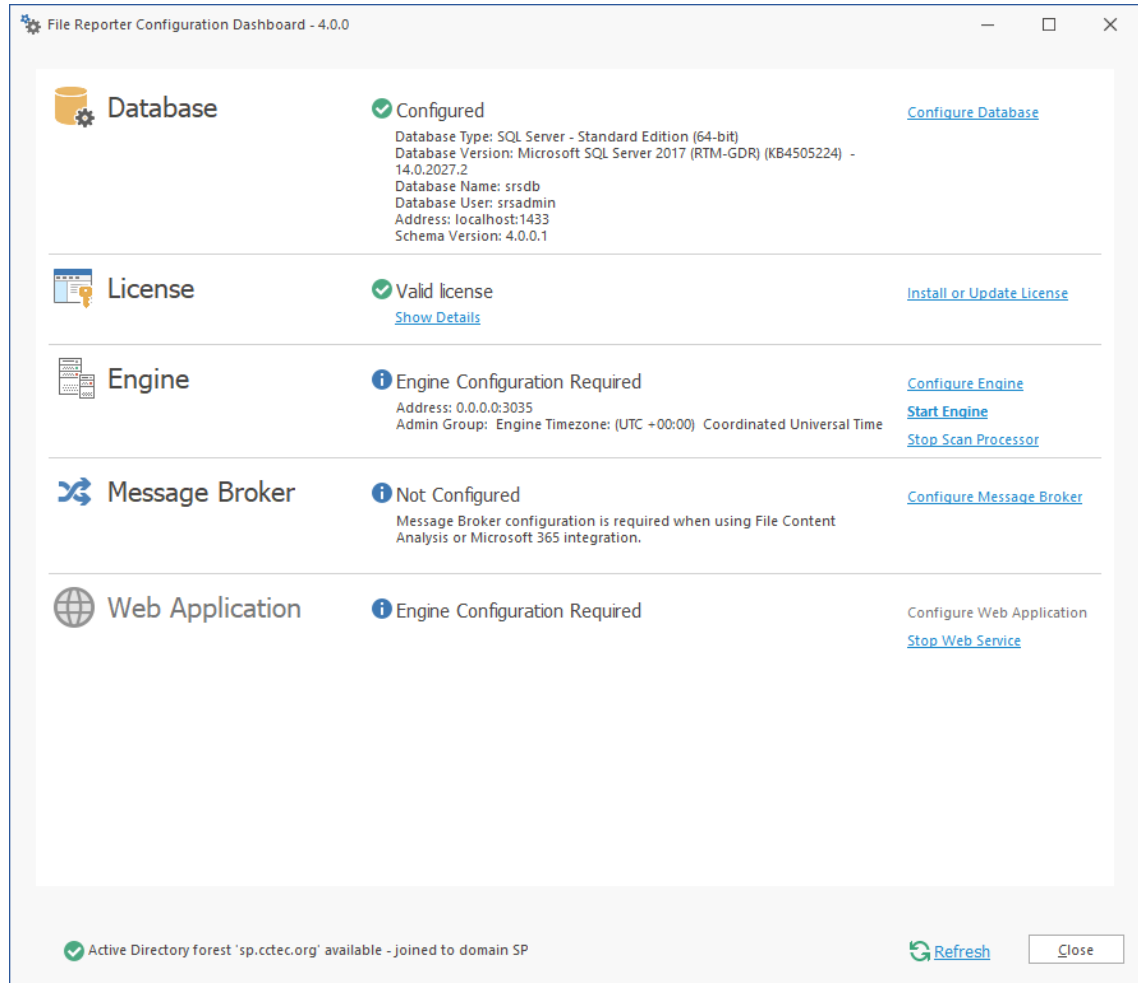
1 Click **Install or Update License**.



The image shows a 'License' dialog box with a close button (X) in the top right corner. The dialog contains several input fields: 'Product', 'License Type', 'Licensed Identity System', 'Identity System Type', 'Licensed Organization', and 'Expiration Date'. Below these is a larger 'Licensed Features' field with a scroll bar. At the bottom left of the dialog is a 'Load License' button. Below the button is an information icon (i) followed by the text 'Load a license...'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

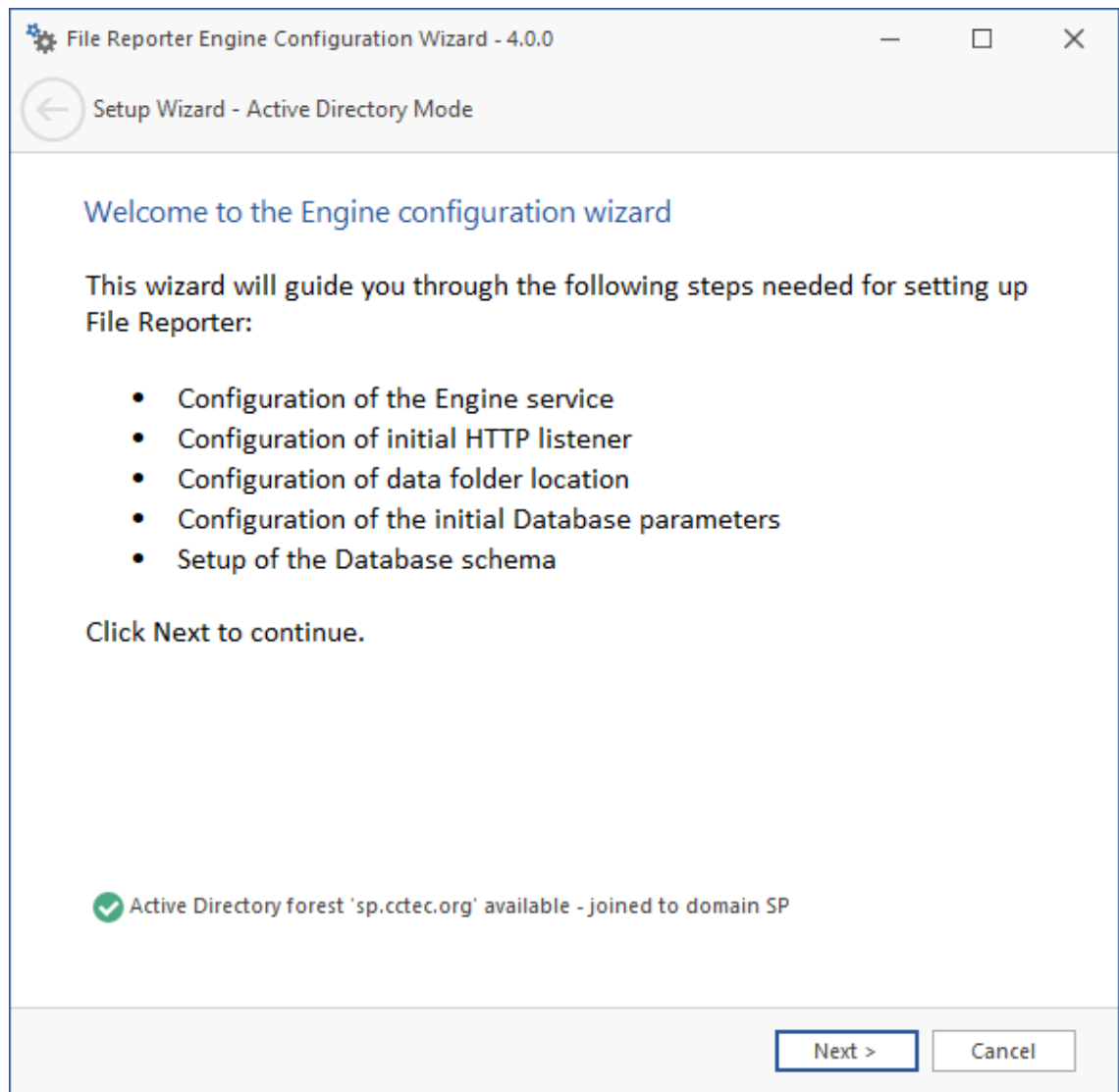
- 2 Click **Load License**, then browse to and select the license file.
- 3 When the confirmation prompt appears, click **Yes**.

4 Click Close.



7.6 Configuring the Engine

1 Click Configure Engine.



2 From the wizard page, read the overview of what will be configured and click **Next**.

File Reporter Engine Configuration Wizard - 4.0.0

Setup Wizard - Active Directory Mode

Basic Options

HTTP Listener

Host Address: 0.0.0.0

SSL Port: 3035

SSL Certificate

Subject Name: srs-m1

Expiration Days: 3,652 Expiration Date: 11/20/2030 4:07:35 PM

Key Length: 4096

Details Generate

Data

Data Folder: C:\ProgramData\Micro Focus\SRS\Engine\data

Move data from C:\ProgramData\Micro Focus\SRS\Engine\data

Next > Cancel

This page lets you confirm or change basic Engine configuration settings.

HTTP Listener: Communication parameters for the Engine.

Host Address: Unless you want the Engine to only listen on a certain IP address, leave this setting as it is.

SSL Port: Unless there is a port conflict, leave the setting at 3035.

SSL Certificate: Details for the SSL certificate that will be generated.

Subject Name: The name of the certificate that will be generated. The server name is listed by default.

Expiration Days: The life span of the security certificate, which is set at 10 years by default.

Key Length: The SSL certificate encryption setting, which is set at 2048 by default.

Details: Click the button to view the certificate data.

Generate: If you modify any of the settings in the **SSL Certificate** region, click this button to generate a new certificate.

Data Folder: The default location of the Data folder. The Data folder is used for a variety of tasks, including storing Agent configuration data, serving as a temporary repository for scans, and mail spooling.

Move data from (Enabled only during an upgrade): Having this check box selected indicates that content from the Engine's data folder for the previous version of File Reporter, will be moved to the path specified in the **Data Folder** field and the original path will be removed. If this check box is not selected, it will use whatever path is specified in the **Data Folder** field, including the original path.

- 3 Edit any needed parameters settings and click **Next**.

File Reporter Engine Configuration Wizard - 4.0.0

Setup Wizard - Active Directory Mode

Active Directory Service Accounts

Proxy Account
Enter the name of a service account used by the Engine and Agents for all operations.

Proxy Rights Group
Enter the name of a service group used for rights assignments for access to server, share, and file resources. The Proxy Account will automatically be assigned as the initial member of this group.

Communications Group
Enter the name of a service group used for communications control of various

Proxy Account: SP\SrsProxy

Proxy Rights Group: SP\SrsProxyRights

Communications Group: SP\SrsCommunications

Manage Accounts in AD

Create new accounts if required

Container: CN=Users,DC=sp,DC=cctec,DC=org [Browse](#)

Next > Cancel

This page lets you establish a name for the proxy account, proxy rights group, and the communications group.

File Reporter uses a proxy account so that Agents can access all of the servers for scanning. A proxy rights group makes it easier to manage the rights of the proxy account. The Scan Processor uses the communications group to secure who can access its service.

The Configuration Wizard establishes default account and group names, which you can modify.

If you are upgrading from a previous version of File Reporter, the **Proxy Account** and **Proxy Rights Group** fields will specify the existing proxy account and proxy rights group.

Clicking **Browse** allows you to place these object in a specified container other than CN=Users.

NOTE: If you choose, these user and group objects can be moved in Active Directory after installation without affecting the product.

4 Click **Next**.

The screenshot shows a configuration wizard window titled "File Reporter Engine Configuration Wizard - 4.0.0" with a sub-header "Setup Wizard - Active Directory Mode". The main content area is titled "User Groups" and contains two sections:

- Admins Group**: The Admins Group is used to restrict access to logon and manage File Reporter. Note that the current logged on user **SP\Administrator** will be added to this group. The group should be entered using Domain\SAMAccount name format where the domain is the current system's domain.
- Report Users Group**: The Report Users Group is used to provide restricted access to stored reports. The group should be entered using Domain\SAMAccount name format where the domain is the current system's domain.

Below the instructions are three text input fields:

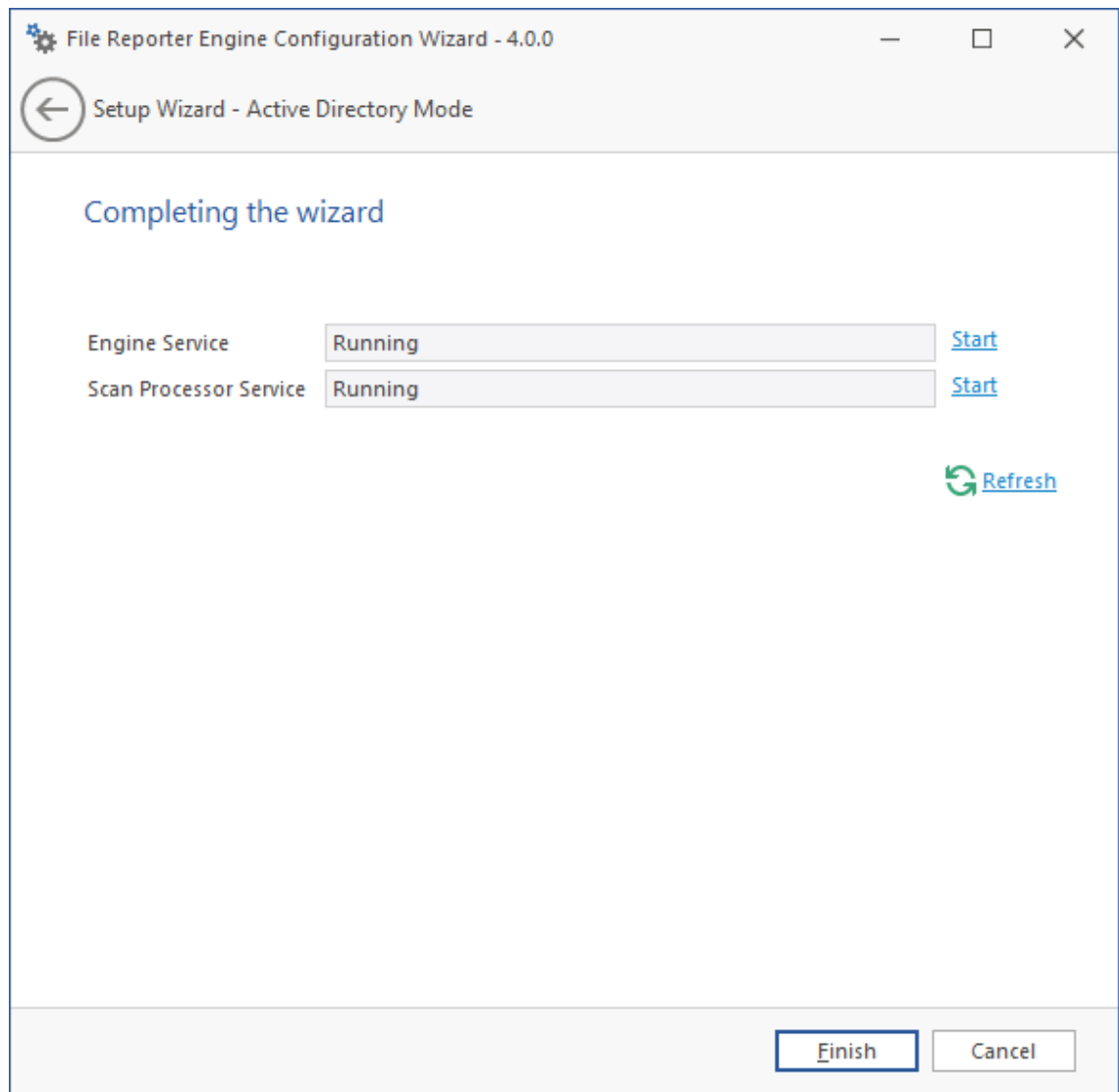
- Admins Group: SP\SrsAdmins
- Report Users Group: SP\SrsReportUsers
- New Accounts Container: CN=Users,DC=sp,DC=cctec,DC=org

At the bottom right of the window are two buttons: "Next >" and "Cancel".

5 Specify the name for the Admins Group and Report Users Group, or use the default names.

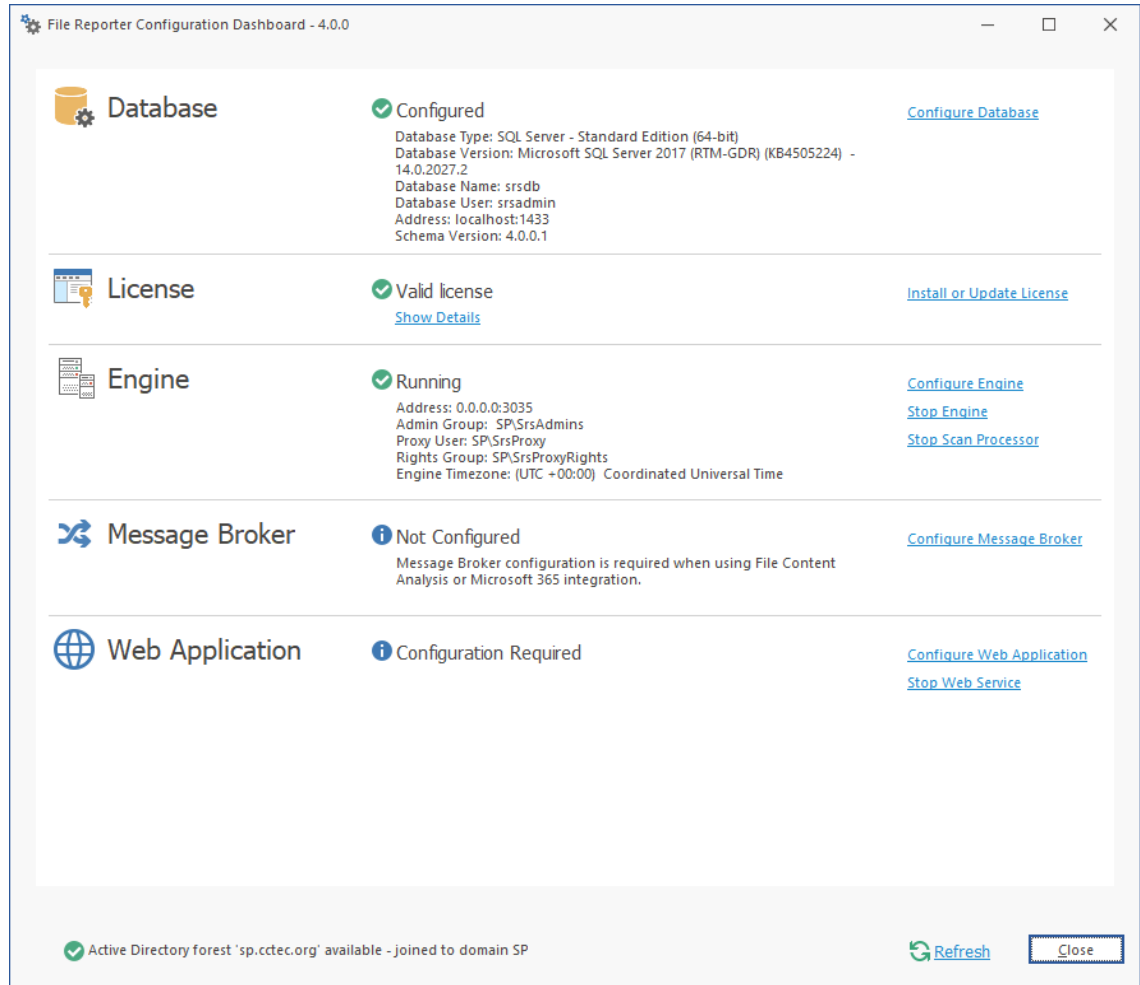
The Report Users Group is a group that File Reporter creates in Active Directory. Members of this group have access to all stored reports.

6 Click **Next** to create the two groups.



7 Click Finish.

The Engine and Scan Processor are now installed, configured, and running.



7.7 Configuring the Message Broker

- 1 Click [Configure Message Broker](#).

Message Broker Config

Message Broker Config Wizard

Message Broker Connection

Basic Configuration

Broker Type: RabbitMQ

Host Address:

Port: 5671 Use TLS

Service Account: srsbroker

[Set Password](#)

Management Interface

Management API Port: 15671 Use TLS

Admin Account:

Password:

[Test](#) Status Unknown

[Next >](#) [Cancel](#)

2 Specify settings in the following fields:

Basic Configuration: This region is where you specify basic configuration settings for the message broker.

Broker Type: This field indicates the RabbitMQ message broker that you installed previously.

Host Address: Specify the IP address or DNS name of the server hosting RabbitMQ.

Port: Unless there is a port conflict, leave the setting at 5671.

Use TLS: The Transport Layer Security protocol is established by default.

Service Account: By default, this field is with the `srsbroker` account name.

Set Password: Click this to establish a password for the service account.

Management Interface: This region is where you specify the admin account and password for the RabbitMQ installation that you performed previously.

Management API Port: Unless there is a port conflict, leave the setting at 5671.

Use TLS: The Transport Layer Security protocol is established by default.

Admin Account: Specify the admin account name that you established when you installed RabbitMQ.

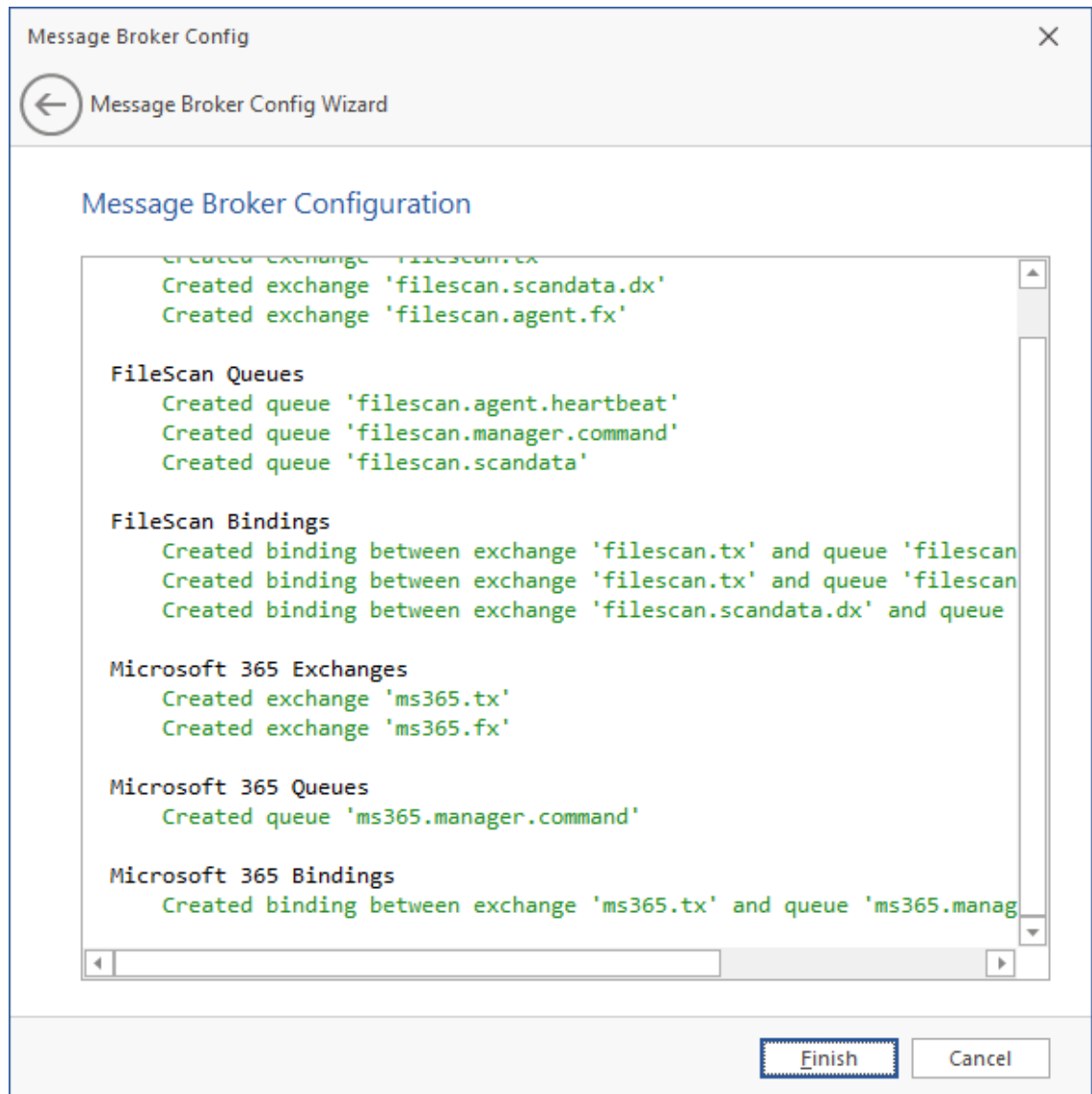
Unless you changed the default name, the admin account name is `sradmin`.

Password: Specify the admin account password that you established when you installed RabbitMQ.

Unless you changed the default password, the admin account password is `admin`.

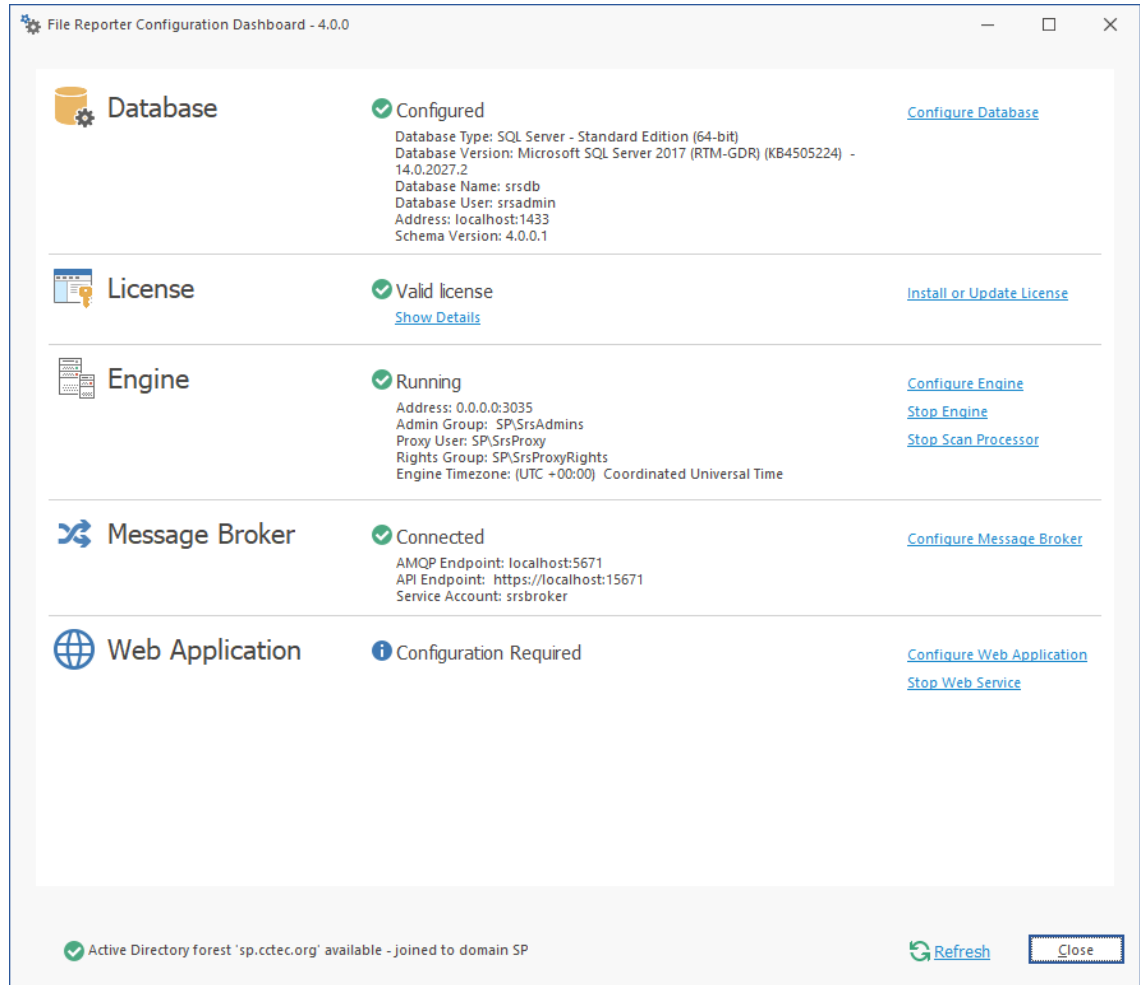
Test: Click this to verify the message broker communication is functioning properly.

3 Click **Next**.



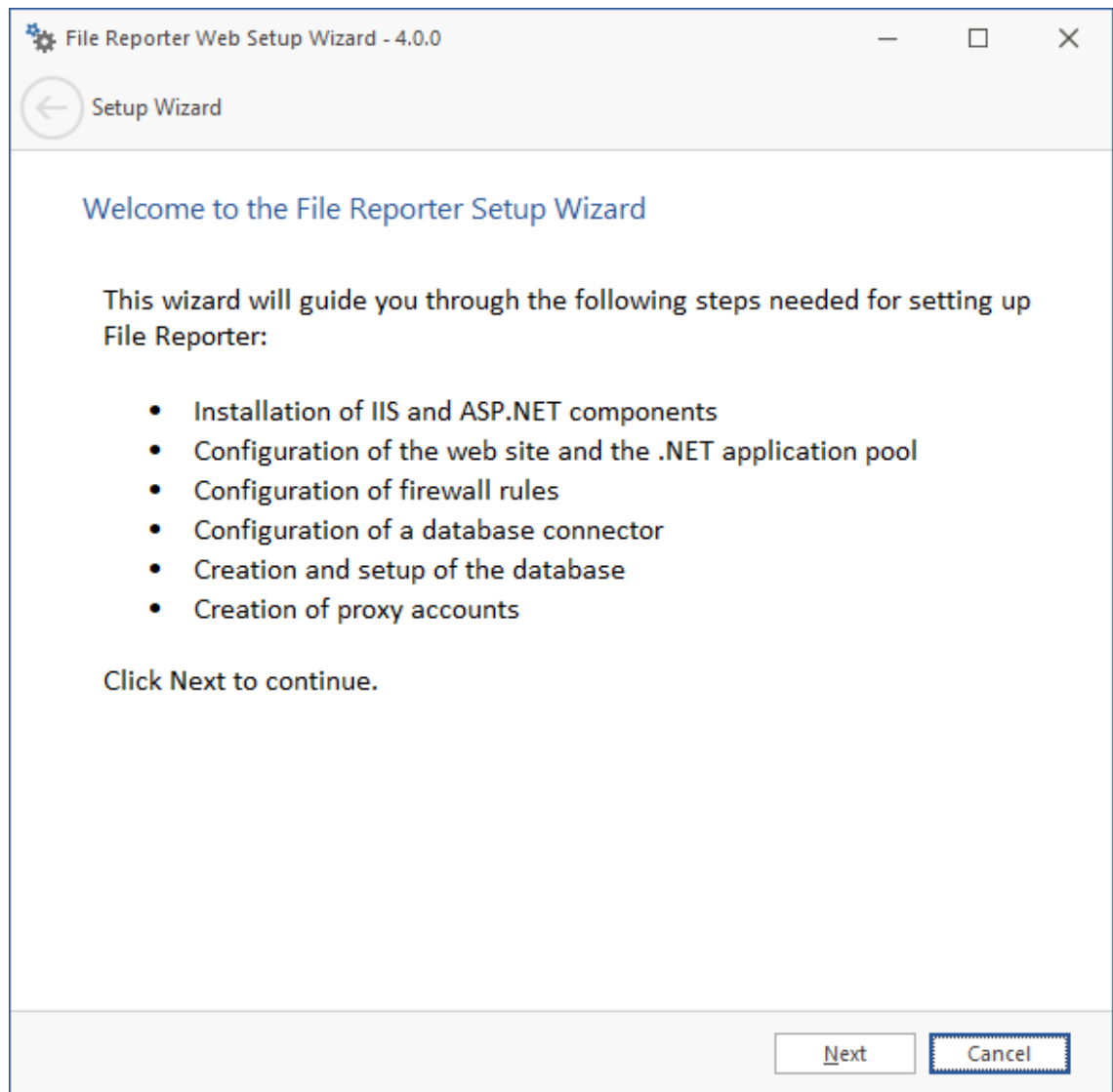
4 Click **Finish**.

The message broker is now configured and connected.

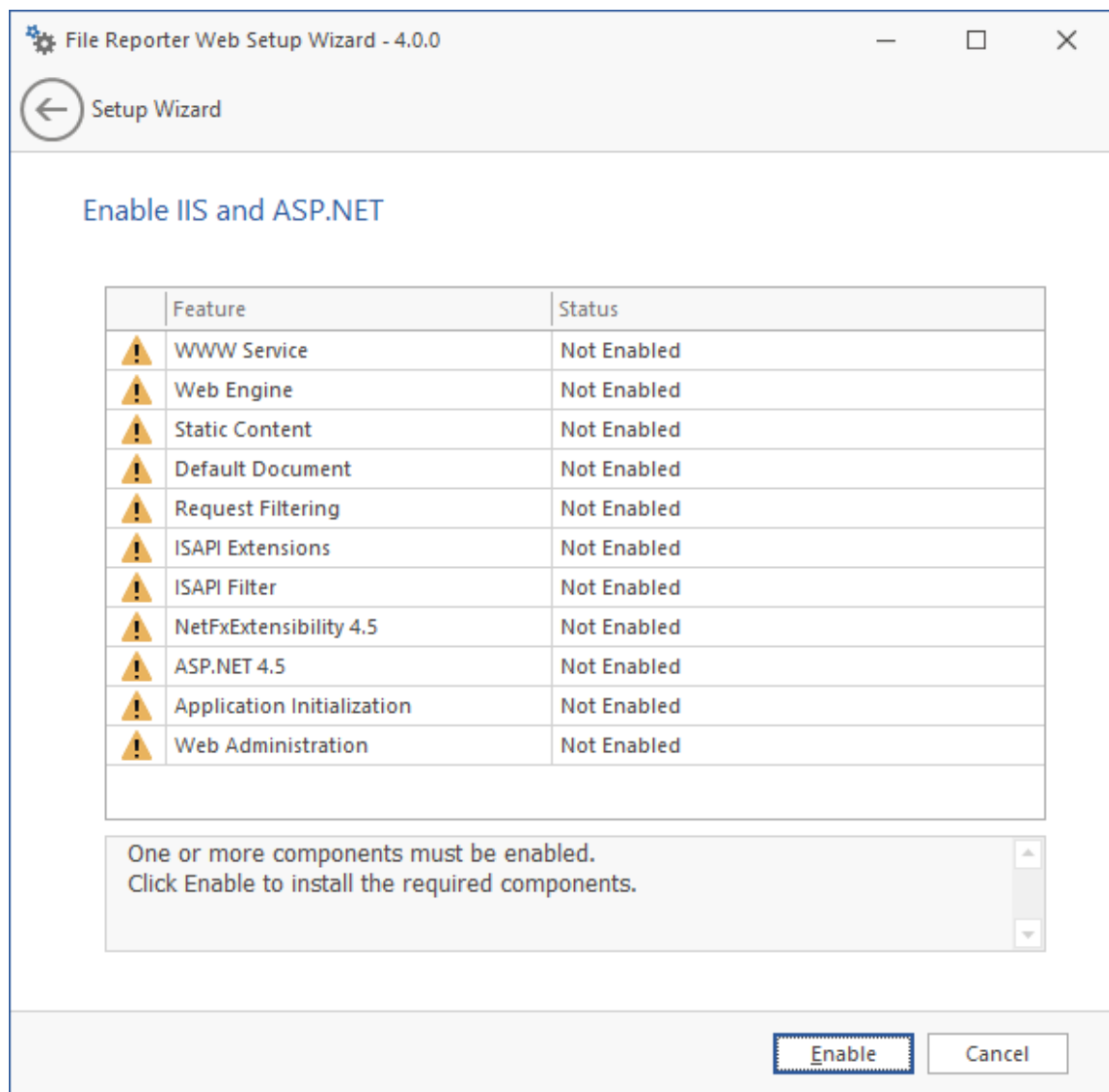


7.8 Configuring the Web Application

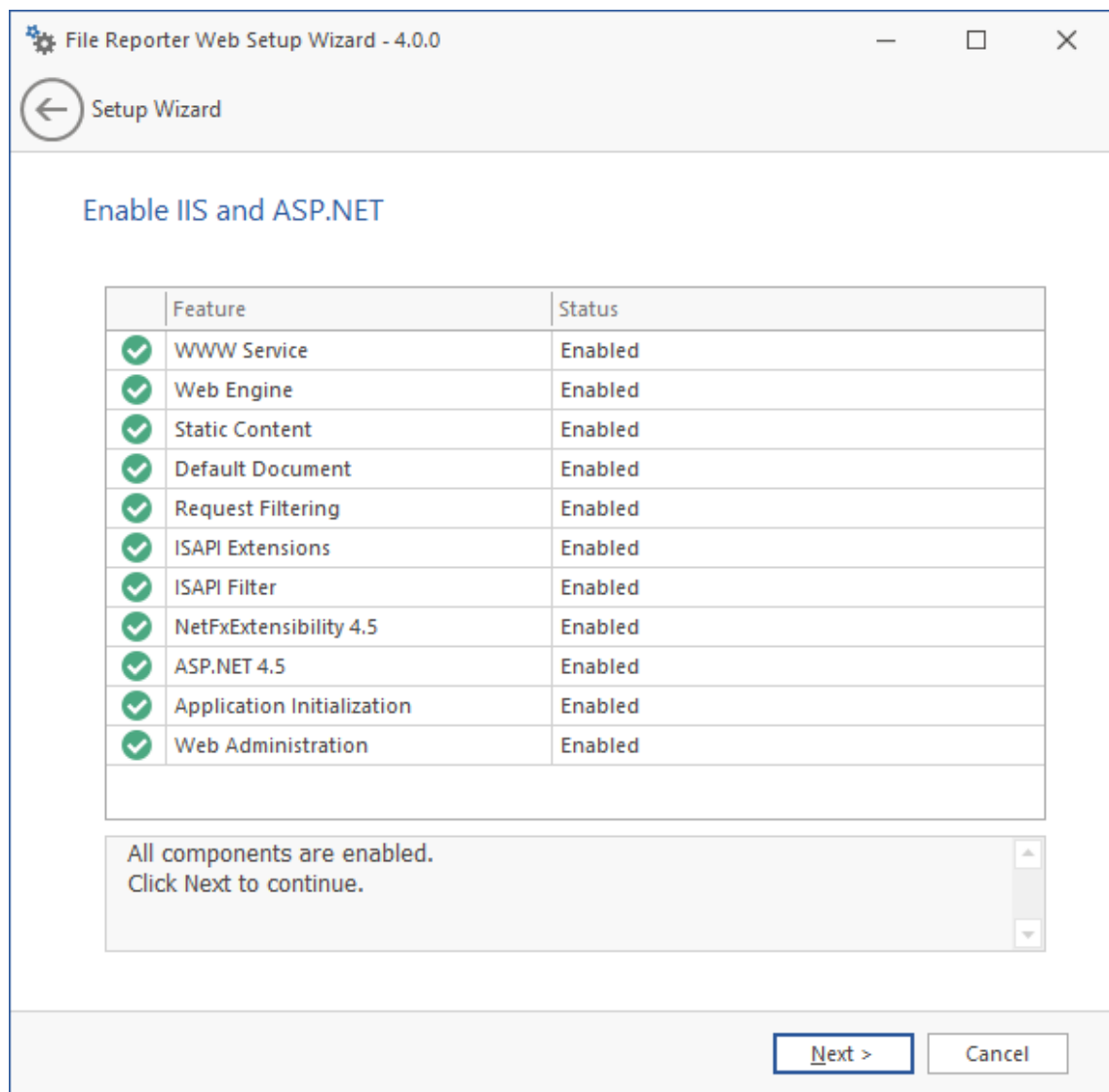
- 1 Click [Configure Web Application](#).



- 2 From the wizard page, read the overview of what will be configured and click **Next**.



3 Click Enable.



4 Click Next.

The screenshot shows the 'File Reporter Web Setup Wizard - 4.0.0' window. The 'Setup Wizard' title bar is at the top left. The main content area is titled 'Web Site Parameters'. Under the 'Web Site' section, there are five fields: 'Web Site' (text box with 'SrsSite' and a green checkmark), 'Physical Path' (text box with 'C:\inetpub\srs_root\'), 'IP Address' (dropdown menu with '0.0.0.0 (All Addresses)'), 'SSL Port' (spin box with '443'), and 'Host Name' (text box with 'filereporter.sp.cctec.org' and a warning icon). Under the 'Application Pool' section, there is a 'Name' field (text box with 'SrsAppPool' and a green checkmark). Under the 'Service Account' section, there are three fields: 'Service Account' (text box with 'SP\SrsAppPoolSvc'), 'Password' (password field with a 'Show' link), and 'Password Confirm' (password field). Below these are two checkboxes: 'Manage Accounts in AD' (checked) and 'Create new accounts if required' (checked). At the bottom of this section is a 'New Account Container' field (text box with 'CN=Users,DC=sp,DC=cctec,DC=org' and a 'Browse' link). At the bottom right of the window are 'Next' and 'Cancel' buttons.

This page lets you review or edit settings applicable to the File Reporter Web application. Unless there is a need to change a setting, we recommend that you leave the settings as they are currently established.

Web Site: Settings for the Microsoft IIS Web site.

Web Site: The default name for the File Reporter Web site. If the default name does not conform to your organization’s naming standards, you can edit it.

Physical Path: This path was specified in [Step 6 on page 45](#) and is the location where files on the Web site are served up. You cannot edit this path.

IP Address: By default, this field indicates that Web requests will be responded to from any IP address available on the server. If the server has multiple IP addresses, you can specify which one you want to use.

SSL Port: The default port is 443. If there is a conflict, you can select another port.

Host Name: The host name as defined in DNS that you specified in [Section 7.2, “Prerequisites,” on page 43](#).

If a warning sign appears next to the **Host Name** entry, the host name is not fully resolved. Verify that there is a DNS entry for the File Reporter Web application and that the resolved IP address or addresses are located on the host machine.

Application Pool: Settings pertaining to the File Reporter application pool in Microsoft IIS.

Name: The default name for the application pool. If the default name does not conform to your organization's naming standards, you can edit it.

Service Account: This field specifies the service account name used by the application pool.

Password: The password is automatically generated.

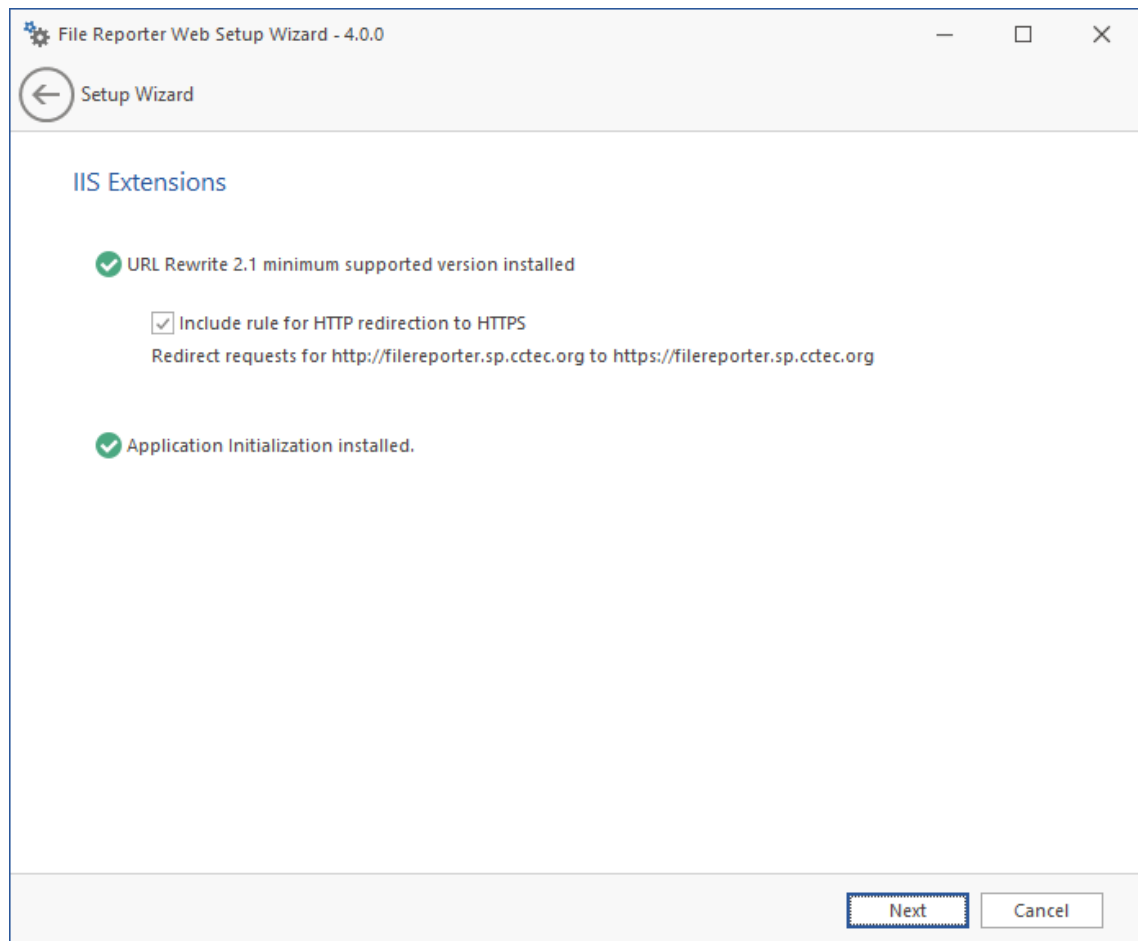
Confirm Password: The automatically generated password is repeated.

Provision in Active Directory: When selected, this provisions the application pool in Active Directory. If this option is not selected, the application pool is provisioned to the local host.

New Account Container: This field specifies the default location of the application pool in Active Directory. If you want to modify the location, click **Browse** and specify a new location.

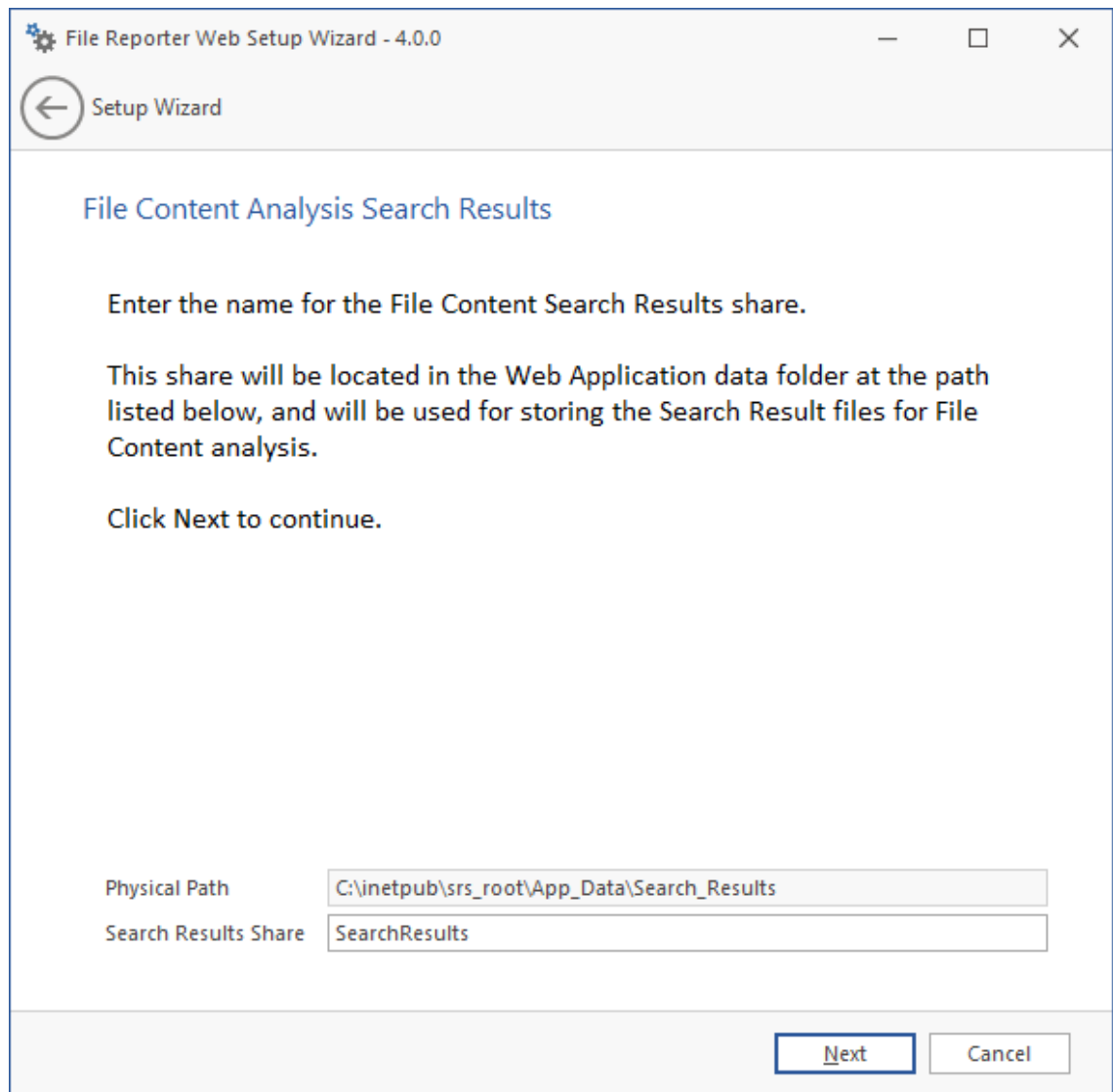
5 (Conditional) If the components are not enabled, click **Enable**.

6 Edit the fields as needed and click **Next**.

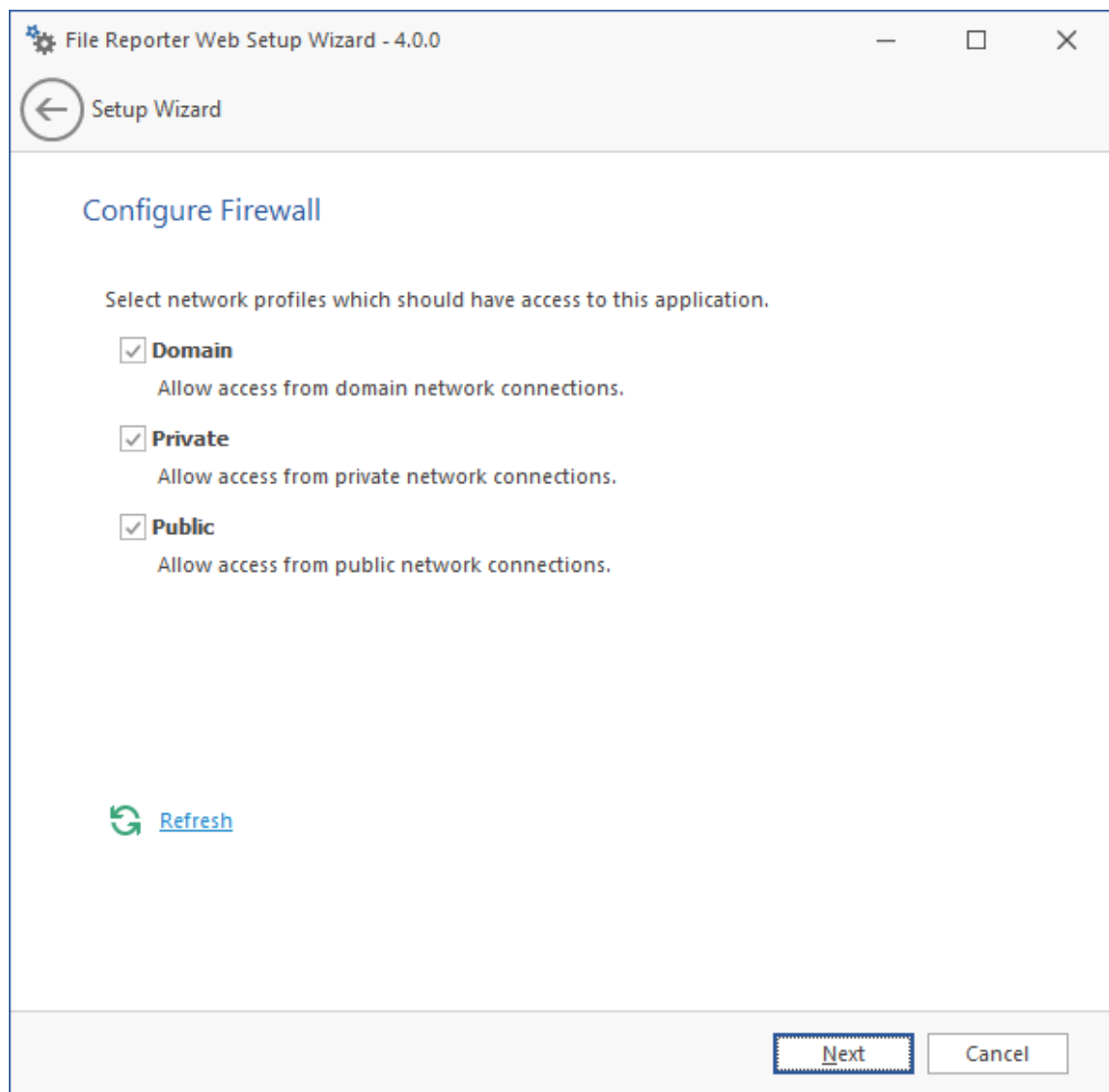


This page lets you install Microsoft IIS URL Rewrite Module 2.0, which will redirect the File Reporter login page from an entered HTTP protocol, to HTTPS. For example, if you enter `http://filereporter.sp.cctec.org`, you would be redirected to the secure login page at `https://filereporter.sp.cctec.org`.

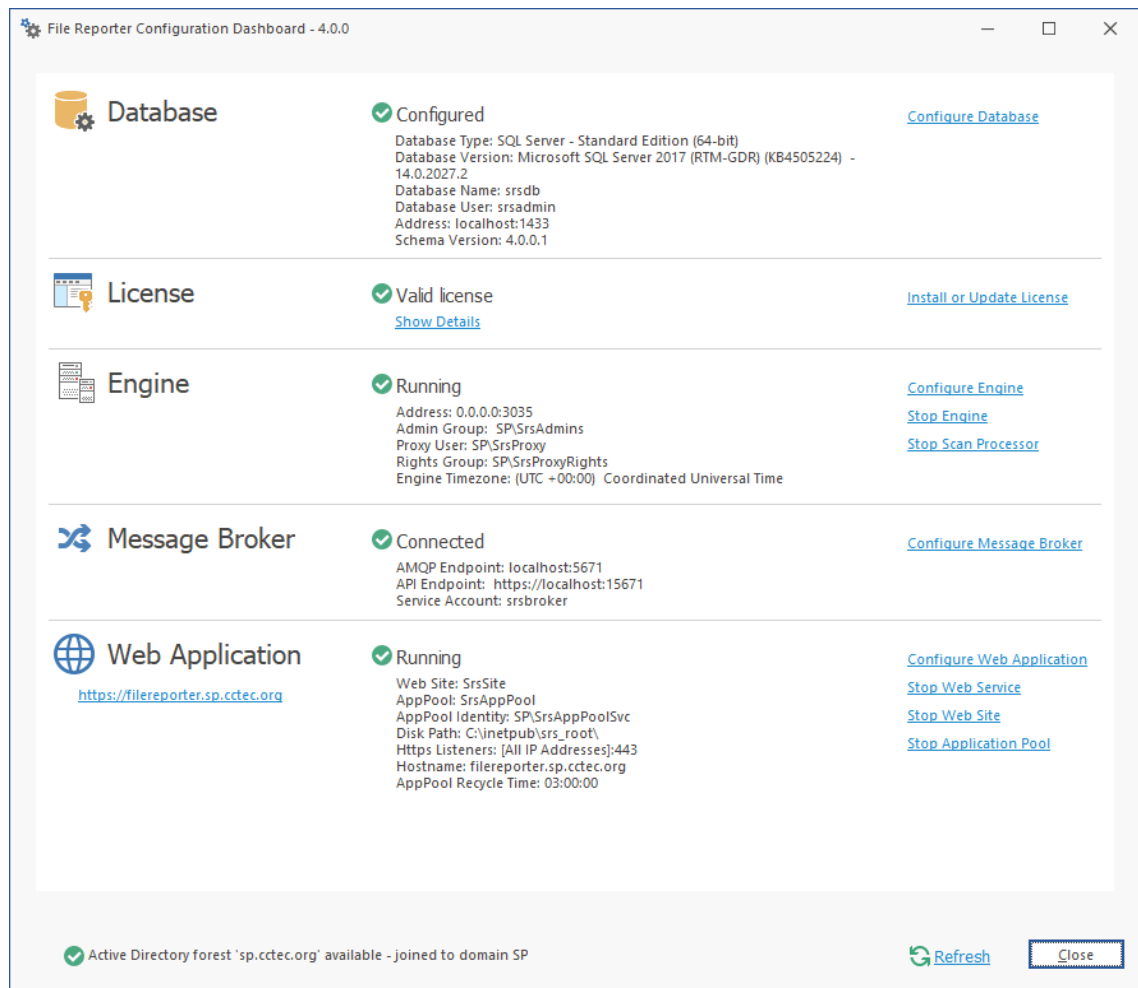
7 Unless your organization has a policy against redirects, leave the check box selected and click **Next**.



8 Click Next.



- 9 Set the network profiles according to your organization's security policies and click **Next**.
- 10 When you are notified that the initial setup for the Web Application is complete, click **Finish**. The database, Engine, and Web Application are now configured.



11 Click the hyperlink to launch the Web-based administrative interface.

The hyperlink is located below the **Web Application** heading.

12 (Conditional) If you are prompted for a security exception, accept it and follow the procedures for establishing `https://filereporter.domain` as a trusted Web site.

8

Installing and Configuring Windows AgentFS

- ♦ [Section 8.1, “Minimum Requirements,” on page 71](#)
- ♦ [Section 8.2, “Active Directory Requirements,” on page 71](#)
- ♦ [Section 8.3, “Installing and Configuring AgentFS,” on page 71](#)

Procedures in this section include those needed for installing and configuring AgentFS on a Windows Server.

8.1 Minimum Requirements

- ♦ Any of the following dual core 64-bit processor servers:
 - ♦ Windows Server 2019
 - ♦ Windows Server 2016
 - ♦ Windows Server 2012 R2

- ♦ The server must be joined to Active Directory
- ♦ .NET 4.8 (this will be installed if not already present)
- ♦ Minimum of 100 MB RAM per concurrent scan

For example, if you planned on your AgentFS conducting scans on 4 volumes or shares concurrently, you would need a minimum of 400 MB of RAM.

NOTE: Performance depends not only on the number of concurrent scans, but also the size of the directory structure for each share. Adding more RAM than the minimum requirement can obviously improve performance.

- ♦ Minimum of 10 GB free disk space for installation and scans

This size might need to be adjusted based on number of concurrent scans this agent performs, as well as the size of the scans themselves.

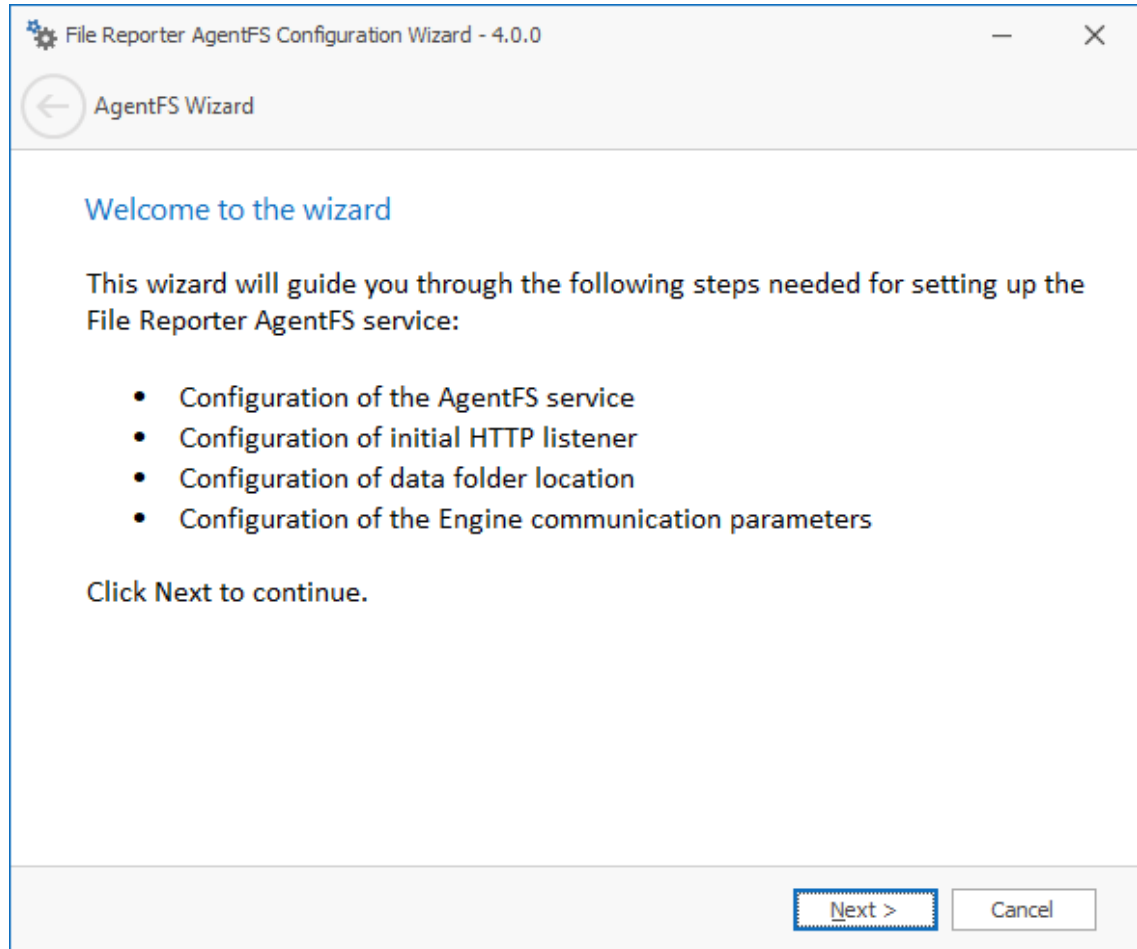
8.2 Active Directory Requirements

File Reporter supports a minimum forest functional level of Windows 2003.

8.3 Installing and Configuring AgentFS

- 1 At the root of the `FileReporter_4.0.iso` image, double-click `FileReporter-AgentFS-4.0.x64-xx.exe`.
- 2 Agree to the license terms and conditions and click **Install**.

- 3 When you are notified that the setup was successful, click **Run Setup Utility**.



- 4 From the wizard page, read the overview of what will be installed and configured and click **Next**.

File Reporter AgentFS Configuration Wizard - 4.0.0

AgentFS Wizard

General Options

Service Listener

Host Address: 0.0.0.0

Port: 3038

TLS Certificate: CN=srs-m1.sp.cctec.org [Details] [Generate]

Data

Data Folder: C:\ProgramData\Micro Focus\SRS\AgentFS\data [Browse]

Move data from C:\ProgramData\Micro Focus\SRS\AgentFS\data

[Next >] [Cancel]

This page lets you confirm or change basic AgentFS configuration settings.

Service Listener: Communication parameters for AgentFS.

Host Address: Unless you want AgentFS to only listen on a certain IP address, leave this setting as it is.

Port: Unless there is a port conflict, leave the setting at 3038.

TLS Certificate: The name of the TLS certificate that will be generated. The server name is listed by default.

Details: Click the button to view the certificate data.

Generate: If you modify any of the settings for the TLS certificate, click this button to generate a new certificate.

Data: Parameters pertaining to the data folder.

Data Folder: The default location of the data folder. The data folder is used for a variety of tasks, including the storage of temporary scan data.

Browse: Click to specify a new path for the data folder.

Move data from: (Enabled only during an upgrade): Having this check box selected indicates that content from the Agent's data folder for the previous version of File Reporter, will be moved to the path specified in the Data Folder field and the original path will be removed. If this check box is not selected, it will use whatever path is specified in the Data Folder field, including the original path.

- 5 Edit any needed parameters settings and click **Next**.

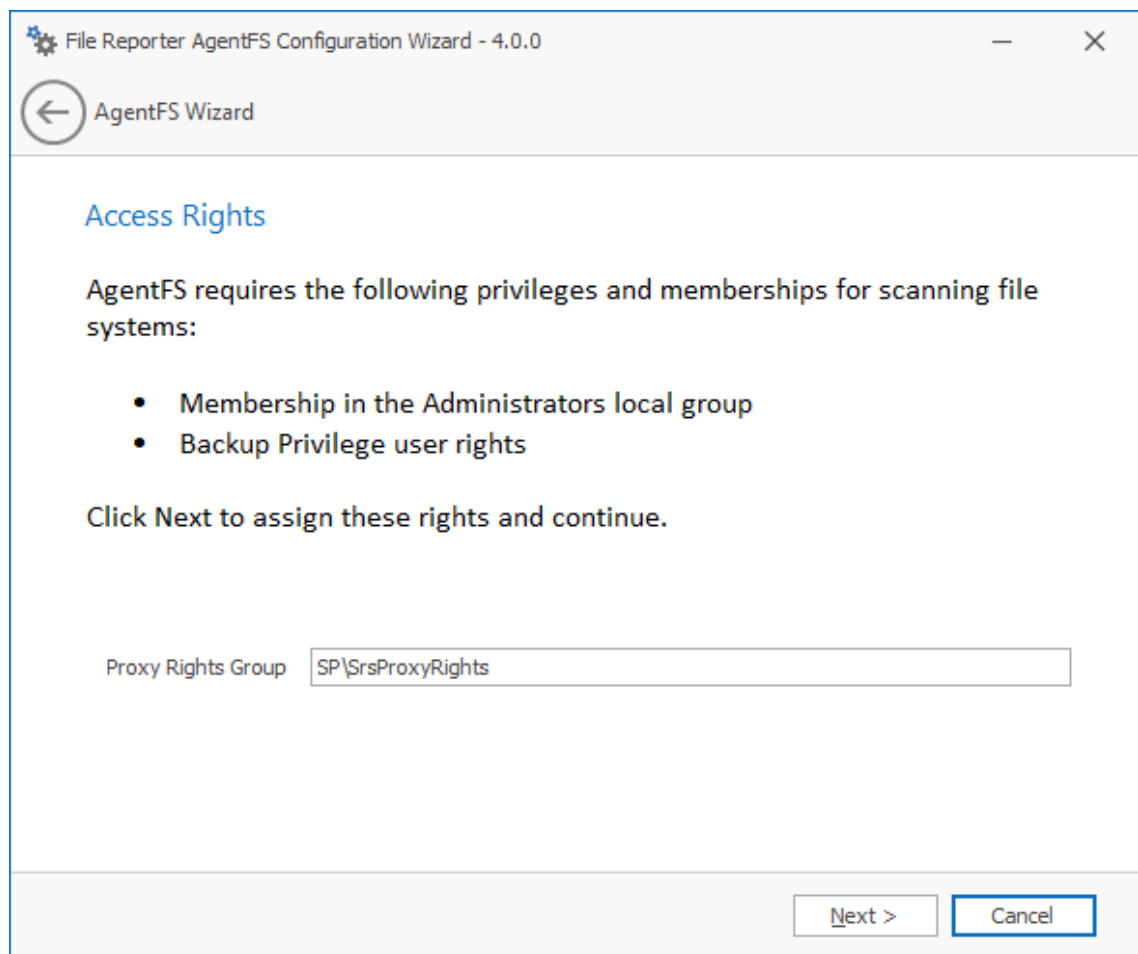
The screenshot shows a configuration window titled "File Reporter AgentFS Configuration Wizard - 4.0.0". The main heading is "AgentFS Wizard" with a back arrow icon. Below this is the "Engine Communication" section. Under "Engine Connection", there are two input fields: "Engine Address" containing "localhost" and "Engine Port" containing "3035". Below these fields is a "Test" button and a status indicator "Status Unknown" with an information icon. At the bottom right, there are two buttons: "Next >" (which is highlighted with a blue dashed border) and "Cancel".

This page lets you set parameters for AgentFS to communicate with the Engine.

Engine Address: Specify the DNS name or IP address to the server hosting the Engine here.

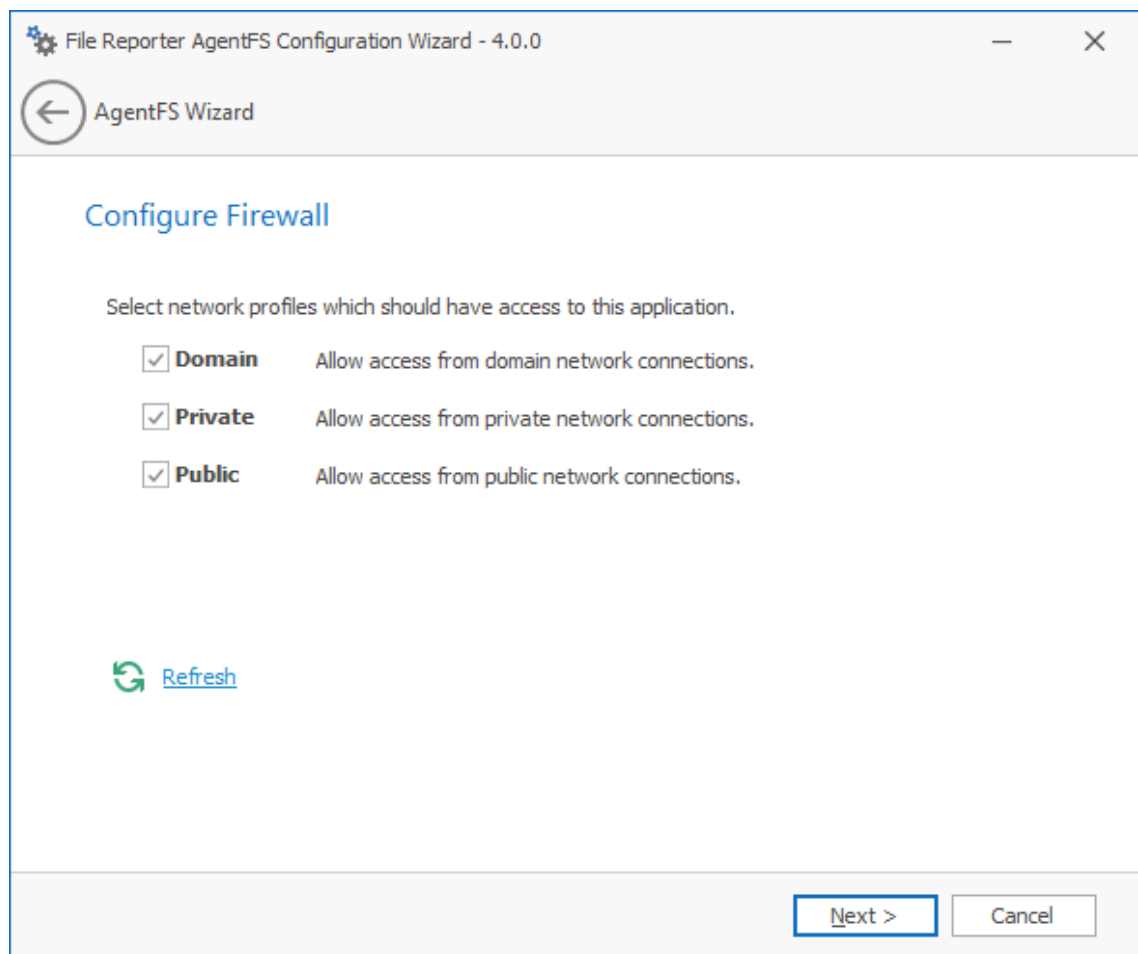
Engine Port: Specify the TLS port for the Engine here.

- 6 Enter the Engine connection settings and click **Next**.

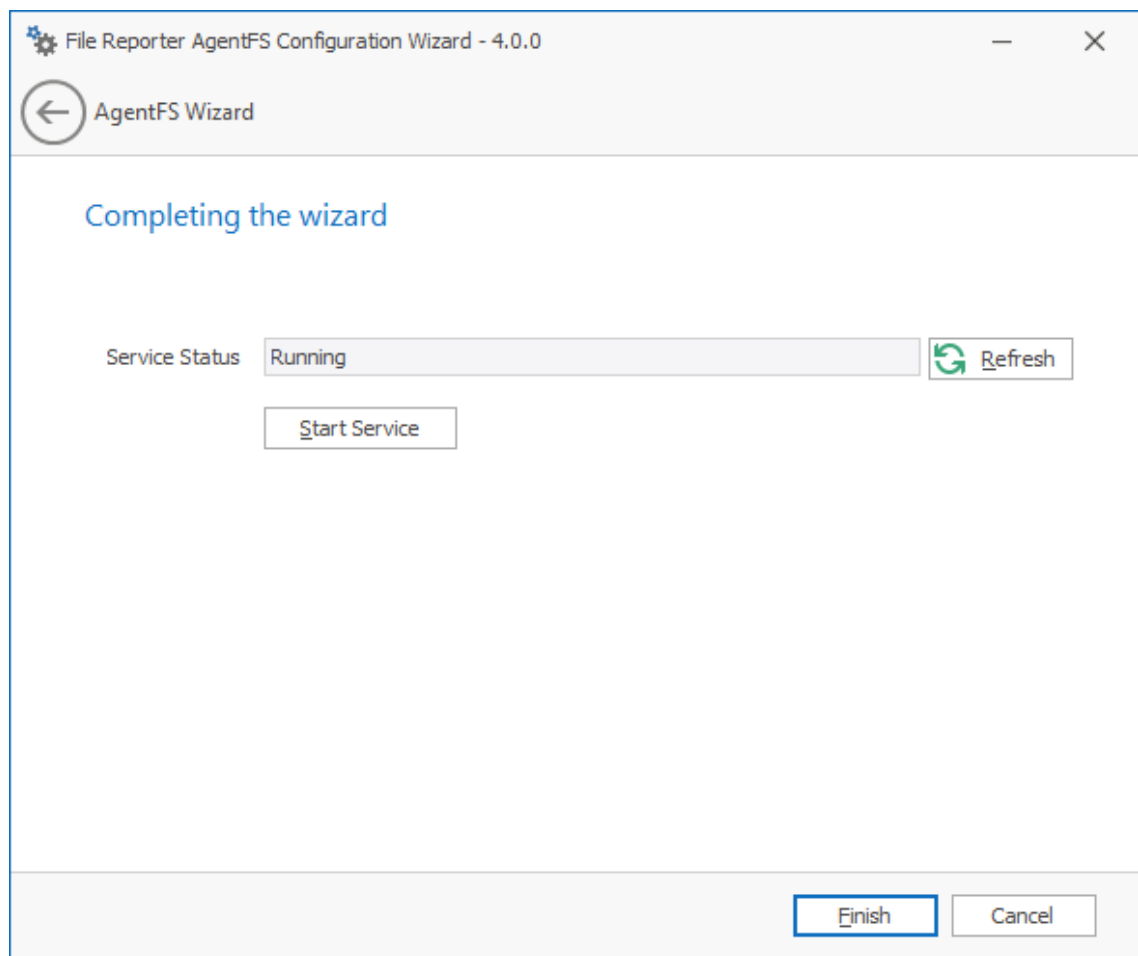


This page lets you establish AgentFS as a member of the Administrators local group and the ability to back up to the SrsProxyRights group.

7 Click **Next**.



- 8 Set the network profiles according to your organization's security policies and click **Next**.



- 9 Click **Finish** to complete the installation of AgentFS.

9 Install ManagerFC

- ♦ [Section 9.1, “Minimum Requirements,” on page 79](#)
- ♦ [Section 9.2, “Installing ManagerFC,” on page 79](#)

The ManagerFC service is responsible for the execution and management of file scan jobs. The service performs the following tasks when processing a scan job:

- ♦ Enumeration of files in target paths
- ♦ Submission of files to scan queues in the message broker based on filter criteria
- ♦ Processing of scan results and update of result data to the database and scan result files

ManagerFC requires .NET Framework 4.8, which is installed automatically if it is not already present.

9.1 Minimum Requirements

The ManagerFC host must meet the following minimum requirements:

Server Platform

- ♦ Windows Server 2019
- ♦ Windows Server 2016

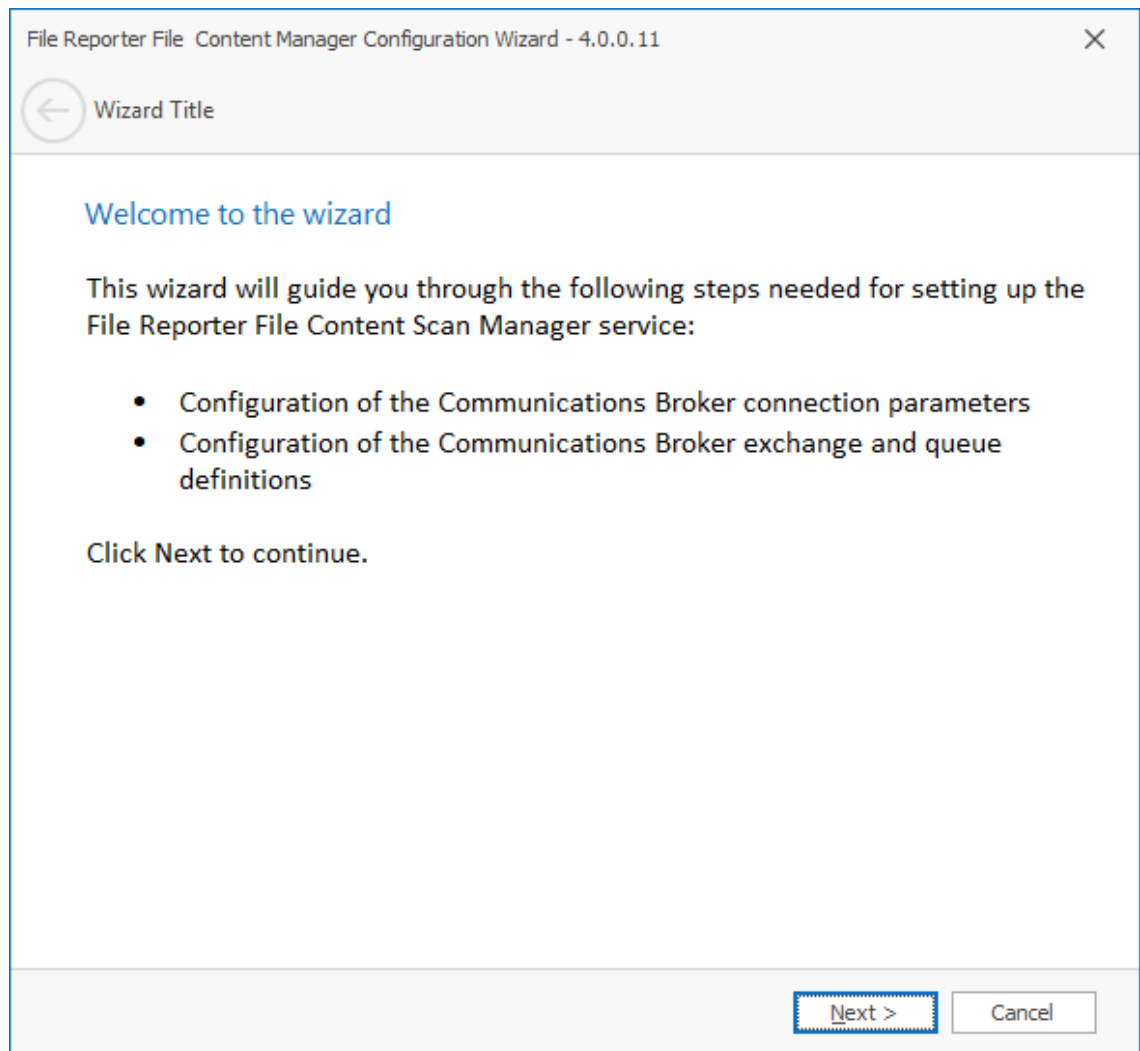
Minimum Hardware Requirements

- ♦ Quad core processor
- ♦ 6 GB RAM
- ♦ 2 GB free disk space

ManagerFC has minimal processor and RAM requirements. As such, Micro Focus recommends that ManagerFC be installed on the same host as the Engine.

9.2 Installing ManagerFC

- 1 At the root of the `FileReporter_4.0.iso` image, double-click `FileReporter-ManagerFC-4.0-x64-xx.exe`.
- 2 Agree to the license terms and conditions and click **Install**.
- 3 When you are notified that the setup was successful, click **Run Setup Utility**.



4 From the wizard page, read the overview of what will be installed and configured and click **Next**.

File Reporter File Content Manager Configuration Wizard - 4.0.0.11

Wizard Title

Message Broker Connection

Basic Configuration

Broker Type: RabbitMQ

Host Address: localhost

Port: 5671 Use TLS

API Port: 15671 Use TLS

Service Account:

Password:

[Test](#) ⓘ Status Unknown

Next > Cancel

Basic Configuration: This section includes fields pertaining to the basic configuration for the message broker.

Broker Type: Displays the RabbitMQ messaging broker.

Host Address: Specify the IP address or DNS name of the server hosting RabbitMQ.

Port: The Management API for RabbitMQ uses this TLS enabled port. The default setting is 5671.

Use TLS: The RabbitMQ messaging broker in File Reporter utilizes Transport Layer Security (TLS) as the cryptographic communications security protocol.

API Port: This is the port the Management API for RabbitMQ is listening on with TLS support enabled. The default setting is 15671.

Use TLS: This is a read-only check box indicating that File Reporter only works with TLS communication channels. TLS is always required.

Service Account: Use the administrator name that you established in [Section 6.5, “Changing the Default Password,”](#) on page 39.

Password: Use the password that you established in [Section 6.5, “Changing the Default Password,”](#) on page 39.

Test: Click to verify the connection between ManagerFC and RabbitMQ.

5 Complete the fields and click **Next**.

File Reporter File Content Manager Configuration Wizard - 4.0.0.11

Wizard Title

Database Connection

Database Server

Type: SQL Server

Host Address: []

Port: 1433

Database Service Account

Account Name: srsadmin

Password: []

Database

Database Name: srsdb

[Test](#) ⓘ Status Unknown

[Next >](#) [Cancel](#)

This page lets you establish the connection between ManagerFC and the database.

Database Server: Information specific to the database host.

Type: Depending on the database you are using, select either **PostgreSQL** or **SQL Server**.

Host Address: Specify the host address of the server where the database is installed.

Port: The default PostgreSQL database port setting is 5432. The default SQL Server port setting is 1433.

Database Service Account: Authentication information for the Database Service User.

Account Name: This field specifies the database account name that is used by File Reporter to manage data in the database. This account has both read and write access to the database.

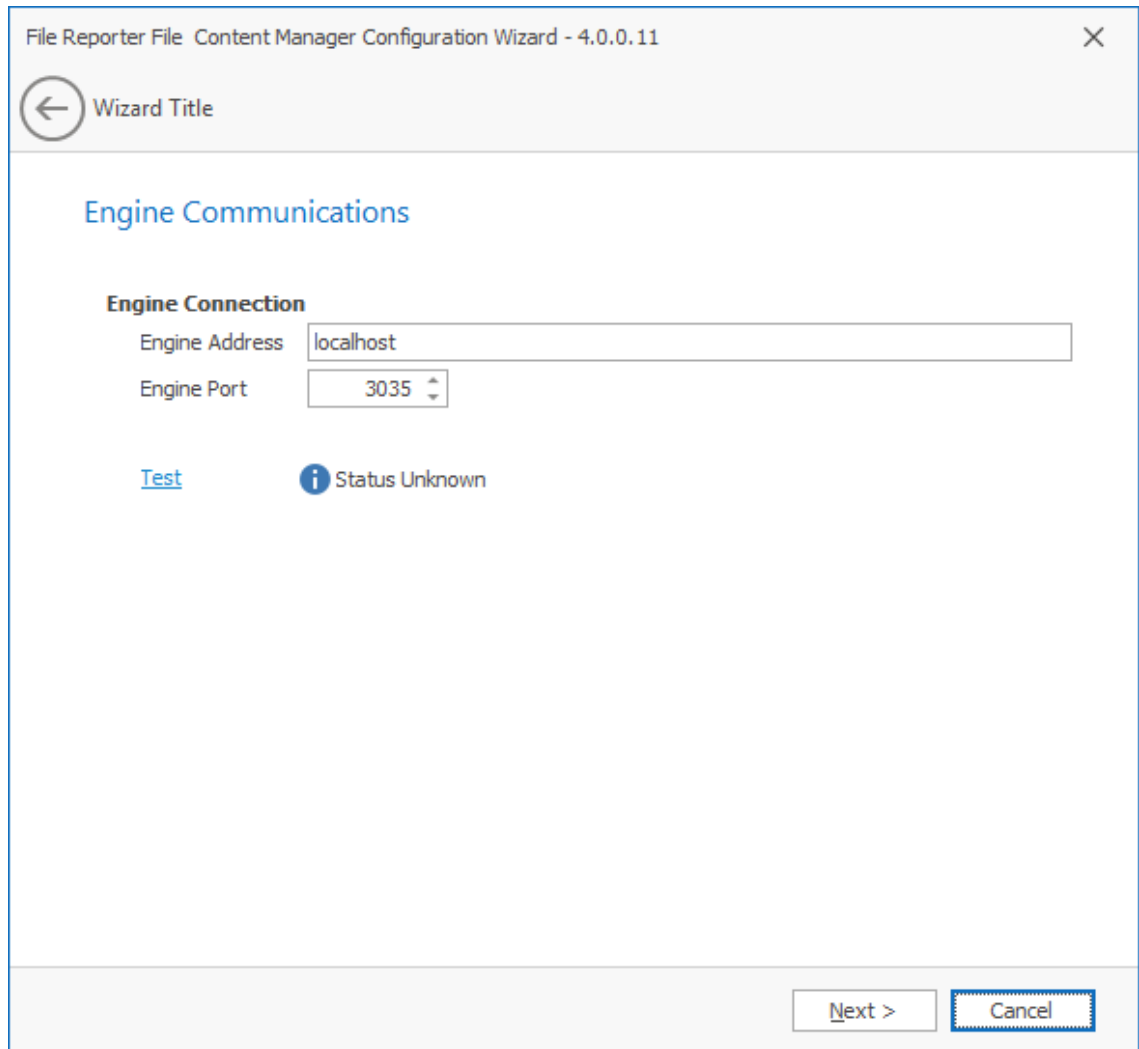
Password: Specify the password for the Database Service User.

Database: Information specific to the database name.

Database Name: Indicates the name of the database that you established when you configured the database.

Test: Click to test the connection between ManagerFC and the database.

6 Complete the fields and click **Next**.



File Reporter File Content Manager Configuration Wizard - 4.0.0.11

Wizard Title

Engine Communications

Engine Connection

Engine Address

Engine Port

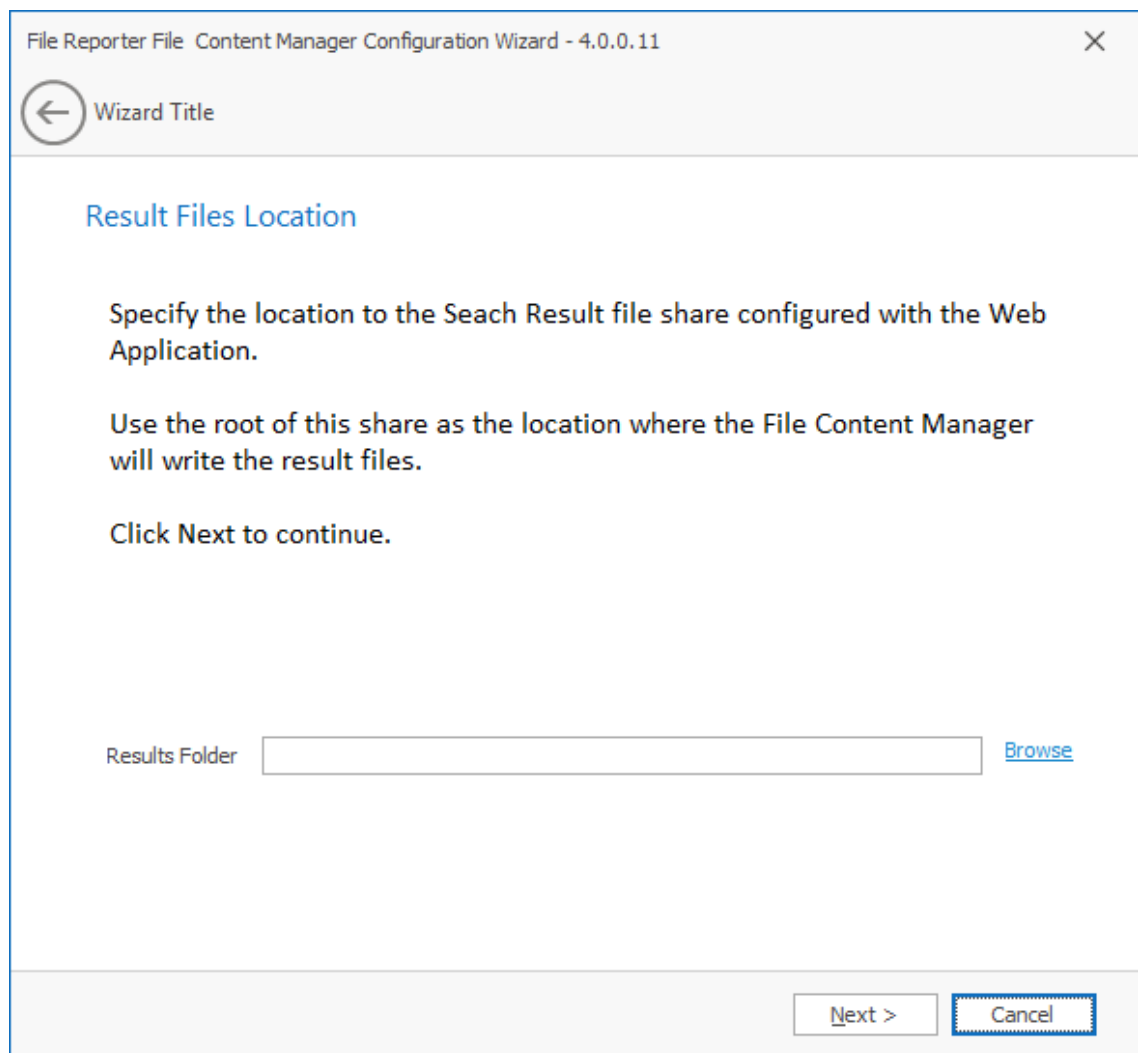
[Test](#) ⓘ Status Unknown

This page lets you set parameters for ManagerFC to communicate with the Engine.

Engine Address: Specify the DNS name or IP address to the server hosting the Engine here.

Engine SSL Port: Specify the SSL port for the Engine here.

7 Enter the Engine connection settings and click **Next**.



Use this page to specify the location where search result files are to be stored when using the **File** option in a File Content Job Definition.

- 8 Click **Browse** to locate the `server_name\Search_Results` share that was created when you installed and configured the Web App.

For more information, see [Section 7.8, “Configuring the Web Application,”](#) on page 62.

- 9 Click **Next**.
- 10 Click **Finish**.

ManagerFC is now running and operational.

10 Installing AgentFC

- ♦ [Section 10.1, “Minimum Requirements,” on page 85](#)
- ♦ [Section 10.2, “Active Directory Requirements,” on page 85](#)
- ♦ [Section 10.3, “Installing and Configuring AgentFC,” on page 86](#)

AgentFC performs file content scans. These scans examine the content of files and performs classification of those files based on the content discovered and the classification settings that you establish.

For example, a file content scan could locate U.S. Social Security numbers in files stored on your network. In a report, these files could be identified with their file paths, as well as classified based on a severity level that you establish. U.S. Social Security numbers might have a higher severity classification for example, than a phone number.

10.1 Minimum Requirements

- ♦ Any of the following dual core 64-bit processor servers:
 - ♦ Windows Server 2019
 - ♦ Windows Server 2016
- ♦ The server must be joined to Active Directory
- ♦ AgentFC is designed to be deployed as a cluster of one or more nodes. Each node has the following minimum requirements:
 - ♦ Quad-core CPU
 - ♦ 8 GB RAM
 - ♦ 10 GB free disk space for temporary files

Depending on the workloads, these numbers may need to be adjusted.

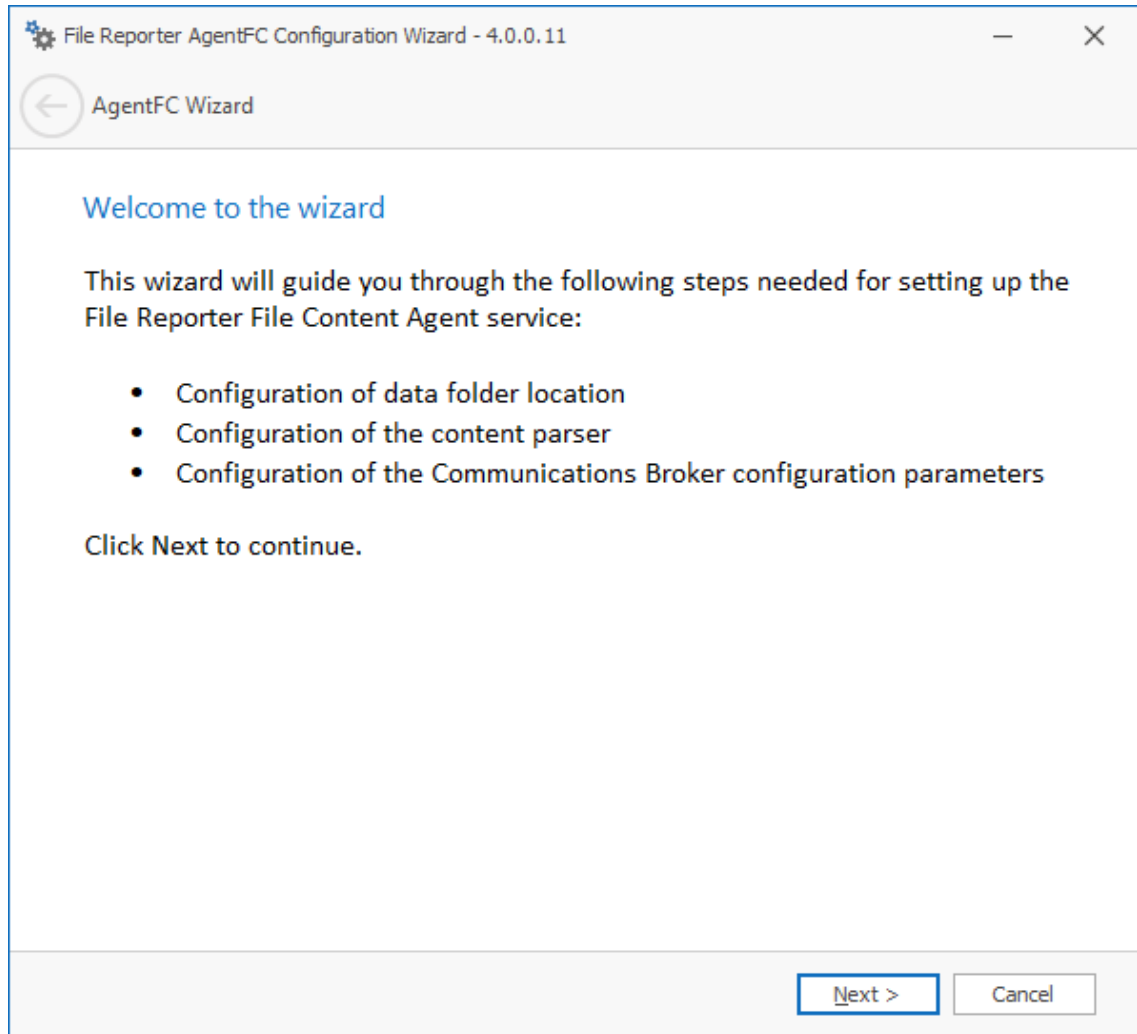
- ♦ Depending on frequency of workloads, it might advisable to install each AgentFC node in a VM environment where resources can be scaled as needed. This can allow for more resources as heavy workloads are in progress, and reclamation of resources when no jobs are currently allocated.
- ♦ For optimum throughput of content scans, consider a cluster of three or more nodes.

10.2 Active Directory Requirements

File Reporter supports a minimum forest functional level of Windows 2003.

10.3 Installing and Configuring AgentFC

- 1 At the root of the `FileReporter_4.0.iso` image, double-click `FileReporter-AgentFC-4.0.x64-xx.exe`.
- 2 Agree to the license terms and conditions and click **Install**.
- 3 When you are notified that the setup was successful, click **Run Setup Utility**.



- 4 From the wizard page, read the overview of what will be installed and configured and click **Next**.

The screenshot shows the 'Text Parser' configuration window. It has a title bar 'File Reporter AgentFC Configuration Wizard - 4.0.0.11' and a subtitle 'AgentFC Wizard'. The main content is organized into three sections: 'Tika Options', 'Java Runtime', and 'Data'. Under 'Tika Options', there is a checked checkbox for 'Use embedded Tika service', a text field for 'Host Address' containing 'localhost', and a spinner box for 'Port' set to '9998'. Below this is an unchecked checkbox for 'Enable Tesseract OCR' with an information icon and a note: 'Note: this option may greatly impact the performance of Tika'. The 'Java Runtime' section has a text field for 'Class Path' with 'lib/*', a text field for 'Start Class' with 'org.apache.tika.server.TikaServerCli', and an empty text field for 'JVM Parameters'. The 'Data' section has a text field for 'Data Folder' with the path 'C:\ProgramData\Micro Focus\SRS\AgentFC\data' and a 'Browse' button. At the bottom right, there are 'Next >' and 'Cancel' buttons.

The settings in this page let you establish specifications pertaining to the utility that performs text parsing, or the analysis of text in files.

Tika Options: These fields are specific to Apache Tika.

Host Address: AgentFC communicates with Tika via the localhost, or the same computer where AgentFC is being hosted. You should not adjust this setting.

Port: Unless there is a conflict, leave this setting at 9998.

Enable Tesseract OCR: Tesseract OCR is an open source optical character recognition engine from Google that can be the means of locating patterns and content in graphical images. Enabling this engine is resource intensive and it is therefore disabled by default. If you enable this option, beware of performance ramifications. Furthermore, if you enable this option, it should be enabled on all deployed instances of AgentFC.

Java Runtime: These fields pertain to settings for the Java runtime that was installed during the installation of AgentFC.

Class Path: Displays the location of Java classes and packages as well as Apache Tika for content analysis. Unless directed by a Micro Focus Support representative during a technical support call, you should not make changes to this field.

Start Class: Specifies Apache Tika as a Java Start Class. This field cannot be edited.

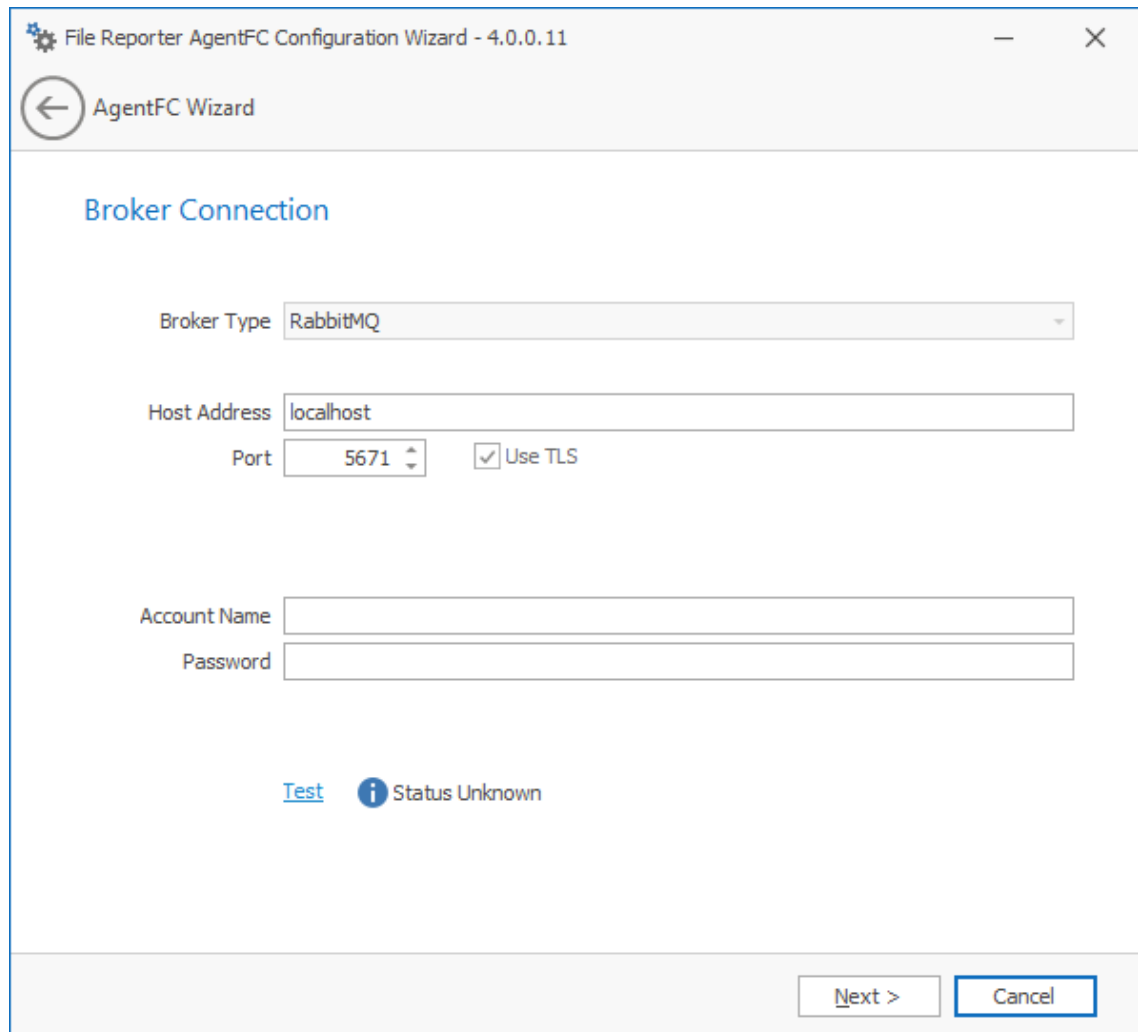
JVM Parameters: This field is provided as a means for a Micro Focus Technical Support representative to help a customer tune the performance of the Java Virtual Machine. Any settings in this field should be done through the direction of a Micro Focus Support representative.

Data: Information specific to the data gathered through text parsing.

Data Folder: This field specifies the temporary location where scanned files are processed before being sent to the database.

Browse: Lets you specify a new location for the data folder.

- 5 Complete the fields and click **Next**.



The screenshot shows a configuration window titled "File Reporter AgentFC Configuration Wizard - 4.0.0.11". The main content area is titled "AgentFC Wizard" and "Broker Connection". The configuration fields are as follows:

- Broker Type: RabbitMQ (dropdown menu)
- Host Address: localhost (text input)
- Port: 5671 (spin box)
- Use TLS: (checkbox)
- Account Name: (empty text input)
- Password: (empty text input)

At the bottom of the configuration area, there is a "Test" button and a status indicator "Status Unknown". At the bottom right of the window, there are "Next >" and "Cancel" buttons.

This page lets you establish settings for communication between AgentFC and the RabbitMQ messaging broker.

Broker Type: Displays the RabbitMQ messaging broker.

Host Address: Specify the IP address or DNS name of the server hosting RabbitMQ.

Port: This is the port that the Management API for RabbitMQ is listening on with TLS support enabled, which by default is 5671.

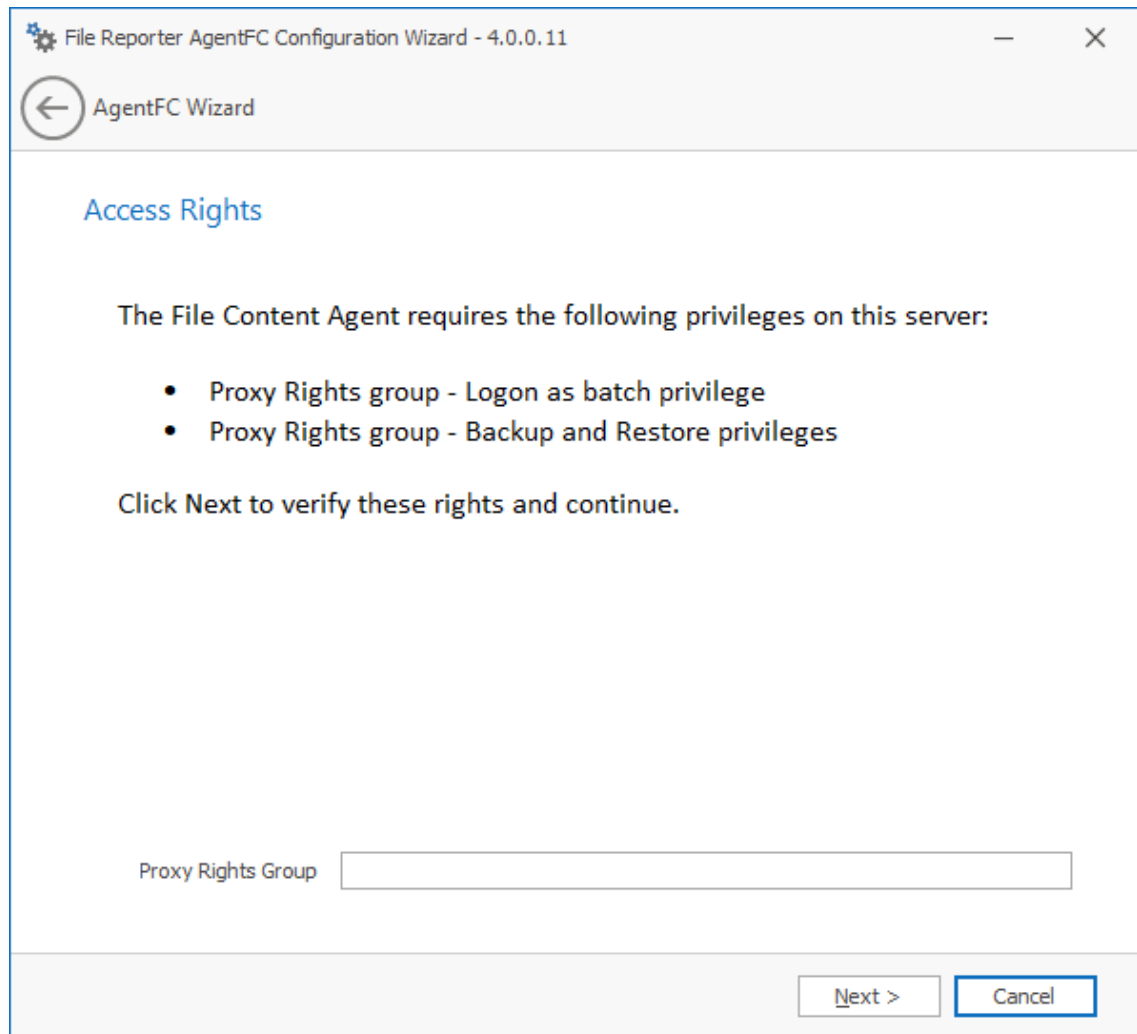
Use TLS: The RabbitMQ messaging broker in File Reporter requires Transport Layer Security (TLS) as the cryptographic communications security protocol.

Account Name: This field displays the default database broker account name used within RabbitMQ. This was created during the configuration of ManagerFC. For more information, see [Section 9.2, “Installing ManagerFC,” on page 79](#).

Password: Enter the admin account password that you set up when you configured ManagerFC.

Test: Click to test the connection between AgentFC and RabbitMQ.

6 Complete the fields and click **Next**.



File Reporter AgentFC Configuration Wizard - 4.0.0.11

AgentFC Wizard

Access Rights

The File Content Agent requires the following privileges on this server:

- Proxy Rights group - Logon as batch privilege
- Proxy Rights group - Backup and Restore privileges

Click Next to verify these rights and continue.

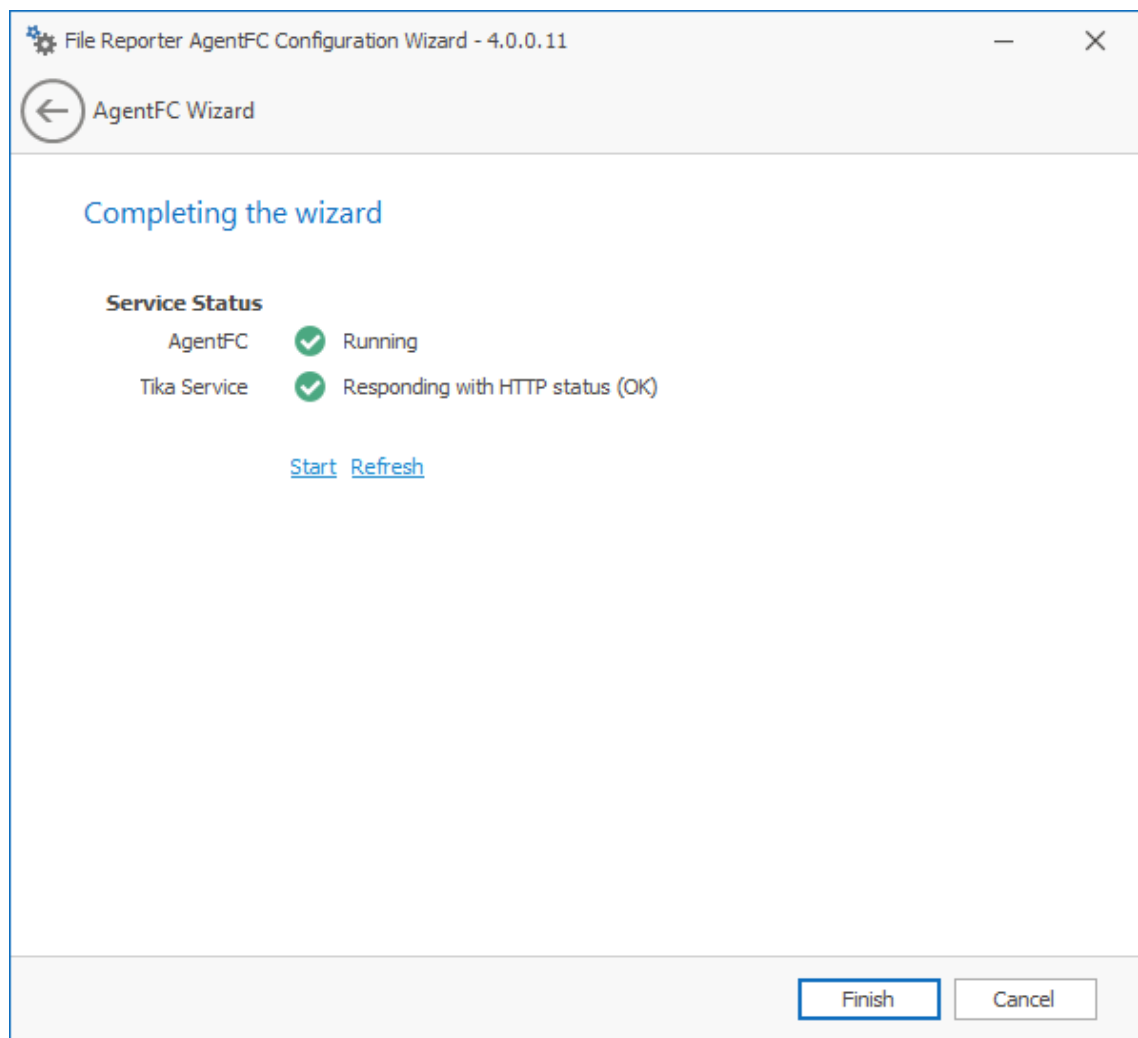
Proxy Rights Group

Next > Cancel

This page lets you establish needed privileges for the AgentFC host via the Proxy Rights Group.

7 In the Proxy Rights Group field, enter the name of the Proxy Right Group, which by default is `SrsProxyRights`.

8 Click **Next**.



9 Click Finish.

11 Enabling Microsoft 365 Reporting and Installing Agent365

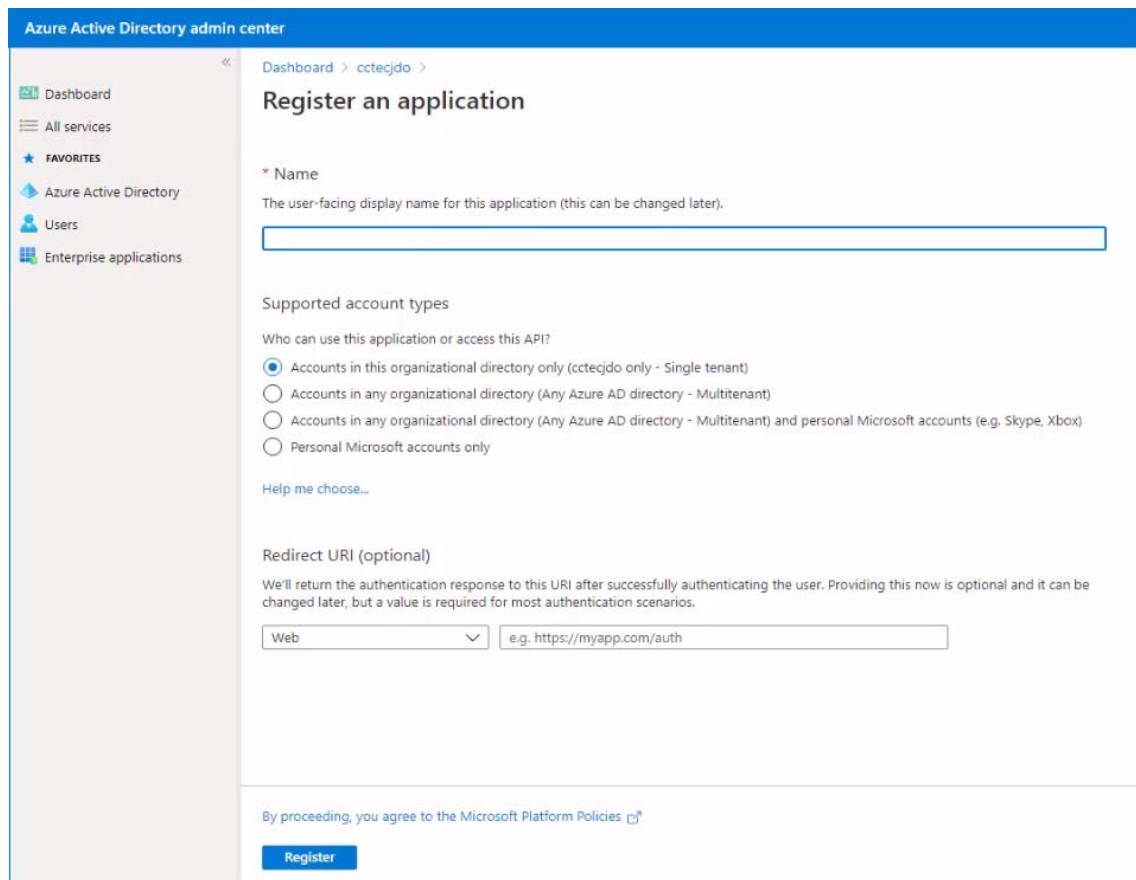
This chapter provides procedures for first configuring Microsoft 365 Cloud applications, including OneDrive for Business, SharePoint Online document libraries, and Teams document libraries for reporting through File Reporter. Afterwards, it provides procedures for installing and configuring Agent365 which performs scans on the Microsoft 365 cloud applications. Scans on Microsoft 365 cloud applications include file metadata, permissions, and user and group relationships.

NOTE: If you will not be reporting on Microsoft 365 cloud applications, you do not need to follow the procedures in this chapter.

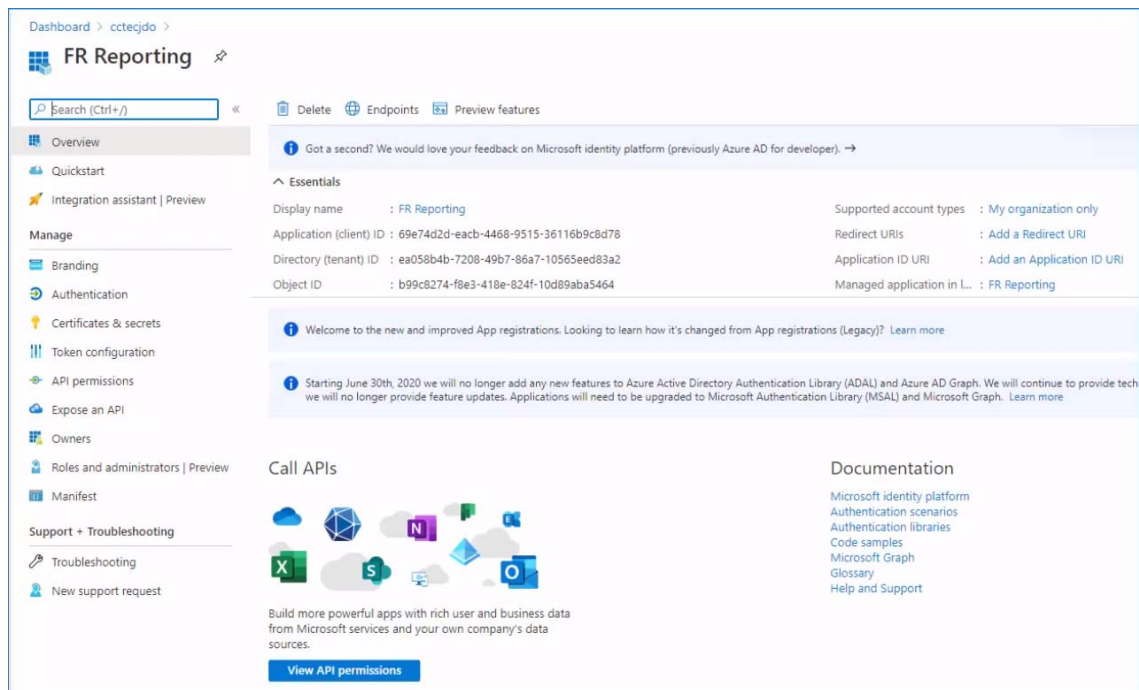
- ♦ [Section 11.1, “Preparing the Microsoft 365 Cloud Tenant,” on page 91](#)
- ♦ [Section 11.2, “Installing Agent365,” on page 97](#)

11.1 Preparing the Microsoft 365 Cloud Tenant

- 1 In web browser, go to <https://admin.microsoft.com>.
This will automatically redirect you to the Microsoft 365 Admin Center for your tenant.
If you are not already authenticated, you will have to do so before being redirected.
- 2 From the **Navigation** menu, select **Show all**.
- 3 Under **Admin centers**, select **Azure Active Directory**.
This launches the Azure Active Directory admin center.
- 4 From the **Dashboard** menu, click **Azure Active Directory**.
- 5 From the **Manage** menu, select **App registrations**.
- 6 Click the **New registration** tab.



- 7 In the **Name** field, enter a descriptive name for the application registration.
For example: FR Reporting
- 8 In the **Supported account types** region, select the **Single tenant** option (the first option).
- 9 Leave the default settings of the **Redirect URI (optional)** region and click **Register**.
The application is registered and the settings are displayed.



10 From the **Manage** menu, select **API permissions**.

11 Set the application permissions.

11a Refer to the following table as you establish application permissions:

API / Permissions Name	Description
Microsoft Graph	
Directory.Read.All	Read directory data
Files.Read.All	Read files in all site collections
Group.Read.All	Read all groups
GroupMember.Read.All	Read all group memberships
Member.Read.Hidden	Read all hidden memberships
Organization.Read.All	Read organization information
Sites.Read.All	Read items in all site collections (previews)
Team.ReadBasic.All	Get a list of all teams
TeamMember.Read.All	Read the members of all teams
TeamSettings.Read.All	Read all teams' settings
User.Read.All	Read all users' full profiles


11b Click the **Add a permission** tab.

Request API permissions













Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs




Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Exchange, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 <p>Azure Rights Management Services Allow validated users to read and write protected content</p>	 <p>Azure Service Management Programmatic access to much of the functionality available through the Azure portal</p>	 <p>Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination</p>
 <p>Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central</p>	 <p>Dynamics CRM Access the capabilities of CRM business software and ERP systems</p>	 <p>Flow Service Embed flow templates and manage flows</p>
 <p>Intune Programmatic access to Intune data</p>	 <p>Office 365 Management APIs Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs</p>	 <p>OneNote Create and manage notes, lists, pictures, files, and more in OneNote notebooks</p>
 <p>Power BI Service</p>	 <p>SharePoint</p>	 <p>Skype for Business</p>

11c Click the Microsoft Graph API.

Request API permissions

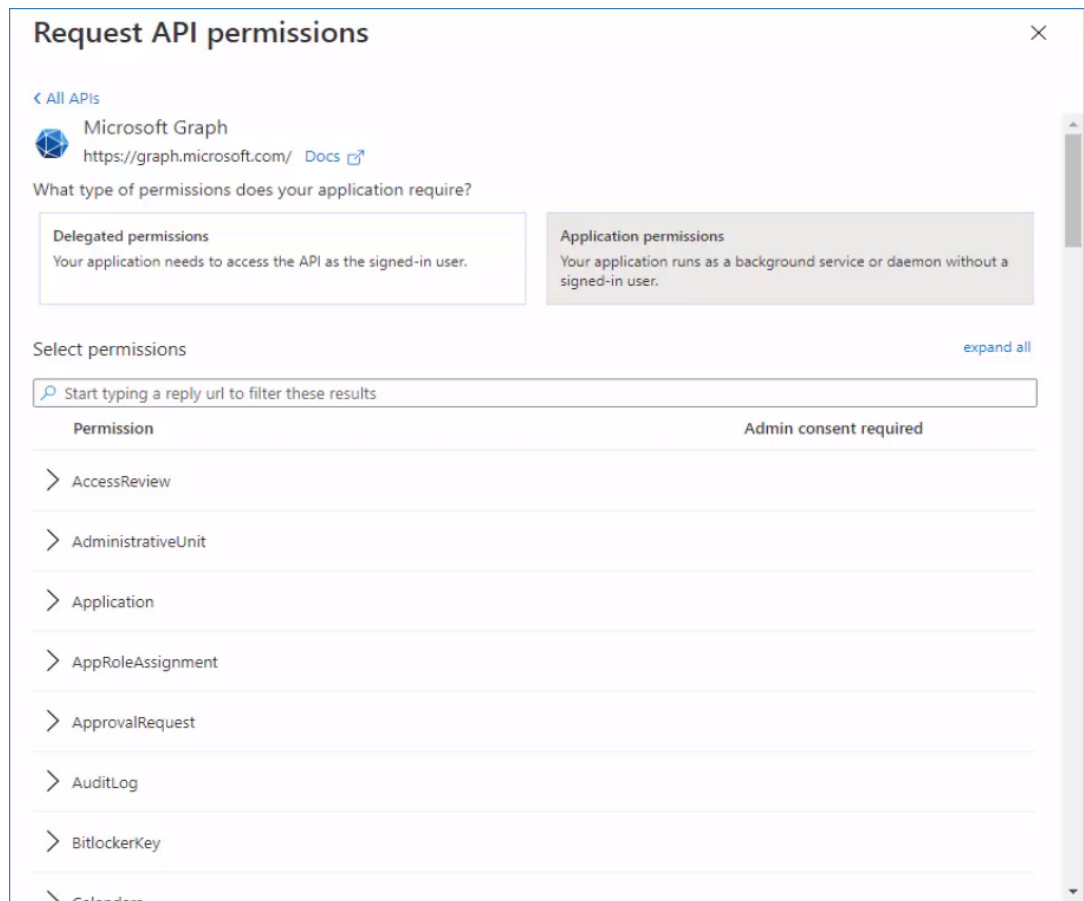
< All APIs

 **Microsoft Graph**
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

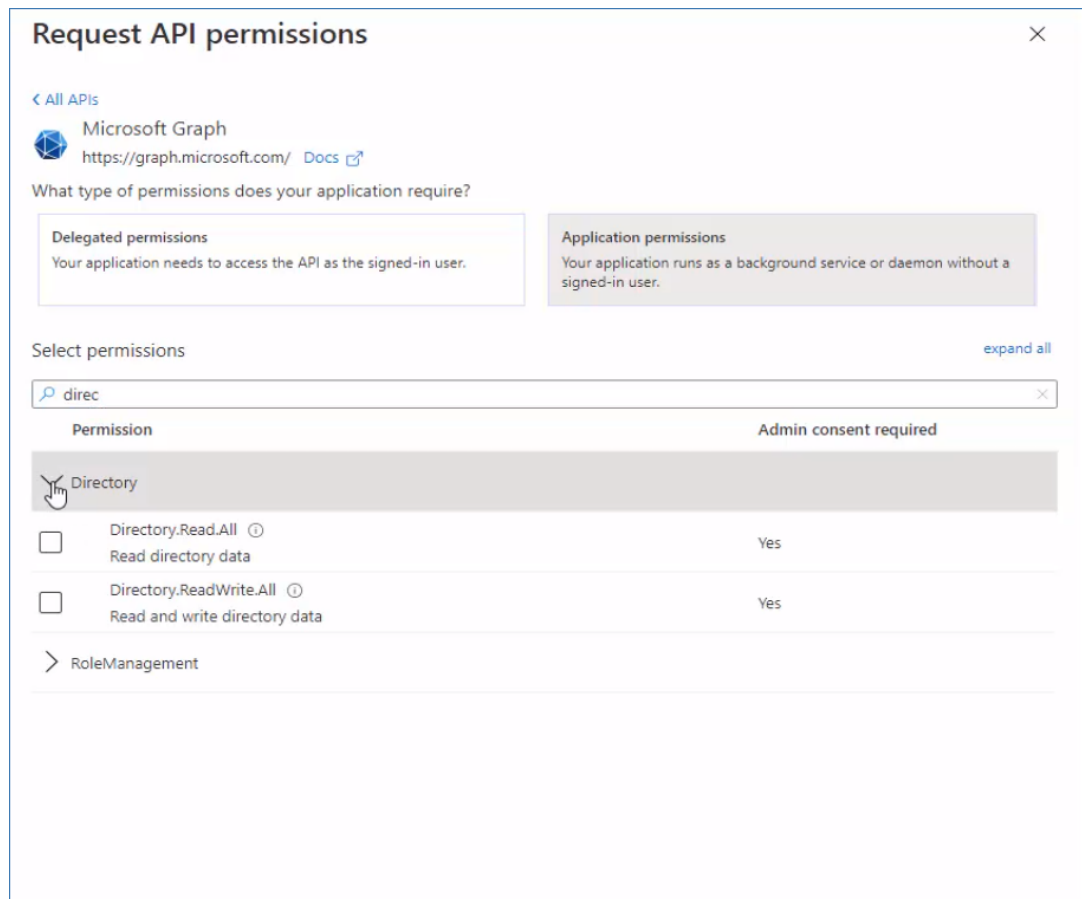
<p>Delegated permissions Your application needs to access the API as the signed-in user.</p>	<p>Application permissions Your application runs as a background service or daemon without a signed-in user.</p>
---	---

11d Click Application permissions.



11e Referring to the table in Substep 8a, begin typing `directory` so that the **Directory** permission shows up below.

11f Expand the **Directory** permission to display the options.



- 11g** From the table in Substep 8a, verify that the permissions to select are **Directory.Read.All Read directory data**, then select that specific check box.
- 11h** Click **Add permissions**.
 The **Directory.Read.All** permission is added to the Configured permissions table.
- 11i** Repeat Substeps 8b-8h to add all of the permissions specified in the table in Substep 8a.
- 11j** When finished, remove the **User.Read** permission by selecting it and then in the Remove permission dialog box, click **Yes, remove**.
- 12** Grant admin consent for the tenant.
 - 12a** Above the list of permissions that you just established, click **Grant admin consent for *tenant_name***.
 - 12b** When asked if you want to grant consent for the requested permissions for all accounts in *tenant_name*, click **Yes**.

The status for each of the permissions is changed to **Granted for *tenant_name***.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for cctecjdo

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (11)				
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for cctecjdo
Files.Read.All	Application	Read files in all site collections	Yes	✓ Granted for cctecjdo
Group.Read.All	Application	Read all groups	Yes	✓ Granted for cctecjdo
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for cctecjdo
Member.Read.Hidden	Application	Read all hidden memberships	Yes	✓ Granted for cctecjdo
Organization.Read.All	Application	Read organization information	Yes	✓ Granted for cctecjdo
Sites.Read.All	Application	Read items in all site collections (preview)	Yes	✓ Granted for cctecjdo
Team.ReadBasic.All	Application	Get a list of all teams	Yes	✓ Granted for cctecjdo
TeamMember.Read.All	Application	Read the members of all teams	Yes	✓ Granted for cctecjdo
TeamSettings.Read.All	Application	Read all teams' settings	Yes	✓ Granted for cctecjdo
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for cctecjdo

11.2 Installing Agent365

11.2.1 Prerequisites

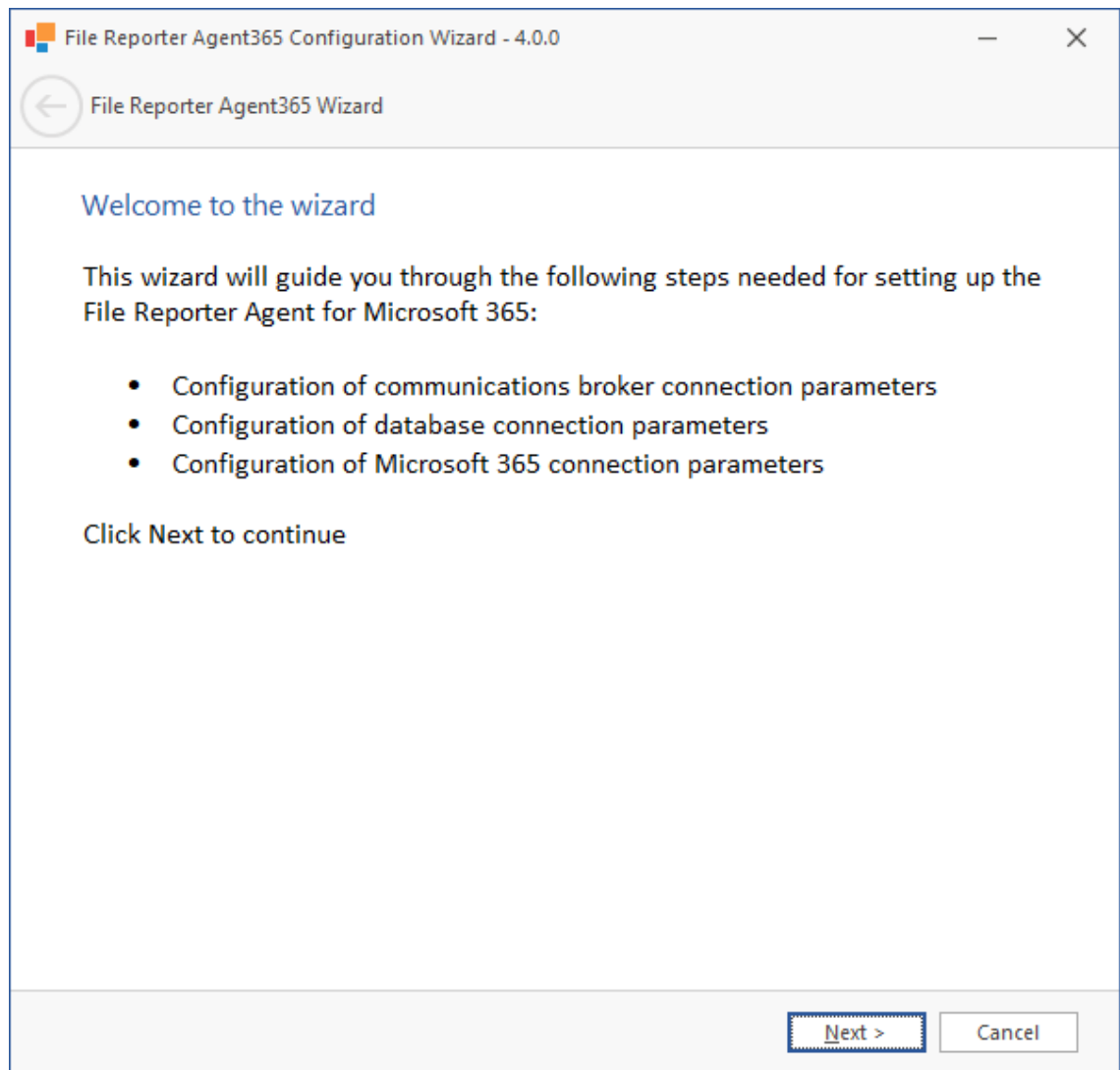
In the Configuration Dashboard, verify that the Message Broker is installed, configured, and connected.

11.2.2 Minimum Requirements

- ◆ Any of the following dual core 64-bit processor servers:
 - ◆ Windows Server 2019
 - ◆ Windows Server 2016
- ◆ The server must be joined to Azure Active Directory
- ◆ For large tenants, Micro Focus recommends a dedicated server for Agent365
- ◆ .NET 4.8 (this will be installed if not already present)
- ◆ Minimum of 200 MB RAM

11.2.3 Installing and Configuring Agent365

- 1 At the root of the FileReporter_4.0.iso image, double-click FileReporter-Agent365-4.0.x64-xx.exe.
- 2 Agree to the license terms and conditions and click **Install**.
- 3 When you are notified that the setup was successful, click **Run Setup Utility**.



- 4 From the wizard page, read the overview of what will be installed and configured and click **Next**.

The screenshot shows a configuration wizard window titled "File Reporter Agent365 Configuration Wizard - 4.0.0". The main heading is "Message Broker Connection". Under "Basic Configuration", there are several input fields and checkboxes:

- Broker Type:** A dropdown menu set to "RabbitMQ".
- Host Address:** An empty text input field.
- Port:** A spinner box set to "5671" with a checked "Use TLS" checkbox.
- API Port:** A spinner box set to "15671" with a checked "Use TLS" checkbox.
- Service Account:** An empty text input field.
- Password:** An empty password input field with a visibility toggle icon.

At the bottom of the configuration area, there is a "Test" link and an information icon followed by the text "Status Unknown". At the very bottom of the window, there are "Next >" and "Cancel" buttons.

Broker Type: Displays the RabbitMQ messaging broker.

Host Address: Specify the IP address or DNS name of the server hosting RabbitMQ.

Port: This is the port that the Management API for RabbitMQ is listening on with TLS support enabled, which by default is 5671.

Use TLS: The RabbitMQ messaging broker in File Reporter requires Transport Layer Security (TLS) as the cryptographic communications security protocol.

API Port: This is the port the Management API for RabbitMQ is listening on with TLS support enabled. The default setting is 15671.

Use TLS: This is a read-only check box indicating that File Reporter only works with TLS communication channels. TLS is always required.

Service Account: Enter the name of the service account, which is by default, `srsbroker`.

For your reference, your Service Account name is displayed in the **Message Broker** region of the Configuration Dashboard.

Password: Enter the password that you established when you configured the Message Broker.

Test: Click to test the connection between Agent365 and RabbitMQ.

5 Complete the fields and click **Next**.

The screenshot shows the 'File Reporter Agent365 Configuration Wizard - 4.0.0' window. The title bar includes a back arrow icon and the text 'File Reporter Agent365 Wizard'. The main content area is titled 'Database Connection' and contains three sections:

- Database Server:** A 'Type' dropdown menu is set to 'SQL Server'. Below it are 'Host Address' and 'Port' (set to 1433) text boxes.
- Database Service Account:** 'Account Name' and 'Password' text boxes. The password box has an eye icon for visibility.
- Database:** A 'Database Name' dropdown menu is set to 'srsdb'.

Below the 'Database' section, there is a blue 'Test Connection' link and a status indicator 'Status Unknown' with an information icon. At the bottom right, there are 'Next >' and 'Cancel' buttons.

Database Server: This region includes fields specific to the communication with the Microsoft SQL Server or PostgreSQL database.

Type: From the drop-down menu, specify the database type.

Host Address: Enter the IP address of the server hosting the database that you configured earlier.

For your reference, the IP address is displayed in the **Database** region of the Configuration Dashboard.

Port: Unless you changed the default port address when you configured the database, leave the setting at 1433.

Database Service Account: This region includes fields for the database service account and password.

Account Name: Unless you changed the default name for the Database Service User, enter srsadmin.

For your reference, the name is displayed in the **Database User** field in the **Database** region of the Configuration Dashboard.

Password: Enter the database administrator password.

Database Name: Unless you changed the default name for the database name, enter `srpdb`.

For your reference, the database name is displayed in the **Database** region of the Configuration Dashboard.

Test Connection: Click to test the connection between Agent 365 and the database.

- 6 Complete the fields and click **Next**.

File Reporter Agent365 Configuration Wizard - 4.0.0

File Reporter Agent365 Wizard

Microsoft 365 Connection

Tenant

Tenant Name
The registered tenant name, such as 'name.onmicrosoft.com'

Application

Application ID

Application Certificate [Details](#)

Subject Name ⚠

Thumbprint

Key Length

Expiration Date

[Test Connection](#) ⓘ Status Unknown

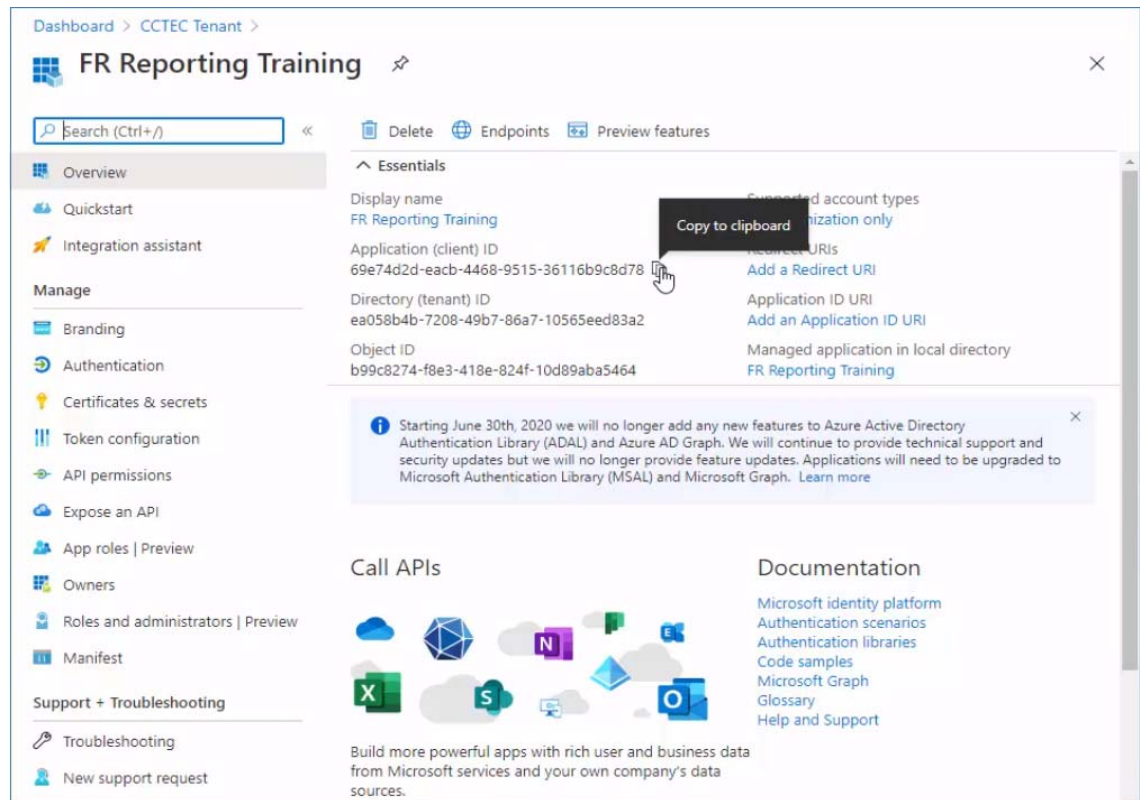
To complete the fields in this page, you will need to log in to your tenant in Azure AD.

Tenant: Enter the name of your tenant here.

For your reference, you can view this in the Azure Active Directory admin center interface by selecting **Azure Active Directory**.

Application ID: Enter the name of the application that you registered and configured previously.

For your reference, you can identify the application ID in the Azure Active Directory admin center by clicking **App registrations**, clicking the listed registered application, and then copying the **Application (client) ID** listing into the **Application ID** field of the File Reporter Agent 365 wizard.



Application Certificate: This region is where you generate the key pair for the application certificate. Once you do so, the fields are filled in automatically.

7 Generate the application certificate.

7a Click **Generate Key Pair**.

7b When the Certificate Update Notice dialog box appears, click **Yes**.

The following dialog box appears:

Create Application Certificate

Subject Name: File Reporter Agent365

Key Length: 4096

Expiration Days: 3,650 Expiration Date: 2030-11-23 11:04

Certificate Password:

Verify Password:

Generate **Cancel**

7c In the **Certificate Password** field, create a password for the certificate.

7d Provide the password again in the **Verify Password** field.

7e Click **Generate**.

The application certificate details are now displayed in the remaining fields of the wizard page.

7f Click **Export Public Certificate**.

7g Save the certificate to a preferred location on the server.

7h In Azure Active Directory admin center, click **Certificates & secrets**.

Dashboard > CCTEC Tenant > FR Reporting Training

FR Reporting Training | Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles | Preview
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
No client secrets have been created for this application.			

7i Click **Upload certificate**, click the folder icon in the dialog box to browse to the location where you saved the certificate, click **Open** and then click **Add**.

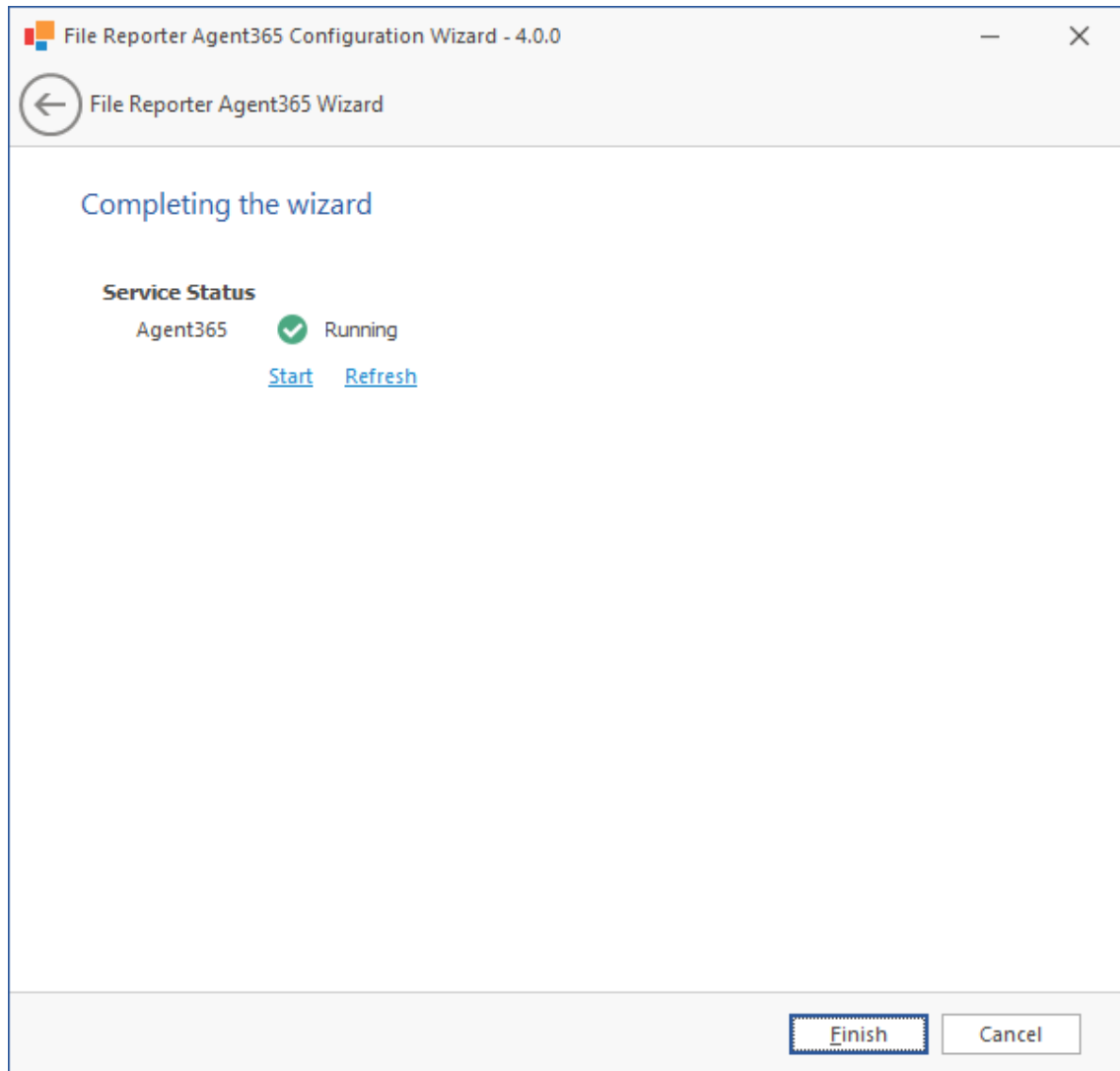
The certificate is now listed in the **Certificates** region of the Azure Active Directory admin center page.

7j Return to the File Reporter Agent365 Wizard and click **Test Connection**.

If you get a failure notice, it most likely means that the tenant has not had enough time to update. If you do, try again until you get a **Connection valid** indication on the wizard page and a Tenant Info dialog appears with the updated tenant information.

7k Click **OK** to close the Tenant Info dialog box.

8 Click **Next** to advance in the wizard.



9 Click **Finish**.

12 Installing the Report Viewer and Client Tools

- ◆ [Section 12.1, “Minimum Requirements,” on page 105](#)
- ◆ [Section 12.2, “Install the Report Viewer,” on page 106](#)
- ◆ [Section 12.3, “Install the Client Tools,” on page 106](#)

The Report Viewer lets you view all stored reports locally from a Windows workstation. Because the Report Viewer utilizes the resources of a Windows workstation, rather than those of the Engine, the Report Viewer can display stored reports much faster in most instances.

The Client Tools are designed to provide members of the administrators group expanded abilities in designing reports and analyzing data. The Client Tools include the Report Designer and the Analytics Tools.

NOTE: You must be a member of the SrsAdmins group to use the Client Tools. The name SrsAdmins is the default name (which you can change) of the File Reporter administrators group created during the installation of the Engine.

12.1 Minimum Requirements

- ◆ Any 64-bit multi-core processor Windows workstation with the .NET 4.8 framework.

Note that significant analytic workloads with the Data Analytics tool might be directly impacted by the number and speed of available cores.

- ◆ A DirectX 10 compatible graphics card required for use with the Data Analytics tool.
- ◆ Report Viewer: Minimum of 8 GB RAM.

Depending on the size of report loading, exporting, and processing, this number might need to be significantly increased.

- ◆ Data Analytics: Minimum of 12 GB RAM

Note that for the Data Analytics tool, a minimum of about 1KB per scan data entry (or 1GB per million entries) is required. Depending on the type of analysis, such as the Pivot Grid, and the number of entries in a single scan, this number might need to be significantly increased.

- ◆ Minimum of 250 MB disk space.
- ◆ Report Designer and Data Analytics users must be members of the SrsAdmins group.

12.2 Install the Report Viewer

- 1 From the root of the `FileReporter_4.0.iso` image, copy the `FileReporter-ReportViewer-4.0-x64-xx.exe` file to all Windows workstations where you will run the Report Viewer.
- 2 From the Windows workstation, double-click `FileReporter-ReportViewer-4.0-x64-xx.exe`.
- 3 Agree to the license terms and conditions, then click **Install**.
- 4 When notified that the setup was successful, click **Close**.

The Report Viewer icon is added to the **Start** menu.

12.3 Install the Client Tools

- 1 From the root of the `FileReporter_4.0.iso` image, copy the `FileReporter-ClientTools-4.0-x64-xx.exe` file to all Windows workstations where you will run the Client Tools.
- 2 From the Windows workstation, double-click `FileReporter-ClientTools-4.0-x64-xx.exe`.
- 3 Agree to the license terms and conditions, then click **Install**.
- 4 When notified that the setup was successful, click **Close**.

The Data Analytics and Report Designer icons are added to the **Start** menu.

A Replace a License File

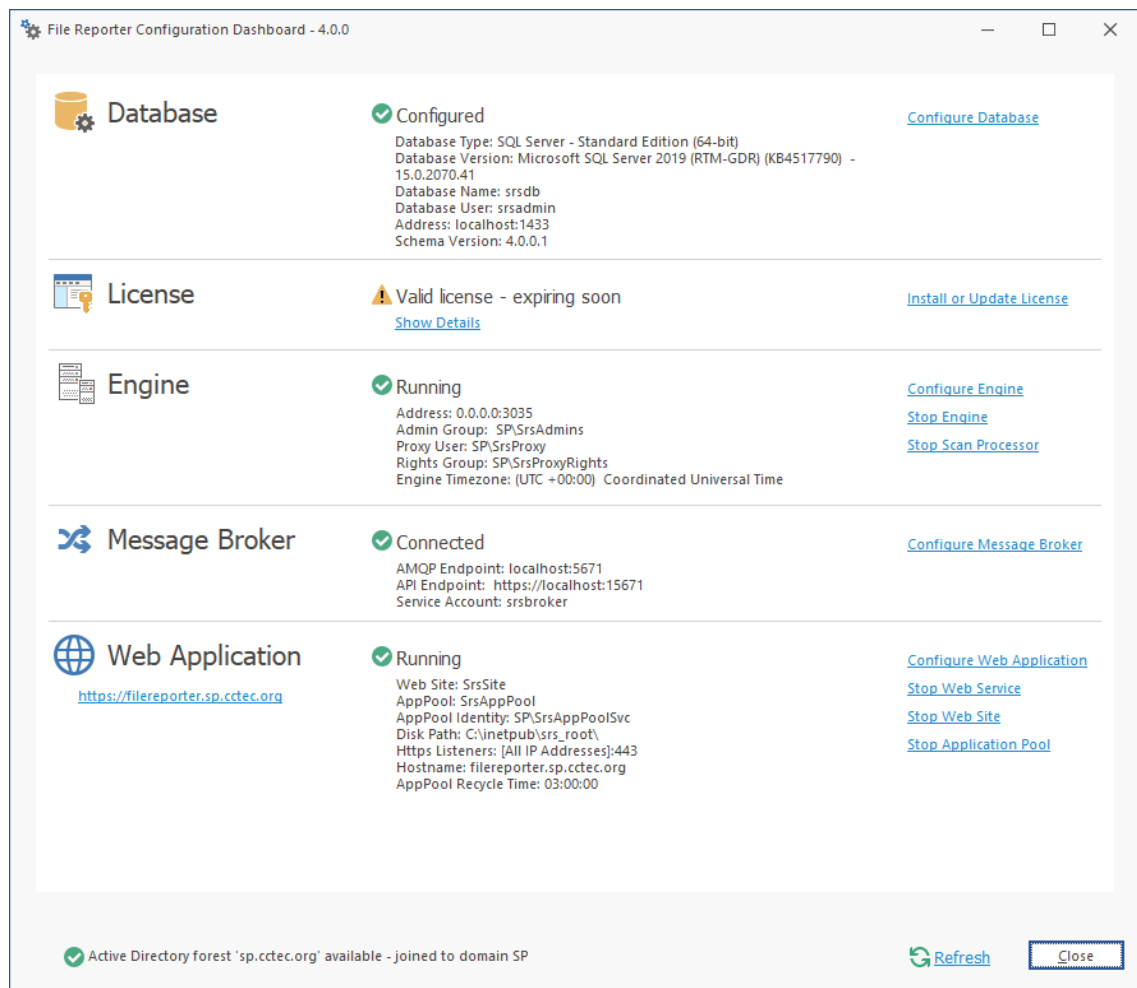
A.1 Replacing a License

You use the File Reporter Configuration Dashboard to replace a File Reporter license, including an evaluation license.

NOTE: License expiration checks are done every 24 hours at midnight.

When the license expires, you cannot log in through the File Reporter Web application until the license is replaced; this can only be done through the File Reporter Engine Configuration utility.

- 1 From the **Start** menu, launch the File Reporter Configuration Dashboard.
- 2 On the File Reporter Configuration Dashboard, click **Install or Update Licensing**.



A page similar to the following appears:

License

Product: File Reporter

License Type: Production

Licensed Identity System: sp.cctec.org

Identity System Type: Active Directory

Licensed Organization: SP Tech

Expiration Date: 2020-12-23 19:11:54

Licensed Features: Core Product, Windows File Systems, Microsoft 365, Content Analysis, Data Access Governance Integration

Load License

✔ - License expires very soon.
- License valid for update. Click 'Save' to apply

Save Cancel


3 Click **Load License**, then browse to and select the production license file.

4 When the confirmation prompt appears, click **Yes**.

The fields on the License page are filled in according to the data in the license file.

License ✕

Product	File Reporter
License Type	Production
Licensed Identity System	sp.cctec.org
Identity System Type	Active Directory
Licensed Organization	SP Tech
Expiration Date	2022-11-05 16:30:09
Licensed Features	Core Product Windows File Systems Microsoft 365 Content Analysis Data Access Governance Integration

 License valid for update. Click 'Save' to apply

5 Click Close.

