# Micro Focus File Reporter 4.1

## Installation Guide

**February 28, 2022**

## 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 © 2022 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion with out 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** 5

**1 Upgrading from a Previous Version** 7

1.1 Database . . . 7
1.2 License . . . 7
1.3 Core Components . . . 7
1.4 Microsoft 365 Reporting . . . 8
1.5 Agents . . . 8
1.5.1 File System Agents . . . 8
1.5.2 File Content Agents . . . 8
1.5.3 Microsoft 365 Agent . . . 8

**2 Deployment Planning** 9

2.1 Requirements Overview . . . 9
2.2 Engine Host . . . 10
2.3 File Content . . . 10
2.4 Microsoft 365 . . . 11
2.5 File System Agents . . . 11
2.6 Database Planning . . . 11
2.6.1 Determine a Database Type . . . 11
2.6.2 Use a Dedicated Server . . . 12
2.6.3 Use a Dedicated Database Instance . . . 12
2.6.4 Provide Sufficient I/O Bandwidth . . . 12

**3 Product Licensing** 15

3.1 Obtaining a Product Activation Key . . . 15
3.2 Obtaining a License File . . . 15
3.3 Installing the License . . . 15

**4 Database Instance Configuration** 17

4.1 PostgreSQL . . . 17
4.1.1 Minimum Requirements . . . 17
4.1.2 Installing and Configuring the PostgreSQL Database . . . 18
4.2 Microsoft SQL Server . . . 18
4.2.1 Minimum Requirements . . . 18
4.2.2 Prerequisites . . . 18
4.2.3 Installing a New Instance of SQL Server . . . 19
4.2.4 Post Configuration Considerations . . . 23

**5 Installing and Configuring RabbitMQ** 25

5.1 Upgrading a Previous Installation . . . 25
5.2 Extracting RabbitMQ . . . 25

5.3 Creating Certificates for RabbitMQ . . . . . 26
5.4 Installing the Rabbit MQ Service . . . . . 29
5.5 Changing the Administrator Password . . . . . 30

**6 Core Components 33**

6.1 Prerequisites . . . . . 33
6.2 Engine Minimum Requirements . . . . . 33
6.3 Installing the Engine . . . . . 34
6.4 Configuring the Database . . . . . 35
6.5 Installing the License . . . . . 39
6.6 Configuring the Engine . . . . . 40
6.7 Configuring the Message Broker . . . . . 45
6.8 Configuring the Web Application . . . . . 48

**7 File System Scans 57**

7.1 Minimum Requirements . . . . . 57
7.2 Installing and Configuring AgentFS . . . . . 57

**8 File Content Scans 65**

8.1 ManagerFC . . . . . 65
8.1.1 Minimum Requirements . . . . . 65
8.1.2 Installation and Configuration . . . . . 65
8.2 AgentFC . . . . . 70
8.2.1 Minimum Requirements . . . . . 71
8.2.2 Installation and Configuration . . . . . 71

**9 Microsoft 365 Integration 77**

9.1 Prerequisites . . . . . 77
9.1.1 Message Broker . . . . . 77
9.1.2 Preparing the Microsoft 365 Tenant . . . . . 77
9.2 Agent365 . . . . . 83
9.2.1 Minimum Requirements . . . . . 83
9.2.2 Installation and Configuration . . . . . 84

# About This Guide


- Chapter 1, “Upgrading from a Previous Version,” on page 7
- Chapter 2, “Deployment Planning,” on page 9
- Chapter 3, “Product Licensing,” on page 15
- Chapter 4, “Database Instance Configuration,” on page 17
- Chapter 5, “Installing and Configuring RabbitMQ,” on page 25
- Chapter 6, “Core Components,” on page 33
- Chapter 7, “File System Scans,” on page 57
- Chapter 8, “File Content Scans,” on page 65
- Chapter 9, “Microsoft 365 Integration,” on page 77


This installation guide is written to provide network administrators the conceptual and procedural information for installing and configuring Micro Focus File Reporter 4.1.

## 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.

## Documentation Updates

For the most recent version of the *Micro Focus File Reporter 4.1 Installation Guide*, visit https://microfocus.com/documentation/file-reporter.

## Additional Documentation

For additional Micro Focus File Reporter 4.1 documentation, see the following guides at the Micro Focus File Reporter Documentation Web site

- *Micro Focus File Reporter 4.1 Administration Guide*
- *Micro Focus File Reporter 4.1 Client Tools Guide*
- *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*

# 1 Upgrading from a Previous Version


- Section 1.1, “Database,” on page 7
- Section 1.2, “License,” on page 7
- Section 1.3, “Core Components,” on page 7
- Section 1.4, “Microsoft 365 Reporting,” on page 8
- Section 1.5, “Agents,” on page 8


You can upgrade from any version of File Reporter 3.5 or greater by installing the updated software on top of the existing software.

New optional Microsoft 365 scanning components include Agent365 and possibly the RabbitMQ message broker if not currently configured for File Content scanning.

## 1.1 Database

File Reporter 4.1 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, “PostgreSQL,” on page 17.

For information on File Reporter supported versions of SQL Server, see Section 4.2, “Microsoft SQL Server,” on page 18.

## 1.2 License

Upgrading from a previous version of File Reporter requires a version 4 license. For procedures on updating the license, see Chapter 3, “Product Licensing,” on page 15.

## 1.3 Core Components

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 6, “Core Components,” on page 33

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 Chapter 8, “File Content Scans,” on page 65.

## 1.4 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.

## 1.5 Agents


- Section 1.5.1, “File System Agents,” on page 8
- Section 1.5.2, “File Content Agents,” on page 8
- Section 1.5.3, “Microsoft 365 Agent,” on page 8


File Reporter 4.1 includes three Agent types:

- File System
- File Content
- Microsoft 365

### 1.5.1 File System Agents

The file system agent AgentFS, formerly known simply as the Agent, is now referred to as the File System Agent to distinguish it from the File Content Agent introduced in File Reporter 3.5.

AgentFS examines and collects file system metadata and permissions for NTFS and CIFS-compatible file systems.

### 1.5.2 File Content Agents

File Reporter includes AgentFC, the File Content agent. This agent performs file content scanning on files stored in NTFS and CIFS-compatible file systems.

If you plan to utilize file content scanning you will need to install File Content Agents as part of the upgrade process. For more information, see Chapter 8, “File Content Scans,” on page 65.

### 1.5.3 Microsoft 365 Agent

Agent365, the Microsoft 365 scan agent, is responsible for scanning the metadata and permissions of files and folders stored in OneDrive for Business, SharePoint Online document libraries, and Teams document libraries.

This agent is new with File Reporter 4.1. For more information, see Section 8.2, “AgentFC,” on page 70.

# 2 Deployment Planning


- Section 2.1, “Requirements Overview,” on page 9
- Section 2.2, “Engine Host,” on page 10
- Section 2.3, “File Content,” on page 10
- Section 2.4, “Microsoft 365,” on page 11
- Section 2.5, “File System Agents,” on page 11
- Section 2.6, “Database Planning,” on page 11


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.

## 2.1 Requirements Overview

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

| Technology | Notes |
|---|---|
| Windows and 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 Application is an ASP.NET application that runs in conjunction with IIS.<br><br>The installer and configuration utilities automatically configure IIS and manage most aspects of the installation for you.<br><br>The Engine and Web Application must run on the same system in this release of the software. |
| DNS | In order to access the File Reporter Web Application with a browser, the web site name as registered with IIS must be used. In other words, the raw IP address does not work.<br><br>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 | 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.<br><br>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. |
| Messaging Broker | To enable messaging between File Reporter components that are needed for file content scanning (ManagerFC and AgentFC) or Microsoft 365 scanning (Agent365), File Reporter utilizes the RabbitMQ message broker. |

## 2.2 Engine Host

- The server hosting the Engine service 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 2022
  - 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 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 United States 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:

- ManagerFC
- AgentFC
- RabbitMQ message broker

For more details on file content scanning, see

## 2.4 Microsoft 365

With the release of File Reporter 4.1, 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:

- Agent365
- RabbitMQ message broker

## 2.5 File System Agents

| Target System | Local Scan | Proxy Scan |
|---|---|---|
| Windows Server | Yes | Yes |
| Network Attached Storage (NAS) Device (CIFS-based) | No | Yes |

When you decide whether to install AgentFS locally on a Windows server, or to have the AgentFS service run as 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.

## 2.6 Database Planning


- Section 2.6.1, “Determine a Database Type,” on page 11
- Section 2.6.2, “Use a Dedicated Server,” on page 12
- Section 2.6.3, “Use a Dedicated Database Instance,” on page 12
- Section 2.6.4, “Provide Sufficient I/O Bandwidth,” on page 12


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

### 2.6.1 Determine a Database Type

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.

### 2.6.2 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, “PostgreSQL,” on page 17.
- For minimum requirements for a SQL Server host, see Section 4.2, “Microsoft SQL Server,” on page 18.

### 2.6.3 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 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.

### 2.6.4 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 Product Licensing


- Section 3.1, “Obtaining a Product Activation Key,” on page 15
- Section 3.2, “Obtaining a License File,” on page 15
- Section 3.3, “Installing the License,” on page 15


This section provides procedures for obtaining and installing a production license.

## 3.1 Obtaining a Product Activation Key

1. In a web browser, go to https://www.microfocus.com/customercenter.
2. Enter you 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.

## 3.3 Installing the License

Use the File Reporter Configuration Dashboard to install or update the license.

---

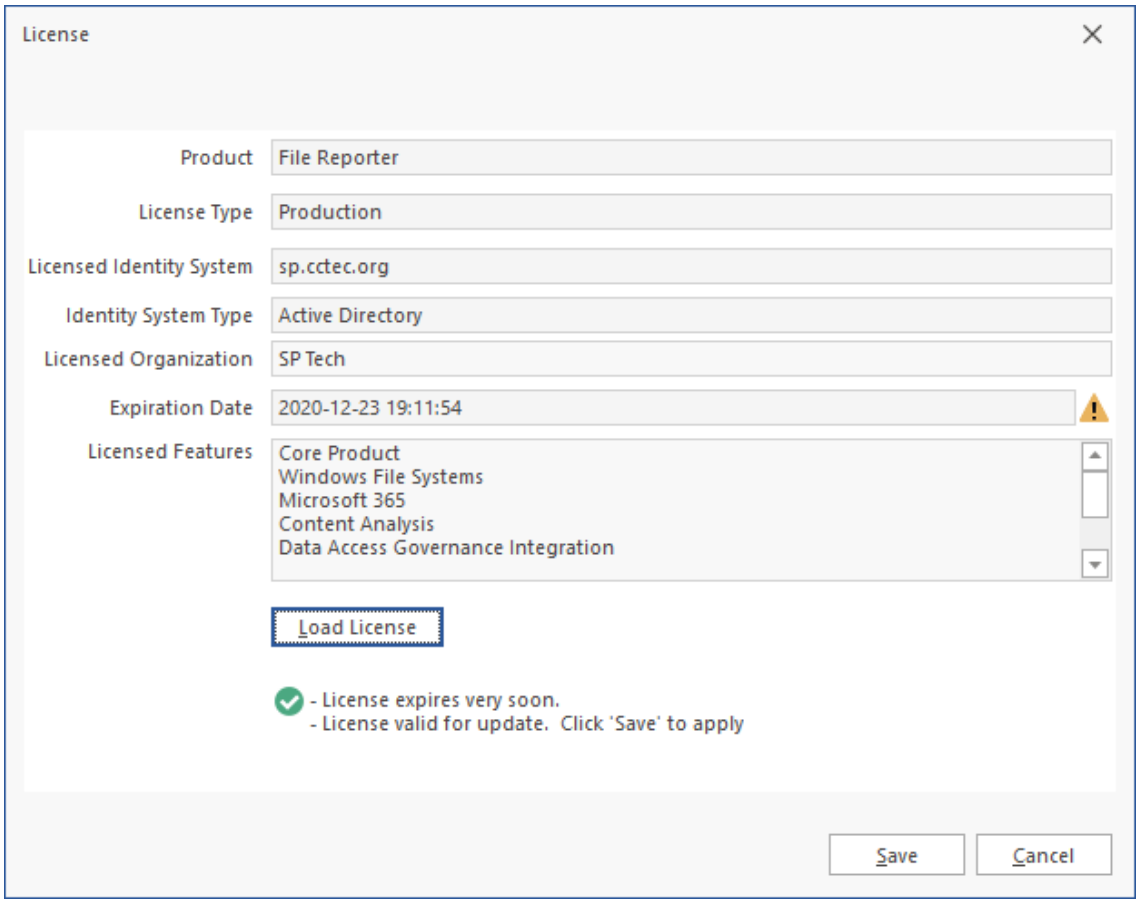
**IMPORTANT:** License expiration checks are done every 24 hours at midnight.

When the license expires, you cannot log in through the 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. In the File Reporter Configuration Dashboard, click **Install or Update Licensing**.

   A page similar to the following appears:




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

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

The license details will appear in the **License** panel.

5 Click **Close**.

# 4 Database Instance Configuration


- Section 4.1, “PostgreSQL,” on page 17
- Section 4.2, “Microsoft SQL Server,” on page 18


This section provides links to procedures for installing and configuring PostgreSQL or Microsoft SQL Server.

Before continuing this section, decide on a database type for use with File Reporter following the guidance provided in Section 2.6, “Database Planning,” on page 11.

## 4.1 PostgreSQL


- Section 4.1.1, “Minimum Requirements,” on page 17
- Section 4.1.2, “Installing and Configuring the PostgreSQL Database,” on page 18


### 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

  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.

## 4.2 Microsoft SQL Server


- Section 4.2.1, “Minimum Requirements,” on page 18
- Section 4.2.2, “Prerequisites,” on page 18
- Section 4.2.3, “Installing a New Instance of SQL Server,” on page 19
- Section 4.2.4, “Post Configuration Considerations,” on page 23


### 4.2.1 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.

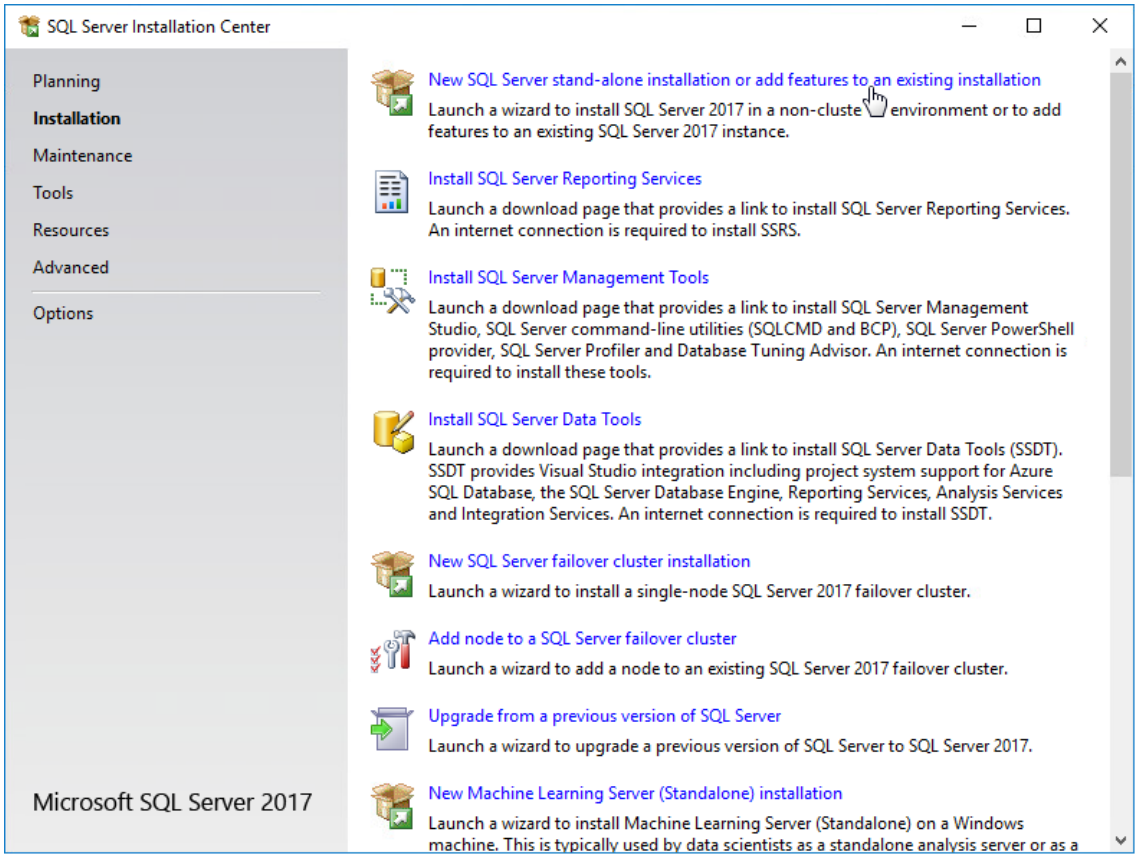
### 4.2.2 Prerequisites

Verify that you have installed the latest SQL Server updates prior to running the File Reporter Database Configuration utility.

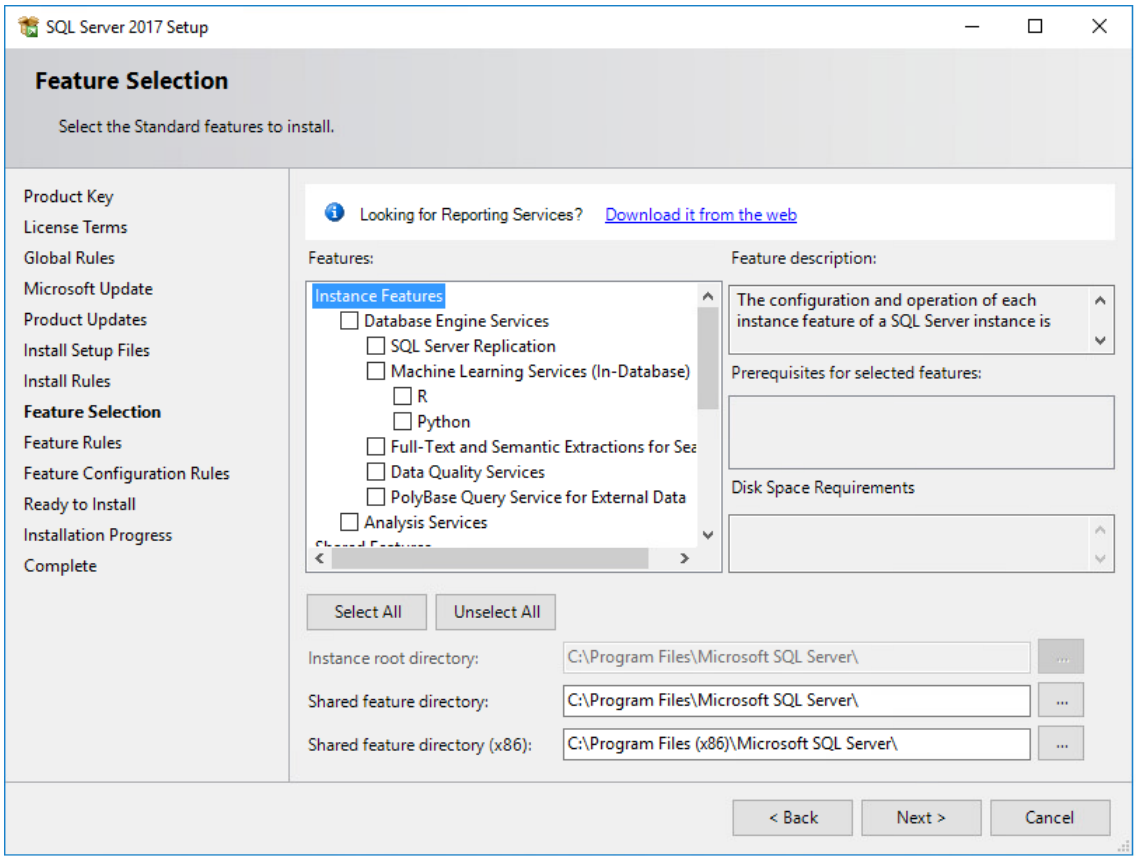
## 4.2.3 Installing a New Instance of SQL Server

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**.




4. When the Setup Support Rules operation is complete, 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**.
8. When the Setup Support Rules operation has completed, click **Next**.




9 On the Feature Selection page, select **Database Engine Services**.

10 Optionally specify custom paths or use the defaults for the installation paths, 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.

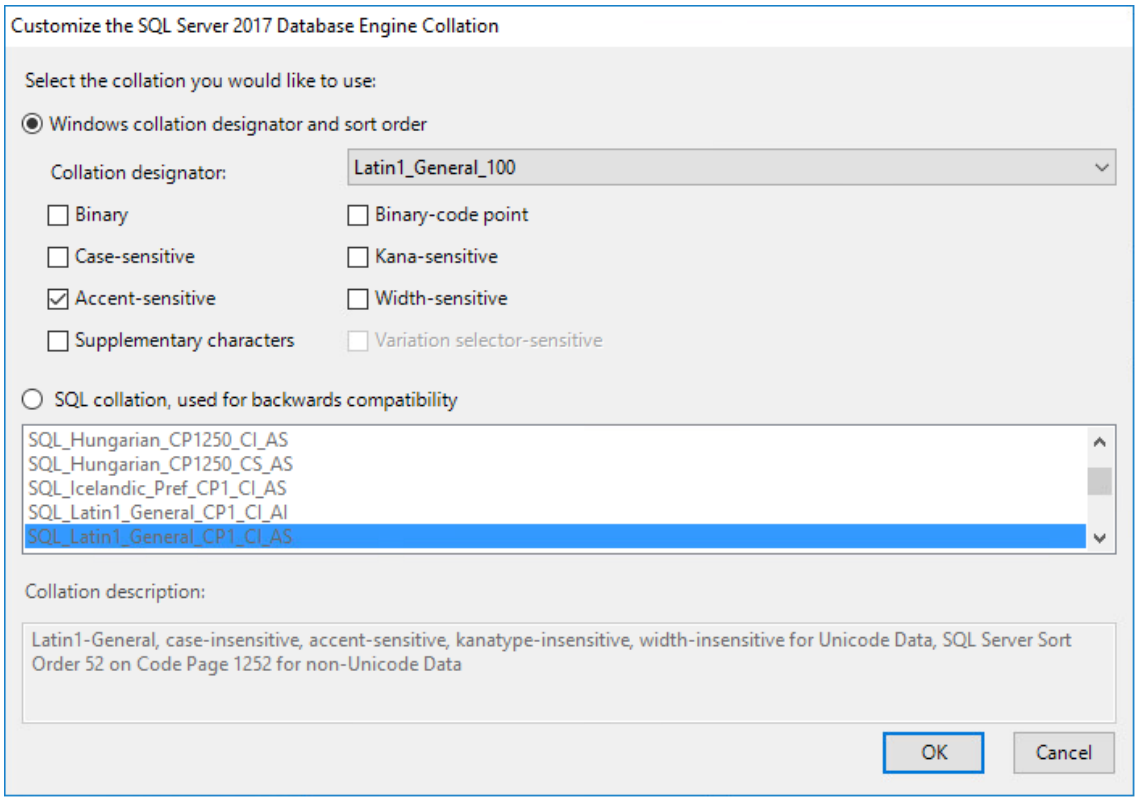
We recommend that you select a collation that aligns with the Windows locale of the server where the Engine is installed.

For more information on collation and locales, refer to https://docs.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support.

---

**IMPORTANT:** File Reporter 4.1 does not support the UTF-8 char/varchar storage options at this time.

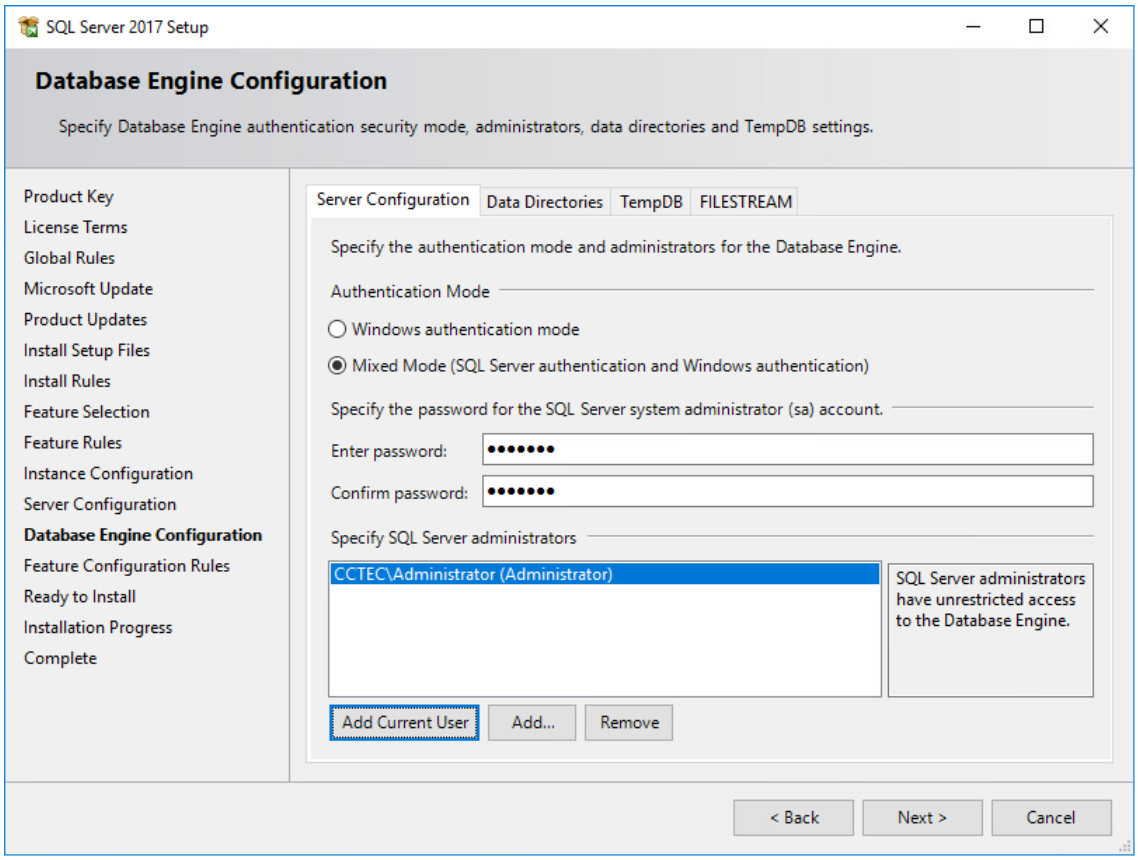
---




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**.

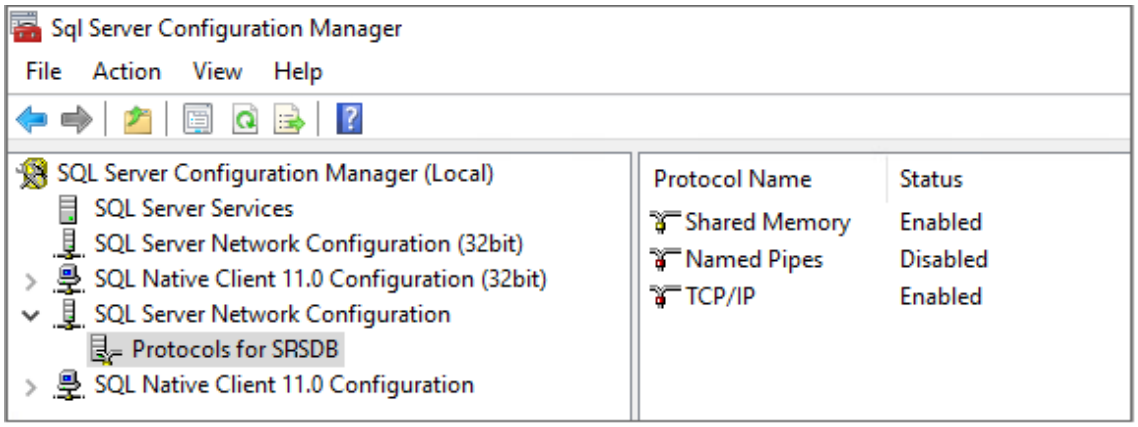
20 Click **Install**.

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 Select the **Protocol** tab.

27 Under the **Enabled** field, click the drop-down menu and select **Yes**.

28 Select the **IP Addresses** tab.

29 Under the **IPAll** heading, set the **TCP Port** field to an available port such as 1433.

30 For the **TCP Dynamic Ports** field, set the value to 0 (zero).

31 Click **Apply**.

32 When the warning dialog box appears, click **OK**.

33 Click **OK** to close the TCP/IP Properties window.

34 Close the SQL Server Configuration Manager.

---

**IMPORTANT:** Firewall rules on the server hosting SQL Server may need configuration to allow for TCP port access to the TCP port specified during configuration.

---

### 4.2.4 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.

# 5 Installing and Configuring RabbitMQ


- Section 5.1, “Upgrading a Previous Installation,” on page 25
- Section 5.2, “Extracting RabbitMQ,” on page 25
- Section 5.3, “Creating Certificates for RabbitMQ,” on page 26
- Section 5.4, “Installing the Rabbit MQ Service,” on page 29
- Section 5.5, “Changing the Administrator Password,” on page 30


RabbitMQ is an open-source message broker that enables messaging between 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: https://www.rabbitmq.com/download.html.

To assist with the introduction of RabbitMQ into the 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.

## 5.1 Upgrading a Previous Installation

File Reporter introduced file content scanning in version 3.5 and subsequently introduced the RabbitMQ message broker as a 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.

## 5.2 Extracting RabbitMQ

1. Install the Visual C++ Redistributable Packages for Visual Studio 2015.

The Erlang runtime for RabbitMQ requires a recent version of the Visual C++ Redistributable Package for Visual Studio 2015. 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://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170 or in the RabbitMQ folder of the image named `vc-redist-vs2015-2022-x64-*.exe`.

2 In the `RabbitMQ` folder of the image, unzip the `RabbitMQ-3.9.x.zip` file to your desired path.

The path cannot contain spaces. The zip file contains the `rabbitmq` folder, so extracting to the root of `C:\`, for example, would produce an install location of `C:\rabbitmq`.

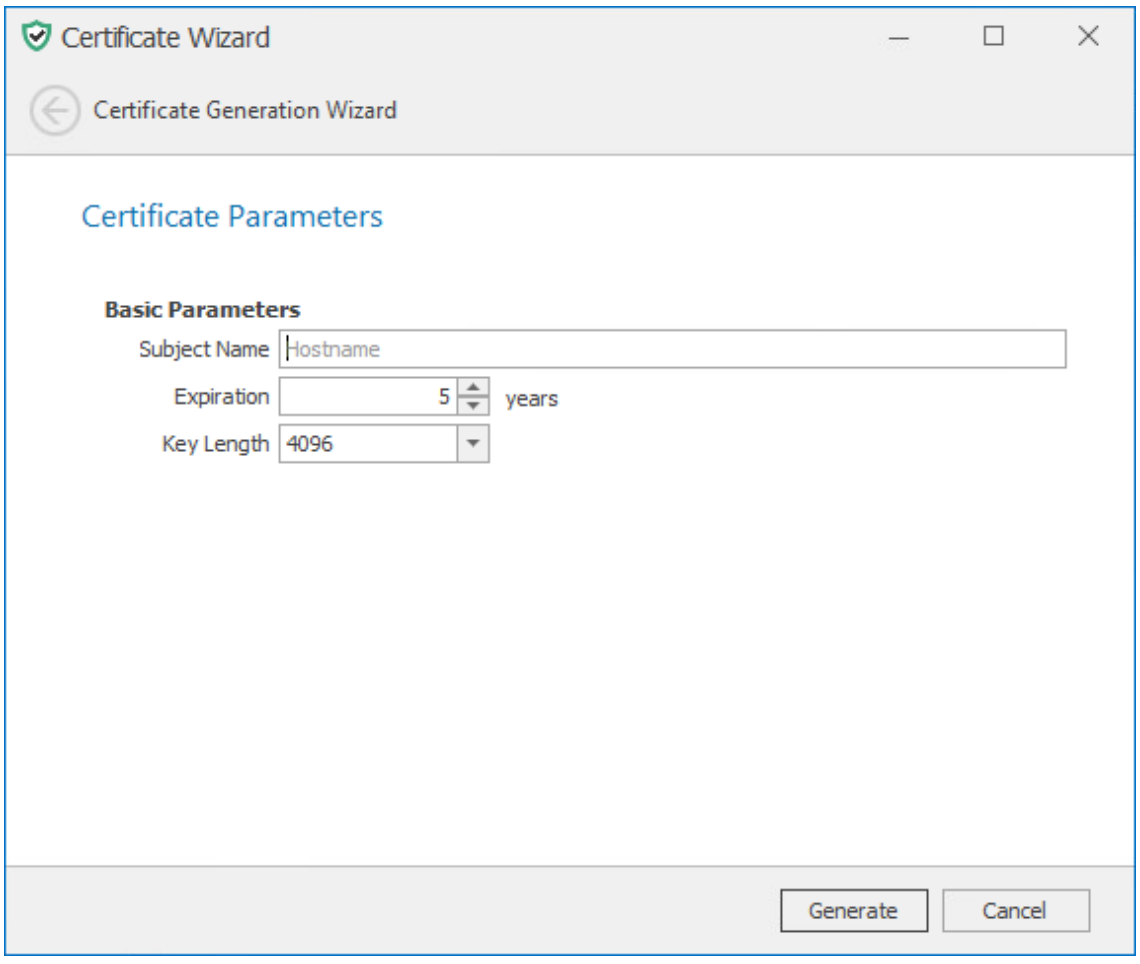
## 5.3 Creating Certificates for RabbitMQ

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

1 (Conditional) If you have not already done so, install the 64-bit .NET 6.0 Desktop Runtime.

A copy of the Desktop Runtime installer is located in the `RabbitMQ` folder of the ISO image or may be downloaded from https://dotnet.microsoft.com/en-us/download/dotnet/6.0.

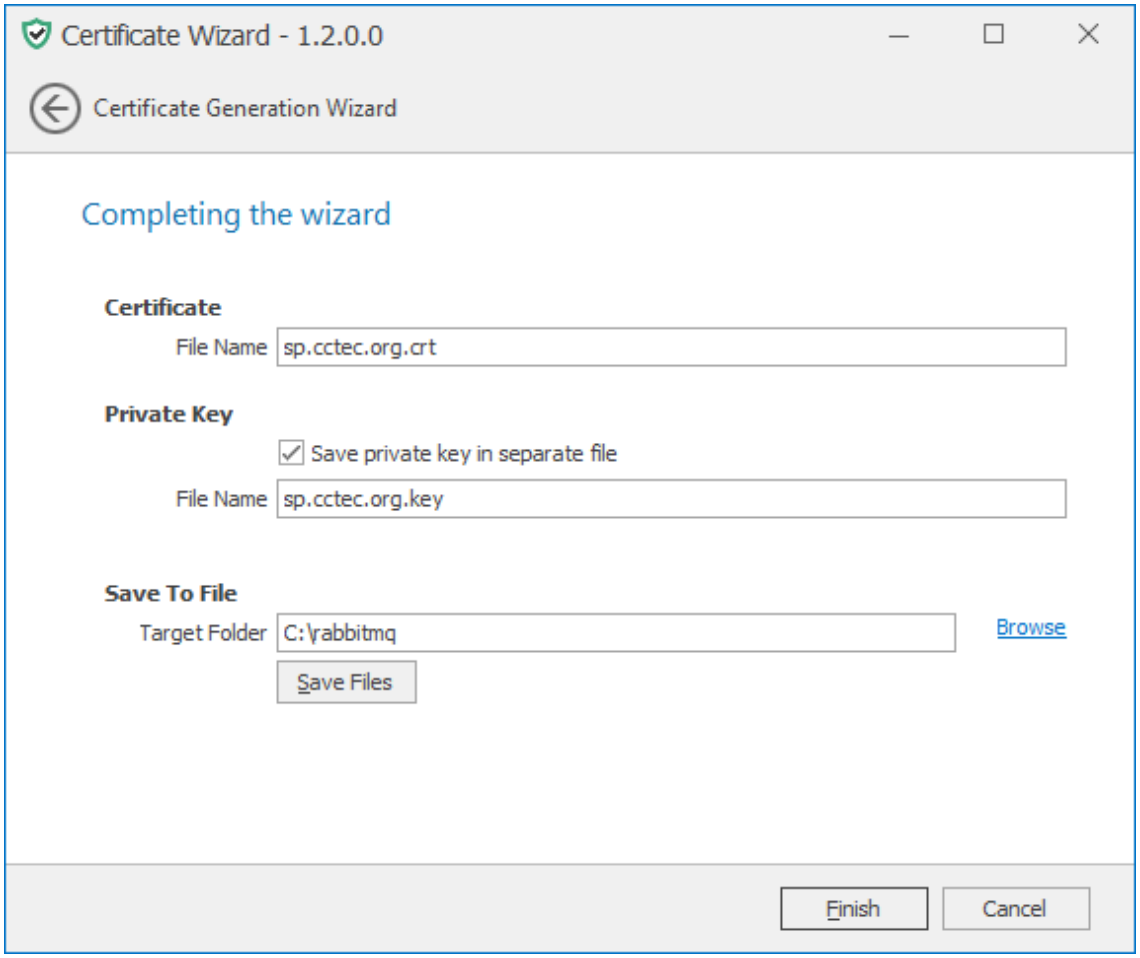
2 In the `RabbitMQ` folder of the ISO image, double-click `CertificateGenerator.exe`.



3 In the **Subject Name** field, enter the DNS for the RabbitMQ service host or endpoint.

4 (Optional) Modify the settings in the other fields.

5 Click **Generate**.




6 In the **Certificate** section of the **File Name** field, enter the desired name of the certificate file to export.

7 (Optional) In the **Private Key** section, select **Save private key in separate file**, then enter a value for **File Name** for the private key file to export.

8 In the **Save to File** section, browse to or enter a path for **Target Folder** where the certificate and key file(s) will be exported.

---

**IMPORTANT:** The path should not contain spaces. As a general recommendation, export the certificate files to the root of the extracted `RabbitMQ` folder.

---

9 Click **Save Files** to export the files.

10 Click **Finish**.

11 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 extracted the `RabbitMQ-3.9.xx.zip` file.

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

13 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
```

14 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
management.ssl.versions.2
```

15 Specify the certificate and private key.

**15a** In the `TLS Options` section, modify the paths for `ssl_options.cacertfile` and `ssl_options.certfile` with the path to the certificate you created earlier in Steps 2-10.

**15b** While still in the `TLS Options` section, modify the path for `ssl_options.keyfile` with the path of the private key.

**15c** In the `Management Interface / REST API` section, modify the paths for `management.ssl.cacertfile` and `management.ssl.certfile` with the path to the certificate.

Note that paths are absolute and use forward slashes.

**15d** While still in the `Management Interface / REST API` section, modify the path for `management.ssl.keyfile` with the path of the private key.

```
# ------------------------------
# TLS Options
# ------------------------------

ssl_options.cacertfile    = c:/rabbitmq/cert.pem
ssl_options.certfile      = c:/rabbitmq/cert.pem
ssl_options.keyfile       = c:/rabbitmq/key.pem
num_acceptors.ssl         = 10
listeners.ssl.default     = 5671


# ------------------------------
# Management Interface / REST API
# ------------------------------
## See https://rabbitmq.com/management.html and https://rabbitmq.com/ssl.html for details.

#management.tcp.ip           = 0.0.0.0
#management.tcp.port         = 15672
management.ssl.port         = 15671
management.ssl.cacertfile   = c:/rabbitmq/cert.pem
management.ssl.certfile     = c:/rabbitmq/cert.pem
management.ssl.keyfile      = c:/rabbitmq/key.pem
management.ssl.versions.1   = tlsv1.2
management.ssl.versions.2   = tlsv1.3
```

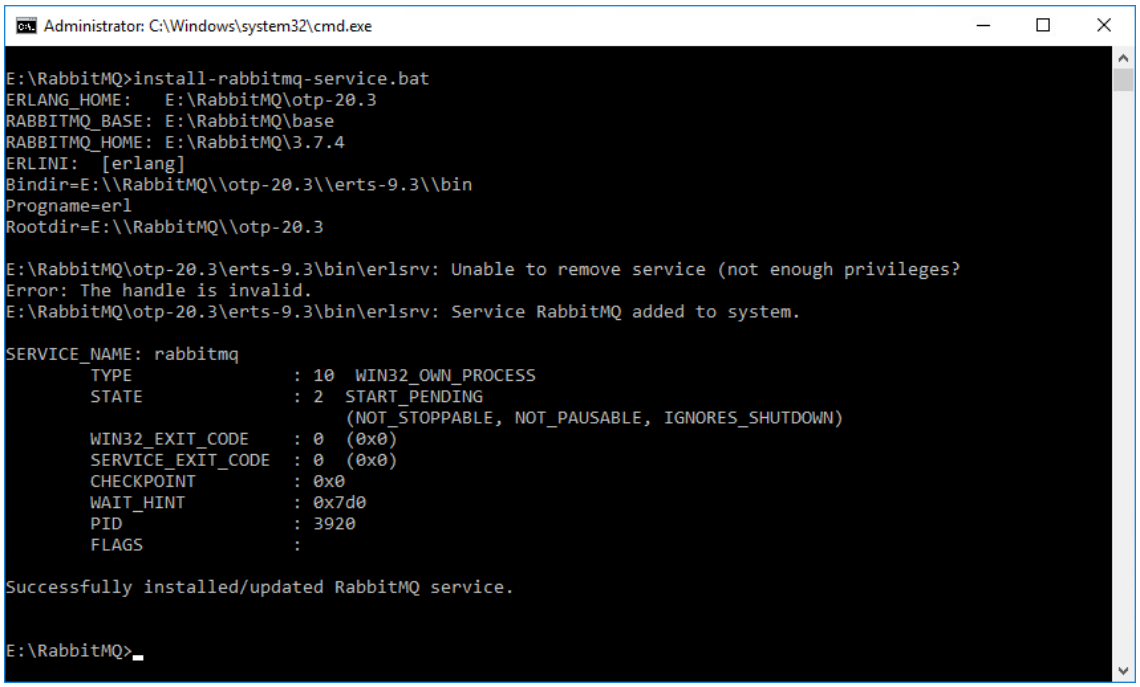
**16** Save the modifications you have made to the configuration file, then close the editor.

## 5.4 Installing the Rabbit MQ Service

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

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

The RabbitMQ service is now installed.




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.

## 5.5 Changing the Administrator Password

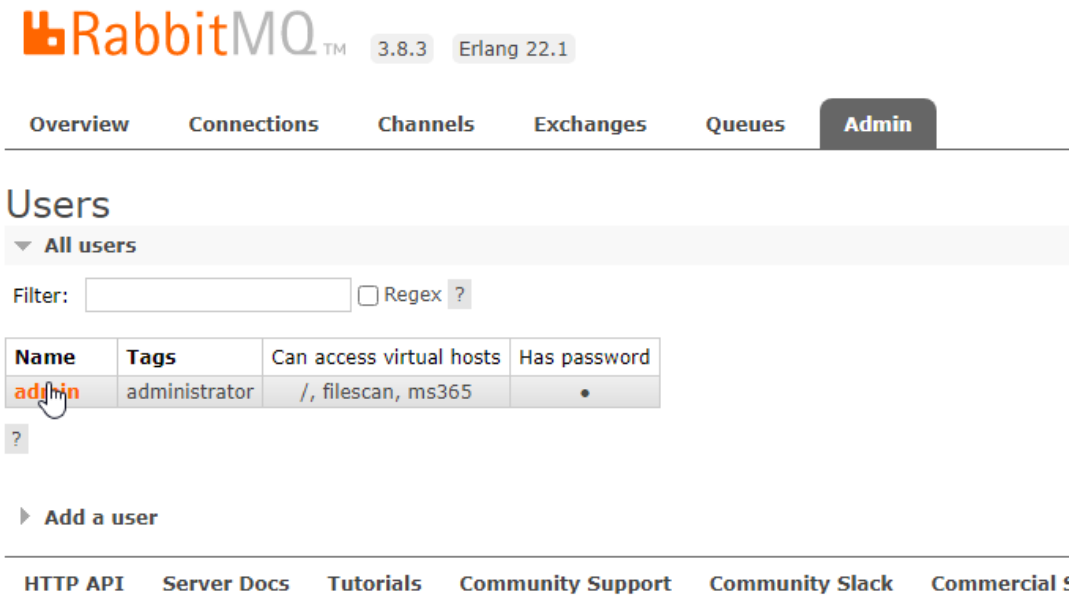
As a best practice, you should change the default administrator password for RabbitMQ before performing any administrative work.

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

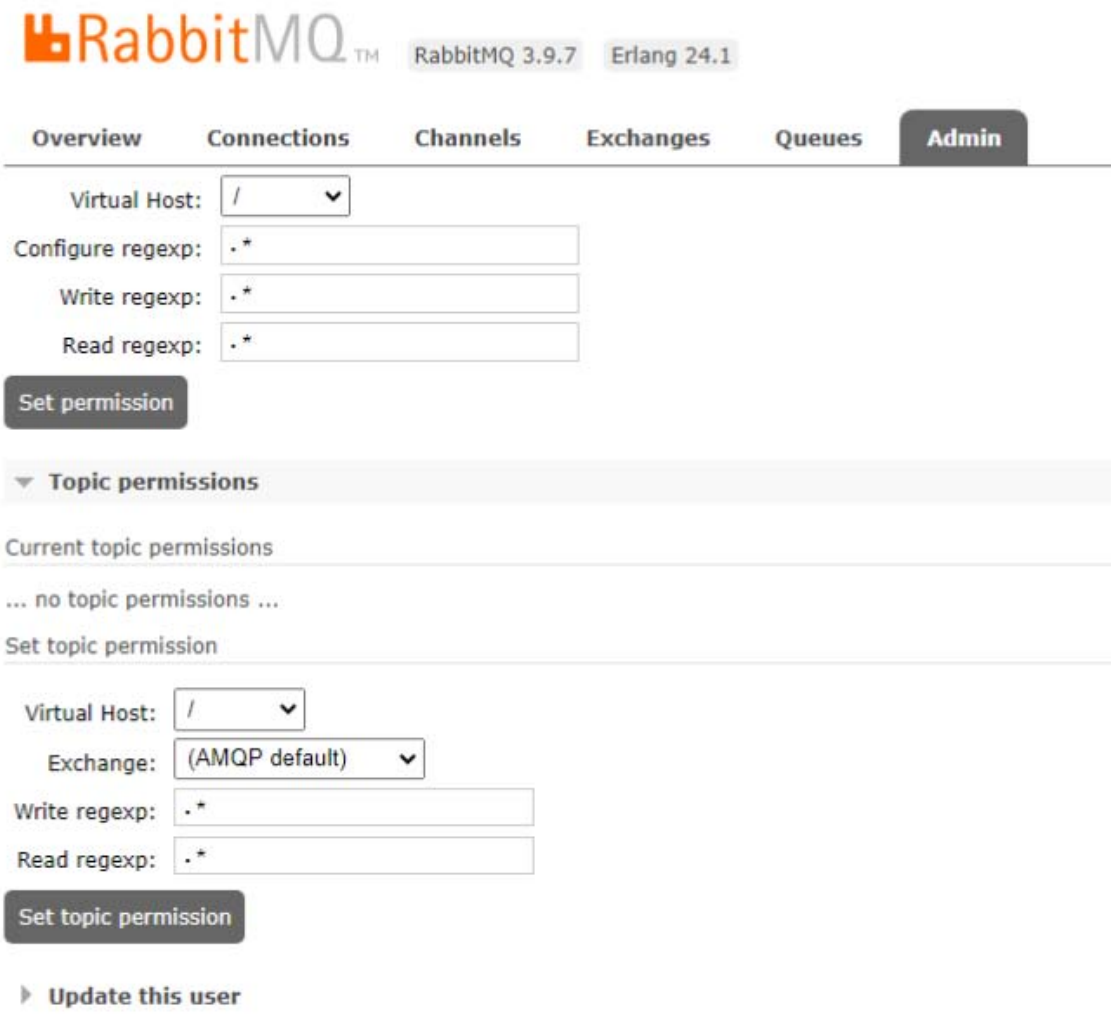
2 In the **Username** field, enter `admin`, in the **Password** field, enter `srsadmin`, then click **Login**.

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**.

# 6 Core Components


- Section 6.1, “Prerequisites,” on page 33
- Section 6.2, “Engine Minimum Requirements,” on page 33
- Section 6.3, “Installing the Engine,” on page 34
- Section 6.4, “Configuring the Database,” on page 35
- Section 6.5, “Installing the License,” on page 39
- Section 6.6, “Configuring the Engine,” on page 40
- Section 6.7, “Configuring the Message Broker,” on page 45
- Section 6.8, “Configuring the Web Application,” on page 48


File Reporter 4.1 is comprised of a set of base components including the Engine and Scan Processor, a database, and a Web Application. Installation and configuration for these components are presented in this section.

Depending on the service requirements, optional components for File Content scanning or Microsoft 365 environments include the requirement for a message broker. For details on installation and configuration of the RabbitMQ message broker, see Chapter 5, “Installing and Configuring RabbitMQ,” on page 25.

## 6.1 Prerequisites

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

  For example: webapp.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 5, “Installing and Configuring RabbitMQ,” on page 25.

## 6.2 Engine 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 2022

- Windows Server 2019
- Windows Server 2016

- Active Directory Requirements
  - The server must be joined to Active Directory
  - Minimum forest functional level of Windows 2003

## 6.3 Installing the Engine

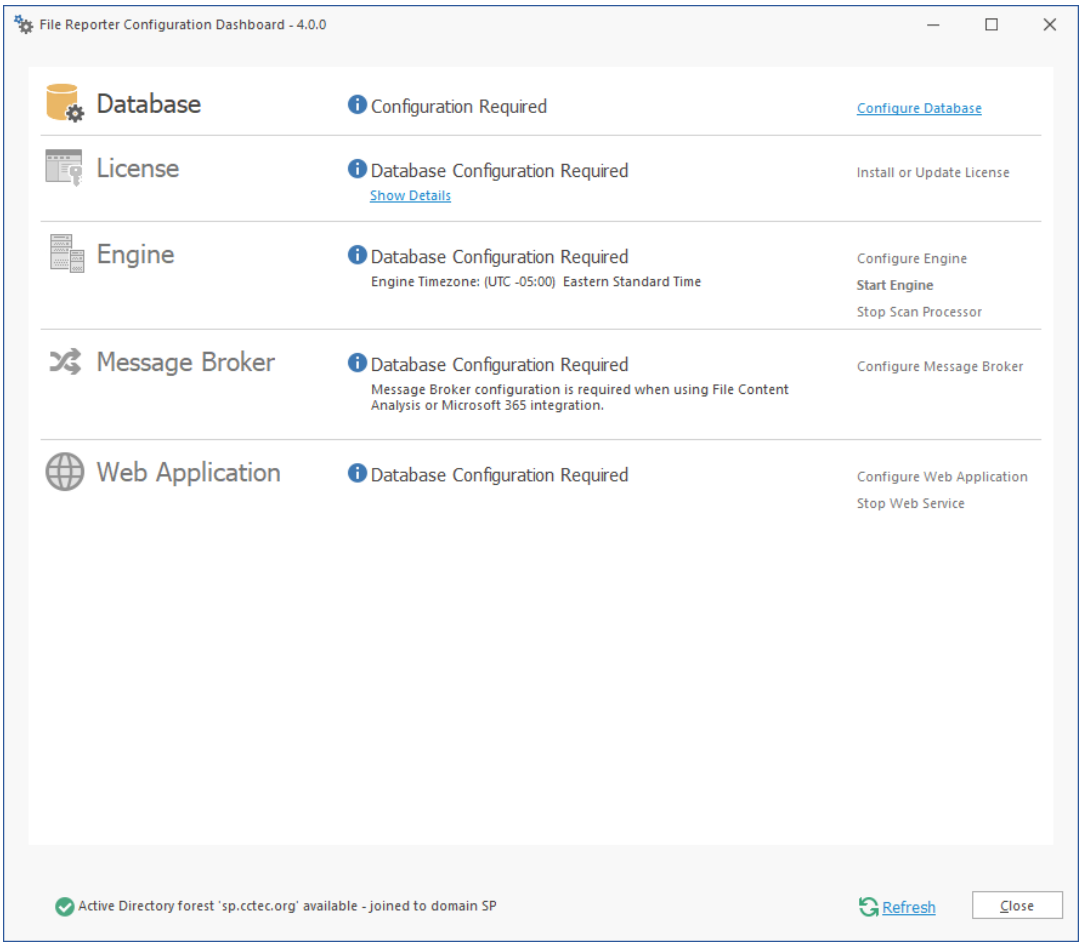
**IMPORTANT:** To successfully install the Engine, you must be logged in as a domain administrator for the domain the computer is a member of. If you are not, the rights are not sufficient.

1. At the root of the `FileReporter_4.1.iso` image, double-click `FileReporter-Engine-4.1-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**.

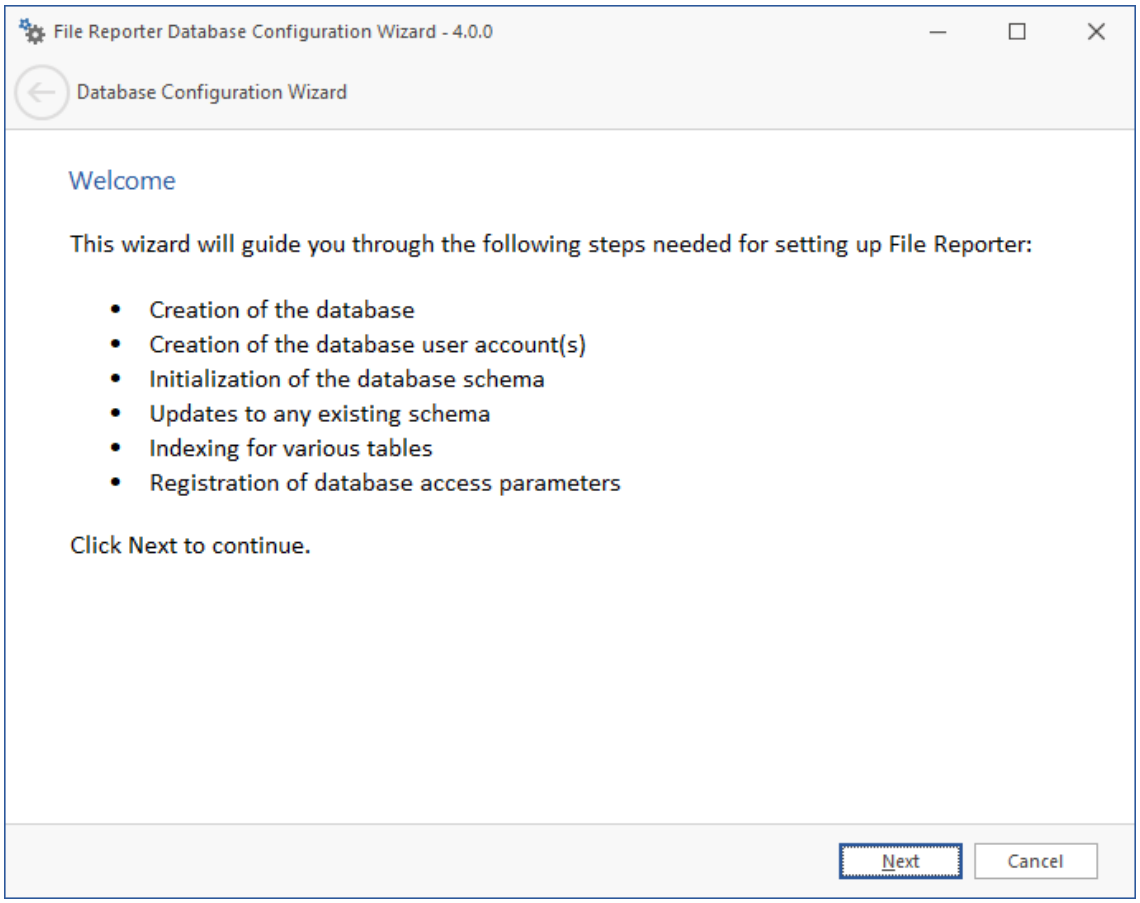
     The File Reporter Configuration Dashboard appears.



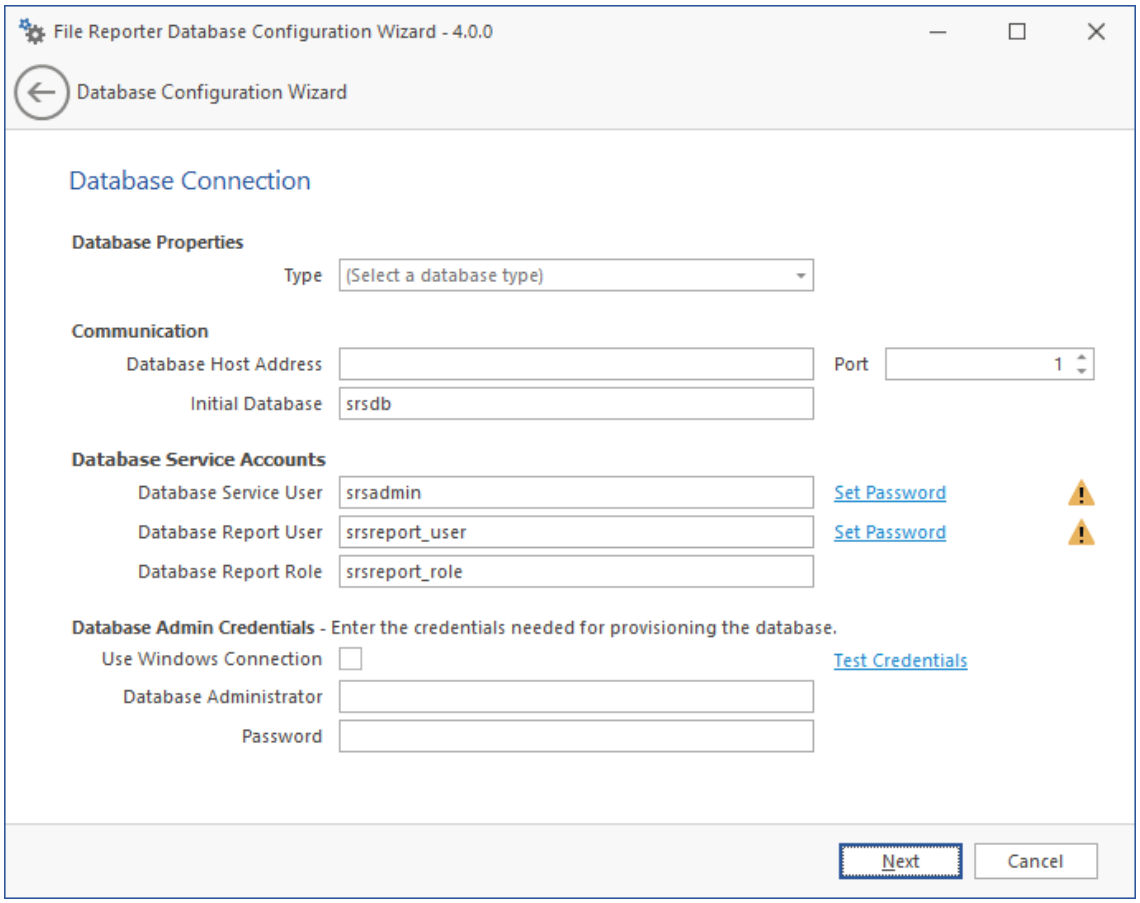

**NOTE:** Each step in the Configuration Utility should be run in sequential order from top to bottom. If you chose not to install RabbitMQ, you can skip the Message Broker section.

## 6.4 Configuring the Database

1 Click **Configure Database**.




**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.

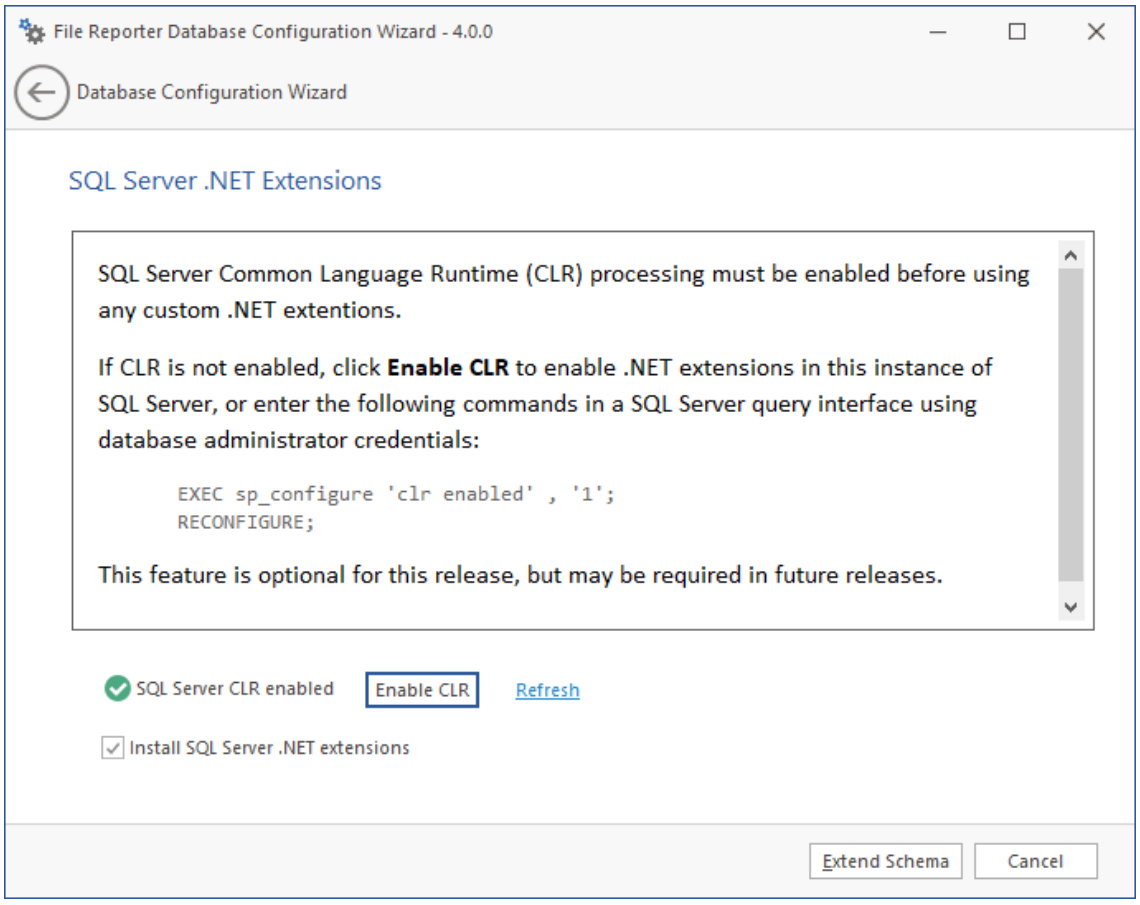
**Database Administrator:** If you are using PostgreSQL, specify the superuser name. If you are using SQL Server, specify the administrator name.

**Password:** If you are using a PostgreSQL, 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.

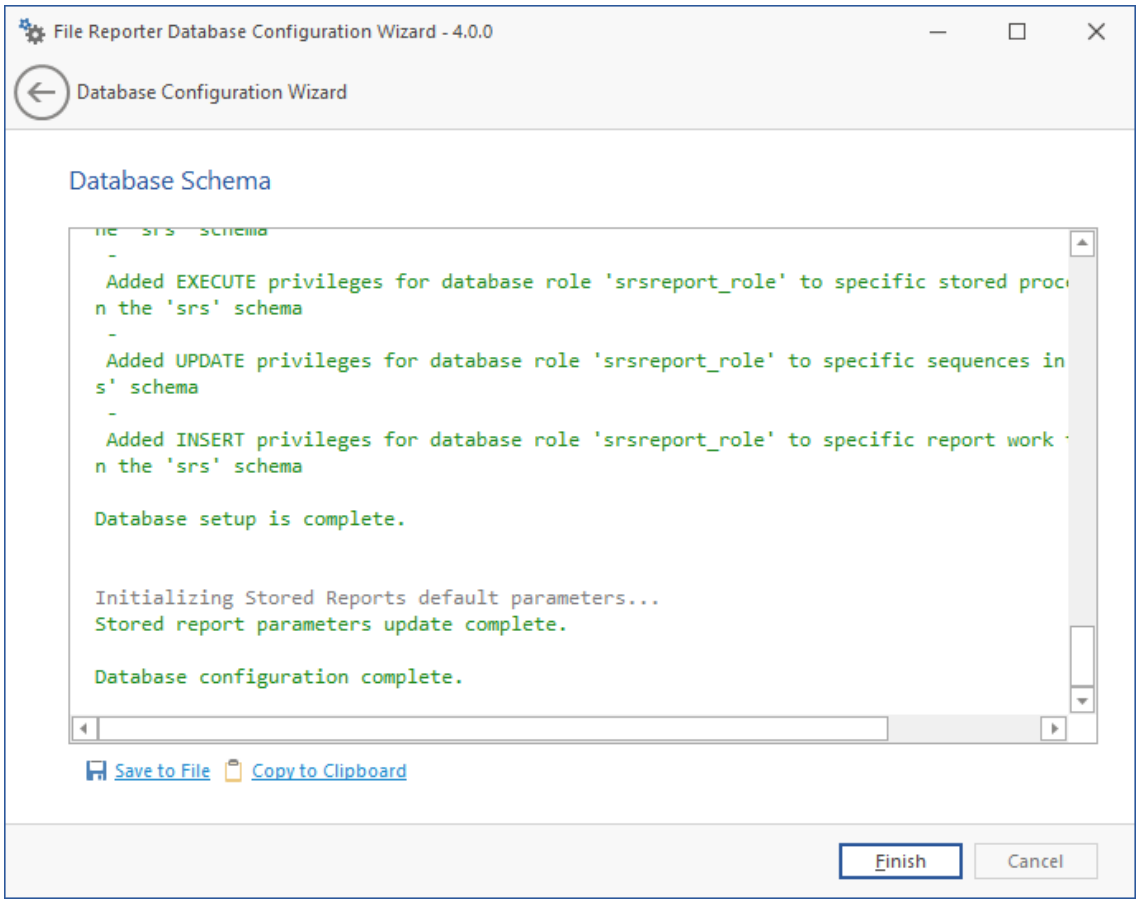
3 Complete the fields and click **Next**.

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**.

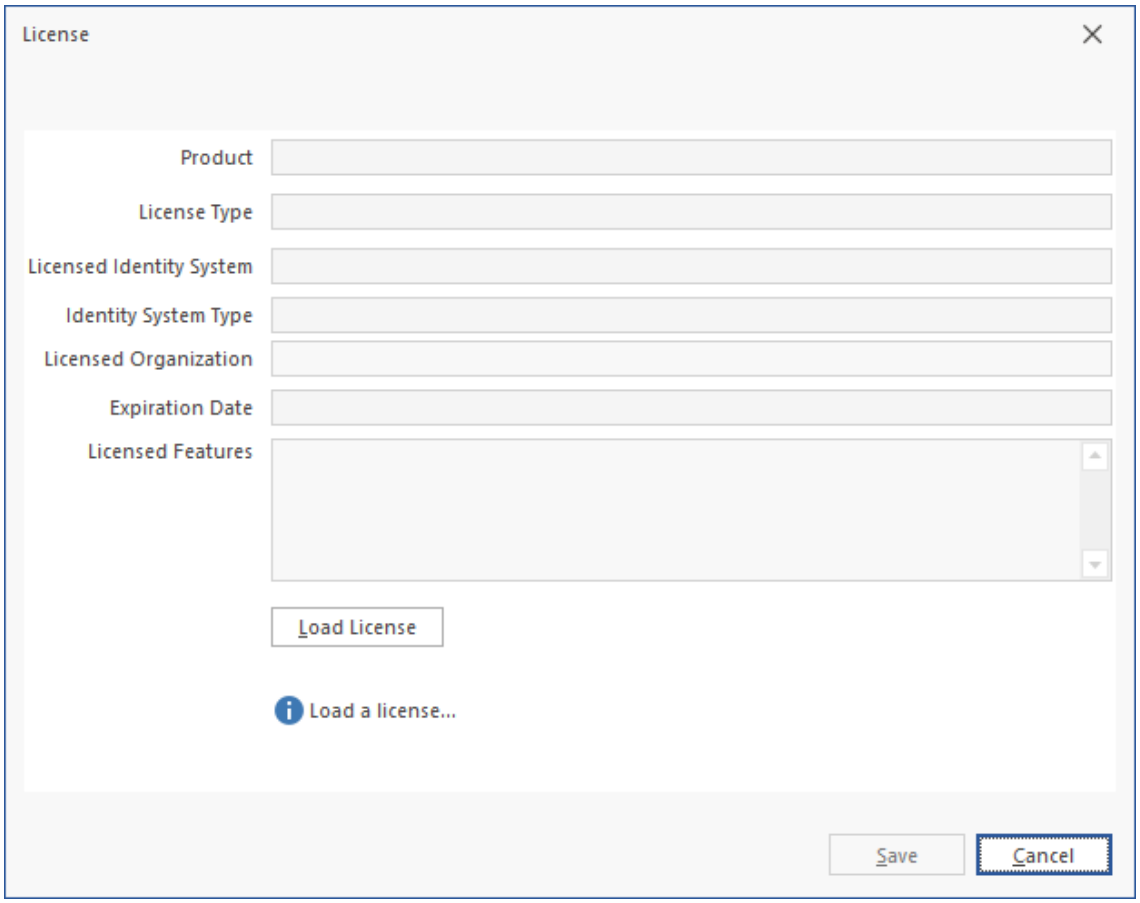



6 Review the configuration log and click **Finish**.

## 6.5 Installing the License

**NOTE:** For details on obtaining a license file, see Chapter 3, “Product Licensing,” on page 15.

1 Click **Install or Update License**.



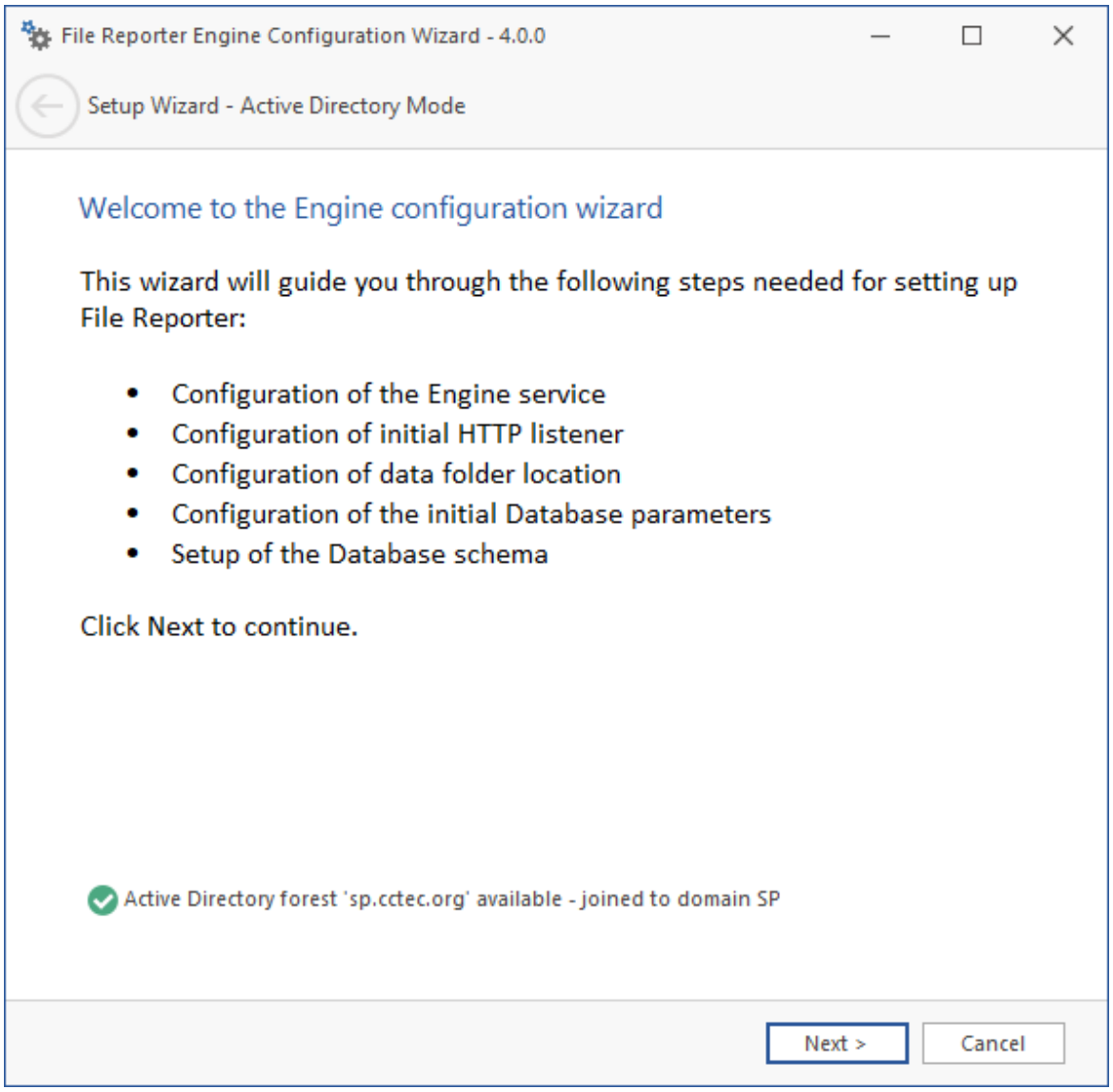

2 Click **Load License**, then browse to and select the license file.

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

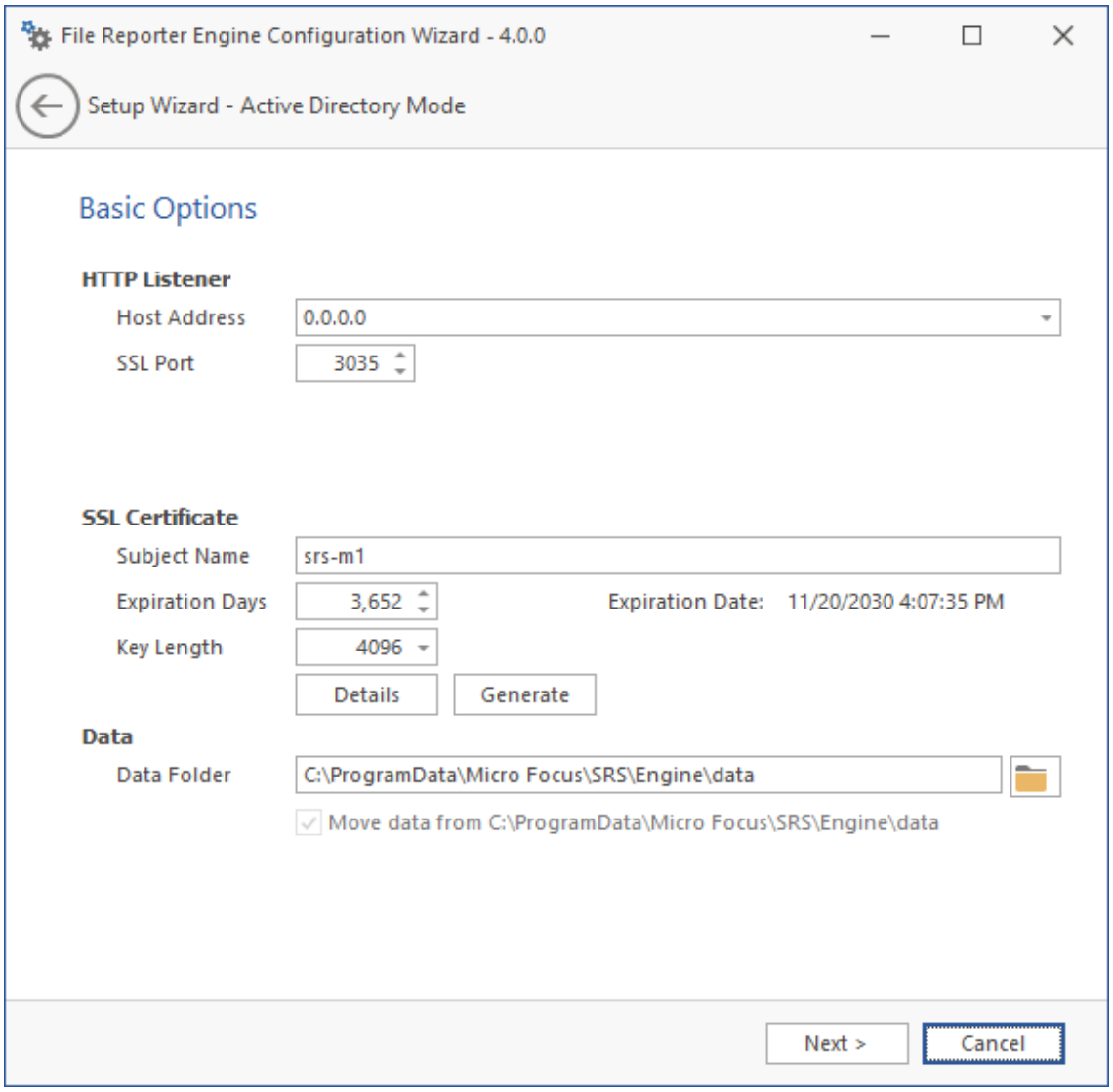
4 Click **Close**.

## 6.6 Configuring the Engine

1 Click **Configure Engine**.




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




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 with 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**.

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.

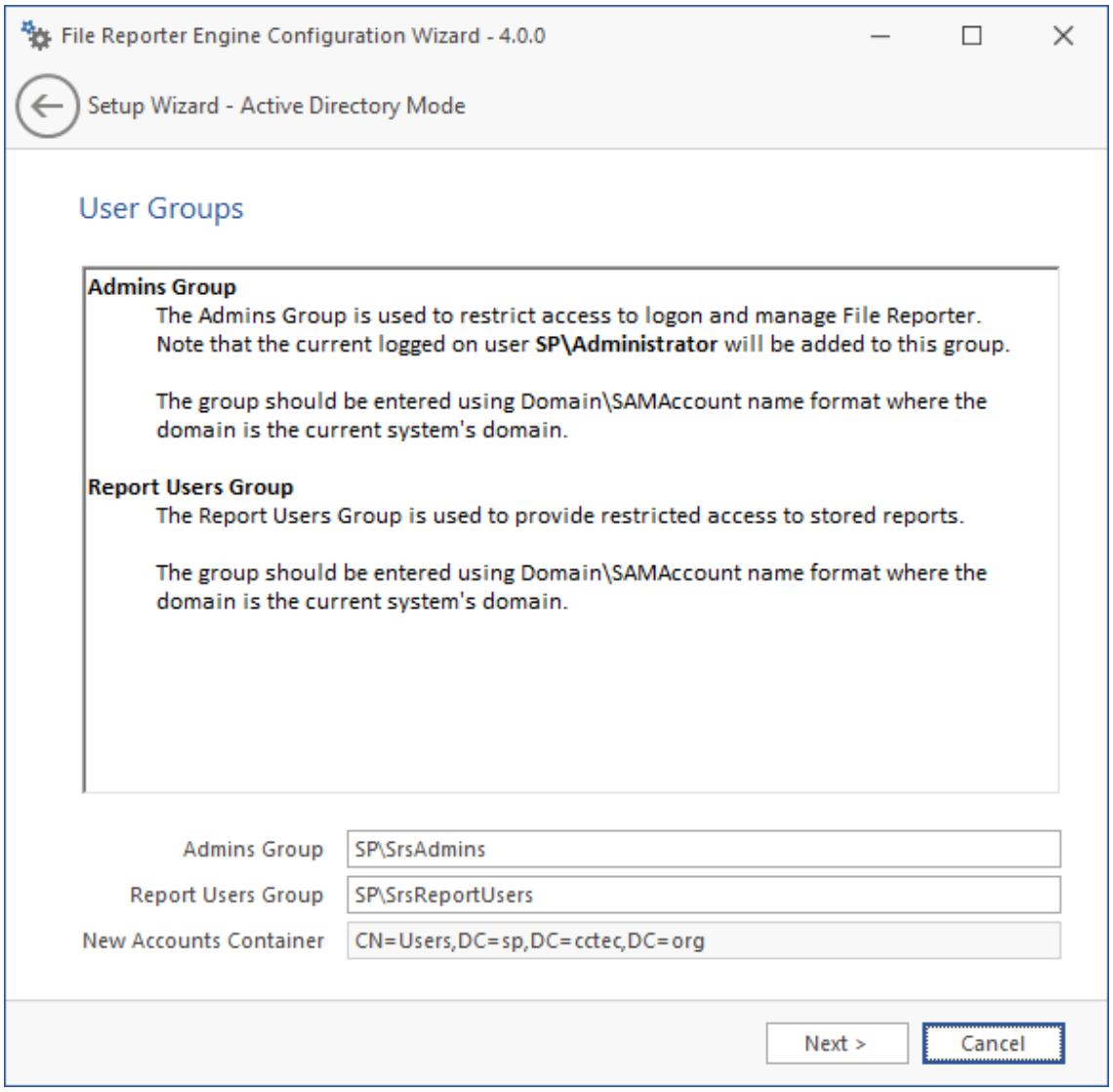
Clicking **Browse** allows you to place these object in a specified container other than `CN=Users`.

---

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

---

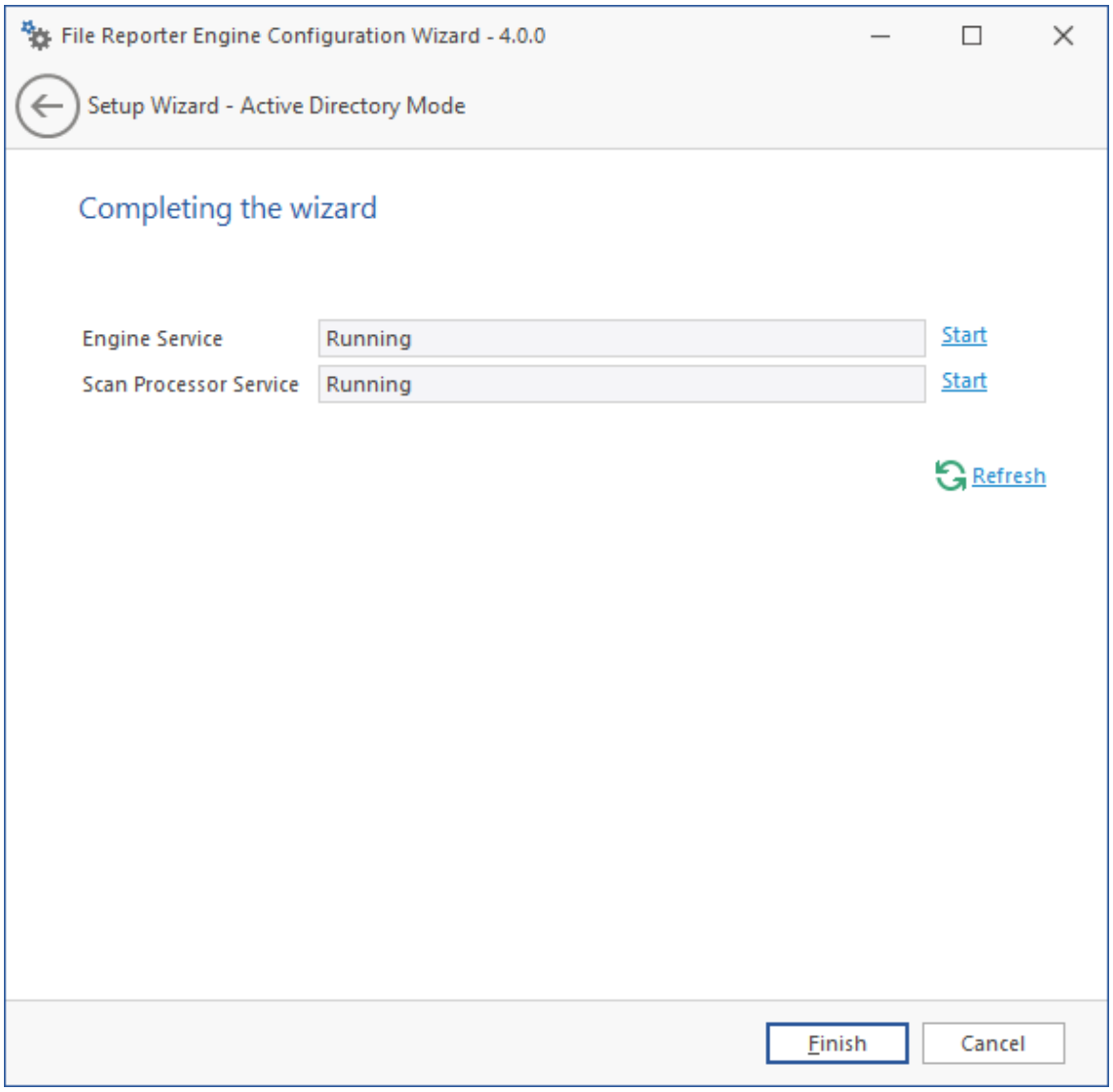
4 Click **Next**.




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.

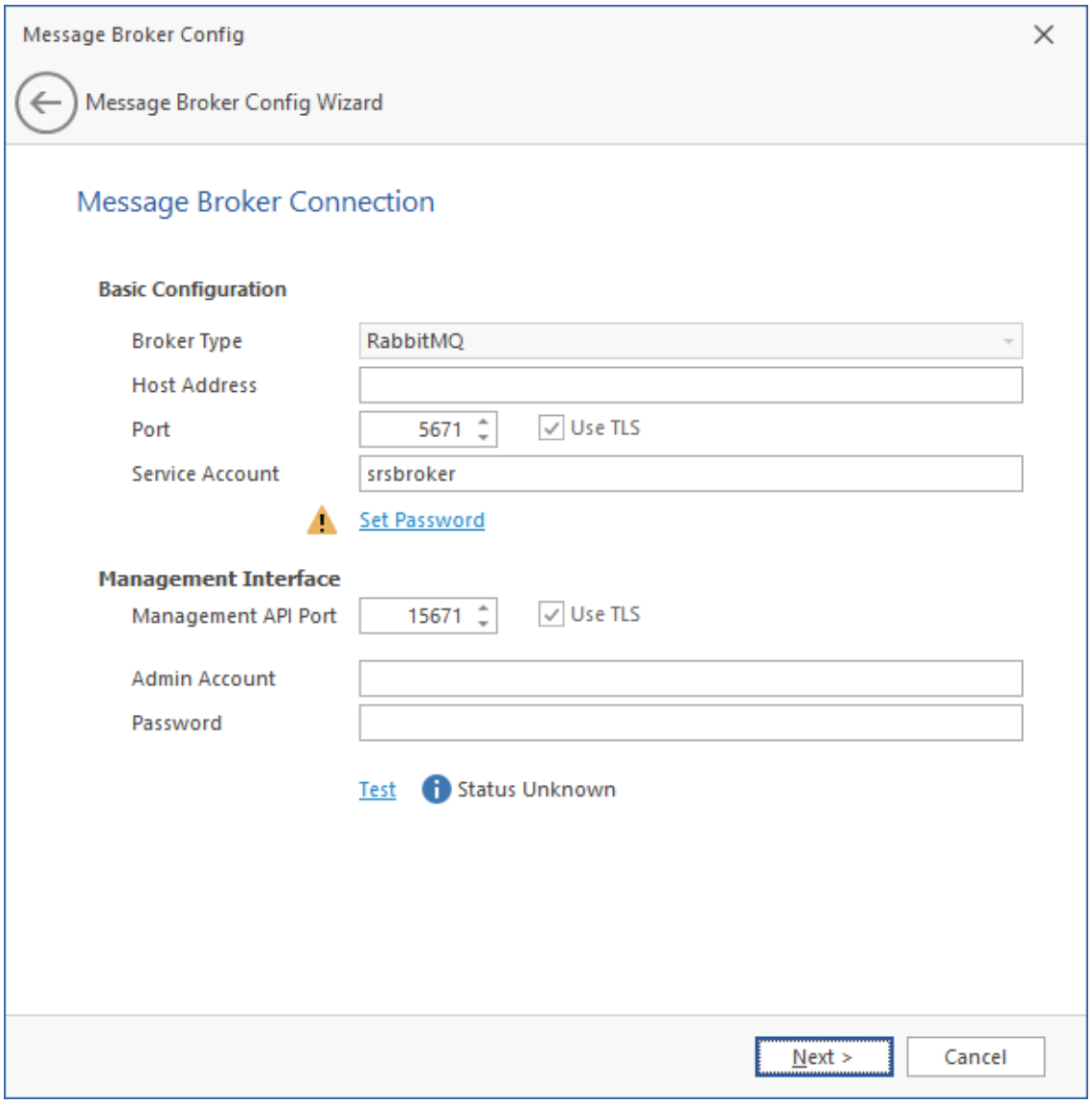



7 Click **Finish**.

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

## 6.7 Configuring the Message Broker

1 Click **Configure Message Broker**.




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.

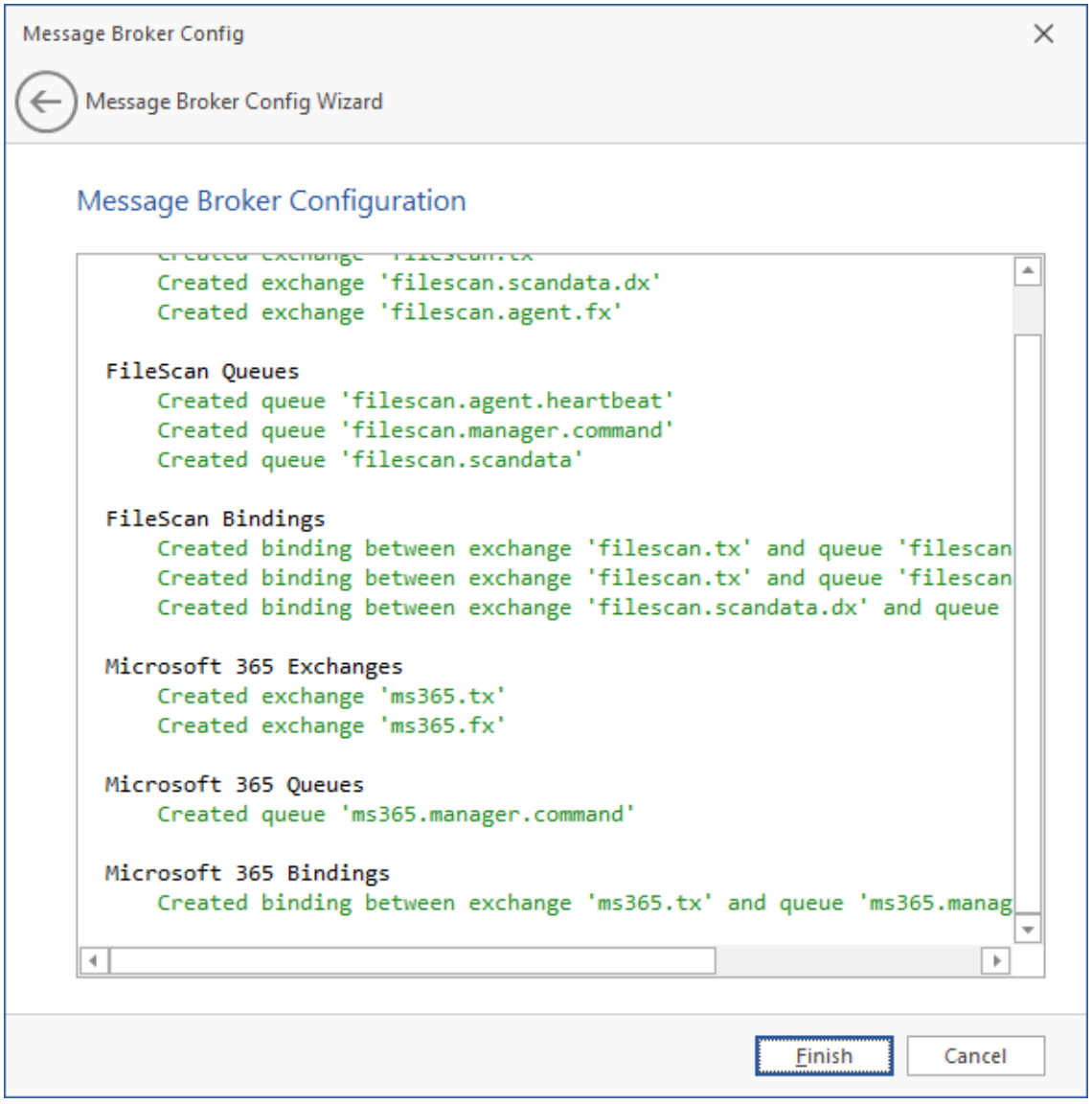
Unless you changed the default name, the admin account name is `admin`.

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

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

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

3 Click **Next**.

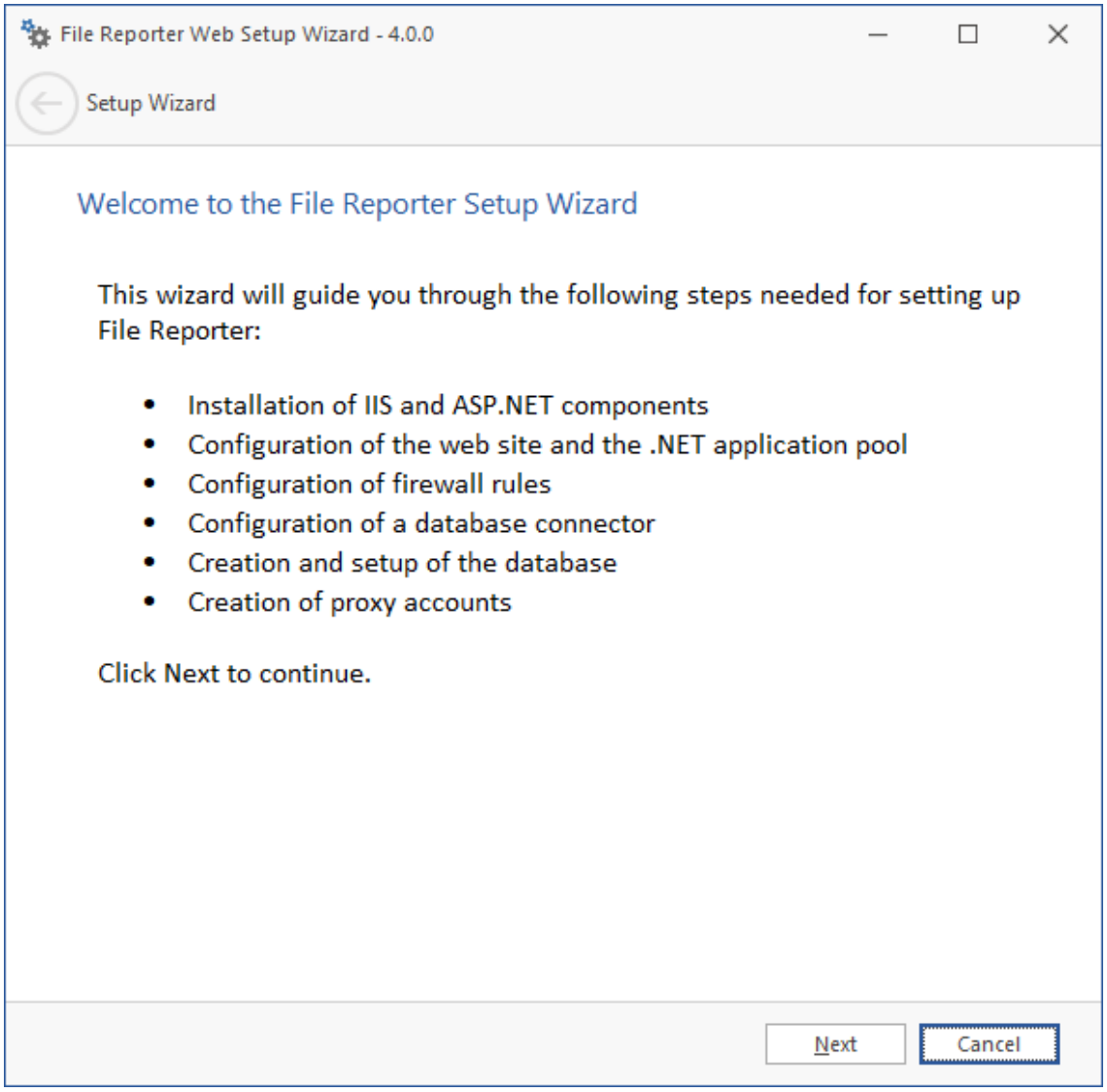



4 Click **Finish**.

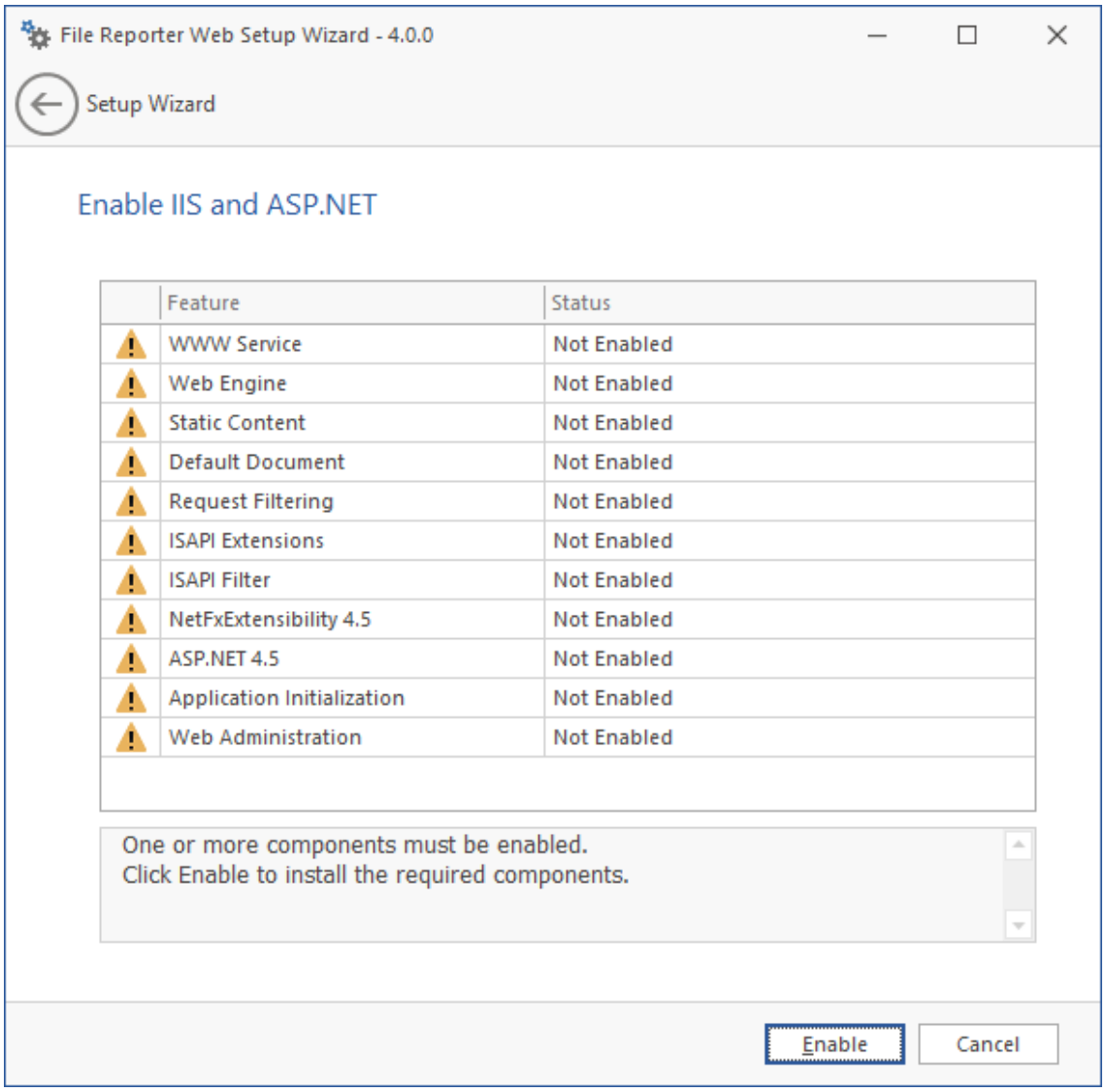
The message broker is now configured and connected.

## 6.8 Configuring the Web Application

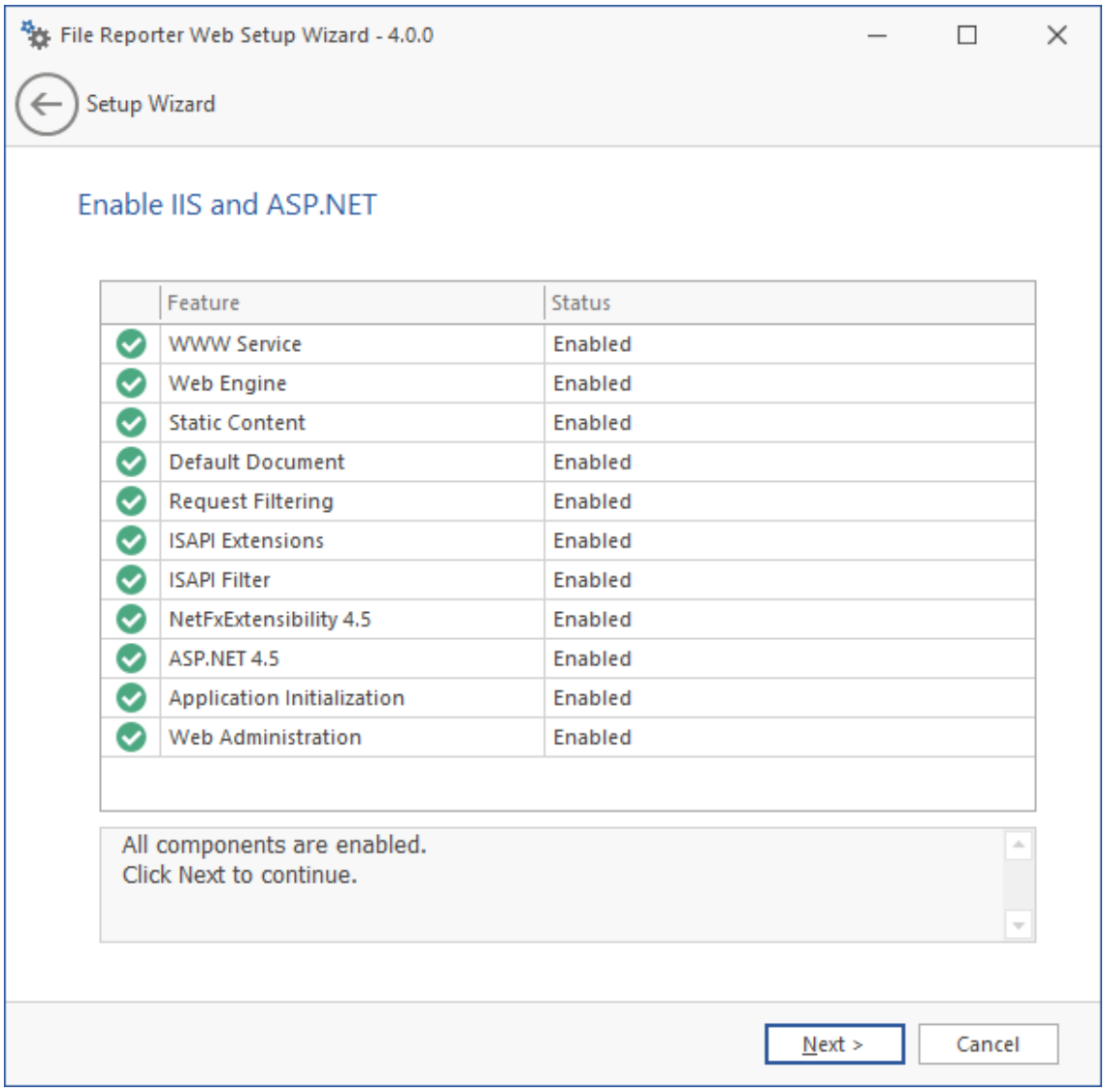
1 Click **Configure Web Application**.



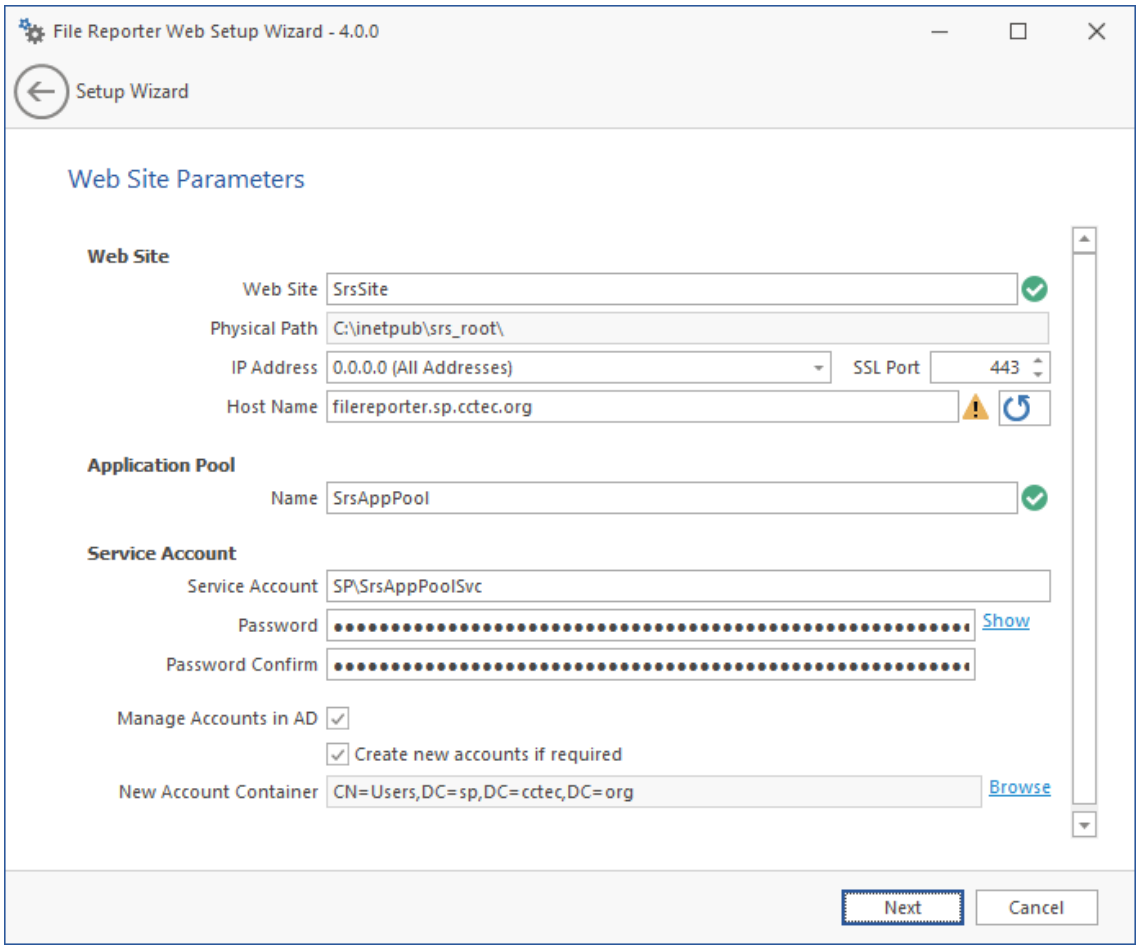

2 From the wizard page, read the overview of what will be configured and click **Next**.




**3** Click **Enable**.


File Reporter Web Setup Wizard - 4.0.0
Setup Wizard
Enable IIS and ASP.NET
Feature
Status
WWW Service
Enabled
Web Engine
Enabled
Static Content
Enabled
Default Document
Enabled
Request Filtering
Enabled
ISAPI Extensions
Enabled
ISAPI Filter
Enabled
NetFxExtensibility 4.5
Enabled
ASP.NET 4.5
Enabled
Application Initialization
Enabled
Web Administration
Enabled
All components are enabled.
Click Next to continue.
Next >
Cancel

**4** Click **Next**.




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 as part of the installation and is the location where content for the website is served up. This field is informational only and cannot be edited.

**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 6.1, "Prerequisites," on page 33.

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.

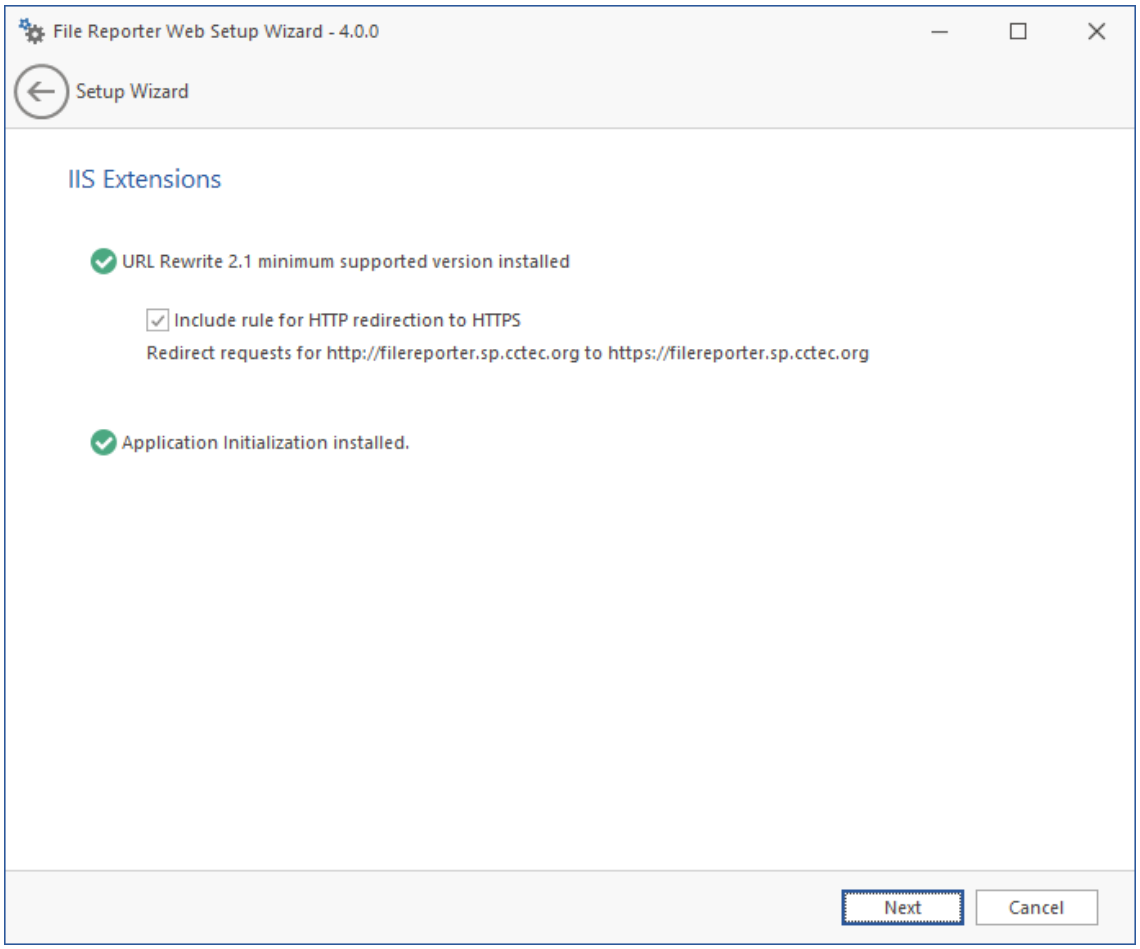
**Confirm Password:** The automatically generated password is repeated.

**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.

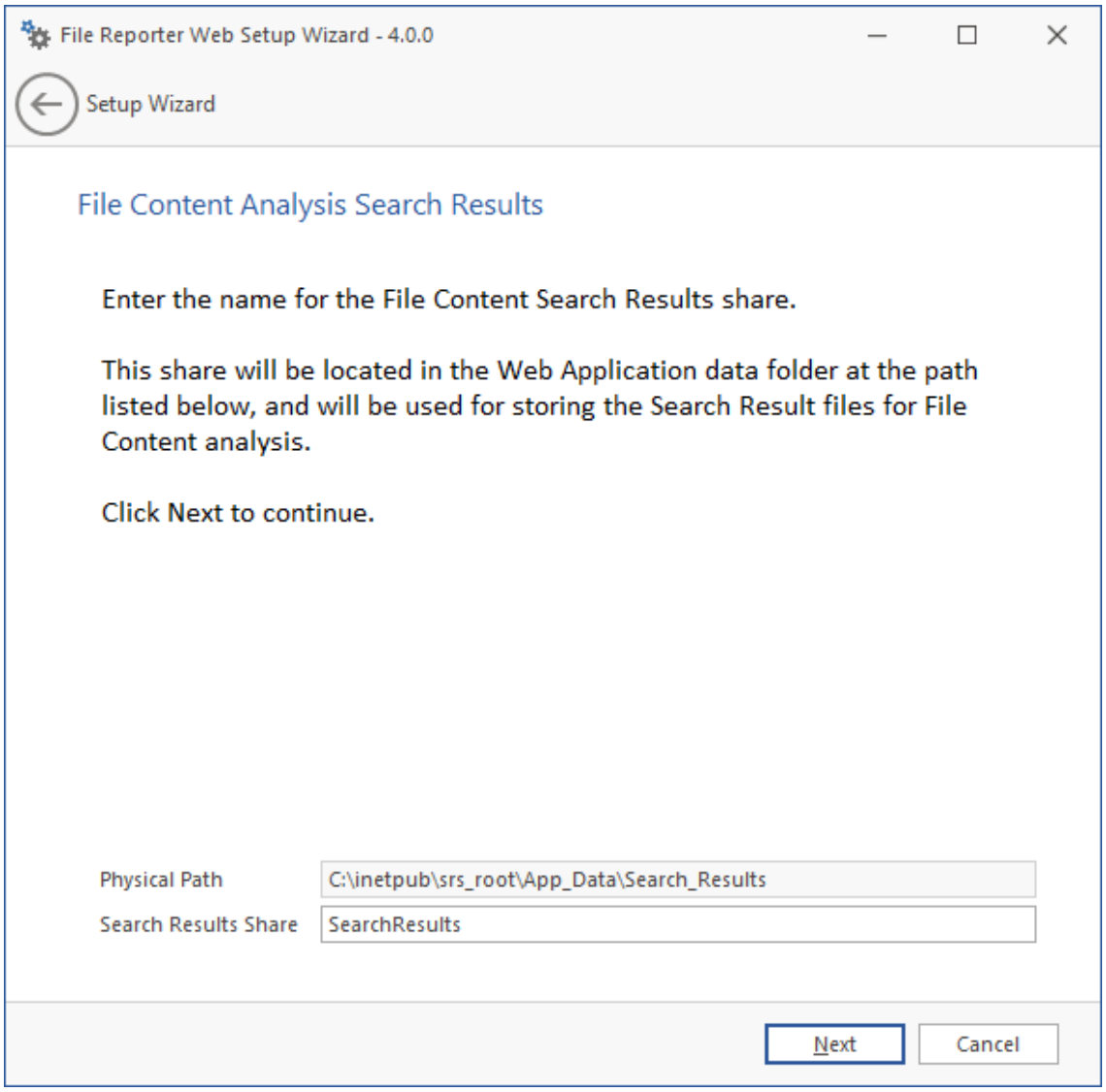
5 (Conditional) If the components are not enabled, click **Enable**.

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

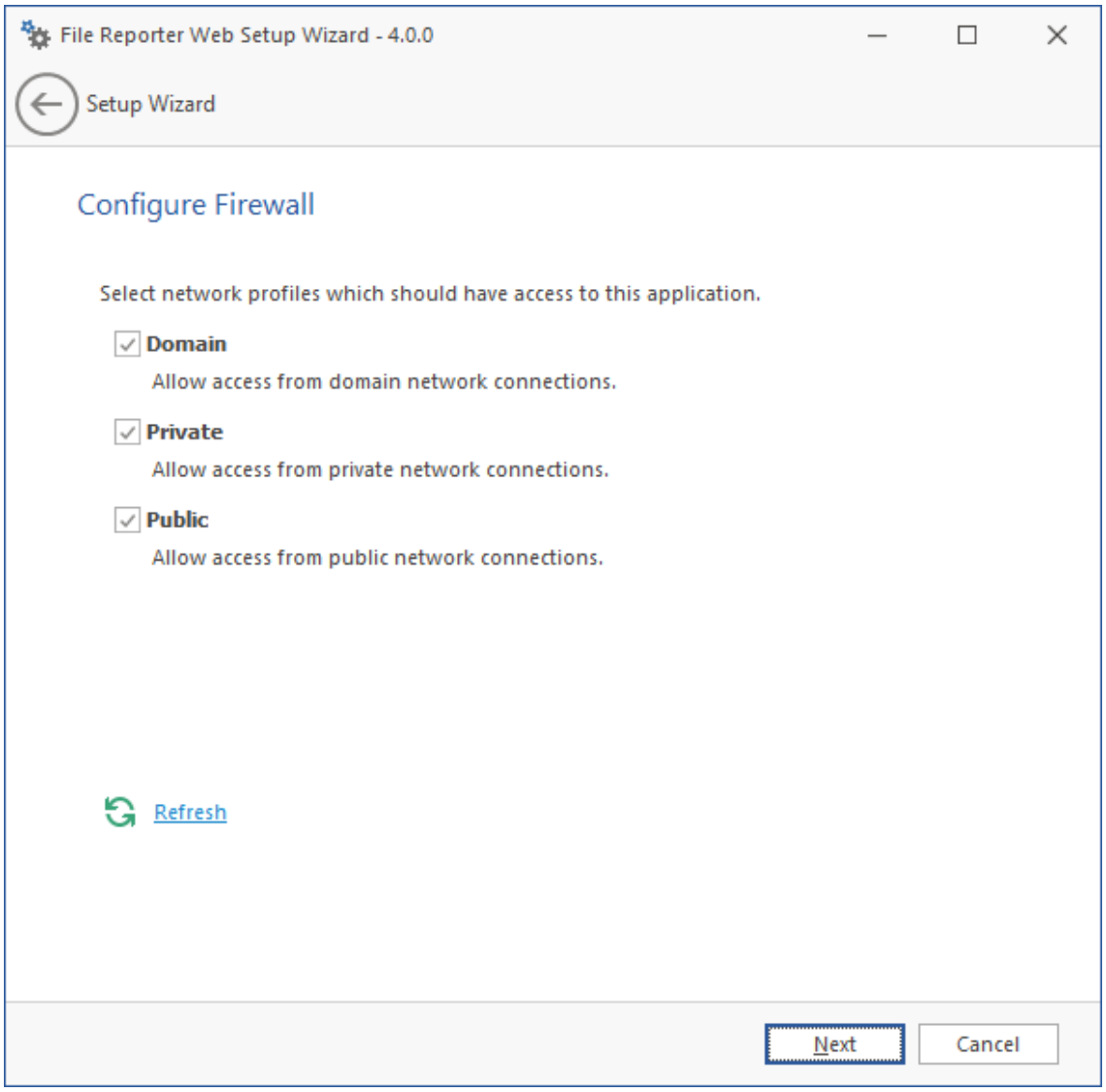



This page lets you install Microsoft IIS URL Rewrite Module 2.0, which will redirect the File Reporter Web Application requests using HTTP to HTTPS. For example, if you enter `http://filereporter.cctec.org` in a web browser, this module would redirect you to a secure page at `https://filereporter.cctec.org`.

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


File Reporter Web Setup Wizard - 4.0.0
Setup Wizard
File Content Analysis Search Results
Enter the name for the File Content Search Results share.
This share will be located in the Web Application data folder at the path listed below, and will be used for storing the Search Result files for File Content analysis.
Click Next to continue.
Physical Path
C:\inetpub\srs_root\App_Data\Search_Results
Search Results Share
SearchResults
Next
Cancel

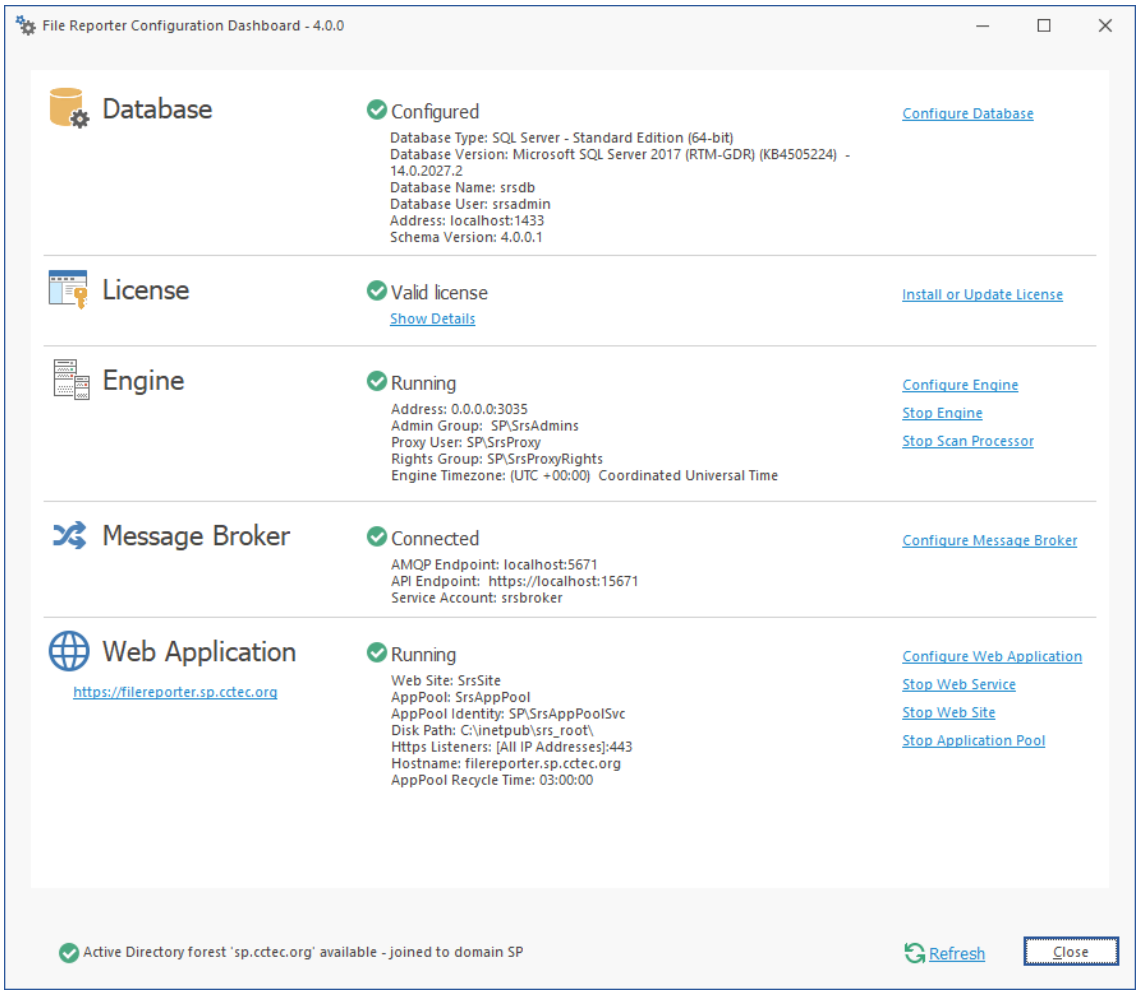
**8** Click **Next**.




9 Set the firewall 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 the Web Application URL as a trusted website.

# 7 File System Scans


- Section 7.1, “Minimum Requirements,” on page 57
- Section 7.2, “Installing and Configuring AgentFS,” on page 57


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

## 7.1 Minimum Requirements

- Any of the following dual core 64-bit processor servers:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
- The server must be joined to Active Directory
- .NET 6.0 (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 might improve performance.

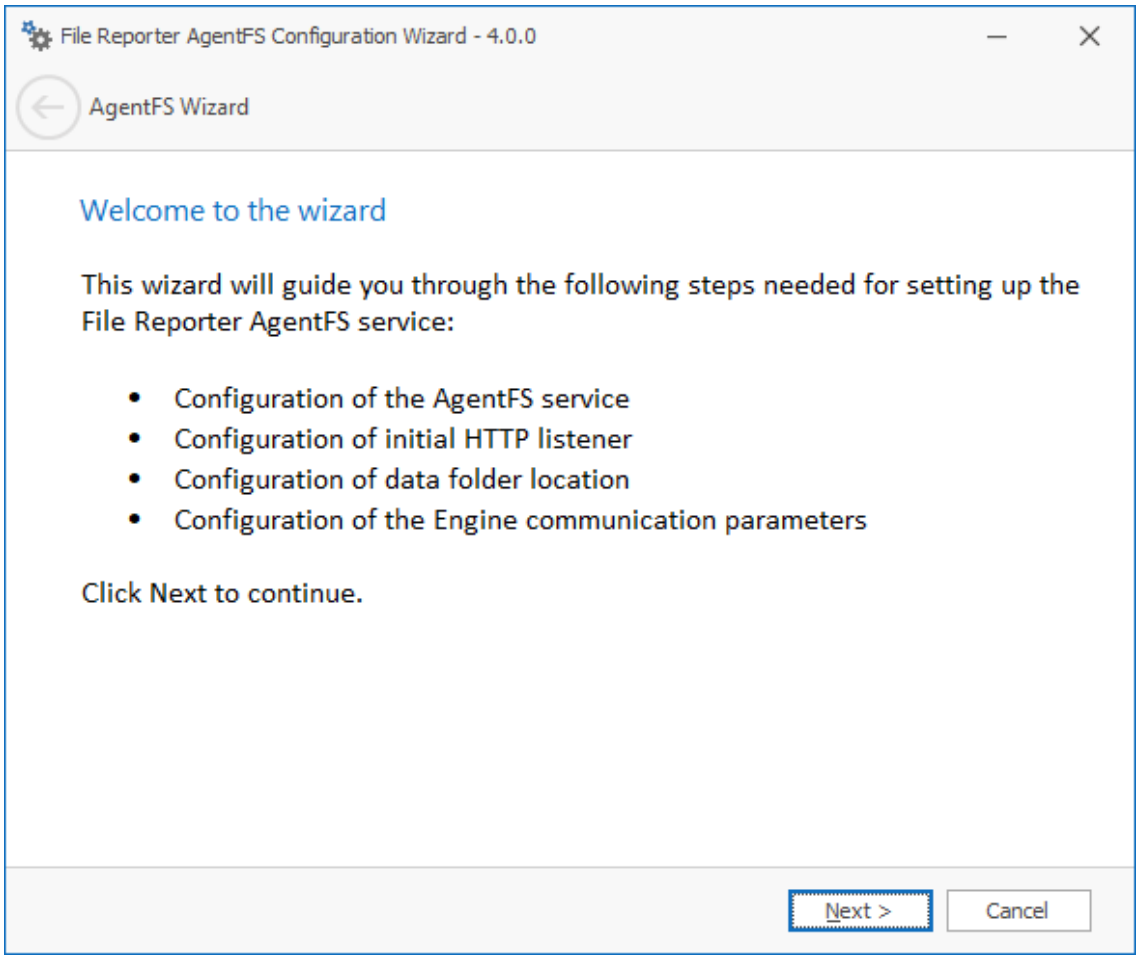
  ---

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

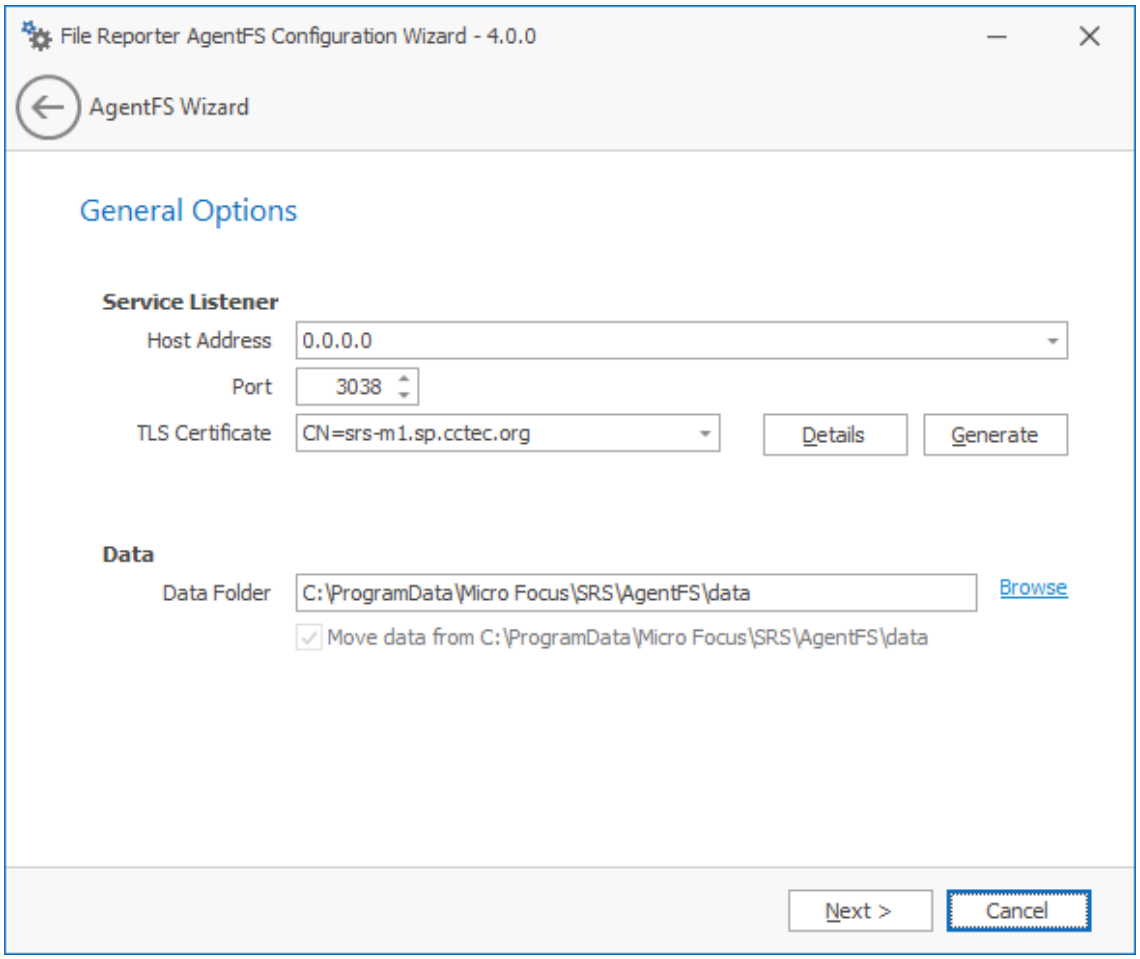
  This size might need to be adjusted based on number of concurrent scans this agent performs, as well as the size of the scans themselves.

## 7.2 Installing and Configuring AgentFS

1. At the root of the `FileReporter_4.1.iso` image, double-click `FileReporter-AgentFS-4.1.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**.




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.

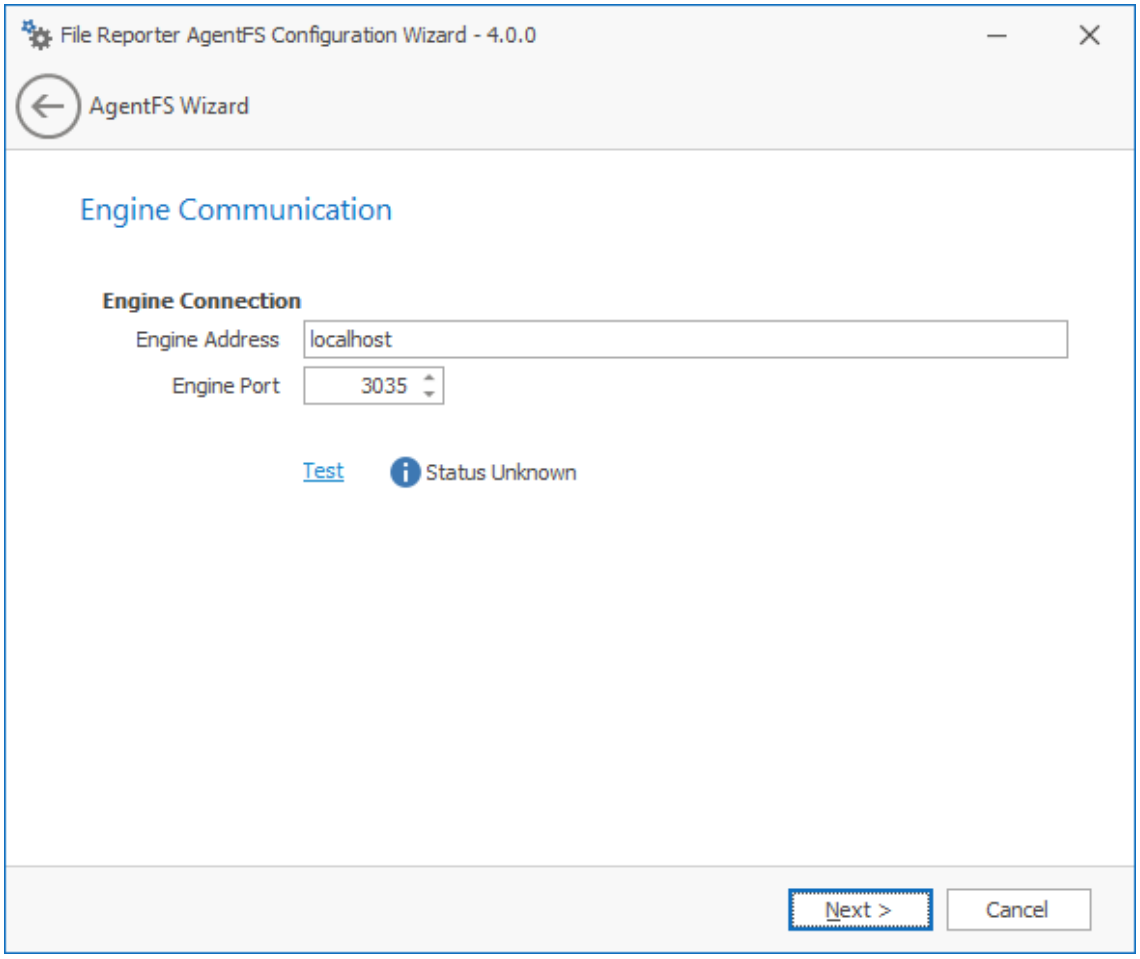
**Data:** Parameters pertaining to the `data` folder.

**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 with 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**.

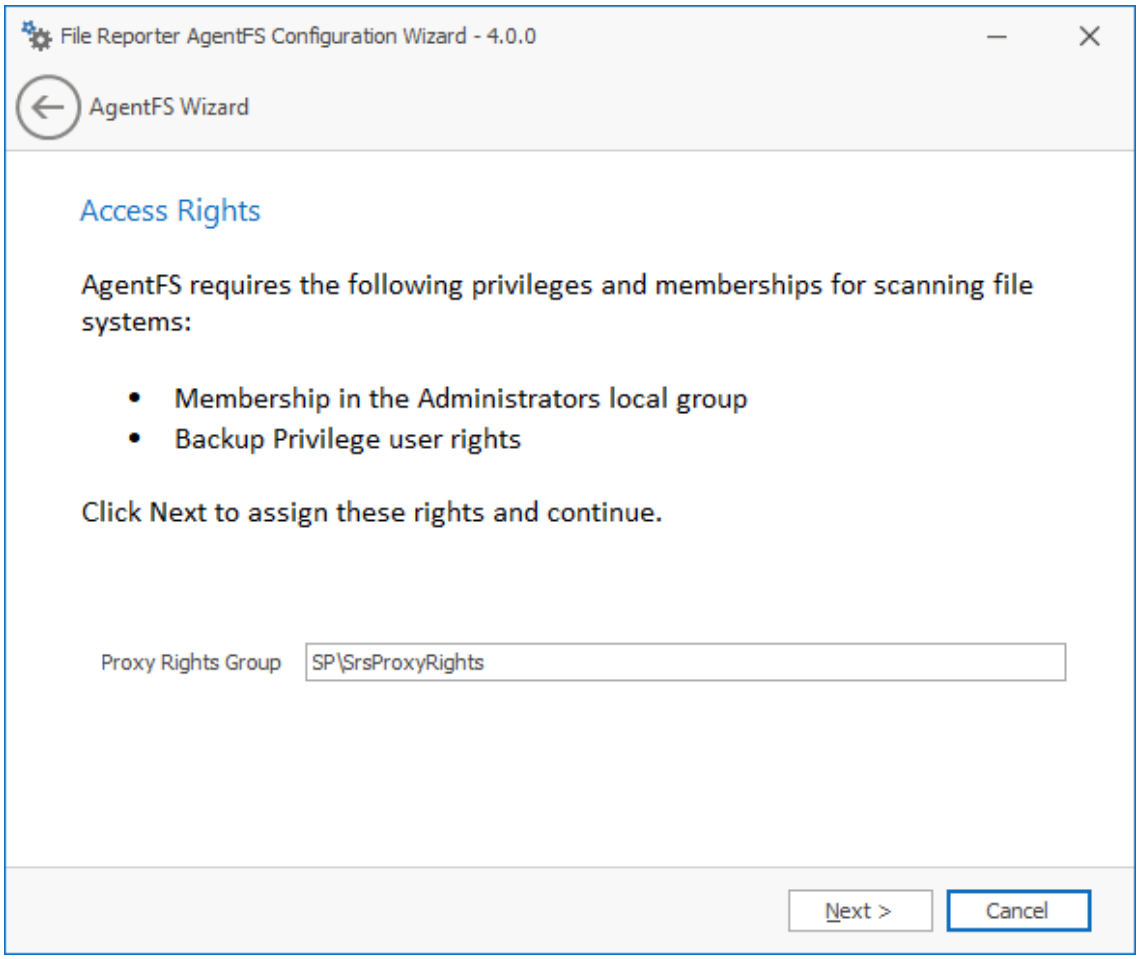



This page lets you set parameters for AgentFS to communicate with the Engine.

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

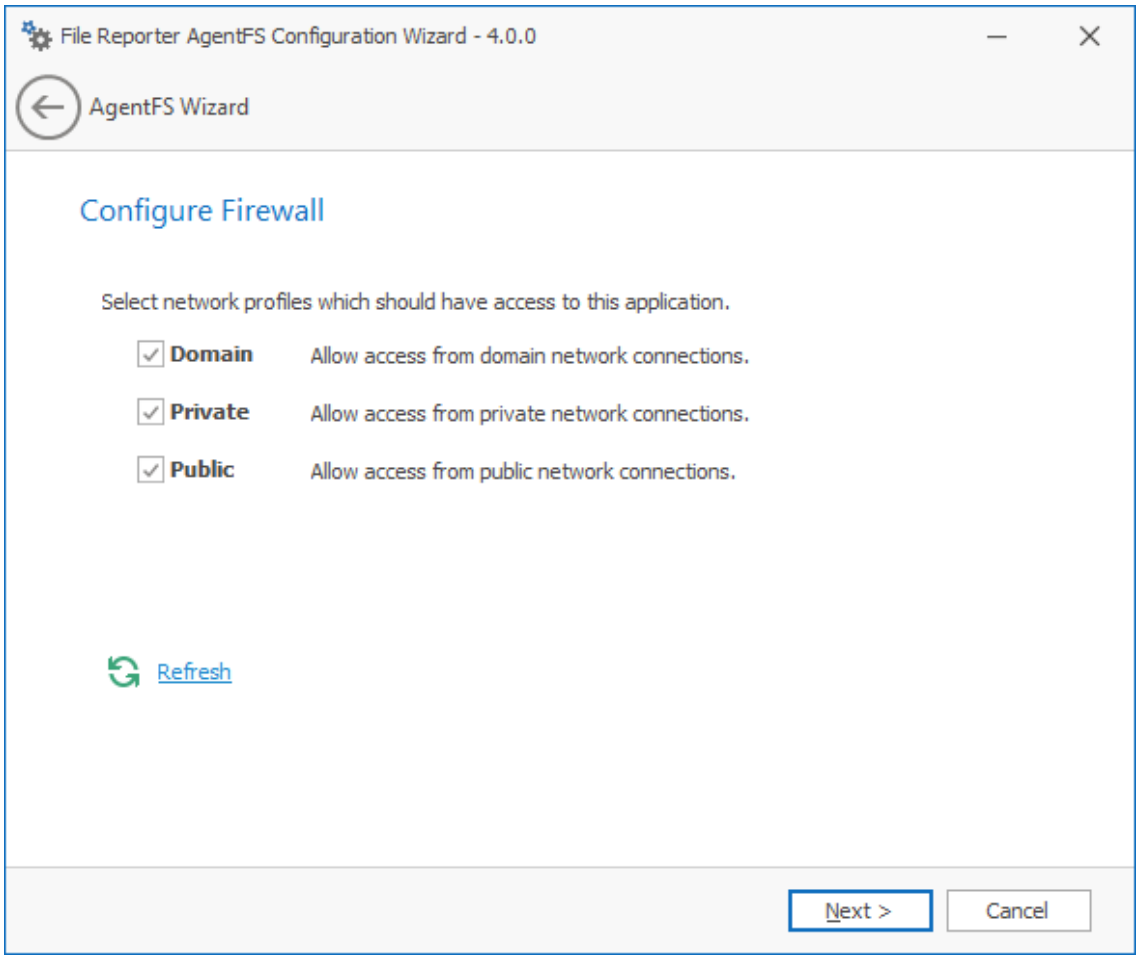
**Engine Port:** Specify the TLS port for the Engine here.

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

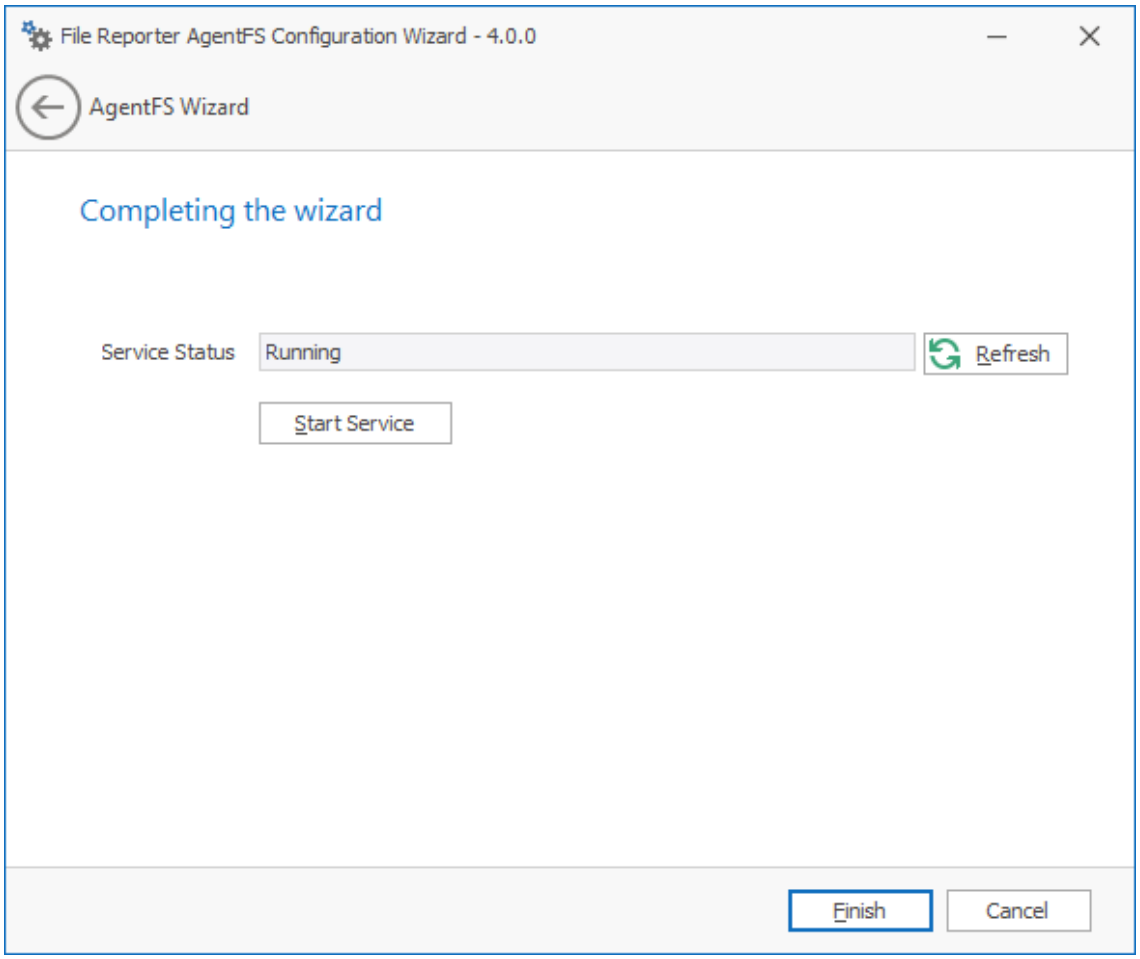



This page lets you establish AgentFS as a member of the Administrators local group and the ability to back up to the SrsProxyRights group.

**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.

# 8 File Content Scans


- Section 8.1, “ManagerFC,” on page 65
- Section 8.2, “AgentFC,” on page 70


File Reporter provides optional components for performing basic file content scans and pattern searching.

File content scanning requires setup of the following components:

- RabbitMQ message broker - see Chapter 5, “Installing and Configuring RabbitMQ,” on page 25.
- ManagerFC - see Section 8.1, “ManagerFC,” on page 65.
- AgentFC - see Section 8.2, “AgentFC,” on page 70.

## 8.1 ManagerFC


- Section 8.1.1, “Minimum Requirements,” on page 65
- Section 8.1.2, “Installation and Configuration,” on page 65

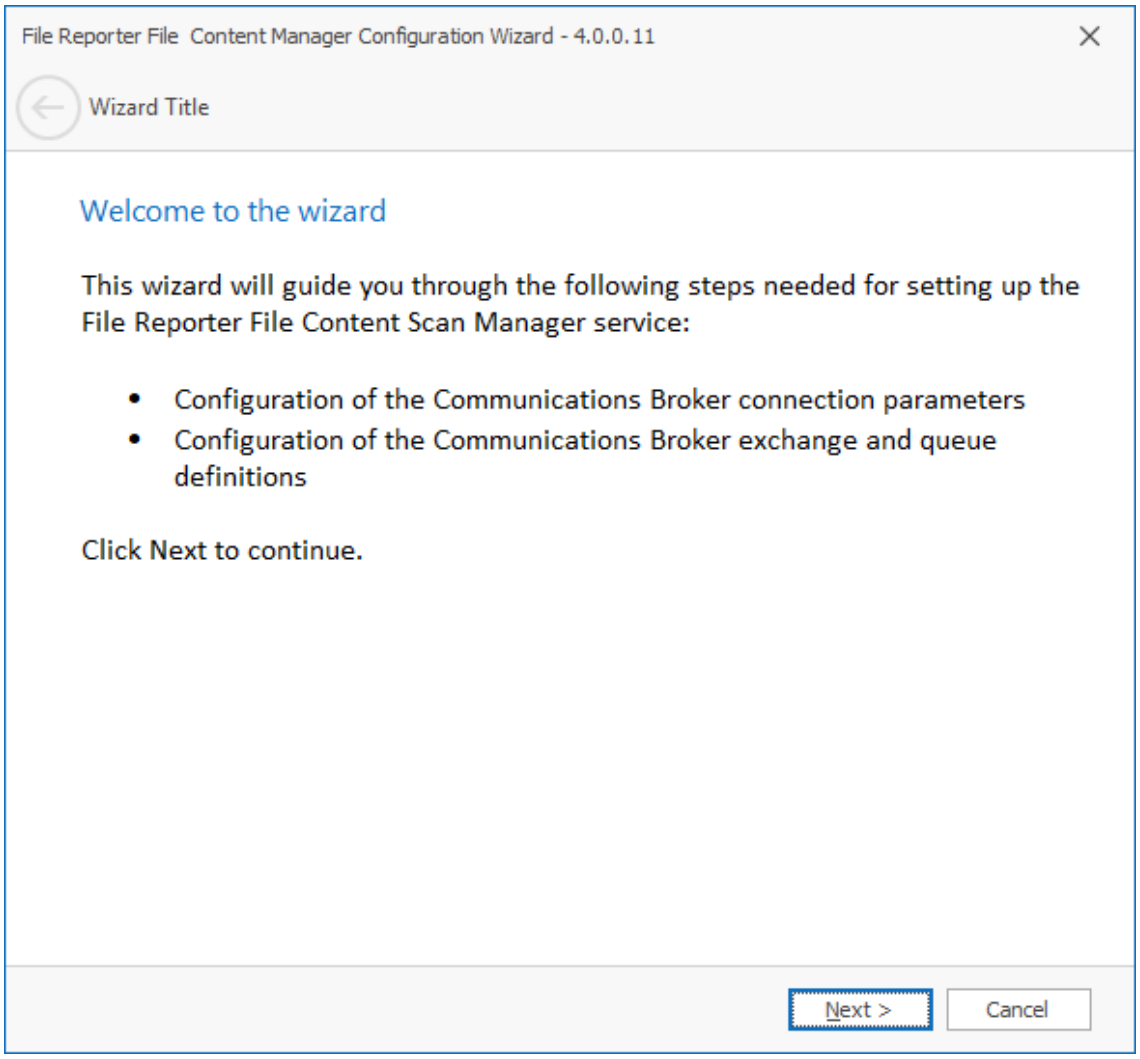

### 8.1.1 Minimum Requirements

- Any of the following server platforms:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
- Quad-core processor
- 6 GB RAM
- 2 GB free disk space

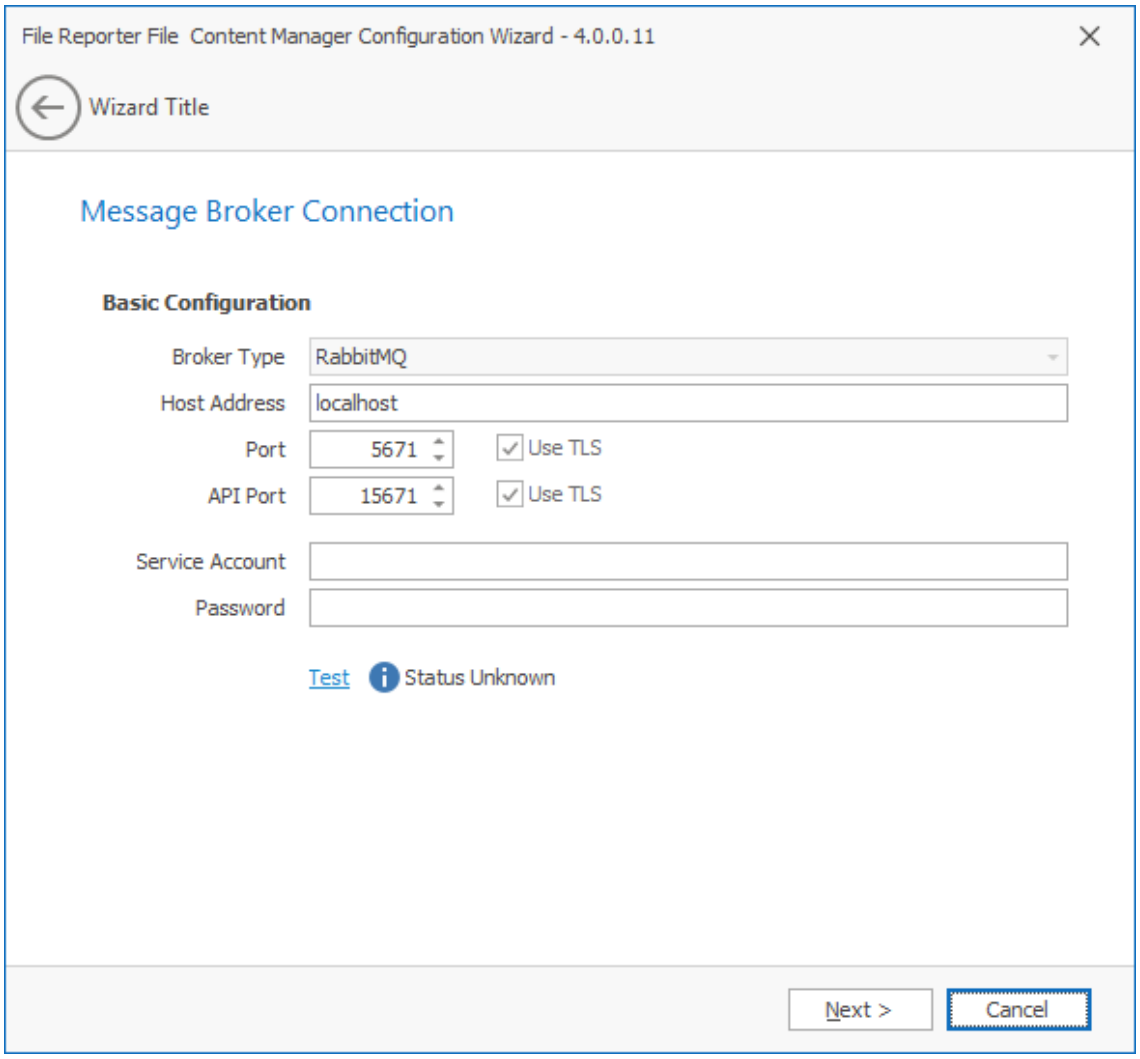
ManagerFC has minimal processor and RAM requirements. As such, Micro Focus recommends that ManagerFC be installed on the same host as the Engine.

### 8.1.2 Installation and Configuration

1. At the root of the `FileReporter_4.1.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**.




**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.

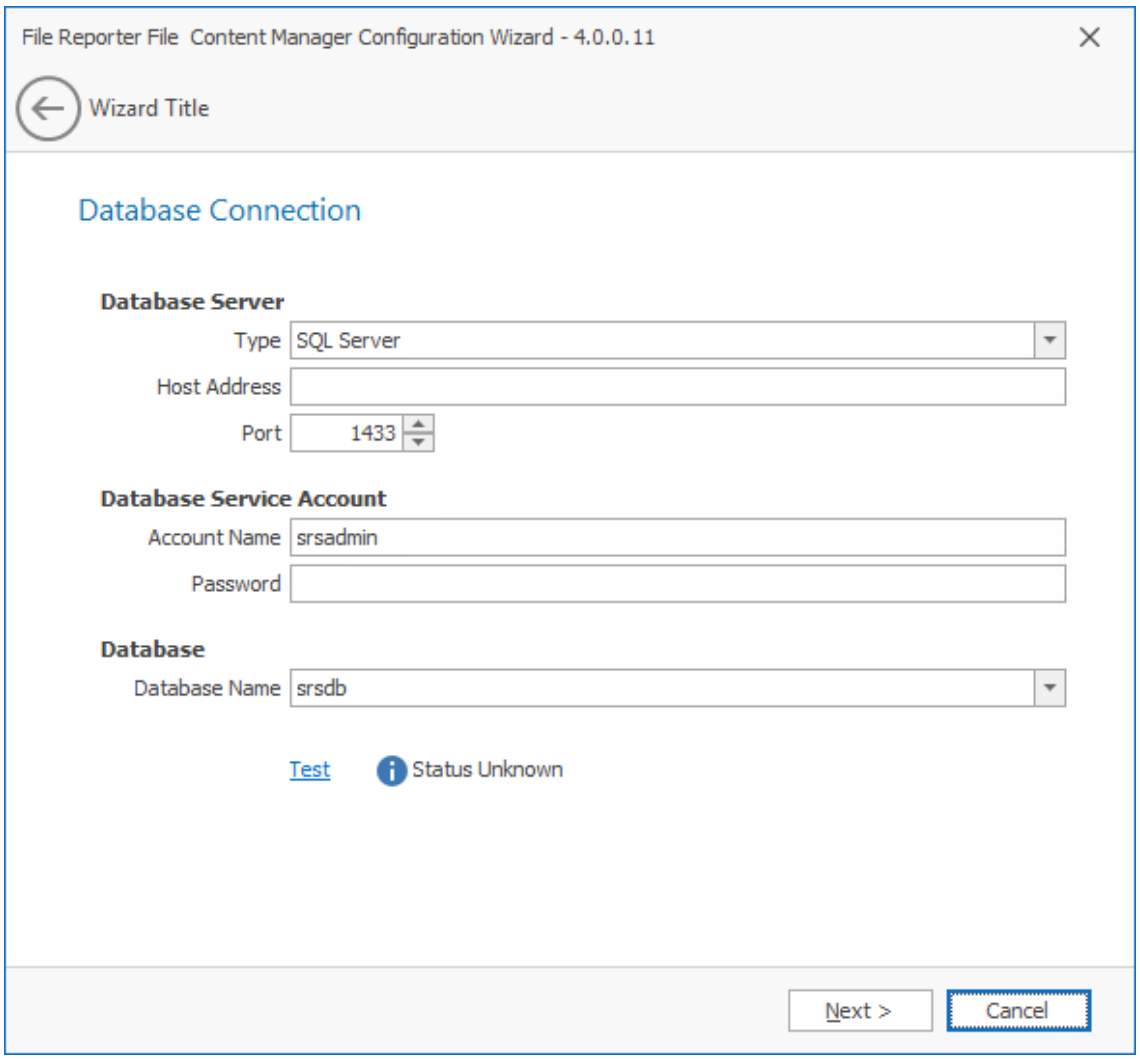
**Use TLS:** This is a read-only check box indicating that File Reporter only works with TLS communication channels. TLS is always required.

**Service Account:** Use the administrator name that you established in Section 6.7, “Configuring the Message Broker,” on page 45.

**Password:** Use the password that you established in Section 5.5, “Changing the Administrator Password,” on page 30.

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

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




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.

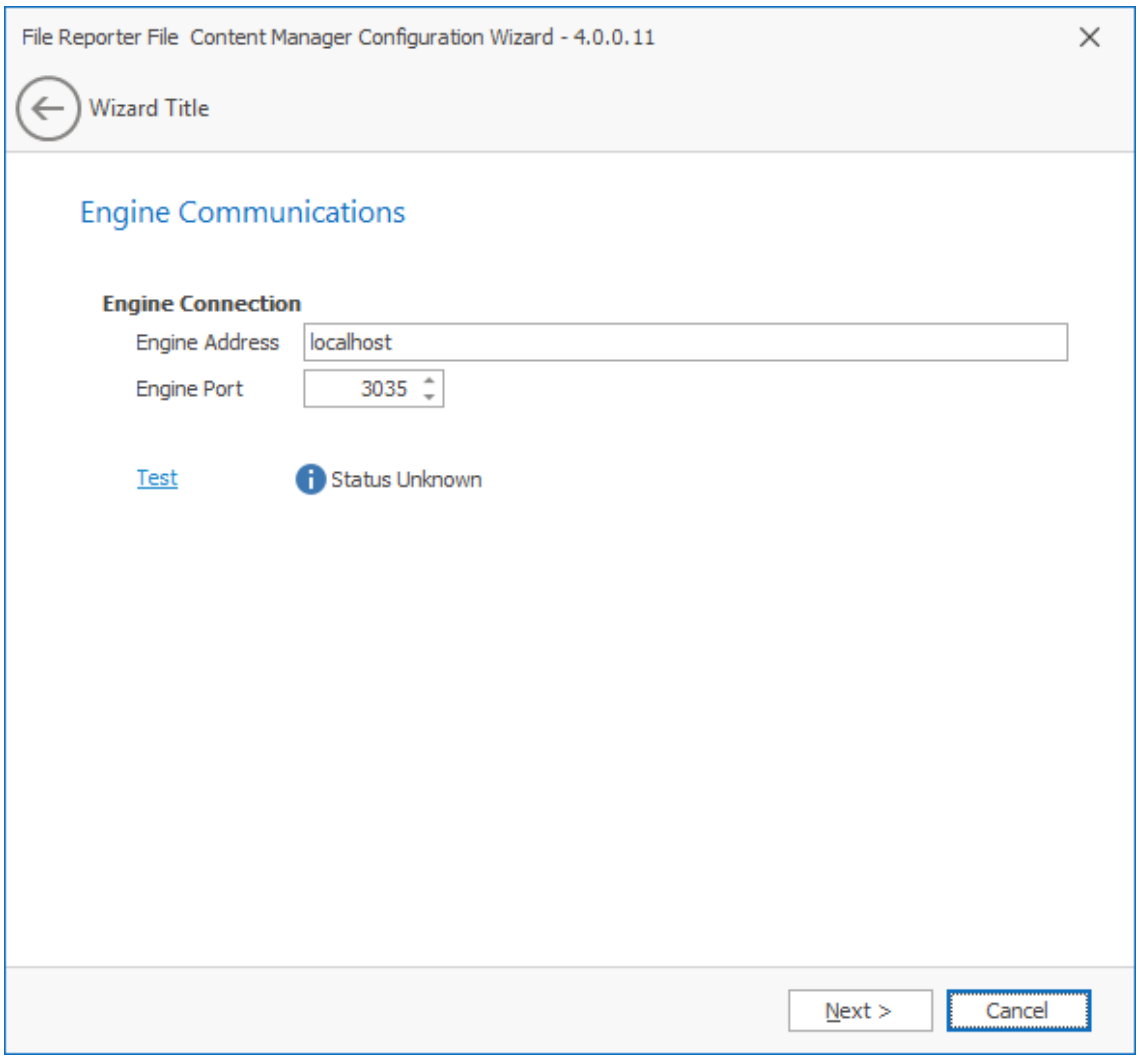
**Password:** Specify the password for the Database Service User.

**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**.

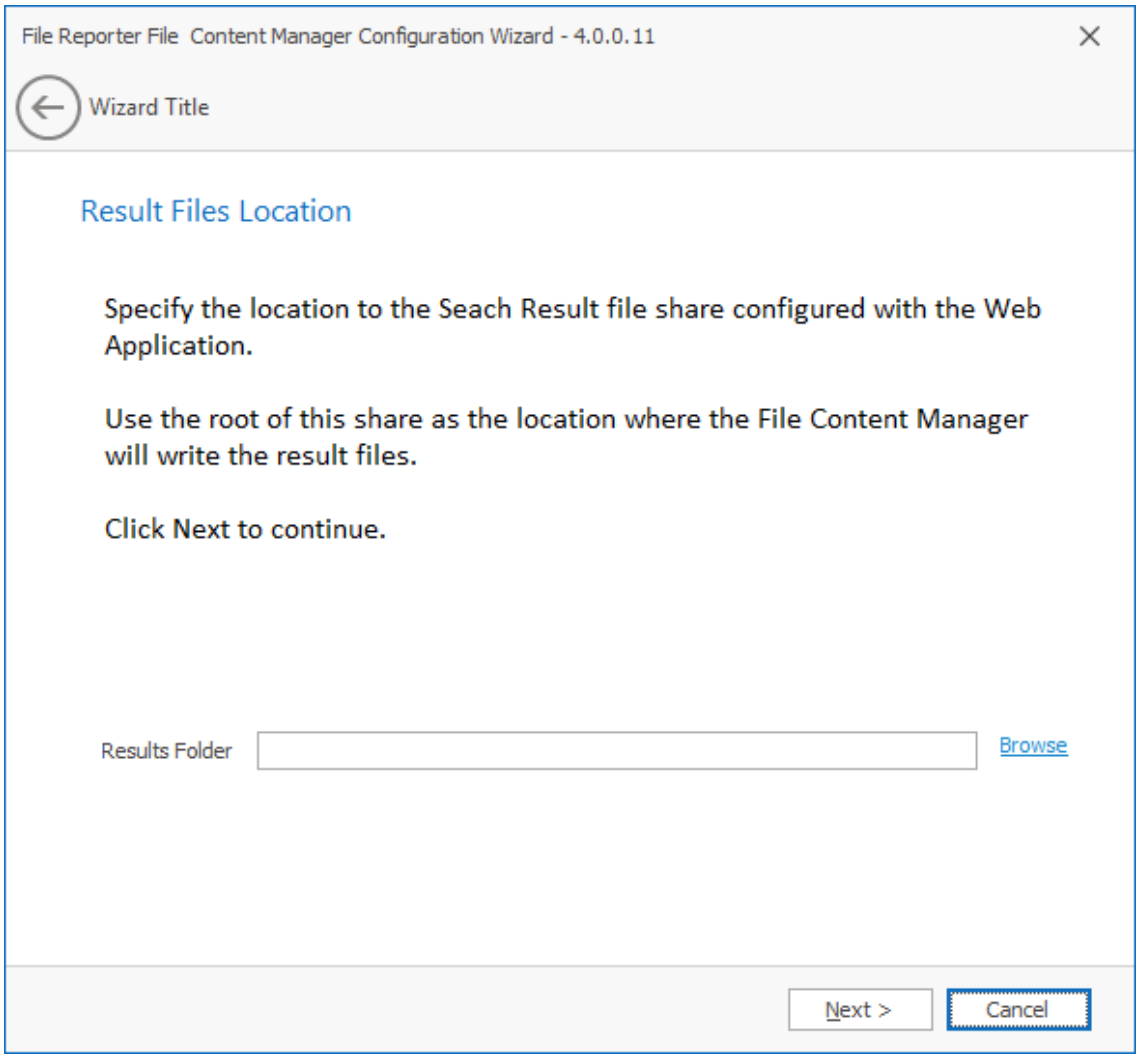



This page lets you set parameters for ManagerFC to communicate with the Engine.

**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 `Search_Results` share that was created when you installed and configured the Web App.

For more information, see Section 6.8, “Configuring the Web Application,” on page 48.

9 Click **Next**.

10 Click **Finish** to complete the configuration of ManagerFC.

## 8.2 AgentFC


- Section 8.2.1, “Minimum Requirements,” on page 71
- Section 8.2.2, “Installation and Configuration,” on page 71

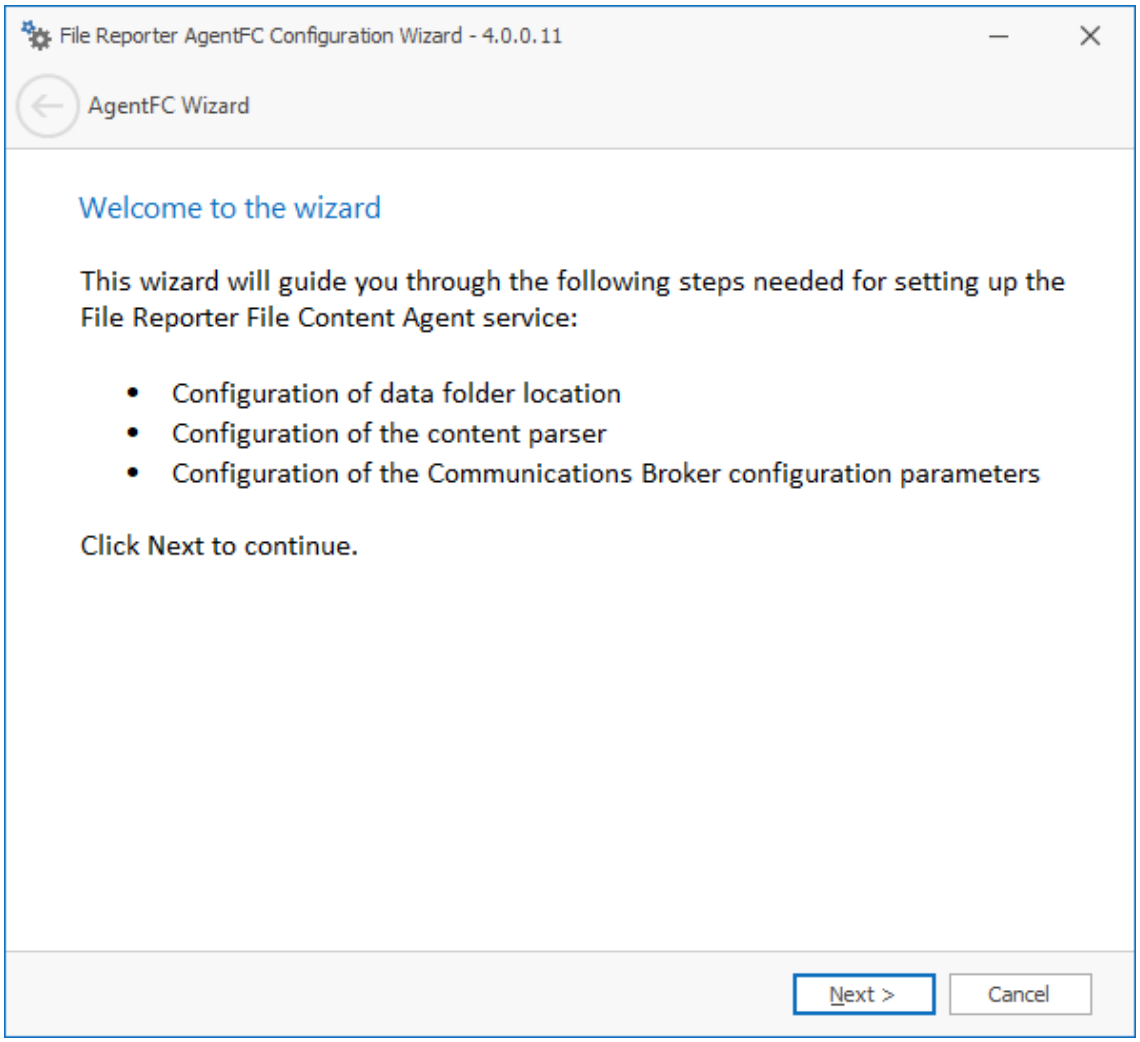
### 8.2.1 Minimum Requirements

- Any of the following dual-core 64-bit processor servers:
  - Windows Server 2022
  - 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

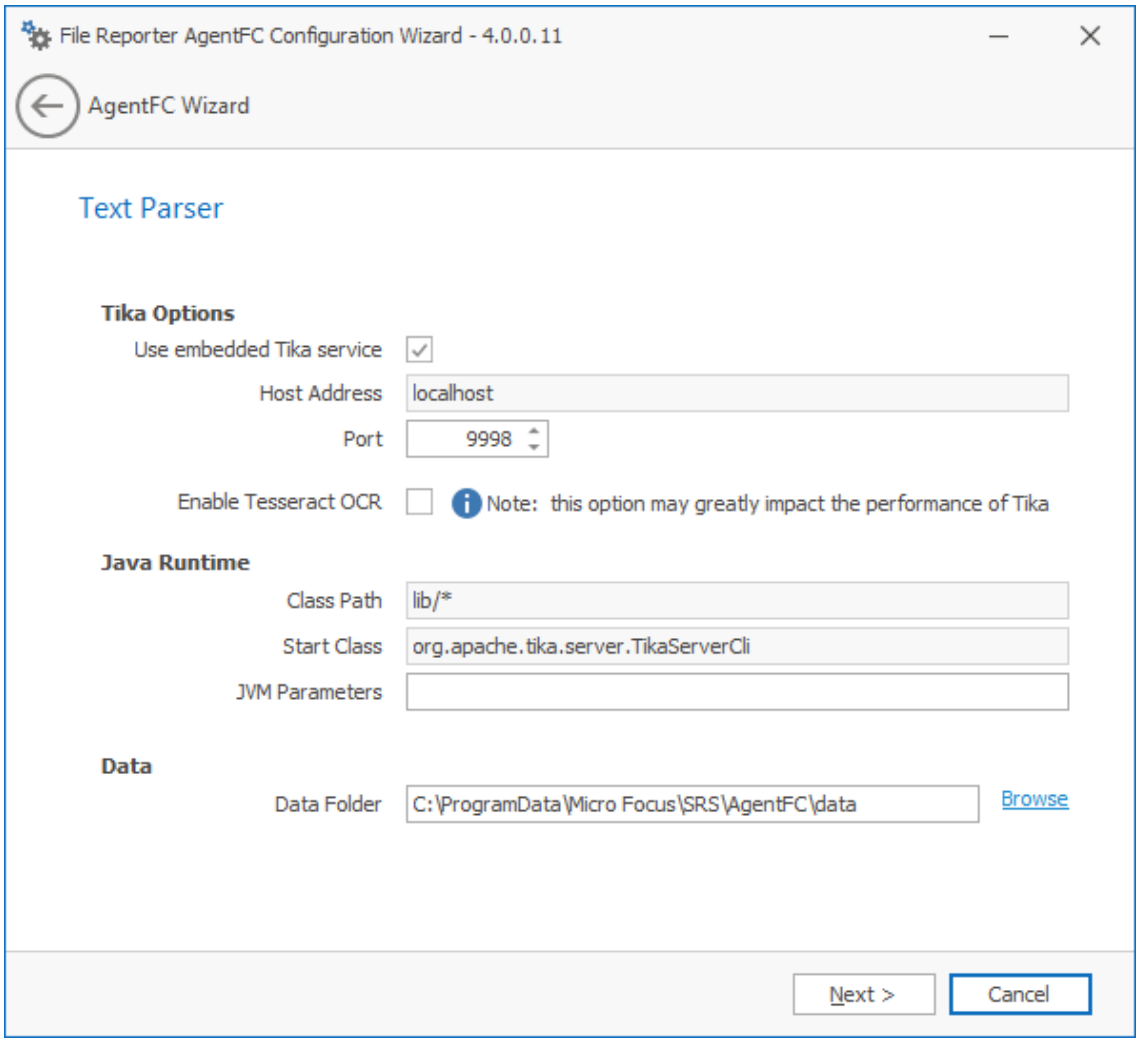
    Depending on the workloads, these numbers might need to be adjusted.
- Depending on the frequency of workloads, it might be advisable to install each AgentFC node in a virtual machine environment where resources can be scaled as needed. This can allow for more resources as heavy workloads are in progress,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

### 8.2.2 Installation and Configuration

1. At the root of the `FileReporter_4.1.iso` image, double-click `FileReporter-AgentFC-4.1.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 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 `localhost` on 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 otherwise 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.

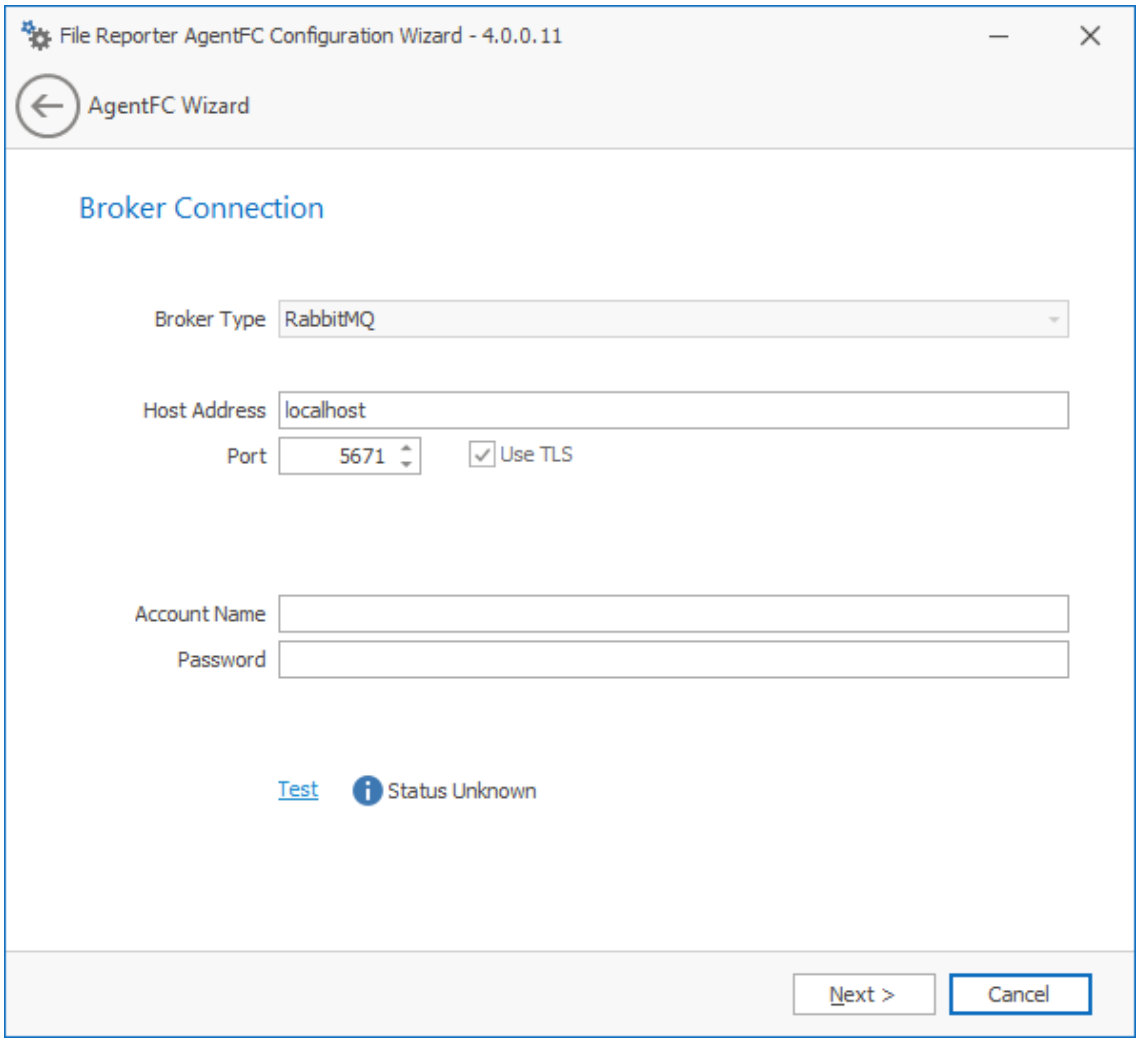
**JVM Parameters:** This field is provided as a means for providing advanced tuning parameters Java Virtual Machine. Any settings in this field should be done through the direction of a Micro Focus technical support representative.

**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:** This lets you specify a new location for the `data` folder.

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




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.

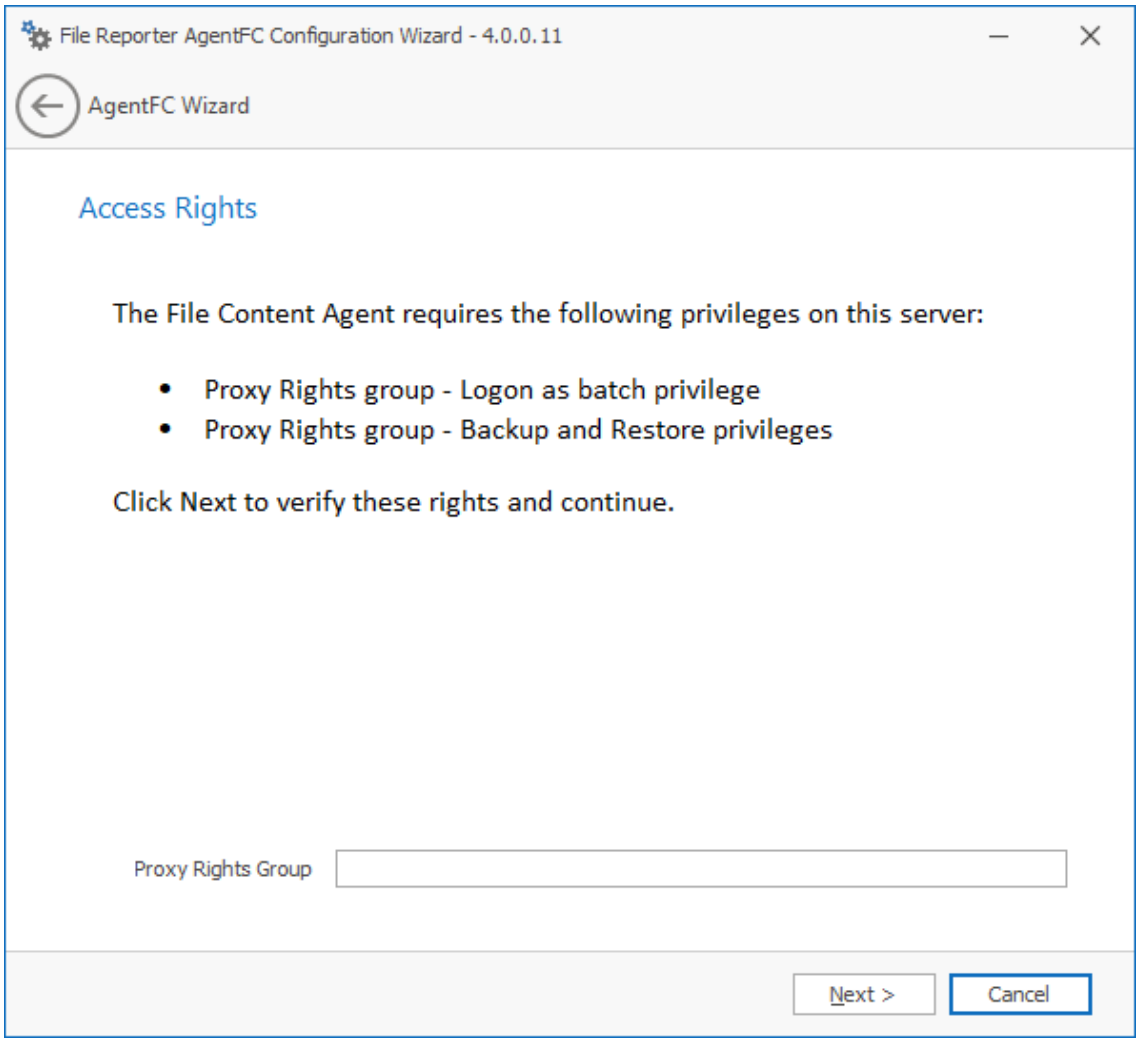
**Use TLS:** The RabbitMQ messaging broker in File Reporter requires Transport Layer Security (TLS) as the cryptographic communications security protocol.

**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 8.1, “ManagerFC,” on page 65.

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

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

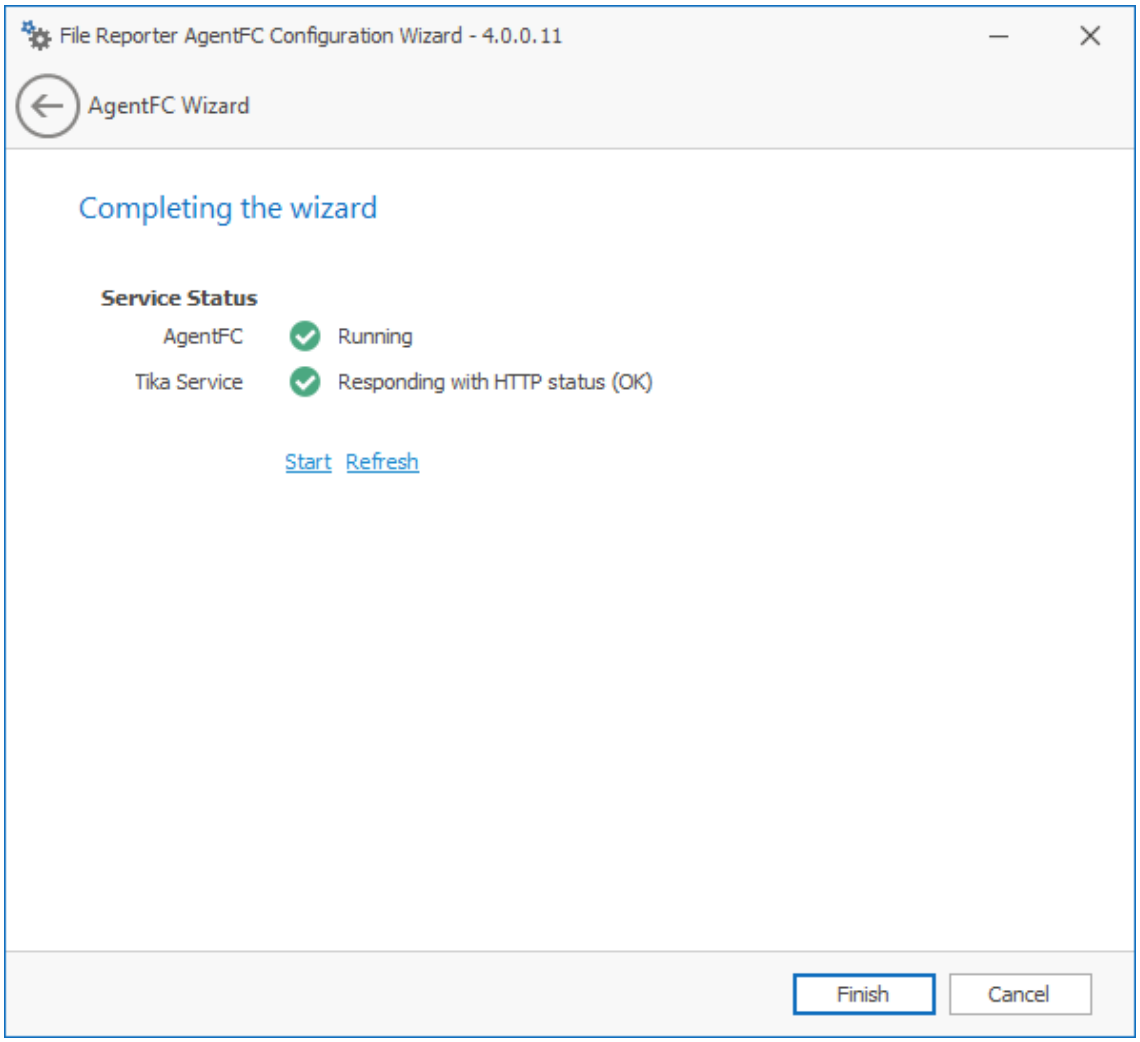
6 Complete the fields and click **Next**.




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 group, which by default is `SrsProxyRights`.

8 Click **Next**.




**9** Click **Finish** to complete the configuration of AgentFC.

# 9 Microsoft 365 Integration


- Section 9.1, “Prerequisites,” on page 77
- Section 9.2, “Agent365,” on page 83


This chapter provides procedures for first configuring your Microsoft 365 tenant for reporting through File Reporter. Afterwards, it provides procedures for installing and configuring Agent365 which performs scans on the Microsoft 365 endpoints.

Scans on Microsoft 365 cloud applications include SharePoint sites and document libraries, OneDrive for Business repositories, file and folder metadata, permissions, users, and groups, including Teams-enabled group metadata.

---

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

---

## 9.1 Prerequisites


- Section 9.1.1, “Message Broker,” on page 77
- Section 9.1.2, “Preparing the Microsoft 365 Tenant,” on page 77


### 9.1.1 Message Broker

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

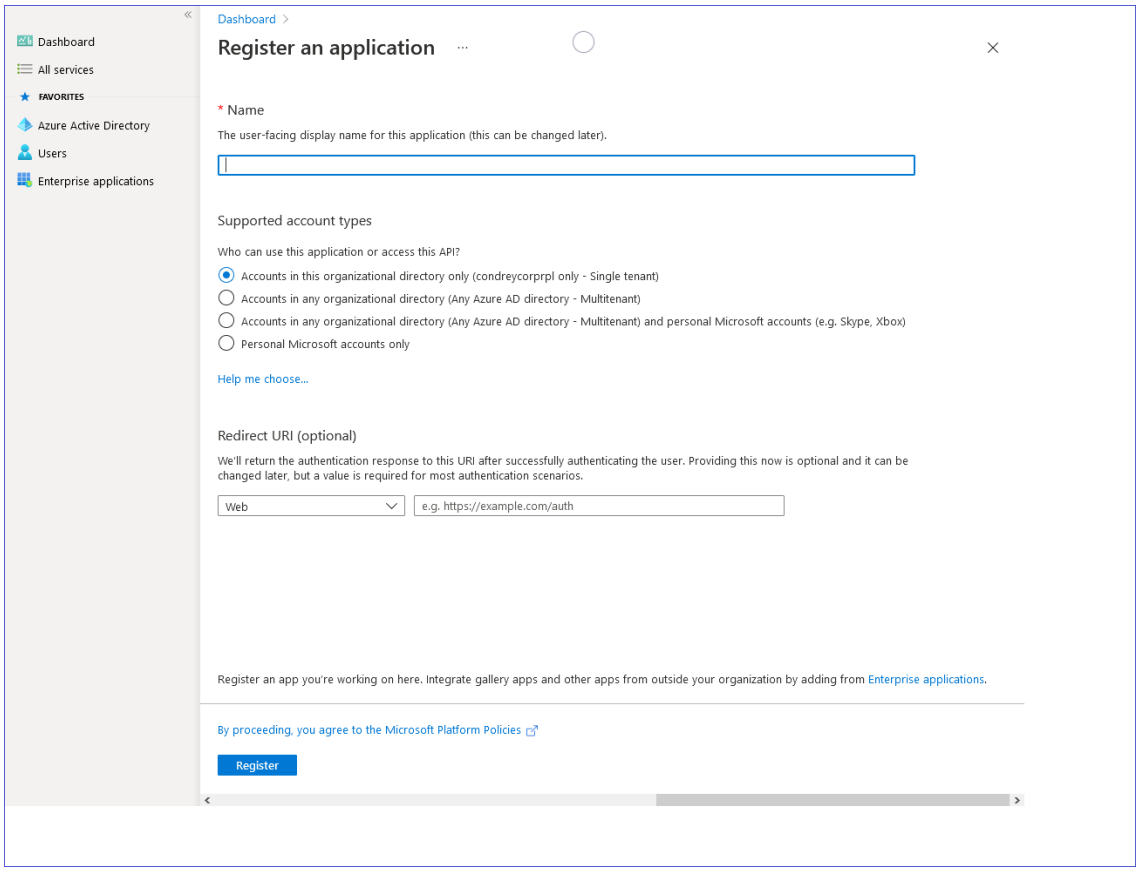
### 9.1.2 Preparing the Microsoft 365 Tenant

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**.

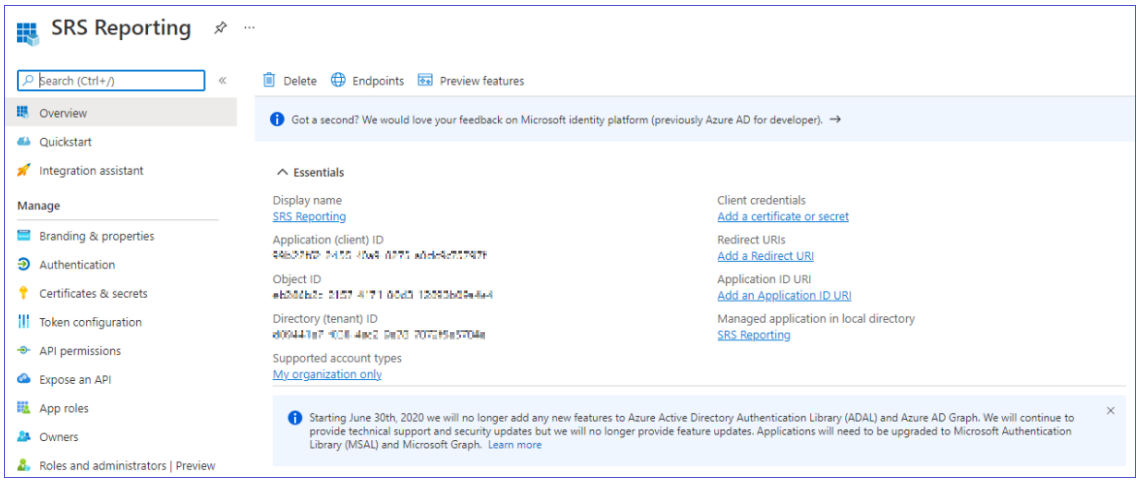
   This launches the Azure Active Directory admin center.
4. From the **Dashboard** menu, click **Azure Active Directory**.
5. From the **Manage** menu, select **App registrations**.
6. Click the **New registration** tab.




7 In the **Name** field, enter a descriptive name for the application registration.
For example: SRS `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.



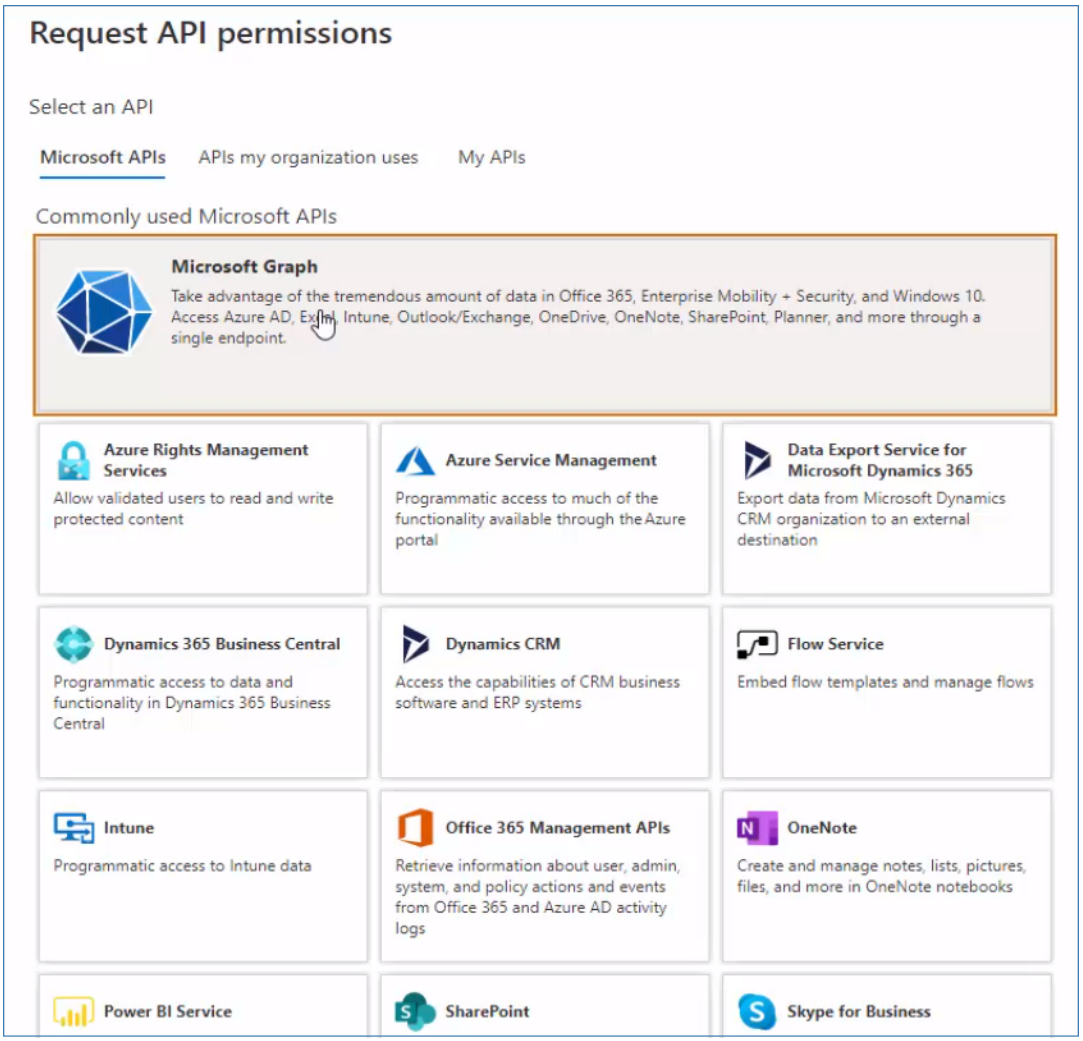

10 From the **Manage** menu, select **API permissions**.

**11** Set the application permissions for the Microsoft Graphi API.

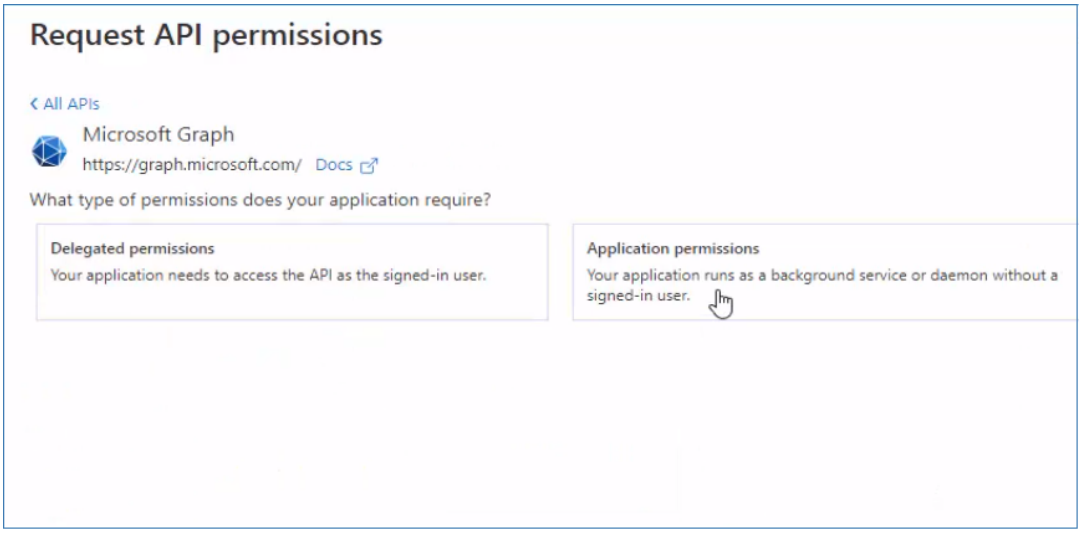
**11a** Refer to the following table as you establish application permissions:

| 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 |

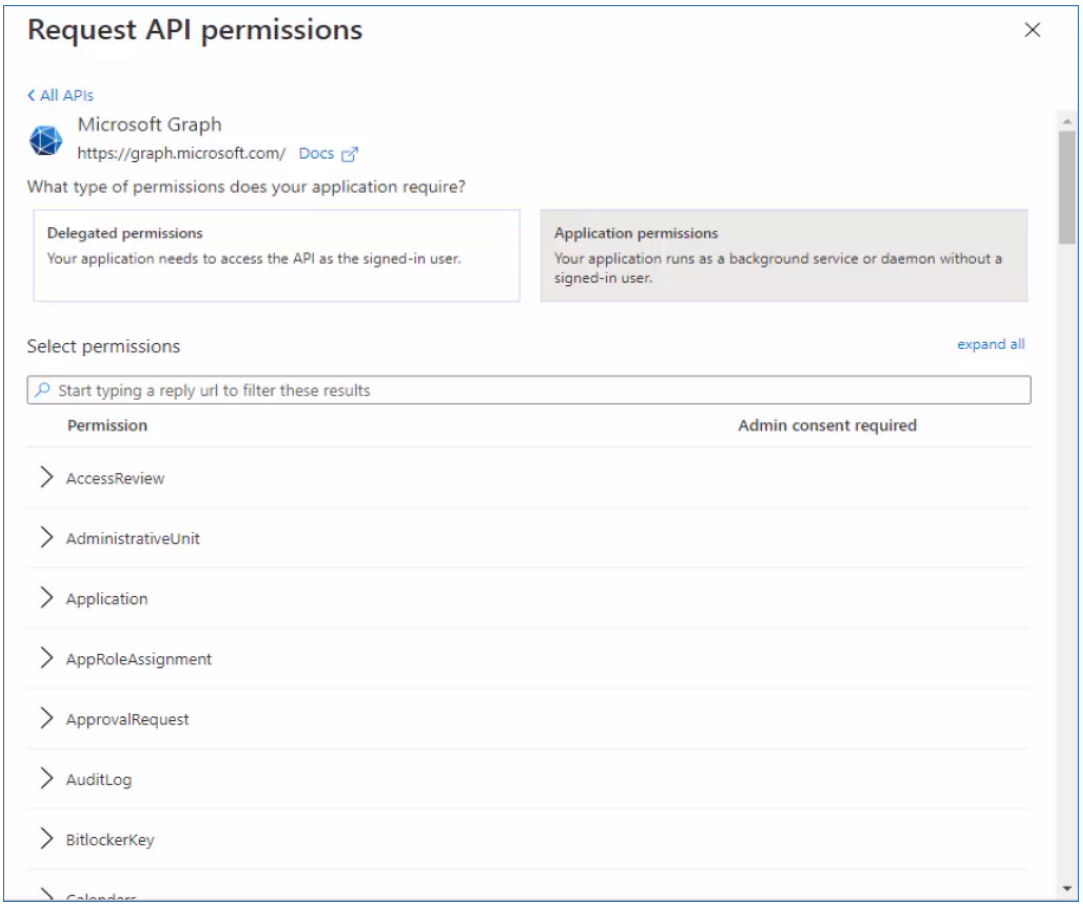
**11b** Click the **Add a permission** tab.




**11c** Click the **Microsoft Graph** API.

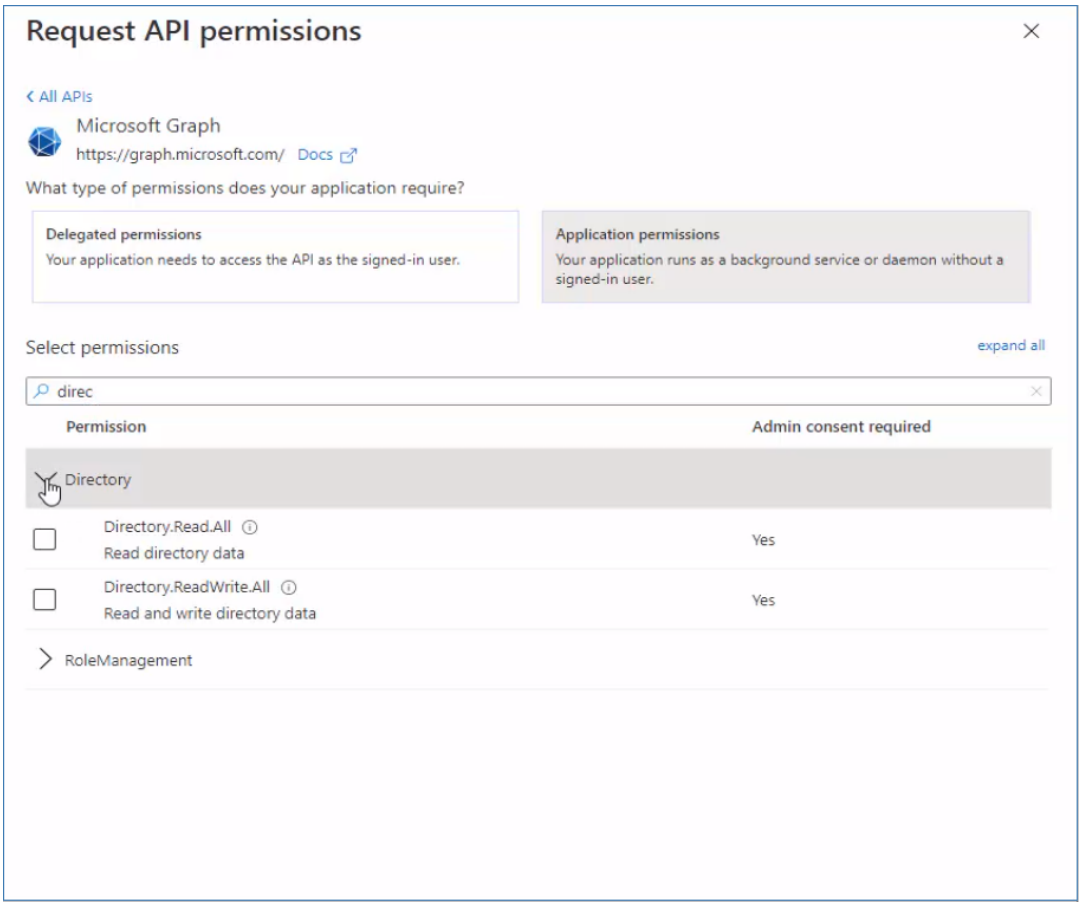



**11d** Click **Application permissions**.




**11e** Referring to the table in Substep 11a, begin typing `directory` to filter on the **Directory** permission.

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




**11g** From the table in Substep 11a, 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 11b-11h to add all of the permissions specified in the table in Substep 11a.

**11j** When finished, remove the **User.Read** permission by selecting it and then in the Remove permission dialog box, click **Yes, remove**.

**12** Set the application permissions for SharePoint.

**12a** Click the **Add a permission** tab.

**12b** Click the SharePoint API.

**12c** Click **Application permissions**.

**12d** Expand the **Sites** permission to display the options.

**12e** Select the **Sites.Full Control.All** option.

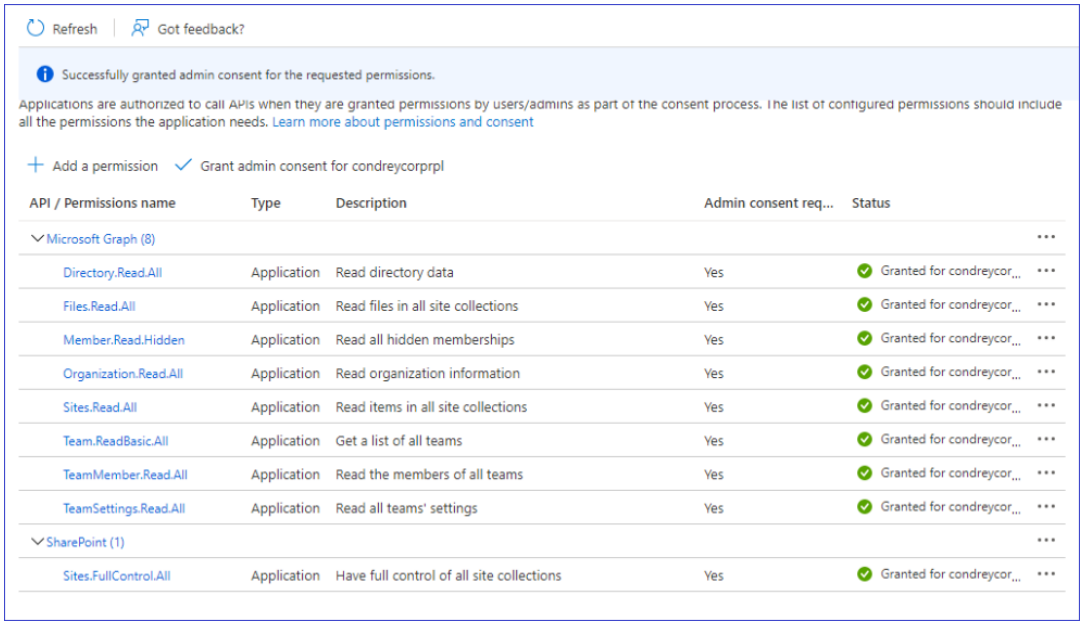
**12f** Click **Add permissions**.

13 Grant admin consent for the tenant.

13a Above the list of permissions that you just established, click **Grant admin consent for *tenant_name***.

13b 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***.




# 9.2 Agent365


- Section 9.2.1, “Minimum Requirements,” on page 83
- Section 9.2.2, “Installation and Configuration,” on page 84


This section includes minimum requirements for hosting and procedures for installing Agent365.

## 9.2.1 Minimum Requirements

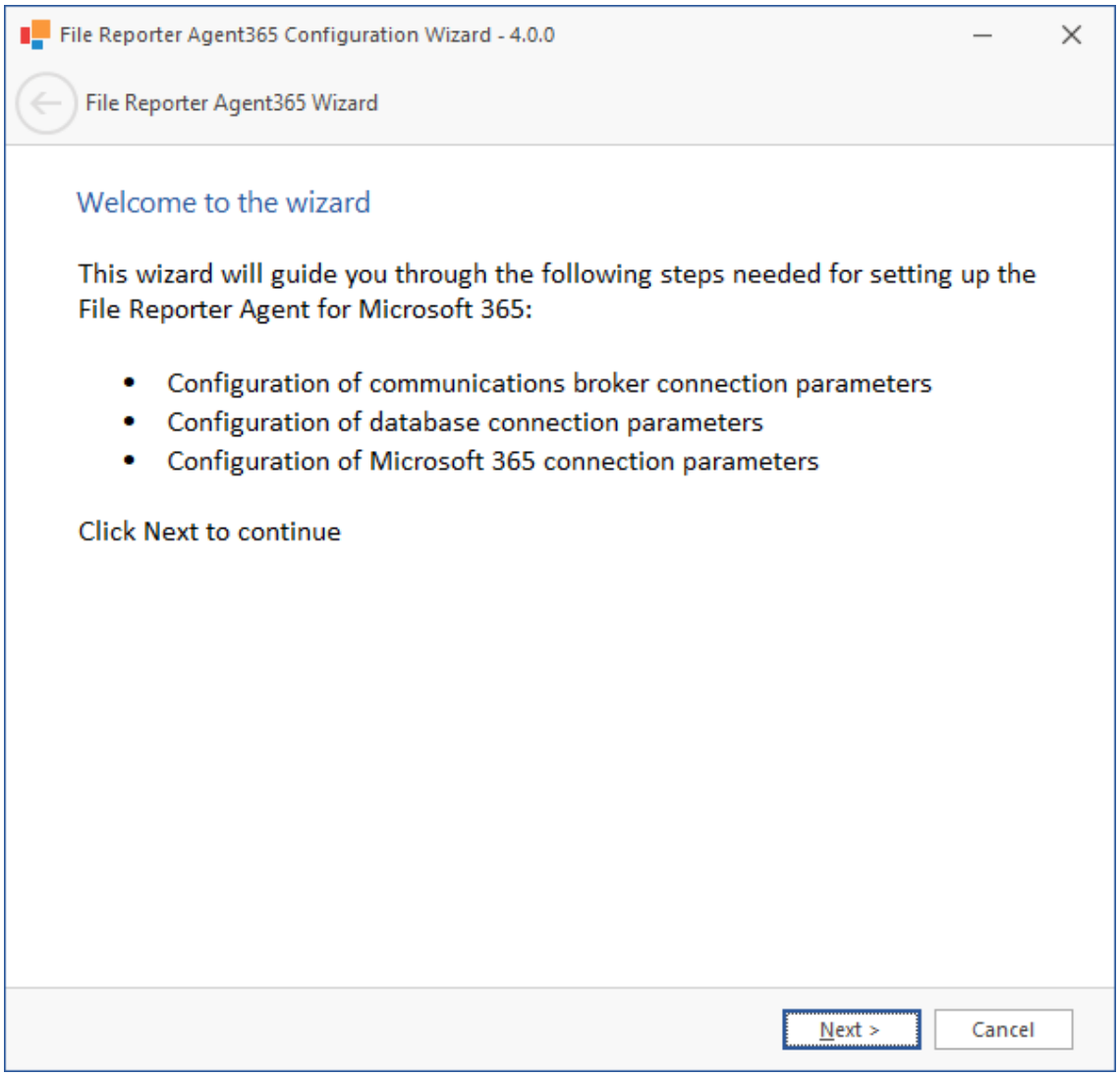
- Any of the following dual core 64-bit processor servers:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
- The server must be joined to Active Directory
- For large tenants, Micro Focus recommends a dedicated server for Agent365
- .NET 6.0 Runtime (this will be installed if not already present)
- Minimum of 200 MB RAM

## 9.2.2 Installation and Configuration

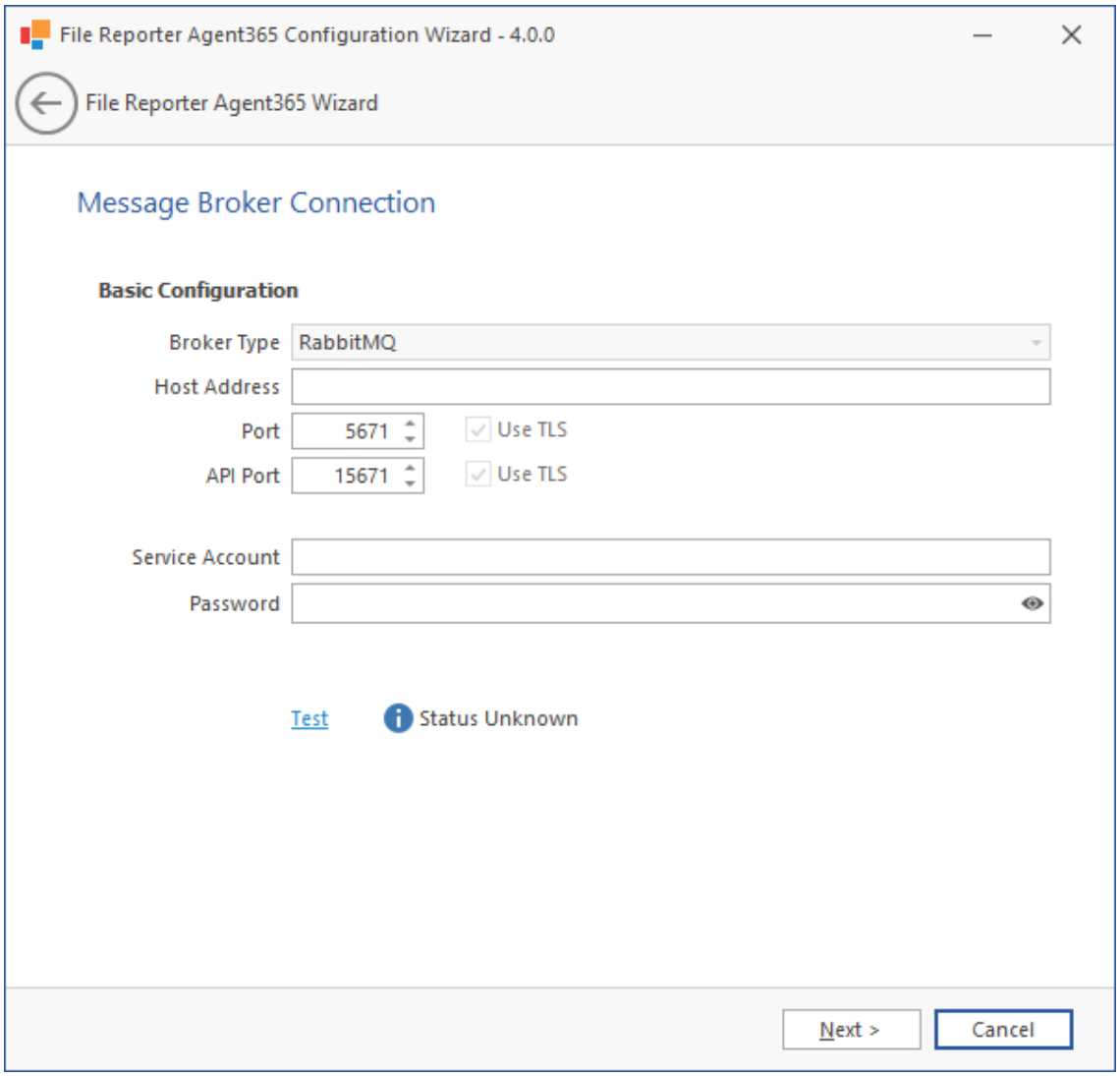
1 At the root of the `FileReporter_4.1.iso` image, double-click `FileReporter-Agent365-4.1.x64-xx.exe`.

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**.




**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.

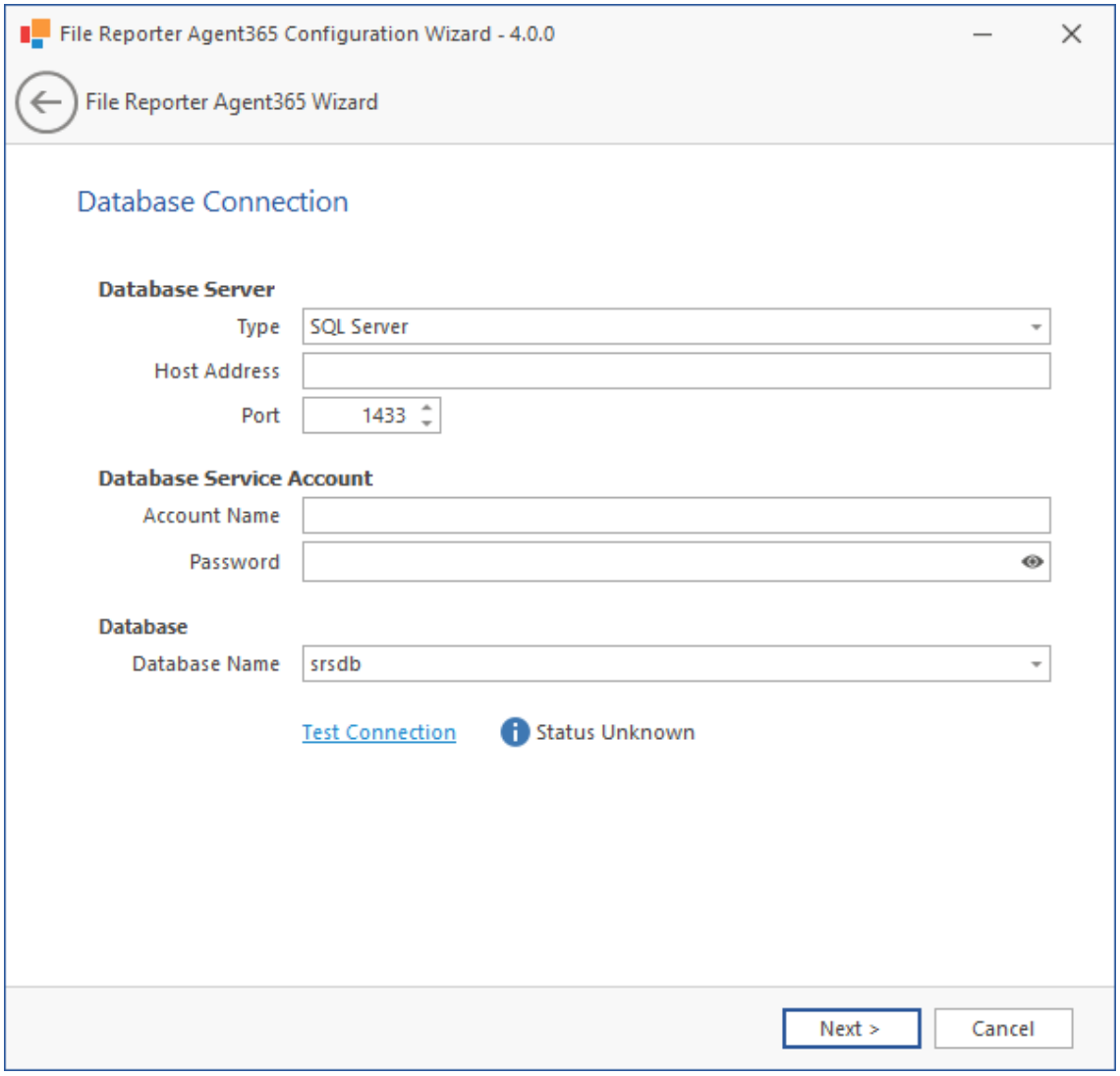
**Service Account:** Enter the name of the service account, which is by default, `srsbroker`.

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**.




**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.

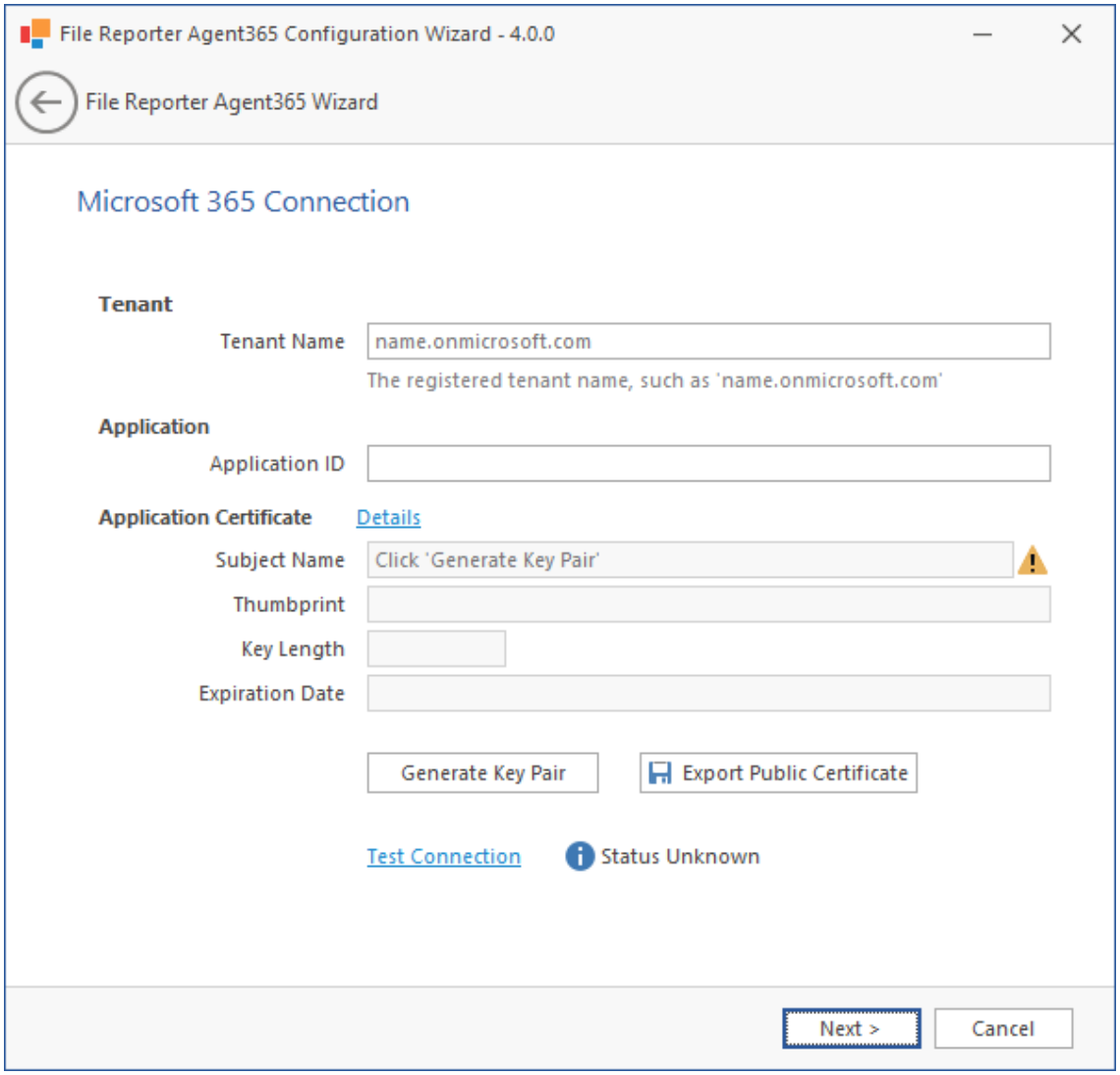
**Password:** Enter the database administrator password.

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

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

**Test Connection:** Click to test the connection between Agent365 and the database.

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



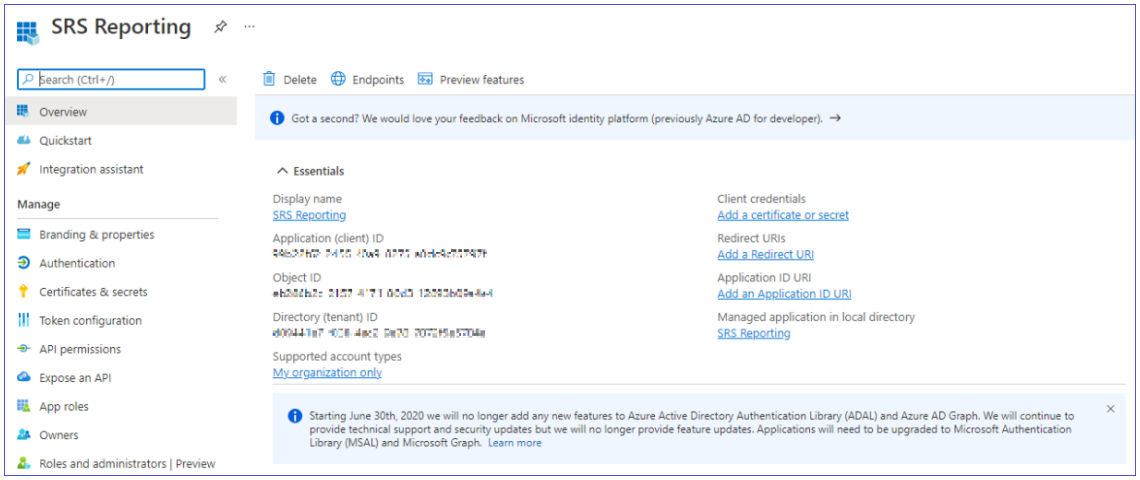

To complete the fields in this page, you will need to log in to your tenant in Azure AD.

**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 Agent365 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:

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

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

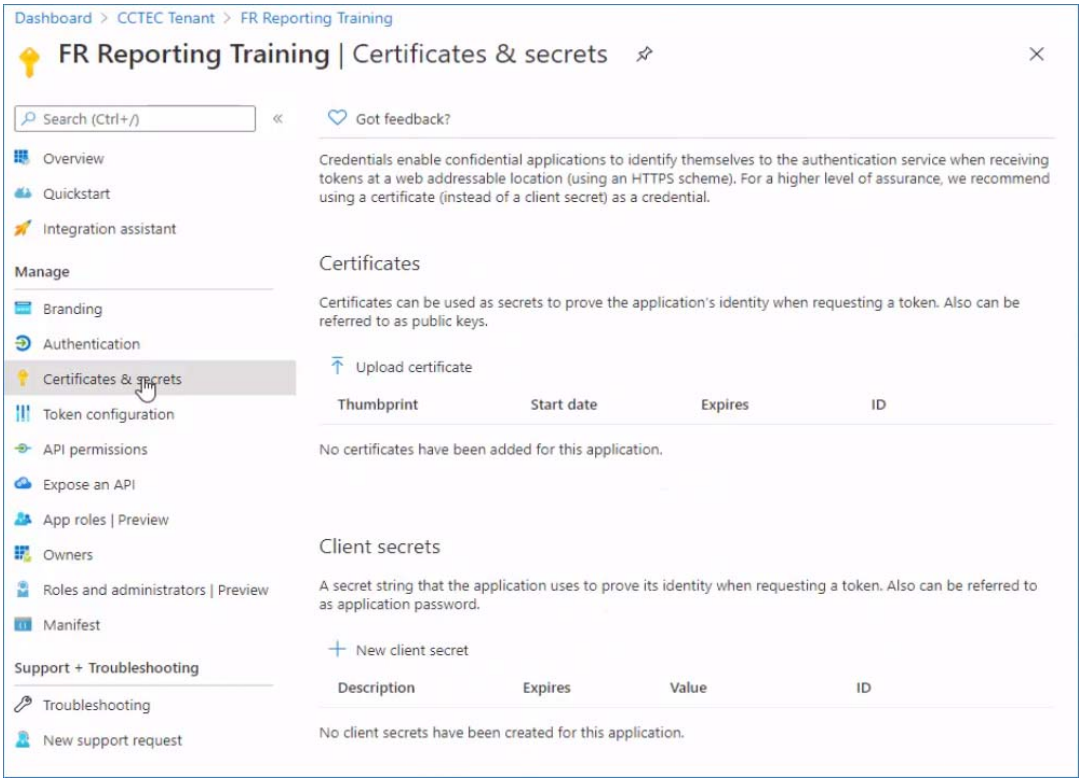
**7e** Click **Generate**.

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.**




**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**.

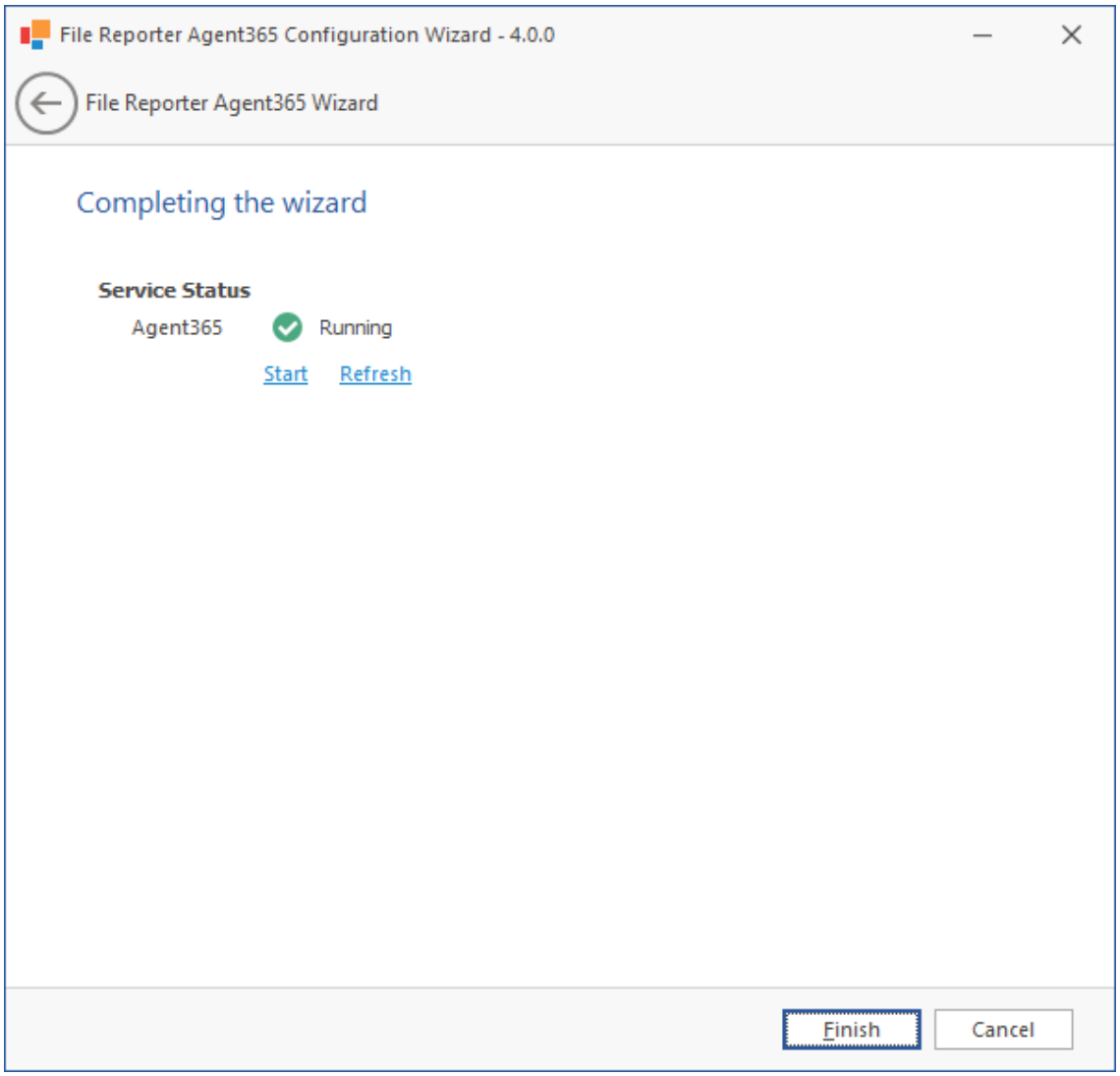
The certificate is now listed in the **Certificates** region of the Azure Active Directory admin center page.

**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**.