opentext™ | File Reporter

Installation Guide

Version 24.4

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.

Condrey Corporation
120 North Laurens St.
Greenville, SC 29601
U.S.A.

https://condreycorp.com/

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 to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth 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 of these elements must fully adhere to and support the appropriate APIs, standards, and protocols 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

This installation guide provides network administrators who manage network storage resources with the concepts and procedures to install and configure File Reporter 24.4.

1 - Upgrading

You can upgrade from any previous version of File Reporter listed in Product Upgrades in the Release Notes.

1.1 - Database

File Reporter 24.4 only supports recent versions of PostgreSQL and Microsoft SQL Server.

- See *Database Instance Configuration (page 19)* for details related to the supported versions and system requirements of each database.

1.2 - License

Upgrading from a previous version of File Reporter requires you to update the license to 7.0.

- See *Licensing the Product (page 17)* for the procedures.

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.

- See *Core Components (page 37)* for the procedures.

1.4 - File System Agents

Upgrade AgentFS by installing the updated package on top of the existing software.

- See *File System Scans (page 63)* for the procedures.

Upgrade the ManagerFC, AgentFC, and RabbitMQ components by installing the updated packages on top of the existing software.

- See *File Content Scans (page 71)* for the procedures.

1.5 - Microsoft 365 Reporting

Upgrade Agent365 by installing the updated package on top of the existing software.

- See *Agent365 (page 92)* for the procedures.

1.6 - RabbitMQ Message Broker

RabbitMQ should be updated to a recent supported version.

- See *RabbitMQ Configuration (page 29)* for procedures on updating RabbitMQ if installed from a previous version of the File Reporter media.
- For all other installations, follow the upgrade instructions provided with that distribution.

2 - Deployment Planning

You can install File Reporter to work in a variety of configurations. Before installation, you should determine how best to deploy File Reporter to meet the needs of your organization.

2.1 - Requirements Overview

Review the following table before installing File Reporter 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. • The installer and configuration utilities configure IIS automatically and manage most aspects of the installation for you. • The Engine and Web Application must run on the same system in this release of the software.
DNS	You must use the site hostname registered with IIS to access the File Reporter Web Application with a browser (i.e., the raw IP address does not work). • You must either create a DNS entry for the name in the environment, or add the entry to the `hosts` file on every machine accessing the File Reporter system.
Database	File Reporter utilizes a PostgreSQL or Microsoft SQL Server database as the back-end data store. • The database must be accessible from the server running the Engine.
Active Directory and Windows Server	To report on Active Directory and Windows file systems, File Reporter uses a proxy object and group in Active Directory that is used by the system as part of day-to-day operations. • You should understand basic Windows file system and Active Directory terminology and operations, and be familiar with the

Technology	Notes
	Windows network that you will report against with File Reporter.
Message Broker	File Reporter uses the RabbitMQ message broker to enable messaging between the File Reporter components required for file content scanning (ManagerFC and AgentFC) or Microsoft 365 scanning (Agent365).

2.2 - Engine Host

The server hosting the Engine service should have significant CPU, disk, and memory resources for all but the smallest installations.

- The Engine runs on any of the following Windows Servers:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
- The Engine host must be joined to the domain.

NOTE: You should install the Engine on a member server and not on a domain controller, as this may become a requirement in a future release.

2.3 - File Content

File Reporter can scan and classify file content. For example, you can scan for files containing US Social Security numbers and then classify these files as restricted documents with access permissions and storage locations that may need to be corrected.

You must install the following additional components to scan Windows network storage devices for file content:

- ManagerFC
- AgentFC
- RabbitMQ message broker

See File Content Scanning in the *File Reporter 24.4 Administration Guide* for details.

2.4 - Microsoft 365

File Reporter 24.4 now scan and report on the metadata and permissions of files stored in OneDrive for Business, SharePoint Online, and Teams.

You must install the following components to scan and report on these Microsoft 365 cloud-stored files:

- Agent365
- RabbitMQ message broker

2.5 - File System Agents

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

When deciding whether to install AgentFS locally on a Windows server or run the AgentFS service as a proxy, be aware that:

- 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. Consider using a proxy rather than installing the agent locally if the server's resources are already constrained.

2.6 - Database Planning

Consider the following guidelines before installing and configuring any database system for File Reporter.

2.6.1 - Determine Database Type

You can use either a PostgreSQL database or a Microsoft SQL Server database.

- You may prefer a PostgreSQL database if you are proficient with Linux.
- You may prefer Microsoft SQL Server if you have a Microsoft Licensing Agreement that entitles you to Microsoft SQL Server. **NOTE:** File Reporter supports Standard and Enterprise versions of SQL Server, but does *not* support Web or Express editions.

2.6.2 - Use a Dedicated Server

Due to the potential size of the collected scan data and the I/O processing required for large database installations, you should install the database on a dedicated server.

- See *PostgreSQL - Minimum Requirements* or *Microsoft SQL Server - System Requirements* for minimum requirements.

2.6.3 - Use a Dedicated Database Instance

Use a dedicated PostgreSQL cluster or SQL Server instance to prevent conflicts with other vendor software.

File Reporter requires access at the instance level to manage the database security principals and roles. In addition, File Reporter ships with optional CLR extensions for SQL Server, which require enablement at the instance level.

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 I/O intensive, especially the persisted storage on disk. For best performance…

- Provide SSD 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, provide at least 10 GB or more throughput (ideally, the SAN link should be faster than the I/O capacity of the back-end storage system, so that it is not the bottleneck).
- 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.

See https://msdn.microsoft.com/en-us/library/ms189133.aspx for procedures on moving database files after installing a SQL Server instance.

For PostgreSQL, moving database files is a simple process: Stop the database server, relocate the `pg_xlog` folder, and then create 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.

*See https://msdn.microsoft.com/en-us/library/ms189563.aspx. for information about SQL Server filegroups.

**See https://www.postgresql.org/docs/current/static/manage-ag-tablespaces.html for information about PostgreSQL tablespaces.

3 - Licensing the Product

This section provides an overview of license types and procedures for managing the license.

3.1 - License Overview

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

For individuals evaluating File Reporter, you can obtain a full-featured limited-time license of the core product.

3.1.1 - License Version

File Reporter 24.4 requires a File Reporter 7.0 license.

3.2 - Updating a License

After you have installed File Reporter, you can update your evaluation license or production license by simply replacing the old license with the new one. For more information, see *Installing or Updating the License (page 39)*.

3.3 - Obtaining an Evaluation License

To schedule a product demonstration or obtain an evaluation license for File Reporter, email support@filereportersupport.com.

Upon receiving an evaluation license install it following the instructions at *Installing or Updating the License (page 39)*.

3.4 - Obtaining a Production License

3.4.1 - Obtain the Activation Code

In order to obtain a production File Reporter 24.4 license file, you will first need to retrieve your activation code from the OpenText software license site.

NOTE: For instructions on downloading and activating the software, go to https://sld.microfocus.com/mysoftware/contact/softwareContact.
The Quick Start Guide and video links can assist with the steps needed to activate the software.

1. In a web browser, go to https://sld.microfocus.com/mysoftware/index.
2. Follow the steps required to activate File Reporter 24.4.

3. Once you have the activation key, have it ready for the next steps when obtaining the license file.

3.4.2 - Obtain the License File

1. In a web browser, go to https://filereportersupport.com/License.
2. Fill out the form providing the required information.
3. Be sure to select version **7.0** for the product version and to enter the correct *Forest Root Name* against which this product will be licensed.
4. For the *License Type* select **Activation**.
5. Enter the *Licensed Seats Count*.
6. Enter the *Activation Code* using the code you obtained from the customer center site earlier.
7. After submitting the form, you will receive an email.
8. Open the email and click **Download License File**, which will present you access to the license file.
9. Install the license following the instructions at *Installing or Updating the License (page 39)*.

4 - Database Instance Configuration

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 *Database Planning (page 15)*.

4.1 - PostgreSQL

4.1.1 - Supported Versions

File Reporter24.4 supports the following versions of PostgreSQL:

- PostgreSQL 17
- PostgreSQL 16
- PostgreSQL 15

4.1.2 - 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:

  - Red Hat Enterprise Linux (RHEL)
  - SUSE Linux Enterprise Server (SLES)
  - 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 the 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.

4.1.3 - Installing and Configuring a PostgreSQL Database

Review the following links for the procedures to install and configure PostgreSQL:

- 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

Follow the references that are specific to the version of PostgreSQL installed in your environment.

4.1.4 - Adding Required Extensions

File Reporter requires the `pgcrypto` PostgreSQL extension.

If the extension has not been installed you will see an error similar to the following when running the File Reporter database configuration utility:

```
Error: 0A000: extension "pgcrypto" is not available
Detail: could not open extension control file
"/usr/share/postgresql15/extension/pgcrypto.control": No such
file or directory
```

NOTE: For details on installing the `pgcrypto` extension please refer to the documentation included with the PostgreSQL package or source used to install the database service.

When using a pre-packaged version of PostgreSQL such as those included with many Linux distributions, you may need to install the **postgresql-contrib** package.

4.2 - Microsoft SQL Server

4.2.1 - Supported Versions

File Reporter 24.4 supports the following versions of SQL Server:

- SQL Server 2022
- SQL Server 2019

4.2.2 - System Requirements

- Any Microsoft supported platform for SQL Server on Windows Server or Linux.
    - https://learn.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-2022

  - https://learn.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-2019
  - https://learn.microsoft.com/en-us/sql/linux/sql-server-linux-overview
- Minimum 16 GB RAM

  Depending on the size and frequency of your scans, you might need significantly more RAM

4.2.3 - Supported Editions

The following editions of SQL Server are supported in production:

- SQL Server Enterprise
- SQL Server Standard

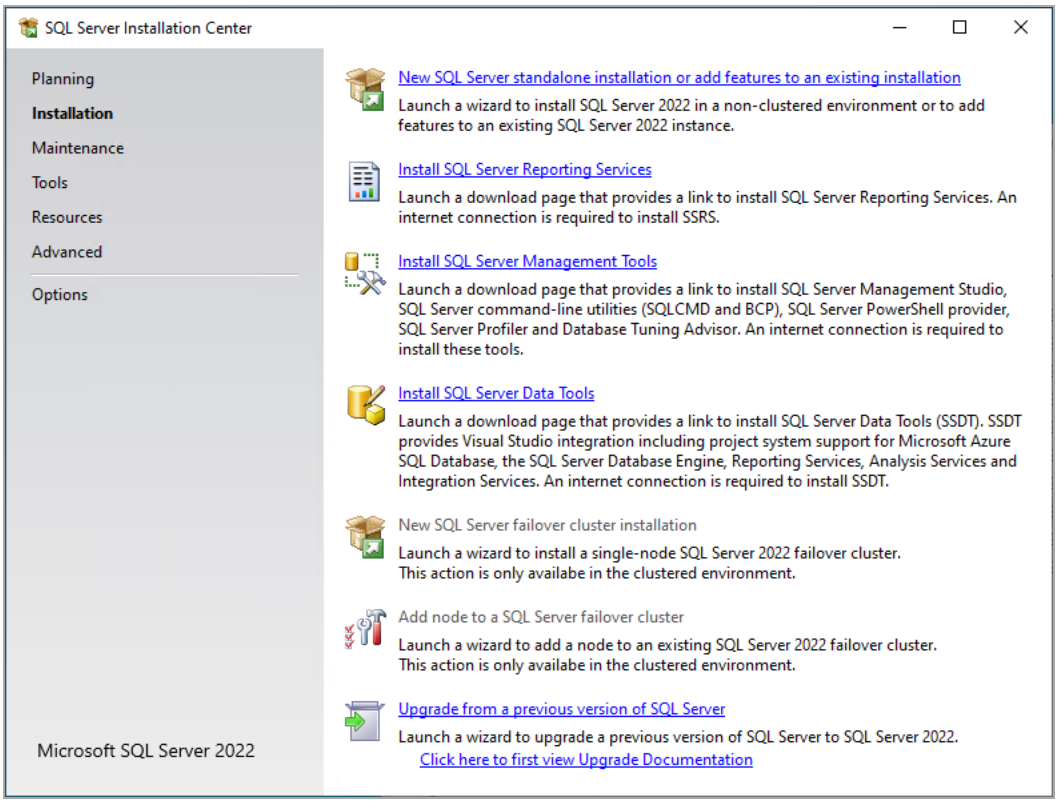
IMPORTANT: Due to considerations with security and Unicode collation support, we strongly recommend installing a dedicated instance of SQL Server for File Reporter .

4.2.4 - Install a New Instance of SQL Server

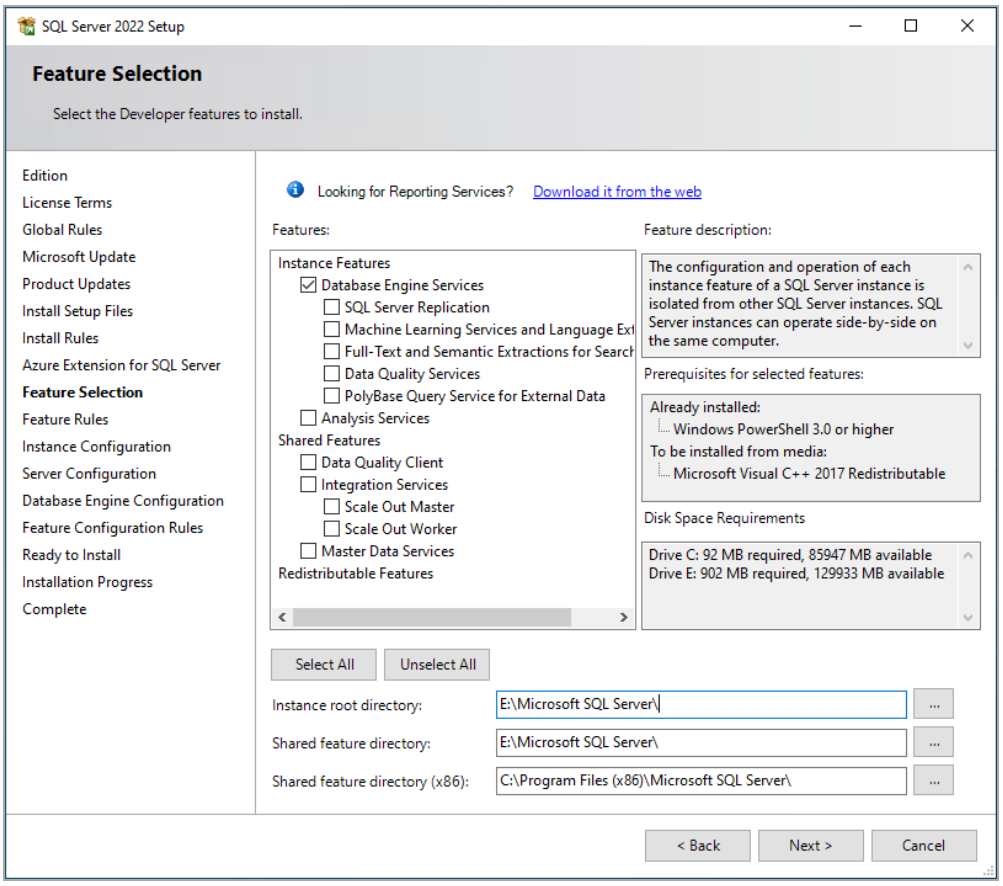
The following procedures are specific to Microsoft SQL Server 2022. Procedures will vary based on your version of SQL Server.

These instructions assume that you are installing a single instance of SQL Server on a Windows Server host with no Azure integration.

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. Complete the following forms in the SQL Server Setup wizard:
    a. *Edition* - select the SQL Server edition, enter the product key, select the license option, then click **Next**.
    b. *License Terms* - accept the license terms and click **Next**.
    c. *Global Rules* - view the results then click **Next**.
    d. *Microsoft Update* - click *Use Microsoft Update to check for updates* then click **Next**.
    e. *Install Rules* - review the results then click **Next**.
    f. *Azure Extension for SQL Server* - uncheck **Azure Extension for SQL Server** then click **Next**.
    g. *Feature Selection* - check **Database Engine Services**.



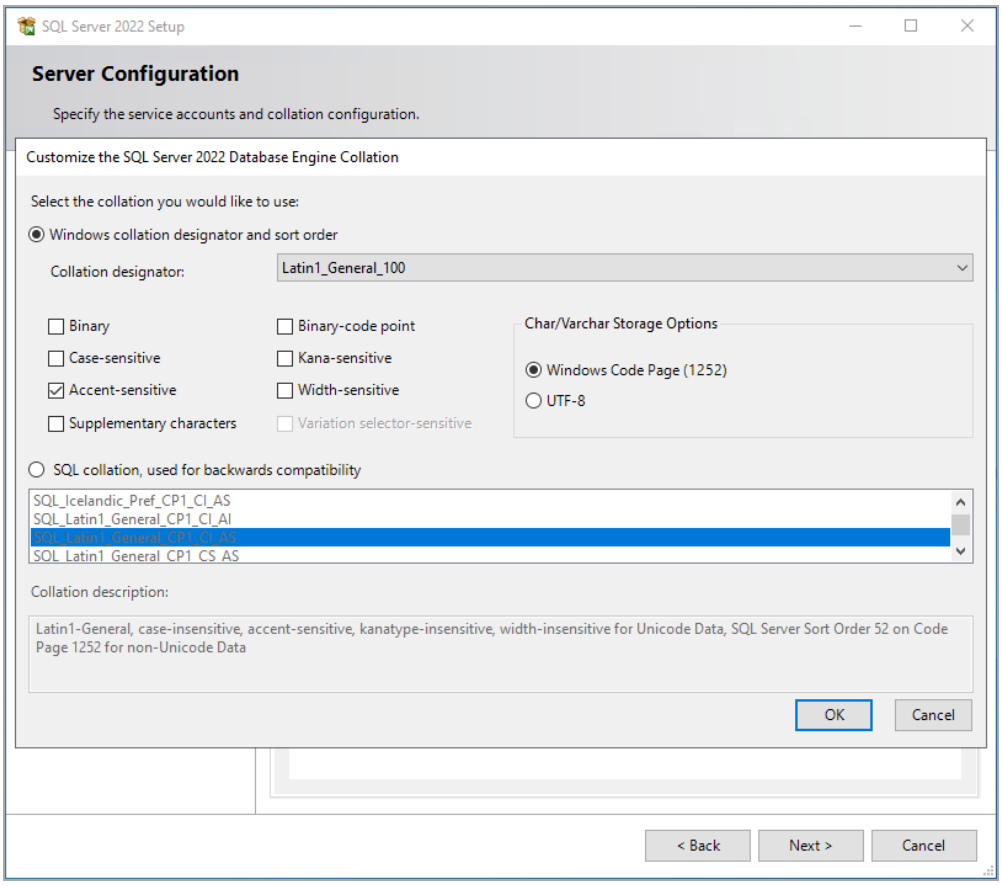
Review the installation paths then click **Next**.

> **NOTE:** For larger installations consider installing the SQL Server instance on a separate volume by changing the *Instance Root Directory* path parameter.

h. *Feature Rules* - review the results then click **Next**.

i. *Instance Configuration* - Select the appropriate instance type, modify the *Instance ID* if desired, then click **Next**.

j. *Server Configuration* - select the **Collation** tab then click **Customize**.



- Select **Windows collation designator and sort order** then select your desired collation.

  If possible select a collation that aligns with the Windows Server hosting the 24.4 Engine.

  If you are unsure which collation to use, select **Latin1_General_100** which is a safe option for File Reporter.

  > **NOTE:** Select one of the *_100 or later collations as these offer the best compatibility for advanced options such as *Supplementary characters*.
  >
  > For more information on collation and locales, refer to this Microsoft document: https://learn.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support.

IMPORTANT: 24.4 requires the use of a Windows collation. Legacy SQL collations are not supported.

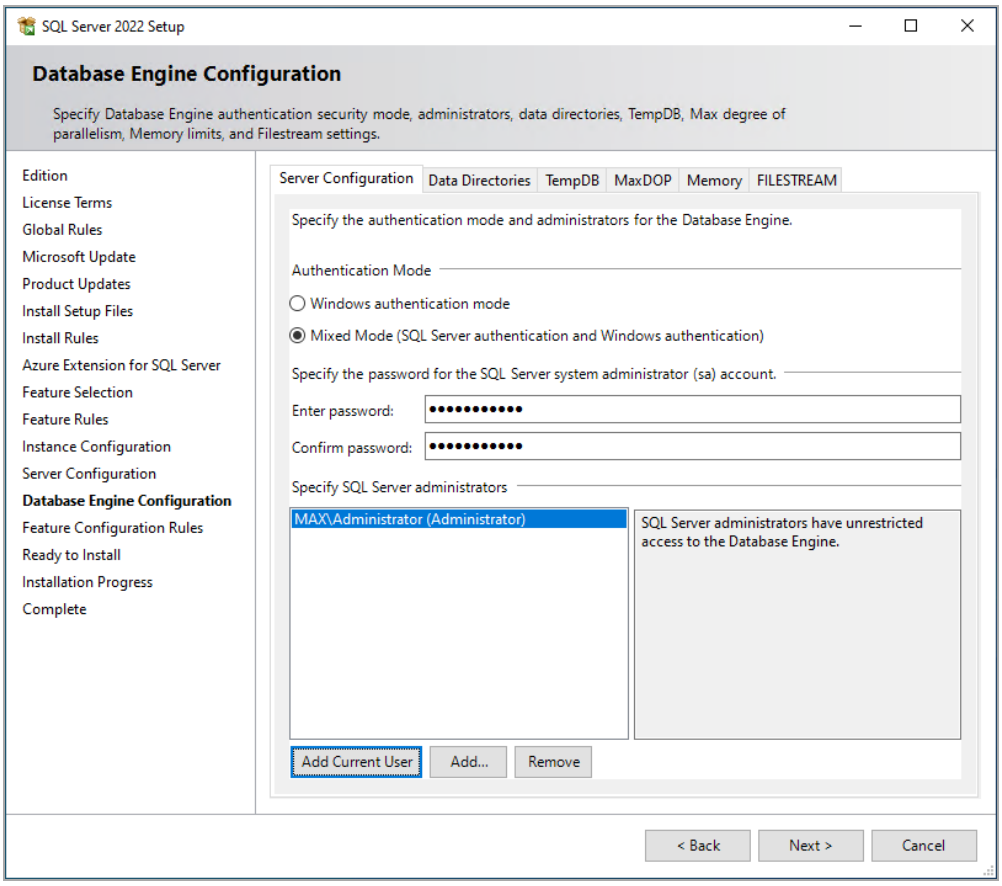
- [Optional] Select **Accent-sensitive** and **Supplementary characters**.
- [Optional] Select options for Kana-sensitive, Width-sensitive, and Variation selector-sensitive if you understand their impact with specific Asian character sets.
- Deselect all other options.
- Select **Windows Code Page (1252)** for the *Char/Varchar Storage Options*.

IMPORTANT: File Reporter does not support the use of UTF-8 as a character storage option at this time.

Click **OK** to close the Collation customization dialog then click **Next**.

Database Engine Configuration - perform the following operations in this panel:

- Select **Mixed Mode (SQL Server authentication and Windows authentication)**.
- Enter a password for the sa account in the *Enter password* and *Confirm password* fields.
- Click **Add Current User** to add your current account to the *SQL Server administrators* list.



Review your selections then Click **Next**.

k. *Feature Configuration Roles* - review any messages then click **Next**.

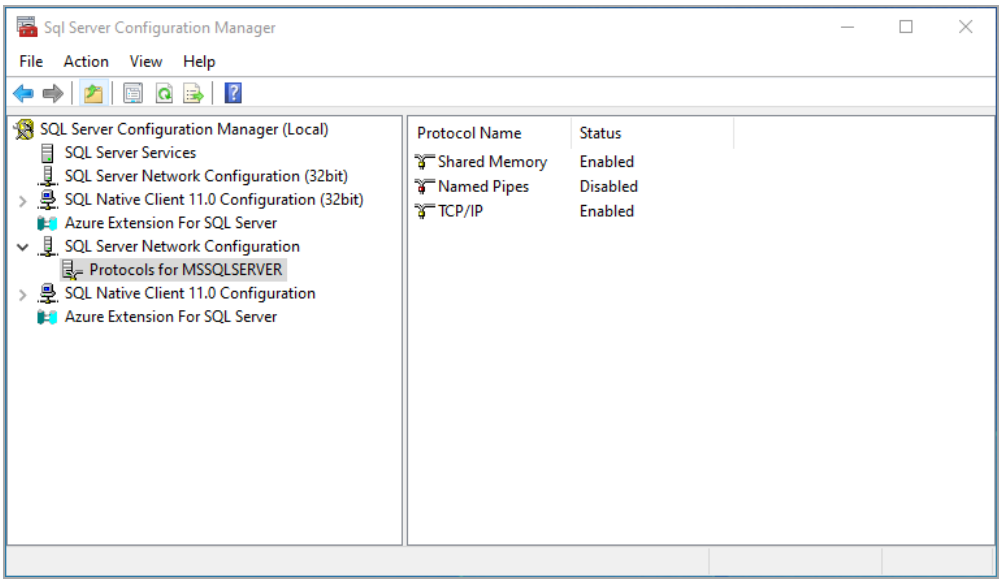
l. *Ready to Install* - perform a final review of all installation options then click **Install**.

m. *Complete* - once the installation is complete click **Close** to exit the setup wizard.

5. From the Windows Start Menu launch **SQL Server Configuration Manager**.

   a. In the left pane, expand **SQL Server Network Configuration**.

   b. Click **Protocols for MSSQLSERVER** (or the name of the database instance you chose earlier).



c. Right-click *TCP/IP* and select **Properties**.

d. Click the **Protocol** tab.

e. Set the *Enabled* field to **Yes**.

f. Set the *Listen All* field to **Yes**.

g. Click the **IP Addresses** tab.

h. Under the *IPAll* heading at the bottom, set the TCP Port field to `1433`

i. Click **OK**.

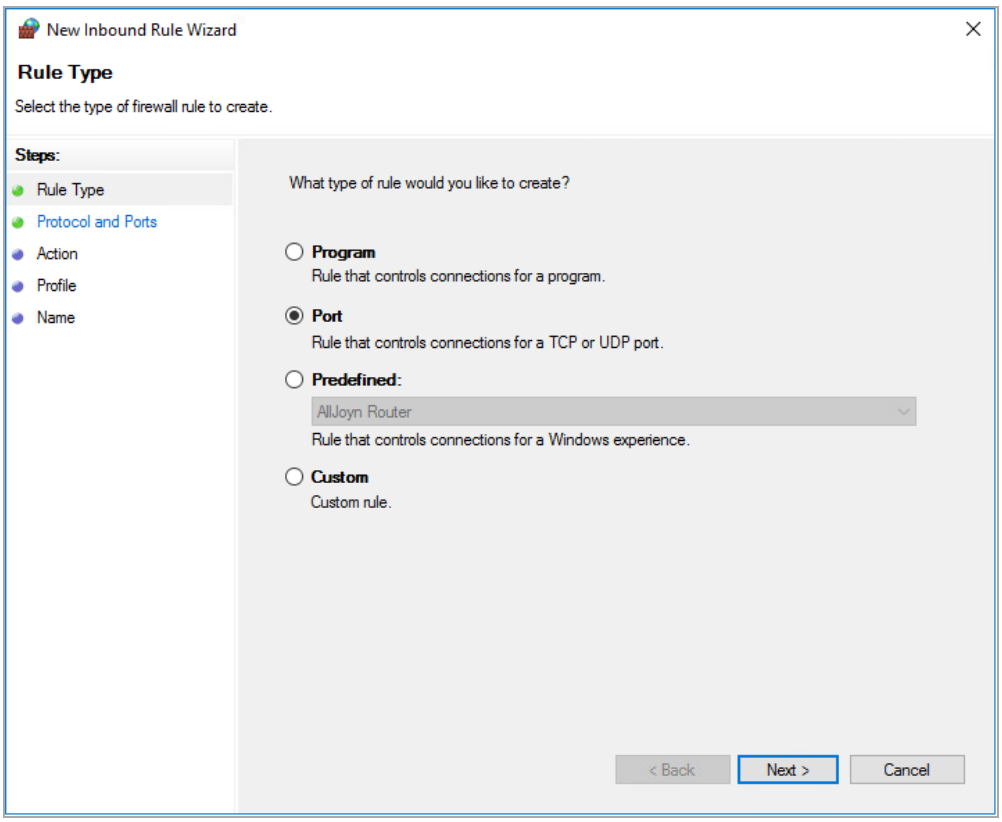
j. Close the SQL Server Configuration Manager.

6. Launch Windows Firewall with Advanced Security.

   a. From the left column, click **Inbound Rules**.

   b. From the *Actions* column, click **New Rule**.

c. In the Rule Type page, select **Port**.



d. Click **Next**.

e. In the Protocol and Ports page, enter `1433` in the *Specific local ports* field, then click **Next**.

f. In the Action page, accept the default setting by clicking **Next**.

g. In the Profile page, accept the default settings by clicking **Next**.

h. In the Name page, specify a name for the new inbound rule in the *Name* field.

   For example, `SQL Server`.

i. Click **Finish**.

5 - RabbitMQ Configuration

RabbitMQ is an open-source message broker that enables messaging between the File Reporter components used for file content scanning or for reporting on Microsoft 365 cloud applications such as OneDrive, SharePoint Online, and Teams.

These components include ManagerFC and AgentFC for content scanning and reporting, and Agent365 for Microsoft 365 cloud reporting. If you do not need to perform file content scanning or reporting on Microsoft 365 cloud applications, then you do not need to install RabbitMQ.

RabbitMQ can be installed using any of the supported distributions found at: https://www.rabbitmq.com/download.html.

To introduce RabbitMQ into the File Reporter framework, a simplified, supported distribution for Windows is included with this release. This distribution is meant solely for use in basic scenarios in which clustering, containerization, or automated upgrades are not required.

The installation steps in this chapter pertain solely to this included distribution. Refer to associated product documentation for other RabbitMQ distributions or installers.

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 File Reporter component. If you installed RabbitMQ previously, you should upgrade to the updated version provided.

Before upgrading...

1. Verify that all scans are completed or canceled.
2. Uninstall the service.
    a. Stop the RabbitMQ service (console command: `sc stop rabbitmq`).
    b. Within the existing RabbitMQ folder, run `remove-rabbitmq-service.bat`.
3. Delete the existing RabbitMQ folder.
4. Follow the steps in the remainder of this chapter to install and set up the new version.

5.2 - Extracting RabbitMQ

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 may already be present. If not:

1. Install the most recent Visual C++ Redistributable Packages for Visual Studio 2015 found either at https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-

redist?view=msvc-170, or in the RabbitMQ folder of the `FileReporter-24.4.iso` image named `vc-redist-vs2015-2022-x64-*.exe`.

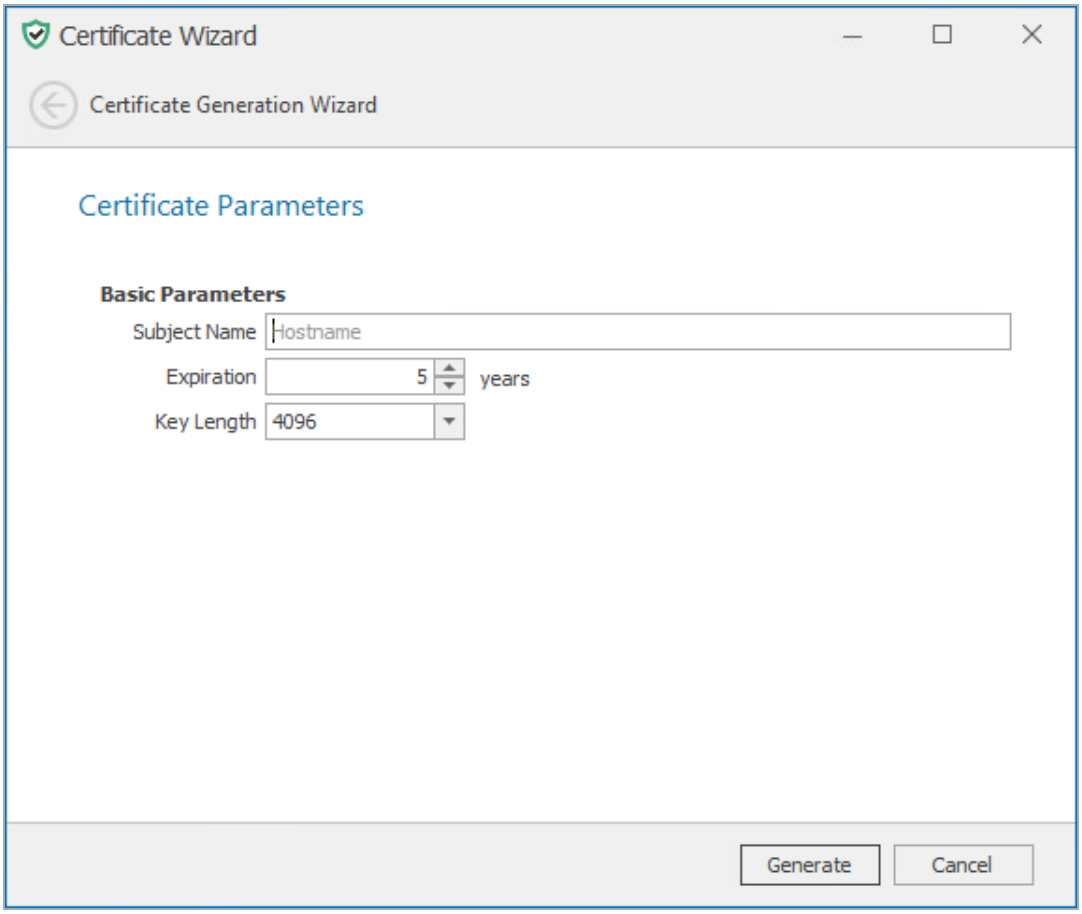
2. Unzip the `RabbitMQ-3.9.x.zip` file to the desired path in the RabbitMQ folder of the `FileReporter-24.4.iso` image.

> **IMPORTANT:** The path cannot contain spaces. The zip file contains the `rabbitmq` folder (i.e., extracting to the root `C:\` produces an install location of `C:\rabbitmq`.

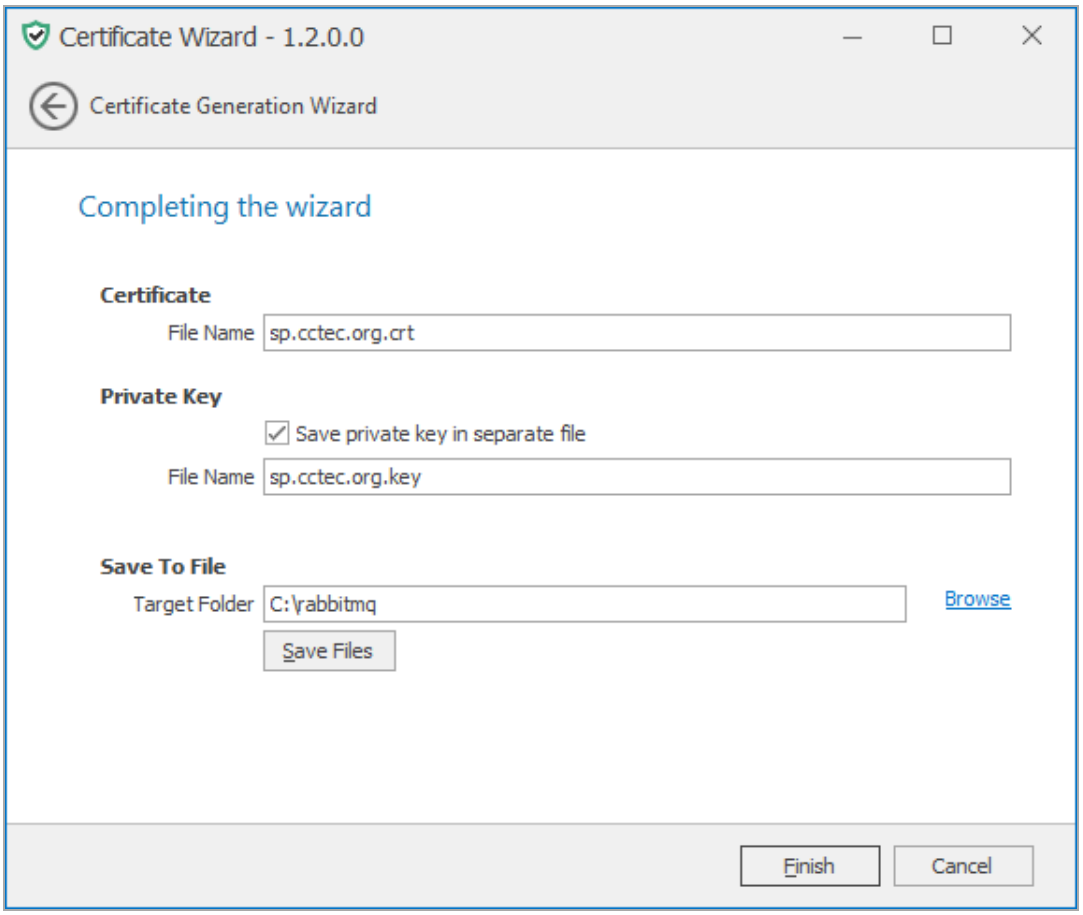
5.3 - Creating Certificates for RabbitMQ

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

1. Double-click `CertificateGenerator.exe` in the RabbitMQ folder of the `FileReporter-24.4.iso` image.



2. Enter the DNS name for the RabbitMQ service host or endpoint in the *Subject Name field.*
3. (Optional) Modify the settings in the other fields.
4. Click *Generate*.



5. Enter the desired name of the certificate file to export in the *File Name* field of the *Certificate* section.
6. (Optional) Check *Save private key in a separate file* in the *Private Key* section and then enter a value for *File Name* for the private key file to export.
7. Enter a path for the *Target Folder* into which the certificate and key file(s) will be exported in the *Save to File* section.

> **IMPORTANT:** The path should not contain spaces. You should export the certificate files to the root of the extracted RabbitMQ folder.

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

9. Click *Finish*.
10. From the location where the files were generated, copy the files to a folder on the RabbitMQ system (e.g., to the RabbitMQ folder created when you extracted the `RabbitMQ-3.9.xx.zip` file).
11. Edit the `rabbitmq.conf` file located in the `rabbitmq\base` folder to which RabbitMQ was extracted (if using the provided archive).
12. 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`
13. Modify the entries for `management.*` interface.

    Optionally comment the following lines:

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

    Uncomment the following lines:

    - `management.ssl.port`
    - `management.ssl.cacertfile`
    - `management.ssl.certfile`
    - `management.ssl.keyfile`
    - `management.ssl.versions.1`
    - `management.ssl.versions.2`
14. Specify the certificate and private key.
    a. Modify the paths for `ssl_options.cacertfile` and `ssl_options.certfile` in the TLS Options section with the path to the RabbitMQ certificate you created.
    b. While still in the TLS Options section, modify the path for `ssl_options.keyfile` with the path of the private key.
    c. Modify the paths for `management.ssl.cacertfile` and `management.ssl.certfile` in the Management Interface / REST API section

with the path to the certificate. Note that paths are absolute and use forward slashes.

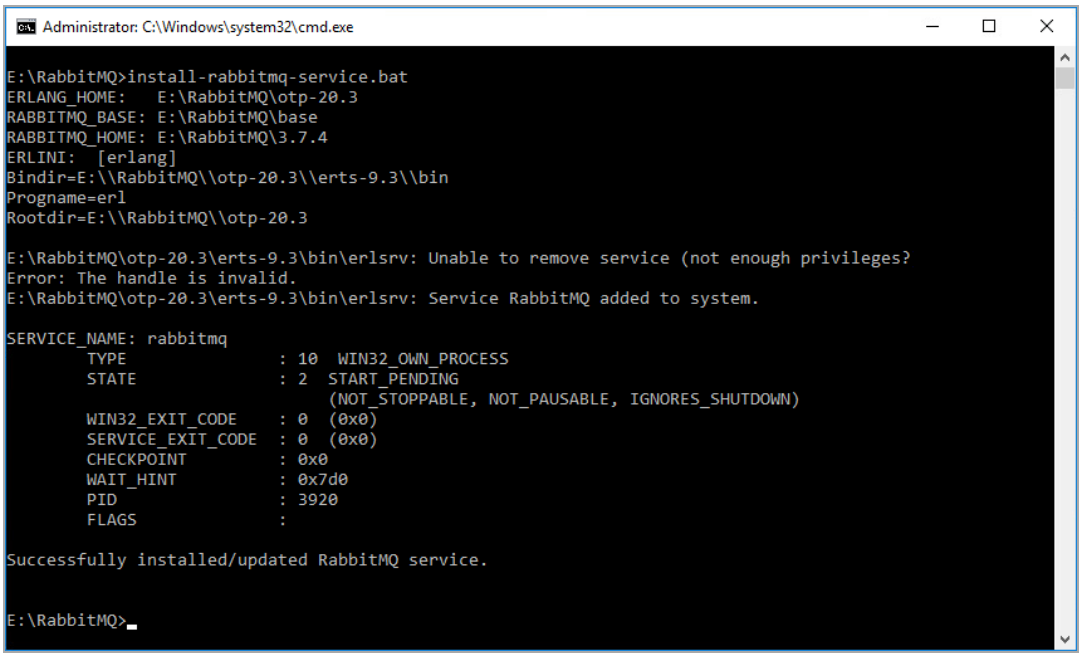
d. While still in the Management Interface / REST API section, modify the path for `management.ssl.keyfile` with the path of the private key.

```
# ------------------------------
# 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
```

15. Save any modifications you made to the configuration file, then close the editor.

5.4 - Installing the RabbitMQ Service

1. Double-click the `rabbitmq` folder from the extracted RabbitMQ files.
2. Double-click the `install-rabbitmq-service.bat` file. The RabbitMQ service is now installed.



The error message: `The handle is invalid` in the image above is normal during an installation and can be ignored.

3. Access the management interface for RabbitMQ at https://*dns_name*:15671. You may need to open this port 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. Access the web-based RabbitMQ management interface at https://*server*:15671, where *server* is the address or DNS name of the server on which RabbitMQ is installed.
2. Enter `admin` in the *Username* field and `srsadmin` in the *Password* field, then click Login.

3. Click the *Admin* tab.

4. Click *admin* under the *Name* column.

5. Scroll down in the new window and select *Update this user*.

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

6 - Core Components

File Reporter 24.4's base components include the Engine and Scan Processor, a database, and a Web Application. The following instructions cover the installation and configuration of these components.

6.1 - Prerequisites

- A new host record in DNS created for use with the Web Application (e.g., `webapp.cctec.org`).
- Optional components for File Content scanning or Microsoft 365 environments also require a message broker – see *RabbitMQ Configuration (page 29)* for details.

6.2 - Engine Minimum Requirements

- Quad-core 64-bit processor or better.
- 16 GB RAM (you may need significantly more RAM, depending on the size and frequency of your reports).
- 20 GB free space for installation files and scan processing space.
- Supported operating systems:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
- Active Directory requirements:
  - The server must be joined to Active Directory.
  - Minimum forest functional level of Windows 2003.

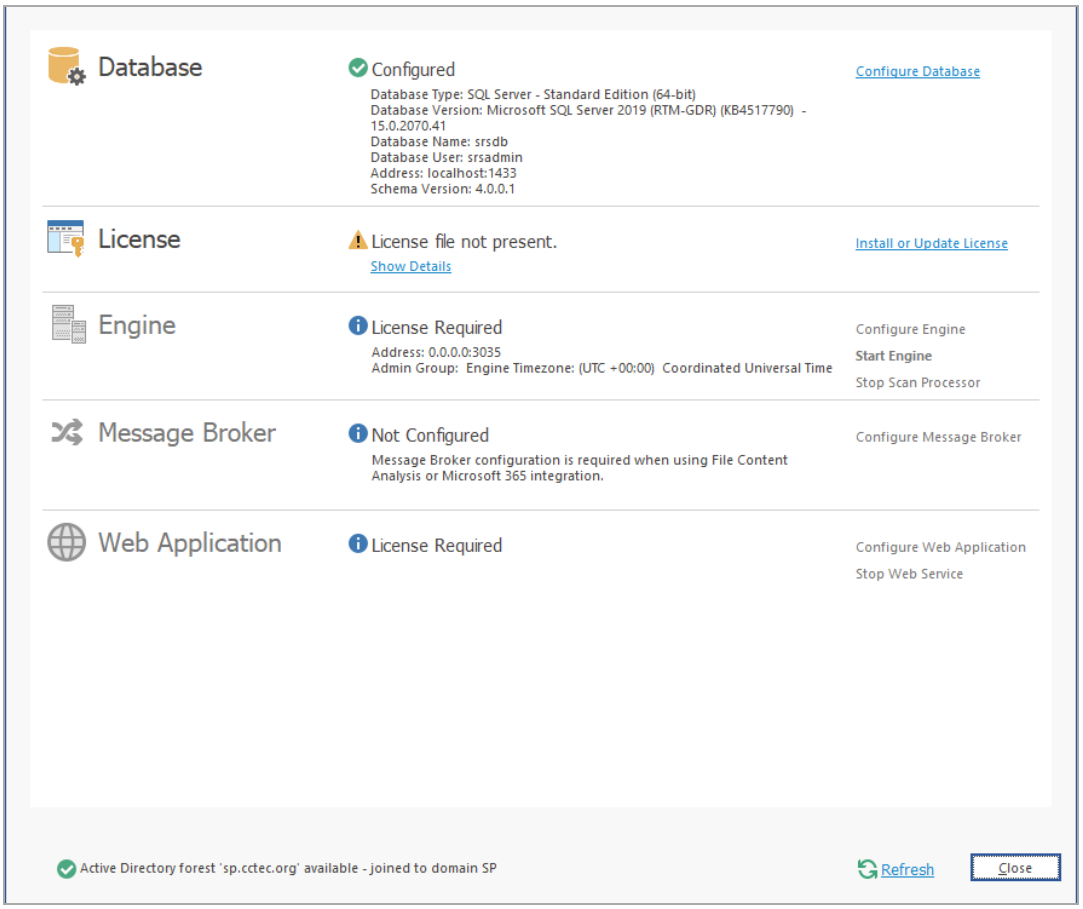
6.3 - Installing the Engine

IMPORTANT: To install the Engine, you must be logged in as a domain administrator for the domain in which the computer is a member.

1. Double-click `FileReporter-Engine-24.4-x64-xxx.exe` at the root of the `FileReporter-24.4.iso` image.
2. Click *Run* when prompted.
3. Agree to the license terms and conditions, and click *Install*.

If your File Reporter deployment uses Microsoft SQL Server as the database, a dialog instructs you to update your OLE DB driver for SQL Server.

4. (Conditional) Update the OLE DB driver.
    a. Click *Yes* to launch the installation wizard.
    b. Click *Next*.
    c. Accept the license terms and click *Next*.
    d. Click *Next* to accept the default feature selections.
    e. Click *Install*.
    f. (Conditional) If notified that there are applications running which prevent the driver from updating, close the listed applications and click *Retry*.
5. Click *Next*.
6. Either accept the installation path or indicate a new path with the *Browse* button, and click *Next*.
7. Click *Install*.
8. Click *Finish*.
9. Finally, either:
    a. Restart the server, if prompted, to activate the updated OLE DB driver. Then, select the *File Reporter* Configuration Dashboard under *File Reporter* in the *Start* menu; or
    b. Click *Run Config Utility* to open the File Reporter Configuration Dashboard.



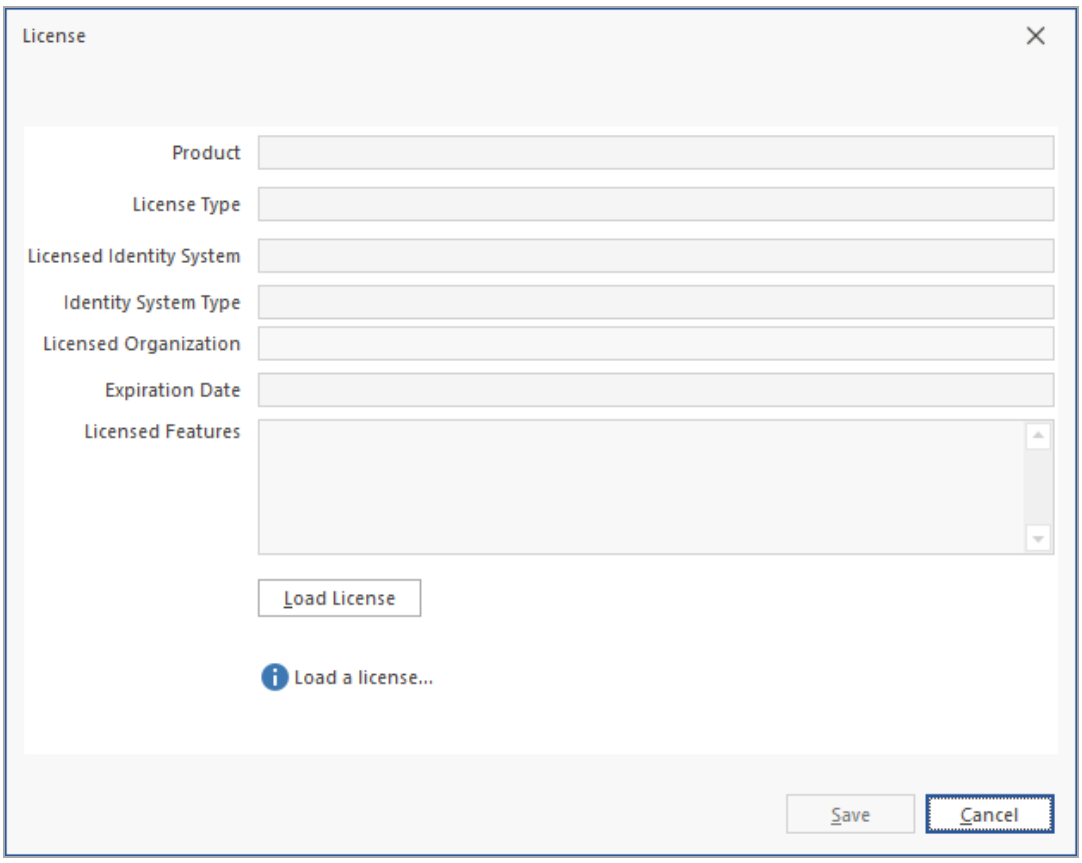
NOTE: Each step in the Configuration Utility should be run in sequential order, from top to bottom. If you chose not to install RabbitMQ, you can skip the Message Broker section.

6.4 - Installing or Updating the License

6.4.1 - Installing a New License

1. From the **Start** menu, launch the File Reporter Configuration Dashboard.
2. In the Configuration Dashboard, click **Install or Update License**.

3. The License dialog box appears.



4. Click **Load License**, then browse to and select the license file.
5. When the confirmation prompt appears, click **Yes**.
6. Examine the license properties to ensure that the license is valid.
7. Click **Close**.

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.

6.4.2 - Updating the License

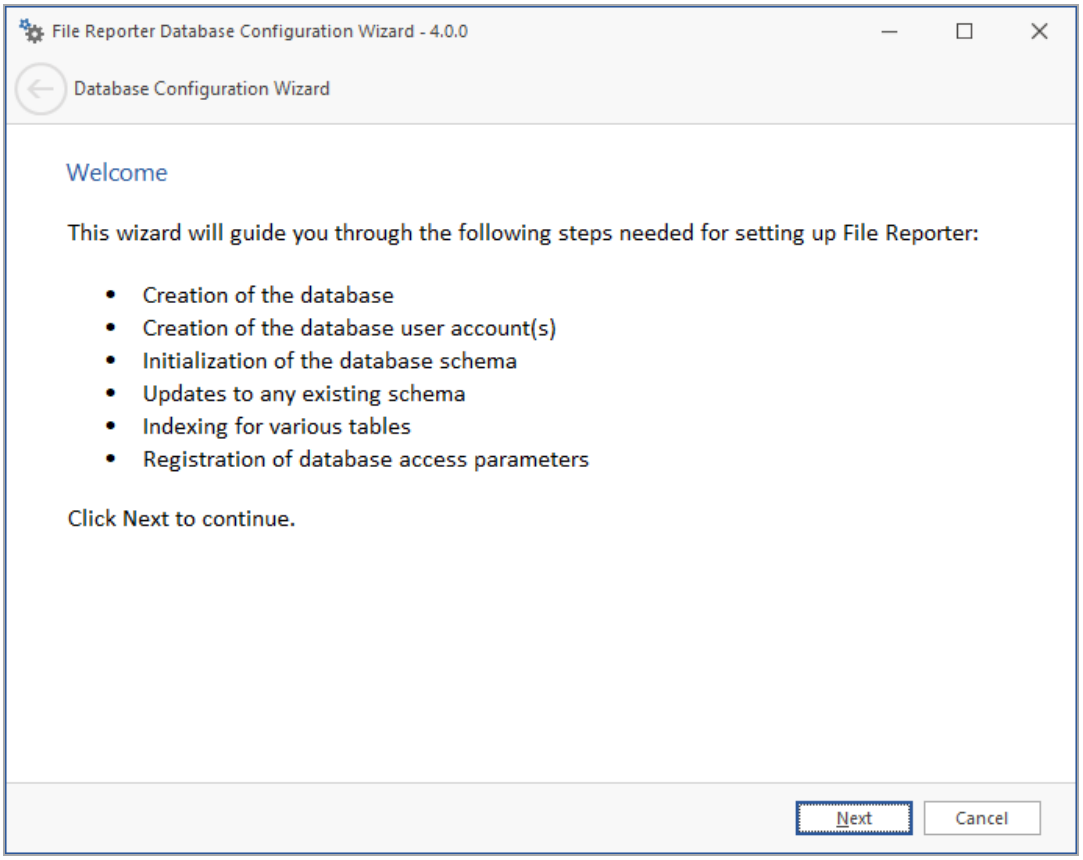
After you have installed File Reporter, you can update your evaluation license or production license by simply replacing the old license with the new one.

To replace an existing license simply install a new one by following the instructions in the previous section *Installing a New License (page 39)*.

6.5 - Configuring the Database

1. Click *Configure Database*.

2. Review what is to be configured and click *Next*.



3. Establish the settings required for the Engine and IIS to communicate with the database.

    - **Database Properties**: Displays the database name and version.
    - **Type**: Select either PostgreSQL or SQL Server.
    - **Communication**: Specifies the database address, port number, and name.
    - **Database Host Address**: Specify the host address of the server on which the database is installed.
    - **Port**: Enter the database port. The default setting is either 5432 (for PostgreSQL) or 1433 (for SQL Server).

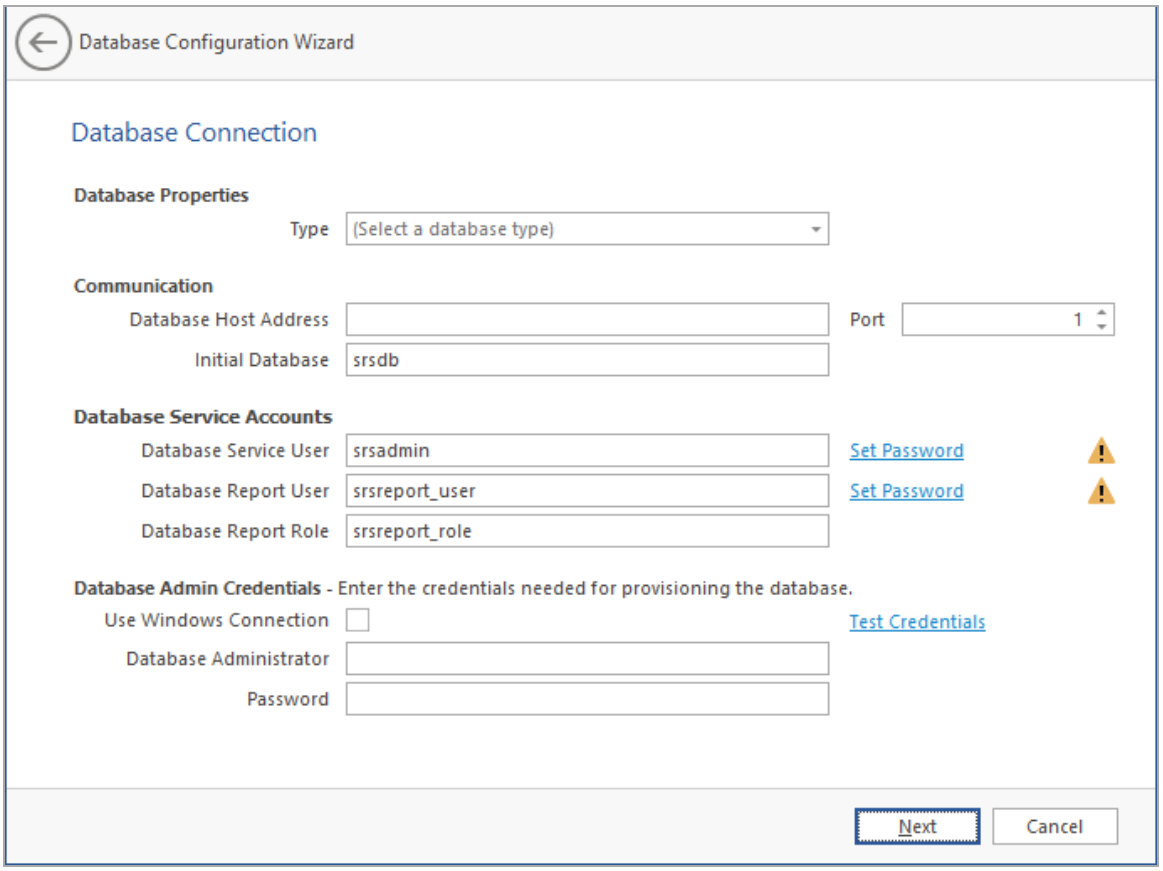
- **Initial Database**: The default name of the File Reporter database.
- **Database Service Accounts**: Set the authentication information for the Database Service User and Database Report User.
- 

  NOTE: Retain the user and password information as it will be required during component configuration.

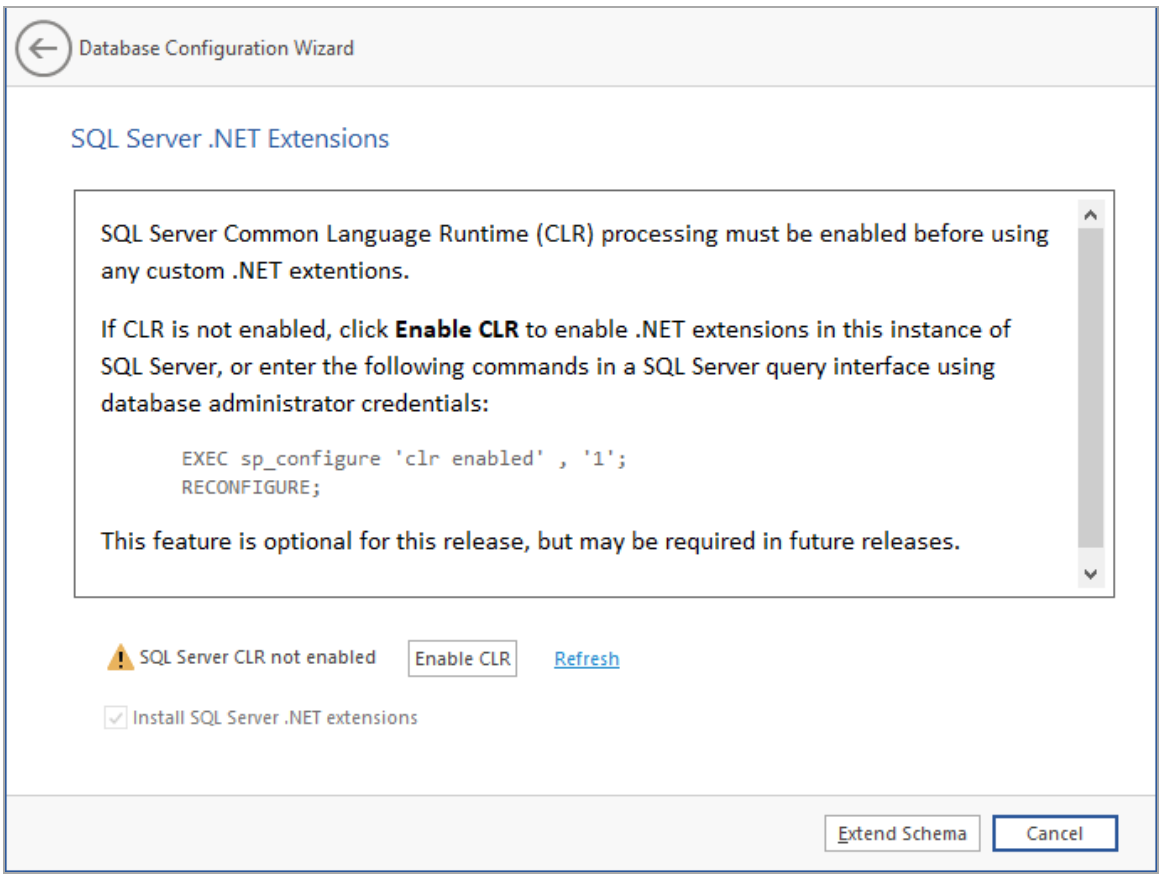
- **Database Service User**: Specify the database account name used by File Reporter to manage data in the database. This account has both read and write access to the database.
- **Set Password**: Establish the password for the Database Service User.
- **Database Report User**: Specify the database account name used by File Reporter to read data in the database while reporting.
- **Set Password**: Establish the password for the Database Report User.
- **Database Report Role**: Specify the account name of the role used to manage access for Report Users.
- **Database Admin Credentials**: Establish the database administrator name and credentials.
- **Database Administrator**: Specify either the superuser name (for PostgreSQL), or the administrator name (for SQL Server).
- **Password**: Specify either the superuser password (for PostgreSQL), or the administrator password (for SQL Server).
- **Test Credentials**: Click to confirm that the entries in the Database Service Accounts region are accurate before advancing in the wizard.

4. Complete the fields and click *Next*.

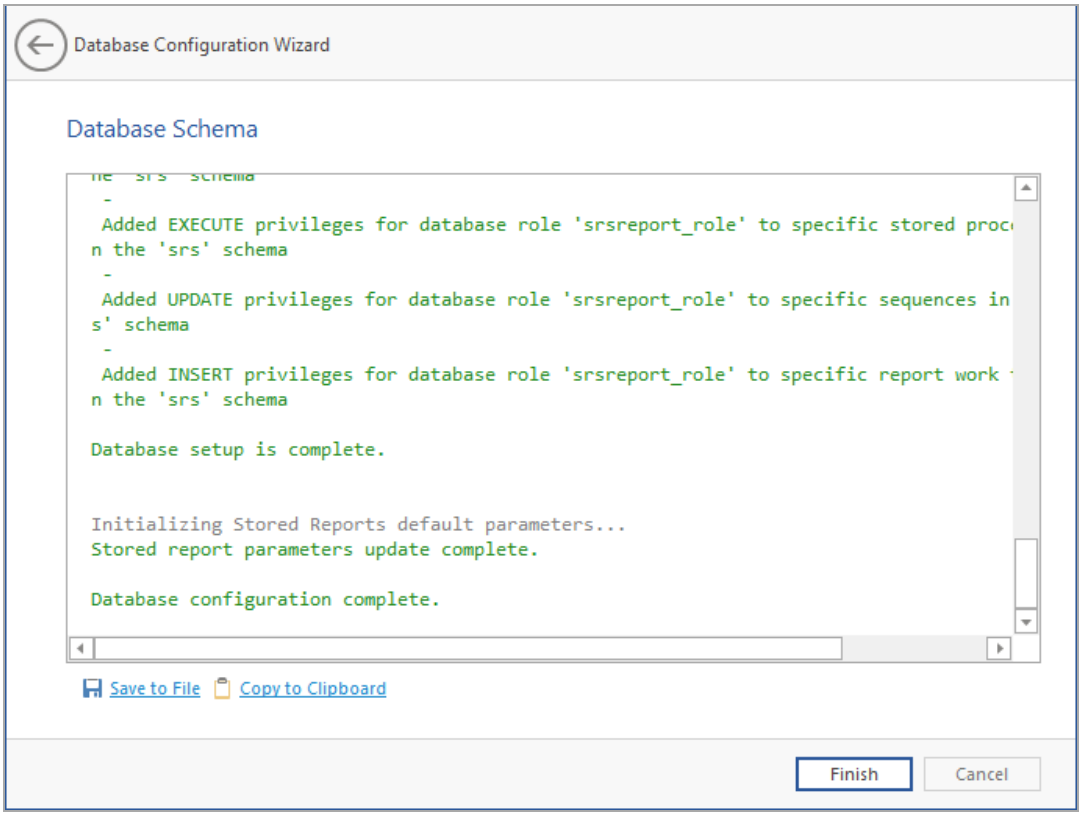
The following page appears if you use a Microsoft SQL Server database, indicating that File Reporter will add custom extensions for SQL Server that help File Reporter with advanced reporting queries.


Database Configuration Wizard
Database Connection
Database Properties
Type
(Select a database type)
Communication
Database Host Address
Port
1
Initial Database
srsdb
Database Service Accounts
Database Service User
srsadmin
Set Password
Database Report User
srsreport_user
Set Password
Database Report Role
srsreport_role
Database Admin Credentials - Enter the credentials needed for provisioning the database.
Use Windows Connection
Test Credentials
Database Administrator
Password
Next
Cancel

5. (Optional) Click *Enable CLR*.



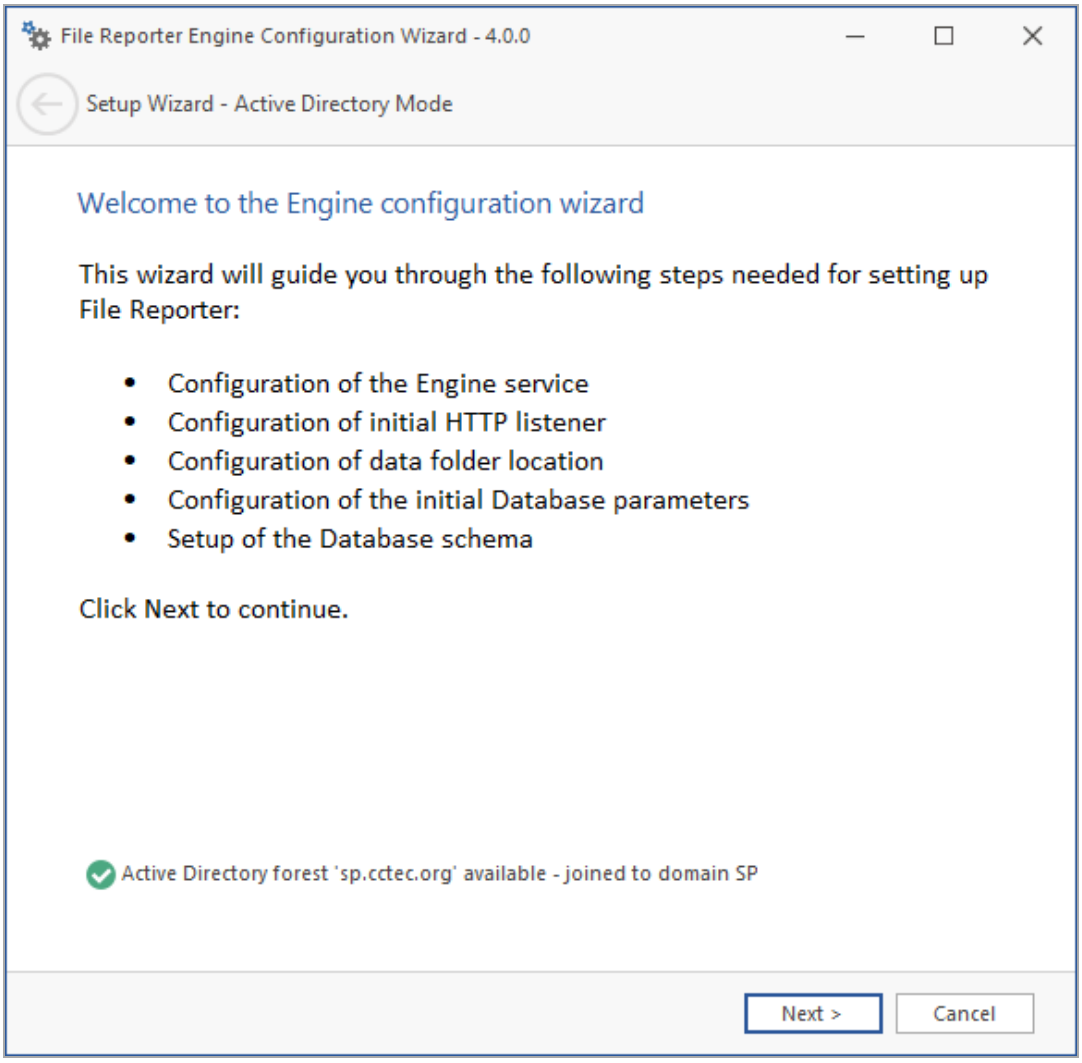
6. Click *Extend Schema*.



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

6.6 - Configuring the Engine

1. Click *Configure Engine*.
2. Review what is to be configured and click *Next*.



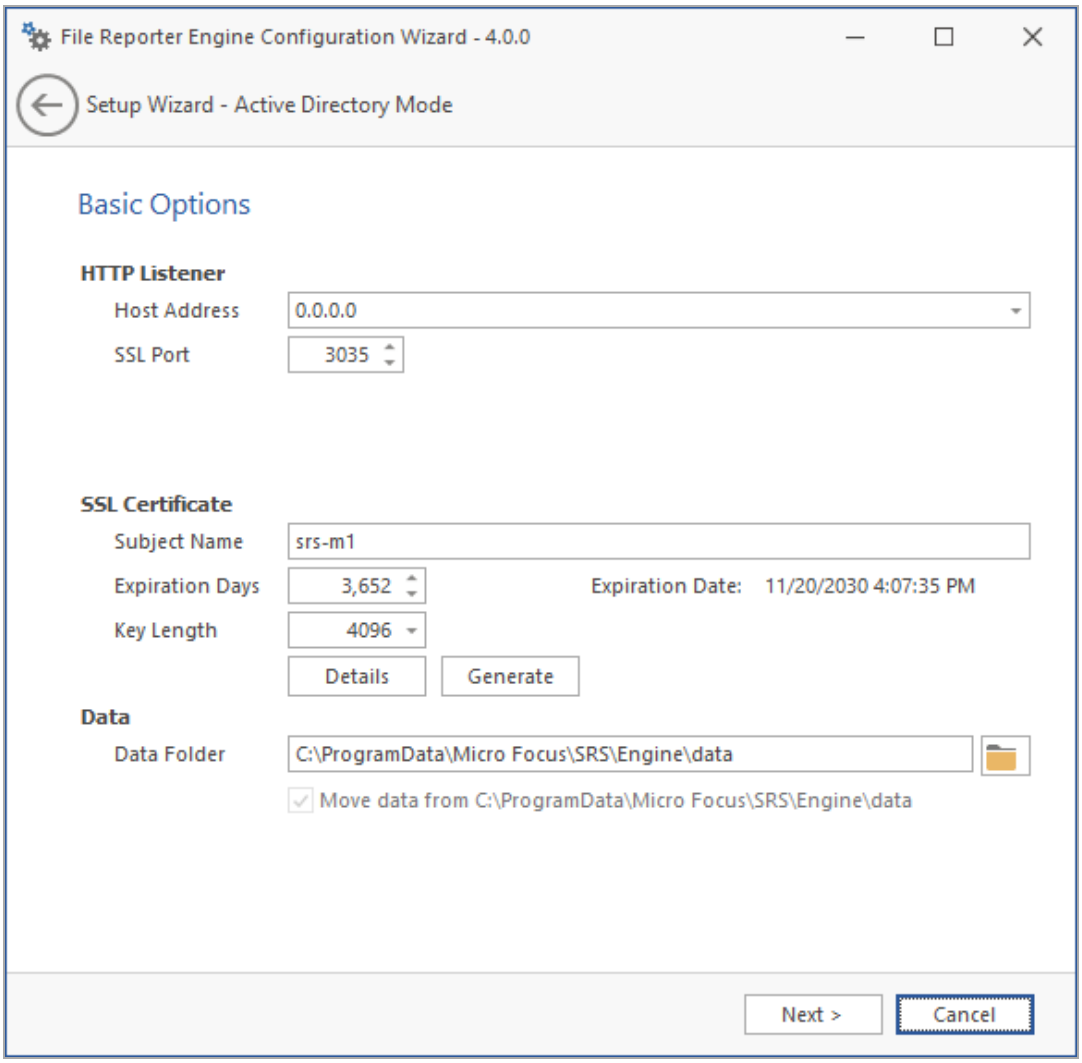
Confirm or change the basic Engine configuration settings in this window.

- **HTTP Listener**: Displays the communication parameters for the Engine.
  - **Host Address**: Leave this setting unchanged unless you want the Engine to only listen on a certain IP address.
  - **SSL Port**: Leave the setting at 3035 unless there is a port conflict.
- **SSL Certificate**: Displays 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 is set to 10 years by default.
- **Key Length:** The SSL certificate encryption setting is set to 2048 by default.
- **Details:** Click to view the certificate data.
- **Generate:** Click to generate a new certificate if you modify any of the settings in the SSL Certificate section.

- **Data Folder**:The default location of the data folder, which is used for a variety of tasks, including the storage of agent configuration and discovered storage resources data, as a temporary repository for scans, and mail spooling.
- **Move data from** (enabled only during an upgrade): If this box is checked, 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 the box is unchecked, the Engine will use the path specified in the *Data Folder* field, including the original path.

3. Edit any necessary parameter settings and click *Next*.



From this window you can establish names for the Proxy Account, Proxy Rights Group, and the Communications Group.

File Reporter uses a Proxy Account so that Agents can access all 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.

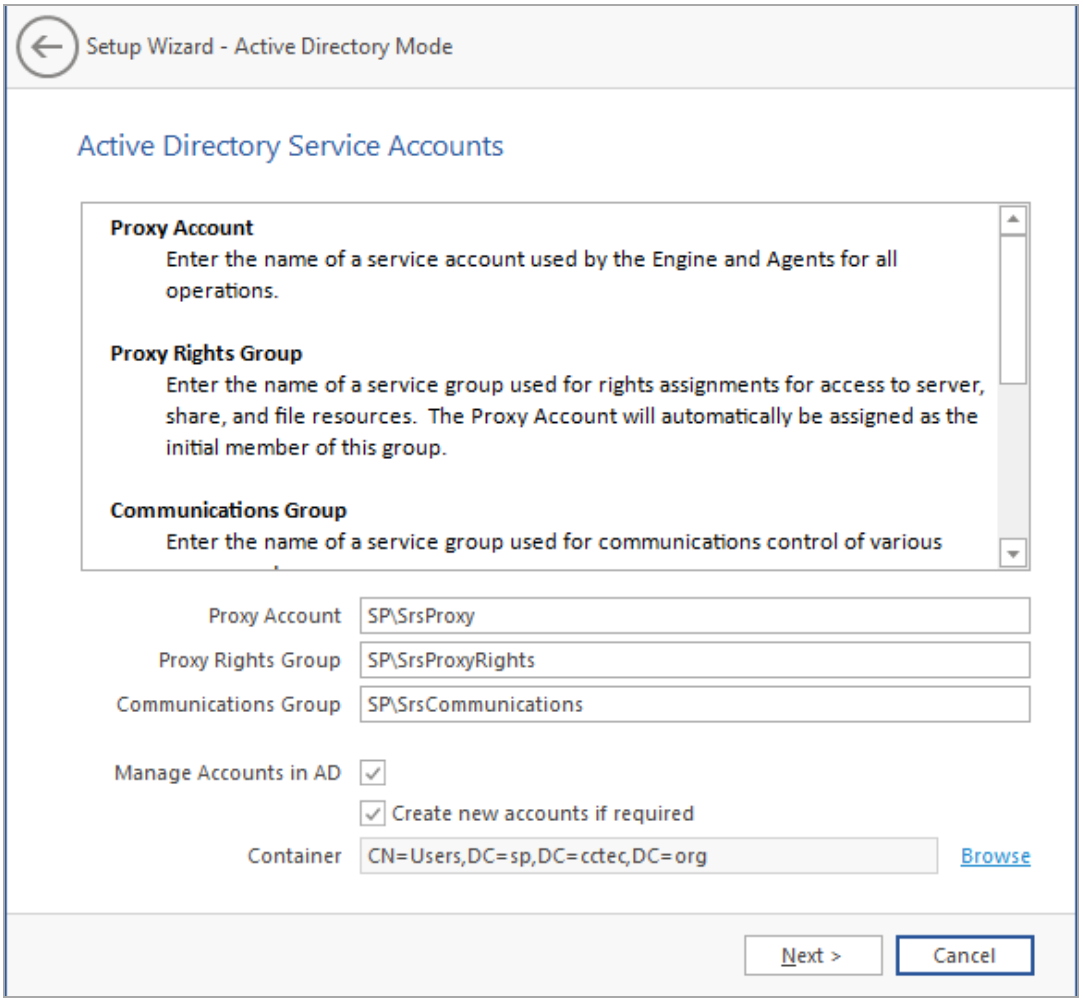
The configuration wizard establishes default account and group names, which you can modify.

If 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.

Click *Browse* to select a specified container for these objects other than `CN=Users`.

NOTE: These user and group objects can be moved in Active Directory after installation without affecting the product.

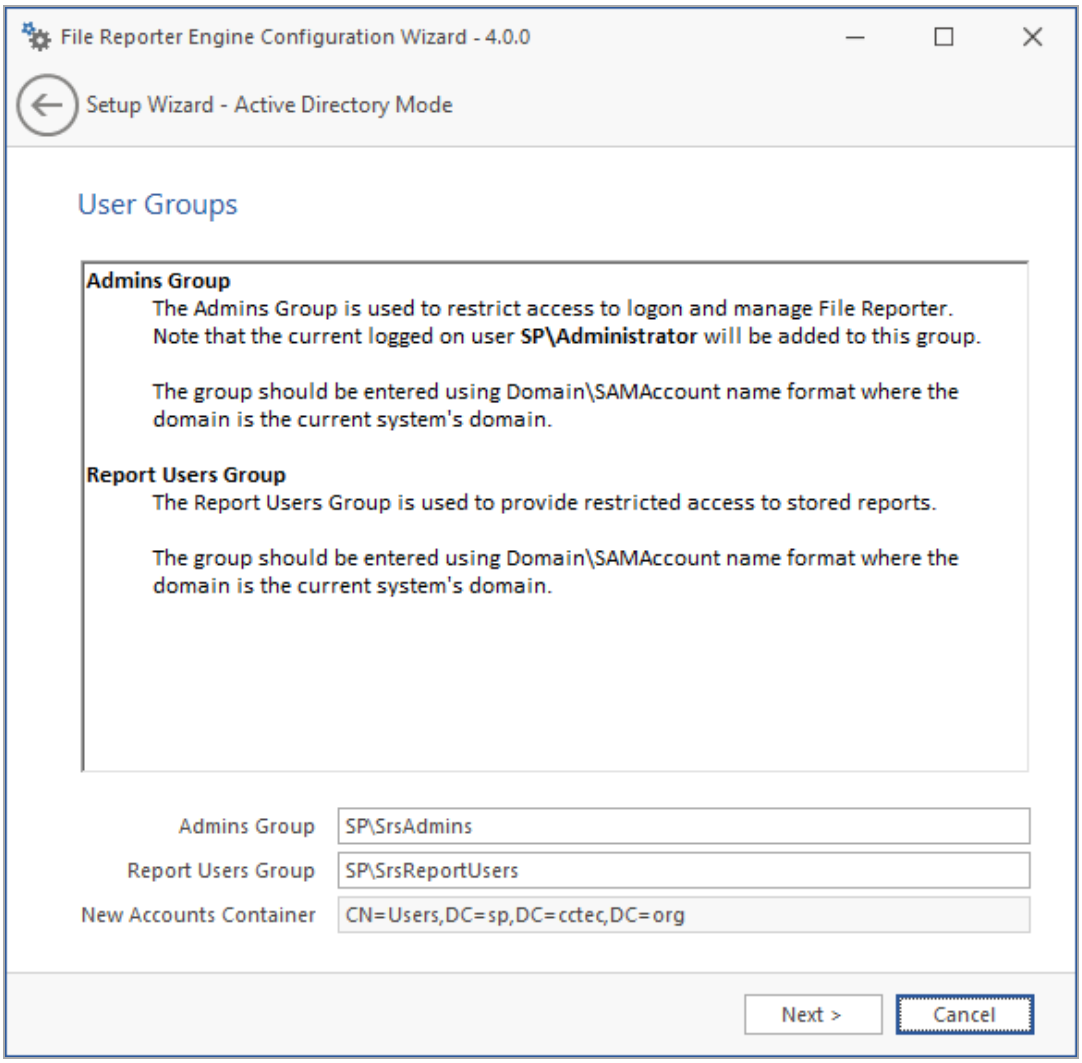
4. Click *Next*.



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

   File Reporter creates the Report Users Group in Active Directory. Members of this group can access all stored reports.

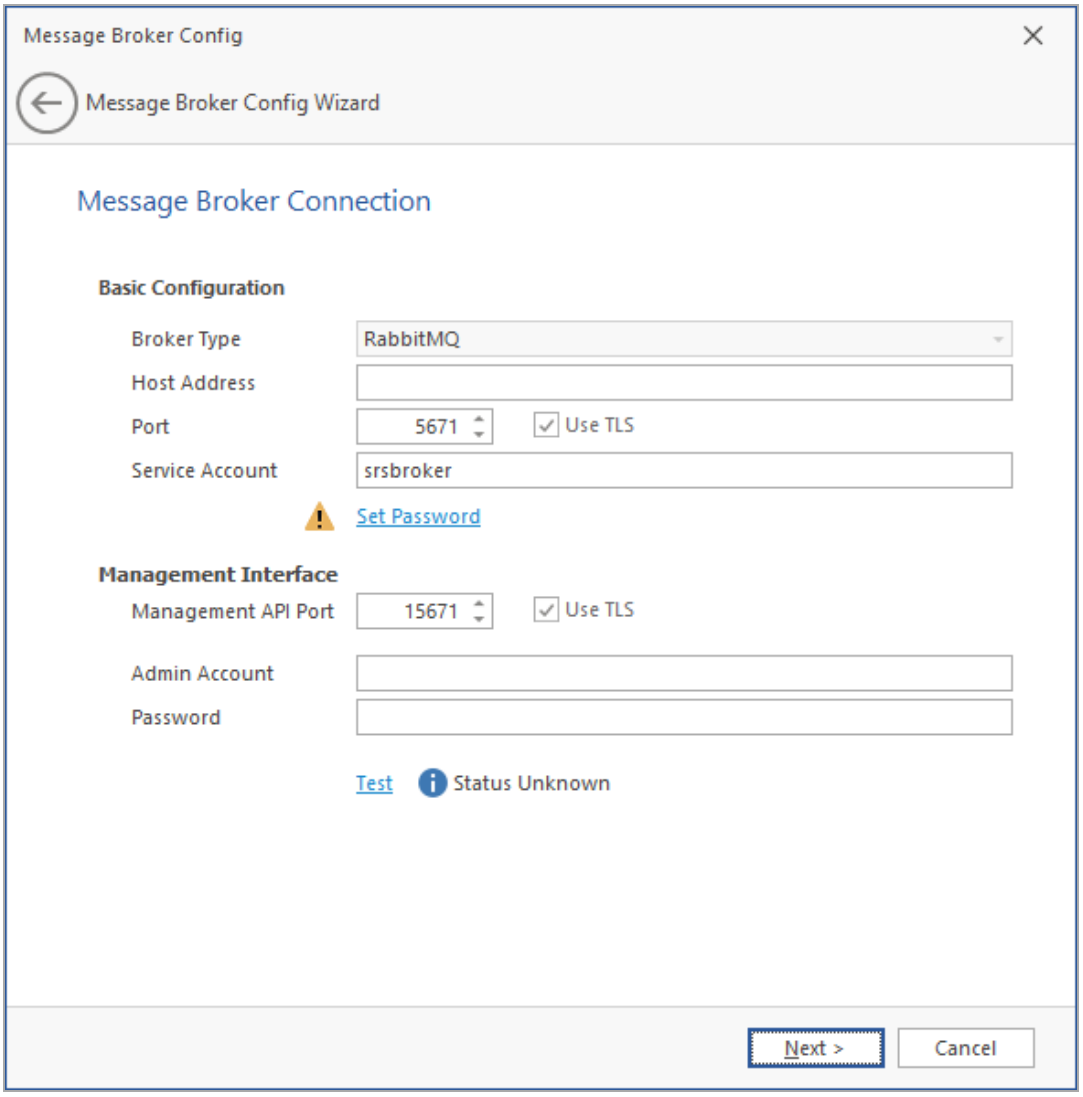
6. Click *Next* to create the two groups.



7. Click *Finish*. The Engine and Scan Processor are now configured and running.

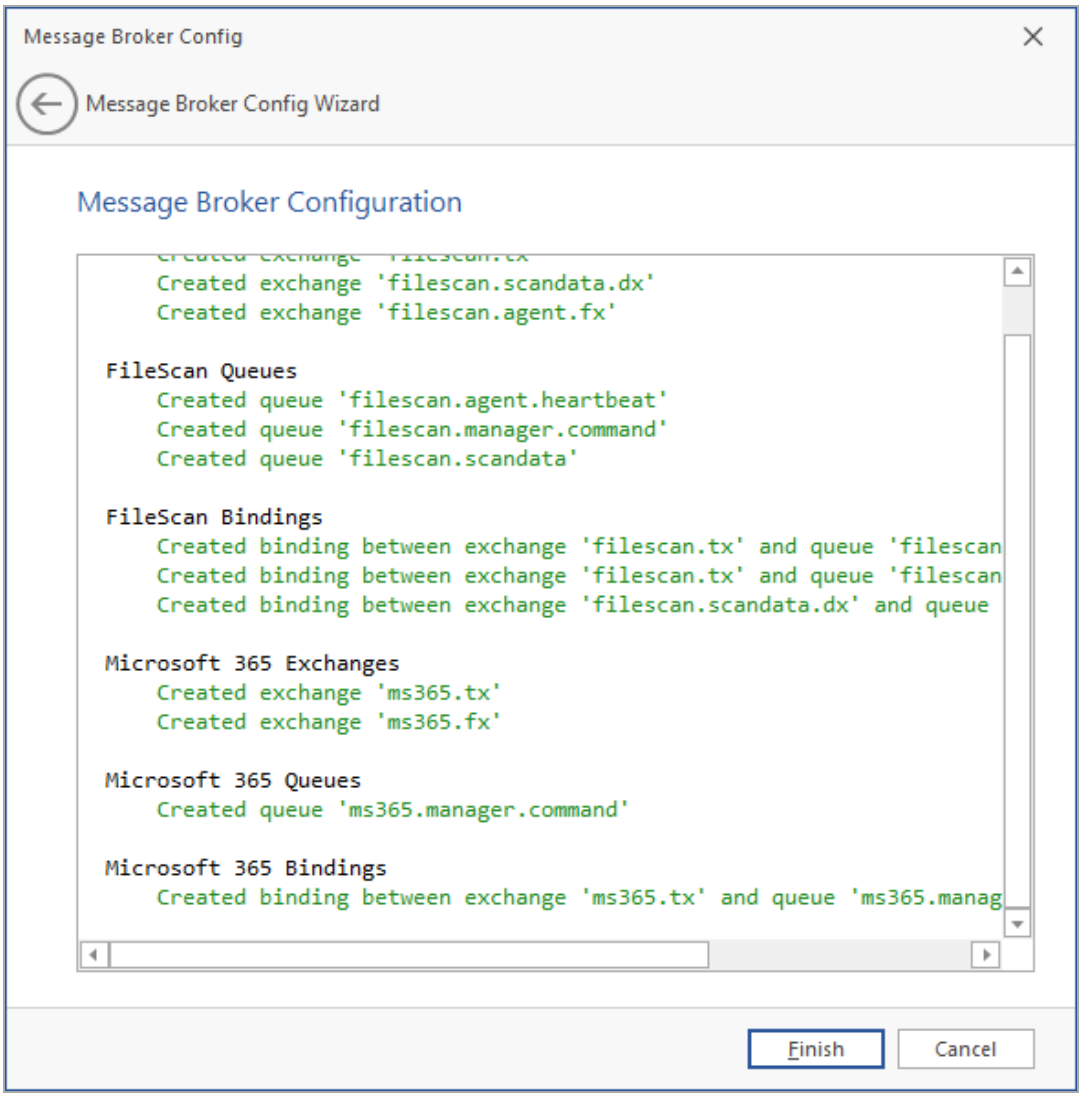
6.7 - Configuring the Message Broker

1. Click *Configure Message Broker*.



2. Specify settings in the following fields:
    - **Basic Configuration**: Details the basic configuration settings for the message broker.
        - **Broker Type**: Indicates the previously-installed RabbitMQ message broker.

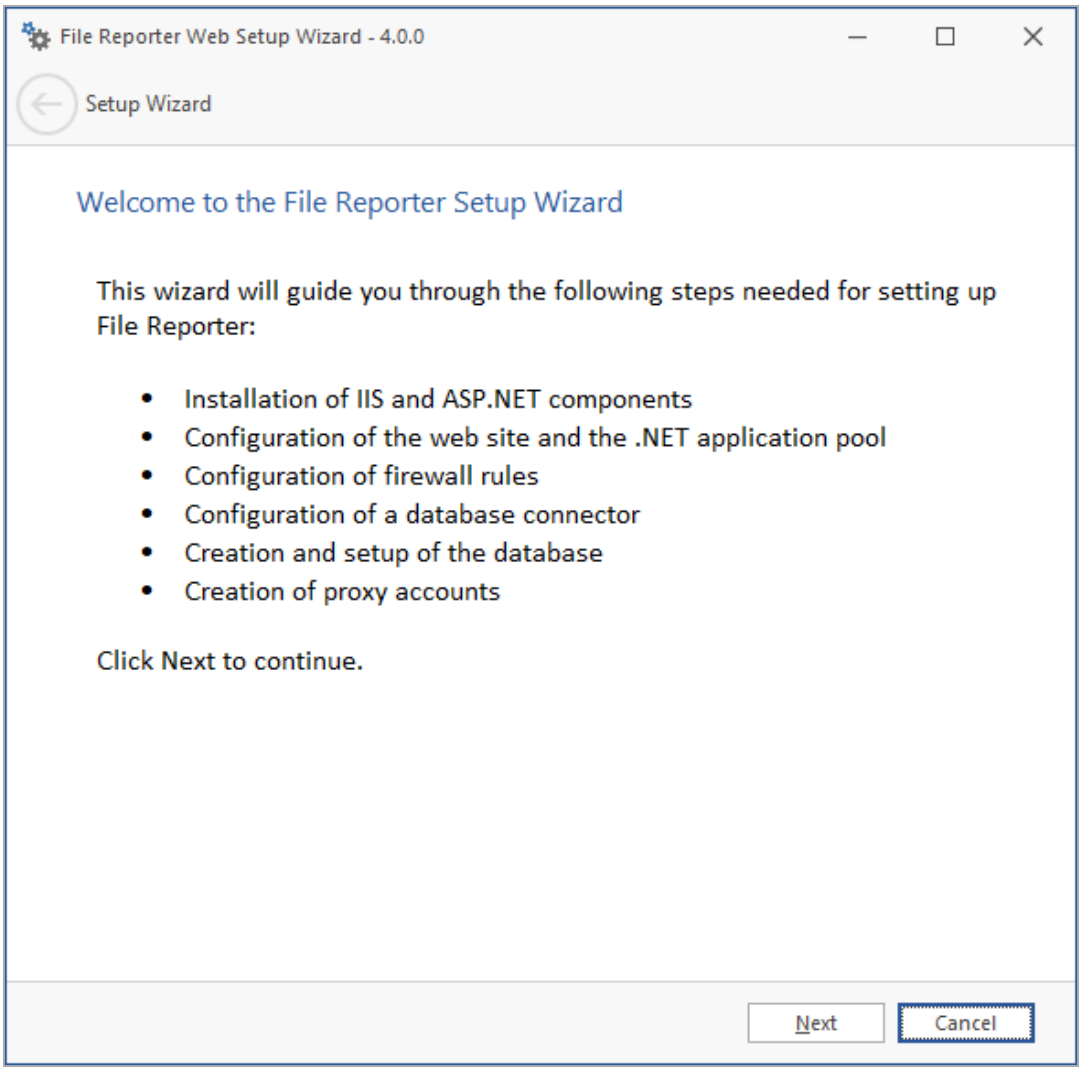
        - **Host Address**: Specify the IP address or DNS name of the server hosting RabbitMQ.
        - **Port**: Leave the setting at 5671 unless there is a port conflict.
        - **Use TLS**: The Transport Layer Security protocol is established by default.
        - **Service Account**: This field contains the `srsbroker` account name by default.
        - **Set Password**: Establish a password for the service account.
    - **Management Interface**: Details the admin account and password for the previously-installed RabbitMQ message broker.
        - **Management API Port**: Leave the setting at 5671 unless there is a port conflict.
        - **Use TLS**: The Transport Layer Security protocol is established by default.
        - **Admin Account**: Specify the admin account name you established when installing RabbitMQ. Unless you changed the default name, the admin account name is `admin`.
        - **Password**: Specify the admin account password you established when installing RabbitMQ. Unless you changed the default password, the admin account password is `srsadmin`.
    - **Test**: Click to verify that the message broker communication is functioning properly.
3. Click *Next*.



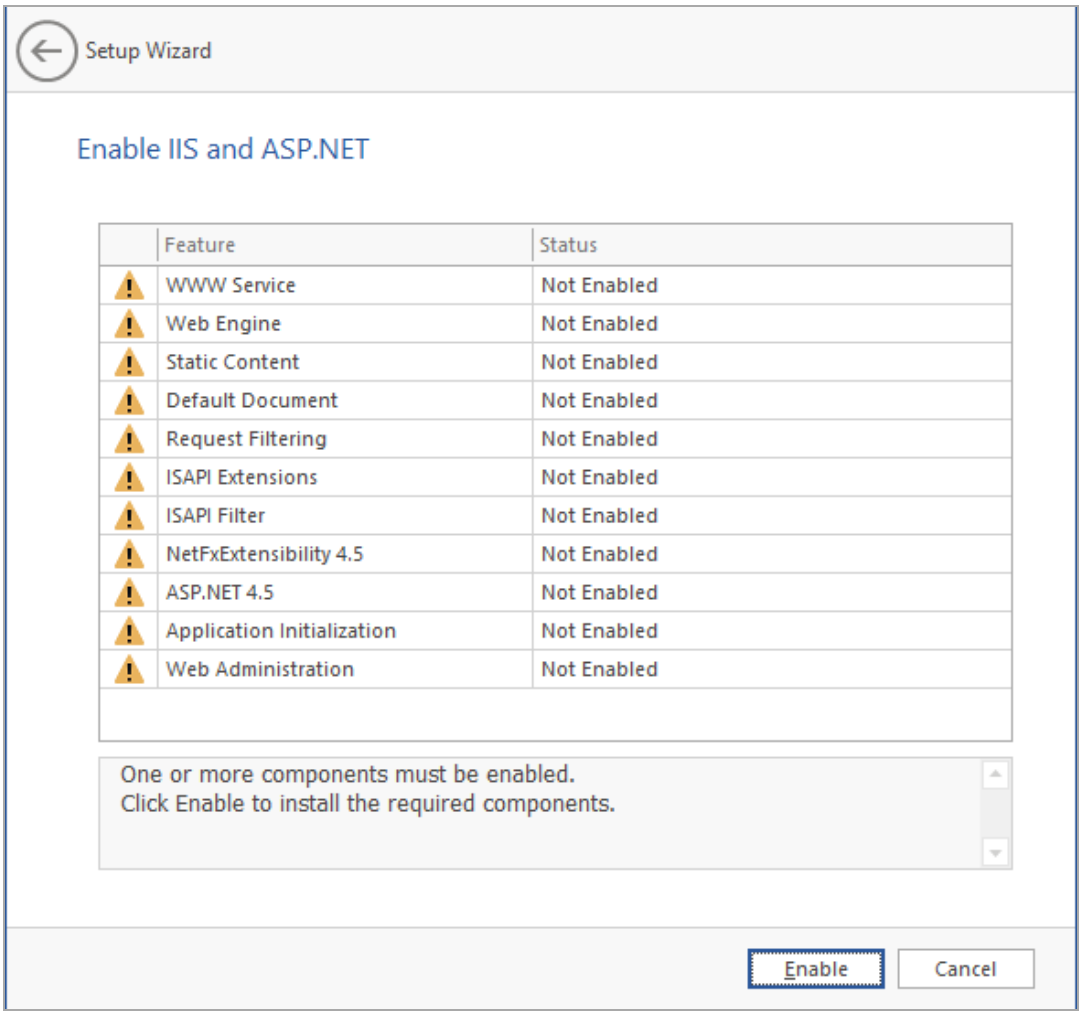
4. Click *Finish*. The message broker is now configured and connected.

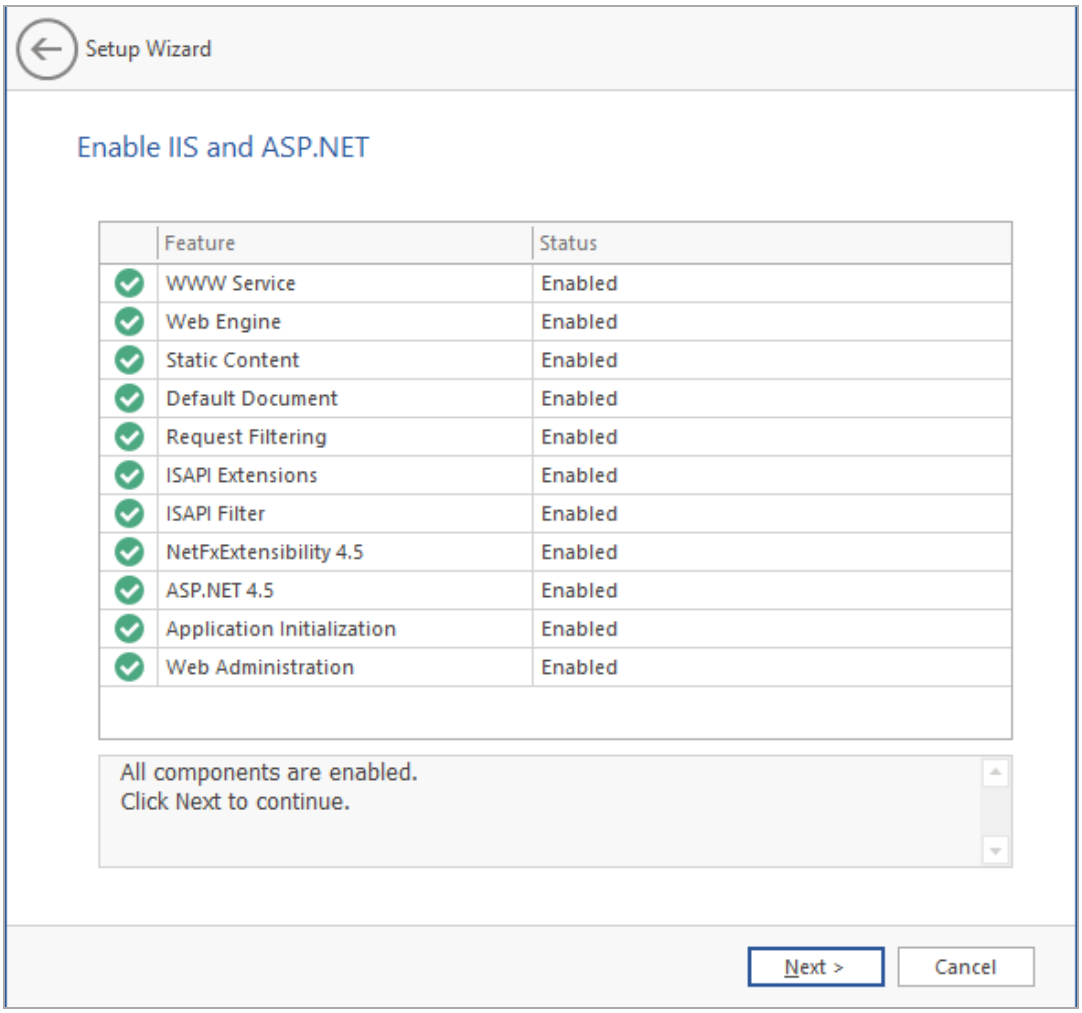
6.8 - Configuring the Web Application

1. Click *Configure Web Application*.
2. Review what is to be configured and click *Next*.

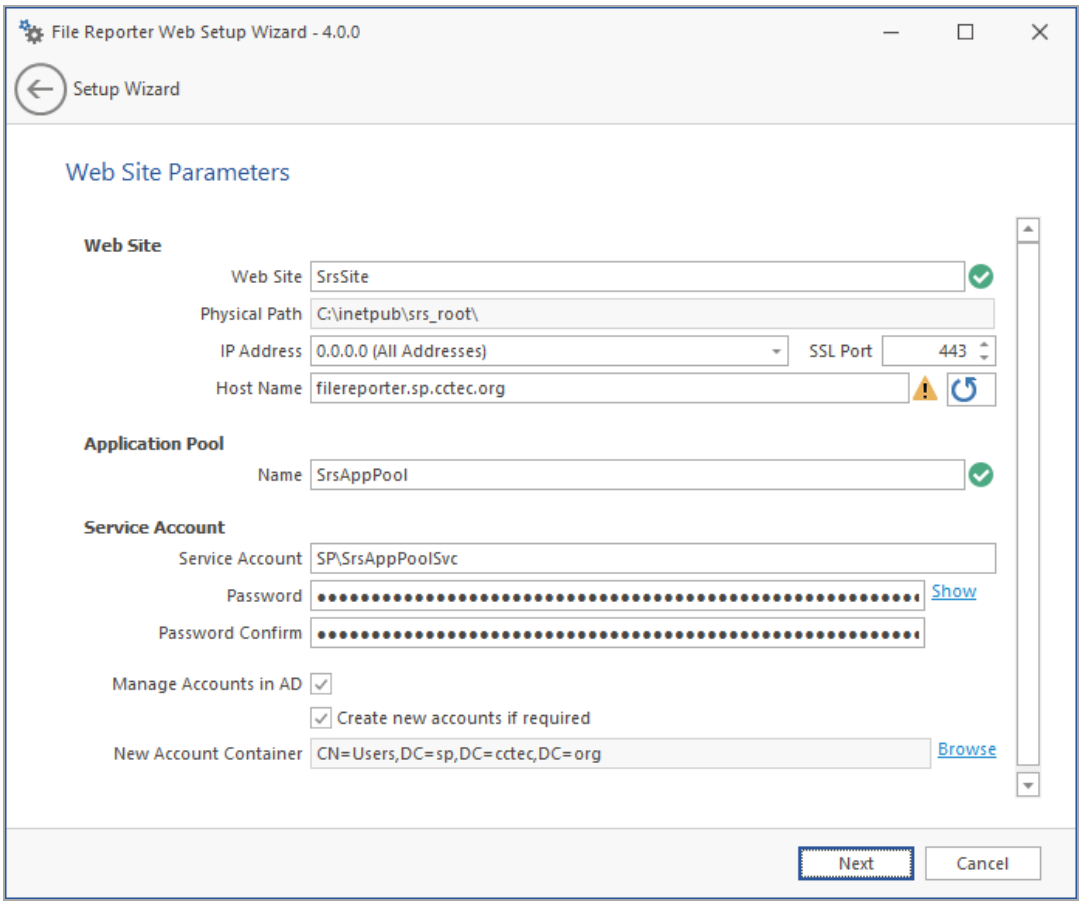


3. (Conditional) If the components are not enabled, click *Enable*.


Setup Wizard
Enable IIS and ASP.NET
Feature
Status
WWW Service
Not Enabled
Web Engine
Not Enabled
Static Content
Not Enabled
Default Document
Not Enabled
Request Filtering
Not Enabled
ISAPI Extensions
Not Enabled
ISAPI Filter
Not Enabled
NetFxExtensibility 4.5
Not Enabled
ASP.NET 4.5
Not Enabled
Application Initialization
Not Enabled
Web Administration
Not Enabled
One or more components must be enabled.
Click Enable to install the required components.
Enable
Cancel



4. Click *Next* when all Microsoft IIS components are enabled.



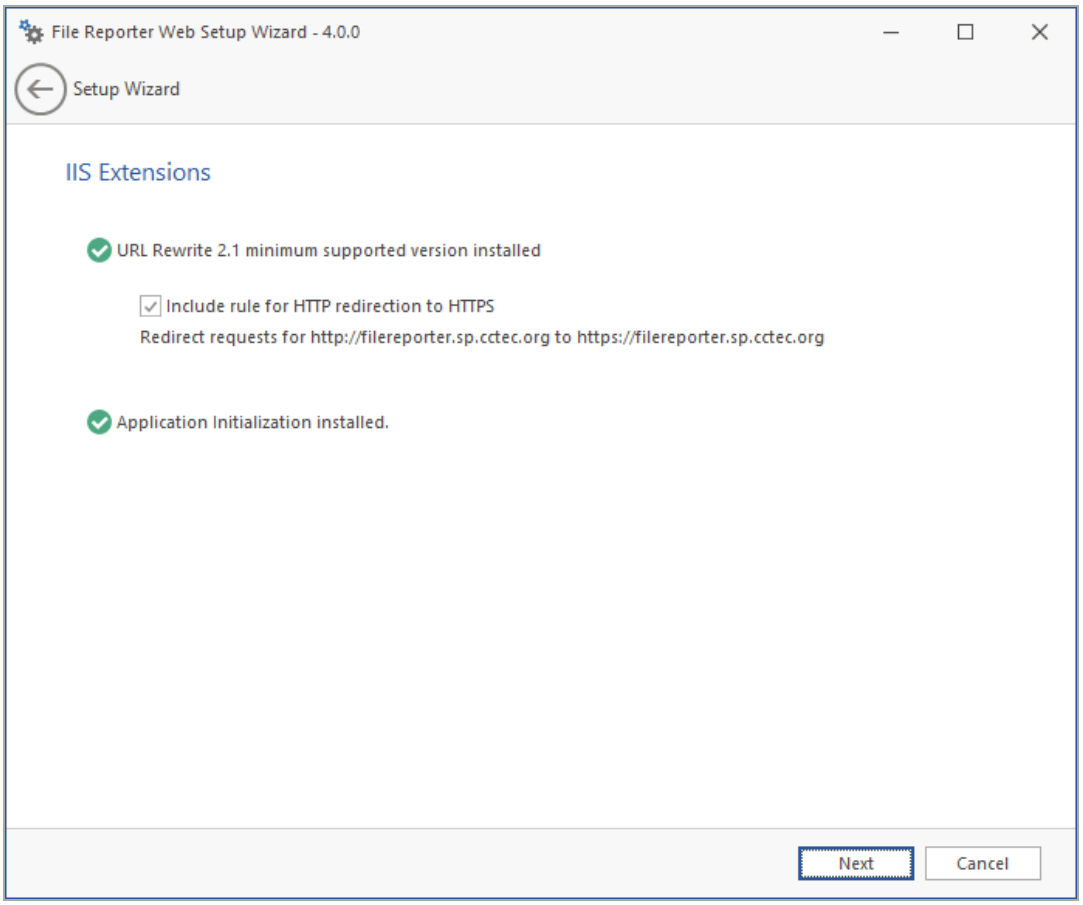
From this window, you can review or edit settings applicable to the File Reporter Web Application. Leave the settings as currently established unless there is a need to change a setting.

- **Web Site**: Details the settings for the File Reporter site in Microsoft IIS.
  - **Web Site**: The default name for the File Reporter site. Edit as needed.
  - **Physical Path**: The path specified during installation as the location that serves up content for the website. This field cannot be edited.
  - **IP Address**: Indicates that web requests will be responded to from any IP address available on the server by default. You can specify which one to use if the server has multiple IP addresses.
  - **SSL Port**: The default port is 443. You can select another port if there is a conflict.
  - **Host Name**: The hostname as defined in the DNS you specified in *Prerequisites (page 37)*.

If a warning sign appears next to the Host Name entry, then the hostname is not fully resolved. Verify that there is a DNS entry for the File Reporter Web application and that the resolved IP address(es) are located on the host machine.

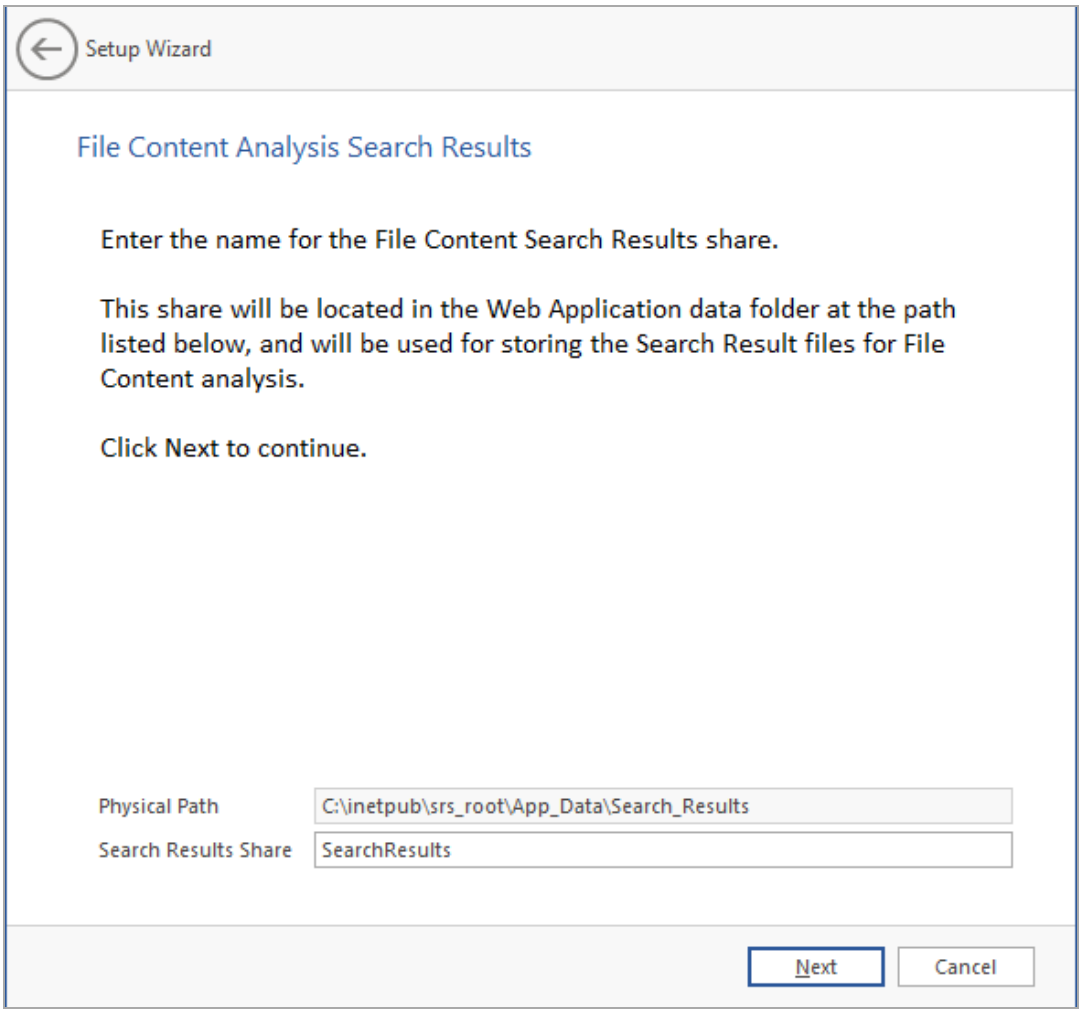
- **Application Pool**: Details the settings for the File Reporter application pool in Microsoft IIS.
    - **Name**: The default name for the application pool. Edit as needed.
    - **Service Account**: Specifies the service account name used by the application pool.
    - **Password**: The password is generated automatically.
    - **Confirm Password**: The automatically-generated password is repeated.
    - **Provision in Active Directory**: This option provisions the application pool in Active Directory when selected. If not selected, the application pool provisions to the local host.
    - **New Account Container**: This option specifies the default location of the application pool in Active Directory.To modify the location, click Browse and specify a new location.

5. Edit the fields as necessary and click *Next*.

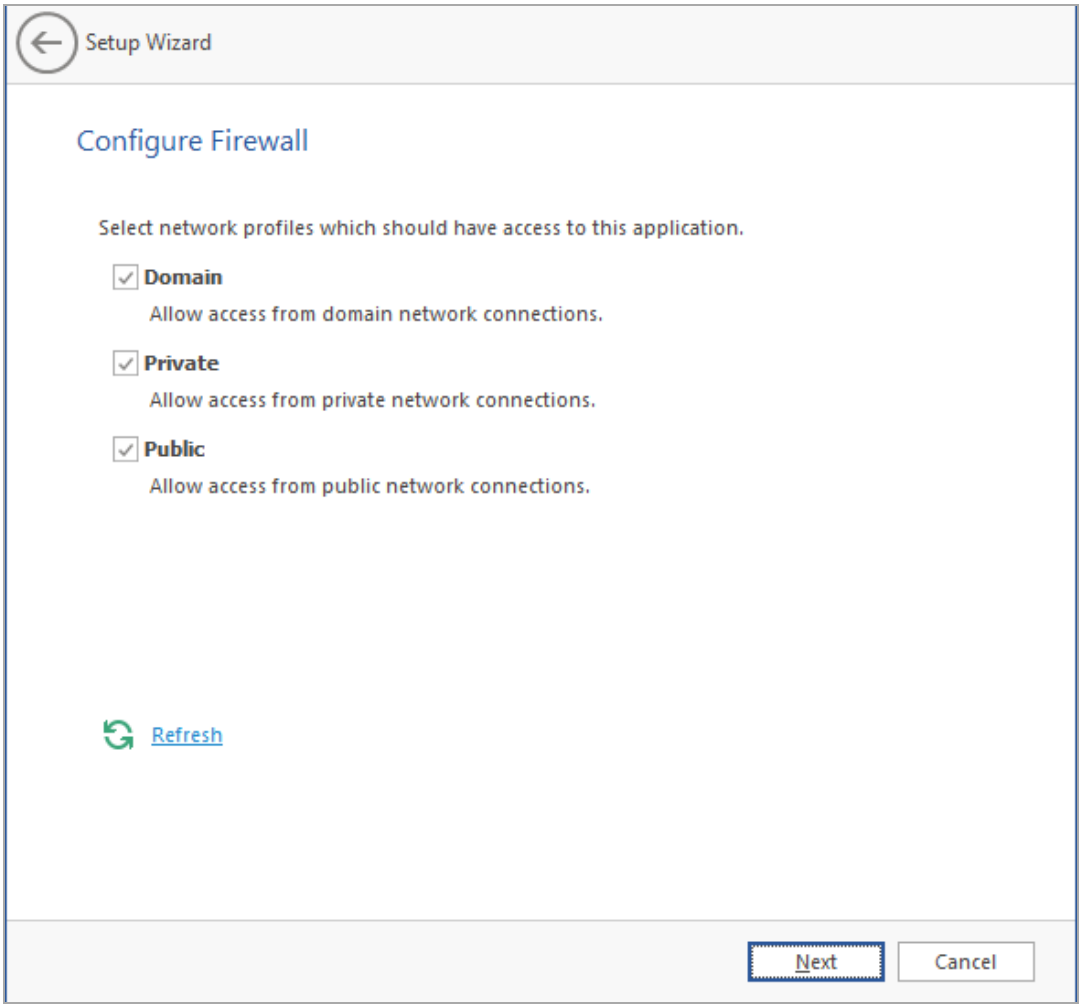


From this window, you can install the Microsoft IIS URL Rewrite Module, which will redirect File Reporter web application requests using HTTP to HTTPS. For example, if you enter http://File Reporter.cctec.org in a browser, this module redirects you to the secure page at https://FileReporter.cctec.org.

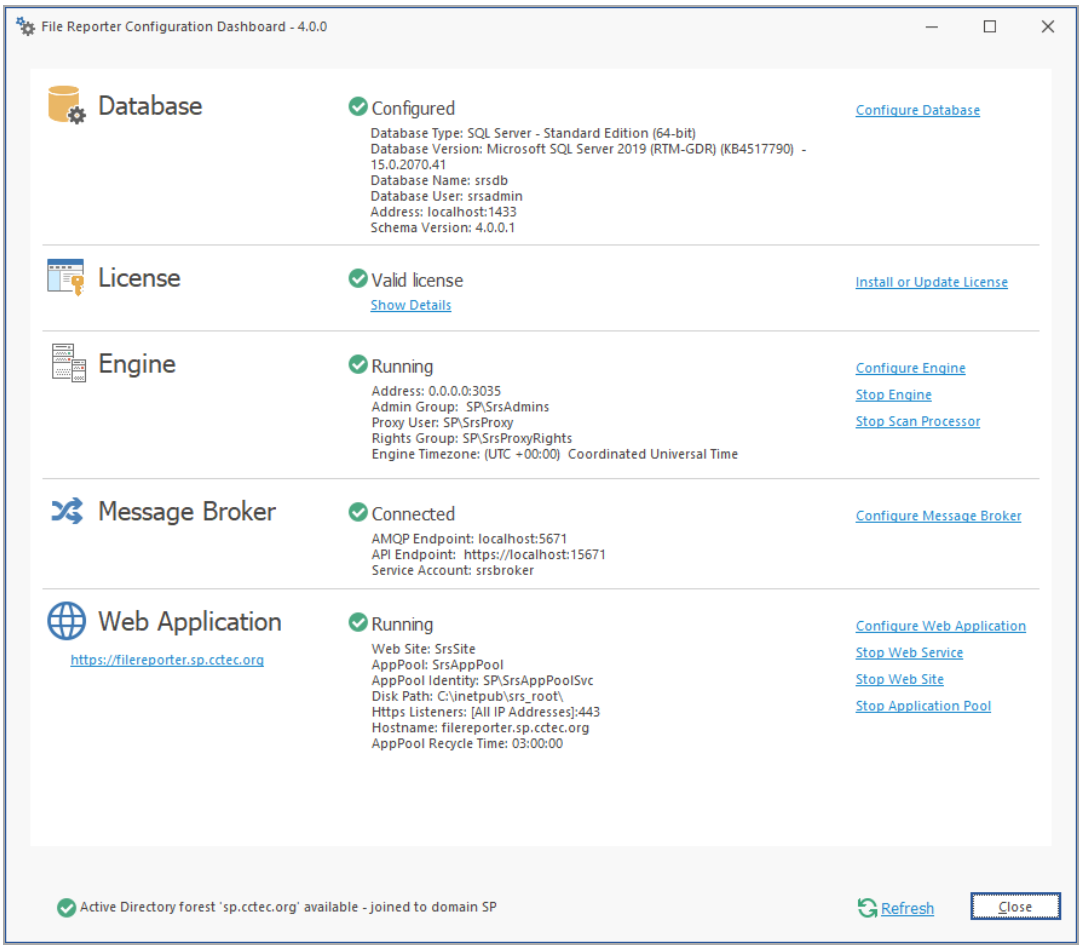
6. Unless your organization has a policy against redirects, leave the check box selected and click *Next*.


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

7. Click *Next*.



8. Set the firewall network profiles according to your organization's security policies and click *Next*.
9. Click *Finish* when the initial setup for the Web Application is complete. The Database, Engine, and Web Application are now configured.



10. Click the hyperlink located below the *Web Application* heading to launch the web-based administrative interface.
11. (Conditional) If 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

The following procedures include those required to install and configure AgentFS on Windows Server.

7.1 - AgentFS - Minimum Requirements

- Any of the following quad-core 64-bit processor servers:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
- The server must be joined to Active Directory
- .NET 8.0 Desktop Runtime (this will be installed if not already present)
- 100 MB RAM per concurrent scan (e.g., if you plan for AgentFS to conduct concurrent scans on four volumes or shares, you need a minimum 400 MB RAM).

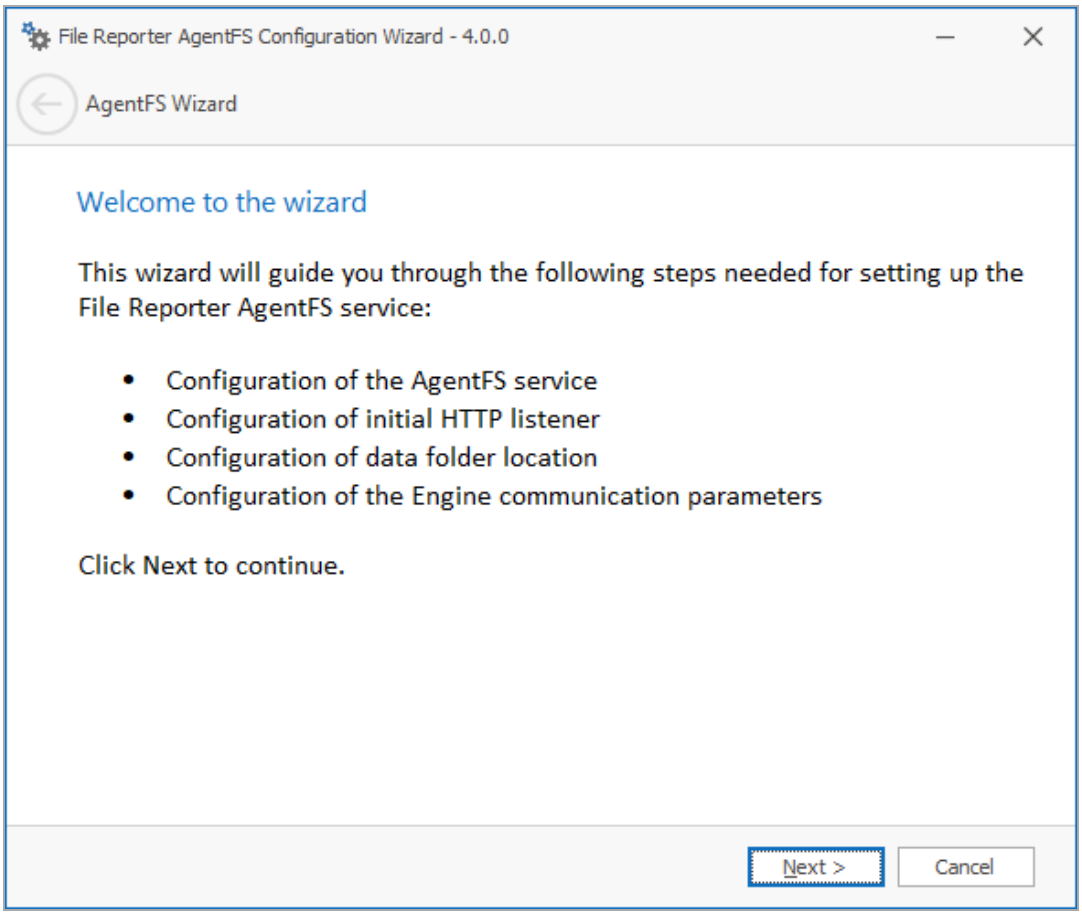
  

  NOTE: Performance depends on the number of concurrent scans and the size of the directory structure for each share. Adding more RAM than the minimum requirement may improve performance.

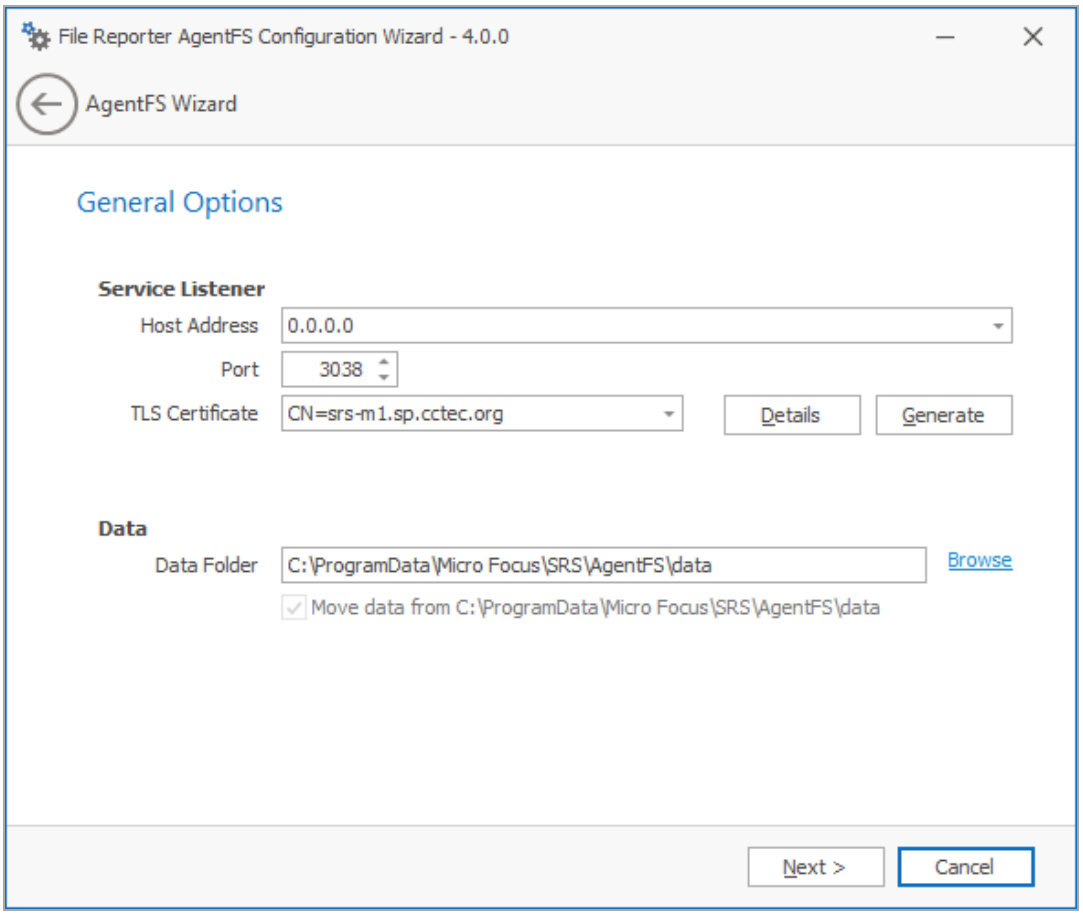
- 10 GB free disk space for installation and scans. You may need to increase this amount based on the number and size of the concurrent scans you intend to run.

7.2 - AgentFS - Installation and Configuration

1. Double-click `FileReporter-AgentFS-24.4.x64-xx.exe` at the root of the `FileReporter-24.4.iso` image.
2. Agree to the license terms and conditions and click *Install*.
3. When notified that the setup was successful, click *Run Setup Utility*.



4. From this window, review what is to be installed and configured, and click *Next*.

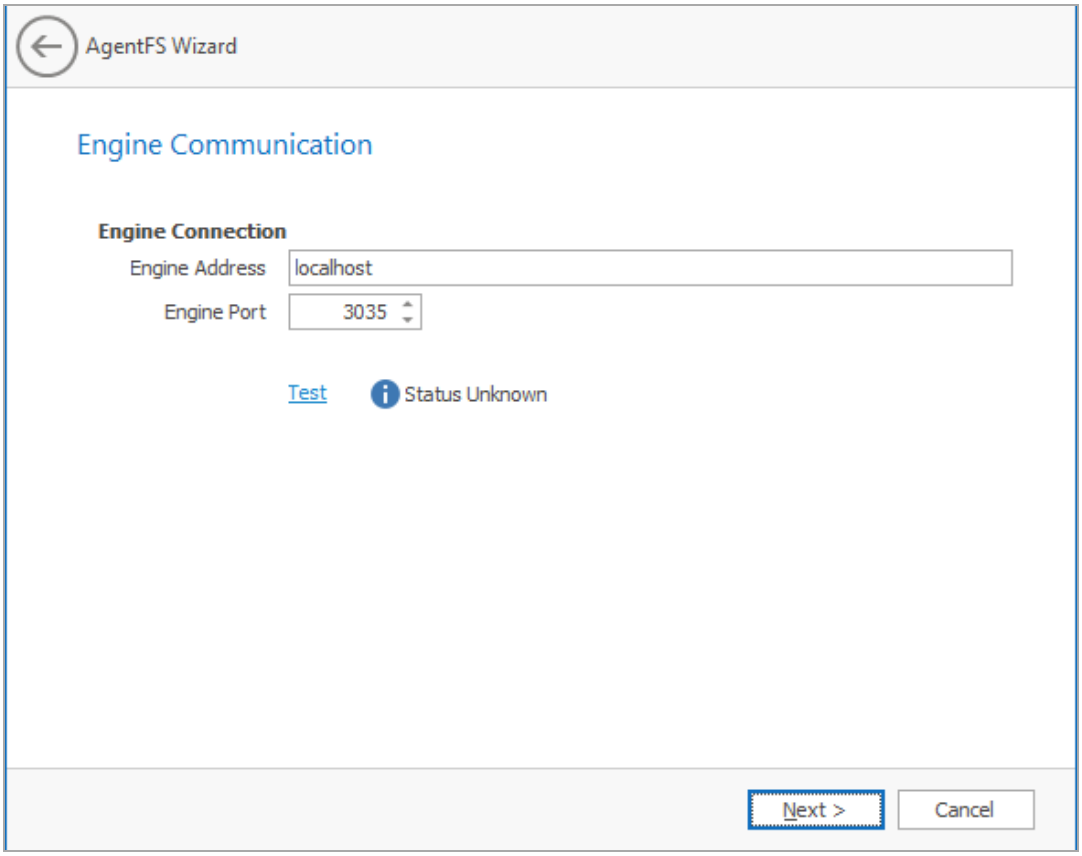


From this window, you can confirm or change AgentFS' basic configuration settings.

- **Service Listener**: Details the communication parameters for AgentFS.
  - **Host Address**: Leave this setting unchanged unless you want AgentFS to listen only on a certain IP address.
  - **Port**: Leave the setting at 3038 unless there is a port conflict.
  - **TLS Certificate**: The name of the TLS certificate to be generated. The server name is listed by default.
  - **Details**: Click to view the certificate data.
  - **Generate**: Click to generate a new certificate if you modify any of the settings for the TLS certificate.
- **Data**: Details the parameters for AgentFS data management.

- **Data Folder**: The default location of the data folder, which 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): If this box is checked, 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 unchecked, AgentFS will use the path specified in the Data Folder field, including the original path.

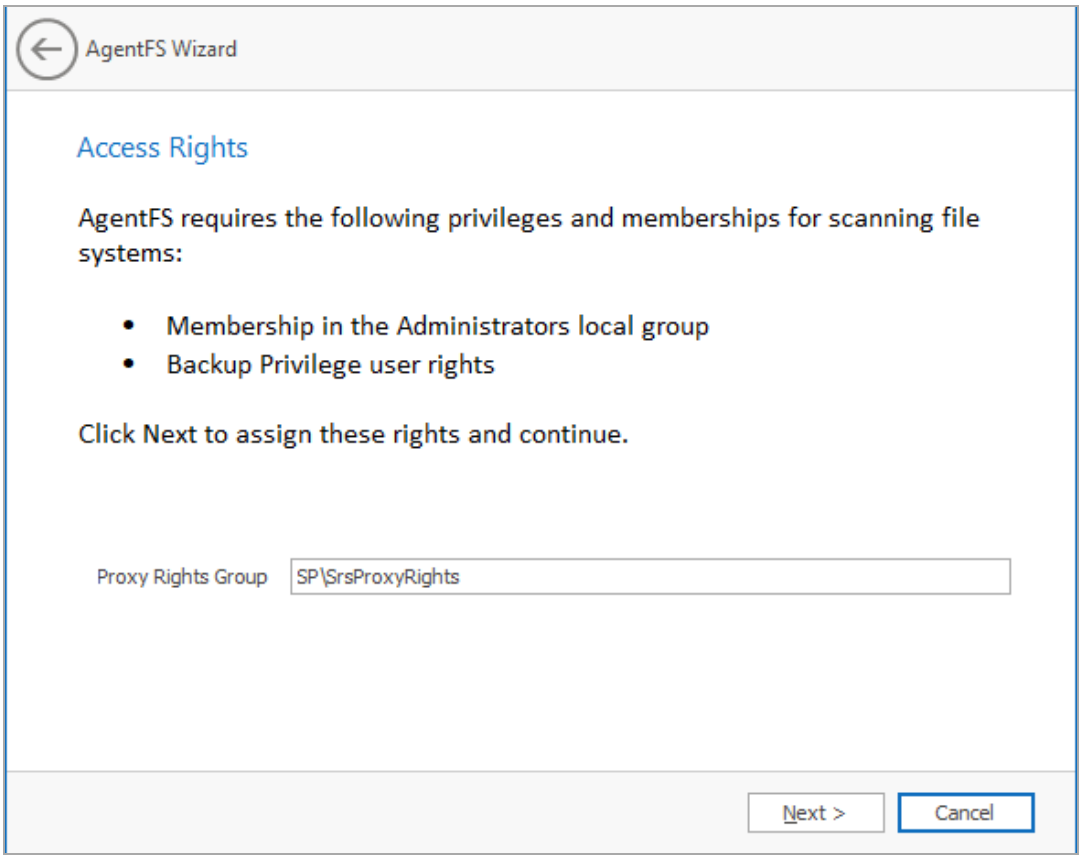
5. Edit any necessary parameter settings and click *Next*.



From this window, you can set parameters for AgentFS to communicate with the Engine.

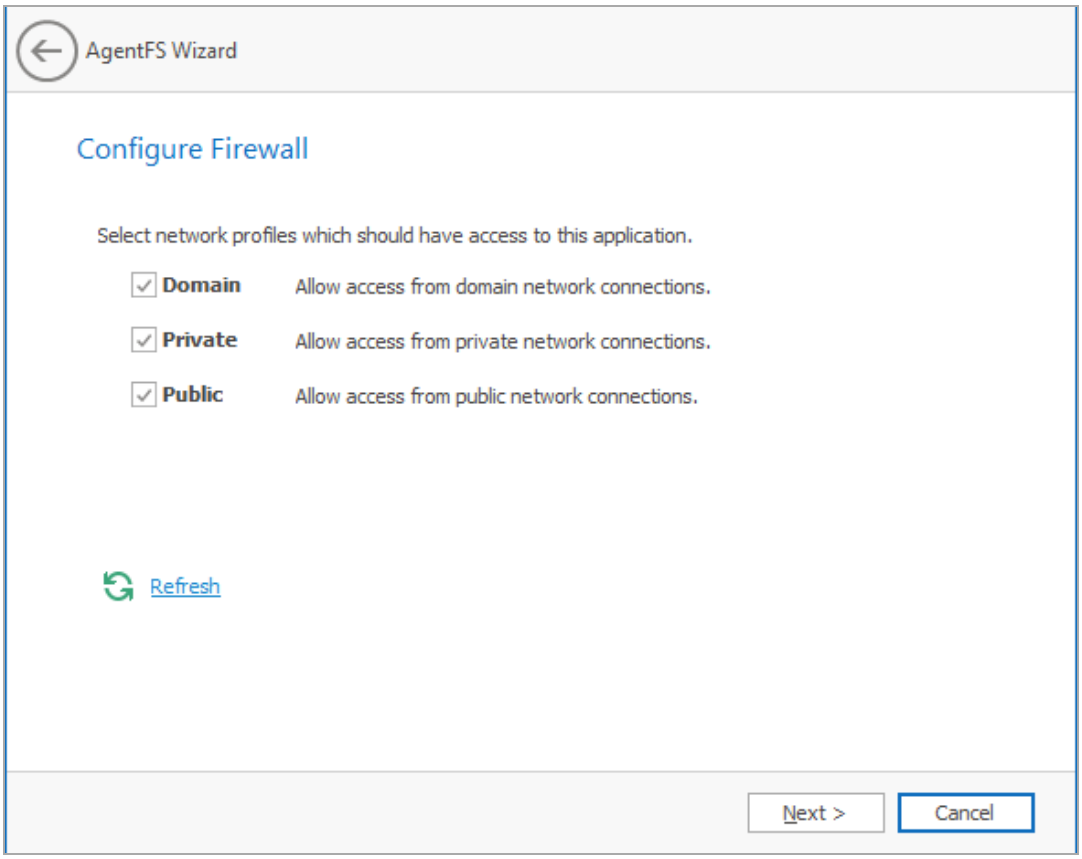
- **Engine Address**: Specify the DNS name or IP address of the server hosting the Engine.
- **Engine Port**: Specify the TLS port for the Engine.

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

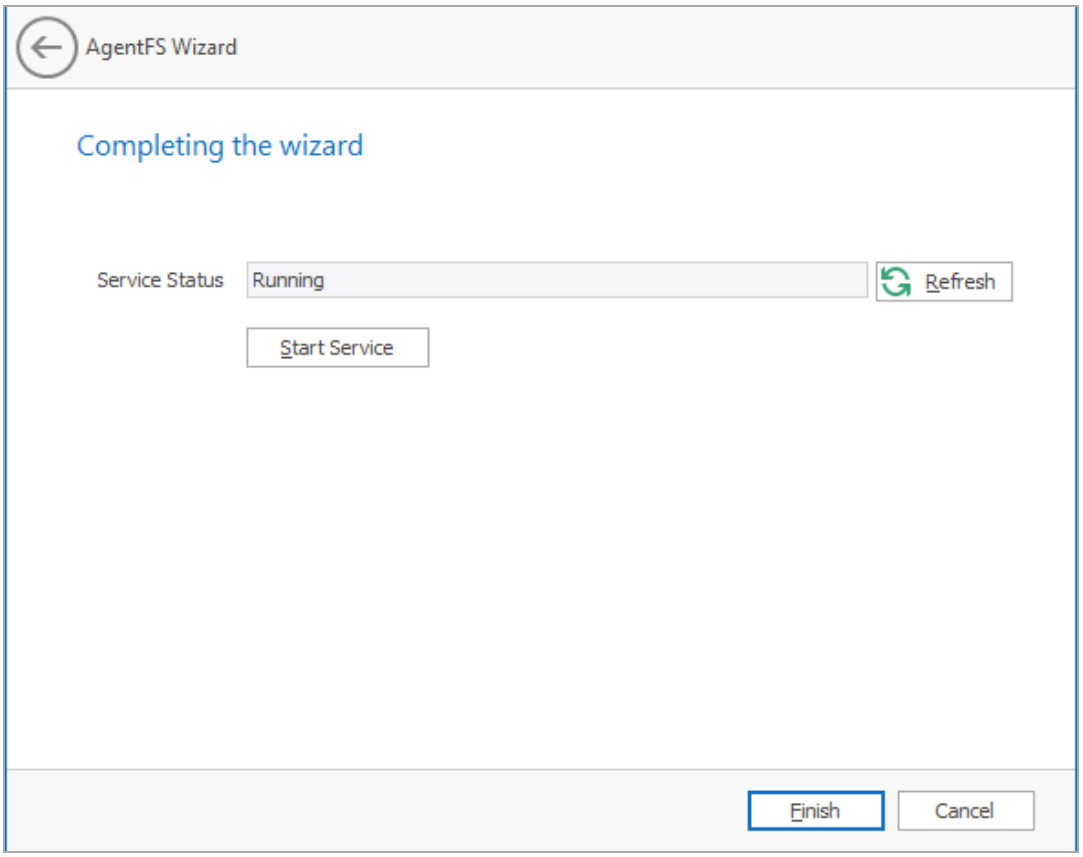


From this window, you can establish AgentFS as a member of the Administrators local group and give it the ability to back up to the SrsProxyRights group.

7. Click *Next*.



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



9. Click *Finish* to complete the AgentFS configuration.

8 - File Content Scans

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

File content scanning requires setup of the following components:

- RabbitMQ message broker —see *RabbitMQ Configuration (page 29)*.
- ManagerFC (see *ManagerFC (page 71)*).
- AgentFC (see *AgentFC (page 77)*).

8.1 - ManagerFC

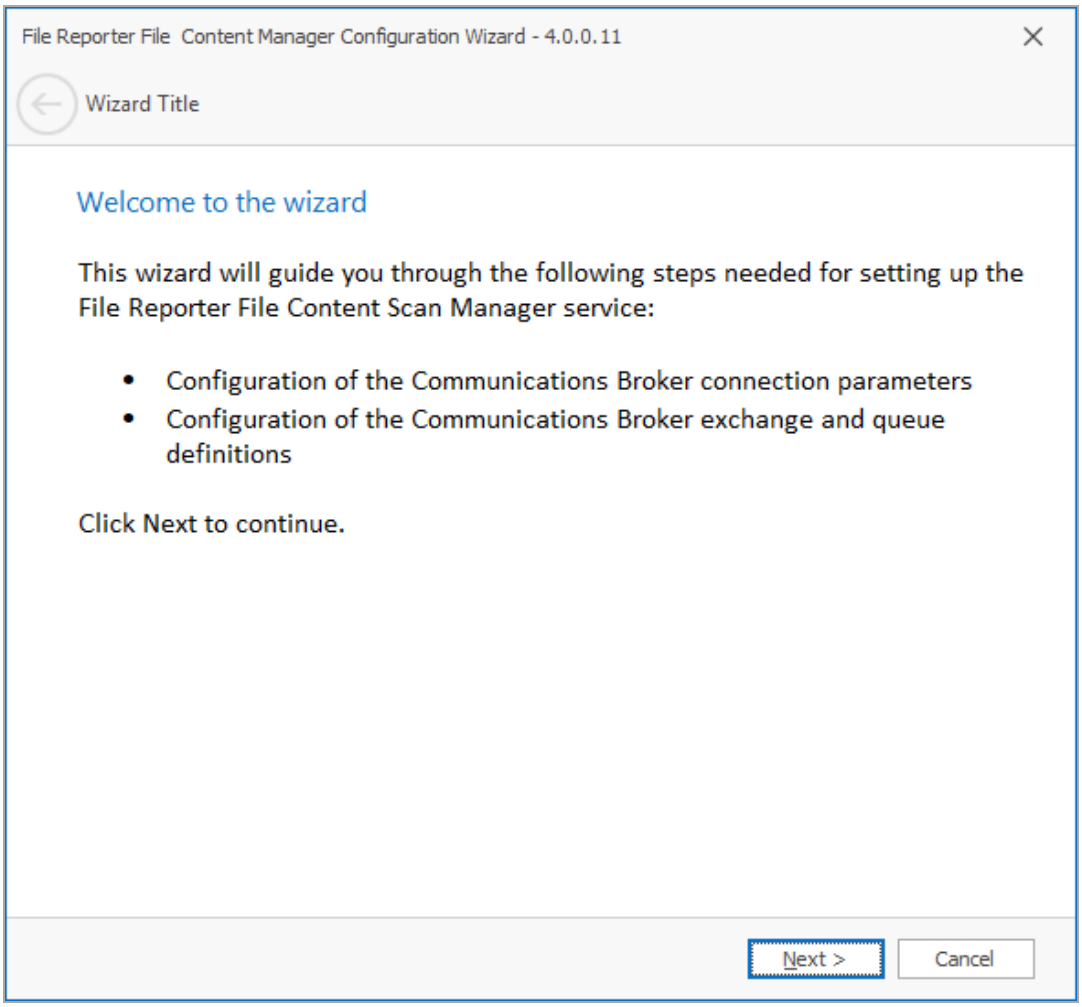
8.1.1 - Minimum Requirements

ManagerFC has minimal processor and RAM requirements, so it should be installed on the same host as the Engine with the following components:

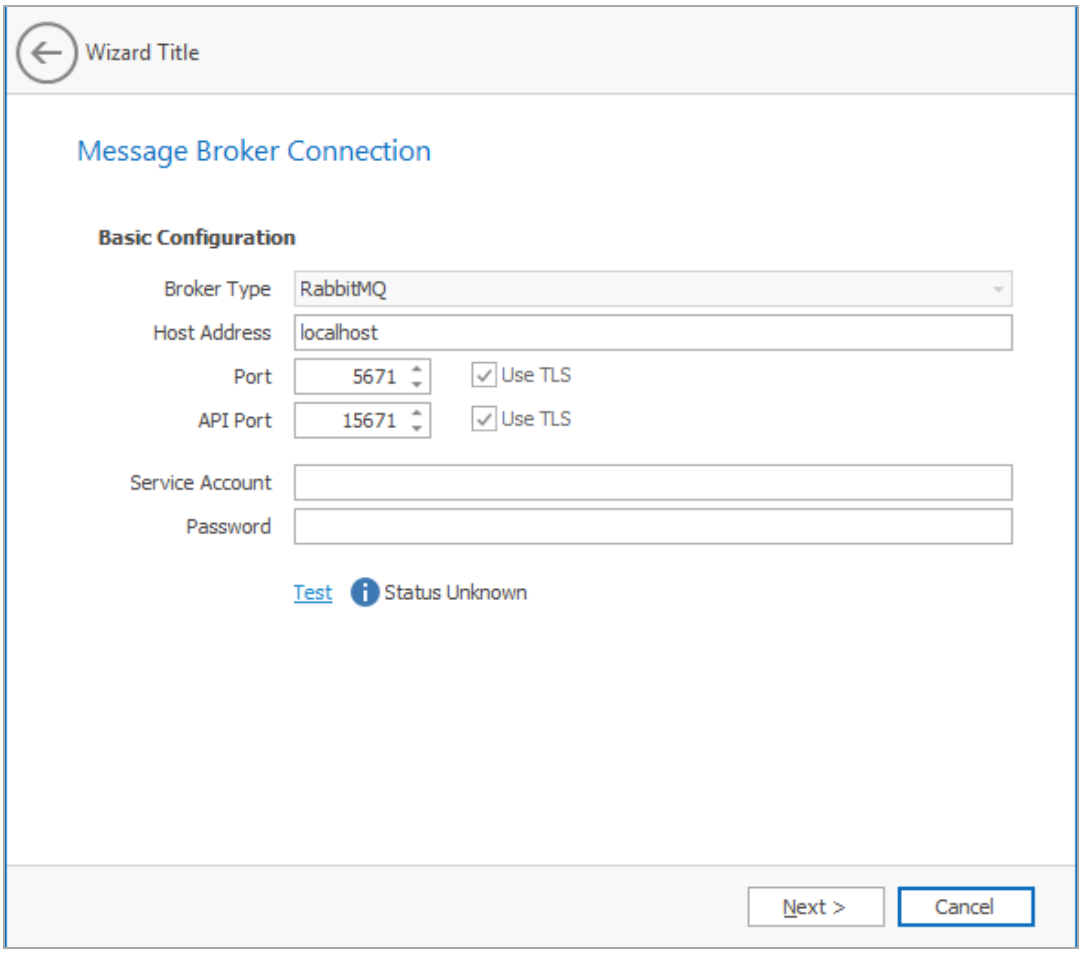
- Any of the following server platforms:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
- Quad-core processor
- 6 GB RAM
- 2 GB free disk space

8.1.2 - Installation and Configuration

1. Double-click `FileReporter-ManagerFC-24.4-x64-xx.exe` at the root of the `FileReporter-24.4.iso` image.
2. Agree to the license terms and conditions, and click *Install*.
3. When notified that the setup was successful, click *Run Setup Utility*.



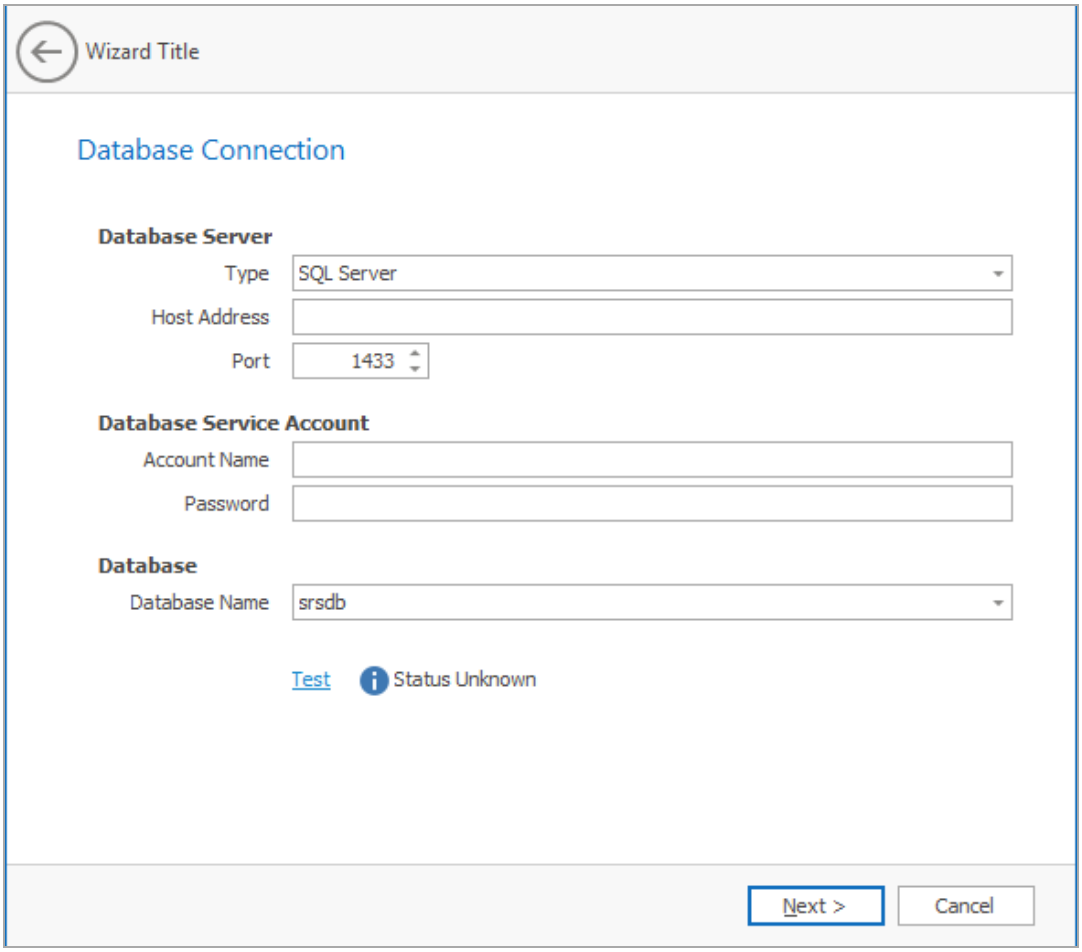
4. From this window, review what is to be installed and configured, and click *Next*.



- **Basic Configuration**: Details the options to configure 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**: RabbitMQ's Management API uses this TLS-enabled port (default: 5671).
  - **Use TLS**: Already checked because RabbitMQ in File Reporter uses Transport Layer Security (TLS) as the cryptographic communications security protocol.
  - **API Port**: RabbitMQ's Management API listens on this port with TLS support enabled (default: 15671).
  - **Use TLS:** Already checked because TLS-enabled communication channels are required for File Reporter.

- **Service Account**: Use the administrator name you established when *Configuring the Message Broker (page 51)*
- **Password**: Use the password you established in *RabbitMQ Configuration - Changing the Administrator Password*
- **Test**: Click to verify the connection between ManagerFC and RabbitMQ.

5. Complete the fields and click *Next*.

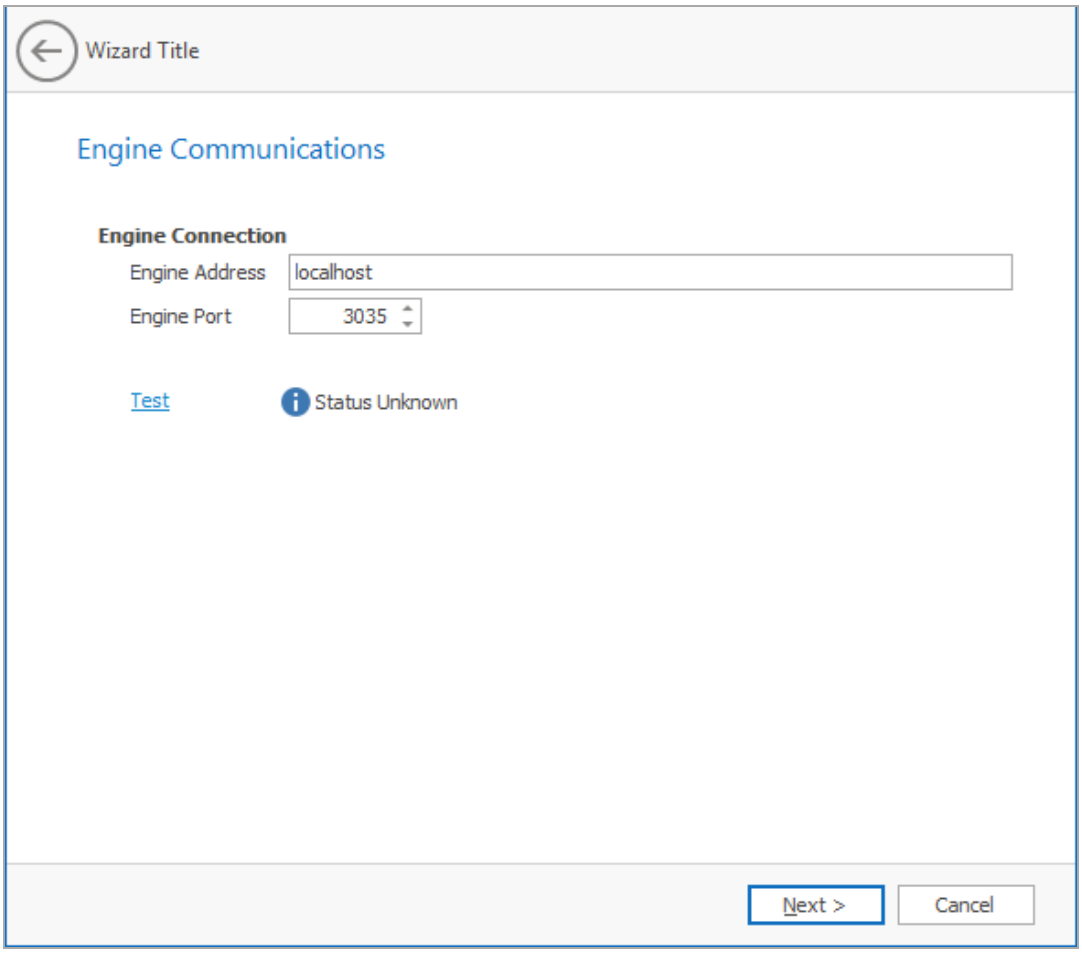


From this window, you can establish the connection between ManagerFC and the database.

- **Database Server**: Details information specific to the database host.
  - **Type**: Select either PostgreSQL or Microsoft SQL Server, depending on the database you use.

    - **Host Address**: Specify the host address of the server on which the database is installed.
    - **Port**: The default PostgreSQL database port setting is 5432. The default Microsoft SQL Server port setting is 1433.
- **Database Service Account**: Details the authentication information for the Database Service User.
    - **Account Name**: Specifies the database account name 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**: Details information specific to the database name.
    - **Database Name**: Indicates the name of the database you established during configuration.
    - **Test**: Click to test the connection between ManagerFC and the database.

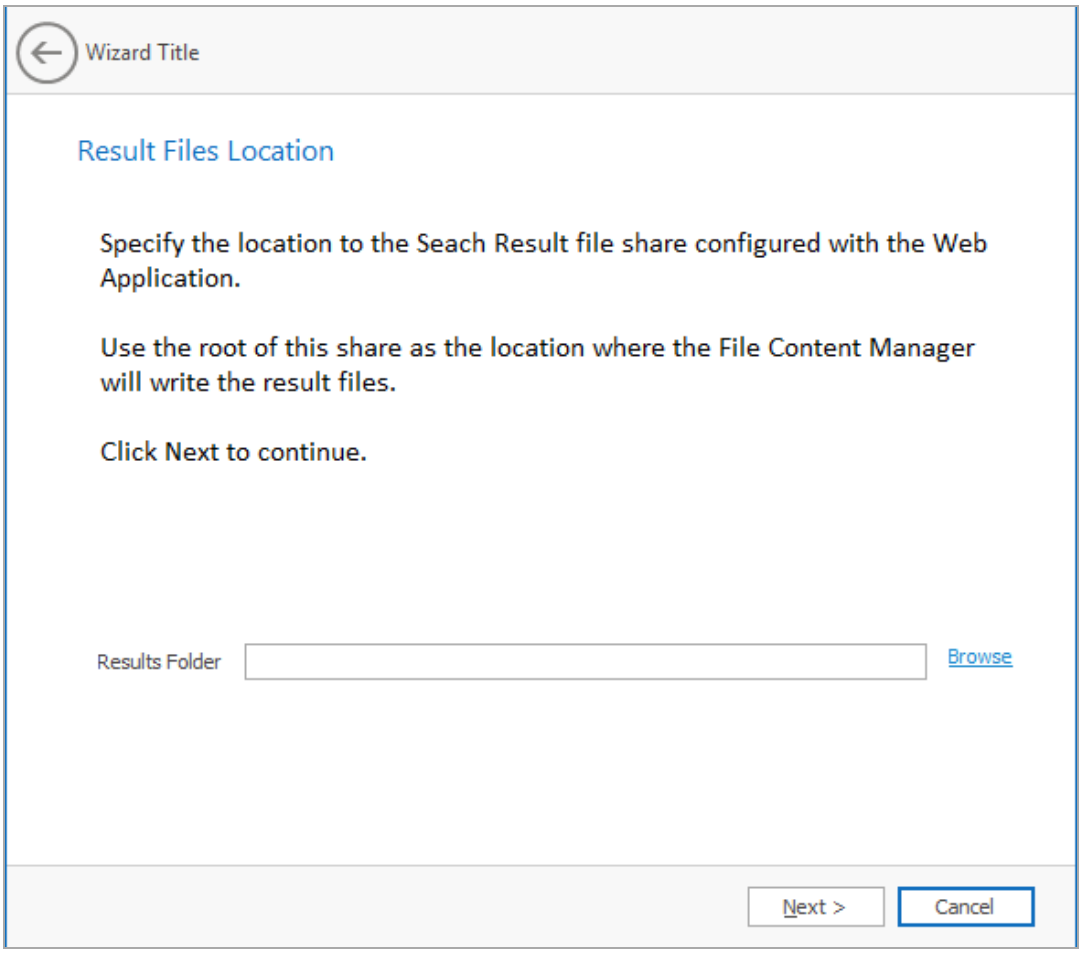
6. Complete the fields and click *Next*.



From this window you can set the parameters for ManagerFC to communicate with the Engine.

- **Engine Address:** Specify the DNS name or IP address of the server hosting the Engine.
- **Engine SSL Port:** Specify the SSL port for the Engine.

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



From this window, you can 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 created when you installed and configured the Web Application —see*Configuring the Web Application (page 53)* .
9. Click *Next*.
10. Click *Finish* to complete the configuration of ManagerFC.

8.2 - AgentFC

8.2.1 - Minimum Requirements

- Any of the following dual-core 64-bit processor servers:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019

- 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

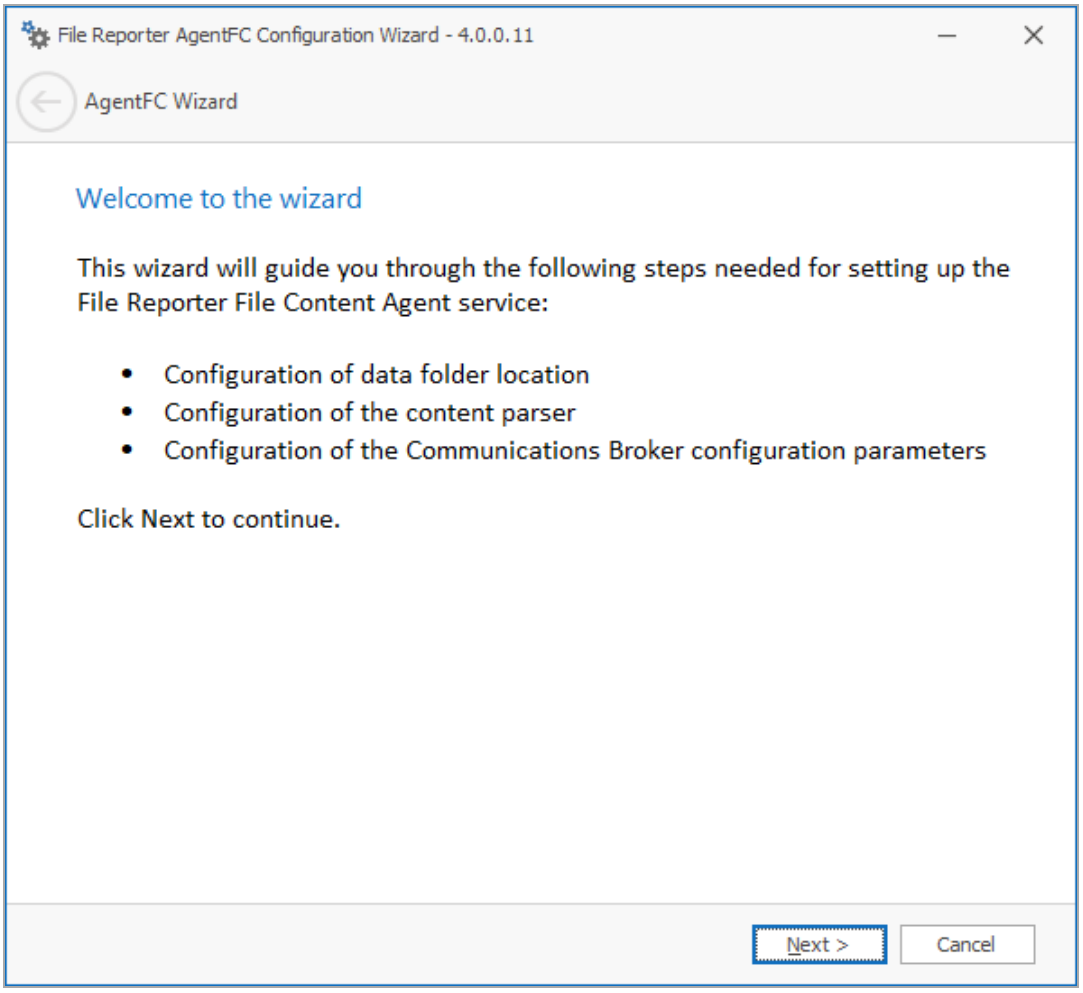
      These numbers may need to be adjusted depending on the workloads.
- Depending on the frequency of workloads, you may want to install each AgentFC node in a virtual machine environment where resources can be scaled as needed.

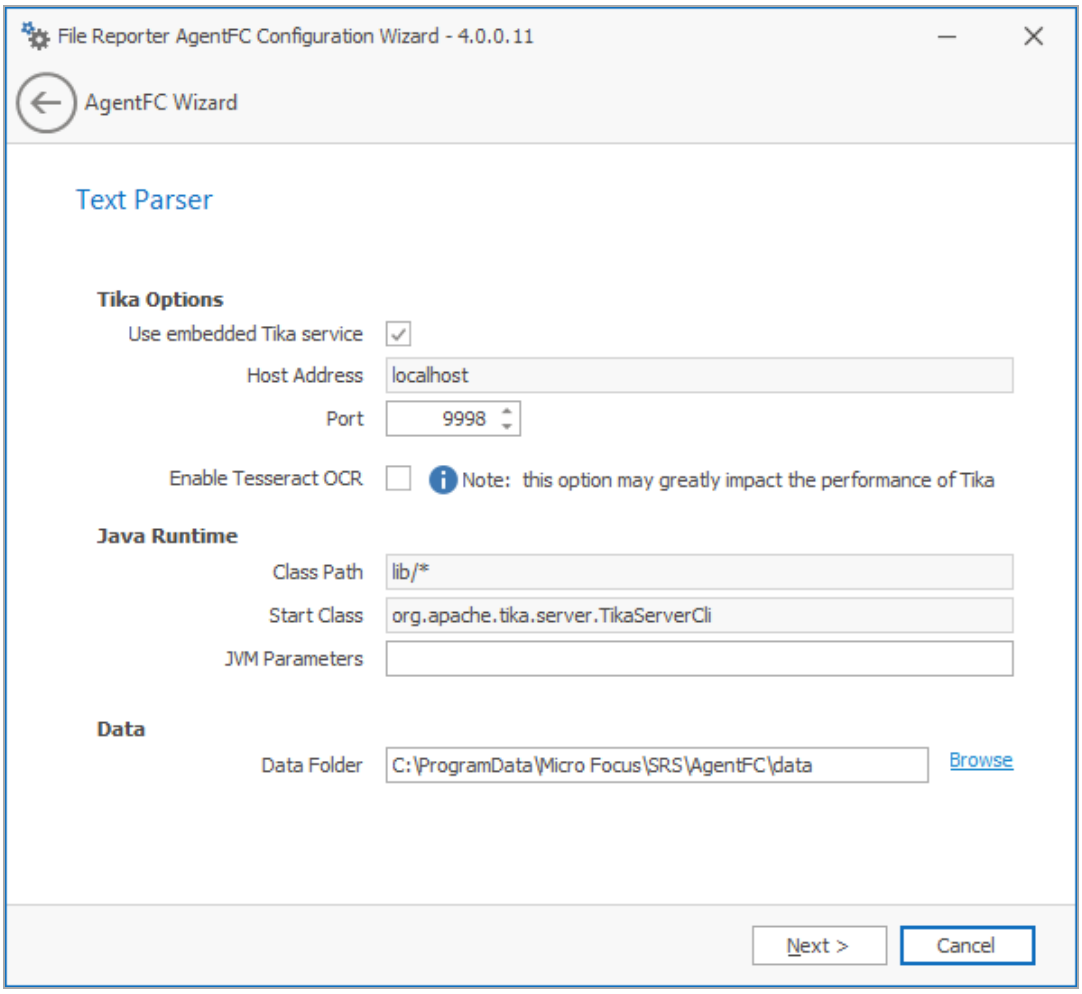
  This can allow for allocation of more resources as heavy workloads are in progress, and reclamation of resources when no jobs are allocated.
- Consider a cluster of three or more nodes for optimum throughput of content scans.

8.2.2 - Installation and Configuration

1. Double-click `FileReporter-AgentFC-24.4.x64-xx.exe` at the root of the `FileReporter-24.4.iso` image.
2. Agree to the license terms and conditions, and click *Install*.

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





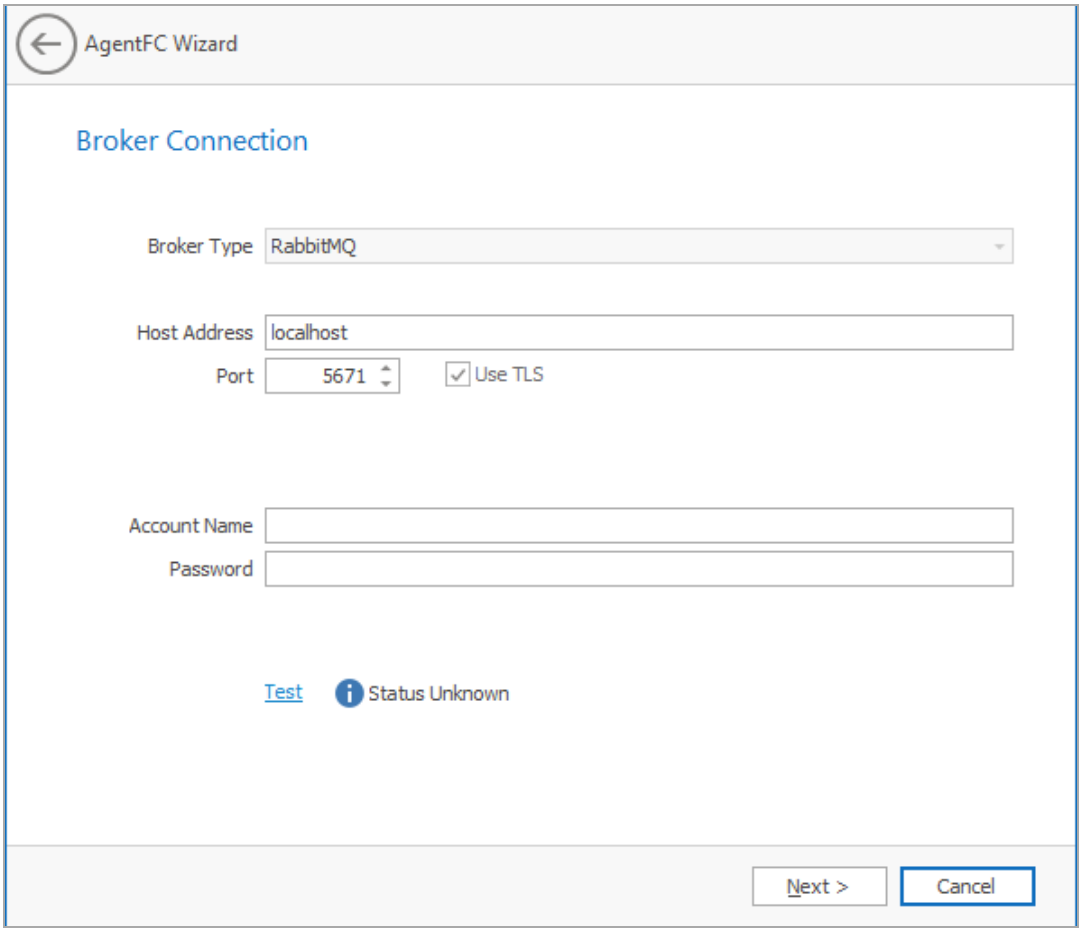
From this window, you can establish specifications for the utilities that perform text parsing and analysis in files.

- **Tika Options**: Details the settings specific to Apache Tika.
    - **Host Address**: AgentFC communicates with Tika via `localhost` on the same computer on which AgentFC is hosted. Do not adjust this setting.
    - **Port**: Leave this setting at 9998 unless there is a conflict.
    - **Enable Tesseract OCR**: This open-source optical character recognition engine from Google analyzes images for textual content. Tesseract OCR is resource-intensive, so it is disabled by default. If you enable Tesseract OCR, you should enable it on all deployed instances of AgentFC, and be aware there may be performance ramifications.
- **Java Runtime**: Details the settings for the Java runtime installed with AgentFC.

- **Class Path**: Displays the location of Java classes and packages, as well as Apache Tika for content analysis. Do not make changes to this field unless directed otherwise during a technical support call.
- **Start Class**: Specifies Apache Tika as a Java Start Class. This field cannot be edited.
- **JVM Parameters**: Advanced tuning parameters for the Java Virtual Machine. Do not make changes to this field unless directed otherwise during a technical support call.

- **Data**: Details information specific to the data gathered through text parsing.
  - **Data Folder**: Specify the temporary location where scanned files are processed before being sent to the database.
  - **Browse**: Specify a new location for the data folder.

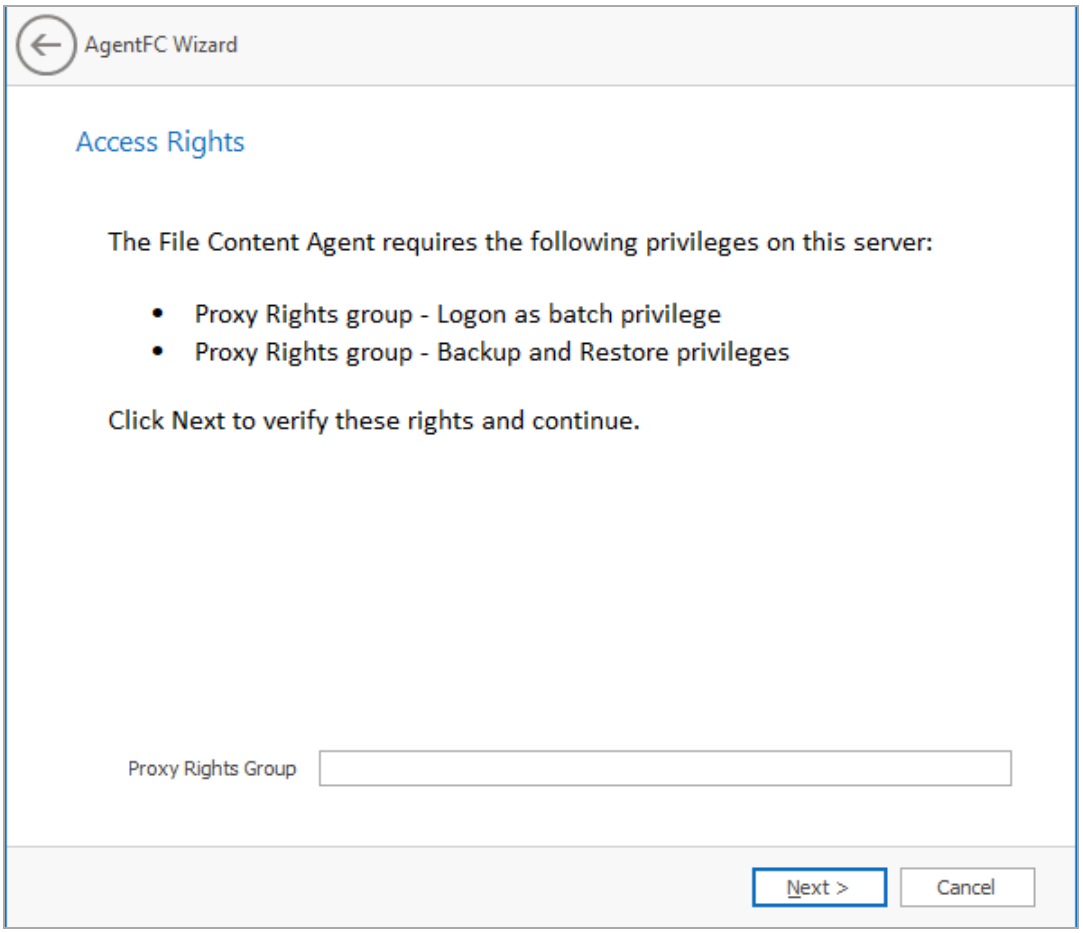
4. Complete the fields and click *Next*.



From this window, you can establish settings for communication between AgentFC and the RabbitMQ messaging broker.

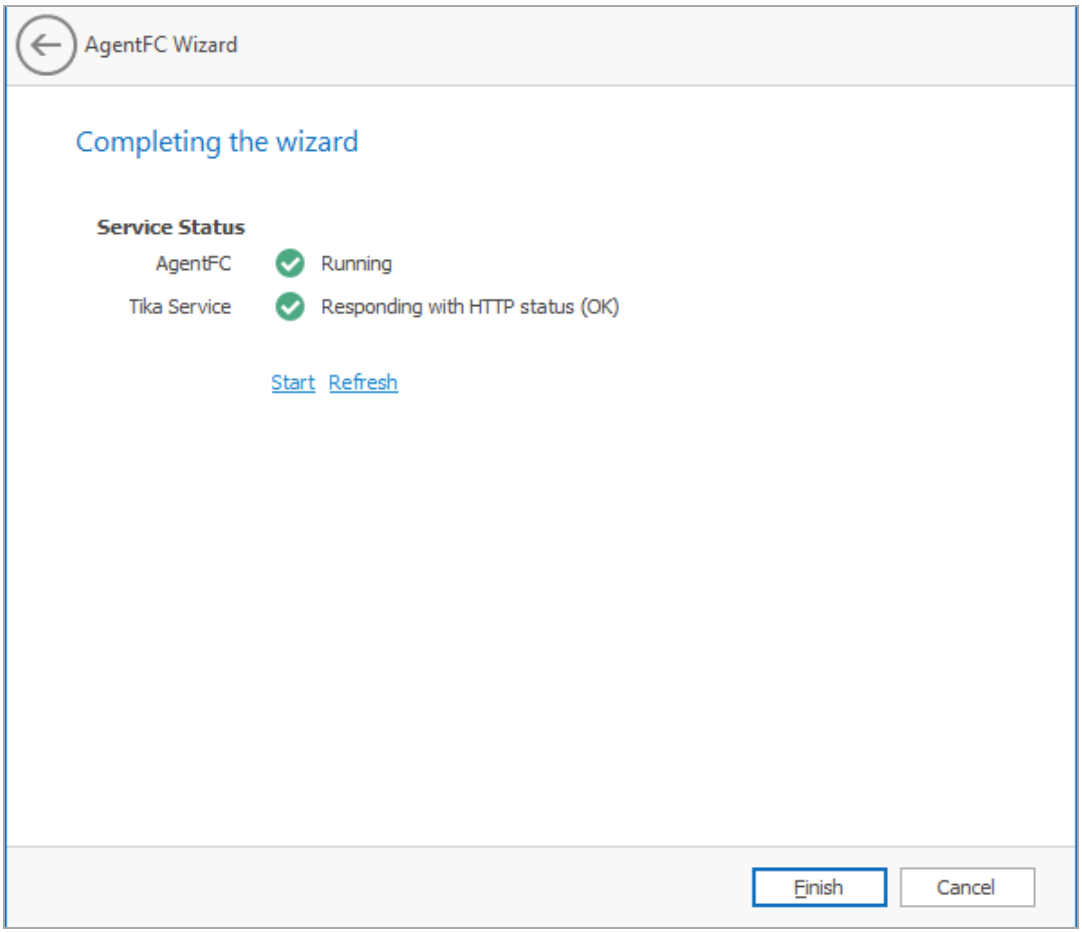
- **Broker Type**: Displays the RabbitMQ messaging broker.
- **Host Address**: Specify the IP address or DNS name of the server hosting RabbitMQ.
- **Port**: This is the port on which RabbitMQ's Management API listens with TLS support enabled (default: 5671).
- **Use TLS**: Already checked because RabbitMQ in File Reporter uses Transport Layer Security (TLS) as the cryptographic communications security protocol.
- **Account Name**: This field displays the default RabbitMQ database broker account name you created during ManagerFC configuration —see *ManagerFC (page 71)* for more information.
- **Password**: Enter the admin account password you set up during ManagerFC configuration.
- **Test**: Click to test the connection between AgentFC and RabbitMQ.

5. Complete the fields and click *Next*.



From this window, you can establish required privileges for the AgentFC host via the Proxy Rights Group.

6. Enter the name of the group in the *Proxy Rights Group* field (default: `SrsProxyRights`).
7. Click *Next*.



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

9 - Microsoft 365 Integration

The following procedures cover the configuration of your Microsoft 365 tenant for reporting through File Reporter, and then the installation and configuration of Agent365 for scanning Microsoft 365 endpoints.

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

NOTE: If you do not intend to report on Microsoft 365 cloud applications, then you can ignore the procedures in this section.

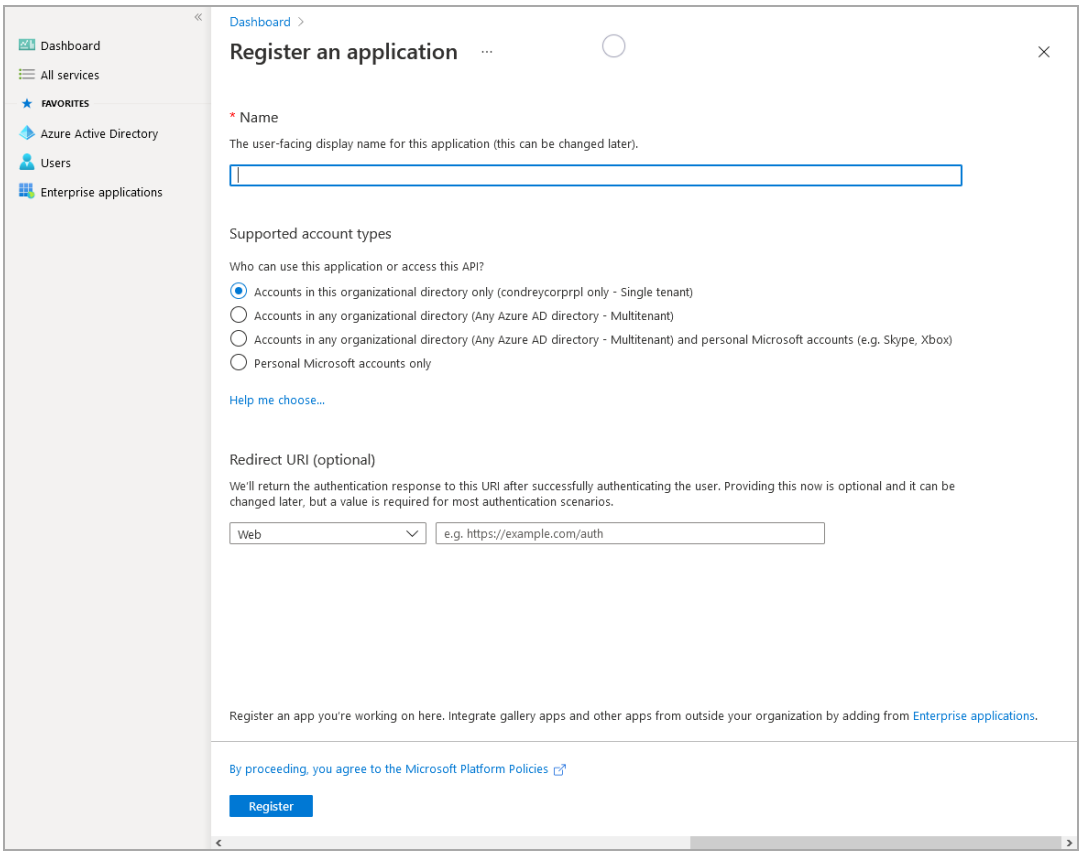
9.1 - Prerequisites

9.1.1 - Message Broker

Verify that the Message Broker is installed, configured, and connected in the Configuration Dashboard.

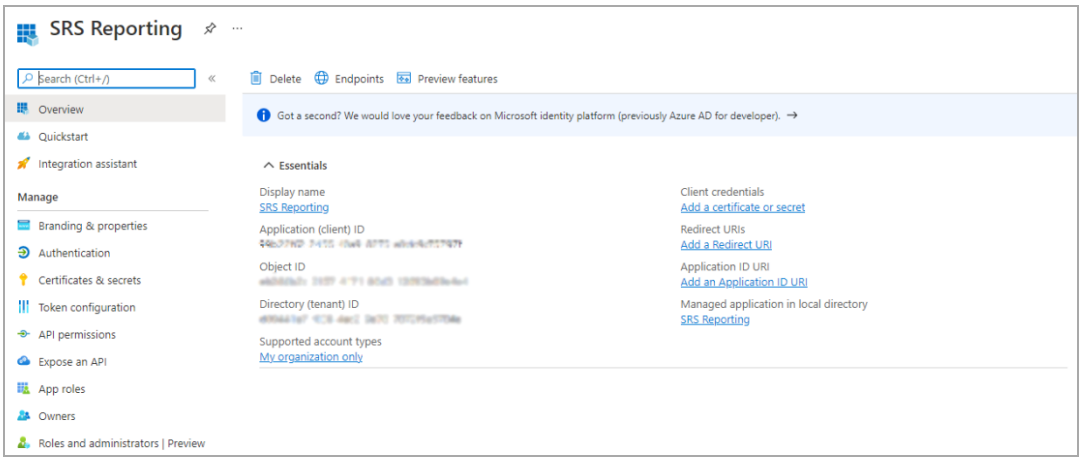
9.1.2 - Preparing the Microsoft 365 Tenant

1. Authenticate to your tenant's Microsoft 365 Admin Center at https://admin.microsoft.com.
2. Select *Show all* in the *Navigation* menu.
3. Select *Identity* under *Admin centers* to launch the Microsoft Entra ID admin center.
4. Expand the *Identity* > *Applications* in the *Navigation* menu.
5. Select *App registrations*.
6. Click the *New registration* tab.



7. Enter a descriptive name for the application registration (e.g., `SRS Reporting`) in the *Name* field.
8. Select the *Single tenant* option (the first option) in the *Supported account types* region.
9. Leave the default settings for *Redirect URI (optional)* and click *Register*.

   The application is now registered, and the settings are displayed.

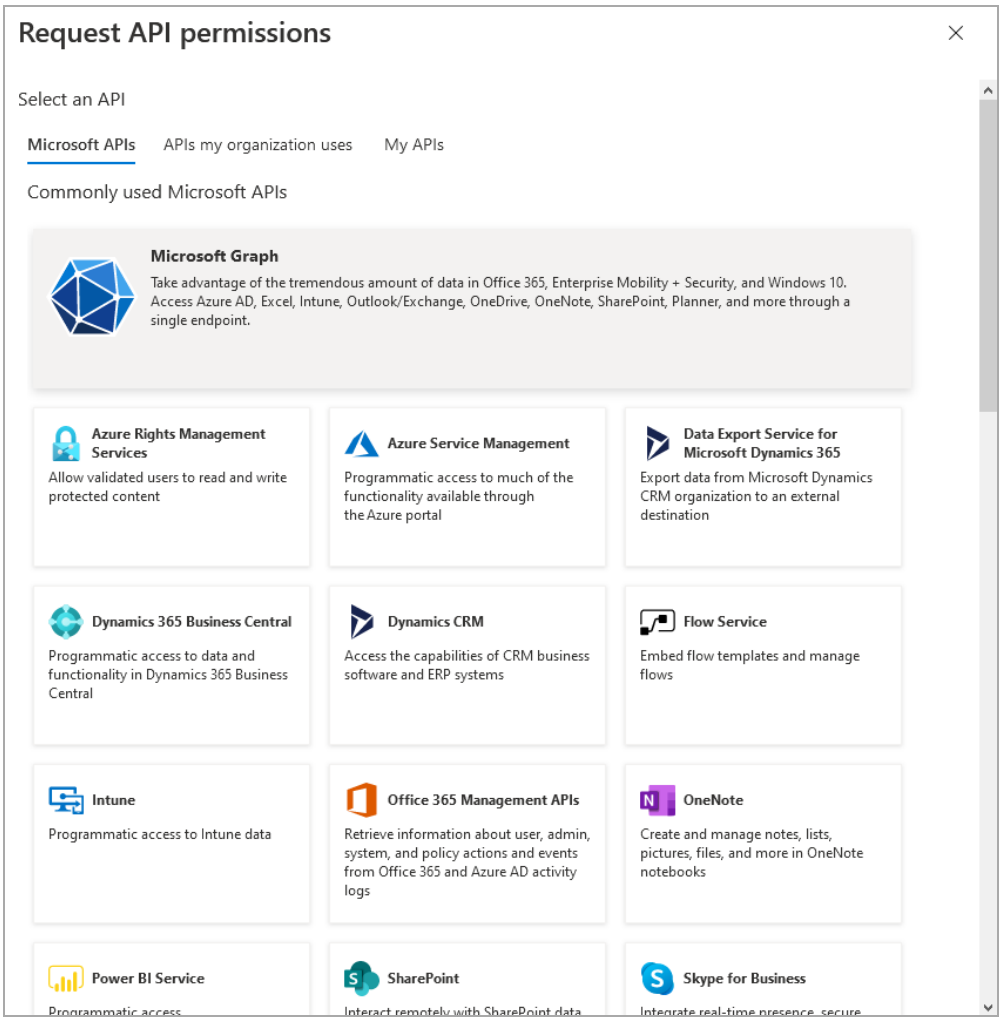


10. Select *API permissions* in the *Manage* menu.
11. Set the following application permissions for the Microsoft Graph API.

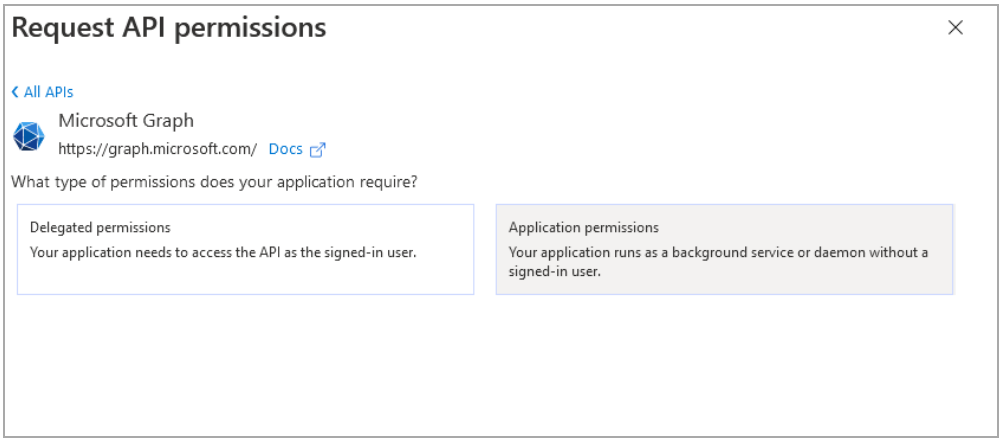
a. Refer to the following table as you establish application permissions:

Microsoft API	API / Permissions	Name Description
Microsoft Graph	Directory.Read.All	Read directory data.
	Files.Read.All	Read files in all site collections.
	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.
SharePoint	Sites.FullControl.All	Read and manage all Sites including site users, groups, and permission levels.

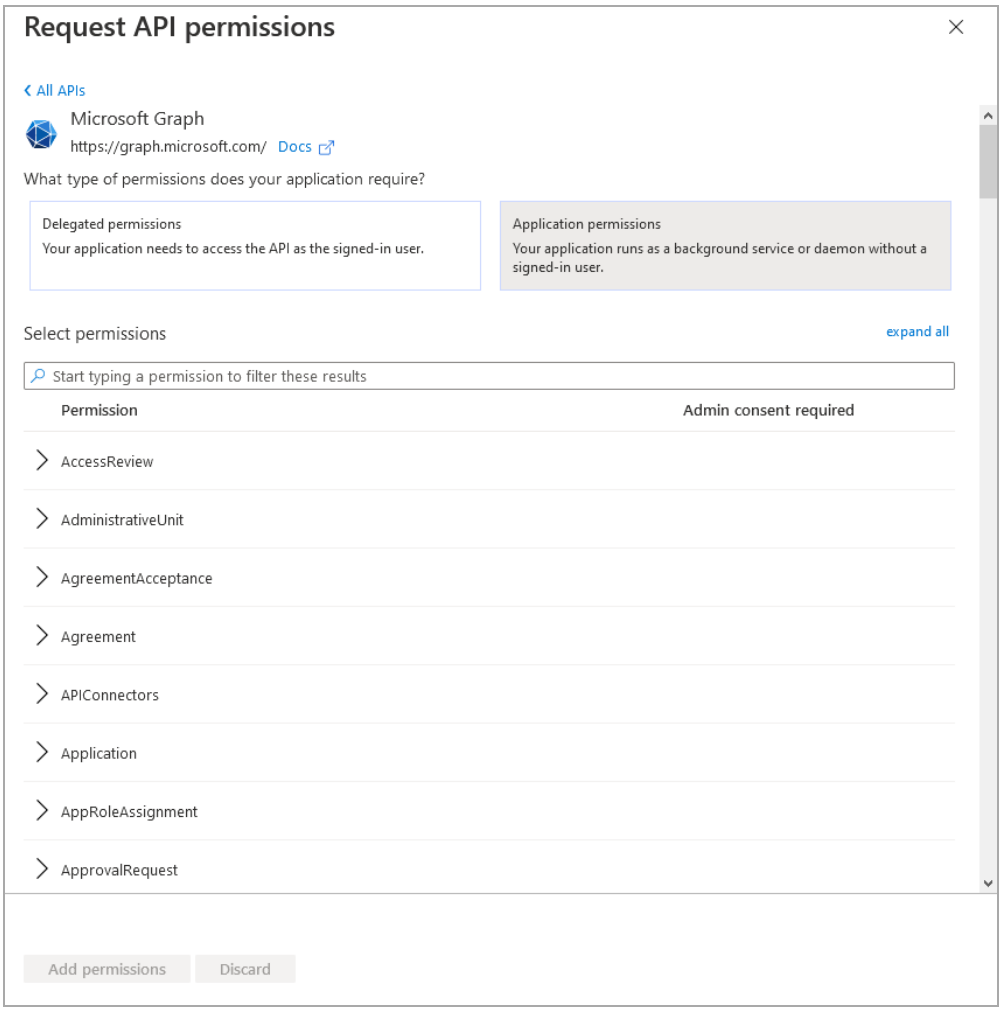
b. Click the *Add a permission* tab.



c. Click the *Microsoft Graph* API.

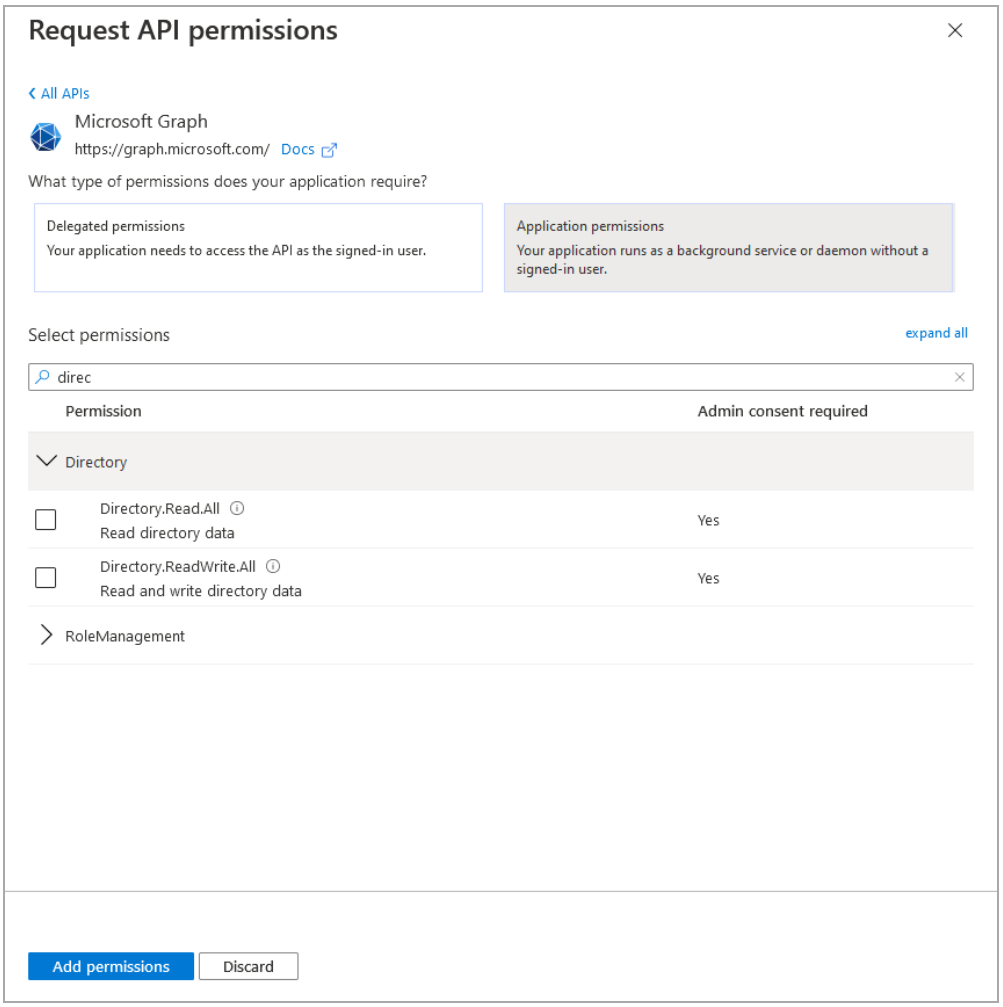


d. Click *Application permissions*.



e. Refer to the table in step 11a and begin typing `directory` to filter the *Directory* permissions.

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



g. Refer to the table in step 11a to verify that the permissions to select are *Directory.Read.All Read directory data*, then check that specific box to add the `Directory.Read.All` permission to the Configured Permissions table.

h. Repeat steps 11e-11g to filter and add each of the permissions specified in the table in step 11a for Microsoft Graph.

i. Click *Add permissions*.

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

12. Set the following application permission for SharePoint.

    a. Click *Add a permission* tab.

    b. Click the SharePoint API.

    c. Click *Application permissions*.

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

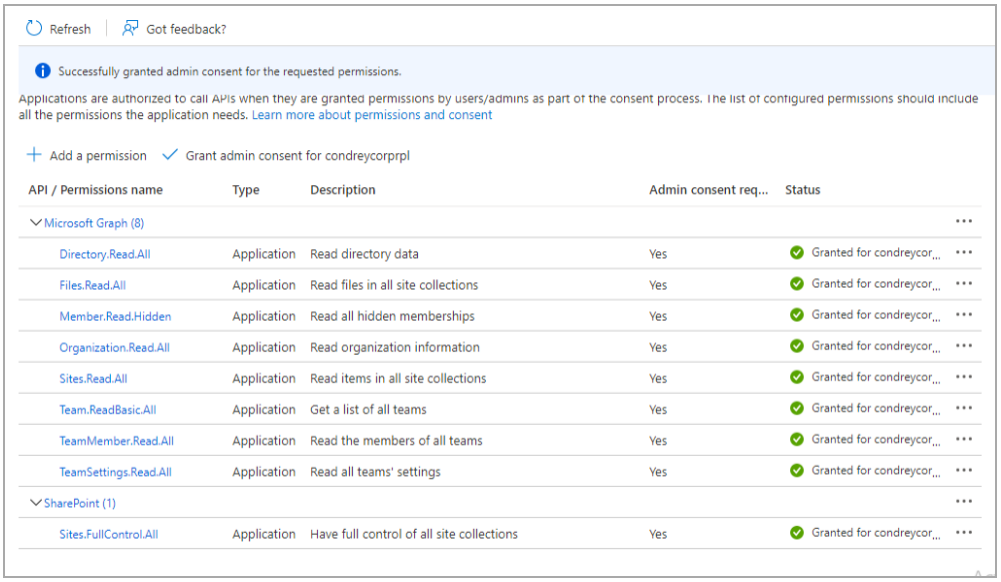
e. Select the *Sites.FullControl.All* option.

f. Click *Add permissions*.

13. Grant admin consent for the tenant.

a. Click *Grant admin consent for tenant_name* above the list of permissions you just established.

b. Click *Yes* when asked if you want to grant consent for the requested permissions for all accounts in *tenant_name*. The status of each permission is changed to *Granted for tenant_name*.



9.2 - Agent365

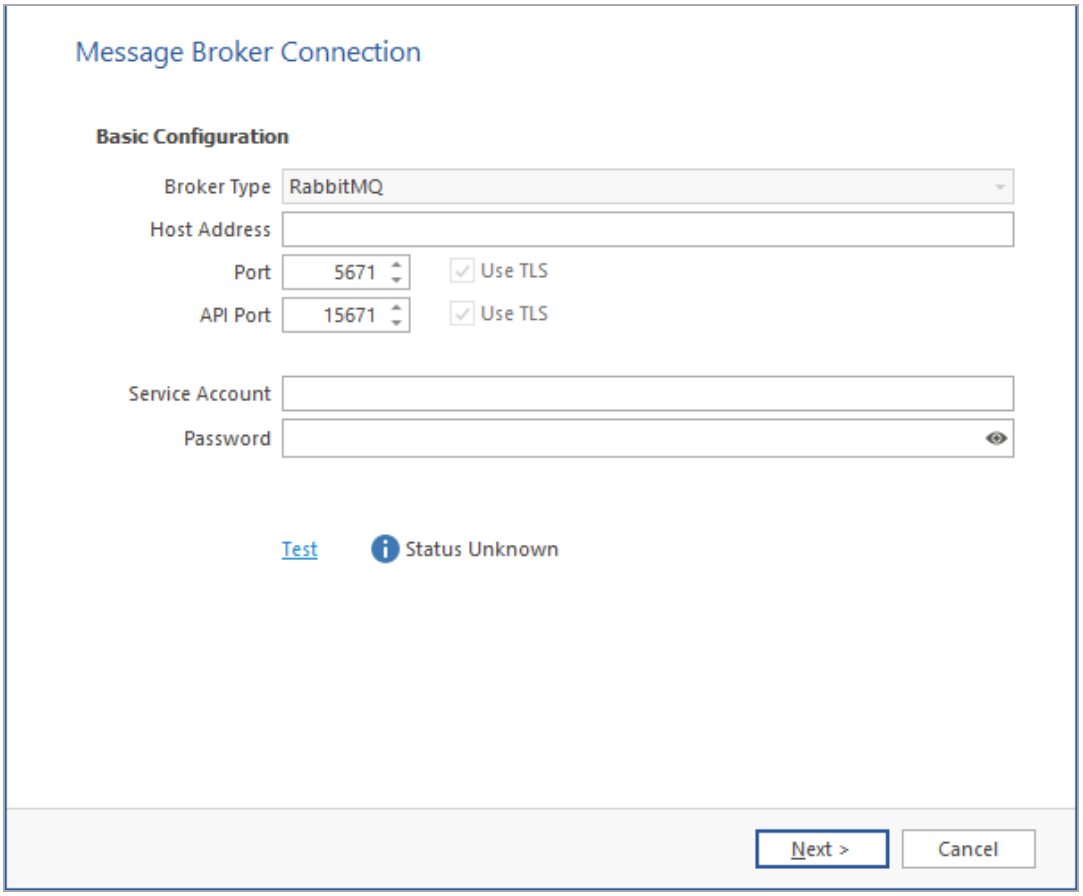
The following describes the procedures for installing and hosting Agent365.

9.2.1 - Minimum Requirements

- Any of the following dual-core 64-bit processor servers:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
- The server must be joined to Active Directory.
- .NET 8.0 Desktop Runtime (this will be installed if not already present)
- 200 MB RAM

9.2.2 - Installation and Configuration

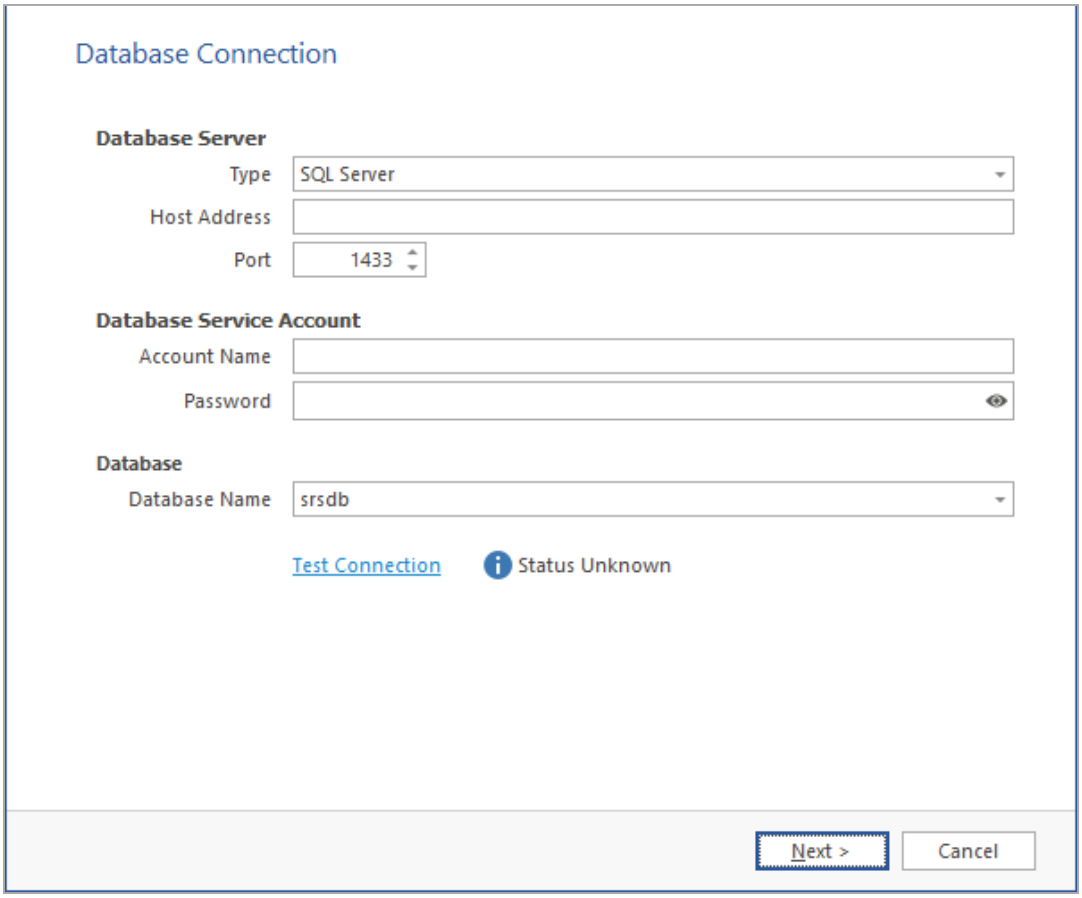
1. Double-click `FileReporter-Agent365-24.4.x64-xx.exe` at the root of the `FileReporter-24.4.iso` image.
2. Agree to the license terms and conditions, and click *Install*.
3. When notified that the setup was successful, click *Run Setup Utility*.
4. From this window, read the overview of what is to 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:** Specifies the port that RabbitMQ's Management API listens on with TLS support enabled (default: 5671).

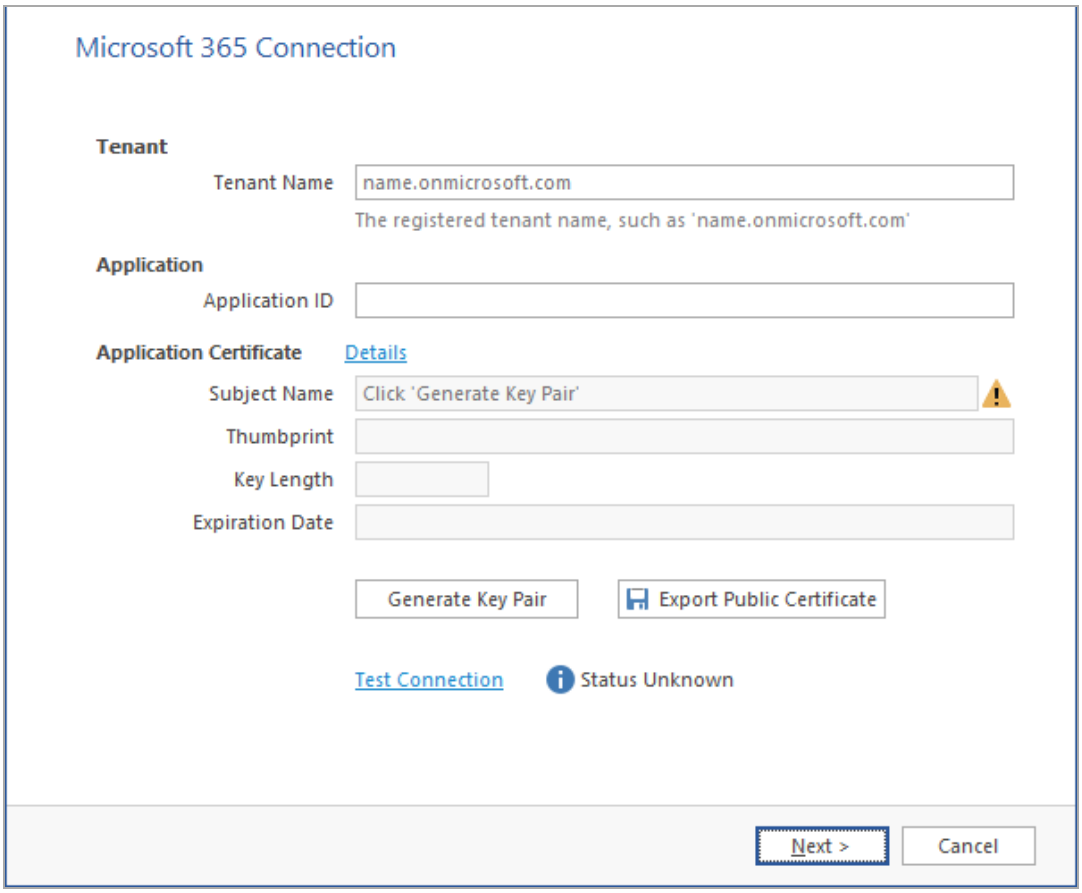
- **Use TLS:** Already checked because File Reporter requires Transport Layer Security (TLS) as the cryptographic communications security protocol.
- **API Port:** Specifies the port RabbitMQ's Management API listens on with TLS support enabled (default: 15671).
- **Use TLS:** Already checked because File Reporter requires TLS-enabled communication channels.
- **Service Account:** Enter the name of the service account (default: `srsbroker`). For reference, your service account name is displayed in the *Message Broker* field of the Configuration Dashboard.
- **Password:** Enter the password you established when configuring the Message Broker.
- **Test:** Click to test the connection between Agent365 and RabbitMQ.

5. Complete the fields and click *Next*.



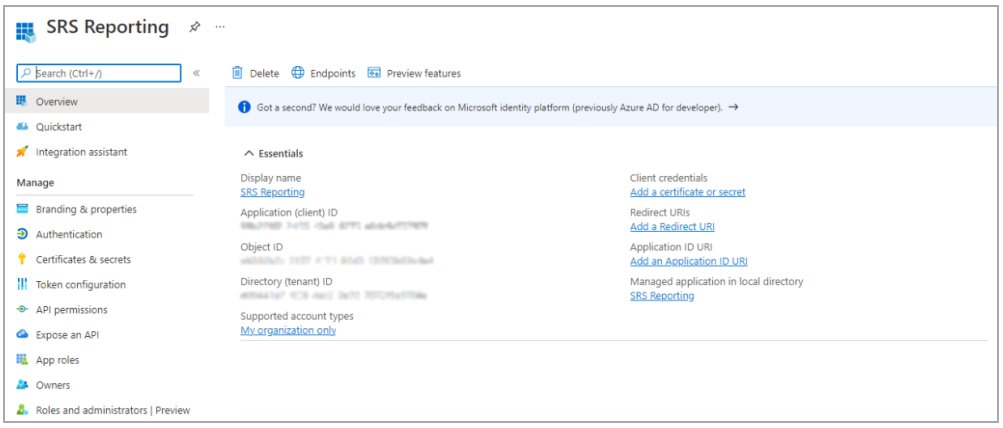
- **Database Server:** Details fields specific to communication with the PostgreSQL or Microsoft SQL Server database.
    - **Type:** From the drop-down menu, specify the database type.
    - **Host Address:** Enter the IP address of the server hosting the database you configured earlier. For reference, the IP address is displayed in the *Database* field of the Configuration Dashboard.
    - **Port:** Leave the setting at `1433` unless you changed the default port address when configuring the database.
- **Database Service Account:** This region includes fields for the database service account and password.
    - **Account Name:** Enter `srsadmin`unless you changed the default name for the Database Service User. For reference, the name is displayed in the *Database User* field in the *Database* section of the Configuration Dashboard.
    - **Password:** Enter the database administrator password.
- **Database Name:** Enter `srsdb` unless you changed the default name for the database name. For reference, the database name is displayed in the *Database* field of the Configuration Dashboard.
- **Test Connection:** Click to test the connection between Agent 365 and the database.

6. Complete the fields and click *Next*.



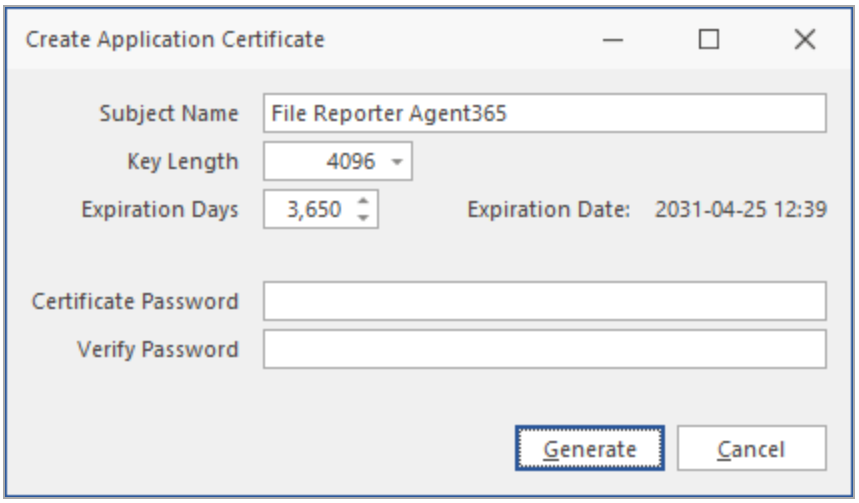
You must log in to your Azure AD tenant to complete the following fields:

- **Tenant:** Enter the name of your tenant. For reference, you can select *Azure Active Directory* in the Azure Active Directory admin center interface to view this name.
- **Application ID:** Enter the name of the application you registered and configured previously. For reference, you can identify the application ID in the Azure Active Directory admin center:
    a. Click *App registrations*.
    b. Click the listed registered application.
    c. Copy the *Application (client) ID* listing into the *Application ID* field of the File Reporter Agent 365 wizard.



- **Application Certificate:** Generate the key pair for the application certificate. When complete, the fields fill in automatically.

7. Generate the application certificate.
    a. Click *Generate Key Pair*.
    b. When the Certificate Update Notice dialog box appears, click *Yes* to open the following dialog box:



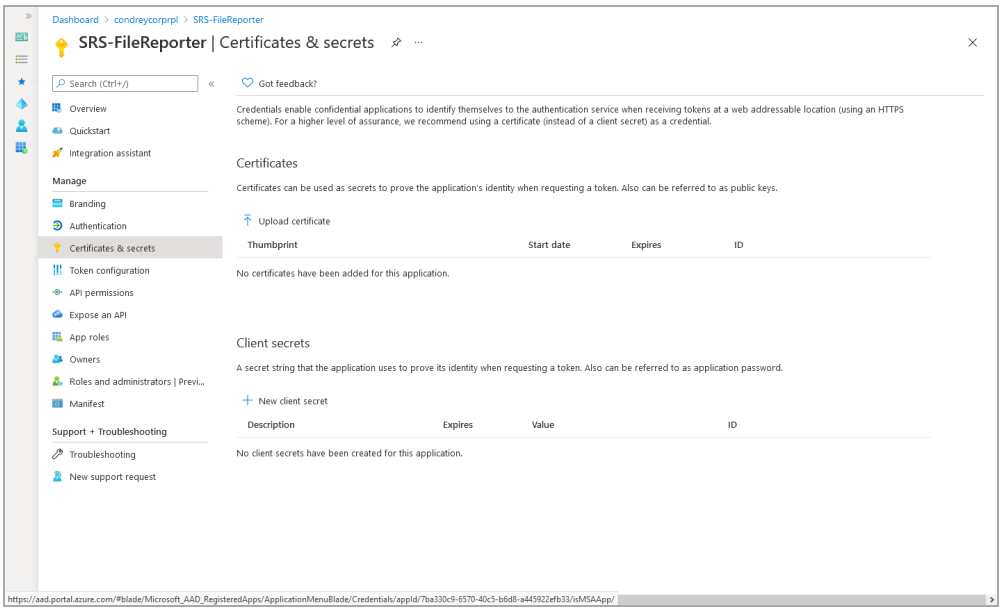
    c. Create a password for the certificate in the *Certificate Password* field.
    d. Enter the password again in the *Verify Password* field.
    e. Click *Generate*.

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

f. Click *Export Public Certificate*.

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

h. Click *Certificates & secrets* in the Azure Active Directory admin center.



i. Click *Upload certificate* to select and *Open* the location where you saved the certificate, then click *Add*.

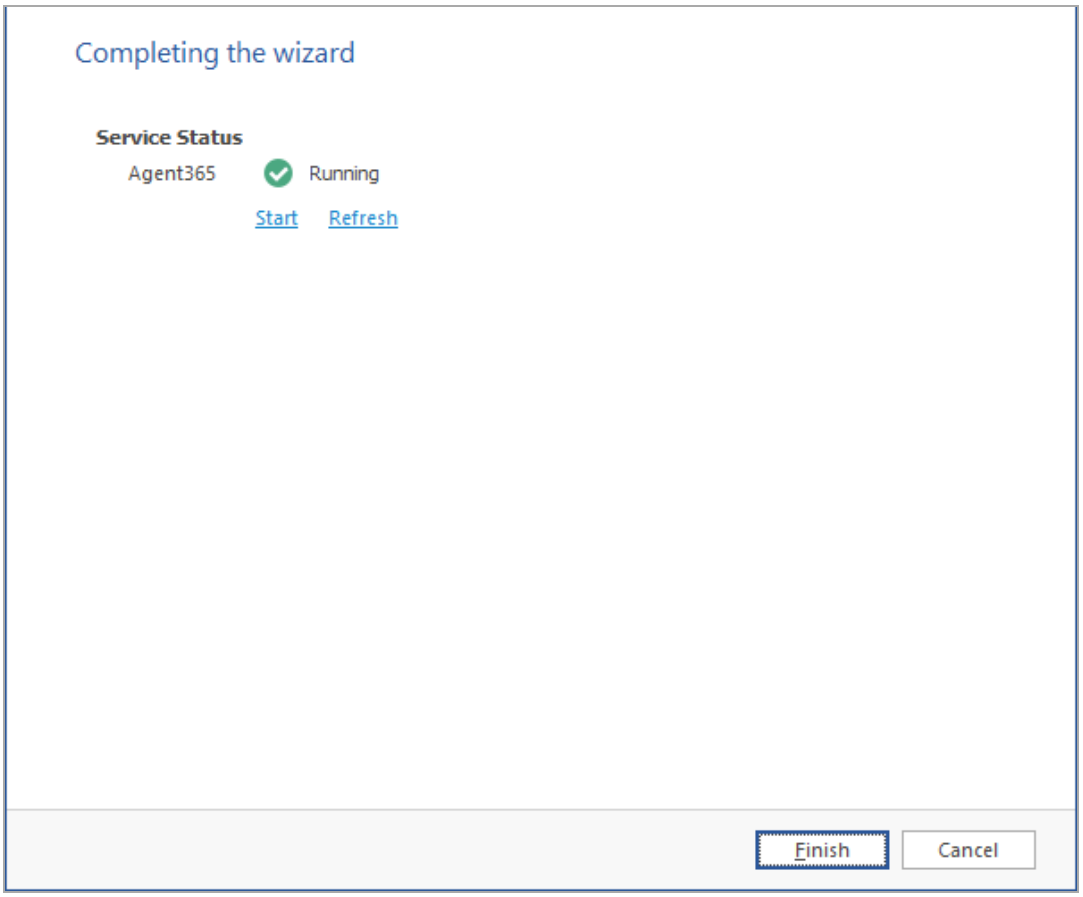
The certificate is now listed in the *Certificates* field of the Azure Active Directory admin center page.

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

> **NOTE:** If you get a failure notice, it most likely means that the tenant has not had enough time to update.
>
> Wait several seconds and click *Test Connection* again until you get a *Connection valid* indication on the wizard page and a Tenant Info dialog appears with the updated tenant information. Synchronization of the public certificate may take a couple minutes to complete.

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

8. Click *Next* to advance the wizard.



9. Click *Finish*.