Micro Focus File Reporter 3.6

Installation Guide

January 6, 2020

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
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

This installation guide is written to provide network administrators the conceptual and procedural information for installing and configuring Micro Focus File Reporter 3.6.

Audience

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

Feedback

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

Documentation Updates

For the most recent version of the *Micro Focus File Reporter 3.6 Installation Guide*, visit the Micro Focus File Reporter Documentation Web site (http://www.novell.com/documentation/filereporter3).

Additional Documentation

For additional Micro Focus File Reporter 3.6 documentation, see the following guides at the Micro Focus File Reporter Documentation Web site (http://www.novell.com/documentation/filereporter3)

- *Micro Focus File Reporter 3.6 Administration Guide*
- *Micro Focus File Reporter 3.6 Database Schema and Custom Queries Guide*

1 Upgrading from a Previous Version

You can upgrade from any version of File Reporter 3.0.*x* or greater by installing the updated software on top of the existing software. In environments where Active Directory is the Primary identity system, there are new optional file content scanning components to be installed. These include The RabbitMQ messaging broker, ManagerFC and AgentFC.

If you are upgrading from File Reporter 2.*x*, you will first need to upgrade to version 3.0. See the documentation at: https://www.novell.com/documentation/filereporter3/file_reporter_3_0_install/data/overview.html. After completing the upgrade to 3.0 you can then follow the instructions here for upgrading to File Reporter 3.6.

- Section 1.1, "Database," on page 9
- Section 1.2, "License," on page 9
- Section 1.3, "Engine, Scan Processor, and Web Application," on page 10
- Section 1.4, "File Content Scanning," on page 10
- Section 1.5, "Agents," on page 10

1.1 Database

File Reporter 3.6 supports only versions of PostgreSQL and Microsoft SQL Server that are supported by The PostgreSQL Global Development Group, and Microsoft, respectively. If you are using a non-supported database, you will need to first upgrade it.

For information on File Reporter supported versions of PostgreSQL, see Section 4.1.1, "Minimum Requirements," on page 21.

For information on File Reporter supported versions of SQL Server, see Section 5.1, "Minimum Requirements," on page 23.

1.1.1 Upgrading the Existing Database

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

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

1.2 License

Upgrading from File Reporter 3.5 to 3.6 does not require an updated license unless you will be integrating File Reporter 3.6 with Micro Focus Identity Governance 3.5. If you are upgrading from a version earlier than 3.5, you will need an updated license. For procedures on updating the license, see Appendix B, "Replace a License File," on page 127.

1.3 Engine, Scan Processor, and Web Application

Upgrade the Engine, Web Application, and Scan Processor by installing the updated Engine installation software on top of the existing software.

To upgrade an Engine where Active Directory is the primary identity system, follow the procedures in Chapter 7, "Installing and Configuring the Engine, Database, and Web Application in an Active Directory Environment," on page 39.

To upgrade an Engine where eDirectory is the primary identity system, follow the procedures in Chapter 8, "Installing and Configuring the Engine, Database, and Web Application in an eDirectory Environment," on page 65.

1.4 File Content Scanning

Introduced with the release of File Reporter 3.5, file content scanning enables you to scan and classify file content. If you plan to utilize this capability, and if you are upgrading from a version of File Reporter other than 3.5, there will be new components to install as part of the upgrade process. For more information, see Section 2.5, "Determine Whether to Scan File Content," on page 16.

1.5 Agents

File Reporter 3.6 includes two Agent types:

- File System
- Content

1.5.1 File System Agents

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

File System Agents include:

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

  The product ISO also includes the legacy Agent for Windows, which you should use only if you need to establish a Windows Agent as a Proxy Agent for an OES storage device.

  NOTE: If you are upgrading the legacy Agent for Windows to AgentFS, uninstall the legacy Agent for Windows after doing so.

- **Agent for OES Linux:** Agent for scanning OES storage devices.

1.5.2 Content Agent

File Reporter currently includes a single Content Agent:

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

If you plan to utilize file content scanning, and if you are upgrading from a version of File Reporter other than 3.5, you will need to install Content Agents as part of the upgrade process. For more information, see Section 2.5, “Determine Whether to Scan File Content,” on page 16.

1.5.3 Upgrading Agents

To upgrade the legacy Agent for Windows, install the legacy Agent for Windows on top of the existing legacy Agent for Windows software. For procedures, see Chapter 10, “Installing and Configuring the Legacy Agent for Windows,” on page 101.

To upgrade the legacy Agent for Windows with AgentFS, install the AgentFS software on top of the existing legacy Agent for Windows software. For procedures, see Chapter 11, “Installing and Configuring Windows AgentFS,” on page 107.

To upgrade the Agent for OES Linux, install the Agent for OES Linux on top of the Agent for OES Linux software. For procedures, see Chapter 12, “Installing and Configuring the Agent for OES Linux,” on page 113.

2 Deployment Planning

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

- Section 2.1, "Understand the Technologies and Expertise You Need," on page 13
- Section 2.2, "Determine the Scope and Choose a Primary Identity System," on page 14
- Section 2.3, "Decide Where to Host the Engine," on page 15
- Section 2.4, "Decide Which Database to Utilize," on page 15
- Section 2.5, "Determine Whether to Scan File Content," on page 16
- Section 2.6, "Develop a Plan for Deploying the Agents for File System Scanning," on page 16
- Section 2.7, "Database Deployment Recommendations," on page 17

2.1 Understand the Technologies and Expertise You Need

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

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

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

2.2 Determine the Scope and Choose a Primary Identity System

You need to decide the scope of your installation and decide whether you will use eDirectory or Active Directory as your primary identity system.

The primary identity system is used by File Reporter for licensing, administrative authentication, and authorization. It is also the source for user email address information used by the notification subsystem.

NOTE: File content scanning and reporting is available only in environments where Active Directory is configured as an identity system.

Scope	Primary Identity System
Single eDirectory tree	The given eDirectory tree
Multiple eDirectory trees	Choose one of the eDirectory trees
Single Active Directory forest	The given AD forest
Single Active Directory forest and single eDirectory tree	Pick one: ◆ The given AD forest ◆ The given eDirectory tree Note: Changing primary identity systems is non-trivial.

Scope	Primary Identity System
Single Active Directory forest and multiple eDirectory trees	Pick one: - The given AD forest - One of the eDirectory trees Note: Changing the primary identity system between eDirectory and Active Directory is non-trivial.

2.3 Decide Where to Host the Engine

- The Engine server host should have significant CPU, disk, and memory for all but the smallest installations.
- The Engine runs on any of the following Windows Servers:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2

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.

Scope	Engine Host Server Configuration Requirement
eDirectory only	Client for Open Enterprise Server Installed
Active Directory only	Joined to the domain
Both eDirectory and Active Directory	Both: - Client for Open Enterprise Server installed - Joined to the domain

2.4 Decide Which Database to Utilize

IMPORTANT: Database deployment recommendations are detailed in Section 2.7, "Database Deployment Recommendations," on page 17.

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, Business Intelligence, and Enterprise versions of SQL Server.
- You might prefer to utilize the PostgreSQL database if you are proficient with Linux.

2.5 Determine Whether to Scan File Content

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

File Content scanning can only be conducted on files stored on Windows network storage devices and requires that Active Directory be configured as one of the identity systems.

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

- RabbitMQ messaging broker
- ManagerFC
- AgentFC

For more details on File Content Scanning, see Content Scanning and Reporting in the *Micro Focus File Reporter 3.6 Administration Guide*.

2.6 Develop a Plan for Deploying the Agents for File System Scanning

Target File System to be Scanned	Agent can be Installed Locally?	Potential Proxy Agents
Windows	Yes	Any of the following: ◆ AgentFS ◆ Legacy Agent for Windows
Open Enterprise Server	Yes	Any of the following: ◆ Agent for OES Linux ◆ Legacy Agent for Windows
Network Attached Storage (NAS) Device (CIFS-based)	No	Any of the following: ◆ AgentFS ◆ Legacy Agent for Windows

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

- Locally installed Agents perform scans faster than proxy-based agents.
- Locally installed Agents share CPU and memory resources with other software running on the system. If a server is already constrained for resources, consider using a proxy instead of installing the Agent locally. For procedures, see “Micro Focus File Reporter 3.6 Administration Guide.”

2.7 Database Deployment Recommendations

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

- Section 2.7.1, “Use a Dedicated Server,” on page 17
- Section 2.7.2, “Use a Dedicated Database Instance,” on page 17
- Section 2.7.3, “Provide Sufficient I/O Bandwidth,” on page 17

2.7.1 Use a Dedicated Server

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

- For minimum requirements for PostgreSQL, see Section 4.1.1, “Minimum Requirements,” on page 21.
- For minimum requirements for a SQL Server host, see Section 5.1, “Minimum Requirements,” on page 23.

2.7.2 Use a Dedicated Database Instance

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

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

2.7.3 Provide Sufficient I/O Bandwidth

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

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

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

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

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

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

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

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

3 Licensing the Product

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

For procedures on replacing a license file, see Appendix B, “Replace a License File,” on page 127.

- Section 3.1, “Obtaining a Product Activation Key,” on page 19
- Section 3.2, “Obtaining a License File,” on page 19

3.1 Obtaining a Product Activation Key

1. In a Web browsers, 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.

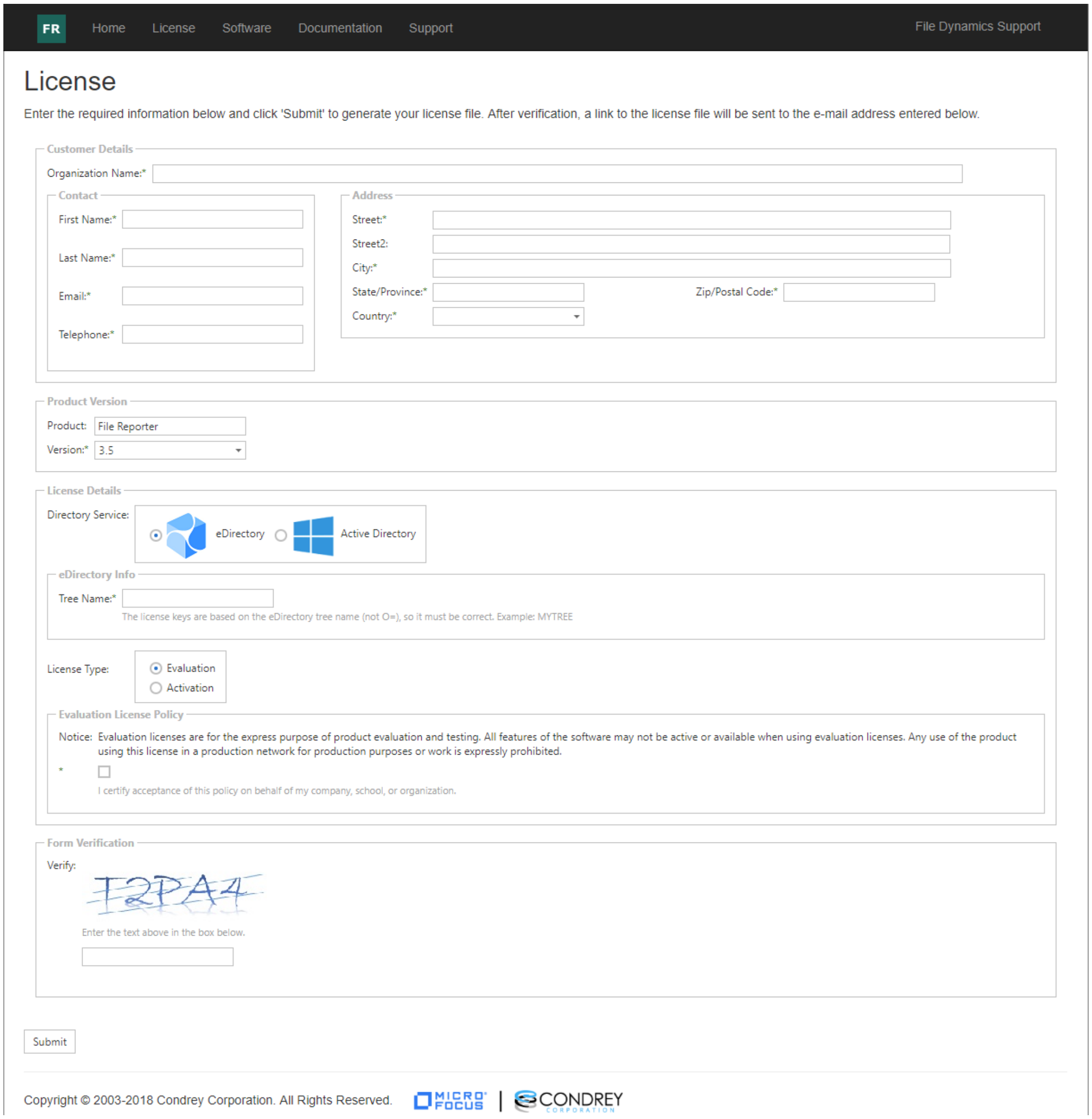
   You will be required to paste the activation key into a form to obtain a production license.

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.



License

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

Customer Details

Organization Name:*

Contact

First Name:*

Last Name:*

Email:*

Telephone:*

Address

Street:*

Street2:

City:*

State/Province:*

Zip/Postal Code:*

Country:*

Product Version

Product: File Reporter

Version:* 3.5

License Details

Directory Service: ● eDirectory ○ Active Directory

eDirectory Info

Tree Name:*

The license keys are based on the eDirectory tree name (not O=), so it must be correct. Example: MYTREE

License Type: ● Evaluation ○ Activation

Evaluation License Policy

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

* □

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

Form Verification

Verify:

T2PA4

Enter the text above in the box below.

Submit

Copyright © 2003-2018 Condrey Corporation. All Rights Reserved.

3 Complete the fields.

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

4 Click **Submit**.

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

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

A new Access Web page is opened.

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

7 Note where the license file is saved.

You need the license file to complete Engine setup wizard.

4 Installing and Configuring the PostgreSQL Database

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

4.1 Installing and Configuring the PostgreSQL Database on a Linux Server

- Section 4.1.1, "Minimum Requirements," on page 21
- Section 4.1.2, "Installing and Configuring the PostgreSQL Database," on page 21

4.1.1 Minimum Requirements

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

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

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

  These major Linux distributions include PostgreSQL in their repositories.

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

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

- Minimum of 16 GB of RAM

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

- Minimum of 100 GB of disk space

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

4.1.2 Installing and Configuring the PostgreSQL Database

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

- https://www.postgresql.org/docs/current/static/creating-cluster.html

- https://www.postgresql.org/docs/current/static/runtime.html
- https://www.postgresql.org/docs/current/static/runtime-config.html

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

5 Installing an SQL Server Instance that Supports File Reporter

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

- Section 5.1, “Minimum Requirements,” on page 23
- Section 5.2, “Prerequisites,” on page 23
- Section 5.3, “Install a New Instance of SQL Server,” on page 24
- Section 5.4, “Post Configuration Considerations,” on page 29

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

5.1 Minimum Requirements

File Reporter supports the Standard, Business Intelligence, and Enterprise versions of SQL Server. It does not support the Express version.

Microsoft SQL Server Software

- SQL Server 2017 (Windows or Linux)
- SQL Server 2016 SP1
- SQL Server 2014 SP2 - 64 bit

NOTE: SQL Server 2012 SP4 will work, but is considered deprecated. If you are upgrading from a previous version of File Reporter, you can do so with an SQL Server 2012 with a warning. New installations of File Reporter should use a supported version of SQL Server listed above.

Server Host

- Any Microsoft supported version of SQL Server running on a 64-bit multi-core processor machine
- Minimum 16 GB RAM

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

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

5.2 Prerequisites

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

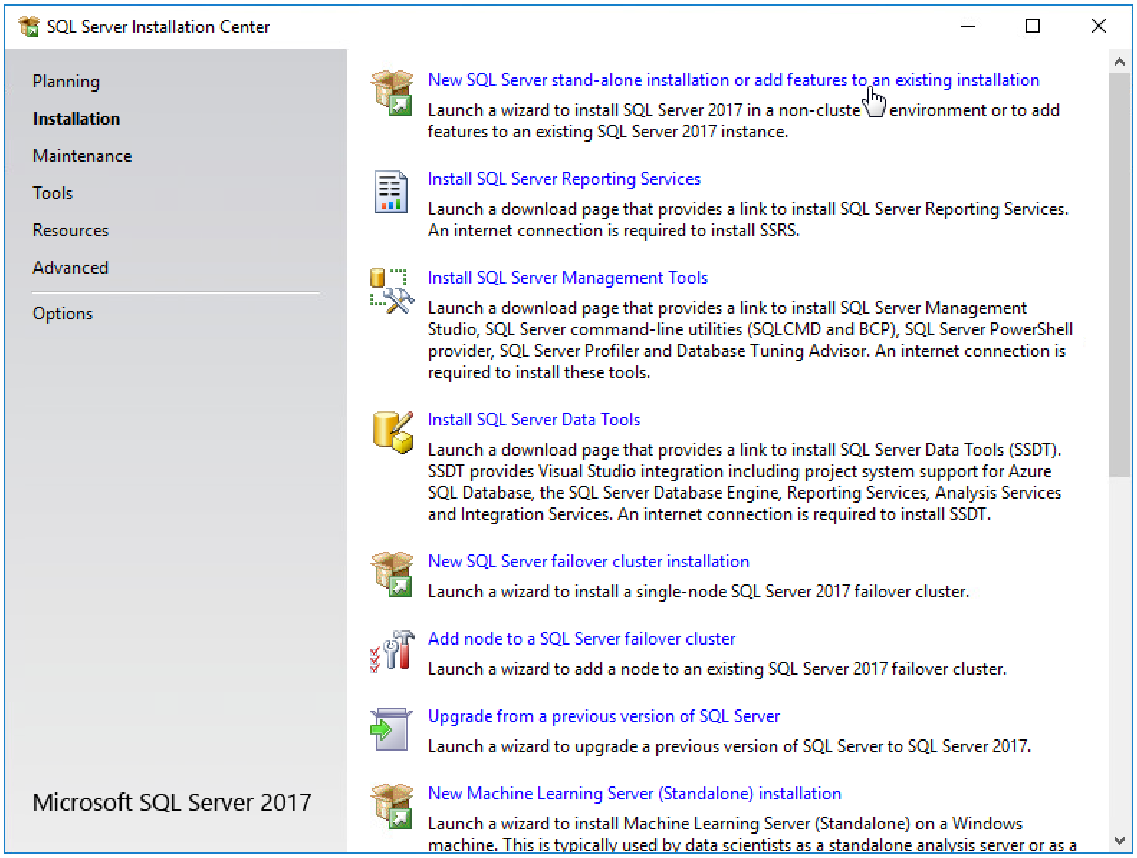
5.3 Install a New Instance of SQL Server

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

1 From the Microsoft SQL Server ISO, double-click `setup.exe`.

2 On the SQL Server Installation Center page, click **Installation**.

3 Select **New SQL Server stand-alone installation or add features to an existing installation**.



New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2017 in a non-cluste environment or to add features to an existing SQL Server 2017 instance.

Install SQL Server Reporting Services
Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools
Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2017 failover cluster.

Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2017 failover cluster.

Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2017.

New Machine Learning Server (Standalone) installation
Launch a wizard to install Machine Learning Server (Standalone) on a Windows machine. This is typically used by data scientists as a standalone analysis server or as a

The Setup Support Rules operation is run.

4 When the operation has completed, click **OK**.

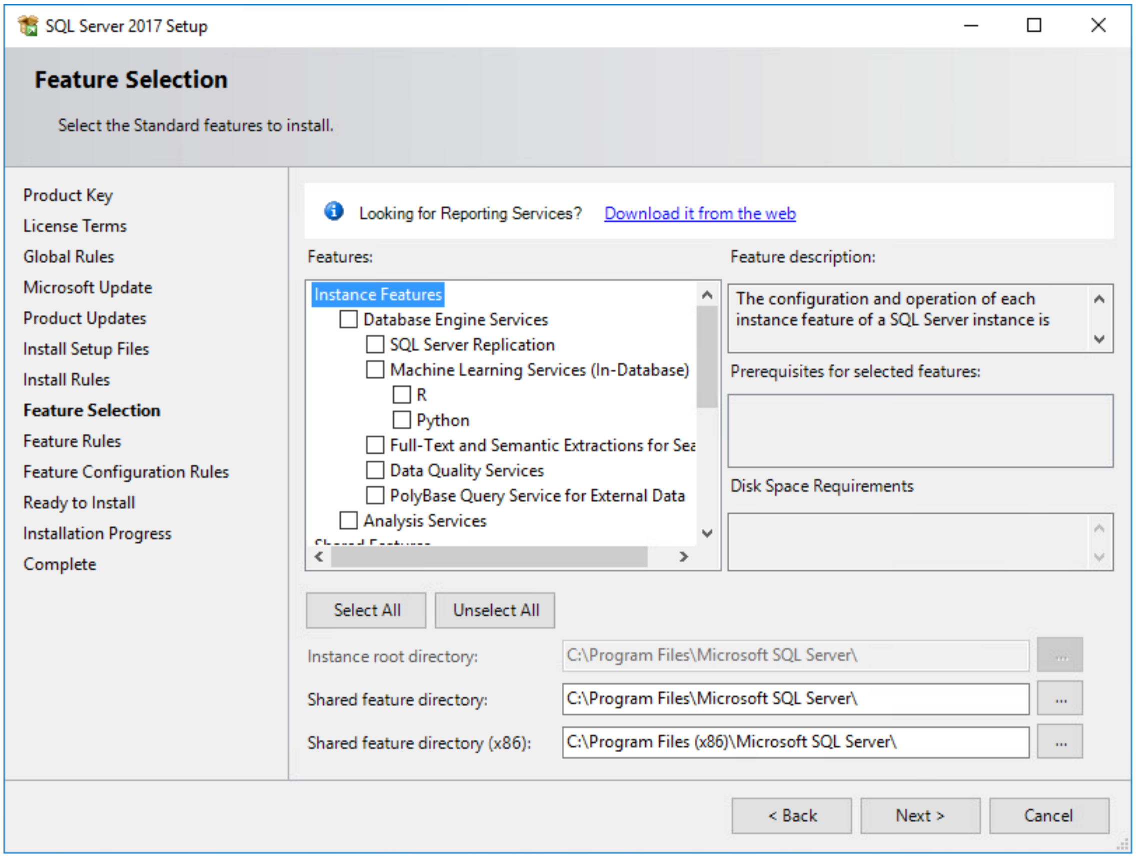
5 When prompted, enter your product key, then click **Next**.

6 Accept the license terms, then click **Next**.

7 Include all Microsoft SQL Server product updates, then click **Next**.

The Setup Support Rules operation is run again.

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



Feature Selection

Select the Standard features to install.

Looking for Reporting Services? Download it from the web

Features:

Instance Features
- □ Database Engine Services
  - □ SQL Server Replication
  - □ Machine Learning Services (In-Database)
    - □ R
    - □ Python
  - □ Full-Text and Semantic Extractions for Sea
  - □ Data Quality Services
  - □ PolyBase Query Service for External Data
- □ Analysis Services

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is

Prerequisites for selected features:

Disk Space Requirements

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

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

10 In the **Instance root directory**, **Shared feature directory**, and **Shared feature directory (x86)** fields, specify the path where you want to SQL instance to reside, then click **Next**.

11 In the Instance Configuration page, click the **Named instance** option and specify a descriptive name for the instance such as `SRSDB` and click **Next**.

12 On the Server Configuration page, click the **Collation** tab.

13 Click **Customize**.

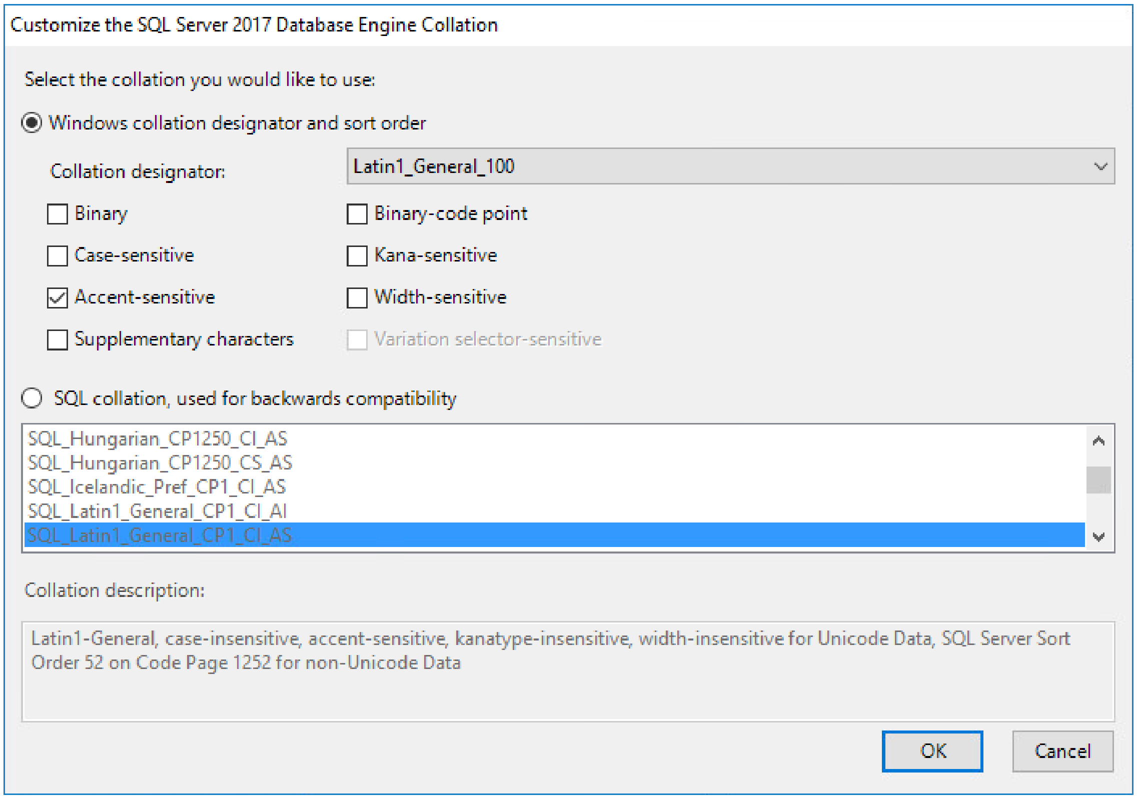
14 Click the **Windows collation designator and sort order** option.

15 From the **Collation designator** drop-down menu, select an acceptable collation and settings for your locale.

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

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

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



Customize the SQL Server 2017 Database Engine Collation

Select the collation you would like to use:

● Windows collation designator and sort order

Collation designator: Latin1_General_100

□ Binary
□ Binary-code point
□ Case-sensitive
□ Kana-sensitive
☑ Accent-sensitive
□ Width-sensitive
□ Supplementary characters
□ Variation selector-sensitive

○ SQL collation, used for backwards compatibility

SQL_Hungarian_CP1250_CI_AS
SQL_Hungarian_CP1250_CS_AS
SQL_Icelandic_Pref_CP1_CI_AS
SQL_Latin1_General_CP1_CI_AI
SQL_Latin1_General_CP1_CI_AS

Collation description:

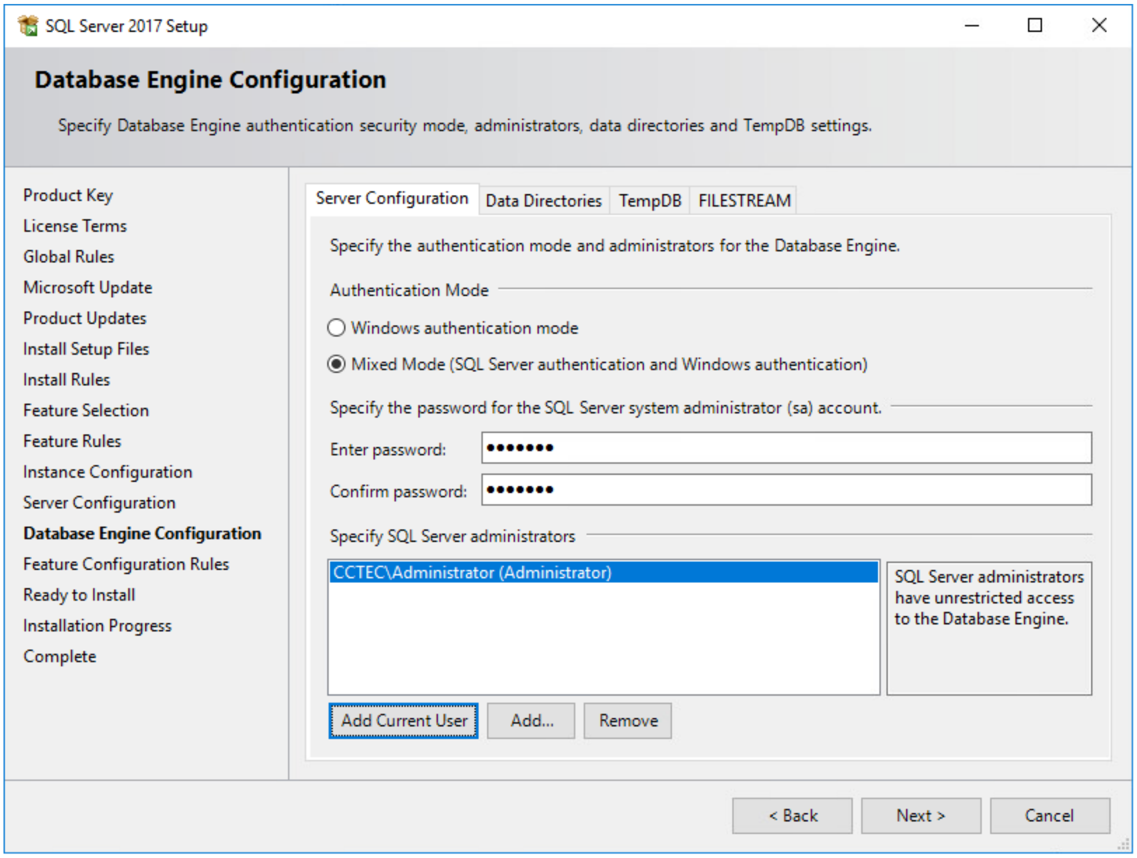
Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data

16 Click **OK**.

17 Click **Next**.

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

19 Click **Next**.



SQL Server 2017 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: •••••••

Confirm password: •••••••

Specify SQL Server administrators

CCTEC\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

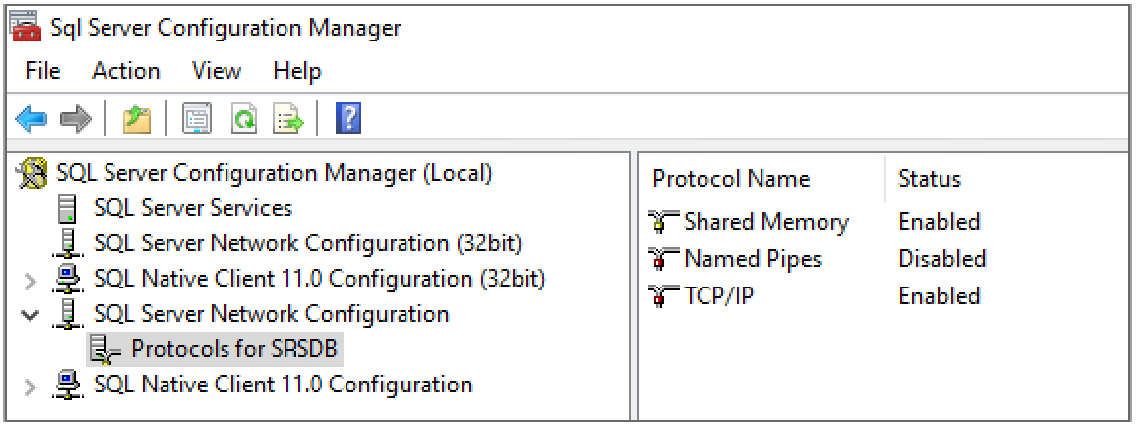
20 Click **Install**.

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).



Sql Server Configuration Manager

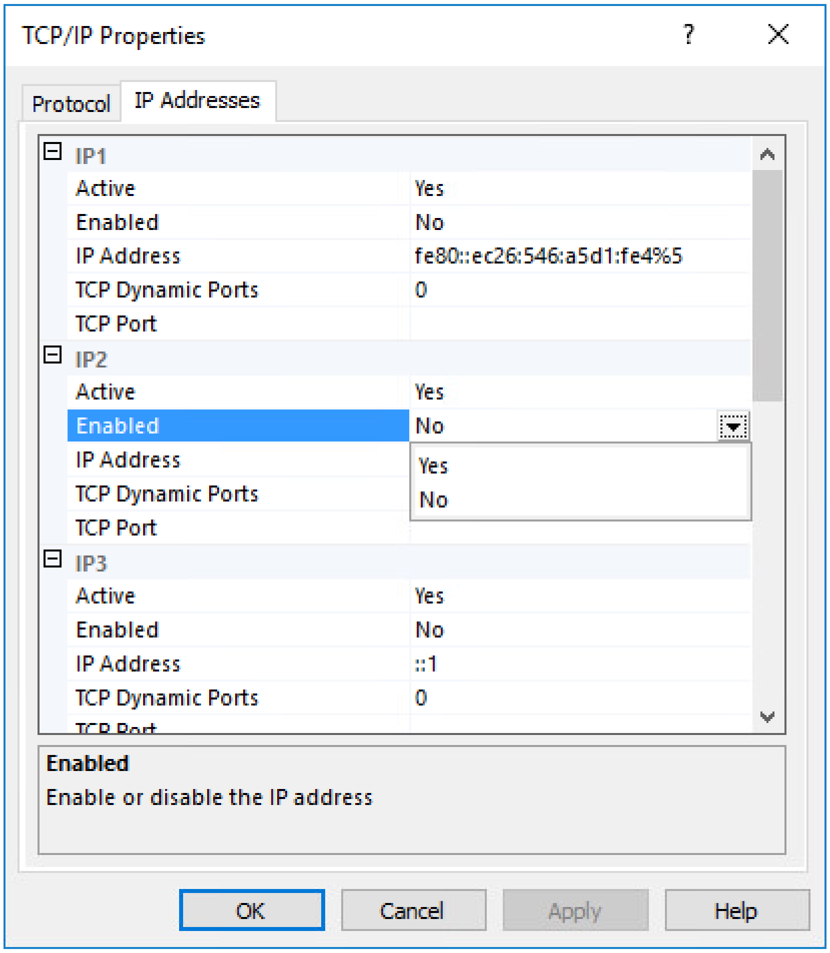
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for SRSDB
SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

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

26 Click the **IP Addresses** tab.

27 Under the **IP2** heading, for the **Enabled** field, right-click to select the drop-down men and change the setting to **Yes**.



IP1	
Active	Yes
Enabled	No
IP Address	fe80::ec26:546:a5d1:fe4%5
TCP Dynamic Ports	0
TCP Port	
IP2	
Active	Yes
Enabled	No
IP Address	
TCP Dynamic Ports	
TCP Port	
IP3	
Active	Yes
Enabled	No
IP Address	::1
TCP Dynamic Ports	0
TCP Port	

Enabled

Enable or disable the IP address

28 Select **TCP Dynamic Ports** and clear the field so there is no number associated to it.

29 Scroll down to the **IPALL** heading and for the **TCP Dynamic Ports** field, clear the field so there is no number associated to it.

30 In the **TCP Port** field, and enter `1433`.

31 Click **Apply**.

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

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

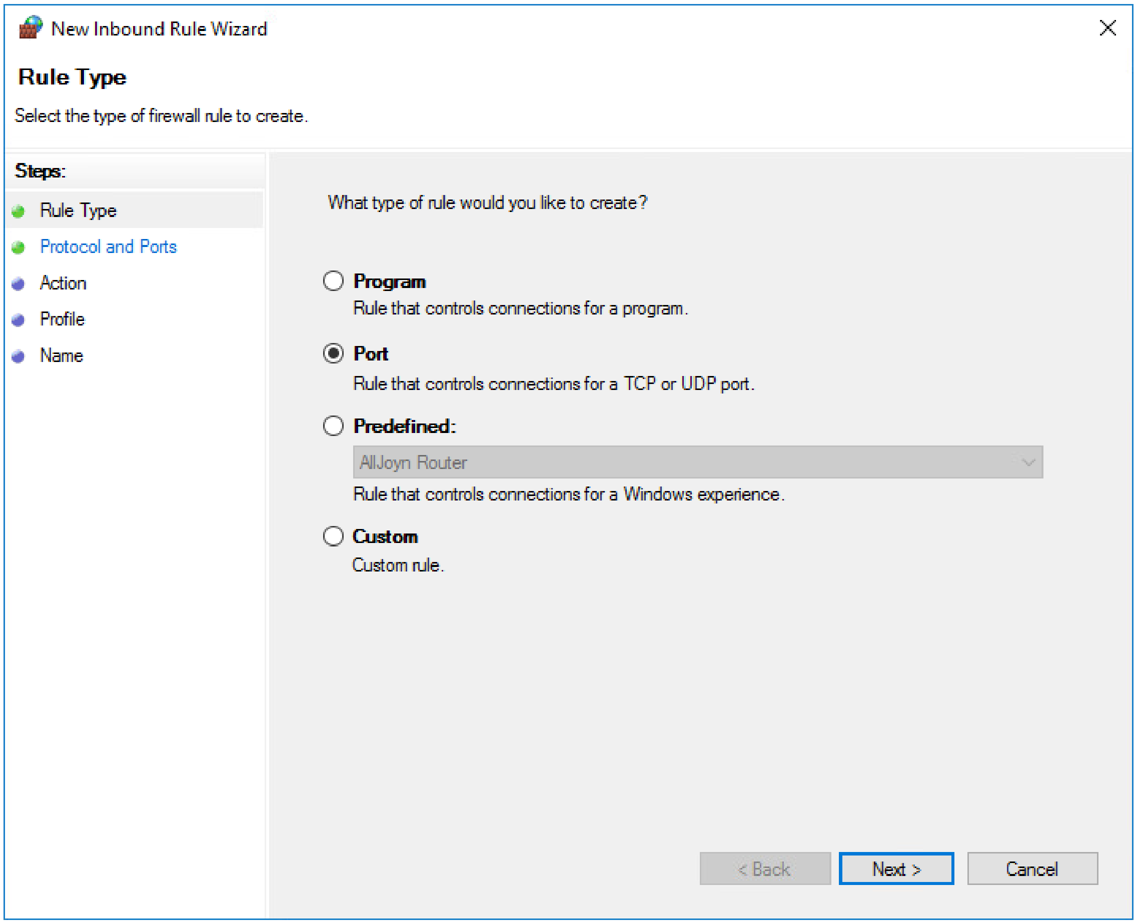
34 Close the SQL Server Configuration Manager.

35 Launch Windows Firewall with Advanced Security.

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

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

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



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

39 Click **Next**.

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

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

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

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

For example `SQL Server`.

44 Click **Finish**.

5.4 Post Configuration Considerations

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

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

6 Installing and Configuring RabbitMQ

RabbitMQ is an open source message broker that enables messaging between File Reporter components that are needed for file content scanning. These components include ManagerFC and AgentFC. If you will not be performing file content scanning, you do not need to install RabbitMQ.

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

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

NOTE: File Content scanning can only be conducted on files stored on Windows network storage devices and requires that Active Directory be configured as one of the identity systems.

6.1 Extracting RabbitMQ

1. (Conditional) Install the Visual C++ Redistributable Packages for Visual Studio 2013.

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

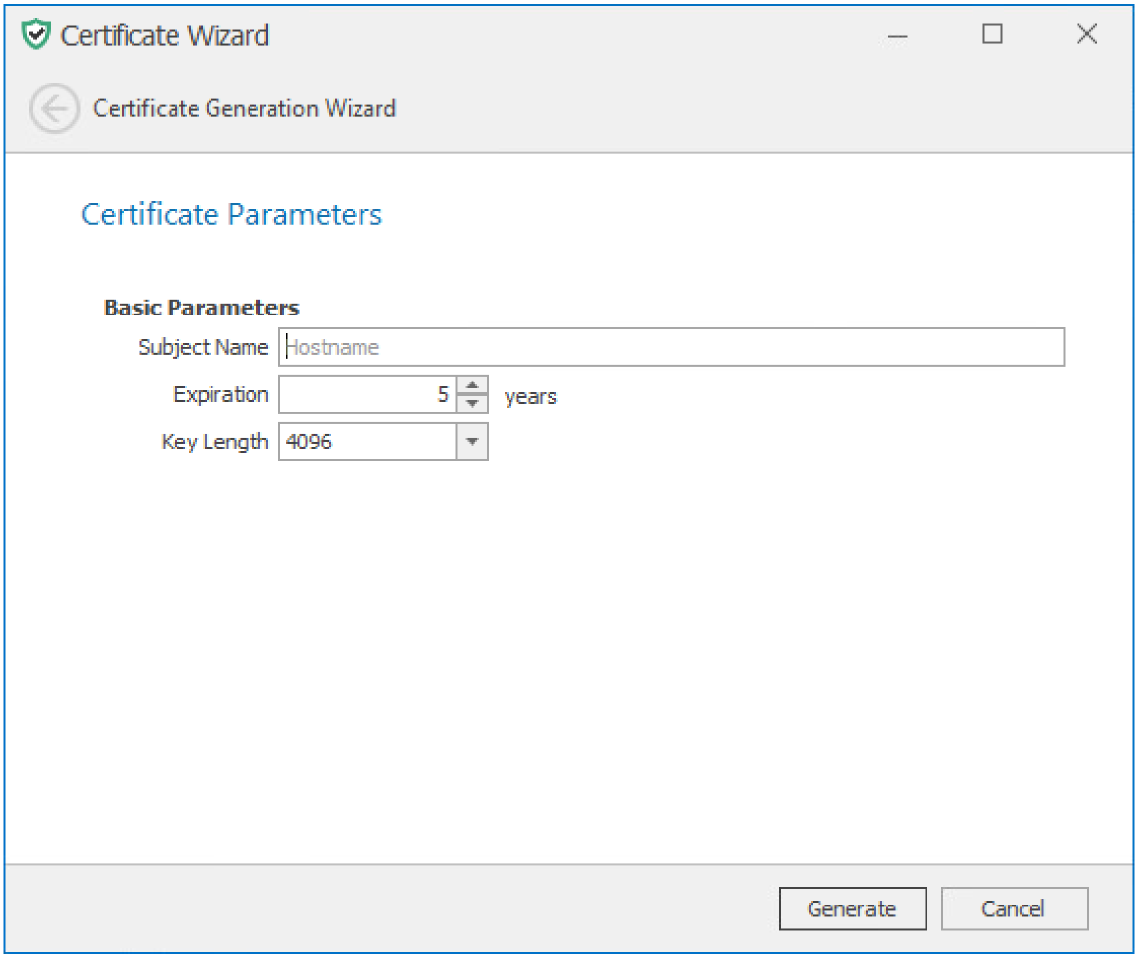
   If this package is not currently installed, it may be found at: https://www.microsoft.com/en-us/download/details.aspx?id=40784.

2. At the root of the `FileReporter_3.6.0.iso` image, unzip the `RabbitMQ-3.7.`*`x`*`.zip` file to the root of a drive.
3. Proceed with Section 6.2, “Creating Certificates for RabbitMQ,” on page 31.

6.2 Creating Certificates for RabbitMQ

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

1. At the root of the `FileReporter_3.6.0.iso` image, double-click `CertificateGenerator.exe`.



Certificate Wizard

Certificate Generation Wizard

Certificate Parameters

Basic Parameters

Subject Name: Hostname

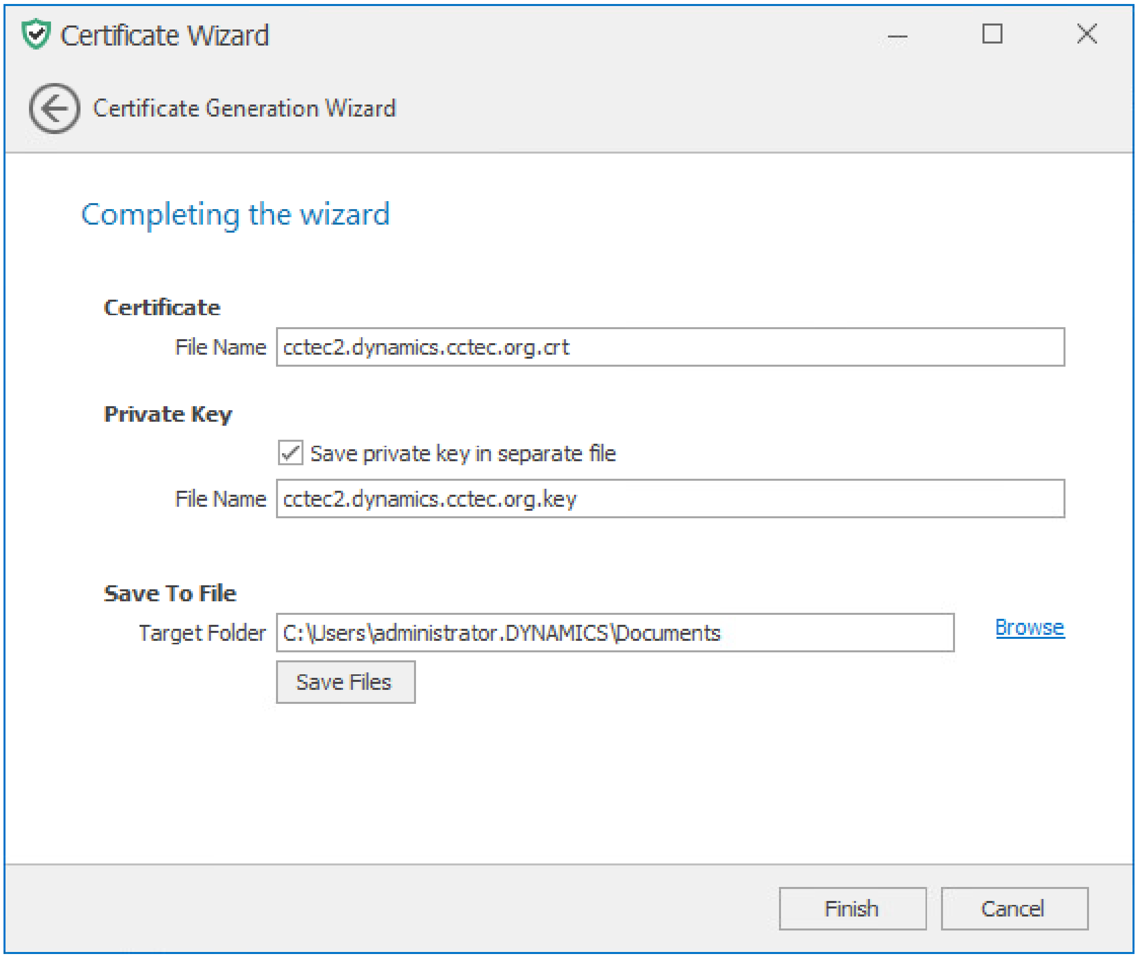
Expiration: 5 years

Key Length: 4096

2 In the **Subject Name** field, enter the DNS or IP address for the RabbitMQ service.

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

4 Click **Generate**.



Certificate Wizard

Certificate Generation Wizard

Completing the wizard

Certificate

File Name cctec2.dynamics.cctec.org.crt

Private Key

☑ Save private key in separate file

File Name cctec2.dynamics.cctec.org.key

Save To File

Target Folder C:\Users\administrator.DYNAMICS\Documents

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

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

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

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

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

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

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

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

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

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

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

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

7 Click **Finish**.

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

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

For example, copy them to the `RabbitMQ` folder that is created when you extract the `rabbitmq.zip` file.

9 From the command line, stop the RabbitMQ service by typing: `sc stop rabbitmq`

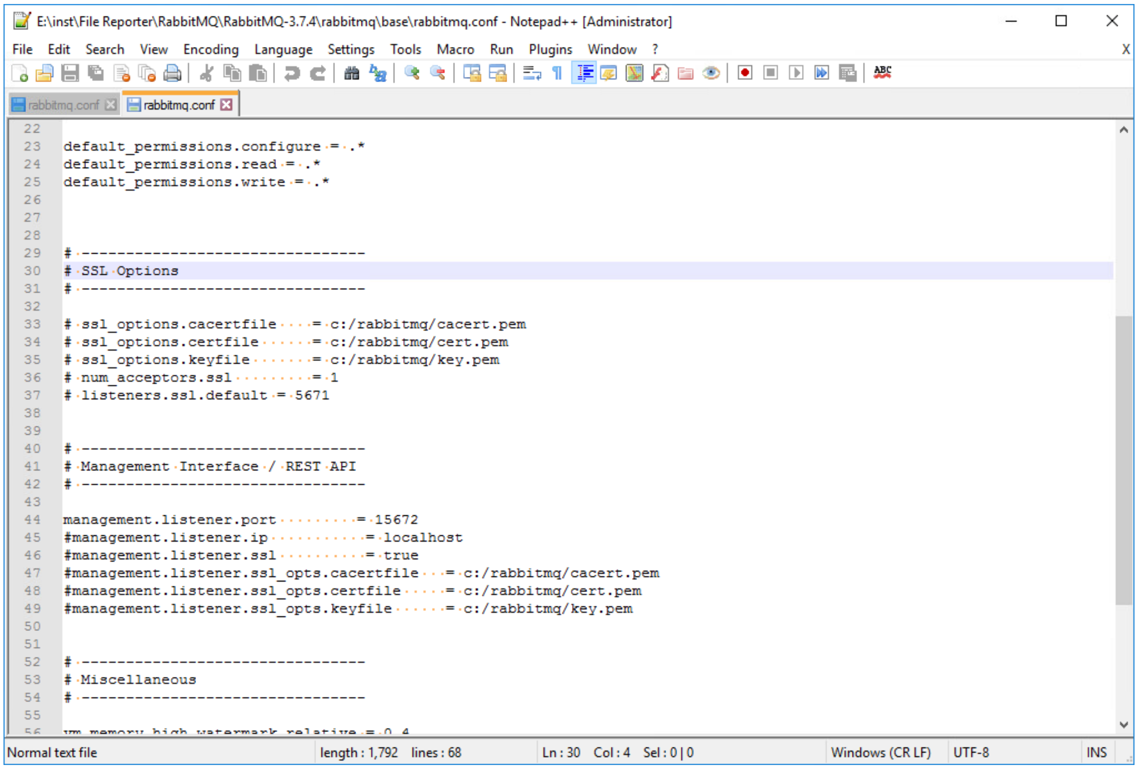
10 Edit the `rabbitmq.conf` file located in the `rabbitmq\base` folder where RabbitMQ was extracted (if using the provided archive).

11 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
```



E:\inst\File Reporter\RabbitMQ\RabbitMQ-3.7.4\rabbitmq\base\rabbitmq.conf - Notepad++ [Administrator]

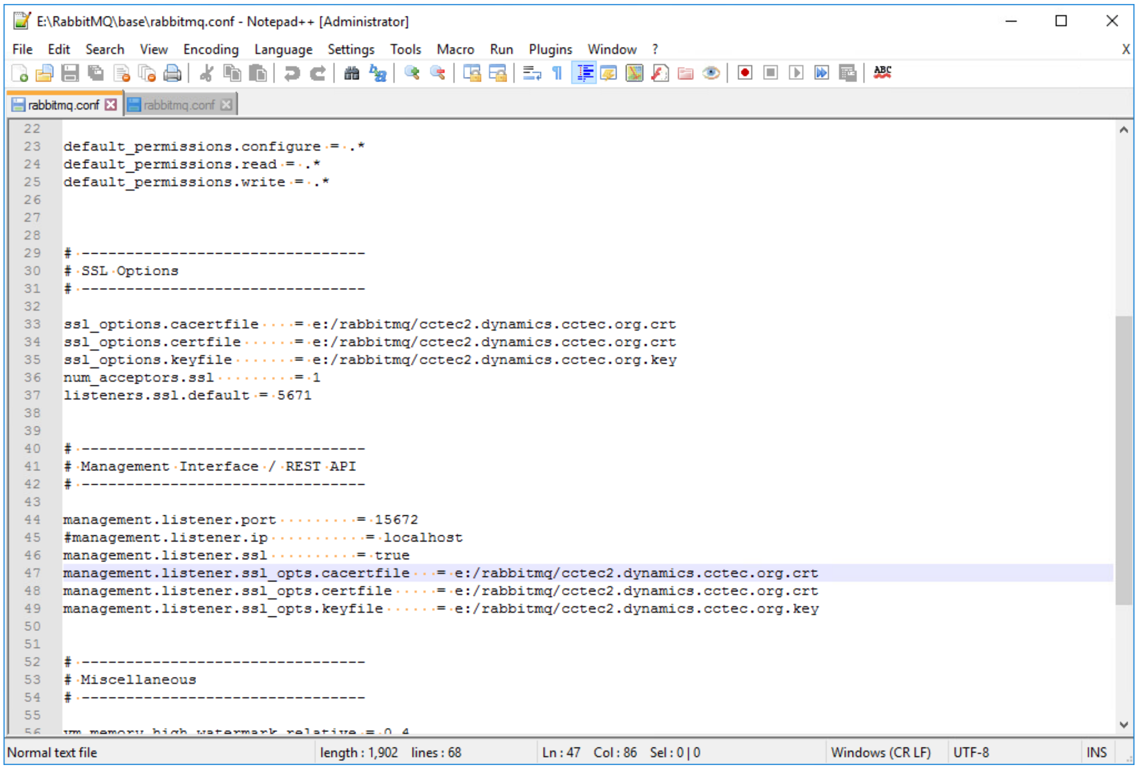
```

default_permissions.configure = .*
default_permissions.read = .*
default_permissions.write = .*



# ---------------------------------
# SSL Options
# ---------------------------------

# ssl_options.cacertfile    = c:/rabbitmq/cacert.pem
# ssl_options.certfile      = c:/rabbitmq/cert.pem
# ssl_options.keyfile       = c:/rabbitmq/key.pem
# num_acceptors.ssl         = 1
# listeners.ssl.default = 5671


# ---------------------------------
# Management Interface / REST API
# ---------------------------------

management.listener.port         = 15672
#management.listener.ip           = localhost
#management.listener.ssl          = true
#management.listener.ssl_opts.cacertfile   = c:/rabbitmq/cacert.pem
#management.listener.ssl_opts.certfile     = c:/rabbitmq/cert.pem
#management.listener.ssl_opts.keyfile      = c:/rabbitmq/key.pem


# ---------------------------------
# Miscellaneous
# ---------------------------------

vm_memory_high_watermark.relative = 0.4
```

12 Modify the entries for `management.*` interface.

Note that paths are absolute and use forward slashes.

Uncomment the following lines:

```
management.listener.port
management.listener.ssl
management.listener.ssl_opts.cacertfile
management.listener.ssl_opts.certfile
management.listener.ssl_opts.keyfile
```


E:\RabbitMQ\base\rabbitmq.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
rabbitmq.conf
rabbitmq.conf
Normal text file
length : 1,902 lines : 68
Ln : 47 Col : 86 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS

```

default_permissions.configure = .*
default_permissions.read = .*
default_permissions.write = .*



# --------------------------------
# SSL Options
# --------------------------------

ssl_options.cacertfile    = e:/rabbitmq/cctec2.dynamics.cctec.org.crt
ssl_options.certfile      = e:/rabbitmq/cctec2.dynamics.cctec.org.crt
ssl_options.keyfile       = e:/rabbitmq/cctec2.dynamics.cctec.org.key
num_acceptors.ssl         = 1
listeners.ssl.default = 5671


# --------------------------------
# Management Interface / REST API
# --------------------------------

management.listener.port         = 15672
#management.listener.ip           = localhost
management.listener.ssl          = true
management.listener.ssl_opts.cacertfile   = e:/rabbitmq/cctec2.dynamics.cctec.org.crt
management.listener.ssl_opts.certfile     = e:/rabbitmq/cctec2.dynamics.cctec.org.crt
management.listener.ssl_opts.keyfile      = e:/rabbitmq/cctec2.dynamics.cctec.org.key


# --------------------------------
# Miscellaneous
# --------------------------------

vm_memory_high_watermark.relative = 0.4
```

Note that all lines are uncommented except for `management.listener.ip`.

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

14 Close the editor.

15 From the command line, restart the RabbitMQ service by typing: `sc start rabbitmq`

16 From a Web browser, access the management interface for RabbitMQ by typing: `https://rabbitmq.`*`domain_name`*`:15672`

This port might need to be opened in the firewall.

17 Verify that the certificate is in use by the Web browser.

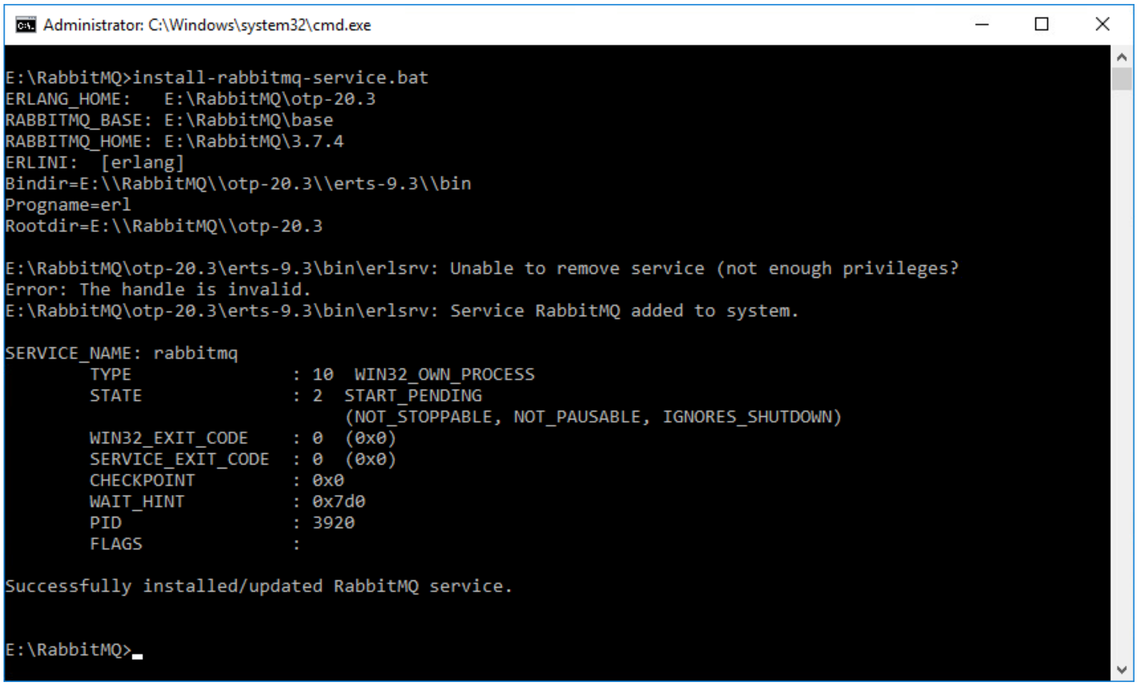
18 Proceed with Section 6.3, “Installing Rabbit MQ,” on page 35.

6.3 Installing Rabbit MQ

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

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

RabbitMQ is installed.



```
E:\RabbitMQ>install-rabbitmq-service.bat
ERLANG_HOME:   E:\RabbitMQ\otp-20.3
RABBITMQ_BASE: E:\RabbitMQ\base
RABBITMQ_HOME: E:\RabbitMQ\3.7.4
ERLINI:  [erlang]
Bindir=E:\\RabbitMQ\\otp-20.3\\erts-9.3\\bin
Progname=erl
Rootdir=E:\\RabbitMQ\\otp-20.3

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

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

Successfully installed/updated RabbitMQ service.


E:\RabbitMQ>_
```

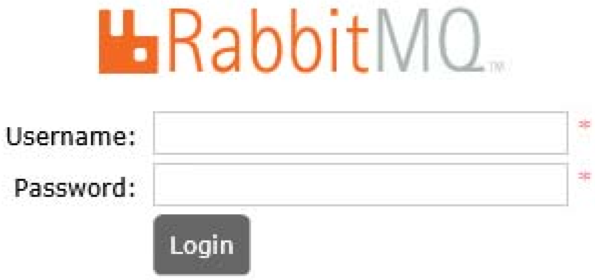
In the graphic above, the error: `The handle is invalid` is normal during an installation and can be ignored.

3 Proceed with Section 6.4, "Changing the Default Password," on page 36.

6.4 Changing the Default Password

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

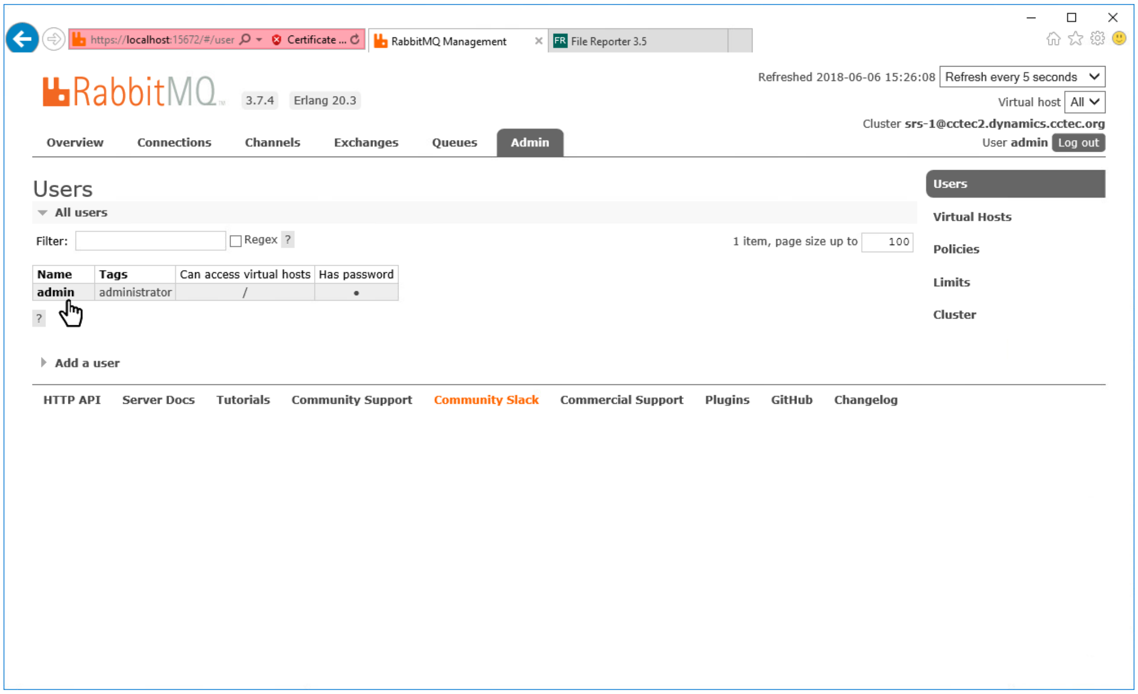
1 From a Web browser access the RabbitMQ management interface by typing: `https://`*`server`*`:15672` where *`server`* is the address of the server where RabbitMQ is installed.



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

3 Click the **Admin** tab.

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



Refreshed 2018-06-06 15:26:08 Refresh every 5 seconds

Virtual host All

Cluster srs-1@cctec2.dynamics.cctec.org

User admin

Users

All users

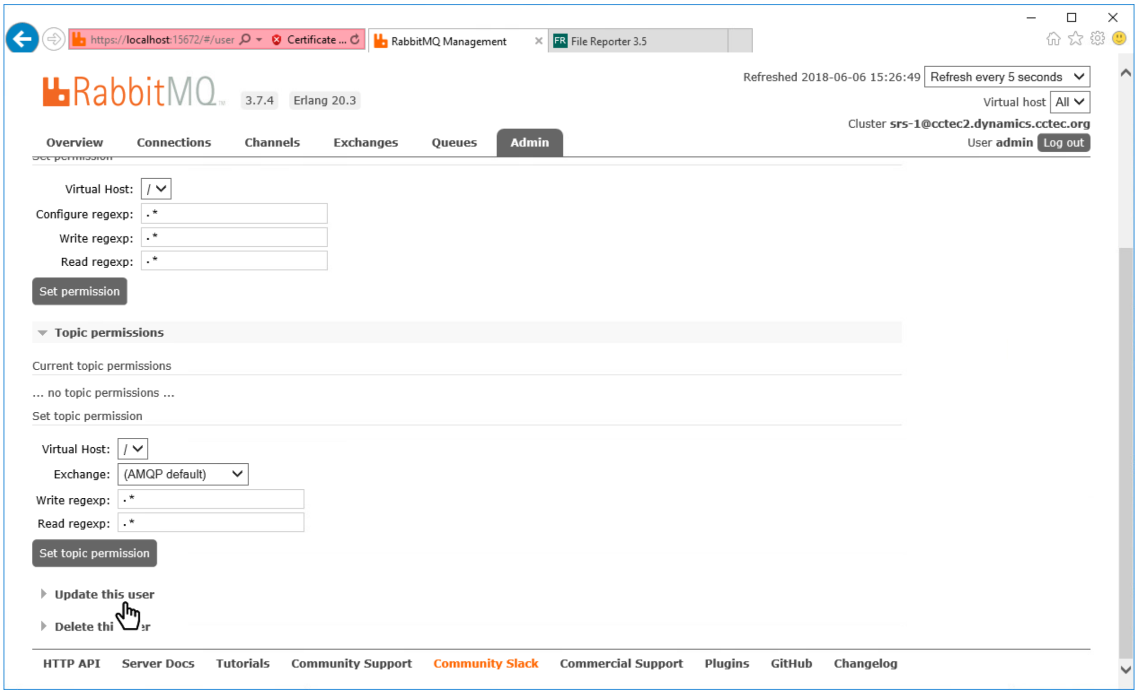
Filter: □ Regex

1 item, page size up to 100

Name	Tags	Can access virtual hosts	Has password
admin	administrator	/	•

Add a user

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



Refreshed 2018-06-06 15:26:49 Refresh every 5 seconds

Virtual host All

Cluster srs-1@cctec2.dynamics.cctec.org

User admin

Set permission

Virtual Host: /

Configure regexp: .*

Write regexp: .*

Read regexp: .*

Topic permissions

Current topic permissions

... no topic permissions ...

Set topic permission

Virtual Host: /

Exchange: (AMQP default)

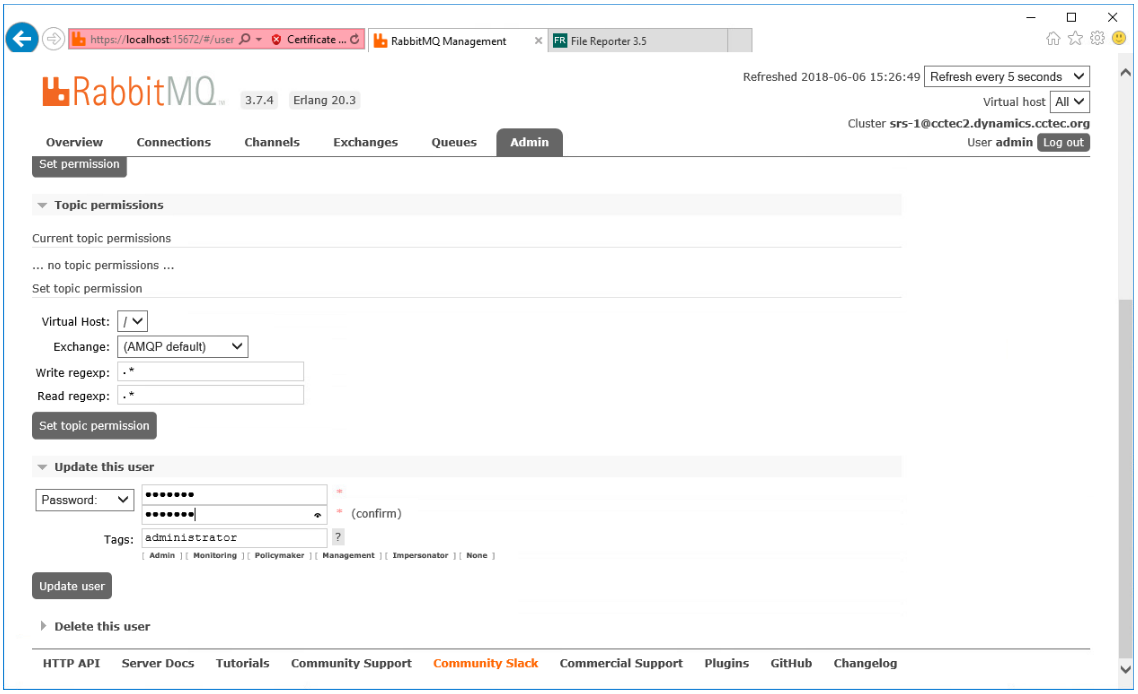
Write regexp: .*

Read regexp: .*

Update this user

Delete thi er

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



https://localhost:15672/#/user

Refreshed 2018-06-06 15:26:49

Refresh every 5 seconds

Virtual host: All

Cluster srs-1@cctec2.dynamics.cctec.org

User admin

Topic permissions

Current topic permissions

... no topic permissions ...

Set topic permission

Virtual Host: /

Exchange: (AMQP default)

Write regexp: .*

Read regexp: .*

Update this user

Password: ••••••• *

••••••• * (confirm)

Tags: administrator

[Admin] [Monitoring] [Policymaker] [Management] [Impersonator] [None]

Delete this user

7 Installing and Configuring the Engine, Database, and Web Application in an Active Directory Environment

Procedures in this section include those needed for installing and configuring the Engine, configuring the database, and configuring the Web Application in an Active Directory network environment.

This assumes that Active Directory is to be the primary identity system for File Reporter. In other words, authentication is to take place via Active Directory. Additionally, the Engine requires a license for the Active Directory version of File Reporter.

NOTE: Although Active Directory is the primary identity system, you can still have File Reporter scan and report on storage resources residing in eDirectory. See Section 7.2, “Prerequisites,” on page 40.

If not already installed, .NET 4.7.2 will be installed during the installation of the Engine.

7.1 Minimum Requirements

- Quad core 64-bit processor or better
- Minimum 16 GB RAM

  Depending on the size and frequency of your reports, you might need significantly more RAM.
- Minimum 20 GB free space for installation files and scan processing space
- Supported operating systems:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
- Directory Services requirements:
  - Requires either Microsoft Active Directory or NetIQ eDirectory
  - Active Directory requirements:
    - The server must be joined to Active Directory
    - Minimum forest functional level of Windows 2003

- eDirectory requirements:
  - Latest Client for Open Enterprise Server on the Engine server

7.2 Prerequisites

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

  For example: fr.cctec.org
- If you will be scanning for file content, you should first install the RabbitMQ messaging broker. For procedures, see Chapter 6, “Installing and Configuring RabbitMQ,” on page 31.

7.2.1 Prerequisites for Reporting on eDirectory Storage Resources

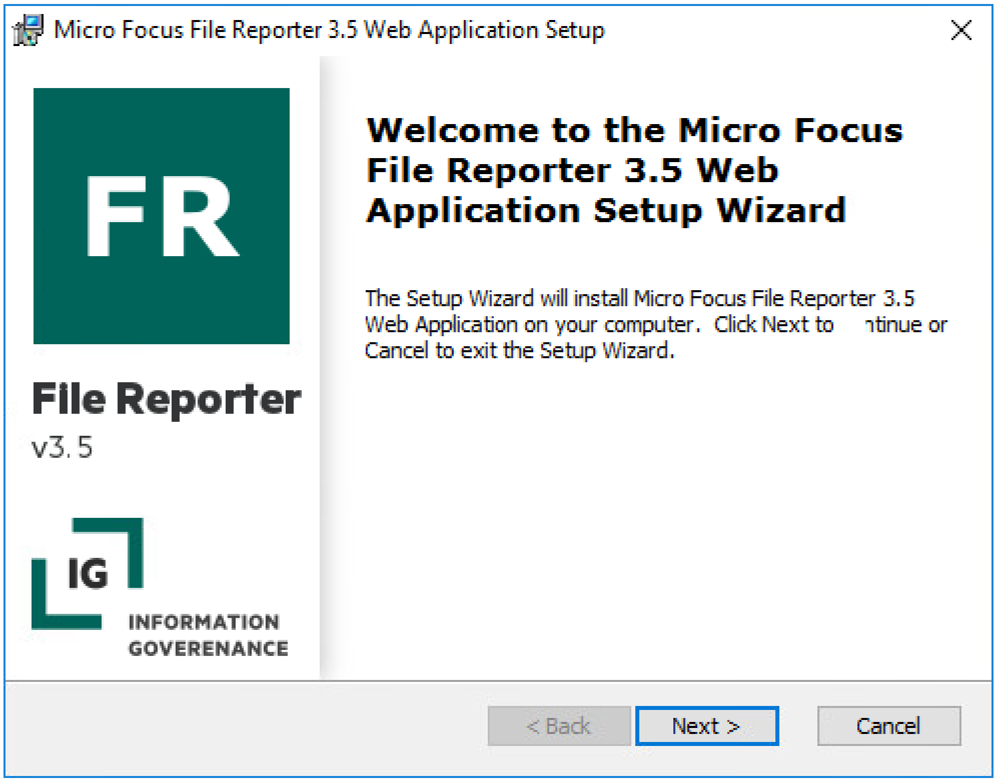
- If you want to report on storage resources that reside in an eDirectory network in addition to the Active Directory storage resources you report on, you must install the Client for Open Enterprise Server software on the same Windows server where you install the Engine:

  Having the Client for Open Enterprise Server installed allows File Reporter to connect to eDirectory and view the storage resources within.
- On the same Windows server, configure the Service Location Protocol settings within the Client for Open Enterprise Server software.
- Review Appendix A, “eDirectory Universal Password Settings,” on page 125 and complete any necessary prerequisite eDirectory Universal Password configurations.

7.3 Installing the Engine

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

1. At the root of the `FileReporter_3.6.0.iso` image, double-click `FileReporter-Engine-3.6.0-x64-`*`xx`*.
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**.


Micro Focus File Reporter 3.5 Web Application Setup

Welcome to the Micro Focus File Reporter 3.5 Web Application Setup Wizard

The Setup Wizard will install Micro Focus File Reporter 3.5 Web Application on your computer. Click Next to ntinue or Cancel to exit the Setup Wizard.

4 Click **Next**.

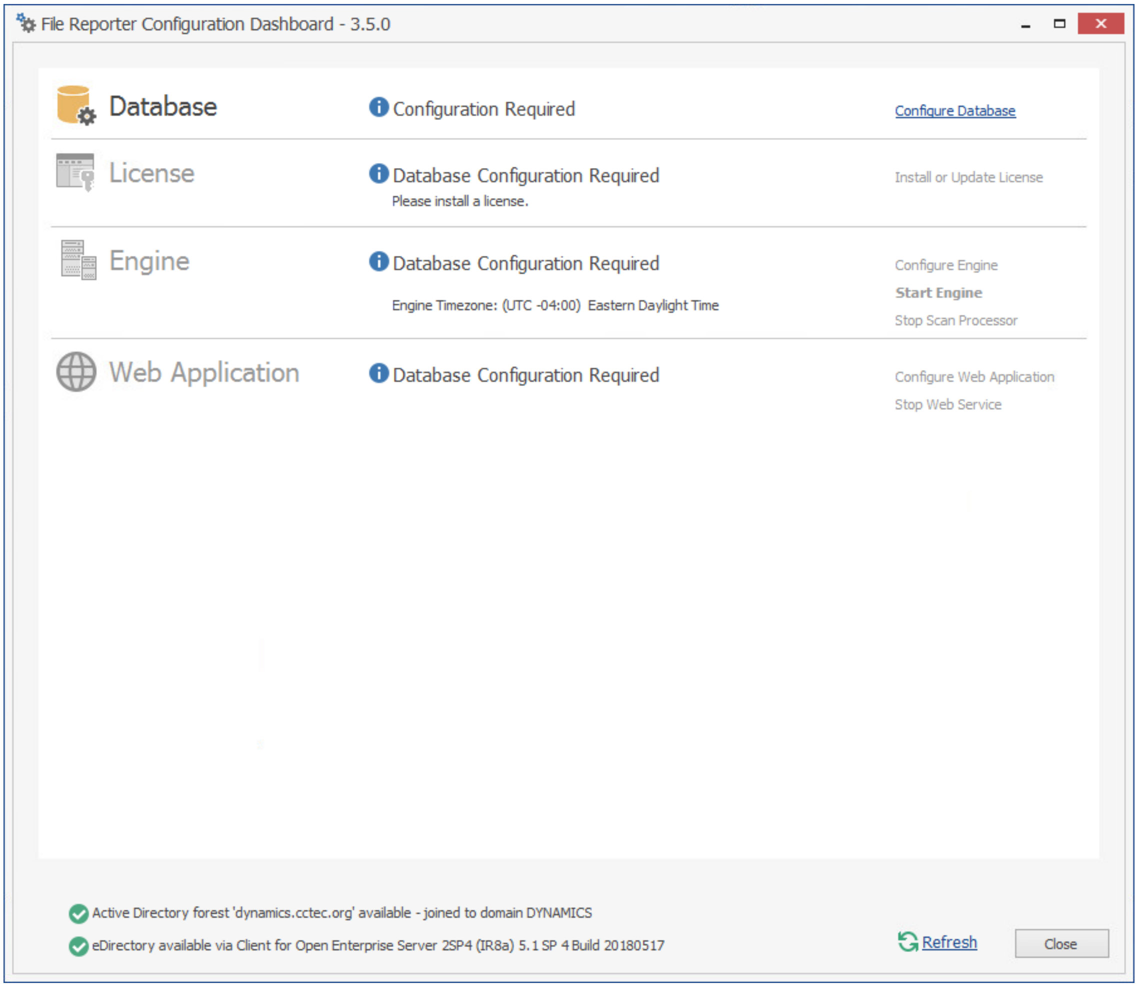
5 Accept the installation path or indicate a new path by using the **Browse** button. and click **Next**.

6 Click **Install**.

7 Click **Finish**.

8 Click **Run Config Utility.**

The File Reporter Configuration Dashboard appears.


File Reporter Configuration Dashboard - 3.5.0
Configure Database
Install or Update License
Configure Engine
Start Engine
Stop Scan Processor
Configure Web Application
Stop Web Service
Refresh
Close

Database — Configuration Required

License — Database Configuration Required
Please install a license.

Engine — Database Configuration Required
Engine Timezone: (UTC -04:00) Eastern Daylight Time

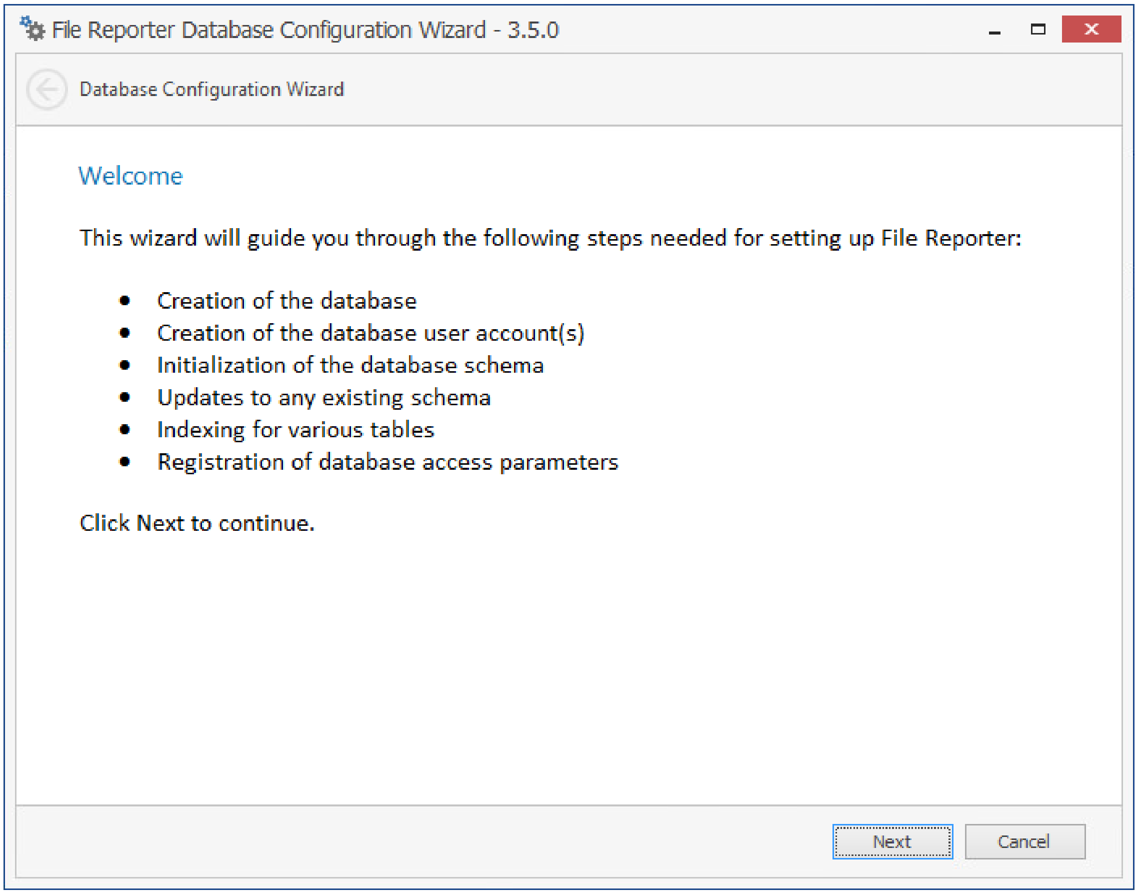
Web Application — Database Configuration Required

Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

7.4 Configuring the Database

1 Click **Configure Database**.


File Reporter Database Configuration Wizard - 3.5.0
Database Configuration Wizard

Welcome

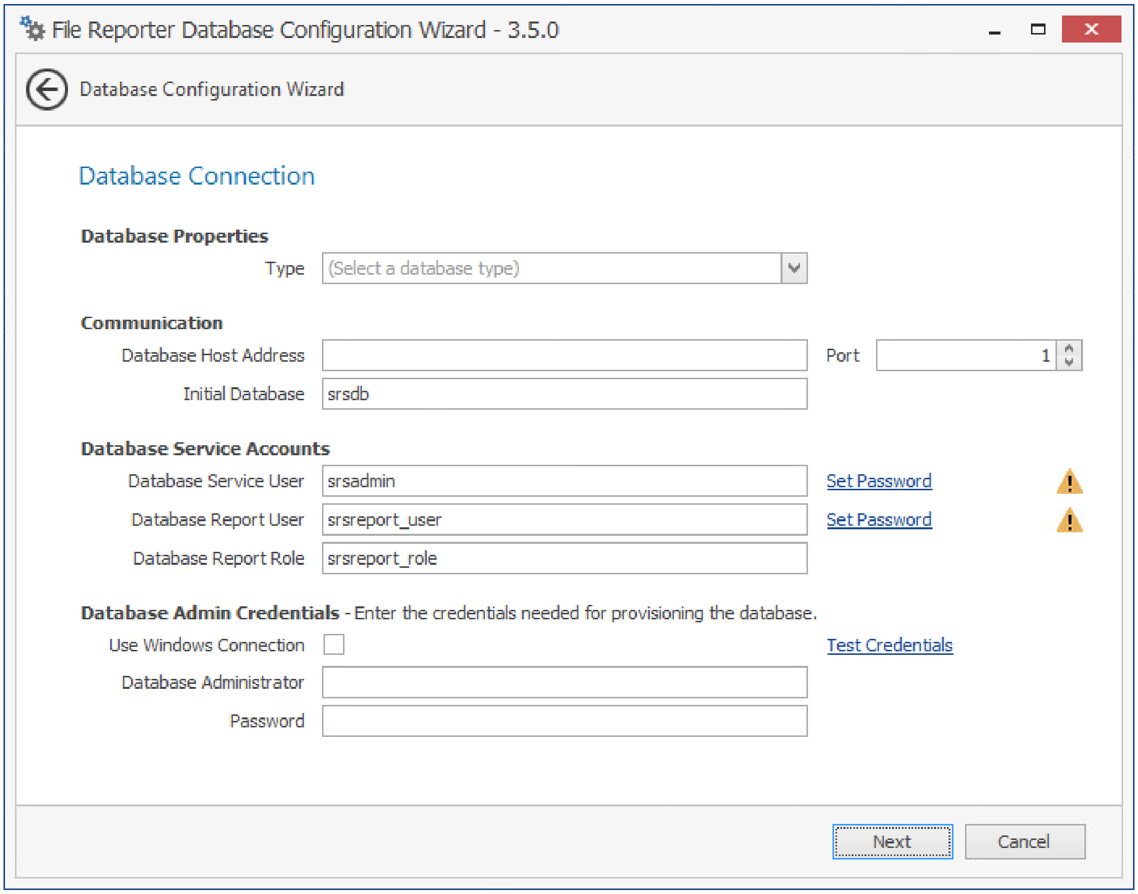
This wizard will guide you through the following steps needed for setting up File Reporter:

- Creation of the database
- Creation of the database user account(s)
- Initialization of the database schema
- Updates to any existing schema
- Indexing for various tables
- Registration of database access parameters

Click Next to continue.

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

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


File Reporter Database Configuration Wizard - 3.5.0
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:

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.

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

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

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

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

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

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

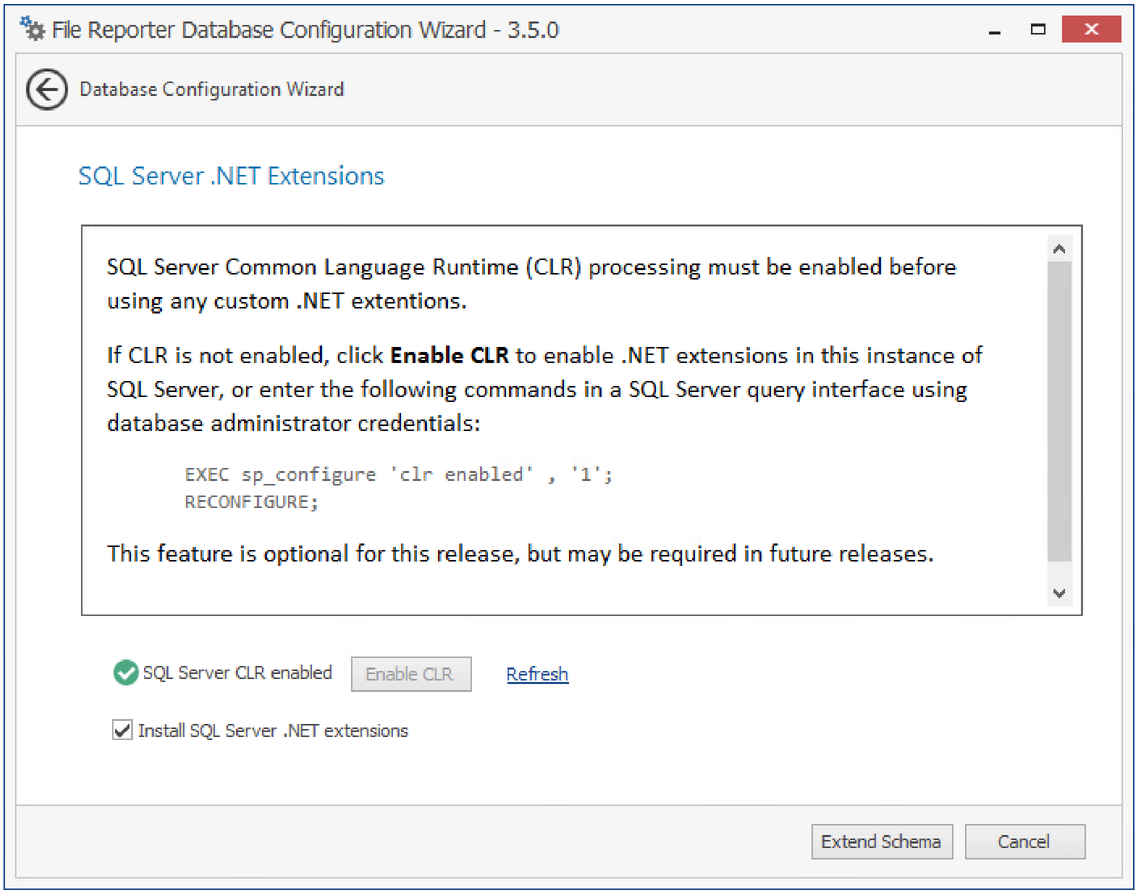
Database Administrator: If you are using a PostgreSQL database, specify the superuser name. If you are using an SQL Server, specify the administrator name.

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

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

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

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


File Reporter Database Configuration Wizard - 3.5.0
Database Configuration Wizard
SQL Server .NET Extensions

SQL Server Common Language Runtime (CLR) processing must be enabled before using any custom .NET extentions.

If CLR is not enabled, click **Enable CLR** to enable .NET extensions in this instance of SQL Server, or enter the following commands in a SQL Server query interface using database administrator credentials:

```
EXEC sp_configure 'clr enabled' , '1';
RECONFIGURE;
```

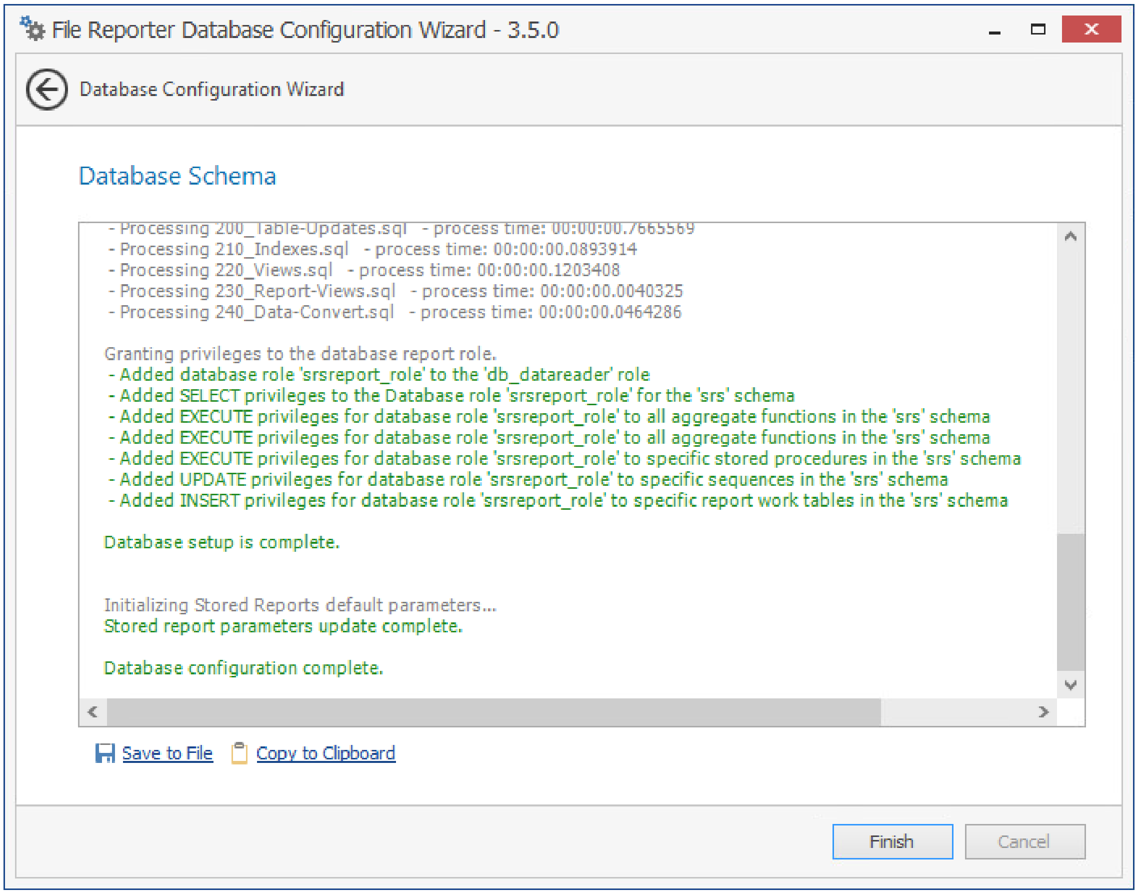
This feature is optional for this release, but may be required in future releases.

✓ SQL Server CLR enabled

☑ Install SQL Server .NET extensions

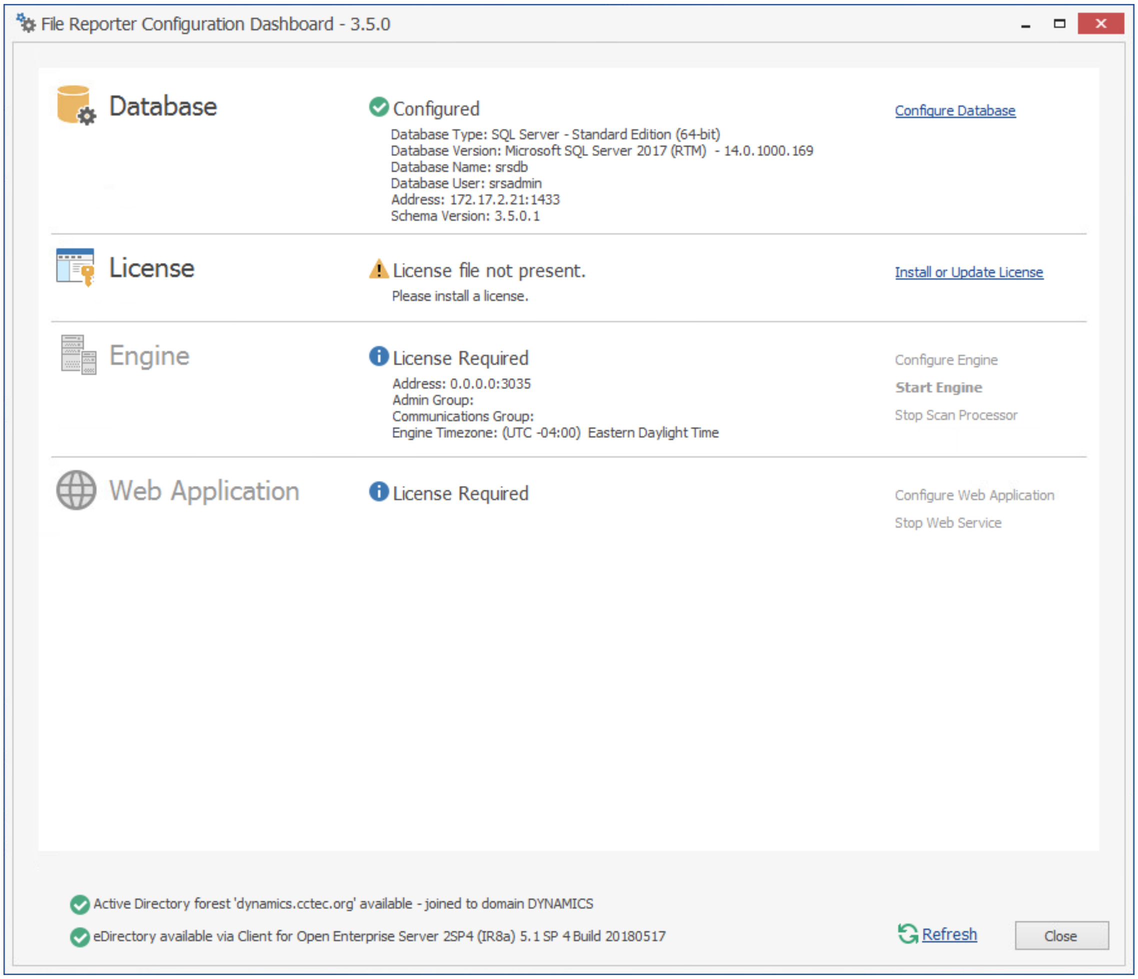
4 (Conditional) Click **Enable CLR**.

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


File Reporter Database Configuration Wizard - 3.5.0
Database Configuration Wizard
Database Schema
Save to File
Copy to Clipboard
Finish
Cancel

```
 - Processing 200_Table-Updates.sql   - process time: 00:00:00.7665569
 - Processing 210_Indexes.sql   - process time: 00:00:00.0893914
 - Processing 220_Views.sql   - process time: 00:00:00.1203408
 - Processing 230_Report-Views.sql   - process time: 00:00:00.0040325
 - Processing 240_Data-Convert.sql   - process time: 00:00:00.0464286

Granting privileges to the database report role.
 - Added database role 'srsreport_role' to the 'db_datareader' role
 - Added SELECT privileges to the Database role 'srsreport_role' for the 'srs' schema
 - Added EXECUTE privileges for database role 'srsreport_role' to all aggregate functions in the 'srs' schema
 - Added EXECUTE privileges for database role 'srsreport_role' to all aggregate functions in the 'srs' schema
 - Added EXECUTE privileges for database role 'srsreport_role' to specific stored procedures in the 'srs' schema
 - Added UPDATE privileges for database role 'srsreport_role' to specific sequences in the 'srs' schema
 - Added INSERT privileges for database role 'srsreport_role' to specific report work tables in the 'srs' schema

Database setup is complete.


Initializing Stored Reports default parameters...
Stored report parameters update complete.

Database configuration complete.
```

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



File Reporter Configuration Dashboard - 3.5.0

Database

✓ Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

License

⚠ License file not present.

Please install a license.

Engine

ⓘ License Required

Address: 0.0.0.0:3035
Admin Group:
Communications Group:
Engine Timezone: (UTC -04:00) Eastern Daylight Time

Web Application

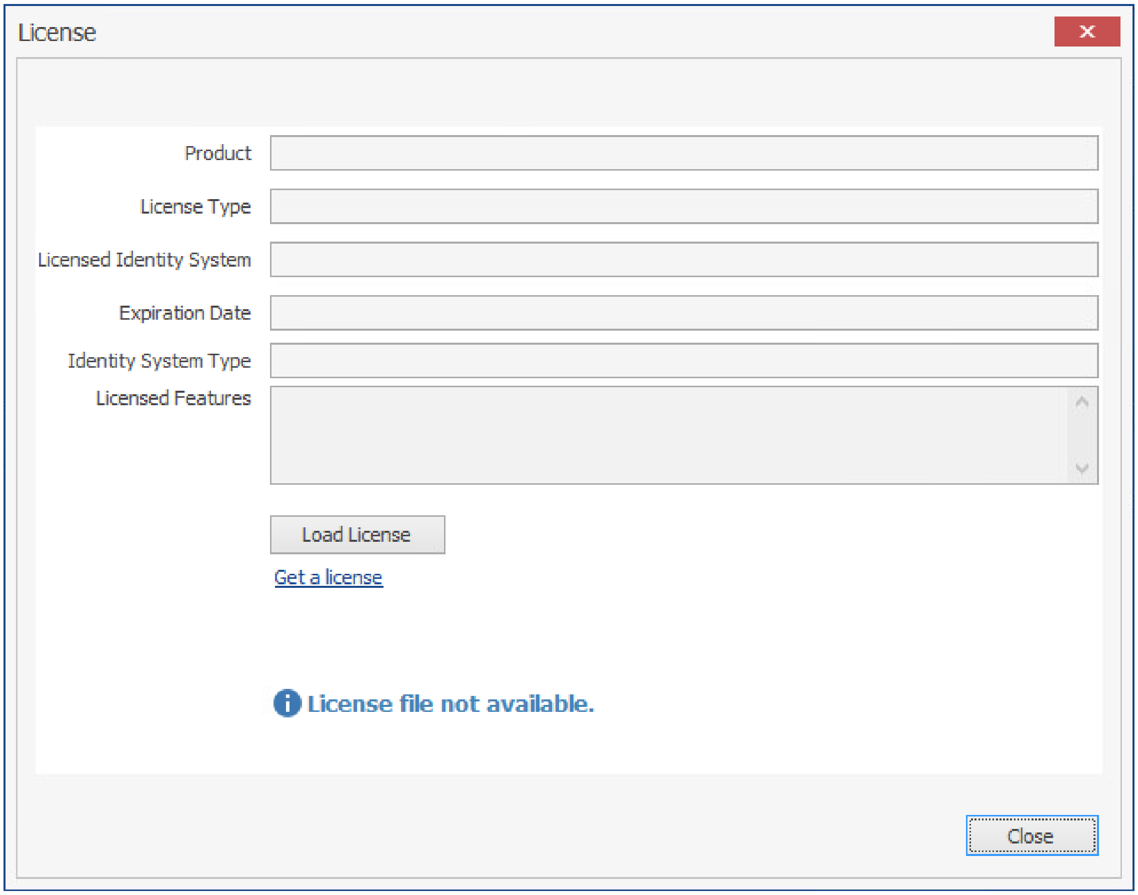
ⓘ License Required

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

7.5 Installing the License

1 Click **Install or Update License**.



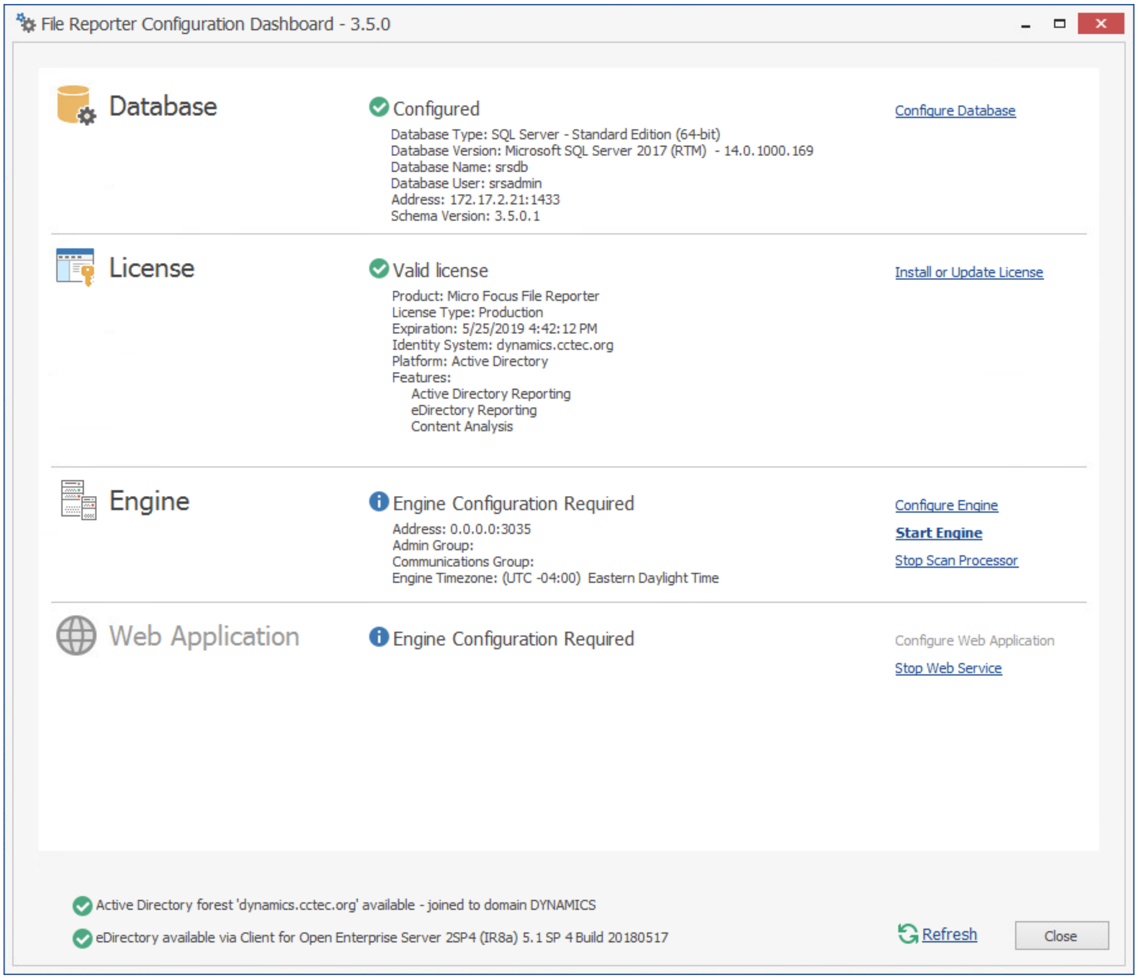
License file not available.

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

You must have a Micro Focus File Reporter license for Active Directory.

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

4 Click **Close**.



Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

Valid license

Product: Micro Focus File Reporter
License Type: Production
Expiration: 5/25/2019 4:42:12 PM
Identity System: dynamics.cctec.org
Platform: Active Directory
Features:
Active Directory Reporting
eDirectory Reporting
Content Analysis

Engine Configuration Required

Address: 0.0.0.0:3035
Admin Group:
Communications Group:
Engine Timezone: (UTC -04:00) Eastern Daylight Time

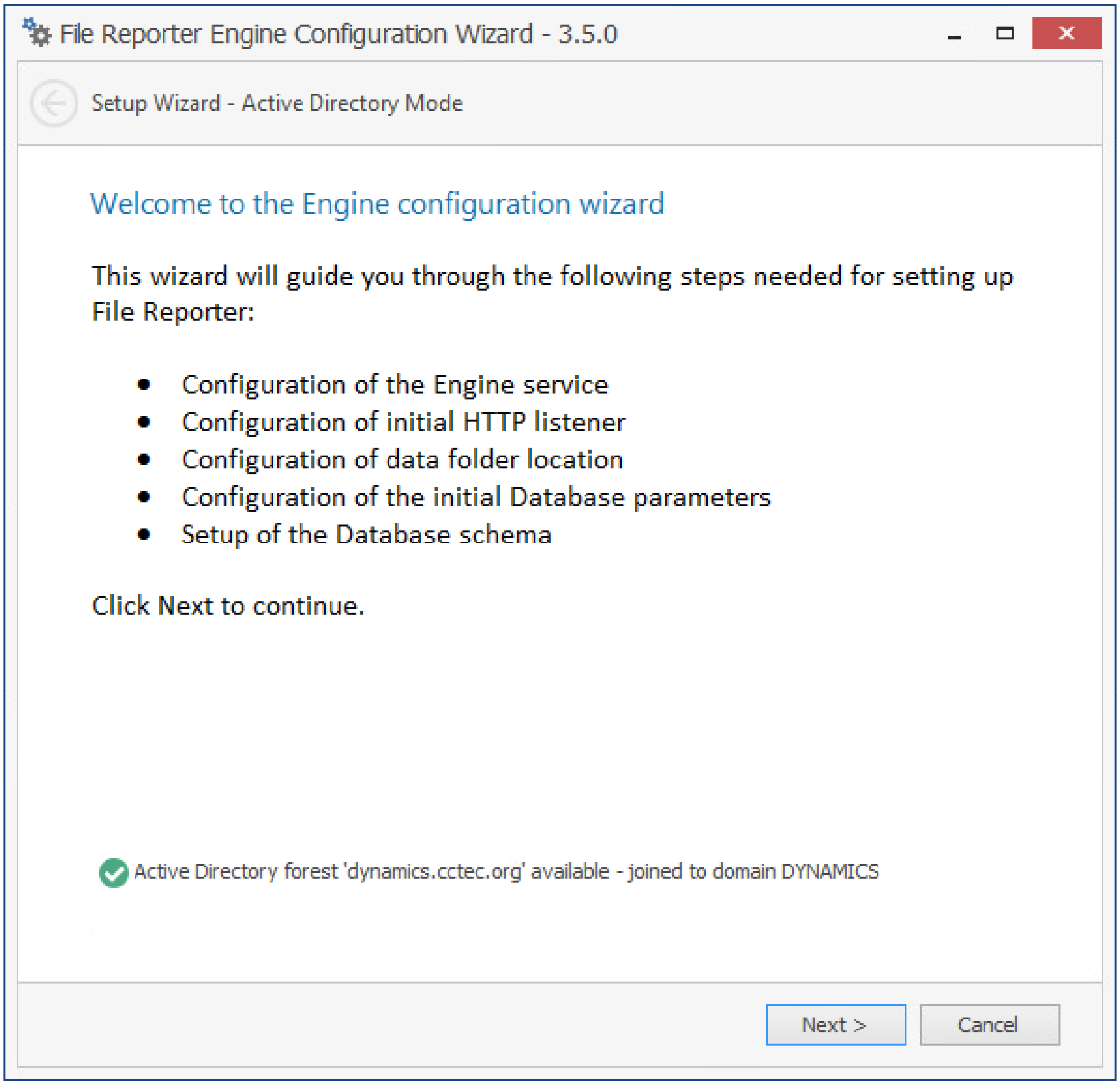
Engine Configuration Required

Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

7.6 Configuring the Engine

1 Click **Configure Engine**.


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - Active Directory Mode

Welcome to the Engine configuration wizard

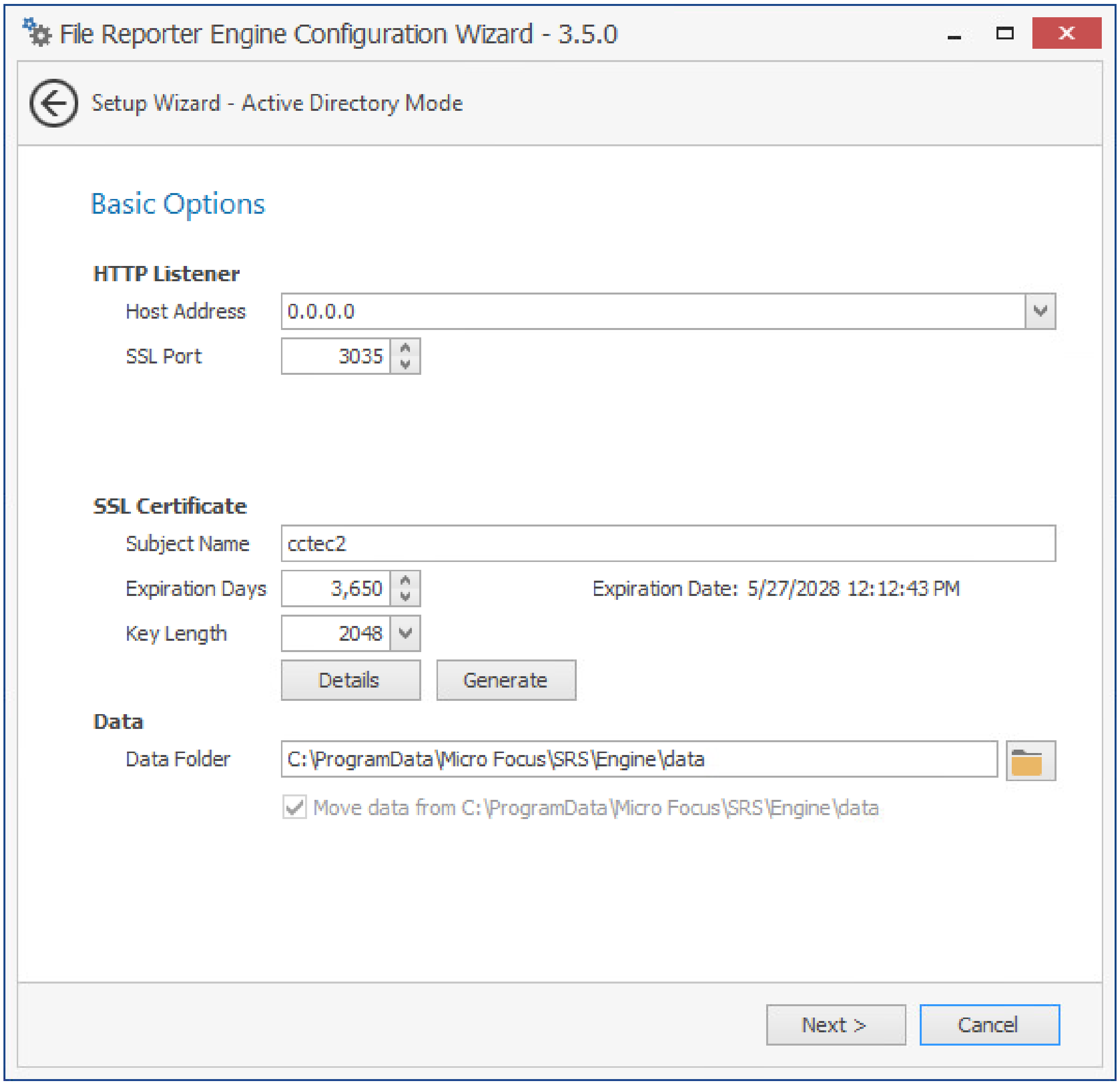
This wizard will guide you through the following steps needed for setting up File Reporter:

- Configuration of the Engine service
- Configuration of initial HTTP listener
- Configuration of data folder location
- Configuration of the initial Database parameters
- Setup of the Database schema

Click Next to continue.

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

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


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - Active Directory Mode
Basic Options
HTTP Listener

Host Address: 0.0.0.0

SSL Port: 3035

Subject Name: cctec2

Expiration Days: 3,650

Expiration Date: 5/27/2028 12:12:43 PM

Key Length: 2048

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

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

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.

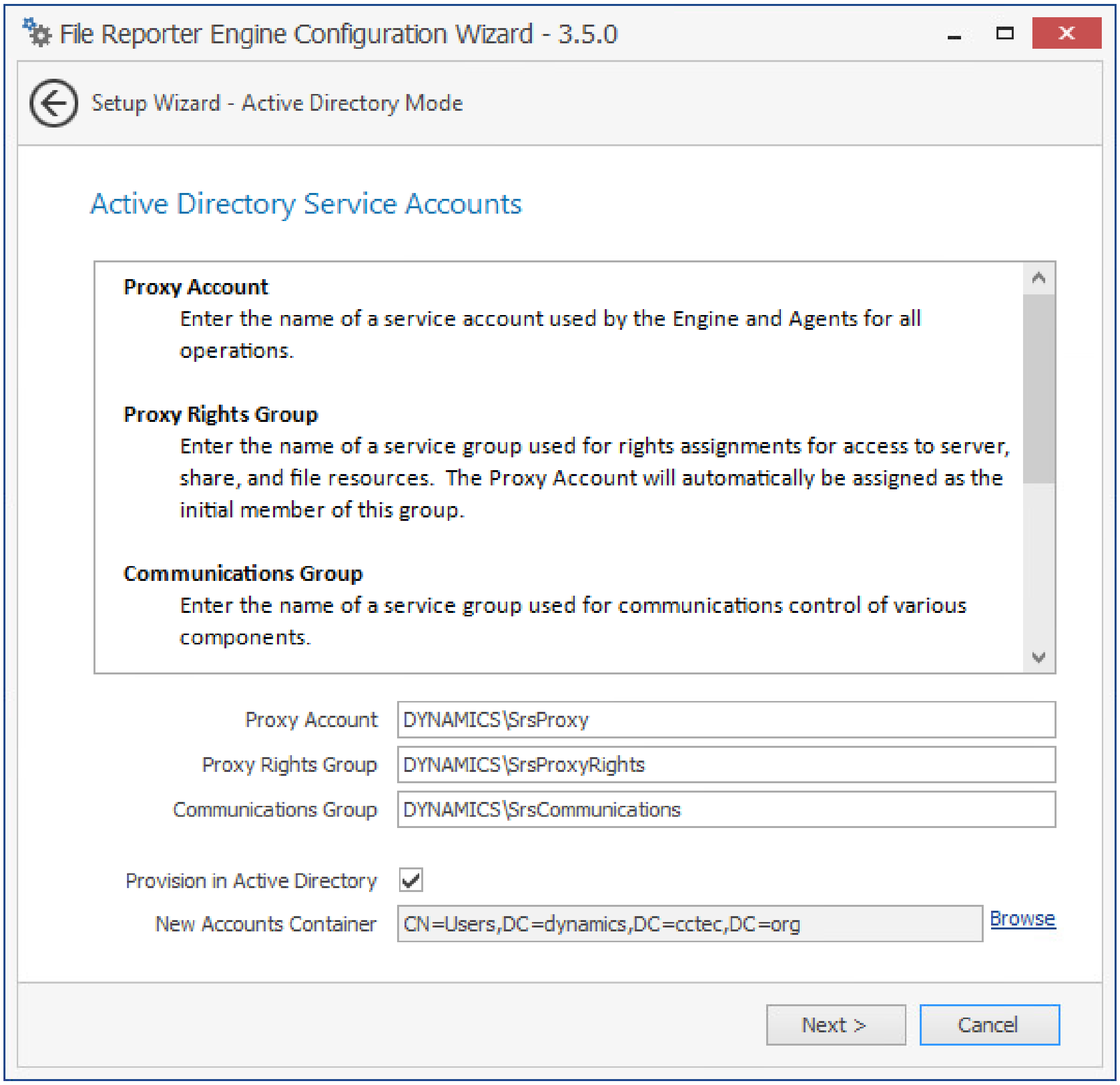
Details: Click the button to view the certificate data.

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**.



File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - Active Directory Mode

Active Directory Service Accounts

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

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

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

Proxy Account: DYNAMICS\SrsProxy
Proxy Rights Group: DYNAMICS\SrsProxyRights
Communications Group: DYNAMICS\SrsCommunications
Provision in Active Directory: ☑
New Accounts Container: CN=Users,DC=dynamics,DC=cctec,DC=org

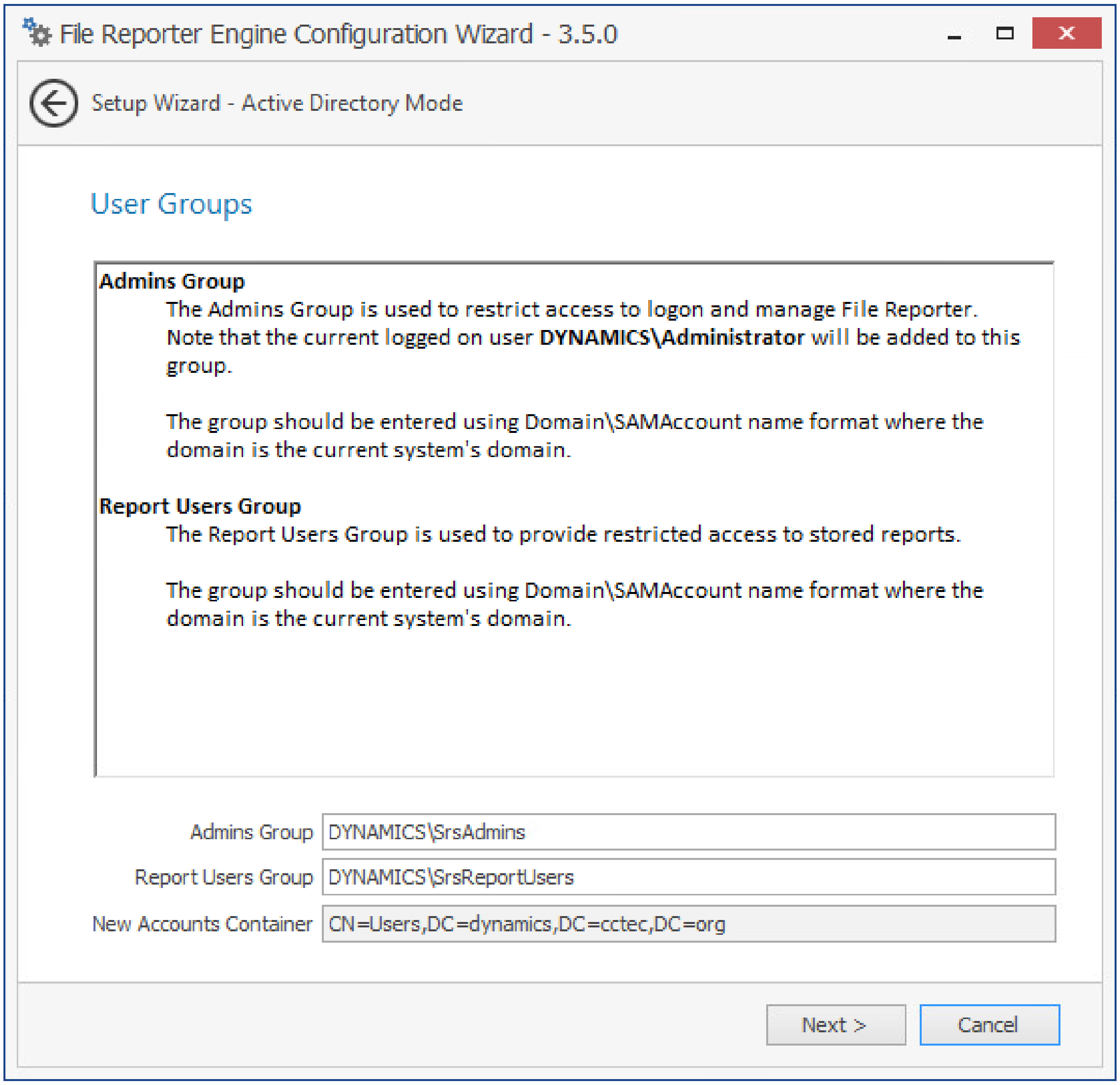
This page lets you establish a name for the proxy account, proxy rights group, and the communications group.

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.

4 Click **Next**.



File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - Active Directory Mode
User Groups

Admins Group

The Admins Group is used to restrict access to logon and manage File Reporter. Note that the current logged on user **DYNAMICS\Administrator** will be added to this group.

The group should be entered using Domain\SAMAccount name format where the domain is the current system's domain.

Report Users Group

The Report Users Group is used to provide restricted access to stored reports.

The group should be entered using Domain\SAMAccount name format where the domain is the current system's domain.

Admins Group: DYNAMICS\SrsAdmins

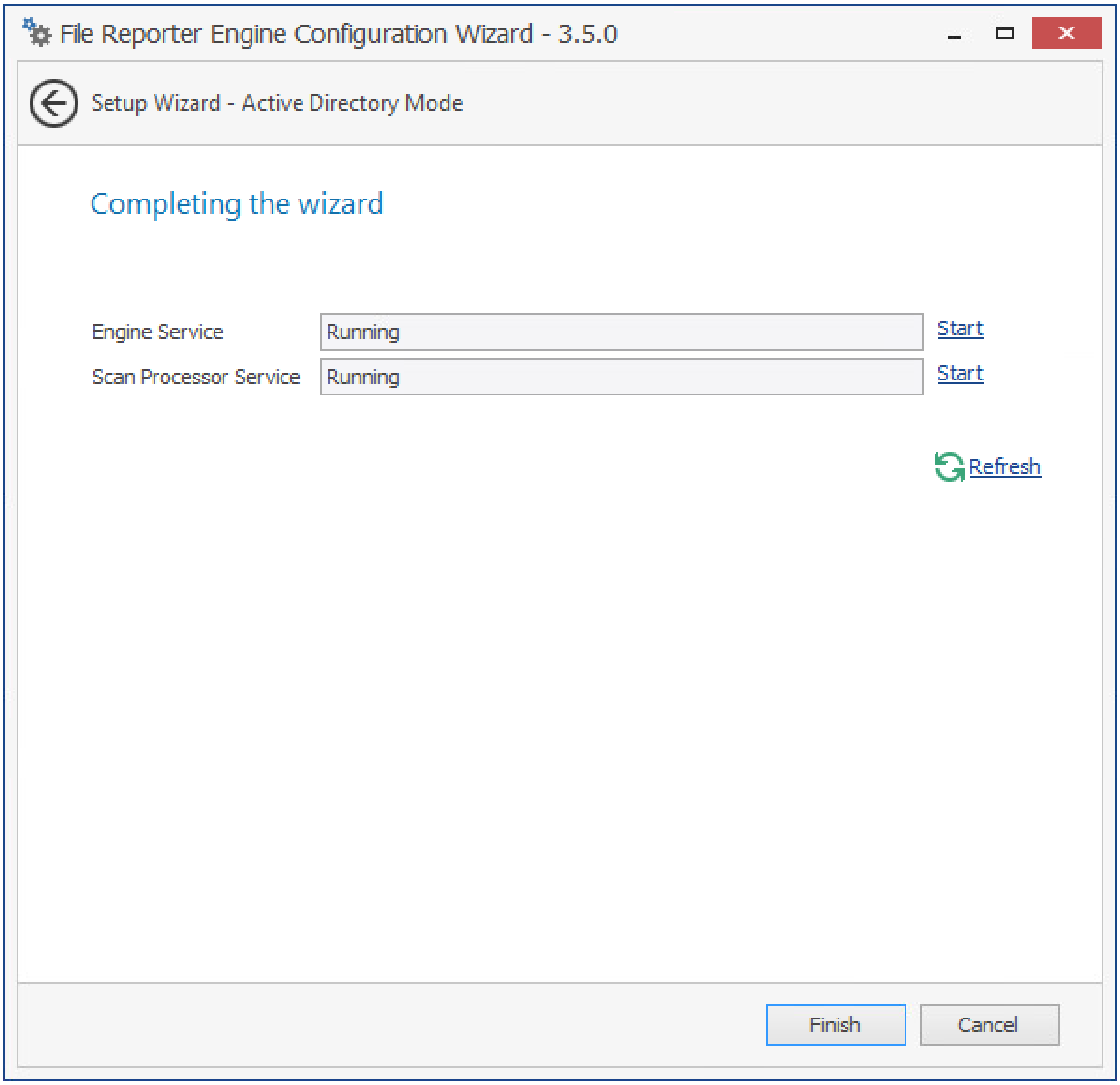
Report Users Group: DYNAMICS\SrsReportUsers

New Accounts Container: CN=Users,DC=dynamics,DC=cctec,DC=org

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.


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - Active Directory Mode
Completing the wizard

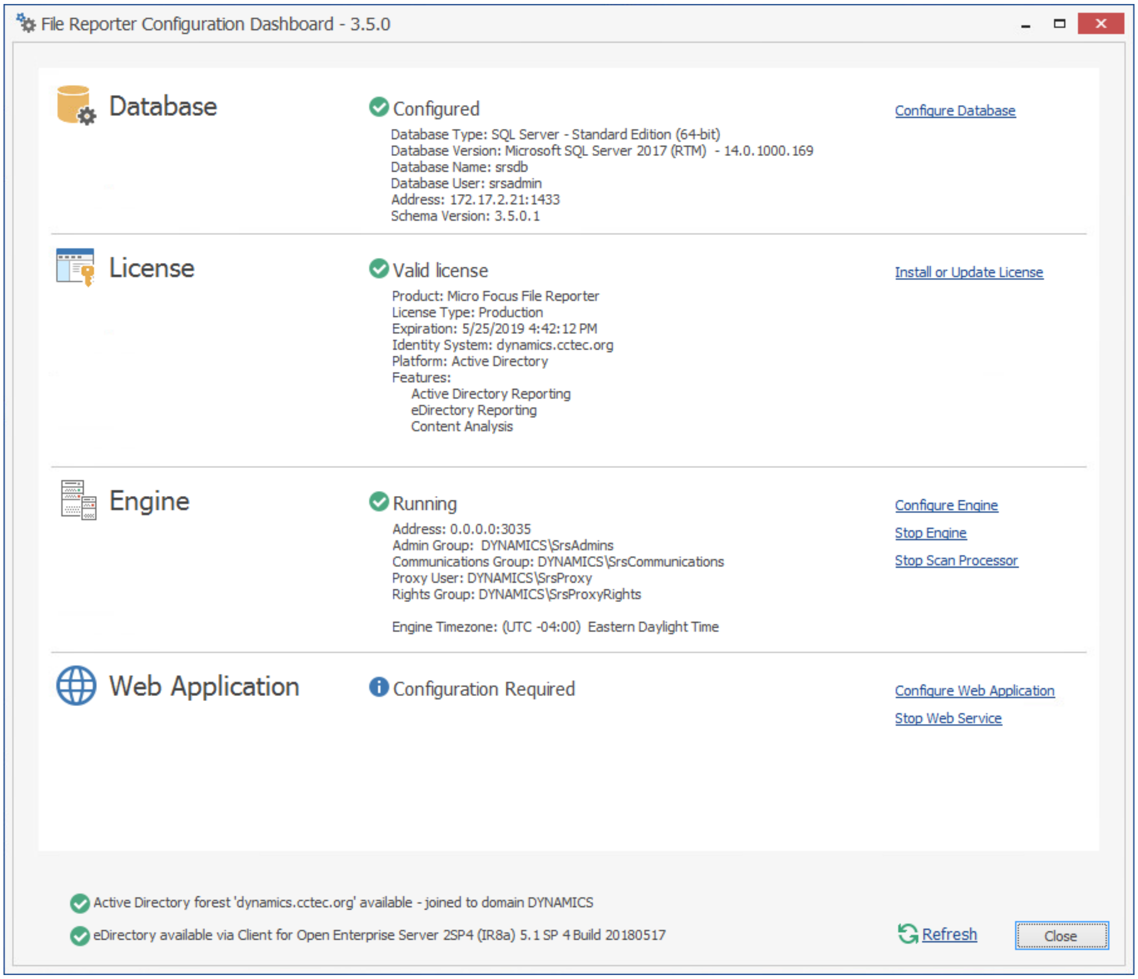
Engine Service: Running

Scan Processor Service: Running

Start
Start
Refresh
Finish
Cancel

7 Click **Finish**.

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


File Reporter Configuration Dashboard - 3.5.0
Configure Database
Install or Update License
Configure Engine
Stop Engine
Stop Scan Processor
Configure Web Application
Stop Web Service
Refresh
Close

Database

Configured
Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

License

Valid license
Product: Micro Focus File Reporter
License Type: Production
Expiration: 5/25/2019 4:42:12 PM
Identity System: dynamics.cctec.org
Platform: Active Directory
Features:
  Active Directory Reporting
  eDirectory Reporting
  Content Analysis

Engine

Running
Address: 0.0.0.0:3035
Admin Group: DYNAMICS\SrsAdmins
Communications Group: DYNAMICS\SrsCommunications
Proxy User: DYNAMICS\SrsProxy
Rights Group: DYNAMICS\SrsProxyRights

Engine Timezone: (UTC -04:00) Eastern Daylight Time

Web Application

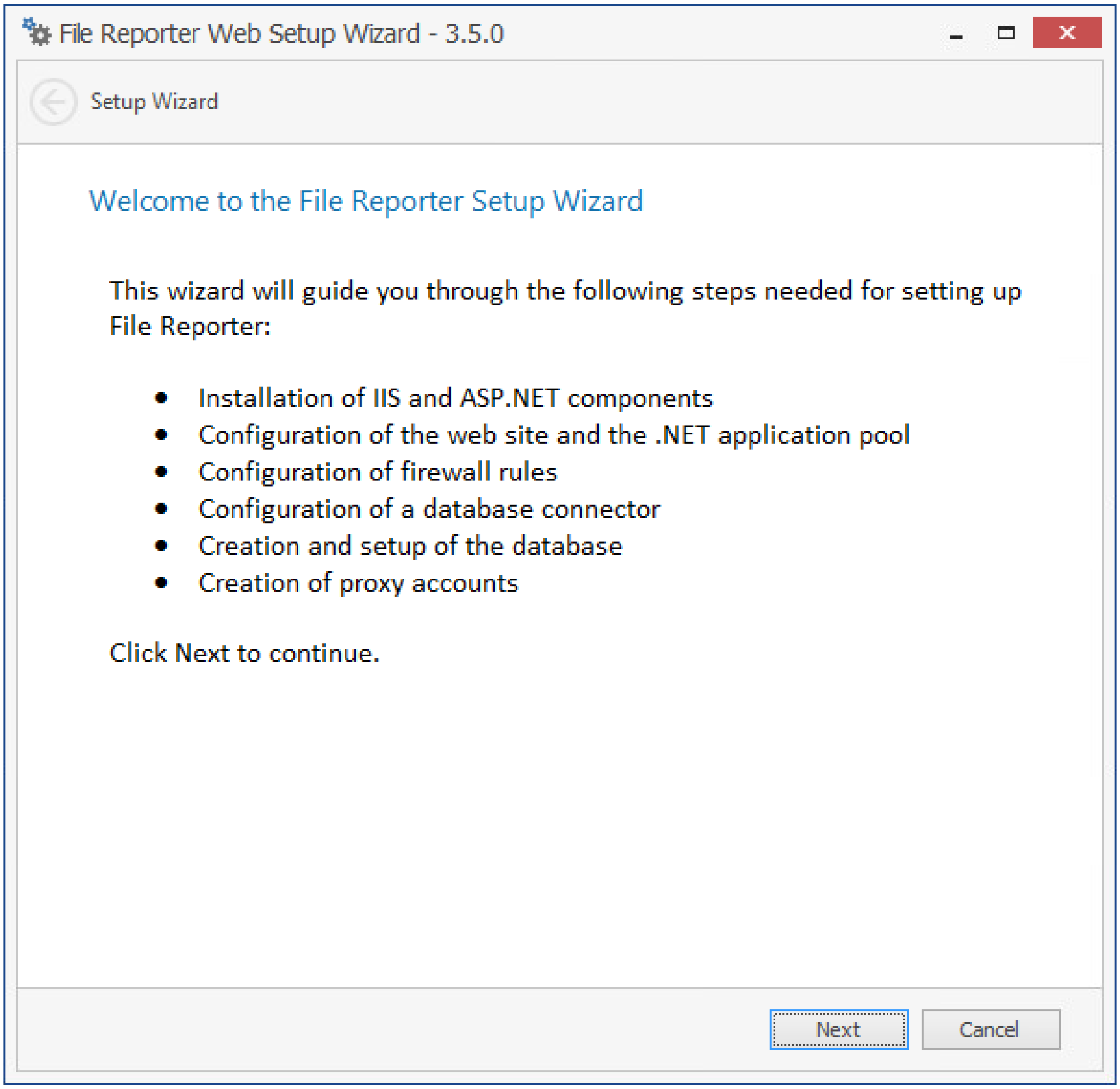
Configuration Required

Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

7.7 Configuring the Web Application

1 Click **Configure Web Application**.



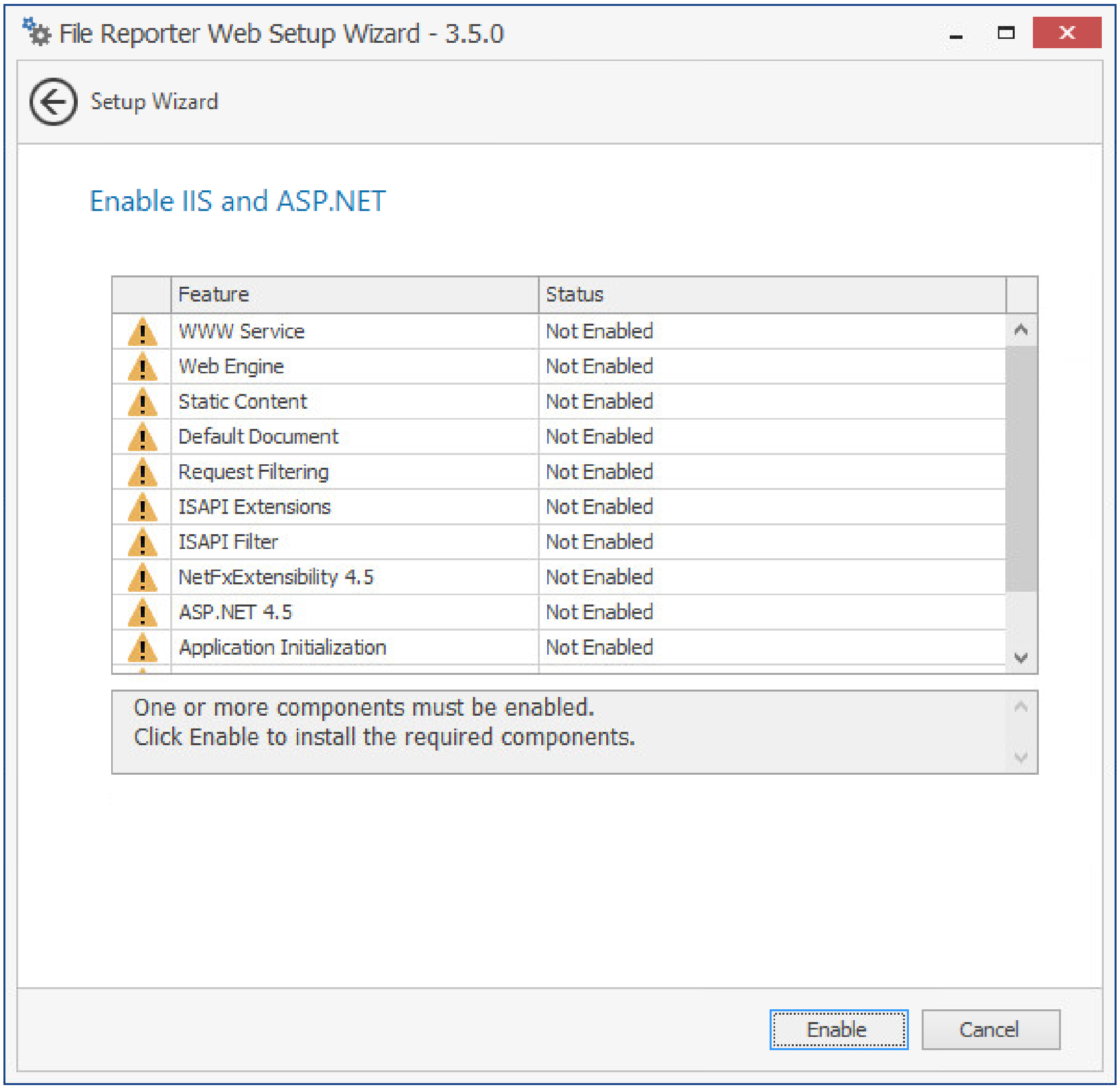
Welcome to the File Reporter Setup Wizard

This wizard will guide you through the following steps needed for setting up File Reporter:

- Installation of IIS and ASP.NET components
- Configuration of the web site and the .NET application pool
- Configuration of firewall rules
- Configuration of a database connector
- Creation and setup of the database
- Creation of proxy accounts

Click Next to continue.

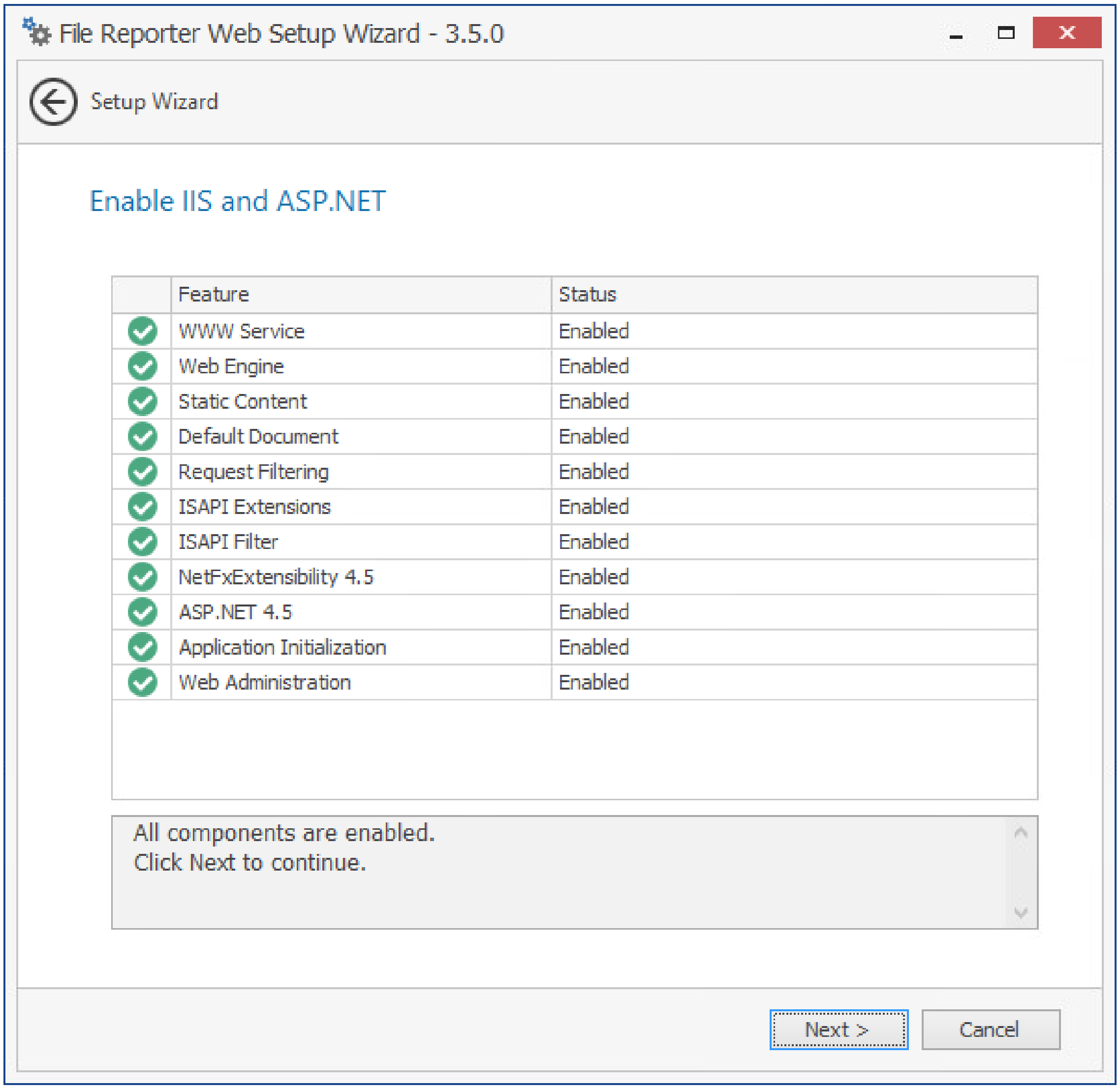
2 From the wizard page, read the overview of what will be configured and click **Next**.



	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

One or more components must be enabled.
Click Enable to install the required components.

3 Click **Enable**.

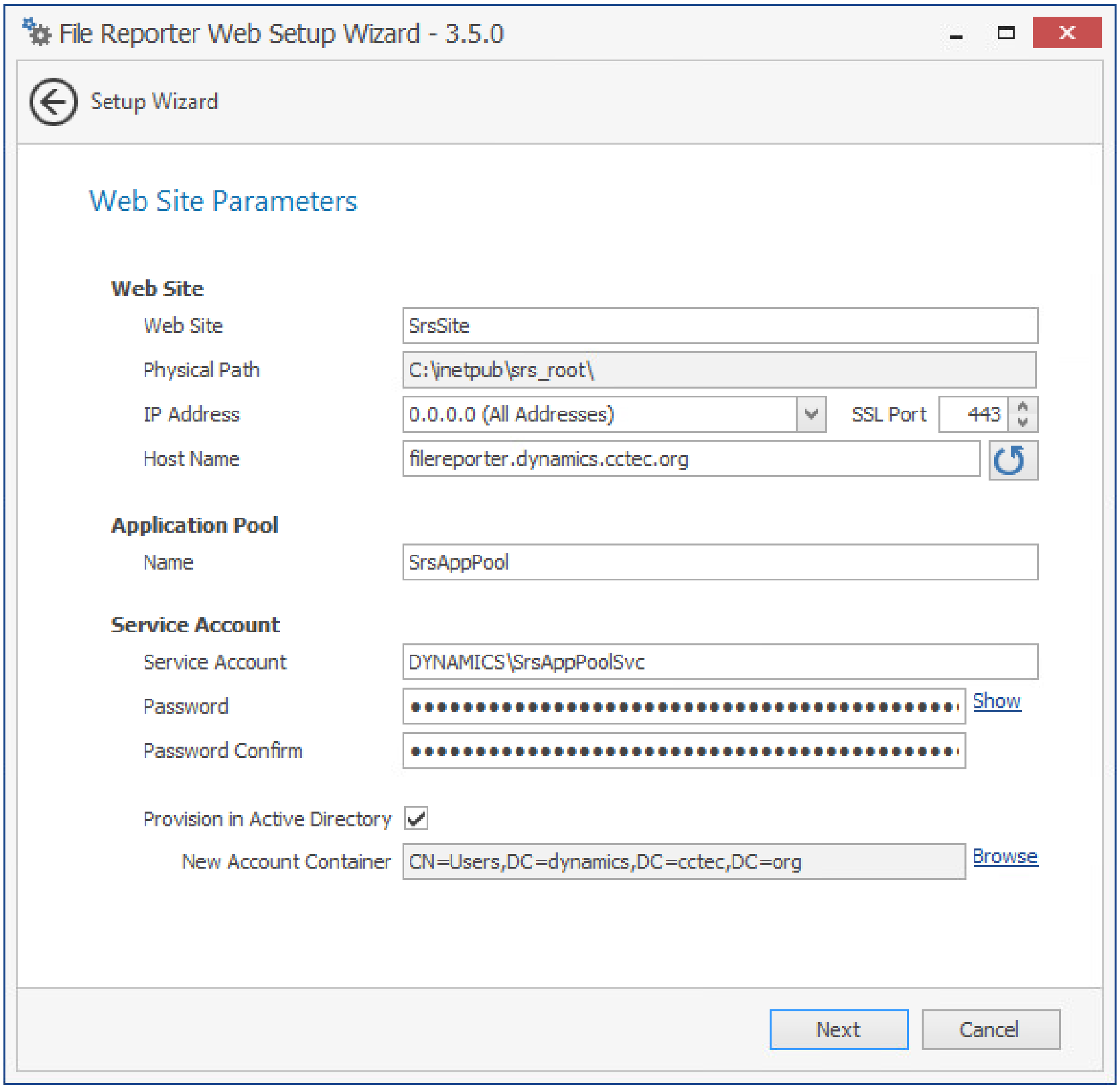


Enable IIS and ASP.NET

	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.

4 Click **Next**.



Web Site Parameters

Web Site

Web Site	SrsSite
Physical Path	C:\inetpub\srs_root\
IP Address	0.0.0.0 (All Addresses)
SSL Port	443
Host Name	filereporter.dynamics.cctec.org

Application Pool

Name	SrsAppPool

Service Account

Service Account	DYNAMICS\SrsAppPoolSvc
Password	••
Password Confirm	••
Provision in Active Directory	☑
New Account Container	CN=Users,DC=dynamics,DC=cctec,DC=org

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

Web Site: Settings for the Microsoft IIS Web site.

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

Physical Path: This path was specified in Step 5 on page 41 and is the location where files on the Web site are served up. You cannot edit this path.

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

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

Host Name: The host name as defined in DNS that you specified in Section 7.2, "Prerequisites," on page 40.

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.

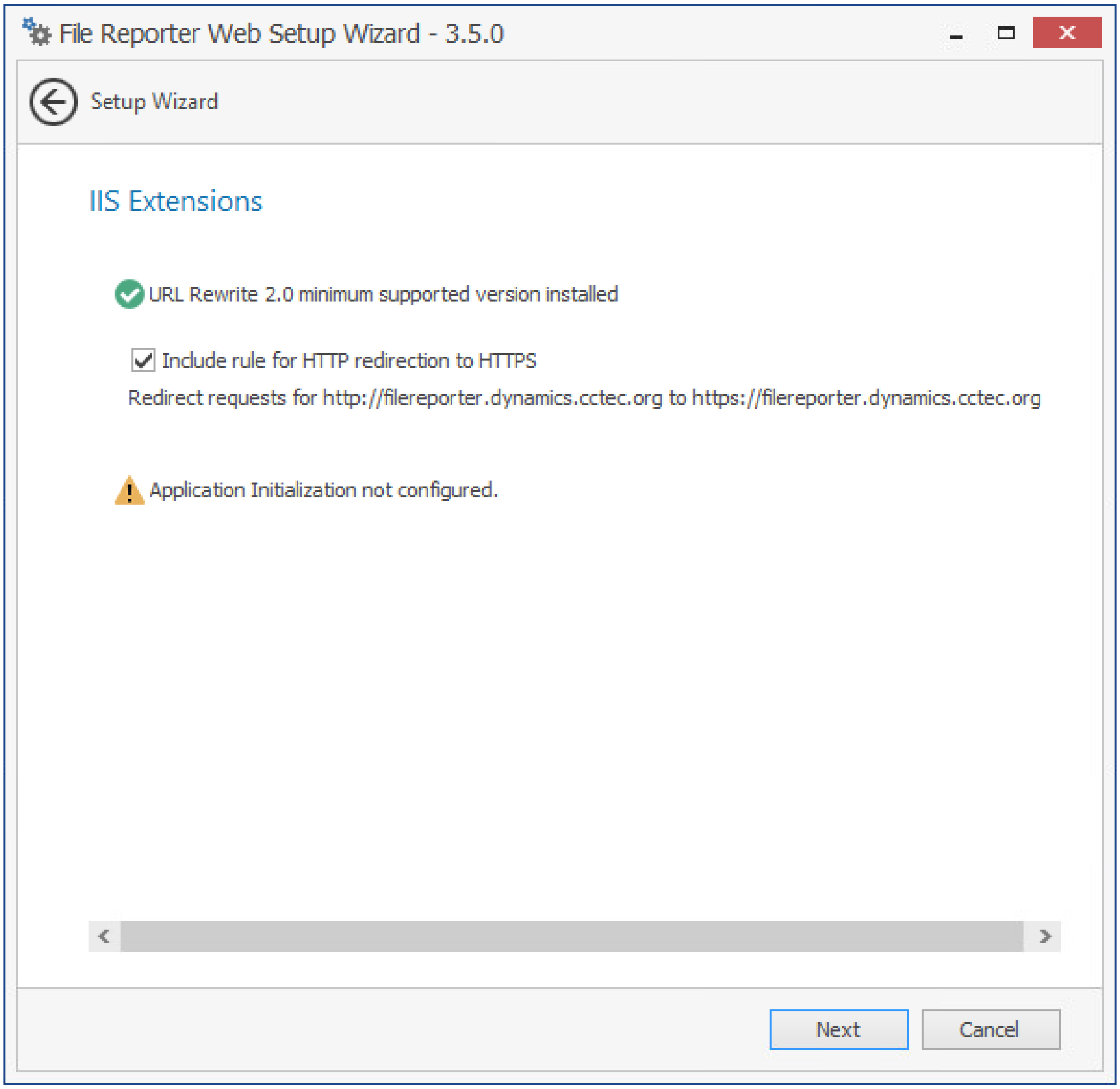
Confirm Password: The automatically generated password is repeated.

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**.



✓ URL Rewrite 2.0 minimum supported version installed

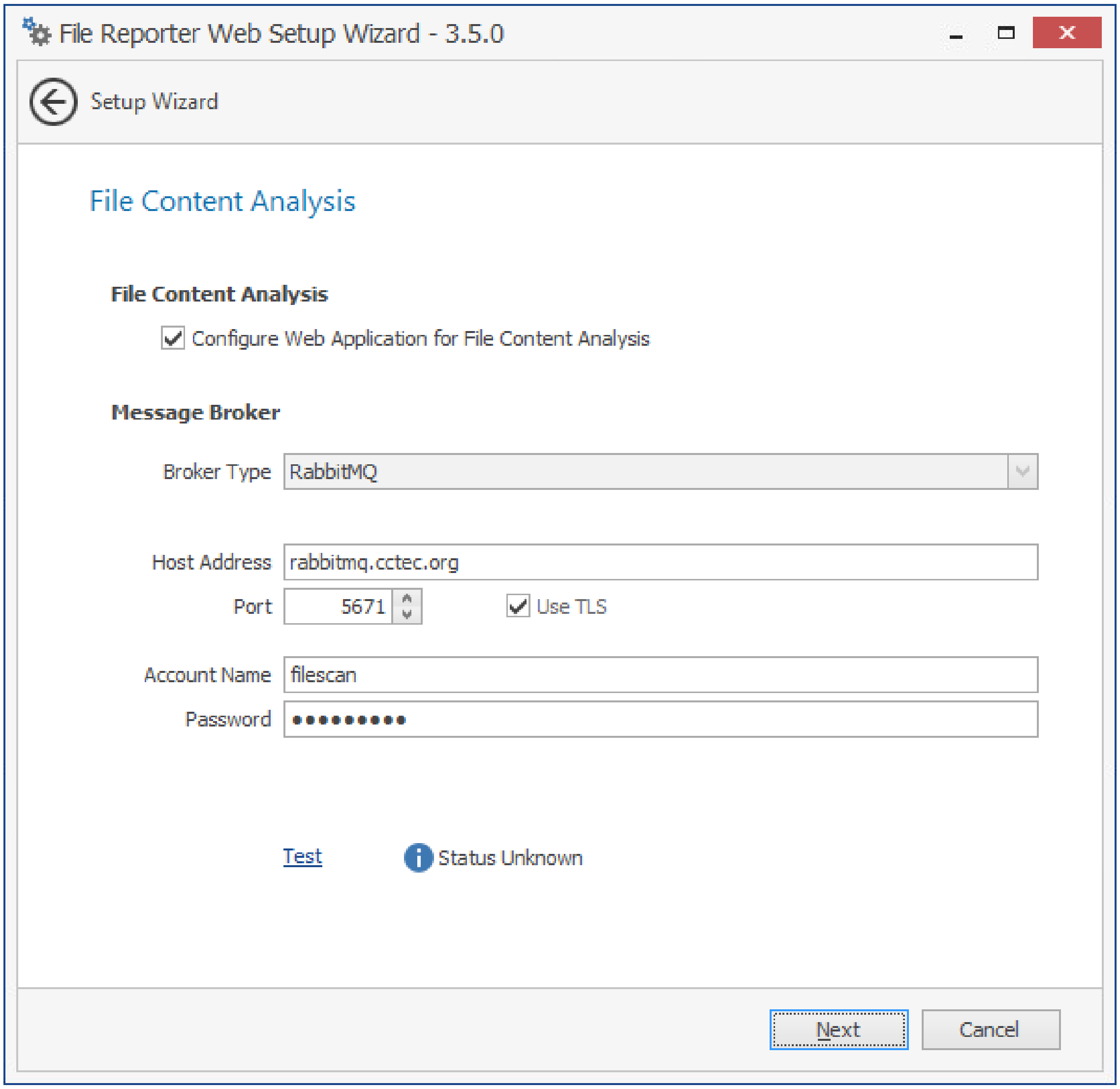
☑ Include rule for HTTP redirection to HTTPS

Redirect requests for http://filereporter.dynamics.cctec.org to https://filereporter.dynamics.cctec.org

⚠ Application Initialization not configured.

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

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



File Reporter Web Setup Wizard - 3.5.0

Setup Wizard

File Content Analysis

File Content Analysis

☑ Configure Web Application for File Content Analysis

Message Broker

Broker Type: RabbitMQ

Host Address: rabbitmq.cctec.org

Port: 5671 ☑ Use TLS

Account Name: filescan

Password: ●●●●●●●●●

Test — Status Unknown

Configure Web Application for File Content Analysis: If you are not set up for File Content scanning or your message broker is not yet configured, deselect this check box. Deselecting this allows you to skip the File Content Analysis step as well as the following File Content Search Results step.

For example, if you are upgrading from File Reporter 3.0.*x* and do not yet want to utilize file content scanning, you can select this option to proceed with the upgrade.

Message Broker: Fields specific to the messaging broker.

Broker Type: Displays the RabbitMQ messaging broker.

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

Port: Change the port setting to 5671.

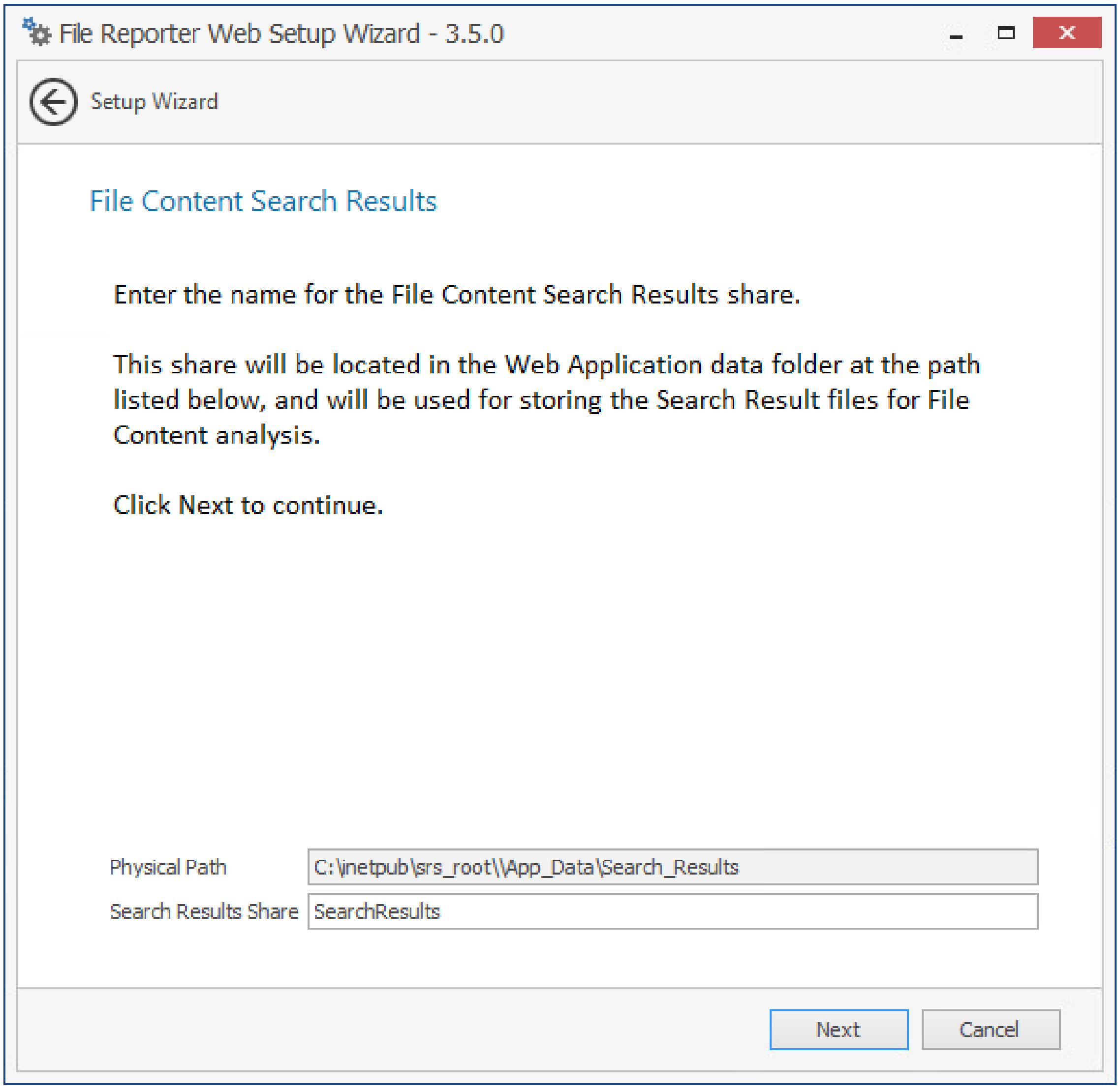
Use TLS: The RabbitMQ messaging broker in File Reporter utilizes Transport Layer Security (TLS) as the cryptographic communications security protocol.

Account Name: The default name is `filescan`.

Password: Enter the updated password that you changed in Section 6.4, "Changing the Default Password," on page 36.

Test: Click to test the connection between the Web App and the RabbitMQ messaging broker.

8 Enter the communications settings for communication with the RabbitMQ messaging broker and click **Next**.



File Content 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.

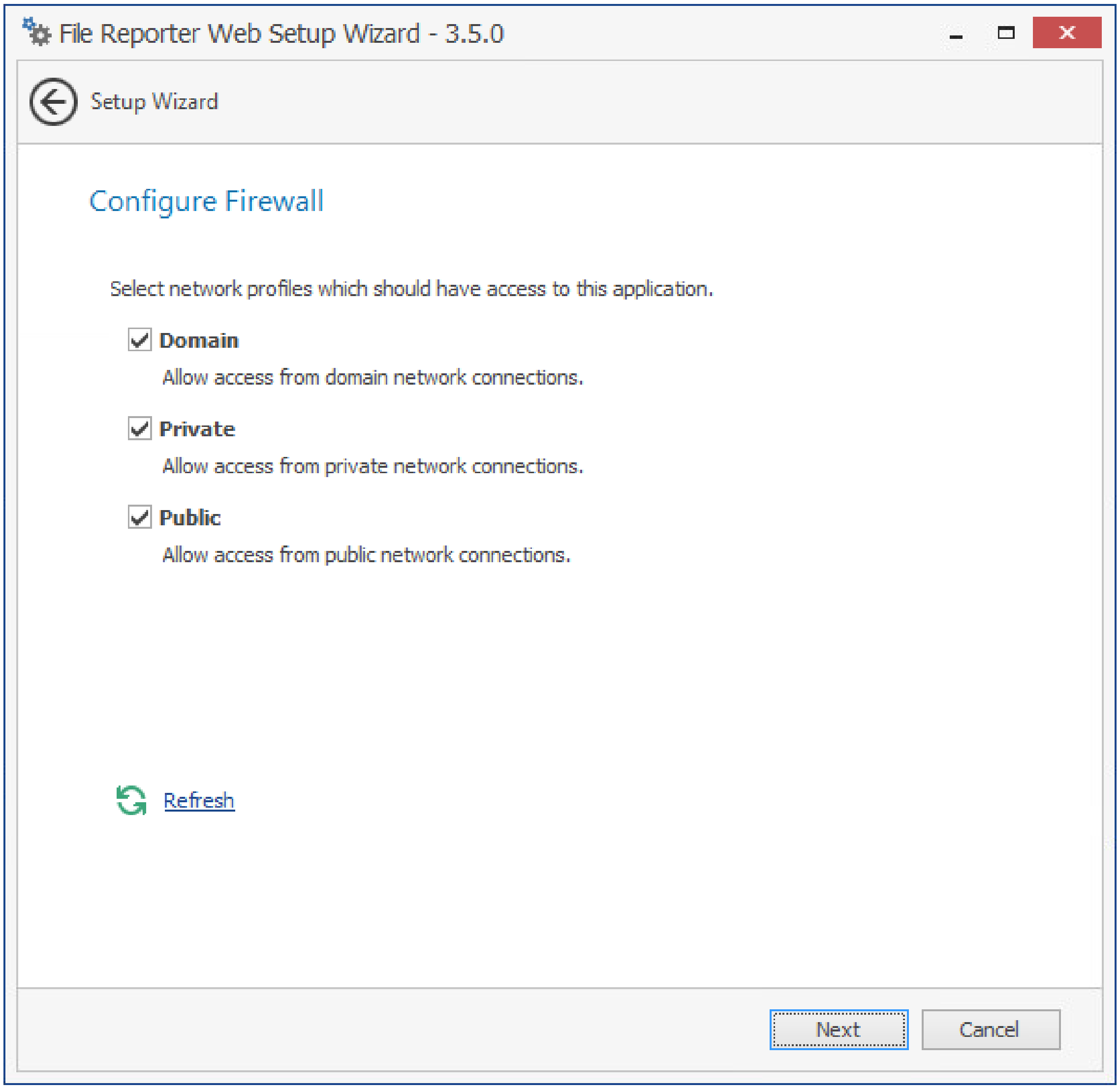
Click Next to continue.

Physical Path: C:\inetpub\srs_root\\App_Data\Search_Results

Search Results Share: SearchResults

This page lets you specify the physical path where content search results are stored.

9 Click **Next**.



Configure Firewall

Select network profiles which should have access to this application.

☑ **Domain**
Allow access from domain network connections.

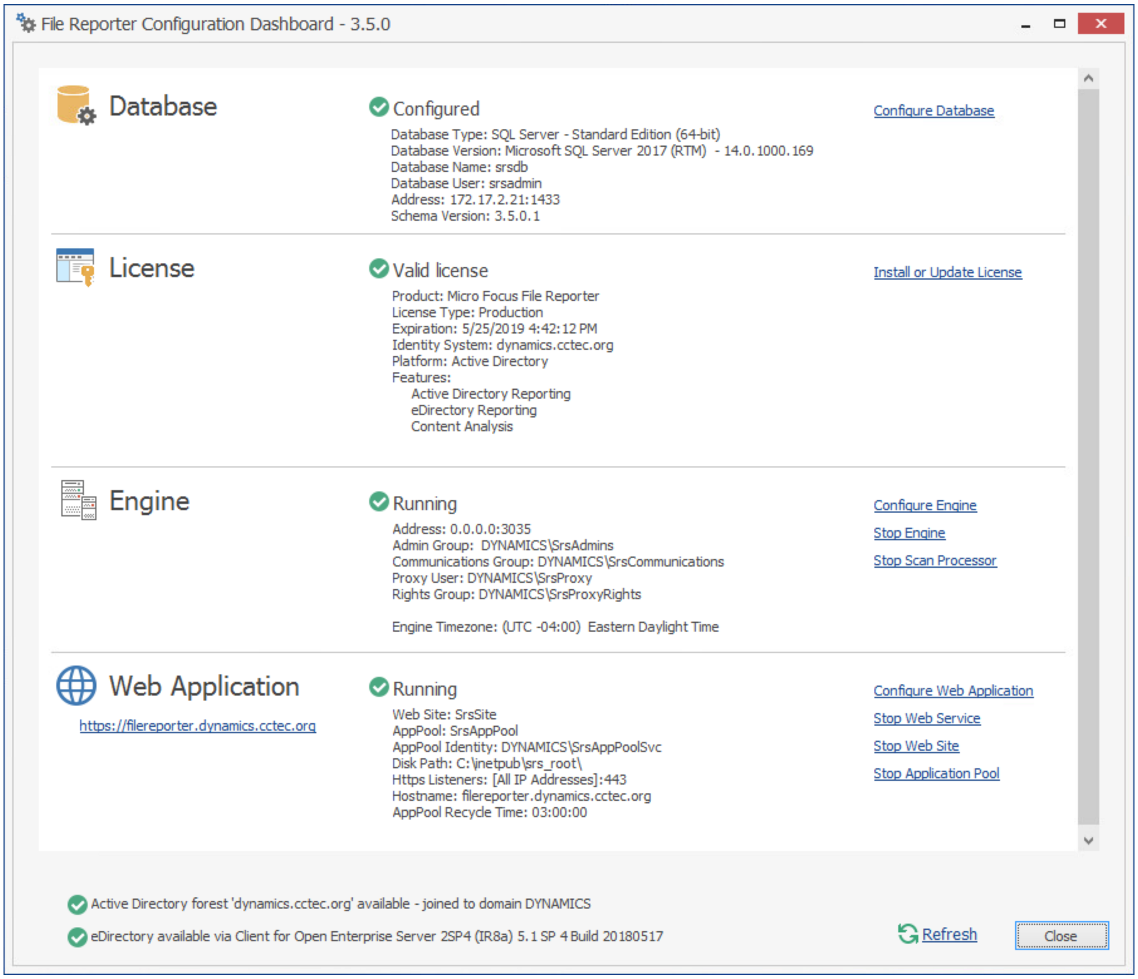
☑ **Private**
Allow access from private network connections.

☑ **Public**
Allow access from public network connections.

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

11 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.



Database

✓ Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

License

✓ Valid license

Product: Micro Focus File Reporter
License Type: Production
Expiration: 5/25/2019 4:42:12 PM
Identity System: dynamics.cctec.org
Platform: Active Directory
Features:
  Active Directory Reporting
  eDirectory Reporting
  Content Analysis

Engine

✓ Running

Address: 0.0.0.0:3035
Admin Group: DYNAMICS\SrsAdmins
Communications Group: DYNAMICS\SrsCommunications
Proxy User: DYNAMICS\SrsProxy
Rights Group: DYNAMICS\SrsProxyRights

Engine Timezone: (UTC -04:00) Eastern Daylight Time

Web Application

https://filereporter.dynamics.cctec.org

✓ Running

Web Site: SrsSite
AppPool: SrsAppPool
AppPool Identity: DYNAMICS\SrsAppPoolSvc
Disk Path: C:\inetpub\srs_root\
Https Listeners: [All IP Addresses]:443
Hostname: filereporter.dynamics.cctec.org
AppPool Recycle Time: 03:00:00

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

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

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

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

8 Installing and Configuring the Engine, Database, and Web Application in an eDirectory Environment

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

This assumes that eDirectory is to be the primary identity system for File Reporter. In other words, authentication is to take place via eDirectory. Additionally, the Engine requires a license for the eDirectory version of File Reporter.

NOTE: Although eDirectory is the primary identity system, you can still have File Reporter scan and report on storage resources residing in Active Directory. See Section 7.1, “Minimum Requirements,” on page 39.

If not already installed, .NET 4.7.2 will be installed during the installation of the Engine.

8.1 Minimum Requirements

- Quad core 64-bit processor or better
- Minimum of 16 GB RAM

  Depending on the size and frequency of your scans, this amount might need to be significantly increased.
- Minimum 20 GB free space for installation files and scan processing space
- Supported operating systems:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
- (Optional) If you want File Reporter to report on storage devices that reside in Active Directory, the server on which you are installing the Engine must be part of a domain.

8.2 Prerequisites

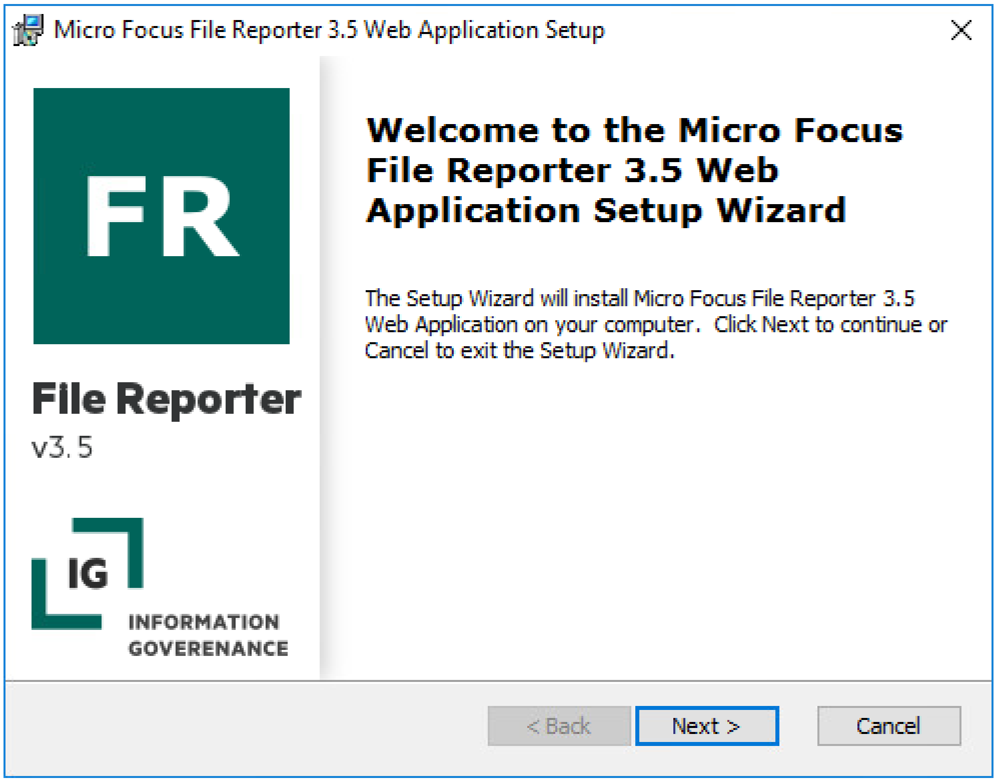
- Install the latest Client for Open Enterprise Server software on the same Windows server where you install the Engine.

  Having the Client for Open Enterprise Server installed allows File Reporter to connect to eDirectory and view the storage resources.
- On the same Windows server, configure the Service Location Protocol settings within the Client for Open Enterprise Server software.
- Create a new host record in DNS for File Reporter.

  For example: `fr.cctec.org`
- Review Appendix A, “eDirectory Universal Password Settings,” on page 125 and complete any necessary prerequisite eDirectory Universal Password configurations.

8.3 Installing and Configuring the Engine

1. At the root of the `FileReporter_3_.6.0.iso` image, double-click the `Windows` folder.
2. Double-click `FileReporter-Engine-3.6.0-x64-`*`xxxx`*`.exe`.
3. When you are asked if you want to run this file, click **Run**.
4. Agree to the license terms and conditions and click **Install**.



Micro Focus File Reporter 3.5 Web Application Setup

Welcome to the Micro Focus File Reporter 3.5 Web Application Setup Wizard

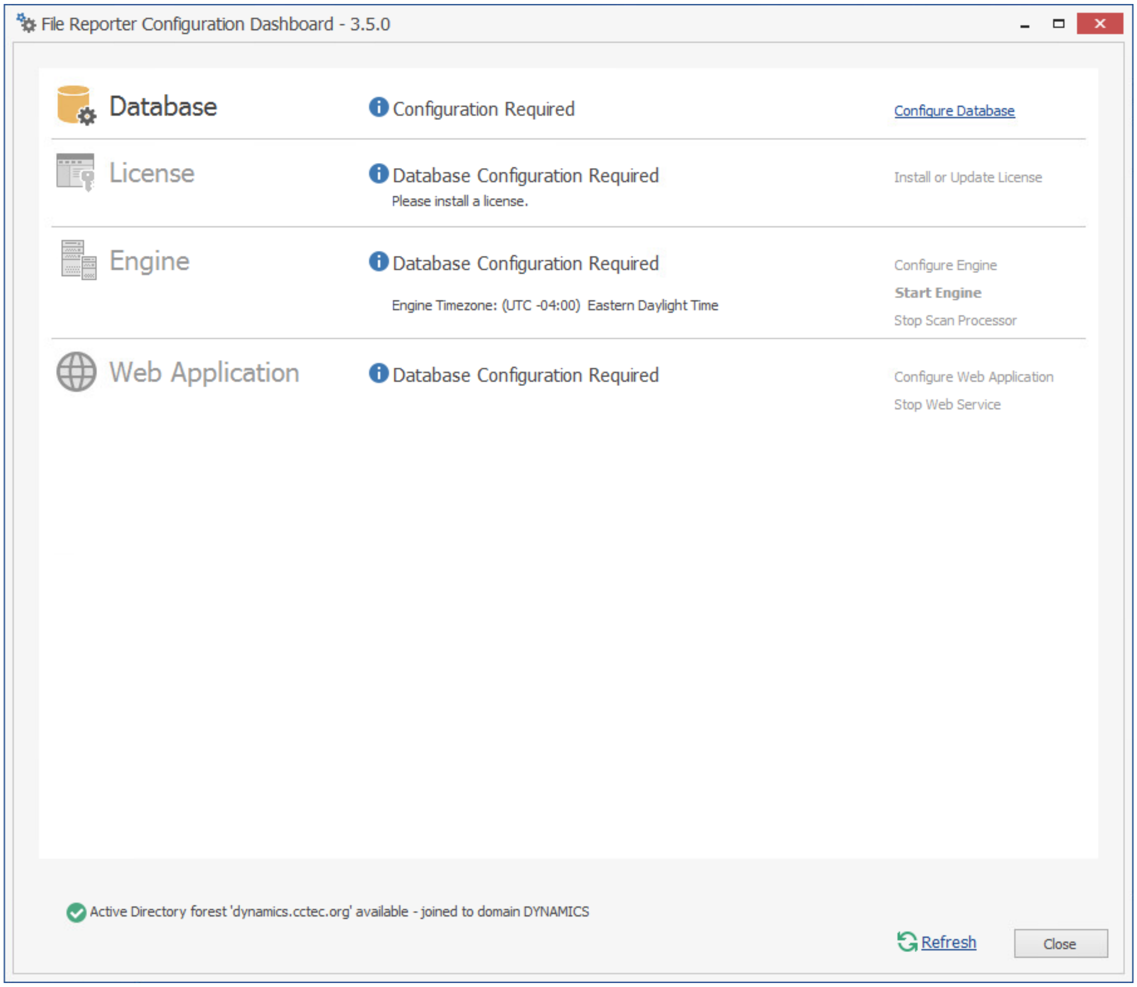
The Setup Wizard will install Micro Focus File Reporter 3.5 Web Application on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

5. Click **Next**.
6. Accept the installation path or indicate a new path by using the **Browse** button.
7. Click **Install**.

8 Click **Finish**.

9 Click **Run Config Utility**.

The File Reporter Configuration page appears.



File Reporter Configuration Dashboard - 3.5.0

Database — Configuration Required — Configure Database

License — Database Configuration Required
Please install a license. — Install or Update License

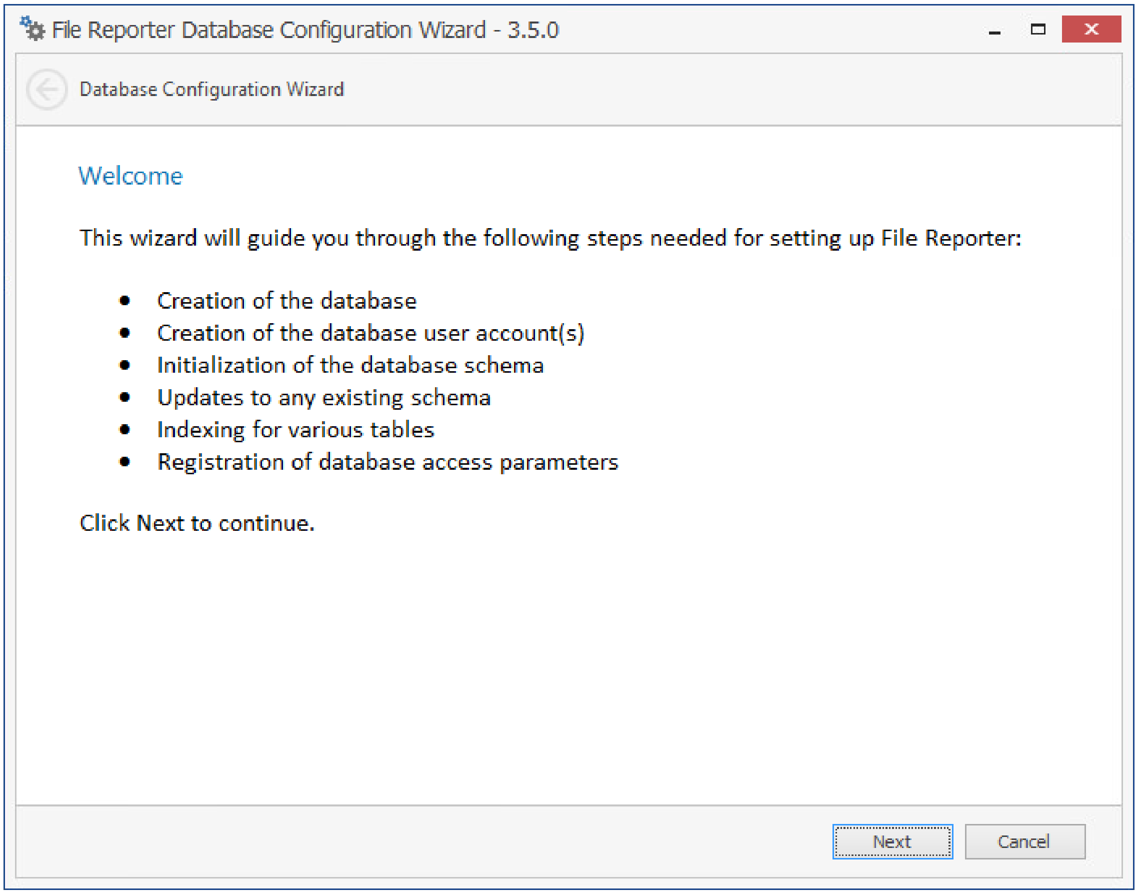
Engine — Database Configuration Required
Engine Timezone: (UTC -04:00) Eastern Daylight Time — Configure Engine, Start Engine, Stop Scan Processor

Web Application — Database Configuration Required — Configure Web Application, Stop Web Service

Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

8.4 Configuring the Database

1 Click **Configure Database**.


File Reporter Database Configuration Wizard - 3.5.0
Database Configuration Wizard

Welcome

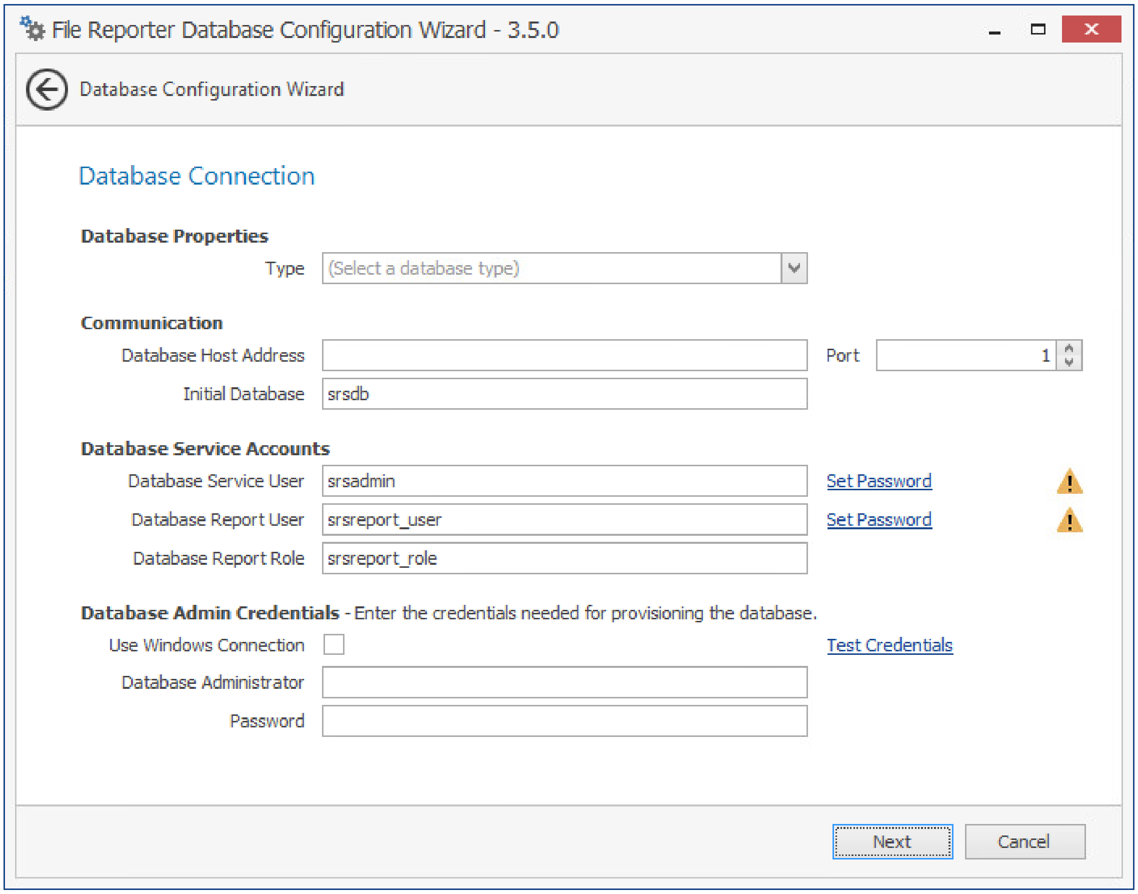
This wizard will guide you through the following steps needed for setting up File Reporter:

- Creation of the database
- Creation of the database user account(s)
- Initialization of the database schema
- Updates to any existing schema
- Indexing for various tables
- Registration of database access parameters

Click Next to continue.

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

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



File Reporter Database Configuration Wizard - 3.5.0

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

Database Report User: srsreport_user

Database Report Role: srsreport_role

Database Admin Credentials - Enter the credentials needed for provisioning the database.

Use Windows Connection: □

Database Administrator:

Password:

The 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 **SQLServer**.

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.

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

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

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

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

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

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

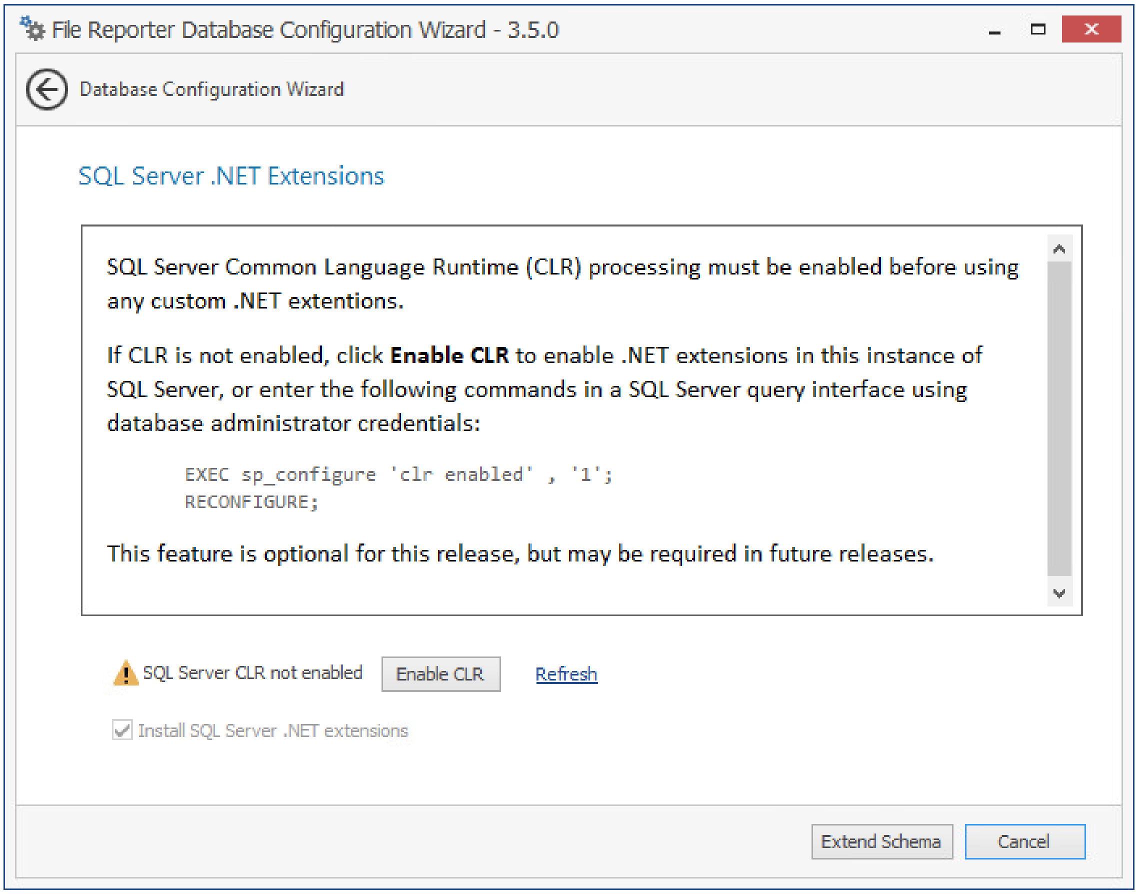
Database Administrator: If you are using a PostgreSQL database, specify the superuser name. If you are using an SQL Server database, specify the administrator name.

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

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

3 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.


File Reporter Database Configuration Wizard - 3.5.0
Database Configuration Wizard

SQL Server .NET Extensions

SQL Server Common Language Runtime (CLR) processing must be enabled before using any custom .NET extentions.

If CLR is not enabled, click **Enable CLR** to enable .NET extensions in this instance of SQL Server, or enter the following commands in a SQL Server query interface using database administrator credentials:

```
EXEC sp_configure 'clr enabled' , '1';
RECONFIGURE;
```

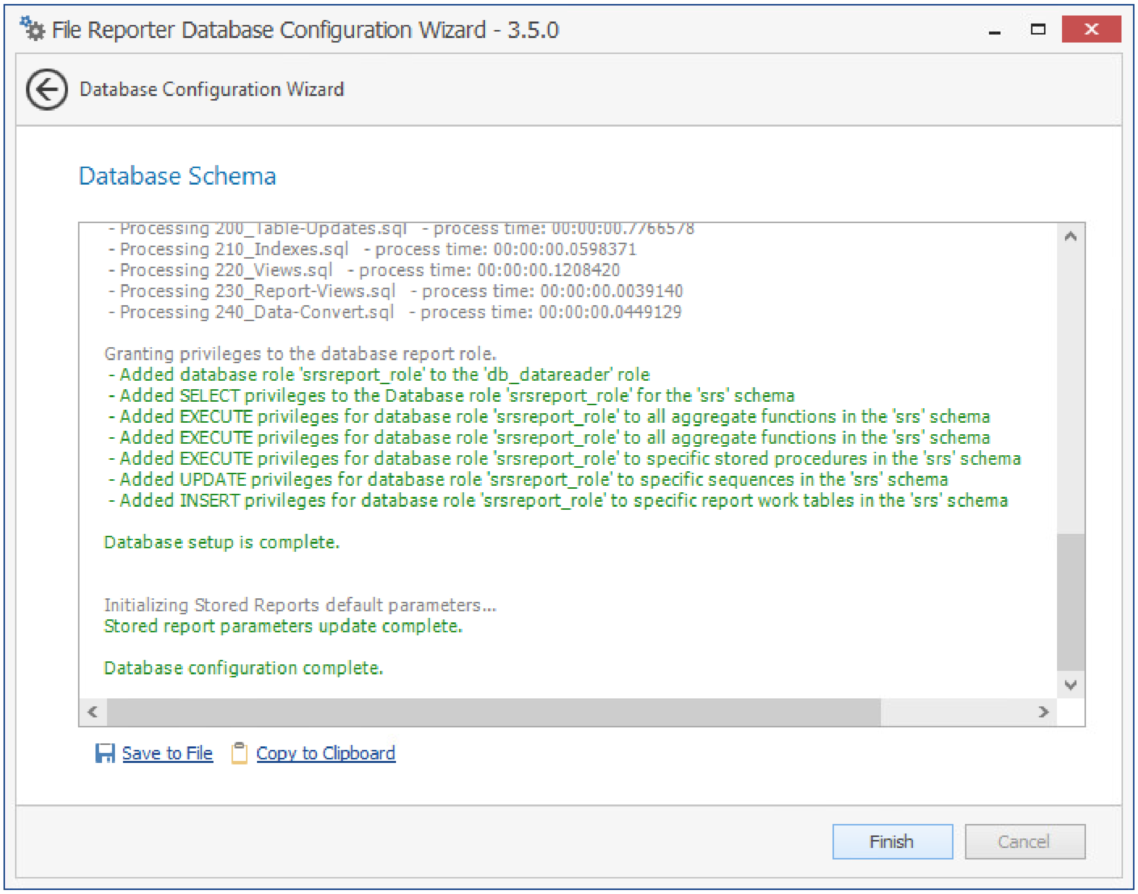
This feature is optional for this release, but may be required in future releases.

SQL Server CLR not enabled

☑ Install SQL Server .NET extensions

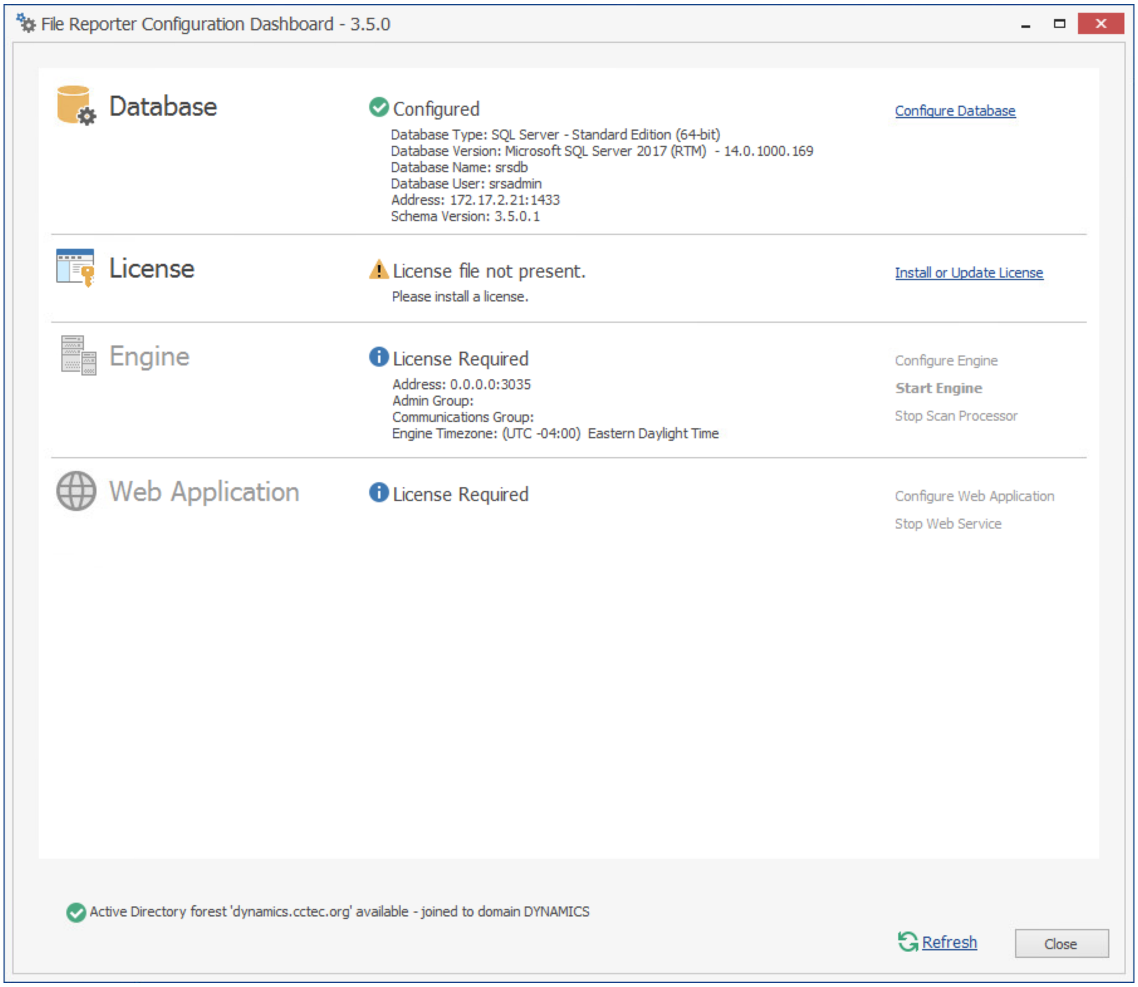
4 (Conditional) Click **Enable CLR**.

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


File Reporter Database Configuration Wizard - 3.5.0
Database Configuration Wizard
Database Schema

```
 - Processing 200_Table-Updates.sql   - process time: 00:00:00.7766578
 - Processing 210_Indexes.sql   - process time: 00:00:00.0598371
 - Processing 220_Views.sql   - process time: 00:00:00.1208420
 - Processing 230_Report-Views.sql   - process time: 00:00:00.0039140
 - Processing 240_Data-Convert.sql   - process time: 00:00:00.0449129

Granting privileges to the database report role.
 - Added database role 'srsreport_role' to the 'db_datareader' role
 - Added SELECT privileges to the Database role 'srsreport_role' for the 'srs' schema
 - Added EXECUTE privileges for database role 'srsreport_role' to all aggregate functions in the 'srs' schema
 - Added EXECUTE privileges for database role 'srsreport_role' to all aggregate functions in the 'srs' schema
 - Added EXECUTE privileges for database role 'srsreport_role' to specific stored procedures in the 'srs' schema
 - Added UPDATE privileges for database role 'srsreport_role' to specific sequences in the 'srs' schema
 - Added INSERT privileges for database role 'srsreport_role' to specific report work tables in the 'srs' schema

Database setup is complete.


Initializing Stored Reports default parameters...
Stored report parameters update complete.

Database configuration complete.
```

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



Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

License file not present.

Please install a license.

License Required

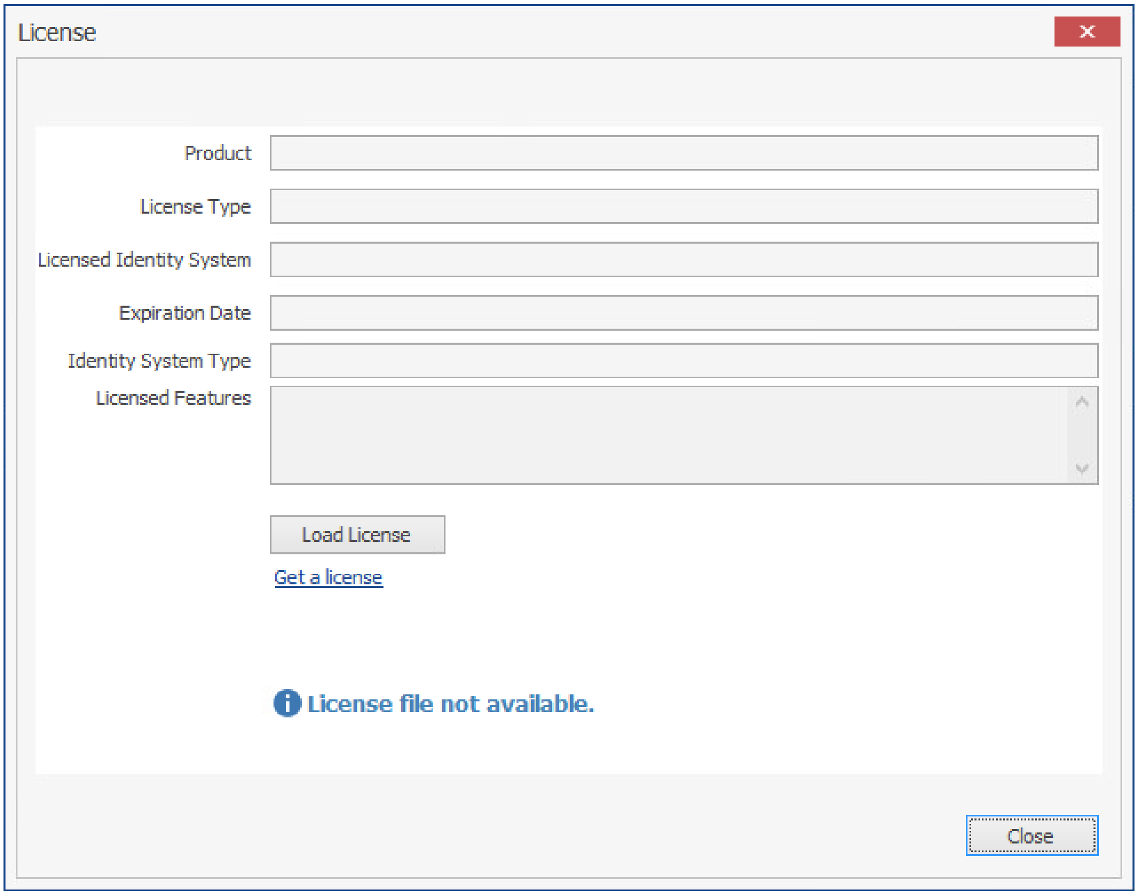
Address: 0.0.0.0:3035
Admin Group:
Communications Group:
Engine Timezone: (UTC -04:00) Eastern Daylight Time

License Required

Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

8.5 Installing the License

1 Click **Install or Update License**.



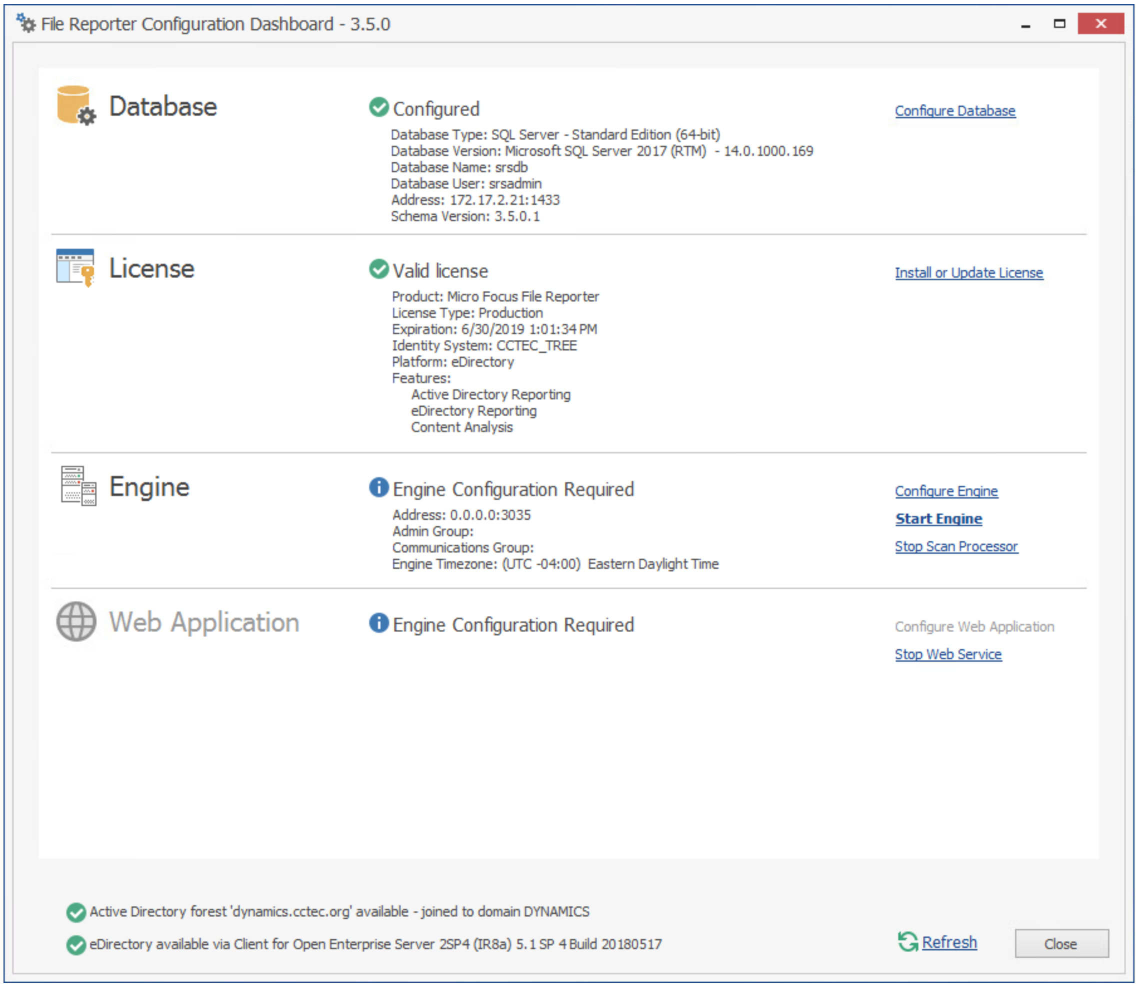
License file not available.

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

You must have a File Reporter license for eDirectory.

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

4 Click **Close**.



File Reporter Configuration Dashboard - 3.5.0

Database

✓ Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

Configure Database

License

✓ Valid license

Product: Micro Focus File Reporter
License Type: Production
Expiration: 6/30/2019 1:01:34 PM
Identity System: CCTEC_TREE
Platform: eDirectory
Features:
  Active Directory Reporting
  eDirectory Reporting
  Content Analysis

Install or Update License

Engine

Engine Configuration Required

Address: 0.0.0.0:3035
Admin Group:
Communications Group:
Engine Timezone: (UTC -04:00) Eastern Daylight Time

Configure Engine
Start Engine
Stop Scan Processor

Web Application

Engine Configuration Required

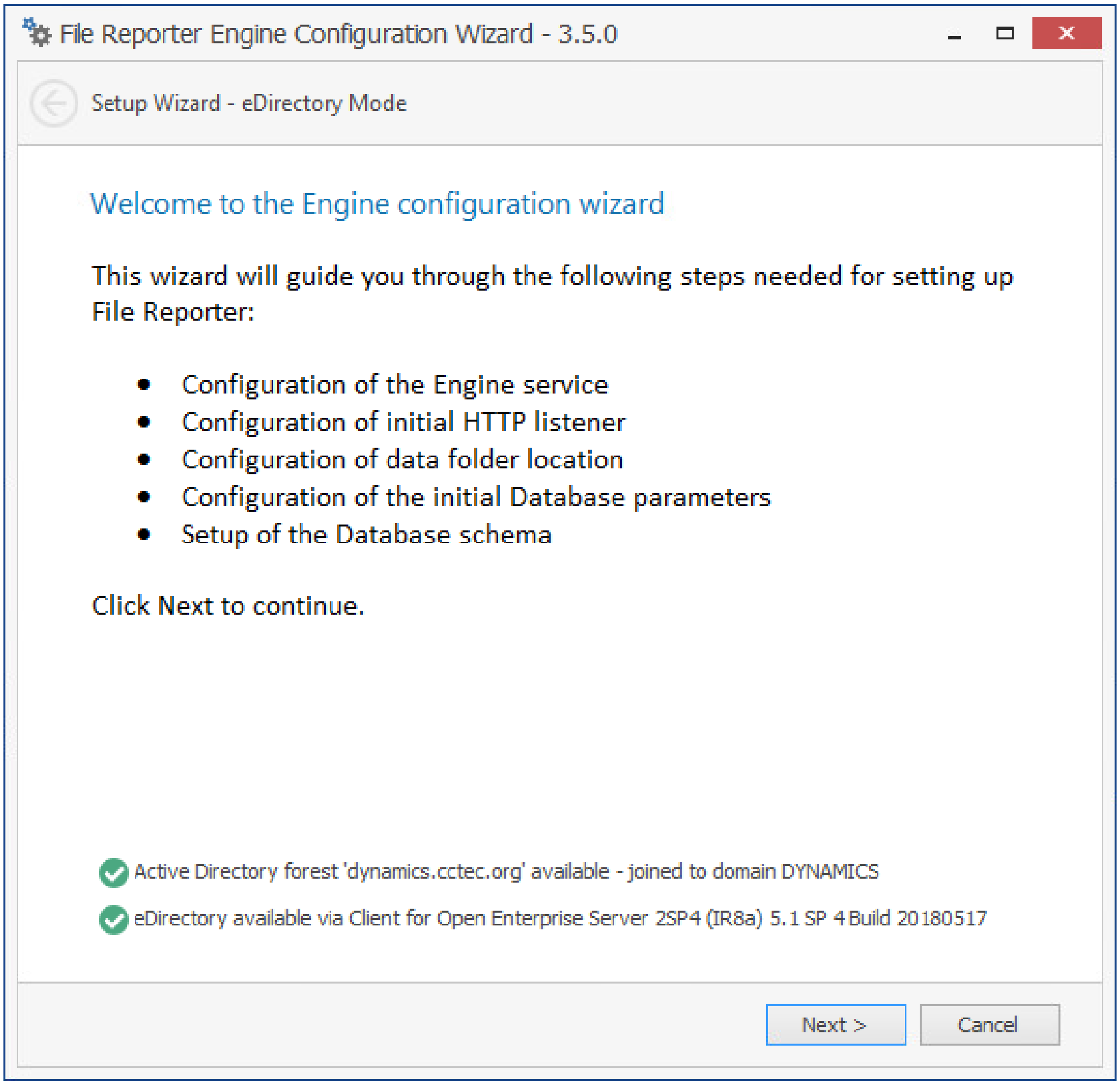
Configure Web Application
Stop Web Service

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

8.6 Configuring the Engine

1 Click **Configure Engine**.


File Reporter Engine Configuration Wizard - 3.5.0

Setup Wizard - eDirectory Mode

Welcome to the Engine configuration wizard

This wizard will guide you through the following steps needed for setting up File Reporter:

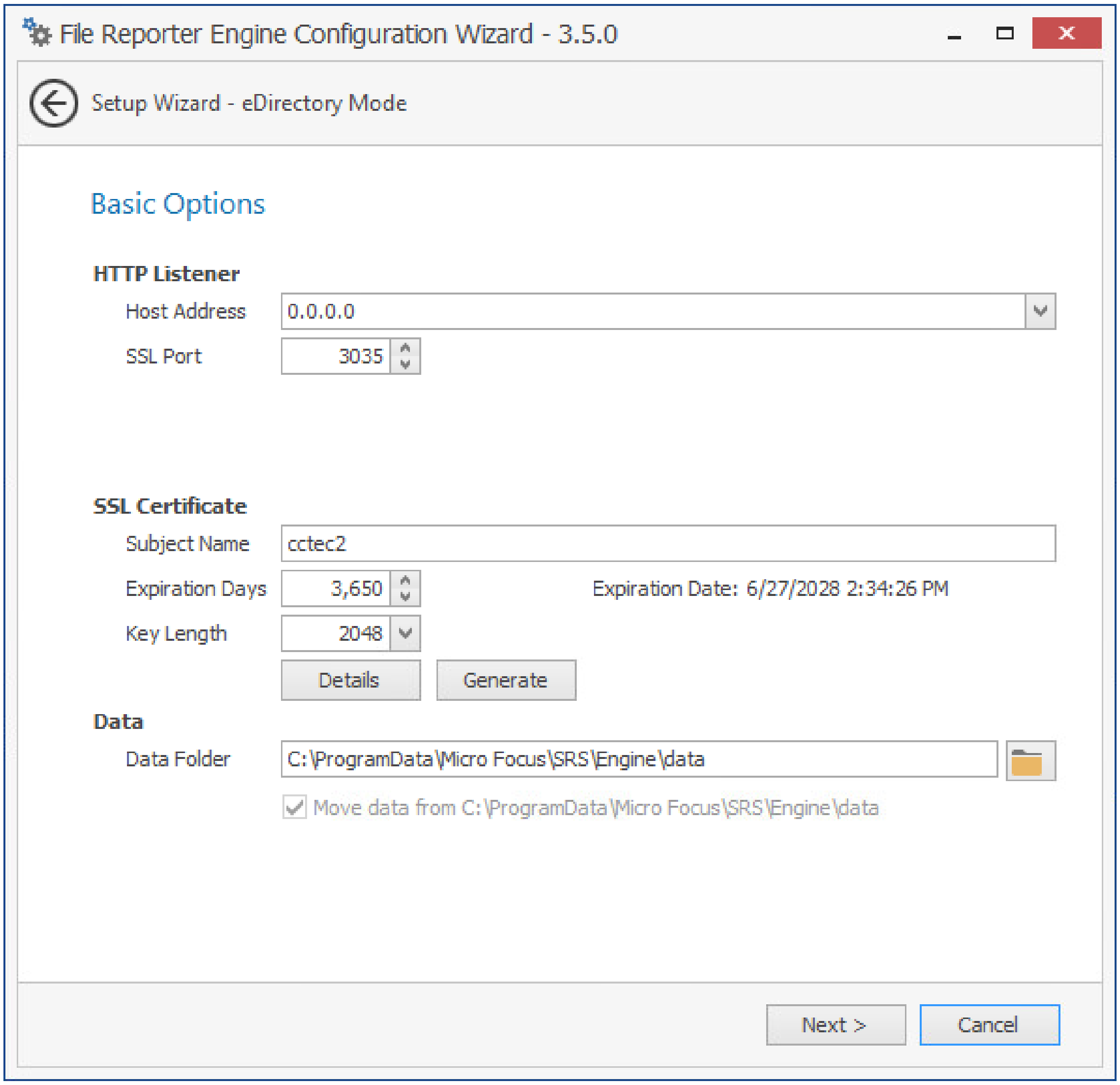
- Configuration of the Engine service
- Configuration of initial HTTP listener
- Configuration of data folder location
- Configuration of the initial Database parameters
- Setup of the Database schema

Click Next to continue.

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

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


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - eDirectory Mode
Basic Options

HTTP Listener

Host Address: 0.0.0.0

SSL Port: 3035

SSL Certificate

Subject Name: cctec2

Expiration Days: 3,650

Expiration Date: 6/27/2028 2:34:26 PM

Key Length: 2048

Data

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

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

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.

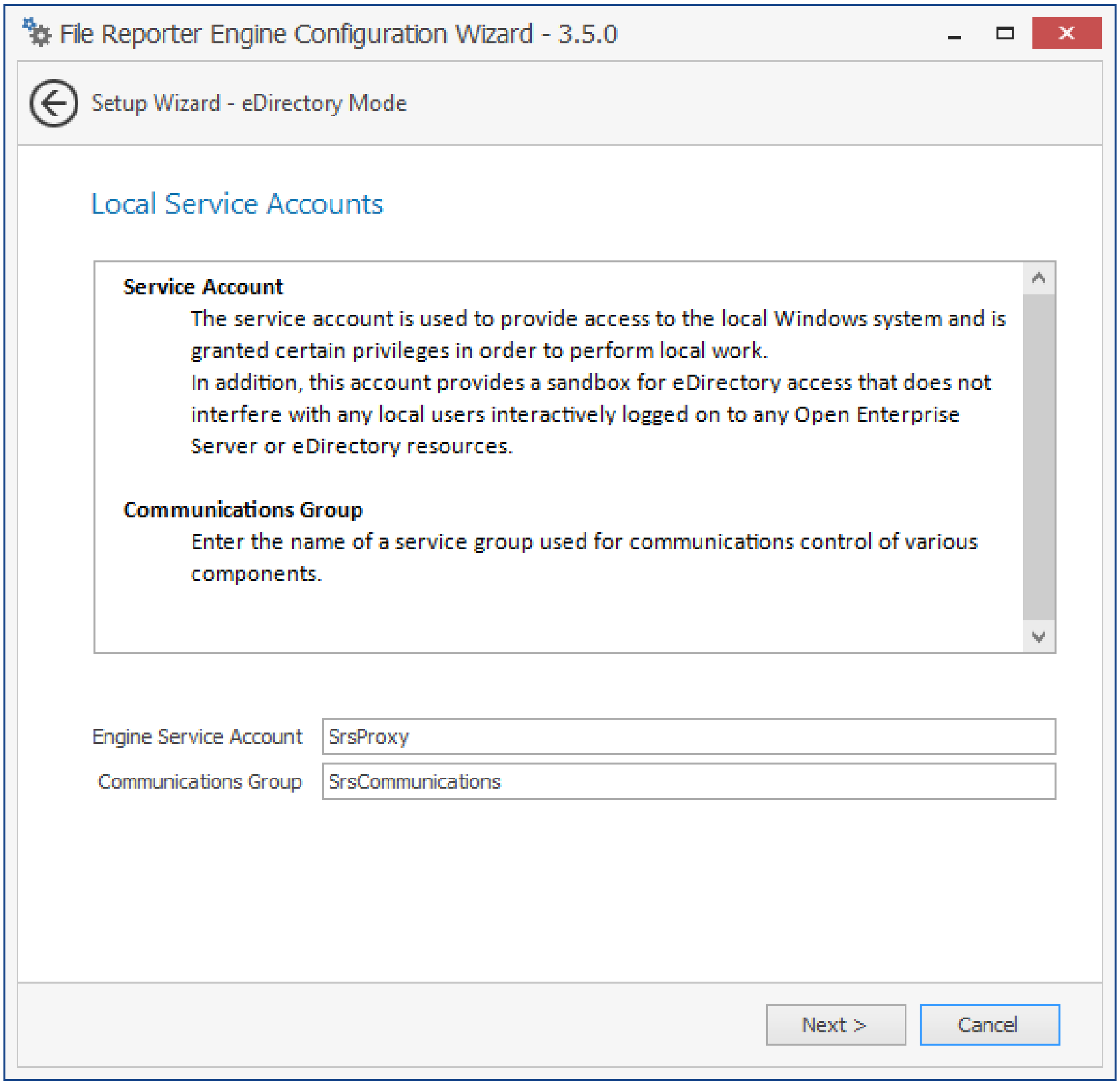
Generate: If you modify any of the settings in the SSL Certificate region, click this button to generate a new certificate.

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**.

If you have installed the Engine and Web Application on a server that is not in a domain, the following page appears:


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - eDirectory Mode

Local Service Accounts

Service Account

The service account is used to provide access to the local Windows system and is granted certain privileges in order to perform local work.

In addition, this account provides a sandbox for eDirectory access that does not interfere with any local users interactively logged on to any Open Enterprise Server or eDirectory resources.

Communications Group

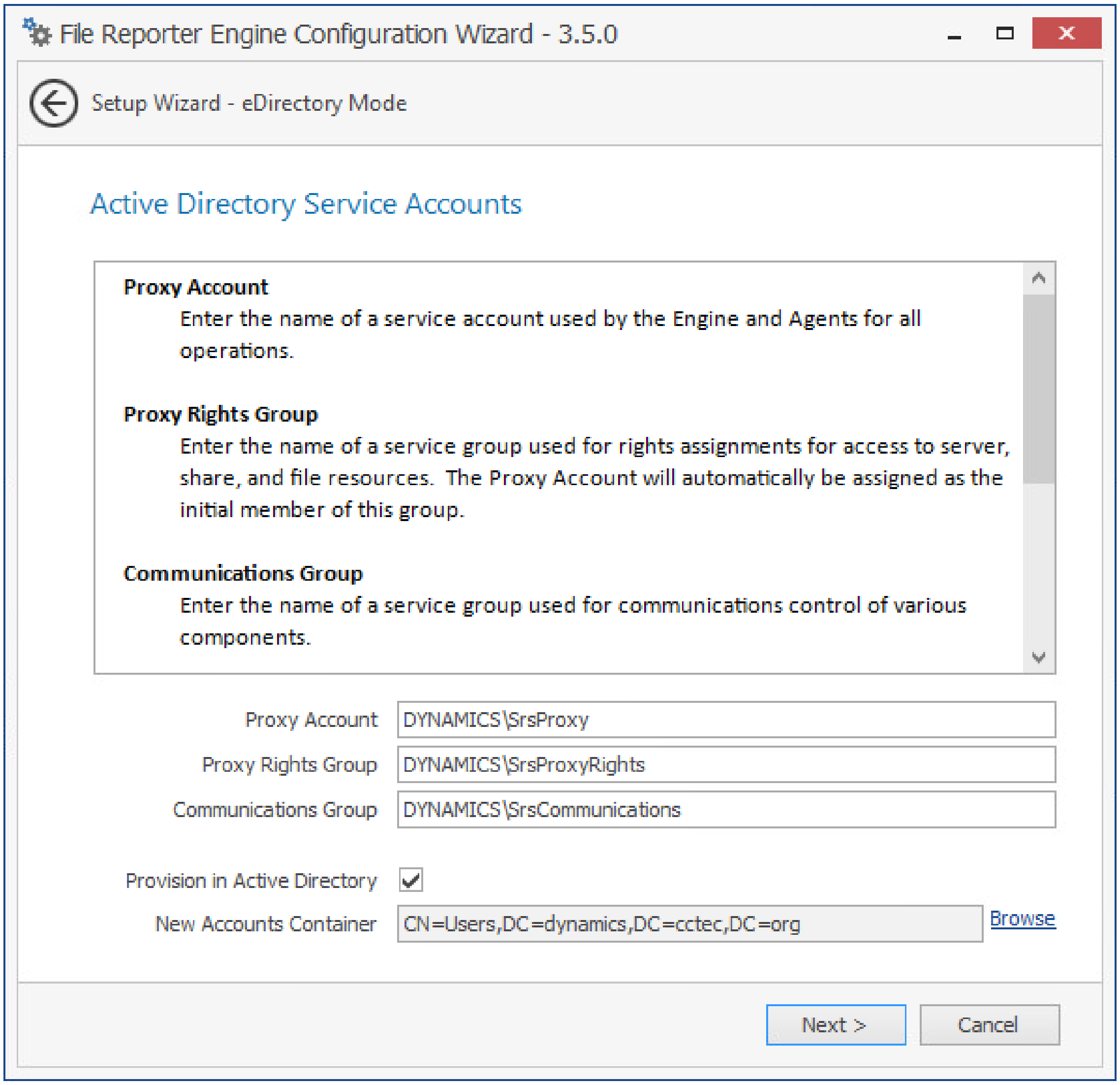
Enter the name of a service group used for communications control of various components.

Engine Service Account: SrsProxy

Communications Group: SrsCommunications

This page lets you establish a local service account.

If, in addition to being logged in to eDirectory as the primary identity system, you are logged into Active Directory, the following page appears:


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - eDirectory Mode

Active Directory Service Accounts

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

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

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

Proxy Account: DYNAMICS\SrsProxy

Proxy Rights Group: DYNAMICS\SrsProxyRights

Communications Group: DYNAMICS\SrsCommunications

Provision in Active Directory ☑

New Accounts Container: CN=Users,DC=dynamics,DC=cctec,DC=org

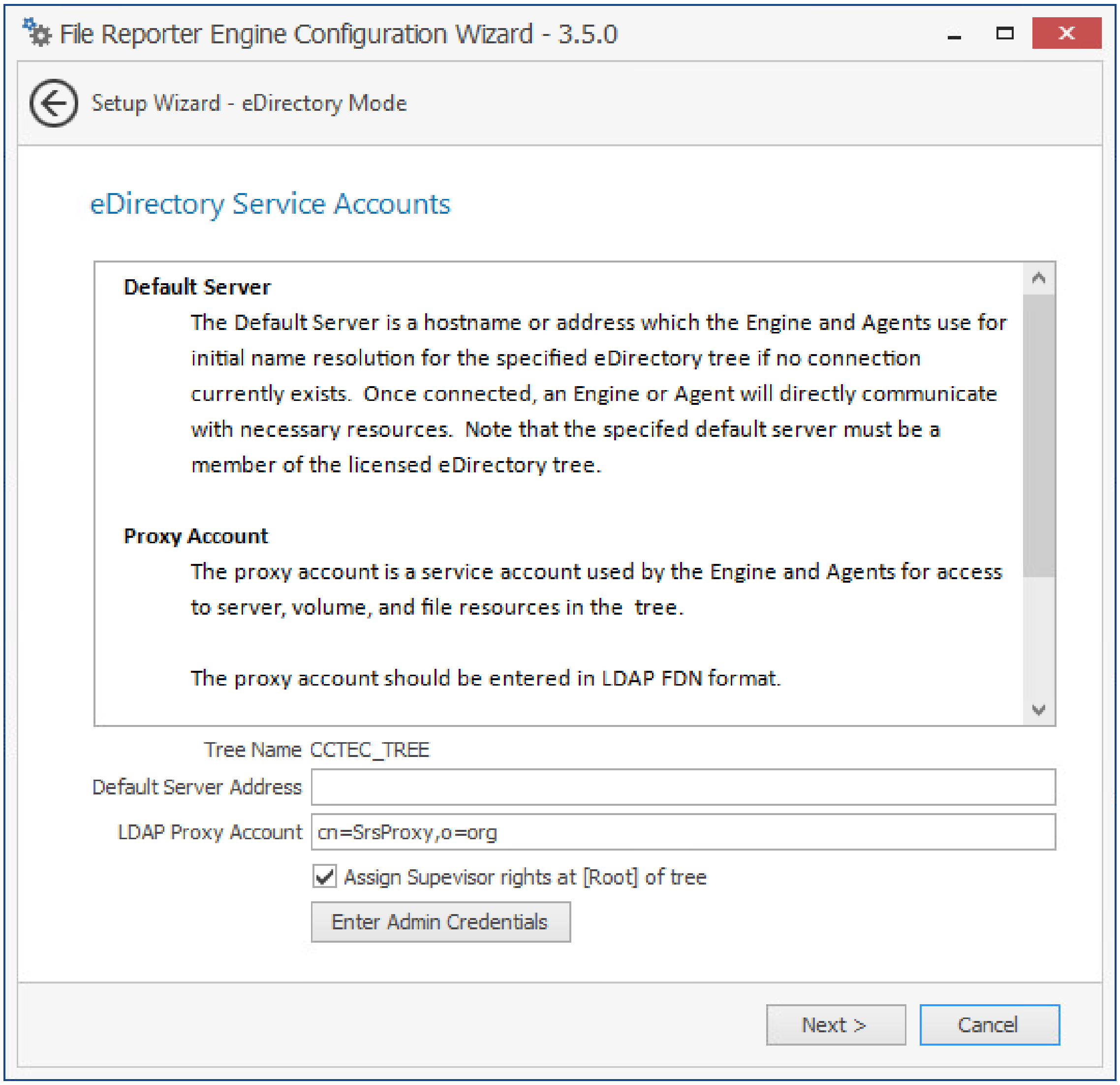
This page lets you establish a name for the proxy account, proxy rights group, and the communications group.

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 such as `nfrproxy` and `nfrproxyrights` respectively.

4 Click **Next**.


File Reporter Engine Configuration Wizard - 3.5.0

Setup Wizard - eDirectory Mode

eDirectory Service Accounts

Default Server

The Default Server is a hostname or address which the Engine and Agents use for initial name resolution for the specified eDirectory tree if no connection currently exists. Once connected, an Engine or Agent will directly communicate with necessary resources. Note that the specifed default server must be a member of the licensed eDirectory tree.

Proxy Account

The proxy account is a service account used by the Engine and Agents for access to server, volume, and file resources in the tree.

The proxy account should be entered in LDAP FDN format.

Tree Name CCTEC_TREE

Default Server Address

LDAP Proxy Account cn=SrsProxy,o=org

☑ Assign Supevisor rights at [Root] of tree

In this page, you create the eDirectory service accounts. These service accounts are needed to access the file system for the files that File Reporter reports on.

Tree Name: Displays the name of the eDirectory tree you are logged in to.

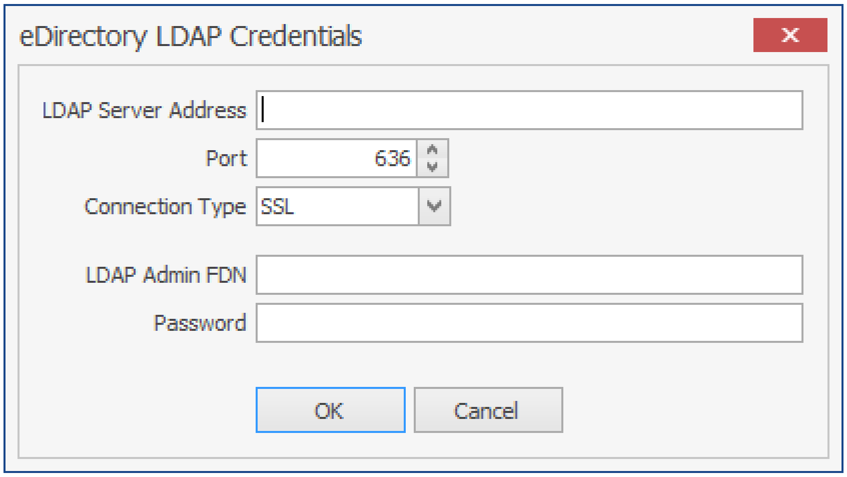
Default Server Address: Specify an IP address or DNS name to any server belonging to the eDirectory tree.

LDAP Proxy Account: Modify the typeful naming to correspond to your organizational structure.

For example, `cn=srsproxy,o=`*`system`*

Assign Supervisor rights at [Root] of tree: By default, the proxy account has Supervisor rights at the [Root] of the directory tree and can therefore report on any network volume. If this option is not selected, File Reporter can only report on volumes where the proxy account is assigned rights.

Enter Admin Credentials: Click this button to access the following dialog box:



Port 636

Connection Type SSL

LDAP Server Address: Specify an IP address to any server belonging to the eDirectory tree.

Port: Unless there is a conflict, leave the port setting at 636.

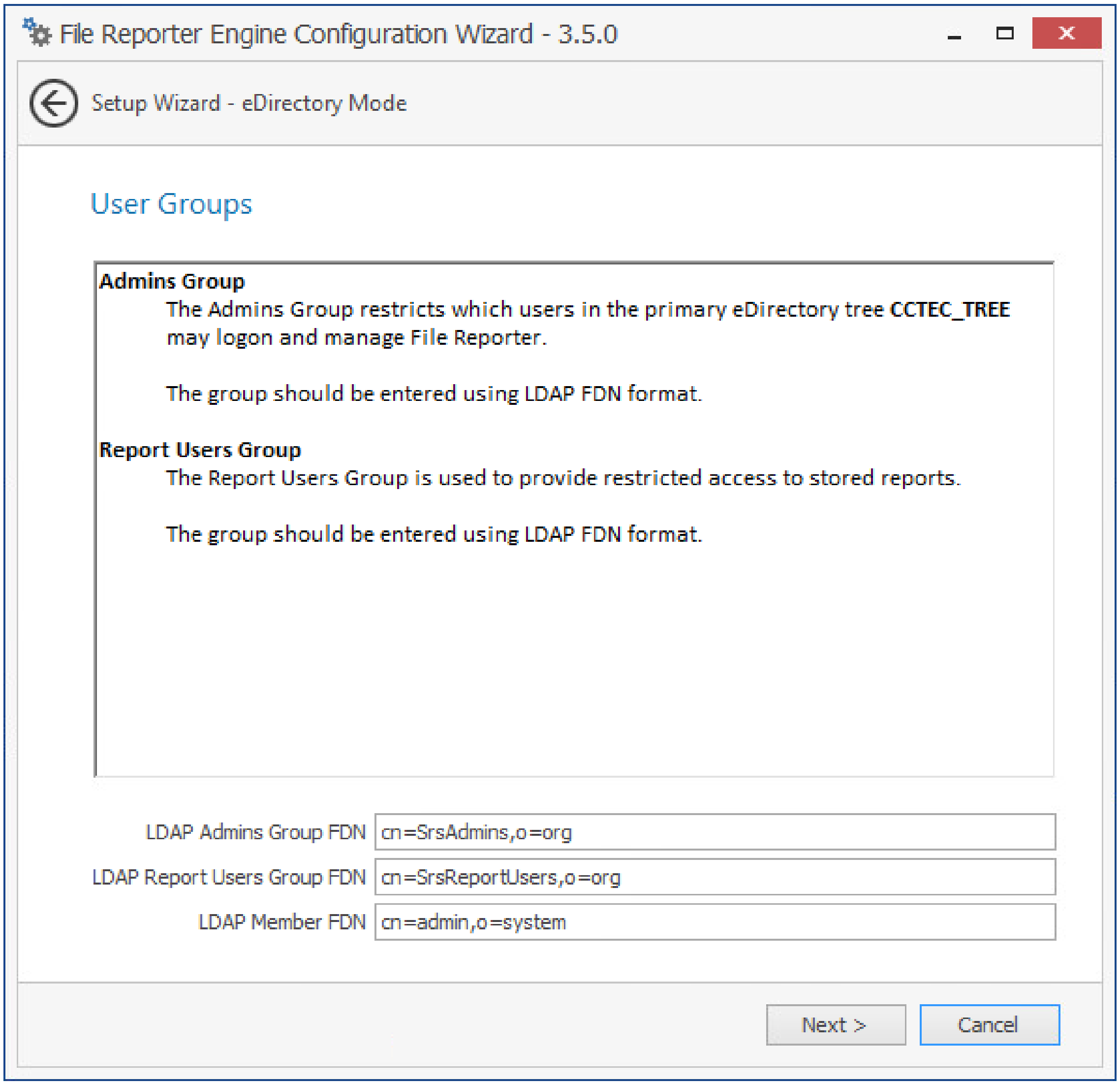
Connection Type: Verify that the setting is **SSL**.

LDAP Admin FDN: Specify the fully distinguished LDAP name for an administrator.

For example: `cn=admin,o=`*`system`*

Password: Specify the password for the administrator.

5 Specify the default server address, LDAP proxy account, and eDirectory LDAP credentials and click **Next**.


File Reporter Engine Configuration Wizard - 3.5.0
Setup Wizard - eDirectory Mode

User Groups

Admins Group

The Admins Group restricts which users in the primary eDirectory tree **CCTEC_TREE** may logon and manage File Reporter.

The group should be entered using LDAP FDN format.

Report Users Group

The Report Users Group is used to provide restricted access to stored reports.

The group should be entered using LDAP FDN format.

LDAP Admins Group FDN: cn=SrsAdmins,o=org

LDAP Report Users Group FDN: cn=SrsReportUsers,o=org

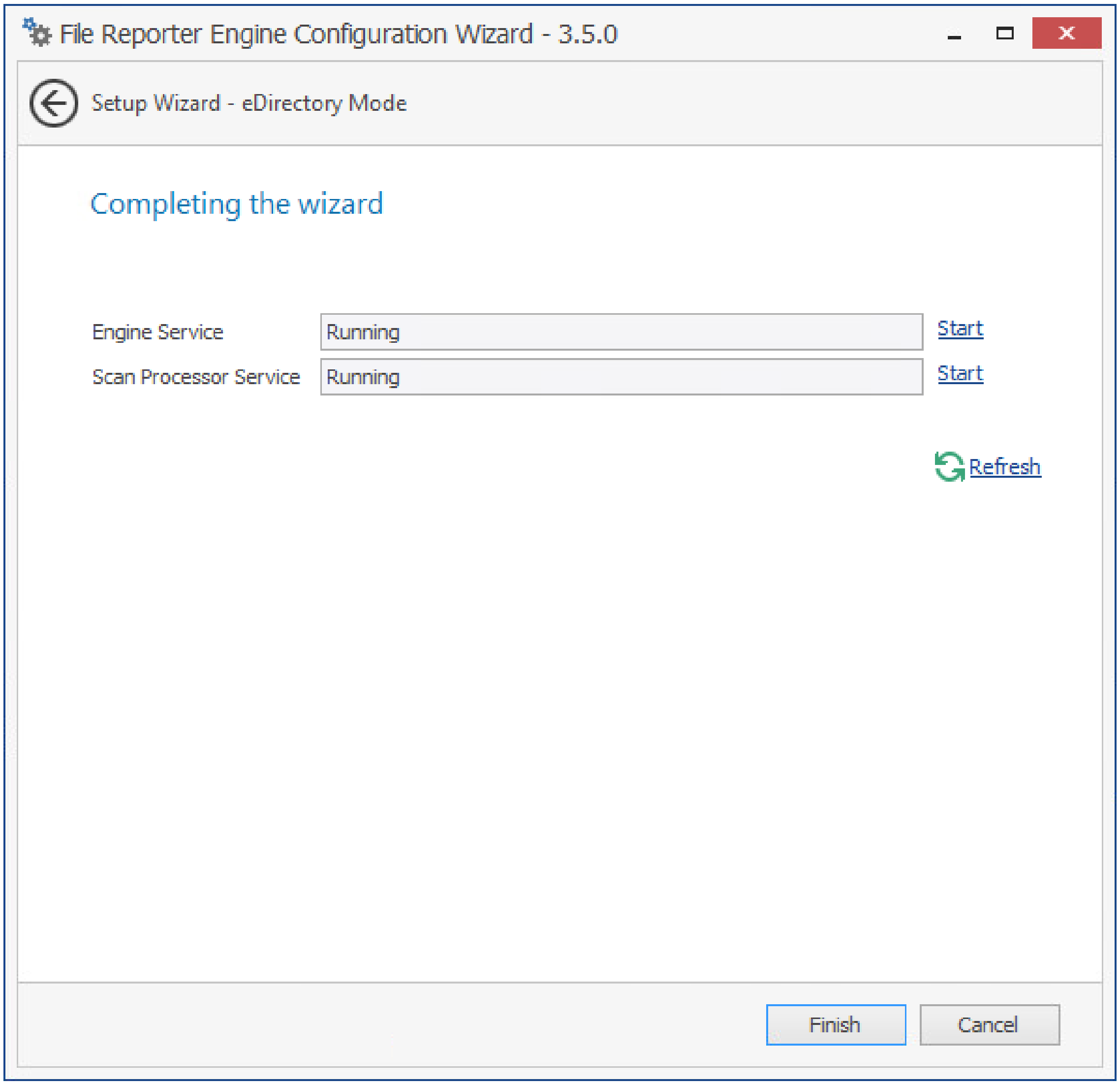
LDAP Member FDN: cn=admin,o=system

LDAP Admins Group FDN: Based on your organizational structure, modify the path for an admins group that File Reporter will create with LDAP fully distinguished naming.

LDAP Report Users Group FDN: Based on your organizational structure, modify the path for an report users group that File Reporter will create with LDAP fully distinguished naming.

LDAP Member FDN: Specify the LDAP fully distinguished name of an administrator.

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



File Reporter Engine Configuration Wizard - 3.5.0

Setup Wizard - eDirectory Mode

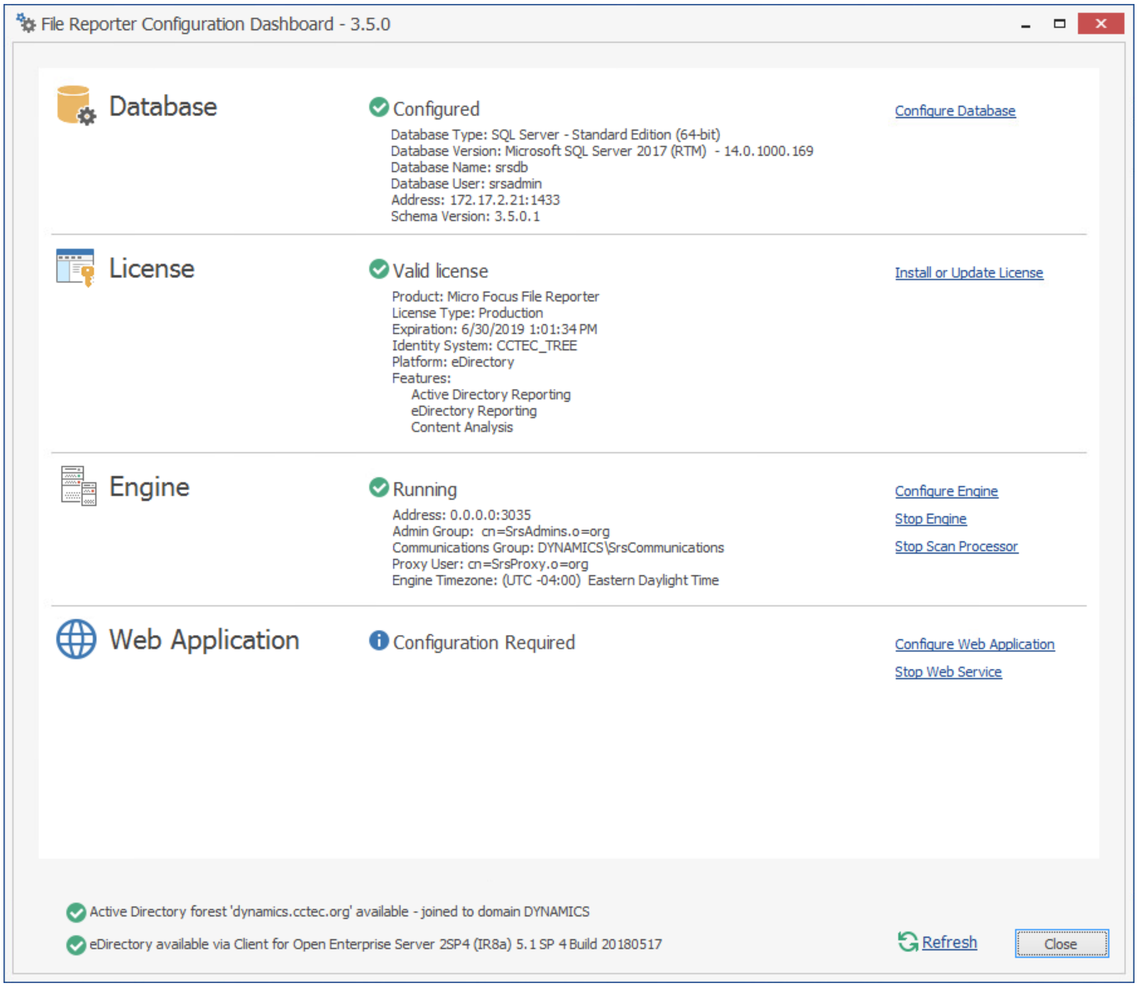
Completing the wizard

Engine Service: Running

Scan Processor Service: Running

7 Click **Finish**.

The Engine is now installed, configured, and running.



File Reporter Configuration Dashboard - 3.5.0

Database — ✓ Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

License — ✓ Valid license

Product: Micro Focus File Reporter
License Type: Production
Expiration: 6/30/2019 1:01:34 PM
Identity System: CCTEC_TREE
Platform: eDirectory
Features:
Active Directory Reporting
eDirectory Reporting
Content Analysis

Engine — ✓ Running

Address: 0.0.0.0:3035
Admin Group: cn=SrsAdmins.o=org
Communications Group: DYNAMICS\SrsCommunications
Proxy User: cn=SrsProxy.o=org
Engine Timezone: (UTC -04:00) Eastern Daylight Time

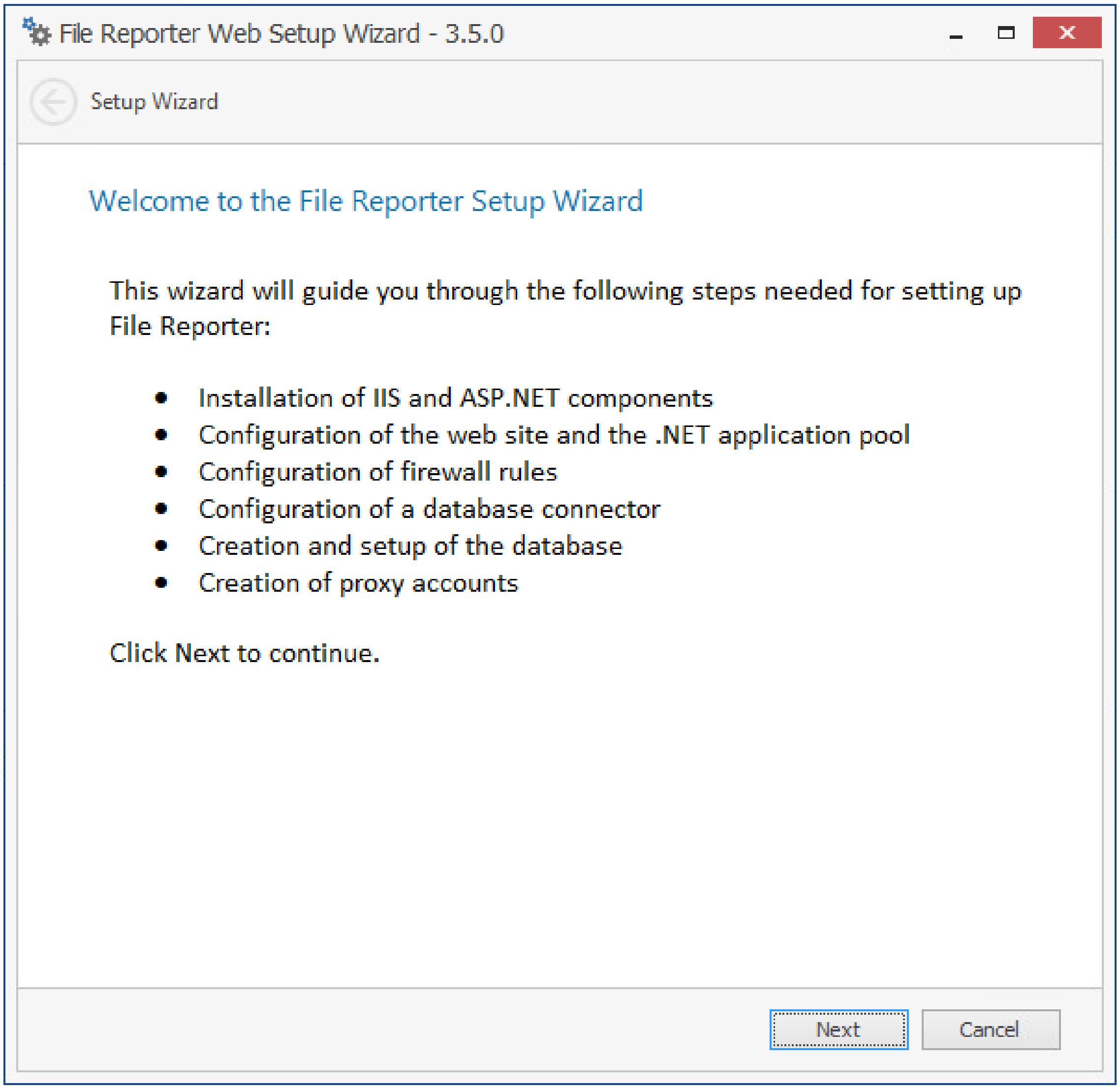
Web Application — Configuration Required

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

8.7 Configuring the Web Application

1 Click **Configure Web Application**.



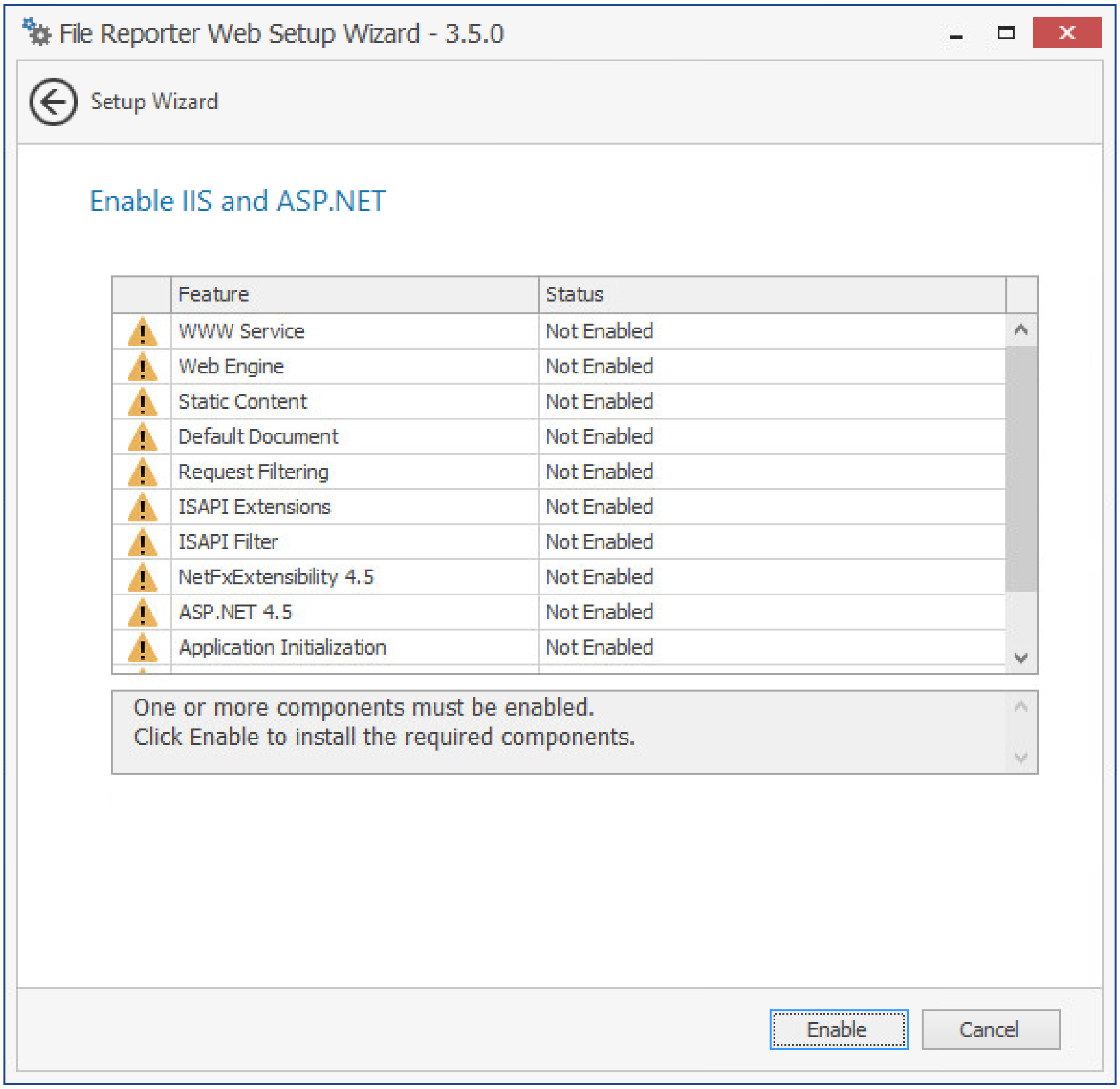
Welcome to the File Reporter Setup Wizard

This wizard will guide you through the following steps needed for setting up File Reporter:

- Installation of IIS and ASP.NET components
- Configuration of the web site and the .NET application pool
- Configuration of firewall rules
- Configuration of a database connector
- Creation and setup of the database
- Creation of proxy accounts

Click Next to continue.

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

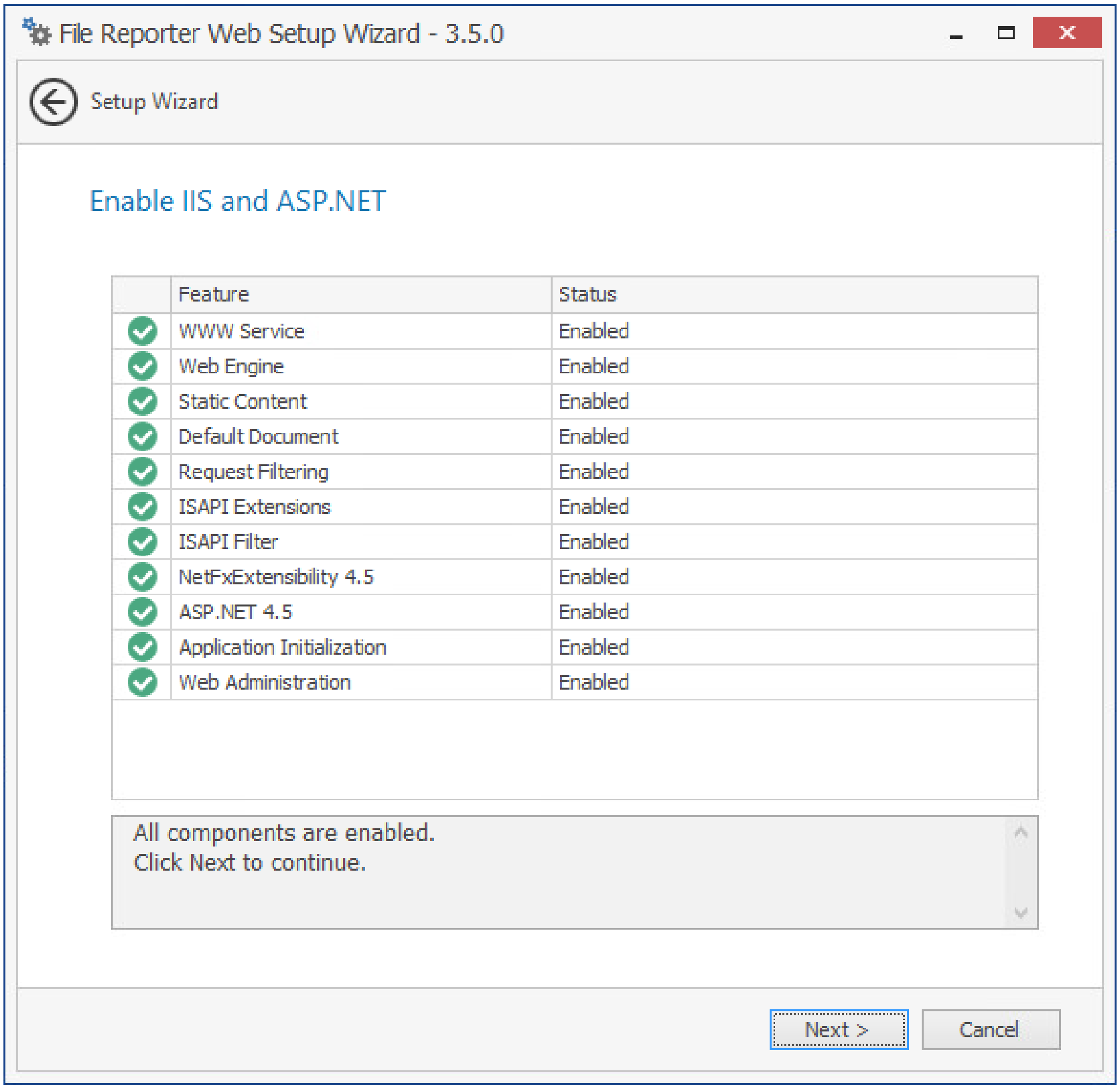


Enable IIS and ASP.NET

	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

One or more components must be enabled.
Click Enable to install the required components.

3 Click **Enable**.

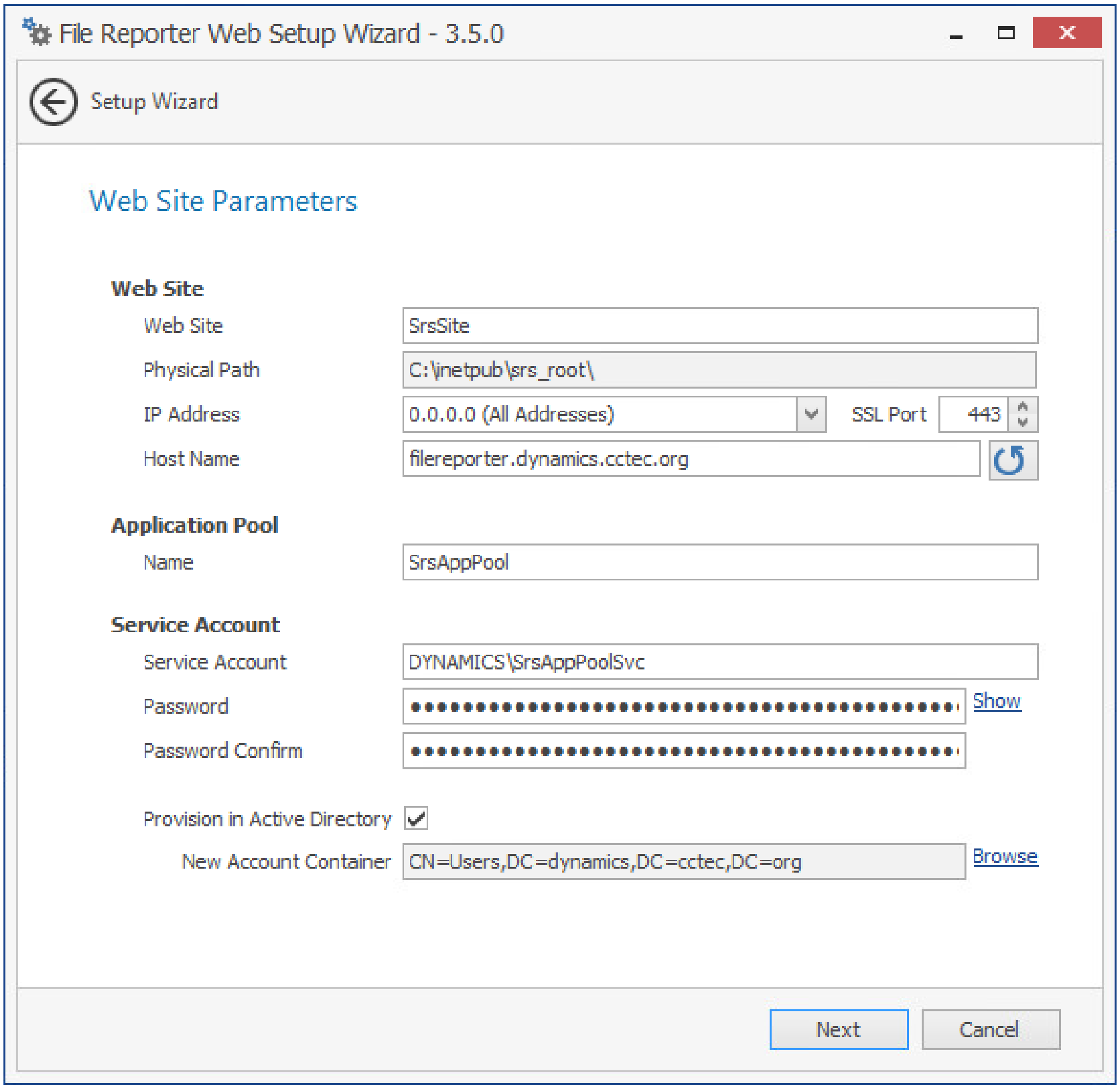


Enable IIS and ASP.NET

	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.

4 Click **Next**.



Web Site Parameters

Web Site

Web Site: SrsSite

Physical Path: C:\inetpub\srs_root\

IP Address: 0.0.0.0 (All Addresses) SSL Port: 443

Host Name: filereporter.dynamics.cctec.org

Application Pool

Name: SrsAppPool

Service Account

Service Account: DYNAMICS\SrsAppPoolSvc

Password: •• Show

Password Confirm: ••

Provision in Active Directory ☑

New Account Container: CN=Users,DC=dynamics,DC=cctec,DC=org Browse

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

Web Site: Settings for the Microsoft IIS Web site.

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

Physical Path: This path was specified in Step 5 on page 41 and is the location where files on the Web site are served up. You cannot edit this path.

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

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

Host Name: The host name as defined in DNS that you specified in Section 8.2, "Prerequisites," on page 66.

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.

Managed Pipeline Mode: Microsoft IIS 7 and later uses the Integrated managed pipeline mode, meaning that requests are handled through a unified pipeline, rather than the classic mode in IIS 6 that utilized two pipelines.

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

Password: The password is automatically generated.

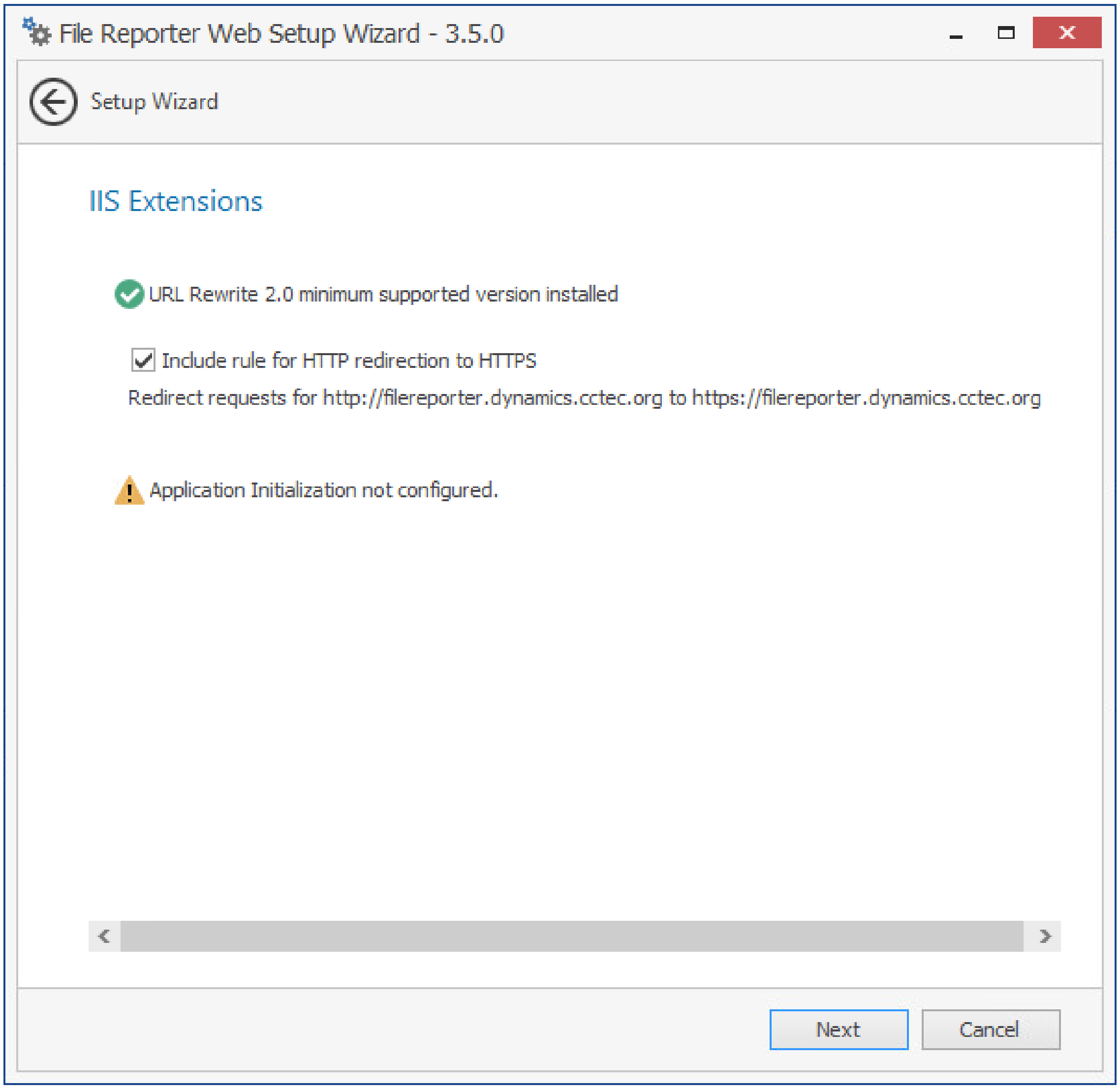
Confirm Password: The automatically generated password is repeated.

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**.



URL Rewrite 2.0 minimum supported version installed

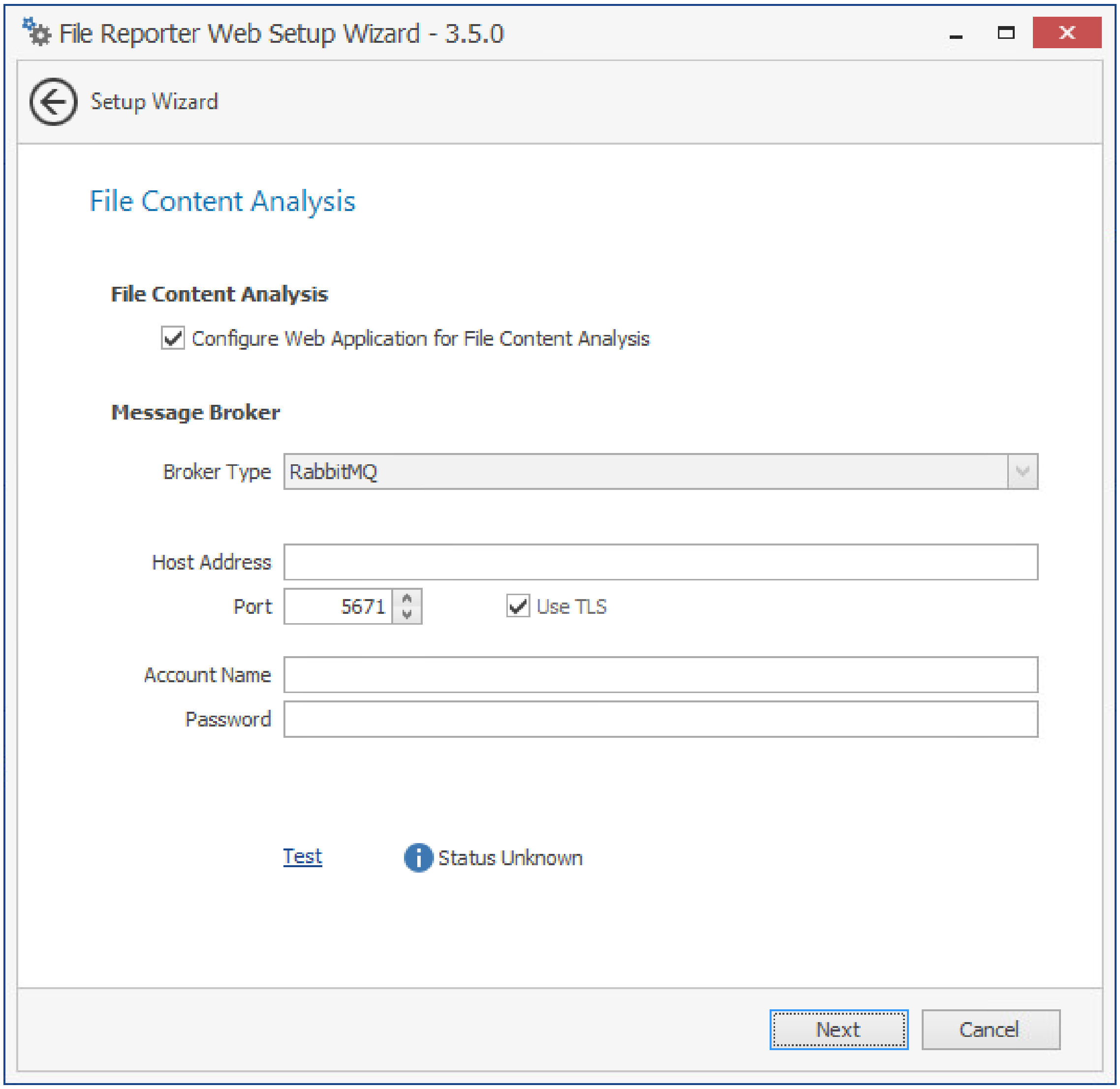
☑ Include rule for HTTP redirection to HTTPS

Redirect requests for http://filereporter.dynamics.cctec.org to https://filereporter.dynamics.cctec.org

Application Initialization not configured.

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

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



File Content Analysis

File Content Analysis

☑ Configure Web Application for File Content Analysis

Message Broker

Broker Type: RabbitMQ

Host Address:

Port: 5671 ☑ Use TLS

Account Name:

Password:

Test Status Unknown

Configure Web Application for File Content Analysis: If you are not set up for File Content scanning or your message broker is not yet configured, deselect this check box. Deselecting this allows you to skip the File Content Analysis step as well as the following File Content Search Results step.

For example, if you are upgrading from File Reporter 3.0.x and do not yet want to utilize file content scanning, you can select this option to proceed with the upgrade.

Message Broker: Fields specific to the messaging broker.

Broker Type: Displays the RabbitMQ messaging broker.

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

Port: Change the port setting to 5671.

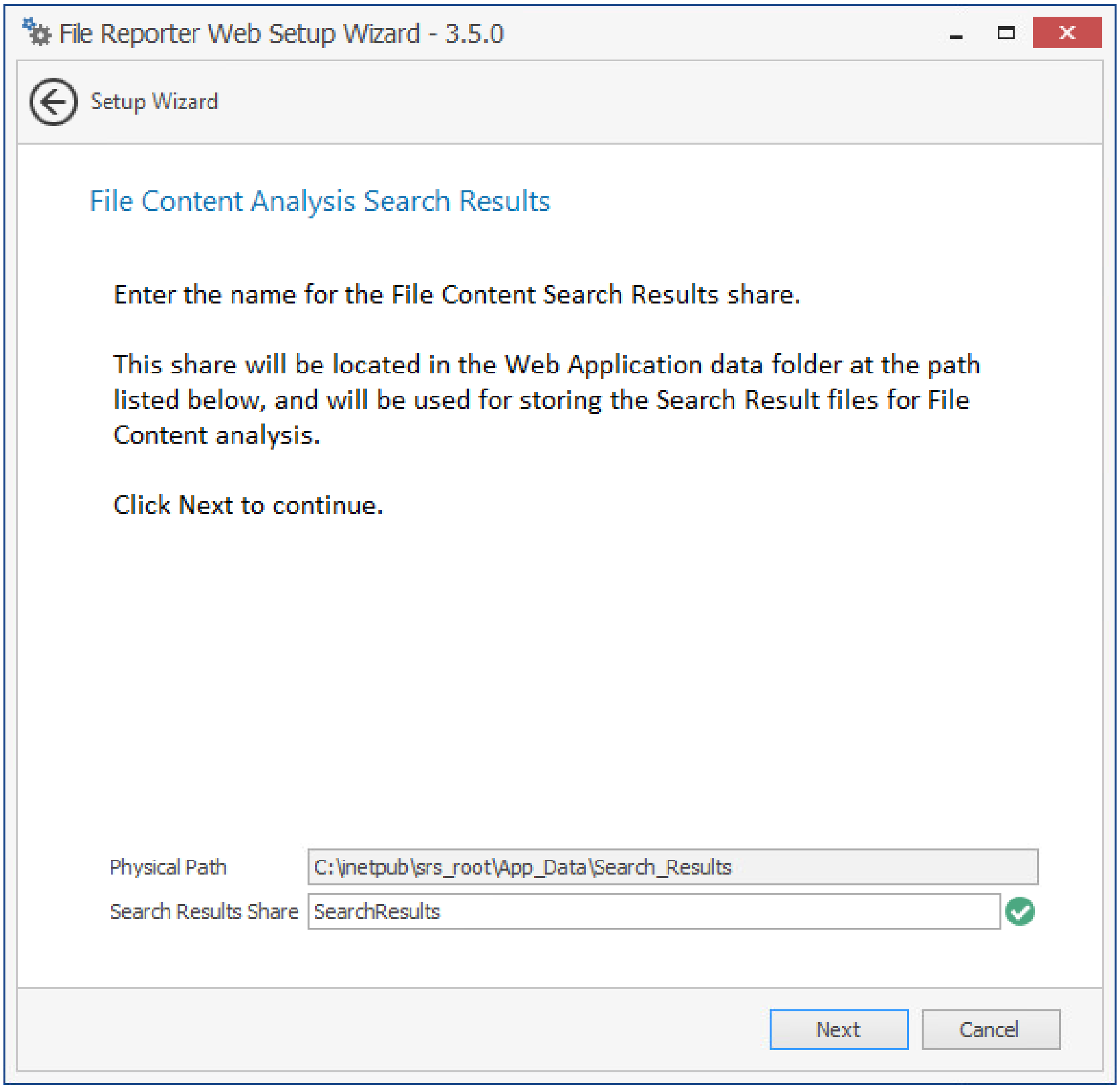
Use TLS: The RabbitMQ messaging broker in File Reporter utilizes Transport Layer Security (TLS) as the cryptographic communications security protocol.

Account Name: Enter `admin`.

Password: Enter the updated password that you changed in Section 6.4, “Changing the Default Password,” on page 36.

Test: Click to test the connection between the Web App and the RabbitMQ messaging broker.

8 Enter the communications settings for communication with the RabbitMQ messaging broker and click **Next**.



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.

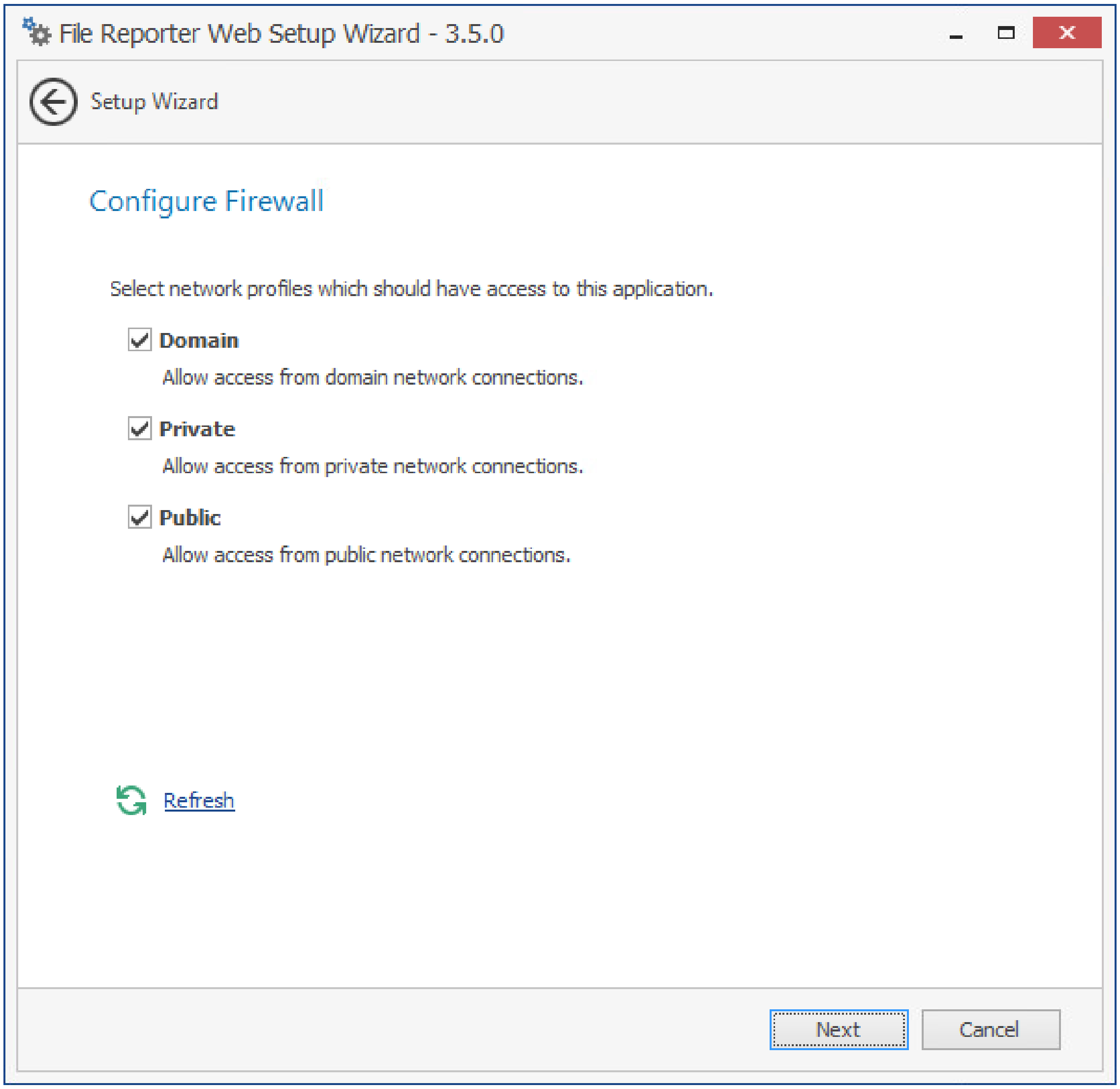
Click Next to continue.

Physical Path: C:\inetpub\srs_root\App_Data\Search_Results

Search Results Share: SearchResults ✓

This page lets you specify the physical path where content search results are stored.

9 Click **Next**.



Configure Firewall

Select network profiles which should have access to this application.

☑ **Domain**
Allow access from domain network connections.

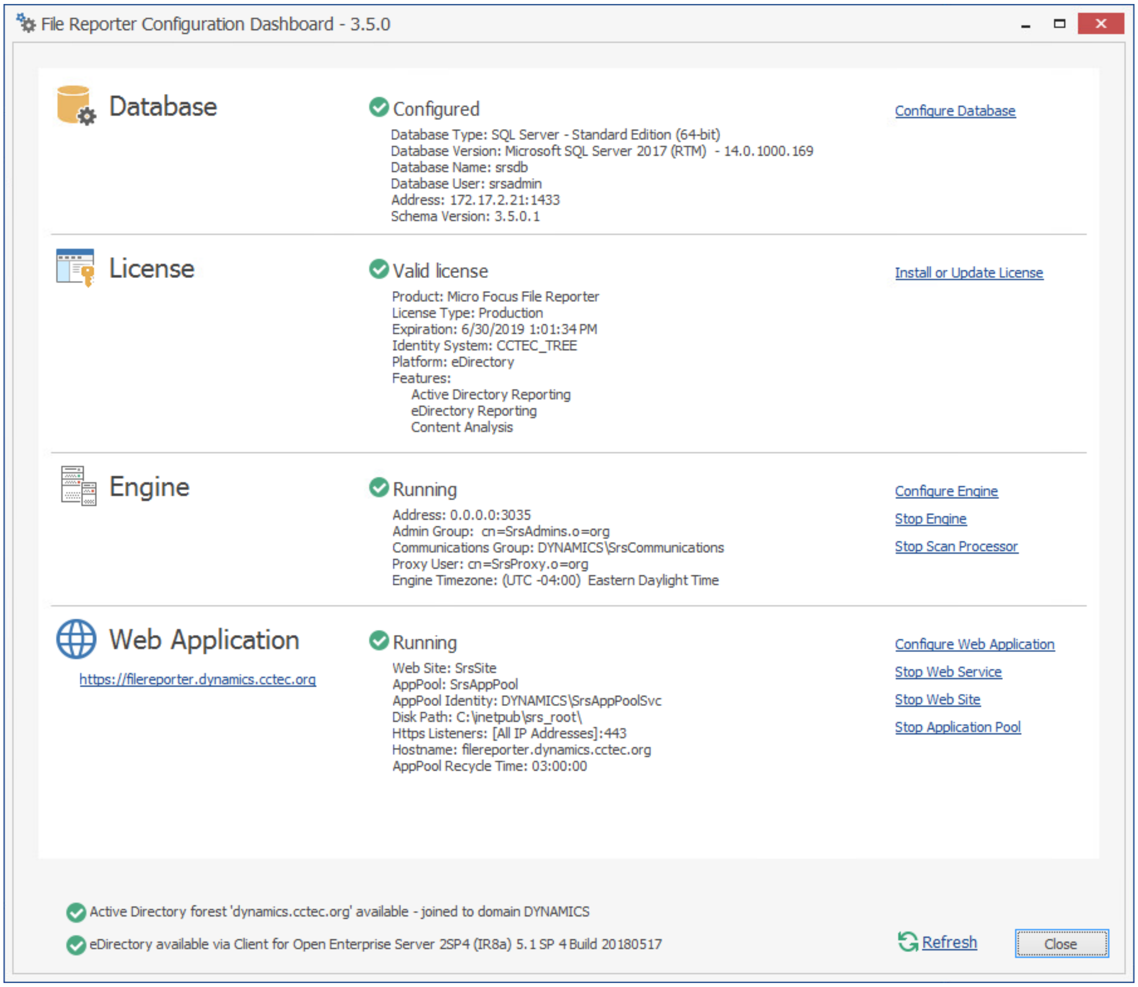
☑ **Private**
Allow access from private network connections.

☑ **Public**
Allow access from public network connections.

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

11 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.



Database

✓ Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

License

✓ Valid license

Product: Micro Focus File Reporter
License Type: Production
Expiration: 6/30/2019 1:01:34 PM
Identity System: CCTEC_TREE
Platform: eDirectory
Features:
Active Directory Reporting
eDirectory Reporting
Content Analysis

Engine

✓ Running

Address: 0.0.0.0:3035
Admin Group: cn=SrsAdmins.o=org
Communications Group: DYNAMICS\SrsCommunications
Proxy User: cn=SrsProxy.o=org
Engine Timezone: (UTC -04:00) Eastern Daylight Time

Web Application

https://filereporter.dynamics.cctec.org

✓ Running

Web Site: SrsSite
AppPool: SrsAppPool
AppPool Identity: DYNAMICS\SrsAppPoolSvc
Disk Path: C:\inetpub\srs_root\
Https Listeners: [All IP Addresses]:443
Hostname: filereporter.dynamics.cctec.org
AppPool Recycle Time: 03:00:00

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2SP4 (IR8a) 5.1 SP 4 Build 20180517

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

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

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

9 Install ManagerFC

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

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

ManagerFC requires .NET Framework 4.7.2, which is installed automatically if it is not already present.

9.1 Minimum Requirements

The ManagerFC host must meet the following minimum requirements:

Server Platform

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

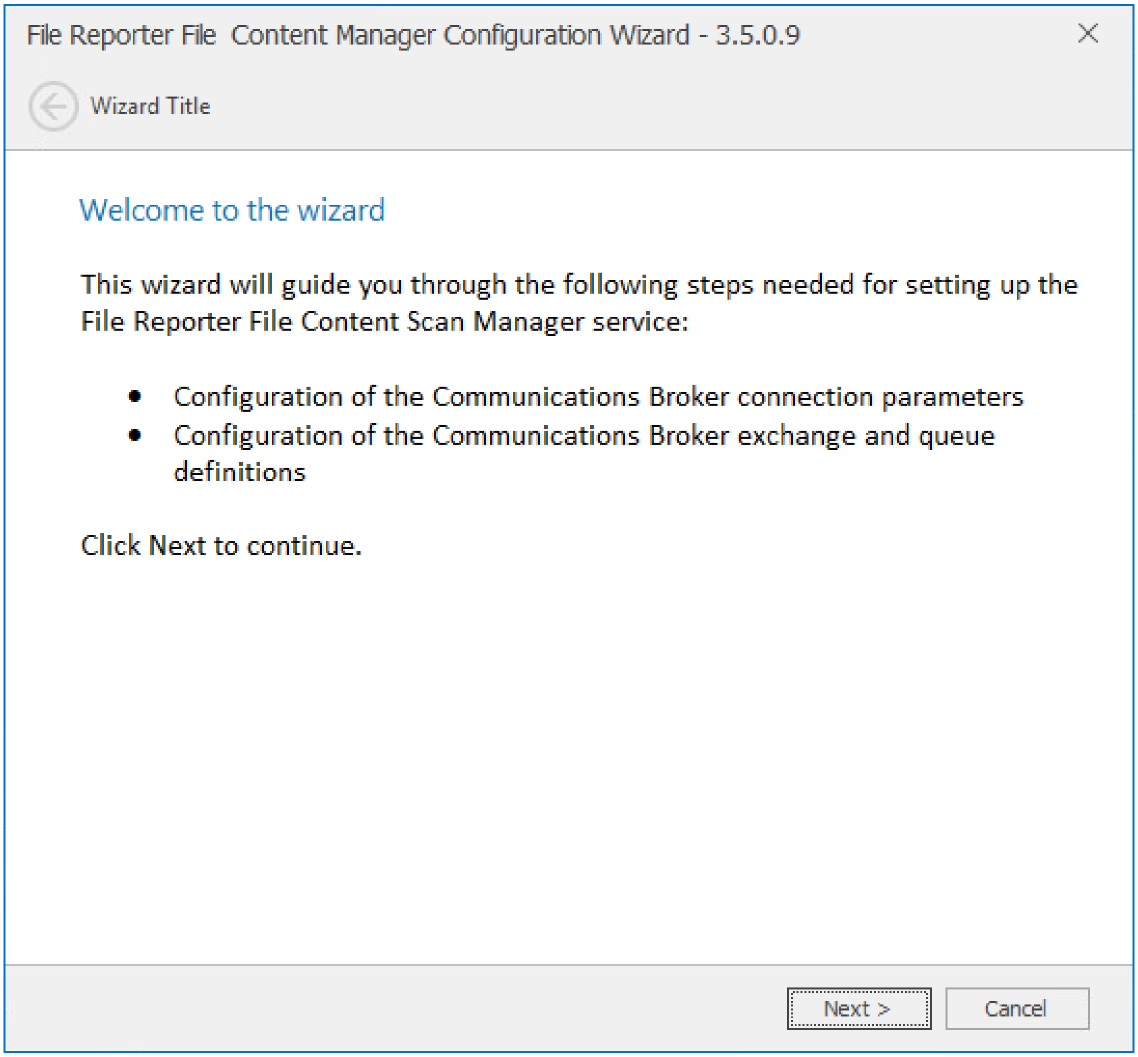
Minimum Hardware Requirements

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

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

9.2 Installing ManagerFC

1. At the root of the `FileReporter_3.6.0.iso` image, double-click `FileReporter-ManagerFC-3.6.0-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**.



File Reporter File Content Manager Configuration Wizard - 3.5.0.9
Wizard Title

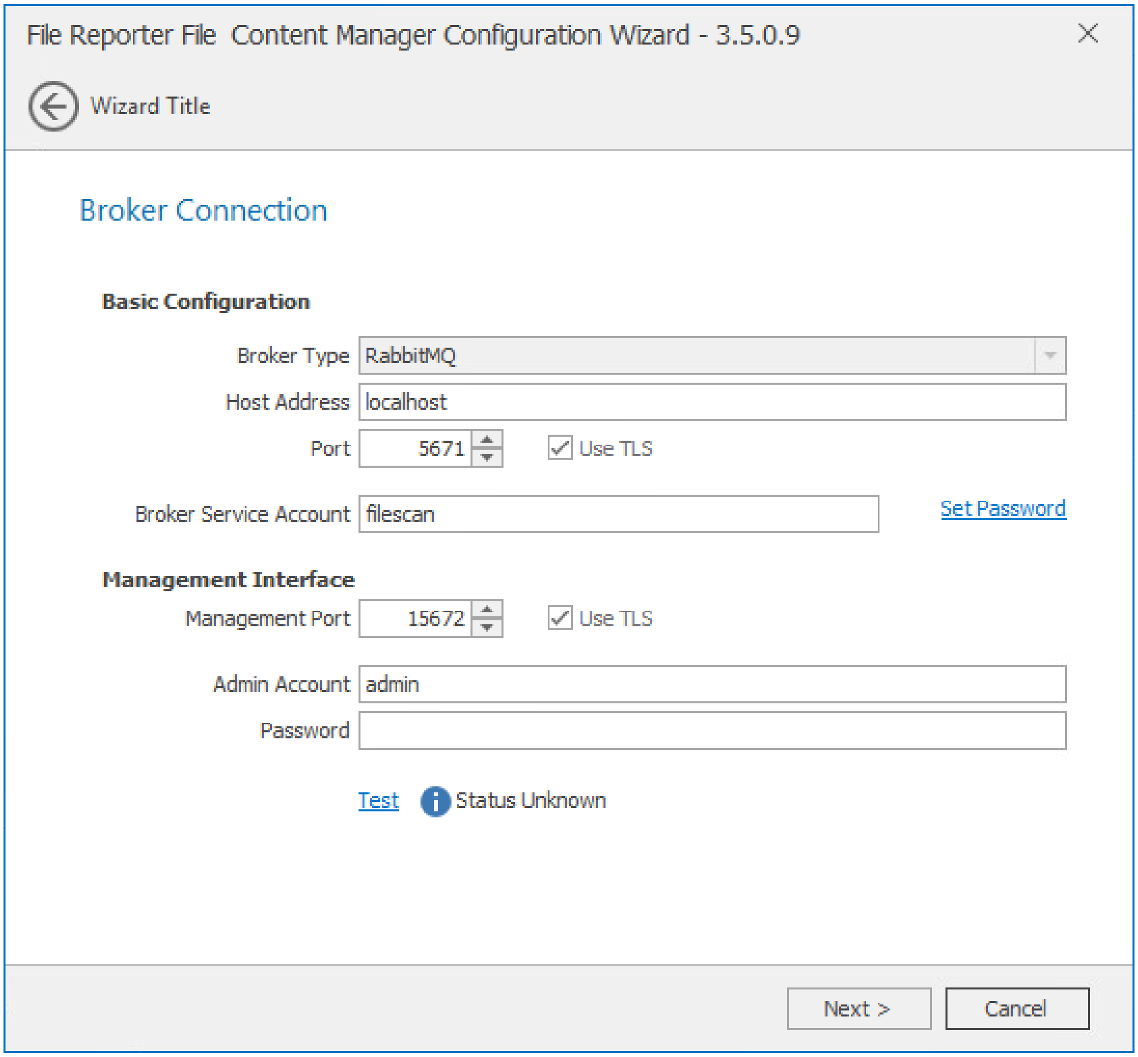
Welcome to the wizard

This wizard will guide you through the following steps needed for setting up the File Reporter File Content Scan Manager service:

- Configuration of the Communications Broker connection parameters
- Configuration of the Communications Broker exchange and queue definitions

Click Next to continue.

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



File Reporter File Content Manager Configuration Wizard - 3.5.0.9

Broker Connection

Basic Configuration

Broker Type RabbitMQ

Host Address localhost

Port 5671 ☑ Use TLS

Broker Service Account filescan

Management Interface

Management Port 15672 ☑ Use TLS

Admin Account admin

Password

Status Unknown

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.

Broker Service Account: The name of the broker service account in the RabbitMQ system. In most cases you will want to leave the default setting as is.

Set Password: Click this to set and confirm the password for the messaging broker service account.

Management Interface: Fields in this section are specific to the RabbitMQ management interface.

Management Port: This is the port the Management API for RabbitMQ is listening on with TLS support enabled. The default setting is 15672.

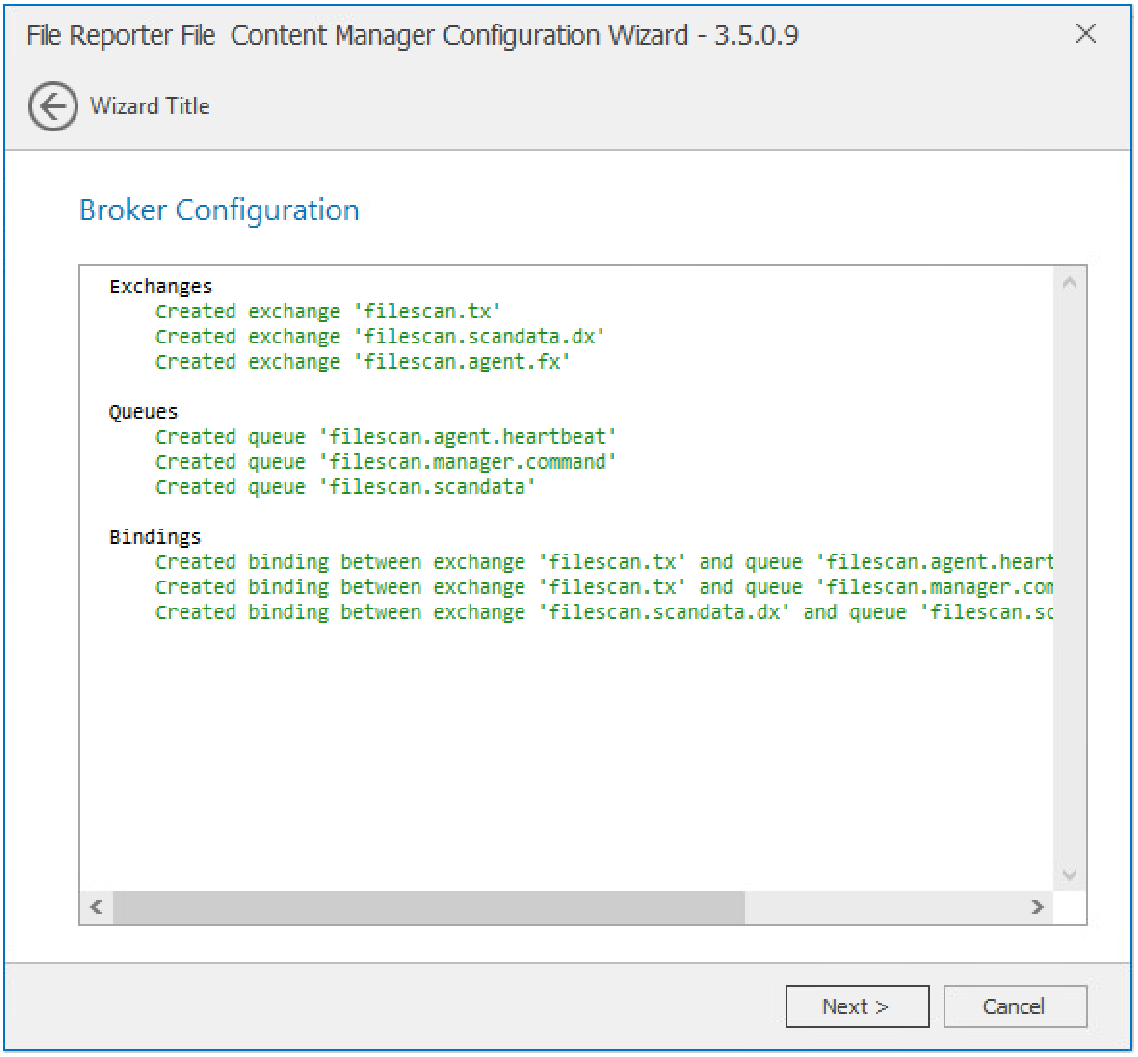
Use TLS: This is a read-only check box indicating that File Reporter only works with TLS communication channels. TLS is always required.

Admin Account: Use the administrator name that you established in Section 6.4, “Changing the Default Password,” on page 36.

Password: Use the password that you established in Section 6.4, “Changing the Default Password,” on page 36.

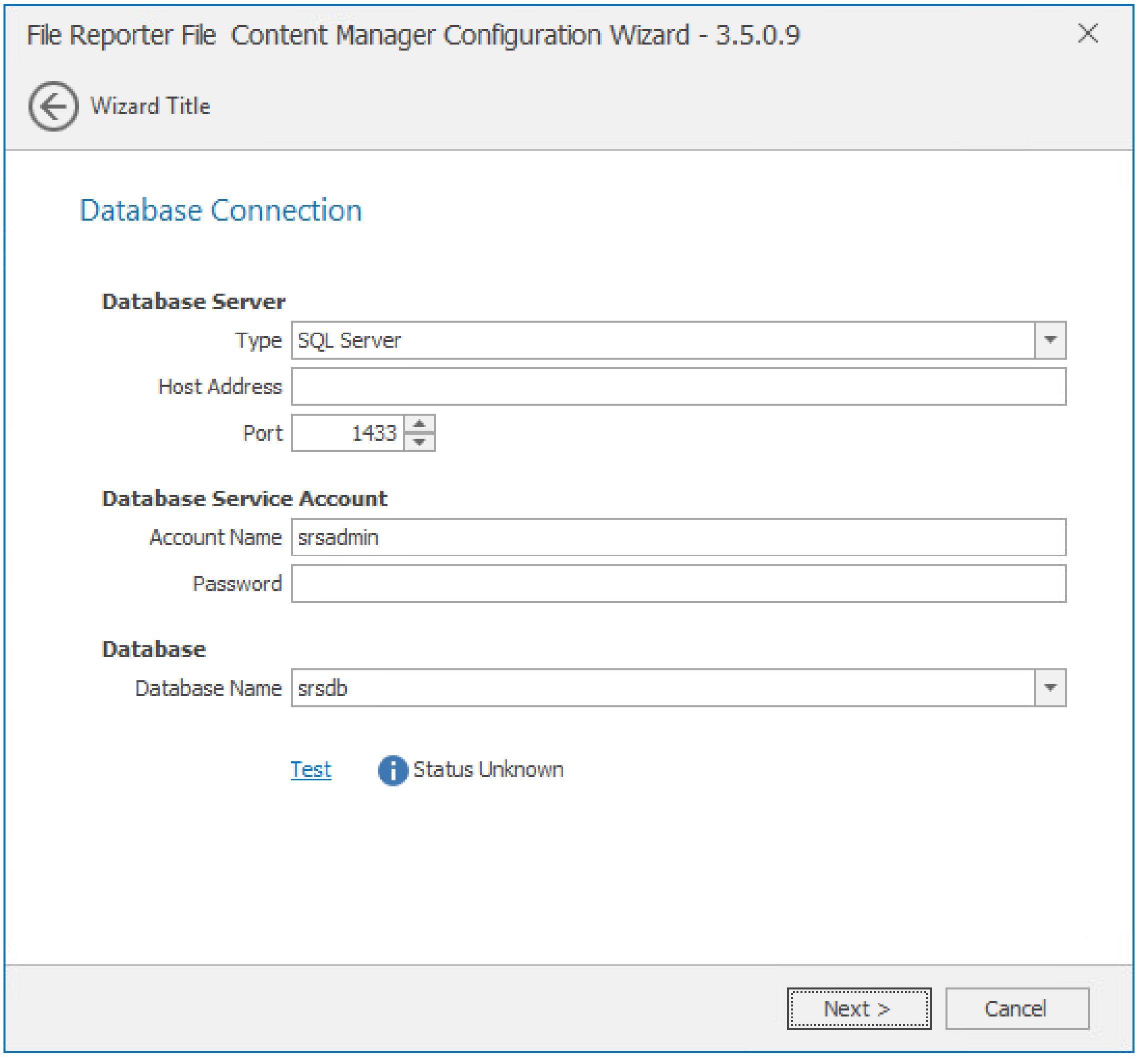
Test: Click to verify the connection between ManagerFC and RabbitMQ.

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


File Reporter File Content Manager Configuration Wizard - 3.5.0.9
Wizard Title
Broker Configuration
Next >
Cancel

```
Exchanges
    Created exchange 'filescan.tx'
    Created exchange 'filescan.scandata.dx'
    Created exchange 'filescan.agent.fx'

Queues
    Created queue 'filescan.agent.heartbeat'
    Created queue 'filescan.manager.command'
    Created queue 'filescan.scandata'

Bindings
    Created binding between exchange 'filescan.tx' and queue 'filescan.agent.heart
    Created binding between exchange 'filescan.tx' and queue 'filescan.manager.com
    Created binding between exchange 'filescan.scandata.dx' and queue 'filescan.sc
```

6 Click **Next**.



File Reporter File Content Manager Configuration Wizard - 3.5.0.9

Wizard Title

Database Connection

Database Server

Type: SQL Server

Host Address:

Port: 1433

Database Service Account

Account Name: srsadmin

Password:

Database

Database Name: srsdb

Test — Status Unknown

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.

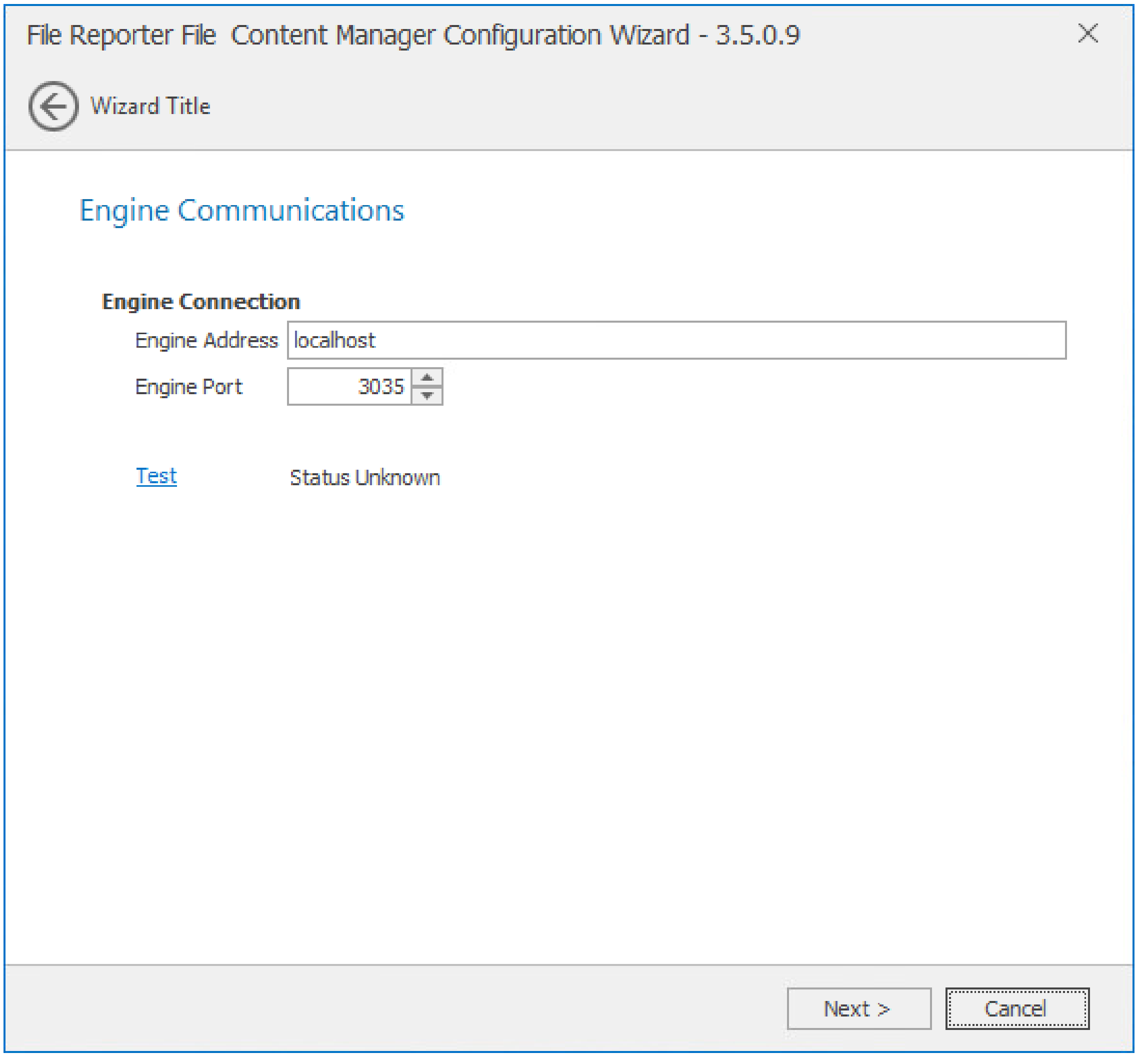
Password: Specify the password for the Database Service User.

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.

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



File Reporter File Content Manager Configuration Wizard - 3.5.0.9

Engine Communications

Engine Connection

Engine Address: localhost

Engine Port: 3035

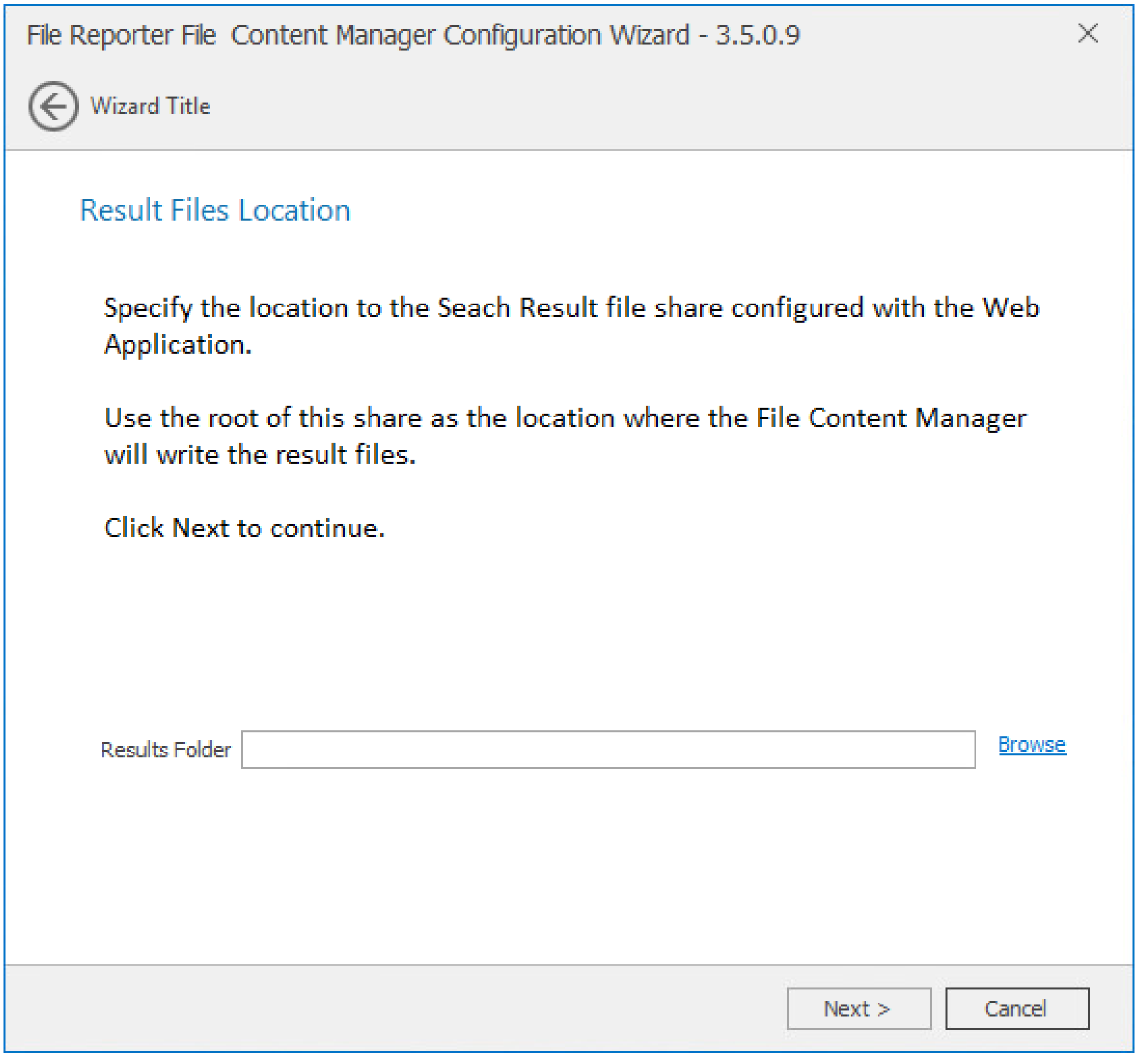
Status Unknown

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

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

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

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



File Reporter File Content Manager Configuration Wizard - 3.5.0.9

Wizard Title

Result Files Location

Specify the location to the Seach Result file share configured with the Web Application.

Use the root of this share as the location where the File Content Manager will write the result files.

Click Next to continue.

Results Folder

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.

9 Click **Browse** to locate the `SearchResults` share that was created when you installed and configured the Web App.

For more information, see Section 7.7, “Configuring the Web Application,” on page 55.

10 Click **Next**.

11 Click **Finish**.

ManagerFC is now running and operational.

10 Installing and Configuring the Legacy Agent for Windows

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

IMPORTANT: Both the legacy Agent for Windows and AgentFS serve the same function of examining and reporting on NTFS file systems, including file system security. AgentFS is an update to the Windows Agent software that is engineered for file scanning features introduced in version 3.5 and future releases. It also addresses a rarely-demonstrated incompatibility with Data Deduplication on Windows Servers. AgentFS cannot presently serve as a Proxy Agent for eDirectory storage resources. You must continue to use the legacy Agent for Windows to do so.

IMPORTANT: You cannot have both AgentFS and the legacy Agent for Windows installed on the same server host.

10.1 Minimum Requirements

- Any of the following quad core 64-bit processor servers:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
- The server must be joined to Active Directory
- Minimum of 100 MB RAM per concurrent scan

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

  NOTE: Performance depends not only the number of concurrent scans, but also the size of the directory structure for each volume or share. Adding more RAM than the minimum requirement can obviously improve performance.
- Minimum of 10 GB free disk space for installation and scans

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

10.2 Active Directory Requirements

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

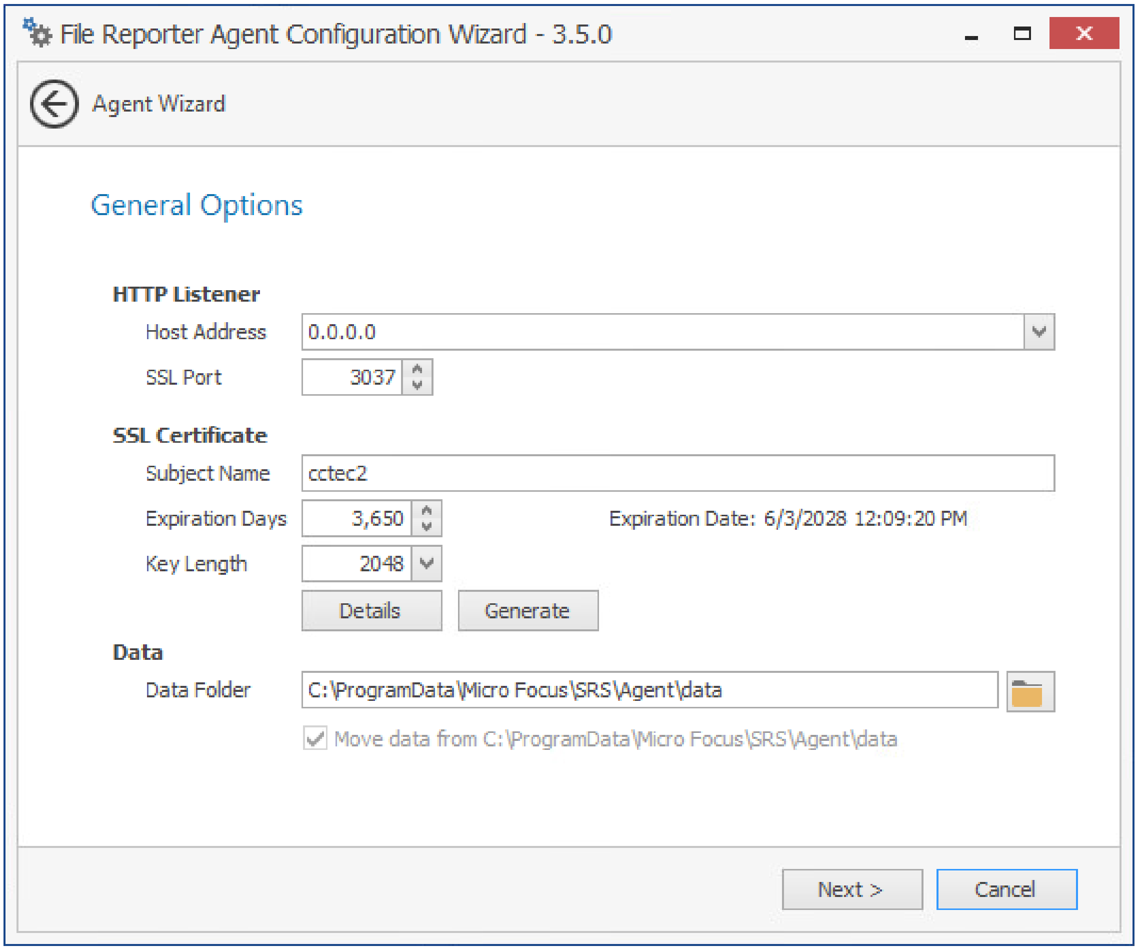
10.3 Prerequisites

- If you want to report on storage resources that reside in an eDirectory network, you must install the Client for Open Enterprise Server software on the same Windows server where you install the Agent:

  Having the Client for Open Enterprise Server installed allows File Reporter to connect to eDirectory and view the storage resources.
- At the same Windows server, configure the Service Location Protocol settings within the Client for Open Enterprise Server software.

10.4 Installing and Configuring the Legacy Agent for Windows

1. At the root of the `FileReporter_3.6.0.iso` image, double-click `FileReporter-Agent-3.6.0-x64-`*`xx`*`.exe`.
2. Agree to the license terms and conditions and click **Install**.
3. When you are notified that the setup was successful, click **Run Setup Utility**.
4. From the wizard page, read the overview of what will be installed and configured and click **Next**.



File Reporter Agent Configuration Wizard - 3.5.0

General Options

HTTP Listener

Host Address 0.0.0.0

SSL Port 3037

SSL Certificate

Subject Name cctec2

Expiration Days 3,650

Expiration Date: 6/3/2028 12:09:20 PM

Key Length 2048

Data

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

☑ Move data from C:\ProgramData\Micro Focus\SRS\Agent\data

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

HTTP Listener: Communication parameters for the Agent.

Host Address: Unless you want the Agent 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 3037.

SSL Certificate: Details for an 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.

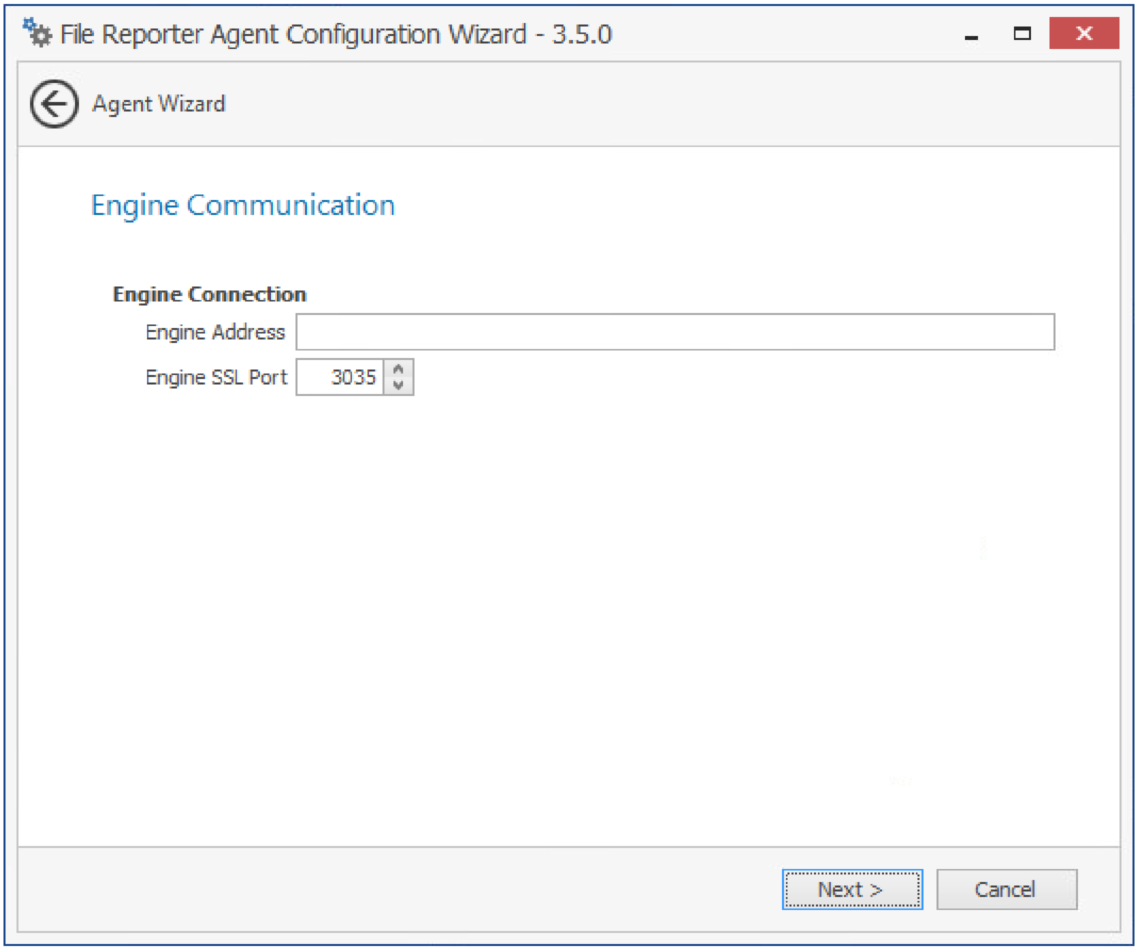
Details: Click the button to view the certificate data.

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 the storage of temporary scan data.

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**.



Engine Communication

Engine Connection

Engine Address

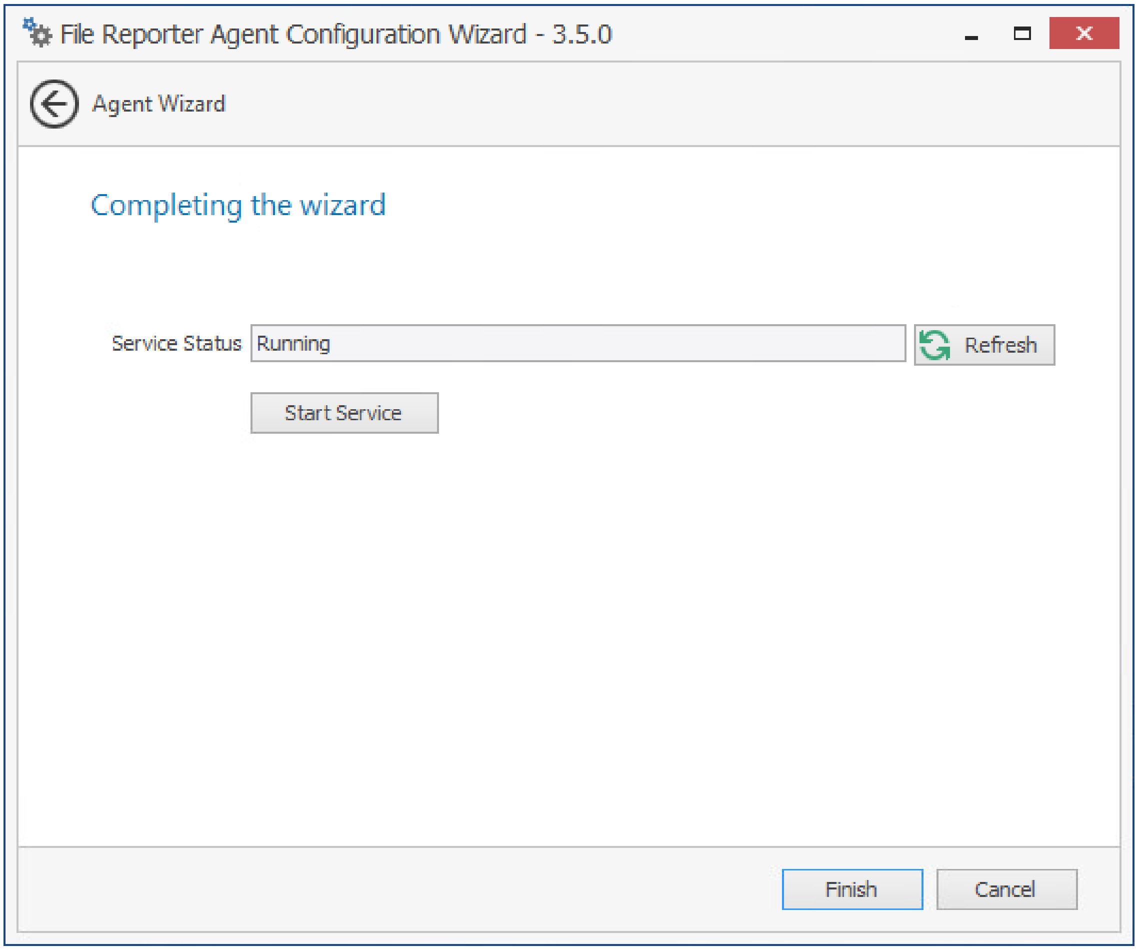
Engine SSL Port 3035

This page lets you set parameters for the Agent 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.

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



File Reporter Agent Configuration Wizard - 3.5.0

Agent Wizard

Completing the wizard

Service Status: Running

7 Click **Finish**.

The Windows Agent is now installed, configured, and running.

11 Installing and Configuring Windows AgentFS

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

IMPORTANT: Both the legacy Agent for Windows and AgentFS serve the same function of examining and reporting on NTFS file systems, including file system security. AgentFS is an update to the Windows Agent software that is engineered for file scanning features introduced in version 3.5 and future releases. It also addresses a rarely-demonstrated incompatibility with Data Deduplication on Windows Servers. AgentFS cannot presently serve as a Proxy Agent for eDirectory storage resources. You must continue to use the legacy Agent for Windows to do so.

IMPORTANT: You cannot have both AgentFS and the legacy Agent for Windows installed on the same server host.

11.1 Minimum Requirements

- Any of the following dual core 64-bit processor servers:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1 or later
- The server must be joined to Active Directory
- .NET 4.5.2 (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 volume or share. Adding more RAM than the minimum requirement can obviously improve performance.
- Minimum of 10 GB free disk space for installation and scans

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

11.2 Active Directory Requirements

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

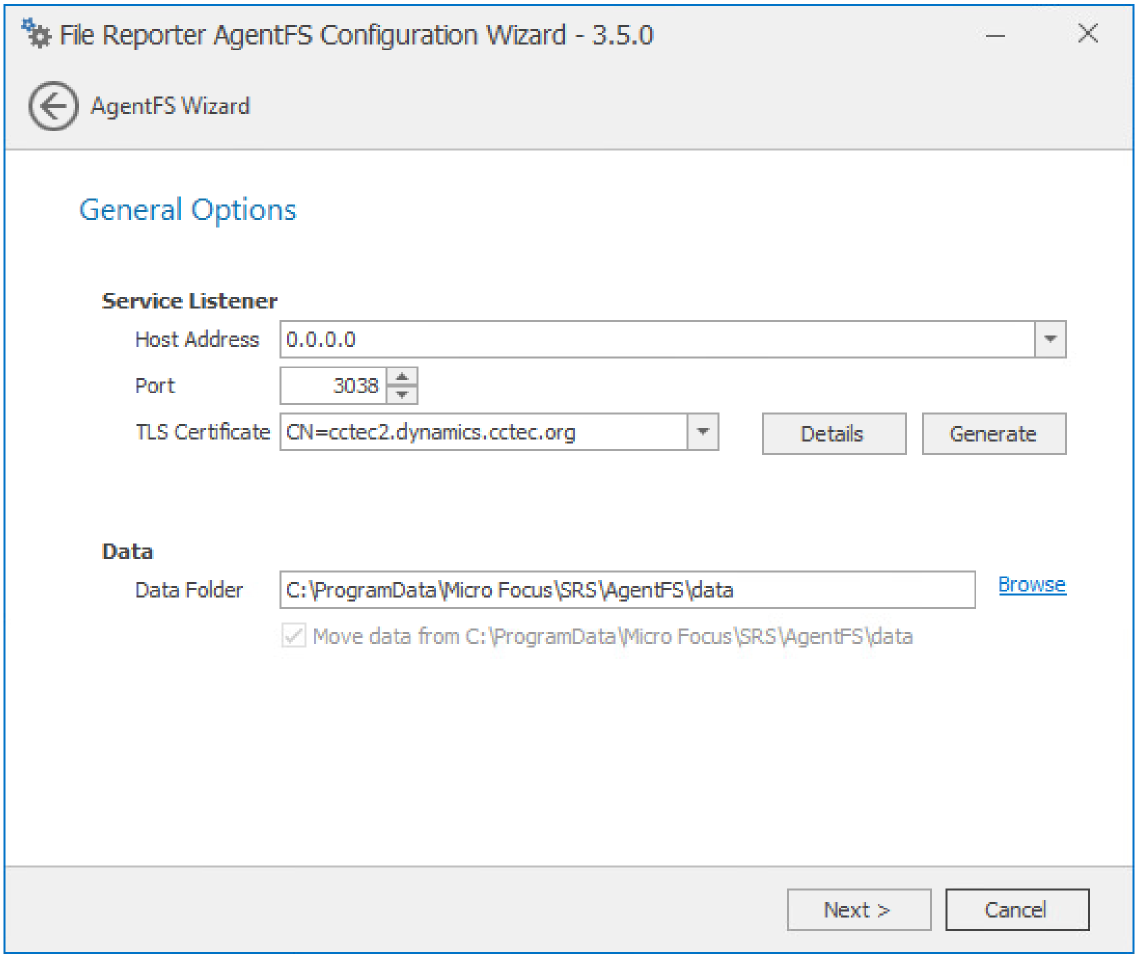
11.3 Installing and Configuring AgentFS

1 At the root of the `FileReporter_3.6.0.iso` image, double-click `FileReporter-AgentFS-3.6.x64-`*`xx`*`.exe`.

2 Agree to the license terms and conditions and click **Install**.

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

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



File Reporter AgentFS Configuration Wizard - 3.5.0

AgentFS Wizard

General Options

Service Listener

Host Address: 0.0.0.0

Port: 3038

TLS Certificate: CN=cctec2.dynamics.cctec.org

Data

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

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

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.

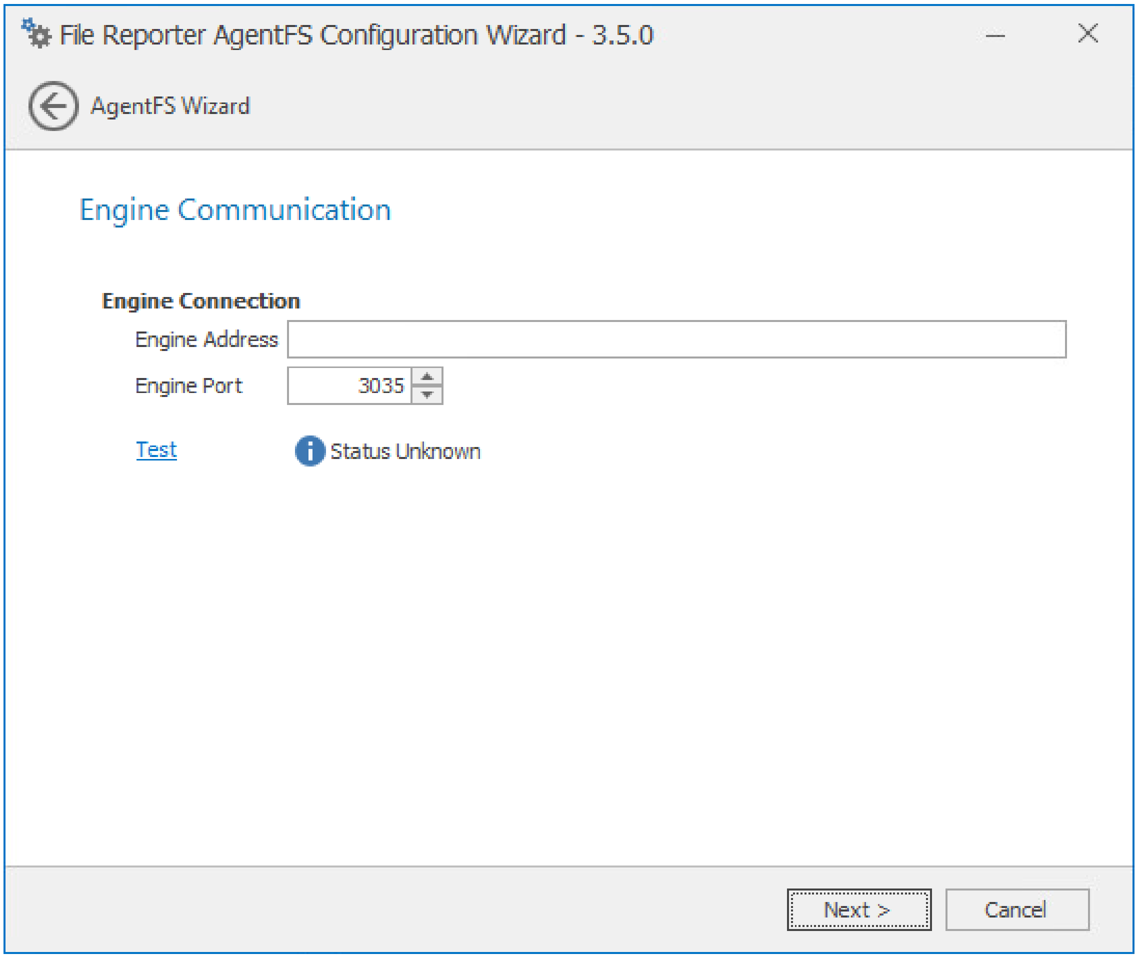
Data: Parameters pertaining to the `data` folder.

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**.



File Reporter AgentFS Configuration Wizard - 3.5.0

AgentFS Wizard

Engine Communication

Engine Connection

Engine Address

Engine Port 3035

Test

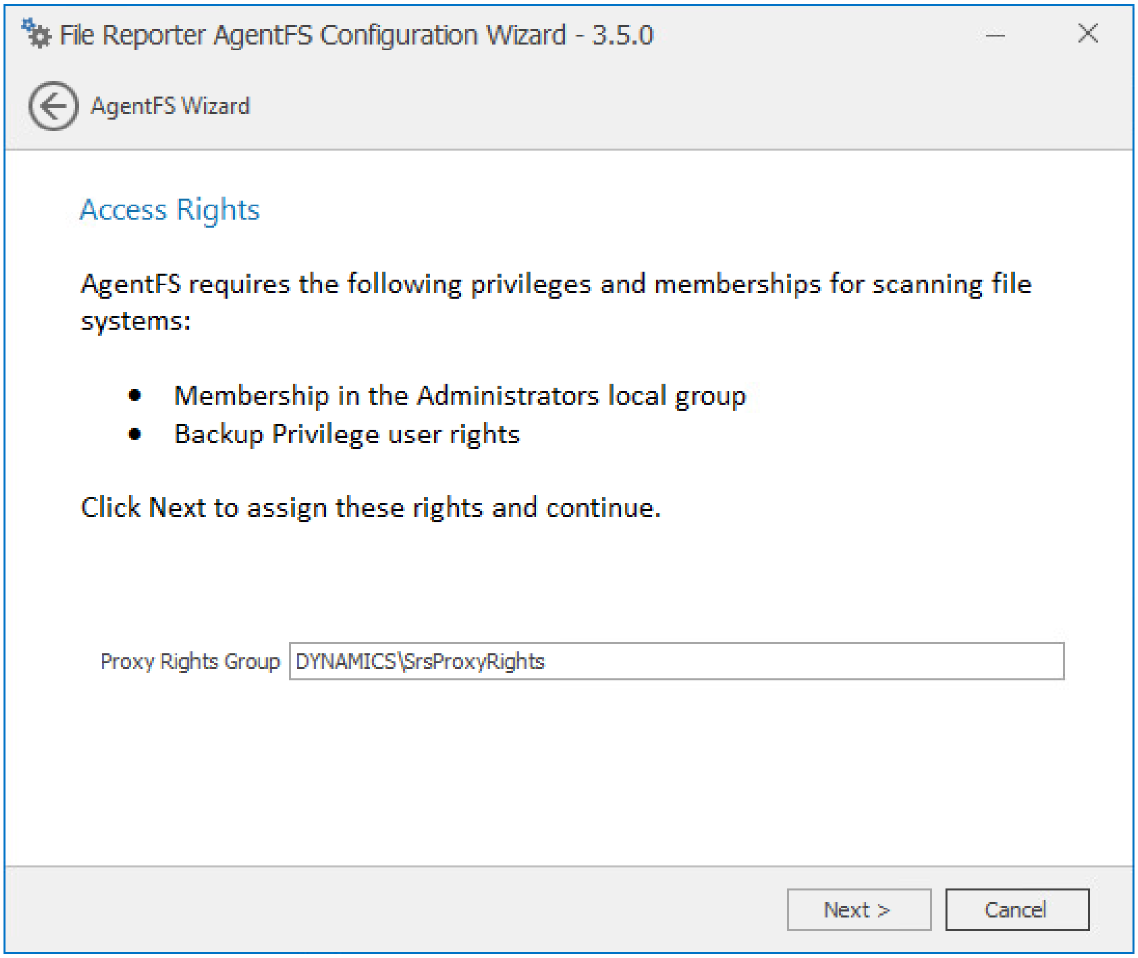
Status Unknown

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**.



Access Rights

AgentFS requires the following privileges and memberships for scanning file systems:

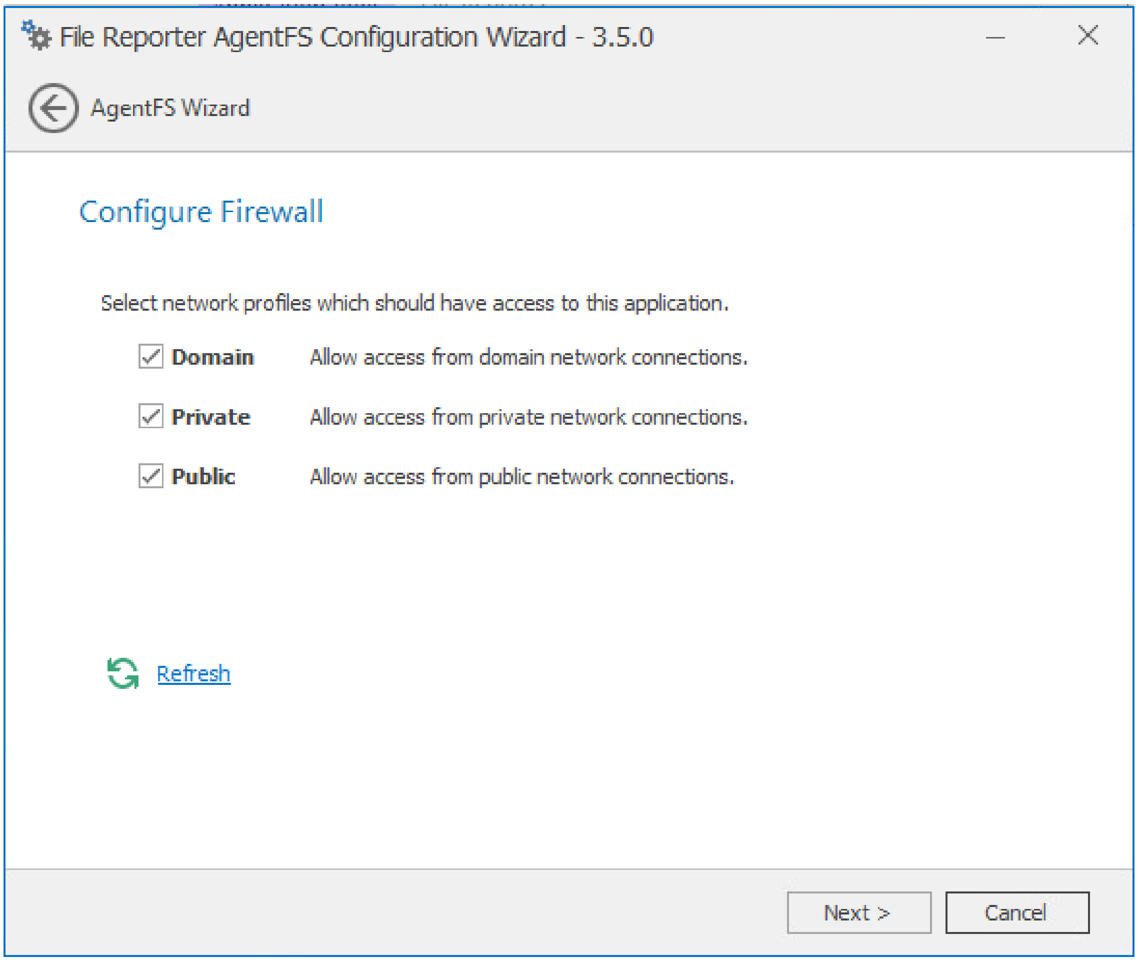
- Membership in the Administrators local group
- Backup Privilege user rights

Click Next to assign these rights and continue.

Proxy Rights Group: DYNAMICS\SrsProxyRights

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**.



Configure Firewall

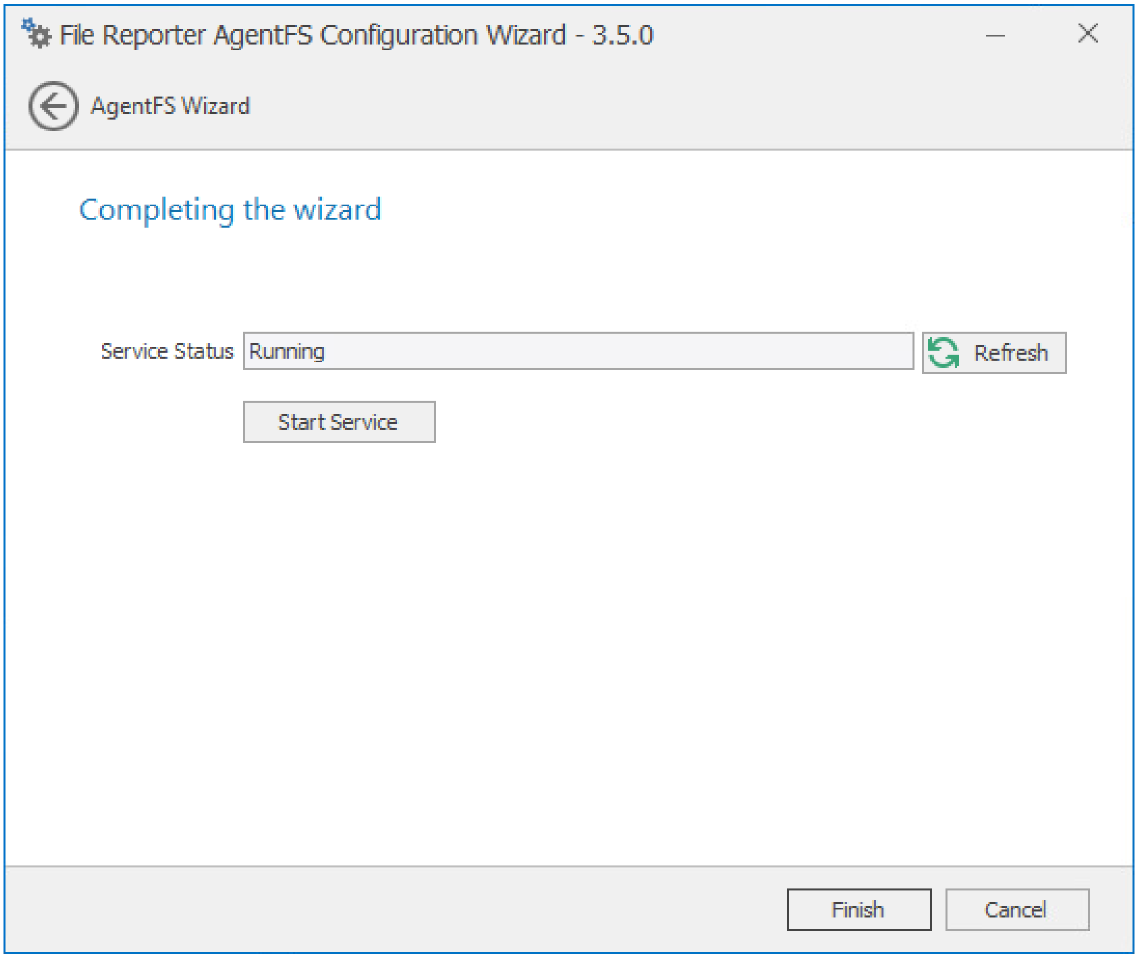
Select network profiles which should have access to this application.

☑ **Domain** Allow access from domain network connections.

☑ **Private** Allow access from private network connections.

☑ **Public** Allow access from public network connections.

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



File Reporter AgentFS Configuration Wizard - 3.5.0

AgentFS Wizard

Completing the wizard

Service Status: Running

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

12 Installing and Configuring the Agent for OES Linux

Procedures in this section include those needed for installing and configuring the Agent for OES Linux on a server running Micro Focus Open Enterprise Server.

12.1 Minimum Requirements

- Any of the following quad core 64-bit processor servers:
  - Open Enterprise Server 2018 SP1
  - Open Enterprise Server 2018
  - Open Enterprise Server 2015 SP1
- Minimum 100 MB RAM per concurrent scan

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

  Performance depends not only the number of concurrent scans, but also the size of the directory structure for each volume or share. Adding more RAM than the minimum requirement can improve performance.
- Minimum of 10 GB free disk space

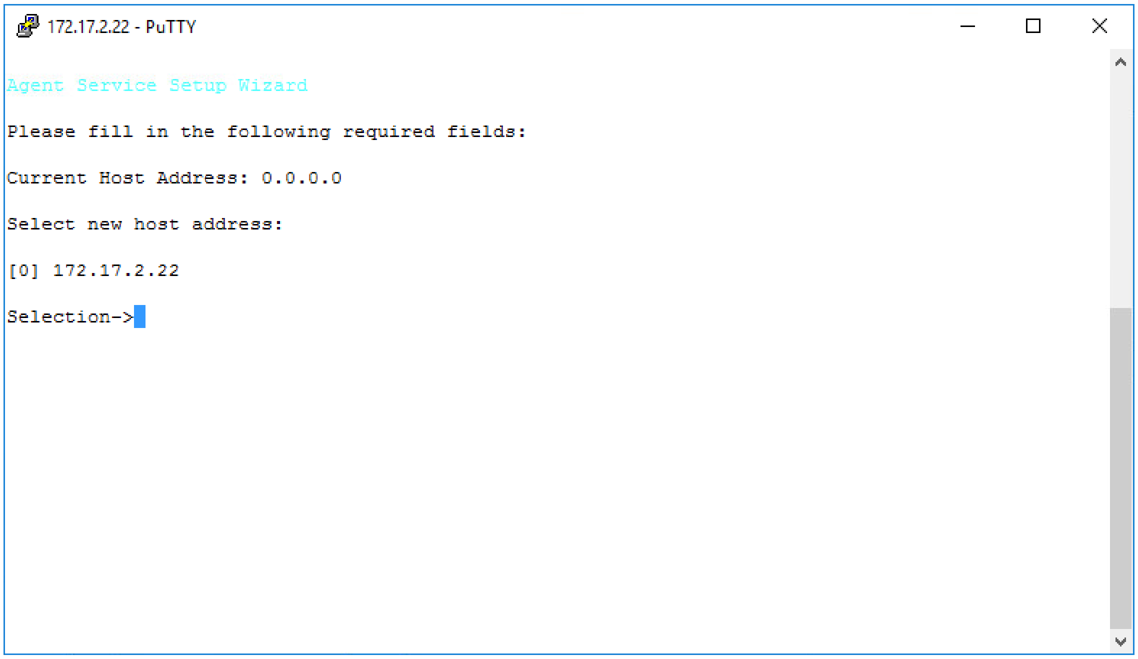
  This size might need to be adjusted based on number of concurrent scans this agent performs, as well as the size of the scans themselves.

12.2 Install and Configure the Agent for OES Linux

1. At the Open Enterprise Server machine, launch a terminal session.
2. At the terminal console, install or upgrade the Linux Agent for OES by typing:

   ```
   rpm –Uvh microfocus-filereporter-agent-3.6.0-xx.x86_64.rpm
   ```
3. Type `srsagent-config` and press Enter.

   The console is updated and appears similar to the one below.

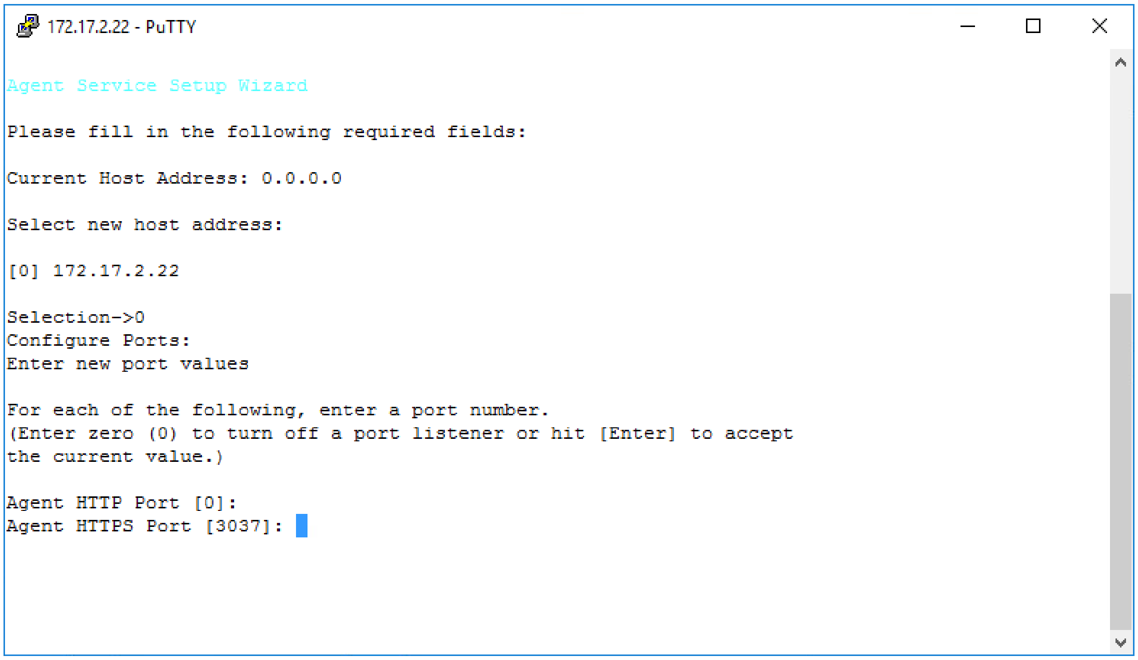


```
Agent Service Setup Wizard

Please fill in the following required fields:

Current Host Address: 0.0.0.0

Select new host address:

[0] 172.17.2.22

Selection->
```

4 Specify the IP address option you want (such as 0 in the example above) and press Enter.

5 When the HTTP Port [0] option appears, type `0` and press Enter.

The console is updated and looks similar to the one below:



```
Agent Service Setup Wizard

Please fill in the following required fields:

Current Host Address: 0.0.0.0

Select new host address:

[0] 172.17.2.22

Selection->0
Configure Ports:
Enter new port values

For each of the following, enter a port number.
(Enter zero (0) to turn off a port listener or hit [Enter] to accept
the current value.)

Agent HTTP Port [0]:
Agent HTTPS Port [3037]:
```

6 Unless there is a conflict, accept the default HTTPS port number of 3037 by pressing Enter. If you need to use another port number, provide the new port number.

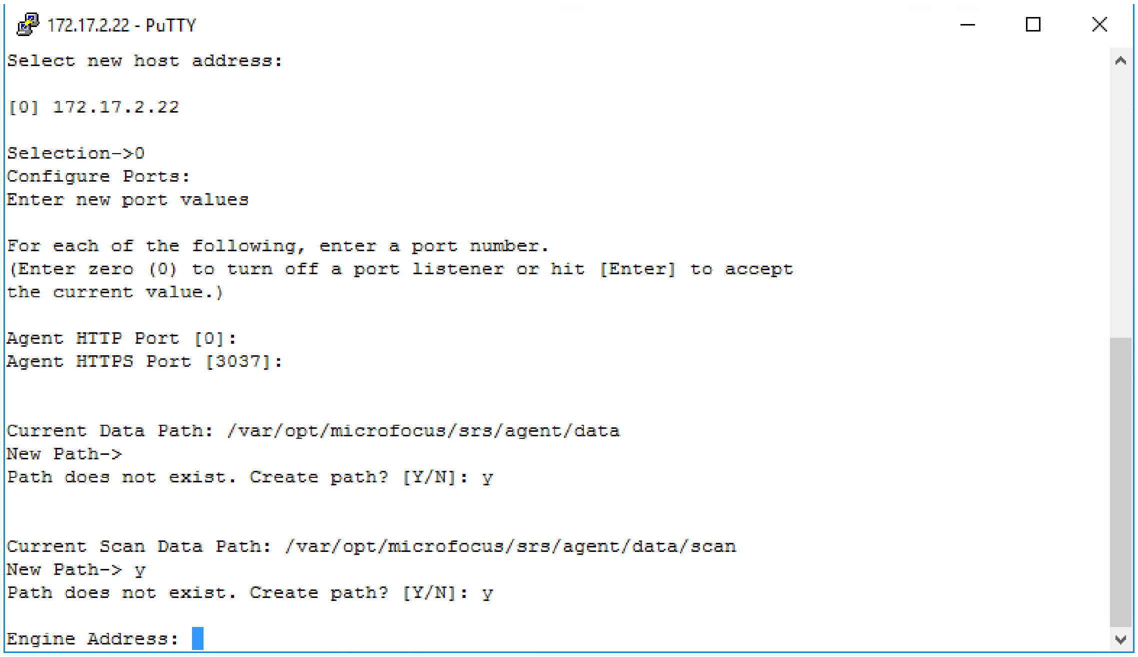
7 Accept the specified data path by pressing Enter.

8 When you are prompted to create the path, type `Y` and then press Enter.

9 Accept the specified scan data path by pressing Enter.

10 When you are prompted to create the path, type Y and then press Enter.

The console is updated and looks similar to the one below:



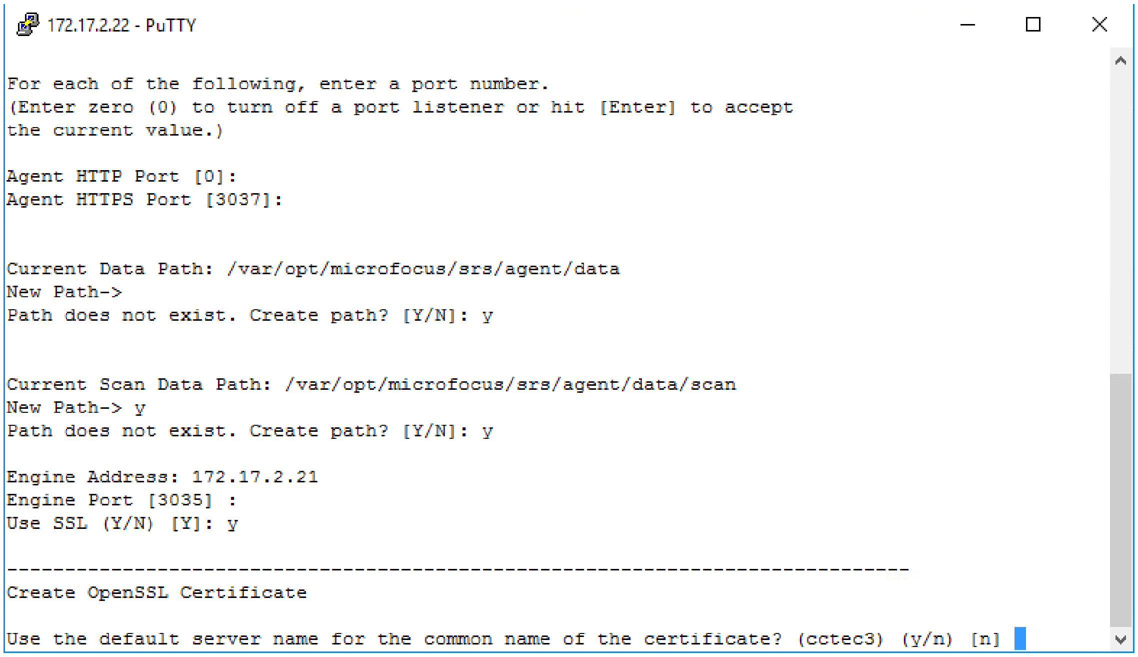
```
Select new host address:

[0] 172.17.2.22

Selection->0
Configure Ports:
Enter new port values

For each of the following, enter a port number.
(Enter zero (0) to turn off a port listener or hit [Enter] to accept
the current value.)

Agent HTTP Port [0]:
Agent HTTPS Port [3037]:


Current Data Path: /var/opt/microfocus/srs/agent/data
New Path->
Path does not exist. Create path? [Y/N]: y


Current Scan Data Path: /var/opt/microfocus/srs/agent/data/scan
New Path-> y
Path does not exist. Create path? [Y/N]: y

Engine Address:
```

11 Type the IP address of the server hosting the Engine and press Enter.

12 Press Enter to accept the specified port number.

13 When prompted to use SSL, type Y and then press Enter.

The console is updated and looks similar to the one below:



```
For each of the following, enter a port number.
(Enter zero (0) to turn off a port listener or hit [Enter] to accept
the current value.)

Agent HTTP Port [0]:
Agent HTTPS Port [3037]:


Current Data Path: /var/opt/microfocus/srs/agent/data
New Path->
Path does not exist. Create path? [Y/N]: y


Current Scan Data Path: /var/opt/microfocus/srs/agent/data/scan
New Path-> y
Path does not exist. Create path? [Y/N]: y

Engine Address: 172.17.2.21
Engine Port [3035] :
Use SSL (Y/N) [Y]: y

------------------------------------------------------------------------------
Create OpenSSL Certificate

Use the default server name for the common name of the certificate? (cctec3) (y/n) [n]
```

14 Do one of the following:

- Type `Y` and then press Enter to select oeslinux as the name for the SSL certificate.
- Type `N`, type a certificate name, and press Enter.

15 After the private key has been created, press Enter to continue.

16 After the certificate has been created, press Enter to continue.

17 When you are prompted to start the service, type `Y` and then press Enter.

The Agent Service Config screen appears.

18 Type `Q` and then press Enter to close the Agent Service Config screen.

The Agent for OES Linux is now installed, configured, and running on the server.

13 Installing AgentFC

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

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

13.1 Minimum Requirements

- Any of the following dual core 64-bit processor servers:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
- The server must be joined to Active Directory
- AgentFC is designed to be deployed as a cluster of one or more nodes. Each node has the following minimum requirements:
  - Quad-core CPU
  - 8 GB RAM
  - 10 GB free disk space for temporary files

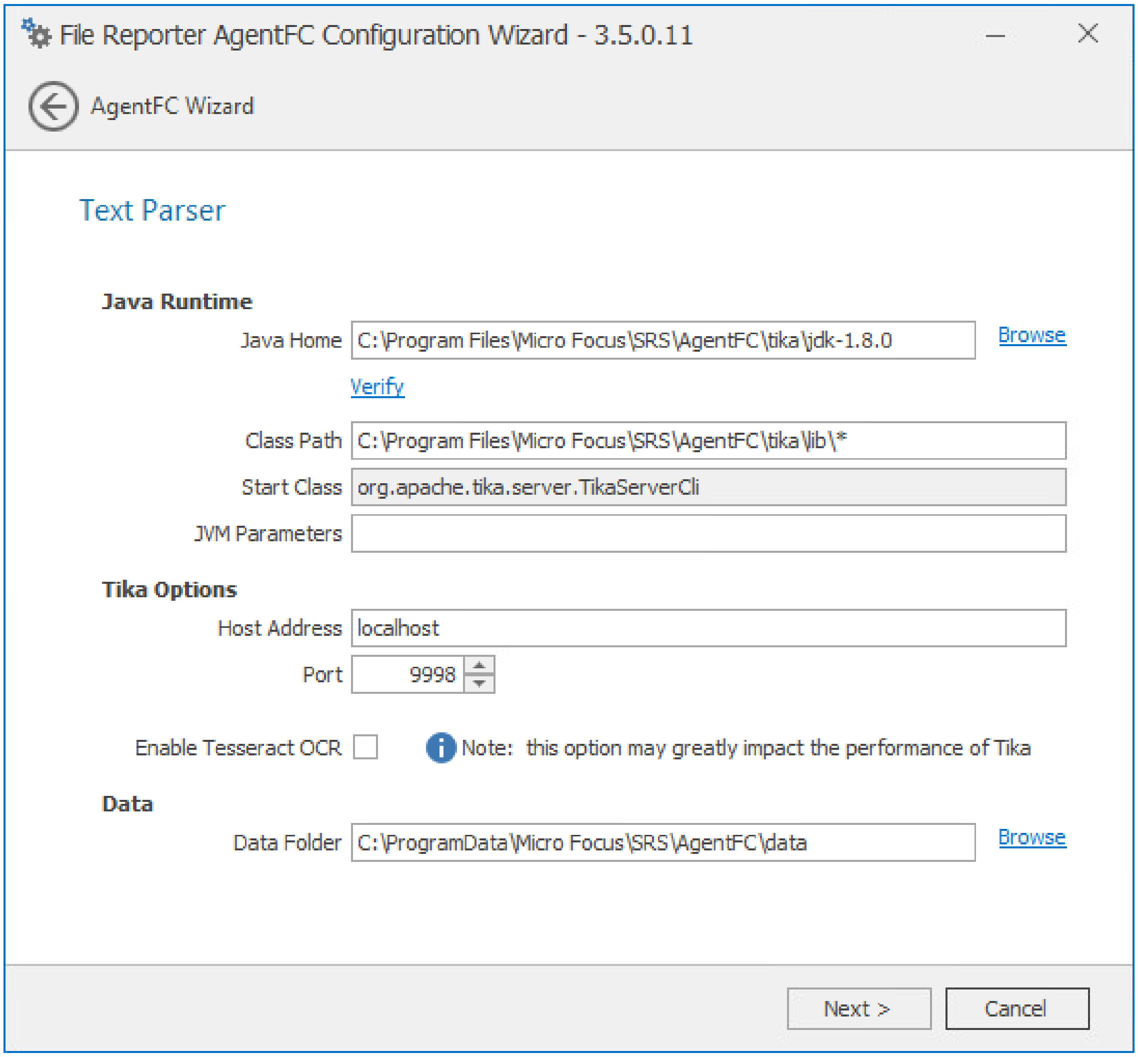
    Depending on the workloads, these numbers may need to be adjusted.
- Depending on frequency of workloads, it might advisable to install each AgentFC node in a VM environment where resources can be scaled as needed. This can allow for more resources as heavy workloads are in progress, and reclamation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

13.2 Active Directory Requirements

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

13.3 Installing and Configuring AgentFC

1. At the root of the `FileReporter_3.6.0.iso` image, double-click `FileReporter-AgentFC-3.6.x64-`*`xx`*`.exe`.
2. Agree to the license terms and conditions and click **Install**.
3. When you are notified that the setup was successful, click **Run Setup Utility**.
4. From the wizard page, read the overview of what will be installed and configured and click **Next**.



File Reporter AgentFC Configuration Wizard - 3.5.0.11

AgentFC Wizard

Text Parser

Java Runtime

Java Home: C:\Program Files\Micro Focus\SRS\AgentFC\tika\jdk-1.8.0

Class Path: C:\Program Files\Micro Focus\SRS\AgentFC\tika\lib\*

Start Class: org.apache.tika.server.TikaServerCli

JVM Parameters:

Tika Options

Host Address: localhost

Port: 9998

Enable Tesseract OCR □

Note: this option may greatly impact the performance of Tika

Data

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

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

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

Java Home: Specifies the location of where the Java runtime and related files are installed.

Browse: Allows you to specify a new path. In most cases, you should utilize the default path.

Verify: Click to verify that AgentFC can properly access a valid Java runtime.

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

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

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

Tika Options: These fields are specific to Apache Tika.

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

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

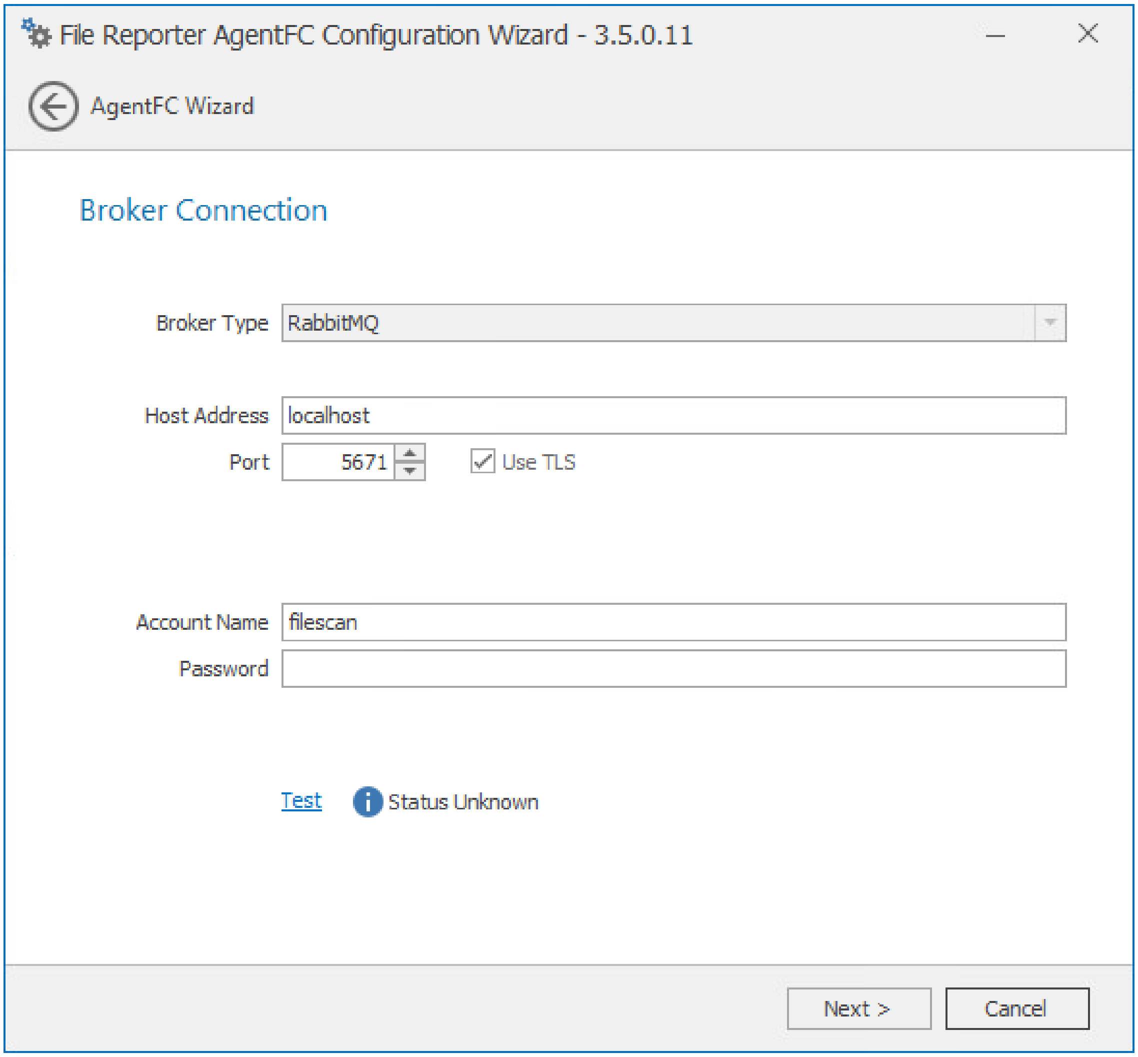
Enable Tesseract OCR: Tesseract OCR is an open source optical character recognition engine from Google that can be the means of locating patterns and content in graphical images. Enabling this engine is resource intensive and it is therefore disabled by default. If you enable this option, beware of performance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

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

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

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

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



File Reporter AgentFC Configuration Wizard - 3.5.0.11

AgentFC Wizard

Broker Connection

Broker Type: RabbitMQ

Host Address: localhost

Port: 5671 ☑ Use TLS

Account Name: filescan

Password:

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

Broker Type: Displays the RabbitMQ messaging broker.

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

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

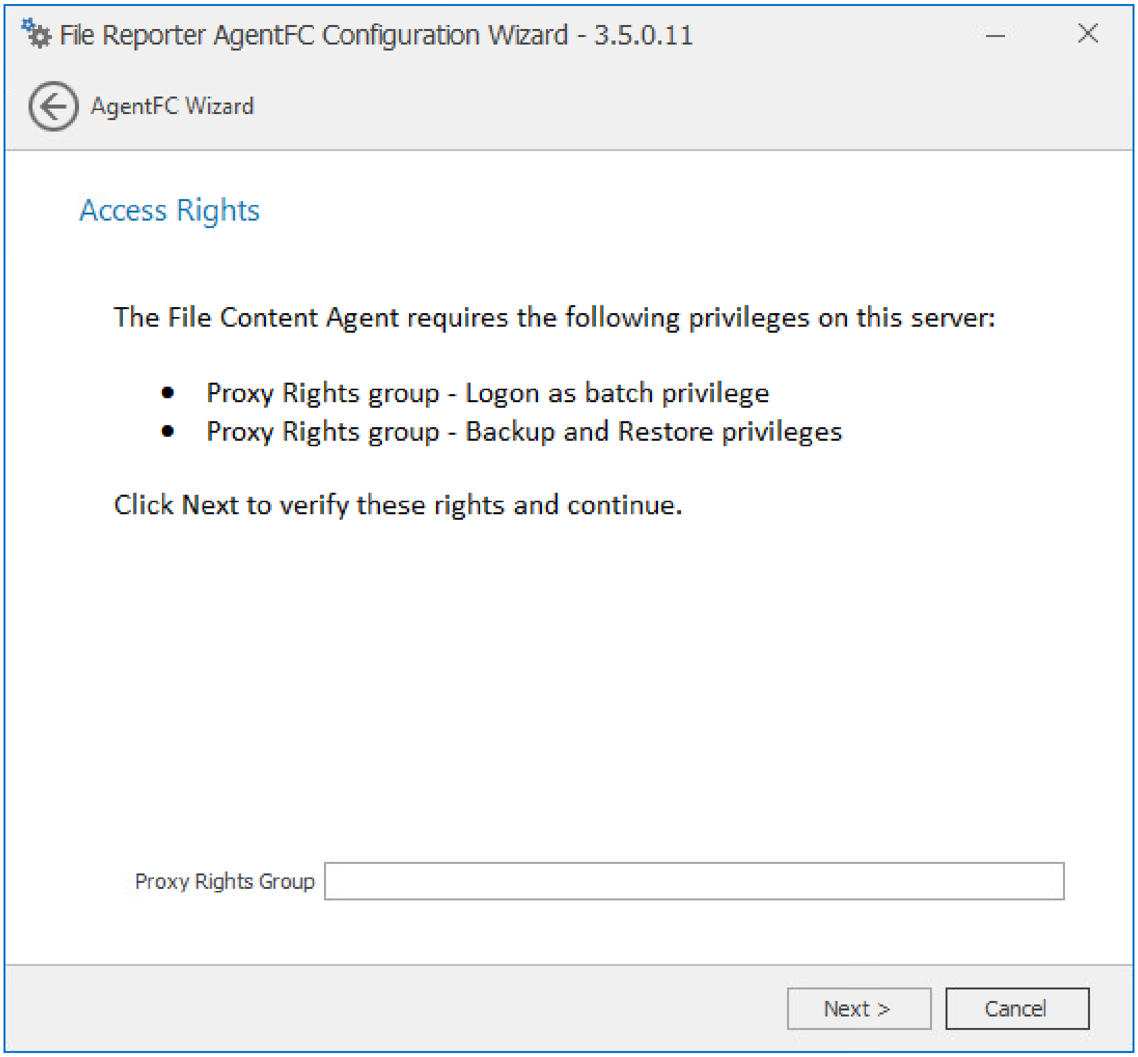
Use TLS: The RabbitMQ messaging broker in File Reporter requires Transport Layer Security (TLS) as the cryptographic communications security protocol.

Account Name: This field displays the default database broker account name used within RabbitMQ. This was created during the configuration of ManagerFC. For more information, see Section 9.2, “Installing ManagerFC,” on page 93.

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

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

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



File Reporter AgentFC Configuration Wizard - 3.5.0.11

AgentFC Wizard

Access Rights

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

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

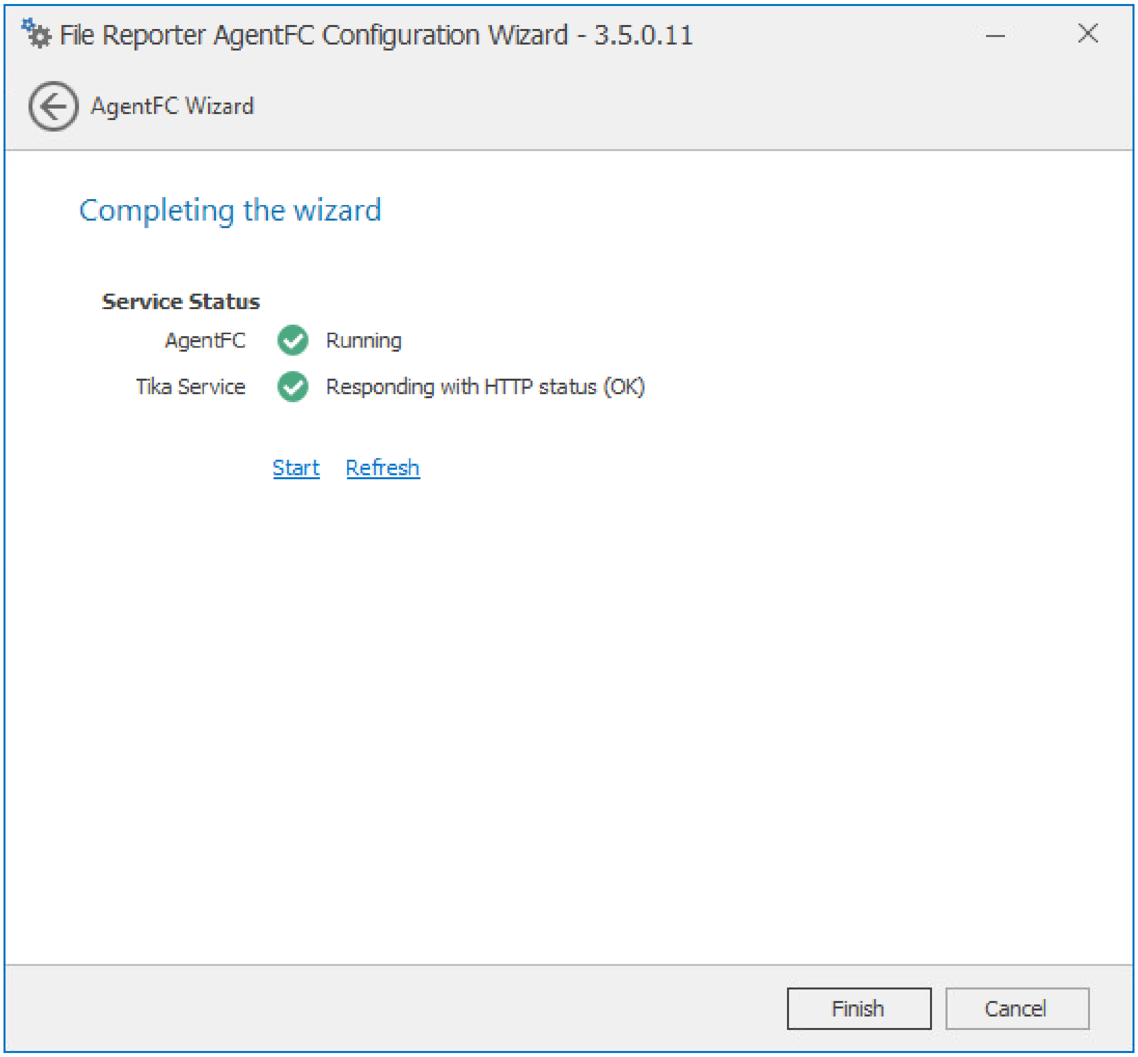
Click Next to verify these rights and continue.

Proxy Rights Group

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

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

8 Click **Next**.



File Reporter AgentFC Configuration Wizard - 3.5.0.11

AgentFC Wizard

Completing the wizard

Service Status

AgentFC ✓ Running

Tika Service ✓ Responding with HTTP status (OK)

9 Click **Finish**.

14 Installing the Report Viewer and Client Tools

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

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

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

14.1 Minimum Requirements

- Any 64-bit multi-core processor Windows workstation with the .NET 4.7.2 framework.

  Note that significant analytic workloads with the Data Analytics tool might be directly impacted by the number and speed of available cores.
- A DirectX 10 compatible graphics card required for use with the Data Analytics tool.
- Report Viewer: Minimum of 8 GB RAM.

  Depending on the size of report loading, exporting, and processing, this number might need to be significantly increased.
- Data Analytics: Minimum of 12 GB RAM

  Note that for the Data Analytics tool, a minimum of about 1KB per scan data entry (or 1GB per million entries) is required. Depending on the type of analysis, such as Pivot Grid, and the number of entries in a single scan, this number might need to be significantly increased.
- Minimum of 250 MB disk space.
- Report Designer and Data Analytics users must be members of the SrsAdmins group.

14.2 Install the Report Viewer

1. From the root of the `FileReporter_3.6.0.iso` image, copy the `FileReporter-ReportViewer-3.6.0-x64-`*`xx`*`.exe` file to all Windows workstations where you will run the Report Viewer.
2. From the Windows workstation, double-click `FileReporter-ReportViewer-3.6.0-x64-`*`xx`*`.exe`.

3. Agree to the license terms and conditions, then click **Install**.
4. When notified that the setup was successful, click **Close**.

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

14.3 Install the Client Tools

1. From the root of the `FileReporter_3.6.0.iso` image, copy the `FileReporter-ClientTools-3.6.0-x64--`*`xx`*`.exe` file to all Windows workstations where you will run the Client Tools.
2. From the Windows workstation, double-click `FileReporter-ClientTools-3.6.0-x64-`*`xx`*`.exe`.
3. Agree to the license terms and conditions, then click **Install**.
4. When notified that the setup was successful, click **Close**.

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

A eDirectory Universal Password Settings

To function properly, File Reporter proxy objects require that Universal Password Policy settings in eDirectory meet certain conditions.

A.1 Universal Password Policy Settings

If you will enable File Reporter in eDirectory and you have Universal Passwords set up for all users in your tree, do the following before installing and configuring any File Reporter components:

1. Before installing the Engine, create a new container in eDirectory to store the proxy objects.
2. Create a Universal Password Policy using iManager.
3. Make sure that the following settings are met:

   ```
   - Number of days before password can be changed: 0 or not set
   - Number of days before password expires: 0 or not set
   - Use Microsoft complexity policy OR
   - Use syntax with the following settings:
   --- Maximum number of characters in password: 36 or greater
   --- Minimum number of unique characters: 1+
   --- Maximum number of times a specific character can be used: NOT SET
   --- Maximum number of times a specific character can repeat sequentially: NOT
   SET
   --- Allow the password to be case-sensitive
   --- Allow numeric characters in password
   --- Allow non-alphanumeric characters in the password
   --- Allow non-US ASCII characters
   ```

4. Associate the Universal Password Policy with the new container you created in Step 1.
5. When creating your proxy objects during the installation of the Engine, make sure that you specify the FDN of this container.

B Replace a License File

B.1 Replacing a License

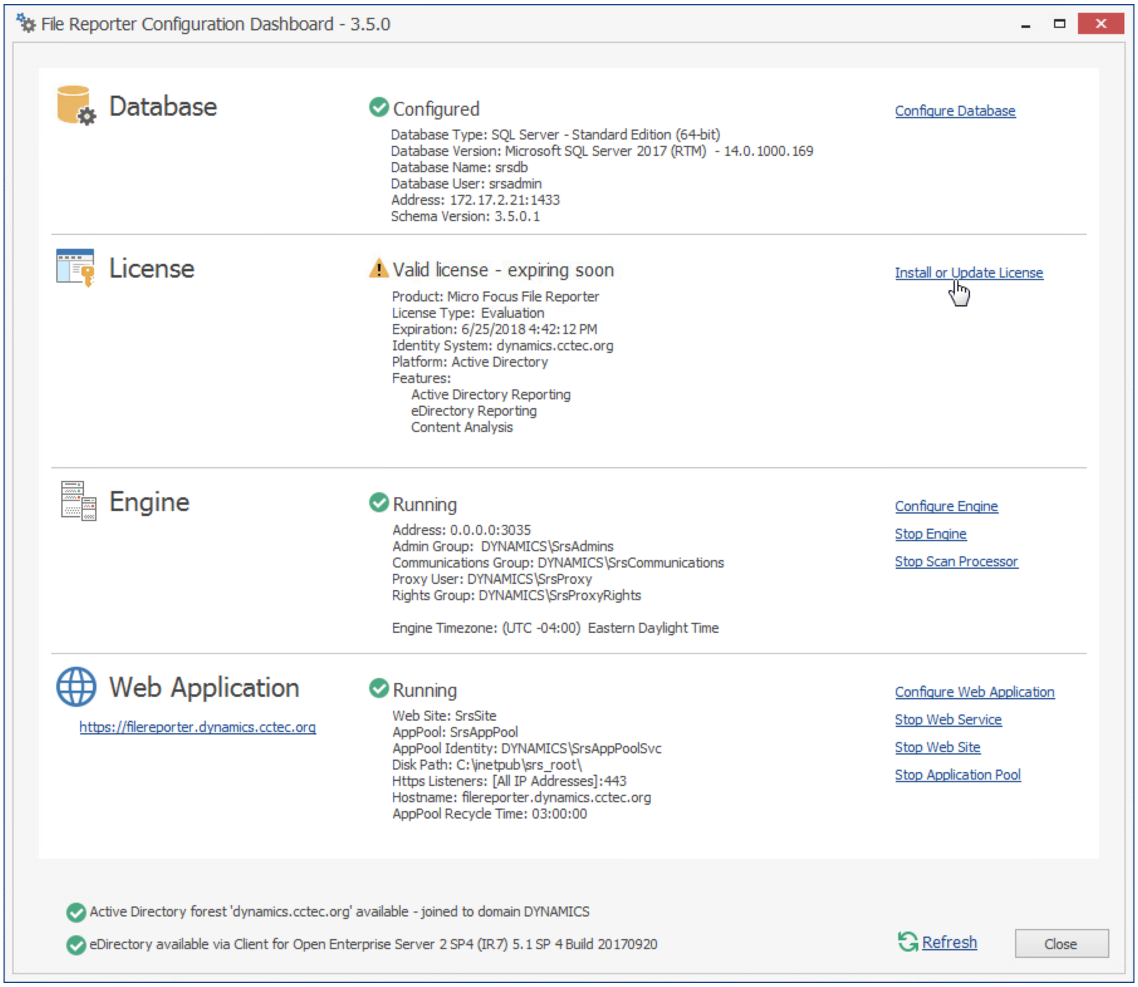
You use the File Reporter Configuration Dashboard to replace a File Reporter license, including an evaluation license.

NOTE: The Engine generates Web and email notifications 60, 30, and 15 days before a license expires. License expiration checks are done every 24 hours at midnight.

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

1 From the **Start** menu, launch the File Reporter Configuration Dashboard.

2 On the File Reporter Configuration Dashboard, click **Install or Update Licensing**.



Configured

Database Type: SQL Server - Standard Edition (64-bit)
Database Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169
Database Name: srsdb
Database User: srsadmin
Address: 172.17.2.21:1433
Schema Version: 3.5.0.1

Valid license - expiring soon

Product: Micro Focus File Reporter
License Type: Evaluation
Expiration: 6/25/2018 4:42:12 PM
Identity System: dynamics.cctec.org
Platform: Active Directory
Features:
Active Directory Reporting
eDirectory Reporting
Content Analysis

Running

Address: 0.0.0.0:3035
Admin Group: DYNAMICS\SrsAdmins
Communications Group: DYNAMICS\SrsCommunications
Proxy User: DYNAMICS\SrsProxy
Rights Group: DYNAMICS\SrsProxyRights

Engine Timezone: (UTC -04:00) Eastern Daylight Time

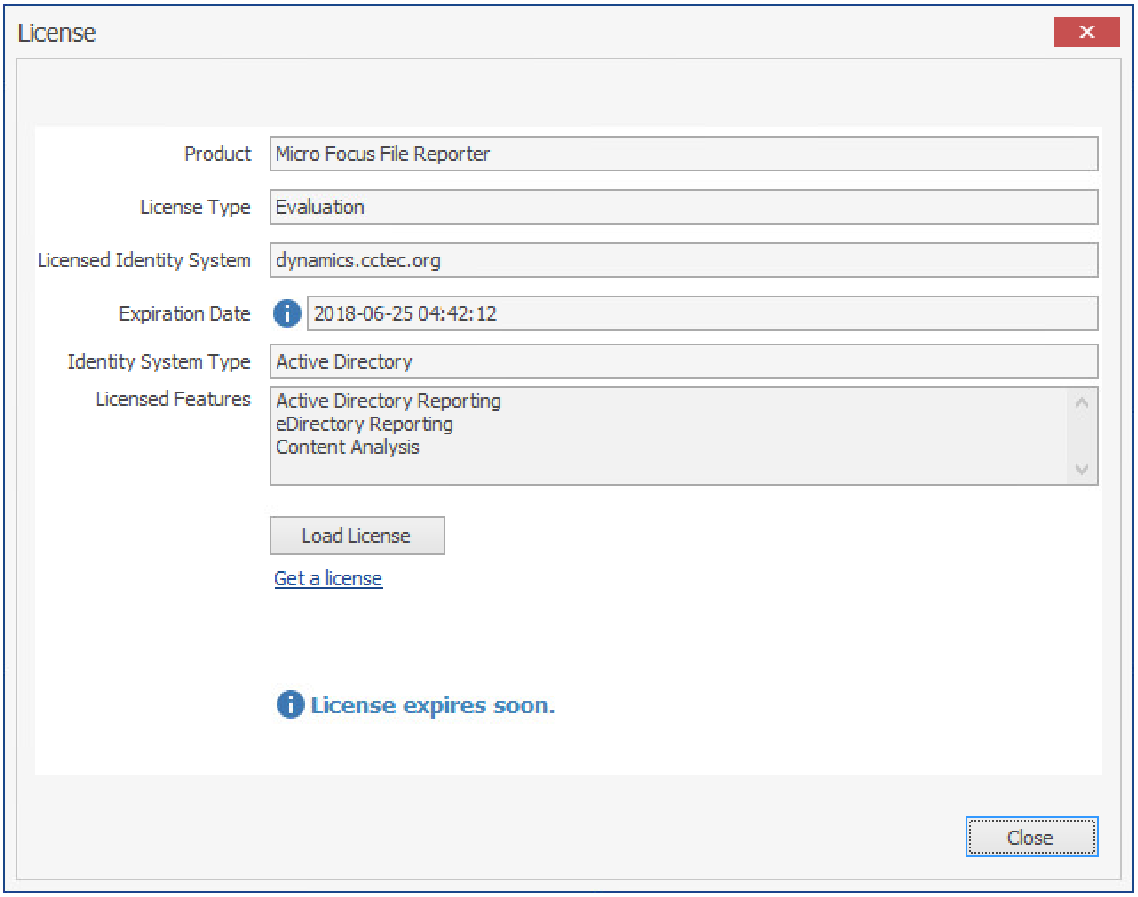
Running

Web Site: SrsSite
AppPool: SrsAppPool
AppPool Identity: DYNAMICS\SrsAppPoolSvc
Disk Path: C:\inetpub\srs_root\
Https Listeners: [All IP Addresses]:443
Hostname: filereporter.dynamics.cctec.org
AppPool Recycle Time: 03:00:00

✓ Active Directory forest 'dynamics.cctec.org' available - joined to domain DYNAMICS

✓ eDirectory available via Client for Open Enterprise Server 2 SP4 (IR7) 5.1 SP 4 Build 20170920

A page similar to the following appears:



License

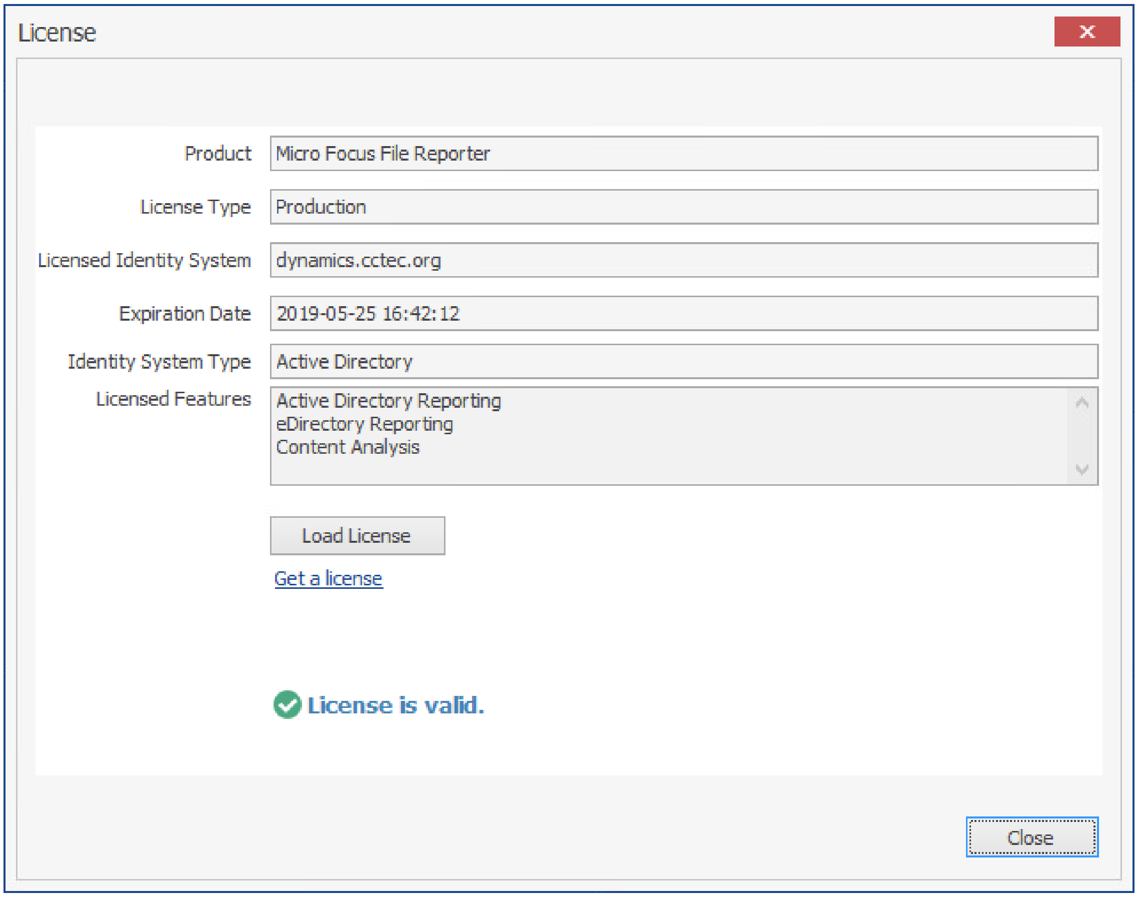
Product	Micro Focus File Reporter
License Type	Evaluation
Licensed Identity System	dynamics.cctec.org
Expiration Date	2018-06-25 04:42:12
Identity System Type	Active Directory
Licensed Features	Active Directory Reporting eDirectory Reporting Content Analysis

License expires soon.

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

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

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



License

Product: Micro Focus File Reporter

License Type: Production

Licensed Identity System: dynamics.cctec.org

Expiration Date: 2019-05-25 16:42:12

Identity System Type: Active Directory

Licensed Features: Active Directory Reporting
eDirectory Reporting
Content Analysis

✓ License is valid.

5 Click **Close**.

C Documentation Updates

This section contains information about documentation content changes that were made in this *Micro Focus File Reporter 3.6 Installation Guide* after the initial release of File Reporter 2.0. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

C.1 January 6, 2020

Updates were made to the following sections:

Location	Update Description
Section 2.3, “Decide Where to Host the Engine,” on page 15.	Updated section to include support for Windows Server 2019.
Chapter 6, “Installing and Configuring RabbitMQ,” on page 31.	Updated procedures.
Section 7.1, “Minimum Requirements,” on page 39.	Updated section to include support for Windows Server 2019.
Section 8.1, “Minimum Requirements,” on page 65.	Updated section to include support for Windows Server 2019.
Section 9.1, “Minimum Requirements,” on page 93.	Updated section to include support for Windows Server 2019.
Section 10.1, “Minimum Requirements,” on page 101.	Updated section to include support for Windows Server 2019.
Section 11.1, “Minimum Requirements,” on page 107.	Updated section to include support for Windows Server 2019.
Section 12.1, “Minimum Requirements,” on page 113.	Updated section to include support for Open Enterprise Server 2018 SP1.
Section 13.1, “Minimum Requirements,” on page 117.	Updated section to include support for Windows Server 2019.

C.2 July 2, 2018

Updates were made to the following sections:

Location	Update Description
Section 1.4, “File Content Scanning,” on page 10.	New section.
Section 1.5, “Agents,” on page 10.	Updated section.
Section 2.1, “Understand the Technologies and Expertise You Need,” on page 13.	Updated section.
Section 2.5, “Determine Whether to Scan File Content,” on page 16.	New section.
Chapter 3, “Licensing the Product,” on page 19.	Updated procedures.
Chapter 6, “Installing and Configuring RabbitMQ,” on page 31.	New chapter.
Chapter 7, “Installing and Configuring the Engine, Database, and Web Application in an Active Directory Environment,” on page 39.	Updated procedures.
Chapter 9, “Install ManagerFC,” on page 93.	New chapter.
Chapter 11, “Installing and Configuring Windows AgentFS,” on page 107.	New chapter.
Chapter 13, “Installing AgentFC,” on page 117.	New chapter.
Appendix B, “Replace a License File,” on page 127.	New appendix.

C.3 January 12, 2017

Updates were made to the following section:

Location	Update Description
Chapter 4, “Installing and Configuring the PostgreSQL Database,” on page 21.	Corrected an incorrectly documented command.

C.4 July 19, 2016

Updates were made to the following sections:

Location	Update Description
Section 2.4, “Decide Which Database to Utilize,” on page 15.	Updated the list of supported Linux servers. Removed mention of support for the PostgreSQL database on Windows.

C.5 November 10, 2015

Updates were made to the following sections:

Location	Update Description
Installation requirements for PostgreSQL, Engine, Web Application, and Agents.	Removed references of support for these on Windows 7 and 8 workstations.

C.6 April 27, 2015

Updates were made to the following sections:

Location	Update Description
Section 2.7, "Database Deployment Recommendations," on page 17.	New section.
Section 5.1, "Minimum Requirements," on page 23.	New section.

C.7 October 7, 2014

Updates were made to the following sections:

Location	Update Description
Section 7.4, "Configuring the Database," on page 42.	Added descriptions of updated fields in the Database Configuration Wizard.
Section 7.7, "Configuring the Web Application," on page 55.	Provided procedures for installing the URL Rewrite Module 2.0 for IIS.
.Section 8.4, "Configuring the Database," on page 67.	Added descriptions of updated fields in the Database Configuration Wizard.
Section 8.7, "Configuring the Web Application," on page 83.	Provided procedures for installing the URL Rewrite Module 2.0 for IIS.
Chapter 14, "Installing the Report Viewer and Client Tools," on page 123.	New section.

C.8 February 18, 2014

Updates were made to the following sections:

Location	Update Description
Section 2.4, "Decide Which Database to Utilize," on page 15.	New section.
Chapter 5, "Installing an SQL Server Instance that Supports File Reporter," on page 23.	New section.
Chapter 7, "Installing and Configuring the Engine, Database, and Web Application in an Active Directory Environment," on page 39.	New procedures.

Location	Update Description
Section 7.2.1, “Prerequisites for Reporting on eDirectory Storage Resources,” on page 40.	New section.
Chapter 8, “Installing and Configuring the Engine, Database, and Web Application in an eDirectory Environment,” on page 65.	New procedures.

C.9 November 26, 2013

Updates were made to the following sections:

Location	Update Description
Section 10.1, “Minimum Requirements,” on page 101.	Changed the RAM requirements.

C.10 July 30, 2013

Updates were made to the following sections:

Location	Update Description
Appendix A, “eDirectory Universal Password Settings,” on page 125.	Changed `--- Maximum number of characters in password: 32 or greater` to `--- Maximum number of characters in password: 36 or greater`

C.11 April 25, 2013

Updates were made to the following sections:

Location	Update Description
Chapter 1, “Upgrading from a Previous Version,” on page 9.	New chapter.
Section 2.3, “Decide Where to Host the Engine,” on page 15.	Added that the Engine can be hosted on a sufficiently enabled 64-bit Windows 7 or Windows 8 workstation. Inserted a recommendation to not install the Engine on a Domain Controller.
Section 4.1.1, “Minimum Requirements,” on page 21.	Updated requirements.
Section 4.1.2, “Installing and Configuring the PostgreSQL Database,” on page 21.	Updated the procedures.
Section 7.1, “Minimum Requirements,” on page 39.	Updated requirements.
Section 8.1, “Minimum Requirements,” on page 65.	Updated requirements.

Location	Update Description
Section 10.1, “Minimum Requirements,” on page 101.	Updated requirements.
Section 12.1, “Minimum Requirements,” on page 113.	Updated requirements.
Appendix A, “eDirectory Universal Password Settings,” on page 125.	New appendix.

C.12 February 13, 2013

Updates were made to the following sections:

Location	Update Description
Section 4.1, “Installing and Configuring the PostgreSQL Database on a Linux Server,” on page 21.	Expanded the section to include procedures for installing the PostgreSQL database on a Linux host server.