opentext™ | File Dynamics

Installation Guide

Version 6.6

Legal Notices

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

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

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

Copyright © 2023 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion with out the express written consent of the publisher.

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

http://condrey.co

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

Installation Guide ... ***1***

Version 6.6 ... *1*

Legal Notices ... ***3***

Third Party Systems ... ***5***

Contents ... ***7***

About This Guide ... ***1***

Audience ... *1*

2 - Overview ... ***2***

3 - Licensing the Product ... ***3***

3.1 - License Overview ... *3*

3.1.1 - License Version ... *3*

3.2 - Updating a License File ... *3*

3.3 - Obtaining an Evaluation License ... *3*

3.4 - Obtaining a Production License ... *4*

3.4.1 - Obtain the Activation Code ... *4*

3.4.2 - Obtain the License File ... *4*

4 - Configuring a SQL Server Instance ... ***5***

4.1 - SQL Server Requirements ... *5*

4.1.1 - Supported Versions ... *5*

4.1.2 - Supported Editions ... *5*

4.1.3 - Dedicated Instance ... *6*

4.2 - Install a New Instance of SQL Server ... *6*

4.3 - SQL Server Post Configuration ... *12*

5 - Installing CouchDB ... ***13***

5.1 - Recommendations ... *13*

5.2 - Download and Install CouchDB ... 13
5.3 - Configure CouchDB Integration ... 15
6 - Upgrading to File Dynamics 6.6 ... ***17***
6.1 - Upgrading from File Dynamics 6.x ... 17
7 - Installing File Dynamics 6.6 ... ***19***
7.1 - Administrator Access ... 19
7.1.1 - Installing Components on Member Servers ... 19
7.1.2 - Managing Active Directory Accounts ... 19
7.1.3 - Granting Proxy Access to Resource Servers ... 19
7.2 - Accessing the Product Contents ... 20
7.3 - Installing the Engine ... 20
7.4 - Installing or Updating the License ... 22
7.4.1 - Installing a New License ... 22
7.4.2 - Updating the License ... 22
7.5 - Configuring the Database ... 23
7.6 - Configuring the Engine ... 26
7.7 - Active Directory Schema ... 30
7.7.1 - Extending the Active Directory Schema ... 31
7.8 - Granting Access to Managed Storage ... 32
7.8.1 - Granting Rights ... 32
7.8.2 - Granting Privileges on a Member Server ... 33
7.8.3 - Granting Privileges on a Domain Controller ... 33
7.9 - Installing the Event Monitor ... 34
7.10 - Installing File System Agents ... 37
7.11 - Installing Phoenix Agents ... 41
7.12 - Installing the Admin Client ... 46

7.13 - Authorizing the Event Monitor *47*

7.14 - Authorizing the Agents *47*

7.15 - Configuring Storage Resources *47*

7.16 - Configuring the Data Owner Web Service *48*

7.16.1 - Replacing the Self-Signed Certificate *52*

8 - Administering File Dynamics ***55***

About This Guide

This installation guide is written to provide network administrators the conceptual and procedural information for installing and configuring OpenText File Dynamics 6.6.

Audience

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

2 - Overview

If you are upgrading from File Dynamics 6.5 to File Dynamics 6.6:

1. Proceed with *Licensing the Product (page 3)*.
2. Follow the procedures in *Upgrading to File Dynamics 6.6 (page 17)*.

If you are installing File Dynamics 6.6:

1. Proceed with *Licensing the Product (page 3)*.
2. Follow the procedures in *Configuring a SQL Server Instance (page 5)* to install a SQL Server instance that File Dynamics supports.
3. Complete the installation by following the procedures in *Installing File Dynamics 6.6 (page 19)*.

3 - Licensing the Product

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

3.1 - License Overview

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

For individuals evalutaing File Dynamics, you can obtain a full-featured 60-day license of the core product.

3.1.1 - License Version

File Dynamics 6.6 requires a File Dynamics 6.6 license.

3.2 - Updating a License File

After you have installed File Dynamics, you can update your evaluation license or production license by simply replacing the old license with the new one. For more information, see *Installing or Updating the License (page 22)*.

3.3 - Obtaining an Evaluation License

1. In a web browser, go to https://filedynamicssupport.com/License.
2. Fill out the form providing the required information.
3. Be sure to select version 6.6 for the product *Version* field and to enter the correct *Forest Root Name* against which this product will be licensed.
4. For the *License Type* select *Evaluation*.
5. After submitting the form, you will receive an email.
6. Open the email and click **Download License File**, which will present you access to the license file.
7. Install the license following the instructions at *Installing or Updating the License (page 22)*.

3.4 - Obtaining a Production License

3.4.1 - Obtain the Activation Code

In order to obtain a production File Dynamics 6.6 license file, you will first need to retrieve your activation code from the OpenText software license site.

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

1. In a web browser, go to https://sld.microfocus.com/mysoftware/index.
2. Follow the steps required to activate File Dynamics 6.6.
3. Once you have the activation key, have it ready for the next steps when obtaining the license file.

3.4.2 - Obtain the License File

1. In a web browser, go to https://filedynamicssupport.com/License.
2. Fill out the form providing the required information.
3. Be sure to select version 6.6 for the product *Version* and to enter the correct *Forest Root Name* against which this product will be licensed.
4. For the *License Type* select *Activation*.
5. Enter the *Licensed Seats Count*.
6. Enter the *Activation Code* using the code you obtained from the customer center site earlier.
7. After submitting the form, you will receive an email.
8. Open the email and click **Download License File**, which will present you access to the license file.
9. Install the license following the instructions at *Installing or Updating the License (page 22)*.

4 - Configuring a SQL Server Instance

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

SQL Server is a fully-featured database service, and as such requires installation and maintenance planning before deployment. While a complete analysis of this maintenance is beyond the scope of this product's documentation, we strongly recommend that you review Microsoft's SQL Server documentation to plan for separation of data and transaction logs, regular database backups, and transaction log and data growth.

4.1 - SQL Server Requirements

4.1.1 - Supported Versions

File Dynamics 6.6 supports the following versions of SQL Server:

- SQL Server 2022
- SQL Server 2019

SQL Server 2017 will work but is considered deprecated and will no longer be supported in a later release. Please consider upgrading to SQL Server 2019 or later.

4.1.2 - Supported Editions

The following editions of SQL Server are supported in production:

- SQL Server Express
- SQL Server Standard
- SQL Server Enterprise

We do not recommend that you install the Engine on the same server running SQL Server. If you will be using SQL Server Express, you can run it on the same server host, but you will most likely experience better performance if they are running on a separate server.

If you do not already own SQL Server, you can use SQL Server Express. You can download a current version of SQL Server Express for free at: https://www.microsoft.com/en-us/sql-server/sql-server-downloads.

NOTE: While SQL Server Express is sufficient in many cases, please be aware of its current limits around processing and disk capacity. Some scenarios may require more than the 10GB storage limit that this edition current supports.

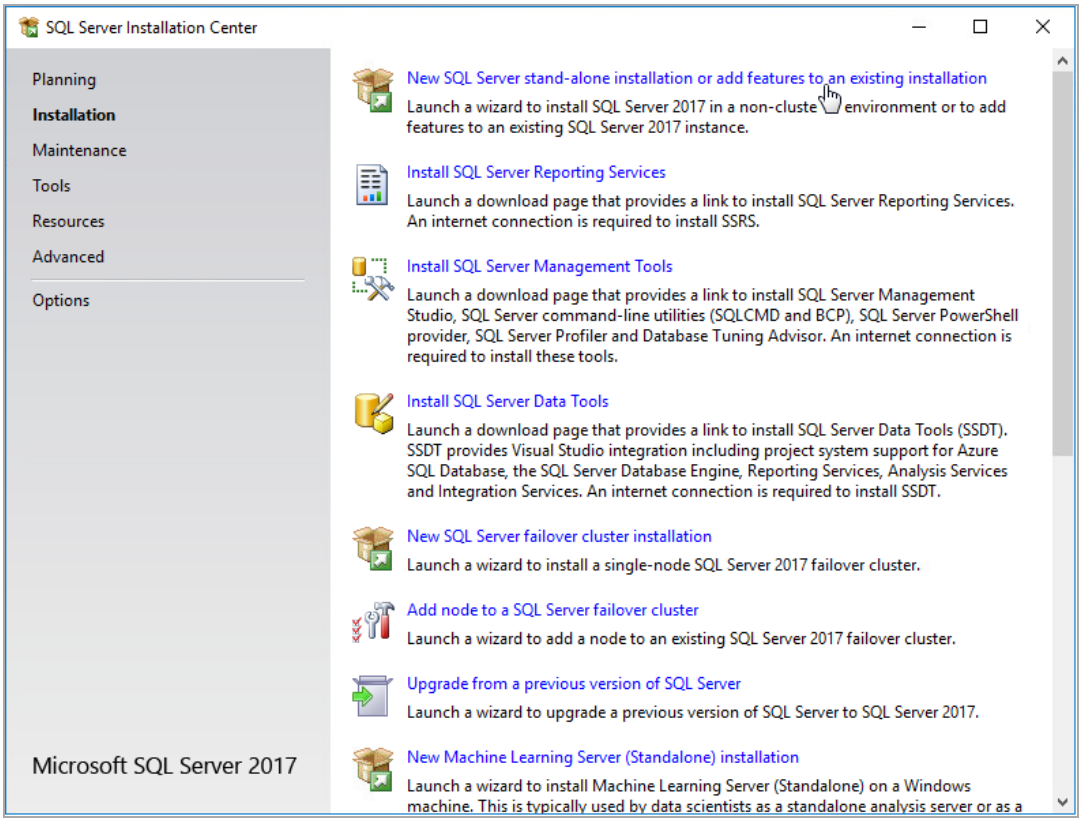
4.1.3 - Dedicated Instance

It is strongly recommended that you use configure a dedicated instance of SQL Server for File Dynamics, due to considerations with security and collation.

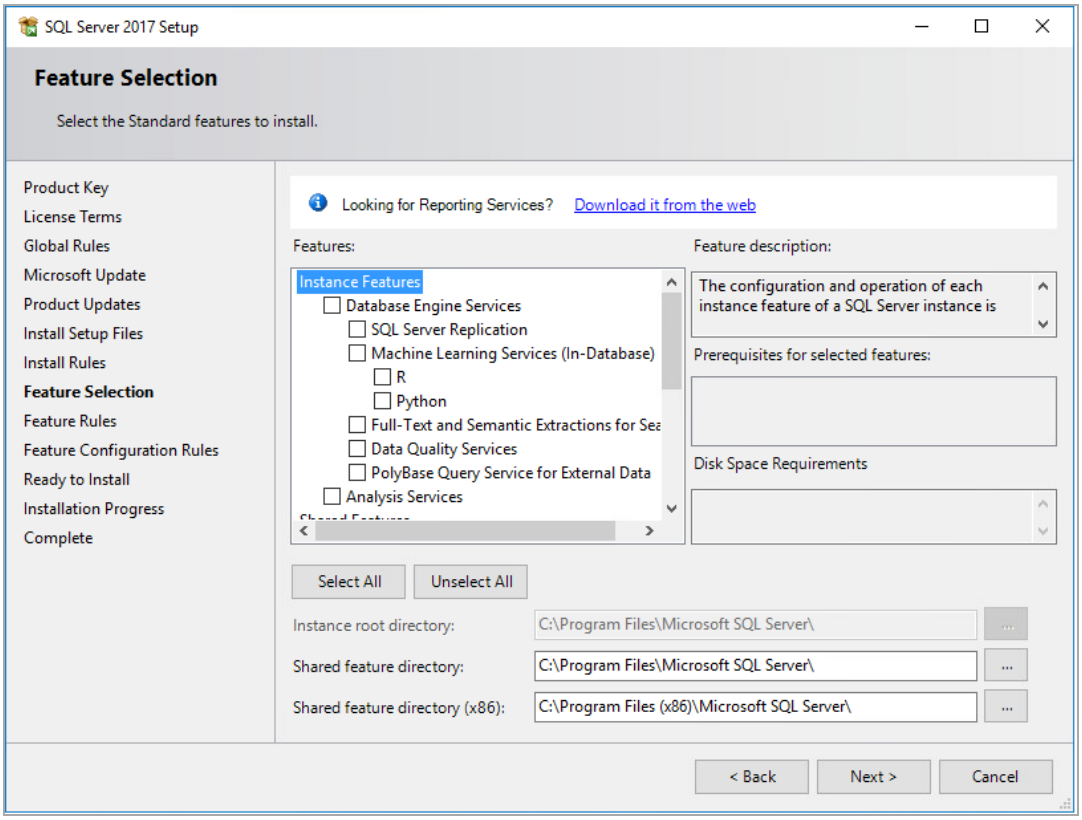
4.2 - Install a New Instance of SQL Server

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*.

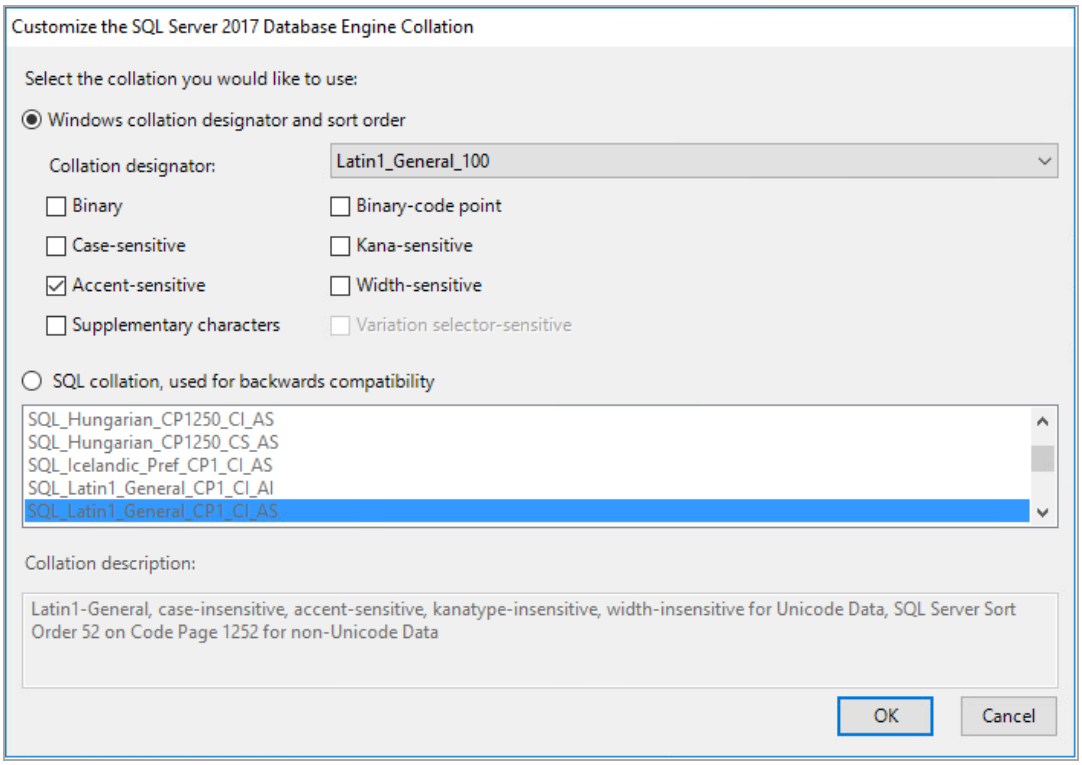


4. The Setup Support Rules operation is run.
5. When the operation has completed, click *OK*.
6. When prompted, enter your product key, then click *Next*.
7. Accept the license terms and click *Next*.
8. Include all Microsoft SQL Server product updates, then click *Next*.
9. The Setup Support Rules operation is run again.
10. When the operation has completed, click Next.



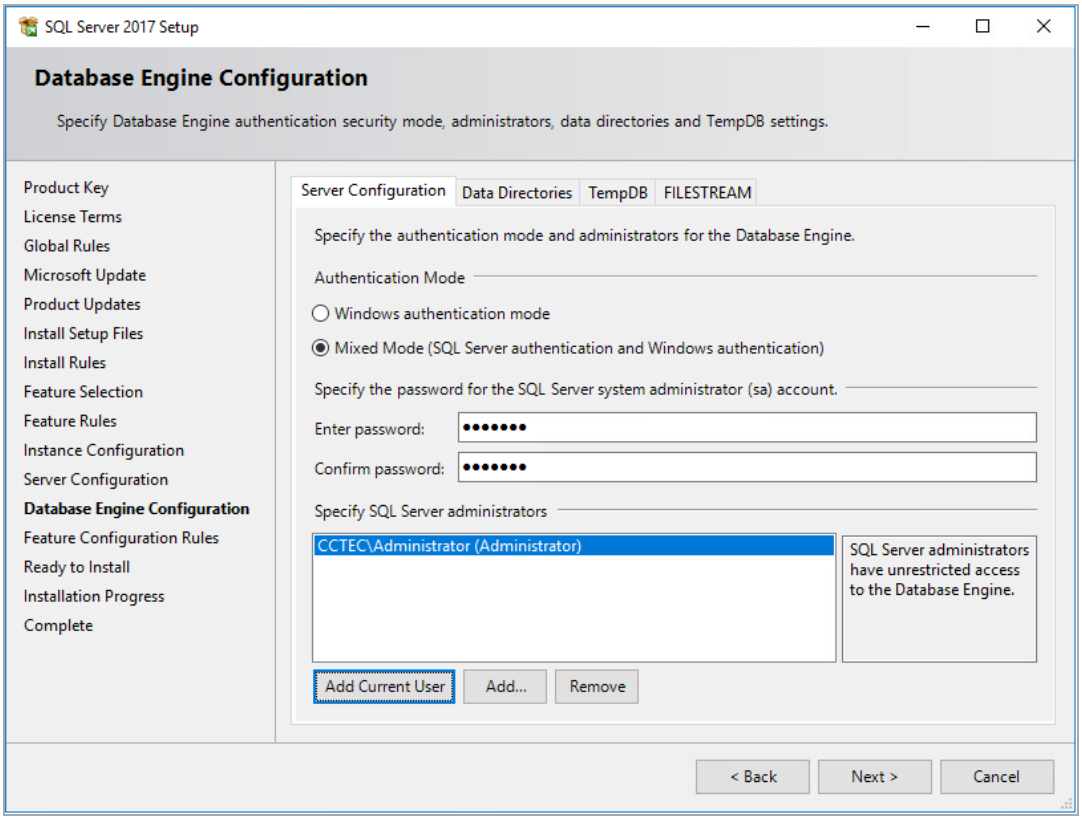
11. On the Feature Selection page, select *Database Engine Services*.
12. In the *Instance root directory*, *Shared feature directory*, and *Shared feature directory (x86)* fields, specify the path where you want to SQL instance to reside, then click *Next*.
13. In the Instance Configuration page, click the Named instance option and specify a descriptive name for the instance such as `FSFDB` and click *Next*.
14. On the Server Configuration page, click the *Collation* tab.
15. Click *Customize*.

16. Click the *Windows collation designator and sort order* option.
17. From the *Collation designator* drop-down menu, select an acceptable collation and settings for your locale.
18. For example, in North America, an acceptable collation would be *Latin1_General_100* with the *Accent-sensitive* check box selected.
19. We recommend that you select a collation that aligns with the Windows locale of the server where the Engine is installed.
20. For more information on collation and locales, refer to this Microsoft document: https://learn.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support.

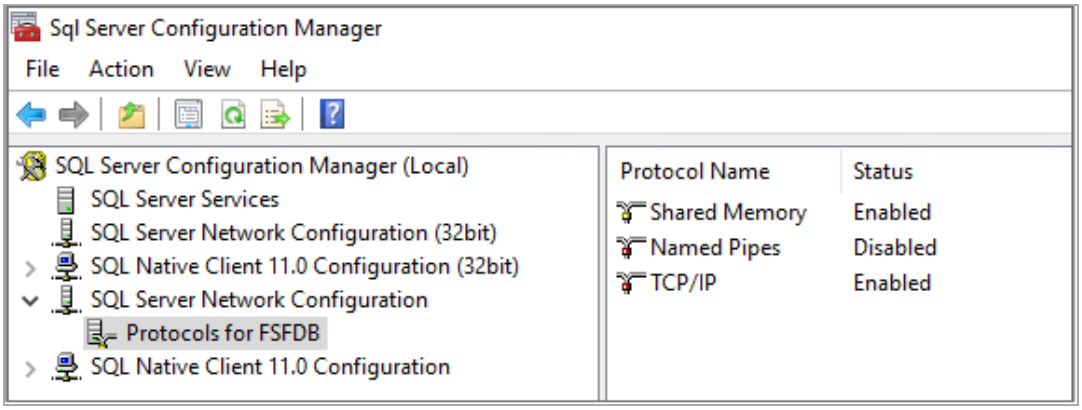


21. Click *OK*.
22. Click *Next*.
23. On the Database Engine Configuration page, select the *Mixed Mode (SQL Server authentication and Windows authentication)* option, enter and confirm

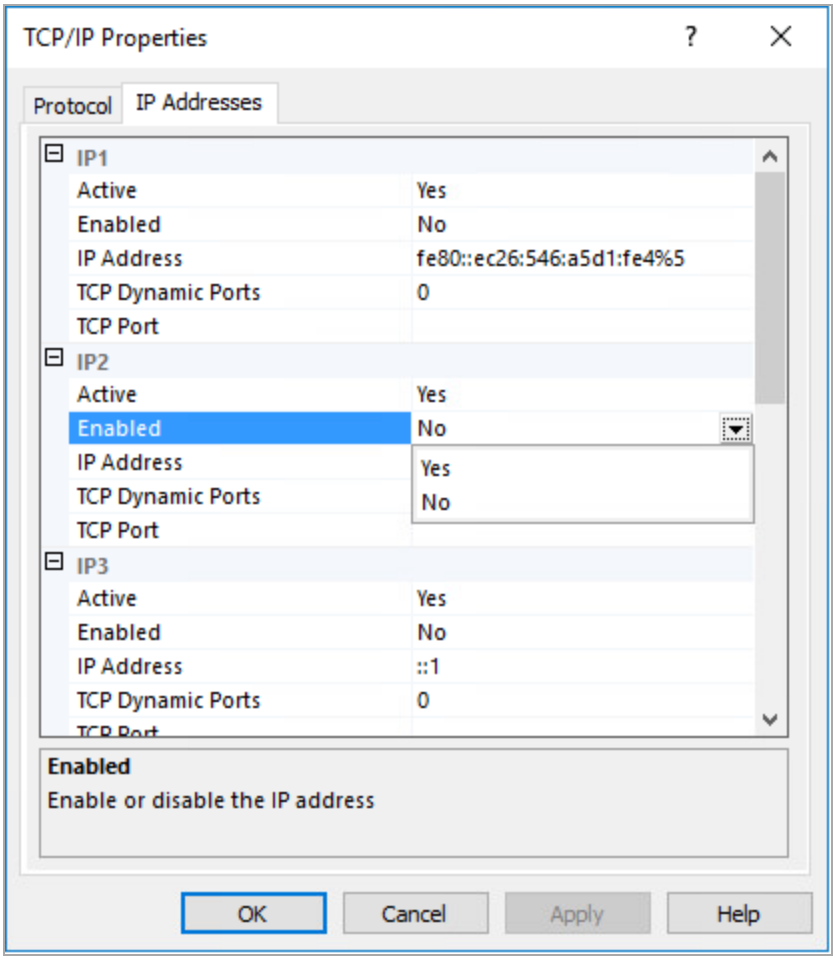
the SQL Server administrator password, then click *Add Current User*.



24. Click *Install*.
25. When the installation has completed, click *Close* to close the wizard.
26. Launch SQL Server Configuration Manager.
27. In the left pane, expand *SQL Server Network Configuration*.
28. Click *Protocols for FSFDB* (or the name of the database instance you chose earlier).

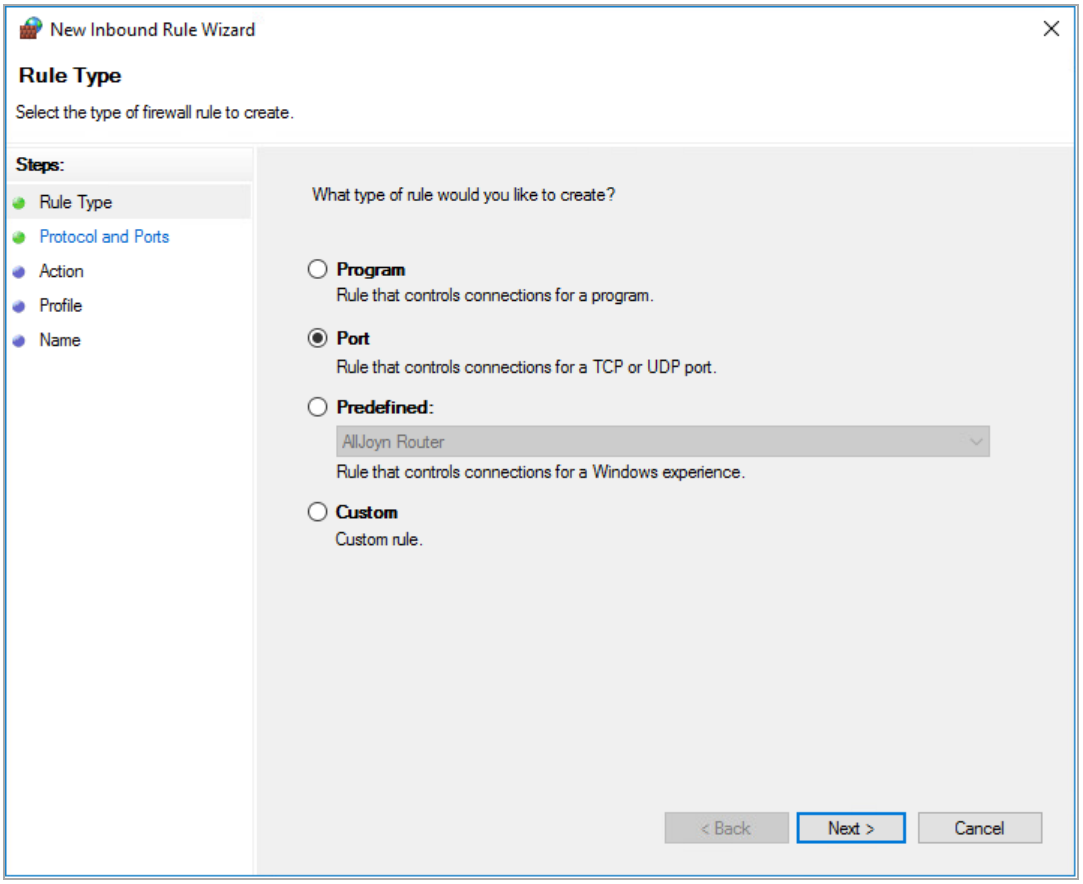


29. Right-click *TCP/IP* and select *Properties*.
30. Click the *IP Addresses* tab.
31. Under the *IP2* heading, for the *Enabled* field, right-click to select the drop-down men and change the setting to *Yes*.



32. Select *TCP Dynamic Ports* and clear the field so there is no number associated to it.
33. Scroll down to the *IPALL* heading and for the *TCP Dynamic Ports* field, clear the field so there is no number associated to it.
34. In the *TCP Port* field, and enter `1433`.
35. Click *Apply*.
36. When the warning dialog box appears, click *OK*.
37. Click *OK* to close the TCP/IP Properties page.
38. Close the SQL Server Configuration Manager.

39. Launch Windows Firewall with Advanced Security.
40. From the left column, click *Inbound Rules*.
41. From the *Actions* column, click *New Rule*.
42. In the Rule Type page, select *Port*.



43. Click *Next*.
44. In the Protocol and Ports page, enter `1433` in the *Specific local ports* field, then click *Next*.
45. In the Action page, accept the default setting by clicking *Next*.
46. In the Profile page, accept the default settings by clicking *Next*.
47. In the Name page, specify a name for the new inbound rule in the *Name* field.
48. For example, `SQL Server`.
49. Click *Finish*.

4.3 - SQL Server Post Configuration

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

- The SQL Server service must be listening via TCP/IPv4 as the Engine requires it 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 TCP port of 1433.
- Firewall rules may need updating.

5 - Installing CouchDB

Apache CouchDB is the NoSQL database that File Dynamics uses for:

- Work Log reports
- Epoch Data protection policies
- Security Policy reporting for Notification, Lockdown and Fencing policies
- Workload reporting

If you do not plan to initially create any of these policies, there is no need to install CouchDB. However, we recommend that you do so anyway so that your system will be ready once you decide to do so.

5.1 - Recommendations

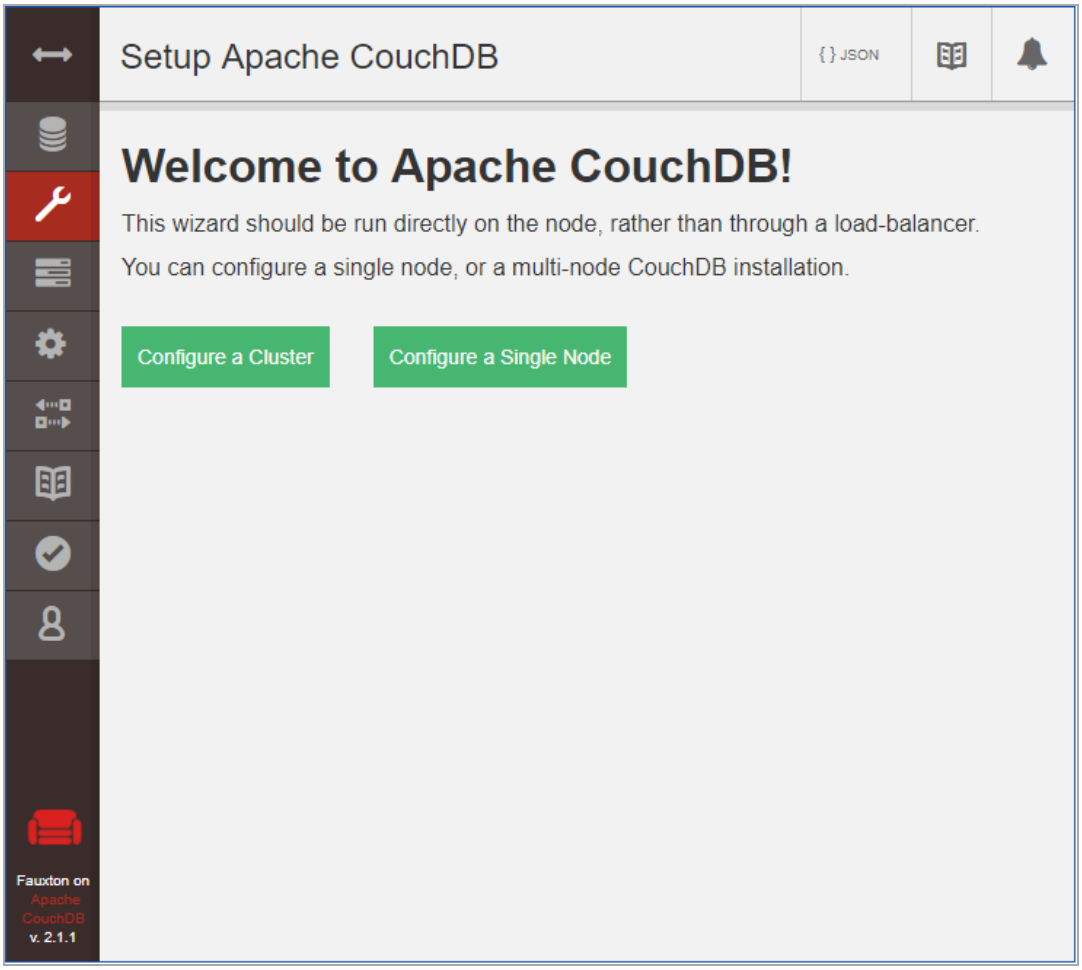
- Disk space requirements depend on a number of variables including the number of policy target paths, the number of files and folders in each target, and the frequency of policy execution.
- OpenText recommends that the CouchDB host be a multi-processor system with a minimum of 4 GB of RAM. If you host CouchDB on a server that also hosts the Engine, Event Monitor, or SQL Server, the RAM requirements are in addition to the RAM for those services.
- While CouchDB may be installed on any of its supported platforms, we only support troubleshooting of CouchDB instances installed on Windows or Linux platforms.

5.2 - Download and Install CouchDB

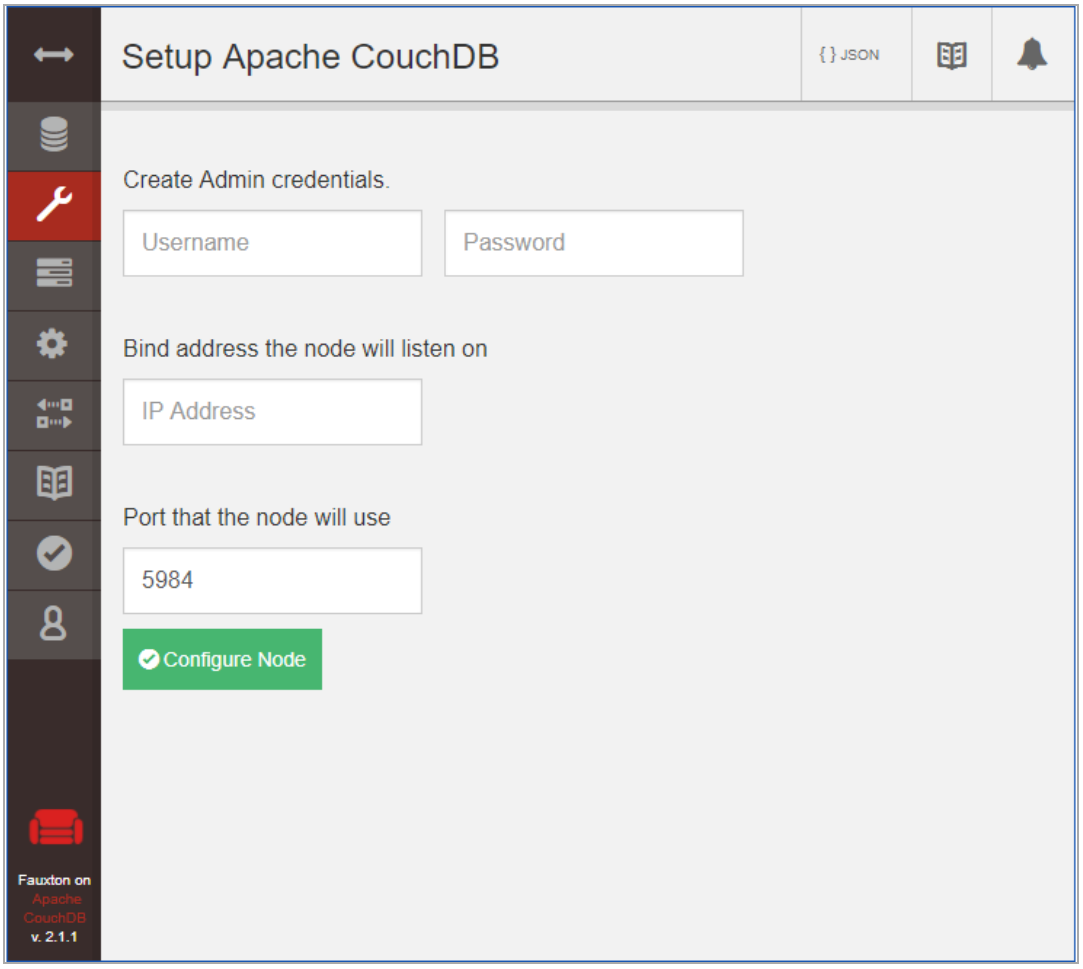
The following are a minimal set of procedures for installing CouchDB.

1. From https://couchdb.apache.org/#download, download the latest version of CouchDB for the server that will host the CouchDB database.
2. Launch the downloaded installation file.
3. Follow the wizard steps to complete the installation. Installation and configuration guides can be found at https://docs.couchdb.org/en/stable/install/index.html.
4. Launch Apache CouchDB Fauxton. This launches the Apache CouchDB administrative interface in a web browser.

5. Click *Setup* (the wrench icon).



6. Click *Configure Single Node*.



7. Specify the Admin credentials entered during installation, or create a new administrator username and password.
8. Leave the IP address setting open or 0.0.0.0, and leave the Port setting at 5984.
9. Click *Configure Node*.

5.3 - Configure CouchDB Integration

Use the File Dynamics Admin Client to configure the CouchDB settings by referring to the appropriate section in the *File Dynamics 6.6 Administration Guide*

- For Security and Workload policies, see Establishing the CouchDB Settings in the Admin Client.

- For the Work Log, see Establishing the Work Log Database Settings in the Admin Client. Establishing the Work Log Database Settings in the Admin Client.

6 - Upgrading to File Dynamics 6.6

File Dynamics 6.6 supports upgrades from version 6.5

To upgrade from an earlier release, first upgrade to File Dynamics 6.5, then perform the upgrade to File Dynamics 6.6.

6.1 - Upgrading from File Dynamics 6.*x*

Upgrading to File Dynamics 6.6 requires updates to all components.

Due to key changes in communication protocols and backend data structures, all components must be upgraded to 6.6 for this release.

While there is no specific order of upgrade required, we generally recommend upgrading components in the following order:

- Engine
- Admin Client
- Event Monitor
- File System Agent
- Phoenix Agent
- Data Owner Client

7 - Installing File Dynamics 6.6

This section provides procedures for installing and configuring the Engine, database, Event Monitor, Agents, and Admin Client. For information on how these components work in a File Dynamics deployment, reference the Overview in the *File Dynamics 6.6 Administration Guide*.

You should follow these procedures only after you have performed the prerequisite tasks in *Installation Prerequisites*, obtained a File Dynamics 6.6 product license as indicated in *Licensing the Product (page 3)*, and installed a SQL Server instance as specified in *Configuring a SQL Server Instance (page 5)*

This section also provides procedures for assigning rights and privileges to the Proxy Rights group that is created when you install the Admin Client.

7.1 - Administrator Access

7.1.1 - Installing Components on Member Servers

In order to successfully configure the Engine, Event Monitor, Agents, and the Data Owner web service, you must be logged in to the member server with an Active Directory domain account that has local Administrators (BUILTIN\Administrators) membership on that server.

7.1.2 - Managing Active Directory Accounts

When configuring the Engine service, you will need to be logged on to the member server with an Active Directory account that has access to create or modify domain groups and a proxy user account. This is in addition to the user also having local Adminstrators group membership.

Typically, having membership in the Domain Admins group of the domain where the Engine server is installed is sufficient. In cases where this is not possible, delegated write and modify access to users and groups in a container may suffice.

7.1.3 - Granting Proxy Access to Resource Servers

For Windows servers hosting managed shares but will not have a File System or Phoenix Agent installed, it is necessary to setup the local Administrators membership and privileges for the proxy account. The user setting this up has the same administrator access requirements as someone configuring an agent on that server.

7.2 - Accessing the Product Contents

1. On the Windows server that will host the Engine, copy to a directory the `FileDynamics_6.6.iso` file that was made available to you following your purchase of File Dynamics 6.6.
2. Mount the `FileDynamics_6.6.iso` file.
3. Note the location of the mounted ISO.
4. This is the installation source you will use to install File Dynamics components.

7.3 - Installing the Engine

File Dynamics uses only one Engine per forest. The Engine can be installed on host server that meets the following **minimum** requirements:

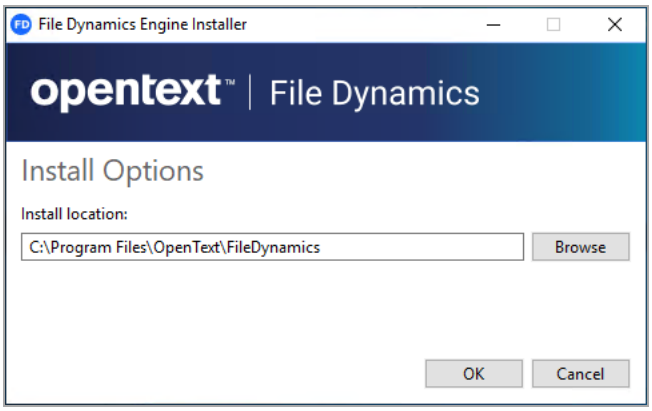
- Microsoft Windows Server 2022 (Member Server)
- Microsoft Windows Server 2019 (Member Server)
- At least 8 GB RAM
    - 4 GB for the Engine service
    - 4 GB for the Data Owner web service installed with the Engine
- For quota management, Microsoft File System Resource Manager (FSRM) must be installed; see File Server Resource Manager in the *File Dynamics6.6 Administration Guide*.
- Forest functional level of Windows Server 2003 or later

Other notable information about the Engine:

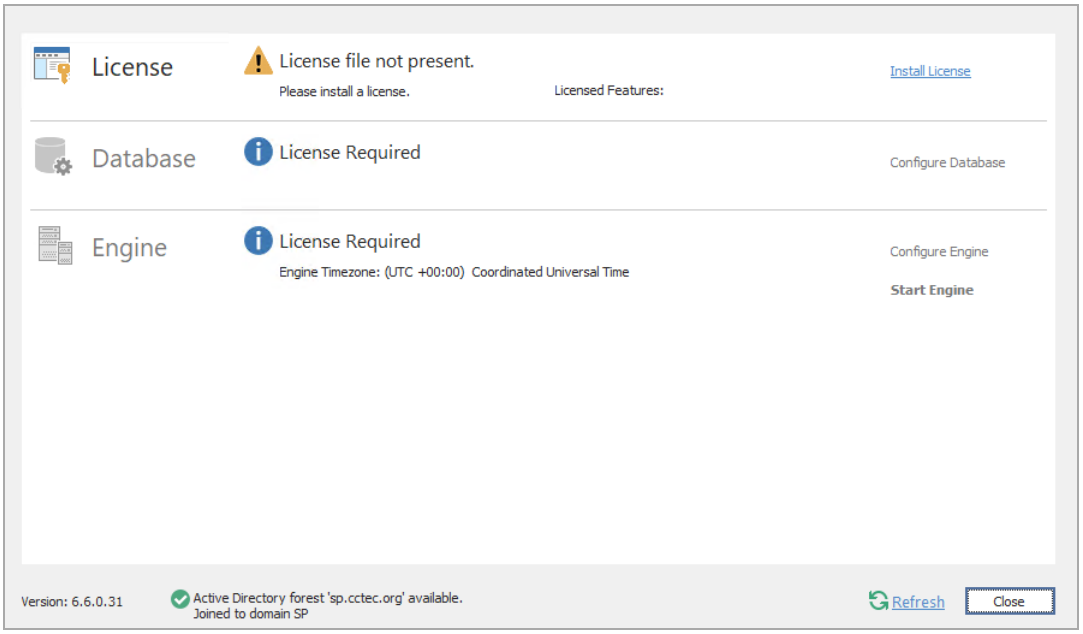
- The Engine runs as a native NT service that is configured to start by using the Local System account
- The default Engine port is 3009
- The firewall inbound rule is added during the Engine installation

1. At the root of the `FileDynamics_6.6.iso` image, double-click File Dynamics-Engine-6.6-xx.exe.
2. When you are asked if you want to run this file, click *Run*.
3. Agree to the licensing terms and conditions.

4. (Conditional) If you want to install the Engine to a location other than the default path, click *Options*.



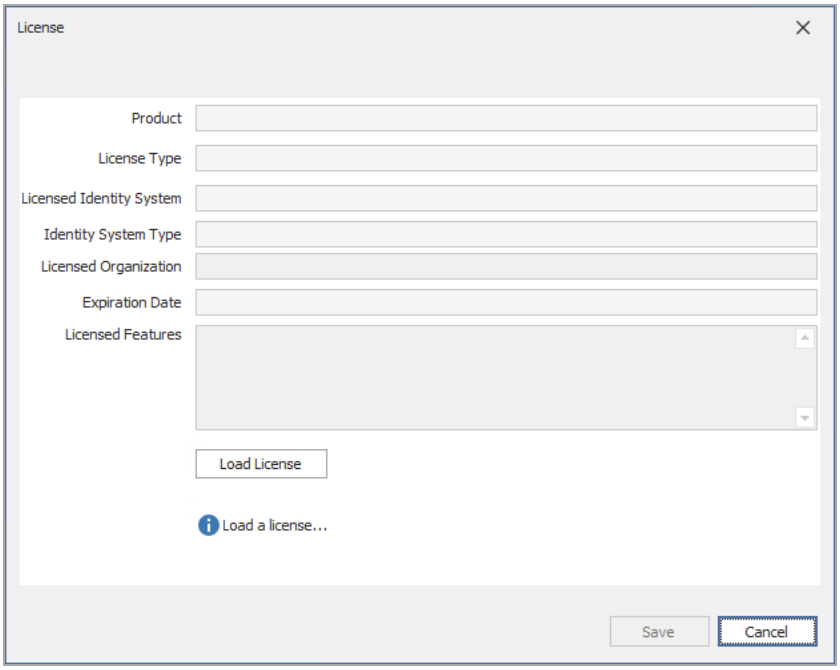
5. In the *Install location* field, specify the new path and click *OK*.
6. Click *Install*.
7. Read the overview on the initial page of the wizard and click *Next*.
8. Click *Install*.
9. Click *Finish* to close the wizard.
10. The Install Successful message indicates that the Engine and Config Utilities were installed successfully.
11. Click *Run Configuration Utility*.
12. The Configuration Utility is launched.



7.4 - Installing or Updating the License

7.4.1 - Installing a New License

1. In the Configuration Utility, click *Install or Update License*.
2. The License dialog box appears.



3. If no license is found, the license properties will be empty.
4. Click *Load License*, then browse to and select the license file.
5. When the confirmation prompt appears, click *Yes*.
6. Examine the license properties to ensure that the license is valid.
7. Click *Close*.

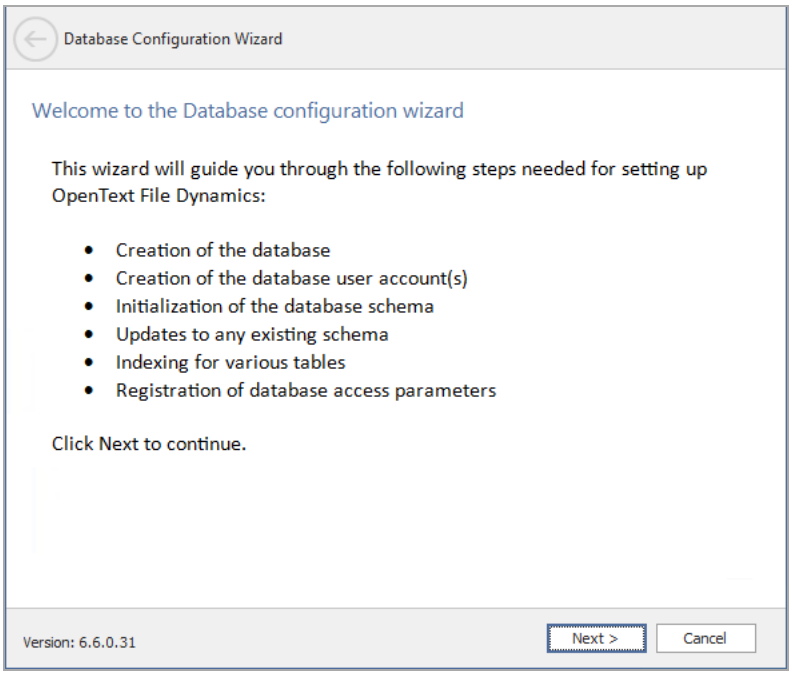
7.4.2 - Updating the License

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

To replace an existing license simply install a new one by following the instructions in the previous section *Installing a New License (page 22)*.

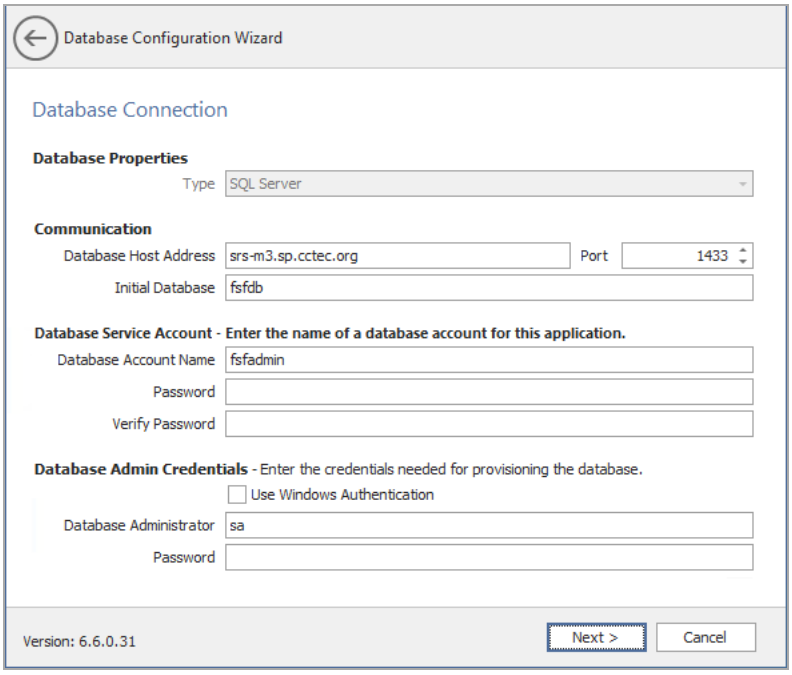
7.5 - Configuring the Database

1. In the Configuration Utility, click *Configure Database*.



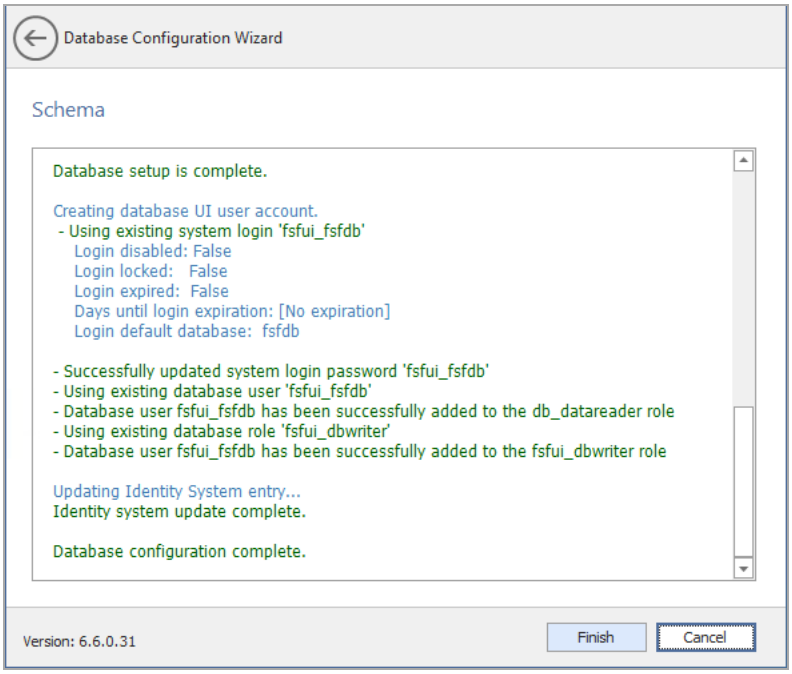
2. The page indicates what database configuration tasks are to be completed in this wizard.
3. From the wizard page, read the overview of what will be configured and click *Next*.

4. The following page appears:



5. This page lets you establish the settings needed for the Engine to communicate with the database.
6. **Database Properties:** Displays information on the database.
7. **Type:** Displays the supported database.
8. **Communication:** Specifies address, port number, and name of the database.
9. **Database Host Address:** Specify the host address of the server where the database is installed.
10. **Port:** The default SQL Server port setting is 1433. If there is a port conflict, you can change it.
11. **Initial Database:** The default name of the File Dynamics database.
12. **Database Service Account:** Use this region to set authentication information for the database service account, which is the database account that the Engine uses to sign in to the database.
13. **Database Account Name:** By default, the database account is fsfadmin, which you can change in this field.
14. **Password:** Specify a password for the service account to connect to the database.

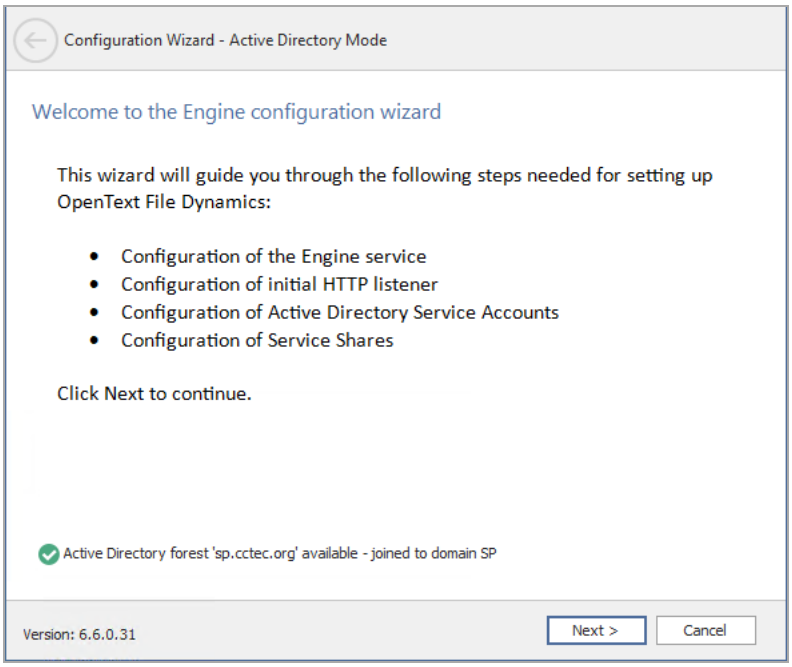
15. **Verify Password:** Specify the password again in this field.
16. **Database Admin Credentials:** Use this region to establish the database administrator name and credentials.
17. **Use Windows Authentication:** Selecting this check box specifies that you want to configure the database using the authentication credentials of a Windows network administrator, rather than the credentials of a SQL Server database administrator. Selecting this check box disables the *Database Administrator* and *Password* fields.
18. **Database Administrator:** Specify the SQL Server administrator name.
19. **Password:** Specify the SQL Server administrator password.
20. Complete the fields and click *Next*.



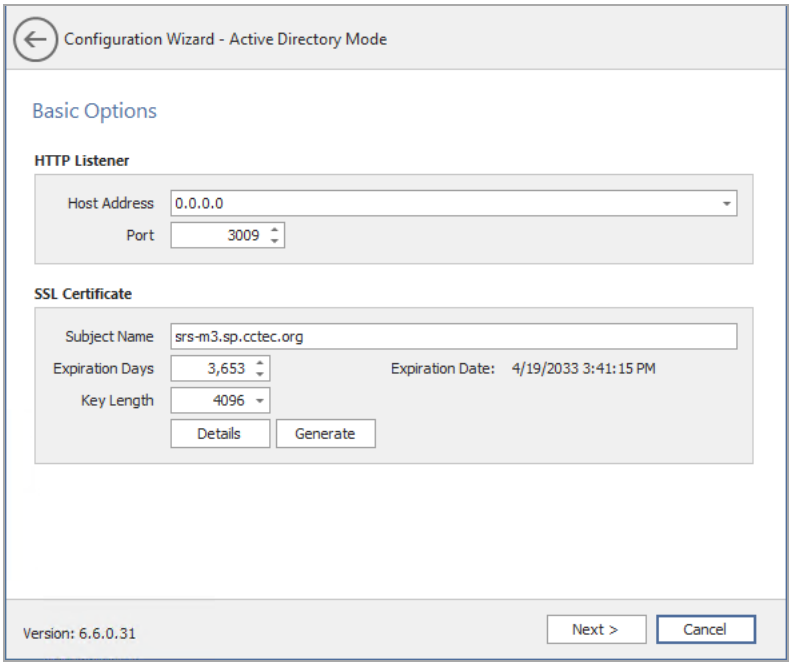
21. Review the configuration log and click *Finish*.

7.6 - Configuring the Engine

1. In the Configuration Utility, click *Configure Engine*.

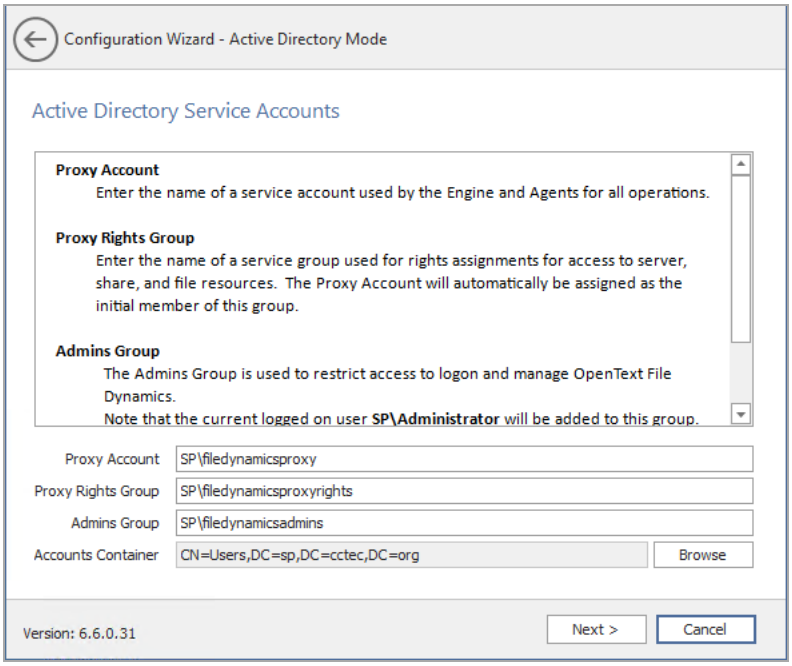


2. From the wizard page, read the overview of what will be configured and click *Next*.



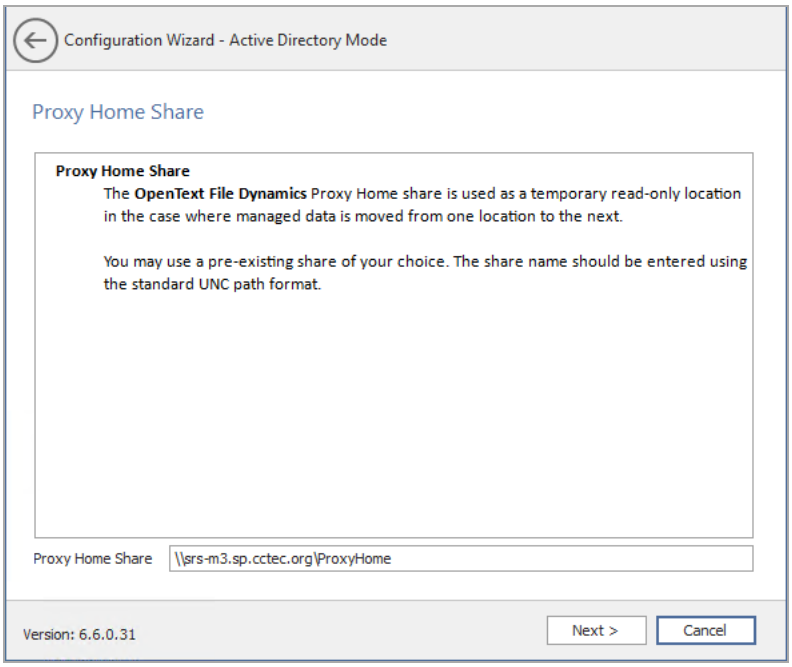
3. This page lets you confirm or change basic Engine configuration settings.

4. **HTTP Listener:** Communication parameters for the Engine.
5. **Host Address:** To listen to all addresses, leave the setting at 0.0.0.0. To limit listening to a specific address, enter the address here.
6. **Port:** The default port is 3009.
7. **SSL Certificate:** Details for the SSL certificate that will be generated.
8. **Subject Name:** The name of the certificate that will be generated. The server name is listed by default.
9. **Expiration Days:** The life span of the security certificate, which is set at 10 years by default.
10. **Key Length:** The SSL certificate encryption setting, which is set at 2048 by default.
11. **Details:** Click the button to view the certificate data.
12. **Generate:** If you modify any of the settings in the SSL Certificate region, click this button to generate a new certificate.
13. Edit any needed parameters settings and click *Next*.



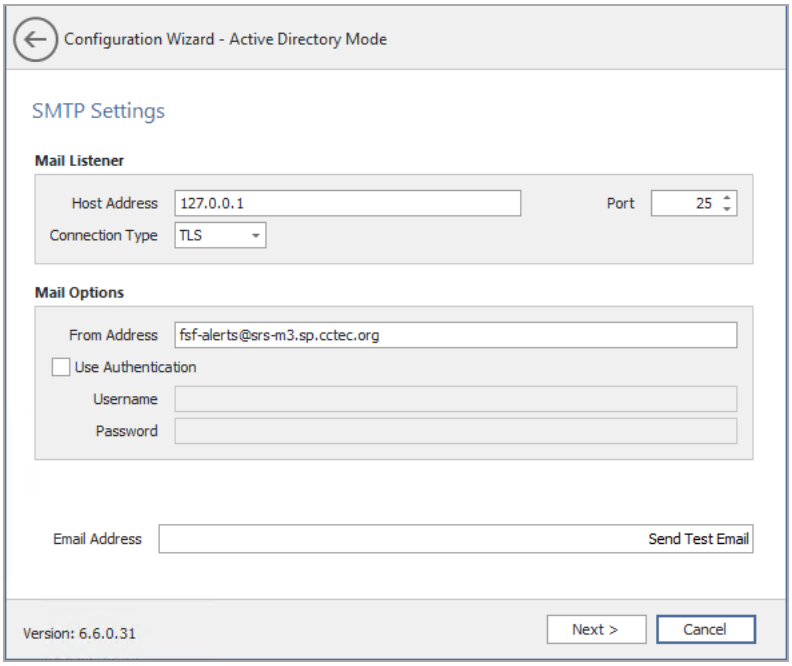
14. This page lets you establish a name for the Proxy Account, Proxy Rights, and Admins Groups.
15. File Dynamics uses proxy accounts so that it can perform tasks necessary for storage management.

16. Because you will want to create the proxy objects in an Active Directory container appropriate to your environment, you can specify the container using the *Browse* button.
17. In this example, the proxy objects are being created in the Service Accounts container.
18. Establish your proxy account settings and click *Next*.



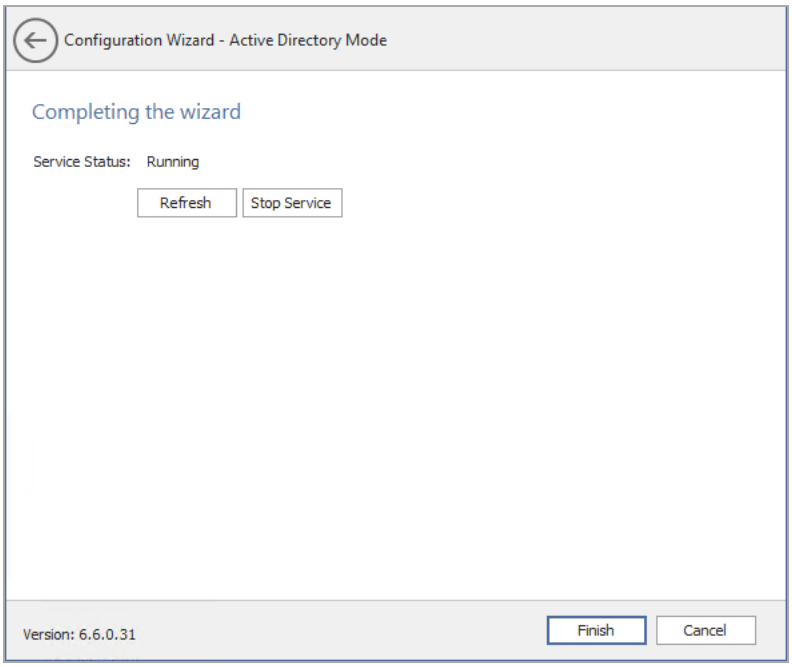
19. The Proxy Home Share that you establish in this page is the read-only location where users' managed path attributes are temporarily set when data is moved because of a change in policy.

20. Click *Next*.



21. Target-Driven security policies allow for email notifications to be sent to designated recipients. These notifications are sent to your email server to be relayed.
22. Completing fields in this page is optional.
23. **Mail Listener:** These fields specify information pertaining to the mail server that is sending alerts.
24. **Host Address:** Specify the IP address or DNS name of the mail server.
25. **Port:** Specify the port number for the mail server.
26. **Connection Type:** From the drown-down menu, select the encryption type used by your mail server.
27. **Mail Options:** These fields specify additional mail information.
28. **From Address:** This field specifies the default address where the alerts come from.
29. **Use Authentication:** In most cases, SMTP will require authentication. Selecting this check box activates the *Username* and *Password* fields where you can enter the credentials for authenticating to the SMTP server.
30. **Email Address:** Specify an email address for a test alert.

31. **Send Test Email:** Click this button to send a test email to the recipient specified in the Email Address field.
32. OpenText recommends that a specialized email account be used such as an alerts@domain or no-reply@domain account if authentication is required for relay. You might need to contact your email administrator for the correct settings.
33. Establish your SMTP settings and click *Next*.



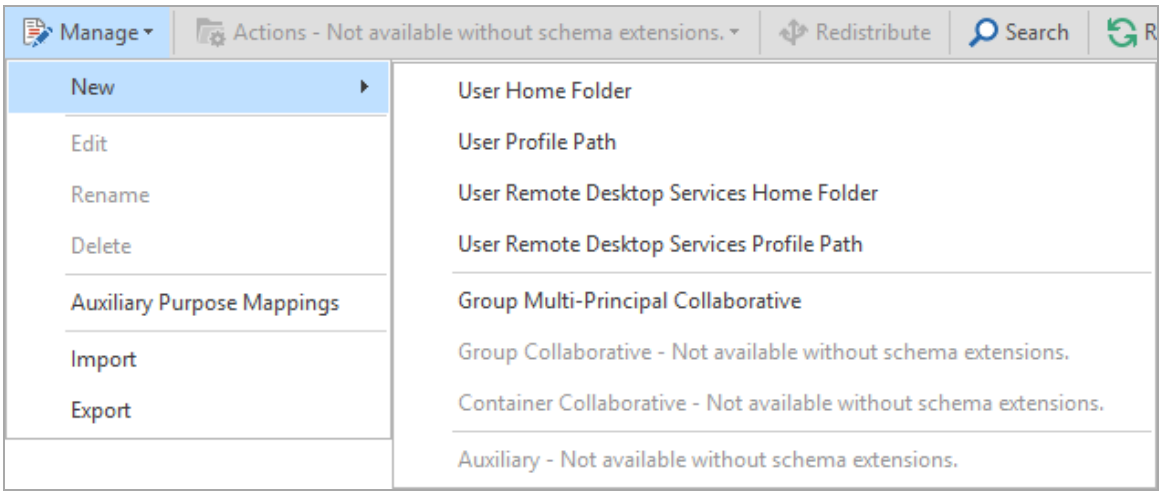
34. Click *Finish*.

7.7 - Active Directory Schema

The Microsoft Active Directory schema contains formal definitions of every object class that can be created in an Active Directory forest. The schema also contains formal definitions of every attribute that can exist in an Active Directory object.

To enable collaborative storage or auxiliary storage management, File Dynamics extends the Active Directory schema to enable File Dynamics attributes. These attributes are specified in Active Directory Schema Extensions in the *File Dynamics 6.6 Administration Guide*.

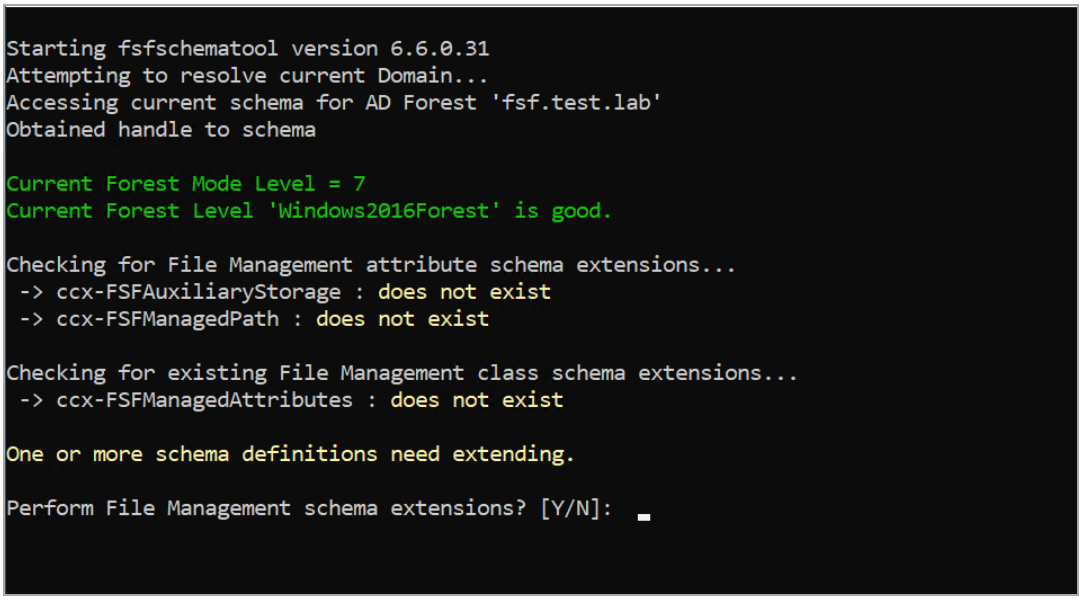
The dimmed options in the menu in the graphic below display which policy types require that the Active Directory schema be extended.



For example, User Home Folder policies do not require an Active Directory schema extension; Group Collaborative policies do.

7.7.1 - Extending the Active Directory Schema

1. Log in to the forest or domain as a user with Schema administration privileges.
2. You can do this by being a member of the Schema Admins group.
3. From the *Start* menu, select *File Dynamics* > *File Dynamics Schema Utility*.
4. When you are asked if you want to run this file, click *Run*.



5. Type `Y` to extend the schema.

```
Starting fsfschematool version 6.6.0.31
Attempting to resolve current Domain...
Accessing current schema for AD Forest 'fsf.test.lab'
Obtained handle to schema

Current Forest Mode Level = 7
Current Forest Level 'Windows2016Forest' is good.

Checking for File Management attribute schema extensions...
 -> ccx-FSFAuxiliaryStorage : does not exist
 -> ccx-FSFManagedPath : does not exist

Checking for existing File Management class schema extensions...
 -> ccx-FSFManagedAttributes : does not exist

One or more schema definitions need extending.

Perform File Management schema extensions? [Y/N]:  y

Extending any missing File Management schema...
Successfully added attribute 'ccx-FSFAuxiliaryStorage
Successfully added attribute 'ccx-FSFManagedPath
Successfully added class 'ccx-FSFManagedAttributes'
Setting Attribute Security GUID to:  cd55682f-3987-446d-a18e-cfd8d53b95f2
Setting Attribute Security GUID to:  cd55682f-3987-446d-a18e-cfd8d53b95f2
All File Management schema successfully extended!
Refreshing schema cache...
Press any key to exit
```

7.8 - Granting Access to Managed Storage

File Dynamics must have the proper rights set on each network share that it will manage; this is, shares that contain managed home folders or collaborative storage. In addition, certain privileges must be granted to File Dynamics on each server where storage will be managed.

7.8.1 - Granting Rights

Every share to be managed by File Dynamics must have proper rights assigned to the Proxy Rights group.

1. As a user with privileges to manage shares, authenticate to the server where the storage is located.
2. Grant Full Control sharing privileges to the Proxy Rights group for each share that File Dynamics will manage.
3. Do one of the following:

4. If you are proxying storage on a member server, go to *Granting Privileges on a Member Server (page 33)*.
5. If you are proxying storage on a domain controller, go to *Granting Privileges on a Domain Controller (page 33)* .

7.8.2 - Granting Privileges on a Member Server

Every server that has storage managed by File Dynamics must have certain privileges granted to the Proxy Rights group. If you install the Agent on a server, this privilege assignment is made automatically. If you use the Agent on one server to act as a Proxy Agent on another server—rather than installing an Agent on that server—you need to manually assign these privileges on that server.

1. Authenticate to a domain controller within the domain where the storage is located.
2. Be sure to log in as a domain administrator.
3. At any domain controller or any computer where the Admin or Remote Server administration tools are installed, click *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
4. This brings up the Active Directory Users and Computers page.
5. In the left pane, select the container where the server is so that it is listed in the right pane.
6. In the right pane, right-click the server and select *Manage*.
7. This brings up the Computer Management page.
8. In the left pane, expand *Local Users and Groups*.
9. Select *Groups*.
10. In the right pane, double-click *Administrators*.
11. This brings up the Administrators Properties dialog box.
12. Click *Add*.
13. This brings up the Select Users, Computers, or Groups dialog box.
14. In the *Enter the object names to select* field, type: `domain_name\[Proxy Rights group name]`.
15. Click *OK* to save the setting.

7.8.3 - Granting Privileges on a Domain Controller

Every server that has storage managed by File Dynamics must have certain privileges granted to the Proxy Rights group. If you install the Agent on a server,

this privilege assignment is made automatically. If you use the Agent on one server to act as a Proxy Agent on another server—rather than installing an Agent on that server—you need to manually assign these privileges on that server.

1. Authenticate to a domain controller within the domain where the storage is located.
2. Be sure to log in as a domain administrator.
3. Launch Active Directory Users and Computers.
4. This brings up the Active Directory Users and Computers page.
5. In the left pane, select *Builtin*.
6. In the right pane, double-click the *Administrators* group.
7. Click the *Members* tab.
8. Click *Add*.
9. In the *Enter the object names to select* field, type the Proxy Rights group name.
10. Click *Check Names*.
11. Click *OK*.
12. Click *OK*.

7.9 - Installing the Event Monitor

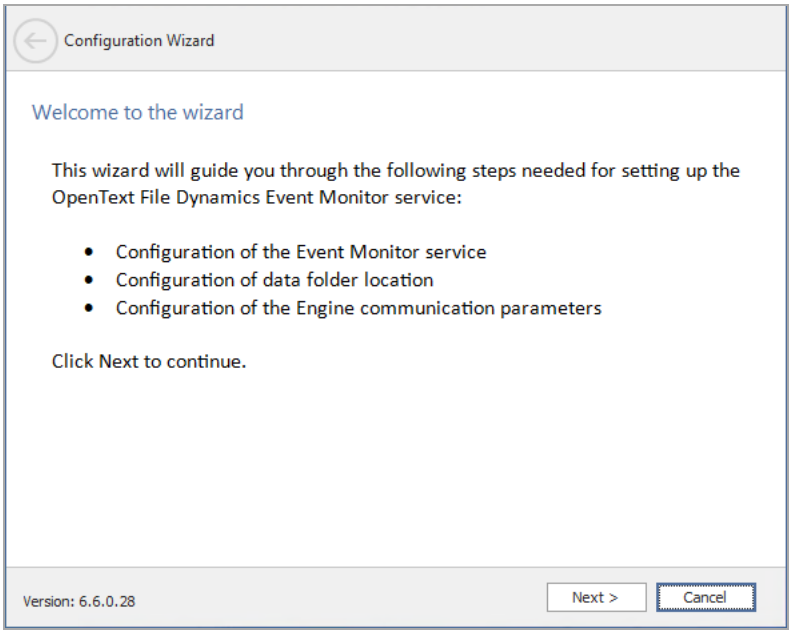
The Event Monitor can be installed on a Windows Server machine that meets the following minimum requirements:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019 (Member Server)
- At least 4 GB RAM, more maybe required for larger environments
- At least 4 processor cores, more maybe required for larger environments
- Forest functional level 2003 or later in native mode

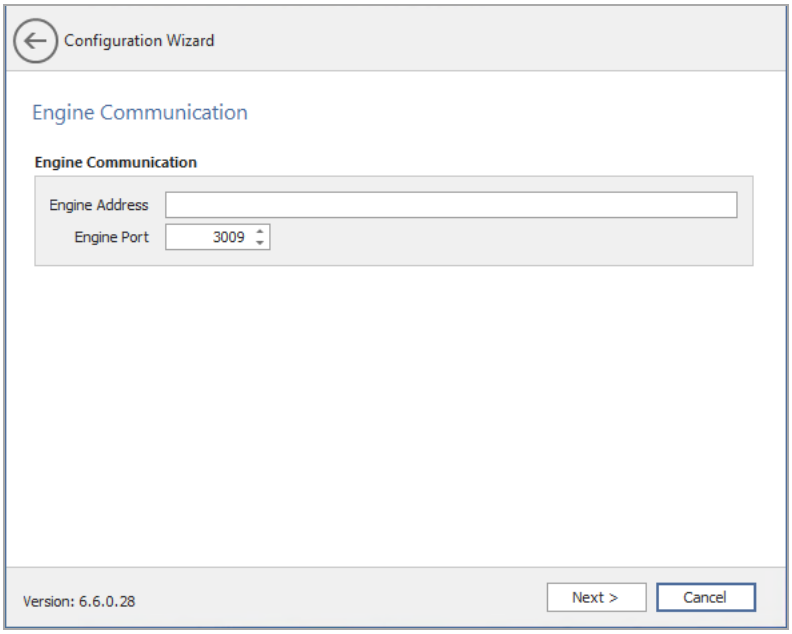
Other notable information about the Event Monitor:

- There is only one Event Monitor per domain
- The Event Monitor runs as a native NT service that is configured to start by using the Local System account
- The Event Monitor must be permitted to make outbound connections through the firewall

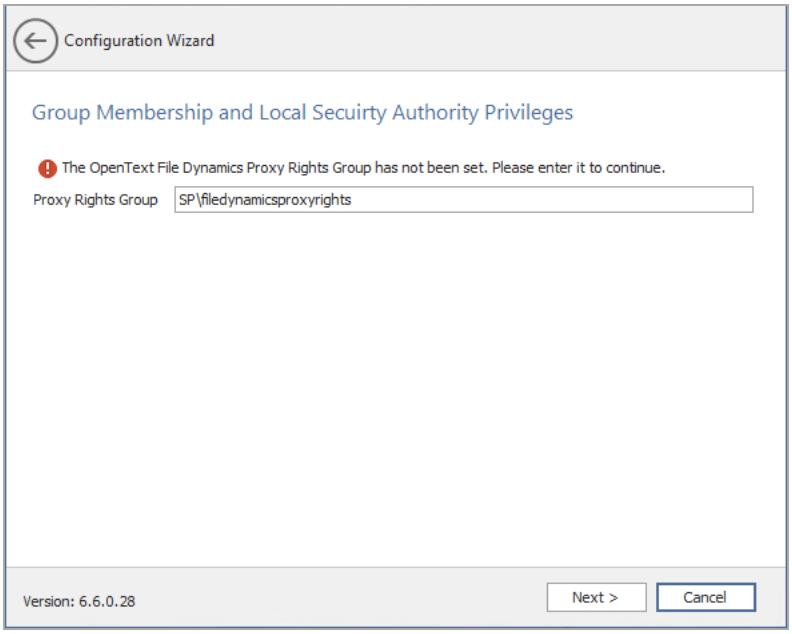
1. On the Windows server that will host the Event Monitor, copy to a directory the `FileDynamics_6.6.iso`.
2. Mount the `FileDynamics_6.6.iso` file.
3. At the root of the `FileDynamics_6.6.iso` image, double-click `File Dynamics-EventMonitor-6.6-xx.exe`.
4. When you are asked if you want to run this file, click *Run*.
5. Agree to the licensing terms and conditions and click *Install*.
6. When notified that the setup was successful, click *Run Configuration Utility*.



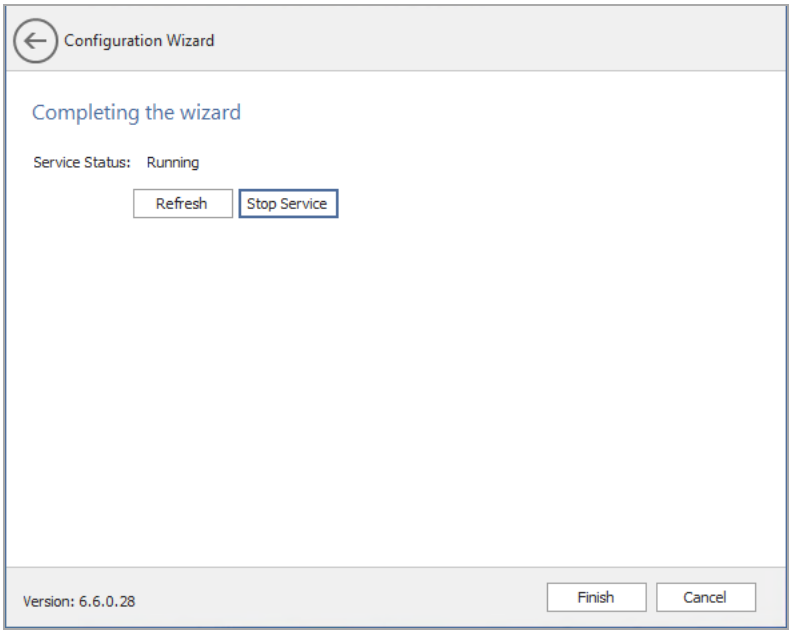
7. From the wizard page, read the overview of the setup steps and click *Next*.



8. This page lets you set parameters for the Event Monitor to communicate with the Engine.
9. **Engine Address:** Specify the DNS name or IP address to the server hosting the Engine here.
10. **Engine SSL Port:** Specify the SSL port for the Engine here.
11. Enter the Engine connection settings and click *Next*.



12. (Conditional) If you chose a name that was not the default name for the Proxy Rights group, enter the name in the *Proxy Rights Group* field.
13. Click *Next*.



14. Click *Finish*.
15. The Event Monitor is now installed and running. You must still authorize it using the Admin Client. For procedures, see *Authorizing the Event Monitor (page 47)*.

7.10 - Installing File System Agents

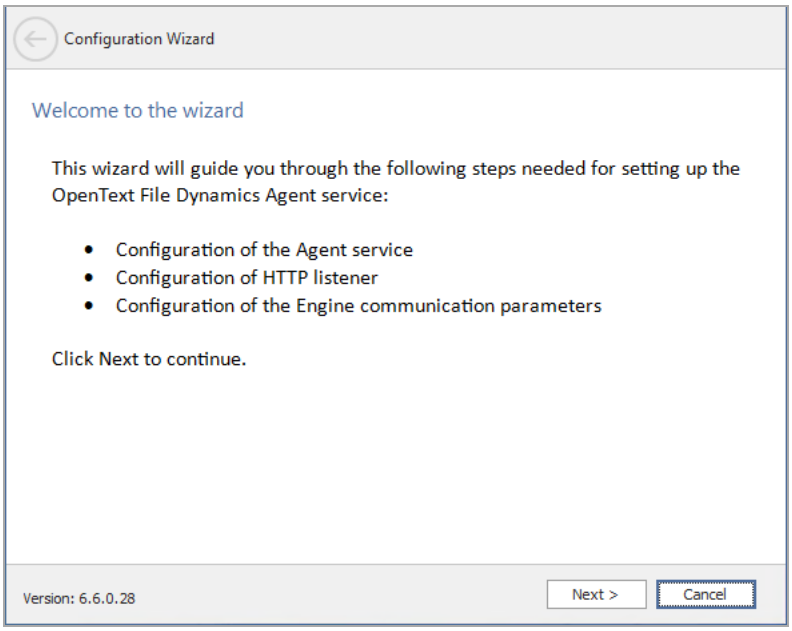
A File System Agent can be installed on a Windows Server machine that meets the following minimum requirements:

- Microsoft Windows Server 2022 (Member Server)
- Microsoft Windows Server 2019 (Member Server)
- Microsoft Windows Server 2016 (Member Server)
- At least 4 GB RAM
- For quota management, Microsoft File System Resource Manager (FSRM) must be installed
- See File Server Resource Manager in the *File Dynamics 6.6 Administration Guide*.

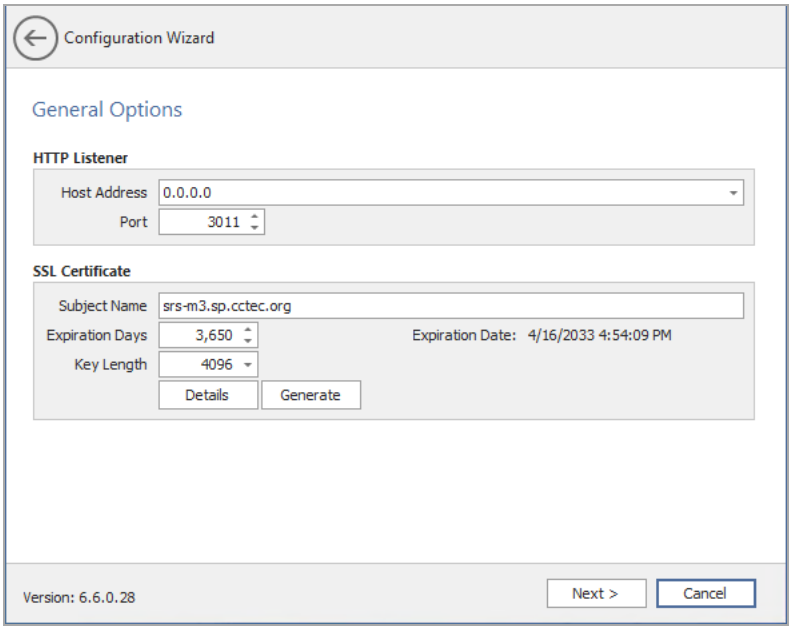
Other notable information about File System Agents:

- A File System Agent runs as a native NT service that is configured to start by using the Local System account
- The default File System Agent port is 3011
- A firewall inbound rule for the File System Agent is created during the installation

1. On the Windows server that will host the File System Agent, copy to a directory the `FileDynamics_6.6.iso`.
2. Mount the `FileDynamics_6.6.iso` file.
3. At the root of the `FileDynamics_6.6.iso` image, double-click `File Dynamics-FileSystemAgent-6.6-xx.exe`.
4. When you are asked if you want to run this file, click *Run*.
5. Agree to the licensing terms and conditions and click *Install*.
6. When notified that the setup was successful, click *Run Configuration Utility*.

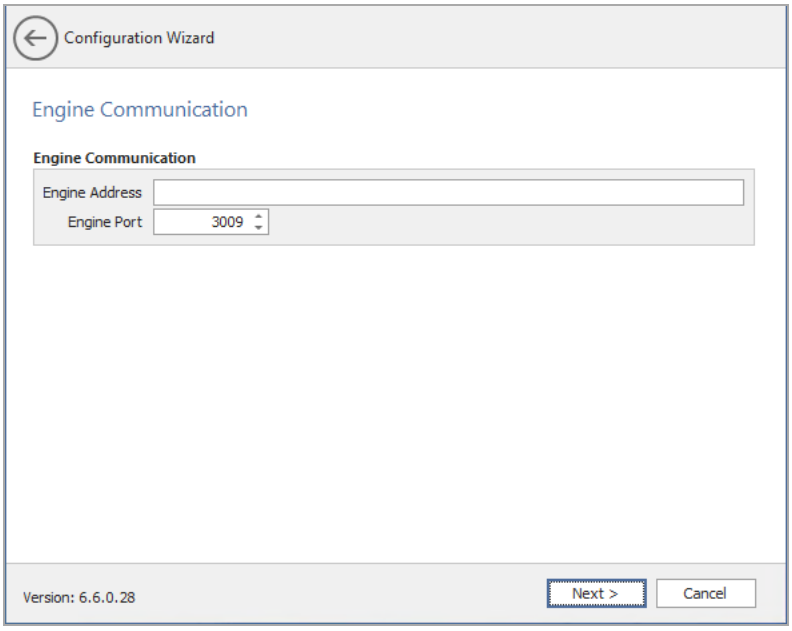


7. From the wizard page, read the overview of the setup steps and click *Next*.

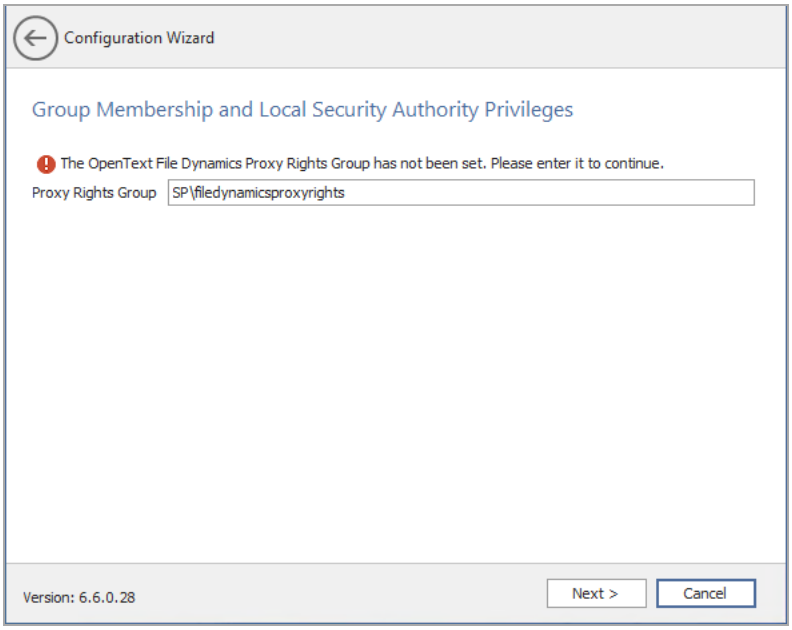


8. This page lets you confirm or change basic File System Agent configuration settings.
9. **HTTP Listener:** Communication parameters for the File System Agent.
10. **Host Address:** To listen to all addresses, leave the setting at 0.0.0.0. To limit listening to a specific address, enter the address here.
11. **Port:** The default port is 3011.
12. **SSL Certificate:** Details for an SSL certificate that will be generated.
13. **Subject Name:** The name of the certificate that will be generated. The server name is listed by default.
14. **Expiration Days:** The life span of the security certificate, which is set at 10 years by default.
15. **Key Length:** The SSL certificate encryption setting, which is set at 2048 by default.
16. **Details:** Click the button to view the certificate data.
17. **Generate:** If you modify any of the settings in the SSL Certificate region, click this button to generate a new certificate.

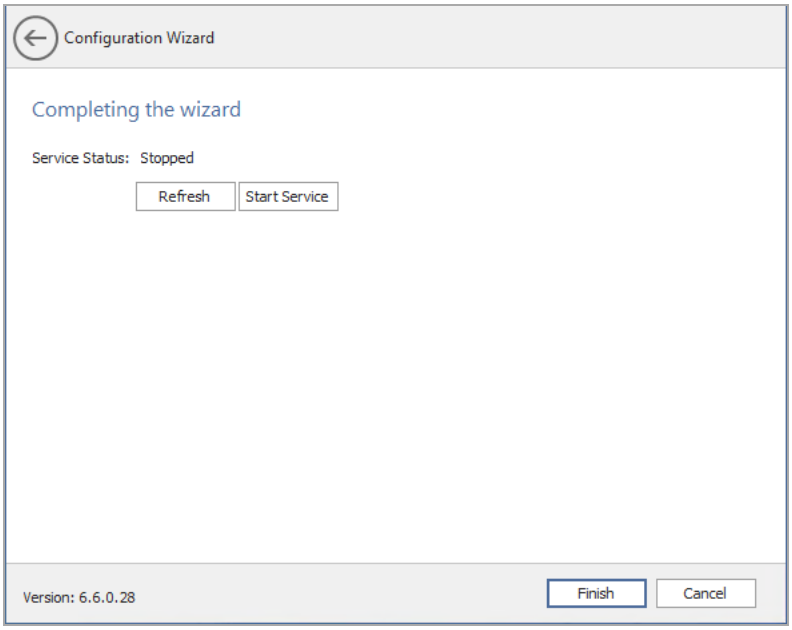
18. Edit any needed parameters settings and click *Next*.



19. This page lets you set parameters for the File System Agent to communicate with the Engine.
20. **Engine Address:** Specify the DNS name or IP address to the server hosting the Engine here.
21. **Engine SSL Port:** Specify the SSL port for the Engine here.
22. Enter the Engine connection settings and click *Next*.



23. (Conditional) If you chose a name that was not the default name for the File Dynamics Proxy Rights group, enter the name in the *Proxy Rights Group* field.
24. Click *Next*.



25. Click *Finish*.
26. The File System Agent is now installed, configured, and running. You must still authorize it using the Admin Client. For procedures, see *Authorizing the Agents (page 47)*.

7.11 - Installing Phoenix Agents

Phoenix Agents execute the jobs necessary for Epoch Data Protection policies that are managed by the Engine as well as performing scans for Security Notification policies. If you are deploying Epoch Data Protection, a Phoenix Agent must be either deployed on or associated to (via proxy assignment) each server or NAS device where protected high-value targets are located on the network.

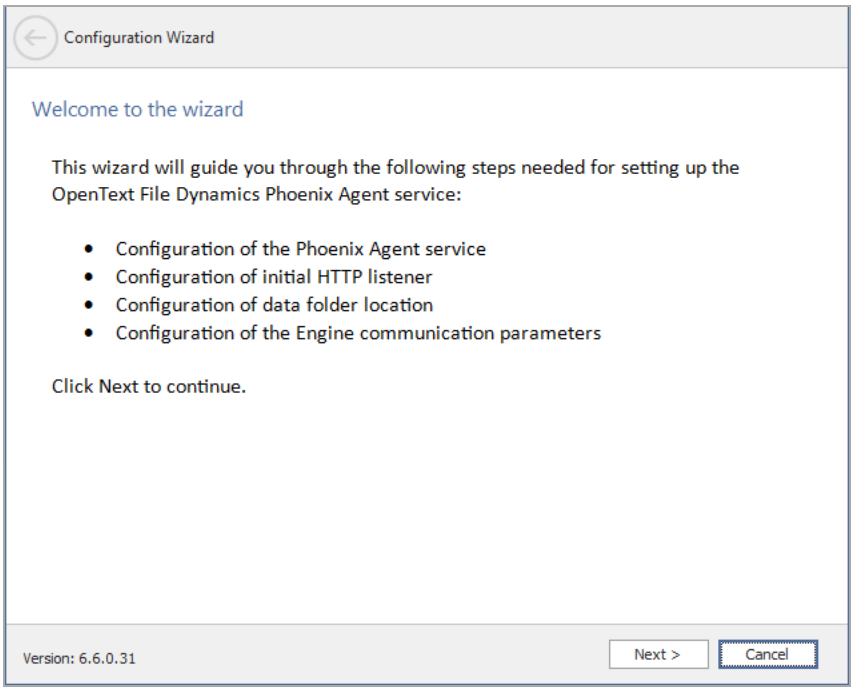
A Phoenix Agent can be installed on a Windows Server machine that meets the following minimum requirements:

- Microsoft Windows Server 2022 (Member Server)
- Microsoft Windows Server 2019 (Member Server)
- Microsoft Windows Server 2016 (Member Server)
- At least 4 GB RAM

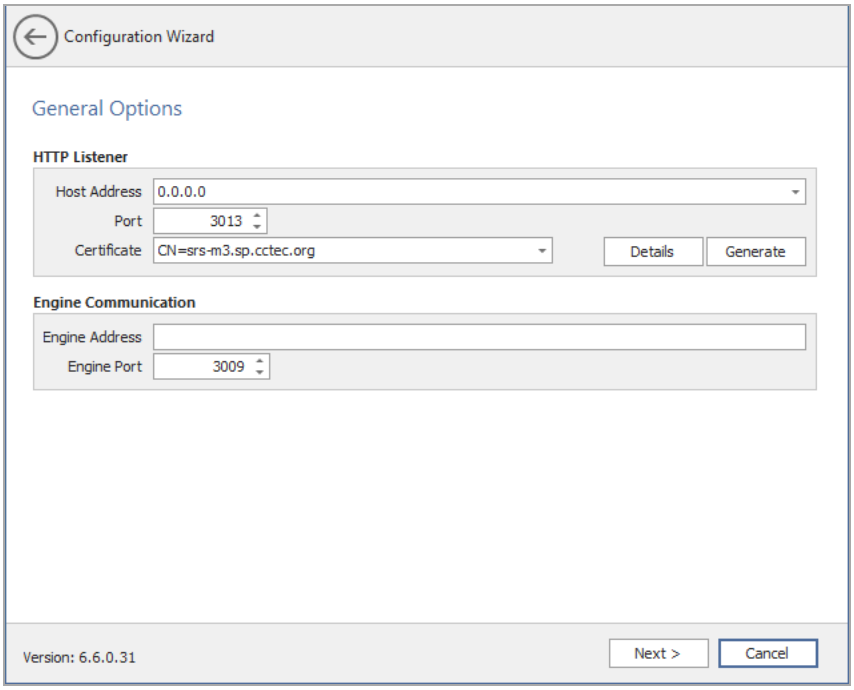
Other notable information about Phoenix Agents:

- A Phoenix Agent runs as a native NT service that is configured to start by using the Local System account
- The default Phoenix Agent port is 3013
- A firewall inbound rule for the Phoenix Agent is created during the installation

1. On the Windows server that will host the Phoenix Agent, copy to a directory the FileDynamics_6.6.iso.
2. Mount the `FileDynamics_6.6.iso` file.
3. At the root of the `FileDynamics_6.6.iso` image, double-click `File Dynamics-PhoenixAgent-6.6-xx.exe`.
4. When you are asked if you want to run this file, click *Run*.
5. Agree to the licensing terms and conditions and click *Install*.
6. When notified that the setup was successful, click *Run Configuration Utility*.

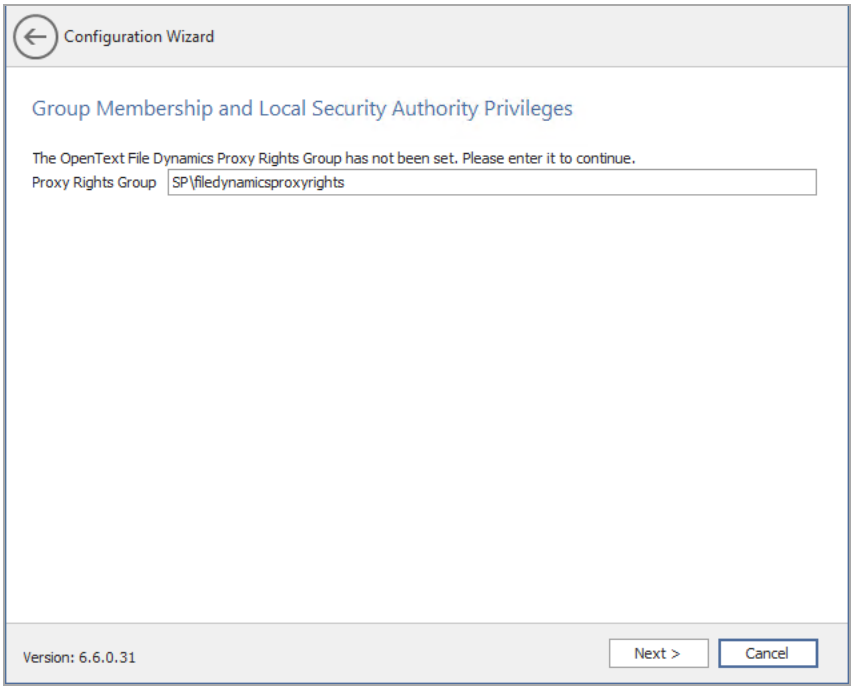


7. From the wizard page, read the overview of the setup steps and click *Next*.



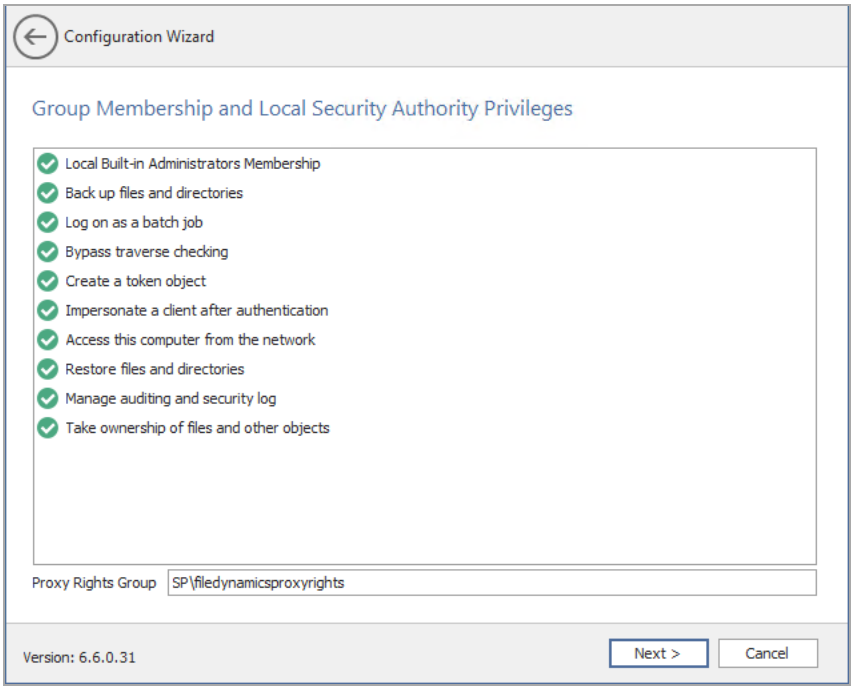
8. This page lets you confirm or change basic Phoenix Agent configuration settings.
9. **HTTP Listener:** Communication parameters for the Phoenix Agent.
10. **Host Address:** To listen to all addresses, leave the setting at 0.0.0.0. To limit listening to a specific address, enter the address here.
11. **Port:** The default port is 3013.
12. **Certificate:** Details for an SSL certificate that will be generated.
13. **Details:** Click the button to view the certificate data.
14. **Generate:** If you modify any of the settings in the SSL Certificate region, click this button to generate a new certificate.
15. **Engine Communication:** Communication information for the Engine host.
16. **Engine Address:** Specify the DNS name or IP address to the server hosting the Engine here.
17. **Engine Port:** Specify the SSL port for the Engine here.

18. Enter the parameter settings and click *Next*.

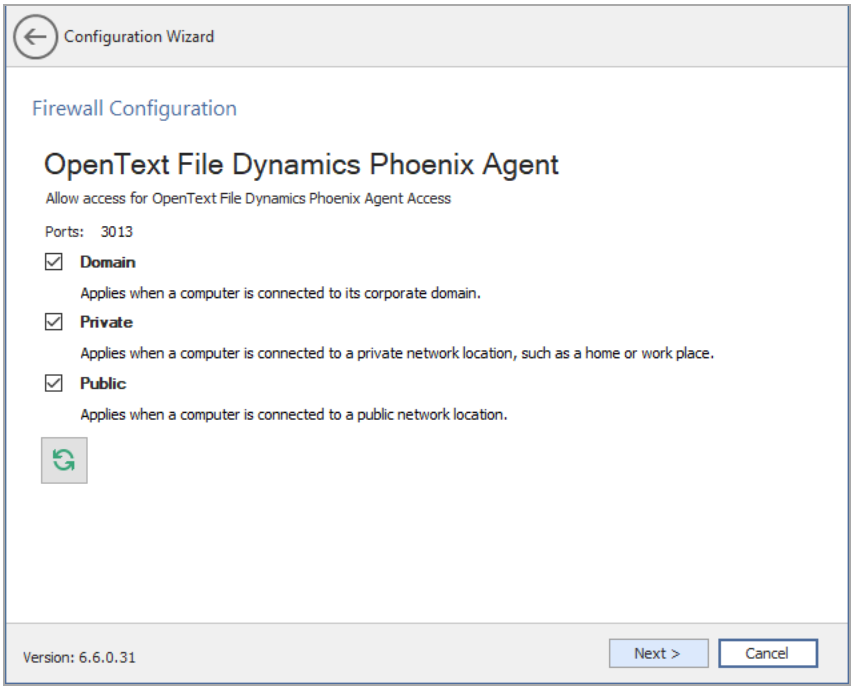


19. (Conditional) If you chose a name that was not the default name for the Proxy Rights group, enter the name in the *Proxy Rights Group* field.
20. Click *Next*.
21. (Conditional) If permissions for the Proxy Rights group have already been established (such as when you upgrading an Agent), the following page will

appear:



22. (Conditional) Review the privileges and click *Next*.



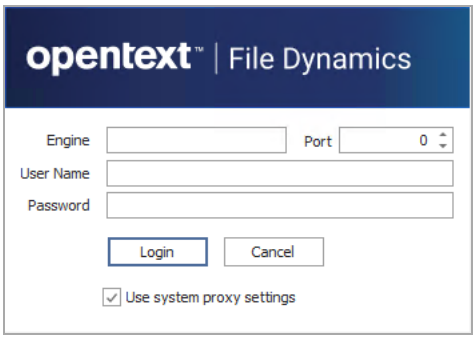
23. Set the network profiles according to your organization's security policies and click *Next*.

24. The wizard indicates that the Phoenix Agent service is running.
25. Click *Finish*.

7.12 - Installing the Admin Client

The Admin Client is the administrative interface for File Dynamics. It can be installed on any Windows platform where .NET 7.0 can run.

1. On the Windows server or workstation where you will run the Admin Client, copy to a directory the `FileDynamics_6.6.iso`.
2. Mount the `FileDynamics_6.6.iso` file.
3. At the root of the `File Dynamics_6.6.0.iso` image, double-click `File Dynamics-Admin-6.6-xx.exe`.
4. When you are asked if you want to run this file, click *Run*.
5. Agree to the licensing terms and conditions and click *Install*.
6. When notified that the setup was successful, click *Run Admin Client*.
7. The Admin Client login dialog box appears.



8. In the *Engine* field, specify the DNS name or IP address.
9. In the *Port* field, specify the secure port number.
10. The default setting is 3009.
11. Specify the username and password.
12. The user must be a member of the File Dynamics Admins group to be able to log in.
13. Click *Login*.

7.13 - Authorizing the Event Monitor

1. In the Admin Client, click the *Home* tab.
2. Click *Event Monitors*.
3. Select the listed domain.
4. Click *Authorize*.
5. When you are asked if you want to authorize the selected event monitor, click *Yes*.
6. When the Results page appears, click *Close*.

7.14 - Authorizing the Agents

1. In the Admin Client, click the *Home* tab.
2. Click *Agents*.
3. Select a listed server.
4. Click *Authorize*.
5. When you are asked if you want to authorize the selected event monitor, click *Yes*.
6. When the Results page appears, click *Close*.
7. Repeat Steps 3-6 for all File System Agents and Phoenix Agents.

7.15 - Configuring Storage Resources

Before File Dynamics can manage, protect, and report on your network storage, you must first configure your storage resources and in the process, specify what servers to include for scoping and those to ignore.

1. In the Admin Client, click the *Home* tab.
2. Click *Storage Resources*.
3. In the *Scope* region, browse to locate the containers or servers you want included and drag them to the *Include* frame.
4. If you do not specify the containers or servers to include, File Dynamics will process all of the servers on your network, which can affect the ability of File Dynamics to perform management and reporting tasks.
5. (Optional) From the *Include* frame, right click a server and select *Share* to view information on the shares of that server.

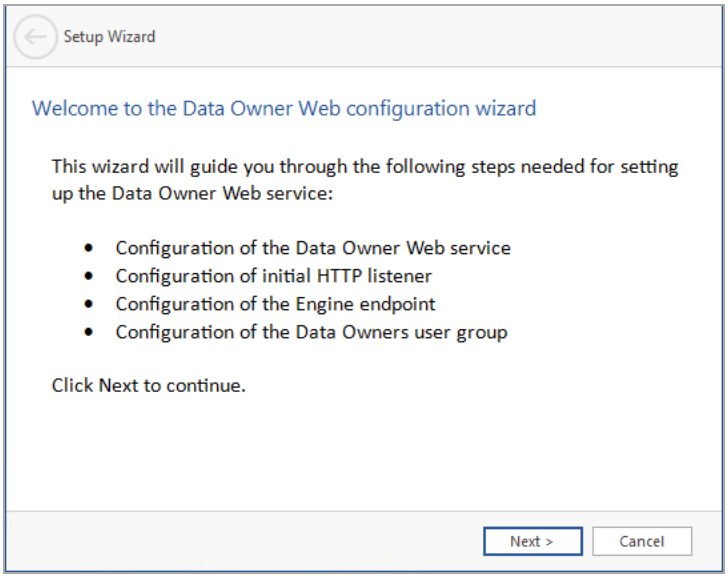
6. Click *Save*.
7. When asked if you want to start the update of the storage resources, click *Yes*.

7.16 - Configuring the Data Owner Web Service

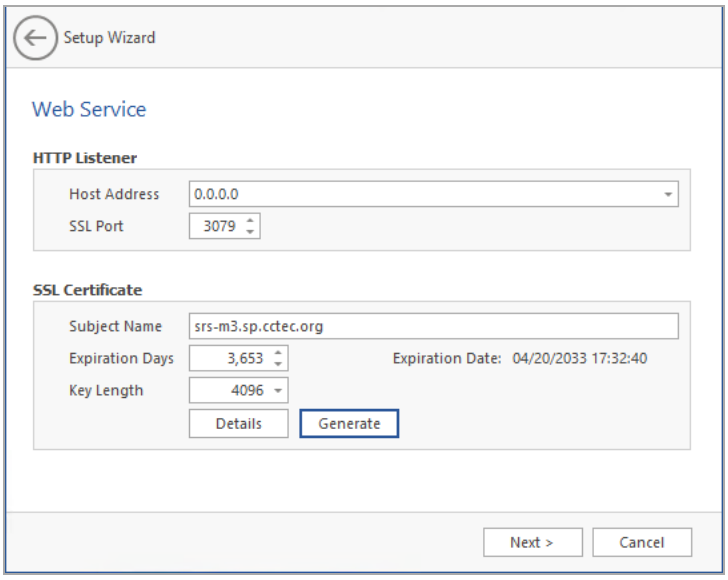
When installing File Dynamics the Data Owner web service is installed as part of the Engine package.

The following section provides procedures for configuring the Data Owner web service.

1. Launch the configuration utility from the Windows start menu: *Start* > *File Dynamics* > *File Dynamics Data Owner Web Config*.



2. Click **Next**.



3. Set any needed parameters for the HTTP Listener.

   Host Address: Select an IP address the service will use. To listen on all available IP addresses, select the default *0.0.0.0* entry.

   SSL Port: Use the default port 3079 or enter a different one for the web service.

4. Use the default self-signed certificate or click **Generate** after updating the fields:

   Subject Name: DNS name used when accessing the service.

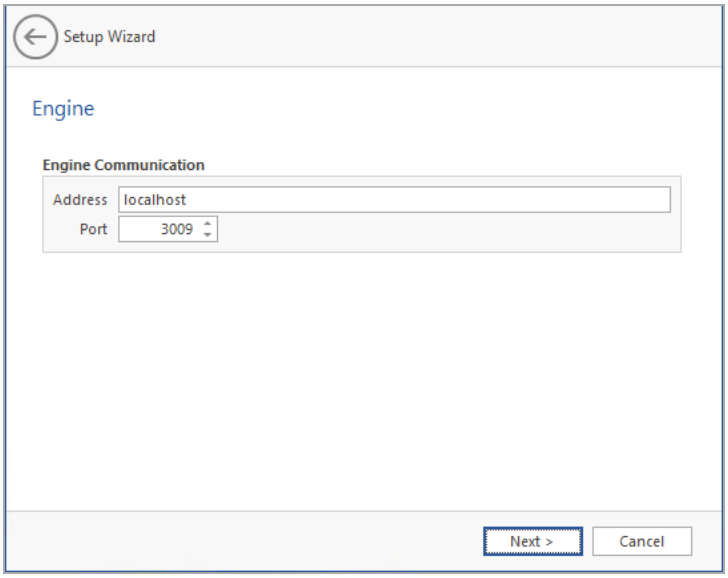
   Expiration Days: number of days the certificate will be valid

   Key Length: specifies the key length for the encryption key

NOTE: While a default self-signed certificate is created, we strongly recommend using a proper certificate issued by a trusted Certificate Authority.

See *Replacing the Self-Signed Certificate (page 52)* for details on performing this task.

5. Click Next.

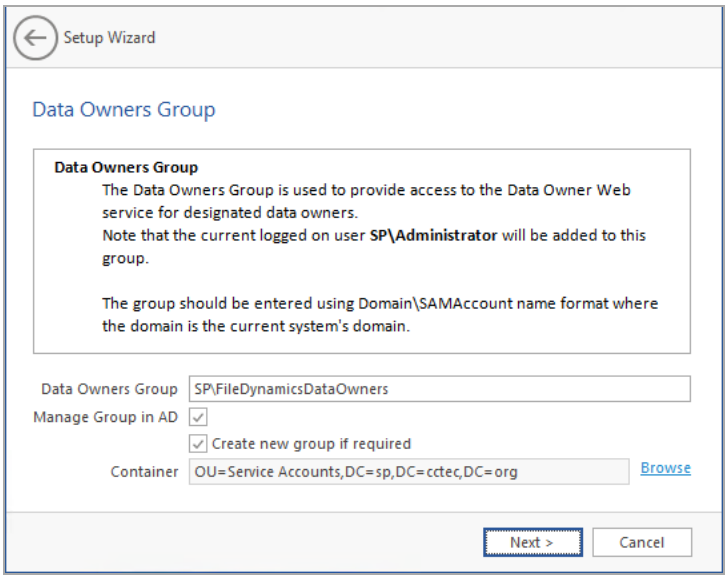


6. Enter the parameters for communicating with the Engine service.

   Address: Enter the DNS name or IP address where the Engine service is listening. If the Data Owner web service is on the same server, localhost may be used here.

   Port: Enter the port the Engine service listens on. By default this is 3009.

7. Click **Next**.



8. Specify the Data Owners group that provides basic access to the web service. Designated Data Owners must be a member of this group in order to use the Data Owner web service.

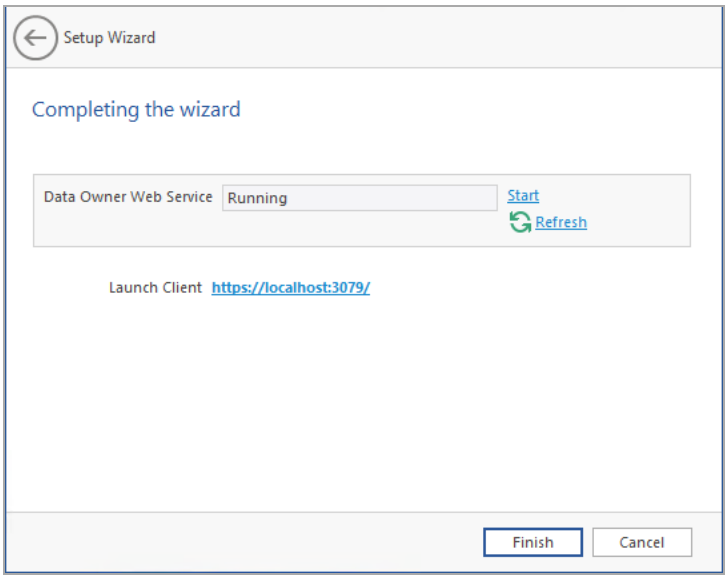
   Data Owners Group: Enter the name of the group to use or create in Domain\Account name format.

   Manage Group in AD: select this to update an existing group or create a new one. If this is selected, the current user will be added as a member to the group.

   Create new group if required: select this to create the group if it does not already exist.

   Container: click **Browse** to navigate and select the container in Active Directory where a new group if created will be placed.

9. Click **Next**.



10. The Data Owner web service should now start.

    Click **Start** if the web service is not yet started.

11. [Optional] Click the **Launch Client** URL to open a brower and access the Data Owner web interface.

12. Click **Finish** to complete the configuration.

7.16.1 - Replacing the Self-Signed Certificate

Overview

The self-signed certificate generated during initial configuration provides a quick means for initial administrator setup. Once setup is complete and any DNS names have been appropriately assigned, we recommend replacing the self-signed certificate with a certificated signed by a trusted authority. Using a certificate issued from a trusted Certificate Authority (CA) reduces end-user confusion when accessing a web site with an otherwise untrusted certificate.

Any SSL/TLS certificate issued from a commercial vendor or an organizational CA is sufficient.

Certificate Requirements

The certificate must be in **PEM** format and should include both the certificate and the private key. Depending on the format of the certificate you acquire, conversion

from other formats such **PKCS#12** or **PFX** may be required. Online examples and help for certificate conversion include:

- https://knowledge.digicert.com/solution/SO26449.html
- https://www.ssl.com/how-to/export-certificates-private-key-from-pkcs12-file-with-openssl/
- General search: https://www.google.com/search?q=convert+certificate+pkcs12+to+pem

An example using the **openssl** command line tool to convert a certificate from PFX to PEM format is shown here:

```
openssl pkcs12 -in my-certificate.pfx -out my-certificate.pem -
nodes
```

NOTE: The *-nodes* parameter is required here as the resulting PEM file cannot be password protected.

Updating the Certificate

Once you have a valid PEM file including the certificate and private key that is not password protected, replace the **server.pem** file found on the server hosting the Data Owner web service here:

```
%PROGRAMDATA%\
OpenText\FileDynamics\DataOwnerWeb\config\server.pem
```

Typically this is located at:

```
C:\ProgramData\
OpenText\FileDynamics\DataOwnerWeb\config\server.pem
```

1. Using the Windows services manager, stop the **fsfdataownerweb** service.
2. Replace the **server.pem** file with the updated certificate file, keeping the same name.
3. Restart the **fsfdataownerweb** service.

8 - Administering File Dynamics

You have now completed the installation of File Dynamics 6.6. For administration procedures, refer to the *File Dynamics 6.6 Administration Guide*.