Micro Focus File Dynamics 6.1
Installation Guide

September 28, 2018

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

Contents

About This Guide 5

1 Prerequisites 7

1.1 Folder Redirection and DNS Names . . . 7
1.2 File Server Resource Manager . . . 8
1.2.1 Installing File Server Resource Manager . . . 8
1.3 Active Directory Schema . . . 10
1.3.1 Extending the Active Directory Schema . . . 11
1.4 Verifying Proper Configurations and Permissions . . . 11
1.5 Create a New Host Record in DNS for File Dynamics . . . 12
1.6 What's Next . . . 12

2 Licensing the Product 13

2.1 License Overview . . . 13
2.2 Obtaining a Product Activation Key . . . 13
2.3 Obtaining a License File . . . 14
2.4 Updating a License File . . . 15

3 Installing and Configuring an SQL Server Instance 17

3.1 Determine Which Version of SQL Server to Use . . . 17
3.2 Install SQL Server Express . . . 17
3.3 Install a New Instance of SQL Server . . . 25
3.4 SQL Server Post Configuration Considerations . . . 31

4 Migrating from Storage Manager 3.1.1 33

4.1 Prerequisites . . . 33
4.2 Understanding the Migration Process . . . 33
4.3 Accessing the Product Contents . . . 34
4.4 Stopping and Disabling Components . . . 34
4.4.1 Stopping and Disabling the Engine . . . 34
4.4.2 Stopping and Disabling the Event Monitor . . . 34
4.4.3 Stopping and Disabling the Agents . . . 35
4.5 Installing the Engine . . . 35
4.6 Installing the License . . . 36
4.7 Configuring the Database . . . 38
4.8 Migrating the Database . . . 42
4.9 Configuring the Engine . . . 46
4.10 Migrating the Engine Data . . . 53
4.11 Installing NSMAdmin . . . 55
4.12 Review Migrated Policies . . . 57
4.13 Upgrading to File Dynamics 6.1 . . . 57

5 Upgrading from Storage Manager 4.1, 5.*x*, or File Dynamics 6.0 to File Dynamics 6.1 **59**

5.1 Upgrading from Storage Manager 4.1 or 5.*x* . . . 59
5.2 Upgrading from File Dynamics 6.0 . . . 59
5.2.1 Required Component Upgrades . . . 59
5.2.2 Optional Component Upgrades . . . 59

6 Installing File Dynamics 6.1 **61**

6.1 Domain Administrator Permissions . . . 61
6.2 Accessing the Product Contents . . . 61
6.3 Installing the Engine . . . 62
6.4 Installing the License . . . 63
6.5 Configuring the Database . . . 64
6.6 Configuring the Engine . . . 67
6.7 Configure the Epoch File Viewer . . . 75
6.8 Setting Rights and Privileges on Managed Storage . . . 85
6.8.1 Granting Rights . . . 85
6.8.2 Granting Privileges on a Member Server . . . 86
6.8.3 Granting Privileges on a Domain Controller . . . 87
6.9 Installing and Configuring the Event Monitor . . . 89
6.10 Installing and Configuring the File System Agents . . . 94
6.11 Installing and Configuring the Phoenix Agents . . . 100
6.12 Installing the Admin Client . . . 104
6.13 Authorizing the Event Monitor . . . 105
6.14 Authorizing the Agents . . . 105
6.15 Installing the Data Owner Client . . . 106
6.16 Installing Other Components . . . 107
6.17 Administering File Dynamics . . . 107

A Documentation Updates **109**

A.1 September 28, 2018 . . . 109

About This Guide

This installation guide is written to provide network administrators the conceptual and procedural information for installing and configuring Micro Focus File Dynamics 6.1.

- Chapter 1, “Prerequisites,” on page 7
- Chapter 2, “Licensing the Product,” on page 13
- Chapter 3, “Installing and Configuring an SQL Server Instance,” on page 17
- Chapter 4, “Migrating from Storage Manager 3.1.1,” on page 33
- Chapter 5, “Upgrading from Storage Manager 4.1, 5.*x, or File Dynamics 6.0 to File Dynamics 6.1,” on page 59*
- Chapter 6, “Installing File Dynamics 6.1,” on page 61
- Appendix A, “Documentation Updates,” on page 109

Audience

This guide is intended for network administrators who manage user and collaborative 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 Dynamics 6.1 Installation Guide*, visit the Micro Focus File Dynamics Documentation website (https://www.novell.com/documentation/file-dynamics-60/).

Additional Documentation

For additional Micro Focus File Dynamics documentation, see the following guide at the Micro Focus File Dynamics Documentation website (https://www.novell.com/documentation/file-dynamics-60/):

- *Micro Focus File Dynamics 6.1 Administration Guide*
- *Micro Focus File Dynamics 6.1 Cross-Empire Data Migration Guide*
- *Micro Focus File Dynamics 6.1 Data Owner Client Guide*

1 Prerequisites

This section provides procedures that you must do before installing the Micro Focus File Dynamics 6.1 components.

- Section 1.1, “Folder Redirection and DNS Names,” on page 7
- Section 1.2, “File Server Resource Manager,” on page 8
- Section 1.3, “Active Directory Schema,” on page 10
- Section 1.4, “Verifying Proper Configurations and Permissions,” on page 11
- Section 1.5, “Create a New Host Record in DNS for File Dynamics,” on page 12
- Section 1.6, “What’s Next,” on page 12

1.1 Folder Redirection and DNS Names

Micro Focus File Dynamics 6.1 exclusively uses DNS Fully Distinguished Names (FDNs) for server names in all UNC paths set in and by File Dynamics. This is a change from Storage Manager 3.*x* and earlier, where NetBIOS names were used (although a config file-only option to use DNS names existed in Storage Manager 3.1.*x*). This is per Microsoft’s own recommendations, as Microsoft slowly attempts to phase out NetBIOS and WINS.

However, there are known bugs related to Folder Redirection when the DNS name for a server is used in a user’s home folder path (or any other path specified for folder redirection). These Windows bugs, which can result in loss of data in the redirected folders or the entire redirected folder, are described in the following Microsoft KB articles:

- “You are unable to update the target location of offline file shares in the Offline File client side cache without administrative permission in Windows Server 2008 R2 or in Windows 7.” http://support.microsoft.com/kb/977229
- “After you apply a GPO to redirect a folder to a new network share, the redirected folder is empty on client computers that are running Windows Vista or Windows Server 2008.” https://support.microsoft.com/en-gb/help/2610379/the-folder-redirection-policy-does-not-work-if-a-previous-user-sets-a

These KB articles specifically apply to users logging on through Windows Vista or Windows 7 computers, as well as users logging on interactively on Windows Server 2008 and Windows Server 2008 R2. Users on other operating systems might be affected as well, however.

Both of the KB articles above include links to hotfixes that help resolve these issues.

While this is not a File Dynamics issue *per se*, File Dynamics’ exclusive use of DNS FDNs in UNC paths can exacerbate this problem, or introduce it into an environment that was previously exclusively using NetBIOS naming for servers and using folder redirection.

IMPORTANT: If your environment uses folder redirection, we strongly recommend reading the KB articles above and applying any relevant hotfixes before managing storage with File Dynamics. (In fact, we strongly recommend applying these hotfixes if you use folder redirection in your AD

environment with the affected operating systems, even if you are not managing user storage with File Dynamics. Microsoft's continuing push to move away from NetBIOS and WINS may eventually introduce this issue into your environment with or without File Dynamics installed.)

1.2 File Server Resource Manager

Microsoft File Server Resource Manager is a suite of tools from Microsoft that allows administrators to better understand, control, and manage the quantity and type of data stored on their servers. File Dynamics uses File Server Resource Manager to enable quota management.

NOTE: You must install FSRM on all servers where File Dynamics will be managing quotas, including the server that will host the Engine. Even if the Engine host does not contain shares that will be managed, FSRM is still required because the FSRM COM interfaces must be present for the Engine to call them remotely on other servers.

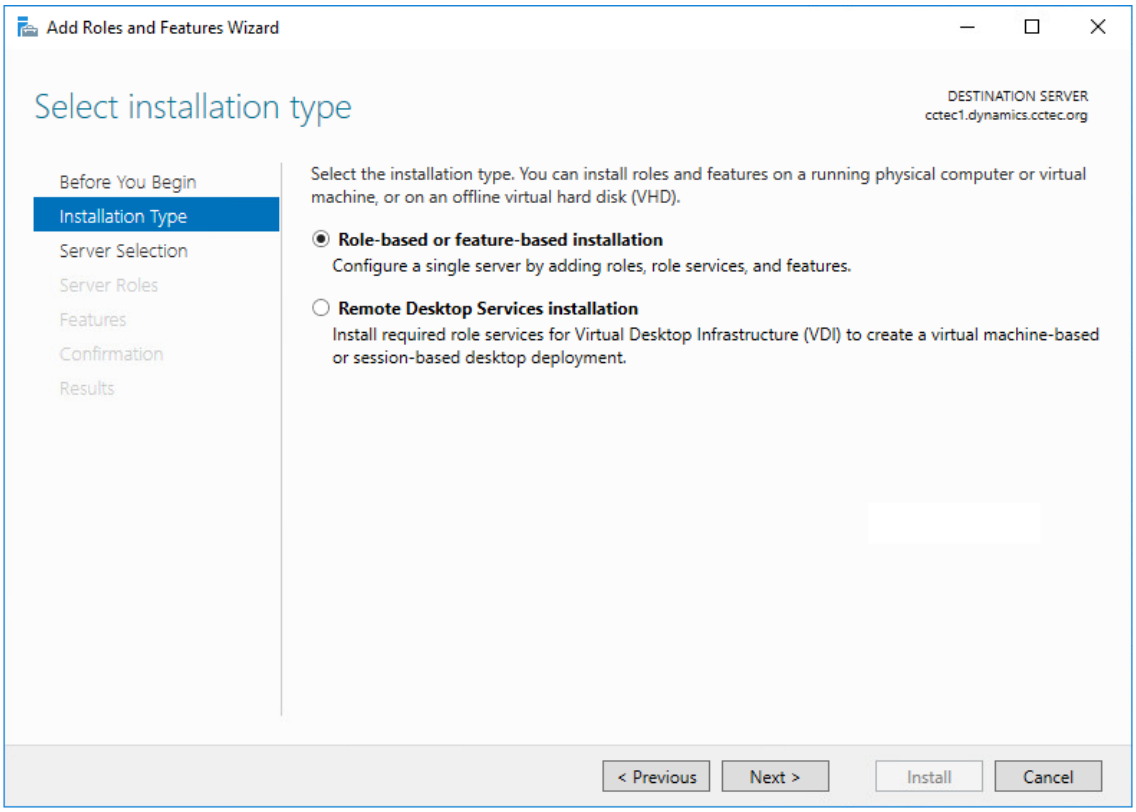
1.2.1 Installing File Server Resource Manager

Quotas for user and collaborative storage can be managed through File Dynamics on all versions of Windows Server from 2008 and beyond. You need to install File Server Resource Manager on every server or active node that will be hosting user or collaborative quota-managed storage.

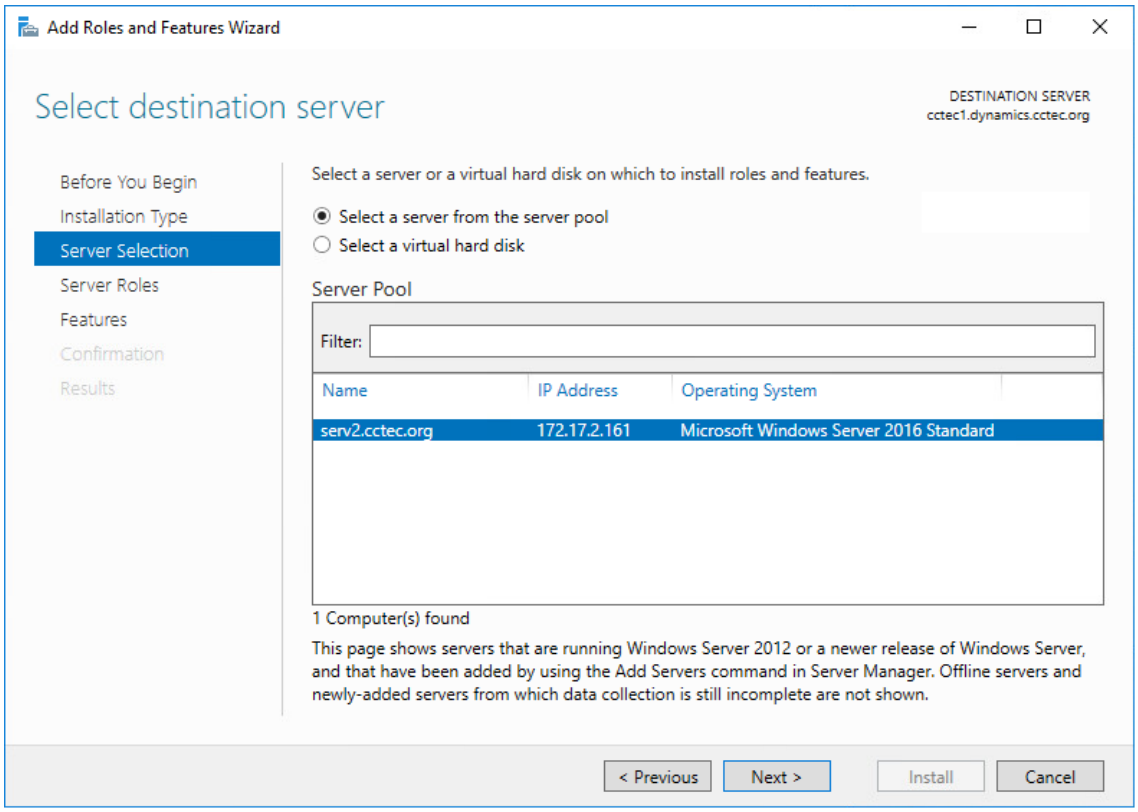
NOTE: These procedures are specific to Windows Server 2016. Procedures vary for each version of Windows Server.

1. Launch Server Manager.
2. Click **Add roles and features**.

   This launches the Add Roles and Features Wizard.
3. Click **Next**.



4 Verify that **Role-based or feature-based installation** is selected and click **Next**.

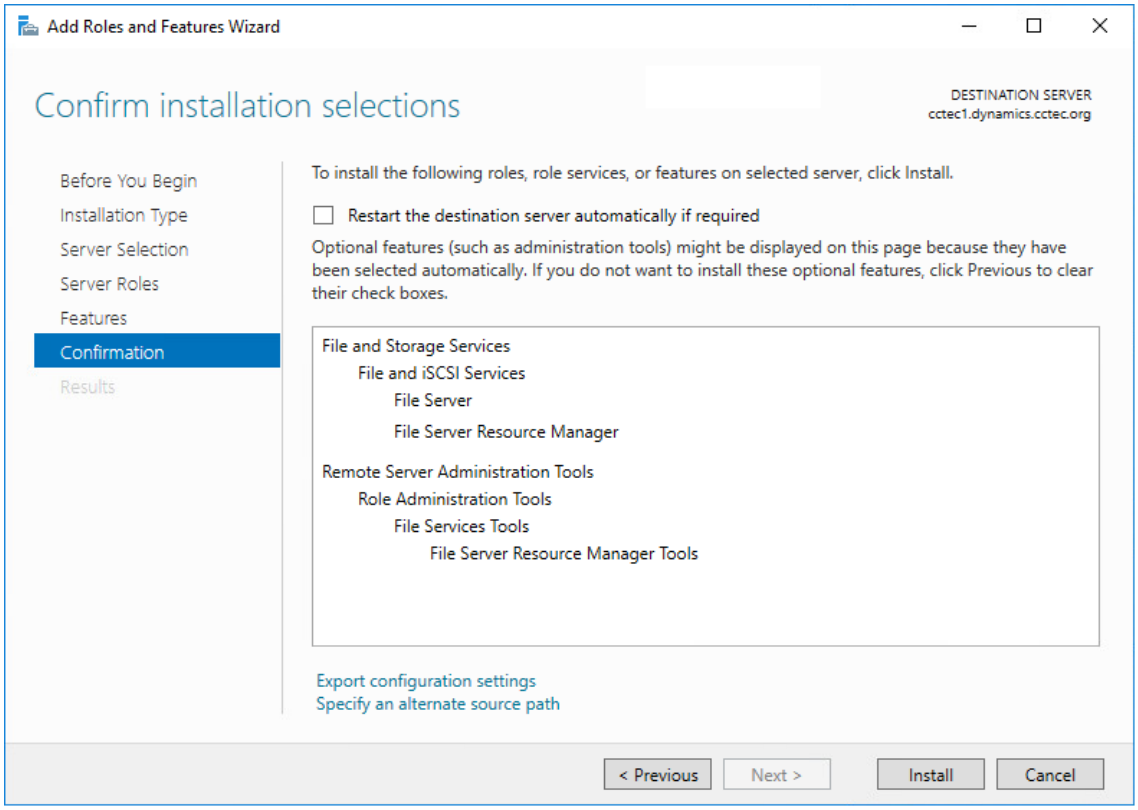


5 Select the server where you are going to install the Engine and click **Next**.

6 From the list of roles, expand **File and Storage Services**.

7 Expand **File and iSCSI Services**.

8 Select the **File Server Resource Manager** check box.



9 Click **Add Features**.

10 Click **Next**.

11 Click **Next**.

12 Click **Install**.

1.3 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.

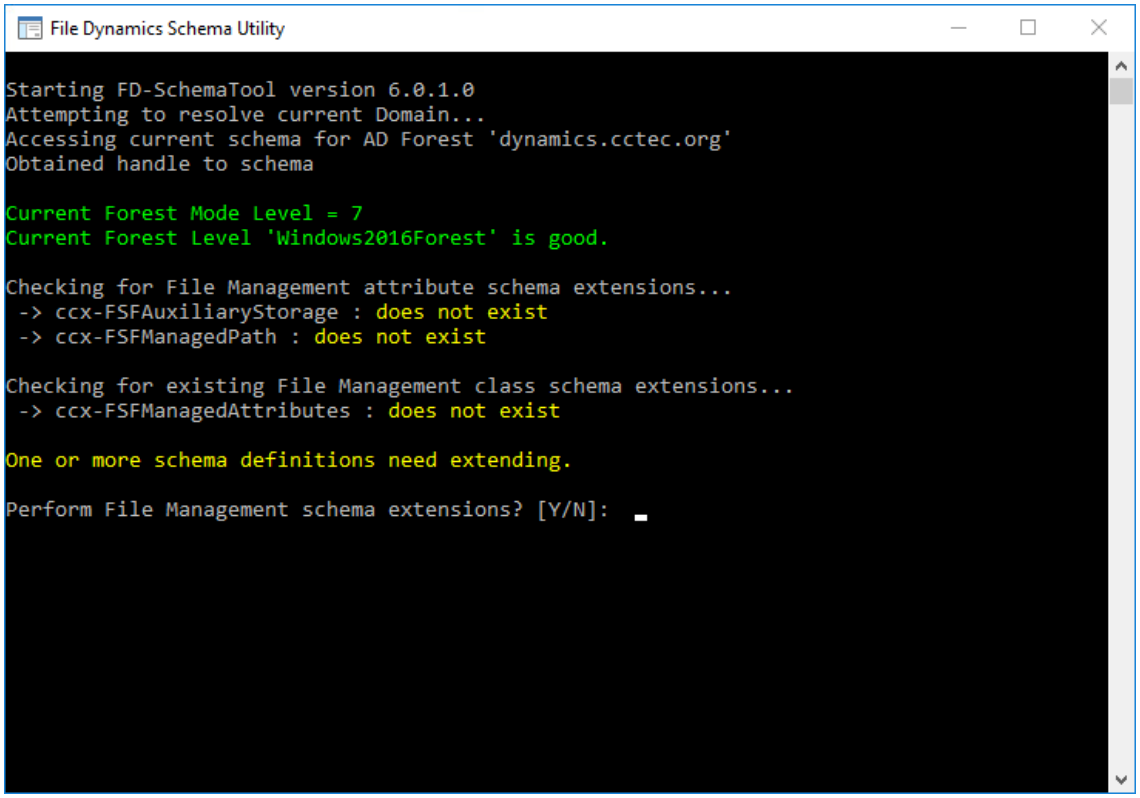
To enable collaborative storage or auxiliary storage management, File Dynamics extends the Active Directory schema to enable File Dynamics attributes. These attributes are specified in Active Directory Schema Extensions in the *Micro Focus File Dynamics 6.1 Administration Guide*.

NOTE: If your File Dynamics deployment will not include support for collaborative storage or auxiliary storage management, there is no need to extend the Active Directory schema.

1.3.1 Extending the Active Directory Schema

1. Log in to the forest or domain as a user with Schema administration privileges.

   You can do this by being a member of the Schema Admins group.
2. At the root of the ISO image, locate the `AD-SchemaTool.exe` file, and double-click it.
3. When you are asked if you want to run this file, click **Run**.



4. Type `Y` to extend the schema.

1.4 Verifying Proper Configurations and Permissions

In some cases, you might find that you are unable to install a File Dynamics component because of an improper configuration or permissions setting. Micro Focus recommends that you review the following sections in the *Micro Focus File Dynamics 6.1 Administration Guide* and make any needed adjustments before proceeding:

- Windows Firewall Requirements
- LSA Rights and Privileges
- ProxyRights Group Permissions

1.5 Create a New Host Record in DNS for File Dynamics

For example `fdfileviewer.cctec.org`

This is needed during the configuration of the Microsoft IIS Website for the Epoch File Viewer.

1.6 What's Next

If you are migrating your Storage Manager 3.*x* for Active Directory environment to File Dynamics 6.1:

1. Proceed with Chapter 2, "Licensing the Product," on page 13.
2. Follow the procedures in Chapter 3, "Installing and Configuring an SQL Server Instance," on page 17 to install an SQL Server instance that File Dynamics supports.
3. Begin the migration by following the procedures in Chapter 4, "Migrating from Storage Manager 3.1.1," on page 33.
4. Then conclude with Chapter 5, "Upgrading from Storage Manager 4.1, 5.*x, or File Dynamics 6.0 to File Dynamics 6.1," on page 59*.

If you are upgrading from Storage Manager 4.*x* to File Dynamics 6.1:

1. Proceed with Chapter 2, "Licensing the Product," on page 13.
2. Follow the procedures in Chapter 5, "Upgrading from Storage Manager 4.1, 5.*x, or File Dynamics 6.0 to File Dynamics 6.1," on page 59*.

If you are upgrading from Storage Manager 5.*x* to File Dynamics 6.1:

1. Proceed with Chapter 2, "Licensing the Product," on page 13.
2. Follow the procedures in Chapter 5, "Upgrading from Storage Manager 4.1, 5.*x, or File Dynamics 6.0 to File Dynamics 6.1," on page 59*.

If you are installing File Dynamics:

1. Proceed with Chapter 2, "Licensing the Product," on page 13.
2. Follow the procedures in Chapter 3, "Installing and Configuring an SQL Server Instance," on page 17 to install an SQL Server instance that File Dynamics supports.
3. Complete the installation by following the procedures in Chapter 6, "Installing File Dynamics 6.1," on page 61.

2 Licensing the Product

This section provides an overview of license types and procedures for obtaining the product software and an evaluation license file.

- Section 2.1, “License Overview,” on page 13
- Section 2.2, “Obtaining a Product Activation Key,” on page 13
- Section 2.3, “Obtaining a License File,” on page 14
- Section 2.4, “Updating a License File,” on page 15

2.1 License Overview

Micro Focus File Dynamics has the following license types:

Table 2-1 *File Dynamics License Types*

License Type	Product Capabilities
Core	Network file system management through Identity-Driven, Target-Driven, and Workload policies.
Core + eDirectory to Active Directory Cross-Empire Data Migration	Core features of File Dynamics plus the ability to migrate the contents, rights, security, and metadata of user and group network directories from an Open Enterprise Server or NetWare platform, to a Microsoft network platform. Once the migration is complete, you can use the core features of File Dynamics to manage your Microsoft network file system.
Core + Active Directory to Active Directory Cross-Empire Data Migration	Core features of File Dynamics plus the ability to migrate the contents, permissions, security, and metadata of user and group network folders from one Active Directory forest to another. Once the migration is complete, you can use the core features of File Dynamics to manage your Microsoft file system.

For individuals evaluating File Dynamics, you can obtain a full-featured 30-day license of the core product.

2.2 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 Dynamics**.
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.

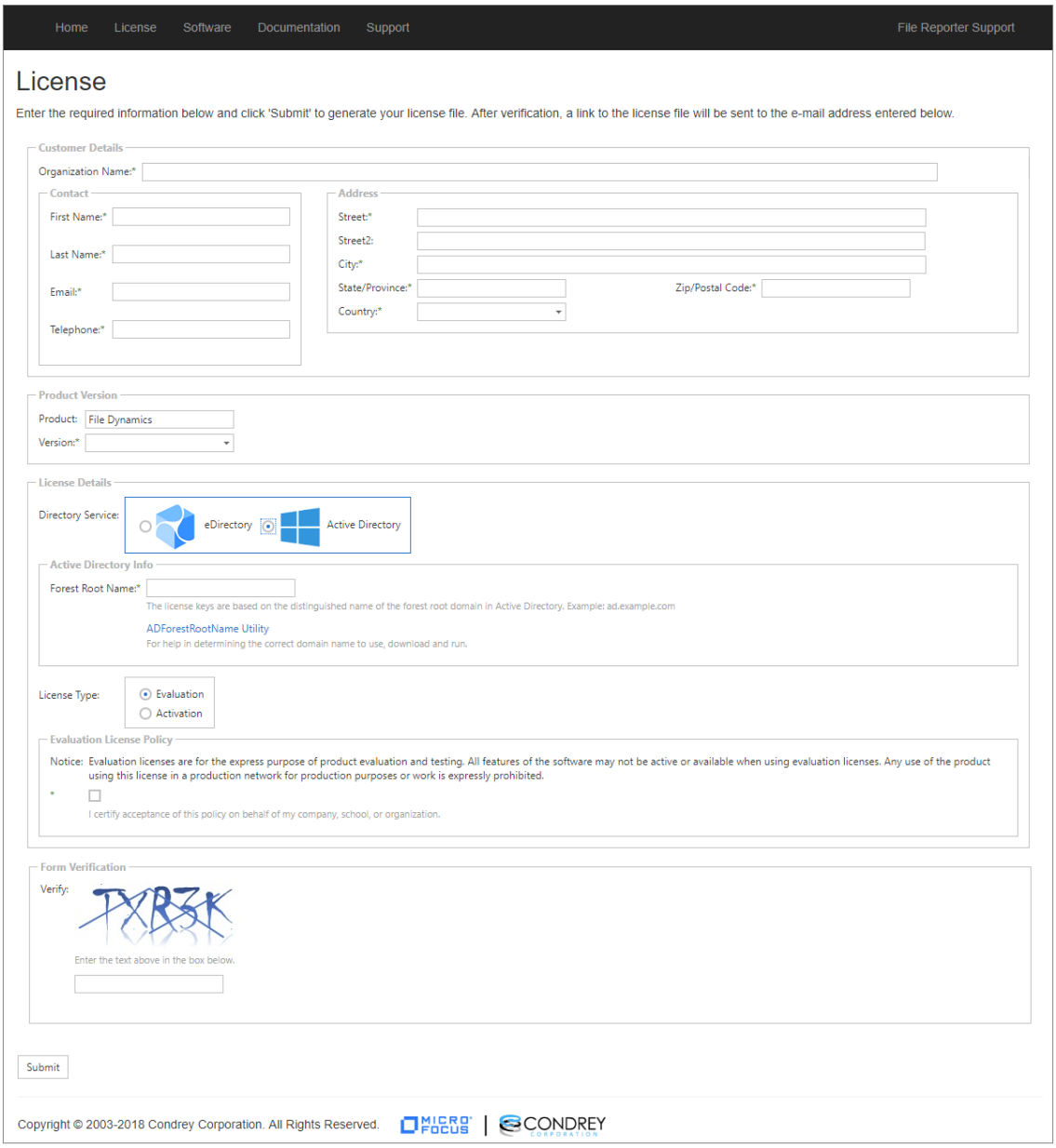
2.3 Obtaining a License File

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

1 In a web browser, go to `https://www.filedynamicssupport.com`.

2 On the top banner of the web page, click **License**.

A new web page appears with options for obtaining the license.



3 Complete the fields.

3a In the **Directory Service** region, verify that the **Active Directory** option is selected.

File Dynamics works only in a Microsoft Active Directory network.

3b 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 Dynamics 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.

2.4 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 file with the new one. You must first rename the new license file to `fd.lic`. For more information, see Section 6.4, “Installing the License,” on page 63.

3 Installing and Configuring an SQL Server Instance

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

File Dynamics requires a Microsoft SQL Server as the database and does not support the SQLite database that was utilized in previous versions of Storage Manager for Active Directory.

IMPORTANT: 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.

NOTE: File Dynamics supports all versions of SQL Server 2012, 2014,and 2016, including the Express version.

- Section 3.1, “Determine Which Version of SQL Server to Use,” on page 17
- Section 3.2, “Install SQL Server Express,” on page 17
- Section 3.3, “Install a New Instance of SQL Server,” on page 25
- Section 3.4, “SQL Server Post Configuration Considerations,” on page 31

3.1 Determine Which Version of SQL Server to Use

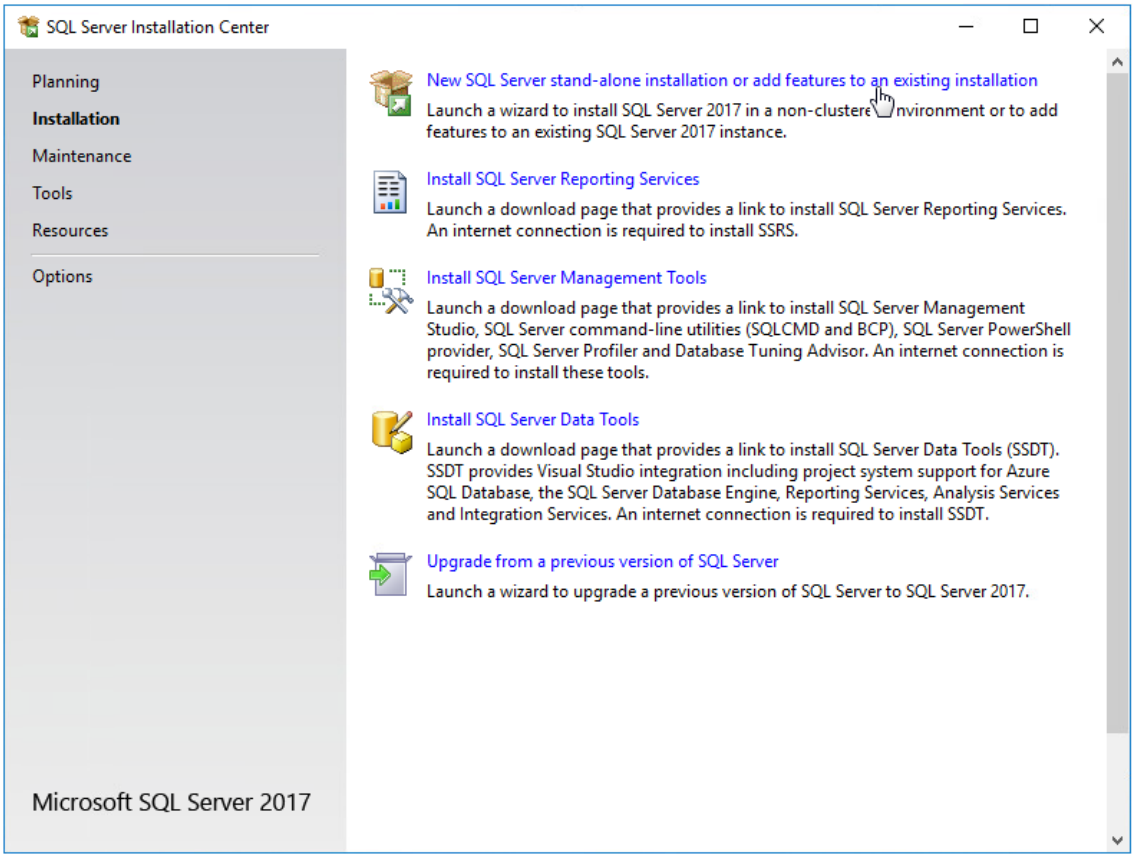
- If you do not already own SQL Server, you can use SQL Server Express. You can download SQL Server 2017 Express for free at: https://www.microsoft.com/en-us/sql-server/sql-server-editions-express. After downloading the software, proceed with “Install SQL Server Express.”

  IMPORTANT: 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 separate server.

- If you already own a version of SQL Server, proceed with Section 3.3, “Install a New Instance of SQL Server,” on page 25.

3.2 Install SQL Server Express

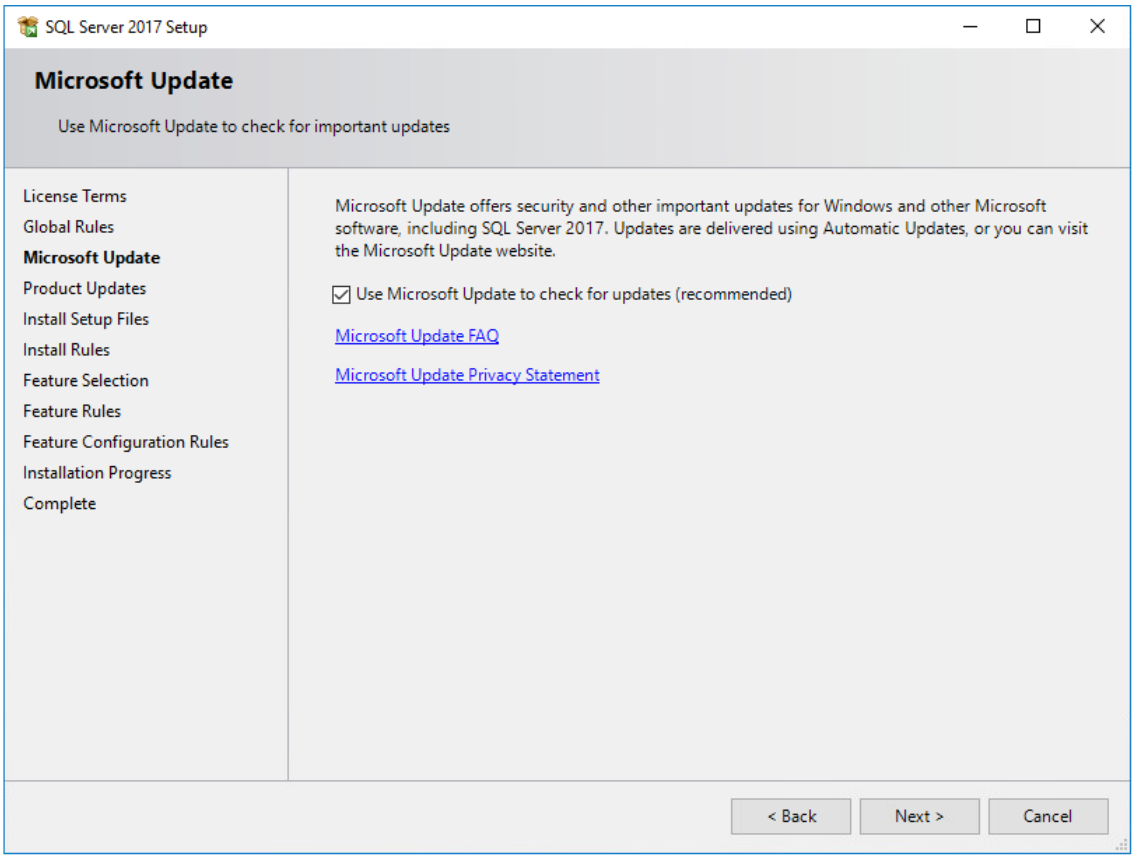
1. Launch the SQL Server Express installation file.
2. Choose a directory for the extracted files and click **OK**.
3. Select **New SQL Server stand-alone installation or add features to an existing installation**.



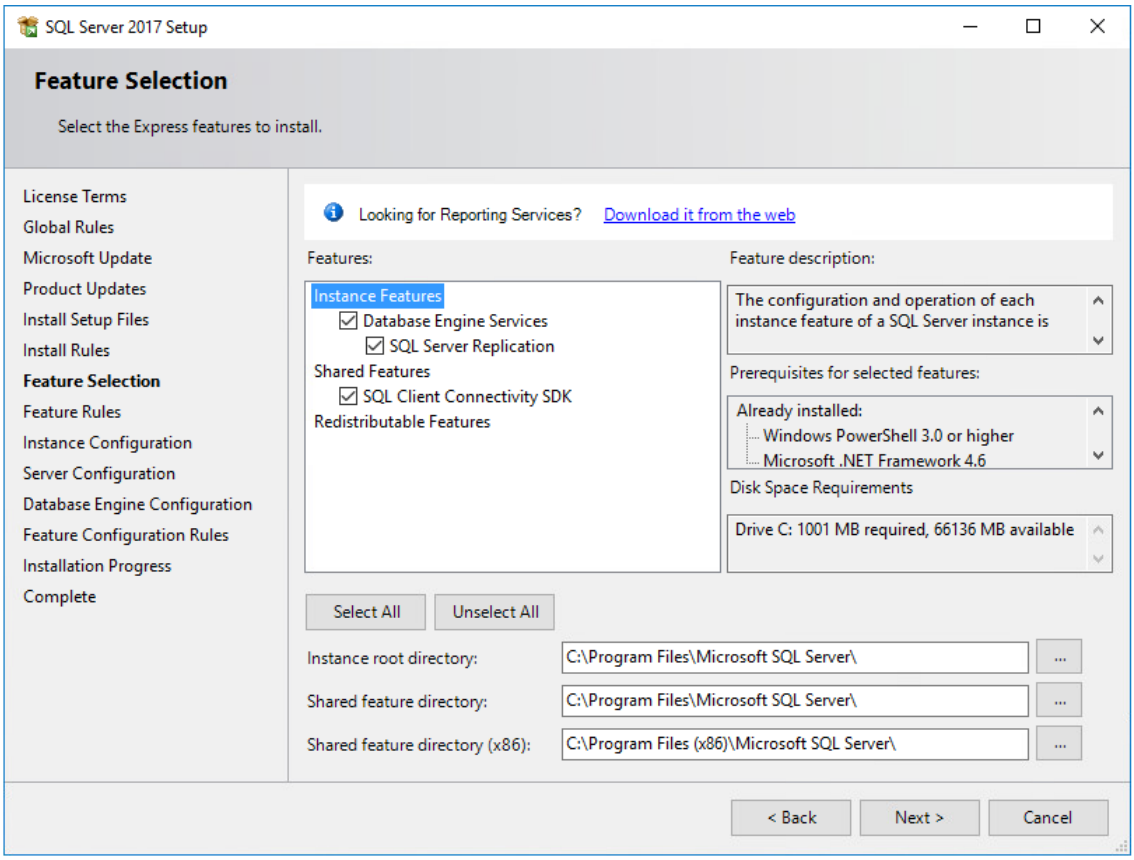
4 In the License Terms page, accept the license terms and click **Next**.

5 In the Product Updates page, click **Next**.

6 Select **Use Microsoft Update to check for updates (recommended)**, then click **Next**.



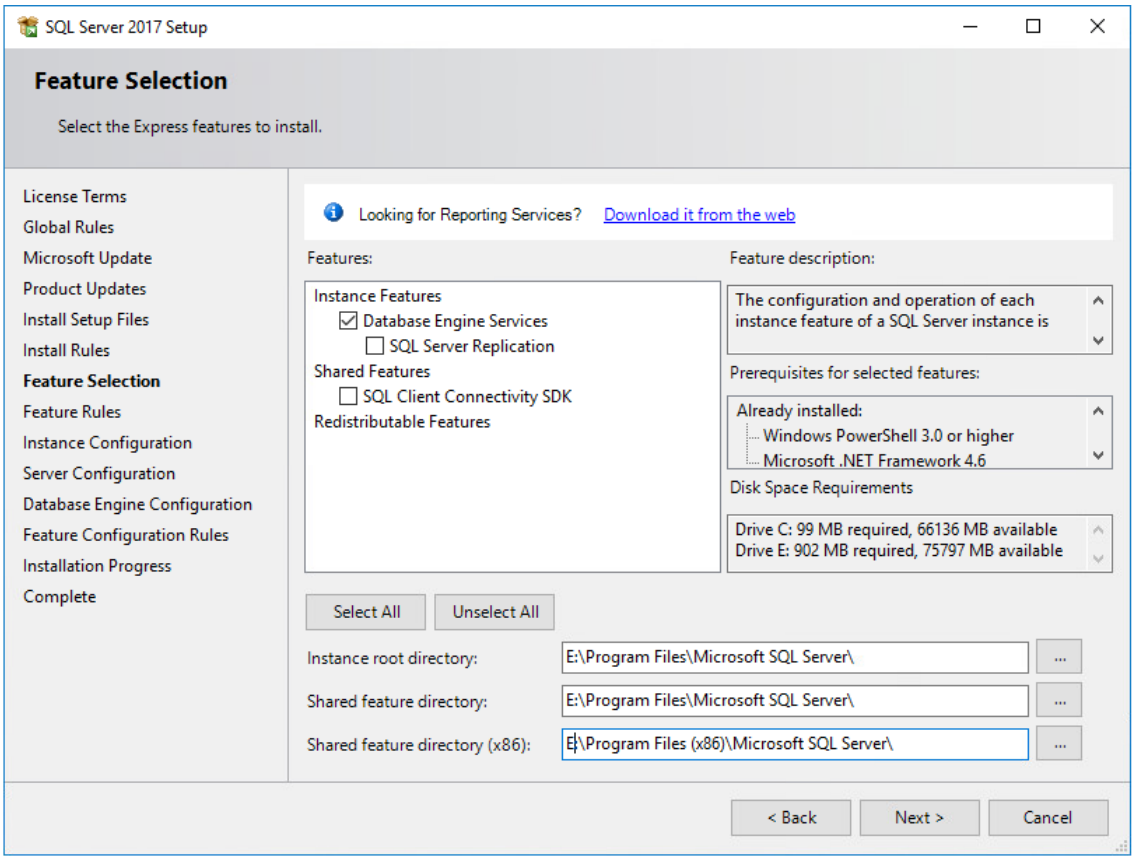
7 In the Install Rules page, click **Next**.



8 Click **Unselect All**.

9 Select the **Database Engine Services** check box.

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.



11 Click **Next**.

12 In the Feature Rules page, 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 In the Server Configuration page, click the **Collation** tab and then click **Customize**.

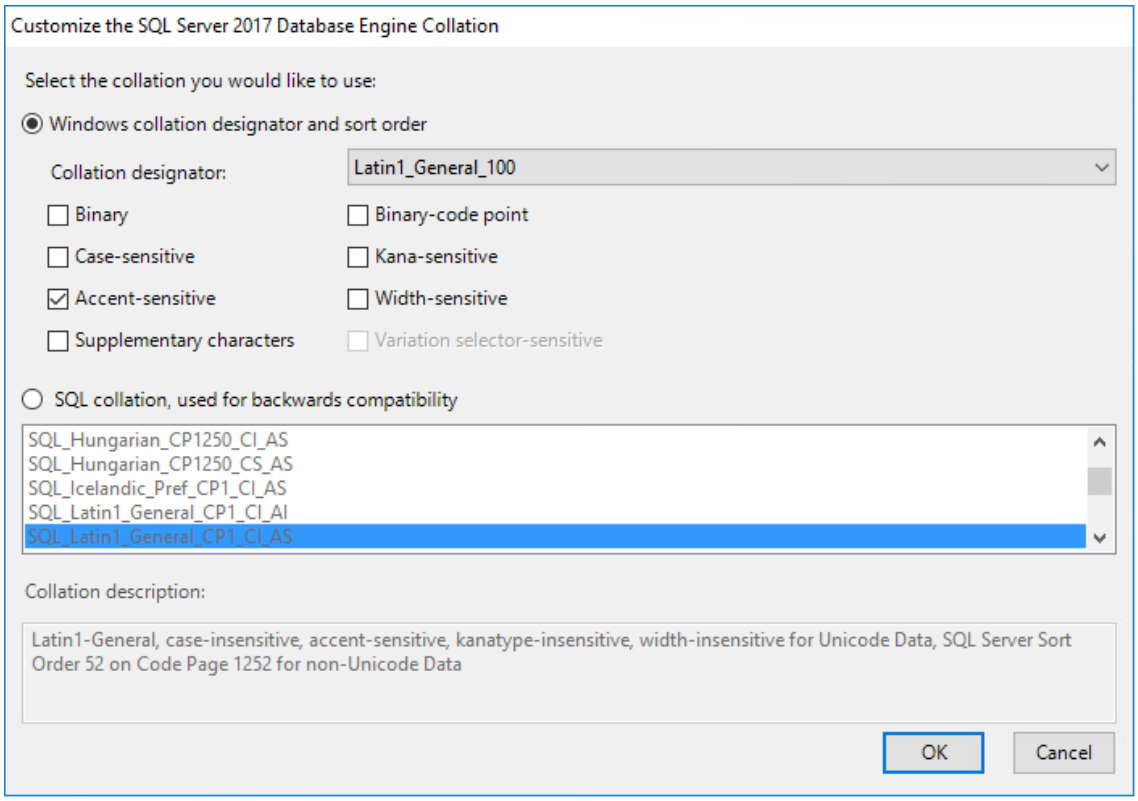
15 Click the **Windows collation designator and sort order** option.

16 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.

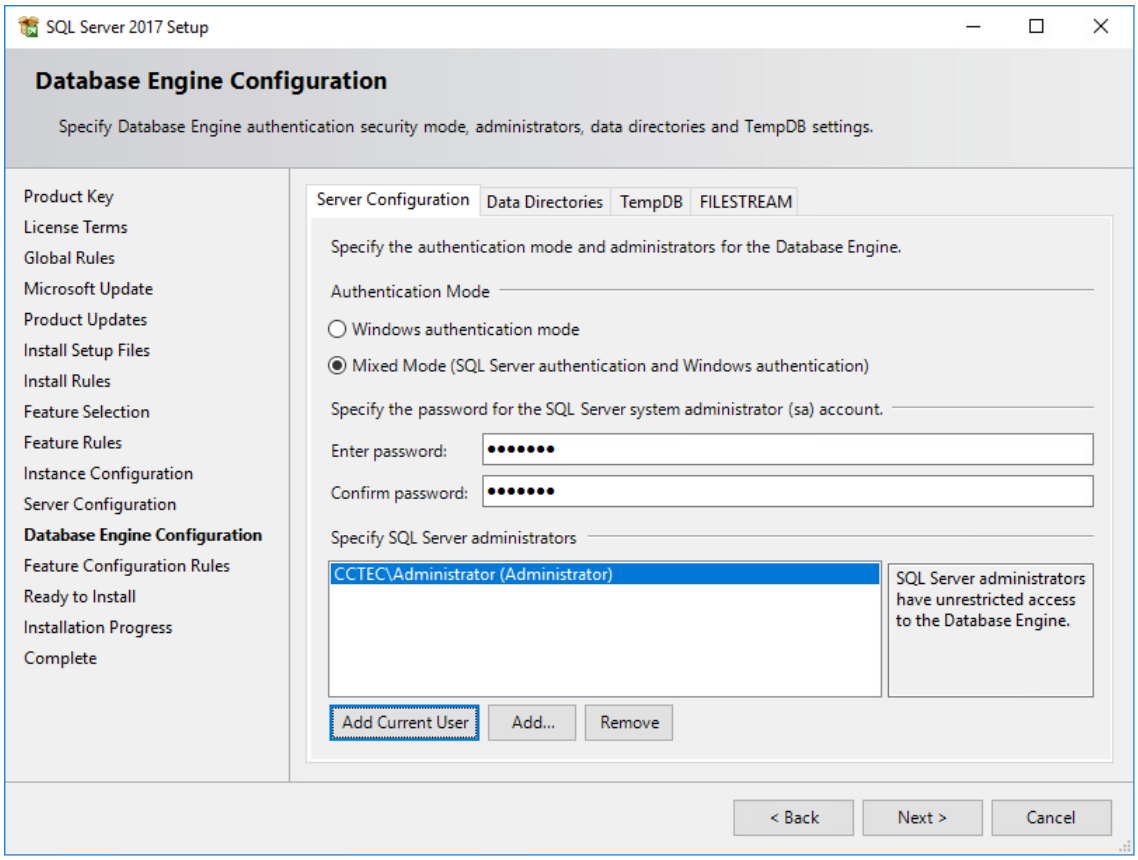
For more information on collation and locales, refer to this Microsoft document (http://technet.microsoft.com/en-us/library/ms175194%28v=sql.105%29.aspx).



17 Click **OK**.

18 Click **Next**.

19 Select the **Mixed Mode (SQL Server authentication and Windows authentication)** option, enter and confirm an SQL Server administrator password, and then click **Add Current User**.



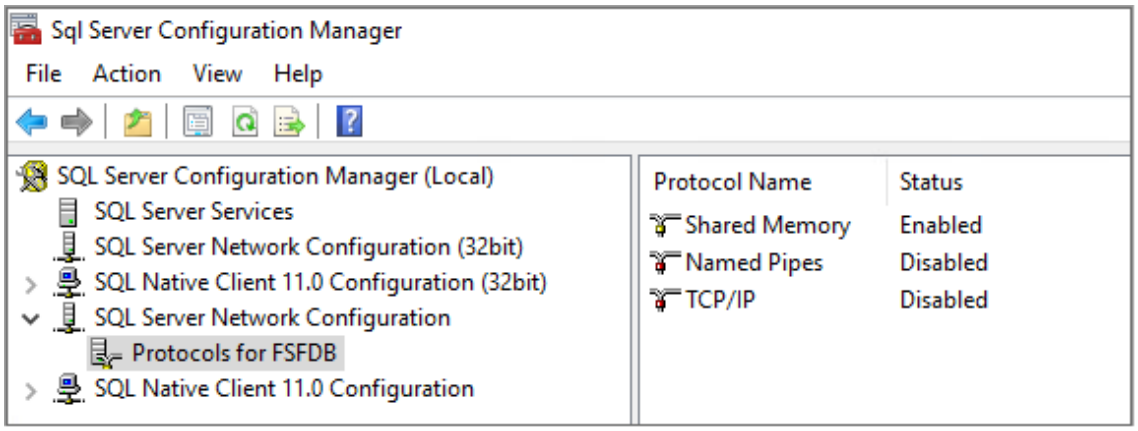
20 Click **Next**.

21 In the Complete page, click **Close**.

22 Launch SQL Server Configuration Manager.

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

24 Click Protocols for FSFDB (or the name of the database instance you chose earlier).

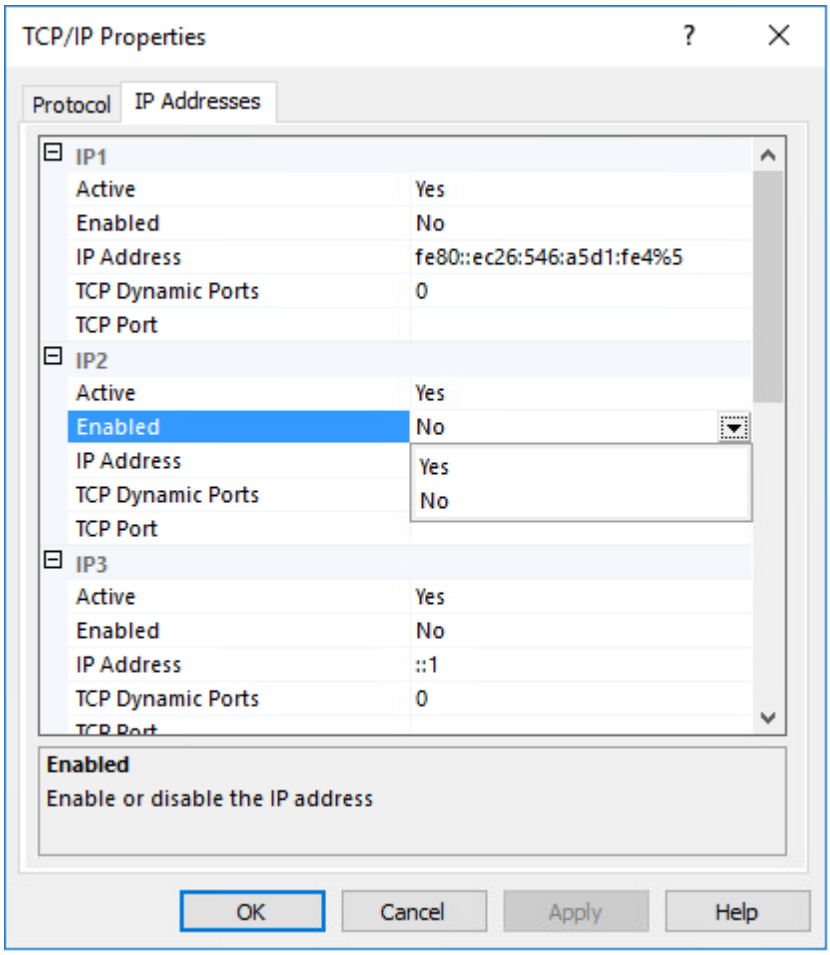


25 In the right pane, right-click **TCP/IP** and select **Enable**.

26 In the warning dialog box, click **OK**.

27 Right-click **TCP/IP** again and select **Properties**.

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



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

30 Scroll down to the **IPALL** heading and for 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 In the SQL Server Configuration Manager, click **SQL Server Services**.

35 Right-click **SQL Server (FSFDB)** and select **Restart**.

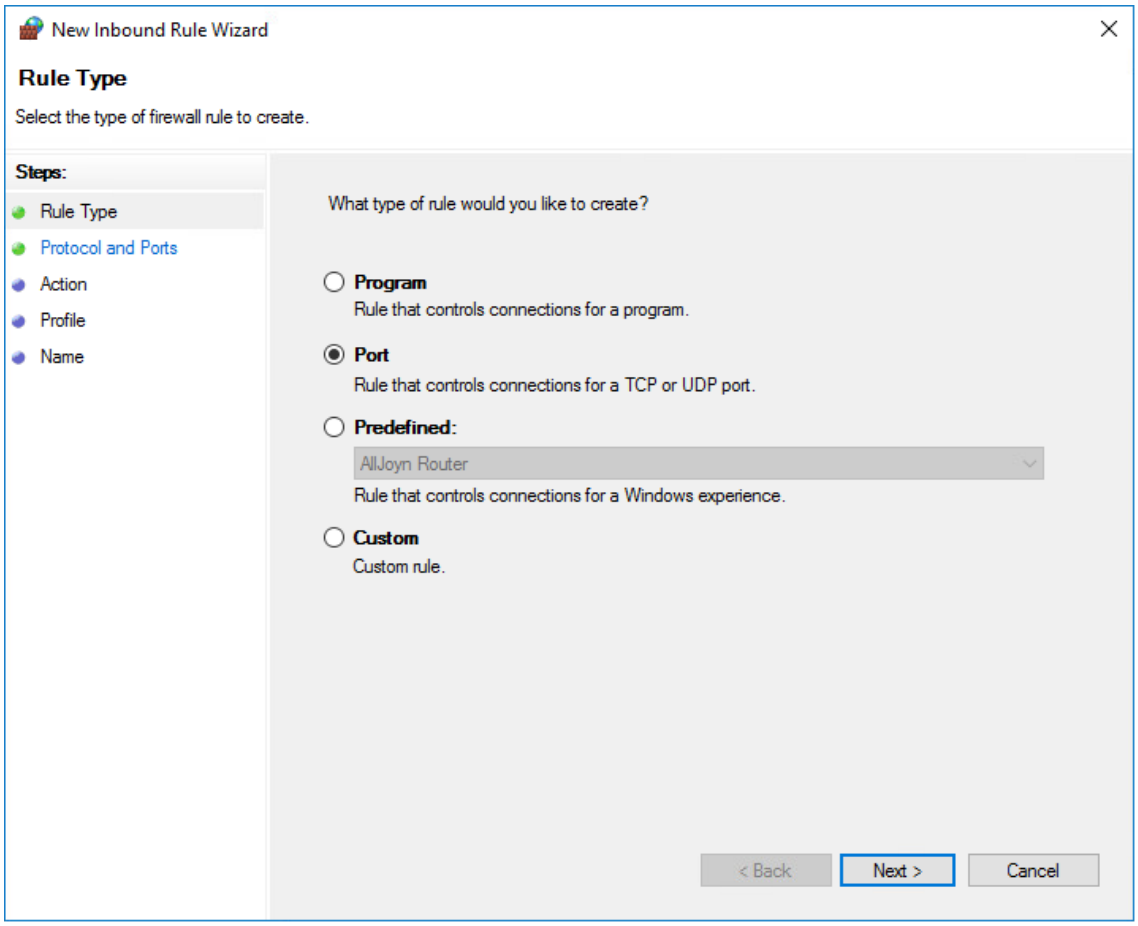
36 Close the SQL Server Configuration Manager.

37 Launch Windows Firewall with Advanced Security.

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

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

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



41 Click **Next**.

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

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

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

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

For example `SQL Server Express`.

46 Click **Finish**.

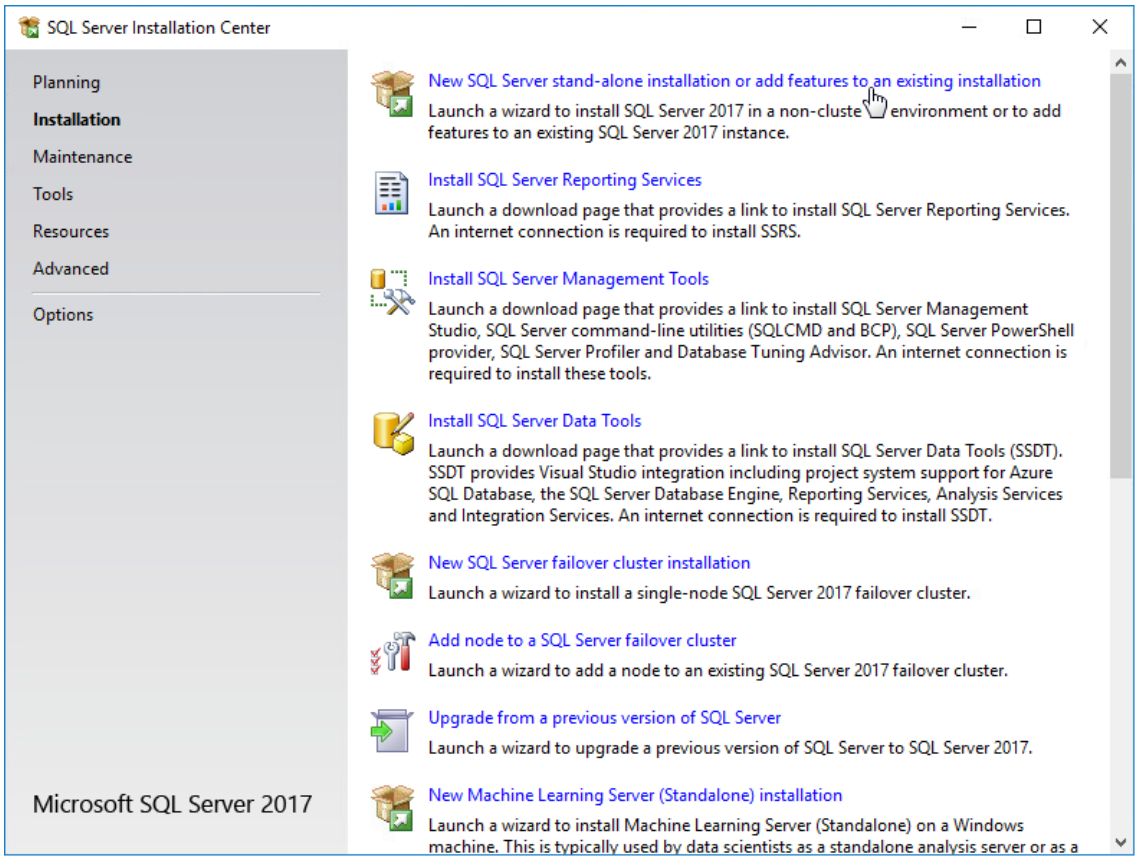
3.3 Install a New Instance of SQL Server

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

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

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

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



The Setup Support Rules operation is run.

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

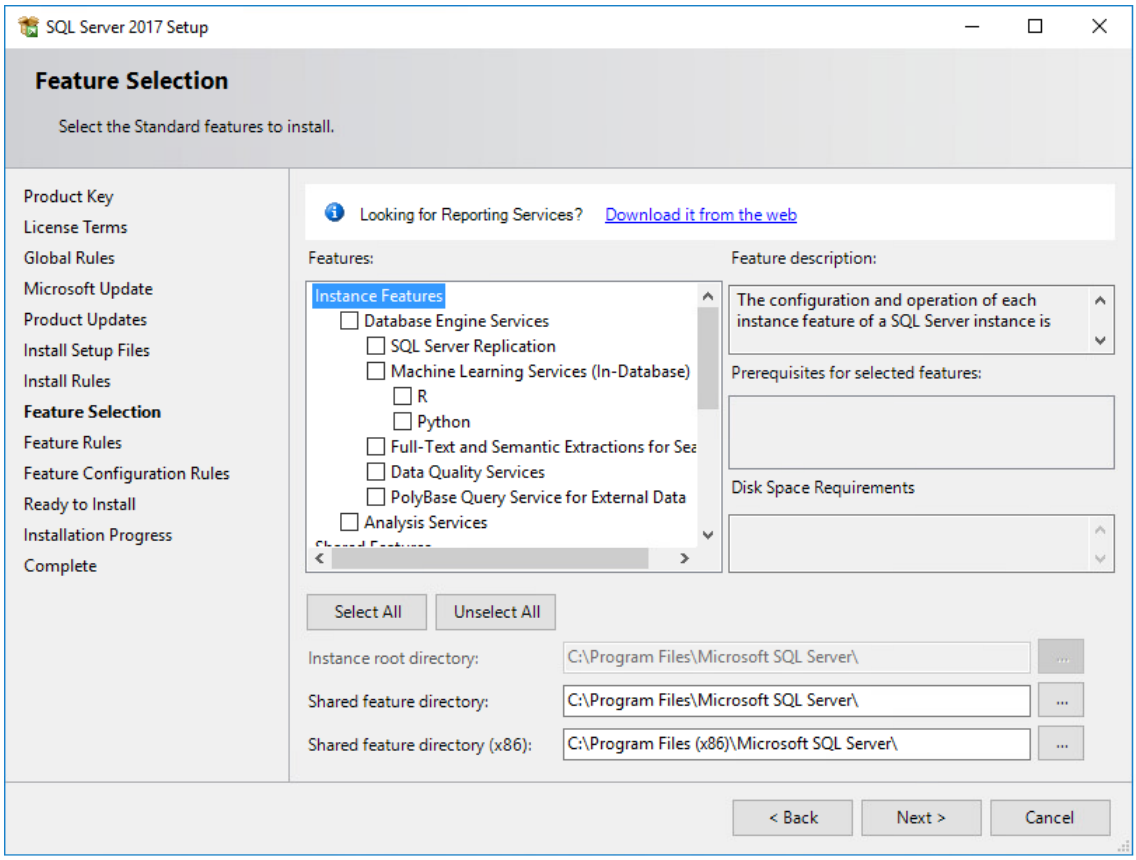
5 When prompted, enter your product key, then click **Next**.

6 Accept the license terms and click **Next**.

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

The Setup Support Rules operation is run again.

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



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

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

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

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

13 Click **Customize**.

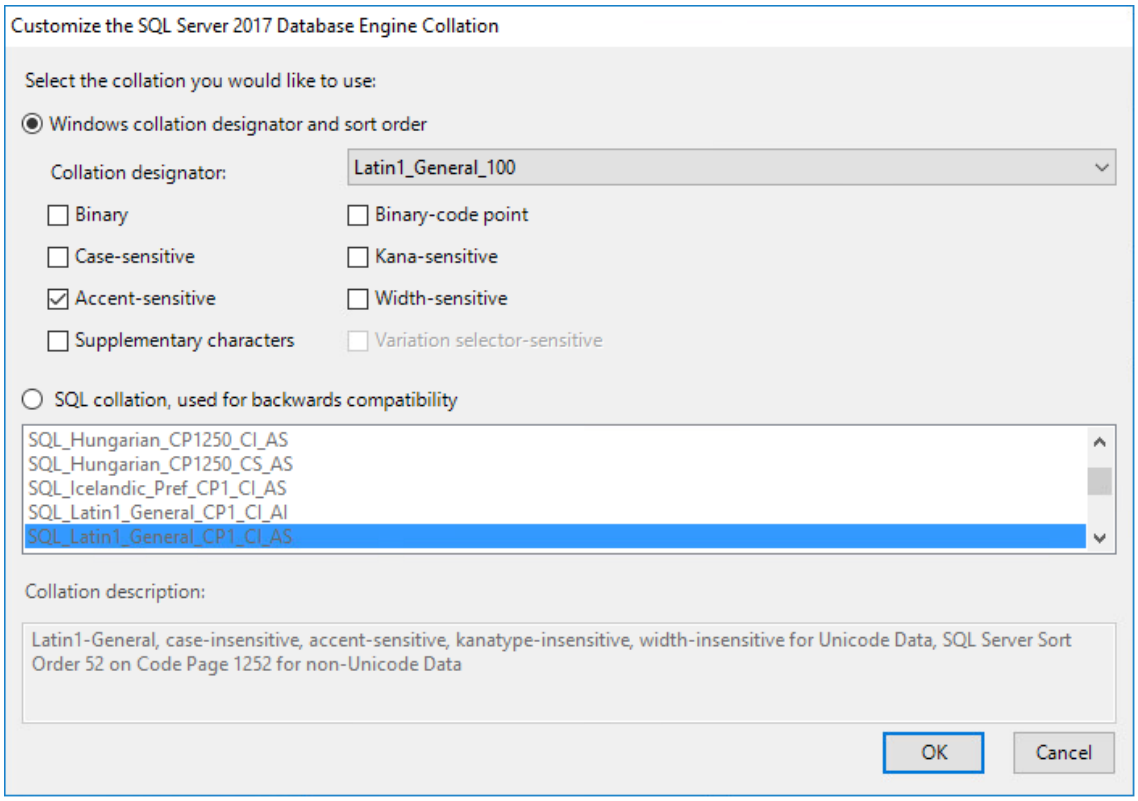
14 Click the **Windows collation designator and sort order** option.

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.

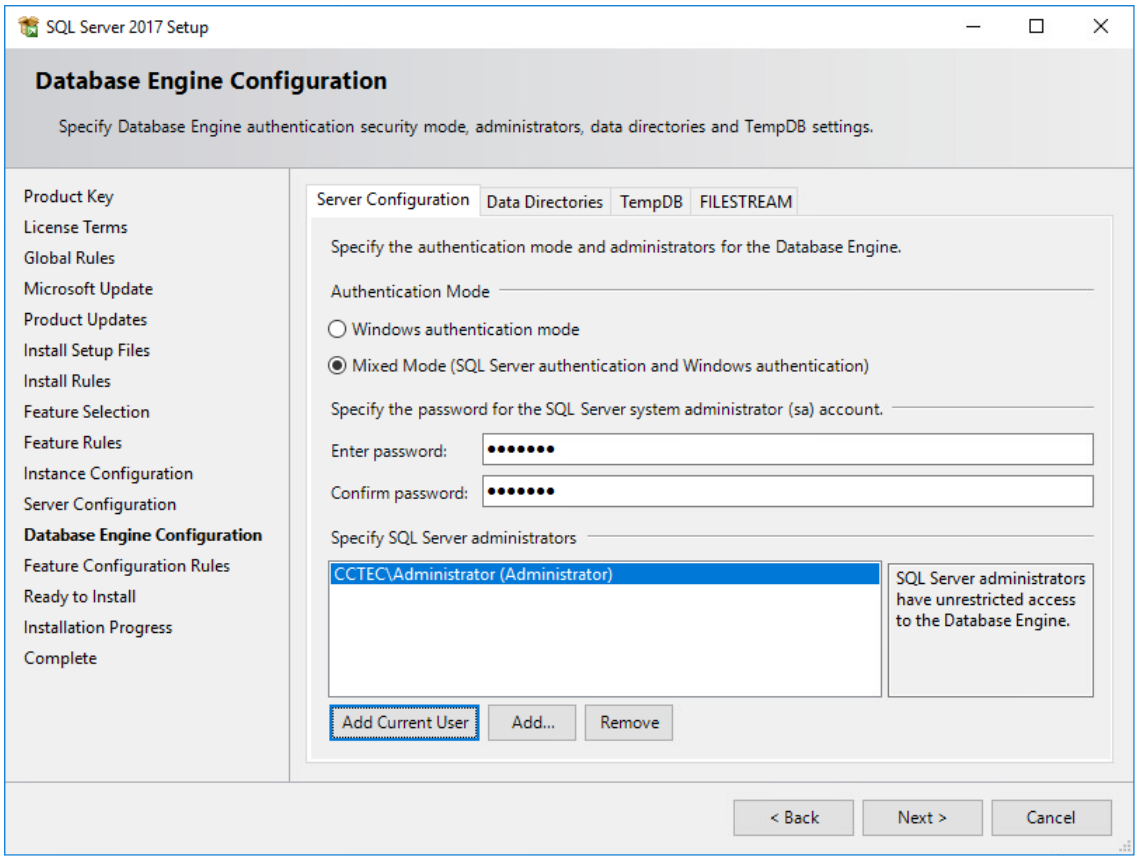
For more information on collation and locales, refer to this Microsoft document (http://technet.microsoft.com/en-us/library/ms175194%28v=sql.105%29.aspx).



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**.



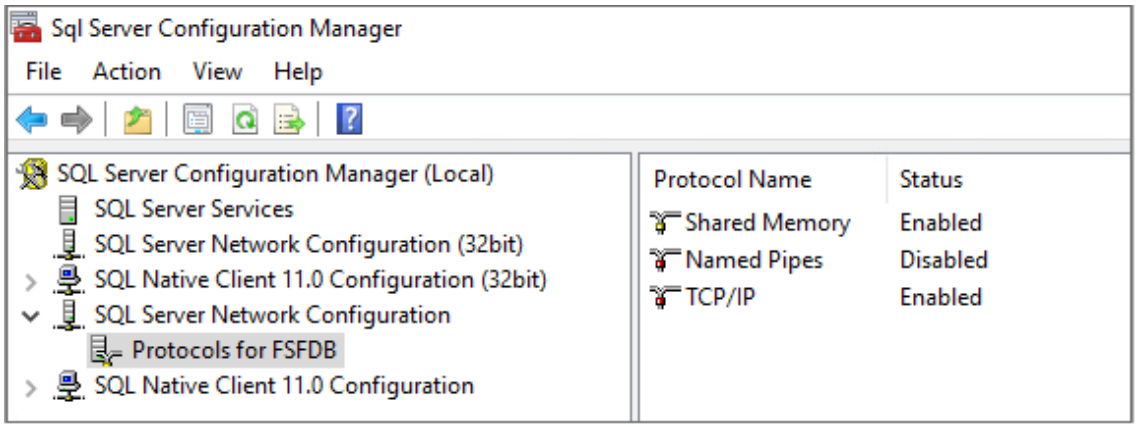
19 Click **Install**.

20 When the installation has completed, click **Close** to close the wizard.

21 Launch SQL Server Configuration Manager.

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

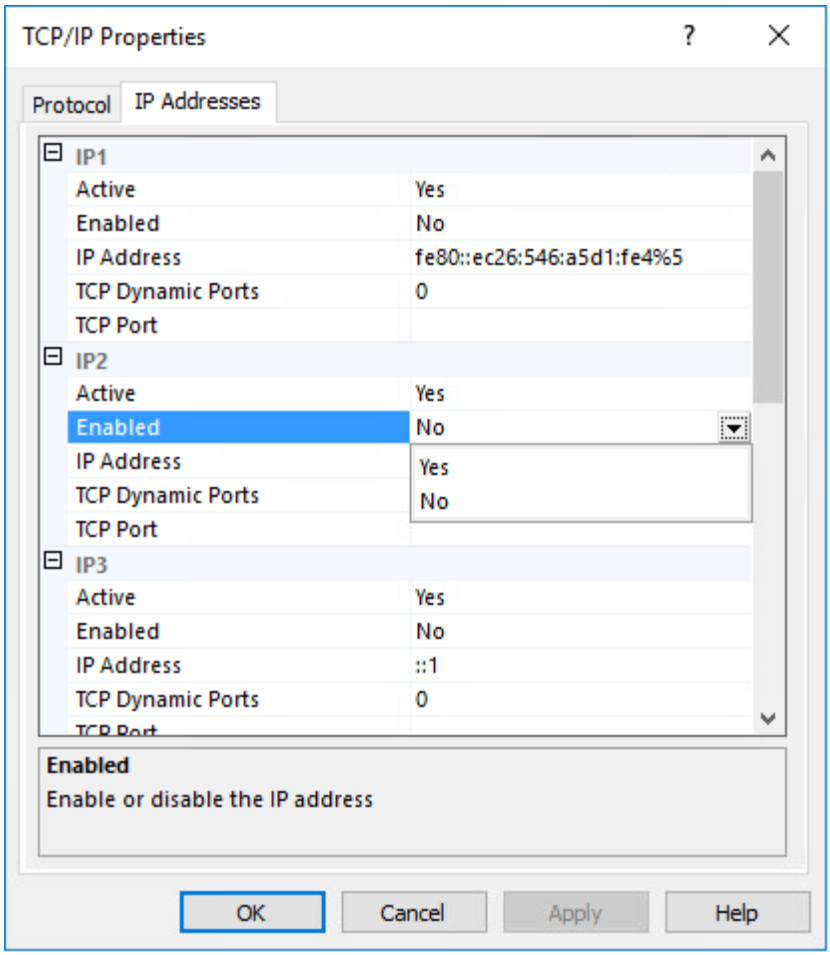
23 Click **Protocols for FSFDB** (or the name of the database instance you chose earlier).



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

25 Click the **IP Addresses** tab.

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



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

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

29 In the **TCP Port** field, and enter 1433.

30 Click **Apply**.

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

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

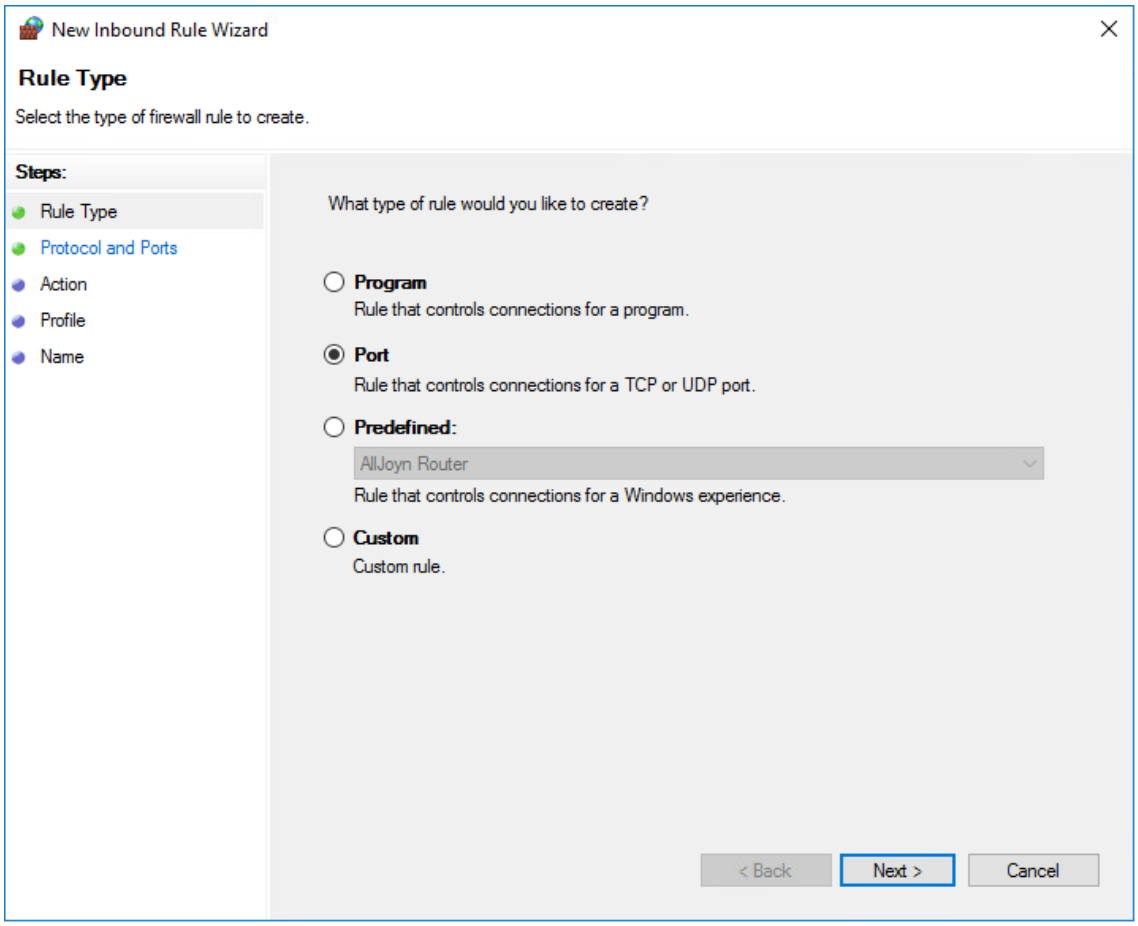
33 Close the SQL Server Configuration Manager.

34 Launch Windows Firewall with Advanced Security.

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

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

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



38 Click **Next**.

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

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

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

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

For example `SQL Server`.

43 Click **Finish**.

3.4 SQL Server Post Configuration Considerations

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/IP v4, because the Engine requires TCP/IP via port number 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.

4 Migrating from Storage Manager 3.1.1

- Section 4.1, “Prerequisites,” on page 33
- Section 4.2, “Understanding the Migration Process,” on page 33
- Section 4.3, “Accessing the Product Contents,” on page 34
- Section 4.4, “Stopping and Disabling Components,” on page 34
- Section 4.5, “Installing the Engine,” on page 35
- Section 4.6, “Installing the License,” on page 36
- Section 4.7, “Configuring the Database,” on page 38
- Section 4.8, “Migrating the Database,” on page 42
- Section 4.9, “Configuring the Engine,” on page 46
- Section 4.10, “Migrating the Engine Data,” on page 53
- Section 4.11, “Installing NSMAdmin,” on page 55
- Section 4.12, “Review Migrated Policies,” on page 57
- Section 4.13, “Upgrading to File Dynamics 6.1,” on page 57

IMPORTANT: There is no direct upgrade path from Storage Manager 3.1.1 to File Dynamics 6. You must upgrade in two phases 1) From Storage Manager 3.1.1 to 4.1 and 2) From Storage Manager 4.1 to File Dynamics 6.1.

You will need a Storage Manager 4 license. Since only an evaluation one is needed, you can request one at http://www.storagemanagersupport.com (http://www.storagemanagersupport.com).

Once you have completed this section, you should proceed with Chapter 5, “Upgrading from Storage Manager 4.1, 5.*x*, or File Dynamics 6.0 to File Dynamics 6.1,” on page 59.

Use the procedures in this section to migrate your deployment of Storage Manager 3.1.1 for Active Directory to Version 4.1. You should follow these procedures only after you have performed the prerequisite tasks in Chapter 1: Chapter 1, “Prerequisites,” on page 7, obtained a Storage Manager 4 for Active Directory license, and installed an SQL Server instance as specified in Chapter 3: Chapter 3, “Installing and Configuring an SQL Server Instance,” on page 17.

4.1 Prerequisites

If your Engine is not already running Version 3.1.1, update it before proceeding.

4.2 Understanding the Migration Process

The migration process involves the following steps:

- Accessing the product contents
- Stopping and disabling components
- Installing the 4.*x* Engine

- Installing the license
- Migrating the database
- Configuring the Engine
- Migrating the Engine Data
- Installing NSMAdmin
- Reviewing the migrated policies

Your options for migration can be either installing the components on the same server where the Storage Manager components are located, or on a different server. The only real migration that takes place is the database, which can be done in-place or across the wire.

4.3 Accessing the Product Contents

1. On the Windows server that will host the Engine, copy to a directory the `NSM-AD_4_1.iso` file that was made available to you following your purchase of Storage Manager 4.1 for Active Directory.
2. Mount the `NSM-AD_4_1.iso` file.
3. Note the location of the mounted ISO.

   This is the installation source you will use to install Storage Manager 4.1 for Active Directory components.

4.4 Stopping and Disabling Components

Since Storage Manager 4.1 components use the same port settings as the Storage Manager 3.1.1 components, you must stop and disable those components to avoid conflicts during the migration.

4.4.1 Stopping and Disabling the Engine

Follow procedures below.

1. On the server hosting the Engine, load `Services.msc`.
2. Right-click **Novell Storage Manager 3 Engine** and select **Stop**.
3. Right-click **Novell Storage Manager 3 Engine** and select **Properties**.
4. From the **Startup type** drop-down menu, select **Disabled**.
5. Click **OK**.

4.4.2 Stopping and Disabling the Event Monitor

1. On the server hosting the Event Monitor, load `Services.msc`.
2. Right-click **Novell Storage Manager Event Monitor** and select **Stop**.
3. Right-click **Novell Storage Manager Event Monitor** and select **Properties**.
4. From the **Startup type** drop-down menu, select **Disabled**.
5. Click **OK**.

4.4.3 Stopping and Disabling the Agents

1. On the server hosting the Agent, load `Services.msc`.
2. Right-click **Novell Storage Manager Agent** and select **Stop**.
3. Right-click **Novell Storage Manager Agent** and select **Properties**.
4. From the **Startup type** drop-down menu, select **Disabled**.
5. Click **OK**.

4.5 Installing the Engine

Storage Manager 4.1 for Active Directory uses only one Engine per forest. The Engine can be installed on a host server that meets the following minimum requirements:

- Microsoft Windows Server 2016 (Member Server)
- Microsoft Windows Server 2012 R2 (Member Server)
- Microsoft Windows Server 2012 (Member Server)
- Microsoft Server 2008 R2 (Member Server)
- At least 4 GB RAM
- For quota management, Microsoft File System Resource Manager (FSRM) must be installed; see Section 1.2, “File Server Resource Manager,” on page 8.
- Forest functional level of Windows Server 2003 or later

IMPORTANT: Once the Engine has been migrated, the existing Event Monitor and Agents become legacy components because they cannot perform their duties until they are also migrated. These legacy components are not deauthorized, nor are they removed, until you remove them yourself.

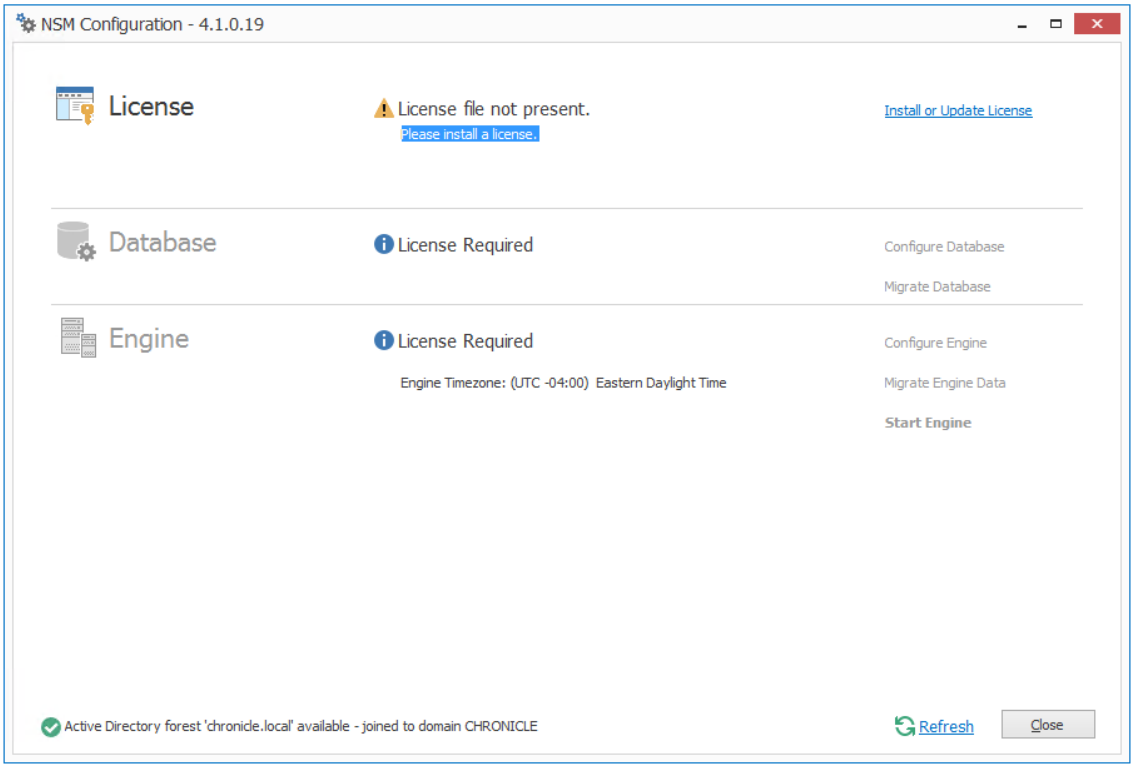
Having legacy components allows you to view the configuration settings and proxy assignments so you can reestablish them when you install the new Event Monitor and Agents.

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
- A firewall inbound rule is added during the Engine installation

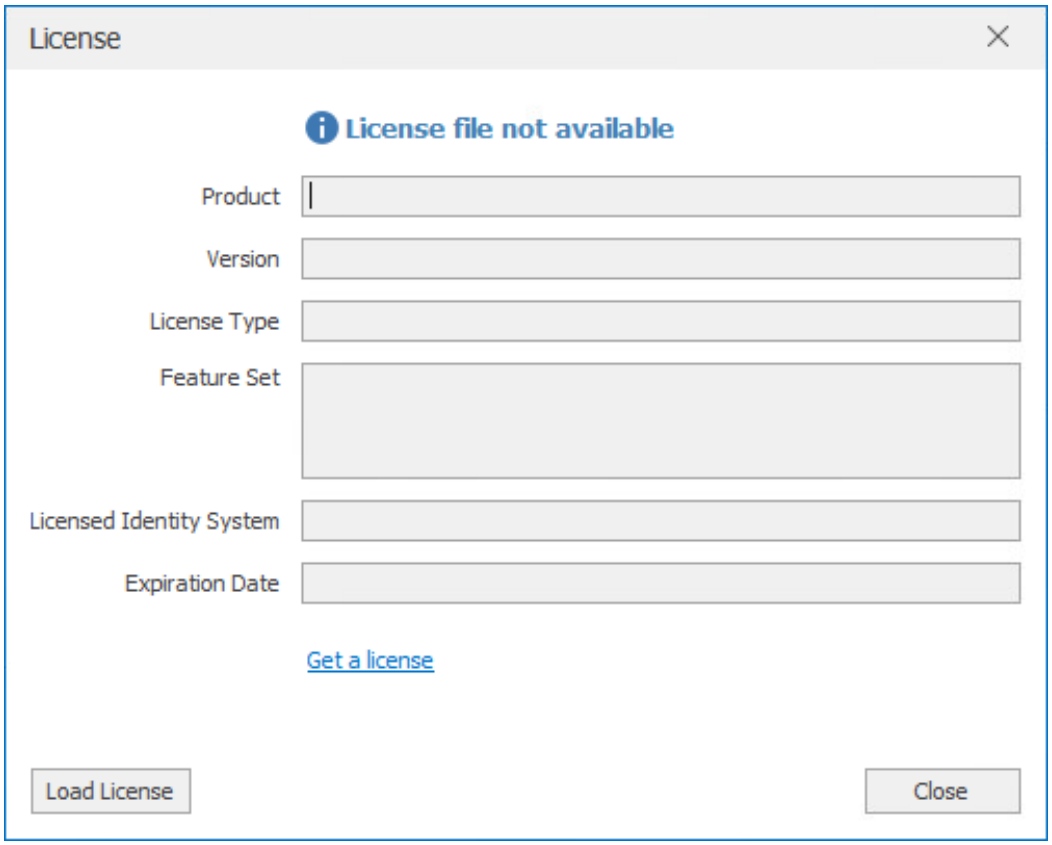
1. At the root of the `NSM-AD_4_1.iso` image, double-click the `Windows` folder.
2. Double-click the `x86_64` folder.
3. Double-click `NSMEngine-Installer-4.1-x64-`*`xxxx`*`.exe`.
4. When you are asked if you want to run this file, click **Run**.
5. Agree to the licensing terms and conditions and click **Install**.
6. When notified that the setup was successful, click **Run Setup Utility.**

The Configuration Dashboard appears.



4.6 Installing the License

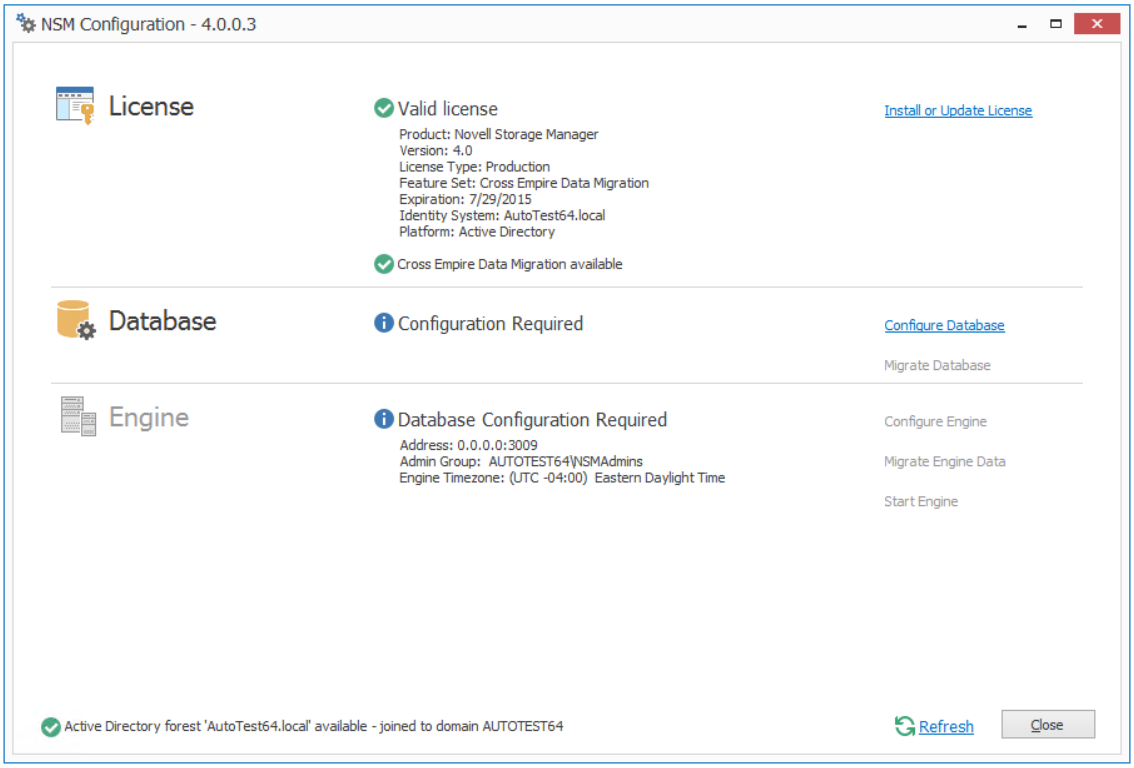
1 Click **Install or Update License**.



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

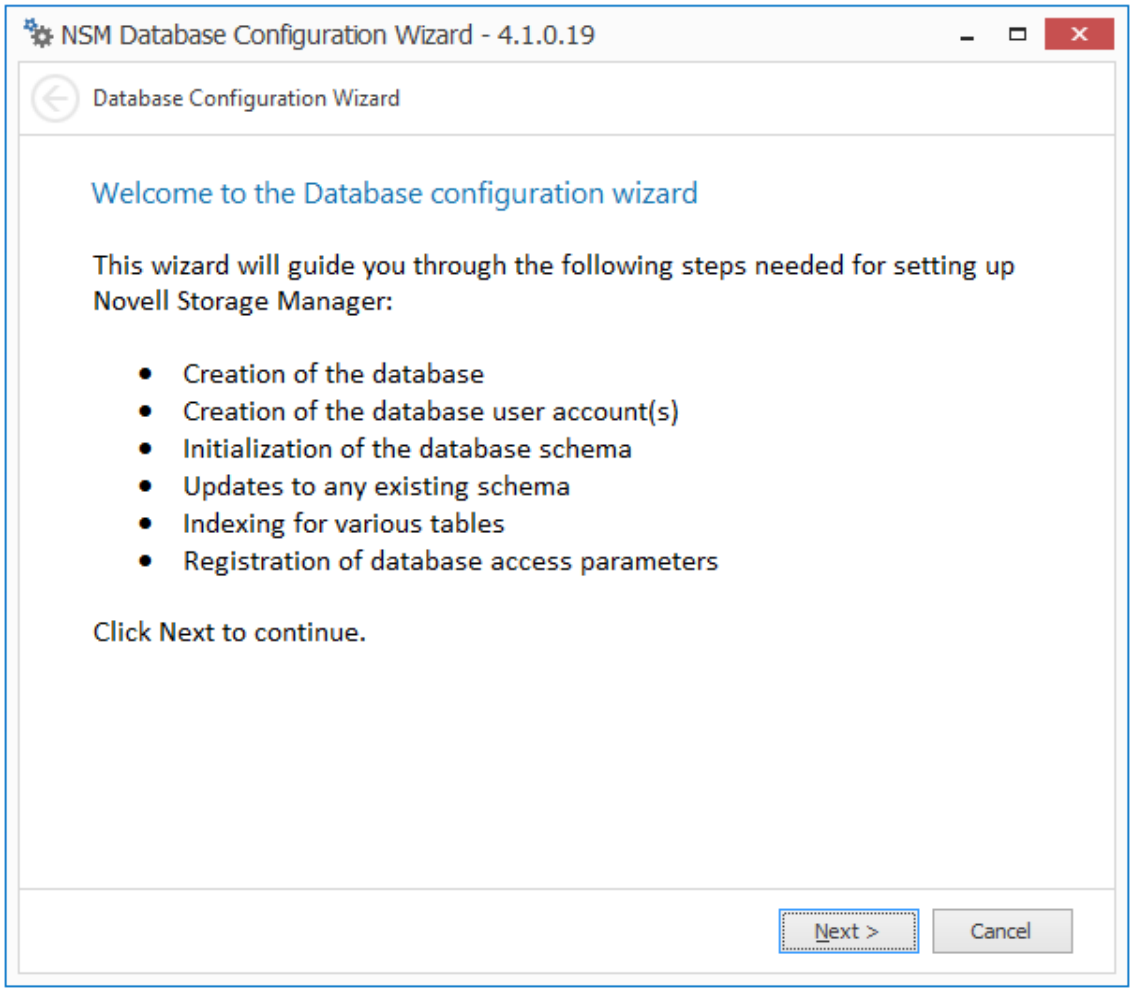
3 When the confirmation prompt appears, click **Yes**.

4 Click **Close**.



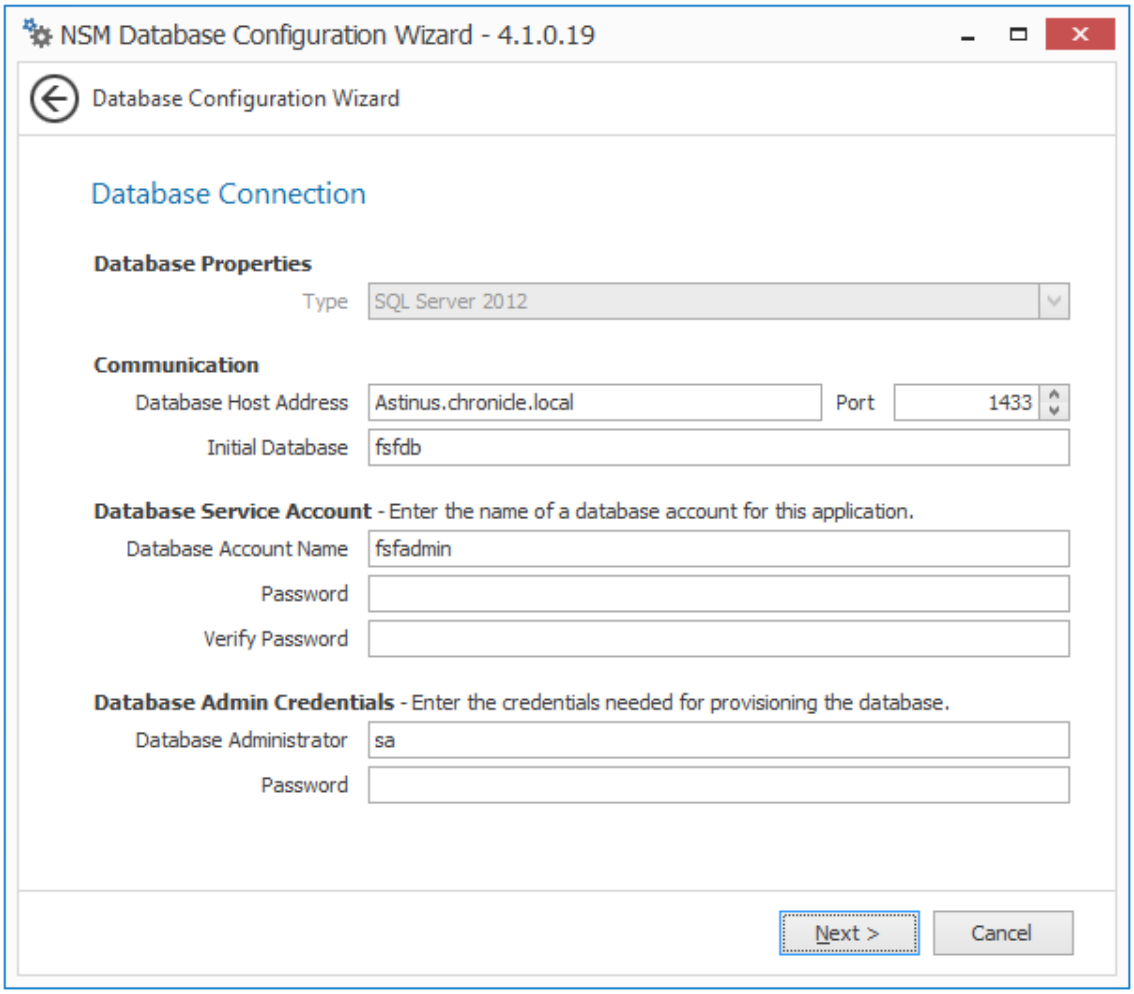
4.7 Configuring the Database

1 Click **Configure Database**.



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

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



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

Database Properties: Displays information on the database.

Type: Displays the minimum supported version of the database, which is SQL Server 2012.

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: The default SQL Server port setting is 1433. If there is a port conflict, you can change it.

Initial Database: The default name of the Novell Storage Manager database.

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.

Database Account Name: By default, the database account is fsfadmin, which you can change in this field.

Password: Specify a password for the service account to connect to the database.

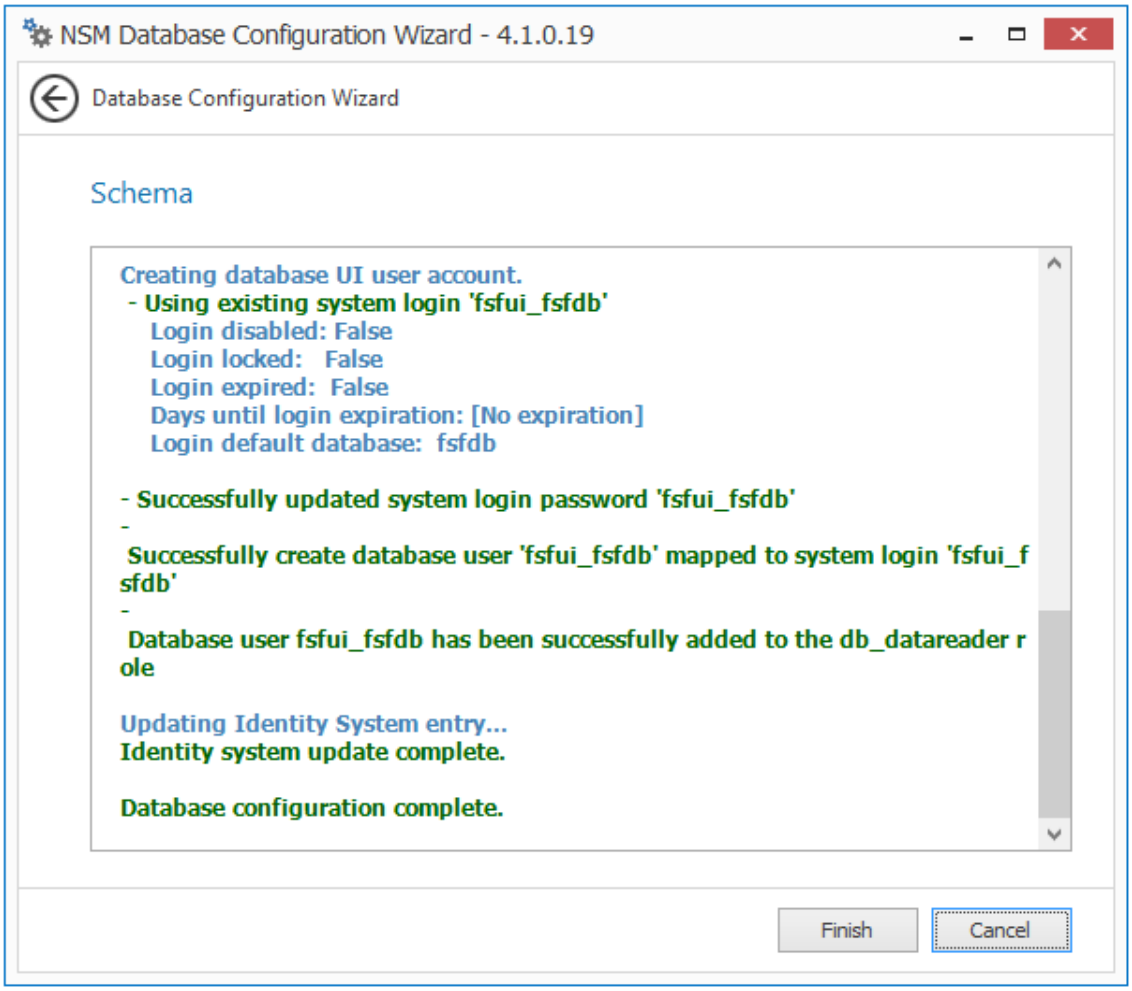
Verify Password: Specify the password again in this field.

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

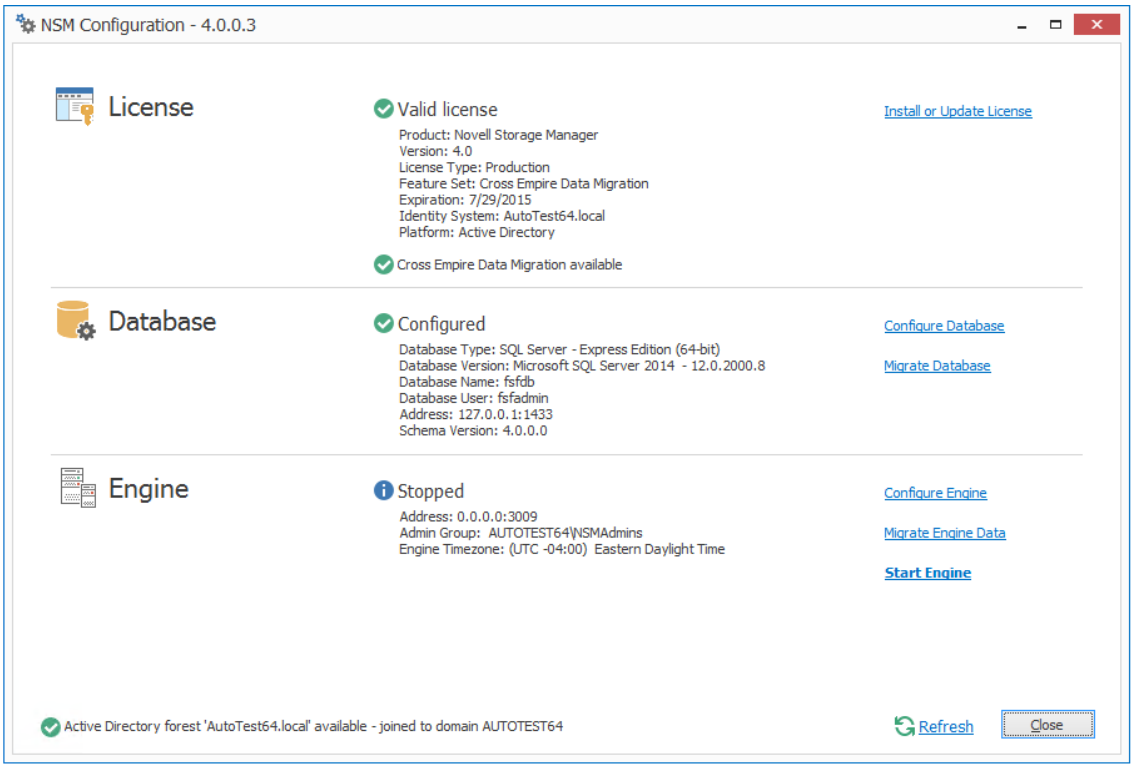
Database Administrator: Specify the SQL Server administrator name.

Password: Specify the SQL Server administrator password.

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



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

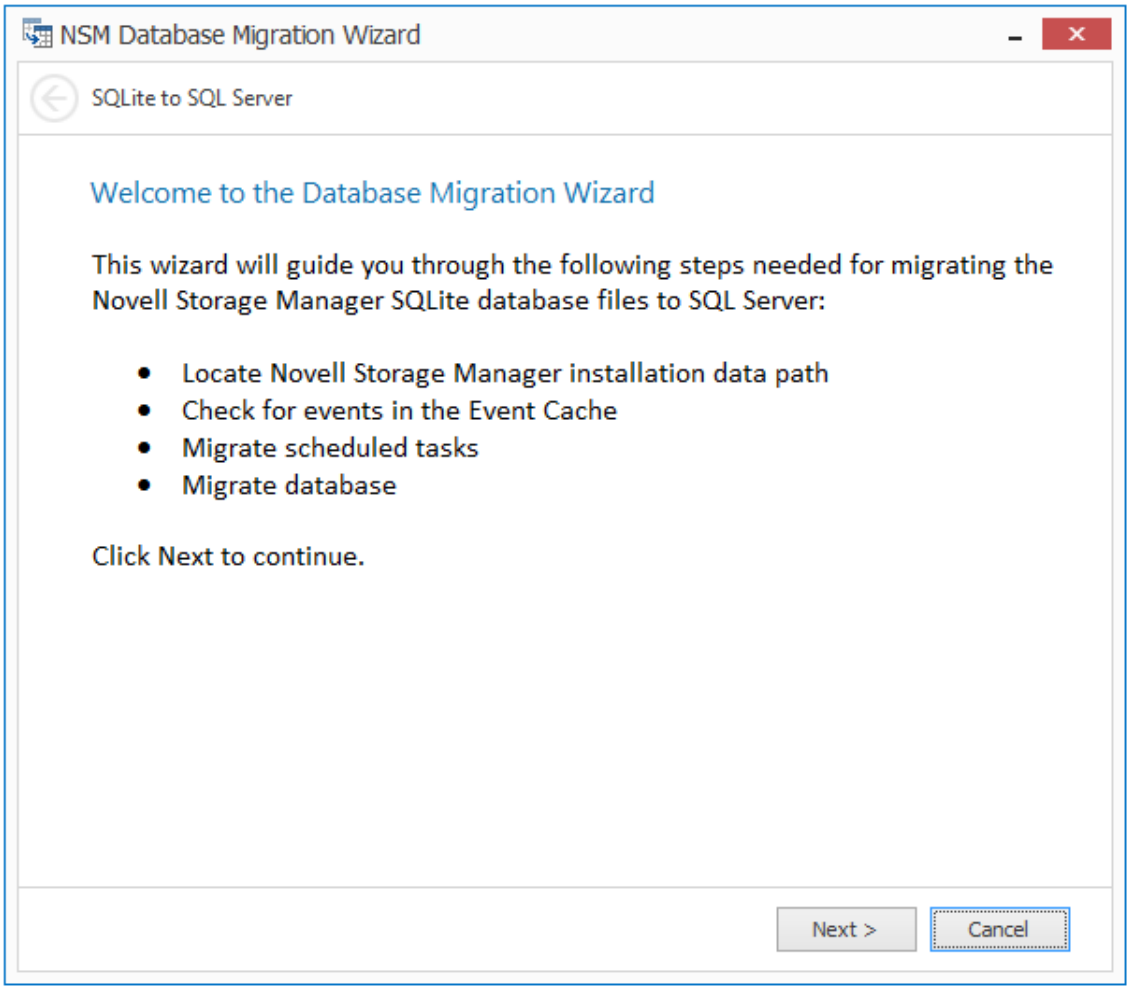


Note that the Configuration Dashboard now has the **Migrate Database** option.

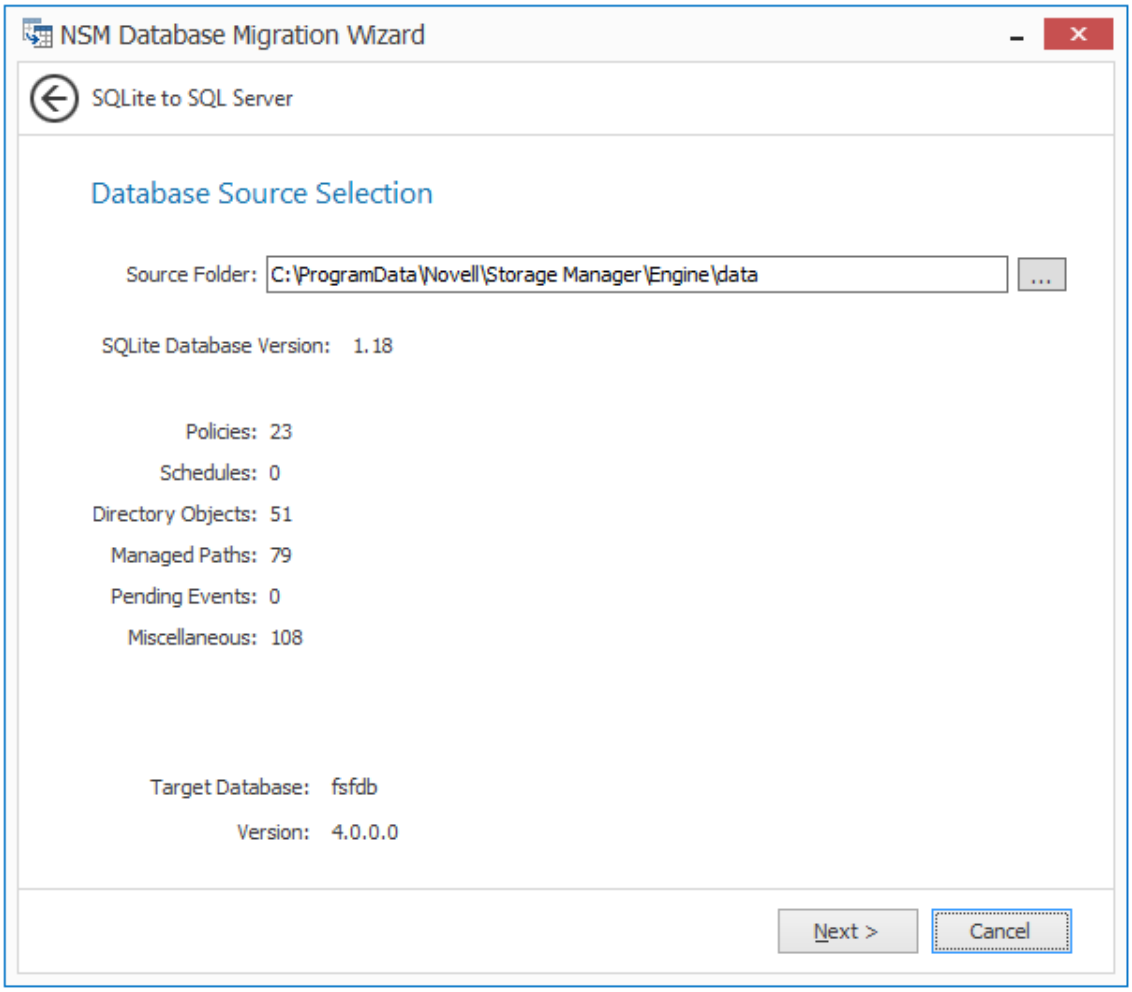
4.8 Migrating the Database

This procedure migrates the contents of the Storage Manager 3.1.1 SQLite database to the Storage Manager 4.1 SQL Server database. These contents include policies, schedules, pending events, etc.

1 Click **Migrate Database**.



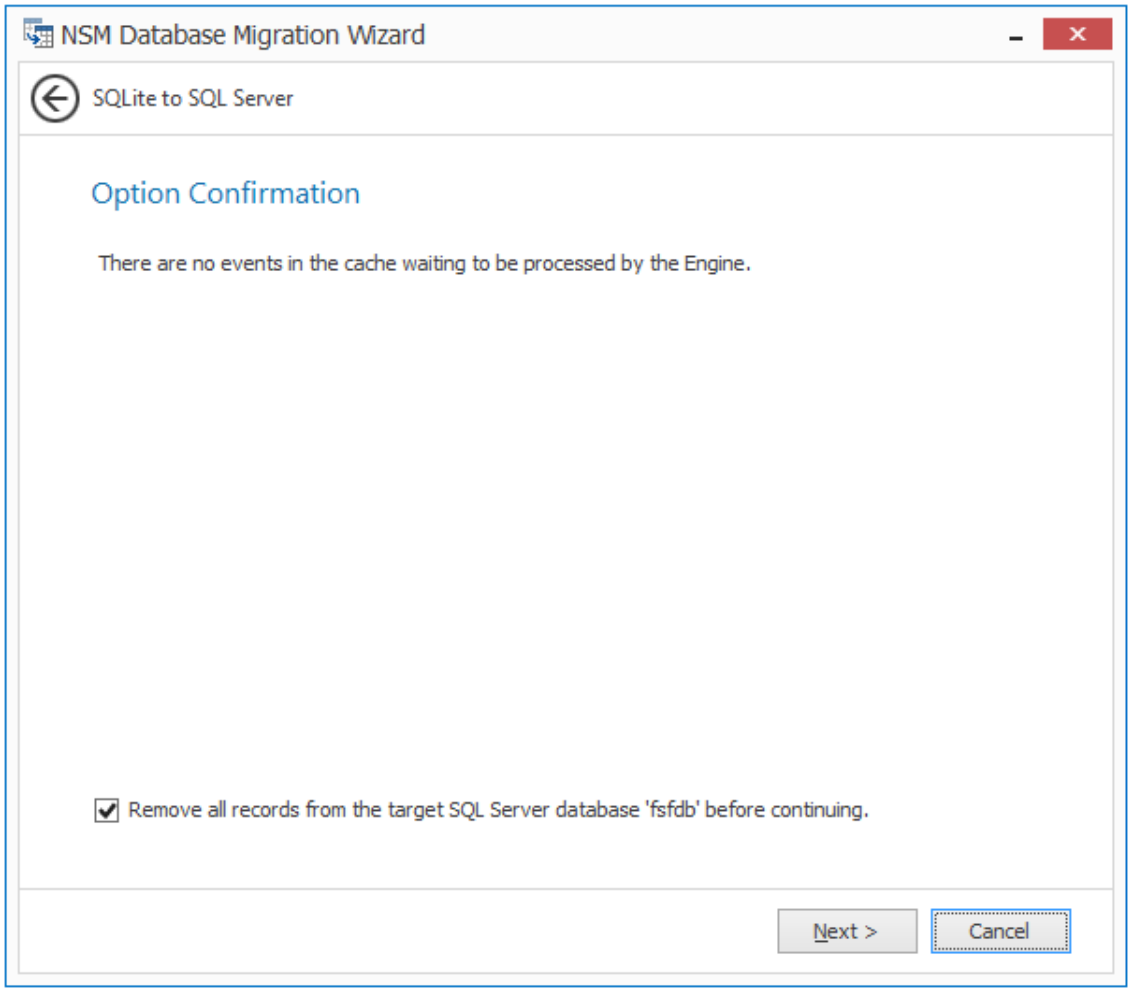
2 From the wizard page, read the overview of the migration process and click **Next**.



3 Verify that the Source Folder field displays the following path:
`C:\ProgramData\Novell\Storage Manager\Engine\data`

If the path is not displayed, click the browse button to specify the path.

4 Click **Next**.

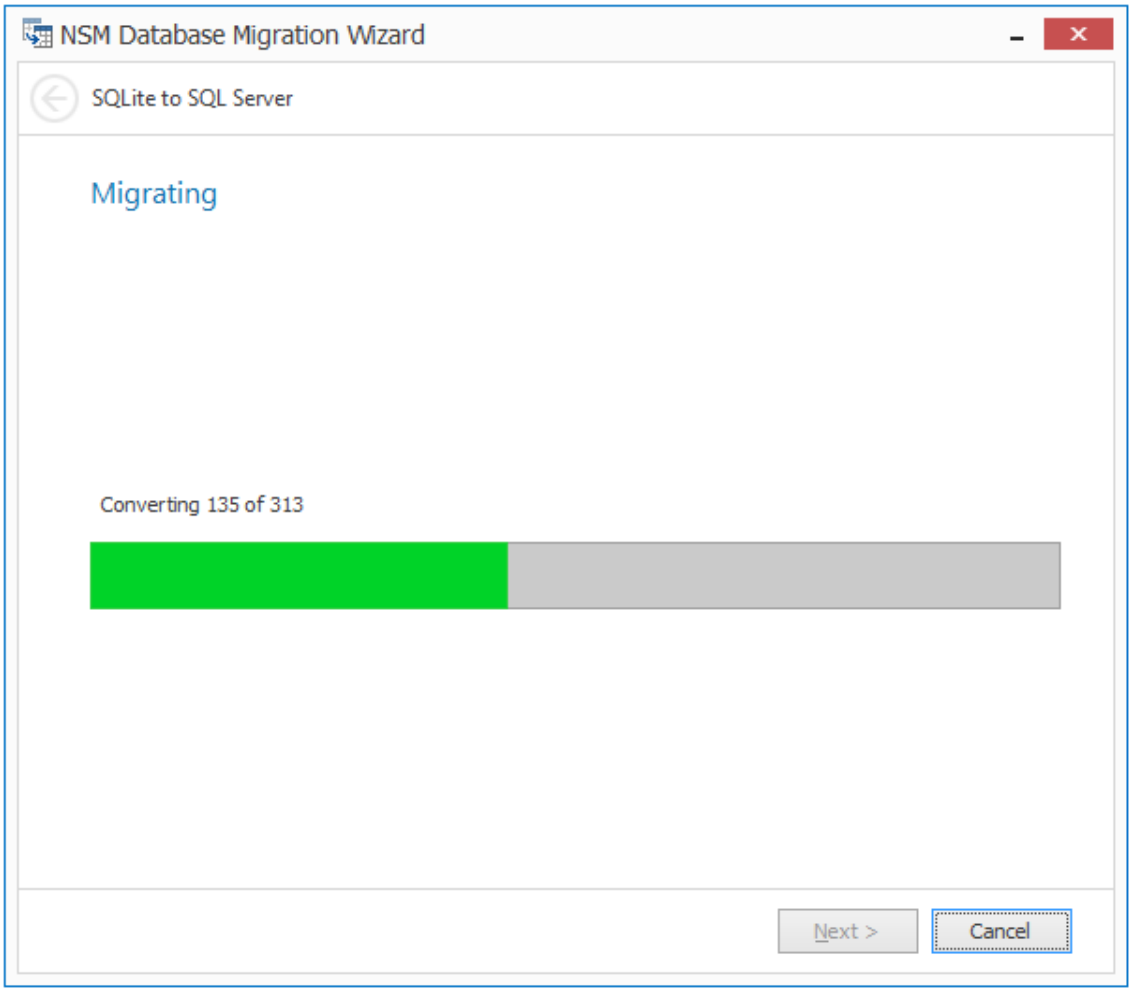


If there are any events in cache (and therefore not yet pending events), the events are displayed.

The **Remove all records from the target SQL Server database before continuing** option lets you remove any existing records in the target database instance before migrating. If there are any existing records in the SQL Server database instance, you should select this option to maintain the integrity of the database contents that are being migrated. This is applicable even if you decide to migrate the SQLite database again.

It is not safe to migrate a Novell Storage Manager SQLite database to a SQL Server database that contains policies or other critical data. Doing so is not supported as it could result in unpredictable behavior with the database.

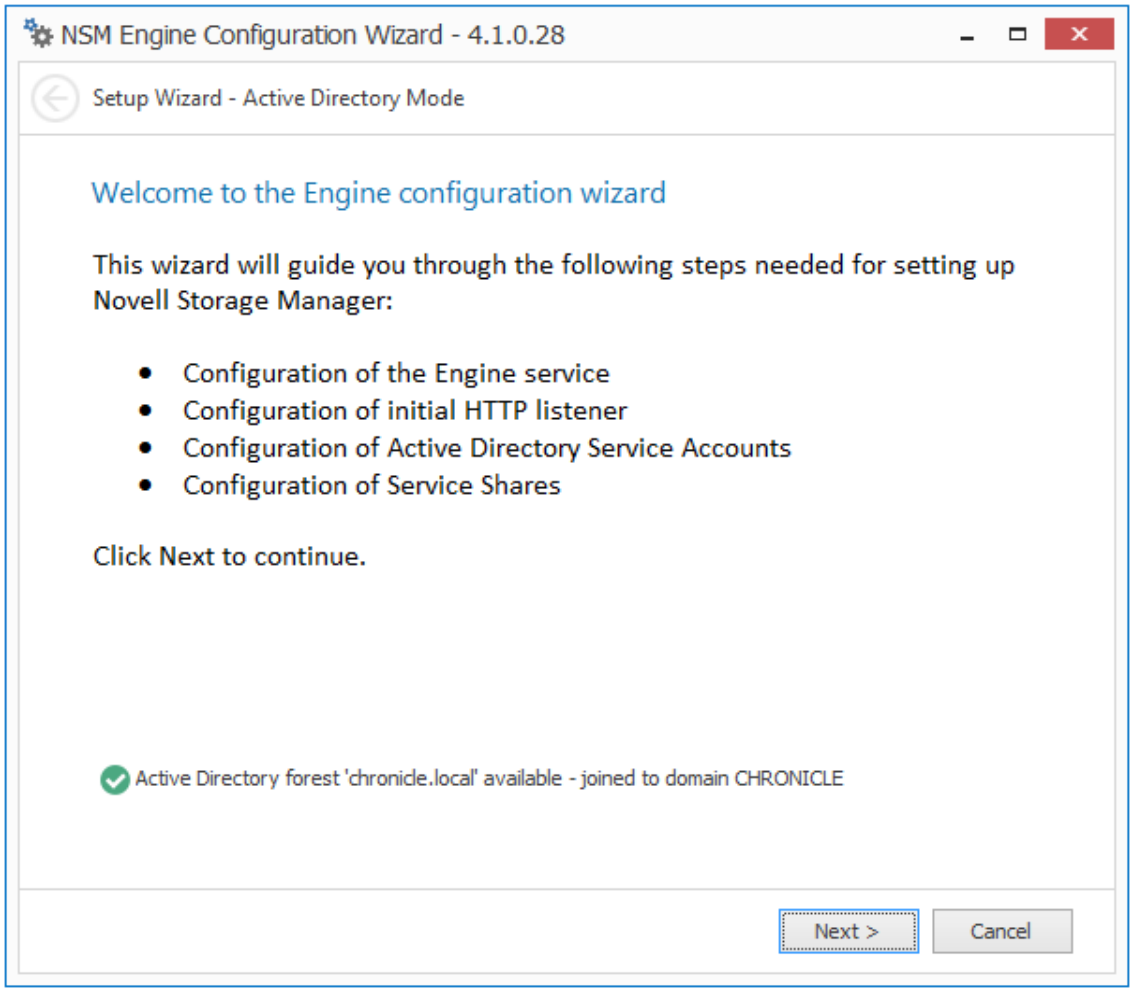
5 Specify whether to remove any existing records in the target database and click **Next**.



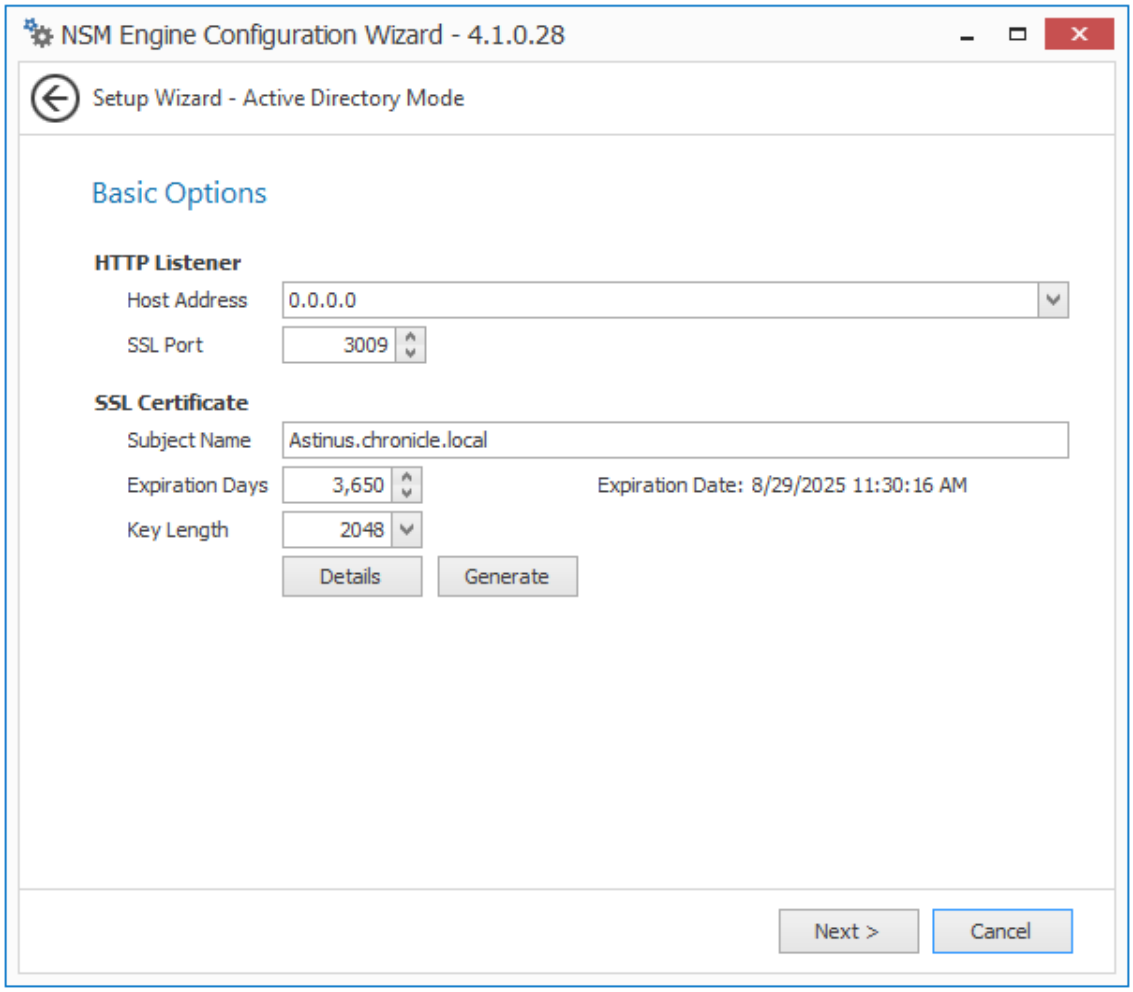
6 When notified that the migration has completed, click **Finish**.

4.9 Configuring the Engine

1 From the Configuration Dashboard, click **Configure Engine**.



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



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

HTTP Listener: Communication parameters for the Engine.

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

SSL Port: Unless there is a port conflict, leave the setting at 3009.

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.

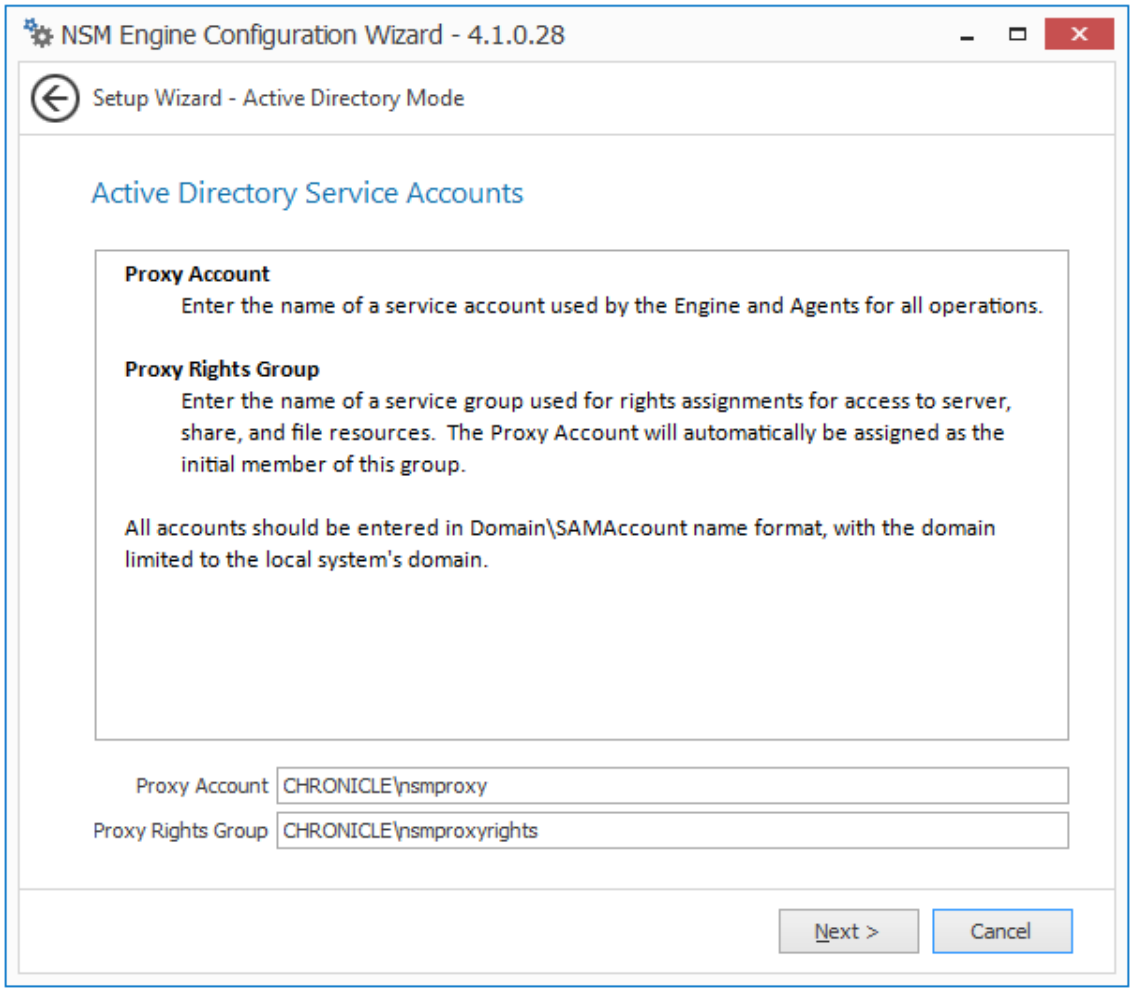
Key Length: The SSL certificate encryption setting, which is set at 2048 by default.

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, Event Monitor configuration data, and application specific historical data.

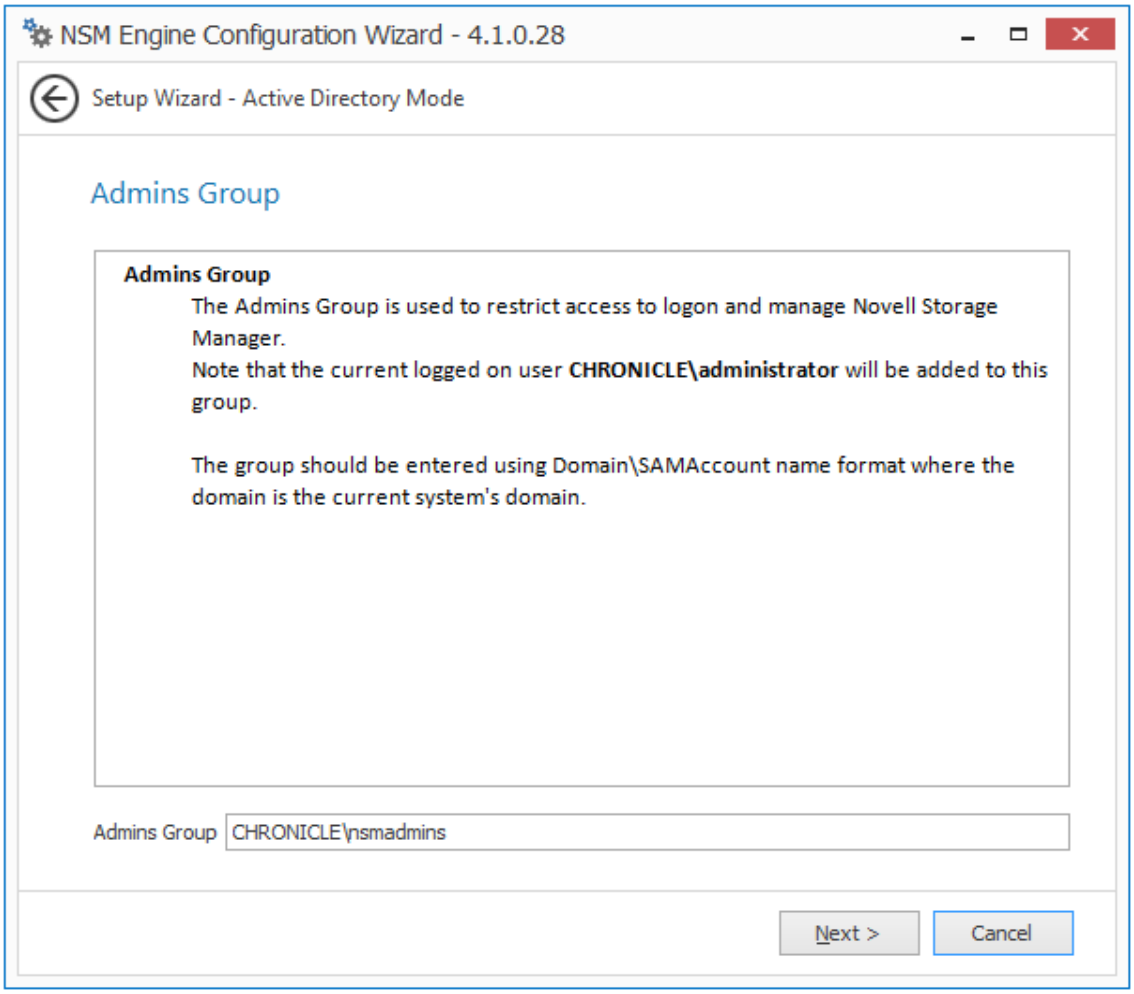
3 Edit any needed parameters settings and click **Next**.



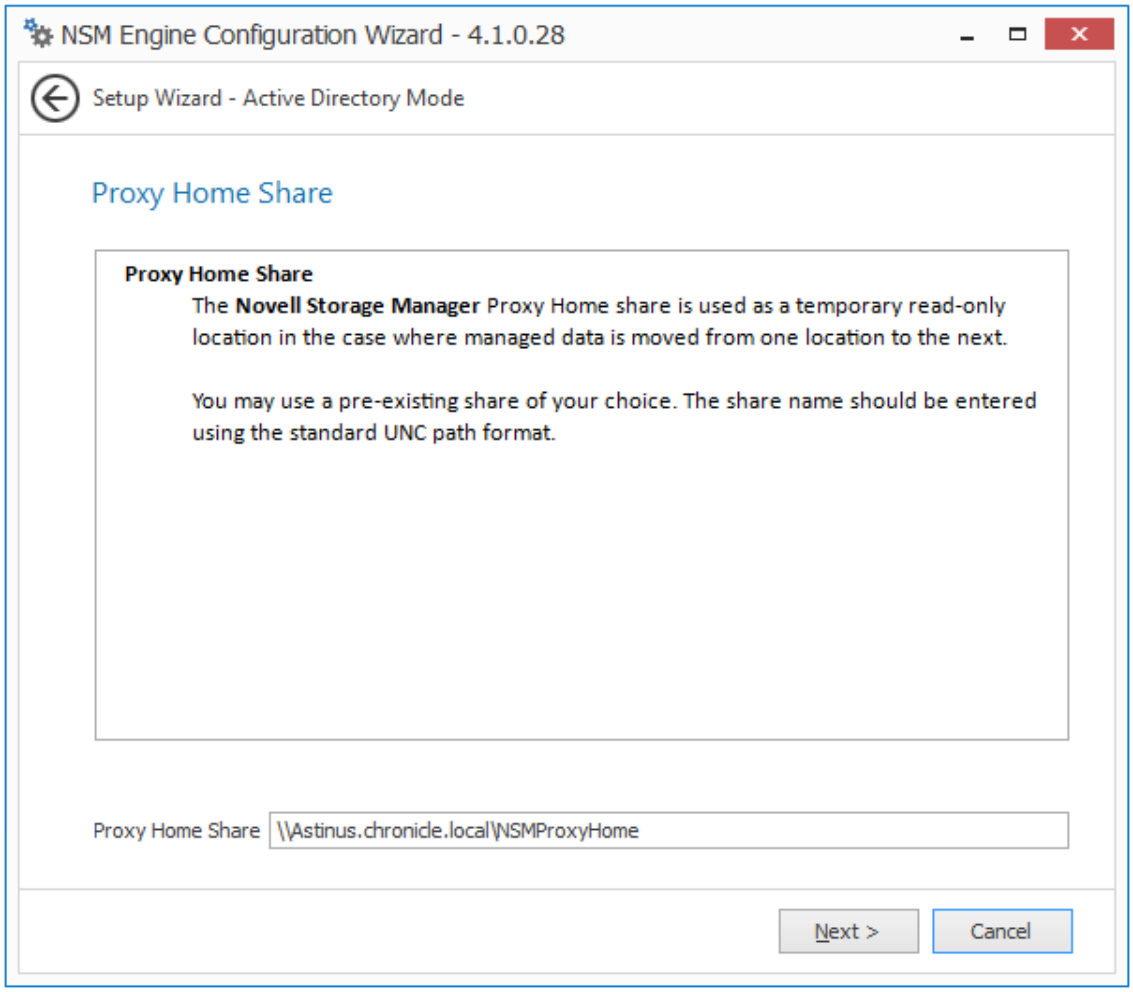
This page lets you establish a name for the proxy account and proxy rights group.

Novell Storage Manager uses a proxy account so that it can perform tasks necessary for storage management.

4 Click **Next**.



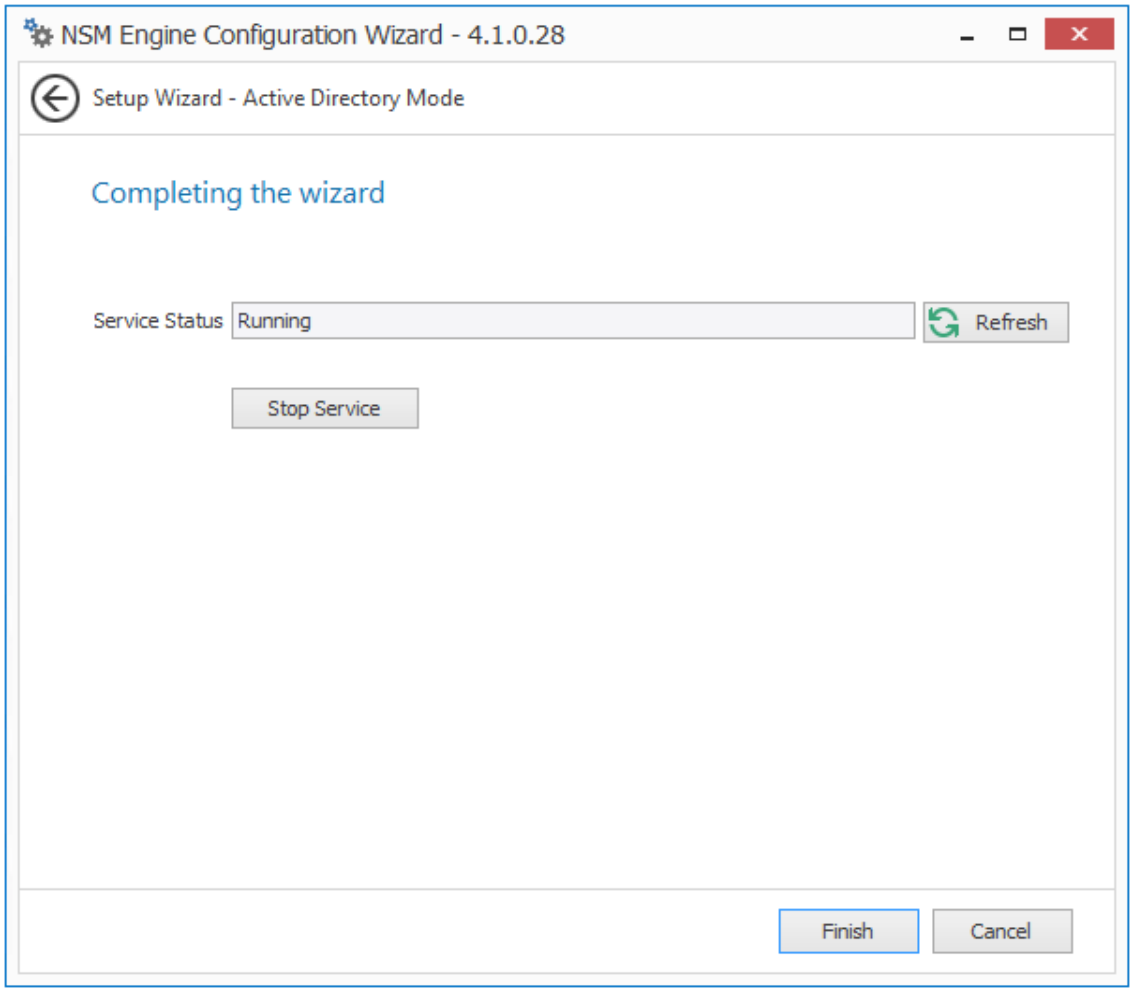
5 Specify the name for the Admins Group, or use the default name, and click **Next** to create the group.



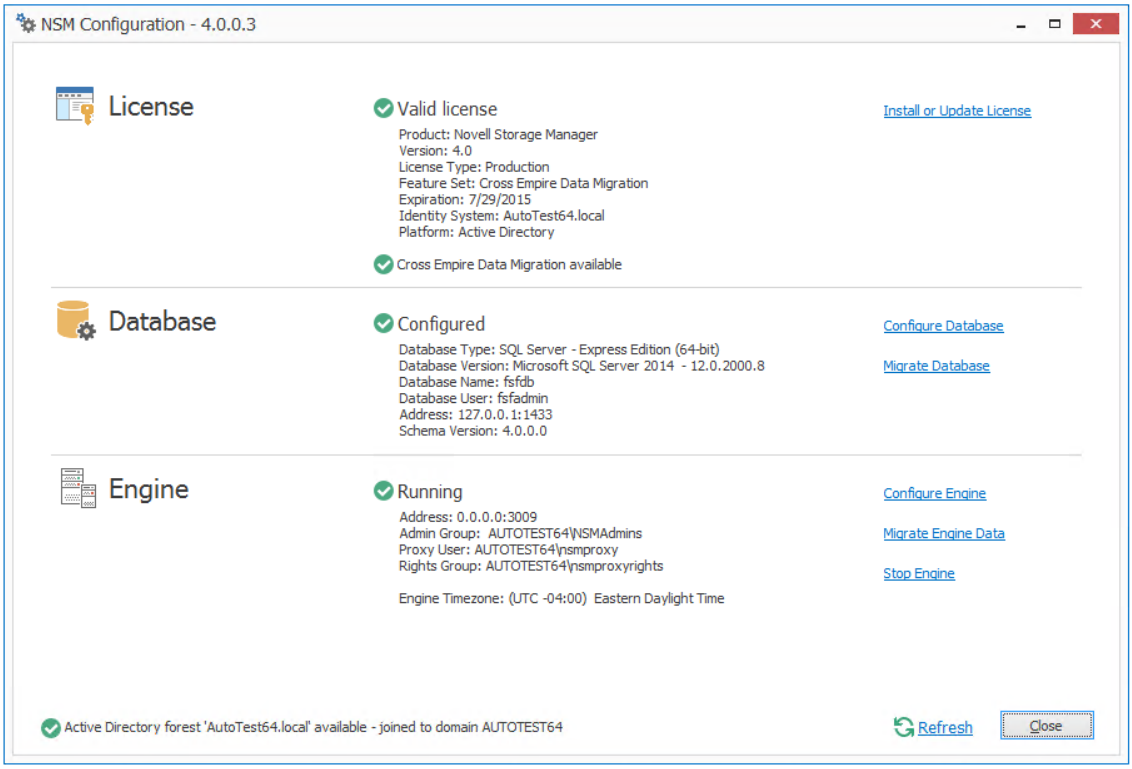
The Proxy Home Share that you establish in this page is the read-only location where users' managed path attributes are temporarily set when data is moved because of a change in policy.

The **Overwrite Existing Files** option lets the administrator specify whether files being placed in the Proxy Home Share are to replace existing files with the same name.

6 Specify whether to overwrite existing files and the Proxy Home Share path, then click **Next**.



7 Click **Finish**.



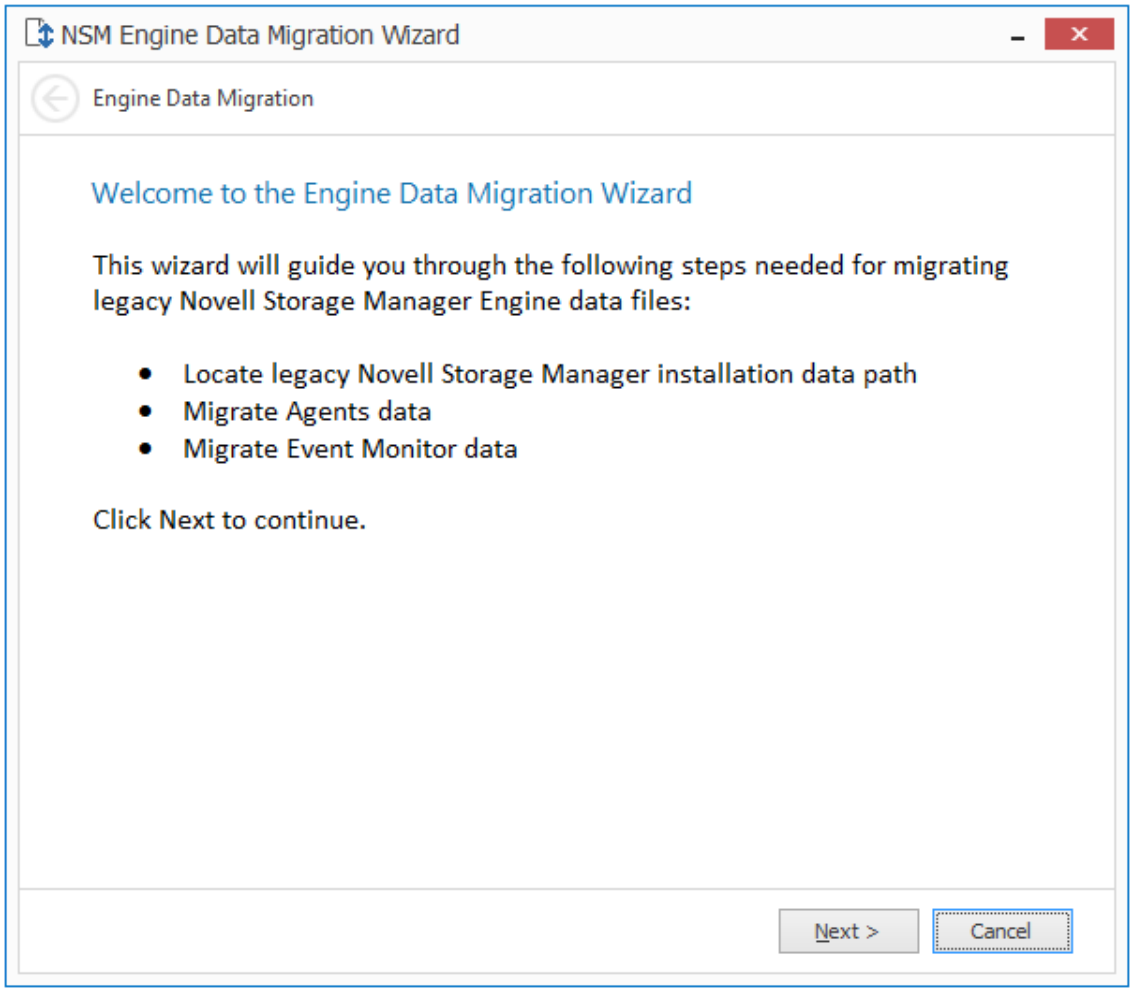
8 Proceed with Section 4.10, “Migrating the Engine Data,” on page 53.

4.10 Migrating the Engine Data

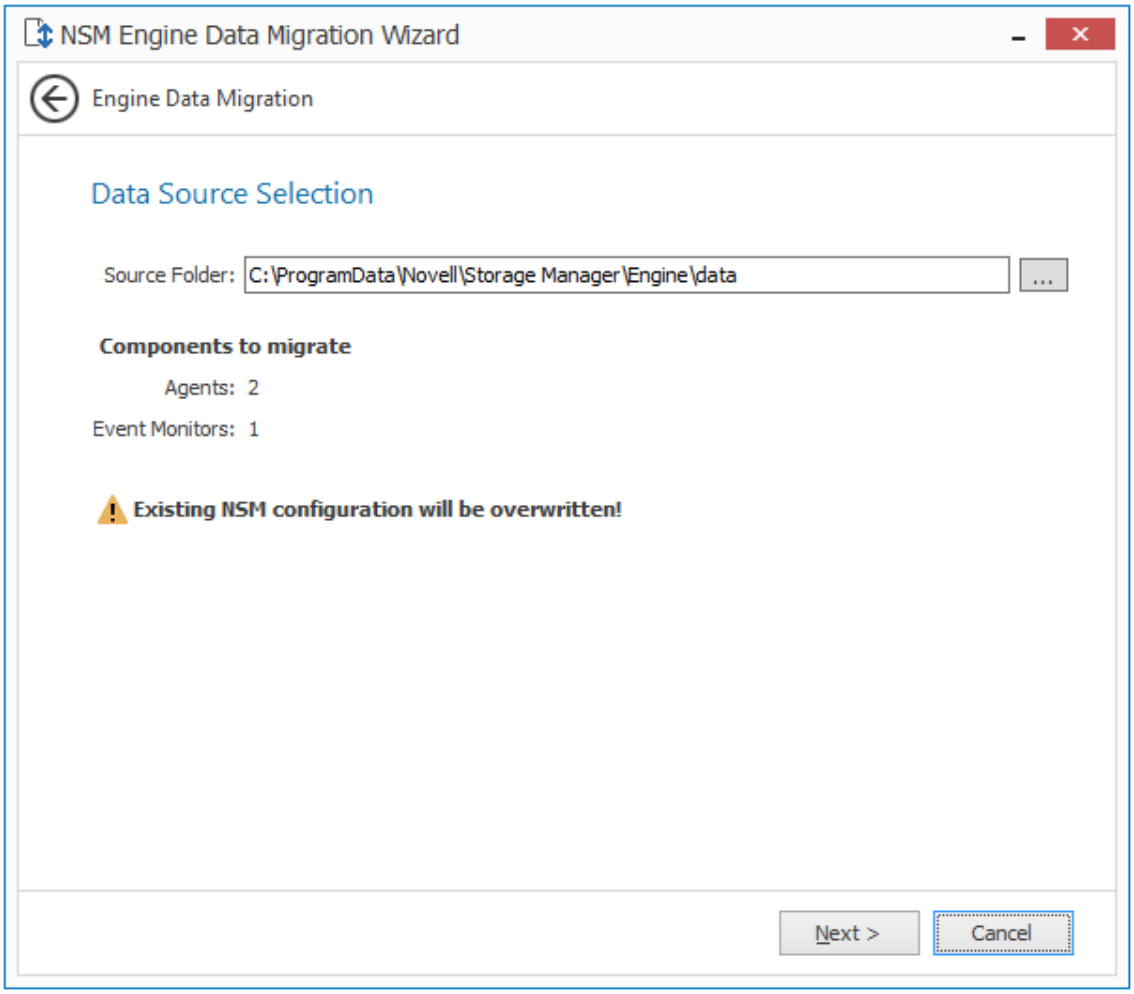
Migrated Engine data includes the list of authorized Agents, the authorized Event Monitor, and the list of servers hosting Agents that are serving as Proxy Agents.

1 From the Configuration Dashboard, click **Migrate Engine Data.**

2 When prompted to stop the Engine, click **Yes**.



3 Read the summary of what is going to be migrated and click **Next**.



If the Storage Manager data folder was installed using the default installation path, the path is displayed.

4. (Conditional) If the path to the data folder is not displayed, use the browse button to locate it.
5. Click **Next**.
6. When notified that the migration has completed, click **Finish**.
7. Click **Start Engine**.
8. Proceed with Section 4.11, “Installing NSMAdmin,” on page 55.

4.11 Installing NSMAdmin

NSMAdmin is the administrative interface for Novell Storage Manager. It can be installed on:

- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2012 R2, 2012, 2008 R2, or 2008

IMPORTANT: Storage Manager 4.x introduces new database requirements for NSMAdmin. For details and requirements, see Admin Client Database User Setup in the *File Dynamics 6.1 Administration Guide*.

1. On the Windows server or workstation where you will run NSMAdmin, copy to a directory the `NSM-AD_4_1.iso`.
2. Mount the `NSM-AD_4_1.iso` file.
3. At the root of the `NSM-AD_4_1.iso` image, double-click the `Windows` folder.
4. Double-click `NSMAdmin-AD-Installer-4.1-xxxx.exe`.
5. When you are asked if you want to run this file, click **Run**.
6. Agree to the licensing terms and conditions and click **Install**.
7. When notified that the setup was successful, click **Run Admin Client**.

   The NSMAdmin 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.

   The default setting is 3009.
10. Specify the username and password.

    The user must be a member of the nsmadmins group to be able to log in.
11. Click **Login**.

    If you are unable to log in, your proxy settings might be preventing you from doing so. Until you enter a proxy exception in your proxy settings, you can click **Proxy and Logging Options**, select **Do not use a Proxy**, then click **Login**.
12. Proceed with Section 4.12, “Review Migrated Policies,” on page 57.

4.12 Review Migrated Policies

While in NSMAdmin, you should verify that your policies migrated properly and that the settings are accurate.

1. In NSMAdmin, click the **Main** tab.
2. Click **Policy Management**.
3. Verify that all of the policies from Novell Storage Manager 3.1.1 for Active Directory are listed.
4. Verify the settings in the policies to make sure that they are accurate.

4.13 Upgrading to File Dynamics 6.1

Now that you have upgraded to Storage Manager 4.0, you can upgrade to File Dynamics 6.1. For procedures, see Chapter 5, “Upgrading from Storage Manager 4.1, 5.*x, or File Dynamics 6.0 to File Dynamics 6.1,” on page 59*.

5 Upgrading from Storage Manager 4.1, 5.*x*, or File Dynamics 6.0 to File Dynamics 6.1

5.1 Upgrading from Storage Manager 4.1 or 5.*x*

Upgrading from Storage Manager for Active Directory 4.1 or 5.x to File Dynamics 6.1 generally follows the same procedures as those for a new installation. You will need to update the license, configure the database, configure the Engine, and install the Epoch File Viewer.

For procedures, see Chapter 6, “Installing File Dynamics 6.1,” on page 61.

NOTE: It is not necessary to upgrade the Event Monitor following the upgrade, although you might want to do so to have the latest version. You must upgrade the existing Agents, which are now referred to as “File System Agents.”

5.2 Upgrading from File Dynamics 6.0

Upgrading from File Dynamics 6.0 to 6.1 involves some required upgrades to components, along with some optional component upgrades.

5.2.1 Required Component Upgrades

- Admin Client
- Engine
  - Configure the database to support Security Notify policies
  - Configure the Engine to repair the firewall rule
- Phoenix Agents

  This is necessary to support Security Notify policies and so that you can set ownership on files via Workload.

5.2.2 Optional Component Upgrades

- Event Monitor
- File System Agents
  - Configure the FS Agents to repair the firewall rule
- Data Owner Client

6 Installing File Dynamics 6.1

This section provides procedures for installing and configuring the Engine, database, Epoch File Viewer, Event Monitor, Agents, and Admin Client. For information on how these components work in a File Dynamics deployment, see The Directory in the *File Dynamics 6.1 Administration Guide*.

You should follow these procedures only after you have performed the prerequisite tasks in Chapter 1, “Prerequisites,” on page 7, obtained a File Dynamics 6 product license as indicated in Chapter 2, “Licensing the Product,” on page 13, and installed an SQL Server instance as specified in Chapter 3, “Installing and Configuring an SQL Server Instance,” on page 17.

- Section 6.1, “Domain Administrator Permissions,” on page 61
- Section 6.2, “Accessing the Product Contents,” on page 61
- Section 6.3, “Installing the Engine,” on page 62
- Section 6.4, “Installing the License,” on page 63
- Section 6.5, “Configuring the Database,” on page 64
- Section 6.6, “Configuring the Engine,” on page 67
- Section 6.7, “Configure the Epoch File Viewer,” on page 75
- Section 6.8, “Setting Rights and Privileges on Managed Storage,” on page 85
- Section 6.9, “Installing and Configuring the Event Monitor,” on page 89
- Section 6.10, “Installing and Configuring the File System Agents,” on page 94
- Section 6.11, “Installing and Configuring the Phoenix Agents,” on page 100
- Section 6.12, “Installing the Admin Client,” on page 104
- Section 6.13, “Authorizing the Event Monitor,” on page 105
- Section 6.14, “Authorizing the Agents,” on page 105
- Section 6.15, “Installing the Data Owner Client,” on page 106
- Section 6.16, “Installing Other Components,” on page 107
- Section 6.17, “Administering File Dynamics,” on page 107

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

6.1 Domain Administrator Permissions

In order to successfully install the Engine, Event Monitor, Agents, and the Admin Client, you must be logged in to the computer as a domain administrator. If you are not, the permissions are not sufficient.

6.2 Accessing the Product Contents

1. On the Windows server that will host the Engine, copy to a directory the `FileDynamics-6_1.iso` file that was made available to you following your purchase of Micro Focus File Dynamics 6.1.
2. Mount the `FileDynamics-6_1.iso` file.

3 Note the location of the mounted ISO.

   This is the installation source you will use to install File Dynamics components.

6.3 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 2016 (Member Server)
- Microsoft Windows Server 2012 R2 (Member Server)
- Microsoft Windows Server 2012 (Member Server)
- Microsoft Windows Server 2008 R2 (Member Server)
- At least 4 GB RAM
- For quota management, Microsoft File System Resource Manager (FSRM) must be installed; see Section 1.2, “File Server Resource Manager,” on page 8.
- Forest functional level of Windows Server 2003 or later

Other notable information about the Engine:

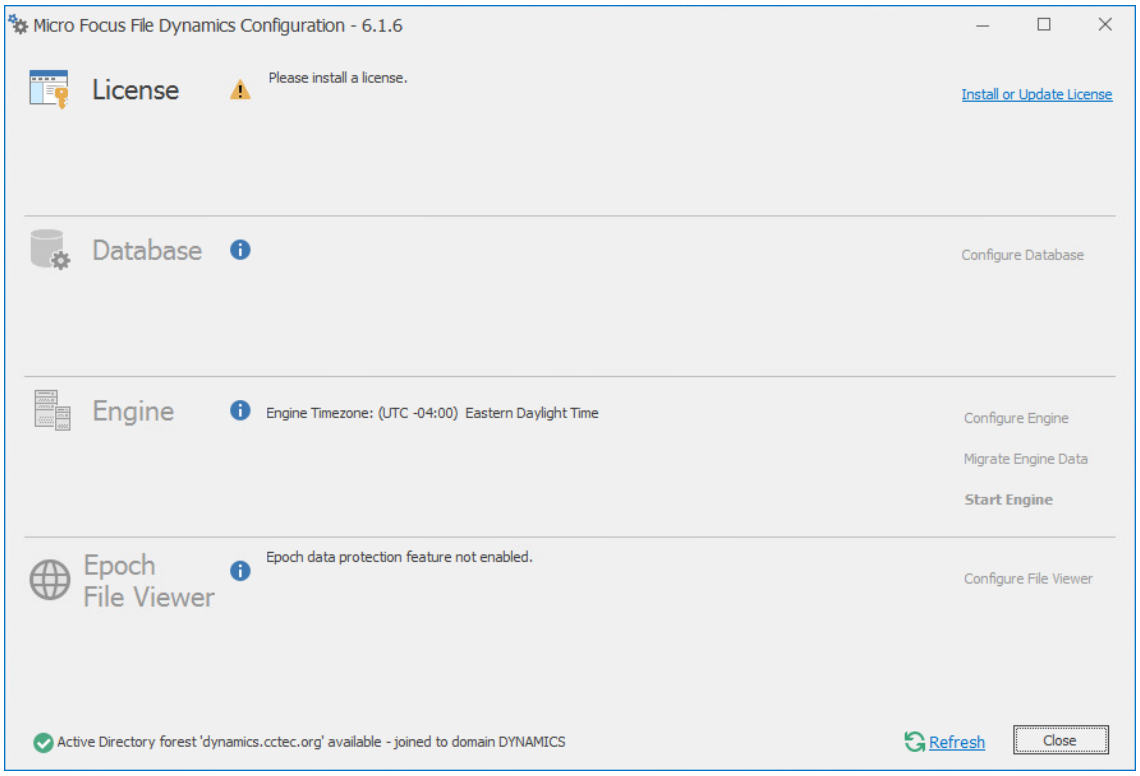
- The Engine runs as a native NT service that is configured to start by using the Local System account
- The default Engine port is 3009
- The firewall inbound rule is added during the Engine installation

1 At the root of the `FileDynamics-6_1.iso` image, double-click `FileDynamics-Engine-6.1-xx.exe`.
2 When you are asked if you want to run this file, click **Run**.
3 Agree to the licensing terms and conditions and click **Install**.

   The File Dynamics File Viewer Setup Wizard is launched.
4 Read the overview on the initial page of the wizard and click **Next**.
5 For the Web Application and the Config Utilities, accept the installation paths or indicate a new path by using the **Browse** button.
6 Click **Install**.
7 Click **Finish** to close the wizard.

   The Install Successful message indicates that the Web Application and Config Utilities were installed successfully.
8 Click **Run Configuration Utility**.

The Configuration Utility is launched.

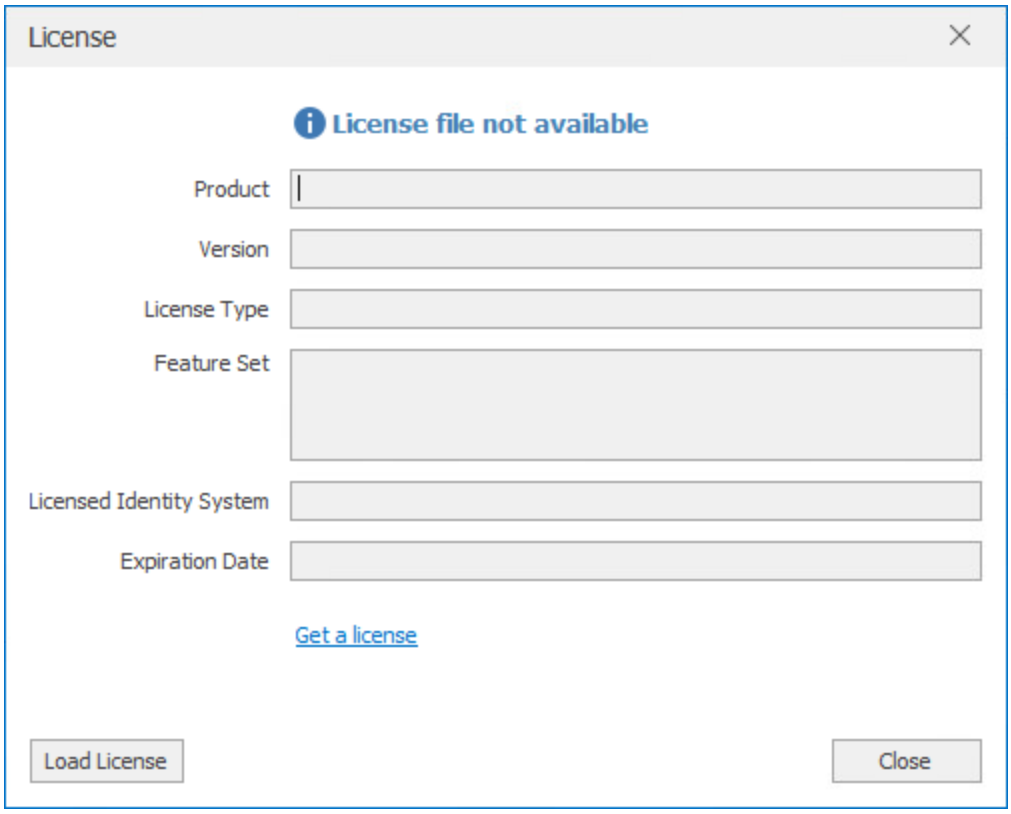


6.4 Installing the License

1 In the Configuration Utility, click **Install or Update License**.

The License dialog box appears.

If no license is found, the license properties will be empty.



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

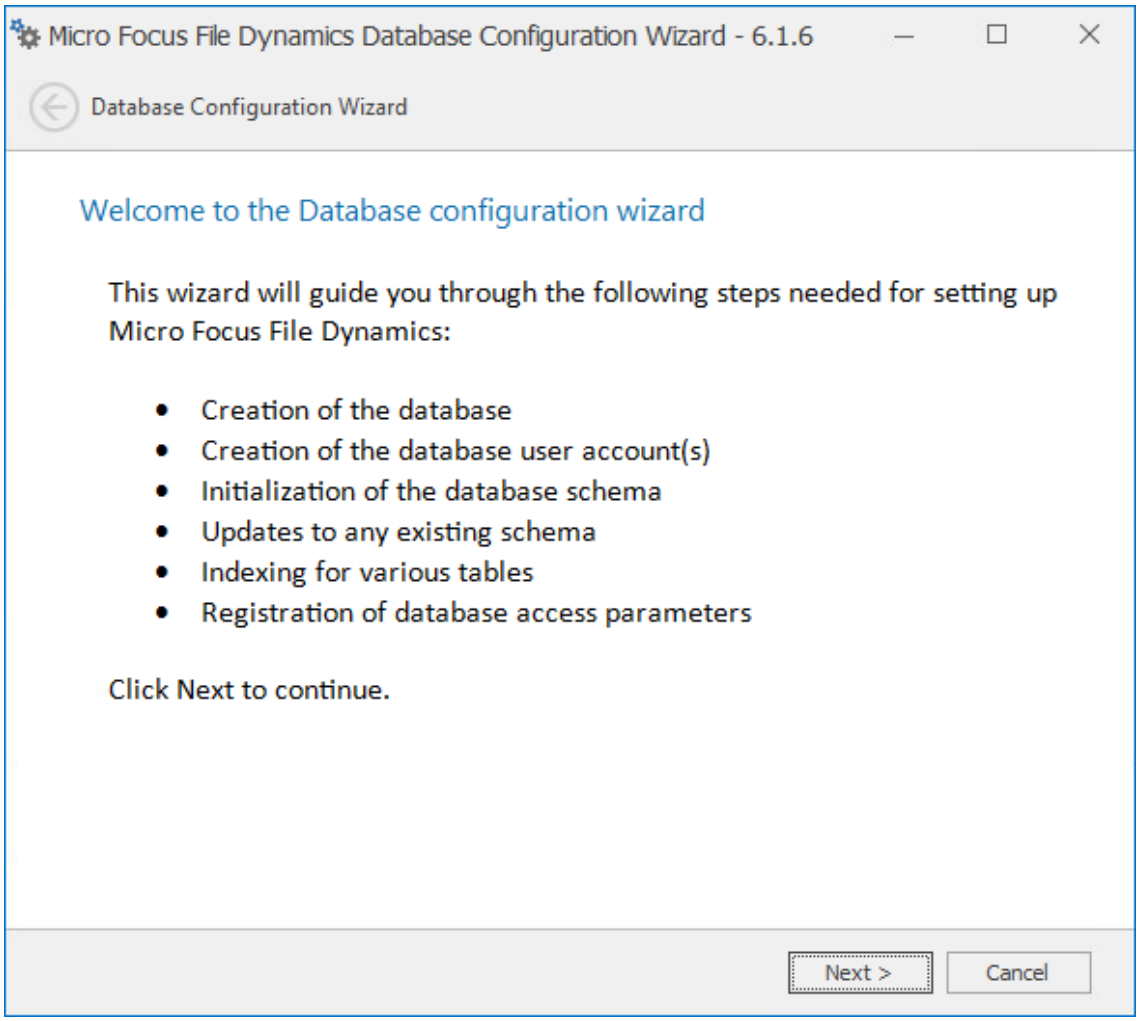
3 When the confirmation prompt appears, click **Yes**.

4 Examine the license properties to ensure that the license is valid.

5 Click **Close**.

6.5 Configuring the Database

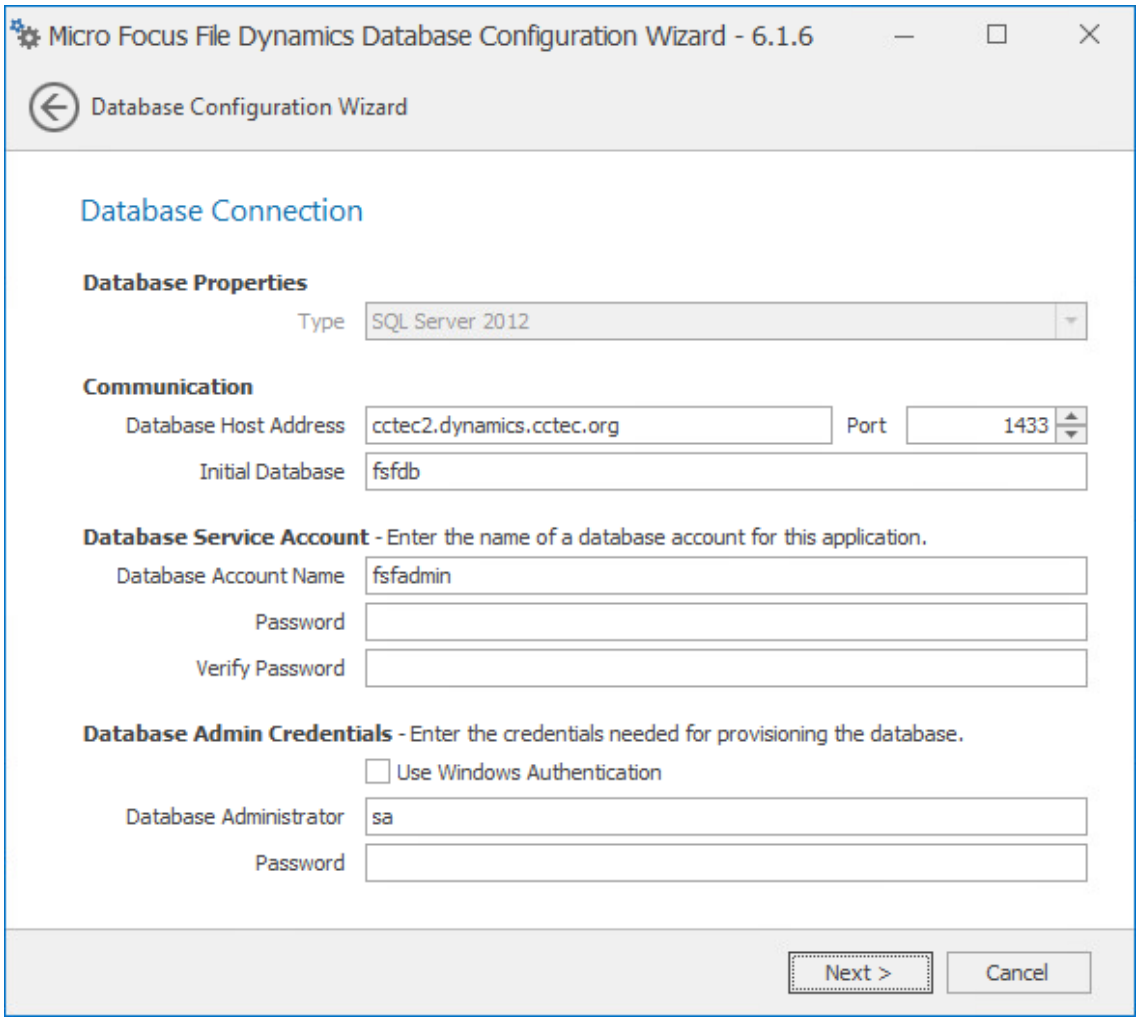
1 In the Configuration Utility, click **Configure Database**.



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

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

The following page appears:



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

Database Properties: Displays information on the database.

Type: Displays the minimum supported version of the database, which is SQL Server 2012.

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: The default SQL Server port setting is 1433. If there is a port conflict, you can change it.

Initial Database: The default name of the Storage Manager database.

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.

Database Account Name: By default, the database account is fsfadmin, which you can change in this field.

Password: Specify a password for the service account to connect to the database.

Verify Password: Specify the password again in this field.

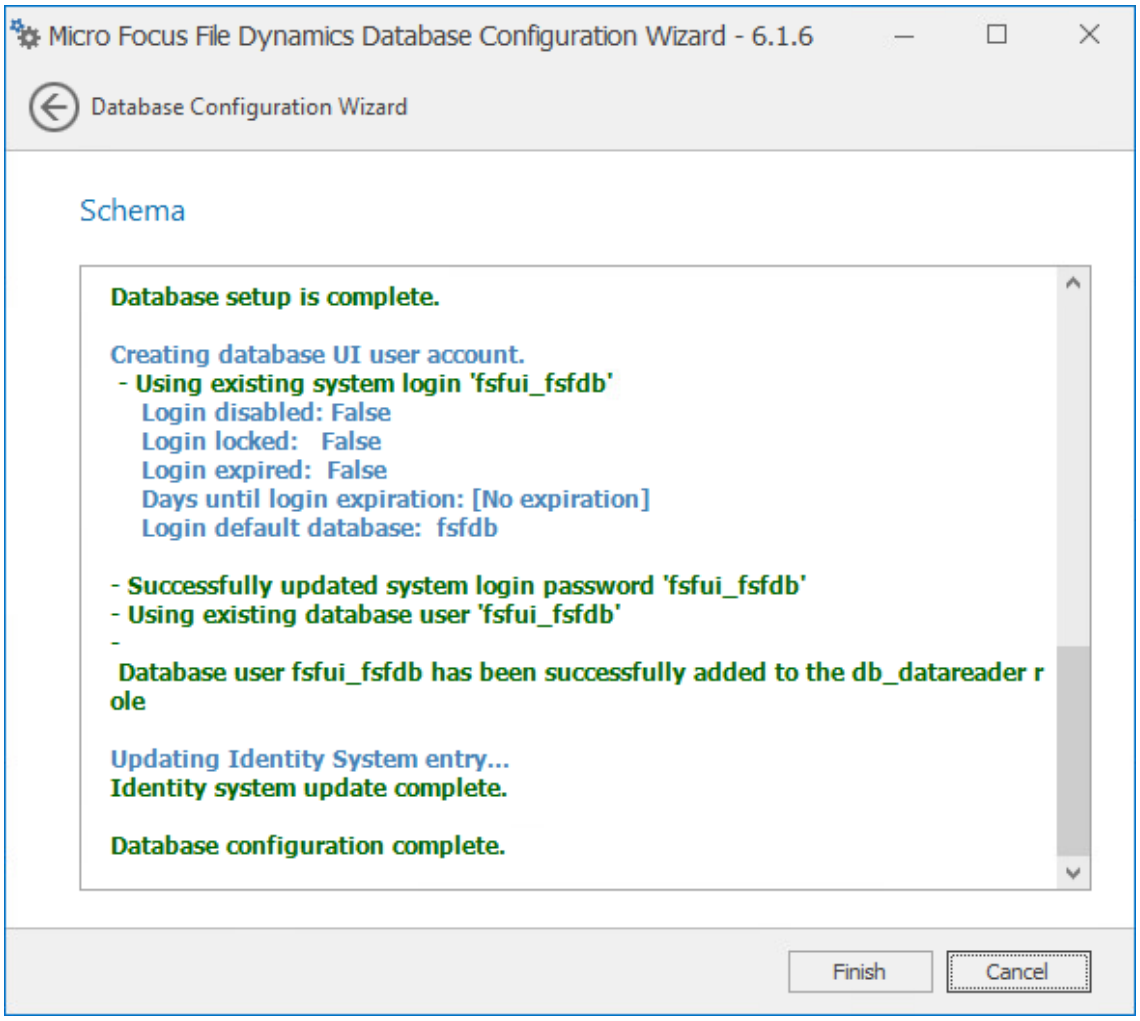
Database Admin Credentials: Use this region to establish the database administrator name and credentials.

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 an SQL Server database administrator. Selecting this check box disables the Database Administrator and Password fields.

Database Administrator: Specify the SQL Server administrator name.

Password: Specify the SQL Server administrator password.

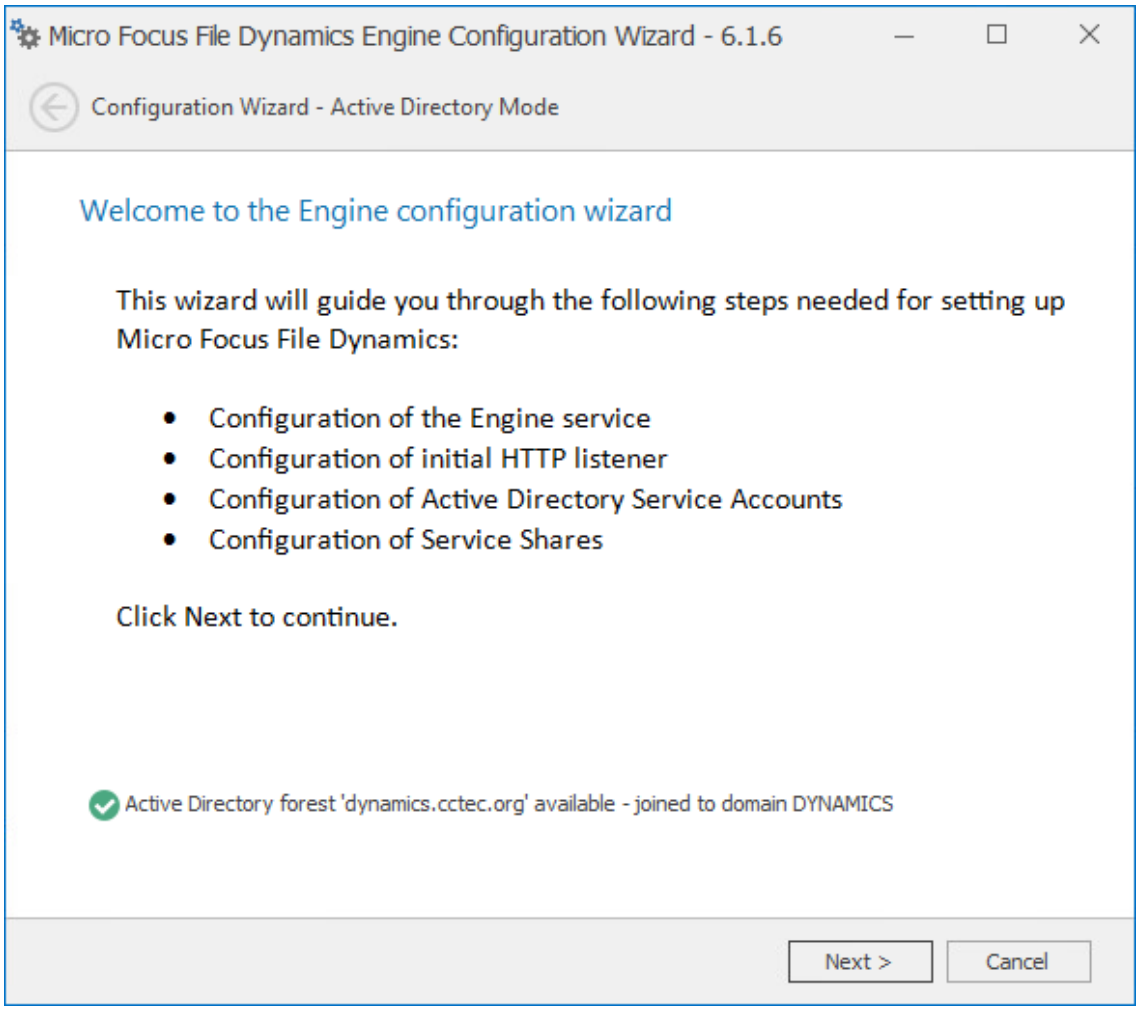
3 Complete the fields and click **Next**.



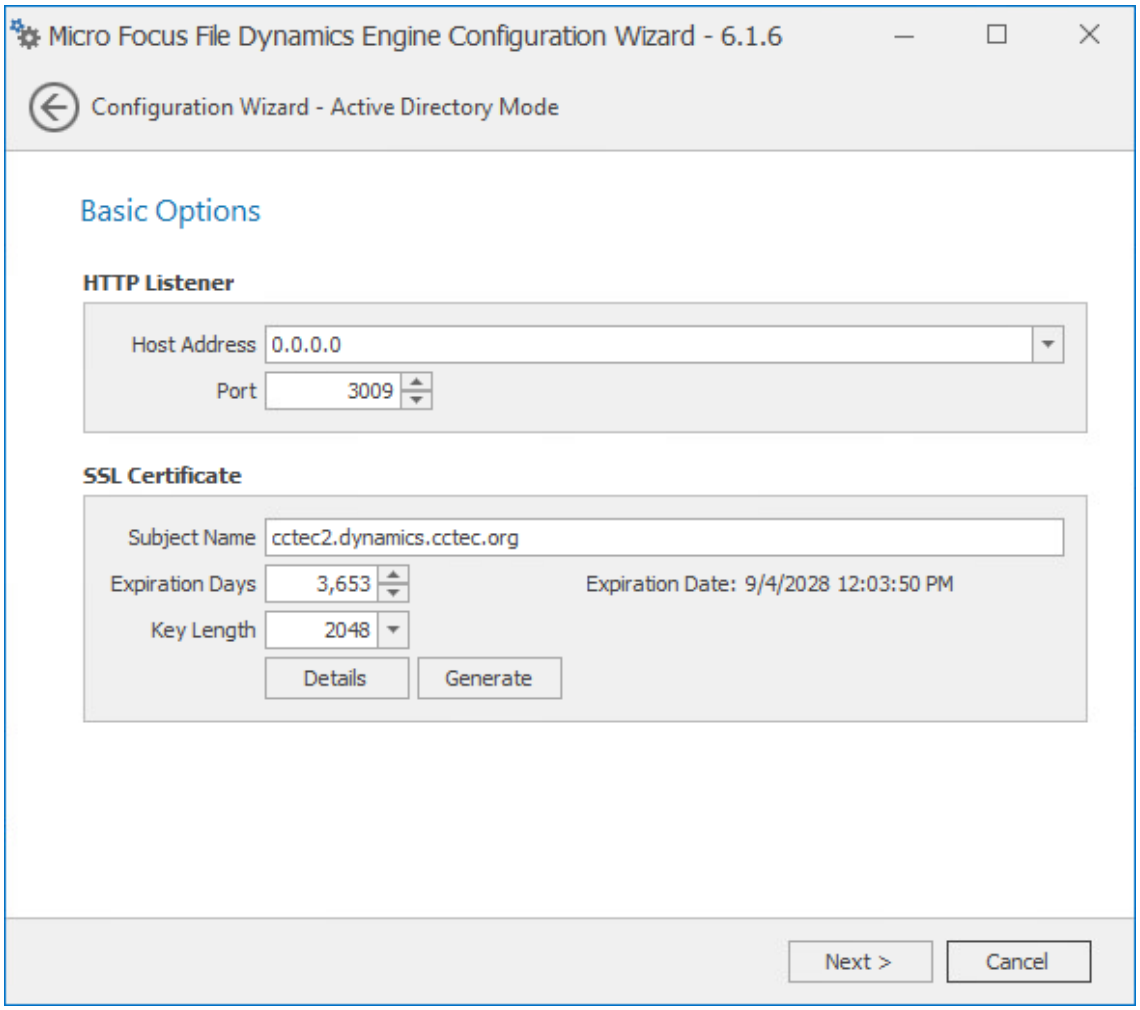
4 Review the configuration log and click **Finish**.

6.6 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**.



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 3009.

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.

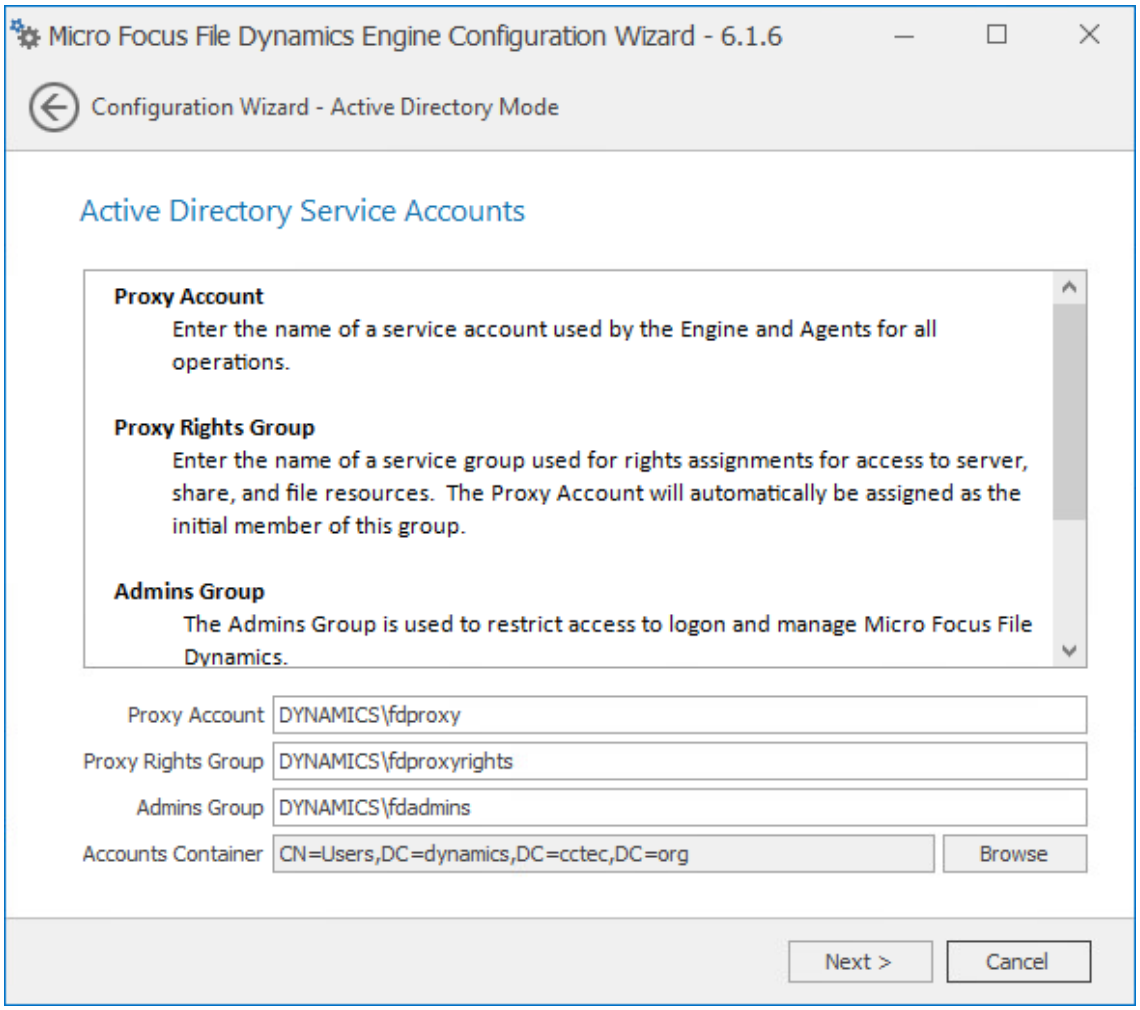
Expiration Days: The life span of the security certificate, which is set at 10 years by default.

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.

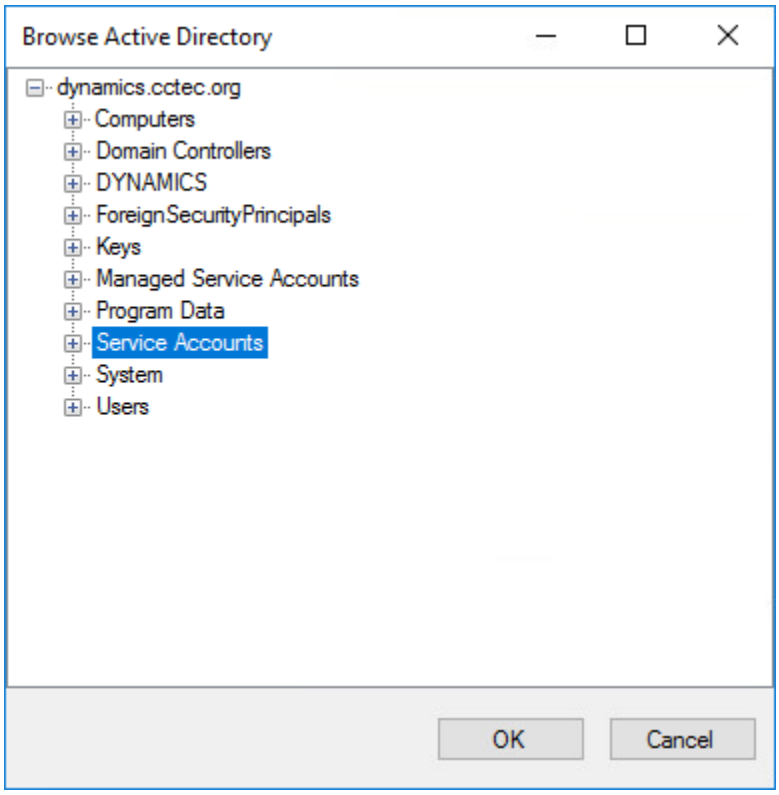
3 Edit any needed parameters settings and click **Next**.



This page lets you establish a name for the Proxy Account, Proxy Rights, and Admins Groups.

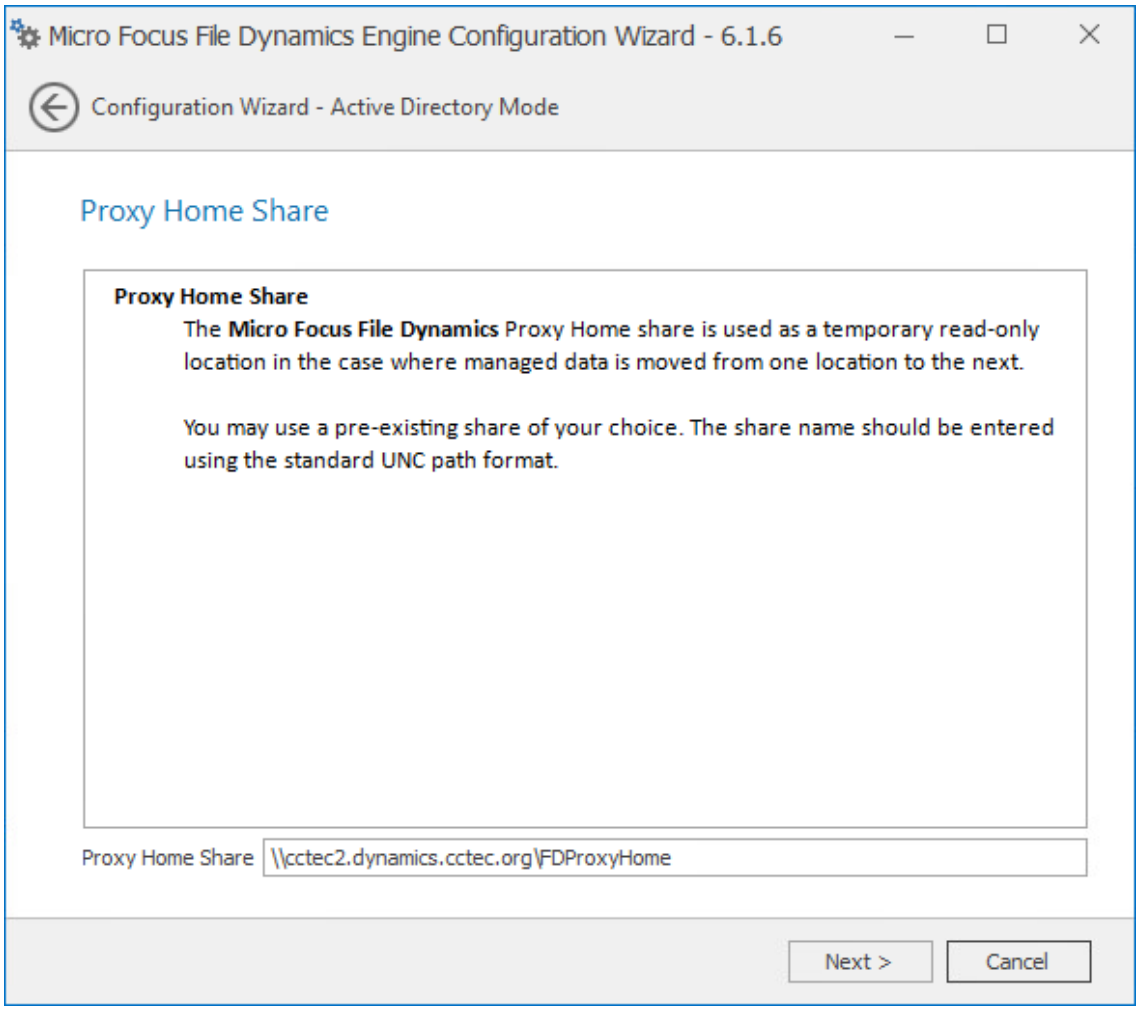
File Dynamics uses proxy accounts so that it can perform tasks necessary for storage management.

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.



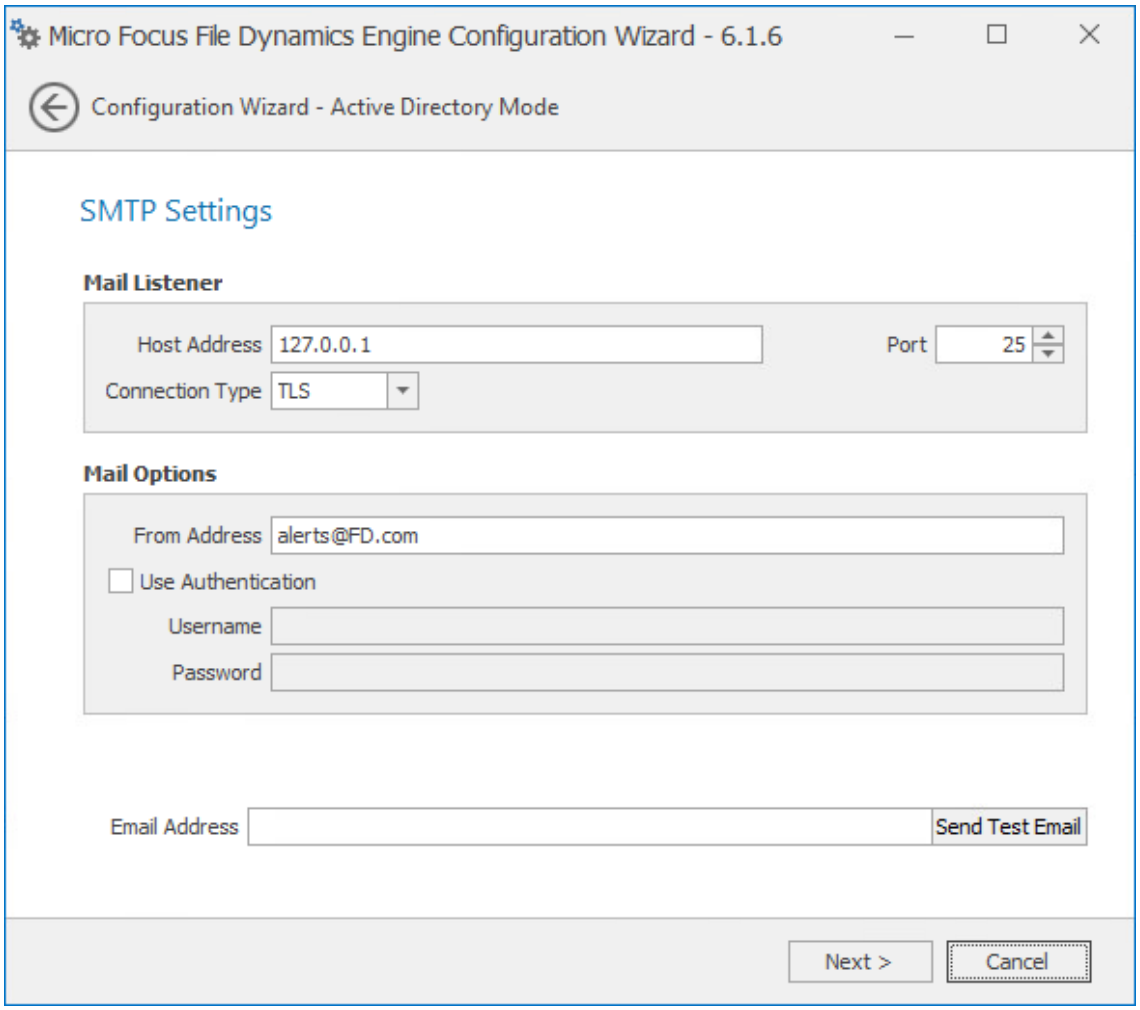
In this example, the proxy objects are being created in the `Service Accounts` container.

4 Establish your proxy account settings and click **Next**.



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.

5 Click **Next**.



Email alerts are available for Workload related jobs submitted via the Data Owner Client. For example, an administrator specified in a Workload policy, could be alerted when files have been relocated as a result of a Workload policy.

Completing fields in this page is optional.

Mail Listener: These fields specify information pertaining to the mail server that is sending alerts.

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

Port: Specify the port number for the mail server.

Connection Type: From the drown-down menu, select the encryption type used by your mail server.

Mail Options: These fields specify additional mail information.

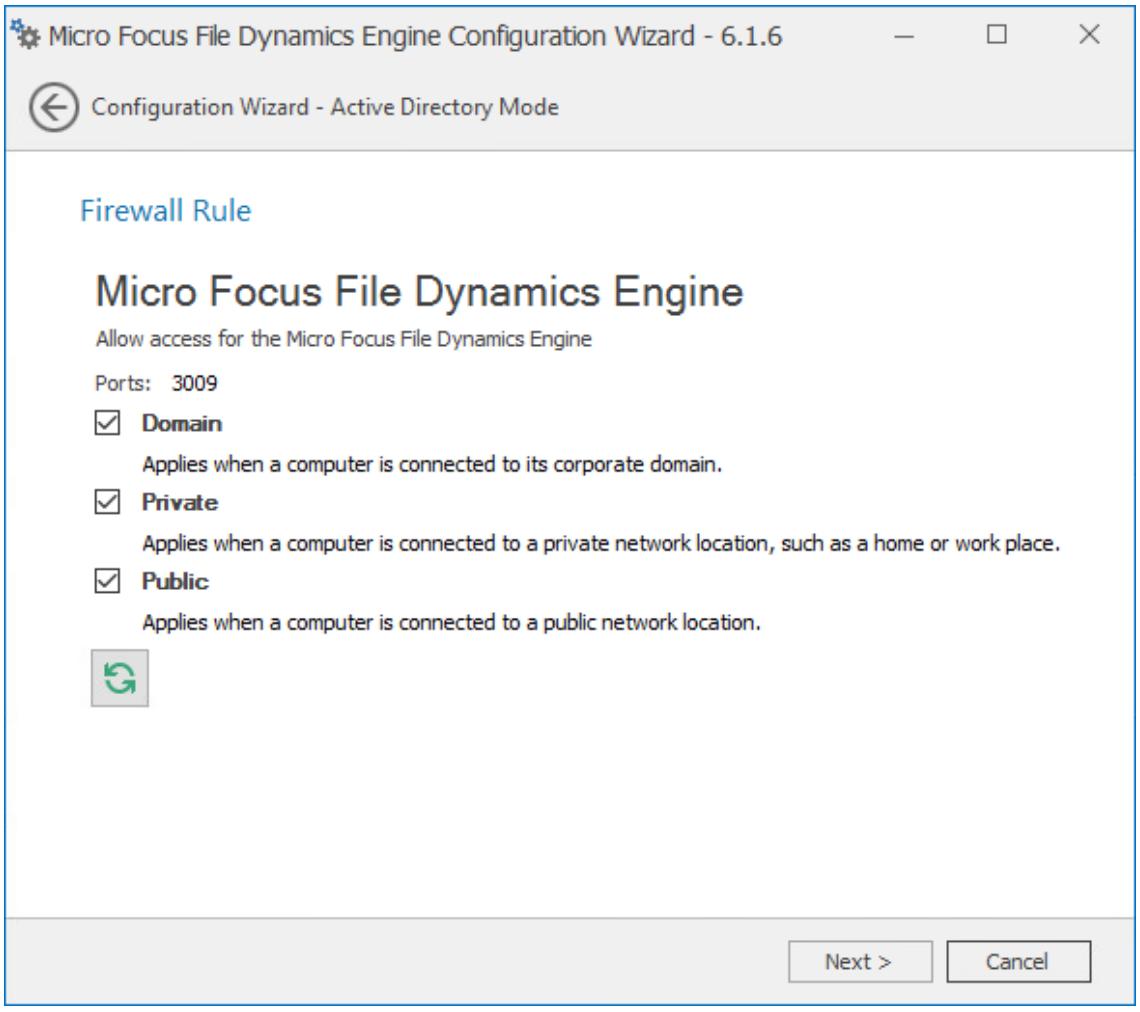
From Address: This field specifies the default address where the alerts come from.

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.

Email Address: Specify an email address for a test alert.

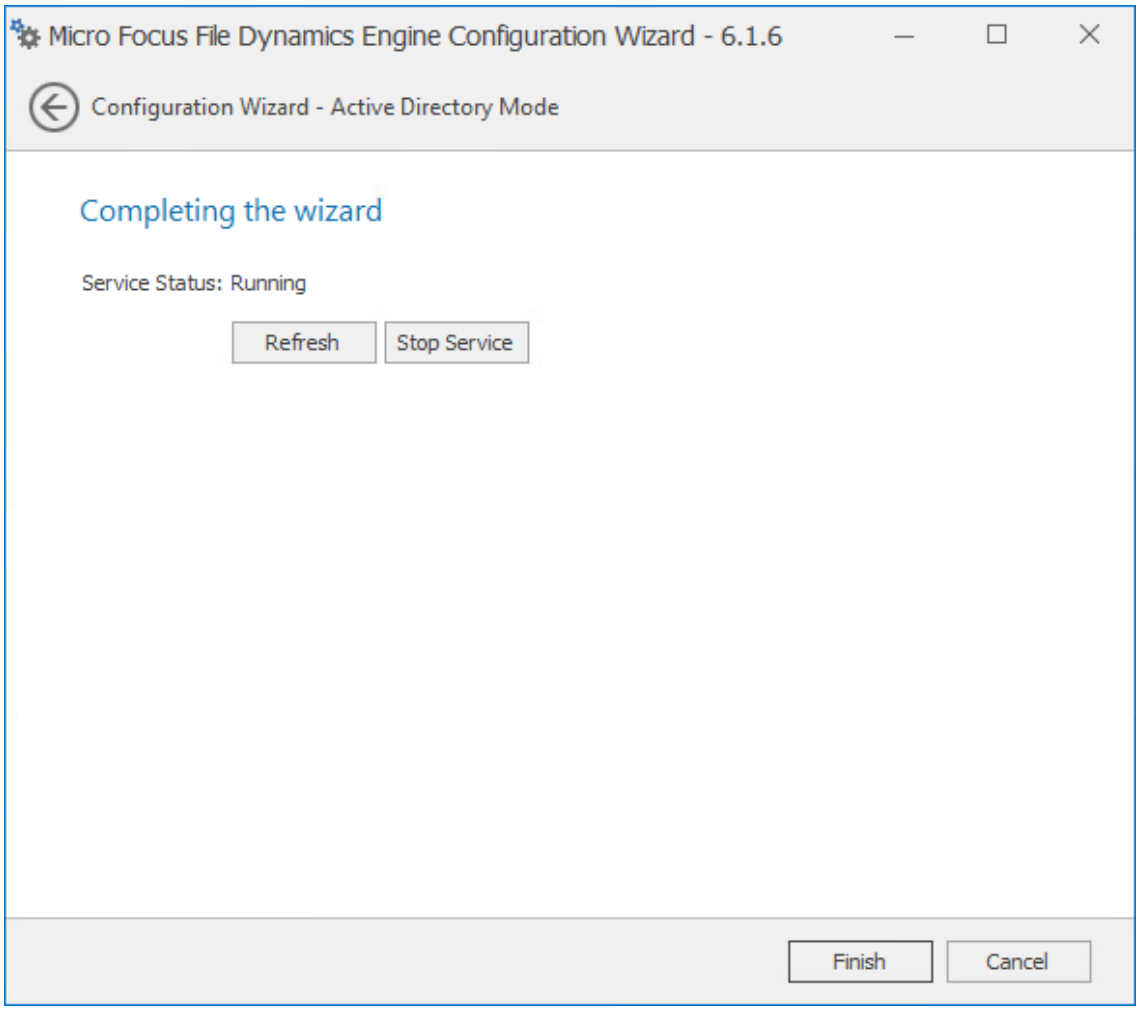
Send Test Email: Click this button to send a test email to the recipient specified in the **Email Address** field.

6 Establish your SMTP settings and click **Next**.



This page displays the current Windows firewall rules that pertain to the Engine. You can enable or disable these profiles as needed.

7 Click **Next**.



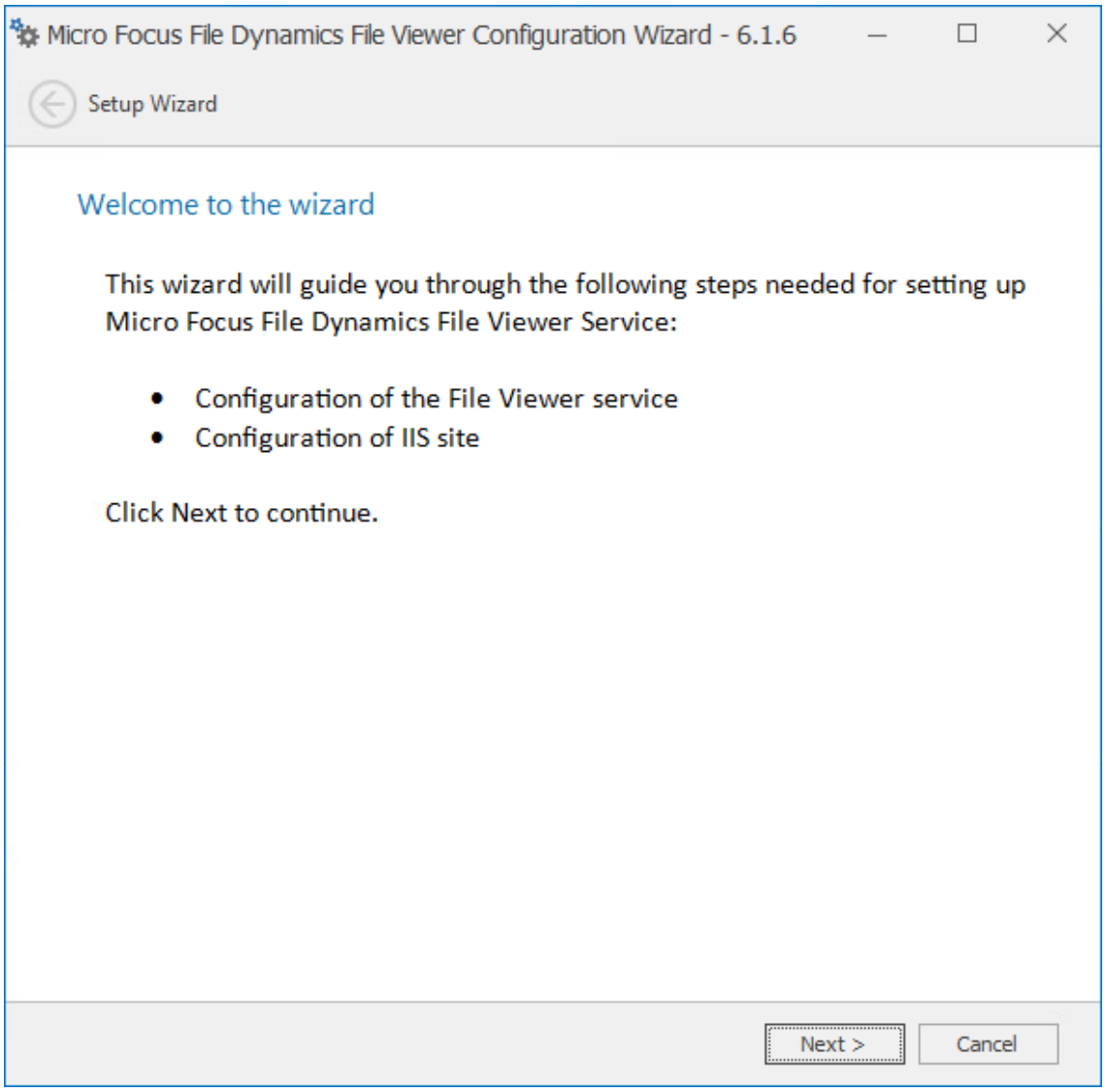
8 Click **Finish**.

6.7 Configure the Epoch File Viewer

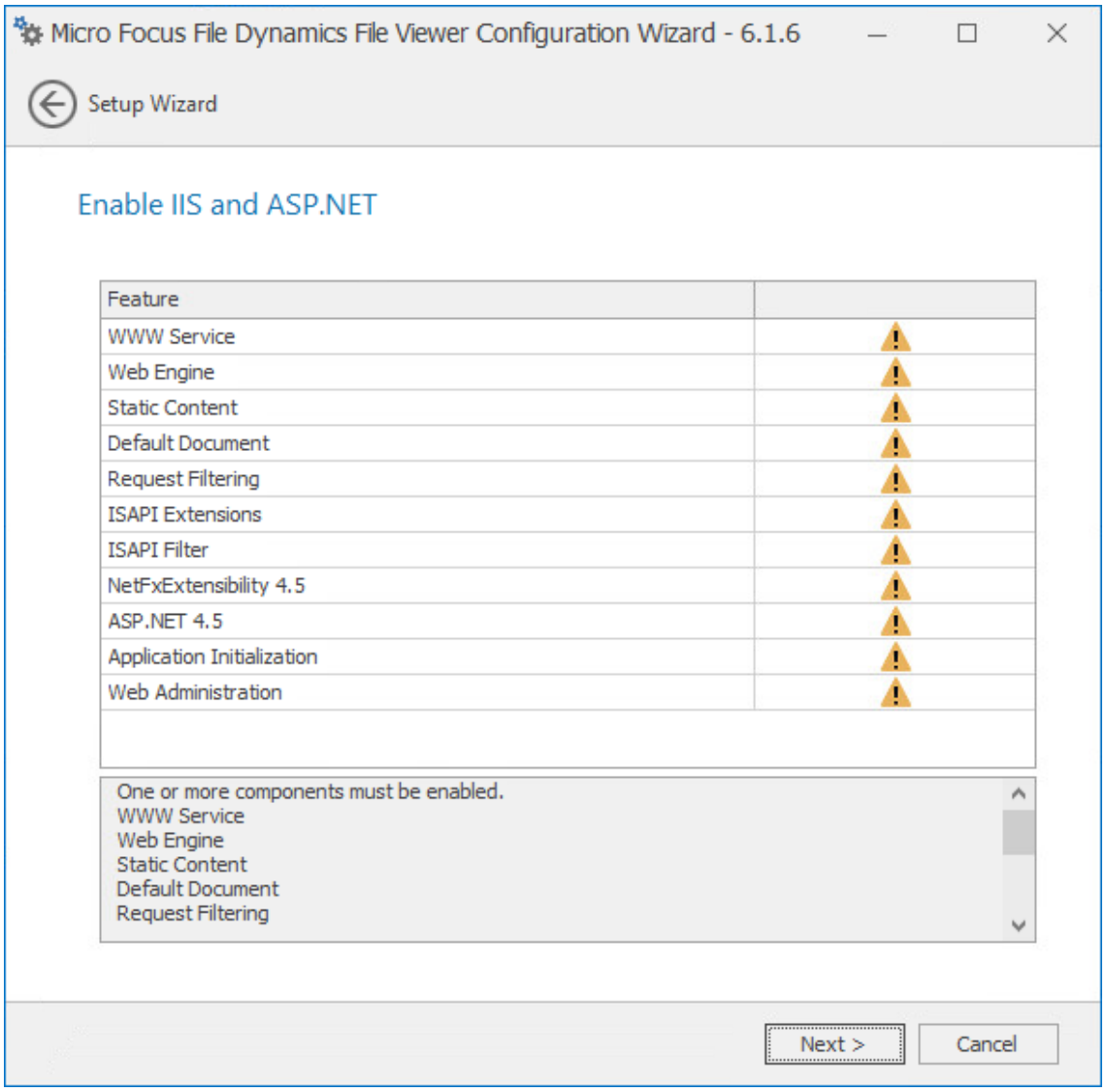
The Epoch File Viewer is what the Data Owner Client (needed for Epoch Data Protection) uses to see a rendering of a file before it is recovered. This procedure sets up Microsoft IIS and ASP.NET.

1 Click **Configure File Viewer**.

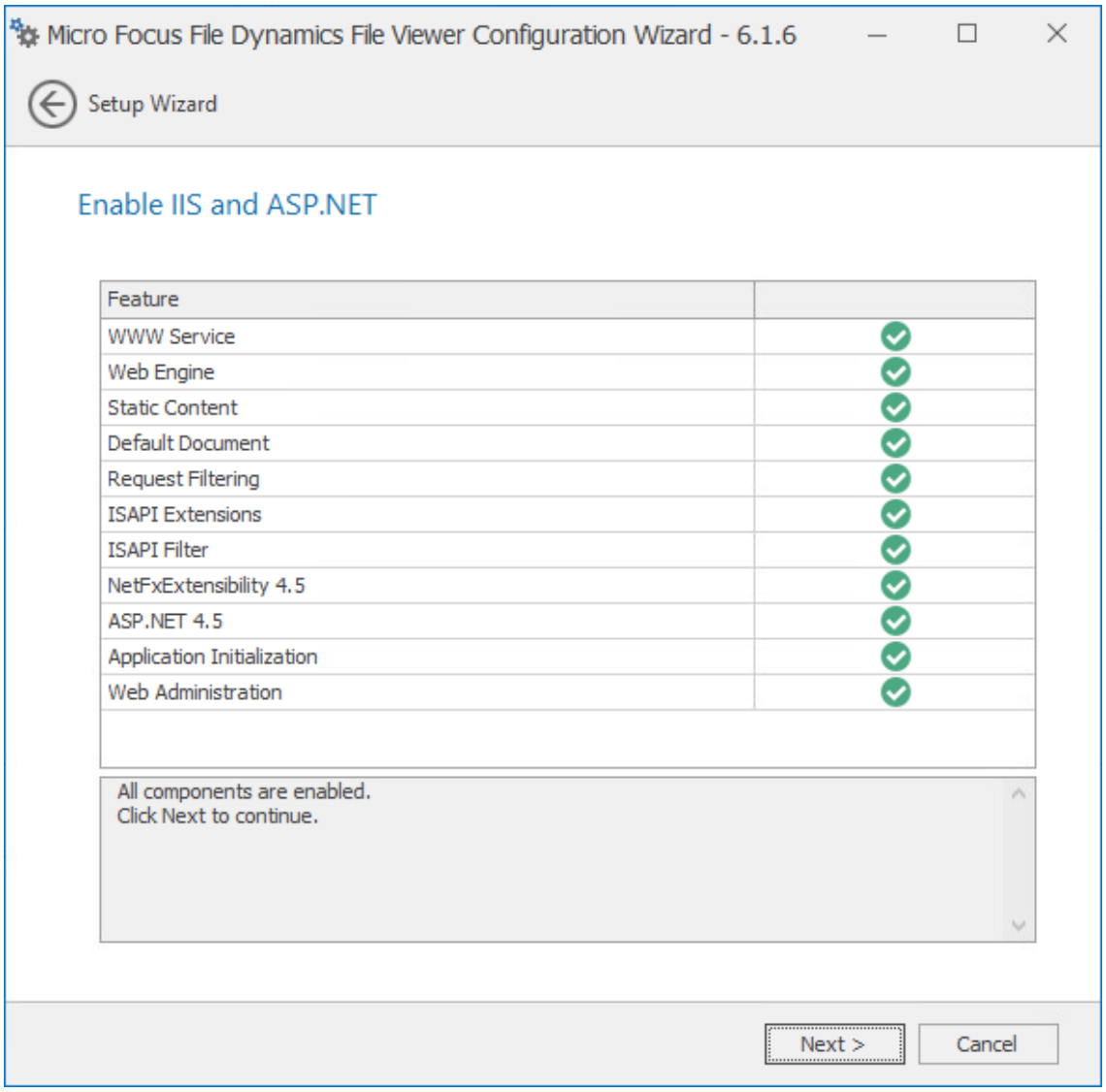
2 When the confirmation prompt to stop the Engine appears, click **Yes**.



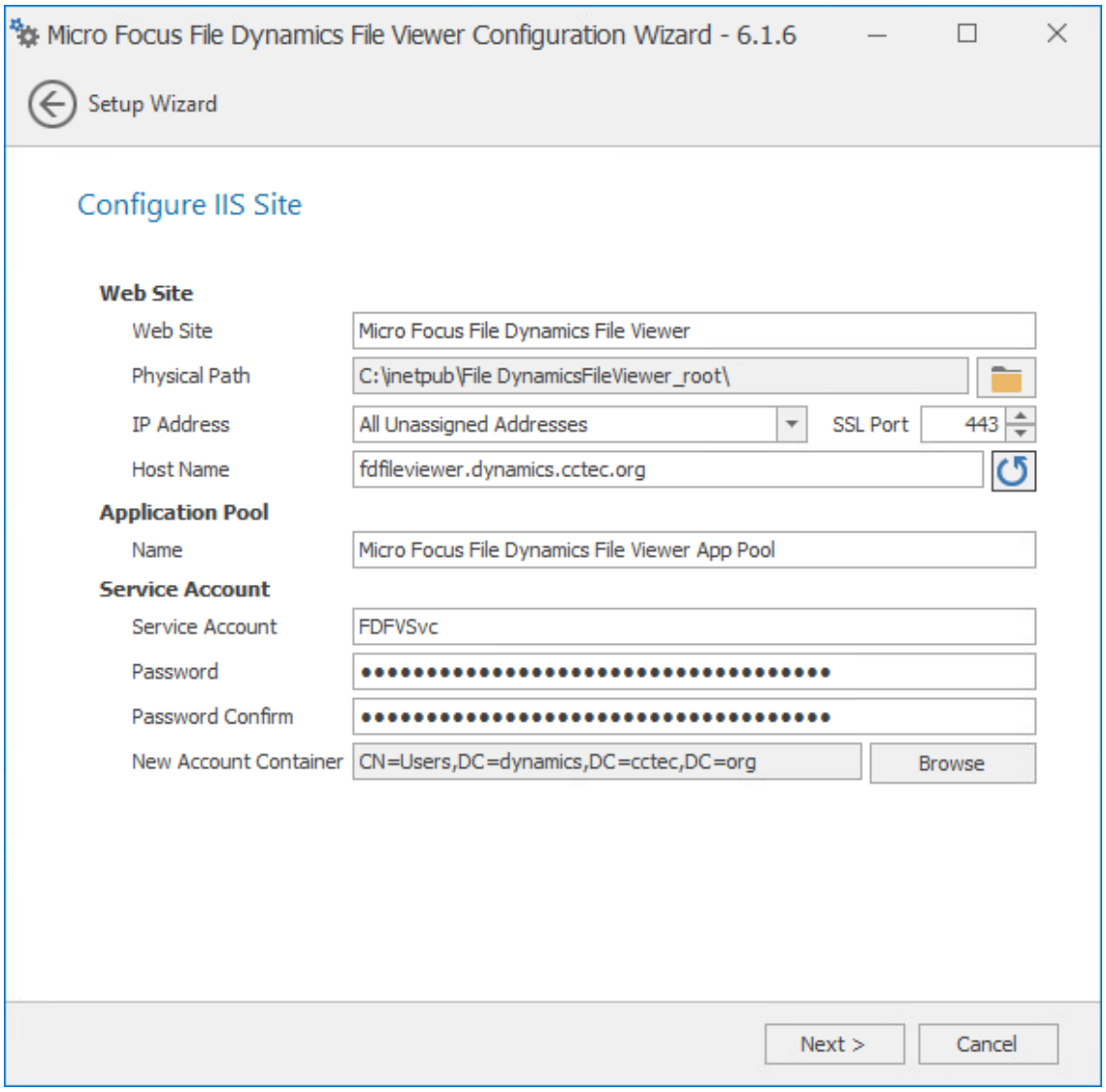
3 From the wizard page, read the overview of what will be configured and click **Next**.


Micro Focus File Dynamics File Viewer Configuration Wizard - 6.1.6
Setup Wizard
Enable IIS and ASP.NET
Feature
WWW Service
Web Engine
Static Content
Default Document
Request Filtering
ISAPI Extensions
ISAPI Filter
NetFxExtensibility 4.5
ASP.NET 4.5
Application Initialization
Web Administration
One or more components must be enabled.
WWW Service
Web Engine
Static Content
Default Document
Request Filtering
Next >
Cancel

4 Click **Next**.


Micro Focus File Dynamics File Viewer Configuration Wizard - 6.1.6
Setup Wizard
Enable IIS and ASP.NET
Feature
WWW Service
Web Engine
Static Content
Default Document
Request Filtering
ISAPI Extensions
ISAPI Filter
NetFxExtensibility 4.5
ASP.NET 4.5
Application Initialization
Web Administration
All components are enabled.
Click Next to continue.
Next >
Cancel

5 Click **Next**.



This page lets you review or edit settings applicable to the Microsoft IIS configuration. 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 website.

Web Site: The default name for the File Dynamics file viewer 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 during the installation of the Engine and is the location where files on the website are served up.

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 Chapter 1, "Prerequisites," on page 7 of this manual.

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 Dynamics Epoch File Viewer and that the resolved IP address or addresses are located on the host machine.

Application Pool: Settings pertaining to the File Dynamics 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: Authentication settings that the application pool will be using with Active Directory.

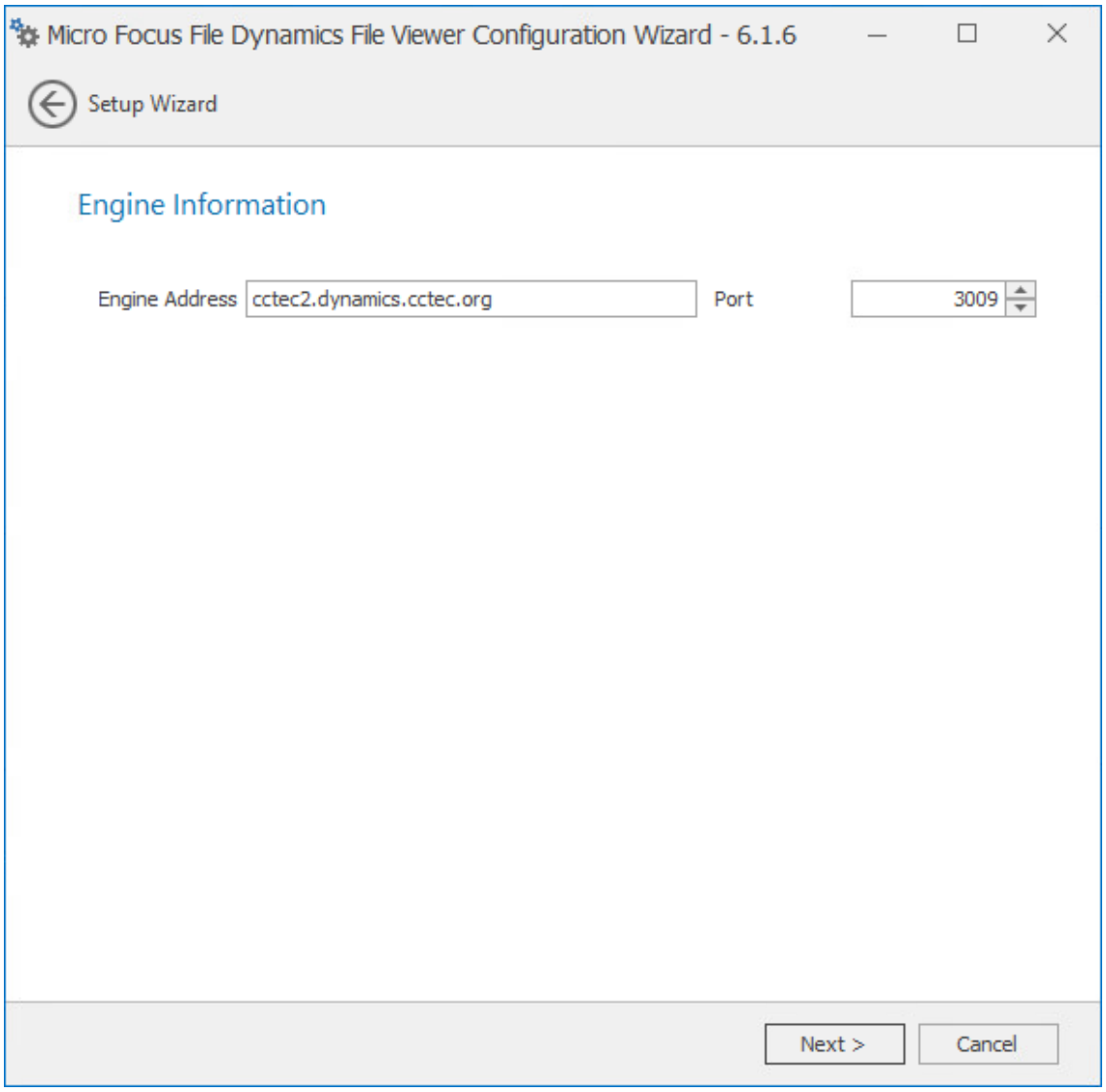
Service Account: The default name of the service account. If the default name does not conform to your organization's naming standards, you can edit it.

Password: A randomly-generated password for the service account. You do not need to know or remember this password.

Confirm Password: The randomly-generated password is duplicated in this field.

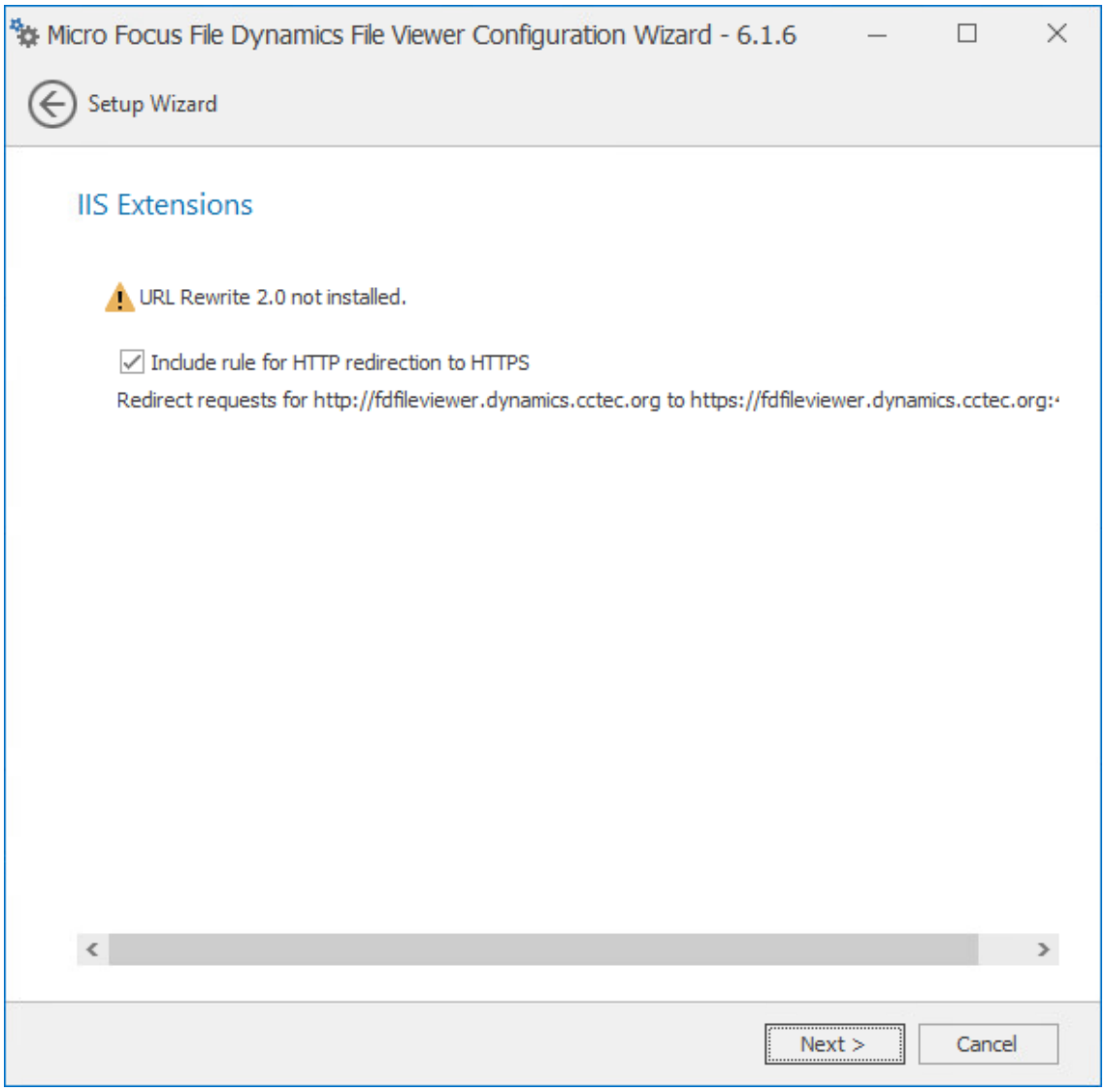
New Account Container: A default LDAP path is displayed where the service account will be created. If you do not have rights to the displayed container, you can use the **Browse** button to change the path.

6 Modify any settings you need to, then click **Next**.



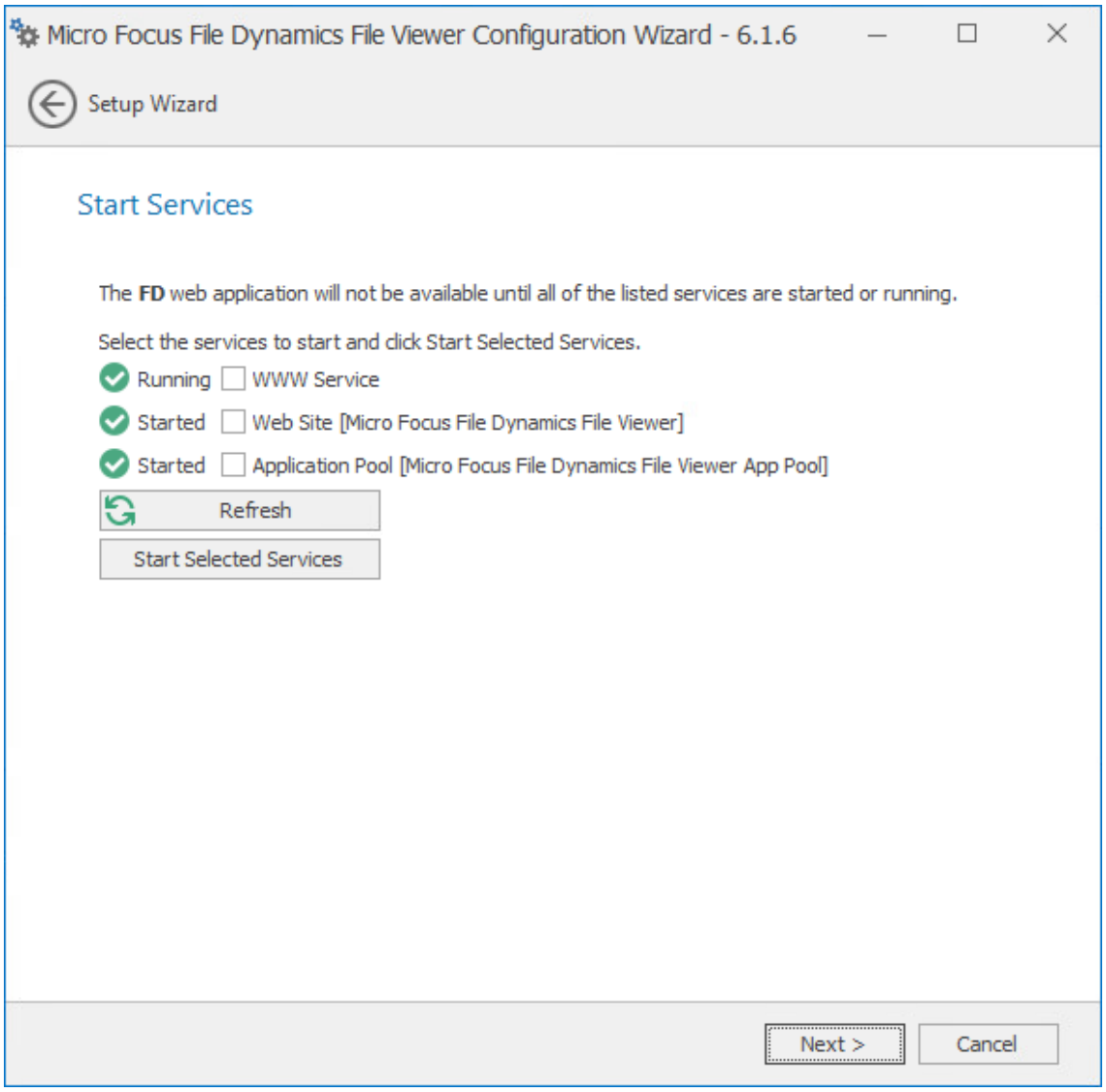
This page displays the Engine address and port number. The name be either in FQDN format or as an IP address.

7 Click **Next**.



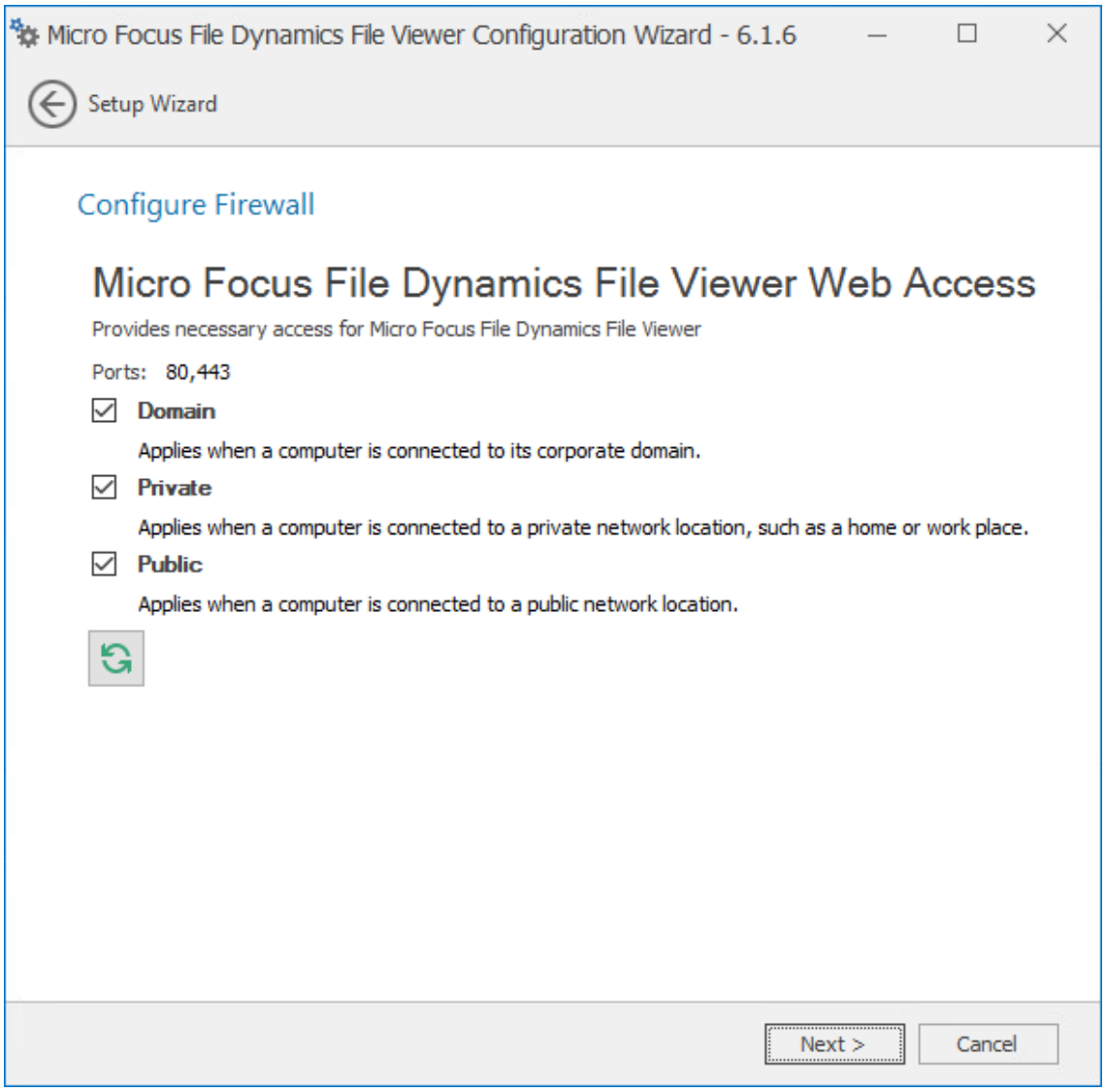
This page lets you install Microsoft IIS URL Rewrite Module 2.0, which will redirect the File Dynamics login page from an entered HTTP protocol, to HTTPS.

8 Click **Next**.



In most cases, all three listed services should be running. If a service is not running and you need to start one manually, you can do so.

9 Click **Next**.



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 Epoch File Viewer are now configured.

12 Click **Test File Viewer**.

13 Do one of the following:

- If you are notified that “It worked!”, the communication between the IIS Server and the Engine is working.
- If you are prompted for a security exception, accept it and follow the procedures for establishing `https://fdfileviewer.`*`domain`* as a trusted website.

6.8 Setting Rights and Privileges on 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.

6.8.1 Granting Rights

Every share to be managed by File Dynamics must have proper rights assigned to the fdproxyrights 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 fdproxyrights group for each share that File Dynamics will manage.

3 Do one of the following:

- If you are proxying storage on a member server, go to Section 6.8.2, “Granting Privileges on a Member Server,” on page 86.
- If you are proxying storage on a domain controller, go to Section 6.8.3, “Granting Privileges on a Domain Controller,” on page 87.

6.8.2 Granting Privileges on a Member Server

Every server that has storage managed by File Dynamics must have certain privileges granted to the fdproxyrights 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.

Be sure to log in as a domain administrator.

2 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**.

This brings up the Active Directory Users and Computers page.

3 In the left pane, select the container where the server is so that it is listed in the right pane.

4 In the right pane, right-click the server and select **Manage**.

This brings up the Computer Management page.

5 In the left pane, expand **Local Users and Groups**.

6 Select **Groups**.

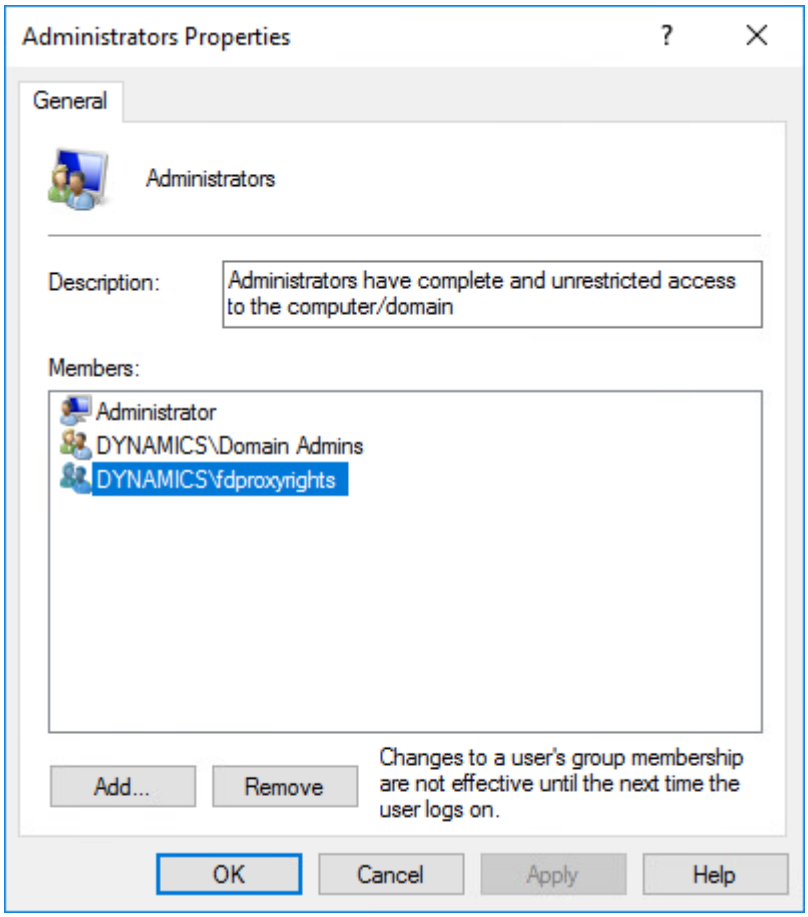
7 In the right pane, double-click **Administrators**.

This brings up the Administrators Properties dialog box.

8 Click **Add**.

This brings up the Select Users, Computers, or Groups dialog box.

9 In the **Enter the object names to select** field, type: *domain_name*\fdproxyrights.



10 Click **OK** to save the setting.

11 Proceed with Section 6.9, “Installing and Configuring the Event Monitor,” on page 89.

6.8.3 Granting Privileges on a Domain Controller

Every server that has storage managed by File Dynamics must have certain privileges granted to the fdproxyrights 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.

Be sure to log in as a domain administrator.

2 Launch Active Directory Users and Computers.

This brings up the Active Directory Users and Computers page.

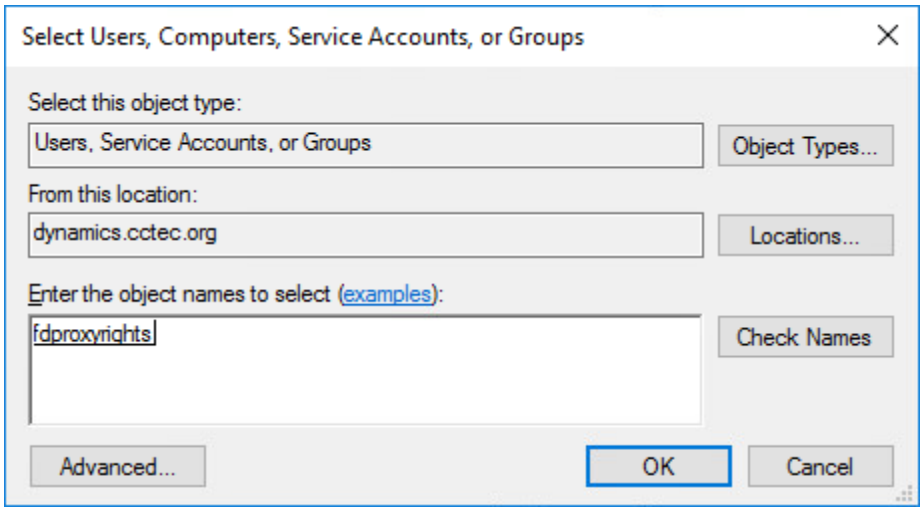
3 In the left pane, select **Builtin**.

4 In the right pane, double-click the **Administrators** group.

5 Click the **Members** tab.

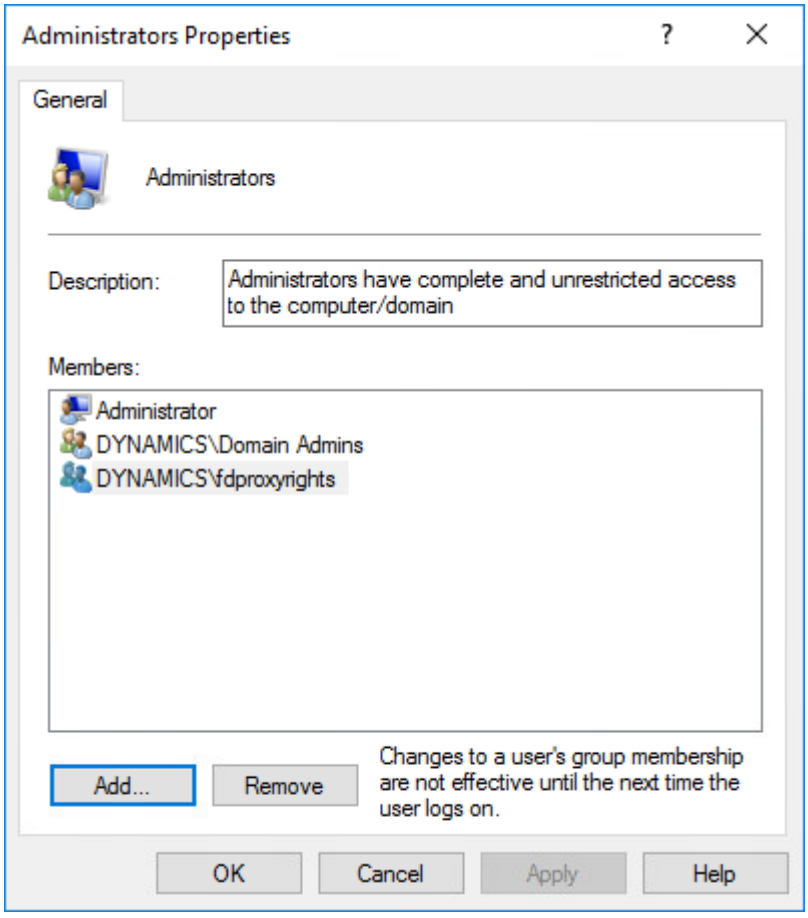
6 Click **Add**.

7 In the **Enter the object names to select** field, type: `fdproxyrights`



8 Click **Check Names**.

9 Click **OK**.



10 Click **OK**.

6.9 Installing and Configuring the Event Monitor

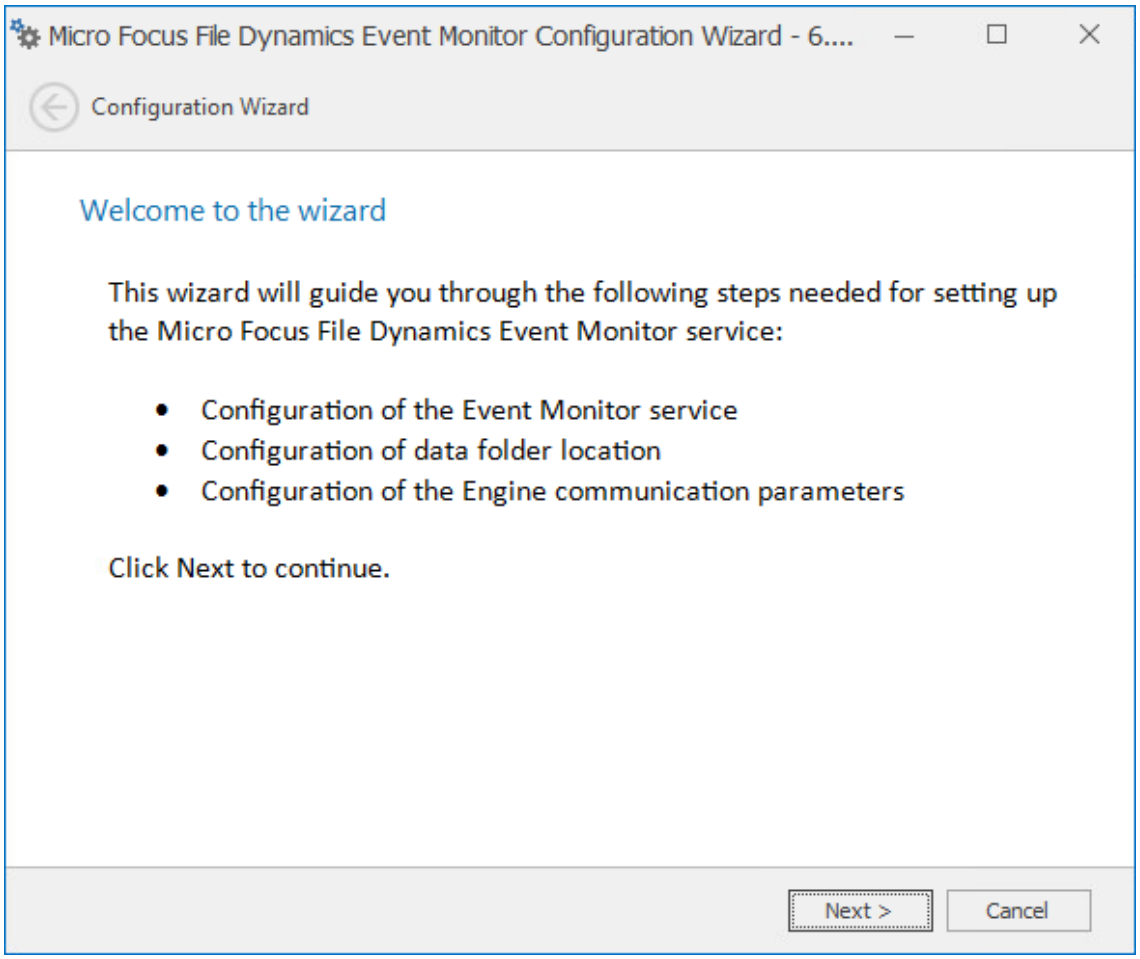
The Event Monitor can be installed on a Windows Server machine that meets the following minimum requirements:

- Microsoft Windows Server 2016 (Member Server)
- Microsoft Windows Server 2012 R2 (Member Server)
- Microsoft Windows Server 2012 (Member Server)
- Microsoft Windows Server 2008 R2 (Member Server)
- At least 4 GB RAM
- Forest functional level 2003 or later in native mode

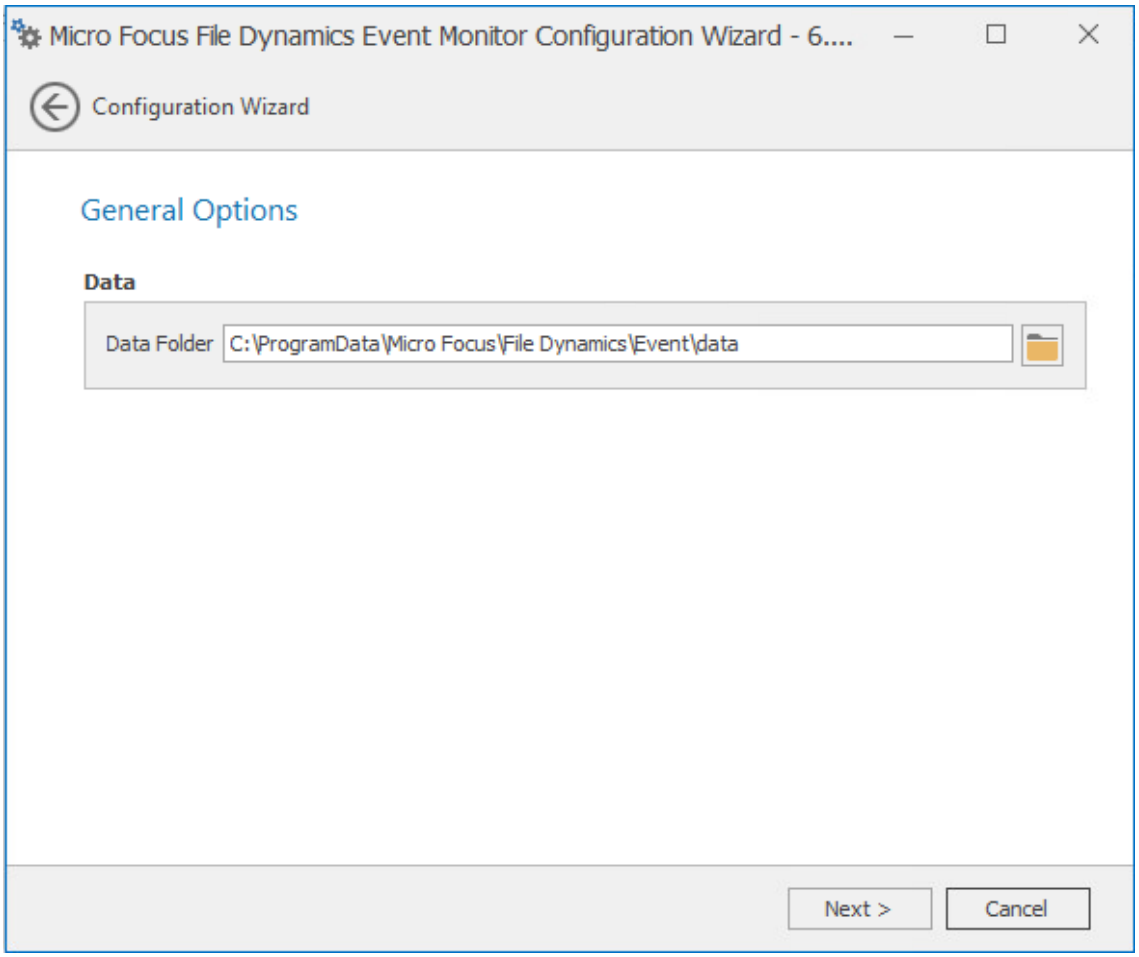
Other notable information about the Event Monitor:

- 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_1.iso`.
2. Mount the `FileDynamics-6_1.iso` file.
3. At the root of the `FileDynamics-6_1.iso` image, double-click `FileDynamics-EventMonitor-6.1-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**.

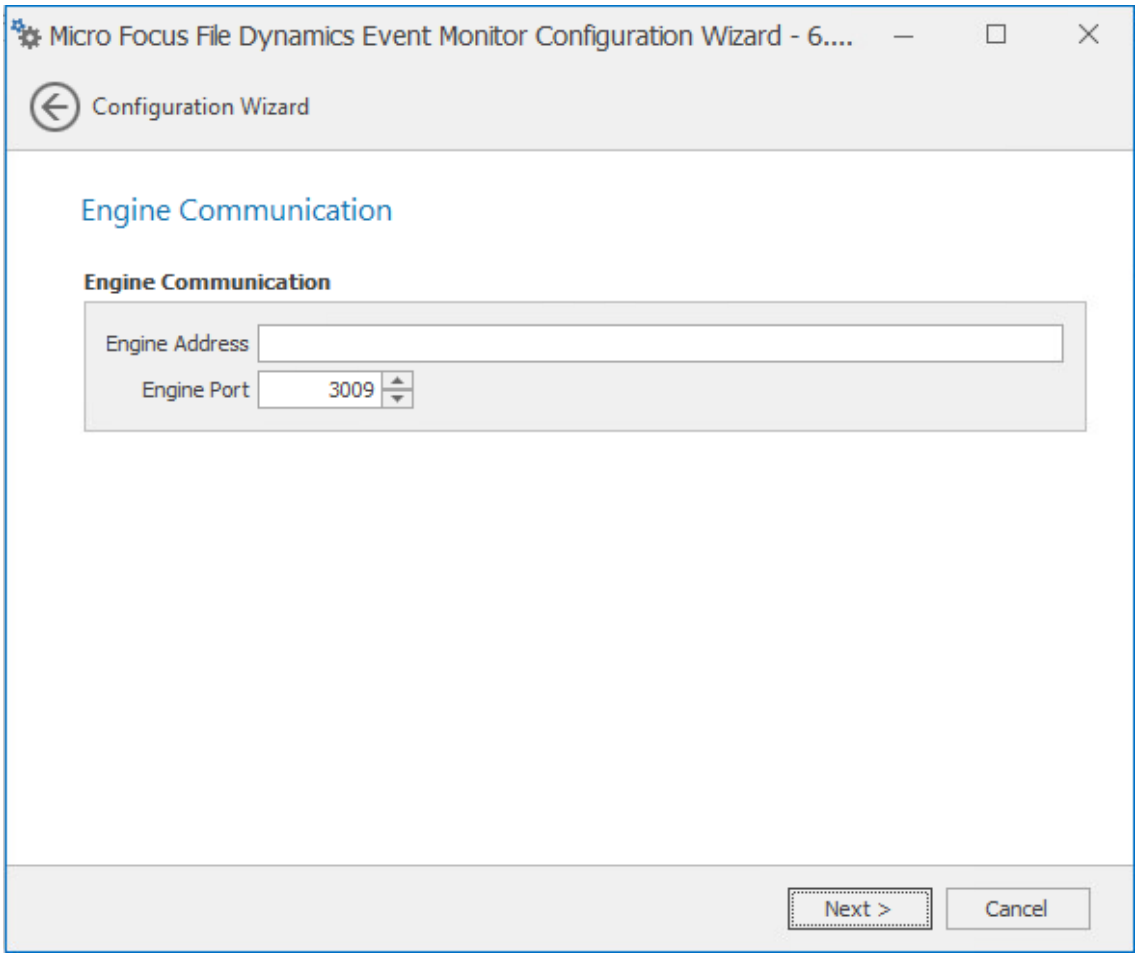


7 From the wizard page, read the overview of the setup steps and click **Next**.



The default path of the Data Folder is displayed, which you can edit. The Data folder contains application data needed by File Dynamics.

8 Click **Next**.

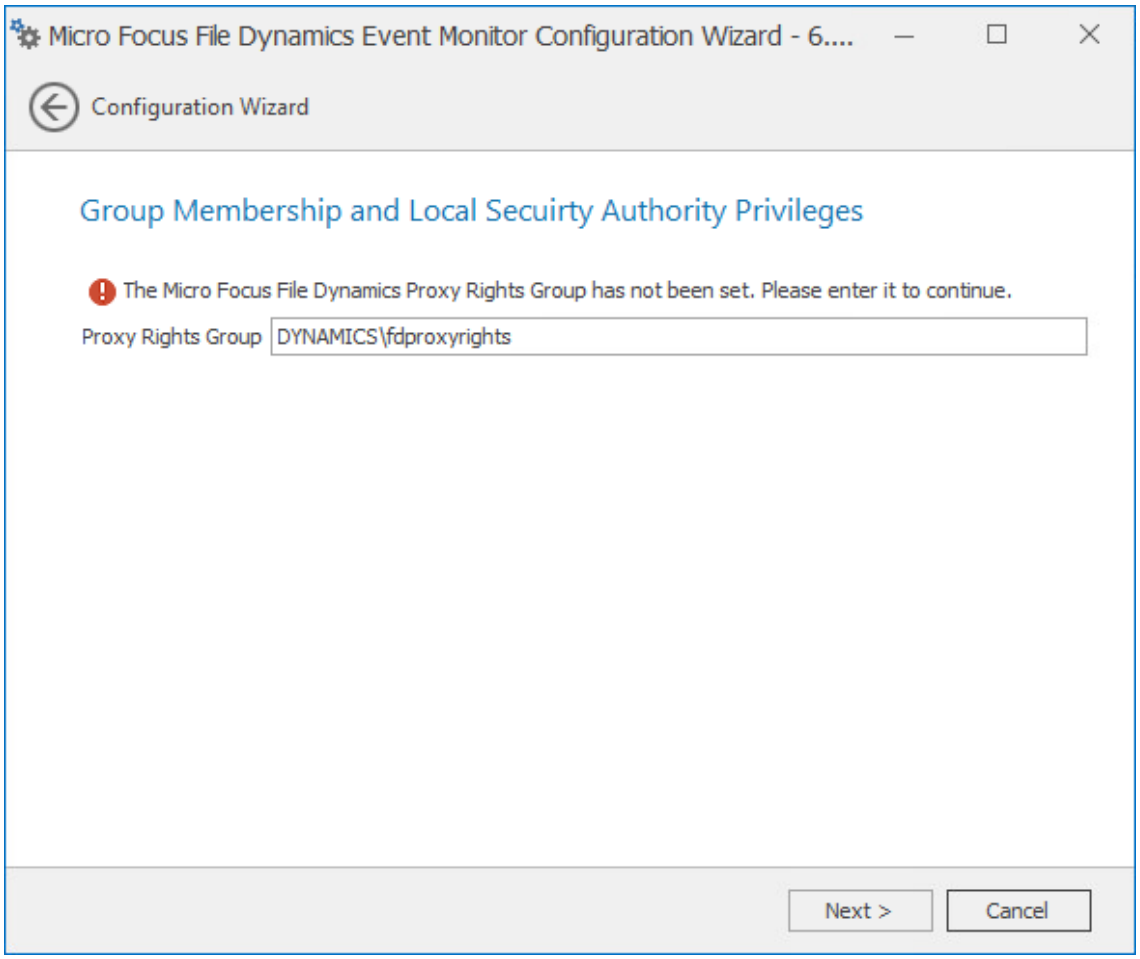


This page lets you set parameters for the Event Monitor to communicate with the Engine.

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

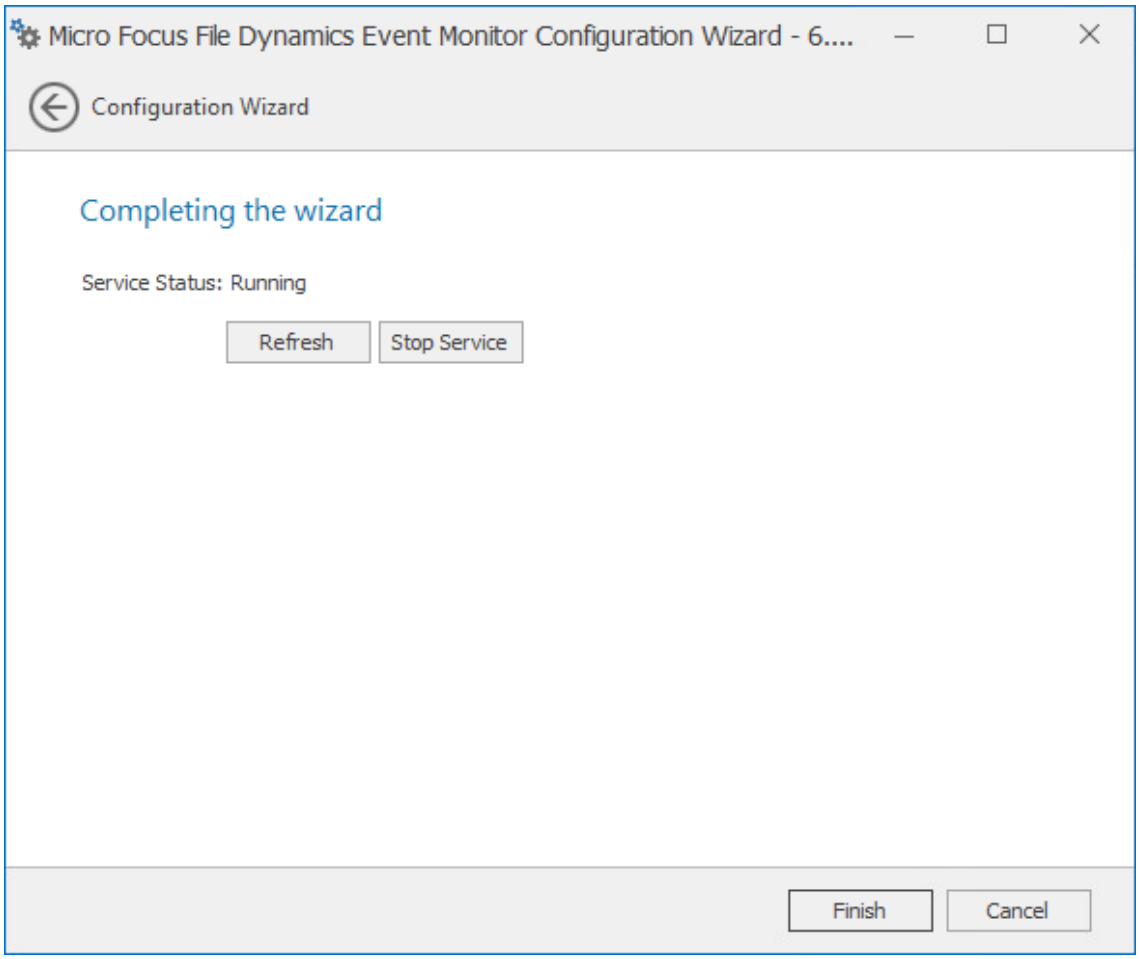
Engine SSL Port: Specify the SSL port for the Engine here.

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



10 (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.

11 Click **Next**.



12 Click **Finish**.

The Event Monitor is now installed and running. You must still authorize it using the Admin Client. For procedures, see Section 6.13, “Authorizing the Event Monitor,” on page 105.

6.10 Installing and Configuring the File System Agents

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

- Microsoft Windows Server 2016 (Member Server)
- Microsoft Windows Server 2012 R2 (Member Server)
- Microsoft Windows Server 2012 (Member Server)
- Microsoft Windows Server 2008 R2 (Member Server)
- At least 4 GB RAM
- For quota management, Microsoft File System Resource Manager (FSRM) must be installed

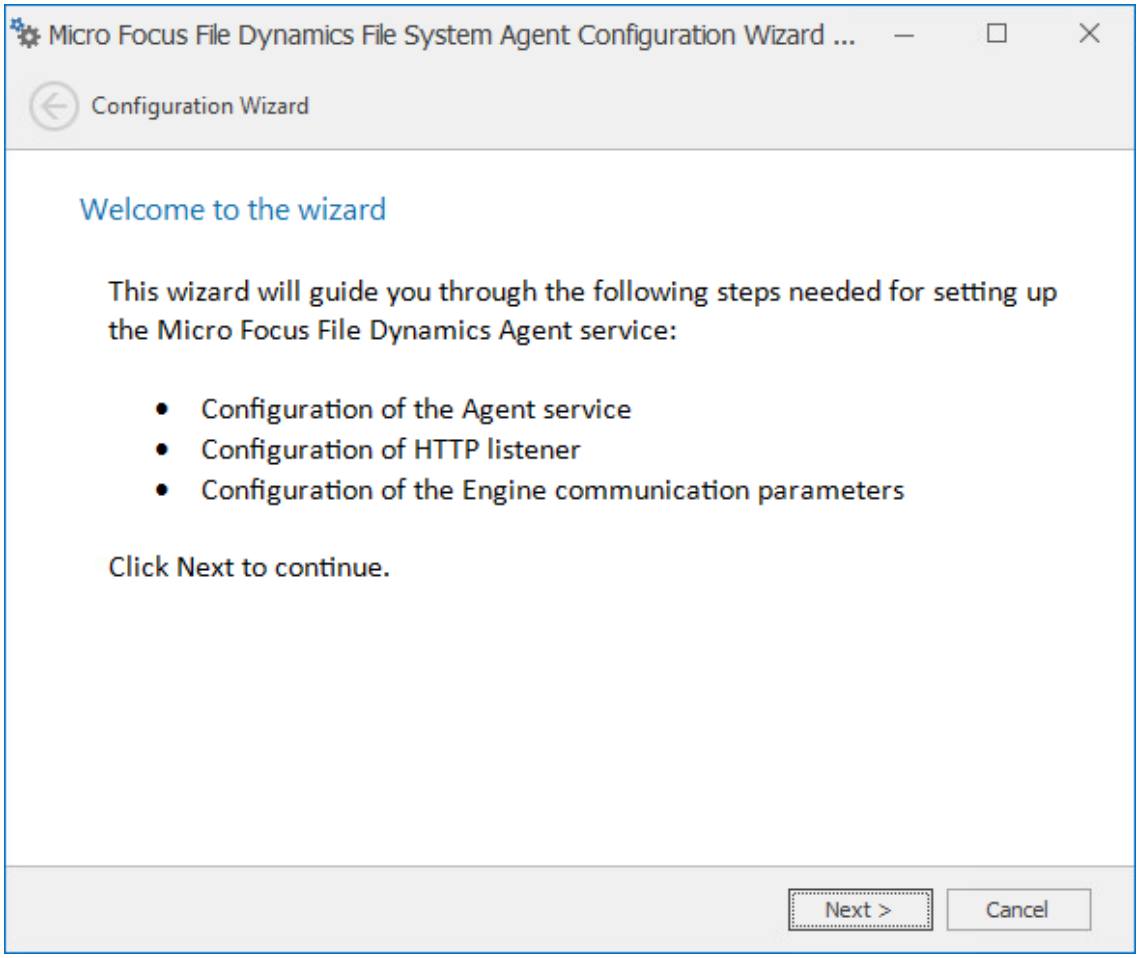
  See Section 1.2, “File Server Resource Manager,” on page 8.

Other notable information about File System Agents:

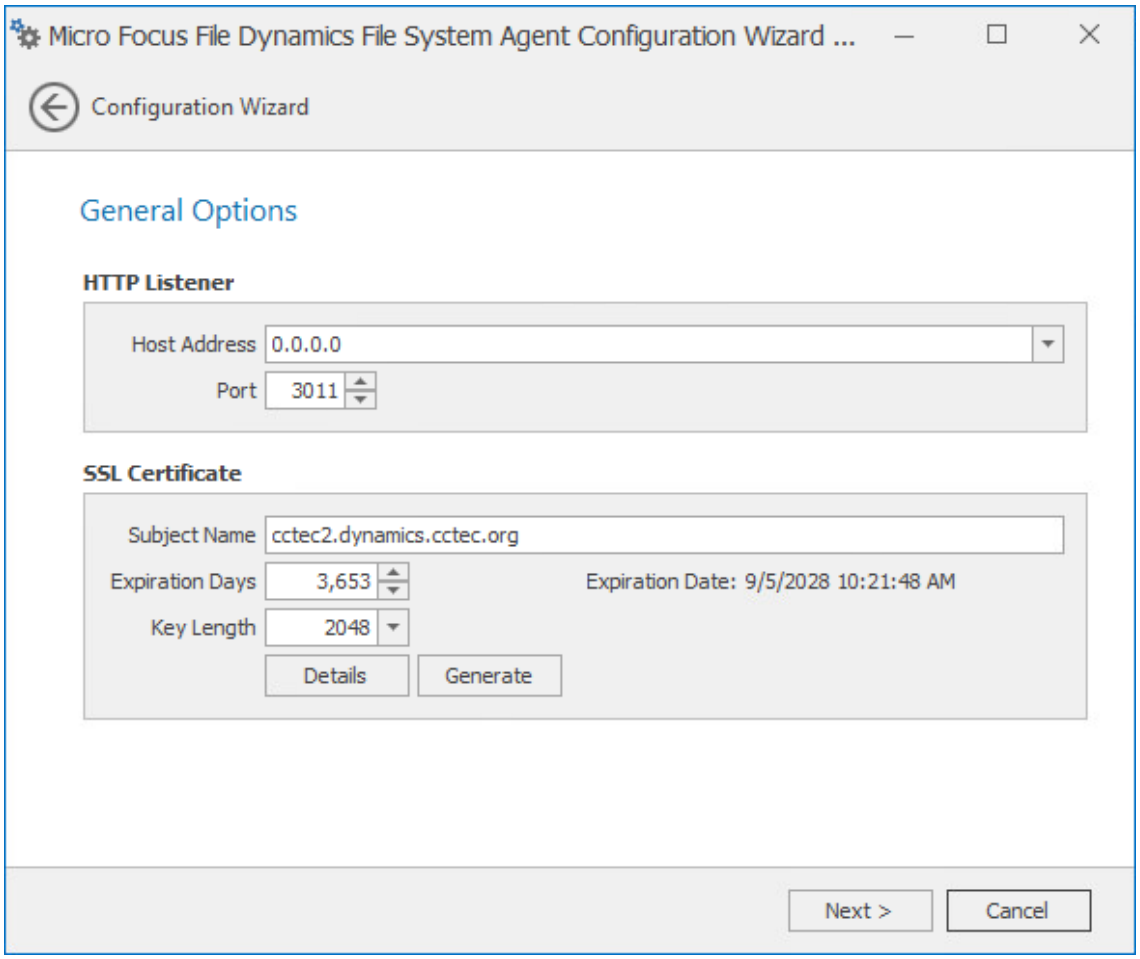
- A File System Agent runs as a native NT service that is configured to start by using the Local System account

- 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_1.iso`.
2. Mount the `FileDynamics-6_1.iso` file.
3. At the root of the `FileDynamics-6_1.iso` image, double-click `FileDynamics-FileSystemAgent-6.1-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**.



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

HTTP Listener: Communication parameters for the File System Agent.

Host Address: Unless you want the File System Agent 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 3011.

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.

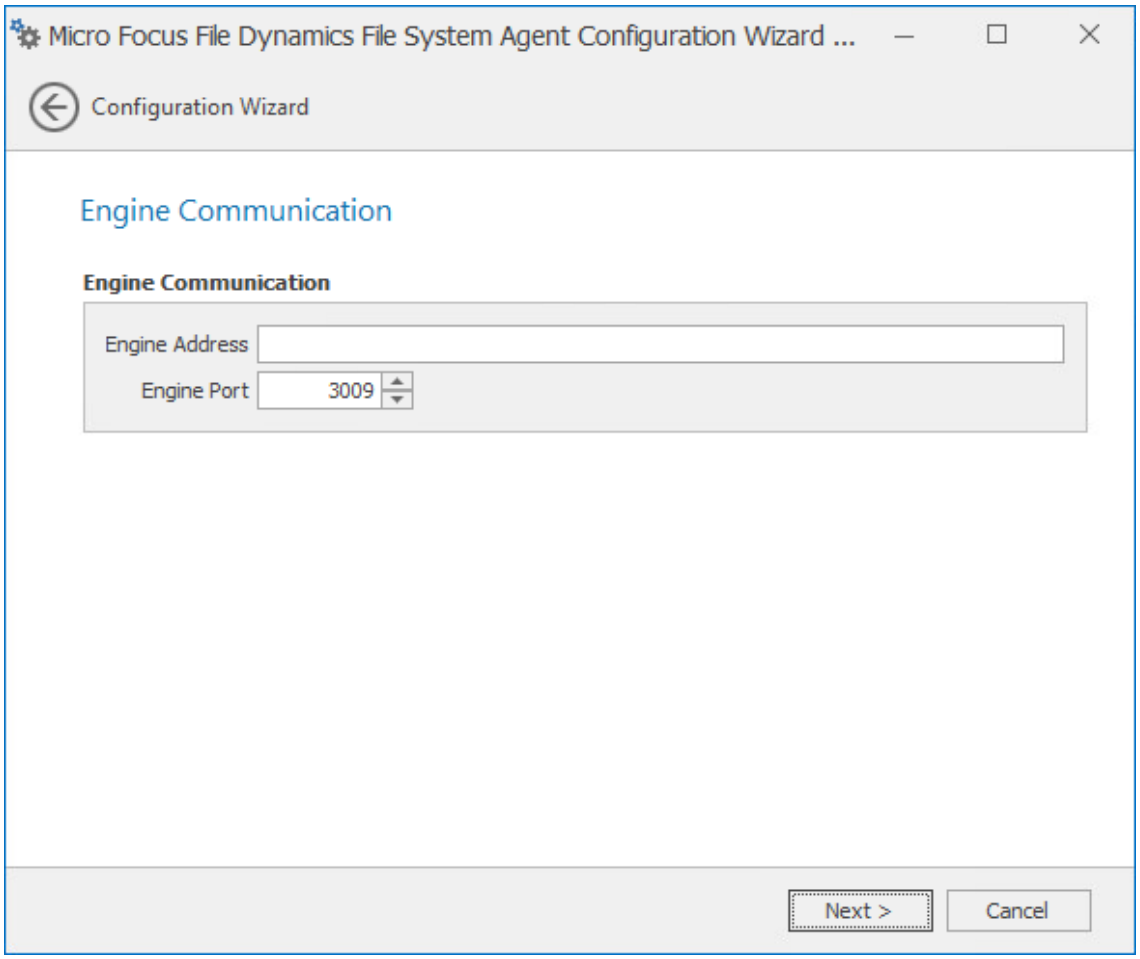
Expiration Days: The life span of the security certificate, which is set at 10 years by default.

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.

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

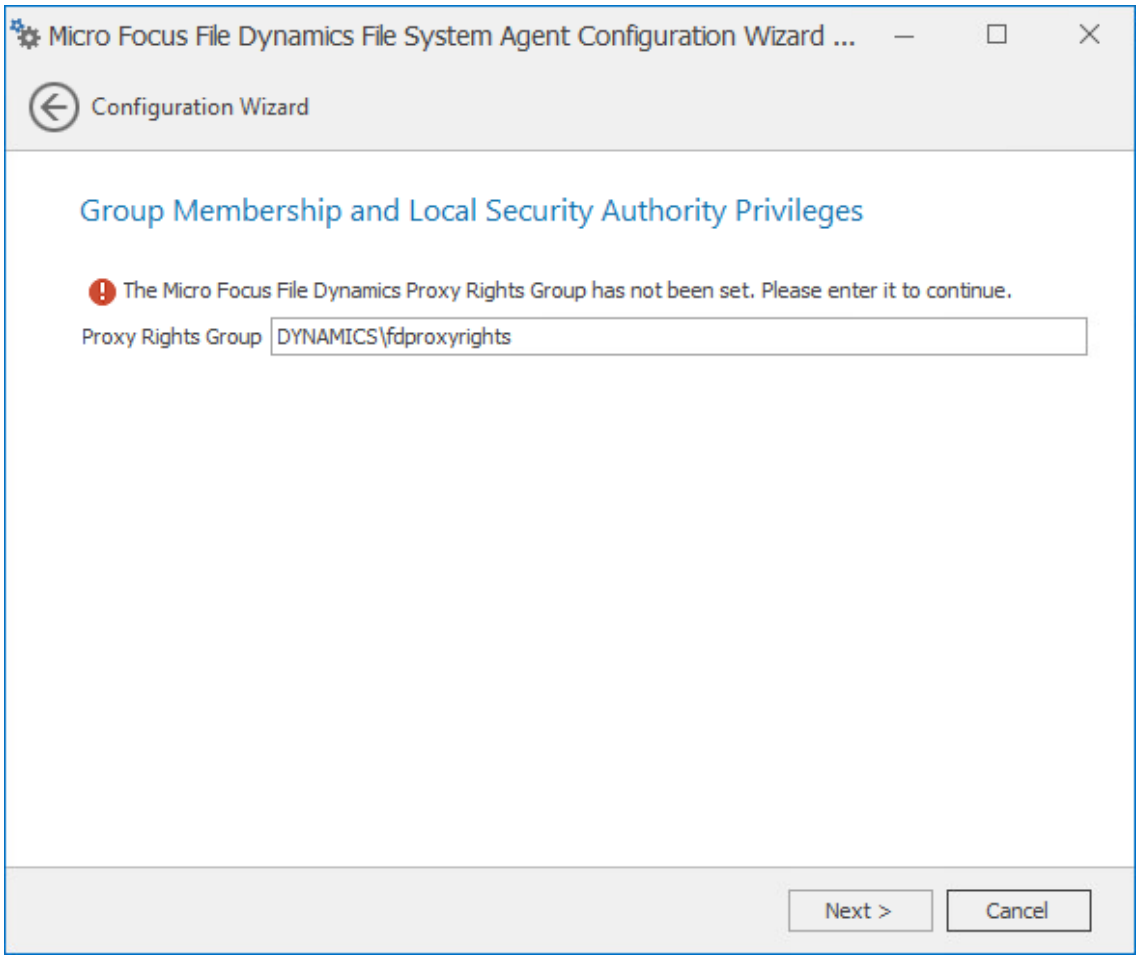


This page lets you set parameters for the File System Agent to communicate with the Engine.

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

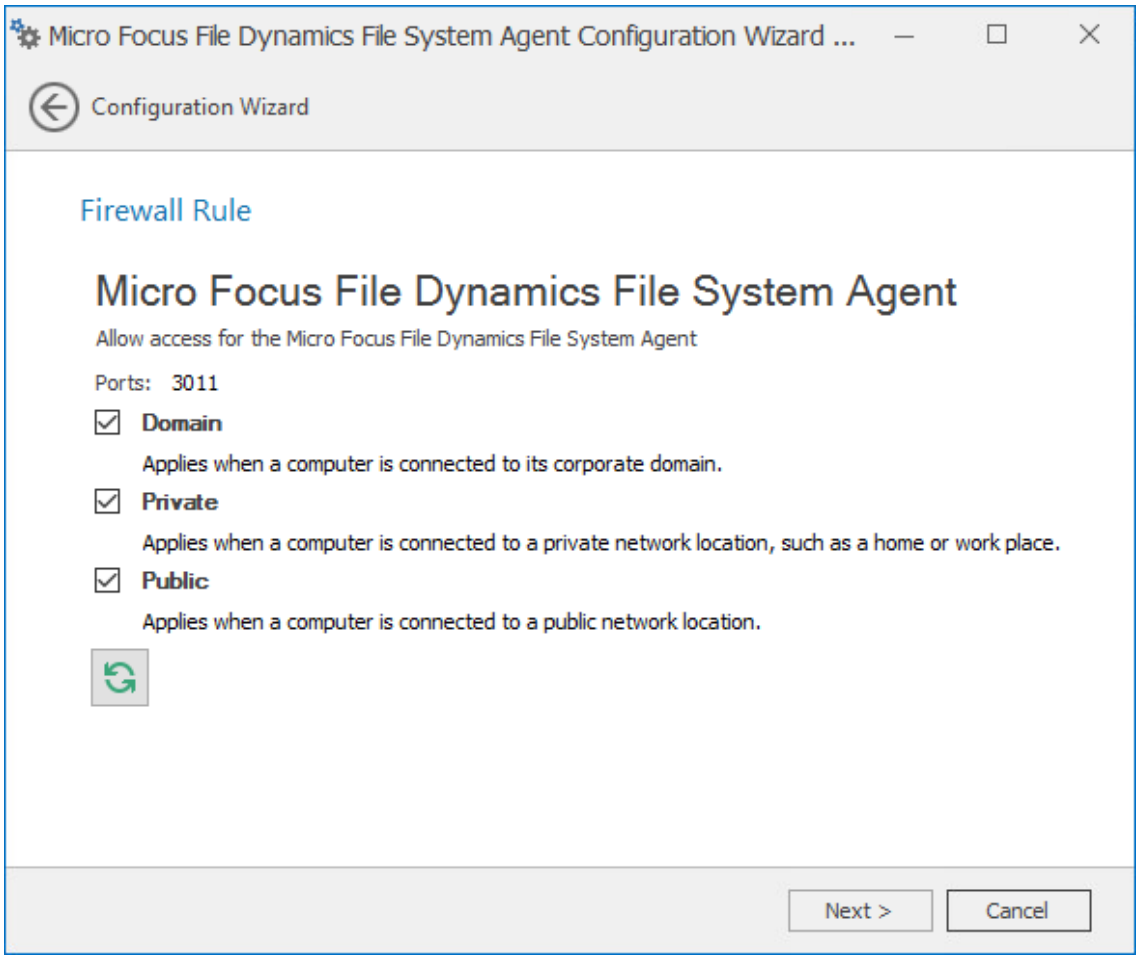
Engine SSL Port: Specify the SSL port for the Engine here.

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

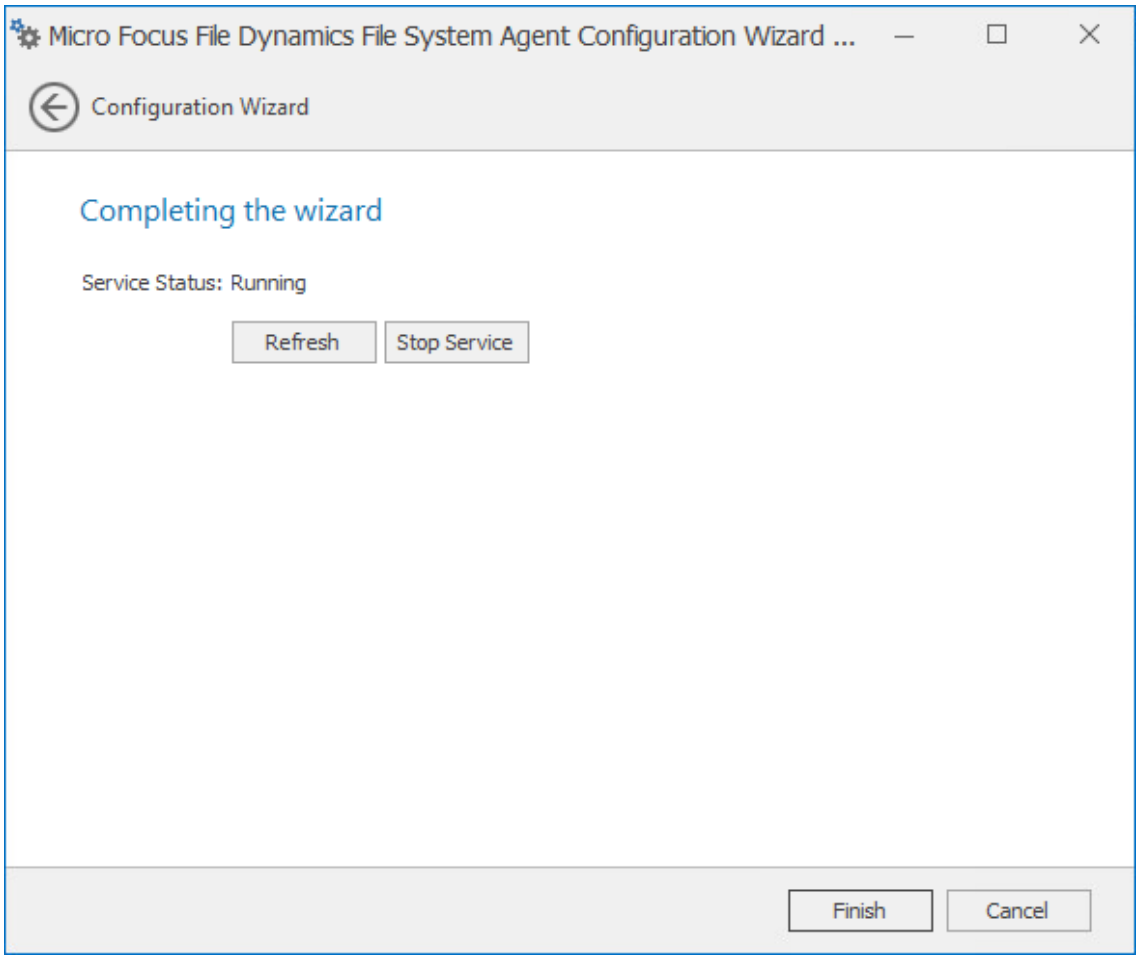


10 (Conditional) If you chose a name that was not the default name for the File Dynamics Proxy Rights group, enter the name in the Proxy Rights Group field.

11 Click **Next**.



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



13 Click **Finish**.

The File System Agent is now installed, configured, and running. You must still authorize it using the Admin Client. For procedures, see Section 6.14, “Authorizing the Agents,” on page 105.

6.11 Installing and Configuring the 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 Notify 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.

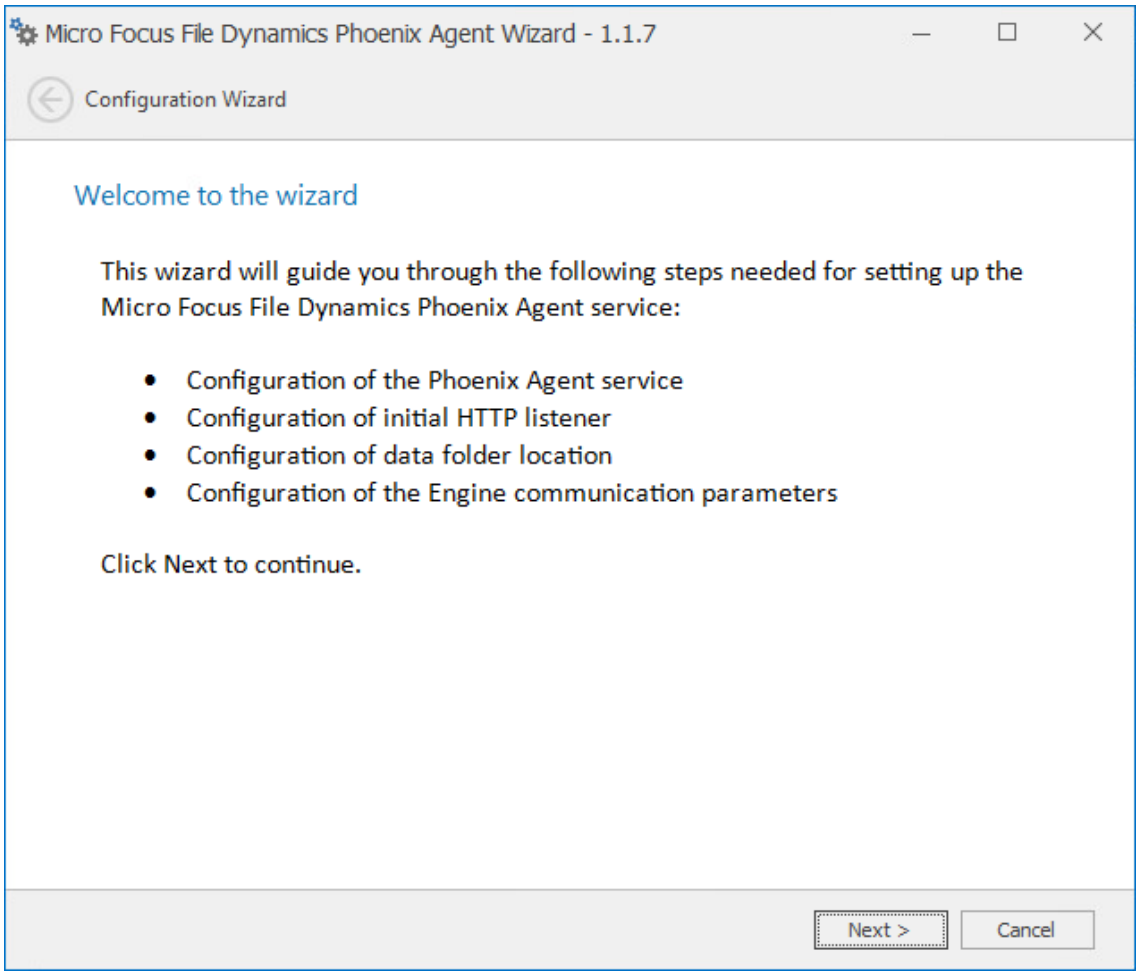
A Phoenix Agent can be installed on a Windows Server machine that meets the following minimum requirements:

- Microsoft Windows Server 2016 (Member Server)
- Microsoft Windows Server 2012 R2 (Member Server)
- Microsoft Windows Server 2012 (Member Server)
- Microsoft Windows Server 2008 R2 (Member Server)
- At least 4 GB RAM

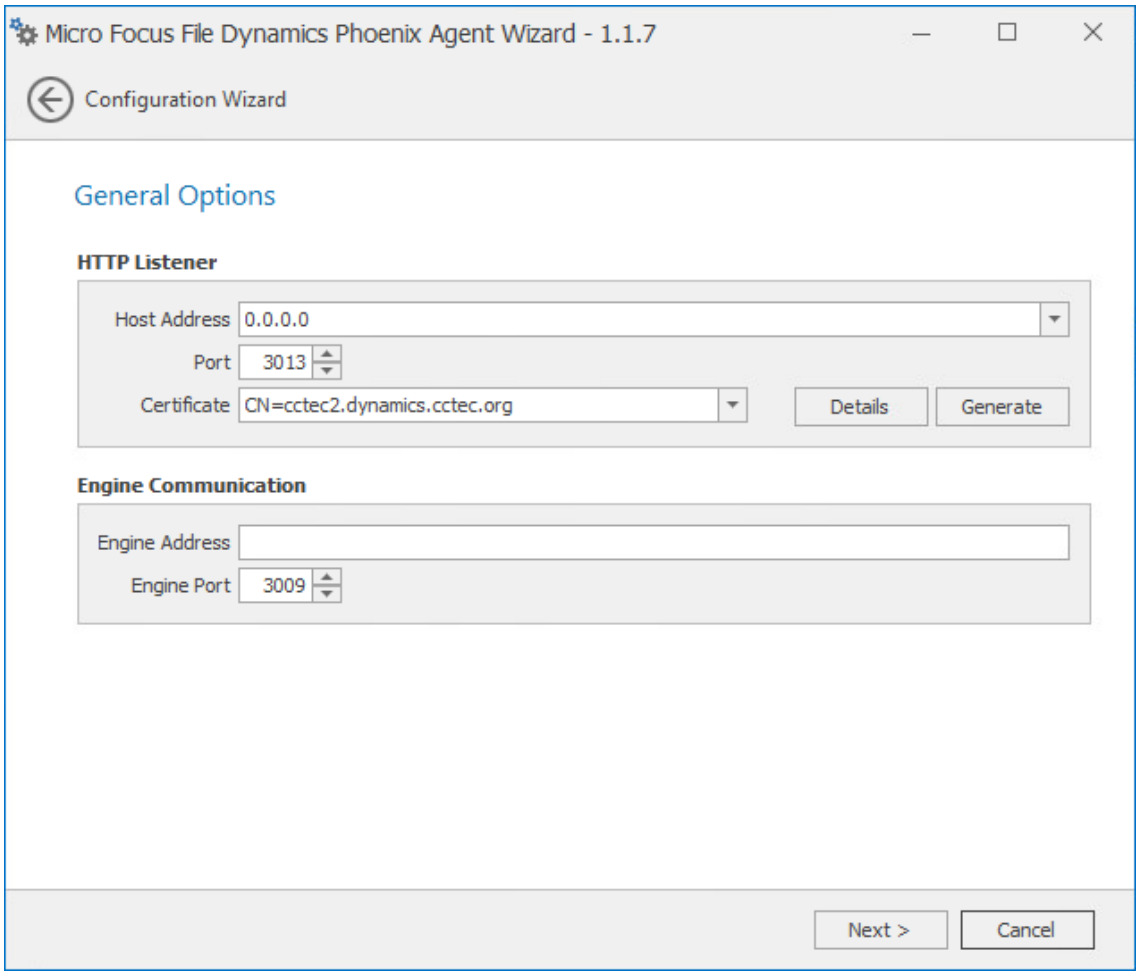
Other notable information about Phoenix Agents:

- 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_1.iso`.
2. Mount the `FileDynamics-6_1.iso` file.
3. At the root of the `FileDynamics-6_1.iso` image, double-click `FileDynamics-PhoenixAgent-6.1-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**.



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

HTTP Listener: Communication parameters for the Phoenix Agent.

Host Address: Unless you want the Phoenix Agent 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 3013.

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

Details: Click the button to view the certificate data.

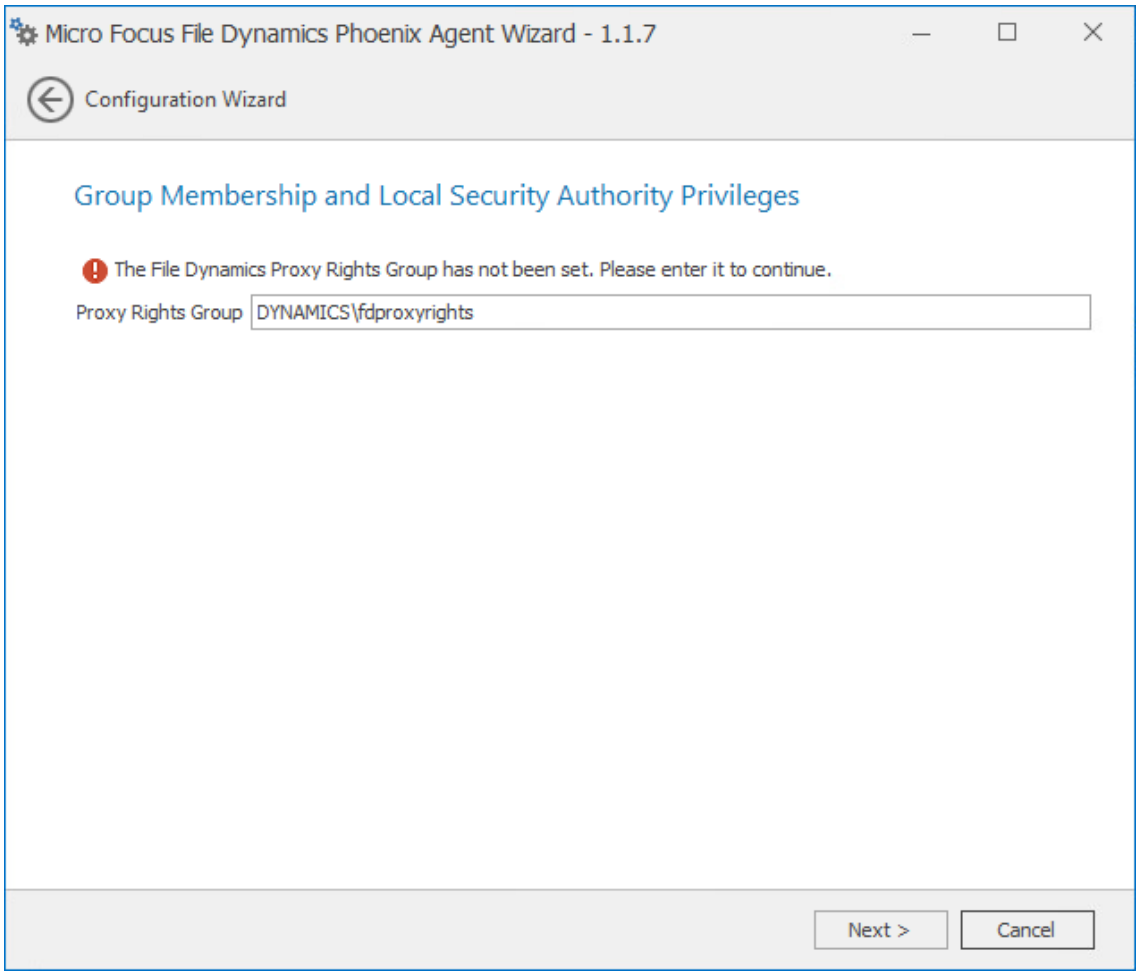
Generate: If you modify any of the settings in the **SSL Certificate** region, click this button to generate a new certificate.

Engine Communication: Communication information for the Engine host.

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

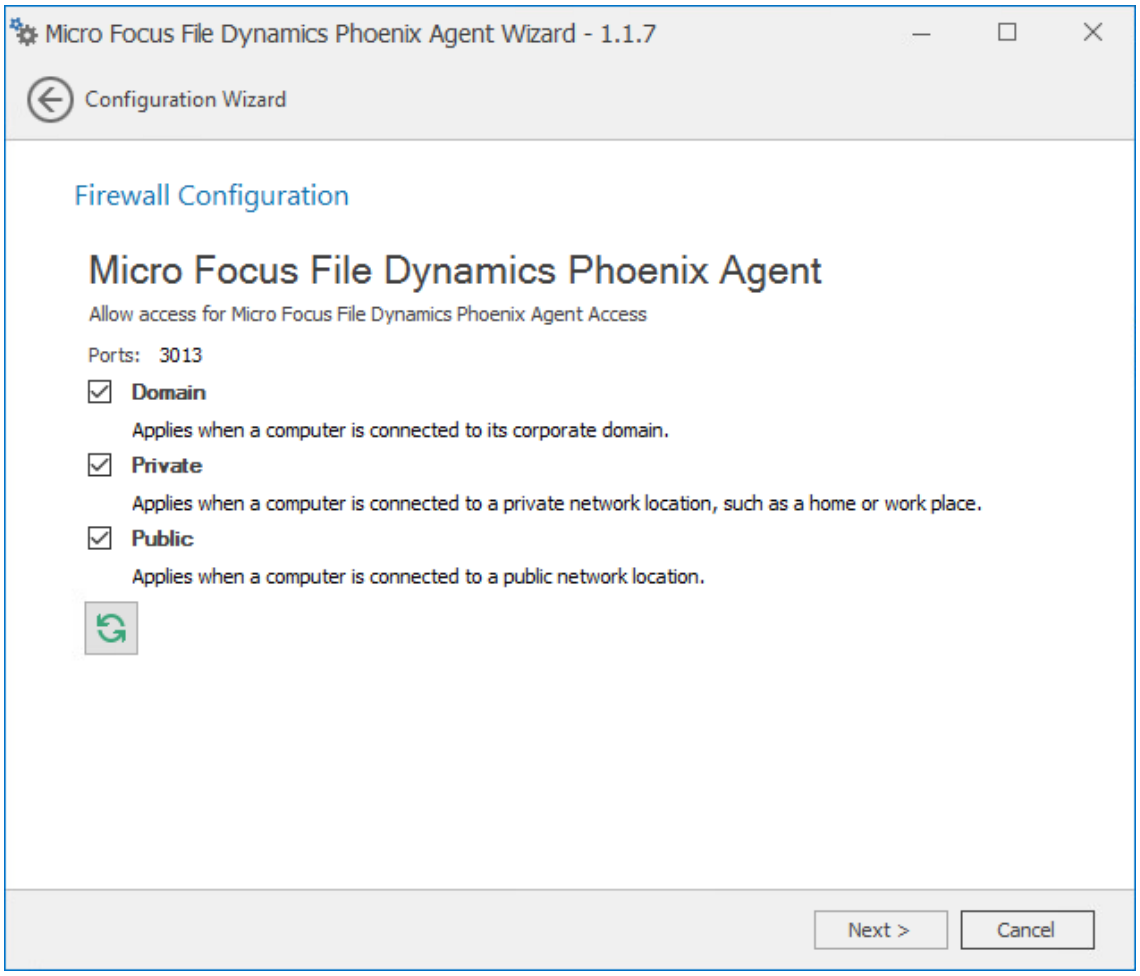
Engine Port: Specify the SSL port for the Engine here.

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



9 (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.

10 Click **Next**.



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

The wizard indicates that the Phoenix Agent service is running.

12 Click **Finish**.

6.12 Installing the Admin Client

The Admin Client is the administrative interface for File Dynamics. It can be installed on the following hosts:

- Windows 10, 8, or 7
- Windows Server 2016, 2012 R2, 2012, 2008 R2, or 2008

1 On the Windows server or workstation where you will run the Admin Client, copy to a directory the `FileDynamics-6_1.iso`.

2 Mount the `FileDynamics-6_1.iso` file.

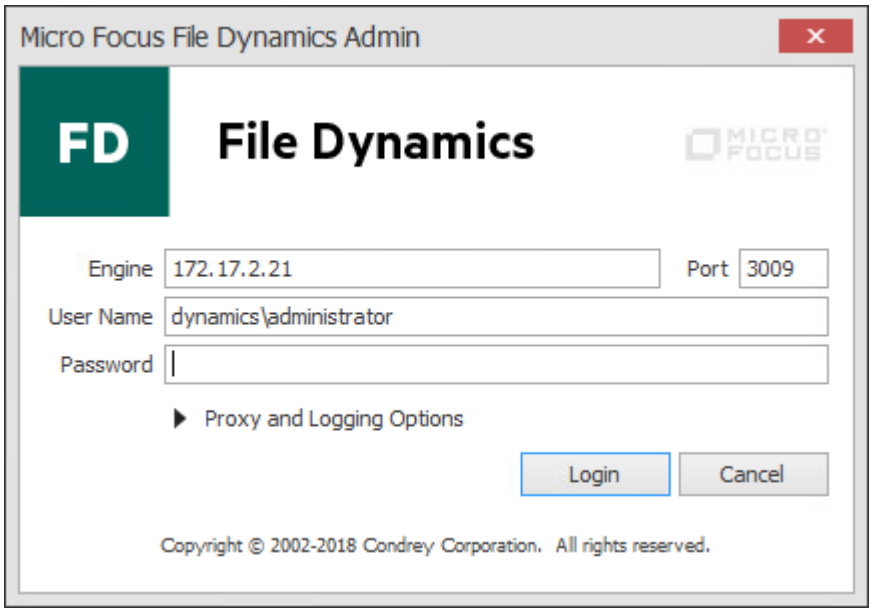
3 At the root of the `FileDynamics-6_1.iso` image, double-click `FileDynamics-Admin-6.1-xx.exe`.

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**.

The Admin Client login dialog box appears.



7 In the **Engine** field, specify the DNS name or IP address.

8 In the **Port** field, specify the secure port number.

The default setting is 3009.

9 Specify the username and password.

The user must be a member of the fdadmins group to be able to log in.

10 Click **Login**.

If you are unable to log in, your proxy settings might be preventing you from doing so. Until you enter a proxy exception in your proxy settings, you can click **Proxy and Logging Options**, select **Do not use a Proxy**, then click **Login**.

6.13 Authorizing the Event Monitor

1 In the Admin Client, click the **Engine** 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**.

6.14 Authorizing the Agents

1 In the Admin Client, click the **Engine** 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.

6.15 Installing the Data Owner Client

The Data Owner Client is the administrative tool used by designated Data Owners to perform specific types of data management actions. These include recovering archived data and permissions from High-Value Targets (HVTs) and initiating data operations from externally-generated files through Workload policies.

The Data Owner Client can be installed on the following hosts:

- Windows 10, 8, or 7
- Windows Server 2016, 2012 R2, 2012, 2008 R2, or 2008

1 On the Windows server or workstation where you will run the Data Owner Client, copy to a directory the `FileDynamics-6_1.iso`.

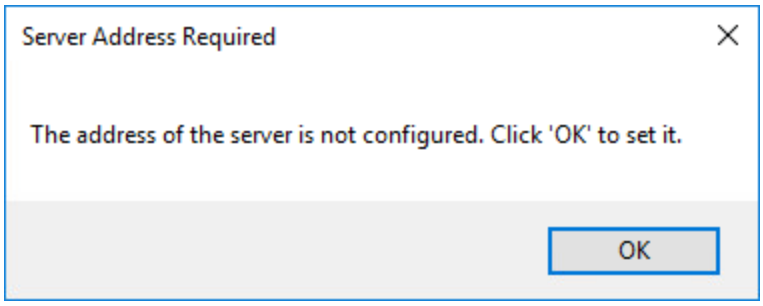
2 Mount the `FileDynamics-6_1.iso` file.

3 At the root of the `FileDynamics-6_1.iso` image, double-click `FileDynamics-DataOwnerClient-1.1-xx.exe`

4 Agree to the licensing terms and conditions and click **Install**.

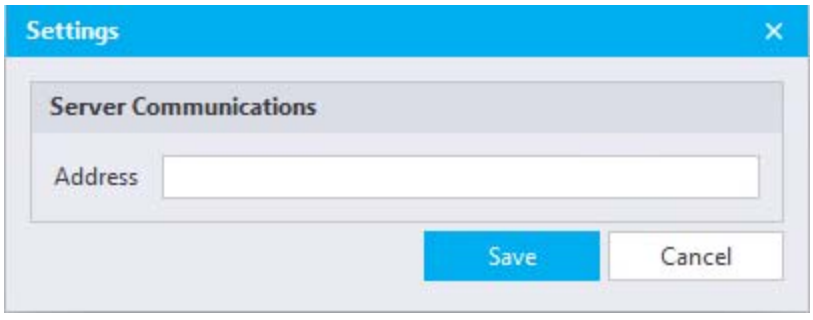
5 When notified that the setup was successful, click **Run Data Owner Client**.

The following notification appears:



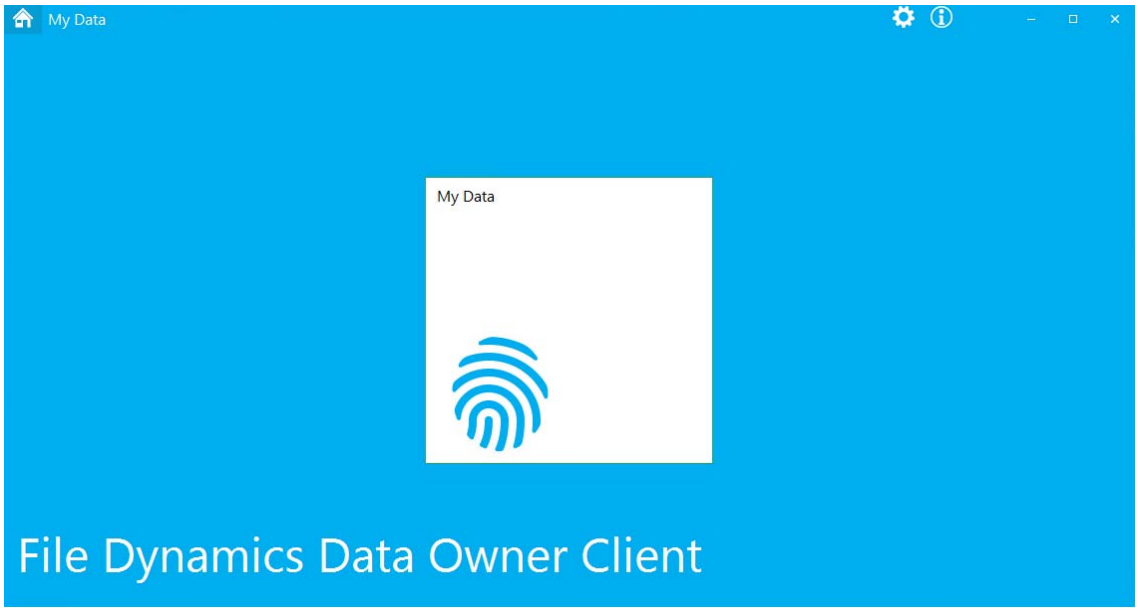
6 Click **OK**.

The following dialog box appears:



7 In the **Address** field, specify the DNS name or IP address of the server hosting the File Dynamics Engine.

The following interface appears, indicating that the Data Owner Client is configured.



6.16 Installing Other Components

If you will be creating Epoch Data Protection policies or generating Work Log reports, you will need to install the CouchDB database. Procedures for doing so, including where to download CouchDB, are provided in both Creating Target-Driven Policies and Building Work Log Reports of the *Micro Focus File Dynamics 6.1 Administration Guide*.

CEDMScanCompare.exe is a workstation utility that you can run to compare a source and target following a Cross-Empire Data Migration. Procedures for installing the application are located in both Performing an eDirectory to Active Directory Cross-Empire Data Migration and Performing an Active Directory to Active Directory Cross-Empire Data Migration of the *Micro Focus File Dynamics 6.1 Cross-Empire Data Migration Guide*.

6.17 Administering File Dynamics

You have now completed the installation of File Dynamics 6.1. For administration procedures, refer to the *Micro Focus File Dynamics 6.1 Administration Guide*.

A Documentation Updates

This section contains information about documentation content changes that were made in this *Micro Focus File Dynamics 6.1 Installation Guide* after the initial release of File Dynamics 6.0. 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:

A.1 September 28, 2018

Updates were made to the following sections:

Location	Update Description
Section 5.2, “Upgrading from File Dynamics 6.0,” on page 59	New section.