SureSync MFT

Evaluator's Guide

Software Pursuits

Table of Contents

Introduction

SureSync Managed File Transfer (MFT) is a next generation enterprise grade managed file transfer application. Data is the lifeblood of modern business. Files must be readily available and accessible from wherever an employee needs access. Companies need a detailed audit trail and powerful reporting capabilities to know what data processing has been completed and what remains to be done. SureSync MFT provides a flexible, efficient, and intuitive solution to these data management challenges.

This Evaluator's Guide is designed to walk you through the initial setup of SureSync MFT using a common example. This guide will configure a multi-directional synchronization with file locking. This is only one scenario SureSync MFT can handle. Other examples include:

- One-way distribution of files to remote offices. For example, publishing new sales collateral to remote sales offices
- Archiving commonly used files into the cloud for disaster recovery purposes
- Backing up data from remote / mobile desktop and laptop computers

By working through this guide, you will develop a deeper understanding of how to configure SureSync MFT. A single document cannot describe all the powerful functionality available to you. Our support team is always available to provide additional guidance. We recommend scheduling an initial conversation with the team when planning your trial.

System Requirements

SureSync MFT's basic operating system and hardware requirements are:

- **Supported Operating Systems:** Windows 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 SP1; Windows 10 Version 1607 or newer; Windows 8.1; Windows 7 SP1
- **Processor:** Dual-core CPU of at least 2.5Ghz (minimum); Quad-core CPU or greater of at least 2.5Ghz (recommended)
- **RAM (total for system):** 4GB of free memory (recommended minimum)
- **Hard Disk:** 100MB for application files; 20MB+ for database

SureSync MFT can synchronize data to older Windows platforms and non-Windows machines such as Mac or Linux via UNC path on a scheduled basis. The software itself must be installed on one of the supported operating systems above.

For File Locking, ReFS volumes are not supported on Windows 2008 R2, Windows 2012 or Windows 7.

Virtualization

SureSync MFT can be run on Windows operating systems hosted in virtualization software such as VMWare or Hyper-V. Each virtual machine involved in processing requires appropriate licensing.

SureSync MFT Database Requirements

SureSync MFT requires a database to store configuration information. The following formats are supported:

- SQL Server Express 2012, 2014, 2016, 2017, 2019 and 2022
- SQL Server 2012, 2014, 2016, 2017, 2019 and 2022

Database Size

SureSync MFT uses the SQL database extensively. This database includes records for each file processed, logs / audit information and more. When planning a SureSync MFT deployment, consider the number of files in the environment and the impact that will have on the resulting SQL database size.

Assume approximately 3GB of database storage will be consumed per 1 million files in the data set.

This guidance assumes that you are using the defaults for history retention. The longer you store history, the larger the resulting database. This guidance is to provide you with an idea of SQL storage requirements. The amount of storage consumed in your specific environment may be different depending on configuration.

Current versions of SQL Express have a 10GB file size limit. If you intend to use SQL Express in an environment with more than 3 million files, you have couple of options:

- Use multiple SQL Express instances with multiple MFT Hubs. This solution requires breaking your Jobs up across multiple machines to keep the overall data usage of each under the 10GB file size limit.
- Use a SQL Standard or better edition of SQL server. If your environment already has a SQL server, this is recommended.

SQL Authentication

SureSync MFT requires a SQL server configured for Mixed Mode authentication. The account that accesses the SureSync MFT database must be a SQL account. You can check the configuration of your SQL Server instance with SQL Management Studio.

In SQL Management Studio, right click on the SQL Instance name as shown below.
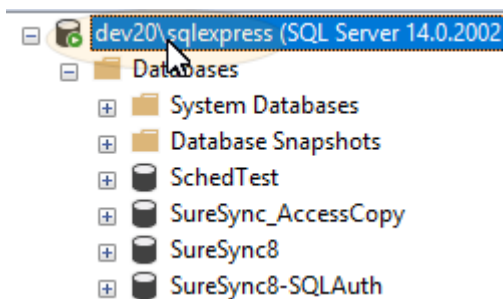
Select Properties, click Security and make sure "SQL Server and Windows Authentication mode" is selected.
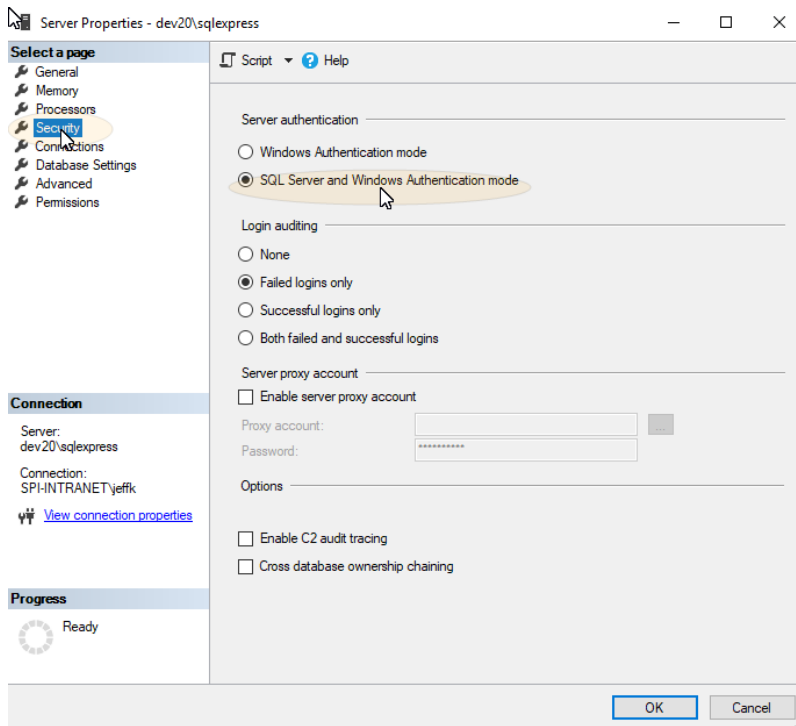
The SureSync MFT account can be created by expanding Security in the SQL Management Studio menu, right clicking on Logins and selecting "New Login…"

For account permissions, you have two choices:

1. Use a SQL account with sysadmin permissions. This will allow the account to create the SQL database in the SureSync MFT wizard.
2. Create a blank database with SQL Management Studio and assign the SQL account "DBOwner" permissions. You would then open the database in the SureSync MFT wizard instead of creating one.

Required Microsoft Components

SureSync MFT requires several Microsoft components to be installed on the system. The installer will inspect your system for these components and offer to upgrade or install them as needed.

- Microsoft .NET Framework 4.8
- Microsoft Visual C++ Runtime 14.0 Update 3

Using the installer to install these prerequisites could result in a reboot being necessary before the setup can continue. If a reboot is necessary, the installer will prompt you. In environments where a reboot is disruptive, we recommend installing the required components manually during your normal maintenance schedules before installing SureSync MFT.

Contact Information

If you need further information about SureSync MFT or need clarification on anything within this guide, please contact our support group. They will be happy to assist with your evaluation.

Software Pursuits, Inc.
140 Chestnut Ln
San Mateo, CA 94403

Phone: +1-650-372-0900
Fax: +1-650-372-2912

Sales e-mail: sales@softwarepursuits.com
Support e-mail: support@softwarepursuits.com

Technical support is available between 7:00AM and 4:00PM PST Monday through Friday.

Our Scenario

This guide will walk you through the configuration of SureSync MFT to accomplish a multi-way synchronization of files between *DEV20*, *SPITEST-WIN2K8* and *SPITEST-WIN2K12* with file locking.

> SureSync MFT is capable of one-way and multi-way file processing. It can process files in real-time or on a scheduled (clock) basis. The intent of this guide is to show you the basics of configuring SureSync MFT. Please consult the help file, Ed Center training videos and contact our support team if you require additional guidance specific to your environment.
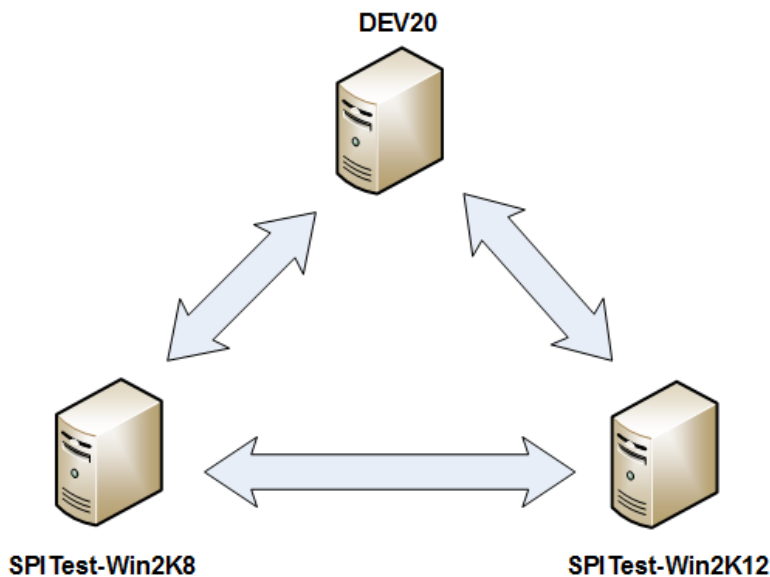
In this example, the contents of a folder C:\Documents will be processed with a multi-directional Rule with file locking. This is a common scenario for enabling collaborative file shares.

Understanding SureSync MFT Terminology

Understanding the building blocks of the SureSync MFT architecture will make it easier to deploy the solution.

Hub

The Hub is the brain of SureSync MFT. This machine has access to the MFT database and coordinates the actions of the other machines in the environment to achieve the required data movement.

SureSync MFT Database

MFT requires a Microsoft SQL database. This database is accessed by the Hub and is used for storing file state, configuration, and reporting information. This database can exist on the same machine as the Hub service or on a remote machine accessible from the Hub machine.

Communications Agent

The Communications Agent should be installed on all Windows machines that house data being processed by SureSync MFT. This service enables much of the advanced performance enhancing functionality in SureSync MFT. Non-Windows machines must be accessed via UNC path and processed with Schedules.

Job

A Job identifies the directory structure that should be processed, and the machines involved. The Job includes settings such as file masks, how to handle security copying and much more. Jobs are automated via a Schedule or an Interval Set.

Interval Set

An Interval Set will process file changes as they occur (real-time processing). The Interval Set can contain multiple Intervals that cover different spans of time with different options. An Interval Set is applied to a Group, a Job or a Root Path.

Schedules

A Schedule is used to process changes on a clock basis, such as once an hour. A Schedule is applied to a Group, a Job or a Root Path.

What is File Locking?

File Locking makes it simple to collaboratively share files between multiple offices while ensuring that users cannot make changes to the same file at the same time.

ServerA   ServerB
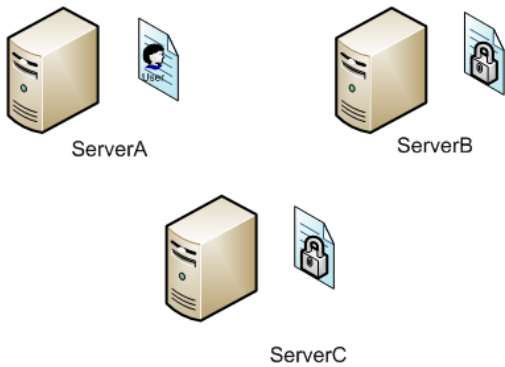
ServerC

File Locking will lock a file on all paths when a user opens the file on one machine. In this example, we have three servers named "ServerA," "ServerB," and "ServerC." These machines all contain a copy of a folder being processed by a SureSync MFT Job. Assume that UserA on ServerA has opened Document1.doc that results in a lock being established.

> File Locking does not block users on the server where the initial open happens. For example, if a user opens the file on Server A, SureSync MFT's locks occur only on ServerB and ServerC. The behavior a user encounters opening the same file on ServerA depends on the application. This allows multi-user programs such as Microsoft Access to work properly on the one machine while blocking access from the others.

While the file is locked, no other user can access a write-enabled copy of the file. If a user attempted to open the "Document1.doc" file on "ServerB," they would receive a read-only copy. If LockStatus is installed on the client, a tray notification would be provided to the user encountering the lock.

Once UserA saves the change and closes the file, SureSync MFT will replicate the changed version of the file to "ServerB" and "ServerC."

ServerA   ServerB

ServerC
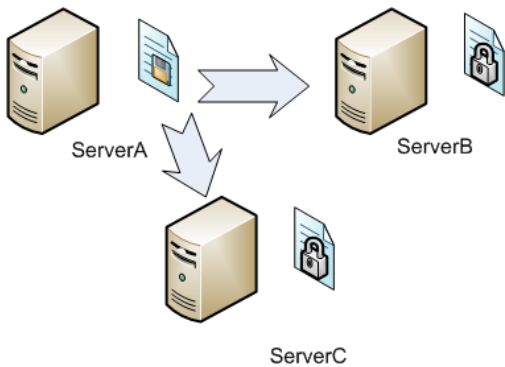
Once the file has been synchronized to the other machines, the lock will be released by SureSync MFT. At that time, other users can access the updated file with write access.
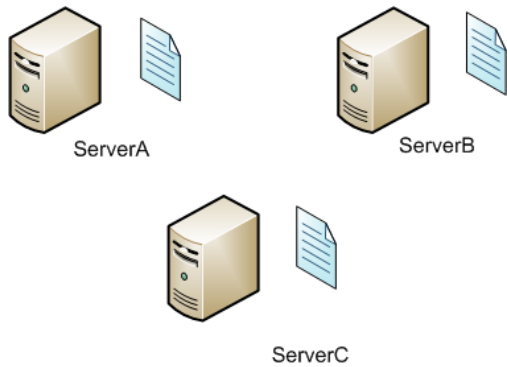
Supported Applications for File Locking

Applications use handles to open files. When an application opens a file and maintains an open file handle, the operating system and other applications know that the file is open. Applications that open files in this manner are supported by File Locking.

An application can also open a file, read it into memory and release the handle. When opens are handled in this manner, SureSync MFT cannot tell that the file is still open, so a lock will not be maintained.

The application opening the file determines if locking will function, not the file type. For example, if you open a .txt file in Notepad, that .txt file will not be locked. Notepad does not maintain the required handle in the file system. If you open that same .txt file in Microsoft Word a lock will be established because Word properly maintains the open file handle.

This list contains applications that Software Pursuits has tested with File Locking and have determined that locking will occur. If an application that supports multiple file types appears on this list, all compatible file types should be lockable.

If an application used in your environment is not on this list, we recommend performing a test open with SureSync MFT enabled to see if locking occurs.

Supported Applications

- Autodesk AutoCAD
- Microsoft Word
- Microsoft Excel (except when using the Shared workbook function)
- Microsoft PowerPoint
- Microsoft Publisher
- Microsoft Visio
- Microsoft Access
- Adobe InDesign
- Adobe PageMaker
- QuarkXPress
- OpenOffice.org Writer
- OpenOffice.org Calc
- OpenOffice.org Draw
- OpenOffice.org Impress
- OpenOffice.org Math
- OpenOffice.org Base

<u>Unsupported Applications</u>

- Adobe Illustrator
- Adobe Photoshop
- Adobe Acrobat
- Macromedia Dreamweaver
- Microsoft Wordpad
- Microsoft Notepad

## Expected Application Behavior when Encountering Locks

The behavior an end user will encounter when opening a locked file depends on the application. When deploying File Locking, it is strongly recommended that you inform end users in advance about what they can expect to experience when encountering locks.

The LockStatus application can be used to provide pop-up notification from the system tray on an end user's computer when they attempt to open a locked file.

This section highlights the behavior of a couple of common applications used with File Locking.

Microsoft Office

In the Microsoft Office applications, the file will open with [Read-Only] in the title bar.

| File | Tools | View | Test03Model.docx [Read-Only] [Compatibility Mode] - Word | | | | |
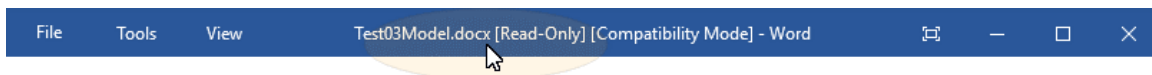
This is a test Word document in .DOCX format.

Change 001

End of document ■

AutoCAD

In AutoCAD, an alert like the one below is presented allowing the user to open a read-only copy.

AutoCAD Alert ✕

❌ \\spitest-win2k3\Jeff's Test Folders\File Locking M1-A\Drawing1.dwg is currently in use by :
admin , DEV13 .
Would you like to open the file read-only?

[Yes]   [No]
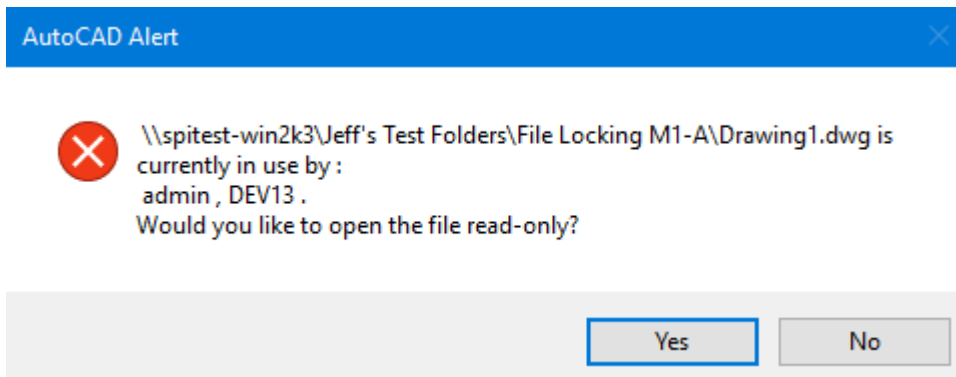
Installation

To get started with your SureSync MFT trial, you must install the correct components on each machine involved.

For the scenario covered in this guide, the Hub components will be installed on one machine (*DEV20*) and the Communications Agent will be installed on two machines (*SPITEST-WIN2K8* and *SPITEST-WIN2K12*).
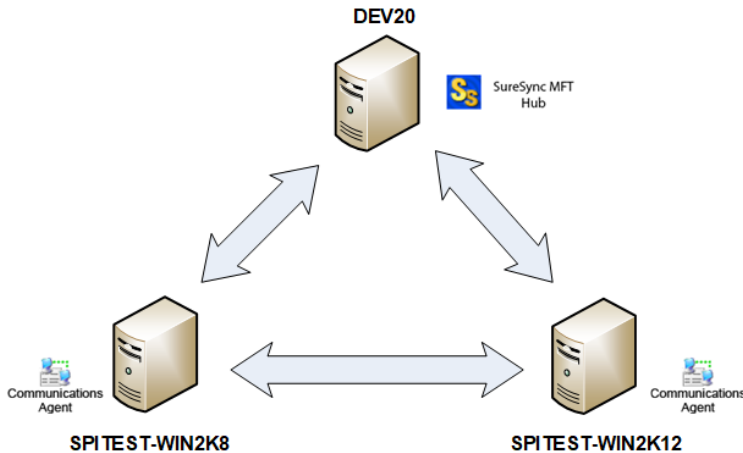
On the *DEV20* machine, we will run SureSyncMFTSetup.exe and select "Full / MFT Hub" as the installation type. This will install the complete SureSync MFT application (user interface and a Communications Agent) and designate *DEV20* as the machine where we configure and run Jobs.
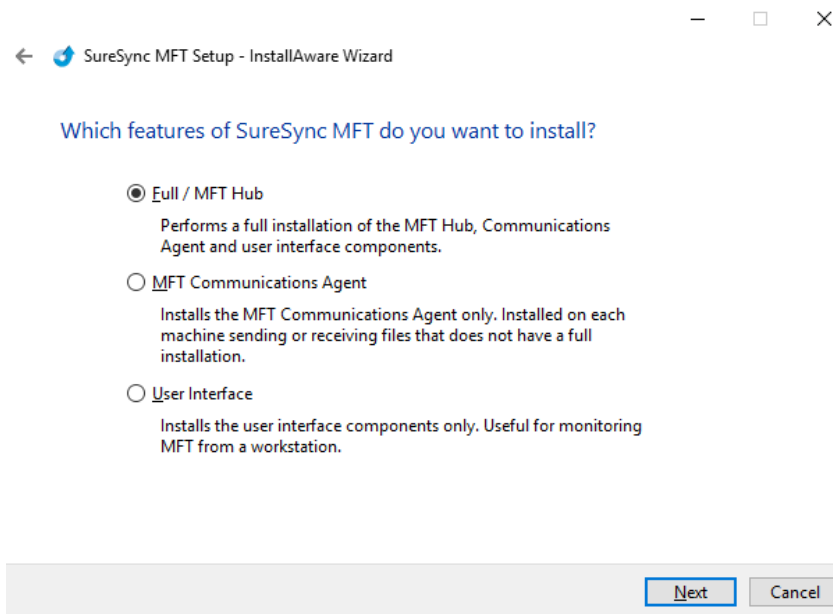
On *SPITest-Win2K8* and *SPITest-Win2K12*, the "MFT Communications Agent" setup type should be used.
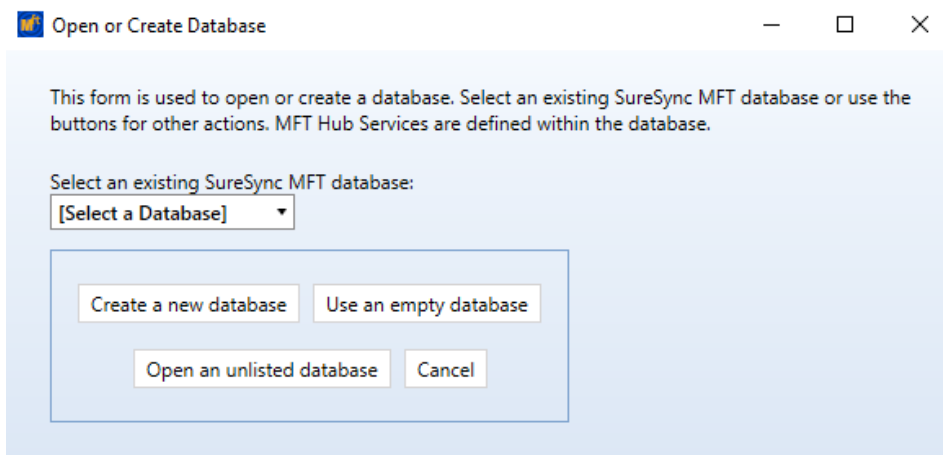
Launch SureSync MFT for the First Time

To launch SureSync MFT for the first time, go to the Start menu, select the SureSync MFT folder and click on the SureSync MFT Desktop icon. This will launch the SureSync MFT Desktop where you will complete the configuration of your environment.
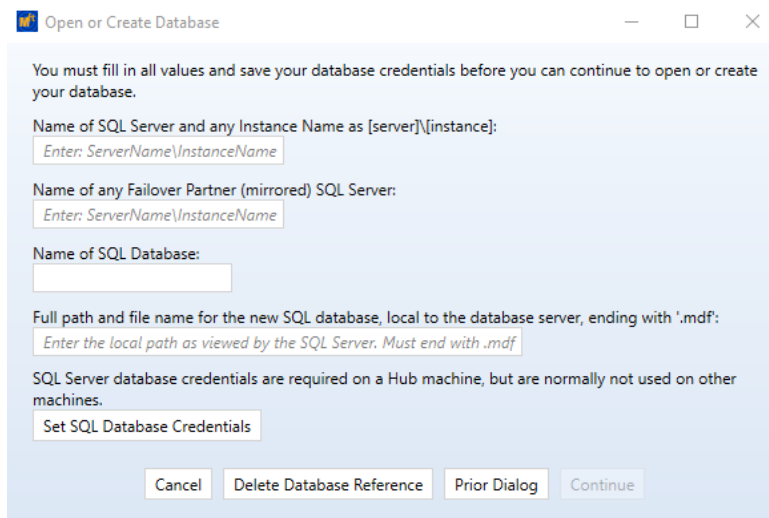
In this example, we will create the database using the wizard. The SQL account used must be a sysadmin in SQL. If you decide to create a blank database in SQL Management Studio first, you would use the 'Open an unlisted database' option instead.

Creating a SureSync MFT Database

On first launch of the SureSync MFT Desktop, you will be presented with the following prompt:

This panel is used to create the Hub database. To start the process, click the 'Create a new database' button.

Enter the following information to create the SureSync MFT database:

- **Name of the SQL Server and any Instance Name**: Enter the name of the SQL server and an instance name if used. For example, dev20\sqlexpress.
- **Name of any Failover Partner (mirrored) SQL Server**: This is an optional field that allows you to use a SQL Failover Partner. This functionality has been deprecated from SQL but is currently still available. Should be defined as machinename\instancename.
- **Name of SQL Database**: Enter the name of the SQL database that should be created.
- **Full path and file name of the new SQL database**: Enter the path on the SQL server where the database files should be created. This folder must already exist. For example, G:\Databases\SureSyncMFT.mdf.

Once the form is filled in, click on the 'Set SQL Database Credentials' button to provide the SQL user account to be used to create and access the database.

The fields that need to be filled out are:

- **SQL Server account name**: Enter the account name such as SQLAdmin.
- **Password/Repeat Password**: Enter the password for the account twice.

> By default the "Use the SQL Server account only for the Hub Service" option is checked. When in this mode, any Windows user accounts that will be accessing the MFT Desktop to make configuration changes must also have db_owner permissions granted so any configuration values defined can be saved to the database.
>
> If you uncheck that option, the SQL credential will be used for the MFT Desktop as well. This means if you are using the MFT Desktop from multiple machines to access the Hub database, you will need to provide that credential on the open database dialog and uncheck the "Use the SQL Server account only for the Hub service" option.

Click the 'Save' button to save the credential.

You will be returned to the main panel. Click the 'Continue' button to create the SureSync MFT database.

Configuring the Hub Communications Agent Credential

Once the database has been created, you will be prompted to provide a Windows credential for the Communications Agent on the Hub to use for accessing files. The following panel will be displayed:
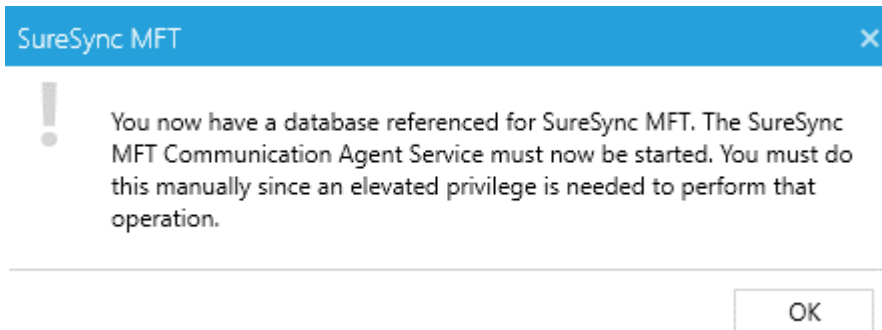

Enter the following information:

- **User Name**: Enter a valid Windows account in domain\user or machine\user format. This account will be used to access files that need to be processed by SureSync MFT if a root path exists on the Hub server.
- **Password/Repeat Password**: Enter the password for the account twice.

Optionally, you have some encryption options for the credentials. By default, a new self-signed certificate will be generated. You can also use your own certificate to encrypt the credential as long as that certificate is in the local certificate store.

Click the 'Save' button to save the credential.

The following dialog will be displayed:

SureSync MFT

You now have a database referenced for SureSync MFT. The SureSync MFT Communication Agent Service must now be started. You must do this manually since an elevated privilege is needed to perform that operation.

OK

To complete the SureSync MFT Hub configuration, launch the Windows Services MMC and start the Software Pursuits SureSync MFT Communications Agent service.

Importing a License

The installer includes a trial license. The included trial allows for 1 Hub, 5 Servers and 5 workstations. Larger trials can be arranged by calling our sales team at 1-800-367-4823.

If you have already purchased SureSync MFT licensing, the license should be imported into SureSync MFT Desktop.

To import a license, click the "Licenses" button ( ) in the ribbon bar of the SureSync MFT Desktop and click the "Import License…" button.

Configure the Additional Communications Agents

Before defining the data that should be processed by SureSync MFT, you want to add the computers that will be involved. To add a machine, expand the 'Computers and Volumes' section of the left-hand tree view in the SureSync MFT Desktop. Click on 'Servers' and then click the 'Computer' button in the ribbon bar.
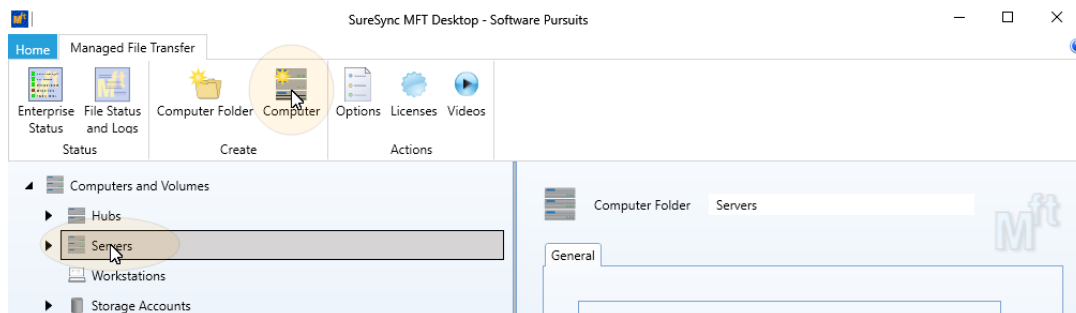
The 'Create Computer' wizard will be launched.

Define the Computer Name

The first panel is where you provide details about the name of the computer and the address needed to reach the computer. The following panel is displayed:

Please provide the following details:

- **Computer Name**: This field must contain the NetBIOS computer name of the computer you are adding. Duplicate computer names are not allowed in the same SureSync MFT environment. In the example above, we are adding the *SPITest-Win2K8* machine.
- **Default Access Name**: The Default Access Name is the DNS name or IP address that SureSync MFT will use to access this computer. If this field is left blank, the NetBIOS computer name will be used. If this does not resolve, you will want to enter a different IP address or DNS name here.

Click 'Next' to continue.

Define User Account and Other Details

The next panel allows you to enable actions to the Communications Agent, provide a credential and more.
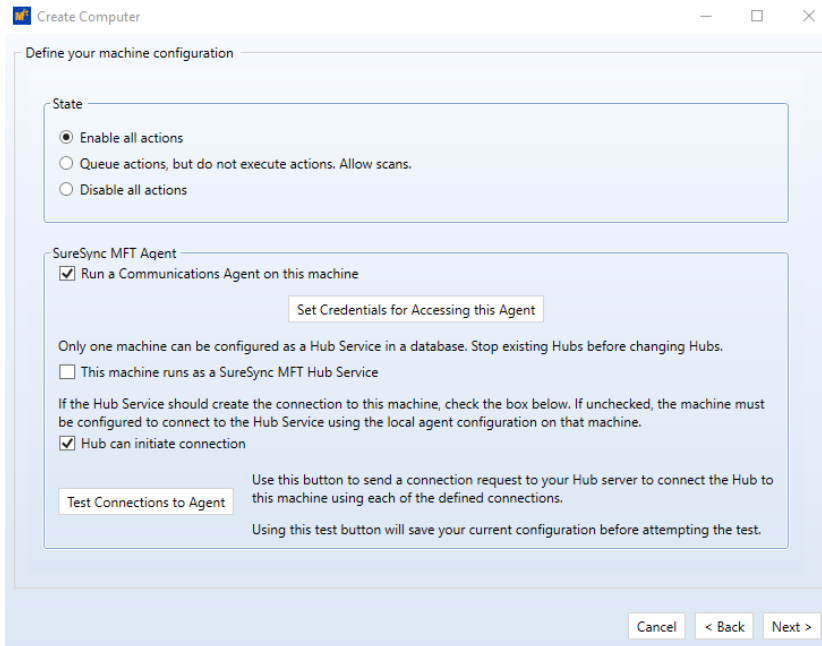
Each computer defined in SureSync MFT has a 'State' setting. This setting defines what type of processing should be performed on a computer wide basis. Similar settings are available for individual root paths.

The following options are available:

- **Enable all actions**: All actions on all root paths defined on this machine will be processed. This is the recommended setting.
- **Queue actions, but do not execute actions. Allow scans.**: Actions on all root paths defined in Jobs are queued to be processed. The actions will not be performed until the Status is changed to "enable all actions." This is useful when you want to build a backlog of actions to be performed later.
- **Disable all actions**: With this option enabled, no files will be processed on paths on this machine. This is true even in instances when a Job that includes a path on this machine is enabled.

For our example scenario, we accept the default 'Enable all actions' radio button.

The 'Run a Communications Agent on this machine' option is checked by default.

Click on the 'Set Credentials for Accessing this Machine' button. The following panel will launch:
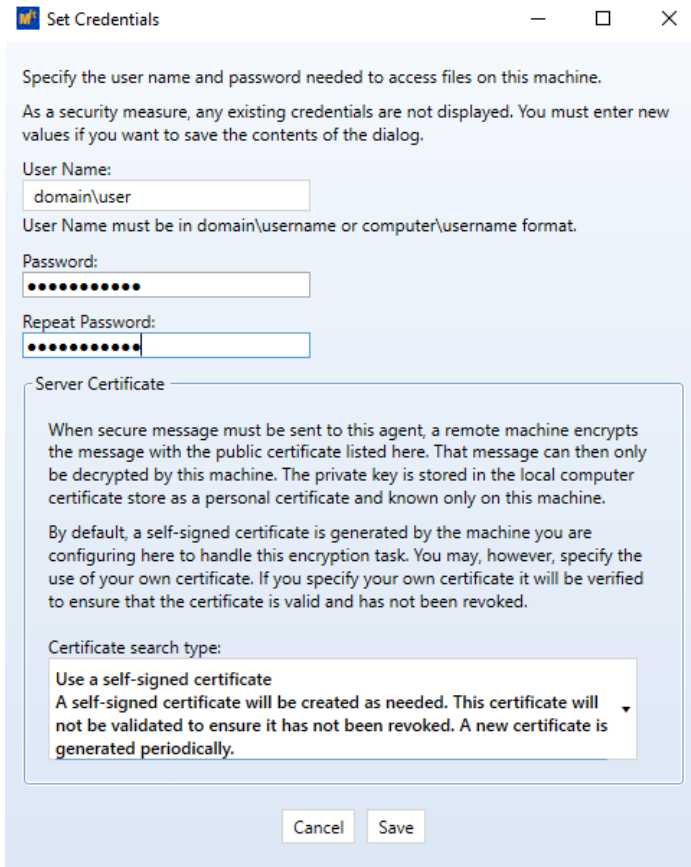
Enter the following information:

- **User Name**: Enter a valid Windows account in domain\user or machine\user format. This account will be used to access files that need to be processed by SureSync MFT.
- **Password/Repeat Password**: Enter the password for the account twice.

Optionally, you have some encryption options for the credentials. By default, a new self-signed certificate will be generated. You can also use your own certificate to encrypt the credential as long as that certificate is in the local certificate store.

Click the 'Save' button to save the credential.

Click the 'Next' button to continue and click the 'Finish Server' button on the final panel to save the computer configuration to the MFT database.

Repeat this process to add each computer you're planning to use in SureSync MFT. This step should be done before creating a Job any time a new computer is involved. The computers must be added first to appear in the Job wizard.

Creating the Jobs

Jobs are the basic building blocks of SureSync MFT. Each Job contains the root paths (source and destination paths) that apply to that Job and options for the Job. Each Job also contains one or more Rules that tell SureSync MFT how to replicate & synchronize data. The Job and Rule are created together in one wizard.

The Job and a default Rule are defined in one wizard. The default Rule processes all files in the root path(s). The Rule uses a mirror for one-way paths and a multi-mirror for multi-directional paths. The Rule can be altered using the SureSync MFT Desktop after creating it.

> The wizards are designed to quickly configure the basic options needed to get a Job configured. SureSync MFT is a flexible product with many advanced options. Additional options can be specified on the properties panels for the Job after it has been created.

Click on the Job button (Job) in the ribbon bar to launch the Job. The Job Wizard will be used to configure your Job.

Name Your Job

The first panel of the wizard allows you to name the Job and provide an optional description.

Since we want to use File Locking in this scenario, you should also check the 'Check if file locking is to be used for this Job' option.

Click the 'Next' button to continue.

Set Job Properties

The 'Set Job Properties' panel allows you to define options related to adjusting priority and scheduling. By default, all Jobs inherit a default "Always On" Interval Set that provides real-time processing of changes.
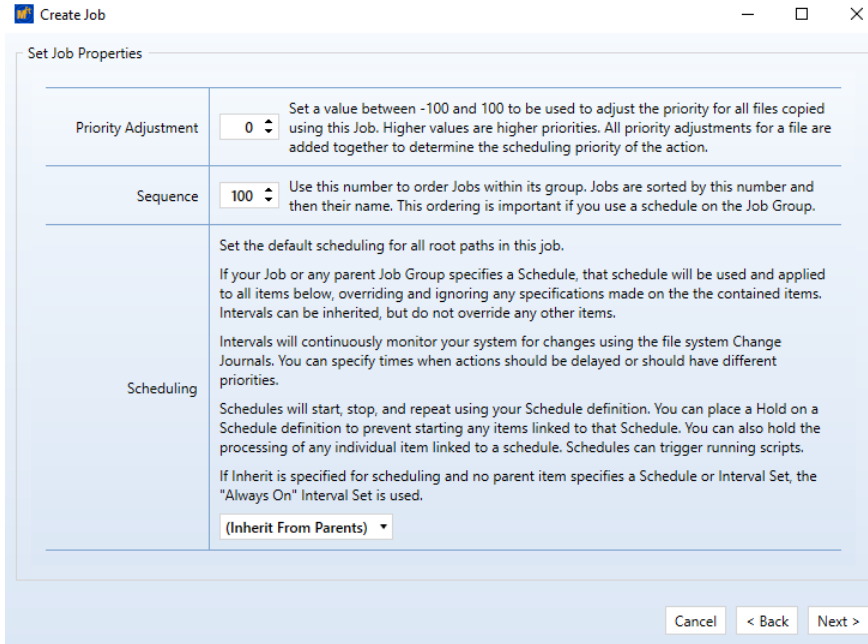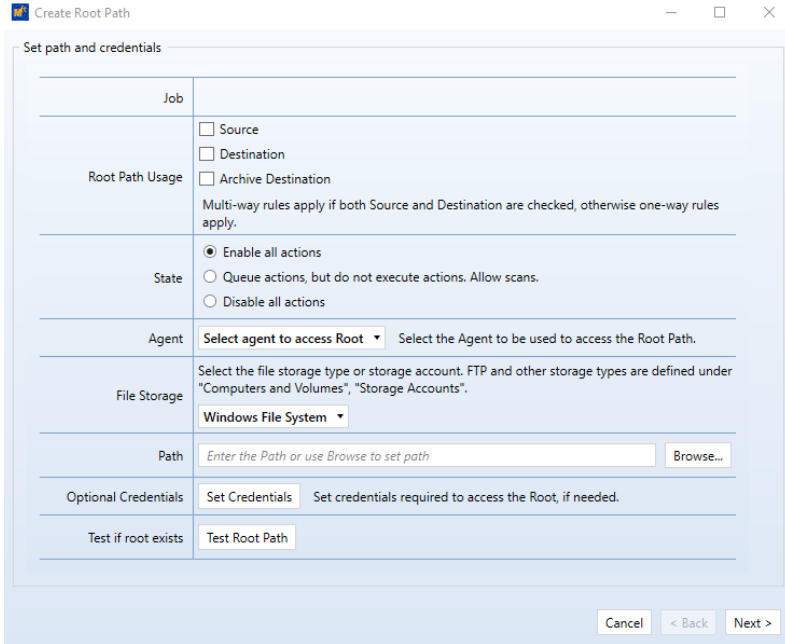
Click 'Next' to continue.

Add Your Root Paths

The 'Create Root Paths' panel is used to specify the paths that the Job should process files within. All of the paths involved, both source and destination, must be listed here.
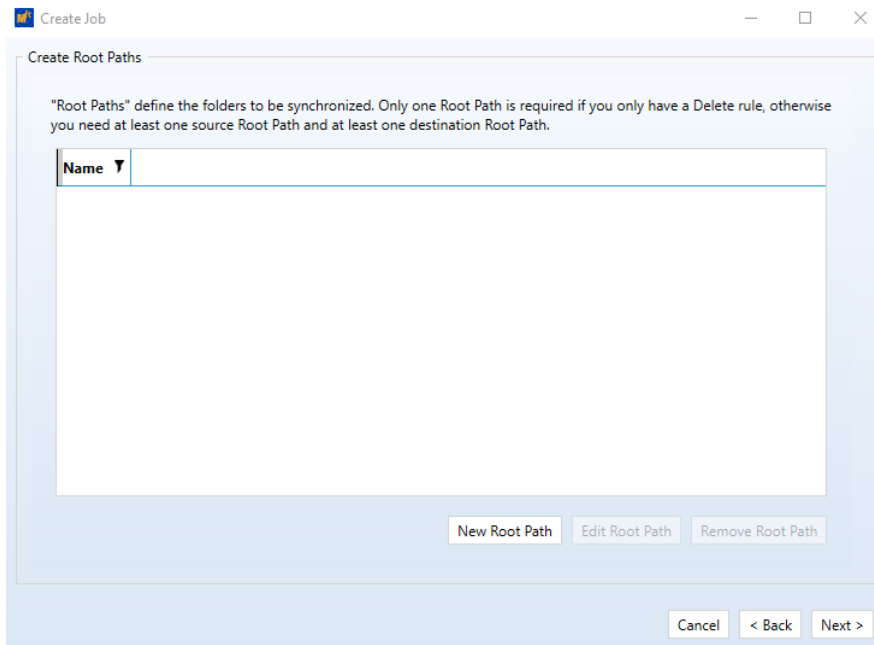

Click on the 'New Root Path' button to add your first Root Path. The following dialog will be displayed:

The 'Root Path Usage' of this panel provides a 'Source' and 'Destination' check box. A Root Path can be a source, destination or both (multi-directional Rules).

For this example, the paths will be C:\Documents on the *DEV20*, *SPITEST-WIN2K8* and *SPITEST-WIN2K12* machines.

A completed panel for a path would look like the following screenshot:
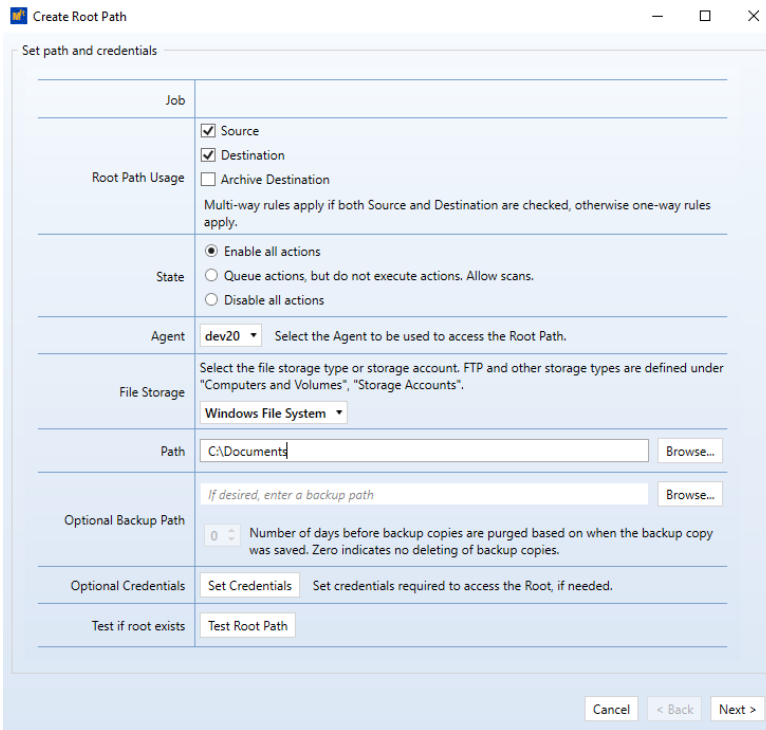
The following configuration options have been set:

- **Root Path Usage**: Since this is a multi-directional file locking Job, the 'Source' and 'Destination' checkboxes should be checked.
- **Agent**: For each path, you select the machine the path resides on from the 'Agent' drop-down.
- **Path**: Enter the path from the perspective of that machine as a local drive letter.

> In SureSync MFT, Root Paths are processed independently of one another. For example, you could have 3 paths processed with an Interval Set for real-time processing and a 4th path that was processed with a Schedule. The Scheduled path would only receive updated data on the defined clock basis. Locking is not available with Scheduled processing.
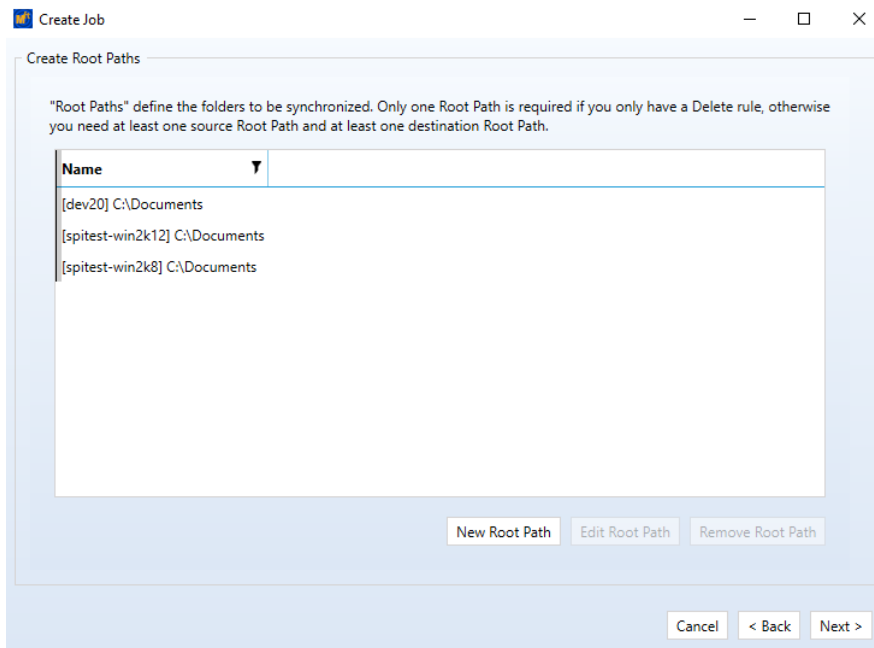
Click the 'Next' button to continue.
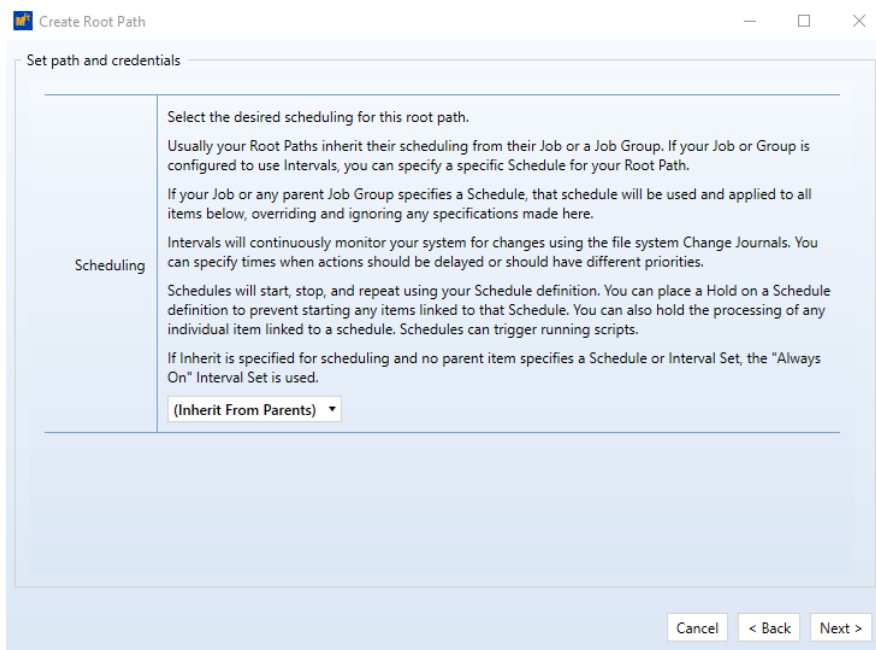
On the next panel, we will accept the defaults and click the 'Finish Root Path' button to add the path.
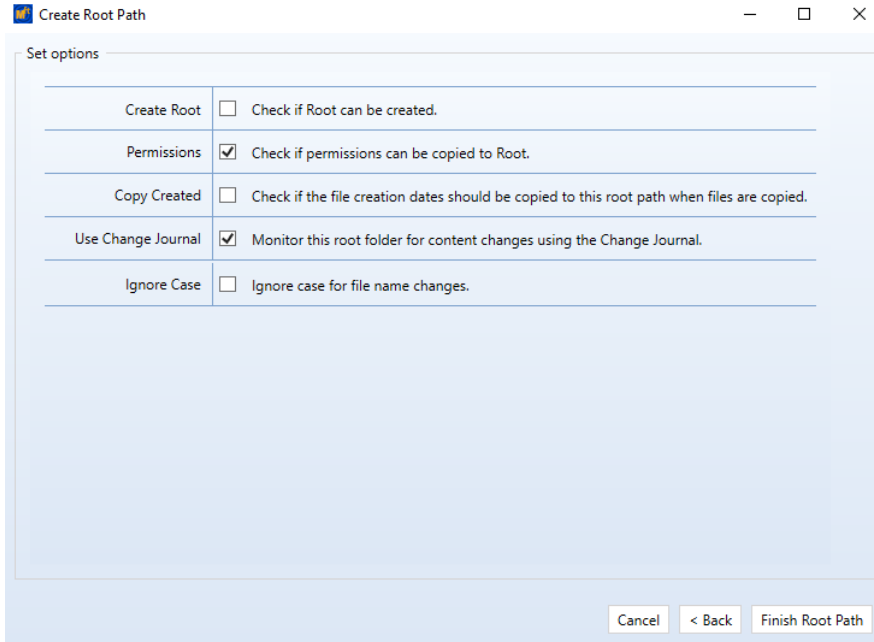
Repeat the process to add all of the root paths. Back on the 'Create Root Paths' panel of the 'Create Job' wizard, you should now have a panel that looks like this:

Click the 'Next' button to continue. Finally, click the 'Finish Job' button on the next panel to save the Job to the MFT database.

The wizards are designed to get the Job configured with a set of default options quickly and easily. If you want to enable advanced features such as NTFS Security copying or Advanced Open File Support (VSS), those can be enabled on the Rule Property Sheets

The Job will be saved in a disabled state, meaning no files will be processed. To enable processing, you must click on the Job in the SureSync MFT Desktop, select 'Enable All Actions' on the General tab of the Job and click the 'Apply' button.


Configuring E-mail Alerts

E-mail alerts are part of the Alert system within SureSync MFT and can be a useful way of notifying the administrator of a problem that should be investigated.

Configuring a SMTP Profile

To start the configuration of e-mail alerts, you should click on the Options (Options) button in the Ribbon bar. Click on the "Alerts" tab to access the appropriate configuration panel.

The first item configured is the SMTP Profile. The SMTP Profile provides SureSync MFT with the necessary details about your SMTP e-mail server so the program can send e-mail messages to you.
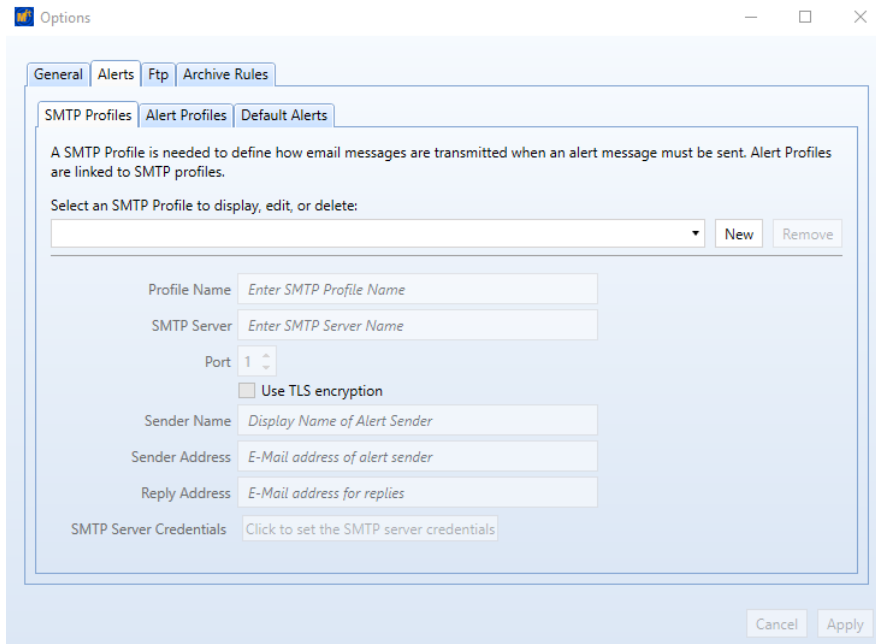
To create a SMTP Profile, click on the "New" button on the SMTP Profiles tab.

The following fields must be configured:

- **Profile Name:** The name of the profile that you are configuring. For example, you might use the name of the SMTP server.
- **SMTP Server:** The server address of the SMTP server. For example, smtp.mail.com.
- **Port:** The SMTP port for the SMTP server. The default SMTP port is 25.
- **Use TLS Encryption:** If your SMTP server requires encryption, check this box.
- **Sender Name:** The name that will appear in the From: field of messages sent by SureSync MFT.
- **Sender Address:** The e-mail address that will appear on messages sent by SureSync MFT.
- **Reply Address:** The reply address that will appear on messages sent by SureSync MFT.

You can also define SMTP Server Authentication settings if your SMTP server requires a valid logon to send messages (most do). To define a credential, click the 'Click to set the SMTP server credentials' button. The following fields will be presented:

- **User Name:** The username that SureSync MFT will log into this SMTP server with when sending an e-mail alert.
- **Password:** The password for the username defined in "User Name" should be entered here.
- **Repeat Password:** The password for the username defined in "User Name" should be confirmed here.

Click "Apply" to save the SMTP Profile.

Configuring an Alert Profile

The second part of configuring E-mail Alerts is to define an Alert Profile. The Alert Profile defines the e-mail address(es) that will be sent messages when errors occur. To configure an Alert Profile, click on the Alert Profiles tab and click the "New" button.
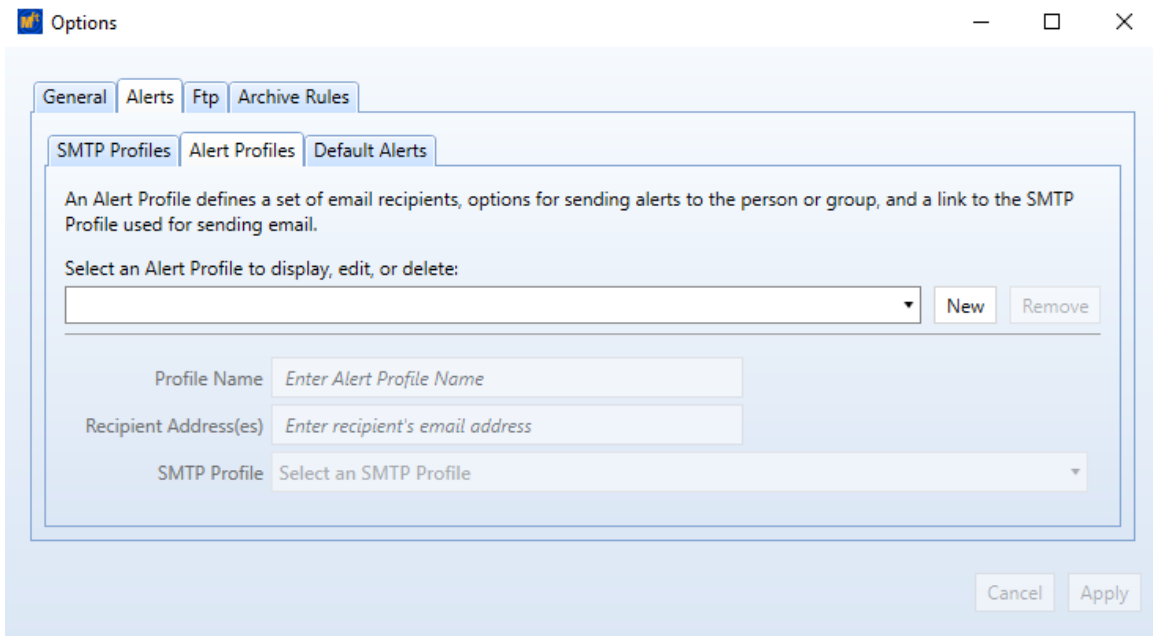
The following fields need to be configured:

- **Profile Name:** The name of the profile.
- **Recipient Address(es):** The e-mail address(es) that SureSync MFT will send the alert messages to.
- **SMTP Profile:** The SMTP profile that will be used to send the message.

> Multiple e-mail addresses can be added by separating the addresses with commas (,) or semi-colons (;). This allows you to easily send messages to a group of SureSync MFT administrators.

Configuring Alert Filters on the Job

The final step for receiving e-mail alerts is to define an Alert Filter on the Job. Expand the Job in question and click on the 'Alerts Filters' node on the left-hand tree view of the SureSync MFT Desktop as highlighted below.
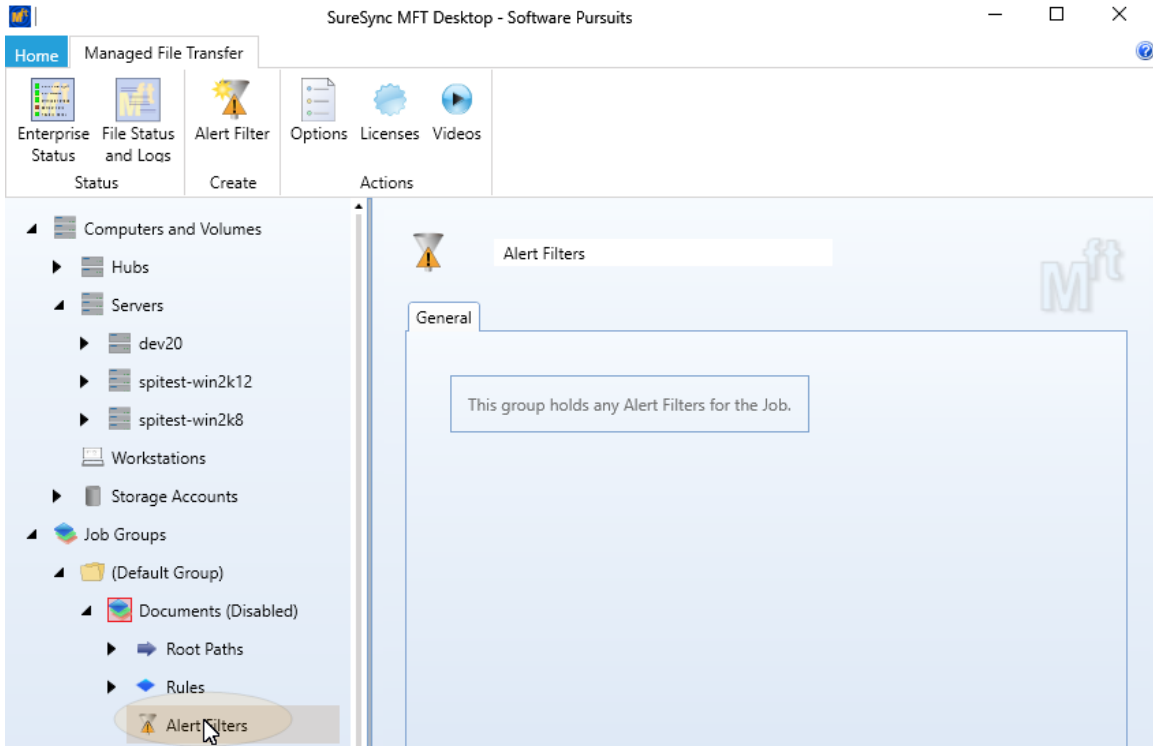
Click on the Alert Filters icon in the Ribbon Bar to launch the Alert Filters wizard
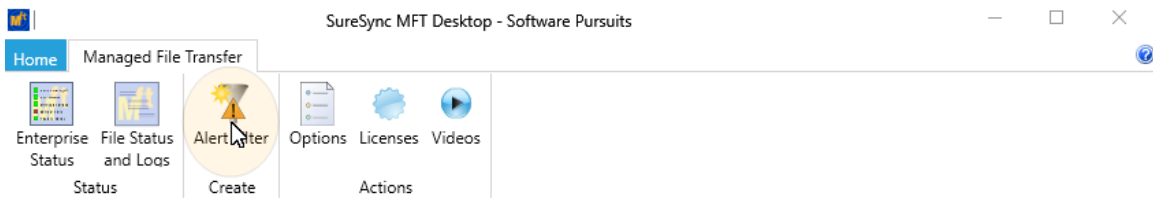
The 'Create Alert Filter' wizard will be loaded. The drop down allows you to select an existing Alert Profile or you can click the 'Create Alert Profile' button to create a new one.
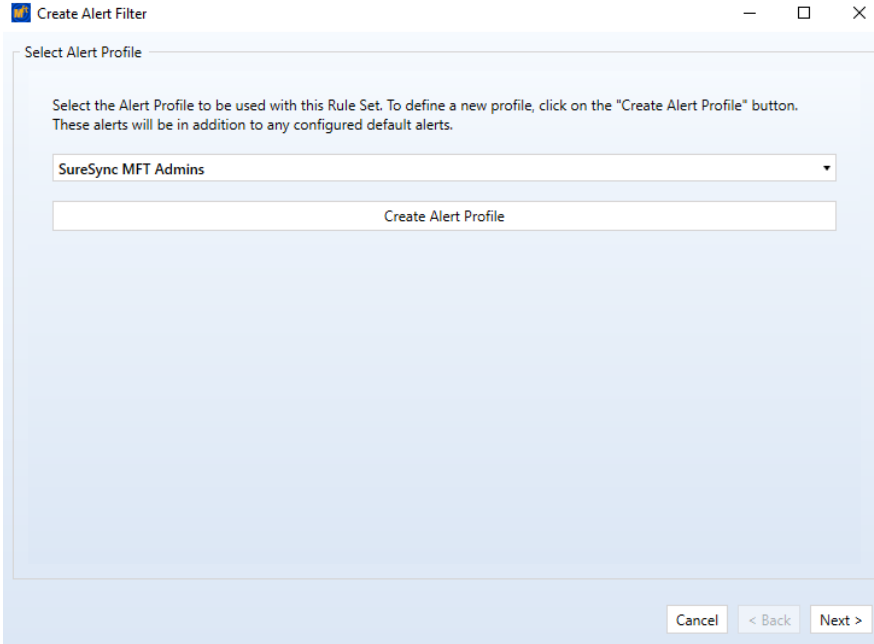
Select the appropriate Alert Profile from the drop-down and click the 'Next' button to continue.

> Alerts can also be defined globally to apply to all Jobs in the SureSync MFT database. This is done on the Alerts tab of Options by clicking on the 'Default Alerts' tab and defining an Alert Profile. This results in less configuration work but can produce substantially more alerts.
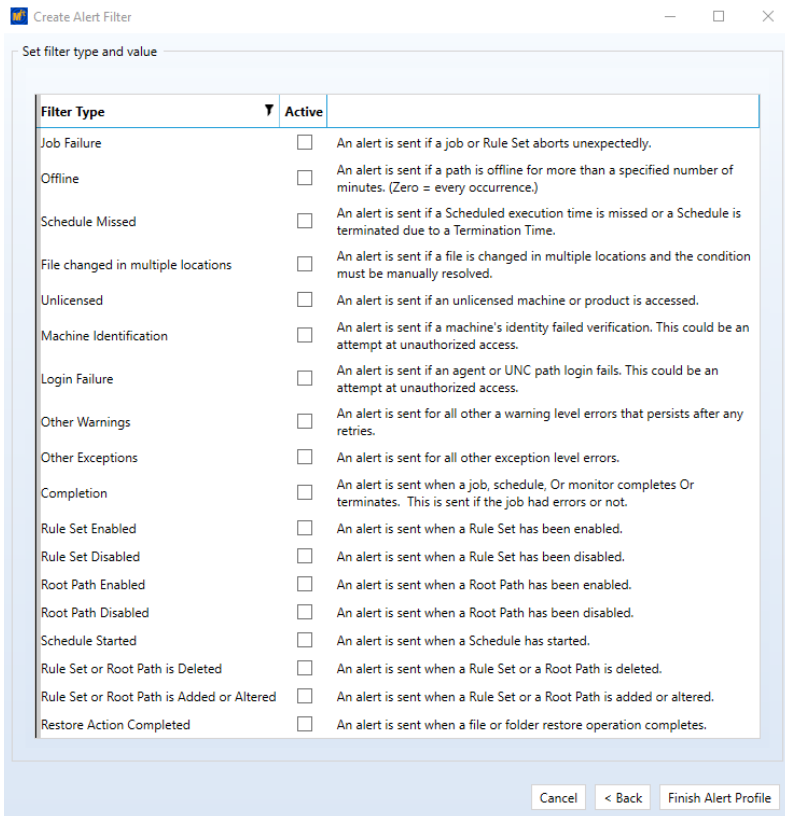
Check the alert types you would like to have an e-mail alert generated for and click the 'Finish Alert Profile' button to create the Alert Profile for the Job.

Monitoring the Environment

Monitoring your SureSync MFT Jobs is important, and this process is made easy by the various status panels.

Detailed Status

The Detailed Status panel will show you live file level activity for a selected Job. It also includes common counters such as files added and files deleted and details about the backlog of work to be performed.

To launch Detailed Status, click on the Job you would like to view status information about and

then click on the 'Detailed Status' button (Detail Status) in the Ribbon Bar.


Enterprise Status

The Enterprise Status panel provides a centralized view of all the SureSync MFT tasks in your environment, even when there are multiple Hub servers. This provides an easy way to stay current on the status of all your Jobs, no matter where they are running.

Enterprise Status can be launched by clicking on the "Enterprise Status" button ( ) in the Ribbon Bar in the SureSync MFT Desktop.
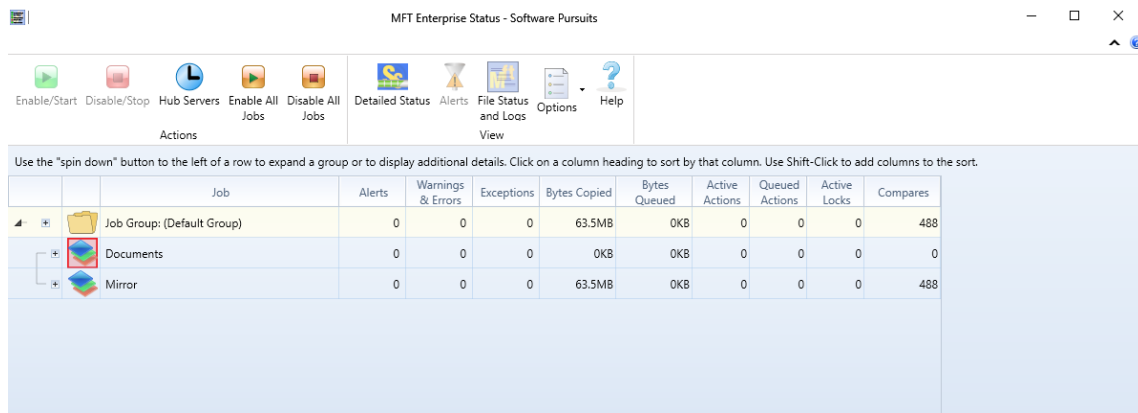
File Status

The File Status panel provides status about current and pending activity from a number of different perspectives. This panel can be extremely helpful when you want to determine how much work remains to bring folders on the various machines in the environment current.

In addition, File Status provides the ability to review Action Logs and process Alerts.

Details on how to use each tab of File Status can be accessed by pressing F1 on the appropriate tab to access context sensitive help.