LockStatus Evaluator's Guide

Table of Contents

Introduction

LockStatus helps to make the file locking process more transparent to the users on your network. This program is included with your SureSync MFT license.

When a user attempts to open a file that is locked by another user, the LockStatus tray application will display a pop-up message informing the user that they have been blocked from accessing the file. The notification will also tell the user who has the file locked. LockStatus will also notify the user when the file has been closed so they can attempt to gain access to a writable copy of the file.

LockStatus helps minimize end user confusion when file locking is deployed in your environment. Without LockStatus your users will see different behaviors depending on the application. For example, the user will see the text "Read-Only" added to the title bar of a Word document. This notification, in many cases, is not clear enough to avoid confusion about why the user is unable to change a file.

This Evaluator's Guide is designed to walk you through the initial setup of LockStatus. To use LockStatus, you must have SureSync MFT installed and configured. Please review the SureSync MFT Evaluator's Guide for more information about completing that part of the configuration.

System Requirements

LockStatus' 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.

Required Microsoft Components

LockStatus requires several Microsoft components to be installed. The LockStatus installer will detect the versions your system is running and offer to upgrade them as needed. These components are needed on both the server and client machines.

- Microsoft .NET Framework 4.8

Contact Information

If you need further information about LockStatus or need clarification on anything within this guide, please contact our support group and they will be happy to assist you.

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.

LockStatus Architecture

LockStatus is a tray application that interacts with SureSync MFT to provide file locking notification to users. Understanding the names of the LockStatus and SureSync MFT components, where they are installed and what they do is essential to deploying LockStatus successfully.

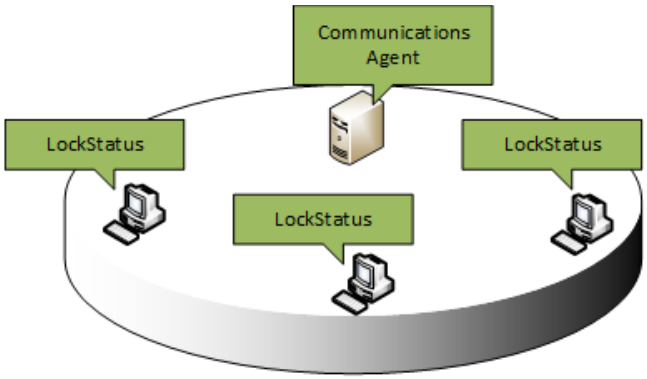
- **Software Pursuits Communications Agent**: The Communications Agent is the service within MFT responsible for providing communications, I/O functionality, and other features. This service includes the necessary functionality to support LockStatus right out of the box.
- **LockStatus**: LockStatus is the client application installed on each user's workstation. This application resides in the system tray and provides pop-up notification when the user encounters a locked file or when a previously locked file becomes available.
- **Hub**: The Hub service is the "brain" of the MFT environment. Generally, one server in an environment is defined as the Hub. This is the machine that provides the locking status information for LockStatus.

The server-side components of LockStatus are completely integrated into MFT. This provides significant benefit because you are likely to have the required Communications Agent already present in each office or subnet due to the MFT deployment already being in place. With a few minor configuration tweaks, LockStatus can be added.

A few example scenarios will help clarify aspects of the LockStatus architecture.

Deployment on a Single Subnet

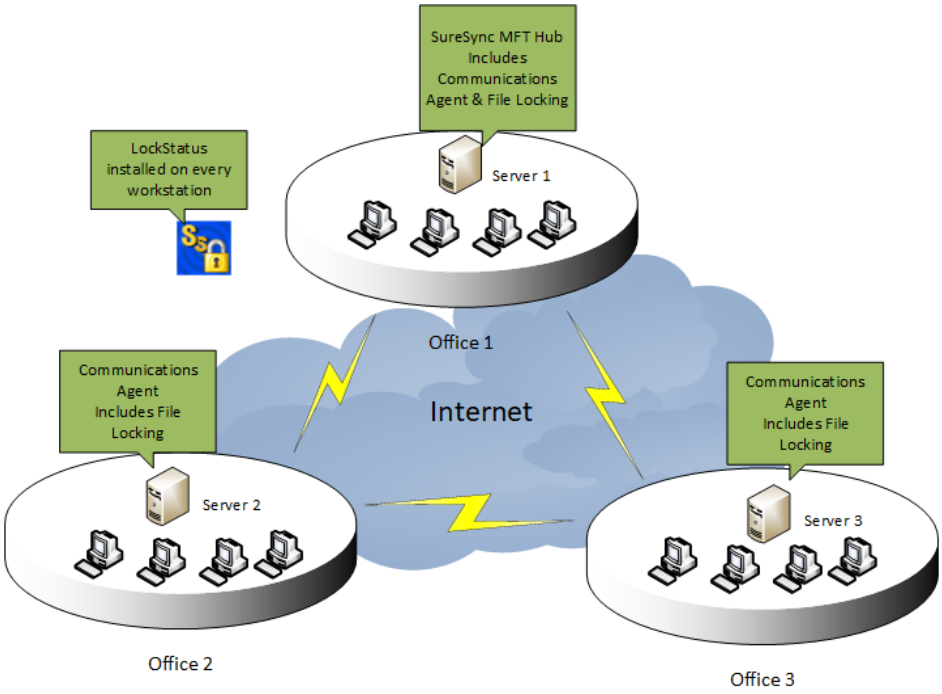
The graphic below represents a standard deployment of LockStatus on a subnet in a network. The Communications Agent is installed on a server and LockStatus on each workstation. The Communications Agent service is included on the Hub.



In small deployments such as the example above, LockStatus deployment is simple and can be implemented quickly. More complex network environments require some planning as discussed in the next section.

Deployment in a Complex Network Environment

Many network environments consist of multiple offices and/or subnets that require file locking status for users. Consider the following network:



In this scenario, a company has three servers in three offices. These servers are participating in a multi-way real-time Job with file locking enabled. Each office also has workstations that need to receive locking notification.

When working in complex network environments, some planning is required to ensure a smooth deployment. Keep in mind the following setup requirements:

#1: Name Resolution

Each remote Communications Agent needs to be able to connect to the Hub machine. In the example network, the Hub is running on Server 1. Server 2 and Server 3 need to be able to connect to Server 1 to retrieve file locking status.

A public IP address or DNS name is required to allow name resolution over a public network like the Internet. This IP address or DNS name must be resolvable to Server 1. Server 2 and Server 3 will be configured to use that IP address or DNS name to make a connection with Server 1.

#2: Firewalls

Using the scenario above, LockStatus requires that Server 2 and Server 3 can initiate a connection to Server 1 to retrieve locking status information. The firewall at Office 1 must be configured with a port forward or NAT rule to forward TCP port 7033 to the Server1 machine (if you're using the default port). This rule will allow requests coming to the selected public IP or DNS from Server 2 and Server 3 to be forwarded to Server 1 properly. Please consult the documentation for your firewalls to make these configuration changes.

LockStatus Deployment Methods

LockStatus can be deployed in three different ways:

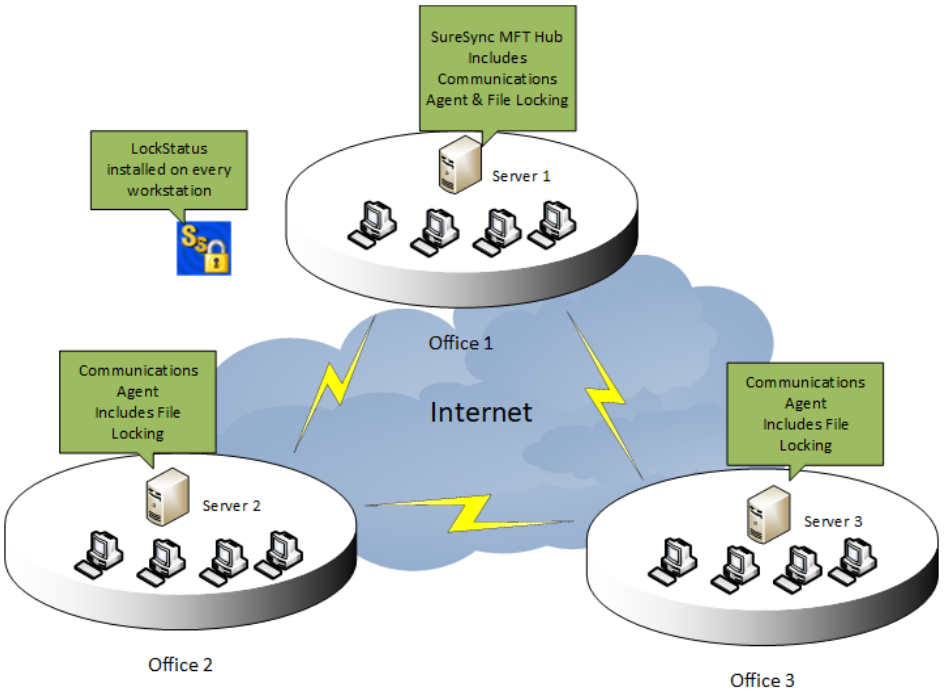
- Using auto discovery (recommended when possible)
- Manual configuration on each workstation
- Command line switch configuration retrieval during installation

This guide will cover all three methods of deployment. You only need to review the section for the deployment method you have selected.

Deployment via Autodiscovery

Autodiscovery results in the smallest amount of configuration on the individual workstations. By default, a broadcast is issued when a LockStatus client launches that attempts to locate a Communications Agent. If a Communications Agent exists on the same subnet that has been configured to respond to these requests, LockStatus will receive a reply containing the configuration information necessary to complete the connection.

In environments with a single subnet, this deployment method is extremely quick and easy. In environments with multiple subnets, some planning is necessary to ensure a Communications Agent exists in each subnet that includes workstations requiring locking status. We will consider a deployment strategy for the network environment mentioned earlier in this guide. To review:



The basic steps for this type of deployment will be:

- Identify a public IP or DNS name to use for LockStatus. This will be used for remote offices (Office 2 and Office 3 in this scenario) to retrieve lock status information from the main SureSync MFT installation.
- Configure firewalls as necessary to allow the required connections.
- Configure an Outbound Connection on each remote Communications Agent that defines how to connect back to SureSync MFT Hub server.
- Configure each Communications Agent to respond to autodiscovery requests from the LockStatus clients.
- Publish the configuration changes to the remote Communications Agent machines.
- Deploy LockStatus to the client machines.

Step 1: Identify a Public IP or DNS Name for use with LockStatus

Identify a public IP address or DNS name that can be used for the remote Communications Agent machines to reach the Hub. Note this IP address or DNS name before proceeding.

Step 2: Configure firewalls to allow the connections

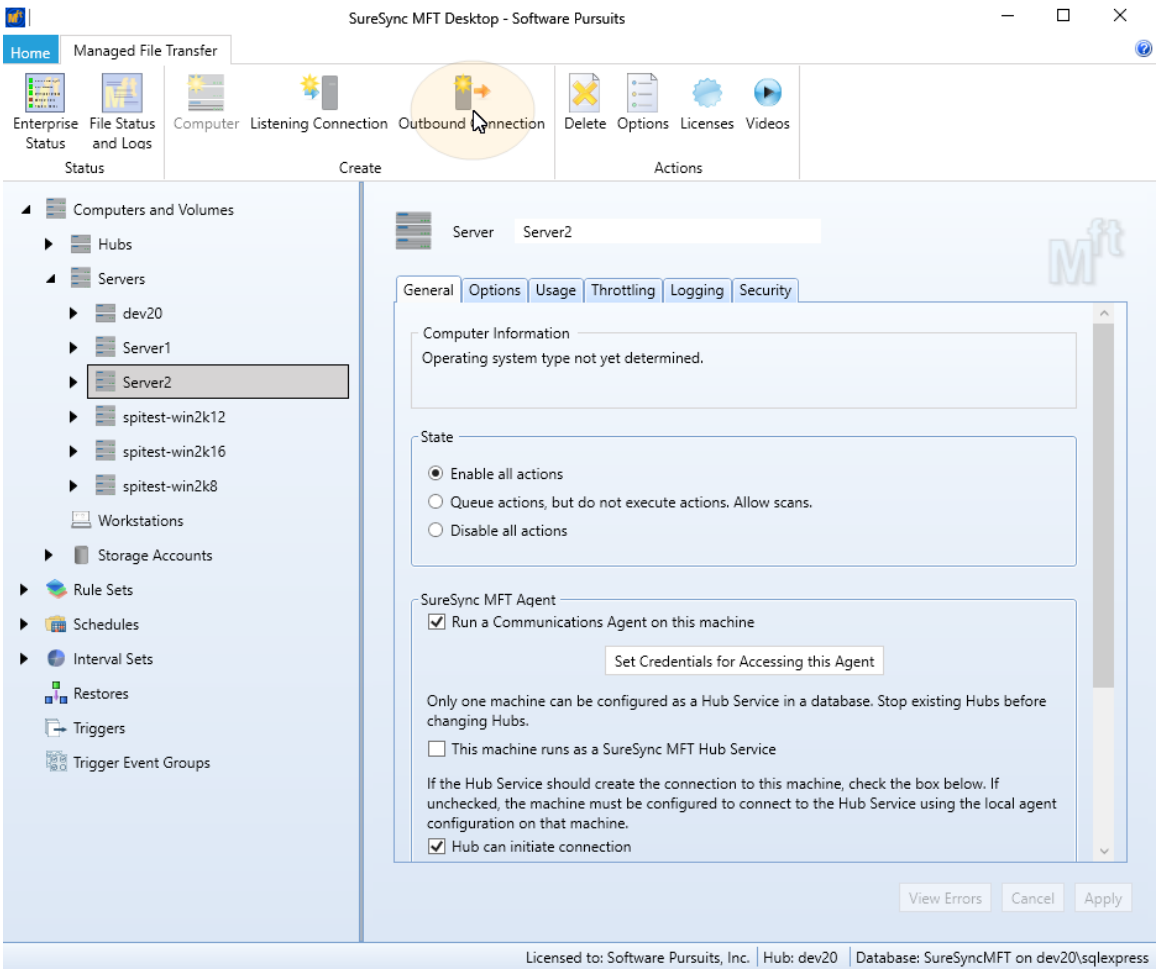
Make any firewall configuration changes necessary to allow the traffic through to the Hub. Often these rules will be referred to as Port Forwarding or NAT rules within the firewall. By default, the port that needs to be forwarded is TCP 7033. Please refer to the documentation for your firewall for further information.

Step 3: Configure an Outbound Connection for Remote Agent(s)

An Outbound Connection must be configured for each remote Communications Agent that will provide connection information to LockStatus clients. This Outbound Connection provides the IP

address or DNS name identified in step 2 that clients can use to reach the Hub. In this guide's scenario, an Outbound Connection is needed for Server 2 and Server 3.

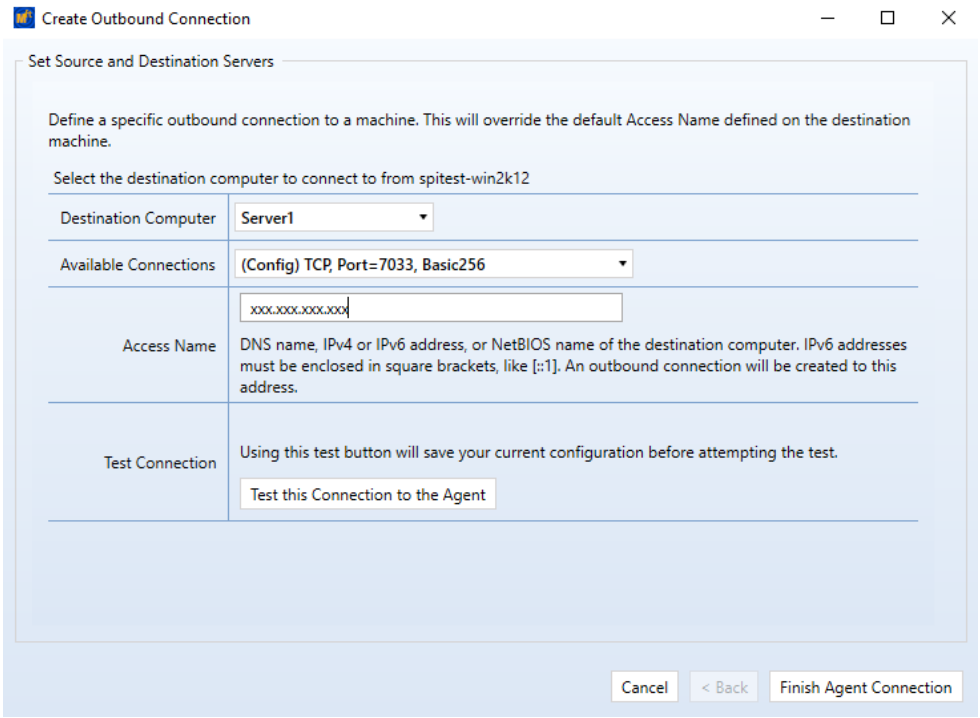
To define an Outbound Connection, expand Computers in the left tree of the SureSync MFT Desktop and click on the machine you would like to add the Outbound Connection to. Click on the "Outbound Connection" button in the Ribbon Bar



On the wizard that appears, you will configure three options:

- **Destination Server:** The machine the Outbound Connection is intended to reach is defined here by selecting it from the drop-down menu.
- **Available Connections:** All LockStatus messaging is done over the (Config) connection. From the 'Available Connections' drop-down, select the option in the drop-down with (Config) in the name.
- **Destination Server Access Name:** Enter the public IP address or DNS name that can be used to reach the SureSync MFT Hub machine.

The completed panel will look like:



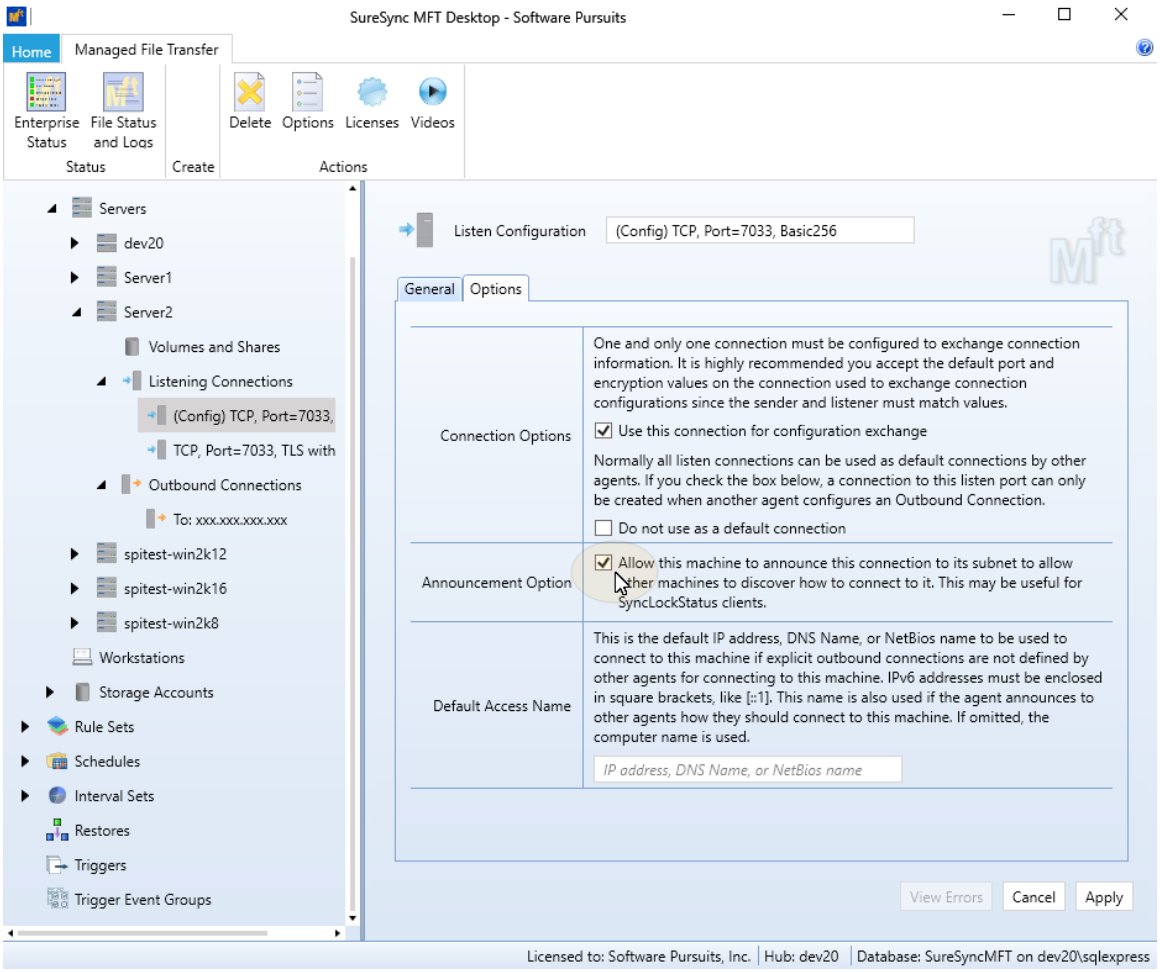
Click the 'Finish Agent Connection' button to add the Outbound Connection.

Step 4: Configure Agent(s) to respond to auto-discovery requests

Each remote Communications Agent machine that will respond to auto-discovery requests from LockStatus must be configured to do so.

To complete this step, expand the machine in question under the Computers node of the left tree view of the SureSync MFT Desktop. Expand "Listen Configurations." By default, you will see two connections. Click on the Listen Configuration starting with (Config) and click on the 'Options' tab.

Check the 'Allow this machine to announce this connection to its subnet to allow other machines to discover how to connect to it" option as shown below.



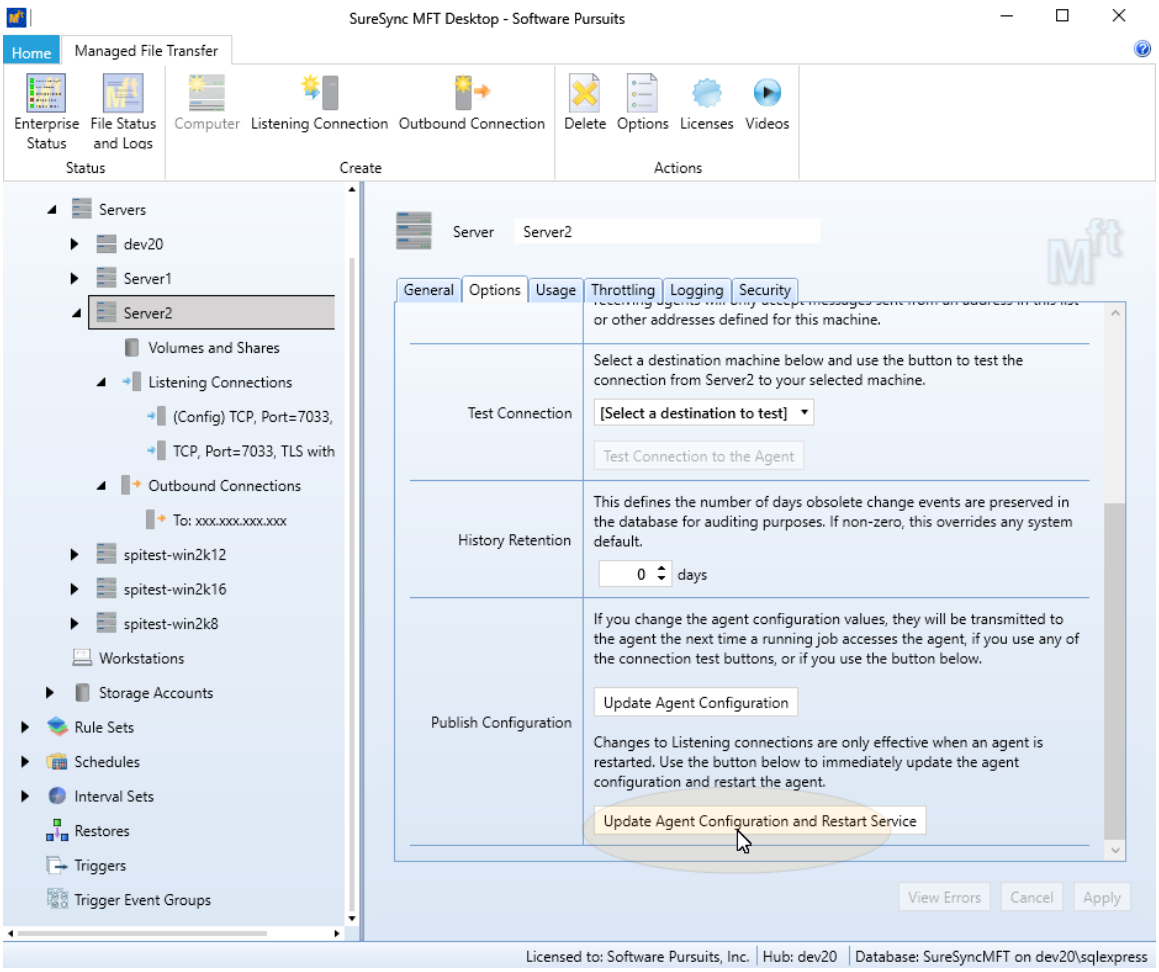
Click the “Apply” button to save the change.

Step 5: Publish configuration information to remote Communications Agent(s)

The next step involves publishing the configuration information to each remote Communications Agent machine.

In the SureSync MFT Desktop, go to the Computers node of the left tree view. Click on the machine you want to publish configuration information to. For example, Server2.

On the Options tab, click the ‘Update Agent Configuration and Restart Service’ button. This will publish the configuration file and cycle the Communications Agent service, so the settings become active. If you have any Jobs actively running to that machine you will encounter path losses while the restart occurs.



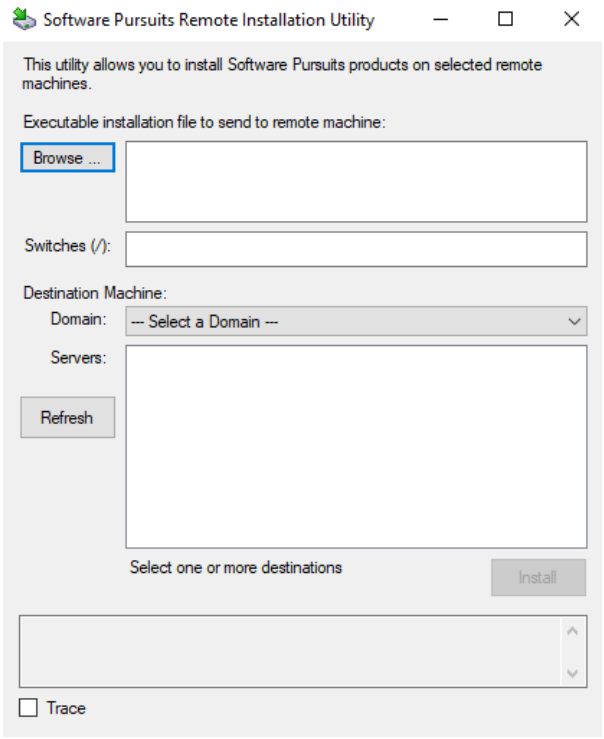
Step 6: Install LockStatus clients on the workstations

The final step of an autodiscovery deployment is to install the LockStatus client on the workstations. There are multiple ways to accomplish this task.

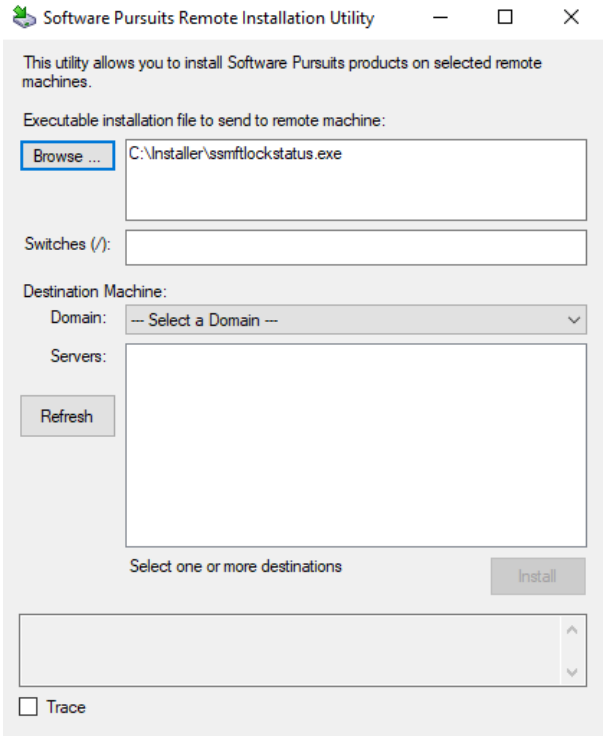
- Install on each client manually
- Use the Software Pursuits Remote Installation Utility
- Use a third party install management application

This document will show you how to use the Software Pursuits Remote Installation Utility.

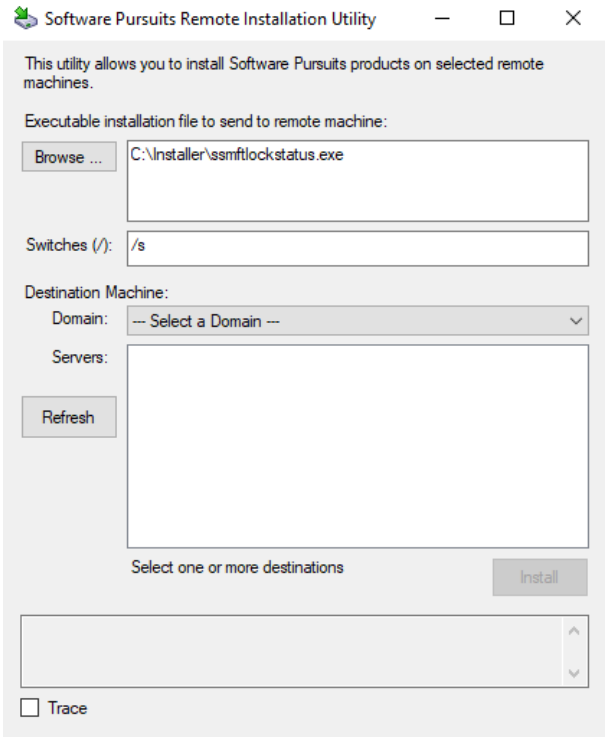
Go to the Start menu, select All Programs, SureSync MFT and select Remote Installation Utility. The Software Pursuits Remote Installation Utility will launch. You should see a program window that looks like the screenshot below.



Click the “Browse” button and select the ssmftlockstatus.exe setup file or manually type the path to the file into the “Executable installation file to send to remote machine” field.

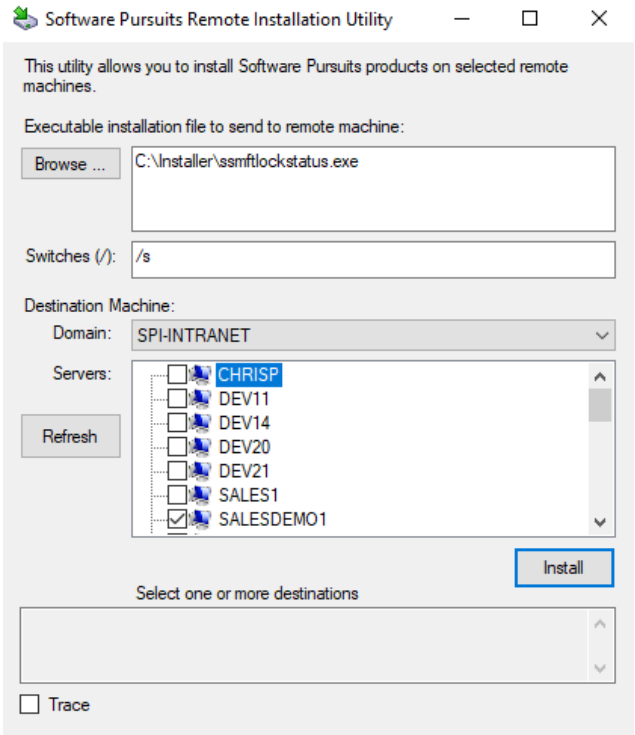


To install the LockStatus components silently, you should enter */S* in the “Switches” field. The */S* sets the installer to silent mode.



Click on the “Domain” drop-down and select the domain where the workstation(s) you want to install LockStatus on reside.

From the list that displays, check the machines where you want to install the LockStatus client application. Click the ‘Install’ button to perform the installation on the selected workstations.



Deployment via Manual Configuration

Deployment via manual configuration is only recommended in small environments with a limited number of workstations. When deploying LockStatus manually, the administrator must install and configure the LockStatus client software on each workstation requiring status notification.

Configuring the Server Side

With manual deployment, there is no server-side configuration since each LockStatus client will be configured with details for reaching the Hub machine.

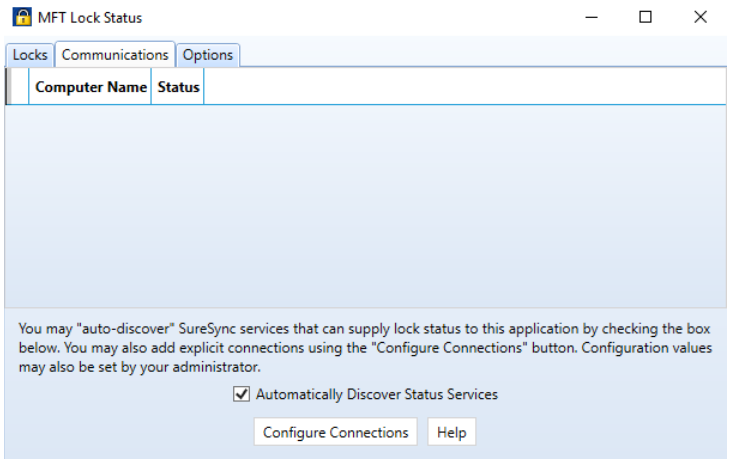
Configuring the Client Side

Step 1: Install the LockStatus client on the appropriate workstation(s)

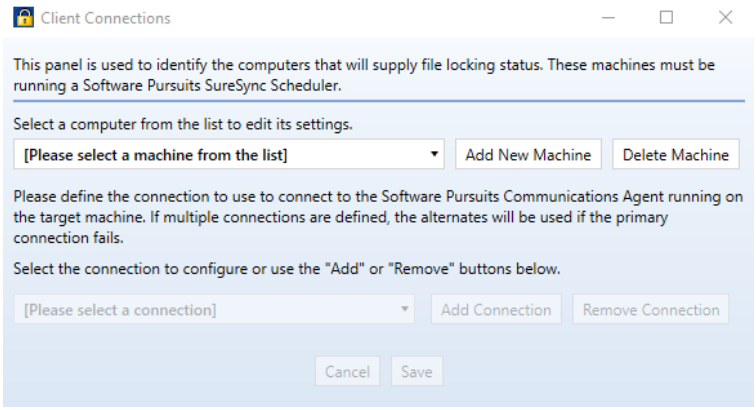
The LockStatus client software is installed by launching the ssmftlockstatus.exe installer. Follow the prompts to complete the installation and then launch LockStatus.

Step 2: Configure LockStatus to retrieve lock information from SureSync MFT

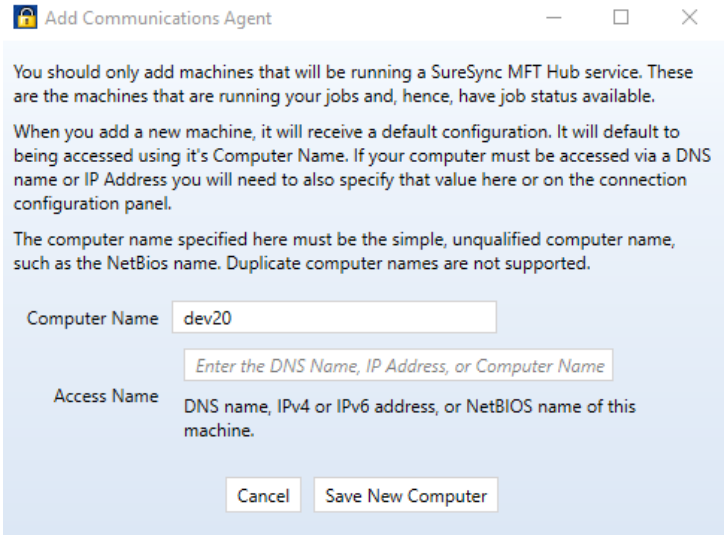
The next step involves defining the connection that should be used to retrieve lock status information. To do this, double click on the LockStatus tray icon and then click on the Communications tab. You can also right click on the same icon and select Servers from the menu. The following panel will be displayed:



Click on the “Configure Connections” button and the following panel will be displayed:



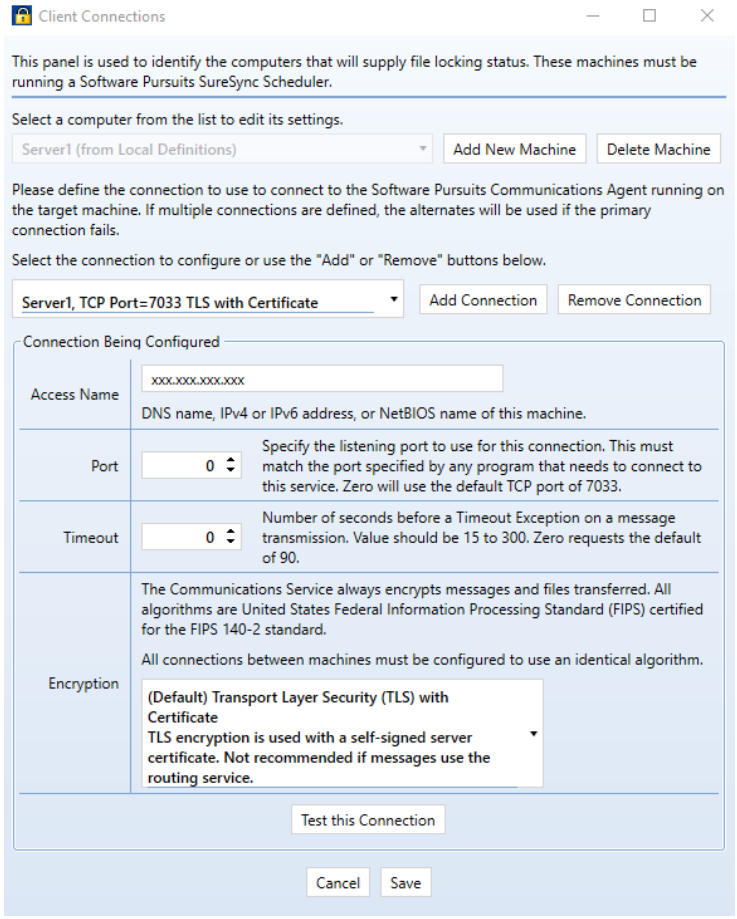
Click the “Add New Machine” button.



In the dialog that displays, you will enter the computer name of the SureSync MFT Hub. The ‘Access Name’ field is important. If the Hub is not accessible via NetBIOS name, you must enter an IP address or public DNS name that will allow the LockStatus client to communicate with the MFT Hub.

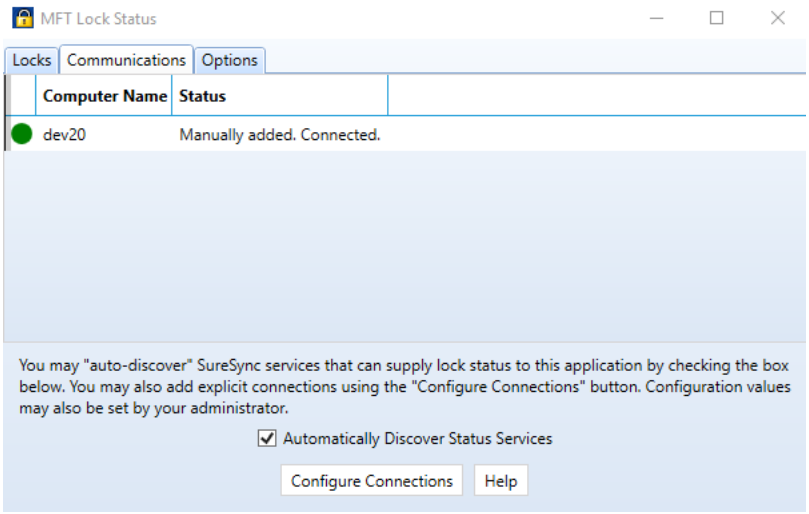
When you add a Communications Agent to LockStatus, a default connection is created. This connection uses TCP port 7033. We strongly recommend using this port whenever possible as it reduces configuration.

After clicking the “Save New Computer” button you will be brought back to the main configuration panel that will now show your newly created connection.



You can click the “Test this Connection” button. Finally, click the “Save” button to save the configuration. You can then click the “X” in the upper right corner to close the panel.

You should now see an active connection, as shown below:



You’re done, LockStatus is ready to be used! These steps should be repeated for each machine requiring LockStatus notification.

Deployment via Command Line Switch Configuration Retrieval

In some environments, administrators do not want autodiscover broadcasts on their networks. Deploying LockStatus with a manual configuration addresses this issue. In large environments the overhead of configuring LockStatus on each workstation is problematic. The LockStatus client can be installed with a command line switch that allows retrieval of a configuration file from a network share. This method helps reduce the amount of configuration effort needed for manual configuration.

Configure the First LockStatus Client

The LockStatus configuration is stored in an XML file and read when the program loads.

Follow the steps in the "Deployment via Manual Configuration" section of this document. This will create the XML file that will be used by the remaining LockStatus clients.

Create a Network Share to Store the Configuration File

Step 1: Select a Server to Store the Configuration File

A server must be selected to store the template configuration file. This server must be in a location accessible via UNC path by the client machines.

Step 2: Configure the Share

Using Windows Explorer create a folder on the server that will store the configuration file. Configure this folder to have a share with appropriate permissions for the client machine's users to read the file within the share.

Step 3: Copy the Configuration File to the Share

On the machine where you configured LockStatus, browse to the following folder:

- **Windows Vista / 2008 and Newer**: C:\Users\Public\Software Pursuits\SureSync MFT1
- **Windows XP / 2003**: C:\Documents and Settings\All Users\Application Data\Software Pursuits\SureSync MFT1

This folder contains a file named MFTLockStatus.xml. This file contains the LockStatus configuration completed earlier. Copy this file to the network share.

Install LockStatus on the Client Machines

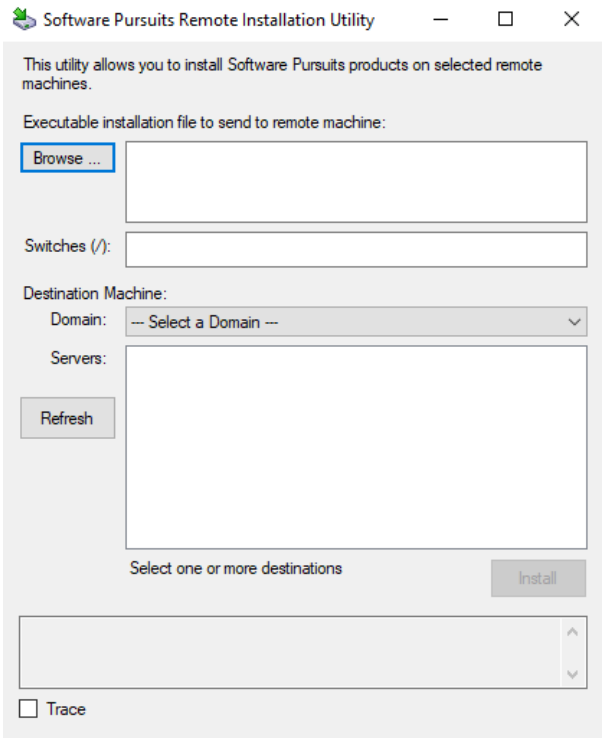
The final step to deploying LockStatus involves executing the installer with a command line switch that provides the UNC path to load the configuration from. There are several different ways you can accomplish this task.

- Install on each client manually using the /XMLPath switch from a Run dialog. For example: "C:\Installers\ssmftlockstatus.exe" /XMLPath="\\server\share"
- Use the Software Pursuits Remote Installation Utility
- Use a third party install management application if it supports installation using command line switches

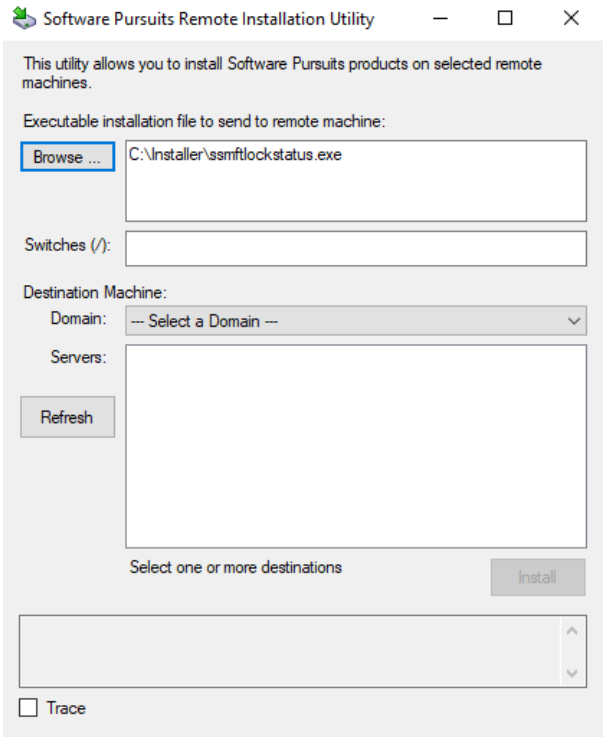
The /XMLPath switch tells the installer to generate a registry entry on the client machine with the UNC path to the location where the configuration file can be found. When the LockStatus client loads, the registry key is read, and the configuration file is applied to the software.

This document will show you how to use the Software Pursuits' Remote Installation Utility.

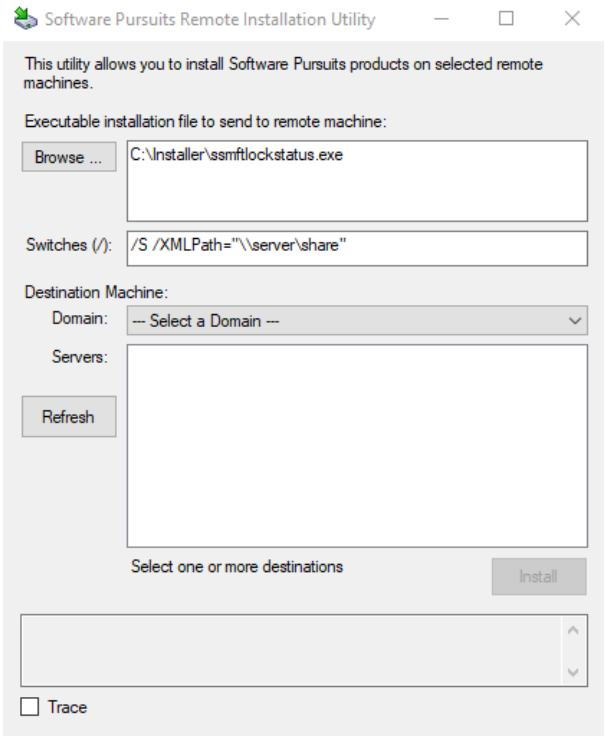
Go to the Start menu, select All Programs, SureSync MFT and select Software Pursuits Remote Installation Utility. The Software Pursuits Remote Installation Utility will launch. You should see a program window that looks like the screenshot below.



Click the "Browse" button and select the Ssmftlockstatus.exe setup file or manually type the path to the file into the "Executable installation file on local machine" field.

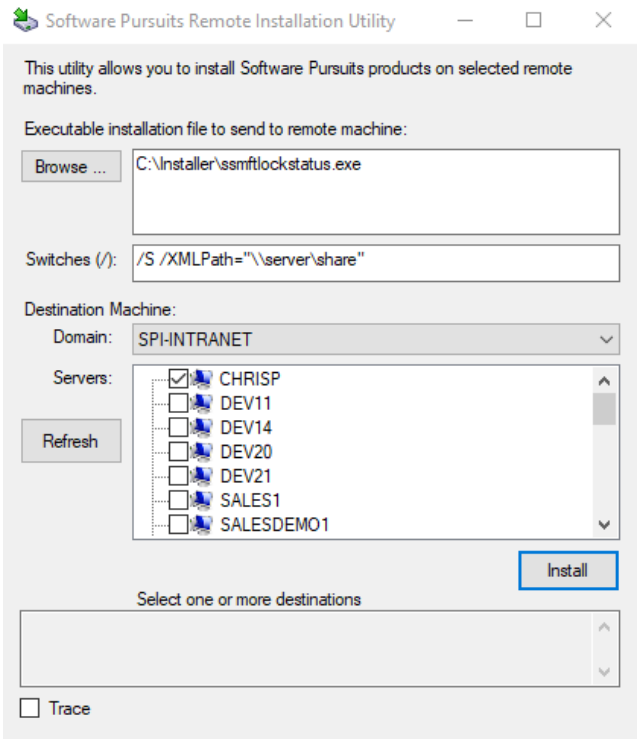


To install the LockStatus components silently, you should enter */S and /XMLPath="\\server\share"* in the "Switches" field. The */S* sets the installer to silent mode. The /XMLPath= switch tells the installer where to locate the configuration file.



Click on the "Domain" drop-down and select the domain where the workstation(s) you want to install LockStatus on reside.

From the list that displays, check the machines where you want to install the LockStatus client application. Click the ‘Install’ button to perform the installation on the selected workstations.



When the LockStatus clients launch, they will now retrieve the appropriate configuration details and connect to the Hub to retrieve lock status information.