SyncLockStatus
Evaluator's Guide

Table of Contents

Introduction

SyncLockStatus is an Add-on to SureSync's Collaboration Edition (SureSync with the SPIAgent and SPIAgent File Locking Add-on licenses) that makes the file locking process more transparent to end users on your network. This is accomplished through the installation of a server application that will transmit lock status information to client machines; an application installed on each client machine will receive the lock status information. When an end user attempts to open a file which is locked by another user, the workstation application will display a pop-up message from the system tray informing the user that they have been blocked from accessing the file and informing them of the user that has the file locked. In addition, the application 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.

SyncLockStatus makes the Collaboration Edition of SureSync even more valuable by eliminating confusion from end users when file locking is deployed in your environment. Without SyncLockStatus your end users will see different behaviors depending on the application installed. For example, the user might not see an error message but just 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. Eliminating this confusion represents a significant value add to your collaboration environment.

This Evaluator's Guide is designed to walk you through the initial setup of the SyncLockStatus product. To use the SyncLockStatus application, you must have SureSync installed in your environment and configured to use SPIAgent File Locking. Please review the SureSync with SPIAgent File Locking Evaluator's Guide for more information about completing that part of the configuration. Once File Locking has been setup for your environment, the installation of SyncLockStatus can begin.

System Requirements

SyncLockStatus' basic operating system and hardware requirements are:

- **Supported Operating Systems:** Windows Server 2008 R2; Windows Server 2008; Windows Server 2003 R2; Windows Server 2003; Windows 7; Windows Vista; Windows XP
- **Processor:** 1Ghz Pentium (or equivalent) or higher
- **RAM (total for system):** 512MB or higher
- **Hard Disk:** Less than 5MB for program components plus required space for the .NET Framework

Required Microsoft Components

SyncLockStatus requires a number of Microsoft components to be installed. The SyncLockStatus 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 4.0
- Microsoft Windows Installer 3.1
- Microsoft Internet Explorer 5.0.1 or later (required by the .NET Framework)

Contact Information

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

Software Pursuits, Inc.
1900 South Norfolk Street, Suite 330
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

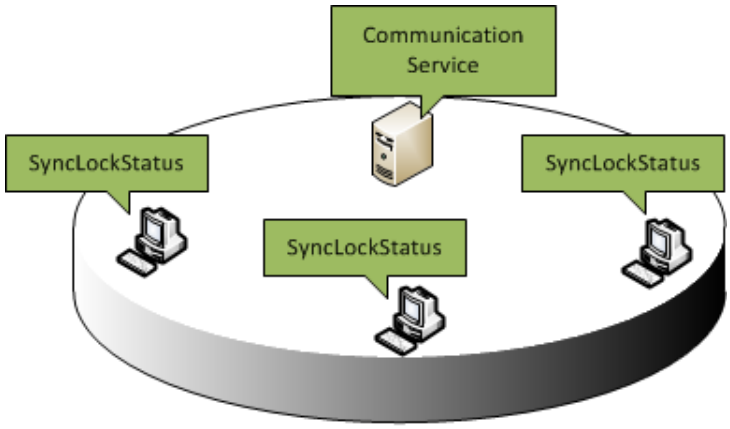
Technical support is available between 8:00AM and 5:00PM PST Monday through Friday.

SyncLockStatus Architecture

The SyncLockStatus product consists of two different components. Understanding the names of these components, where they are installed and what they do is essential to a successful SyncLockStatus deployment.

- **Software Pursuits Communication Service**: The Communication Service is the server component of the SyncLockStatus application. As the administrator, you will configure the ports used to connect to this service, define the SureSync Schedulers to pull file locking status information from and other settings. This service will then respond to requests from the SyncLockStatus application installed on the workstation(s)
- **SyncLockStatus**: SyncLockStatus 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.

The graphic below represents a standard deployment of SyncLockStatus on a subnet in a network. The Communication Service is installed on a server and SyncLockStatus on each workstation



SyncLockStatus Licensing

SyncLockStatus licensing is very simple. You need a SyncLockStatus license for each workstation that will be running the application. The Communication Service (the server component) is not licensed. You can install the Communication Service on as many servers as needed to provide status to your SyncLockStatus clients. For example, if your network has 50 workstations that need to receive file locking status using SyncLockStatus then you would need 50 SyncLockStatus licenses.

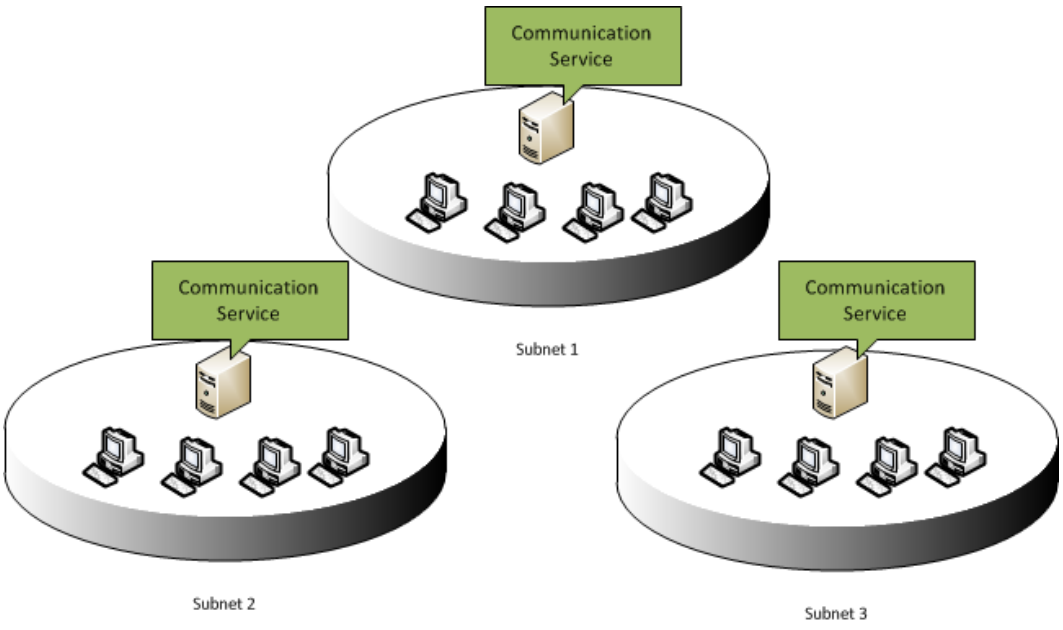
Licenses for SyncLockStatus are all managed from the server side. You will import the licenses and manage the license activations from the Communication Service Configuration Utility.

Recommended Deployment Configuration

SyncLockStatus was designed with easy deployment to the workstation in mind. SyncLockStatus is capable of autodiscovering a Communication Service running on the same subnet. This functionality allows the administrator to eliminate all configuration steps on the workstations. With autodiscovery on, the only setup step for the workstations is the installation of SyncLockStatus. When SyncLockStatus is launched, it will automatically locate and connect to the Communication Service on the subnet with no additional configuration needed.

> *You can also configure the product with autodiscovery off but this is discouraged unless absolutely necessary. This setup scenario requires more configuration effort. Please consult the SyncLockStatus help file for further information about this type of configuration.*

When using autodiscovery, you must install and configure the Communication Service on a server in each subnet containing workstations that will be receiving file locking status. Consider the network below which consists of 3 different subnets. To use the preferred autodiscover method, you would install a Communication Service on a server in each subnet. When installed in this manner, no client configuration is necessary. When the client application loads, it will automatically detect the Communication Service and configure itself to receive file locking status.

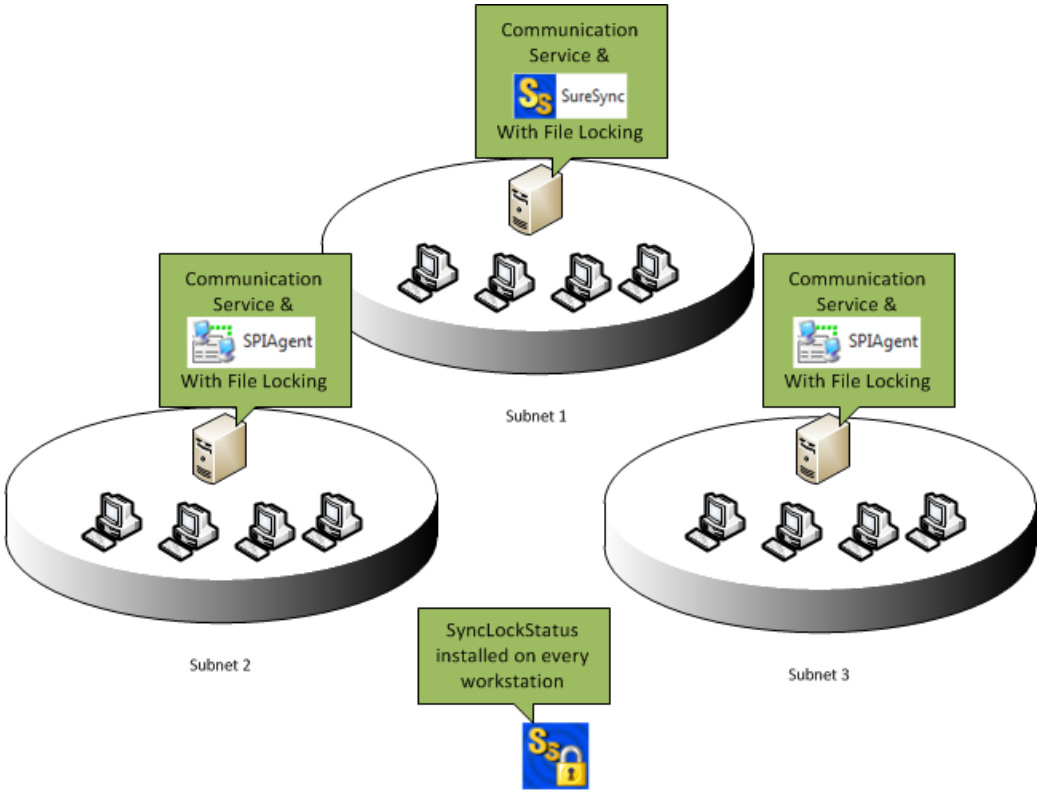


This configuration is correct regardless of where the SureSync server is located. When you configure the Communication Service, you will provide a DNS name or IP address that the service can use to communicate with the Scheduler on the SureSync machine via the SPIAgent.

In the scenario above, the SyncLockStatus workstation application would be installed on each of the 12 desktop machines. Each machine will automatically discover the Communication Service installed on its subnet and will get file locking status information from that Communication Service.

The Communication Services in the environment use the SPIAgent to communicate with the SureSync Scheduler service on the main SureSync machine(s) to retrieve the status.

The entire configuration would look something like the graphic below.



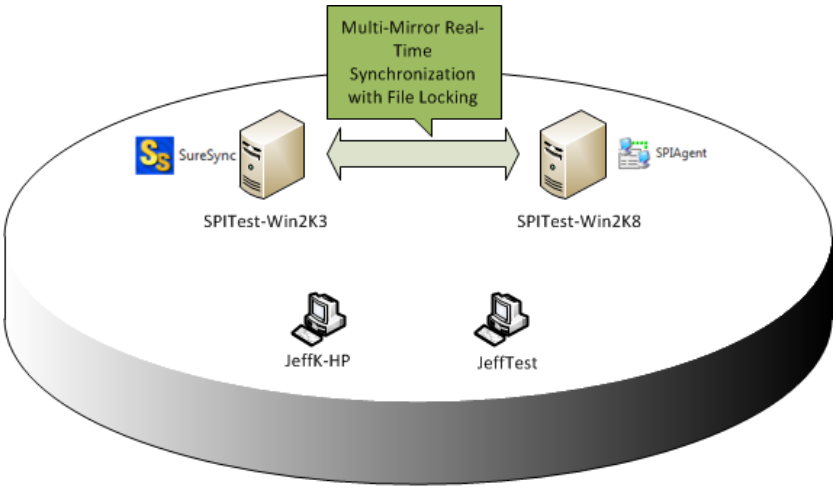
This full scenario is showing how SyncLockStatus can simply plug into an existing SureSync environment. In this example, SureSync was already being used to synchronize data between the three servers. The server in Subnet 1 has the full SureSync installation with a Scheduler while the machines in the other subnets have the SPIAgent only. In this scenario, it makes sense to add a Communication Service to each server allowing autodiscovery to be used by the workstations.

SyncLockStatus components can co-exist on the same hardware as other SureSync components. You can also install SyncLockStatus components on machines with no SureSync components. If you have a subnet that needs file locking status for workstations but has no SureSync components installed, you can install the Communication Service on a server in that subnet. This allows Autodiscovery for the SyncLockStatus applications installed on the workstations in that subnet.

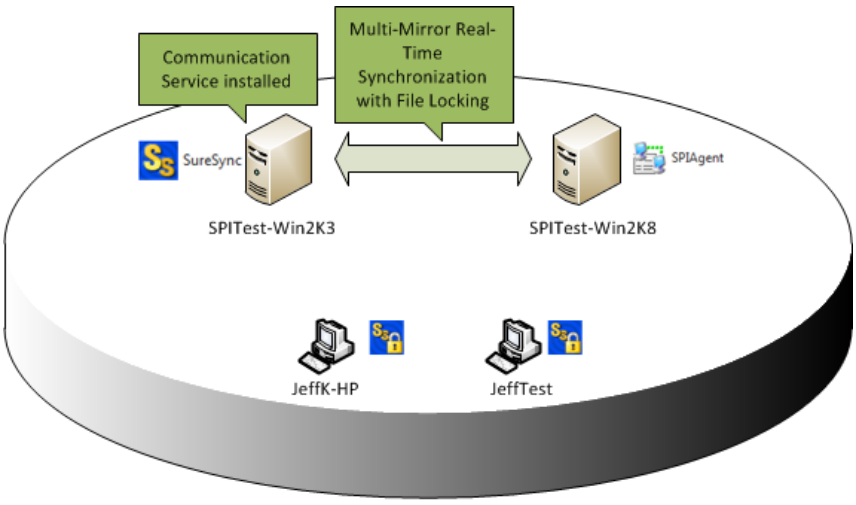
Our Scenario

This guide will walk you through the configuration of SyncLockStatus to provide file locking information to clients on a network with a single subnet using auto-discovery. The guide will also provide tips for deploying in larger network environments.

First, let's review the existing SureSync environment in this scenario. The environment consists of two servers named SPITest-Win2K3 and SPITest-Win2K8. Two workstations exist in the same subnet called JeffK-HP and JeffTest. The goal is to implement SyncLockStatus so the two workstation machines can receive file locking status from the SureSync job.



We will be installing the Communication Service (the server component) on SPITest-Win2K3 to provide file locking status information to the SyncLockStatus applications on the JeffK-HP and JeffTest workstation machines. The final configuration will look like the graphic below.



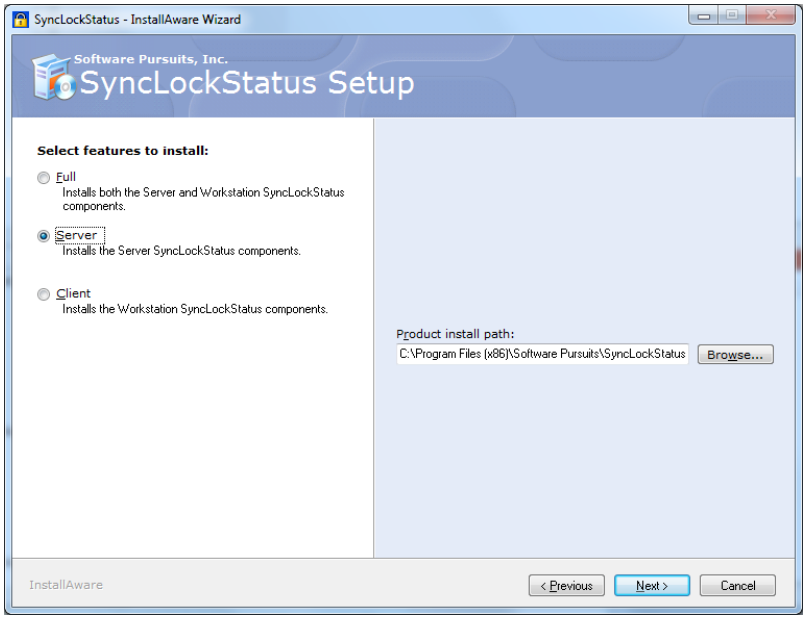
Installing the Communication Service

The first step in deploying SyncLockStatus in your SureSync file locking environment involves installing and configuring the Communication Service on the appropriate servers. In our scenario, the machine with the Communication Service installed will be SPITest-Win2K3.

> *If your environment has more than one subnet, this section should be repeated so each subnet has a Communication Service installed and configured on a machine. We recommend installing the Communication Service on a server whenever possible. However, if a particular subnet has no servers you can select a workstation machine to install the Communication Service.*

Step 1: Install the Communication Service

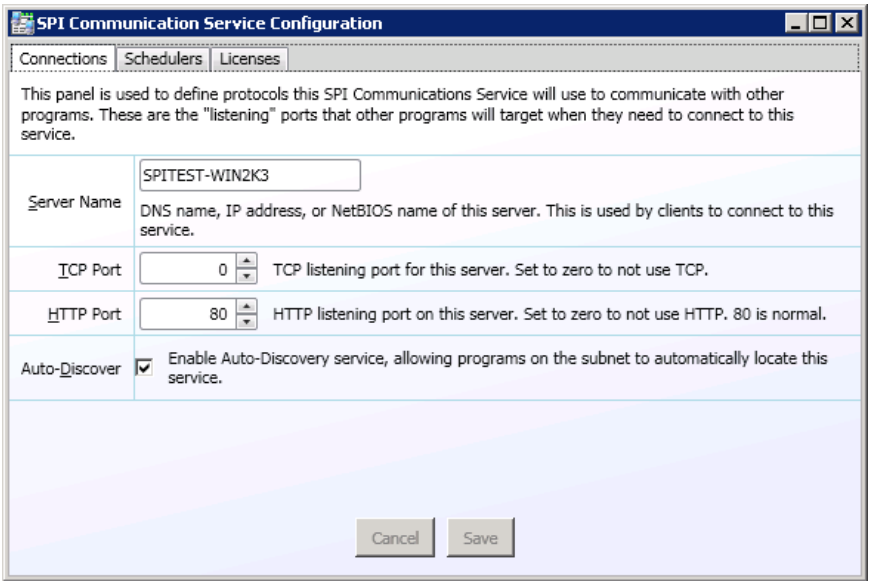
Log into the server as an administrator and launch the SyncLockStatusSetup.exe executable. Follow the on-screen prompts until you arrive at the "Select features to install" panel. Select the "Server" installation type. Click "Next" and then follow the remaining prompts to complete the installation.



Step 2: Launch the Communication Service Configuration Utility

To configure the Communication Service you must launch the Communication Service Configuration Utility. This is accomplished by going to **Start | Programs | SyncLockStatus** and clicking on "Communication Service Configuration Utility."

Step 3: Configure the Connections Tab

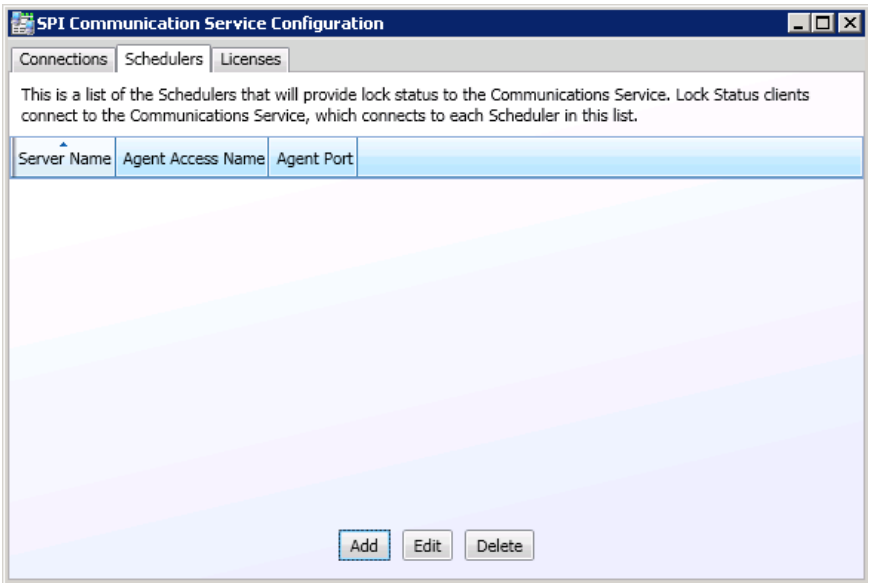


The first tab is the “Connections” tab. This tab defines the settings that the SyncLockStatus workstation clients will use to connect to the Communication Service.

To complete configuration of this panel, do the following:

- **Server Name**: For the “Server Name” field, enter in the DNS name, IP address or NetBIOS name of the machine that the Communication Service is installed on. The name entered here must be resolvable from the client machines.
- **TCP Port**: By default, the TCP Port is set to 0. This configures the Communication Service to not use TCP for communication with the workstations. If you want to use TCP, configure a port number here. This can be any available TCP port you want to use. The SPIAgent port range of 9002-9033 cannot be used. We recommend using port 9000 or 9034 if you’re going to use TCP.
- **HTTP Port**: By default, port 80 is selected. This configures the Communication Service to listen on HTTP port 80 for requests from the SyncLockStatus workstations. You can configure the Communication Service to listen on both HTTP and TCP by having a port configured for both options. If you do not want to use HTTP, set this option to 0.
- **Auto-Discover**: By default, the Communication Service is set to allow SyncLockStatus workstations to auto-discover the service. For this example, we will leave Auto-Discover turned on.

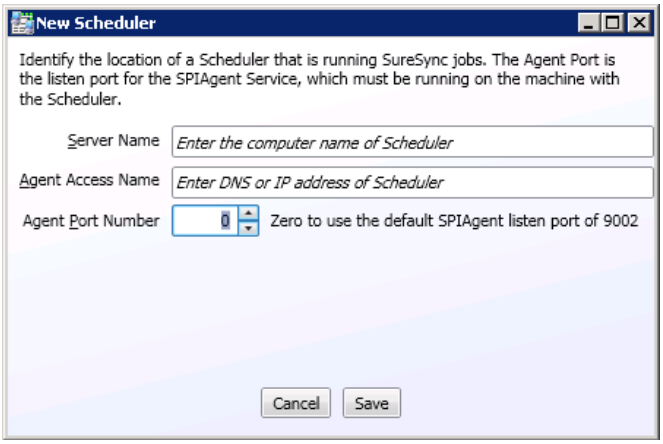
Step 4: Configure the Schedulers Tab



The second tab in the Communication Service Configuration Utility is the "Schedulers" tab. This tab allows you to define which SureSync Schedulers the Communication Service should communicate with to retrieve file locking status. If you're installing the Communication Service on the same machine as your main SureSync installation, as in the example scenario, then you will add that machine's Scheduler here. However, you can also provide details to access a SureSync Scheduler on a remote machine.

> *The communication with the SureSync Scheduler is performed via the SPIAgent service on the machine. This communication occurs on the default SPIAgent port by default. The default port is 9002.*

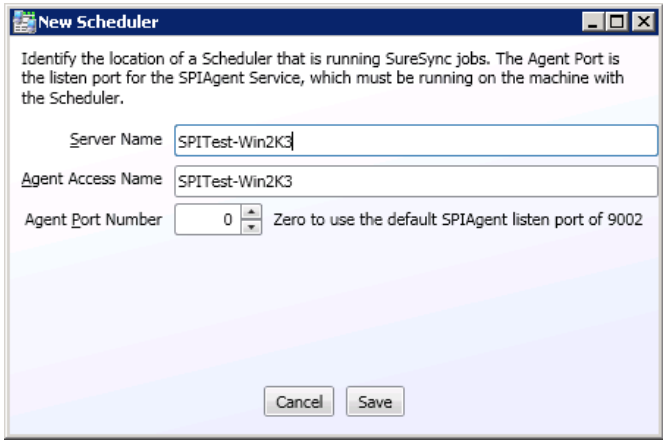
To add a Scheduler, click the "Add" button.



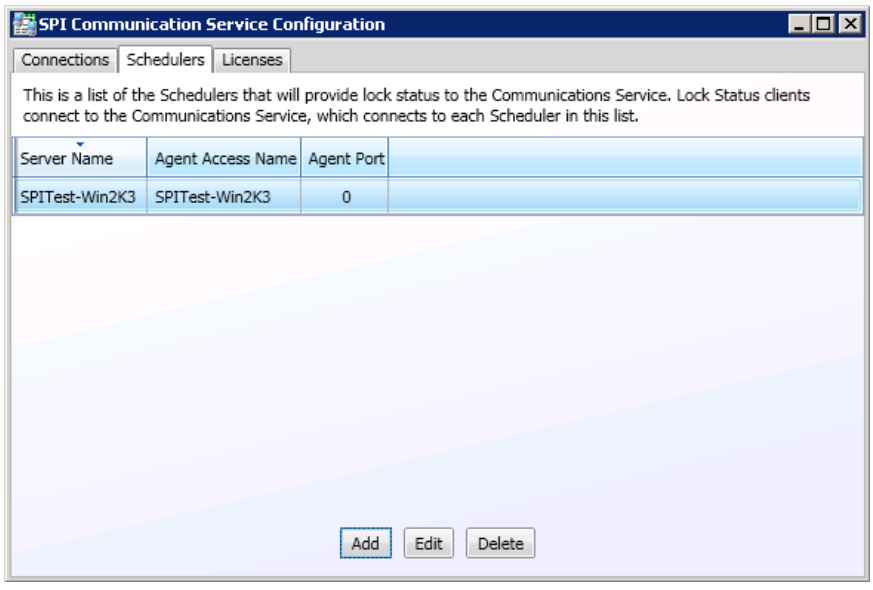
To configure the connection to the Scheduler, do the following:

- **Server Name**: Enter the NetBIOS computer name of the service that is running the SureSync Scheduler Service. For our example, this will be SPITest-Win2K3.
- **Agent Access Name**: Enter the DNS name or IP address of the machine that is running the SureSync Scheduler service. For our example, this will be SPITest-Win2K3. It could also be configured in the Fully Qualified Domain Name (FQDN) format of SPITest-Win2K3.domain.com or by IP address if the machine has a fixed IP.
- **Agent Port Number**: Zero is the default and represents the default SPIAgent listen port of 9002. This should be left at default in all environments unless you have manually configured a different port range for the SPIAgent service.

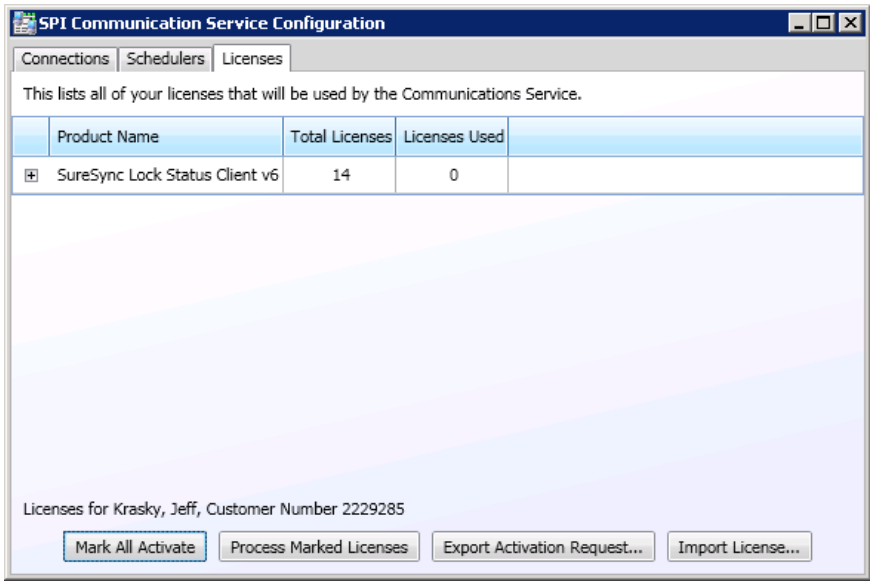
Once you have completed the configuration the panel should look like the screenshot below.



Click “Save” to save your configuration and add the Scheduler to the Communication Service. Your Schedulers tab should now look like the screenshot below.



Step 5: Configure the Licenses Tab



SyncLockStatus is licensed by the number of SyncLockStatus workstations that will be connecting to the Communication Service. You're free to install as many Communication Services as necessary for your environment without additional licensing requirements. For example, if you have 50 workstations that will have SyncLockStatus installed and receiving file locking status then you would need 50 licenses. This is true even if you have 3 or 4 Communication Services installed.

The trial license distributed with SyncLockStatus allows 10 workstations for a period of 30 days. For the trial, no configuration of the Licenses tab is necessary. If you purchase, you can import your licenses via the "Licenses" tab of the Communication Service Configuration panel by clicking on the "Import License…" button.

Step 6: Restart the Communication Service

Once the configuration is complete, the Software Pursuits Communication Service must be restarted to allow the changes to take effect. This can be accomplished by going to **Start | Programs | Administrative Tools | Services**, selecting the Software Pursuits Communication Service and then clicking on the "restart" button in the toolbar.

Installing SyncLockStatus on the Workstations

Once the Software Pursuits Communication Service has been configured in each subnet, the SyncLockStatus client application must be deployed to each workstation that wants to receive notification from the file locking system. This can be accomplished in a number of ways:

- Manually run the SyncLockStatusSetup.exe on each workstation
- Using Active Directory deployment or a third party deployment application
- Using the Software Pursuits Remote Installation Utility

The Windows Firewall or other software based firewall on the client computers can block the process of communicating with the Communications Service. Please be sure that you open the port(s) you configured the Communication Service to use on the workstation machines or the communication will fail.

If deploying using autodiscovery as suggested in this guide, we recommend using the SPI Remote Installation Utility from the SyncLockStatus server in each subnet to deploy the SyncLockStatus workstation software to each machine. The Remote Installation Utility can be accessed by logging into that server and then going to **Start | SyncLockStatus | Remote Installation Utility**.

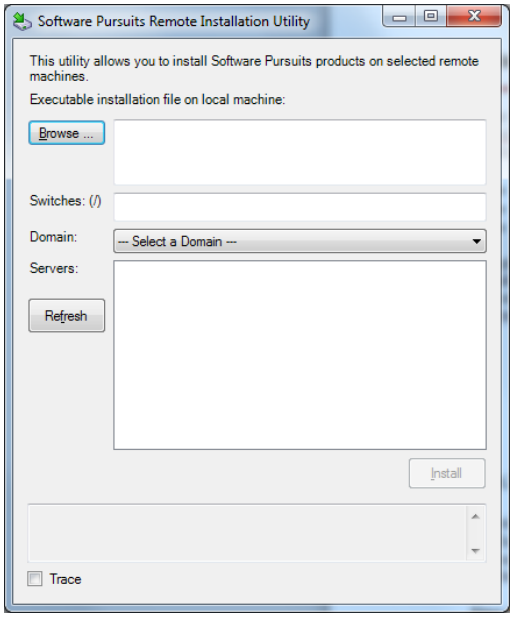
You must be logged into the server as an administrator account with access to the administrative share on the C: drive of each machine you're installing SyncLockStatus. A domain administrator account should have appropriate permissions. The software can only be deployed to machines using this utility if they are accessible from the server via UNC path.

Step 1: Log into the SyncLockStatus Server as an Administrator

Physically login to or use Remote Desktop to access the SyncLockStatus server machine running the Software Pursuits Communication Service. Make sure to log in as a domain administrator account with permissions to access the administrative share on the C: drive of the client machines in question.

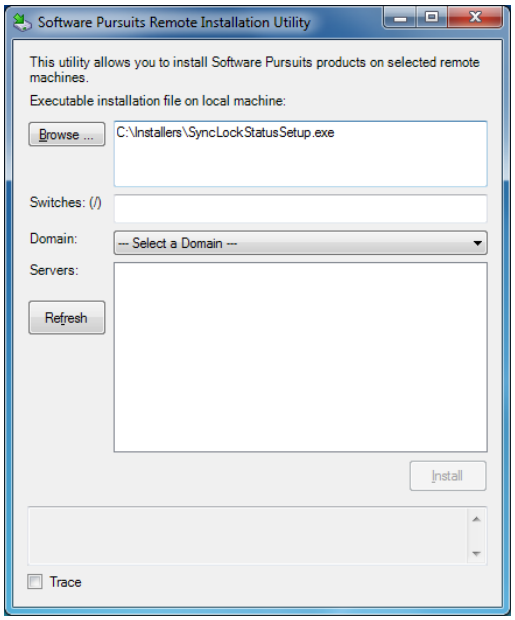
Step 2: Launch the Software Pursuits Remote Installation Utility

Go to **Start | Programs | SyncLockStatus | Remote Installation Utility** and the application will load. You should see a program window that looks like the screenshot below.



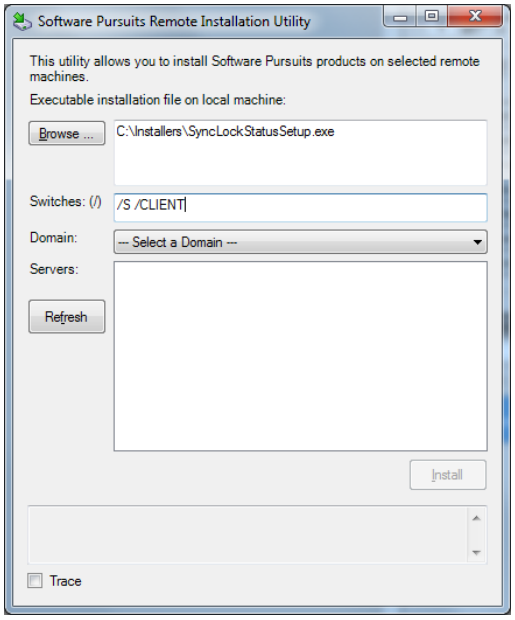
Step 3: Select the SyncLockStatus Setup

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



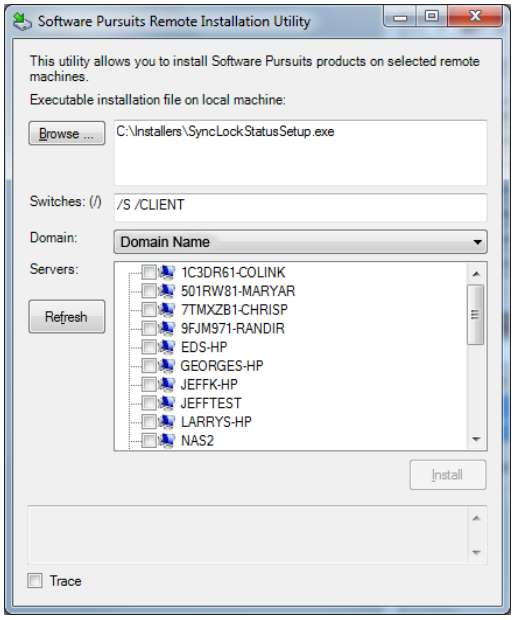
Step 4: Define the Installation Switches

To install the SyncLockStatus components silently, you should enter */S /CLIENT* in the “Switches” field. The */S* sets the installer to silent mode and the */CLIENT* selects the Client setup type.



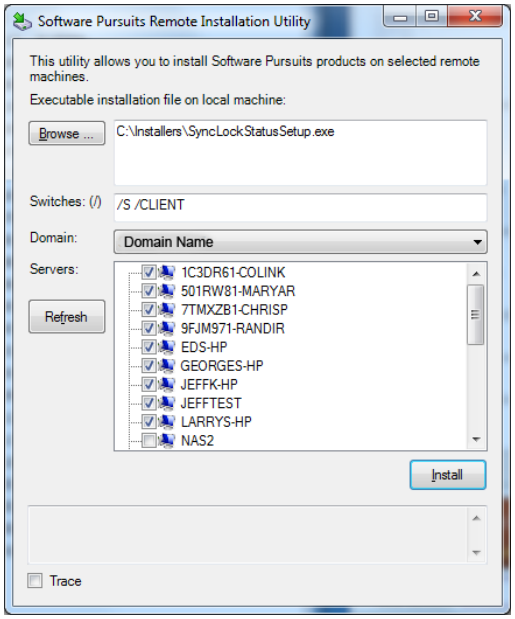
Step 5: Select the Domain to Locate the Workstations

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



Step 6: Select the Target Workstations

From the list that displays, check the machines that you want to install the SyncLockStatus client application on.



Step 7: Click Install and Monitor

Finally, click the Install button and monitor the messages that will appear at the bottom of the panel. When the installation is complete, the installer will automatically launch the SyncLockStatus application on the workstation(s).