SureSync®

SyncLockStatus Evaluator's Guide

Software Pursuits

Windows Server 2012 Certified

Windows 8 Compatible

Microsoft Partner
Silver Application Development

Table of Contents

Introduction

SyncLockStatus is an Add-on to SureSync's Collaboration Bundle that makes the file locking process more transparent to the users on your network. When a user attempts to open a file that is locked by another user, the SyncLockStatus 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. In addition, SyncLockStatus will notify the user when the file has been closed so they can attempt to gain access to a writable copy of the file.

SyncLockStatus adds value to the SureSync Collaboration Bundle by minimizing end user confusion when file locking is deployed in your environment. Without SyncLockStatus your users will see different behaviors depending on the application installed. For example, the user might just 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 SyncLockStatus. To use SyncLockStatus, you must have the SureSync Collaboration bundle installed and configured in your environment. Please review the SureSync Collaboration Bundle Evaluator's Guide for more information about completing that part of the configuration.

System Requirements

SyncLockStatus' basic operating system and hardware requirements are:

- **Supported Operating Systems:** Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2; Windows Server 2008; Windows Server 2003 R2; Windows Server 2003; Windows 8.1; Windows 8; 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

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

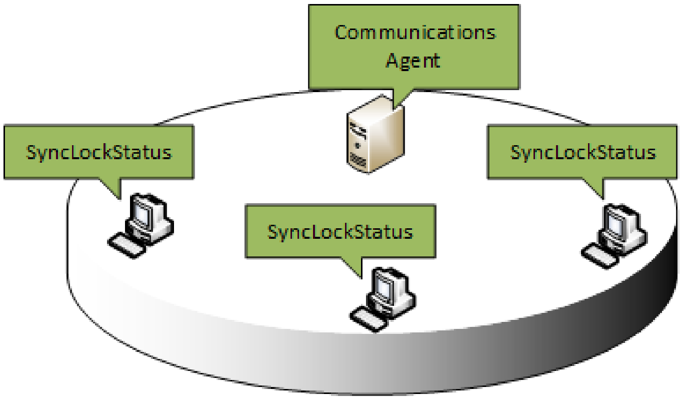
- **Software Pursuits Communications Agent**: The Communications Agent is the service within SureSync responsible for providing real-time monitors and other advanced functionality. This service includes the necessary functionality to support SyncLockStatus right out of the box. This makes it quick and easy to add SyncLockStatus to your collaboration environment.
- **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.
- **SureSync Scheduler Service**: The SureSync Scheduler is used to provide licensing information and other SyncLockStatus related functionality. The Scheduler is accessed through the Communications Agent on the server where the Scheduler is installed. This guide will walk you through the process of identifying the machine(s) in your environment running the Scheduler service. Doing so will allow SyncLockStatus clients will be able to connect to the Scheduler service to retrieve file locking notificiations.

The server side components of SyncLockStatus are completely integrated into SureSync. This provides significant benefit because you are likely to have the required Communications Agent already present in each office or subnet due to the file replication / synchronization need already being solved with SureSync. With a few minor configuration tweaks, SyncLockStatus can be added.

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

Deployment on a Single Subnet

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

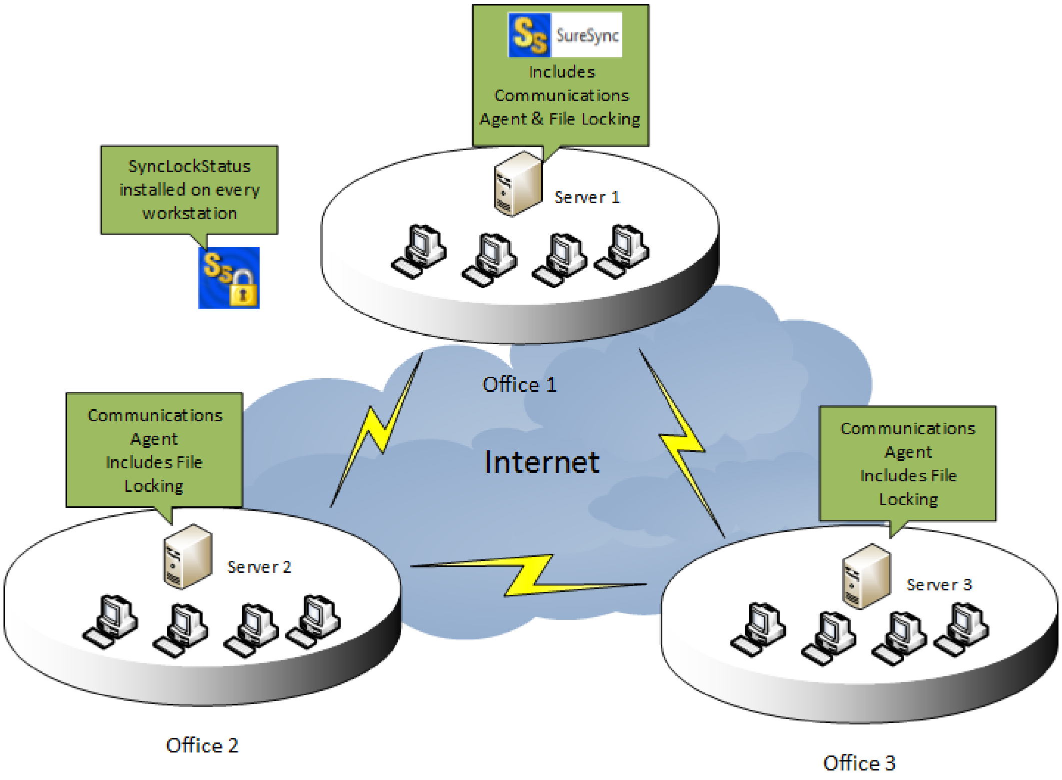


Subnet 1

In small deployments such as the example above, SyncLockStatus deployment is simple and can be done 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:


SureSync
Includes Communications Agent & File Locking
SyncLockStatus installed on every workstation
Server 1
Office 1
Internet
Communications Agent Includes File Locking
Server 2
Communications Agent Includes File Locking
Server 3
Office 2
Office 3

In this scenario, a company has three servers in three offices. These servers are participating in a multi-way real-time synchronization 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 a SureSync machine running the Scheduler service. In the example network, SureSync (and the Scheduler) are running on Server 1. Server 2 and Server 3 need to be able to connect to Server 1 to retrieve file locking status notification.

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, SyncLockStatus requires that Server 2 and Server 3 be able to 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. This rule will allow requests coming to the selected public IP or DNS from Server 2 and Server 3 to be forwarded to the Server 1 machine properly. The default port for all SureSync and SyncLockStatus communications is TCP 9033. Please consult the documentation for your firewalls to make these configuration changes.

SyncLockStatus Licensing

SyncLockStatus licensing is very simple. You need a SyncLockStatus license for each workstation that will be running the application. For example, if your network has 50 workstations that need to receive file locking status using SyncLockStatus then you would need 50 SyncLockStatus licenses.

If you need to install additional Communications Agents to deploy with autodiscovery, no additional licensing is needed as long as no data is being synchronized to that agent with SureSync.

Licenses for SyncLockStatus are managed from within SureSync. The SyncLockStatus licenses are part of your SureSync license file and are imported into SureSync by clicking on the Home button, selecting Licenses and then clicking on the “Import License...” button.

SyncLockStatus Deployment Methods

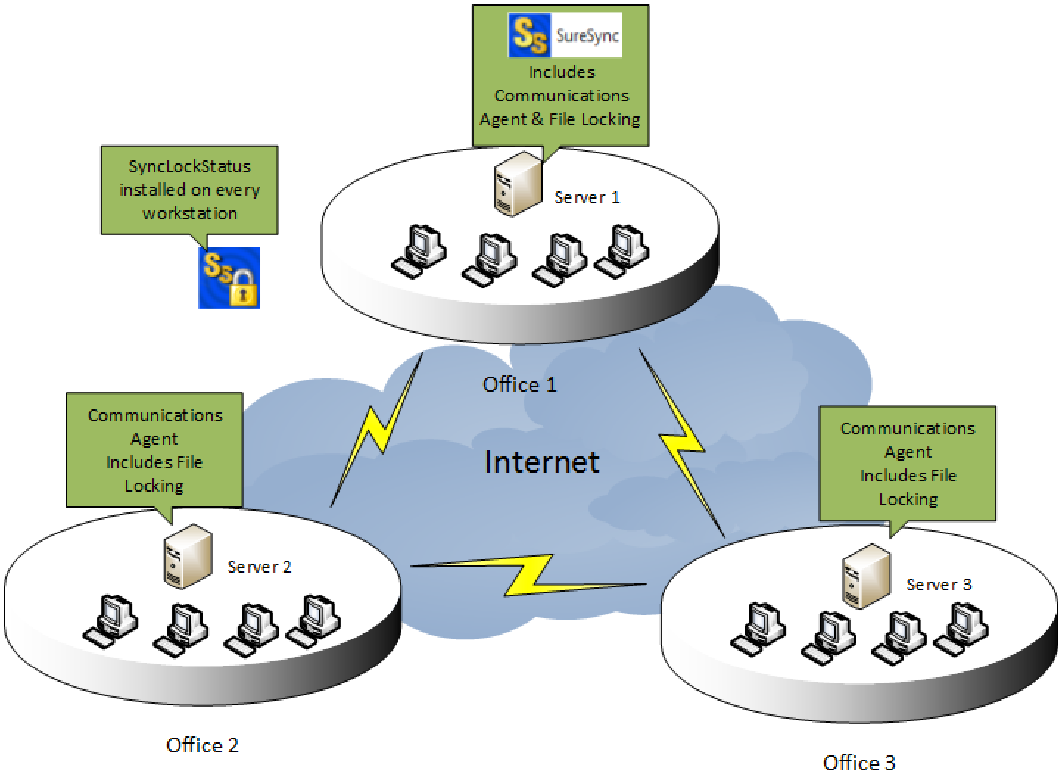
SyncLockStatus can be deployed in three different ways:

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

Deployment via Autodiscovery

Autodiscovery results in the smallest amount of configuration on the individual workstations. By default, a broadcast is issued when a SyncLockStatus 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 then SyncLockStatus 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:


SureSync
Includes Communications Agent & File Locking
SyncLockStatus installed on every workstation
Server 1
Office 1
Internet
Communications Agent Includes File Locking
Server 2
Office 2
Communications Agent Includes File Locking
Server 3
Office 3

The basic steps for this type of deployment will be:

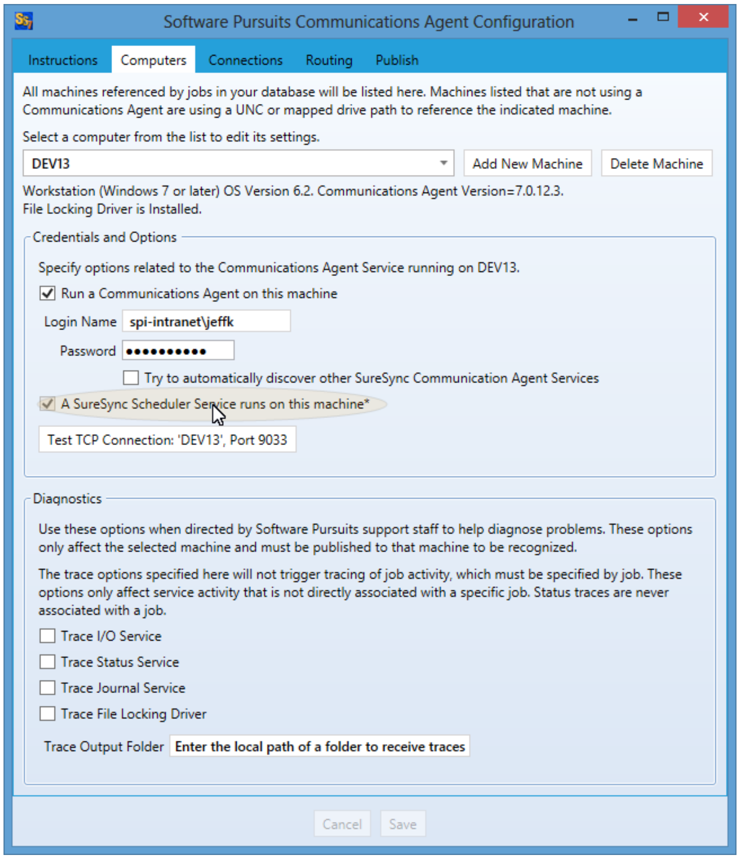
- Ensure the Scheduler is identified as running on the appropriate machine(s).
- Configure each Communications Agent to respond to autodiscovery requests from the SyncLockStatus clients.
- Identify a public IP or DNS name to use for SyncLockStatus. This connection will be used for remote offices (Office 2 and Office 3 in this scenario) to retrieve lock status information from the main SureSync installation.
- Configure firewalls as necessary to allow the required connections.
- Configure a connection on each remote Communications Agent that defines how to connect back to main SureSync server.
- Deploy SyncLockStatus to the client machines.

Step 1: Ensure the Scheduler service option is set for the appropriate machine(s)

Within the Communications Agent Configuration Utility is an option that tells SureSync and other Communications Agent machines within the SureSync environment that a particular machine is running a Scheduler. This option should already be enabled because the Scheduler installation procedure automatically sets it. However, it’s recommended to confirm the option is set.

Launch the SureSync desktop, click on the Home button, then click Communications Agents and then click Configure Communications Agents. When the Communications Agent Configuration panel loads click on the “Computers” tab. Once on the “Computers” tab select your SureSync machine that is running the Scheduler service.

Once on that panel, ensure the option “A SureSync Scheduler Service runs on this machine” is checked as shown in the screenshot below.



All machines referenced by jobs in your database will be listed here. Machines listed that are not using a Communications Agent are using a UNC or mapped drive path to reference the indicated machine.

Select a computer from the list to edit its settings.

DEV13

Workstation (Windows 7 or later) OS Version 6.2. Communications Agent Version=7.0.12.3.
File Locking Driver is Installed.

Credentials and Options

Specify options related to the Communications Agent Service running on DEV13.

☑ Run a Communications Agent on this machine

Login Name spi-intranet\jeffk

Password ●●●●●●●●●●

□ Try to automatically discover other SureSync Communication Agent Services

☑ A SureSync Scheduler Service runs on this machine*

Test TCP Connection: 'DEV13', Port 9033

Diagnostics

Use these options when directed by Software Pursuits support staff to help diagnose problems. These options only affect the selected machine and must be published to that machine to be recognized.

The trace options specified here will not trigger tracing of job activity, which must be specified by job. These options only affect service activity that is not directly associated with a specific job. Status traces are never associated with a job.

□ Trace I/O Service

□ Trace Status Service

□ Trace Journal Service

□ Trace File Locking Driver

Trace Output Folder Enter the local path of a folder to receive traces

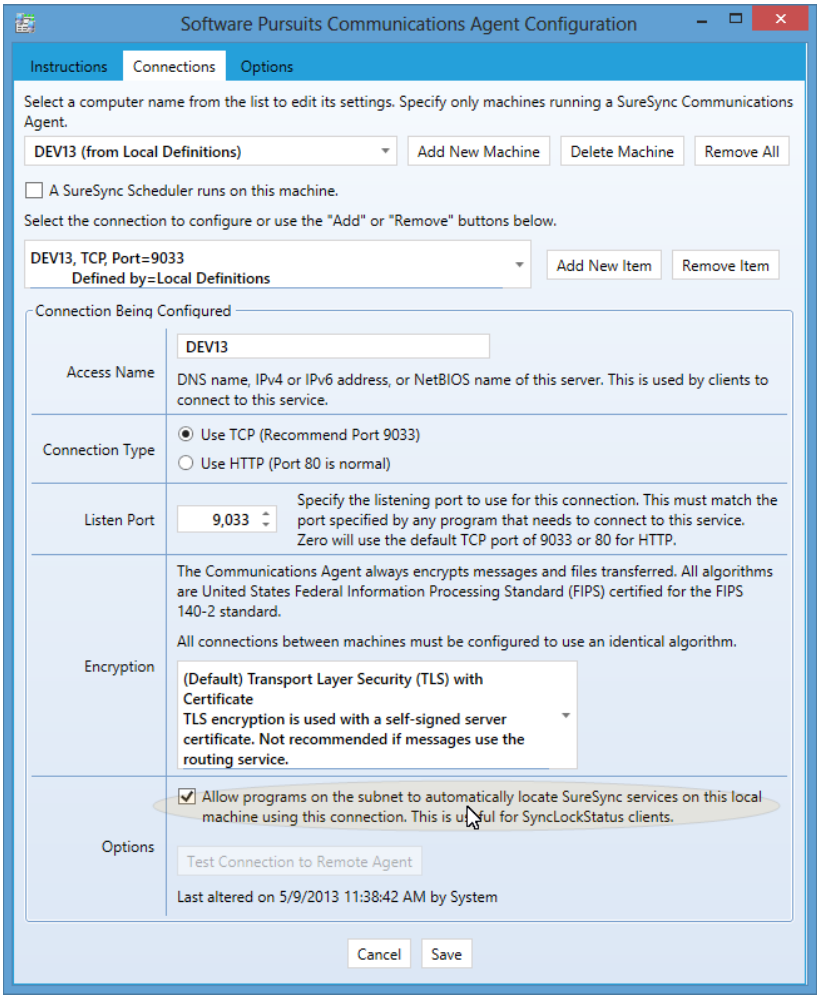
Step 2: Configure Communications Agent(s) to respond to autodiscovery requests

Each Communications Agent that will respond to autodiscovery requests from SyncLockStatus clients must have an option turned on to enable this functionality. The option is off by default.

In the scenario outlined, there are 3 Communications Agents in the environment and each of them will be providing autodiscovery services for SyncLockStatus clients in their respective offices. This means that this step will be performed on all three servers.

Log into the Communications Agent server in question and go to the Start menu. Select All Programs, SureSync 7, and Communications Agent Configuration Utility 7.

After the Software pursuits Communications Agent Configuration panel loads click on the “Connections” tab. Click on the “[Please select a machine from this list]” drop-down and select the machine name of the server you’re currently on. You should see the following:



Select a computer name from the list to edit its settings. Specify only machines running a SureSync Communications Agent.

DEV13 (from Local Definitions)

□ A SureSync Scheduler runs on this machine.

Select the connection to configure or use the "Add" or "Remove" buttons below.

DEV13, TCP, Port=9033
Defined by=Local Definitions

Connection Being Configured

Access Name: DEV13
DNS name, IPv4 or IPv6 address, or NetBIOS name of this server. This is used by clients to connect to this service.

Connection Type: ● Use TCP (Recommend Port 9033) ○ Use HTTP (Port 80 is normal)

Listen Port: 9,033
Specify the listening port to use for this connection. This must match the port specified by any program that needs to connect to this service. Zero will use the default TCP port of 9033 or 80 for HTTP.

Encryption: The Communications Agent always encrypts messages and files transferred. All algorithms are United States Federal Information Processing Standard (FIPS) certified for the FIPS 140-2 standard.

All connections between machines must be configured to use an identical algorithm.

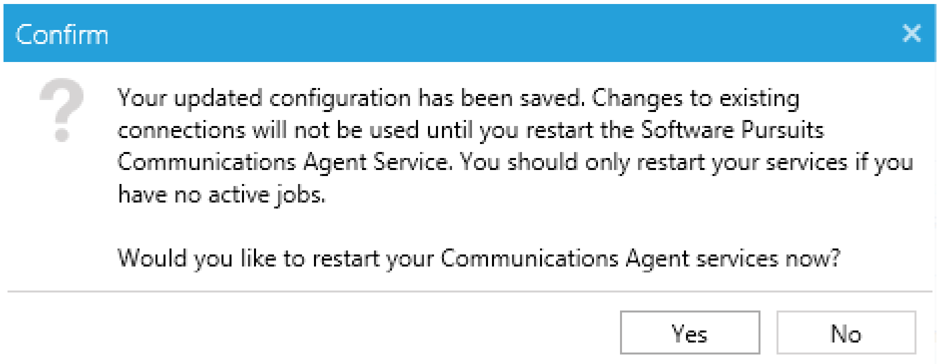
(Default) Transport Layer Security (TLS) with Certificate
TLS encryption is used with a self-signed server certificate. Not recommended if messages use the routing service.

Options: ☑ Allow programs on the subnet to automatically locate SureSync services on this local machine using this connection. This is useful for SyncLockStatus clients.

Last altered on 5/9/2013 11:38:42 AM by System

Check the box for “Allow programs on the subnet to automatically locate SureSync services on this local machine using this connection.”

Click “Save” and you will receive the following prompt:



Your updated configuration has been saved. Changes to existing connections will not be used until you restart the Software Pursuits Communications Agent Service. You should only restart your services if you have no active jobs.

Would you like to restart your Communications Agent services now?

Click the “Yes button to restart the Communications Agent service. Once this has completed, your Communications Agent will be ready to respond to SyncLockStatus client requests for autodiscovery services.

Step 3: Identify a Public IP or DNS name for use with SyncLockStatus

A public IP address or DNS name is needed to allow the remote Communications Agent machines to establish connections to the main SureSync machine. These connections are used to retrieve lock status information to forward to the SyncLockStatus clients. You will need the IP address or DNS name to proceed to the following step.

Step 4: Configure Firewalls as Appropriate

Once the public address has been identified, you must make any necessary firewall configuration changes. Most firewall configuration will already be done because you have a working SureSync collaboration environment deployment at the time you implement SyncLockStatus. The one addition is a port forward or NAT rule on the firewall at the main SureSync office (Office 1 in the example) to forward traffic received on the SureSync port to the SureSync server. The default port is TCP 9033.

Step 5: Create connections to reach Scheduler for remote machines

This step must be performed when you have multiple offices and/or subnets. Broadcasts only reach machines in the same subnet so there must be a Communications Agent in each subnet that can respond to SyncLockStatus clients in that subnet. Single subnet environments can skip this step.

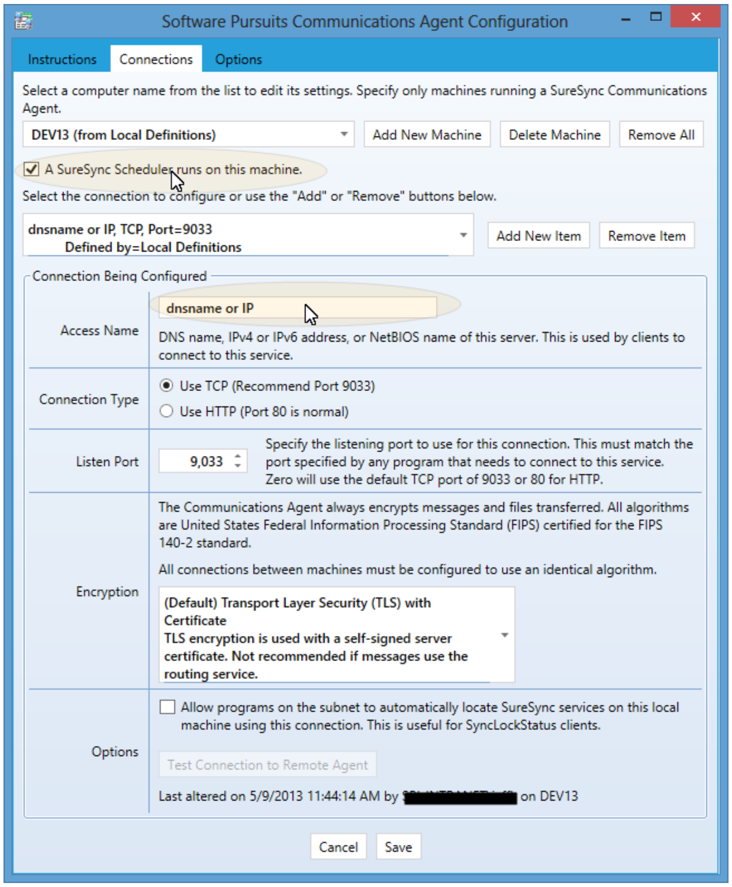
Generally speaking, your primary SureSync machine runs the SureSync Scheduler service. This is the service responsible for running Schedules and Real-Time Monitors at their appropriate times. The service also hands out SyncLockStatus licenses to clients and helps relay lock information to the clients through the Communications Agent.

When dealing with remote Communications Agent machines (as in this scenario), you must provide connection details to those remote agents telling them how to reach the Scheduler machine (the main SureSync machine). This connection provides a public IP or DNS name that the server can use to reach the appropriate machine. In the scenario being discussed, the servers in Office 2 and Office 3 need a connection defined to reach the server in Office 1.

Log into the Communications Agent server in question and go to the Start menu. Select All Programs, SureSync 7, and Communications Agent Configuration Utility 7.

After the Software Pursuits Communications Agent Configuration panel loads click on the “Connections” tab. Click on the “[Please select a machine from this list]” drop-down and see if a connection for the main SureSync machine exists already. If so, click on it. If not, click “Add New Machine” and enter the name of the machine to create a new connection.

You should then see a panel like this:


Software Pursuits Communications Agent Configuration
Instructions
Connections
Options
Add New Machine
Delete Machine
Remove All
Add New Item
Remove Item
Connection Being Configured
Test Connection to Remote Agent
Cancel
Save

Select a computer name from the list to edit its settings. Specify only machines running a SureSync Communications Agent.

DEV13 (from Local Definitions)

☑ A SureSync Scheduler runs on this machine.

Select the connection to configure or use the "Add" or "Remove" buttons below.

dnsname or IP, TCP, Port=9033
Defined by=Local Definitions

Access Name: dnsname or IP

DNS name, IPv4 or IPv6 address, or NetBIOS name of this server. This is used by clients to connect to this service.

Connection Type:
● Use TCP (Recommend Port 9033)
○ Use HTTP (Port 80 is normal)

Listen Port: 9,033

Specify the listening port to use for this connection. This must match the port specified by any program that needs to connect to this service. Zero will use the default TCP port of 9033 or 80 for HTTP.

Encryption: The Communications Agent always encrypts messages and files transferred. All algorithms are United States Federal Information Processing Standard (FIPS) certified for the FIPS 140-2 standard.

All connections between machines must be configured to use an identical algorithm.

(Default) Transport Layer Security (TLS) with Certificate
TLS encryption is used with a self-signed server certificate. Not recommended if messages use the routing service.

Options: □ Allow programs on the subnet to automatically locate SureSync services on this local machine using this connection. This is useful for SyncLockStatus clients.

Last altered on 5/9/2013 11:44:14 AM by [redacted] on DEV13

Please perform the following:

- Check “A SureSync Scheduler runs on this machine.”
- Under “Access Name” enter the publicly accessible IP or DNS name that this Communications Agent should use to reach the main SureSync Scheduler.
- Click the “Save” button.
- You can click “Test connection to Remote Agent” to ensure the connection works.

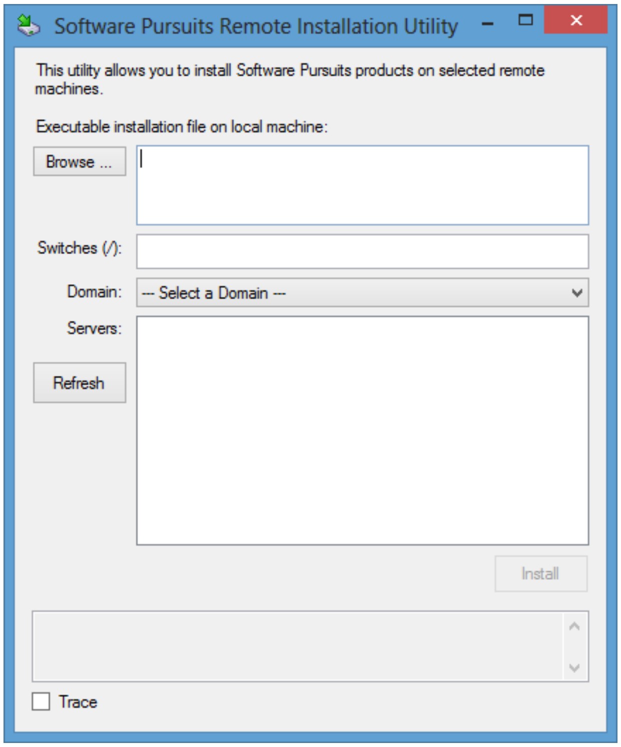
Step 6: Install SyncLockStatus clients on the workstations

The final step of an autodiscovery deployment is to install the SyncLockStatus client on the workstations. There are a number of different ways you can 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 7 and select Remote Installation Utility 7. The Software Pursuits Remote Installation Utility will launch. You should see a program window that looks like the screenshot below.

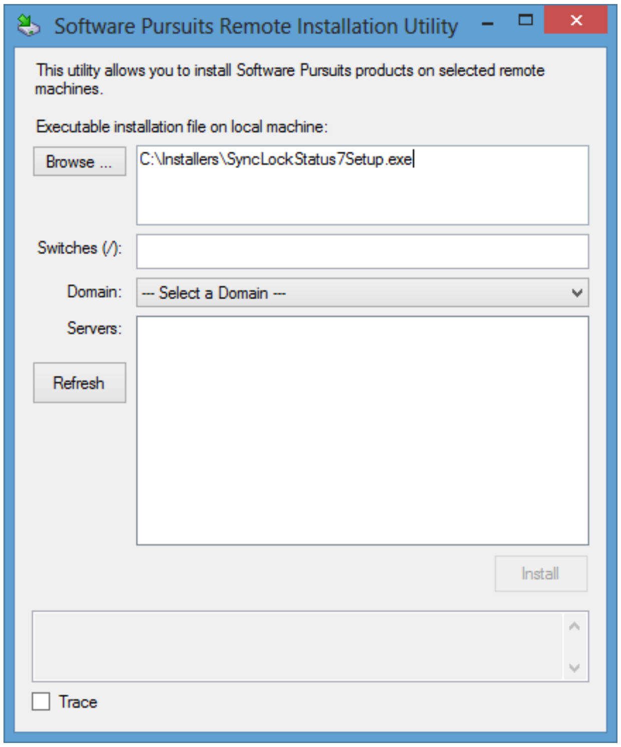


This utility allows you to install Software Pursuits products on selected remote machines.

Executable installation file on local machine:

Domain: -- Select a Domain --

Click the “Browse” button and select the SyncLockStatus7Setup.exe setup file or manually type the path to the file into the “Executable installation file on local machine” field.

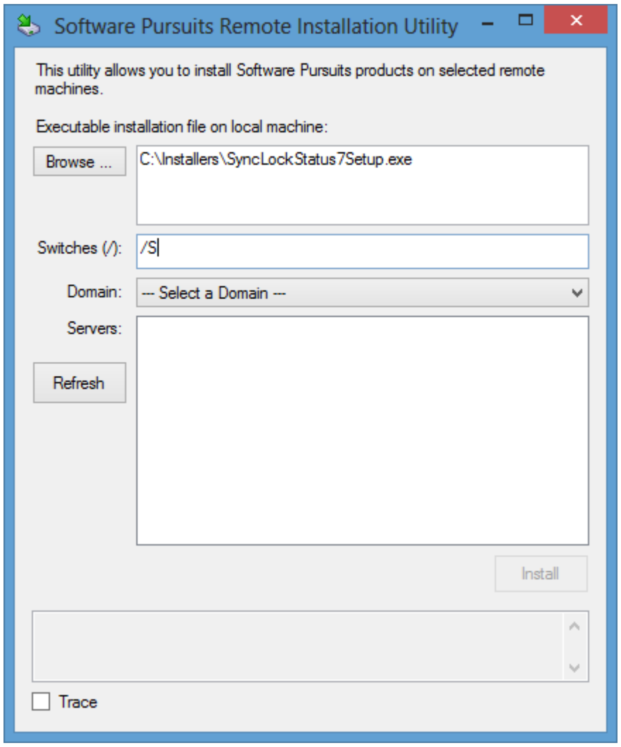


This utility allows you to install Software Pursuits products on selected remote machines.

Executable installation file on local machine: C:\Installers\SyncLockStatus7Setup.exe

Domain: -- Select a Domain --

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



This utility allows you to install Software Pursuits products on selected remote machines.

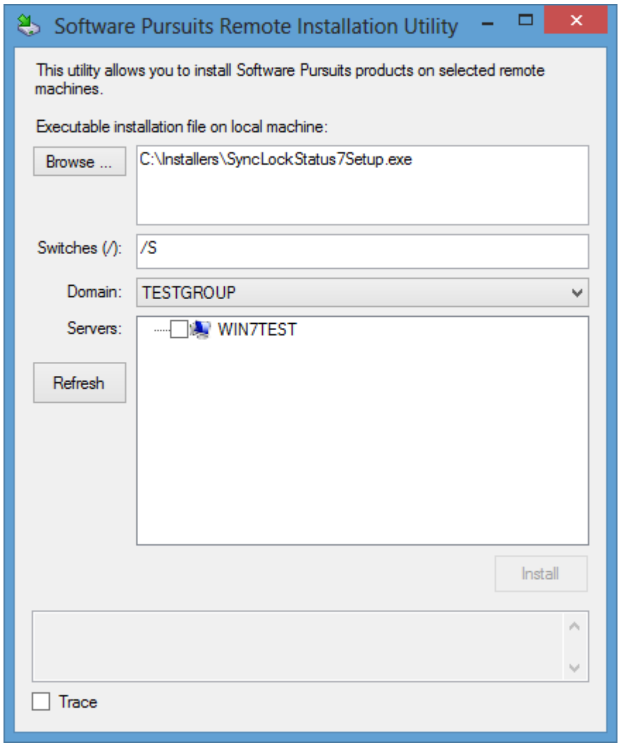
Executable installation file on local machine: C:\Installers\SyncLockStatus7Setup.exe

Switches (/): /S

Domain: --- Select a Domain ---

Servers:

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



This utility allows you to install Software Pursuits products on selected remote machines.

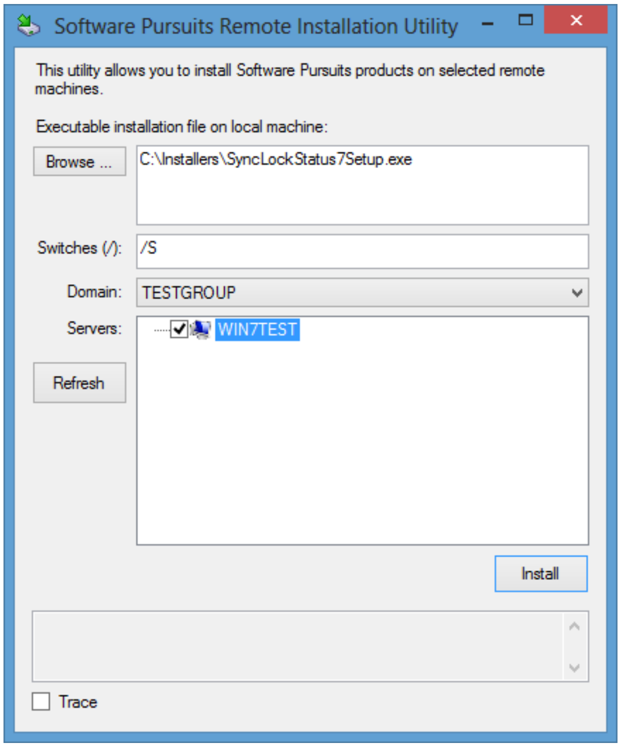
Executable installation file on local machine: C:\Installers\SyncLockStatus7Setup.exe

Switches (/): /S

Domain: TESTGROUP

Servers: □ WIN7TEST

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



Software Pursuits Remote Installation Utility

This utility allows you to install Software Pursuits products on selected remote machines.

Executable installation file on local machine: C:\Installers\SyncLockStatus7Setup.exe

Switches (/): /S

Domain: TESTGROUP

Servers: ☑ WIN7TEST

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).

Deployment via Manual Configuration

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

Configuring the Server Side

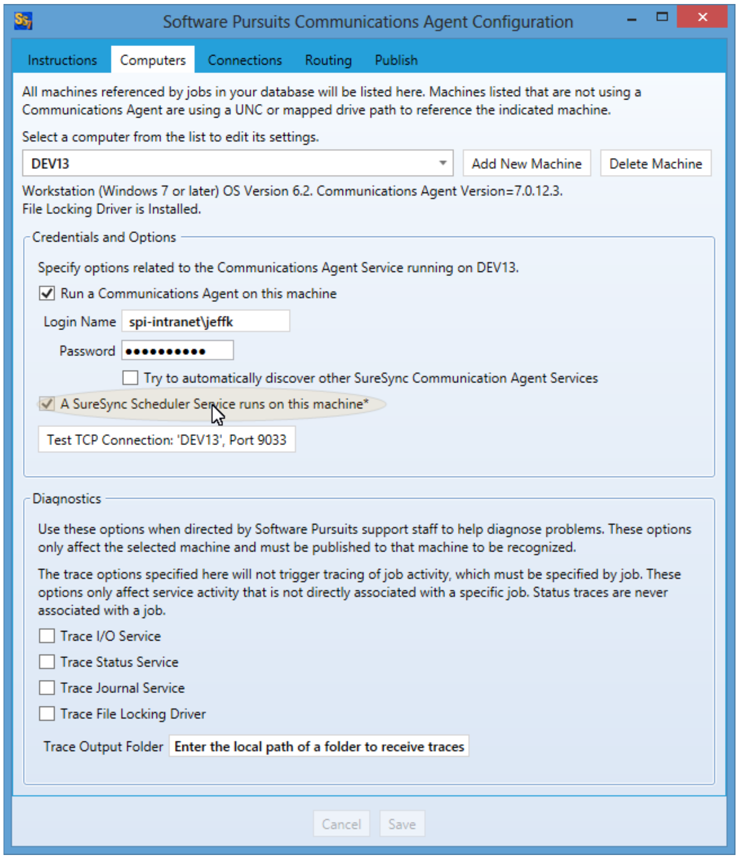
The SureSync software includes all necessary components to provide status to SyncLockStatus clients in a file locking environment out of the box. The Scheduler service within SureSync is responsible for distributing locking status information to SyncLockStatus clients. Within the Communications Agent configuration, an option exists to denote the machine(s) running Scheduler services. This flag is used to know what machine(s) will be providing locking status notifications.

Step 1: Ensure the Scheduler service option is set for the appropriate machine(s)

Within the Communications Agent Configuration Utility is an option that tells SureSync and other Communications Agent machines within the SureSync environment that a particular machine is running a Scheduler. This option should already be enabled because the Scheduler installation procedure automatically sets it. However, it’s recommended to confirm the option is set.

Launch the SureSync desktop, click on the Home button, then click Communications Agents and then click Configure Communications Agents. When the Communications Agent Configuration panel loads click on the Computers tab. From there, select your SureSync machine that is running the Scheduler service.

Once on that panel, ensure the option “A SureSync Scheduler Service runs on this machine” is checked as shown in the screenshot below.


Software Pursuits Communications Agent Configuration
Instructions
Computers
Connections
Routing
Publish
Add New Machine
Delete Machine
Test TCP Connection: 'DEV13', Port 9033
Cancel
Save

All machines referenced by jobs in your database will be listed here. Machines listed that are not using a Communications Agent are using a UNC or mapped drive path to reference the indicated machine.

Select a computer from the list to edit its settings.

DEV13

Workstation (Windows 7 or later) OS Version 6.2. Communications Agent Version=7.0.12.3.
File Locking Driver is Installed.

Credentials and Options

Specify options related to the Communications Agent Service running on DEV13.

☑ Run a Communications Agent on this machine

Login Name: spi-intranet\jeffk

Password: ••••••••••

☐ Try to automatically discover other SureSync Communication Agent Services

☑ A SureSync Scheduler Service runs on this machine*

Diagnostics

Use these options when directed by Software Pursuits support staff to help diagnose problems. These options only affect the selected machine and must be published to that machine to be recognized.

The trace options specified here will not trigger tracing of job activity, which must be specified by job. These options only affect service activity that is not directly associated with a specific job. Status traces are never associated with a job.

☐ Trace I/O Service

☐ Trace Status Service

☐ Trace Journal Service

☐ Trace File Locking Driver

Trace Output Folder: Enter the local path of a folder to receive traces

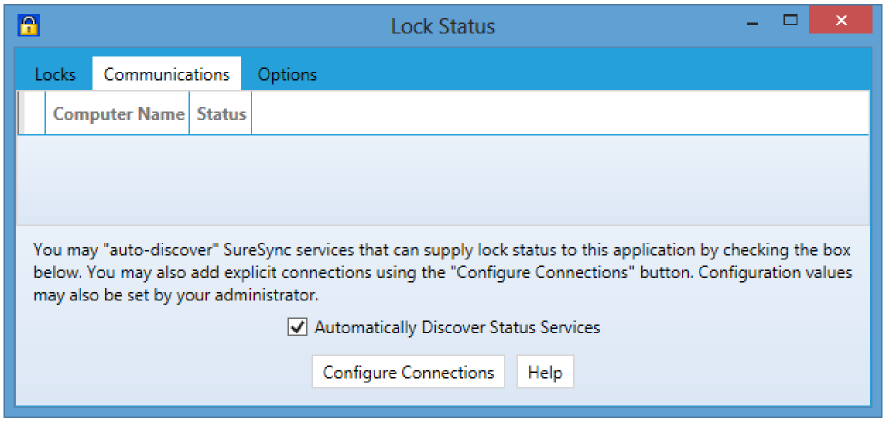
Configuring the Client Side

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

The SyncLockStatus client software is installed by launching the SyncLockStatus7Setup.exe. Follow the prompts to complete the installation and then launch SyncLockStatus.

Step 2: Configure SyncLockStatus to retrieve lock information from SureSync

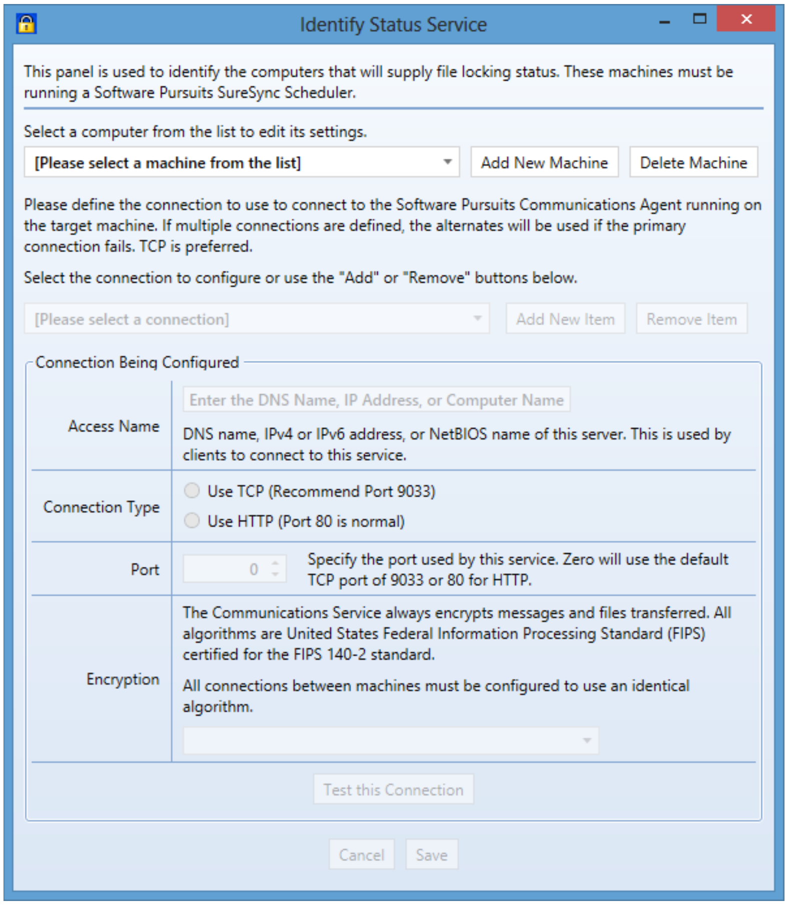
The next step involves defining the connection that should be used to retrieve lock status information from the SureSync Scheduler within SyncLockStatus. To do this, either double click on the SyncLockStatus tray icon and then click on the Communications tab. You can also right click on the same icon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



You may "auto-discover" SureSync services that can supply lock status to this application by checking the box below. You may also add explicit connections using the "Configure Connections" button. Configuration values may also be set by your administrator.

☑ Automatically Discover Status Services

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



This panel is used to identify the computers that will supply file locking status. These machines must be running a Software Pursuits SureSync Scheduler.

Select a computer from the list to edit its settings.

[Please select a machine from the list]

Please define the connection to use to connect to the Software Pursuits Communications Agent running on the target machine. If multiple connections are defined, the alternates will be used if the primary connection fails. TCP is preferred.

Select the connection to configure or use the "Add" or "Remove" buttons below.

[Please select a connection]

Access Name: Enter the DNS Name, IP Address, or Computer Name

DNS name, IPv4 or IPv6 address, or NetBIOS name of this server. This is used by clients to connect to this service.

Connection Type:

○ Use TCP (Recommend Port 9033)

○ Use HTTP (Port 80 is normal)

Port: 0

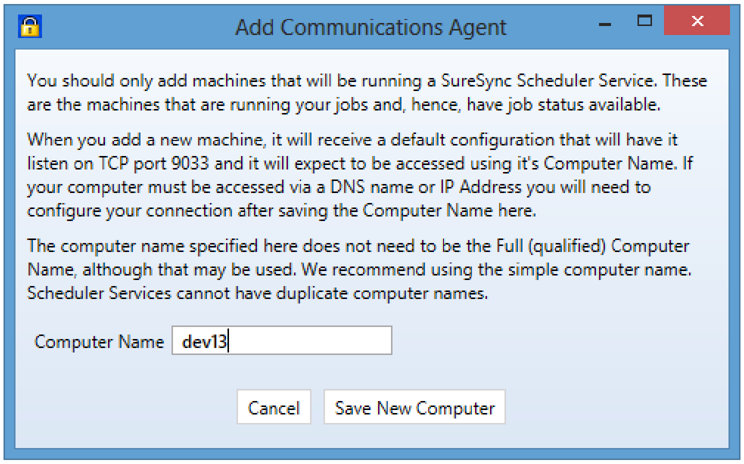
Specify the port used by this service. Zero will use the default TCP port of 9033 or 80 for HTTP.

Encryption:

The Communications Service always encrypts messages and files transferred. All algorithms are United States Federal Information Processing Standard (FIPS) certified for the FIPS 140-2 standard.

All connections between machines must be configured to use an identical algorithm.

Click the “Add New Machine” button. In the dialog that displays, you will enter the computer name of the SureSync machine running the Scheduler service.



Add Communications Agent

You should only add machines that will be running a SureSync Scheduler Service. These are the machines that are running your jobs and, hence, have job status available.

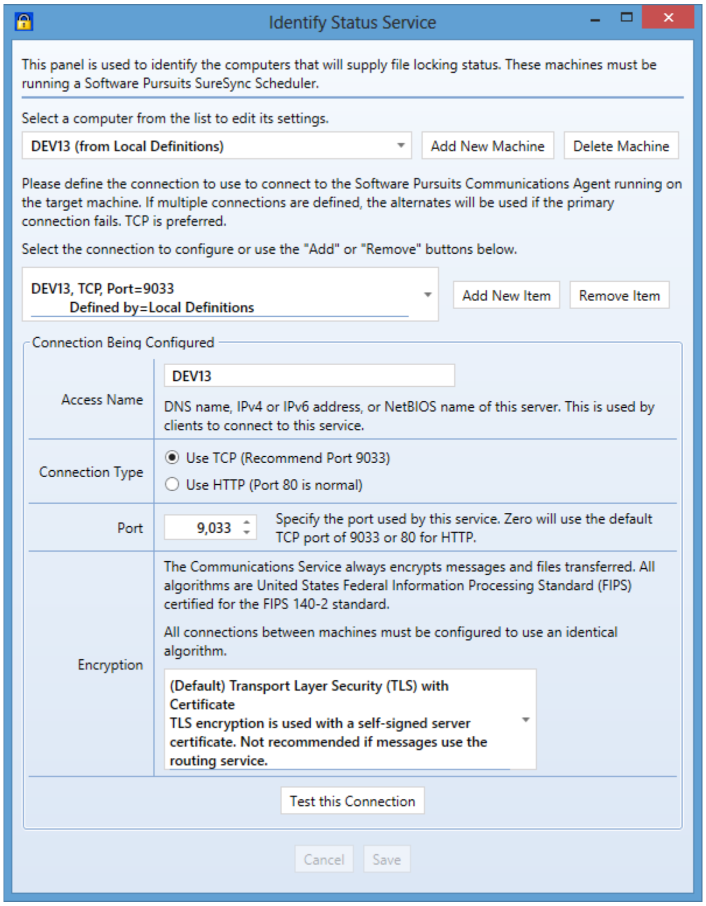
When you add a new machine, it will receive a default configuration that will have it listen on TCP port 9033 and it will expect to be accessed using it's Computer Name. If your computer must be accessed via a DNS name or IP Address you will need to configure your connection after saving the Computer Name here.

The computer name specified here does not need to be the Full (qualified) Computer Name, although that may be used. We recommend using the simple computer name. Scheduler Services cannot have duplicate computer names.

Computer Name: dev13

When you add a Communications Agent to SyncLockStatus, a default connection is created. This connection uses TCP port 9033. This is the same port used by SureSync's Communications Agent. 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.



Identify Status Service

This panel is used to identify the computers that will supply file locking status. These machines must be running a Software Pursuits SureSync Scheduler.

Select a computer from the list to edit its settings.

DEV13 (from Local Definitions)

Please define the connection to use to connect to the Software Pursuits Communications Agent running on the target machine. If multiple connections are defined, the alternates will be used if the primary connection fails. TCP is preferred.

Select the connection to configure or use the "Add" or "Remove" buttons below.

DEV13, TCP, Port=9033
Defined by=Local Definitions

Connection Being Configured

Access Name: DEV13
DNS name, IPv4 or IPv6 address, or NetBIOS name of this server. This is used by clients to connect to this service.

Connection Type:
● Use TCP (Recommend Port 9033)
○ Use HTTP (Port 80 is normal)

Port: 9,033
Specify the port used by this service. Zero will use the default TCP port of 9033 or 80 for HTTP.

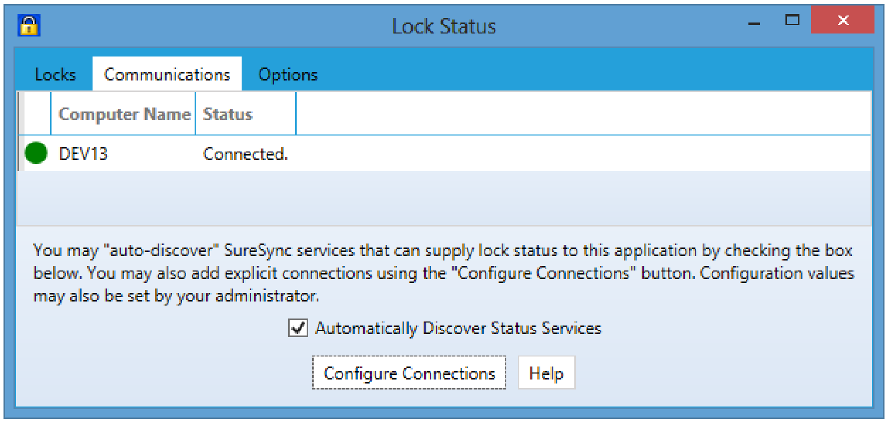
Encryption:
The Communications Service always encrypts messages and files transferred. All algorithms are United States Federal Information Processing Standard (FIPS) certified for the FIPS 140-2 standard.

All connections between machines must be configured to use an identical algorithm.

(Default) Transport Layer Security (TLS) with Certificate
TLS encryption is used with a self-signed server certificate. Not recommended if messages use the routing service.

You can click the "Test this Connection" button. Finally, click the "Save" button to save the configuration. You can then click the red "x" to close the panel.

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



	Computer Name	Status
●	DEV13	Connected.

You may "auto-discover" SureSync services that can supply lock status to this application by checking the box below. You may also add explicit connections using the "Configure Connections" button. Configuration values may also be set by your administrator.

☑ Automatically Discover Status Services

If you have a yellow status indicating no licenses found, this indicates that either your SureSync machine's Scheduler service is not running or no SyncLockStatus licenses are included in your license file. First, launch SureSync on the server side. Click on the Home button and then Licenses. Confirm that your license file includes SyncLockStatus workstation licenses. Once this is done, launch the Services MMC in Windows and confirm that the Software Pursuits SureSync 7 Scheduler service is running. Finally, launch SyncLockStatus on the workstation again and the connection should be successful.

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

Deployment via Command Line Switch Configuration Retrieval

In some network environments, network administrators do not want autodiscover broadcasts happening on their networks. Deploying SyncLokcStatus with a manual configuration addresses this issue. However, in large environments the overhead of configuring SyncLockStatus on each workstation is problematic. In these situations, the SyncLockStatus client can be installed with a command line switch that allows retrieval of a configuration file from a network share.

Configure the First SyncLockStatus Client

The SyncLockStatus 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 SyncLockStatus 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 SyncLockStatus, browse to the following folder:

- **Windows Vista / 2008 and Newer**: C:\Users\Public\Software Pursuits\SyncLockStatus7
- **Windows XP / 2003**: C:\Documents and Settings\All Users\Application Data\Software Pursuits\SyncLockStatus7

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

Install SyncLockStatus on the Client Machines

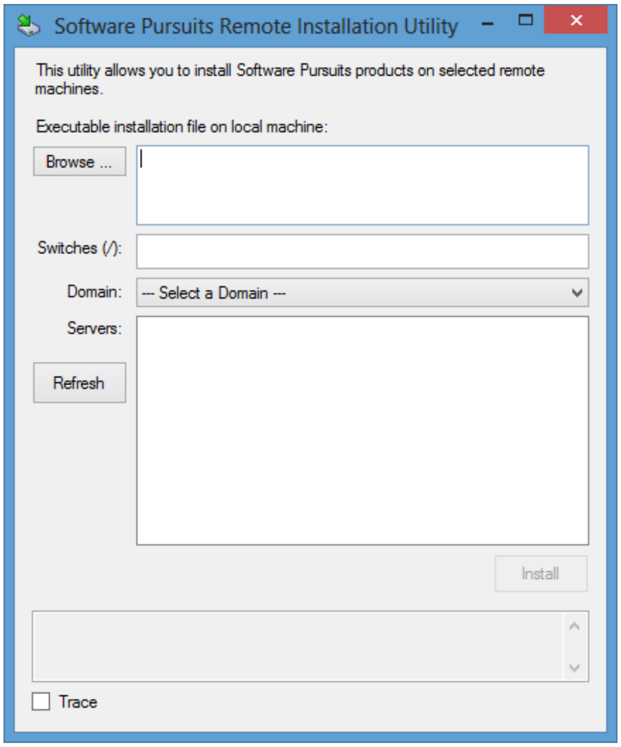
The final step to deploying SyncLockStatus involves executing the installer with a command line switch that provides the UNC path to load the configuration from. There are a number of different ways you can accomplish this task.

- Install on each client manually using the /XMLPath switch from a Run dialog. For example: "C:\Installers\SyncLockStatus7Setup.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 SyncLockStatus 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 7 and select Remote Installation Utility 7. The Software Pursuits Remote Installation Utility will launch. You should see a program window that looks like the screenshot below.



Software Pursuits Remote Installation Utility

This utility allows you to install Software Pursuits products on selected remote machines.

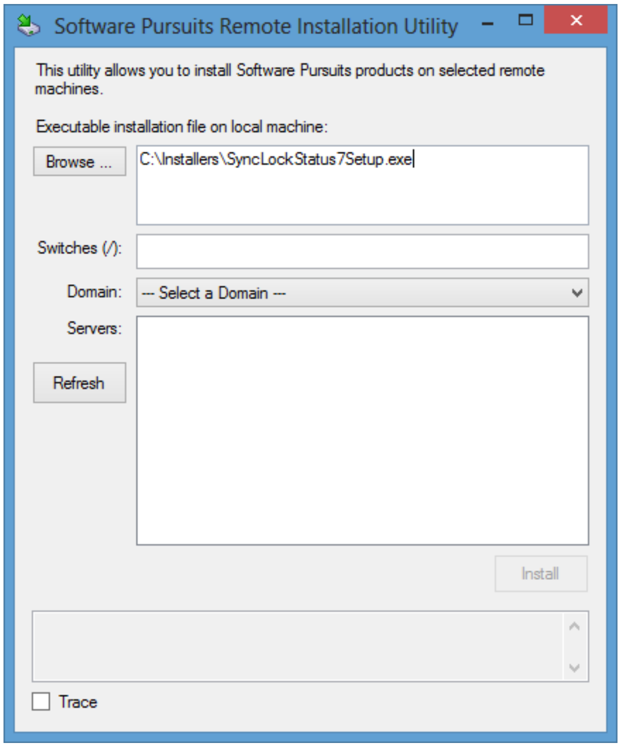
Executable installation file on local machine:

Switches (/):

Domain: --- Select a Domain ---

Servers:

Click the “Browse” button and select the SyncLockStatus7Setup.exe setup file or manually type the path to the file into the “Executable installation file on local machine” field.



Software Pursuits Remote Installation Utility

This utility allows you to install Software Pursuits products on selected remote machines.

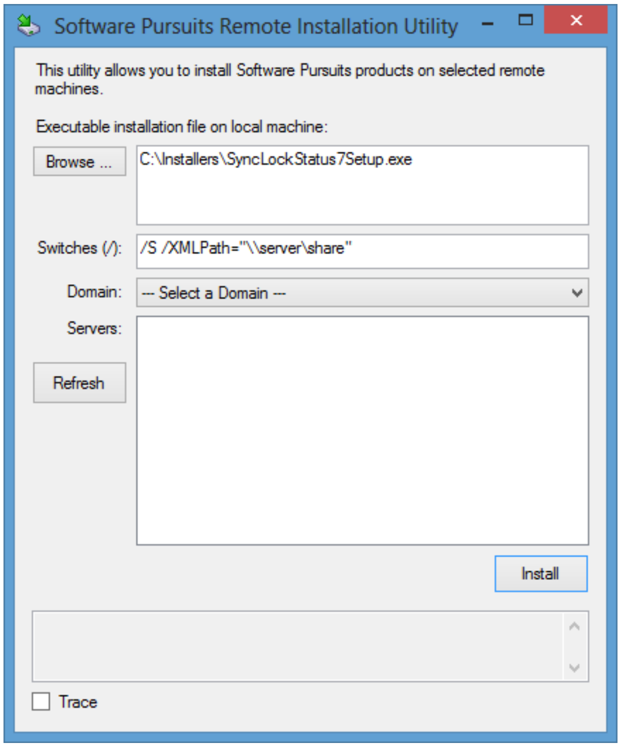
Executable installation file on local machine: C:\Installers\SyncLockStatus7Setup.exe

Switches (/):

Domain: --- Select a Domain ---

Servers:

To install the SyncLockStatus 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.



Software Pursuits Remote Installation Utility

This utility allows you to install Software Pursuits products on selected remote machines.

Executable installation file on local machine:

Browse ... C:\Installers\SyncLockStatus7Setup.exe

Switches (/): /S /XMLPath="\\server\share"

Domain: --- Select a Domain ---

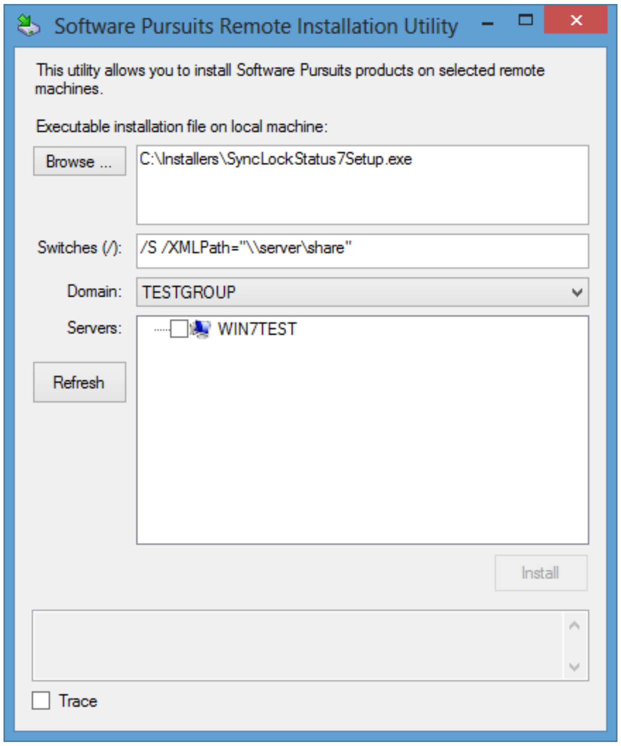
Servers:

Refresh

Install

□ Trace

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



Software Pursuits Remote Installation Utility

This utility allows you to install Software Pursuits products on selected remote machines.

Executable installation file on local machine:

Browse ... C:\Installers\SyncLockStatus7Setup.exe

Switches (/): /S /XMLPath="\\server\share"

Domain: TESTGROUP

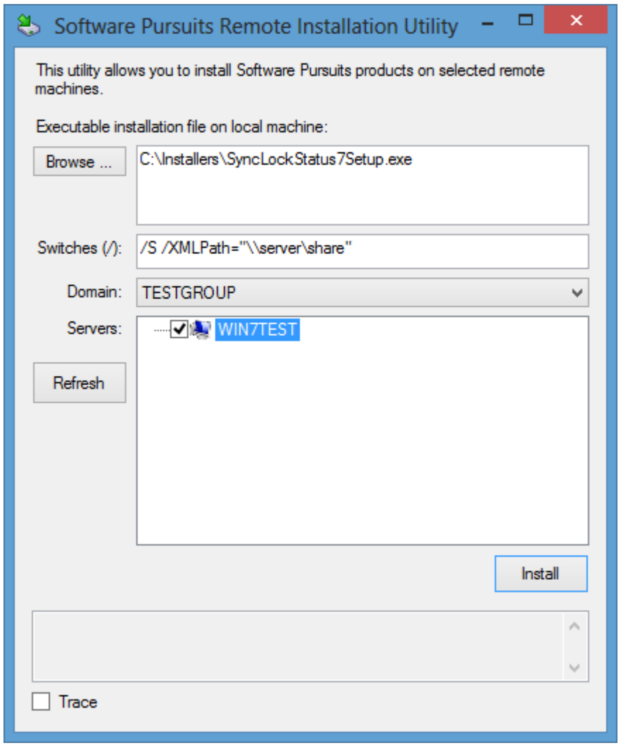
Servers: □ WIN7TEST

Refresh

Install

□ Trace

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



Software Pursuits Remote Installation Utility

This utility allows you to install Software Pursuits products on selected remote machines.

Executable installation file on local machine: C:\Installers\SyncLockStatus7Setup.exe

Switches (/): /S /XMLPath="\\server\share"

Domain: TESTGROUP

Servers: ☑ WIN7TEST

☐ Trace

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).