SyncLockStatus
Evaluator's Guide

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 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 with SP1; Windows 11; Windows 10; Windows 8.1; Windows 8; Windows 7 SP1
- **Processor:** Minimum: Dual-core CPU of at least 2.5Ghz; Recommended: Quad-core CPU or greater of at least 2.5Ghz
- **RAM (Server Side):** 4GB of free memory (recommended minimum)
- **RAM (Client Side):** 512GB of free memory (recommended minimum)
- **Hard Disk:** 40MB for the client components

Required Microsoft Components

SyncLockStatus requires 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 4.8

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.
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.

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.

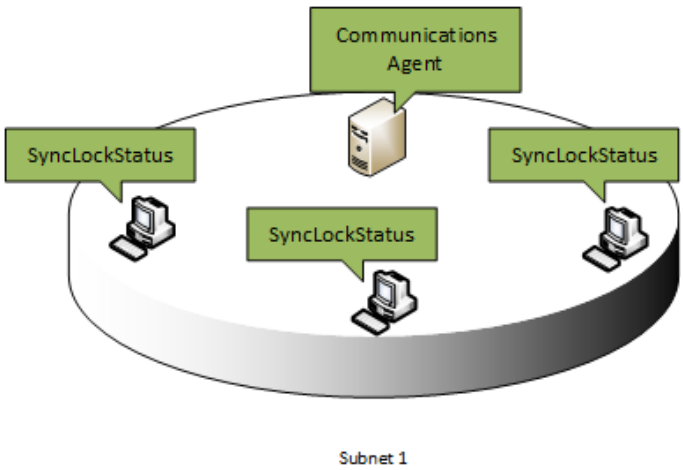
- **Software Pursuits Communications Agent**: The Communications Agent is the service within SureSync responsible for providing real-time monitors and other advanced functionality. This service includes the necessary functionality to support SyncLockStatus right out of the box. This makes it quick and 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 notifications.

The server-side components of SyncLockStatus are completely integrated into SureSync. 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

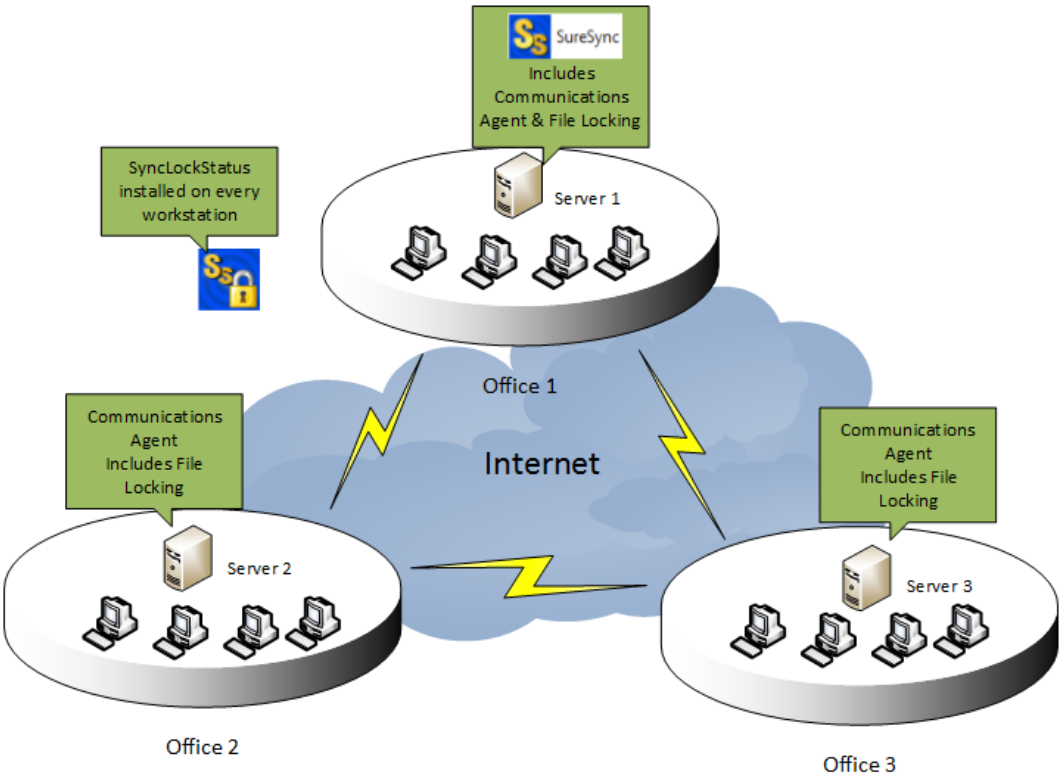
The graphic below represents a standard deployment of SyncLockStatus on a subnet in a network. The Communications Agent is installed on a server and SyncLockStatus on each workstation.



In small deployments such as the example above, SyncLockStatus 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 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 to forward TCP port 9031 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 the Server 1 machine properly. Please consult the documentation for your firewalls to make these configuration changes.

SyncLockStatus Licensing

SyncLockStatus licensing is included in the SureSync Collaboration Bundle with SyncLockStatus.

If you need to install additional Communications Agents to deploy with autodiscovery, no additional licensing is needed if 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:

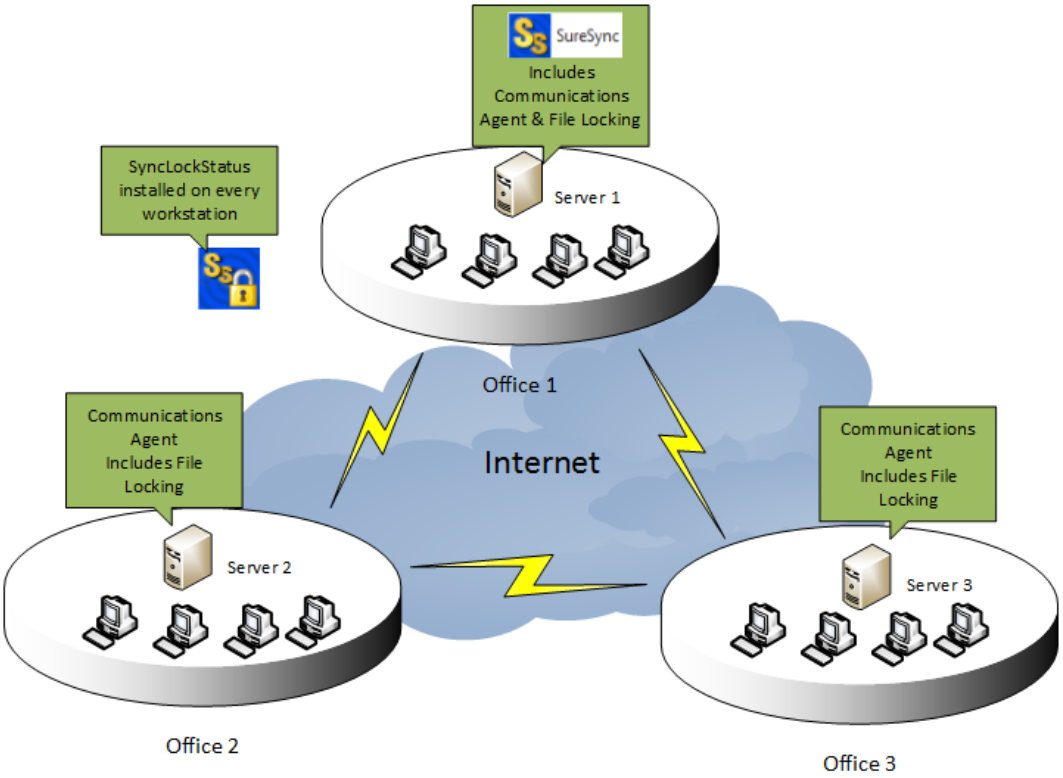
- Using auto discovery (recommended when possible)
- Manual configuration on each workstation
- Command line switch configuration retrieval during installation

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 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, 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:



The basic steps for this type of deployment will be:

- Identify a public IP or DNS name to use for SyncLockStatus. This 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 an Outbound Connection on each remote Communications Agent that defines how to connect back to main SureSync server.
- Configure each Communications Agent to respond to autodiscovery requests from the SyncLockStatus clients.
- Publish the configuration changes to the remote Communications Agent machines.
- Deploy SyncLockStatus to the client machines.

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

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

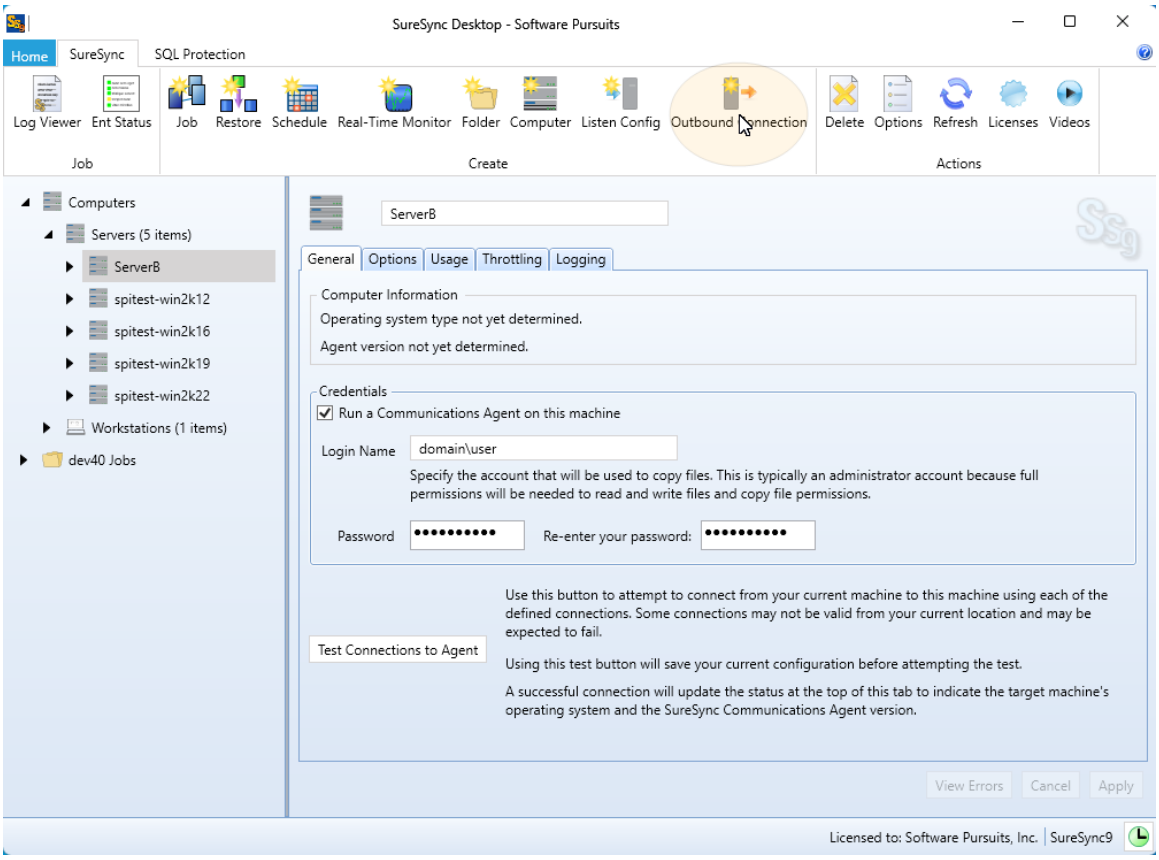
Step 2: Configure firewalls to allow the connections

Make any firewall configuration changes necessary to allow the traffic through to the Scheduler. Often these rules will be referred to as Port Forwarding or NAT rules. By default, the port that needs to be forwarded is TCP 9031. Please refer to the documentation for your firewall for further information.

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

An Outbound Connection must be configured for each remote Communications Agent that will provide connection information to SyncLockStatus clients. This Outbound Connection provides the IP address or DNS name identified in step 2 that clients can use to reach the Scheduler machine. In this guide's scenario, an Outbound Connection is needed for ServerB and ServerC.

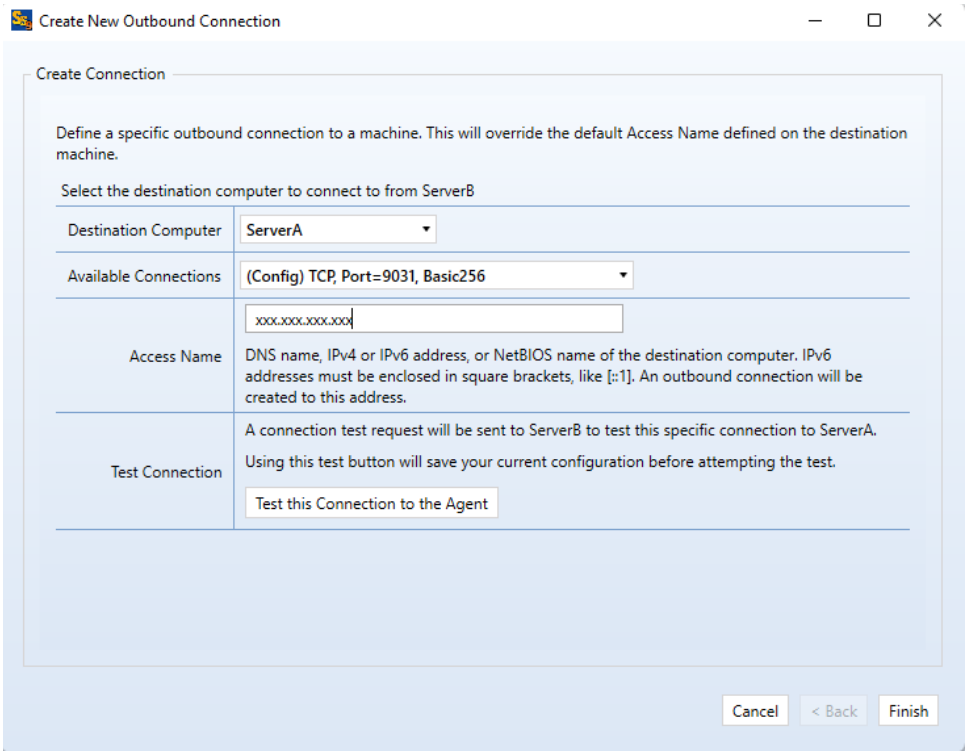
To define an Outbound Connection, expand Computers in the left tree of the SureSync Desktop and click on the machine you would like to add the Outbound Connection to. Click on the "Outbound Connection" button in the Ribbon Bar



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 SyncLockStatus 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 Scheduler machine.

The completed panel will look like:



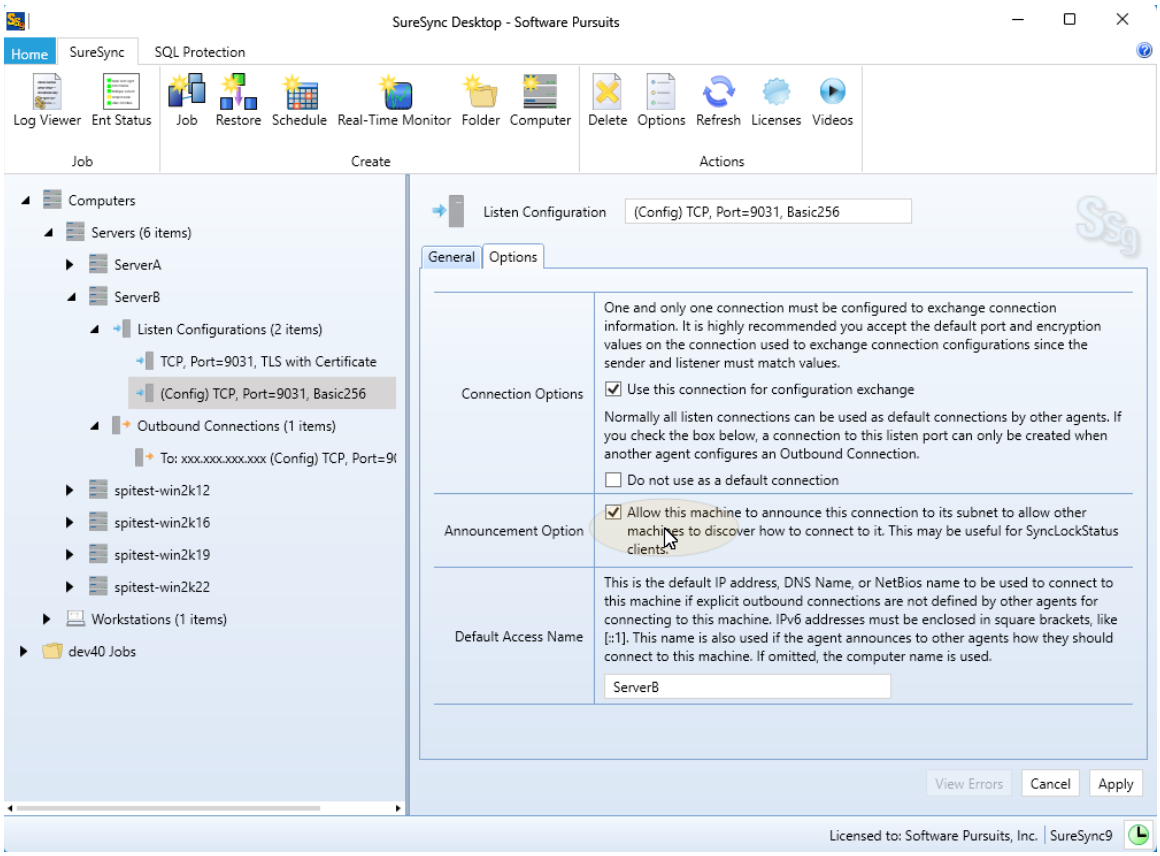
Click the 'Finish' button to add the Outbound Connection.

<u>Step 4: Configure Communications Agent(s) to respond to autodiscovery requests</u>

Each remote Communications Agent machine that will respond to autodiscovery requests from SyncLockStatus 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 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.



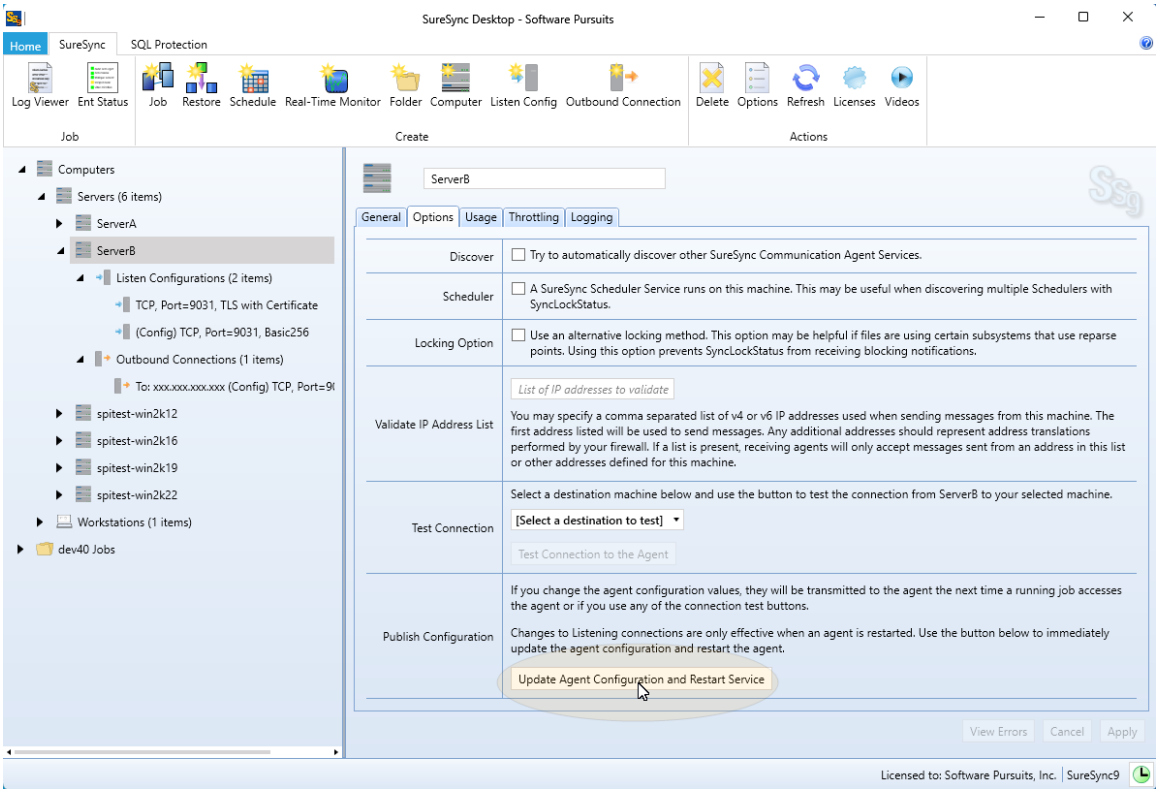
Click the “Apply” button to save the change.

<u>Step 5: Publish configuration information to remote Communications Agent(s)</u>

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

In the SureSync Desktop, under the Computers node of the left tree view and click on the machine you want to publish configuration information to. For example, ServerB.

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 Jobs, Schedules or Real-Time Monitors actively running to that machine you will encounter path losses while the restart occurs.



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 several ways you can accomplish this task.

- Install on each client manually
- Use a third party install management application

The /s switch can be used to install silently.

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

With manual deployment, no server-side configuration is required since each SyncLockStatus client machine will be configured with the information necessary for reaching the SureSync Scheduler machine.

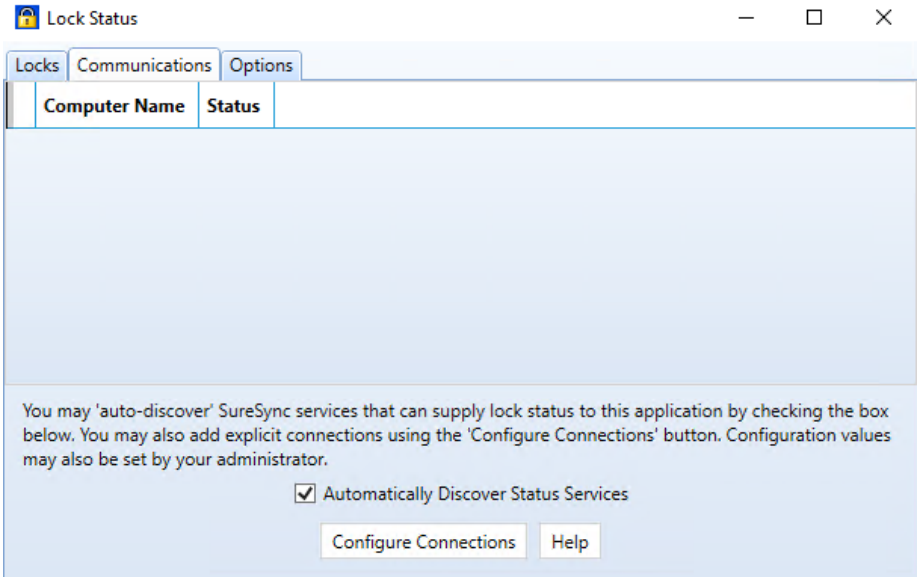
Configuring the Client Side

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

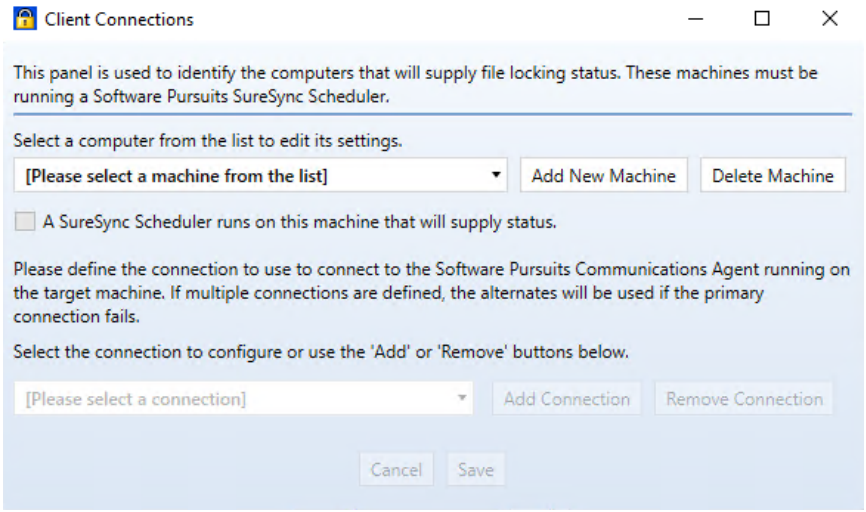
The SyncLockStatus client software is installed by launching the SyncLockStatus8Setup.exe. Follow the prompts to complete the installation and then launch SyncLockStatus.

Step 2: Configure SyncLockStatus to retrieve lock information from SureSync

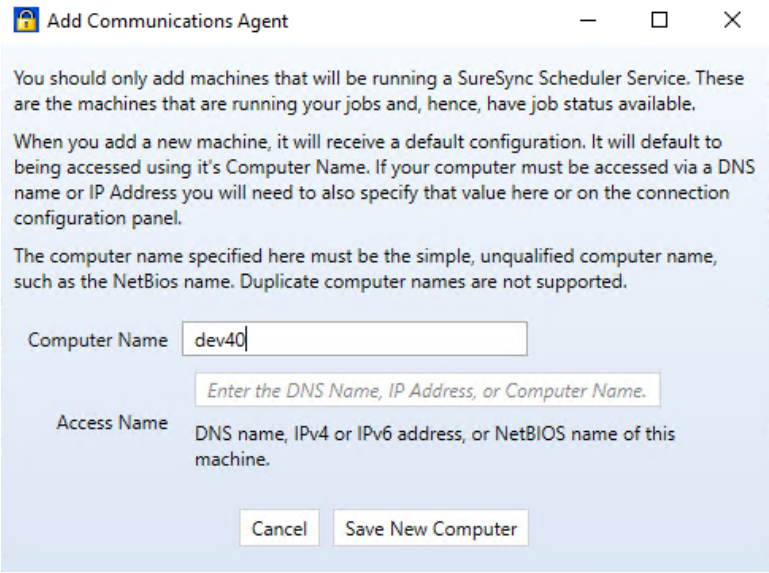
The next step involves defining the connection that should be used to retrieve lock status information from the SureSync Scheduler within SyncLockStatus. To do this, either double click on the SyncLockStatus tray icon and then click on the Communications tab. You can also right click on the same icon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



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

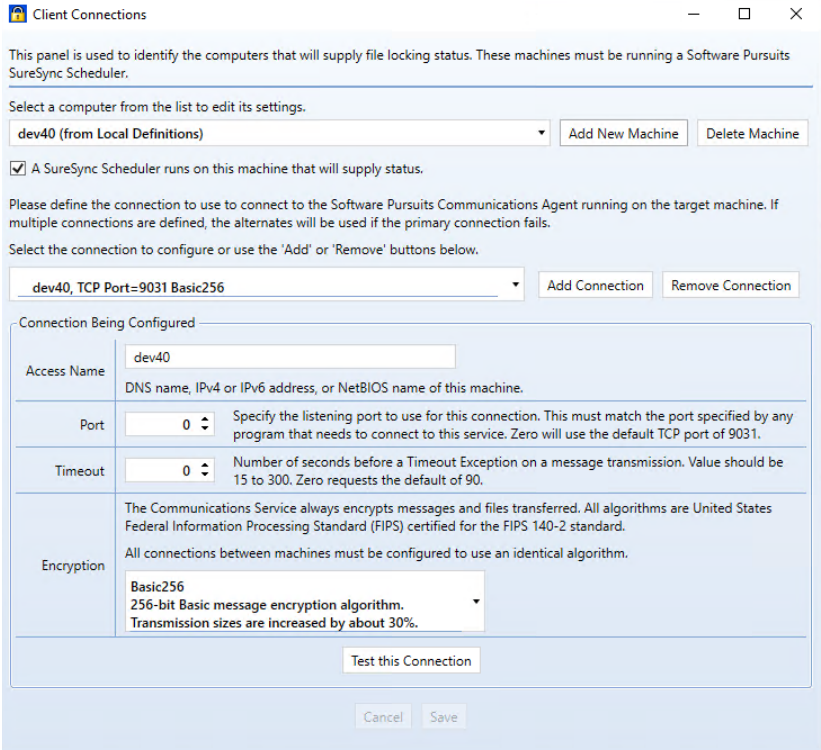


Click the “Add New Machine” button. In the dialog that displays, you will enter the computer name of the SureSync machine running the Scheduler service.



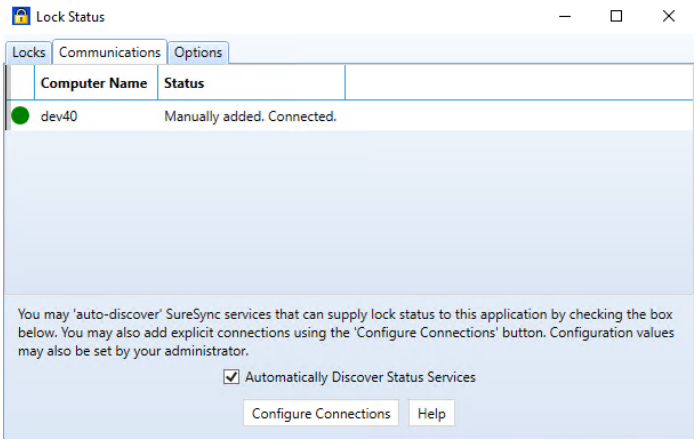
When you add a Communications Agent to SyncLockStatus, a default connection is created. This connection uses TCP port 9031. We strongly recommend using this port whenever possible as it reduces configuration.

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:



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 "Licenses" button in the Ribbon Bar. 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 9 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 SyncLockStatus 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: C:\Users\Public\Software Pursuits\SyncLockStatus9

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 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\SyncLockStatus8Setup.exe” /XMLPath=”\\server\share”
- 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.

The /s switch can be used to perform a silent installation.