

SyncLockStatus Evaluator's Guide



©2024 Software Pursuits, Inc.

Table of Contents

Introduction	2
System Requirements	2
Required Microsoft Components	2
Contact Information	2
SyncLockStatus Architecture	3
Deployment on a Single Subnet	3
Deployment in a Complex Network Environment	4
#1: Name Resolution	5
#2: Firewalls	5
SyncLockStatus Licensing	5
SyncLockStatus Deployment Methods	5
Deployment via Autodiscovery	6
Step 1: Identify a Public IP or DNS Name for use for SyncLockStatus	7
Step 2: Configure firewalls to allow the connections	7
Step 3: Configure an Outbound Connection for Remote Communications Agent(s)	7
Step 4: Configure Communications Agent(s) to respond to autodiscovery requests	8
Step 5: Publish configuration information to remote Communications Agent(s)	9
Step 6: Install SyncLockStatus clients on the workstations	10
Deployment via Manual Configuration	10
Configuring the Server Side	10
Configuring the Client Side	10
Step 1: Install the SyncLockStatus client on the appropriate workstation(s)	10
Step 2: Configure SyncLockStatus to retrieve lock information from SureSync	11
Deployment via Command Line Switch Configuration Retrieval	13
Configure the First SyncLockStatus Client	13
Create a Network Share to Store the Configuration File	13
Step 1: Select a Server to Store the Configuration File	13
Step 2: Configure the Share	13
Step 3: Copy the Configuration File to the Share	14
Install SyncLockStatus on the Client Machines	14

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 <u>SureSync Collaboration Bundle Evaluator's Guide</u> 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: <u>sales@softwarepursuits.com</u> Support e-mail: <u>support@softwarepursuits.com</u>

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.



Subnet 1

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

Seg. (1)		Su	reSync Desktop	- Software P	ursuits					-		×
Home SureSync	SQL Protection											0
Log Viewer Ent Statu	s Job Restore	Schedule Real-Time N	Aonitor Folder	Computer	See Config	Outbound Synnection	Delete	Dptions A	C Refresh) Licenses	V ideos	
Job			Create	•					Actions			
Computers	5 items) trB st-win2k12 st-win2k16	General Option Computer Info Operating syst Agent version	verB Is Usage Thre rmation em type not yet not yet determin	ottling Log determined ned.	ging						S	62
 spite spite 	st-win2k19 st-win2k22	Credentials	nunications Age	ent on this m	achine							
Workstat	ions (1 items)	Levia News	domain\user									
dev40 Jobs		Login Name	Specify the according permissions will	ount that wil be needed	be used to co to read and w	opy files. This is typically rite files and copy file p	r an admin ermissions	istrator acc	ount bea	cause full		
		Password	•••••	Re-en	ter your passv	vord:						
				Use this but defined con	ton to attemp nections. Som fail	t to connect from your e connections may not	current ma be valid fr	achine to th om your cu	is machi rrent loc	ne using e ation and	each of th may be	e
		Test Connectio	ns to Agent	Using this te	st button will	save your current config	guration b	efore attem	pting th	e test.		
				A successful operating sy	connection w stem and the	vill update the status at t SureSync Communicati	the top of ons Agent	this tab to i version.	indicate	the target	machine	's
									View Err	ors Ca	ancel	Apply
							Licens	ed to: Softv	vare Pur	suits, Inc.	SureSyn	c9 🕒

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:

Define a specific outboun machine.	d connection to a machine. This will override the default Access Name defined on the destin	ation
Select the destination co	mputer to connect to from ServerB	
Destination Computer	ServerA •	
Available Connections	(Config) TCP, Port=9031, Basic256	
	000000000000000000000000000000000000000	
Access Name	DNS name, IPv4 or IPv6 address, or NetBIOS name of the destination computer. IPv6 addresses must be enclosed in square brackets, like [::1]. An outbound connection will be created to this address.	
	A connection test request will be sent to ServerB to test this specific connection to ServerA	λ.
Test Connection	Using this test button will save your current configuration before attempting the test.	
	Test this Connection to the Agent	

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

Step 4: Configure Communications Agent(s) to respond to autodiscovery requests

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.

Su Hame SureSync SQL Protection	ireSync Desktop - Software Pu	suits	- c ×
Log Viewer Ent Status Job Restore Schedule Real-Time M	Monitor Folder Computer	Delete Options Refresh Licenses Videos	
Job Create		Actions	
 Computers Servers (6 items) ServerA ServerB Listen Configurations (2 items) 	General Options	on (Config) TCP, Port=9031, Basic256 One and only one connection must be con information. It is highly recommended you	figured to exchange connection accept the default port and encryption
TCP, Port=9031, TLS with Certificate TCP, Port=9031, TLS with Certificate Config) TCP, Port=9031, Basic256 TO: xoc.xoc.xoc.xoc.xoc.(Config) TCP, Port=90 snitest-win2k12	Connection Options	values on the connection used to exchange sender and listener must match values. Use this connection for configuration e Normally all listen connections can be usee you check the box below, a connection to 1 another agent configures an Outbound Co Do not use as a default connection	e connection configurations since the xchange d as default connections by other agents. If this listen port can only be created when nnection.
 spitest-win2k16 spitest-win2k19 	Announcement Option	Allow this machine to announce this co machines to discover how to connect to clients.	nnection to its subnet to allow other o it. This may be useful for SyncLockStatus
 spitest-win2k22 Workstations (1 items) dev40 Jobs 	Default Access Name	This is the default IP address, DNS Name, c this machine if explicit outbound connection connecting to this machine. IPv6 addresses [::1]. This name is also used if the agent and connect to this machine. If omitted, the con-	or NetBios name to be used to connect to ons are not defined by other agents for must be enclosed in square brackets, like nounces to other agents how they should mputer name is used.
		ServerB	
·		licen	View Errors Cancel Apply

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 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.

Home SureSync SQL Protection	SureSync Deskt	op - Software Pursuits		– – ×
Log Viewer Ent Status	Monitor Folder Computer Lis	ten Config Outbound Connection	Delete Options Refresh Licenses Videos	
Job	Create		Actions	
Computers Servers (6 items)	ServerB			
ServerA	General Options Usage	Throttling Logging		
ServerB	Discover	Try to automatically discover o	ther SureSync Communication Agent Services.	
 Site Configurations (2 items) TCP, Port=9031, TLS with Certificate 	Scheduler	A SureSync Scheduler Service r SyncLockStatus.	uns on this machine. This may be useful when d	iscovering multiple Schedulers with
 (Config) TCP, Port=9031, Basic256 Outbound Connections (1 items) 	Locking Option	Use an alternative locking method by points. Using this option preve	nod. This option may be helpful if files are using nts SyncLockStatus from receiving blocking noti	certain subsystems that use reparse fications.
 To: xxxxxxxxxxxxx (Config) TCP, Port=91 spitest-win2k12 spitest-win2k16 spitest-win2k19 	Validate IP Address List	List of IP addresses to validate You may specify a comma separate first address listed will be used to s performed by your firewall. If a list or other addresses defined for this	ed list of v4 or v6 IP addresses used when sendir end messages. Any additional addresses should is present, receiving agents will only accept mes machine.	ng messages from this machine. The represent address translations ssages sent from an address in this list
 Image: spitest-win2k22 Workstations (1 items) Image: dev40 Jobs 	Test Connection	Select a destination machine below [Select a destination to test] Test Connection to the Agent	v and use the button to test the connection from	n ServerB to your selected machine.
	Publish Configuration	If you change the agent configurat the agent or if you use any of the c Changes to Listening connections update the agent configuration and Update Agent Configuration and	ion values, they will be transmitted to the agent connection test buttons. are only effective when an agent is restarted. Us d restart the agent. Restart Service	the next time a running job accesses the button below to immediately
				View Errors Cancel Apply
٠			Licensed t	to: Software Pursuits, Inc. SureSync9

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:

🔒 Lock Status		-		\times
Locks Communication	s Options			
Computer Name	Status			
You may 'auto-discove below. You may also a may also be set by you	r' SureSync services that can supply lock status to this applica dd explicit connections using the 'Configure Connections' but ir administrator.	tion by che tton. Configu	cking the uration v	e box alues
	\checkmark Automatically Discover Status Services			
	Configure Connections Help			

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

Client Connections			-	- 🗆	×
This panel is used to identify the compute running a Software Pursuits SureSync Sche	ers that will supply file eduler.	e locking status. The	ese ma	chines must	be
Select a computer from the list to edit its	settings.				
[Please select a machine from the list]		Add New Mach	nine	Delete Mac	hine
the target machine. If multiple connection connection fails. Select the connection to configure or use	ns are defined, the alt the 'Add' or 'Remove	ernates will be used e' buttons below.	d if the	primary	
[Please select a connection]		Add Connection	Rem	ove Connect	ion
	Cancel Save				

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	-		×
Very should ask add as shines that will be available for Cons. Co		C	These

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. It will default to being accessed using it's Computer Name. If your computer must be accessed via a DNS name or IP Address you will need to also specify that value here or on the connection configuration panel.

The computer name specified here must be the simple, unqualified computer name, such as the NetBios name. Duplicate computer names are not supported.

Computer Name	dev40	
	Enter the DNS	Name, IP Address, or Computer Name.
Access Name	DNS name, IPv4 machine.	or IPv6 address, or NetBIOS name of this
	Cancel	Save New Computer

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.

🔒 Client Connec	tions																																																														-	-]					2
This panel is used SureSync Schedul	to identify the co er.	om	mp	mp	np	pu	ite	ers	s t	h	a	t	w	ril	II	s	u	ŗ	2	p	ł	y	f	il	e	1	0	c	k	ir	n	9		t	a	tu	IS		T	h	e	se	r	n	а	ł	ni	n	e	S I	m	u	st	k	e	n	ur	nn	ir	19	9	a	s	of	ftv	N	a	re	F	Pu	irs	51	ui	it	s
Select a computer	from the list to e	edit	dit	dit	lit	t it	ts	se	ett	tir	19	3	s,																																																														
dev40 (from Loo	cal Definitions)																																													•	•			A	d	d	٢	le	w	1	Ma	ac	h	ir	ne	•			D	e	ele	et	e	N	/a	ac	cł	hi	n
✓ A SureSync Sc	heduler runs on th	this	nis	nis	is	n	na	cł	nir	ne	2	tł	ha	at		w	il	I	s	ı	4	p	p	h	y	s	ta	at	tu	15	5.																																												
Please define the multiple connection	connection to use ons are defined, th	se to the	to ne a	to	to e i	al	te	nr	ne	te	t	te	o wi	tł ill	h	e b	e	50		f	e	N	ł	if	e	F	he	:	p	i	nii	t	5	C	0 7	n c	0	n	u	n	c	a	ti	oi i f	a	il	A s.	9	e	nt		u	n	ni	ng	9	01	1	th	ne		ta	rg	ge	t	m	na	ac	hi	in	e.		If	f	
select the connec	tion to configure of	e or	or u	or	or (u	se	tł	he	1	A	d	ld	ľ	0	or		R	ke	21	n	1	0	v	e	1	b	u	t	to	0	n	s	Ł	e	l	DI	N.	ł																																				
dev40, TCP Po	ort=9031 Basic256	56	5	5		_																																			_		•				1	40	do	d	С	0	n	he	c	ic	on				F	Re	n	10	V	e	C	0	n	ne	ec	ct	tio	0	n
- Connection Bein	g Configured																																																																										
	dev40																																																																										
Access Name	DNS name, IPv4	v4 o	or	or	or	r I	P١	/6	a	d	d	re	es	s		c	or	1	N	le	2	ł	31	c)	s	n	а	In	n	ne	•	0	f	tł	ni	s	n	18	ac	cł	nir	ne																																
Port	0 \$		S F	;	5	Sp	oe roj	ci gr	fy ar	t	h t	e h	li	is t	te n	e	ni	in		9 5		p	0	c	t	t	o	e		se t	e	f	0	r	ti	ni s	s	e	0	n /i	c	e	ct Z	ic e	n	i.	T	'n	is I (i n Us	nı	us t	t h	n	na de	to ef	:h au	tl	he t 1		P	0	rt p	s	pe t i	ec of	ci f	fie 91	ed 03	11	by I.	y	a	ar	Ŋ
Timeout	0 \$		1	1	1	N 15	ur 5 t	mk to	ое 3	er 00	0.	f	s Ze	e ar	0	0	n		de q	s	1		e'	fo		th	e		d	e	ir ef	n	e	o It	u	t	E		e),	P	ot	io	n	c	n	1	а	m	ne	25	sa	g	je	t	ra	n	sn	ni	ss	i	01	n.	۱.	/al	lu	e	s	h	01	ul	d		b	e	
	The Communica	catio	tio	tic	tio	on	D	Se	en	vie	-		a	lv		a	y	s	6		n	0	n 1		p	ts		m N	ne		s	s		9			ar Fo		1	fi	ile	s	t	ra	n	s	fe	en b-	re	d		A		al	g	or	it	hr	m	s	a	iri	e	U	ni	te	20	1	St	at	te	25	5		
Encryption	All connections	is be	bet	be	be	etv	ve	e	nı	m	a	c	h	in	16	2:	5	n	n	u	15	t		5	e	c	0	'n	nf	iq	g	u	Ir	e	d	t	0	u	s	e	2	'n	i	de	er	nt	ic	a	al	al	g	0	ri	th	m																				
	Basic256 256-bit Basic n Transmission si	me size	nes ize	ze	ze	ss	ag	ge	e ir	n	c	rj e	yF	pt se	ti	d	h		a	le a	9	b		i	t		m 3()	%	5.								•																																					
																					Т	e	s	t	t	h	is	(с	0	51	n	n	20	t	ic	or	h																																					

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:

12 Software Pursuits, Inc. www.SoftwarePursuits.com

8	Lock Status		-		×
Lock	S Communications	Options			
	Computer Name	Status			
•	dev40	Manually added. Connected.			
You belo mag	i may 'auto-discover ow. You may also ad y also be set by you	' SureSync services that can supply lock status to this applicatio d explicit connections using the 'Configure Connections' buttor administrator.	n by cheo n. Configu	king the aration va	box lues
		Automatically Discover Status Services			
		Configure Connections Help			

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.

> 13 Software Pursuits, Inc. www.SoftwarePursuits.com

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.