**Protecting Your Mobile Workforces' Data**

# Contents

# Introduction

The growth of mobile workforces has made the task of protecting corporate data stored on laptops a difficult challenge. IT departments must ensure that company files stored on these devices are backed up to a central location; providing a method for data recovery in the event of a system crash, a physically damaged system or even a stolen laptop. This can be daunting because laptops aren't bound to one spot on the network like a desktop machine. An employee might work from their desk at the office, from home, or even from a wireless hotspot in a coffee house. Regardless of where they are working, these users expect and need to have their files protected.

Software Pursuits' file synchronization / replication software, SureSync, provides multiple methods of easily protecting this type of data. This whitepaper will outline the process of configuring SureSync to protect data on laptops that are on the move and discusses the strengths and weaknesses of each method so you can select the option which is most appropriate for your organization.

SureSync, coupled with the SPIAgent Add-on, provides a great deal of flexibility in helping address this issue. The SPIAgent Add-on provides many performance enhancing features and TCP/IP based communications. With the SPIAgent you can synchronize to any Windows machine accessible by IP address or DNS name; even over the Internet. The SPIAgent provides the option to encrypt the data during transfer to secure data being synchronized over the Internet, making SureSync with the SPIAgent an ideal fit for protecting these remote laptops.

# Dealing with Dynamic IP Addresses

When installing SureSync on the server and accessing the SPIAgent service on remote machines you need to be able to access the laptops via a resolvable DNS name or IP address over the Internet. This is not an issue when installing SureSync on the laptops and the SPIAgent on the server if the server has a public IP address. If the server is using a private IP address then you would still need to deal with a dynamic IP address but it would be a single address instead of many.

Most Internet Service Providers assign IP addresses using DHCP which means the IP address of a user's laptop could change at any time. This is particularly true when the user is on the go and connecting to various networks. The SPIAgent add-on references machines by IP address or DNS name. In the instance where the machine does not have a fixed IP address and does not have a resolvable DNS name it would seem that you could not synchronize to it but that is where dynamic DNS services come into the picture.

There are many dynamic DNS services and the features offered vary from service to service. Regardless of the service the basic concept is always the same. You sign up for an account with a dynamic DNS provider and create a DNS name which will be in the format of "name.domain.com". You then install a piece of software on the laptop which monitors your IP address. Each time the IP address changes the software updates your laptop's IP address with their service. This means that "name.domain.com" always points to the laptop in question and

allows you to use that name when you configure the SPIAgent to successfully access that machine regardless of the network the laptop is on at the moment.

Some services are free and others charge fees. Entering the search term "Dynamic DNS" into your favorite search engine will return many options. A couple of these are:

- Dynamic Network Solutions, Inc. (http://www.dyndns.com)
- No-IP Dynamic DNS (http://www.no-ip.com)
- DNS2Go (http://www.dns2go.com)
- TZO (http://www.tzo.com)
- EasyDNS (http://www.easydns.com)

Once you have selected a service you would need to configure a Dynamic DNS name for each laptop. You will also need to install any required software from the Dynamic DNS provider of your choice on each of the laptops to handle the updating of the IP addresses.

# Determining Where to Install SureSync

The biggest decision in deploying SureSync to protect laptop machines is determining if you want to install SureSync on a server and control all of the jobs centrally or if you want to install a full copy of SureSync on each of the laptops and allow the user some level of control over the synchronization.

### *Deploying SureSync on the Server*

Advantages

- Simplified management of the SureSync environment.
- Changes to the SPIAgent can be easily deployed to the laptops.

Disadvantages

- If running Scheduled synchronizations it's possible for some laptops to be missed for multiple runs of the Schedule if the laptop is not connected.

Installing SureSync on the server provides the benefit of central management. You will only need to keep track of one SureSync console. Each laptop would have a copy of the SPIAgent service installed to provide the TCP/IP communications and other advanced functionality that is essential to the project.

SureSync provides a method of easily updating remote agents so this method of installation is by far the easiest in terms of management. When a new version of SureSync is released you would upgrade the server and then deploy the new agent files to the workstations using SureSync's built-in agent update tools.

**NOTE:** Details on updating remote agents can be found in the SureSync help file.

The negative aspect of installing SureSync on the server is that you have no way of knowing when people are connected to your network or to the Internet. Therefore, running on a scheduled basis is a bit of a challenge because some mobile workers may not be connected during the time the job is running. For example, if you configured a Schedule to run every 30 minutes it's possible that some laptops would not be on the network or accessible through the Internet. When this happens an error is logged and that particular machines data is not backed up.

To minimize the connection issue, jobs can be run more frequently, increasing the odds that a user's machine will be accessible to SureSync. You can eliminate the issue entirely by running a real-time monitor. A real-time monitor will monitor the job and add the laptop path back into the synchronization when it is available. If you configure the Monitor for a low retry time like 2 minutes then you will find machines are quickly synchronized whenever they are accessible from SureSync.

### *Deploying SureSync on the Laptops*

Advantages

- User can launch job when connected via a desktop shortcut.
- Job can be configured to run when logging on, when the computer starts and more using the Scheduled Tasks feature in Windows.
- Don't have to worry about dynamic IP addresses except on the server if applicable.

Disadvantages

- A SureSync installation on each laptop creates more management work for tasks like upgrading to the current version.
- A user could either not run the synchronization job or find a way to disable the scheduled task.

Installing SureSync on each laptop provides some additional options to run replication / synchronization jobs. You can configure a desktop shortcut using the command line interface, SyncCmd, which enables to end user to run the backup job whenever they are connected and it is convenient for them.

There is also the option of using the Scheduled Tasks functionality in Windows to schedule a job to be run in an automated manner. The choices available with this option include running the job when the computer starts, when the user logs on, once daily, once a week and more. If you require more flexibility in launch times you could always use the SureSync Scheduler installed on the laptop but that requires a username and password to be defined. If the user accounts on the laptop have password changes frequently this can pose a problem because you must update the password for the SureSync Scheduler service when the username's password changes.

There are some disadvantages to installing the full SureSync application on the laptops. While there is an automated method of updating remote SPIAgent installs built-in to SureSync, there is no such functionality for a remote full SureSync install. The SureSync installer must be run when

an upgrade is performed. This can make upgrading to a new version of SureSync more time consuming.

There is also the issue of a user simply not running the job (if you're using the shortcut method) or disabling the scheduled task which could happen if the user is running as an administrator on the machine in question.

# Determining the Appropriate Rule Type

When backing up data you will want to use a one-way synchronization / replication rule. SureSync offers a number of one-way rules and they all behave a little differently, depending on user preference. For a complete understanding of SureSync's Rules, review "Rule Methods Summary" in the SureSync help file.

A Mirror rule is a logical choice because it makes an exact copy of the contents of the directories in question. The only potential problem is that it deletes files so if someone accidentally deletes a file and a synchronization job runs that delete will be propagated to the server backup copy. If you do not want files removed from the destination when the user deletes them from their laptop then you would want to consider a Recent Master Copy or Differing Master Copy rule. In this case it might be necessary to occasionally run a Mirror rule copy of the job to "clean up" files that reside on the backup destination but not on the laptop.

# How to Configure the Server-Side Scenario

The following steps should be performed to deploy SureSync using the Server-Side Scenario:

- Install SureSync on the server
- Launch SureSync on the server to create your database
- Install the SureSync Scheduler on the server
- Install the SPIAgent on each laptop
- Configure the laptop SPIAgent machines in Tools | SPIAgent Setup
- Configure the Relations used to synchronize the laptop data to the server
- Configure the required Schedule(s) or Real-Time Monitor(s)

It is recommended that you download the SureSync Evaluator's Guide from http://www.softwarepursuits.com/suresync/support.asp#gettingstarted to use with this white paper to aide in configuring the various aspects of SureSync. This document will outline the steps you should take but the Evaluator's Guide provides a step-by-step view of how to configure each aspect of SureSync.

*Install SureSync on the Server*

The first step to deploying this scenario is to install the full SureSync application on the server of your choosing. The full SureSync installer can be downloaded from http://www.softwarepursuits.com/suresync/download.asp.

*Launch SureSync on the Server to Create Your Database*

When you launch SureSync the first time an Access database is created in C:\Documents and Settings\All Users\Application Data\Software Pursuits\SureSync. The database is named SureSync.mdb. If you want to use a SQL database or a different database location please consult the SureSync help file and the SureSync Getting Started Guide for further detail.

*Install the SureSync Scheduler on the Server*

Once SureSync is installed and the database created you will want to install the SureSync Scheduler service on the server. The Scheduler is the service responsible for running Schedules and Real-Time Monitors at their appropriate times.

To install your Scheduler simply go to the Tools menu and then click on Schedulers. Then click the 'Install' button and follow the on-screen prompts.

*Install the SPIAgent on all Workstations*

The SPIAgent installer can be obtained from http://www.softwarepursuits.com/suresync/download.asp. This installer should be run on each laptop that you plan to protect with SureSync.

*Configure the Laptop SPIAgent Machines in SPIAgent Setup*

Each remote SPIAgent machine must be configured in SPIAgent Setup on the SureSync server machine. A detailed walk-through for configuring the SPIAgent can be found in the SureSync Evaluator's Guide.

When synchronizing data from remote laptops you will be using local accounts on the laptops to gain access to the machine because the machine is not going to be connected to a domain. Remember to enter the username in as "machinename\username" (minus the quotes) to ensure proper operation.

*Configure the Relations used to Synchronize the Laptop Data to the Server*

A Relation should be created for each laptop which you're protecting with SureSync. For example, if you have 40 machines which you're backing up there should be 40 Relations. These can be bundled under a single Schedule or Real-Time Monitor to run the jobs in an automated fashion. Please consult the "Determining the Appropriate Rule Type" section of this document for information on which rule to use and the SureSync Evaluator's Guide for setup instructions for the Relation.

Each Relation should synchronize to a different target folder. This keeps the data from each laptop in an organized folder structure. It is recommended to use the machine name of the laptop as the folder name on the server. This makes it easy to determine at a glance which files belong to which laptop.

*Configure the Required Schedule(s) or Real-Time Monitor(s)*

The final step is to determine how you want to run the Relations in an automated manner to ensure that data on the laptops is protected.

If you're planning on using a Schedule it should be configured to run every X number of minutes. It's important that the Schedule run fairly frequently. When a Schedule launches it will synchronize data from any connected laptops to the server and report "path not found" errors for the laptops which are not connected at the time the job is run. It will then reschedule and run again. The next time it runs the process repeats itself. Due to the fact that some machines will most likely always be offline when a Schedule runs you want to run the Schedule frequently to catch machines when they are connected. Repeating every 10 or 15 minutes should be adequate.

A Real-Time Monitor on the other hand will monitor the paths of all the laptops. As users establish a connection, the path on their laptop will be added back into the monitor and files will be synchronized. When the user disconnects they will be removed from the monitor. This is generally far more efficient than running a Schedule.

# How to Configure the Laptop-Side Scenario

The following steps should be performed to deploy SureSync using the Laptop-Side Scenario:

- Install the SPIAgent on the server
- Install SureSync on each laptop which will be protected
- Launch SureSync on each laptop to create your database
- Install the SureSync Scheduler on each laptop (optional)
- Configure the server SPIAgent on each laptop in SPIAgent Setup
- Configure the Relation to synchronize laptop data to the server
- Configure the SureSync Relation on the laptop to run in an automated manner

It is recommended that you download the SureSync Evaluator's Guide from http://www.softwarepursuits.com/suresync/support.asp#gettingstarted to use with this white paper to aide in configuring the various aspects of SureSync. This document will outline the steps you should take but the Evaluator's Guide provides a step-by-step view of how to configure each aspect of SureSync.

*Install the SPIAgent on the Server*

The SPIAgent installer can be obtained from http://www.softwarepursuits.com/suresync/download.asp. This installer should be run on the server which will serve as the target for the laptop synchronizations.

*Install SureSync on all Workstations*

The full SureSync application should be installed on each laptop which will be synchronizing files to the server. The full SureSync installer can be downloaded from http://www.softwarepursuits.com/suresync/download.asp.

*Launch SureSync on each Laptop to Create Your Database*

When installing SureSync on the laptops it is recommended that you use an Access database. In this scenario the laptop is only going to be running a couple of Relations at maximum and there is no need for the extra overhead of running a SQL database for this light of a synchronization load.

When you launch SureSync the first time an Access database is created in C:\Documents and Settings\All Users\Application Data\Software Pursuits\SureSync. The database is named SureSync.mdb. You will want to launch the SureSync desktop on each laptop so the database is created.

*Install the SureSync Scheduler on each Laptop (optional)*

This step only needs to be performed if you're going to run a Schedule or Real-Time Monitor on each of the laptops. The Scheduler is the service responsible for running Schedules and Real-Time Monitors at their appropriate times.

To install your Scheduler simply go to the Tools menu and then click on Schedulers. Then click the 'Install' button and follow the on-screen prompts.

**NOTE:** If you are going to use another method of running the Relation on the laptops such as through a desktop shortcut or using the Windows Scheduled Tasks feature to run the job at log on you can skip this step.

*Configure the server SPIAgent on each Laptop in SPIAgent Setup*

On each laptop you will need to configure the SPIAgent settings for the server machine. A detailed walk-through for configuring the SPIAgent can be found in the SureSync Evaluator's Guide.

When synchronizing data from the laptop with SureSync installed on the laptop you will need to use a domain account which has access to the server in question. This would be represented as domainname\username in SPIAgent Setup. Each user's domain account could be used giving them permission to just their folder or you could use a special SureSync account which has access only to the folders in question and synchronize using that account.

*Configure the Relation to Synchronize Laptop Data to the Server*

Each laptop machine needs to have a Relation created in its SureSync database to synchronize the required data from the laptop to the backup server. Please consult the "Determining the

Appropriate Rule Type" section of this document for information on which rule to use and the SureSync Evaluator's Guide for setup instructions for the Relation.

Each Relation should synchronize to a different target folder. This keeps the data from each laptop in an organized folder structure. It is recommended to use the machine name of the laptop as the folder name on the server. This makes it easy to determine at a glance which files belong to which laptop.

***Configure the SureSync Relation on the laptop to run in an automated manner***

There are three different methods in which you can run the Relation on the laptop in an automated manner.

Run the Relation under a Schedule or Real-Time Monitor

You can run the Relation on the laptop via a Schedule or a Real-Time Monitor just as you can with the server side scenario. The same problems with this method remain. There will be times that the job runs where the laptop is not connected to the Internet. This means you need to configure the Schedule to run frequently to increase the chances that it runs during a period when the laptop is connected or you can run a Real-Time Monitor which stays active all the time and will recover the server path when connected to the Internet allowing the files to be synchronized.

If you're planning on using a Schedule it should be configured to run every X number of minutes. It's important that the Schedule run fairly frequently. When a Schedule launches it will synchronize data from any connected laptops to the server and report "path not found" errors for the laptops which are not connected at the time the job is run. It will then reschedule and run again. The next time it runs the process repeats itself. Due to the fact that some machines will most likely always be offline when a Schedule runs you want to run the Schedule frequently to catch machines when they are connected. Repeating every 10 or 15 minutes should be adequate.

A Real-Time Monitor on the other hand will monitor the path on the laptop and synchronize / replicate files to the remote server when the laptop is connected to the Internet and that remote server is accessible. When the user disconnects from the Internet the Real-Time Monitor keep retrying the connection to the remote server so when an Internet connection is restored the synchronization / replication to the remote server will resume.

Run the Relation via a SyncRun shortcut on the desktop

SureSync inclues a command line utility called SyncRun which can be used to create a desktop shortcut which launches the Relation in question. This method guarantees that the user's laptop is connected to the Internet and can connect to the server because the user manually runs the job when connected. The downside to this method is that the user has to run the job which they may not always remember to do.

To create the shortcut, right click on the Windows Desktop, then select New and finally Shortcut to launch the Windows Create Shortcut wizard.
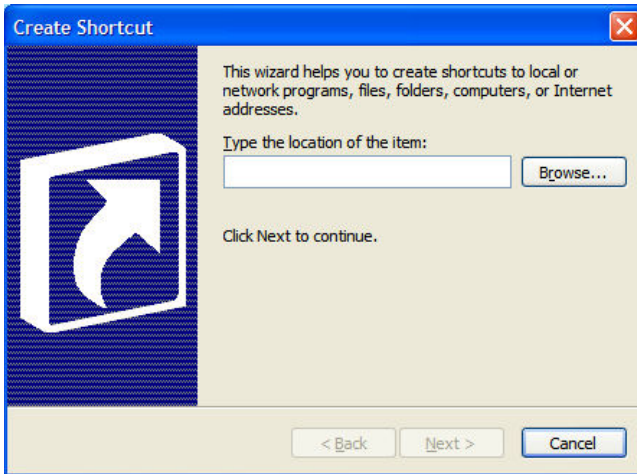
Under "Type the location of the item:" you will want to enter in the path to SyncRun and the correct operands to launch the Relation.

The command below is an example of the basic command to run a Relation. There are additional options available to you which are detailed in the SureSync he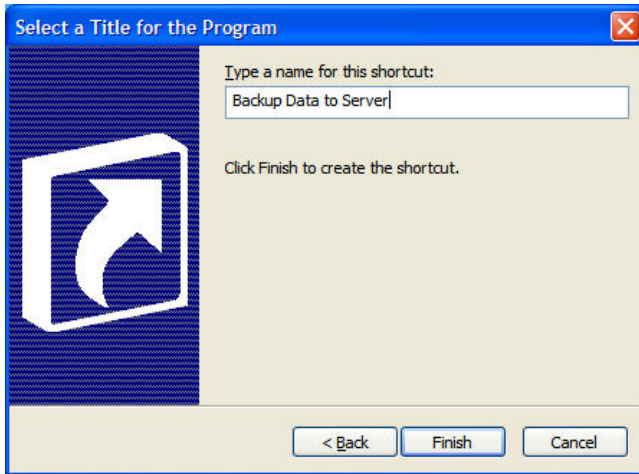lp file under the SyncCmd topic. *Note: In the command there is a space before the first / and then another space before /R. There is no space after R and the first quote. All quotes are needed.*

"C:\Program Files\Software Pursuits\SureSync\SyncCmd.exe" /XStart /R"Relation Name"
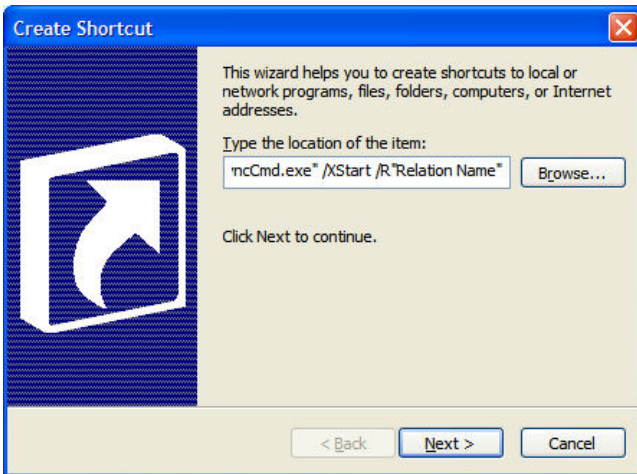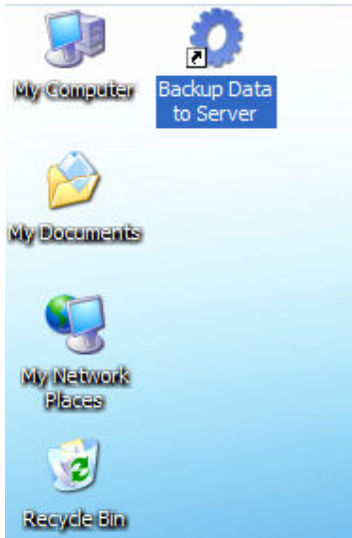


Click "Next" to continue.

The next panel of the Wizard lets you give the shortcut a name. We recommend something like "Backup Data to Server".



Click "Finish" and the shortcut will be created on the Desktop.



The user can now click on the "Backup Data to Server" shortcut on the desktop whenever they are connected to the Internet and want to backup their data to the server.

Run the Relation using SyncRun and Windows Scheduled Tasks

The Windows Scheduled Tasks feature lets you schedule an application to run at certain times. The available options are Daily, Weekly, Monthly, One Time Only, When My Computer Starts, and When I Log On.

This example will configure a SyncRun command to run the Relation using the When I Log On setting. This example assumes that you're running Windows XP. The steps might be slightly different on other operating systems.
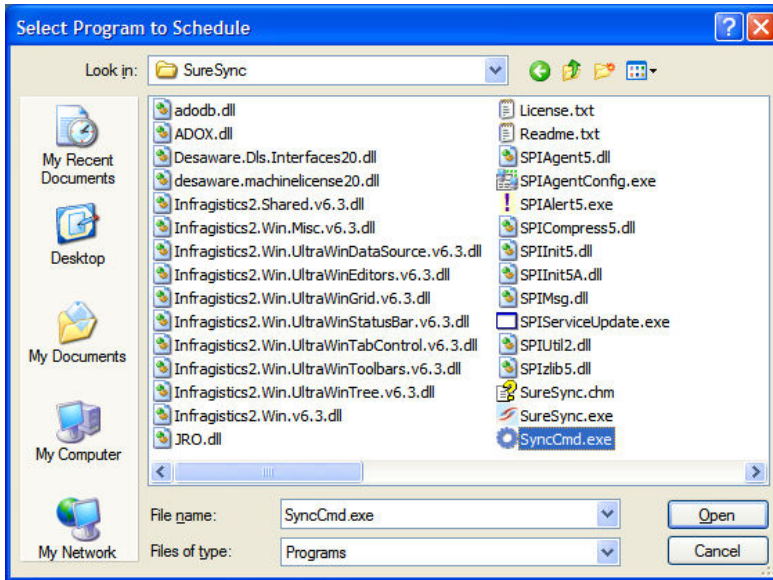
To access the Scheduled Tasks in Windows launch Control Panel, then click on Scheduled Tasks, and finally double click on "Add Scheduled Task" to launch the Scheduled Task Wizard.
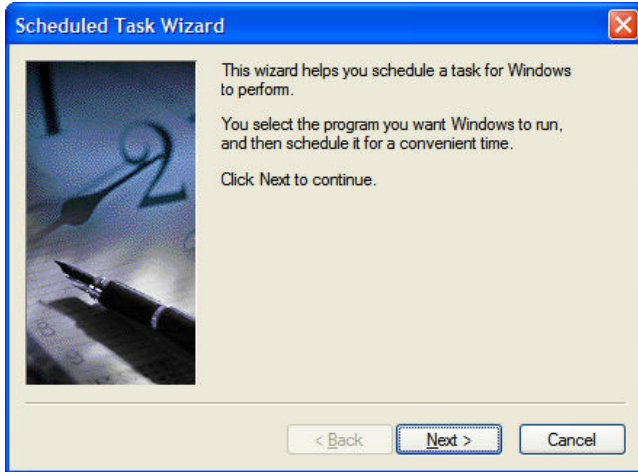


Click "Next" to start the configuration.
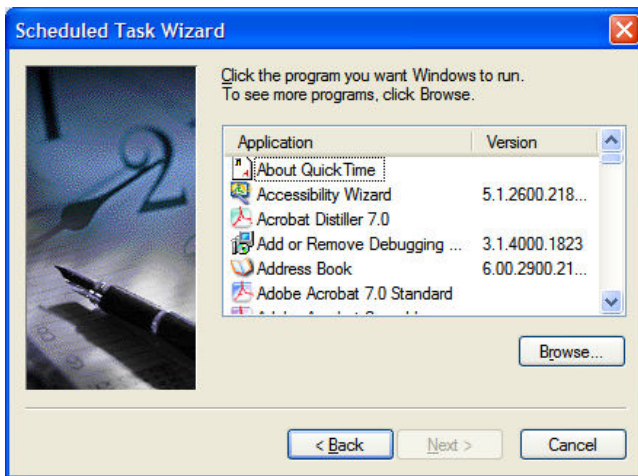


Click on the "Browse" button, browse to C:\Program Files\Software Pursuits\SureSync, select SyncCmd.exe and then click "Open".

The next panel displays a name for the task. This will default to "SyncCmd" but you can change it to any name you like. This name is only displayed in the Scheduled Task list.

This panel also defines the frequency with which you want the job run. For this example we will select "When I log on".
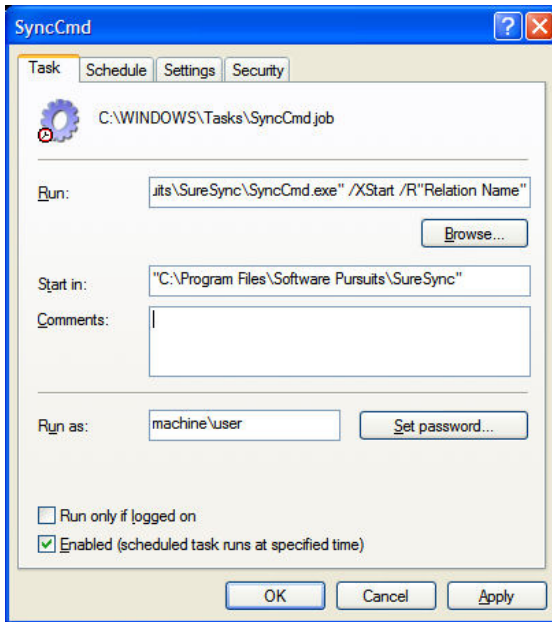


Click "Next" to continue.

The next panel asks for the username and password that the scheduled task should run under. Enter that in here in the format of machine\user or domain\user.

Click "Next" to continue.



On the next panel check the box for "Open advanced properties for this task when I click Finish" and then click "Finish".

On the next panel we need to modify the "Run" text field so it contains the /XStart /R"Relation Name"

The entire command under "Run" should be:

"C:\Program Files\Software Pursuits\SureSync\SyncCmd.exe" /XStart /R"Relation Name"

Click "Apply" and "OK" to complete the configuration. The job will now run at the defined times.

# Licensing

The two methods of protecting laptop machines are licensed differently. This section provides details on determining the licenses that you would need for your environment. We always recommend that you consult with a member of our Sales Team to ensure you receive appropriate licensing information. You will find our contact information at the end of this document.

### Server Side Scenario

When licensing SureSync for the server side scenario you will need a base SureSync server license, a SPIAgent server license, and a SPIAgent workstation license for each laptop.

*Example: If you're synchronizing data from 10 workstations to 1 server you would need 1 server SureSync license, 1 server SPIAgent license, and 10 workstation SPIAgent licenses.*

***Workstation Side Scenario***

When licensing SureSync for the workstation side scenario you will need a server SPIAgent license, a workstation SureSync license for each laptop and a workstation SPIAgent license for each laptop.

*Example: If you're synchronizing data from 10 workstations to 1 server you would need 1 server SPIAgent license, 10 workstation SureSync licenses, and 10 workstation SPIAgent licenses.*

# Conclusion

SureSync provides a powerful and flexible way to backup data from remote laptop machines. You can configure SureSync to grab data from the laptops via an installation on the server which benefits from centralized administration or you can place SureSync on the workstation side which gives the end user control a certain level of control over the process and ensures that the user is connected when the synchronization is performed.  This flexibility gives you a number of powerful ways to protect your remote laptop user's data.

# Contact Us

If you have any further technical questions about deploying SureSync in your environment please contact our support team at support@softwarepursuits.com or via phone at 650-372-0900. Technical Support is available from 8AM to 5PM Pacific Standard Time Monday through Friday.

Our sales team can be reached at sales@softwarepursuits.com or via phone at 800-367-4823.