Son of Snoop on Steroids (SOSOS)

Introduction

SOSOS is a computer hardware and software inventory program. It gathers over 220 pieces of information about computers and optionally stores this information in a database. It can be run locally or can be used by an administrator to scan a network.

It gathers *hardware information* such as CPU, memory, hard drives, and serial numbers; *software information* such as operating system, installed software, and software components; *configuration information* such as IP address, running processes, desktop settings, and services; and *security-related information* such as shared resources, modems, account policies, security patches, and virus activity.

SOSOS is actually a suite of programs consisting of the following:

- SOSOS – the main application (includes all of the features below)
- RunSOSOS – a command-line version for gathering data
- PollSOSOS – a command-line version for network scanning
- ViewSOSOS – a read-only interface to SOSOS database
- ConfigureSOSOS – a setup utility for the SOSOS suite

Release Information

SOSOS is available only as Visual Basic "source code". That means that you'll have to use Microsoft Visual Studio 2005 to compile the source code into a usable program that will run on your computer. Luckily, Microsoft provides the Visual Basic 2005 Express Edition as a free download at http://msdn.microsoft.com/vstudio/express/vb

SOSOS is completely free of charge. The SOSOS source code is considered in the "public domain". That means you can do anything you want with it, to include making money from it.

Download

The "official" home of SOSOS is at http://www.sosos.emmet-gray.com

Emmet P. Gray
egray1@hot.rr.com
http://www.sosos.emmet-gray.com

Son of Snoop on Steroids (SOSOS)
Setup and Configuration Guide

Introduction

SOSOS is a computer hardware and software inventory program. It gathers over 220 pieces of information about computers and optionally stores this information in a database. It can be run locally or can be used by an administrator to scan a network.

It gathers *hardware information* such as CPU, memory, hard drives, and serial numbers; *software information* such as operating system, installed software, and software components; *configuration information* such as IP address, running processes, desktop settings, and services; and *security-related information* such as shared resources, modems, account policies, security patches, and virus activity.

Note: SOSOS does not gather any personal information, look at emails, user documents, or track Internet activity.

SOSOS is actually a suite of programs consisting of the following:

- SOSOS – the main application (includes all of the features below)
- RunSOSOS – a command-line version for gathering data
- PollSOSOS – a command-line version for network scanning
- ViewSOSOS – a read-only interface to SOSOS database
- ConfigureSOSOS – a setup utility for the SOSOS suite

SOSOS is completely free of charge. The SOSOS source code is considered in the “public domain”. That means you can do anything you want with it, to include making money from it. There is no licensing requirement.

The "official" home of SOSOS is at http://www.sosos.emmet-gray.com

Section 1 – Compiling the Source Code

SOSOS is available only as Visual Basic "source code". That means that you'll have to use Microsoft Visual Studio 2005 to compile the source code into a usable program that will run on your computer.

Microsoft provides the Visual Basic 2005 Express Edition as a free download at http://msdn.microsoft.com/vstudio/express/vb. However, the Express Edition cannot build Setup projects (for deployment as an MSI file).

Important: If you intend to use SOSOS to gather information from PCs running Windows Vista, then you should also compile the SOSOS suite on a development PC that's running Windows Vista.

Note: Compiling the SOSOS suite under Windows XP/2000/2003 requires that you use correct Visual Basic project files (.vbproj) from the WinXP_vbproj.zip file*

See Appendix E for a complete "walk through" on how to compile the SOSOS source code.

1.1 SOSOS Distribution Kit

The SOSOS Distribution Kit consists of a zip file that contains the Visual Basic source code, documentation, and a starter "prototype" database.

The files in the Distribution Kit have the following structure:

Root
- Changes.txt – A text-based change log
- DatabaseChanges.txt – Change log for the database
- Empty.mdb – Microsoft Access starter database
- Empty.sql – SQL script for a SQL Server starter database
- FAQ.doc – Frequently Asked Questions (Microsoft Word)
- LocalIntranet.msi – Install file to configure .Net Code Access Security
- Read Me.doc – Introduction (Microsoft Word)
- Setup and Configuration Guide.doc (this document)
- User's Guide.doc – SOSOS User's guide (Microsoft Word)
- ConfigureSOSOS – source code directory
  - ConfigureSOSOS.sln – Visual Basic solution file
- PollSOSOS - source code directory
  - PollSOSOS.sln – Visual Basic solution file
- RunSOSOS - source code directory
  - RunSOSOS.sln – Visual Basic solution file
- SOSOS - source code directory
  - SOSOS.sln – Visual Basic solution file
- ViewSOSOS - source code directory
  - ViewSOSOS.sln – Visual Basic solution file

WinXP_vbproj.zip – Project files for compiling under Windows XP
WinVista_vbproj.zip – Project files for compiling under Windows Vista

1.2 Other SOSOS Applications

There are several other optional applications that are available from the SOSOS web site that are not included in the Distribution Kit.

- AlertSOSOS - Queries the SOSOS database for a list of anomalies. If an anomaly is found it will send emails, send pop-up messages, and write event log entries.
- BackupSOSOS - Archives the contents of the SOSOS database on an SQL Server database into a Microsoft Access database.
- ErrorLogSOSOS - Converts the SOSOS text-based error log file into a Microsoft Access database. This allows for a systematic analysis of errors to identify trends or spot troubled PCs.
- MgmtConsoleSOSOS - a GUI-based "management console" for performing administration tasks for PCs in a LAN. Draws heavily upon the SOSOS database and other SOSOS-related programs.
- ProcessSearch - Searches the SOSOS database against a list of several hundred known spyware, addware, and Peer to Peer applications
- RunSOSOS_fx1.1 – A version of RunSOSOS that uses version 1.1 of the .Net Framework. Useful for organizations that have not fully migrated from v1.1 to v2.0.
- SoftwareSearch - Similar to ProcessSearch, but searches Installed Software
- SOSOS_fx1.1 – A reduced functionality version of SOSOS that uses version 1.1 of the .Net Framework.

1.3 Compiling

The SOSOS source code is configured for compiling under Windows Vista. However, the distribution kit includes the Visual Basic Project Files (*.vbproj) configured for Windows XP in a zip file called WinXP_vbproj.zip. When compiling under Windows XP/2000/2003, you should extract these project files (replacing the existing versions). There is also a WinVista_vbproj.zip file that allows you to switch back to the Windows Vista versions of the project files.

It is always a good idea to compile any .Net applications from a development PC that has the latest operating system, .Net Framework version, and all up-to-date patches. This will ensure that the application is using the latest versions of the required DLLs. After the application is compiled, it will run on all platforms/operating systems that support the .Net framework.

The SOSOS suite automatically runs as a 32-bit application on 32-bit operating systems and runs as a 64-bit application on 64-bit operating systems. There is no additional configuration required to support this feature.

The typical way to compile the application is to double click on each application's solution file. This will launch Visual Studio and load the program's source code.

Important: You should change the encryption keys in the SOSOS\crypt.vb file from their default settings. Pick any 8 bytes for the variables TheKey() and Vector(). You must recompile all members of the SOSOS suite when you change the encryption keys.

To compile, right click on the project in the Solution Explorer (typically in the upper right hand corner) and select the *Build* option. Alternately, you can use the *Build* menu and select *Build Solution*.

After compiling, the contents of the bin\Release directory will contain all of the files required to run the application.

See Section5.4 for information about deploying the applications.

1.4 Compiling the Setup Projects

Each application has a separate "Setup" project to create an MSI file for deploying the application to other PCs.

To compile the Setup Project, right click the *Setup* project in the Solution Explorer and select the *Build* option. You should build the Setup project only after you have tested the applications and performed all of the configuration tasks.

The application's source code should be configured using the ConfigureSOSOS utility prior to creating the Setup projects. It is recommended that you use the ConfigureSOSOS utility on the "*app.config*" file inside the source code directory. This will allow the Setup project to perform a clean build of the application using the settings you configure.

See Section 2 on how to use the ConfigureSOSOS utility.

Important: Failure to perform this step on the source code will mean that you will have to configure each application on the target PC after deployment.

Note: Visual Basic 2005 Express Edition does not support the Setup project type. Sorry…

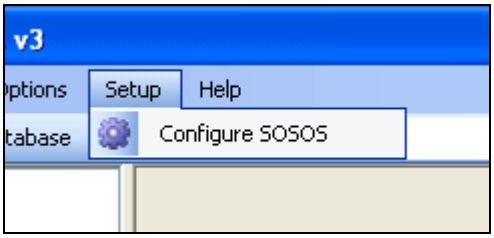
Section 2 – Configuring SOSOS

The run-time settings for each member of the SOSOS suite are contained in XML-based configuration files with a file extension of ".config". For example, the settings for the *SOSOS.exe* application are contained in a file called *SOSOS.exe.config*.

The SOSOS application has its own built-in configuration utility. All of the other members of the SOSOS suite require the use of the stand-alone ConfigureSOSOS utility.

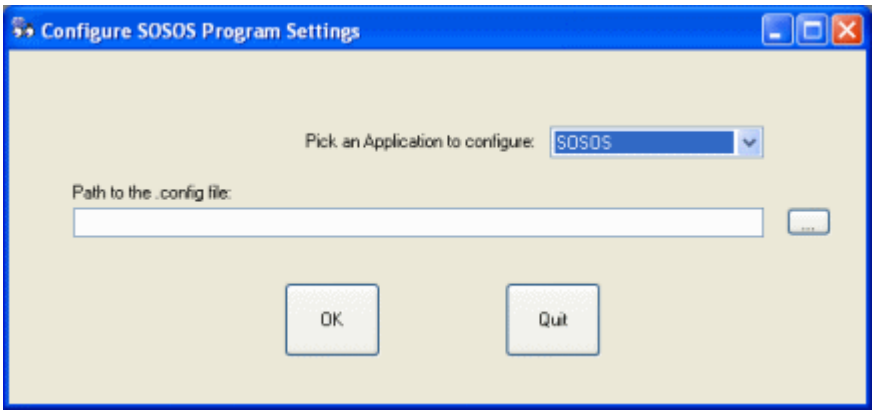
2.1 The Configuration Utility

To launch the configuration utility inside the SOSOS application, you use the main menu to select *Setup* and then click on *Configure SOSOS*. Changes made are not effective until the program is restarted.



Alternately, you can use the stand-alone ConfigureSOSOS application.

Note: You must use this utility to configure the other members of the SOSOS suite.

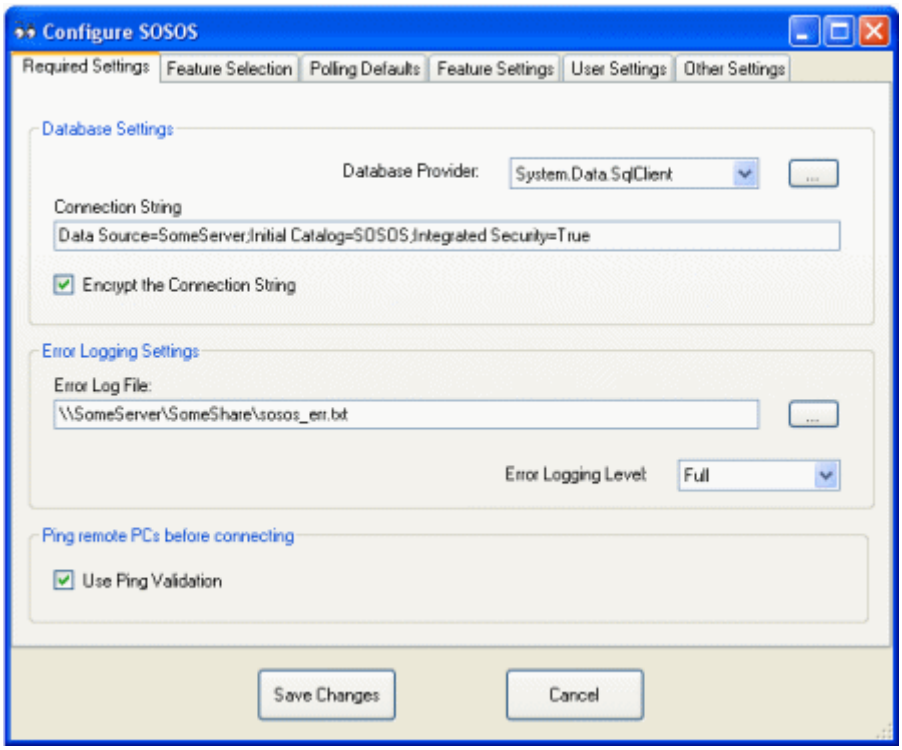


The ConfigureSOSOS utility will prompt you for the path to the "target" application's *.config* file. These files can be either the prototype *app.config* file found in each source code directory or the application-specific configuration file (i.e. *RunSOSOS.exe.config*) found in the same directory as the target application.

2.2 Required Settings

The first configuration "tab" contains settings that must be configured prior to running many of the SOSOS applications.

The *Database Provider* and *Connect String* information is required for database functionality. The *Error Log File* and *Error Logging Level* are required for the central error log functions described in Section 6. The *Use Ping Validation* setting determines if an ICMP "ping" will be used to verify that a remote PC is online prior to attempting a connection.



Database Settings:

- Database Provider – Pull-down list of supported providers
- Connection String – The location and login information to the database
- Encrypt the Connection String – Should the Connection String be encrypted in the application's config file

Note: Use the button to the right of the pull-down to launch a utility that will help you choose a database provider and build the connection string.

Error logging Settings:

- Error Log File – The path to a file that everyone can access and write to
- Error Logging Level – Full, Errors Only, None

See Section 6 for additional information about the Error Logging Level setting.

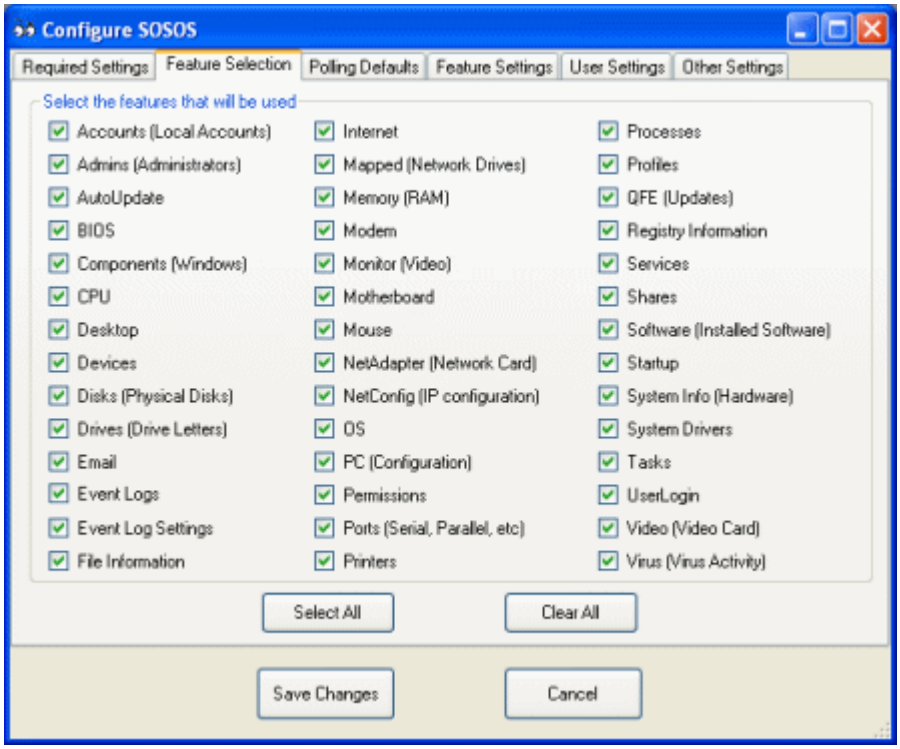
Ping Remote PCs before connecting:

- Use Ping Validation – Use "ping" to verify that a remote PC is online

2.3 Feature Selection

The Feature Selection "tab" allows an administrator to select which features should be used when collecting data. This can be useful in speeding up the collection of data by disabling features that are not required.

Note: The "feature" name corresponds to the database table name as shown in Appendix B.

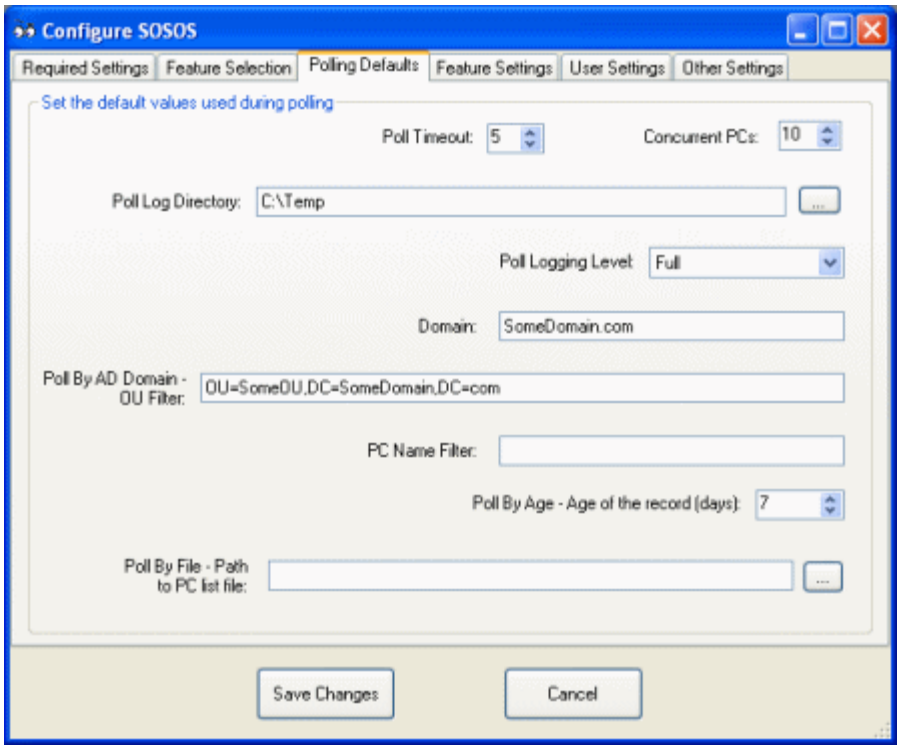


Note: The feature selection settings are useful for performing a "one-off" scan of the network, where you are only concerned about a few features. This technique works best when you collect the data into a separate database (otherwise existing entries in the database will be deleted and replaced with just the few features selected).

2.4 Polling Defaults

The Polling Defaults "tab" will set the defaults used by SOSOS and PollSOSOS to control polling options, set the location and detail level of the log file, and set the default settings to be used to generate the list of PCs to be polled.

Note: Not all settings are applicable to every polling method.



Set the default values used during polling:

- Poll Timeout – Number of minutes to wait before SOSOS will "abandon" the polling of a "stuck" PC and move on to the next PC on the list.
- Concurrent PCs – Number of PCs to concurrently scan. Increasing this setting will make the polling of PCs run faster, but will put additional strain on the one PC performing the polling.
- Poll Log Directory – Path to a directory where that poll log file will be generated. The file name portion of the poll log file is generated automatically and contains the current date (i.e., PollSOSOS_yyyyMMdd)
- Poll Logging Level – The level of details that will appear in the log file (choices are Full, Errors and Summary, Summary Only, or None)
- Domain – Name of the domain/workgroup to be used to generate the list of PCs
- OU Filter – The "distinguished name" of an Organizational Unit used to generate the list of PCs, i.e., OU=Sales,OU=NorthAmerica,DC=SomeDomain,DC=com (used in Poll By AD Domain only)
- PC Name Filter – The name of a single PC or wildcards used to "filter" the list of PCs, (i.e., SALES*)
- Age of the Record – the age of the database records used to generate the list of PCs (used in Poll By Age only)
- Path to PC List File – The full path to a text file that contains a list of PCs (one per line) that will be polled (used by Poll By File only).

Note: These settings are just the defaults… they can be changed during run time.

The SOSOS application provides an opportunity to change these setting via a form prior to polling. See the *User's Guide* for additional details.

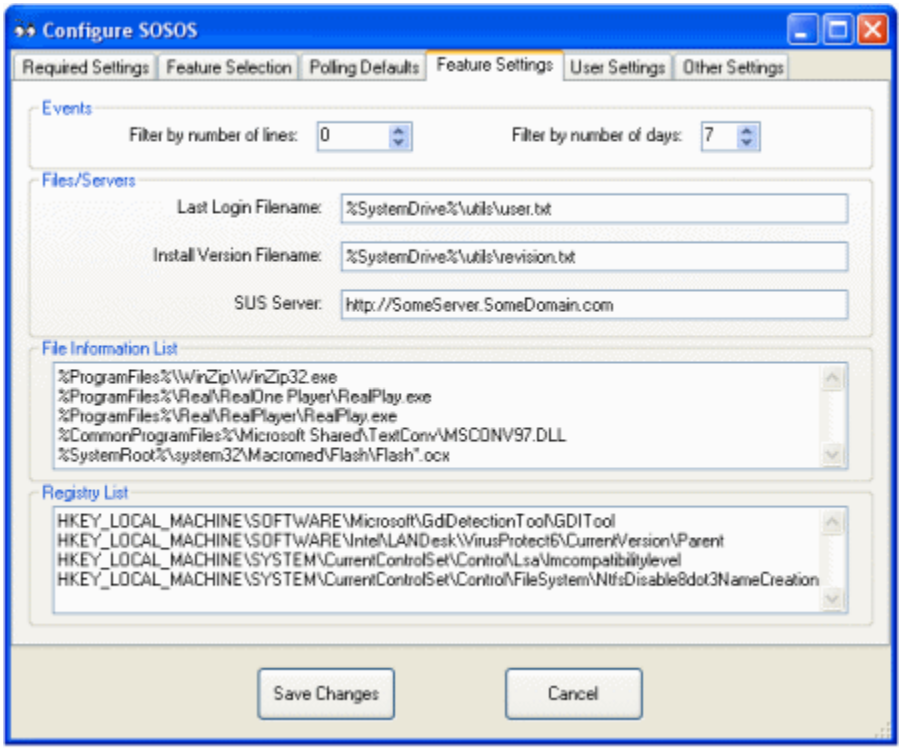
The PollSOSOS application uses command line arguments to override the default settings. See Section 3 for the supported command-line arguments.

Note: You may need to experiment with the value for the Concurrent PCs to file the optimum setting for your environment.

2.5 Feature Settings

The Feature Settings tab is used to change the way certain features work. The settings for the *Events* control how much event log data is collected. The *File/Server* settings are used for gathering login, version, and server status. The File Information List and Registry List allow an administrator to gather information about an ad-hoc list of files and registry keys.

Note: Event log data is often huge and might take several minutes to collect (particularly on servers). Use these feature settings to limit the amount of data collected and thereby speed up the collection process.



Events:

- Filter by number of lines – stop collecting event data after this many rows. A setting of 0 means to collect all events.
- Filter by number of days – collect only the event data for the previous days indicated. A setting of 0 means to collect all events.

Note: When used together, data gather stops when either filter condition is "satisfied" (a logical OR condition).

Files/Servers:

- Last Login Filename – The path to a text file on each PC that contains information created during login. The last modification date of the file is used by SOSOS to determine the last time anyone logged into the PC. (See Appendix D for a list of the supported environmental variables).
- Install Version Filename – The path to a text file on each PC that contains a description of the PC's "Revision Level". Organization might use a master image of a PC for "cloning" other PCs. This provides a method of keeping track of the version of the master image applied to each PC. (See Appendix D for a list of the supported environmental variables).
- SUS Server – The URL to the Microsoft Windows Server Update Services (WSUS) server. Corporate organizations often provide their own server for distributing updates. If your organization doesn't use WSUS, leave this field blank.

See Section 2.8 for additional information about the text files used for Last Login and Install Version.

File Information List

- Ad-hoc list – A list of files that SOSOS uses to collect size, version, and modification date information for the FileInfo table. Enter one file name per line. (See Appendix D for a list of the supported environmental variables).

Registry List

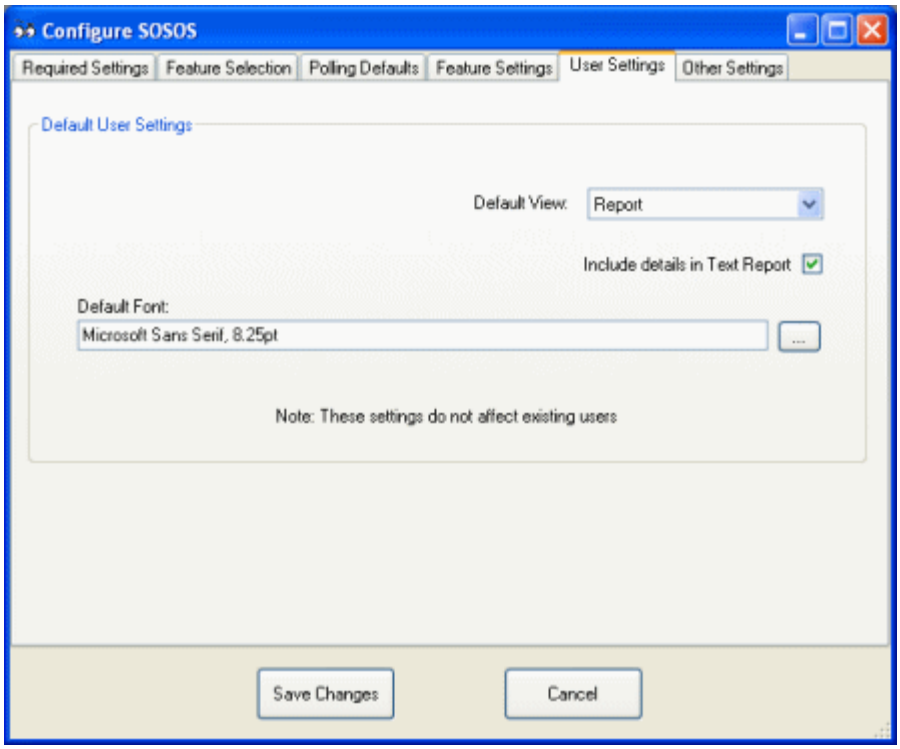
- Ad-hoc list – A list of registry keys that SOSOS uses to collect registry values for the Registry table. Enter one registry key per line.

The File Information List and Registry List features are designed to satisfy the needs for information that might be specific to your organization without the need to modify and recompile the application. Administrators can merely edit the configuration file to start gathering this "ad-hoc" information.

2.6 User Settings

These settings control the program's visual defaults that each user may customize.

Note: The user's default settings are automatically saved when exiting the program. These settings are retrieved and applied the next time the application is launched.



Default User Setting:

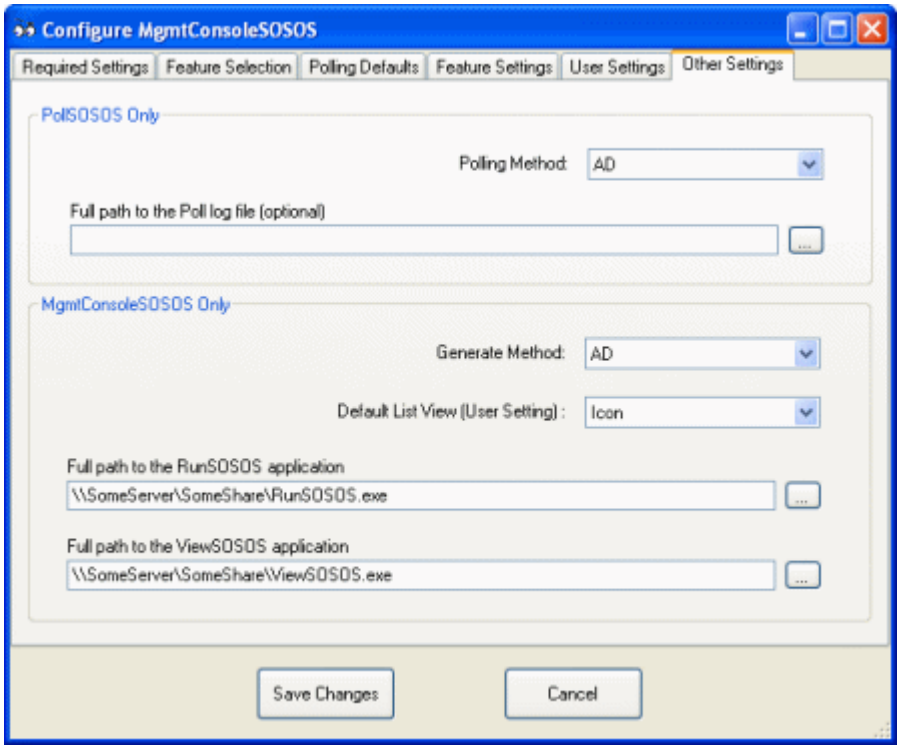
- Default View – Which SOSOS view is the default. Choices are Report, Text, and Grid
- Include Details – Determines if the Text view, saved Text Report, or printed Text Report includes a lot of details. Use this setting to reduce the size of the report by not including details.
- Default Font – The default font used throughout the program

Note: These settings are the defaults for new users of the application. They have no effect on existing users who may have already saved these settings.

2.7 Other Settings

The PollSOSOS and MgmtConsoleSOSOS applications require additional settings.

Note: MgmtConsoleSOSOS is an optional part of the SOSOS suite and is not included in the SOSOS Distribution Kit. It is available from the SOSOS web site as an additional download.



PollSOSOS Only

- Polling Method – The method used to generate the list of PCs for polling. The choices are AD, NT, Browse, File, and Age. See the *User's Guide* for meaning of each polling method.
- Full path to the Poll log file – If used, disable the automatic file-name generation feature and use the supplied file name to receive the results of the polling operation.

MgmtConsoleSOSOS Only

- Generate Method – The method used to generate the list of PCs for the Management Console. The choices are AD, NT, and Browse.
- Default List View – The default view. Choices are Icon or Details.
- RunSOSOS Application – The full path to the RunSOSOS application.
- ViewSOSOS Application – The full path to the ViewSOSOS application.

2.8 Additional Text File Configuration

The SOSOS suite uses several text files that may need to be created or text files that may require permissions to be set.

Error Log: The Error Log file needs to be created on a network share where it is available to all users on the network. This file requires read and write permissions for users of the application.

See Section 5 for the deployment scenarios that may require every user in your organization to have read and write permission to this file.

Last Login: The text file used by the Last Login feature is typically created from a login batch file. The batch file might include the following commands:

echo %USERDOMAIN%\%USERNAME% > C:\Utils\User.txt 2>nul

Note: The contents of the file are not relevant…SOSOS only uses the last modification date of the file.

Appropriate permission would be required for all users to create or overwrite this file.

Install Version: The text file used by the Install Version feature is created when the PC is first loaded. It contains the "signature" of the master image used to clone the PC. The format of the file looks like this:

v1.2.2<tab>1 Jan 2006
<tab><tab>Short description of image v1.2.3
<blank line>
v1.2.3<tab>15 Jan 2006
<tab><tab>Changes made to v1.2.2

Note: Only the last line that starts with the letter "v" is used.

Users only need read access to this file.

Section 3 – Running the Applications

The SOSOS suite consists of the following:

- SOSOS – the main application (includes all of the features below)
- RunSOSOS – a command-line version for gathering data
- PollSOSOS – a command-line version for network scanning
- ViewSOSOS – a read-only interface to SOSOS database
- ConfigureSOSOS – a setup utility for the SOSOS suite

3.1 SOSOS

This is the "main" application that may be the only application that's required in a home or small office environment.

SOSOS has no command-line options. See the *User's Guide* for additional information on the features of the SOSOS application.

3.2 RunSOSOS

This is a "console application" that is designed to run unattended in a login batch file or as a scheduled task to collect and record SOSOS data. It has the following command-line options:

Switch	Meaning	Notes
/q	Quiet	Run with no output to the console
/w	Wallpaper	Puts a summary "watermark" on the user's desktop
/l	Login	Also record login information to the UserLogin table
/s	Server mode	Record progress to the event log
/wlo	Wallpaper & Login Only	Create wallpaper and record only login information
/auto	Automatic	Switch to WLO mode if not an administrator

When run in a login batch file the command line might include:

RunSOSOS /q/l/w

When run from a scheduled task on a server, the command line might include:

RunSOSOS /s

3.3 PollSOSOS

This is a "console application" that is designed to run unattended in a scheduled task on a single PC/Server to poll the network to collect and record SOSOS data from PCs on a LAN. It can be configured by using the ConfigureSOSOS utility to edit the configuration file and/or by using the following command-line options:

Switch	Optional Arguments	Notes
/UsePingValidation	None	Use ICMP "ping" to verify that a PC exists before attempting to collect data
/Domain	Name of the domain or workgroup	The domain/workgroup used to generate the list of PCs
/OU_Filter	The "distinguished name" of the OU	Used to "filter" the list of PCs (Active Directory domains only)
/NameFilter	PC Name with wildcards	Used to "filter" the list of PCs
/PoolSize	Number of concurrent PCs to process	Increase this number to poll the network faster, increases the load on the local PC
/PollLogDirectory	Path to an existing directory	If the polling log file name is generated automatically, this is the location where the file will be created
/PollLogFile	Path to the log file	The full path to the log file (turns off automatic file name generation)
/PollLogLevel	Full, Errors, Summary, or None	Control the level of detail that appears in the Polling log file
/PollByAge	Age (in days) that a database record is considered "old"	Used to "freshen" existing records in the database by polling only those PCs whose records are older than the number of days specified
/PollByFileFile	Path to a text file that contains a list of PCs to be polled	Used to poll a specific list of PCs
/PollMethod	AD, NT, Browse, File, or Age	The method used to generate the list of PCs
/PollTimeout	Minutes to wait	Used to make sure that the polling is not "stuck" on a PC for longer than the number of minutes specified.

Note: Items in the Configuration file are processed first, followed by the options that appear on the command line.

When used to "freshen" the existing records in the database, the command line might include:

PollSOSOS /PollMethod Age /PollByAge 7 /PollLogFile "C:\Temp\SomeLog.txt"

When used to poll an Active Directory domain, the command line might include:

PollSOSOS /PollMethod AD /Domain consoto.com /OU_Filter OU=Sales,DC=Consoto,DC=com

Note: You should run PollSOSOS from a PC that's running the latest operating system (i.e. Windows Vista). See Appendix C for more information about the effects on the data collected.

3.4 ViewSOSOS

This is a read-only database viewer for the SOSOS data in the database. It has no data gathering or scanning capabilities.

ViewSOSOS accepts a single PC name as a command-line argument. When used, it will retrieve the existing data for that PC and display the results.

Note: Administrators may prefer to use direct access to the underlying database to view, query, edit, and manage the SOSOS information.

3.5 ConfigureSOSOS

Use this utility to perform setup configuration tasks for each of the SOSOS-related applications. This application does not support command-line arguments.

Note: The configuration files for the "target application" are found in the same directory as the application's EXE file. Changes are not effective until the target application is restarted.

You can use ConfigureSOSOS to configure applications after deployment or during development. If used during development, you must select the app.config file in the source code directory. When used after deployment, you select the application's config file that resides in the same directory as the application itself (i.e. RunSOSOS.exe.config)

*Note: The ConfigureSOSOS utility cannot be directly used to configure SOSOS_fx1.1 and RunSOSOS_fx1.1 (these programs are available as additional downloads and are not part of the distribution kit). Instead, you must first use ConfigureSOSOS to configure the "normal" versions of SOSOS and RunSOSOS and then copy the encrypted connection string data to the *.config files for SOSOS_fx1.1 and RunSOSOS_fx1.1 by hand (i.e. using Notepad).*

Important: This utility is particularly important since the connection strings to the database may be encrypted and therefore editing the configuration files by hand is not possible.

Section 4 – Database Setup

The SOSOS suite does not have a built-in database… instead it relies on a 3rd-party database application to store its information. See Appendix B for a brief description of each database table.

Note: A database is not absolutely required. However a lot of SOSOS functions are designed around a database and will be disabled when a database is not configured.

SOSOS is designed to record the most current information into the database. This means that older records are completely replaced with new records. Therefore, the database does not contain a "history" of previous data. If your organization requires historical data, then you should consider downloading the optional BackupSOSOS source code from the SOSOS web site to create archive copies of the live database.

4.1 Supported Databases

SOSOS can use any database that is supported by the .Net Framework 2.0. The choice of database "providers" and "drivers" (particularly with the OLEDB and ODBC driver) allows support for practically every database. The more common databases used are:

- Microsoft Access Database File
- Microsoft ODBC Data Source
- Microsoft SQL Server
- Microsoft SQL Server Database File
- Oracle Database

Microsoft SQL Server Express Edition is an excellent choice and is available as a free download at: http://msdn.microsoft.com/vstudio/express/sql/download/.

4.2 Prototype Files

As part of the setup of SOSOS, you will be required to create a database. To aid in the creation of this database, the SOSOS Distribution Kit includes two files that can be used as a "prototype".

- Empty.sql – SQL script suitable for Microsoft SQL Server
- Empty.mdb – Microsoft Access database (use "as is" or as a prototype)

Most databases have a migration tool that will take a Microsoft Access "mdb" file and convert it into the native structure. Alternately, you can use the provided set of SQL scripts to create the database.

The exact steps required to create a database is highly dependent upon the database vendor and is beyond the scope of this document. It is recommended that an experienced database administrator perform these tasks.

Note: When migrating, make sure that the primary key and foreign key constraints are successfully converted from the prototype.

4.3 Database Security

The security requirements of the database need to match the deployment scenario. See Section 5 for additional details on which options are best for your organization.

Database permissions need to be set to allow appropriate access controls to the database. See your database vendor's documentation on how to perform this task.

A typical scenario for SQL Server would be to create a "secret" database login for use by ordinary users and also use "Windows Integrated Security" for administrators to authenticate as themselves. This allows ordinary users to have write permission to the database only when running the applications. Ordinary users would not have any permission if they attempted to connect to the database directly. See Section 4.4 for additional information about how the login and password strings are protected.

You might also consider an additional "tier" of security for protecting the contents of the EventLogs table as these entries may contain password information from failed login attempts.

User	Access Method	Tables	Permission
Administrators	Direct access	All	Read & Write
Junior Admins	Direct access	All (except EventLogs)	Read
Junior Admins	Direct access	EventLogs	None
Database login*	Via application only	All	Read & Write
Ordinary User	Direct access	None	None

* The Login Batch Model, described in Section 5, requires that ordinary users have both read and write permissions to all tables. This is normally accomplished by using a database login and password that only the application can decipher.

Important: The contents of the SOSOS database would be rich find for a hacker! Guard this database well.

4.4 Encrypted Database Connection Strings

Each SOSOS application that connects to the database needs to be configured with a "Connection String" that allows the program to find and login to the database. These strings are stored in each application's configuration file. The configuration file is an XML-based text file with an extension of *.config.

To protect this sensitive data, the Connection String portion of the configuration file may be encrypted by a technique that only the application knows how to decipher. See Section 2 for additional information about how to configure the Connection Strings properties.

In a small office environment the extra complexity of setting up the encrypted connection strings may not be warranted. In those cases where security of the database is not a significant concern, you may optionally disable the encryption of the connection strings in the config files. See Section 2 for additional details.

Important: Changes to the encryption keys in the SOSOS\crypt.c file requires that you recompile all members of the SOSOS suite. Encryption key changes also mean that the previously encrypted connection strings are no longer available.

Important: Do not attempt to edit the configuration file "by hand" or copy a configuration file from one application to another. Use only the provided ConfigureSOSOS application to perform configuration tasks.

Section 5 - Deployment

This section is designed for administrators in a corporate LAN environment, where setting up a system to record information from hundreds of PCs takes a lot of planning.

Note: Home users can safely ignore this section and just double click on the SOSOS.exe file.

An important factor to consider when developing a deployment scenario is whether or not the PCs in your LAN already have the .Net Framework 2.0 installed.

Since SOSOS works best when run with administrator rights, another important factor to consider is whether or not the users are administrators on their own PCs. See Appendix C for the affects of administrator rights on the data that is collected.

5.1 Scenarios

SOSOS can be configured in many different ways to collection information:

- **Manual Model** – An administrator periodically runs the application on each PC
- **Polling Model** – An administrator periodically polls the network from a central PC
- **Login Batch Model** – Each user runs the application every time they login to a PC
- **Scheduled Task Model** –A scheduled task runs the application at a specific time

Consider the merits of each option:

Model	Pros	Cons
Manual	Simple, doesn't require a domain, and database security is simple	Resource intensive, gathers no login information, data becomes outdated , and requires installation of "prerequisite software" on each PC
Polling	Simple, doesn't require installation of "prerequisite software" on remote PCs, and database security is simple	Gathers no login information, PCs must be left on, and could take several hours to poll a large LAN.
Login Batch	Gathers login information and maintains very timely data.	Requires installation of "prerequisite software" on each PC and database security is complex. For best results, users should be administrators on their own PCs
Scheduled Task	Maintains timely data, is faster than polling, and database security is simple	Gathers no login information and requires installation of "prerequisite software"

No single scenario will be appropriate for all situations. In fact, it's anticipated that most users will use a combination of the techniques to obtain full and timely information in the least amount of time.

For example, a typical organization of approximately 10 servers and 300-400 PCs might use the following combination of techniques:

Type	Model	Command line	Notes
PCs	Login Batch	RunSOSOS /q/l/w	Run quietly from Login batch, records login info and creates wallpaper. Takes about 30 seconds to run. Most users are Administrators on their own PCs
Servers	Scheduled Task	RunSOSOS /s	Runs in the middle of the night from a scheduled task on each server. Takes several minutes to run. Quicker than polling servers remotely
Servers	Login Batch	RunSOSOS /wlo	Runs from login batch (on servers only) to record just the login info and creates wallpaper. Takes about 5 seconds to run.
LAN	Polling	PollSOSOS /PollMethod Age	Run PollSOSOS as a scheduled task on a central PC. The Age option updates "stale" data on PCs where users rarely login (like Print Server). Takes about 20 minutes to run.
LAN	Polling	SOSOS	When required, an Administrator runs SOSOS to manually poll a specific PC (or group of PCs) to update existing data

See Section 3 for additional information about the available command-line options.

5.2 Prerequisite Software

All of the SOSOS applications require the .Net Framework 2.0 to be installed on the PC from which the applications run.

Note: When polling PCs remotely, only the local PC requires the .Net Framework… there is no requirement for the .Net Framework on the remote PCs.

Every PC must have Windows Management Instrumentation (WMI) components installed (including remote PCs when polling). Luckily, WMI is already preinstalled on modern operating systems by default.

The minimum requirements for each PC are highly dependent upon the deployment scenario, but use the following as guide:

Note: The table below represents the minimum requirements; it is always advisable to install the latest components.

OS	Scenario	SP	Framework	MDAC	Installer	IE	WMI
WinXP	Local	2	2.0	2.8	3.0	5.01	Preinstalled
WinXP	Remote	N/A	No	No	No	No	Preinstalled
Win2k	Local	3	2.0	2.8	3.0	5.01	Preinstalled
Win2k	Remote	N/A	No	No	No	No	Preinstalled
Win2k3	Local	N/A	2.0	2.8	3.0	6.0	Preinstalled
Win2k3	Remote	N/A	No	No	No	No	Preinstalled
WinNT	Local		Not supported				
WinNT	Remote	4	No	No	No	No	1.5
Win98/Me	Local	N/A	2.0	2.8	2.1	5.01	1.5
Win98/Me	Remote	N/A	No	No	No	No	1.5
Win95	Local		Not supported				
Win95	Remote	N/A	No	No	No	No	1.5

Note: SOSOS_fx1.1 and RunSOSOS_fx1.1 are available as additional downloads and uses the .Net Framework v1.1 to aid organizations that have not completed the migrated from version 1.1 to version 2.0 of the .Net framework. This also allows WinNT to run the application locally.

The prerequisite software is available from the Microsoft web site:

Component	Download URL
.Net Framework 2.0	http://msdn.microsoft.com/netframework/downloads/updates/default.aspx
MDAC	http://www.microsoft.com/downloads/details.aspx?familyid=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&displaylang=en
Jet 4.0	http://www.microsoft.com/downloads/details.aspx?familyid=2deddec4-350e-4cd0-a12a-d7f70a153156&displaylang=en
Windows Installer	http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en
Internet Explorer	http://www.microsoft.com/downloads/details.aspx?FamilyID=1e1550cb-5e5d-48f5-b02b-20b602228de6&displaylang=en
WMI	http://www.microsoft.com/downloads/details.aspx?FamilyID=afe41f46-e213-4cbf-9c5b-fbf236e0e875&DisplayLang=en

5.3 Additional Requirements for Remote PCs

In order to successfully obtain SOSOS data from a remote PC, all of the following must be true:

- You are an administrator on the Remote PC
- Firewall settings must allow “Remote Administration” traffic to pass
- Remote Registry services are installed (Not preinstalled on Win9x clients)
- An “administrative” share (i.e., C$) is available (Not preconfigured on Win9x)

Administrator Account

The account used on the local PC to gather information on a Remote PC must be in the administrators group on the Remote PC. Typically, you'd use an account that's in the Domain Administrators group to remotely gather SOSOS data.

The User Account Control (UAC) feature of Windows Vista doesn't allow for a connections to a remote Windows Vista PC when the user in logged in via a local account. This isn't normally a problem, since members of the Domain Administrators group are "domain accounts" and not a "local accounts". However, in a Workgroup environment (where you only have local accounts), you must disable UAC on the Remote PC.

From the Control Panel, click on User Accounts, and click on "Turn User Account Control on or off". Clear the checkbox and press the OK button. (This change will require a reboot).

Firewall Settings

A common requirement is to configure the firewall settings for Windows XP SP2 clients to allow for "Remote Administration". You can use a Group Policy Object (GPO) or use the following command line on each PC:

netsh firewall set service RemoteAdmin enable

For additional information on configuring the WinXP Firewall to allow Remote Administration traffic, see: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/connecting_through_windows_firewall.asp.

For Windows Vista, the technique used to allow remote connections via WMI is a bit different. From the Control Panel, click Security, click Windows Firewall, click Change Settings, and then click the Exceptions tab. In the Exceptions window, put a check for the item Windows Management Instrumentation (WMI). Alternately, you use the following command line:

netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

For additional information, see: http://msdn2.microsoft.com/en-us/library/aa822854.aspx

The Windows Vista firewall may also need to be configured to allow File and Print Sharing.

Remote Registry Services

By default, Windows Vista has the "Remote Registry" service set to Manual and it is stopped. So, in order to connect to a remote Windows Vista PC, you'll have to set the service "start type" to Automatic (and start the service).

From the Control Panel, click Administrative Tools and then click Services. Select the "Remote Registry" service and change the Start Type to Automatic.

Administrative Share

All modern operating system have a C$ "Administrative Share" that is configured to allow administrators to gain access to the drive remotely. SOSOS typically does not require any changes to the default configuration.

Additional Notes

Some Microsoft operating systems do not allow Remote Administration at all. Both Windows XP Home Edition and Windows Millennium have the Remote Administration feature deliberately disabled.

Note: That means that you can not use SOSOS to gather information remotely from a PC running WinXP Home. But, obviously SOSOS works just fine when run locally on WinXP Home.

You may be able to coax Win9x clients into allowing remote connections via the DCOM configuration utility, remote registry services, and creating an administrative share. But in practice, it's difficult to get to work properly and probably not worth the effort (see http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b141460).

5.4 Deploying the Applications

As with practically all .Net Framework applications, there is no need for a formal install procedure. Instead you can just copy the files to a network share without installing anything on the client PCs. Alternately, you could copy the files to directory on each PC.

However, a more formal procedure may be required to deploy SOSOS via an Active Directory domain's Group Policy Object (GPO). To accommodate this requirement, each application in the SOSOS suite has a Setup project associated with it. You can use these projects to create the necessary setup MSI files to deploy the programs to your client PCs via a GPO.

See Section 2 for additional information about configuring the *app.config* file in each program's source code directory prior to creating the Setup projects.

Note: The free Visual Basic 2005 Express Edition does not support the Setup project type.

For additional information on how to deploy an application via a GPO see http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/featusability/inmnwp.mspx.

5.5 Running from a Network Share

One of the features of the .Net Framework allows users to set “code access permission” for the PC (or individual programs). By default, the Framework's own security settings will not allow *any* program to run from a network share that requires "significant" permissions. Since SOSOS requires a lot of permissions to work properly, the default settings will not allow it run from a network share.

Note: The default Code Access Permission settings are sufficient when SOSOS is run from the local drive.

To solve the problem, you can either copy the program files to a local drive, or adjust the .Net Framework assembly permissions on each PC.

To adjust permissions, you use the *.Net Framework 2.0 Configuration* control panel applet (on a development PC). Navigate to "Configure Code Access Security Policy", “Adjust Zone Security”, "Make changes to this computer". Click on the Local Intranet icon and move the slider up to "Full Trust".

You can also use the *.Net Framework 2.0 Configuration* control panel applet to create an MSI file that you can use to deploy these changes via a GPO or login batch to the other PCs in your LAN. Click on the "Configure Code Access Security Policy", "Create Deployment Package". When the Wizard opens, click on the "Machine" security policy, and select a folder/name of the MSI file that will be created.

Alternately, you can use the *LocalIntranet.msi* file included in the SOSOS Distribution Kit.

Section 6 – Errors

The core technology of SOSOS is Windows Management Instrumentation (WMI). WMI is a great idea, but is not an exact science... Errors are inevitable.

WMI provides its best information when both the OS and BIOS are very modern. Information also may change slightly if the user is (or is not) the administrator on the local PC. Different errors may also appear if the application is run locally or remote.

The SOSOS suite uses an error reporting system that collects application errors and records them to a central error log file.

See Section 2 for additional information about how to configure the Error Log settings.

6.1 Error Messages

If the program is in the "quiet mode", the user is typically unaware of an error condition that might arise… errors are silently recorded to the error log file.

See Section 3 for information about the command line options for the "quiet mode".

Error messages that pop up while not in the quiet mode are intended for the casual user, and do not contain a lot of detailed information. However, the details are still recorded to the error log file.

Note: The error log file was designed to be used by programmers to diagnose problems. So, it includes a bunch of programmer-related gobbly-gook.

6.2 Log Levels

For the first few weeks, it's recommended that you leave the default settings for the *Error Logging Level* and *Poll Logging Level* at "Full". This will help identify problems with deployment. However, these log level settings will also fill the error log file with lots of extraneous information.

See Section 2 for additional information about the configuration options.

Note: With the log levels at "Full", you will get entries in the error log file. This is expected and not necessarily a sign that something is wrong.

It may take a while for you to become familiar with the entries in the error log file and determine what is "normal chatter" and what is a real error that requires some attention.

After you've reached a comfort level with the deployment, then you should consider changing both the *Error Logging Level* and *Poll Logging Level* settings to "Errors". This will reduce the "chatter" in the log files while preserving those entries that are true errors.

6.3 Embedded Database Errors

Most minor errors are also recorded in the database. The error messages are generally short and truncated to fit inside the particular table column. Messages are preceded by the text "Error:". If a numeric field is available, it is set to a negative number.

Note: Logging levels do not affect the appearance of embedded error messages in the database.

Section 7 - Maintenance

The SOSOS suite does not require any maintenance. However the database used by SOSOS will most likely require some periodic tasks.

7.1 Database Maintenance

The database maintenance tasks are highly dependent upon the specific database application installed and therefore are beyond the scope of this document. You should follow the tasks recommended by the database vendor to assure that the following are periodically accomplished:

- Backup of the database
- Compression of database files
- Index "tuning"

7.2 Program Updates

There is no formal update notification procedure. Users are encouraged to check the SOSOS web site for updates. The web site contains a text file called *Changes.txt* which you can use to determine if an update is available.

When updates are available, they are provided as a zip file that contains a complete replacement set of source code files. The updated source code is designed to completely replace all of your existing source code files to include any configuration settings you changed during development.

Important: Remember to record your encryption keys before overwriting your existing source code files.

If changes to the database are required, instructions will be provided in a text file called *DatabaseChanges.txt*.

Updates are available from the SOSOS home at http://www.sosos.emmet-gray.com

7.2 Other Maintenance Tasks

Administrators are encouraged to view the Error Log file for potential problems. A programmer who is experienced with Visual Basic .Net may be able to edit the source code to solve minor problems that are detected in the log file.

See Section 6 for additional information on the Error Log file.

Appendix A – Deployment Checklist

When deploying SOSOS, consider the following steps:

Pre-deployment:

- Read the S*etup and Configuration Guide* (this document) and the *User's Guide*
- Calculate the size of the database
- Determine hardware/software requirements for the database
- Get whatever approval is required to proceed
- Purchase a suitable database program (if required)

Deploy the database:

- Install the database application (if required)
- Create a database using one of the provided "prototypes" as a starter
- Verify primary keys and foreign key constraints
- Establish an authentication/authorization scheme for the database
- Secure the database as appropriate for outsiders, ordinary users, and administrators
- Consider using extra security settings on the EventLogs table

In a lab environment:

- Change the encryption keys (Vector and TheKey) in Crypt.vb
- Compile the SOSOS application
- Copy the SOSOS.exe and SOSOS.exe.config file to a test PC
- Run SOSOS on the test PC to configure the "required settings" sections
- Test SOSOS and the database connectivity

Determine the deployment scenario

- Choose a deployment scenario or a combination of scenarios
- Determine the connect string settings for each SOSOS application
- Run ConfigureSOSOS for each SOSOS application

Deploying the clients (highly dependent on deployment scenario):

- Install missing/outdated components on each client
- Configure .Net Security on each client
- Copy the application and application config files
- Run ConfigureSOSOS on the app.config files and build the Setup projects
- Edit login batch file
- Create scheduled tasks

Post deployment:

- Check the text-based error log file
- Review the data in the tables for embedded error messages
- Verify the security of the database

Appendix B – Database Table Descriptions

Table Name	Description
Accounts	A listing of all local accounts
Admins	Members of the local Administrators group
AutoUpdate	Automatic Update settings
BIOS	BIOS information
Components	Windows components (similar to installed software)
CPU	Processor information
Desktop	User's desktop (screen saver, wallpaper, etc)
Devices	Listing of devices (similar to device manager)
Disks	Physical disk information
Drives	Logical drive information (drive letters)
Email	User's Microsoft Outlook settings
EventLogs	Event Log entries
EventLogSettings	Setting for each Event Log
FileInfo	Information about an ad-hoc list of files
Internet	User's Internet Explorer settings
Mapped	User's mapped network drives and printers
Memory	Quantity and type of RAM
Modem	Modem information
Monitor	Video Monitor information
Motherboard	Motherboard information
Mouse	Mouse
NetAdapter	Network Interface Card (NIC) information
NetConfig	NIC Configuration
OS	Operating System details
PC	Miscellaneous PC information
Permissions	Permissions on network shares
Ports	Number and type of ports
Printers	Local and network printer information
Processes	List of running processes (similar to Task Manager)
Profiles	Listing of User Profiles (i.e. C:\Document and Settings)
QFE	Updates/Patches (QFE=Quick Fix Engineering)
Registry	Information about an ad-hoc list of registry keys
Services	List of Windows Services
Shares	Information about network shares
Software	Listing of installed software
SOS	Summary information (root of many tables)
Startup	User's automatic startup applications
SystemDrivers	List of system drivers (useful in recovery console)
SystemInfo	System identification and serial numbers
Tasks	Listing of scheduled tasks
UserLogin	Record of every login
Video	Video card information
Virus	Norton Antivirus Corporate Edition logs

Appendix C – Affects on Collected Data

Administrator

The following table describes the affect on the information that is collected if the current user is not a member of the local administrators group on the PC.

Table Name	Notes
Desktop	Only entries for the current user and the Default User
Email	Only entries for the current user and the Default User
EventLogs	No entries for the Security Log. All other event logs are recorded
Internet	Only entries for the current user and the Default User
Mapped	Only entries for the current user and the Default User
Permissions	No entries
Startup	Only entries for the current user and the Default User
Tasks	No entries
Video	Only partial data will be collected

User Mapped Drive Letters

SOSOS does not follow files that have mapped drive letters to network shares (such as "H:\SomeFile.txt"). This would most likely happen in the Email table where the user may store his/her PST file on a network share using a mapped drive letter. In this case, the file name is recorded, but the file size will show 0.

Remote Collection

When collecting data from a remote PC running Windows Vista, the Task table will only be populated if the local PC (the one running the application) is also running Windows Vista.

Development Platform

The Task table will only be populated on a PC running Windows Vista if the SOSOS application was also compiled and configured on a development PC running Windows Vista.

Appendix D – Supported Environmental Variables

The use of System Path environmental Variables allows SOSOS to more accurately find files on remote PCs. This feature is particularly handy when creating the list if ad-hoc files for the FileInfo feature (See: Section 2.5)

Note: The 64-bit versions of Windows have both a "C:\Program Files" and "C:\Program Files (x86)" directory to allow side-by-side program installation.

The following environmental variables are supported by the SOSOS suite:

- %ProgramFiles% - typically C:\Program Files
- %ProgramFilesx86% - typically C:\Program Files (x86)
- %CommonProgramFiles% - typically C:\Program Files\Common Files
- %CommonProgramFilesx86% - typically C:\Program Files (x86) \Common Files
- %SystemRoot% – typically C:\Windows
- %SystemDrive% – typically C:
- %windir% - same as SystemRoot

Note: The normal file name wildcards (and ?) can also be used in the ad-hoc files listed in the FileInfo feature. Example: "%SystemRoot%\system32\Macromed\Flash\Flash*.ocx".*

Appendix E – Compiling "Walk Through"

Here is a step-by-step "walk through" for compiling the Visual Basic source code to the SOSOS application. There are 3 basic steps:

- Compile the Visual Basic source code
- Deploy (or just copy) the resulting program files and DLLs
- Configure SOSOS and enjoy

1. **Install Visual Basic 2005** on your computer (any version will do, including the free Visual Basic 2005 Express Edition)

2. **Download the SOSOS source code** (all you need is the SOSOS.zip file)

3. **Create a source code directory** where you will put the SOSOS source code (i.e. C:\SOSOS_Suite)

4. **Extract the source code** from the SOSOS.zip file into the directory created in Step 3 (using WinZip or the built-in "compressed folders" feature of Windows XP and above). Make sure you extract the folder structure along with the files.

5. **Extract the vbproj files** from either the WinXP_vbproj.zip or WinVista_vbproj.zip file. Answer "yes" to overwrite existing files. Again, make sure you extract the folder structure along with the files. If your development PC (the one where you installed Visual Basic 2005) is running Windows XP, then use the WinXP_vbproj.zip file. Otherwise, if you're running Windows Vista, then use the WinVista_vbproj.zip file. These two zip files are included in the SOSOS.zip file and only appear after you've extracted them in Step 4.

6. **Navigate to the SOSOS directory** inside the source code "tree". For example, if you extracted the files into a directory called "C:\SOSOS_Suite", then click on the "C:\SOSOS_Suite\SOSOS" directory.

7. **Double click on the SOSOS.sln** (the solution file) to launch Visual Basic 2005. If you have configured the Explorer to hide file extensions, the SOSOS.sln file is the icon with an "8" in the upper right hand corner. *Note: you might get a window that pops up saying "The application for project c:\SOSOS_Suite\SOSOS\SOSOS.vbproj is not installed". This is because the free Express Edition does not support the Setup project type. This error can be safely ignored.*

8. **Do a "test run"** to make sure everything is working correctly. From the Visual Basic 2005 window, use the "Debug" menu, select "Start Debugging". This will compile the program inside a special debugging environment and launch it for you to play with. Take your time to explore the application, have fun… and after you're satisfied that this is something you'd like to use, move to the next step. *Note: Do not attempt to configure SOSOS inside the debugging environment, since the configuration settings are overwritten each time you start debugging.*

9. **Change the default encryption keys** in the Crypt.vb file. Open the Crypt.vb file by double-clicking it from the "Solution Explorer" (typically in the upper right-hand corner of the Visual Basic screen). Find the lines that start with "`Private TheKey()`" and "`Private Vector()`". There are 16 hexadecimal bytes (on two lines) that should be changed. It really doesn't matter what values you use (unlike a password, you won't have to remember these numbers). Hexadecimal numbers are one or two digits, made up with the numbers 0-9 and the letters A-F. *Note: If you are configuring SOSOS for home use, you can probably ignore this step and turn off the encryption feature in step 13.*

10. **Compile the SOSOS application** by using the "Build" menu, and selecting "Build SOSOS". Take a look at the "Output" windows (typically at the bottom of the Visual Basic 2005 window) for any errors or warnings.

11. **Create a SOSOS home directory** where the SOSOS program will reside (typically this would be "C:\Program files\SOSOS"

12. **Copy the files** from the development environment to this "SOSOS home" directory. The 10 or so files that were created in Step 10 should be in a directory called C:\SOSOS_Suite\SOSOS\bin\Release. Copy all of the files except for the ones named "SOSOS.vshost.exe" and "SOSOS.vshost.exe.config" to C:\Program files\SOSOS. Copy the help file (C:\SOSOS_Suite\SOSOS\Help\SOSOS.chm) to the SOSOS home directory.

13. **Perform a one-time configuration** of SOSOS by navigating to the "SOSOS home" directory (typically C:\Program files\SOSOS) and launch the SOSOS program by double-clicking on the SOSOS.exe program. From the "Setup" menu, select "Configure SOSOS". Configure the items on each of the "tabs". See the "Setup and Configuration" documentation for the details on each configuration setting.

14. Enjoy!

Son of Snoop on Steroids (SOSOS)
User's Guide

1. Background

SOSOS is a computer hardware and software inventory program. It gathers over 220 pieces of information about computers and optionally stores this information in a database. It can be run locally or can be used by an administrator to scan a network.

SOSOS was designed to make the life of the System Administrator easier… many tools are available to gather data similar to SOSOS, but few allow you to automatically record the results into a database.

SOSOS is available only as Visual Basic "source code". That means that you'll have to use Microsoft Visual Studio 2005 to compile the source code into a usable program that will run on your computer.

SOSOS is completely free of charge. The SOSOS source code is considered in the "public domain". That means you can do anything you want with it, to include making money from it. There is no licensing requirement.

The "official" home of SOSOS is at http://www.sosos.emmet-gray.com

2. SOSOS Features

SOSOS gathers information about PCs including *hardware information* such as CPU, memory, hard drives, and serial numbers; *software information* such as operating system, installed software, and software components; *configuration information* such as IP address, running processes, desktop settings, and services; and *security-related information* such as shared resources, modems, account policies, security patches, and virus activity.

Note: SOSOS does not gather any personal information, look at emails, user documents, or track Internet activity.

SOSOS does not have a built-in database… instead it relies on a 3rd-party database application to store its information. A database is not absolutely required. However a lot of SOSOS functions are designed around a database and will be disabled when a database is not configured.

See the *Setup and Configuration Guide* for additional information on how to compile, configure, and deploy SOSOS in your organization.

3. The SOSOS Suite

SOSOS is actually a suite of programs consisting of the following:

 SOSOS – the main application (includes all of the features below)

 RunSOSOS – a command-line version for unattended gathering of data

 PollSOSOS – a command-line version for network scanning

 ViewSOSOS – a read-only interface to SOSOS database

 ConfigureSOSOS – a setup utility for the SOSOS suite

SOSOS.exe is the "main" application that may be the only application that's required in a home or small office environment.

In the most common scenario for a corporate environment, the average user may never see the SOSOS program. The data from their PCs may be gathered by the RunSOSOS program which is designed by default to be "stealthy" and to be run during the login process with no user intervention.

Users can double-click on the SOSOS.exe program to manually scan their PC, save the data, print, or save a report. Administrators can do more…they can use SOSOS to poll remote PCs for their data.

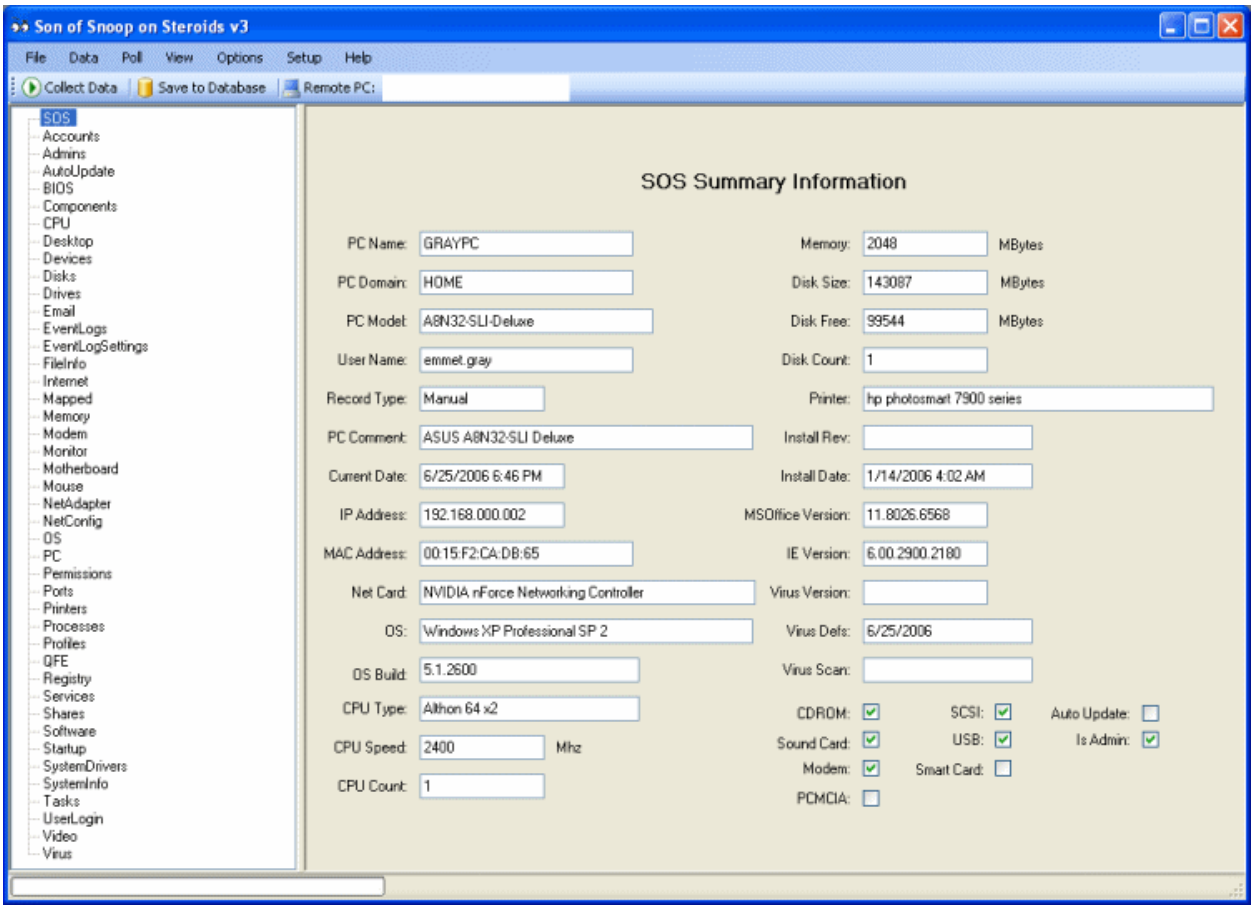
The ViewSOSOS application has the same user interface as the SOSOS application with most of the data gathering features disabled. A user with appropriate database permissions can use ViewSOSOS to look at the data for any PC in the database.

Note: Administrators may prefer to use direct access to the underlying database to view, query, edit, and manage the SOSOS information.

This User's Guide covers only the SOSOS and ViewSOSOS programs. See the *Setup and Configuration Guide* for information about the other members of the SOSOS suite.

4. Running SOSOS

The most common task in SOSOS is to collect data from the local PC. You perform this function by clicking on the *Collect Data* button (or from the *File/Collect Data* menu). The SOSOS screen will look like the following:



Click on the item in the left-hand list (i.e. CPU) to view the data for that item.

SOSOS supports three different methods of viewing the collected data.

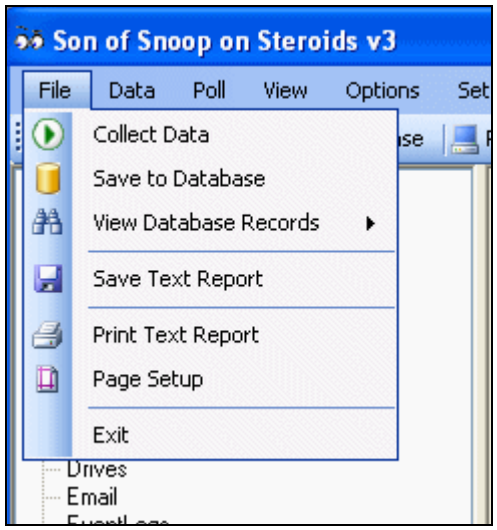
- The Report View uses a database-style navigator to view individual records
- The Grid View displays all records in a grid
- The Text View is a text-based view suitable for printing and saving to a text file

After the data has been collected (via the “Collect Data” button), the user has the opportunity to:

- Save the results to the database
- Write the results to a text file
- Print the results
- Display summary data as a “watermark” on the user’s desktop
- Export the results to an XML file or a Microsoft Access database file

4.1 File Menu

The File Menu is used to perform the most common tasks:

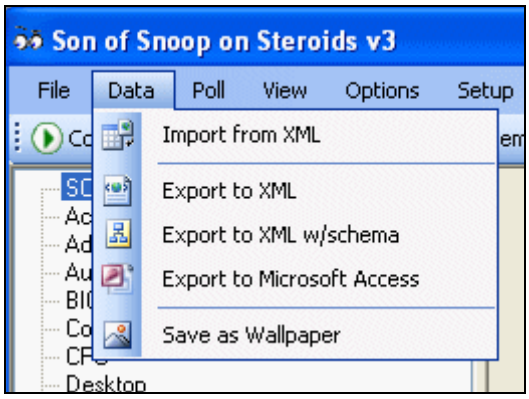


File Menu:

- **Collect Data** – Collects SOSOS data from the local PC
- **Save to Database** – Saves the collected data to the database
- **View Database Records**
  - **For this PC** – View the existing database records for this PC
  - **Enter a PC Name** – Enter the name of a PC to view its database records
- **Save Text Report** – Save the data to a file using the Text View format
- **Print Text Report** – Print the data using the Text View format
- **Page Setup** – Set up the page for printing
- **Exit** – Exits the program

4.2 Data Menu

The Data Menu is used to import and export data



Data Menu:

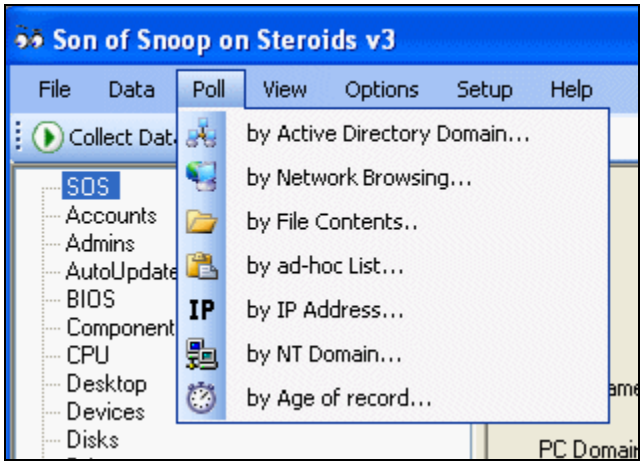
- **Import from XML** – Imports data from a previously exported XML file
- **Export to XML** – Export the data to an XML file. Use this option if you plan to later import the data using the *Import from XML* option.
- **Export to XML w/schema** – Export to an XML file and also include the "schema". Use this option if you plan to export the data into some other application.
- **Export to Microsoft Access** - Export to a Microsoft Access (mdb file)
- **Save as Wallpaper** – Create a summary "watermark" on the user's desktop

There may be situations where you want to record data from PCs that are not connected to any network. To handle this, SOSOS can export its data into an XML file. An Administrator can take this XML file to another PC (that is on the network) import the XML file and save the data to the database.

4.3 Poll Menu

The Poll Menu is used to collect SOSOS data from remote PCs on a LAN. This operation requires the user to have administrator rights on the remote PCs. Typically this function would be performed by a member of the Domain Administrators group.

There are several choices as to the method used to generate the list of PCs that will be "polled".

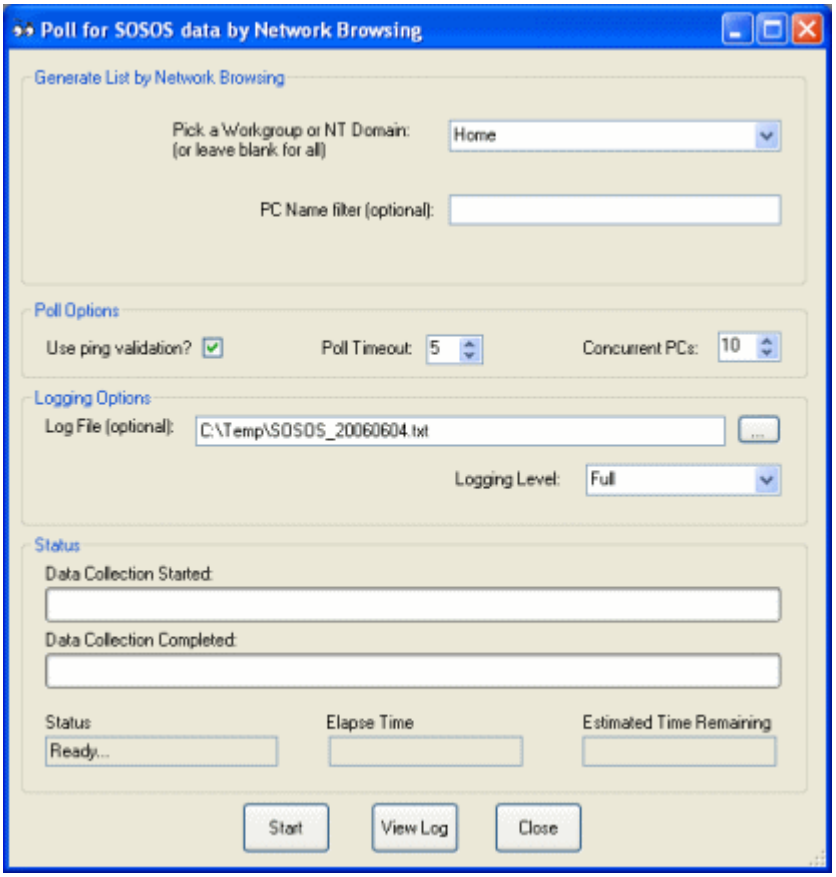


Poll Menu:

- **By Active Directory Domain** – Use Active Directory domain and Organization Unit (OU) to generate the list of PCs
- **By Network Browsing** – Use the list of PCs that are visible in the My Network Places. Does not require a domain.
- **By File Contents** – Use a text file that contains a list of PCs. The PC names should be listed one per line
- **By ad-hoc List** – Type the names (or cut and paste a list of PCs) that will be used
- **By IP address** – Use a list of IP address ranges to poll the network
- **By NT Domain** – Use Window NT-style domain lists

- **By Age of record** – Run a query on the database to produce a list of PCs whose data is older than a certain number of days.

After selection of a polling method, the menu will look similar the following (using the Network Browsing method as an example):



Generate List by Network Browsing:

- **Workgroup or Domain** – Filter the list of PCs to be generated to only those in the selected workgroup/domain
- **PC Name Filter** – Filter the list of PCs by using a wildcard (i.e., SALE* will limit the list of PCs to those whose name begin with SALEs).

Note: The top portion of the form is dependent upon the polling method selected and may display different options from this example (using the Network Browsing method).

Poll Option:

- **Use ping validation?** – Should SOSOS use an ICMP "ping" to verify that the remote PC is actually on line before attempting to connect to the PC? Can speed up the process, but some PC firewalls block ICMP traffic.
- **Poll Timeout** – The number of minutes to wait before abandoning a "stuck" PC and moving on the next PC in the list

- **Concurrent PCs** – The number of PCs to scan at the same time. Increasing this number will make scanning go faster, but put an additional strain on the PC performing the scans.

Logging Options:

- **Log File** – The path to a file that will contain the results of the polling operation.
- **Logging Level** – The level of detail that will appear in the log file. The choices are:
  - Full – Records the progress of all PCs
  - Errors and Summary – Records only the errors (if any) and a summary
  - Summary Only – Records only the summary
  - None – No logging

Note: The file name displayed is automatically generated using an embedded date format for the current day.

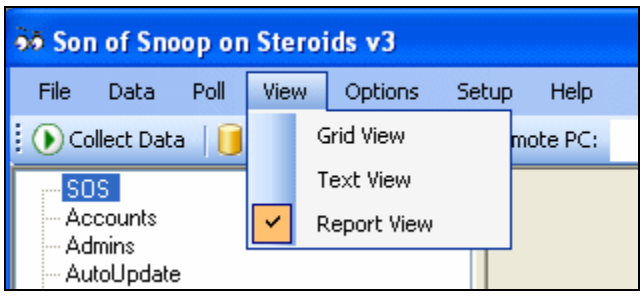
Status:

- **Data Collection Started** – A progress bar showing the number of PCs where data collection has started
- **Data Collection Completed** – A progress bar showing the number of PCs where the collection has completed
- **Status** – A status window showing the current activity
- **Elapse Time** – A running elapse time counter
- **Estimated Time Remaining** – An estimate of the remaining time to complete the polling of all PCs.

Note: During polling, the Close button becomes the Cancel button. It may take several seconds to interrupt the polling process… be patient.

4.4 View Menu

The View Menu controls the visual aspects of the application.



View:

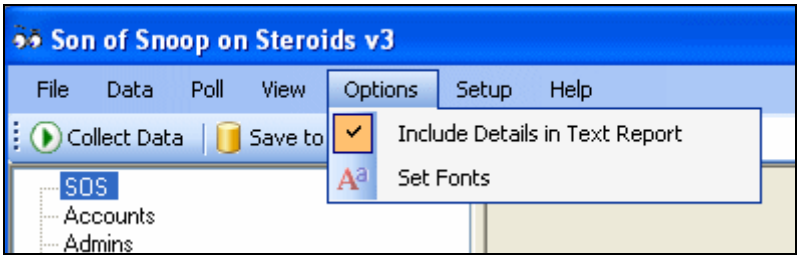
- **Grid View** - Displays all records in a grid similar to that of Microsoft Access. Users can sort by a column by clicking on the column heading
- **Text View** - A text-based view suitable for printing and saving to a text file. Makes use of the *Include Details in Text Report* option to "filter" some of the less interesting data.
- **Report View** – Uses a database-style navigator to view individual records.

Note: Users can edit existing records in the Grid and Report View, but cannot add or delete a record.

Note: The selected view will be remembered and automatically used the next time the program is run.

4.5 Options Menu

The Options Menu allows the user to select view options and display fonts.



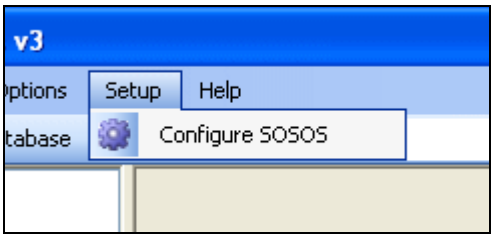
Options:

- **Include Details in Text Report** – Controls the level of detail used in the *Text View*, the *Save Text Report*, and *Print Text Report* functions. The Text View can be quite large (30-40 pages)…this option helps reduce the size of the report by eliminating some of the less interesting parts of the data.
- **Set Fonts** – Allows the user to select the display font that will be used throughout the program.

Note: The selected options will be remembered and automatically used the next time the program is run.

4.6 Setup Menu

The Setup Menu is used to configure the SOSOS options.



Setup:

- **Configure SOSOS** – This topic is covered in the *Setup and Configuration Guide.*

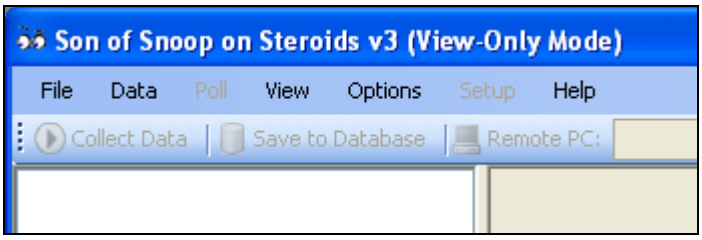
5. Viewing SOSOS Data

SOSOS does not have a built-in database… instead it relies on a 3rd-party database application to store its information.

You can use SOSOS to view existing records in the database for the current PC and for other PCs. However, distributing SOSOS to every user may not be in the best interest of security.

5.1 ViewSOSOS

ViewSOSOS is a read-only interface to the SOSOS application that is designed so that users may view, but not edit the data. The data gathering and database writing features are disabled.



Note: The protection of the data actually takes place at the database application itself by controlling the access given to the individual users or groups of users.

See the *SOSOS Setup and Configuration Guide* for additional information on how to set up and deploy the database applications.

5.2 Direct Database Access

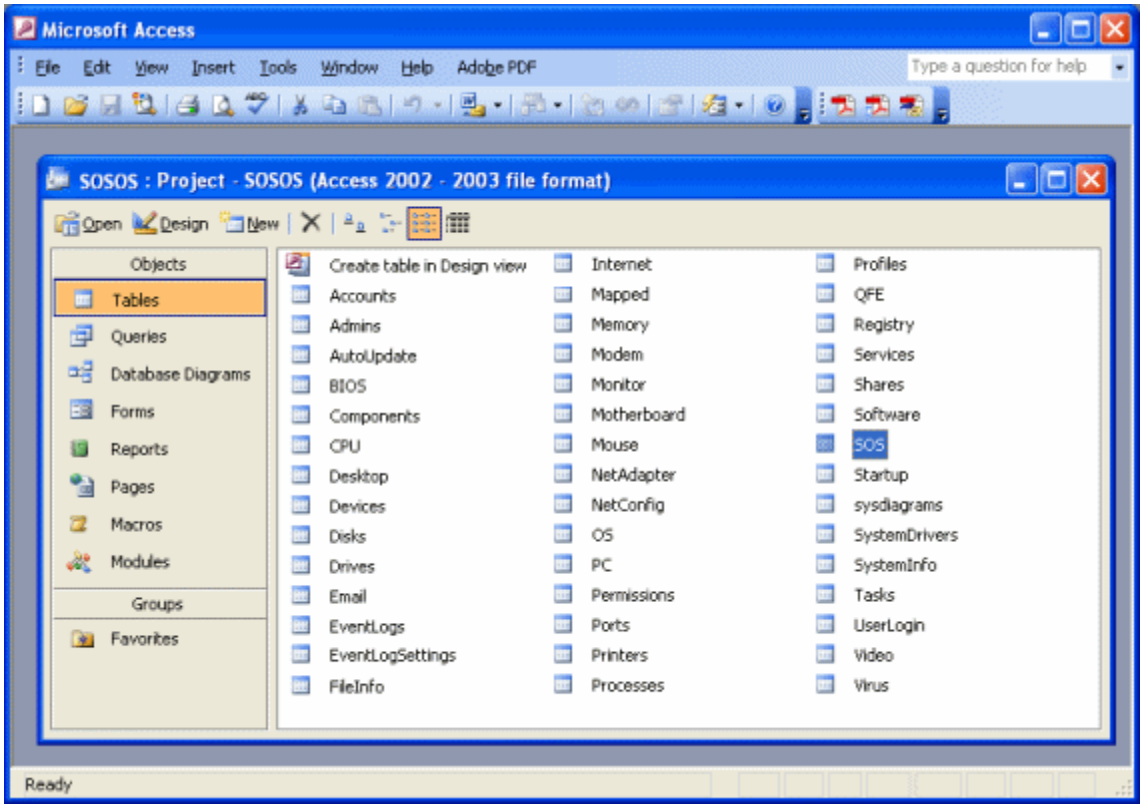
The SOSOS and ViewSOSOS applications are useful for viewing a single PCs set of records at a time, and do not support any type of querying capability.

Administrators will probably prefer to use direct access to the underlying database to view, query, edit, and manage the SOSOS information. The real power of SOSOS is the ability to write queries against the database to quickly answer real-life questions of a system administrator.

A common deployment scenario is to use Microsoft's SQL Server as the database server and to use Microsoft Access as the "front end". Modern versions of Microsoft Access support a "project file" (with an *.adp extension), which provides users with an easy way to interact with data on the SQL Server data without having SQL Server client software installed.

See the Microsoft Access help files for instruction on how to create a project file.

Below is a sample of a Microsoft Access Project file:



With appropriate authority, users can create queries, generate reports, etc., “as if” the entire database was a Microsoft Access *.mdb file.

Frequently Asked Questions

Part 1: Running the applications

Q: I get a message that says that I should install something

A: All of the SOSOS programs require the ".Net Framework" to be installed on the client PC. When using SOSOS to remotely gather information from PCs in a LAN, it is not a requirement that the remote PCs have the .Net Framework installed.

Download and install the .Net Framework 2.0 from:
http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en

Q: I get some message about permissions…

A: One of the features of the .Net Framework allows users to set "code access permission" for the PC (or individual programs). By default, the Framework's own security settings will not allow any program to run from a network share that requires "significant" permissions. Since SOSOS requires a lot of permissions to work properly, the default settings will not allow it run from a network share. *Note: The default settings are sufficient when SOSOS is run from a local drive.*

To solve the problem, you can either copy the program files to a local drive, or adjust the .Net Framework assembly permissions.

Warning: If you have multiple versions of the Framework installed, make sure you're adjusting the setting for correct version. Settings for one version have no affect on other versions.

To adjust permissions, you use the *.Net Framework 2.0 Configuration* control panel applet (on a development PC). Navigate to "Configure Code Access Security Policy", "Adjust Zone Security", "Make changes to this computer". Click on the Local Intranet icon and move the slider up to "Full Trust".

You can also use the *.Net Framework 2.0 Configuration* control panel applet to create an MSI file that you can use to deploy these changes via a GPO or login batch to the other PCs in your LAN. Click on the "Configure Code Access Security Policy", "Create Deployment Package". When the Wizard opens, click on the "Machine" security policy, and select a folder/name of the MSI file that will be created.

Q: I adjusted the permissions, but it still doesn't work

A: Make absolutely sure that you have adjusted the settings for the correct version of the Framework.

For version v1.0 and v1.1, Microsoft included the control panel applet with the Framework. But for reasons that only they know, the control panel applet is not installed with version 2.0. Only the development PCs get the control panel applet for v2.0.

That means to adjust the settings on an ordinary PC without the applet, you must use the technique described above to create and deploy an MSI file.

Q: I can't run SOSOS against a remote computer running WinXP SP2; the connection fails.

A: Most likely the problem is with the firewall settings. The default setting for the built-in firewall for XP Service Pack 2 and beyond excludes remote administration. Run the following on the remote PC to configure the firewall:

netsh firewall set service RemoteAdmin enable

For additional information see: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/connecting_through_windows_firewall.asp

Q: I can't run SOSOS against a remote computer running Windows Vista; the connection fails.

A: By default, Windows Vista blocks WMI traffic, so you should adjust the Windows Firewall settings to allow for WMI traffic to pass. Run the following on the remote PC to configure the firewall:

netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

For additional information, see: http://msdn2.microsoft.com/en-us/library/aa822854.aspx

Q: I still can't get SOSOS to run against a remote Vista PC; I get Permission Denied

A: If you are in a Workgroup environment (not a domain), you will have to disable the User Account Control (UAC) feature on the remote Windows Vista PC.

From the Control Panel, click on User Accounts, and click on "Turn User Account Control on or off". Clear the checkbox and press the OK button. (This change will require a reboot).

Q: I can't run SOSOS against on a remote computer running WinXP Home

A: Microsoft has deliberately removed the ability to remotely administer computers running WinXP Home Edition (and Windows Me). *Note: SOSOS runs locally on WinXP Home without any problems.* Sorry, there is no known work around.

Q: Why does it take so long to gather data on some PCs?

A: The most likely cause is the collection of the event logs. There are several settings that can be used to reduce the amount of data collected from event logs. See Section 2.5 of the *Setup and Configuration Guide* for information about changing the *Filter by number of lines* and *Filter by number of days* settings.

Alternately you can change the audit policy for the PC to reduce the amount of data being recorded to the event log. For details on the audit policy settings, see http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/516.mspx?mfr=true.

Q: The help file comes up but just contains an error message

A: Microsoft recently changed the security settings for compiled HTML help files (*.chm). These new restrictions apply when the help file is being open from a network share. See the following for a fix: http://support.microsoft.com/kb/892675/

Part 2: Compiling the source code

Q: When compiling I get a lot of errors about ADOX.

A: You've probably got the wrong set of Visual Basic Project files (*.vbproj). When compiling on Windows XP (or Windows 2000 or Windows Server 2003), you should use the project files that are in the WinXP_vbproj.zip file

Q: When compiling, I get a lot of errors about ADODB, ADOX, and TaskScheduler.

A: You've probably got the wrong set of Visual Basic Project files (*.vbproj). When compiling on Windows Vista, you should use the project files that are in the WinVista_vbproj.zip file.

Q: Why do I get a few warning about Custom Marshalling when compiling on Vista?

A: This is just a warning saying that the default technique used by the compiler can't figure out how to marshal a few parameters. You can safely ignore those errors.

Q: I get a message saying that a Reference to the Microsoft.Data.ConnectionUI.dll can't be found.

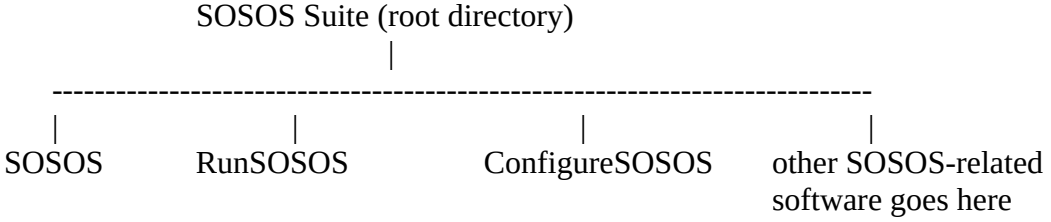
A: The location of this file has changed for Visual Studio 2008. So, just edit the path for the reference to: C:\Program Files\Microsoft Visual Studio 9.0\Common7\IDE\Microsoft.Data.ConnectionUI.dll

Q: When compiling the program, I get a message about something is missing

A: Visual Basic 2005 Express Edition does not support the "Setup" project type, so it will fail to load this part of the solution. You can safely ignore this error.

Q: SOSOS compiles fine, but some of the other programs are missing files

A: Almost all of the SOSOS-related programs share parts of the source code with the main SOSOS program and use "links" to find the files. Therefore you should not change the folder structure of the source code in the zip file. All of the applications should share a common "root" directory (just like in the zip file).



Part 3: The data that's collected

Q: I didn't get the contents of the Security logs in the EventLogs table

A: Windows typically has higher security settings on the Security log and therefore only administrators can read from that log. If the user who runs SOSOS is not an administrator on that PC, then you should consider using another deployment scenario. See the *Setup and Configuration Guide* for details.

Q: Some of the records in the database have an error message

A: SOSOS often records error messages in the database. This is normal. A detailed account of what went wrong may also be recorded in the Error Log file. Some minor errors that are anticipated are not recorded in the log file.

Q: My database is huge! What can I do?

A: The size of the database is probably due to the collection of Event Logs. There are two ways to "filter" the collection of Event Log data using the provided ConfigureSOSOS utility. The "Feature Setting" tab as a place to adjust the "Filter by number of lines" and/or "Filter by number of days".

Alternately, you can adjust the security policy on each PC to not collect as much detail in the event log. For additional information on each of the Audit Policy settings, see http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/aptopnode.mspx?mfr=true

There are also some compile-time variables at the top of the snoop.vb file that will reduce the amount of data that is collected.

In addition to the methods described here to reduce the *quantity* of data in the database, you can also selectively "turn off" and "turn on" entire sections of the database. The Feature Selection tab of the Configuration Utility allows you to select which tables you wish to enable or disable.