



# Sun StorageTek™ Business Analytics Installation Guide

---

Release 5.1

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 819-7181-10  
November 2006, Revision 01

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

# Copyright

## English:

Copyright © 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Use is subject to license terms.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Jiro, Solaris, Sun StorEdge, Sun StorageTek and StorageTek are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

This product is covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

## French:

Copyright © 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

L'utilisation est soumise aux termes de la Licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Jiro, Solaris, Sun StorEdge, Sun StorageTek et StorageTek sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Ce produit est soumis à la législation américaine en matière de contrôle des exportations et peut être soumis à la réglementation en vigueur dans d'autres pays dans le domaine des exportations et importations. Les utilisations, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers les pays sous embargo américain, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exhaustive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.



# Table of Contents

## Chapter 1: Installing Infrastructure Components

Table of Contents.....	4
Introduction.....	6
Central Manager Installation.....	6
Central Manager Prerequisites.....	6
Installing Microsoft SQL Server on a Windows Central Manager.....	8
Installing SQL Server 2000 Service Pack 3 .....	12
Central Manager Installation.....	15
Install the Software License.....	23
Configure the Central Manager Agents.....	23
Smart Agent Configuration.....	23
Remote Share Configuration Tool for SRM Agent.....	42
Business Analytics Agent Diagnostic Tool.....	55
Verify Central Manager Agent Functionality.....	59
SNMP Proxy Agent on Central Manager.....	62
Management Console .....	63
Install/Verify Microsoft IIS Server IIS 5.0.....	63
Additional Configuration Settings for Windows 2003 SP1.....	64
Management Console Configuration.....	70
Add the Local Manager Using the Management Console.....	77
Installing Local Manager - Windows.....	78
Installing SNMP Proxy Agent on Windows Local Manager.....	80
Solaris Local Manager Installation CD Setup Script.....	81
Business Analytics Solaris Base Software and Utilities.....	81
Installing Local Manager – Solaris.....	83
Installing the SNMP Proxy Agent on Solaris Local Manager.....	86
Infrastructure Components Upgrade Summary.....	91
Central Manager Software Upgrade Summary.....	92
Using the aggconvert Utility.....	96
Using gsa_proc_views_users_40_upg.sql .....	97
Uninstall Database Setup.....	98
Upgrade Local Manager - Windows.....	101
Upgrade Local Manager - Solaris.....	102
Device/Application Agents.....	103
Message Infrastructure.....	104
Central Manager Disaster Recovery.....	105



# Chapter 1: Installing Infrastructure Components

## Introduction

This manual describes the procedures to install, configure, and verify installation of Sun StorageTek Business Analytics 5.1 software infrastructure. There are two types of deployments:

- First time deployment of Sun StorageTek Business Analytics Release 5.1 software components
- Upgrade deployment of software components to Sun StorageTek Business Analytics Release 5.1

**Note:** With the acquisition of StorageTek, Sun Microsystems has re-branded and re-named Global Storage Manager (GSM) as Sun StorageTek Analytics, a member of the Enterprise Storage Manager portfolio of software solutions.

This chapter covers the first-time installation of the infrastructure components, including the Central Manager, Management Console, and Local Manager.

**Warning:** Terminate running all virus scan software before you install the Central Manager, Management Console, or Local Manager software.

## Central Manager Installation

The following sections outline the installation steps for the Sun StorageTek Business Analytics Central Manager that:

- Create the databases, schemas, and stored procedures.
- Install user-specified smart agents.
- Install the Configuration Tool.

### Central Manager Prerequisites

If you are installing the Sun Storagetek Business Analytics Central Manager on a Windows 2003 server, the operating system blocks Port 1433 for security purposes. After you install Microsoft SQL Server Service Pack 3, the operating system opens that port. Therefore, install Microsoft SQL Server Service Pack 3 on the Windows 2003 server before you run the GSM Database Setup procedure.

Using SQL Query Analyzer, you can use the following SQL queries to verify the database server environment.

- `select @@version` – Identify the installed version of SQL Server. An example follows.

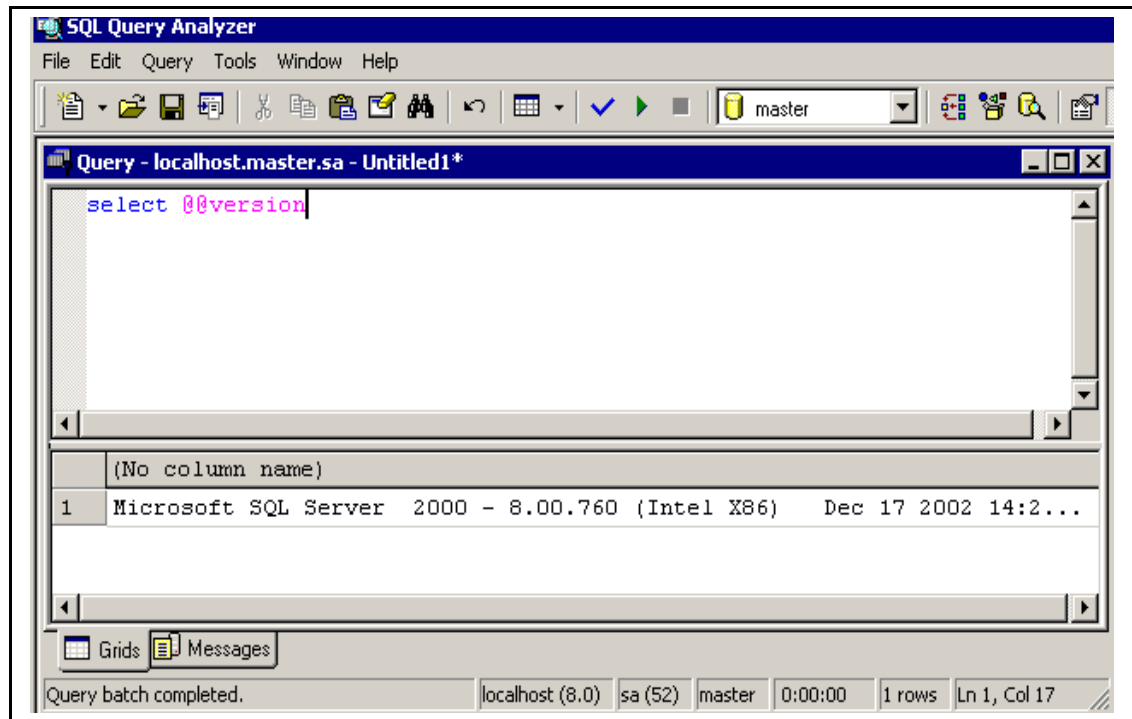


Figure 1 - select @@version

- `exec sp_helpsort` - This query shows if your SQL Server is case sensitive or case insensitive. An example follows.

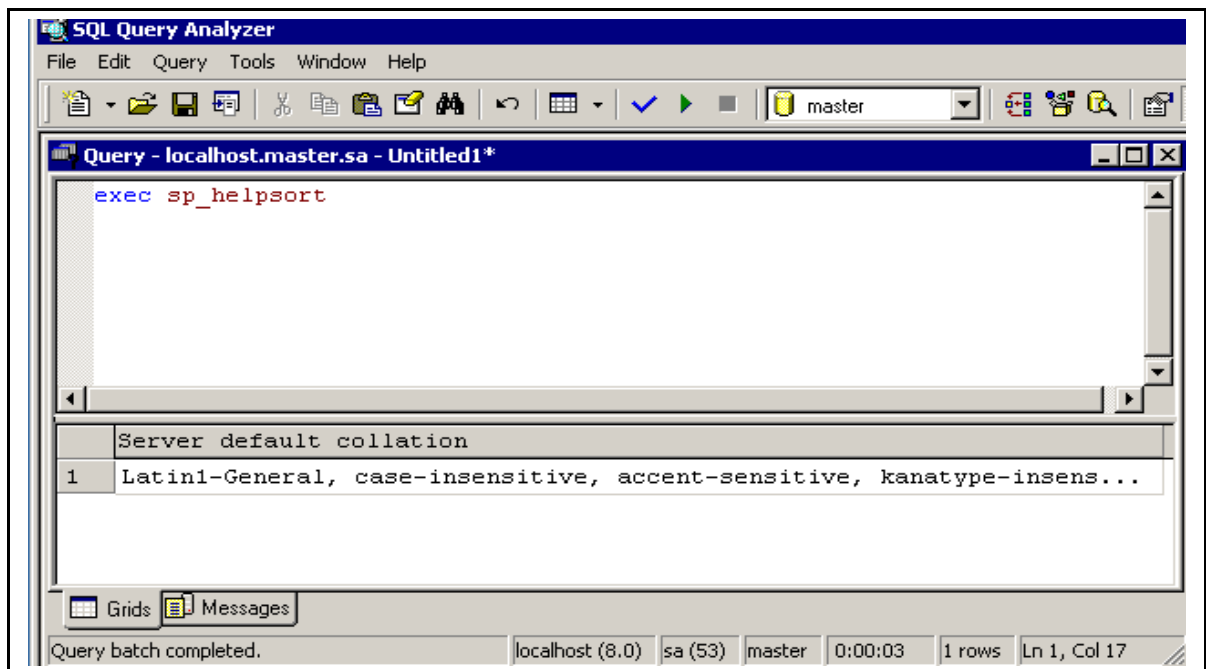


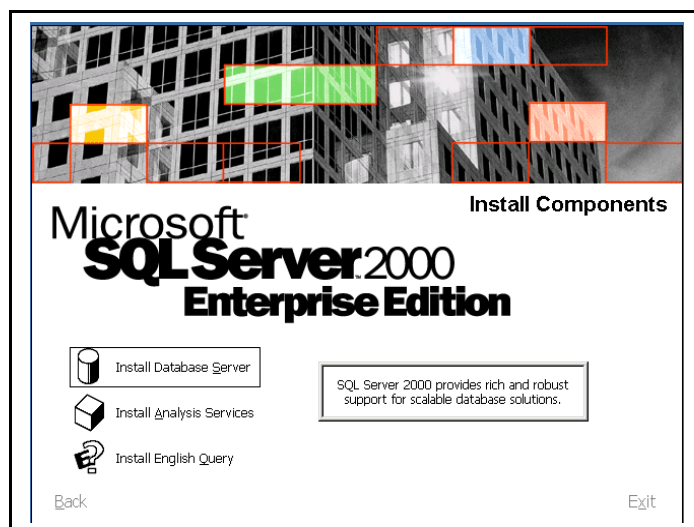
Figure 2 - exec sp\_helpsort

**Note:** The Sun StorageTek Business Analytics Central Manager no longer requires that SQL 2000 Server is configured “Case-Sensitive” unless you are upgrading or attaching an existing, case-sensitive database.

## Installing Microsoft SQL Server on a Windows Central Manager

The Sun StorageTek Business Analytics Central Manager can use MS SQL Server 2000 for its databases. The following section contains installation instructions you follow **if your Windows 2000/2003 server is not installed with this Windows SQL Server database software**. If you have verified a Business Analytics-supported Microsoft SQL Server database is already installed and running, proceed to the following Sun Storagetek Business Analytics *Central Manager Installation* section of this chapter.

1. Insert the SQL 2000 Server or Enterprise Edition CD in the CD-ROM drive.
2. Execute Autorun.exe from the CD (if it does not auto run).
3. Select **SQL Server 2000 Components**.
4. Select **Install Database Server**.



**Figure 3 - Install Components Dialog Box**

5. Setup will continue. When the Welcome Screen dialog appears, click **Next** to continue.
6. When the Computer Name dialog box appears, select **Local Computer** for local installation.

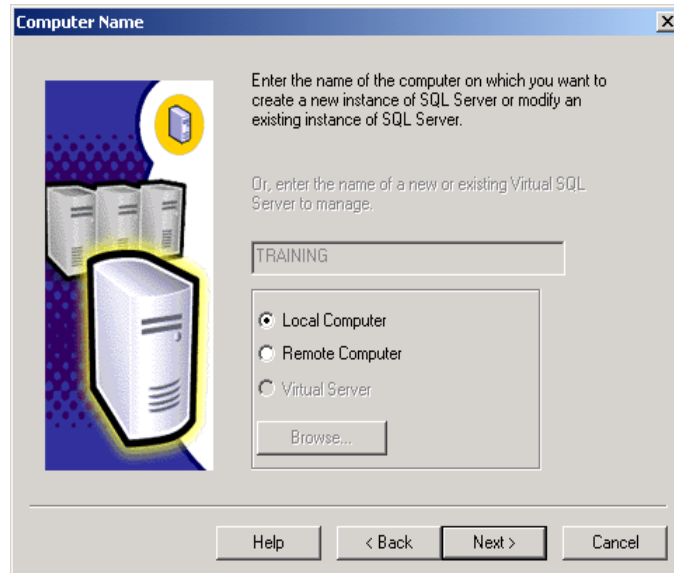


Figure 4 - Computer Name Dialog Box

7. When the Installation Selection screen appears, select **Create a new instance of SQL Server, or Install Client Tools** and click **Next>** to continue.

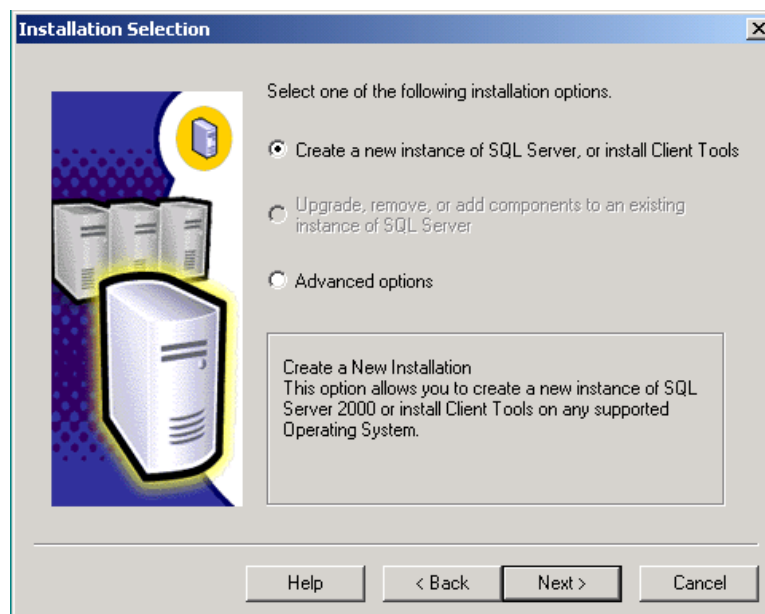
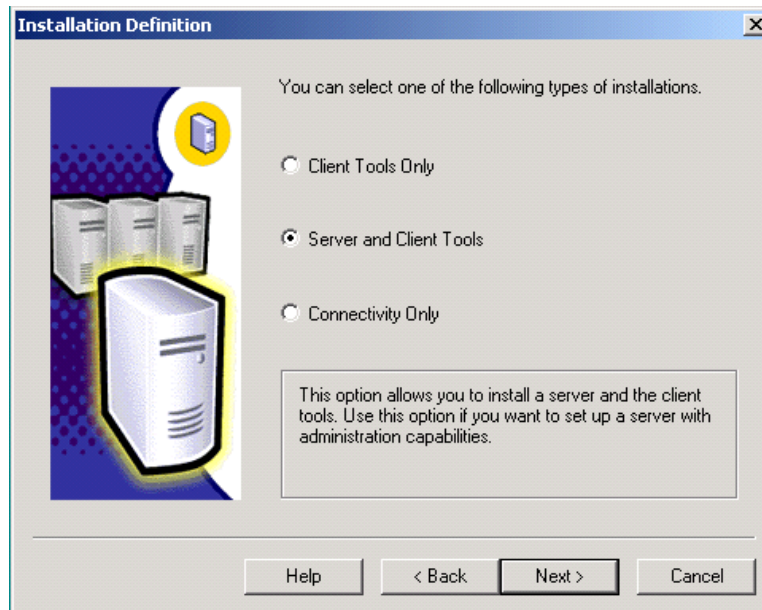


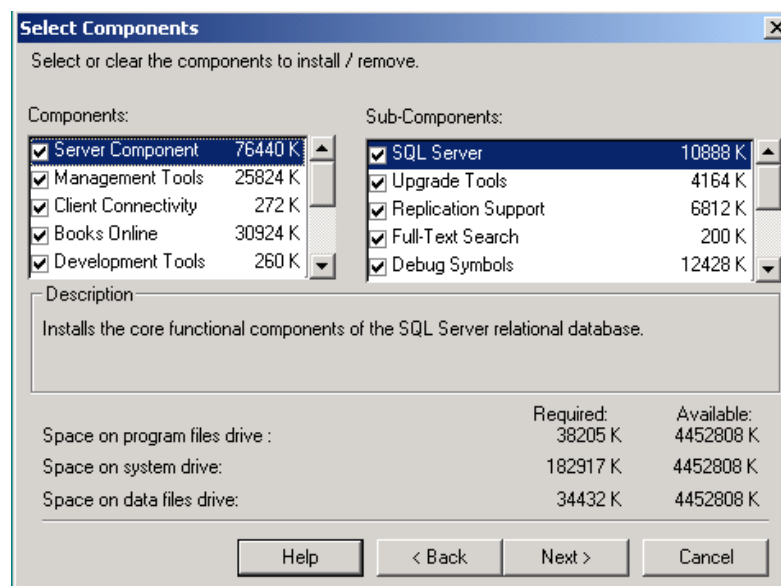
Figure 5 - Installation Selection Dialog Box

8. When the User Information dialog box appears, enter appropriate information for the **Name** and **Company**.
9. When the Software License Agreement screen appears, click **Yes** to continue.
10. When the Installation Definition dialog box appears, select **Server and Client Tools**, and click **Next>** to continue.



**Figure 6 - Installation Definition Dialog Box**

11. When the Instance Name dialog box appears, select **Default** (default value checked) and click **Next>** to continue.
12. When the Setup Type dialog box appears, select **Custom**.
13. Browse to the appropriate Destination Folder where you would like to install the **SQL Program Files** and **Data Files**. Click **Next>** to continue.
14. When the **Select Components** dialog box appears, select and check the appropriate SQL Server Components you would like to install. Uncheck anything you do not want to install.



**Figure 7 - Select Components Dialog Box**

15. When the Service Accounts dialog box appears, select **Use the same account for each server, Auto start SQL Server Service.**
16. Select **Use the Local System Account for local server installation.** Click **Next>** to continue.

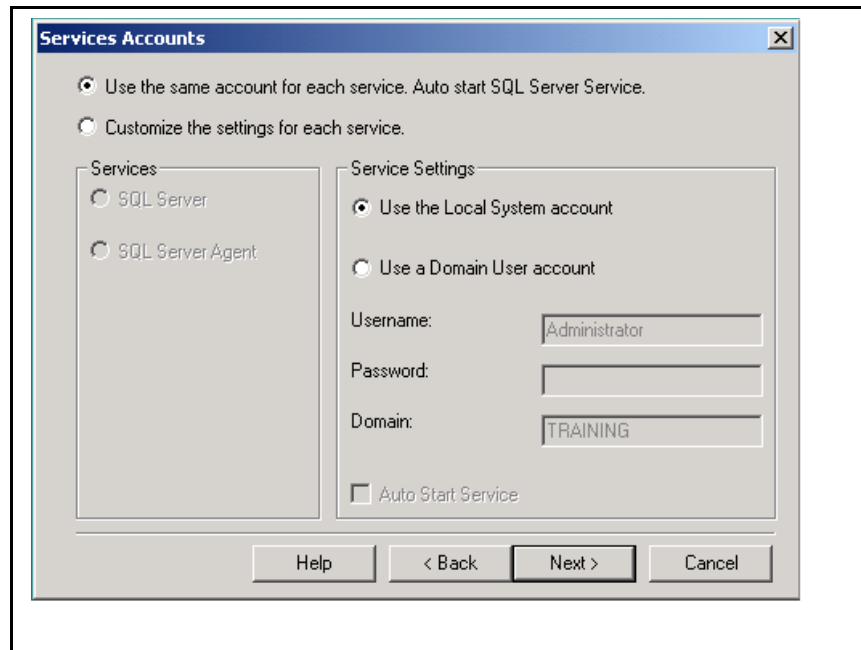


Figure 8 - Service Accounts Dialog Box

17. When the **Authentication Mode** dialog box appears, select **Mixed Mode**, and enter the new SQL 2000 Server system administrator **password**. Click **Next>** to continue.

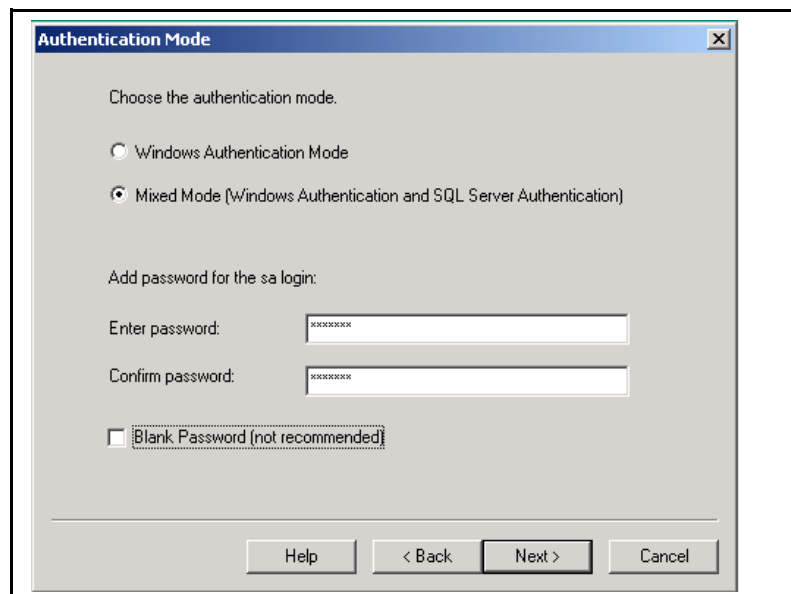
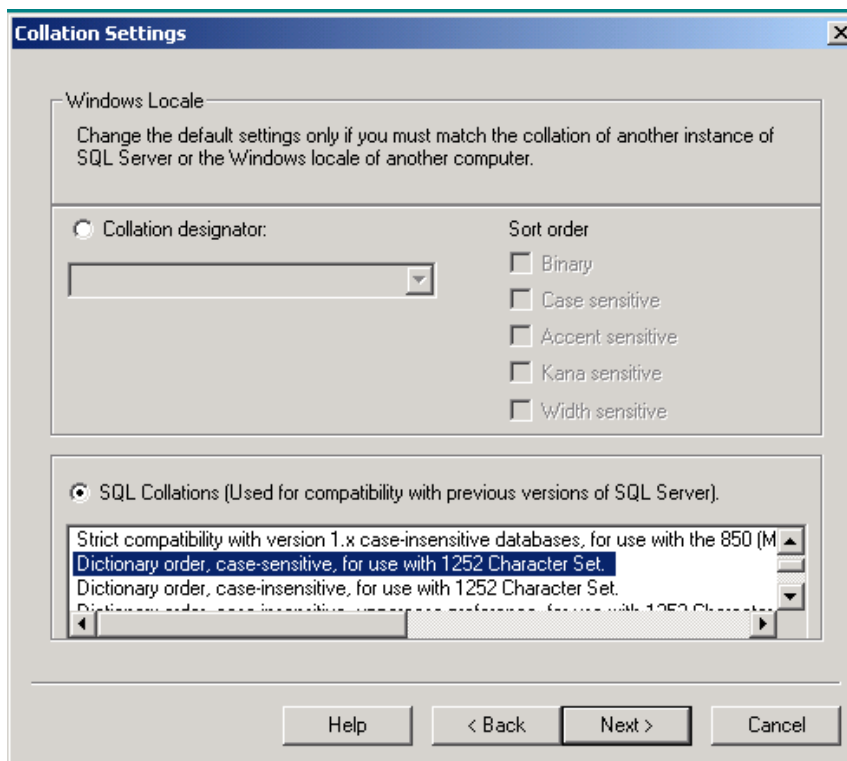


Figure 9 - Authentication Mode Dialog Box

18. When the Collation Settings dialog box appears, highlight **Dictionary order, case-sensitive, for use with 1252 Character Set.**

**Note:** The Sun StorageTek Business Analytics Central Manager no longer requires that SQL 2000 Server is configured "Case-Sensitive" unless you are upgrading or attaching an existing, case-sensitive database.



**Figure 10 - Collation Settings Dialog Box**

19. When the Network Libraries dialog box appears, select **TCP/IP Socket** and the **SQL default port "1433"**. Click **Next>** to continue.
20. When the Start Copying Files dialog box appears, click **Next>** to start copying files and continue with the installation.
21. When the SQL 2000 Server Licensing Mode dialog box appears, enter the appropriate **License**. For Licensing questions, please contact Microsoft.
22. When the Setup Complete dialog box appears, click **Finish**.

Next, reboot the Windows 2000/2003 Server before you install **SQL 2000 Database Component Service Pack 3**, as described in the following section.

## Installing SQL Server 2000 Service Pack 3

The following sections describe how to install Service Pack 3 for SQL Server 2000/2003.

### Identifying the Current Version of SQL Server or Analysis Services

Use the techniques that are described in the following sections to determine which version of SQL Server or Analysis Services you have installed.

#### SQL Server

1. To identify which version of SQL Server 2000 you have installed, type:  
`SELECT @@VERSION` or `SERVERPROPERTY 'ProductVersion'`  
at the command prompt using the **osql** or **isql** utility or the **Query** window in SQL Query Analyzer.
2. Similarly, the product level for a given version of SQL Server 2000 can be determined by executing:

```
SELECT SERVERPROPERTY 'ProductLevel'
```

The following table shows the relationship between the SQL Server 2000 version and level and the version number reported by @@VERSION and the product level reported by SERVERPROPERTY('ProductLevel').

SQL Server 2000 version and level	@@VERSION	ProductLevel
SQL Server 2000 RTM	8.00.194	RTM
Database Components SP1	8.00.384	SP1
Database Components SP2	8.00.534	SP2
Database Components SP3	8.00.760	SP3

Figure 11 - SQL Server 2000 Version and Level and Product Level

## Downloading and Extracting Service Pack 3

The self-extracting files can be downloaded from the Internet at the [Microsoft SQL Server Downloads Web site](http://www.microsoft.com/sql/downloads/default.asp): <http://www.microsoft.com/sql/downloads/default.asp>

## Installing Service Pack 3

1. Run **Setup.bat** and the **Welcome** dialog box appears. Click **Next** to continue.
2. When the **Software License Agreement** dialog box appears, click **Yes** to continue.
3. When the Instance Name dialog box appears, click **Next>** to continue and accept the default instance name.

**Note:** The installation program displays an **Authentication Mode** dialog box if it detects that the installation is using Mixed Mode Authentication with a blank password for the system administrator login. Leaving the system administrator login password blank provides users with easy administrative access to SQL Server or Desktop Engine, and is not recommended; protect your systems by enforcing a strong password.

4. Enter the system administrator ('sa') password. Click **Next>** to continue.

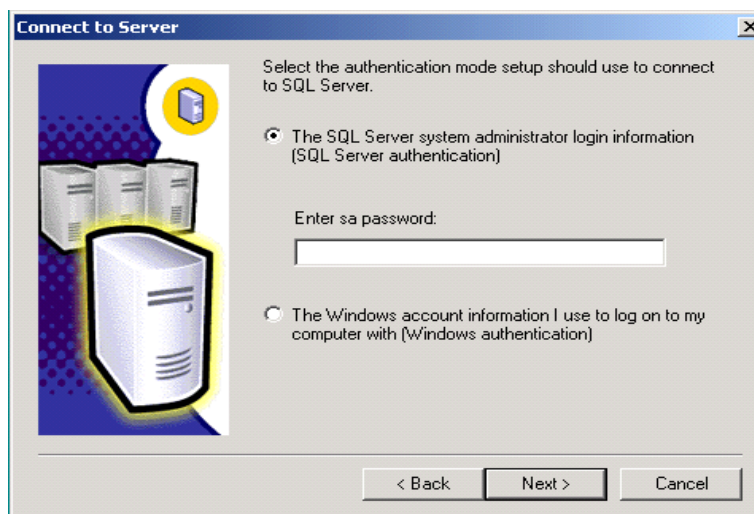


Figure 12 - Connect to Server Dialog Box

The Validating SQL Password dialog box appears if there was no **sa** password previously configured and you entered one on the Connect to Server dialog box.

The installation program displays an **SA Password Warning** dialog box if it detects a blank password currently exists for the **sa** login. Although you can continue the installation with a blank password for the sa login by explicitly choosing to ignore the recommendation and continue Setup, a blank password poses a security risk and is not recommended. This dialog is displayed regardless of the authentication mode you use.



Figure 13 - SA Password Warning Dialog Box

5. When the SQL Server 2000 Service Pack 3 Setup dialog box appears, select **Upgrade Microsoft Search and apply SQL Server 2000 SP3 (required)**. Click **Continue** to start the SP3 installation.

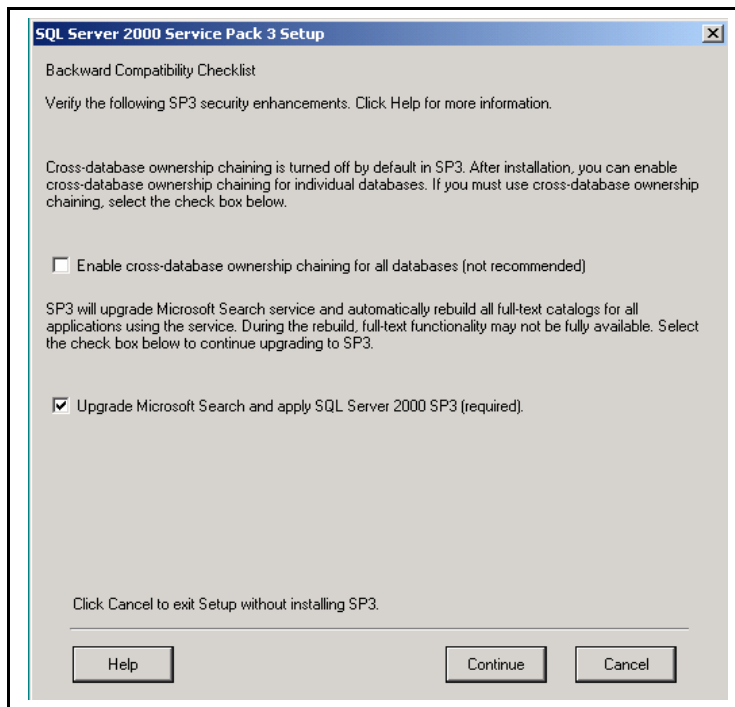


Figure 14 - SQL Server SP3 Setup Dialog Box

- When the Error Reporting dialog box appears, do not check **Automatically send fatal error reports to Microsoft**. Click **OK** to continue.

The "Please wait..." dialog box will appear. This may take a few minutes.

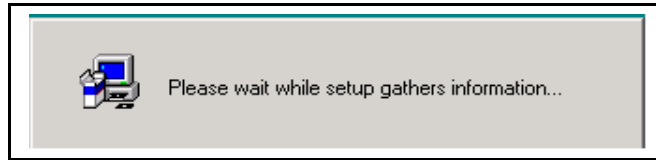


Figure 15 - Gathering Information Dialog Box

- When the **Start Copying Files** dialog box appears, click **Next** to continue.

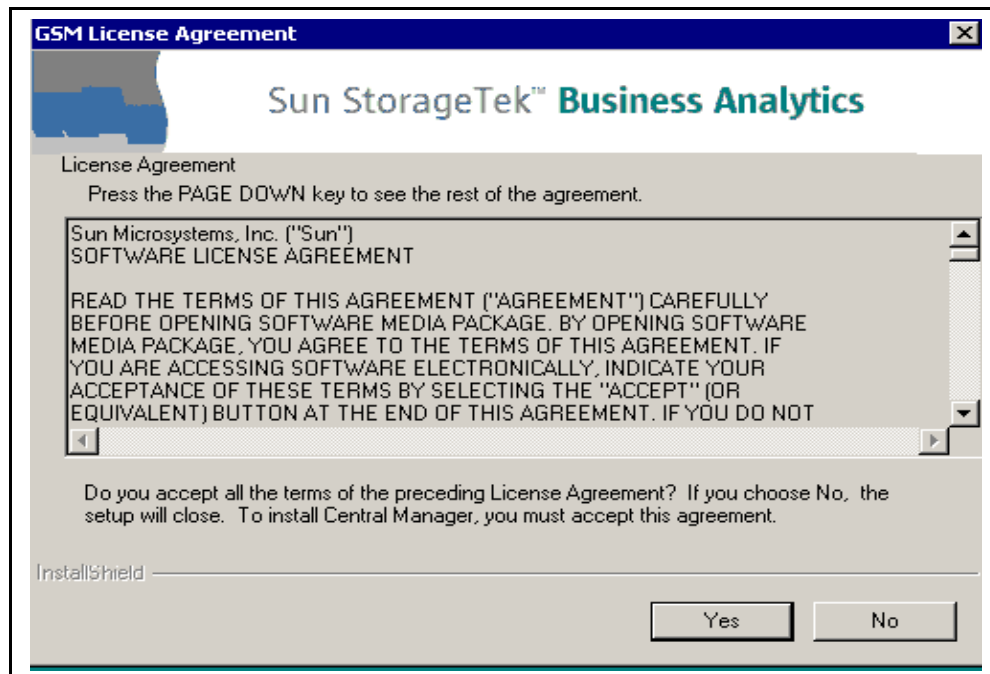
The script will run. This might take a while depending on the database component installed. It updates MDAC components if necessary. In addition, it replaces existing SQL Server 2000 files with SP3 files and runs Transact-SQL script files to update system stored procedures.

- When the **Setup Complete** dialog box appears, click **Finish**. The installation program displays an option to reboot the computer in the final dialog box if Setup determines that a reboot is needed.
- Reboot the Windows 2000 Server.

## Central Manager Installation

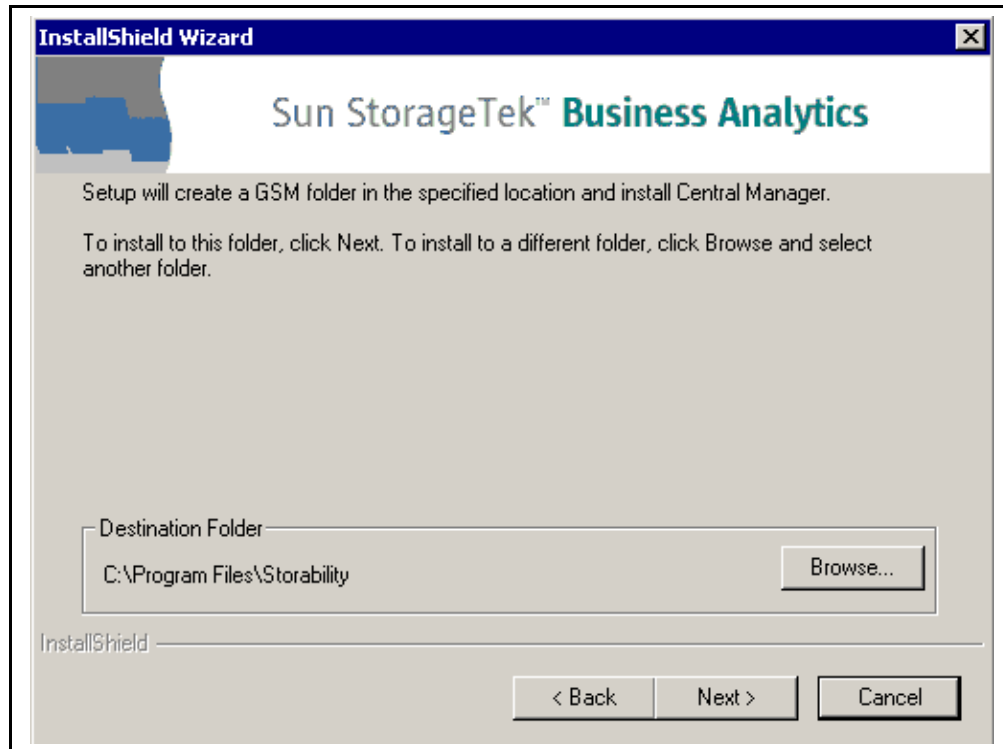
To install the Sun StorageTek Business Analytics Central Manager, proceed as follows:

- Insert the Sun StorageTek Business Analytics Central Manager Installation media into the CD-ROM drive on the Windows 2000/2003 server. The InstallShield-based installation (setup.exe) will start.
- Click **Yes** to accept the terms of the software license agreement.



**Figure 16 - Software License Agreement**

3. Review/change the informational **User Name** and **Company Name** fields and click **Next>** to continue.
4. Click **Next>** to install Central Manager to the default Destination Folder (or click **Browse** to change to desired location).



**Figure 17 - Select Destination Folder**

5. On the "Click the type of setup you prefer" dialog, choose **Typical** or **Custom** and click **Next>**.

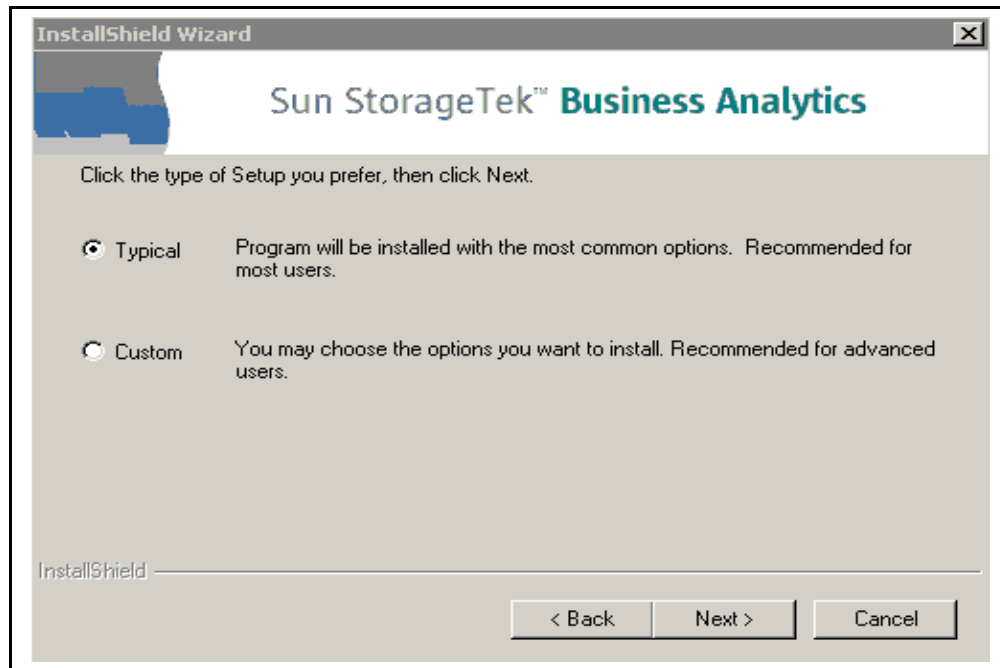


Figure 18 - Setup Type

6. The **Typical** installation option installs the following components:

- **GSM Database Setup** – Creates databases, tables, and installed procedures for first-time installation.
- **Storability Data Aggregator** – Aggregates collected data from Smart Agents into the assured database.
- **Storability Routing Agent** – Uses the agent registration table to allow it to activate, deactivate, and collect data from configured Sun StorageTek Business Analytics Smart Agents.
- **Storability Scheduling Agent** – Is used to support the scheduling of data collection from the deployed agents and policy execution.
- **Storability Data Polling Agent** – Validate data collection schedules and works with the Scheduler Agent to support data polling.
- **Storability Policy Agent** – Executes policies that are configured and scheduled through the Management Console's **Policy Alerting** menus. The Policy Agent must be running to use these menus.
- **Storability Host Agent** – Provides information on host servers, including HBA configuration, operating system, and file system details.
- **Scheduled Jobs** – Adds the Business Analytics scheduled job to the Windows Scheduler.
- **Storability License Agent** – Installs the License Agent used to support the audit license report.

The **Custom** installation allows you to additionally install the following agent(s) by clicking on their respective selection box:

- **Storability SRM Agent** – Provides disk usage statistics about volumes, files, and directories on a host; option is disabled unless the Host Agent has been selected.
- **Storability Proxy Agent** – Supports sending forwarded SNMP traps to a specified SNMP destination.

- **Storability Remote Host Agent** - Provides an interface to collect data from supported Windows and Solaris servers through the Windows Management Instrumentation (WMI) or Web Based Enterprise Management (WBEM) protocol.

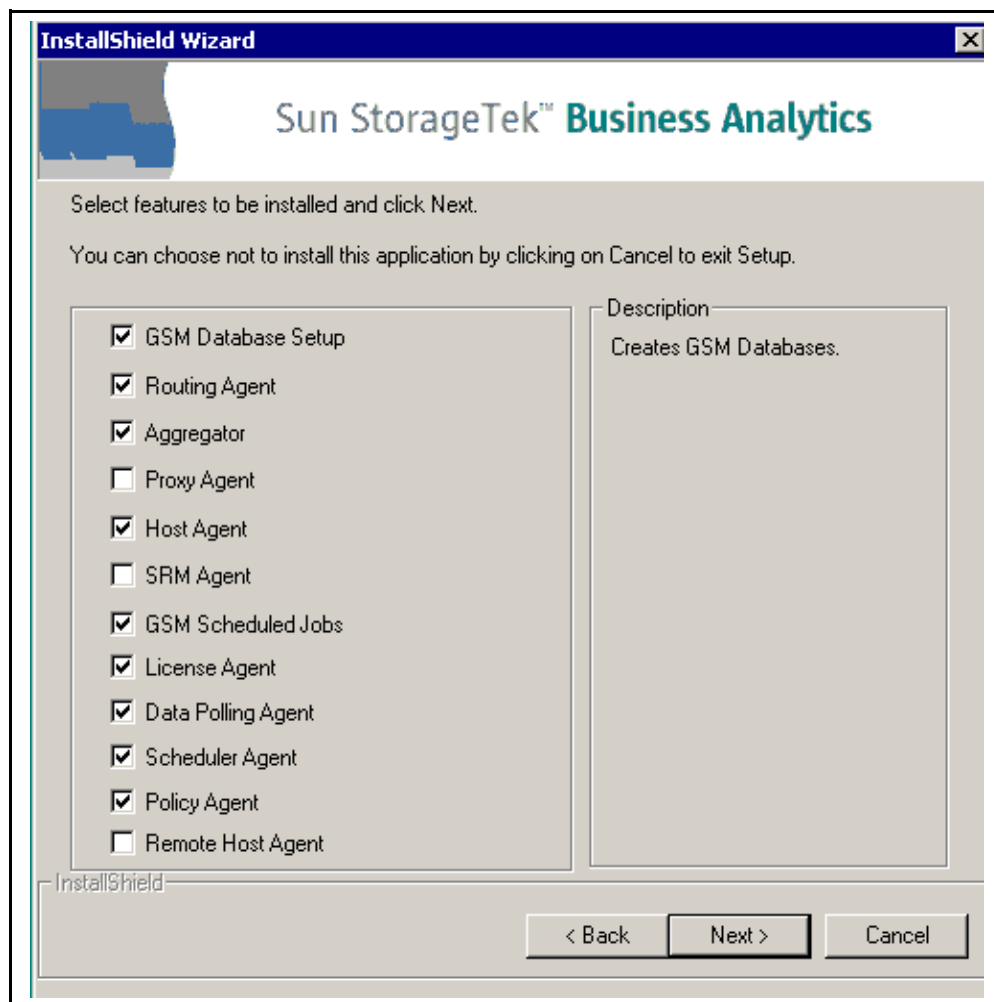


Figure 19 - Custom Install Dialog

7. Review the current settings and click **Next>**. The following screen shows the settings after a **Typical** setup type was selected.

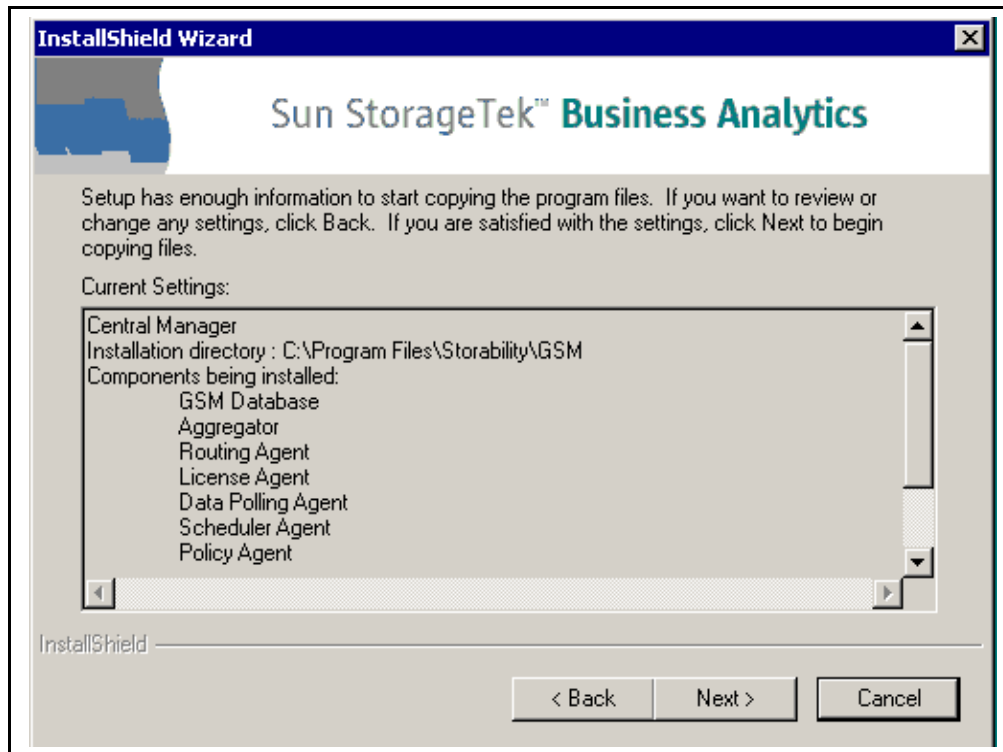
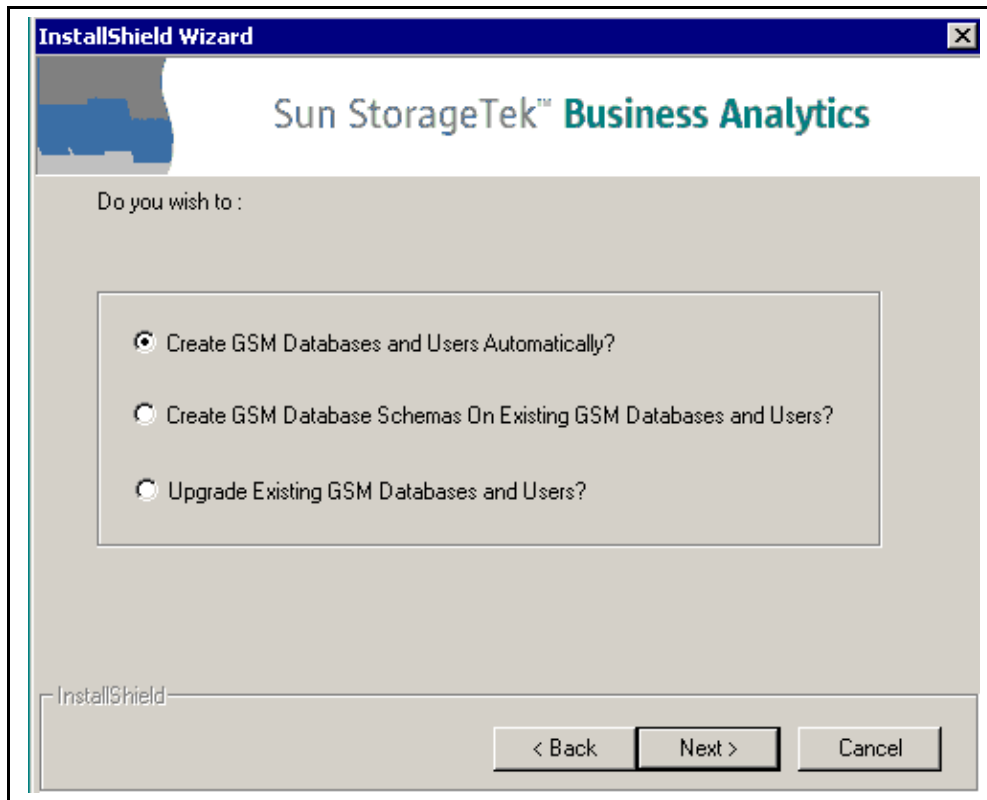


Figure 20 - Current Settings

8. Choose the desired installation type:

- **Create Database and Users Automatically** (default) – Select for first time Sun StorageTek Business Analytics Central Manager installation.
- **Create Database Schemas On Existing Database and Users** – Select to install only the database schema. This option may be used when a Database Administrator has already created the database and users for you.
- **Upgrade Existing Database and Users** – Select to upgrade the Central Manager to the current Sun StorageTek Business Analytics software version.

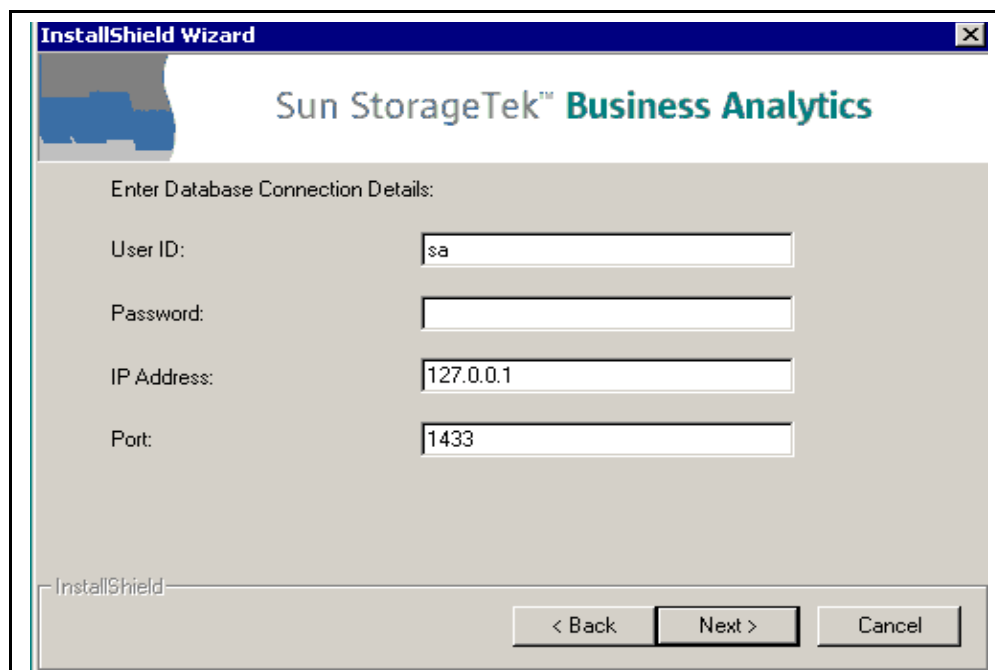
If the installation detects existing databases and their schemas, a dialog box will appear that allows you to choose whether the installation will upgrade or recreate the databases and schemas.



**Figure 21 - Desired Database Setup**

9. When the “Enter Database Connection Details” dialog appears, review/modify the SQL Server user (administrator) ID and password. The user/administrator must have administrative privileges to the SQL Server database that was created as a prerequisite. The default account is sa with no password.

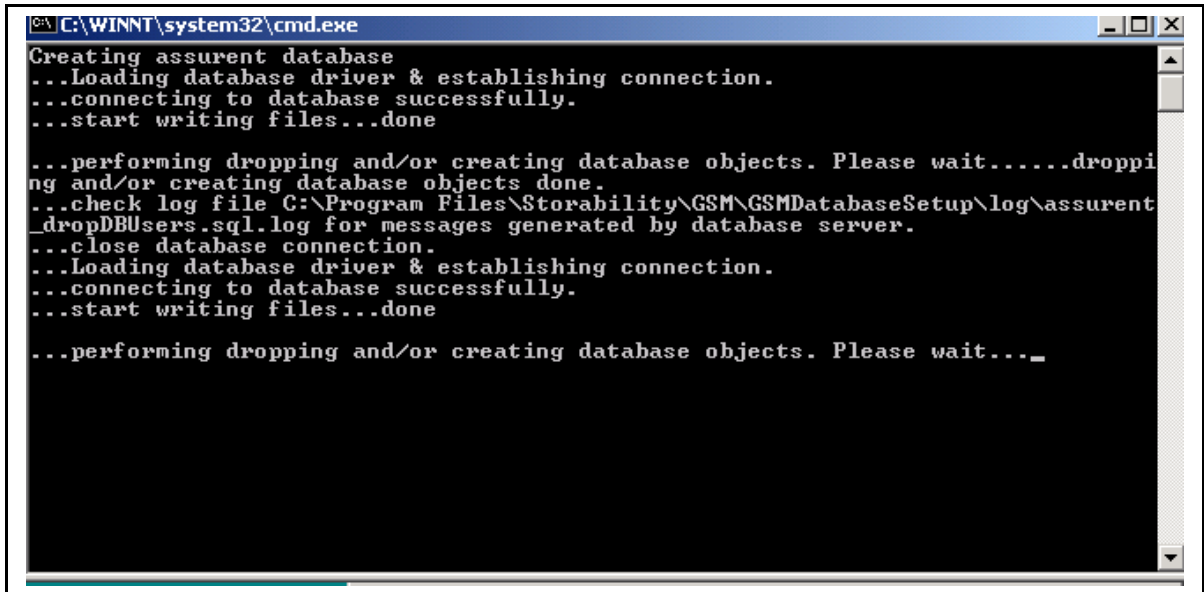
You also specify the IP address of the database server, and TCP port number. The default IP Address is 127.0.0.1 (localhost). After you enter the Database Connection Details, click **Next>** to continue.



**Figure 22 - Database Connection Details**

10. The Sun StorageTek Business Analytics Database Setup creates the assured and portal databases, tables, and stored procedures as well as installs the agents associated with the selected installation type (e.g., Typical). A status dialog box appears in the installation window to show the progress of the installation.

**Note:** If any error messages are displayed during the Central Manager database set up and/or there are problems accessing the databases after the installation, review the log files that are created in <drive>:\Program Files\Storability\GSM\GSMDatabaseSetup\log. Your support representative may request that you supply provide files if database creation cannot be completed successfully.



```
C:\WINNT\system32\cmd.exe
Creating assured database
...Loading database driver & establishing connection.
...connecting to database successfully.
...start writing files...done

...performing dropping and/or creating database objects. Please wait.....droppi
ng and/or creating database objects done.
...check log file C:\Program Files\Storability\GSM\GSMDatabaseSetup\log\assured
_dropDBUsers.sql.log for messages generated by database server.
...close database connection.
...Loading database driver & establishing connection.
...connecting to database successfully.
...start writing files...done

...performing dropping and/or creating database objects. Please wait....
```

Figure 23 - Sample Database Setup Status

11. Before the Central Manager's Host Agent is installed, an informational dialog box appears concerning the Microsoft Disk Management Diagnostic utility being needed for the Host Agent to report on dynamic disks.

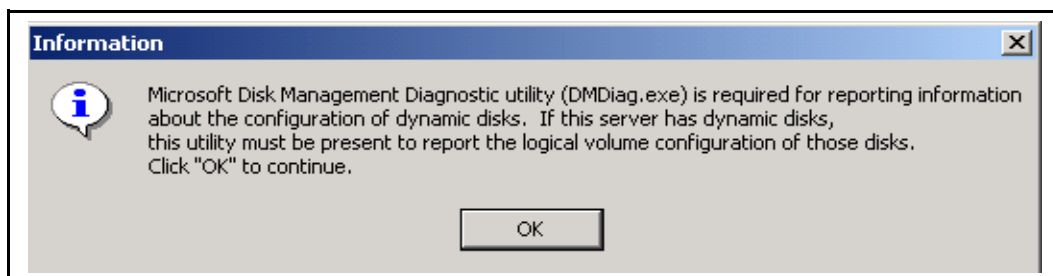


Figure 24 - Host Agent Information

12. Click **OK** to acknowledge the informational dialog box regarding the Microsoft Disk Management Diagnostic (DMdiag.exe) utility and to continue installing the Host Agent. Refer to the *Sun StorageTek Business Analytics Support Matrix* on the Documentation CD to obtain additional information regarding the Microsoft Disk Management Diagnostic (DMdiag.exe) utility if you are running dynamic disks.

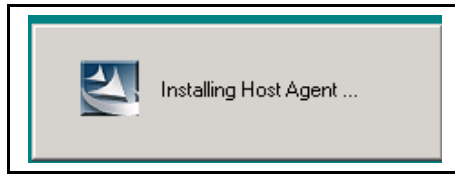


Figure 25 - Host Agent Install Splash Box

13. The **Configuration Tool** is installed and its window can be minimized on the desktop.

You can close or minimize it until after you have configured the Central Manager agents before starting them. Refer to the following **Configure the Central Manager Agents** section.

14. When the "System DSN must be configured for Aggregator to work. Do you want to configure System DSN?" dialog box appears, specify (yes/no) to have the System Data Source Name that the Aggregator uses to connect to the Sun StorageTek Business Analytics database automatically created and verified.

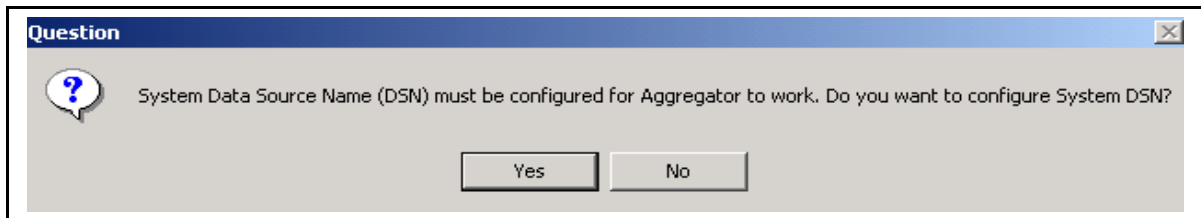


Figure 26 - Create System Data Source?

15. If you selected **Yes** in the previous step, the **Where is your GSM Database located** dialog box appears.
16. Review/modify the settings to suit your installation and click **Next>**. The default values are:
  - DSN Name: atlantis
  - User ID: assurent
  - Password: The password for the assurent database is "st0rage".
  - IP Address: 127.0.0.1
  - Port: 1433
17. Click **OK** when the informational dialog box appears indicating the **System DSN Configuration** is complete.

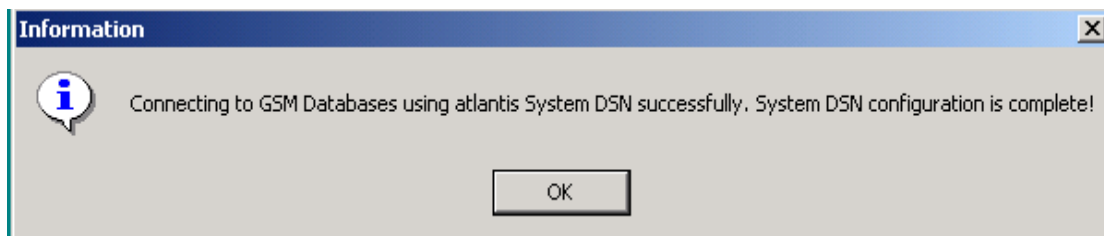


Figure 27 - System DSN configuration is complete!

18. Click **Finish** in the InstallShield Wizard Complete for Central Manager dialog box to complete the installation procedure.

## Install the Software License

The Sun StorageTek Business Analytics software license **must be** installed in the Central Manager Routing Agent folder to enable data collection to occur properly on the Central Manager. Proceed as outlined below.

1. Copy the **license file** (which you Sun Microsystems representative provides) and rename it to **license.txt** if necessary.
2. Paste the license file into the Routing Agent's installed directory. This is typically <install path>:\Program Files\Storability\GSM\Agents\Storability Routing Agent.
3. Start the Routing Agent using the Windows Component Services panel.
4. Using Windows Explorer, locate and open the Message.log for the Storability Routing Agent.
5. Verify there is a logged message indicating that "valid CM license found".

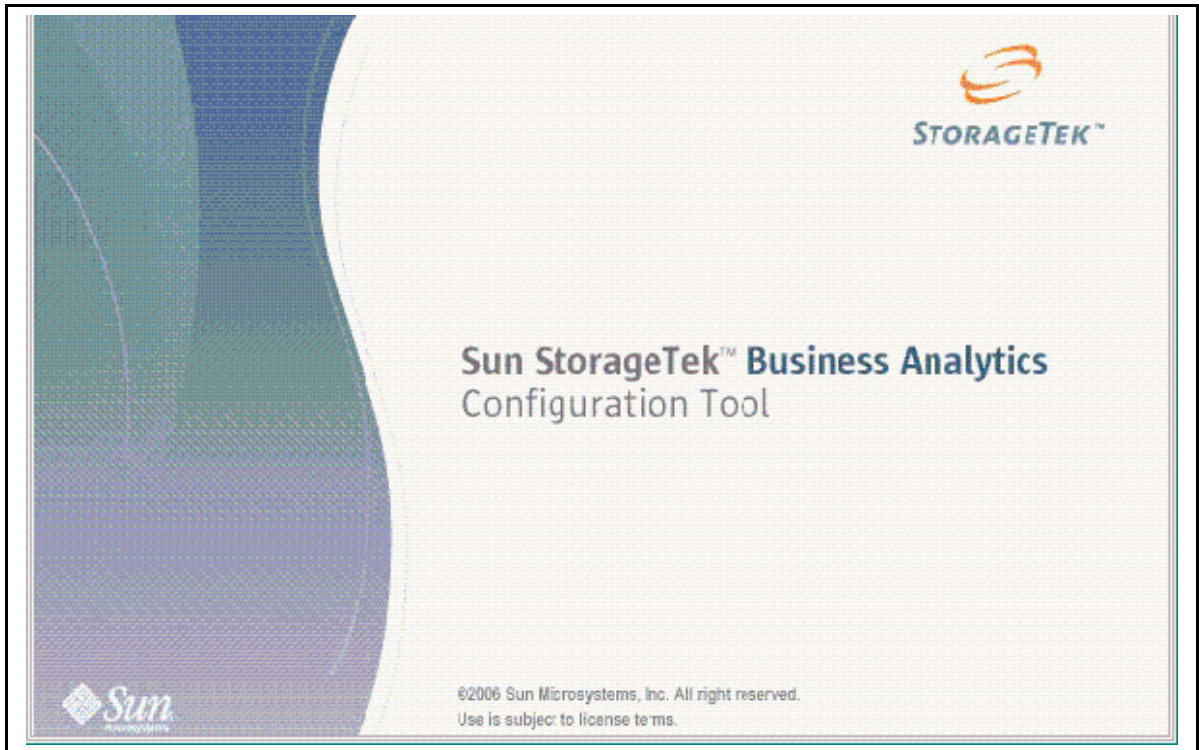
## Configure the Central Manager Agents

The Configuration Tool is used to configure the agents that you have installed on the Central Manager. These Central Manager agents (e.g., Data Aggregator Agent) must be installed, configured, and running before you set up agent data collection using the Management Console's Data Polling Schedule menus.

## Smart Agent Configuration

All Sun StorageTek Business Analytics Smart Agents (including the SMIS agents) read and observe configuration settings stored in the storability.ini (agent initialization) file. The configuration method depends on the platform on which the agent is installed, as described below.

- Windows – Use the Configuration Tool.
- Solaris – Type in confirmation settings during the package installation.
- Other UNIX – Manually enter configuration settings.



**Figure 28 - Configuration Tool Splash Screen**

## Introducing the Configuration Tool

The **Configuration Tool** is used to configure Windows-based Central Managers and Local Managers. This utility allows the administrator to configure all of the parameters associated with the Local Manager's Smart Agents, including device agents, Host Agents, and the Routing Agent.

It is launched automatically during the installation of Windows-based Central and Local Managers. To perform post-installation configuration changes, you can manually run the **Configuration Tool** from the Storability program folder by selecting the **Launch Configuration Tool** menu selection. The Configuration Tool Main Menu appears below.

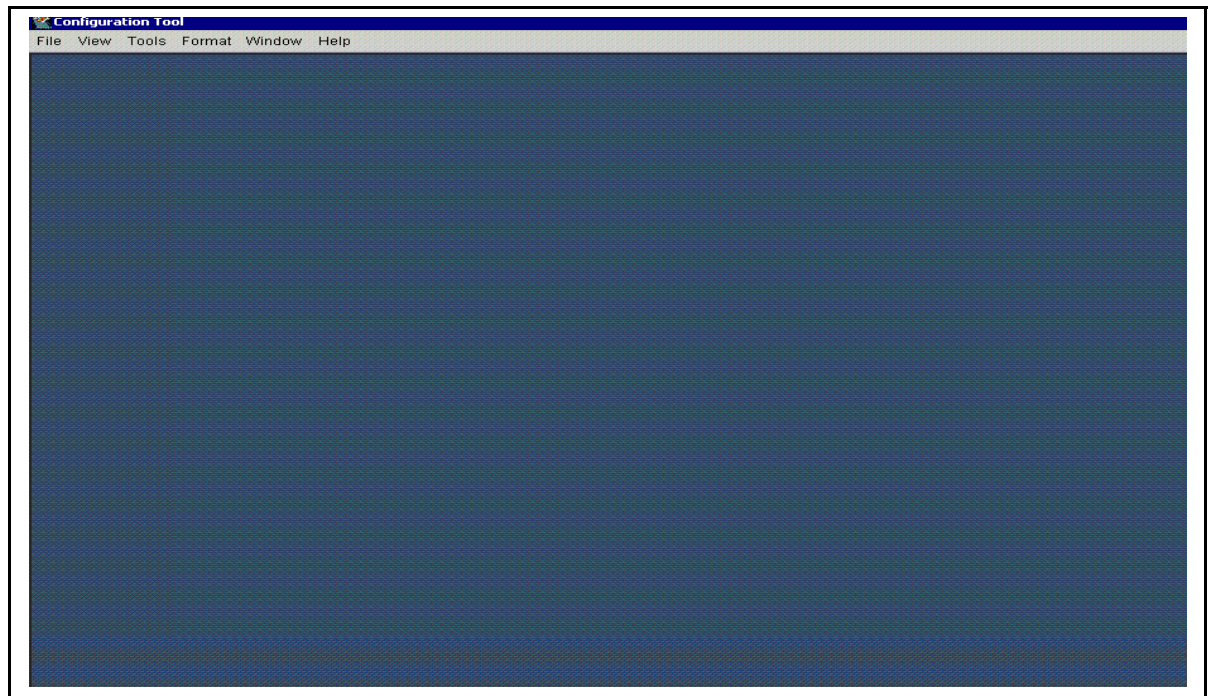


Figure 29 - Configuration Tool Main Menu

The **File** menu selection provides the capabilities described in the following table for the Smart Agent Configuration (storability.ini) and Proxy Configuration (proxyagent.conf) files.

Menu Selection	Description
Edit	Change the current configuration
Save	Save the configuration being edited
Exit	Close the Configuration Tool

Figure 30 - Configuration Tool File Menu

The **View** menu allows you to preview the actual configuration file you are creating or editing before you save it. The **Tools** pull-down menu allows you to start, stop, or restart a context-specific agent.

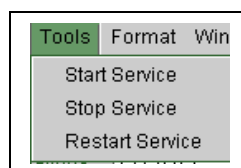
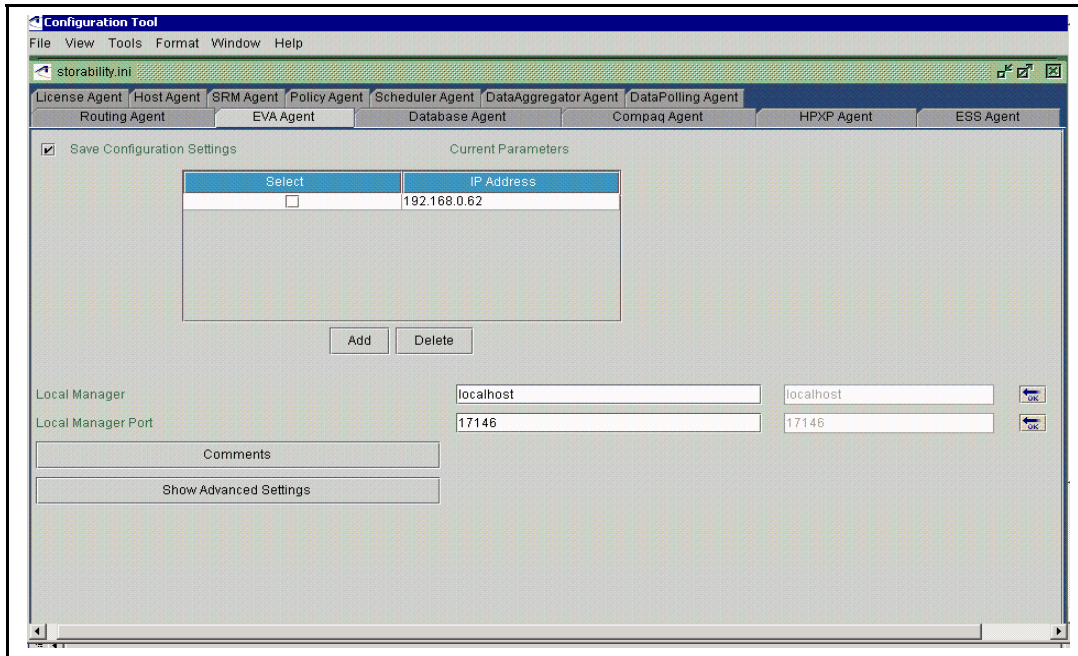


Figure 31 - Tools Menu in Configuration Tool

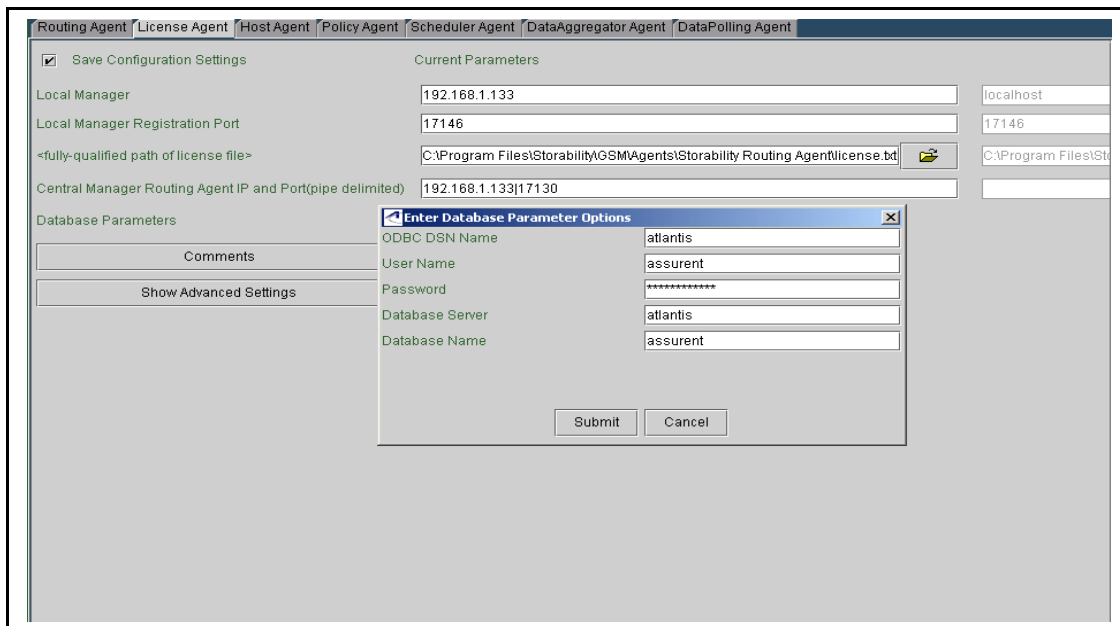
When you edit the Smart Agent configuration, the Configuration Tool provides a tab for each Smart Agent that is installed on the server. Clicking on an Agent tab opens the agent's configurable parameters in the main window and highlights that agent tab. The configuration tab for the Storability EVA agent is shown below.

You click the **Add** button to add agent-specific configuration settings. Conversely, you use the selection box to choose existing configuration details and click **Delete** to delete these settings out of the storability.ini file.



**Figure 32 - Smart Agent Tabs in Configuration Tool**

In some agent configuration windows, you click the **Add** button to add agent-specific configuration settings. In other agent configuration windows, you click the **Change Options** button to add agent-specific configuration settings, as shown below.



**Figure 33 - License Agent Configuration Window**

**Note:** In this configuration window, you must click **Submit** to have the default (or updated) configuration settings be written to the storability.ini file.

You use the selection box to choose existing configuration details and click **Delete** to delete these settings out of the storability.ini file.

Some general guidelines for using the Configuration Tool are briefly described as follows:

- Clicking an agent tab refreshes the window with that agent's configuration parameters and highlights the selected agent tab.

- Clicking the **Add** button allows you to add device-specific configuration parameters for some Smart Agents.
- Make sure the "Save Configuration Settings" is checked before you click **File->Save** to update your storability.ini file.
- Any password (e.g., Brocade admin user's password) is automatically encrypted before it is written to the storability.ini file. Clicking the **left arrow** icon copies a template file parameter to the respective configuration parameter's input box.
- If the variable is a directory path, you can click on the **Folder** icon to browse for a desired directory path.
- The **Comments** button allows you to add comments and click **Submit** to save them to the storability.ini file.
- Optionally click the **Show Advanced Settings** tab to view and/or modify these variables.
- It is recommended that you manually back up an existing configuration file to a different folder/name before you begin an editing session.

Restart a Smart Agent to have its configuration changes take effect.

## Auto Registration

Auto registration feature is a configuration option that allows agents to automatically register with a specified Local Manager for automatic activation of agent data collection. The following configuration parameters are used for auto registration:

- **Local Manager** – Identifies the IP address or DNS-resolvable host name of the Local Manager to be automatically contacted for the agent's auto registration
- **Local Manager Port** – Specifies the Local Manager port on which the Local Manager listens for auto registration requests. The default port number is 17146.
- **Enable Auto Registration** – Turns auto registration on (true) or off (false).

## Agent Upstream Messaging

The Central Manager agents will publish the **gsa\_message** object when the "Allow GSM Upstream Messaging" configuration parameter is set to "true". This published object is necessary to enable certain functionality of the Central Manager agents. With the exception of the Storability Routing Agent, this configuration parameter should be enabled (true) for other Central Manager agents, including the Scheduler Agent, Data Polling Agent, and Policy Agent.

## Configuring Agents on Central Manager Using the Configuration Tool

The Configuration Tool is used to configure the agents that you have installed on the Central Manager. These agents must be installed, configured, and running before you set up agent data collection using the Management Console's **Polling Schedule** menus.

**Note:** The "Save Configuration Settings" check box must contain a check mark before you choose **File->Save** to save an agent's configuration settings into the storability.ini file.

## Launch the Configuration Tool

1. Select **Start->Programs->Storability->Launch Configuration Tool** on the Central Manager to launch the Configuration Tool. The main window is displayed.

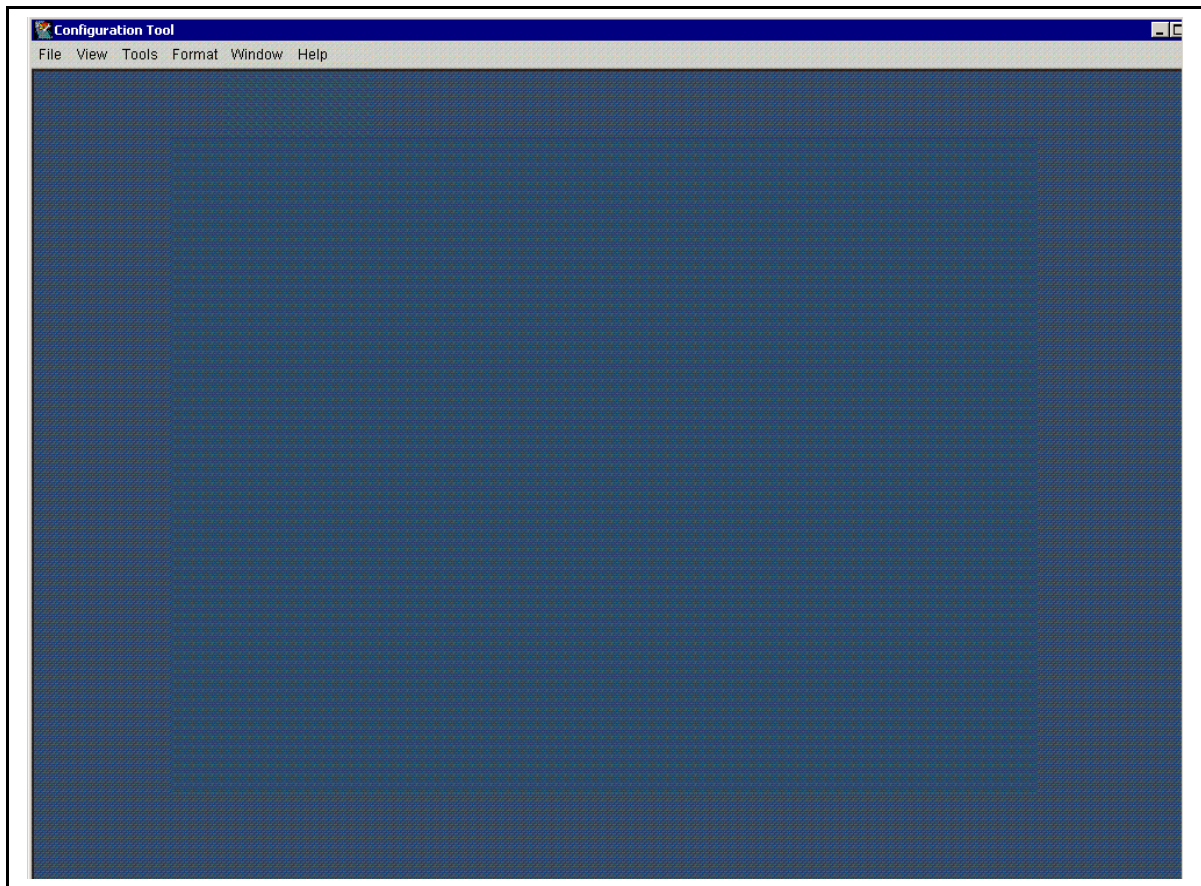


Figure 34 - Configuration Tool Main Window

### Configure Routing Agent

Each Central Manager (or Local Manager) runs a Routing Agent, whose primary responsibility is to perform agent data collection within the messaging infrastructure.

**Note:** Because the Central Manager runs the Routing Agent, it is by definition also a Local Manager. However, the Central Manager Routing Agent serves as the top-level Routing Agent in the messaging infrastructure.

Proceed as follows to configure this agent:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**.
3. Click the **Routing Agent** tab. The Routing Agent Configuration Window, with **Show Advanced Settings** turned on, is shown below.

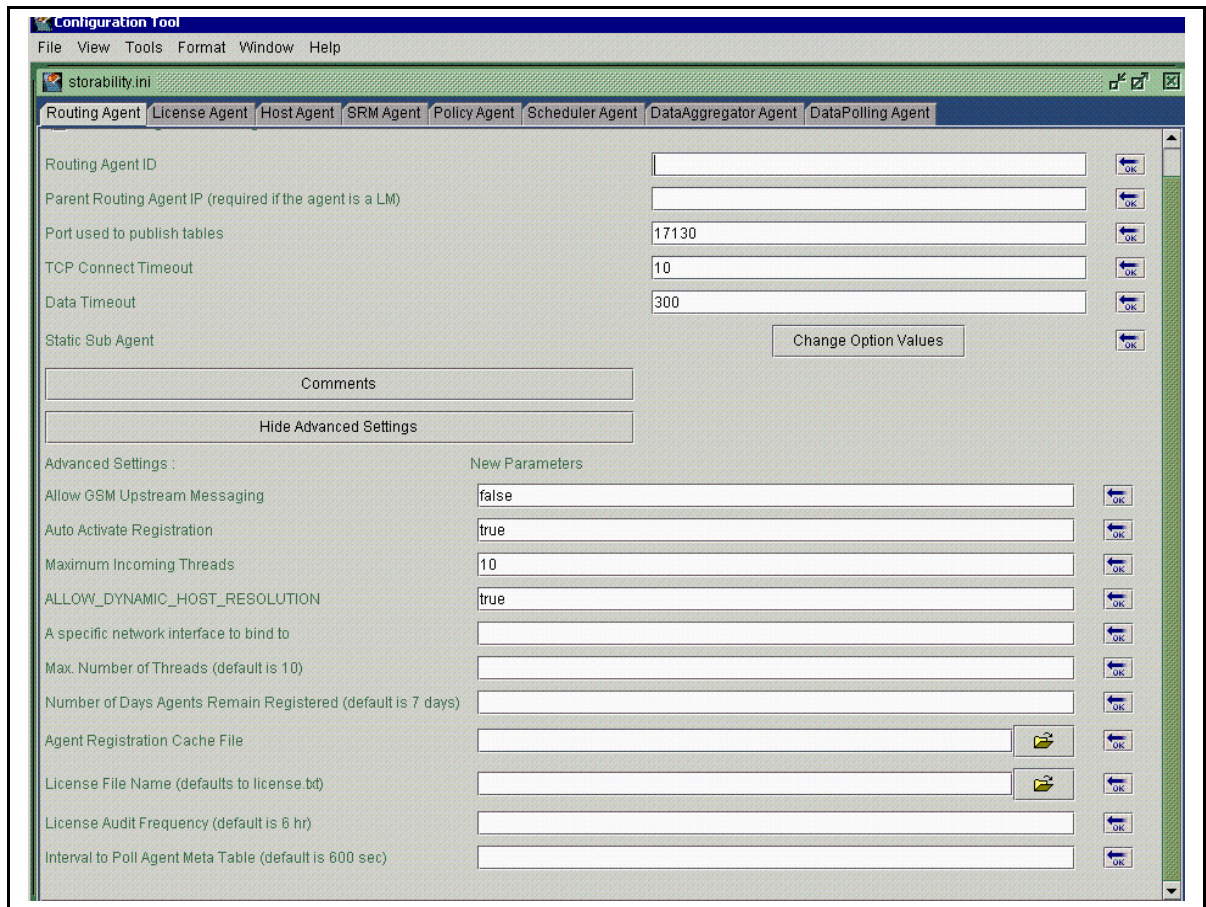


Figure 35 - Routing Agent Configuration Window

4. In the **Routing Agent ID** input box, enter the unique integer value to identify the Central Manager Routing Agent. The default Local Manager ID that the installation creates for the Default Local Manager is 300. Refer to the *Administration* chapter for additional information on **Site/Local Manager Administration** as well as the Default Local Manager and Default Site.  
**Notes:** If you leave the RID parameter field blank, a default RID of 1 is assigned when the Routing Agent is started. This RID will not match any Local Manager ID that is generated using the **Management Console's Site/Local Manager Administration** menus. This condition will cause collected agent data to be written to the Sun StorageTek Business Analytics database, but it will not appear in the Management Console application!
5. Leave the **Parent Routing Agent IP** input box empty (blank); this parameter only has meaning for Local Manager Routing Agents.
6. For the **Port used to publish tables** parameter, specify the TCP port on which the Central Manager publishes its objects. The default port number is 17130.
7. For **TCP Connect Timeout**, accept the default time interval (10 seconds) to connect to an agent, which should be fine for most TCP environments.
8. For **Data Timeout**, this parameter is generally ignored because the value is overridden by a system parameter passed to the Routing Agent by clients. The default value is 300 seconds.
9. If your Central Manager Routing Agent will collect agent data from agents that are not configured to use auto registration, proceed as follows:

- a. Click **Change Option Values** button next to the **Static Sub Agent** heading. The **Enter Static Sub Agent Registrations** dialog box appears.
- b. Type the port number and IP address pair or the port number and server name pair to define each SUB\_AGENT entry in the storability.ini file.
- c. Click **Submit** after you have completed all the static agent registrations.

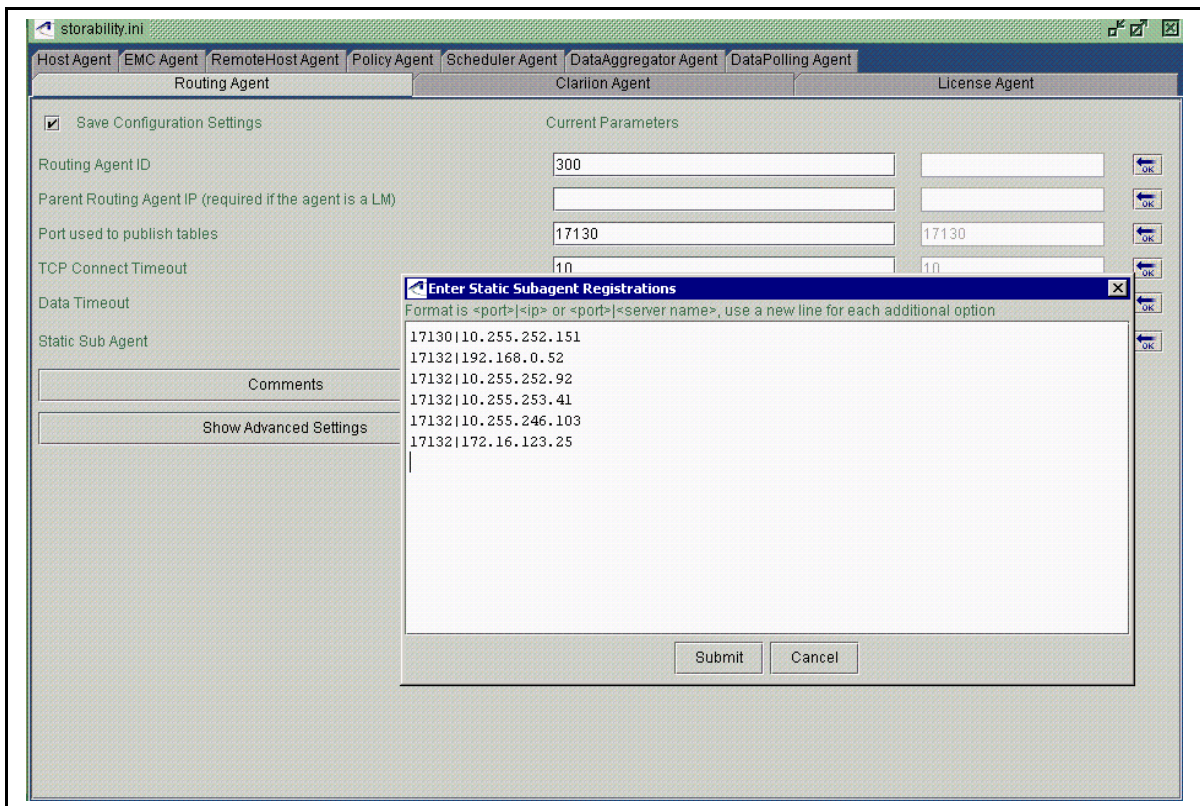


Figure 36 - Enter Static Subagent Registrations

10. Click **Show Advanced Settings** to review/modify the following configuration parameters: (Note: You do not have to make entries in this section unless you want to change from using the agent defaults.)
  - **Allow GSM Upstream Messaging** – Turns on (true) or off (false) having this agent publish the **gsa\_message** object. For the Routing Agent, this value should be turned off (false), which is the default value.
  - **Auto Activate Registration** – Allows the Central Manager by default to automatically activate incoming agent registrations.
  - **Specific Network Interface to Bind to** - The value may be an IP address, specified in standard Internet dot ("x.x.x.x ") notation, or a name service resolvable hostname. This option allows you to bind the Routing Agent to a specific network interface in a dual-homed computer, for example. If you do not bind the Routing Agent to a specific network interface, the Routing Agent will bind to all available local interfaces.
  - **Maximum Number of Incoming Threads** – Is used to control the limited pool of threads that handle the incoming connections for agent registrations. The Routing Agent receives registrations on port 17146. The default value is 10.
  - **ALLOW\_DYNAMIC\_HOST\_RESOLUTION** – Specifies whether dynamic host resolution can be performed using Dynamic Name Resolution (DNS). The default value is true. If host name resolution fails because the host has been removed

from DNS because of an administrative error, for example, the value can be set to false to avoid a valid partial data set from not being returned.

- **Max Number of Threads** – Sets the number of threads the agent will spawn. A rule of thumb is to set this value to one half the number of immediate sub-agents (number of rows in the Routing Agent's **gsa\_agent\_register** object, where rid = RID). This should be set no lower than five (5) and no higher than fifty (50). The default value is ten (10).
- **Number of Days Agents Remain Registered** - Specifies the maximum number of days an agent can be down and remain registered. Its purpose is to provide a simple mechanism for removing records of agents that are no longer installed. When expired, the sub-agent registration is removed. However, the agent can always re-register if it ever comes back online. If necessary, contact your support representative to obtain the
- **Agent Registration Cache File** – Is <drive>:\Program Files\Storability\Agents\Storability Routing Agent\ar.db.dat by default. The agent registration cache file (e.g., ar.db.dat) will be created after the Routing Agent has been started.
- **License File Name** – Use the **Folder** icon to specify the fully qualified name of the software license file; is <drive>:\Program Files\Storability\Agents\Storability Routing Agent\license.txt by default.
- **License Audit Frequency** – Specifies how often to perform license audit; default value is 6 hours. The maximum value is 46 hours.
- **Frequency to Poll Agent Meta Table** - Specifies how often in seconds to gather object schemas from sub agents.

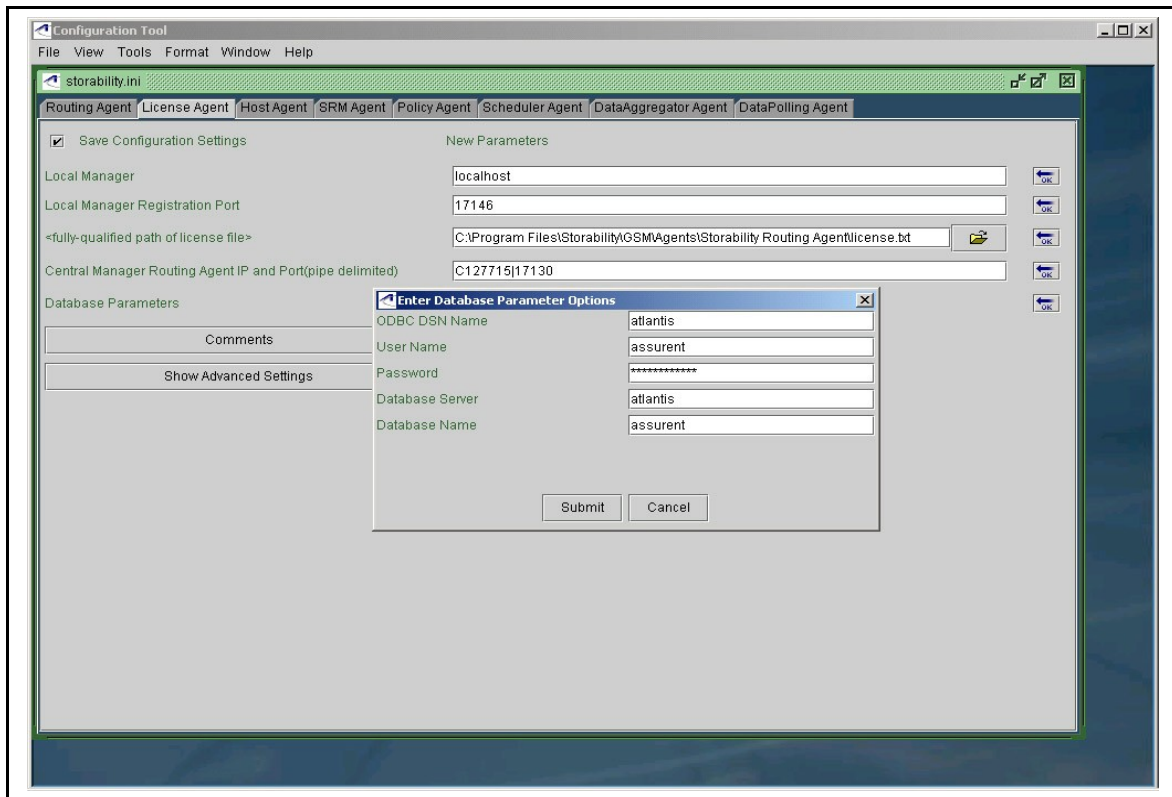
11. With the "Save Configuration Settings" check box enabled, select **File->Save** and confirm your changes to the storability.ini file.
12. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.

## Configure License Agent

The Central Manager License Agent supports the Management Console's **GSM License Report** accessed under the **Tools** menu.

Proceed as follows to configure this agent:

1. Click the **LicenseAgent** tab within the main configuration window.
2. For **Local Manager**, enter the network resolvable host name or IP address of the Local Manager to be contacted for agent auto registration. The default value is localhost.
3. For **Local Manager Registration Port**, specify the TCP port number the Local Manager uses for agent auto registration. The default port number is 17146.
4. To specify the fully qualified path for the license file, click the **Folder** icon. The fully qualified path is <drive>:\Program Files\Storability\Agents\Storability Routing Agent\license.txt by default.
5. In the **Central Manager IP and Port** input box, identify the Central Manager Routing Agent by IP address or host name and the port number on which it publishes its objects. The pipe delimiter must separate these configuration parameters. For example: 127.0.0.1| 17130.  
Click the **Change Option Values** button next to the **Database Settings** heading and the **Enter Database Parameters** Options dialog box appears.



**Figure 37 - License Manager Database Parameter Options**

**Note:** Although default ODBC settings are displayed, you must click **Submit** to have these settings saved to the storability.ini file.

6. Review the ODBC connection parameters that the License Agent will use to connect to the assured database. By default, the Storability License Agent uses the "atlantis" ODBC System Data Source (DSN) that may have been automatically created and verified during software installation.

**Notes:** Your Windows administrator can use the Windows ODBC Configuration menus to verify and test the "atlantis" ODBC System DSN or to set up a separate ODBC System DSN for use by the License Agent. The assured database user's default password is "st0rage".

7. Click **Show Advanced Settings** to review/modify the following configuration parameters:
  - **Enable Auto Registration** – Is used to turn auto registration on (true) or off (false).
  - **Collection Timeout** – Sets how long the License Agent waits to complete data collection; default value is 30 seconds.
  - **Frequency to collect config data** – Sets the frequency for collecting the software license-related configuration data; the default value is 3600 seconds (1 hour).
8. With the "Save Configuration Settings" check box enabled (check mark), select **File->Save** and confirm your changes to the storability.ini file.
9. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.

## Configure Data Aggregator Agent

The Data Aggregator requests agent data collection and is responsible for inserting collected agent data into the Sun StorageTek Business Analytics database. Proceed as follows to configure this agent:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**.
3. Click the **Data Aggregator** tab. The Data Aggregator Agent Configuration window, with Show Advanced Settings turned on, appears below.

The screenshot shows the 'Configuration Tool' window with the 'DataAggregator Agent' tab selected. The 'New Parameters' section contains the following fields and values:

Parameter	Value
Local Manager	localhost
Local Manager Registration Port	17146
ODBC DSN Name	atlantis
Database Server IP	127.0.0.1
Database Name	assurent
Database Login Name	assurent
Database Password	*****

The 'Advanced Settings' section contains the following fields and values:

Parameter	Value
Central Manager IP and Data Port	localhost:17130
Enable Auto Registration	true
Allow GSM Upstream Messaging	true
MIN_MEMORY_DATA_OBJECTS	

Figure 38 - Data Aggregator Configuration Window

4. For **Local Manager**, identify the Local Manager by IP address or host name that will be contacted for agent auto registration. The default value is the local host.
5. For **Local Manager Registration Port**, specify the Local Manager port used for agent auto registration. The default port number for agent auto registration is 17146.
6. In the **ODBC DSN Name** input box, identify the ODBC System Data Source Name the Aggregator will use to update the database. The default value is "atlantis".
7. In the **Database Server IP** input box, specify the IP address of the Central Manager database server.
8. The **Database Name** is "assurent" (default value).
9. The default **Database User** is "assurent".
10. Accept the default **Password** for the assurent database user.
11. Click **Show Advanced Settings** to review/modify:
  - **Central Manager IP and Data Port** – Specify the IP address of the Central Manager and its data port number. The Central Manager default data port number is 17130.
  - **Enable Auto Registration** – Turns auto registration on (true) or off (false) for this agent.

- **Allow GSM Upstream Messaging** – Turns on (true) or off (false) having this agent publish the **gsa\_message** object, used for communication between Storability agents on the Central Manager. This value must be true (enabled) for the Storability Data Aggregator.
- **MIN\_MEMORY\_DATA\_OBJECTS** - The Aggregator does not collect objects on an agent-by-agent basis by default. If a Sun Microsystems support representative requests the use of this Aggregator functionality, you configure the MIN\_MEMORY\_DATA\_OBJECTS setting in the Aggregator's section of the storability.ini file on the Central Manager.

To configure this setting, enter a comma-separated list of objects that should be handled on an agent-by-agent basis. You can optionally specify the special "all" or "All" value that will cause all objects to be collected on an agent-by-agent basis. Multiple MIN\_MEMORY\_DATA\_OBJECTS settings can be entered.

It should be noted that the MIN\_MEMORY\_DATA\_OBJECTS require full versioning to allow different versions of the same data object to be handled differently. An example follows.

```
.....
:aggregator.exe
# DataAggregator Agent -- start    (do not delete this line)
GSM_LM_HOST = localhost
GSM_LM_PORT = 17146
ODBC_DSN_0 = atlantis
.....
MIN_MEMORY_DATA_OBJECTS=gsa_backup_volume_info-2_2
```

In the above example, an incoming request for gsa\_backup\_volume\_info-2\_2 would collect in minimal memory mode any gsa\_backup\_volume\_info-2\_2 objects found. However, minimal memory mode will not be used to collect any gsa\_backup\_volume\_info-2\_1 or gsa\_backup\_volume\_info-2\_0 objects found.

12. With the "Save Configuration Settings" check box enabled, select **File->Save** and confirm saving your changes to the storability.ini file.
13. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.

## Configure Data Polling Agent

In conjunction with the Central Manager Scheduler Agent, the Data Polling Agent is used to control the scheduling of agent data collection and policy management. It is necessary to display the Polling Schedule menu from the Management Console's Tools menu.

Proceed as follows to configure this agent:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**. The Data Polling Agent Configuration window, with Show Advanced Settings turned on, appears below.

**Figure 39 - Data Polling Agent Configuration Window**

3. Click the **Data Polling Agent** tab.
4. For **Local Manager**, identify the Local Manager by IP address or host name to be contacted for agent auto registration. The default value is localhost.
5. For **Local Manager Registration Port**, identify the port number the Local Manager uses for agent auto registration. The default port number is 17146.
6. The **ODBC DSN Name** is *atlantis* by default.
7. The **Database Login Name** is *assurent*.
8. The **Database Password** field is *st0rage* and is displayed as asterisks in the Configuration Tool window. A password is encrypted before stored in the storability.ini file.
9. In the **Scheduler Timeout** field, specify how long the Data Polling Agent waits when communicating with the Scheduler Agent. The default timeout is 30 seconds.
10. Click **Show Advanced Settings** to review/modify the following parameters:
  - **Enable Auto Registration** – Turns agent auto registration on (default) or off.
  - **Data Polling Agent Password** – Is optional.
  - **Portal Database Name** – Is *portal*.
  - **Client Name** – Sets the agent's client name.
  - **Scheduler Agent Name** – Names the client.
  - **Scheduler Agent Password** – Optionally specifies the Scheduler Agent's password.
  - **Allow GSM Upstream Messaging** – Turns on (true) or off (false) having this agent publish the **gsa\_message** object, used for communication between Storability agents on the Central Manager. This value must be true (enabled) for the Storability Data Polling Agent.
14. With the "Save Configuration Settings" check box enabled, select **File->Save** and confirm your changes to the storability.ini file.

15. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.

## Configure Scheduler Agent

In conjunction with the Data Polling Agent, the Scheduler Agent is used to control the scheduling of agent data collection and execution of policy management. To configure the Central Manager Scheduler Agent, you must specify the IP address or network-resolvable host name of the database server.

Proceed as follows to configure this agent:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**.
3. Click the **Scheduler Agent** tab. The Scheduler Agent configuration window, with Show Advanced Settings turned on, appears below.

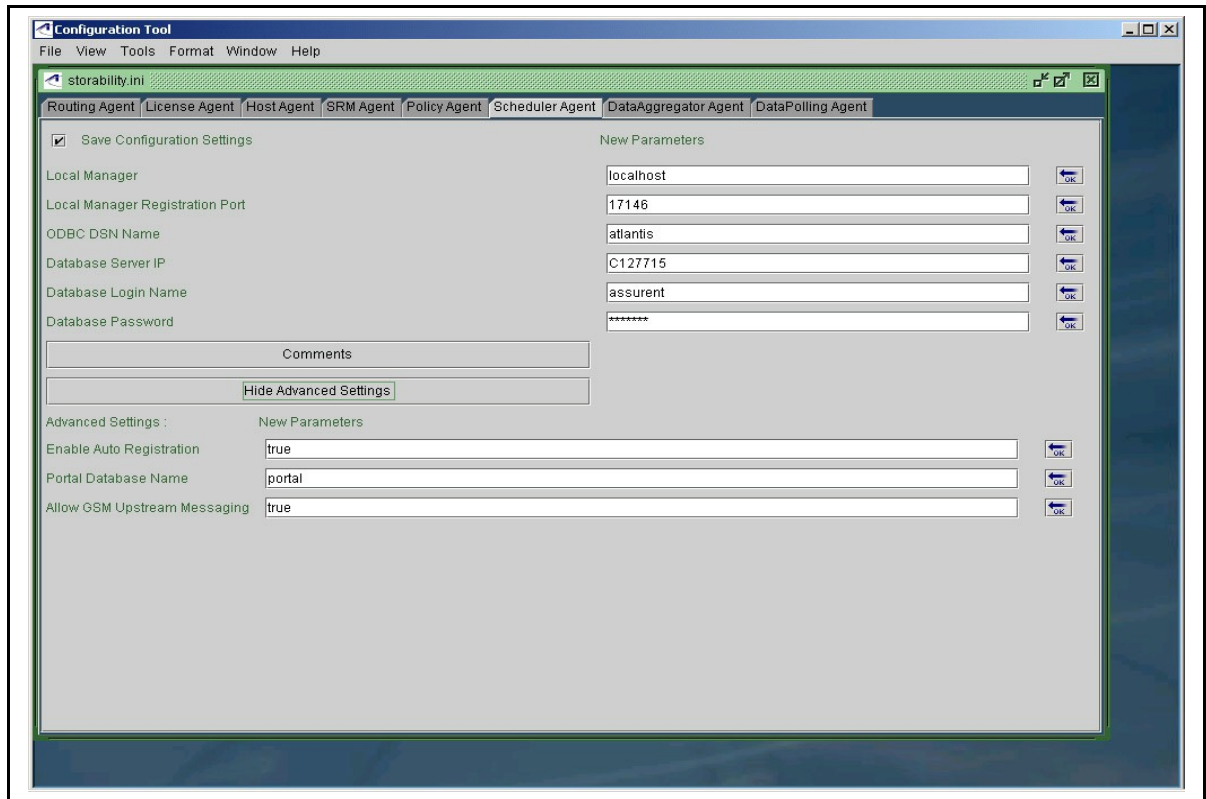


Figure 40 - Scheduler Agent Configuration Window

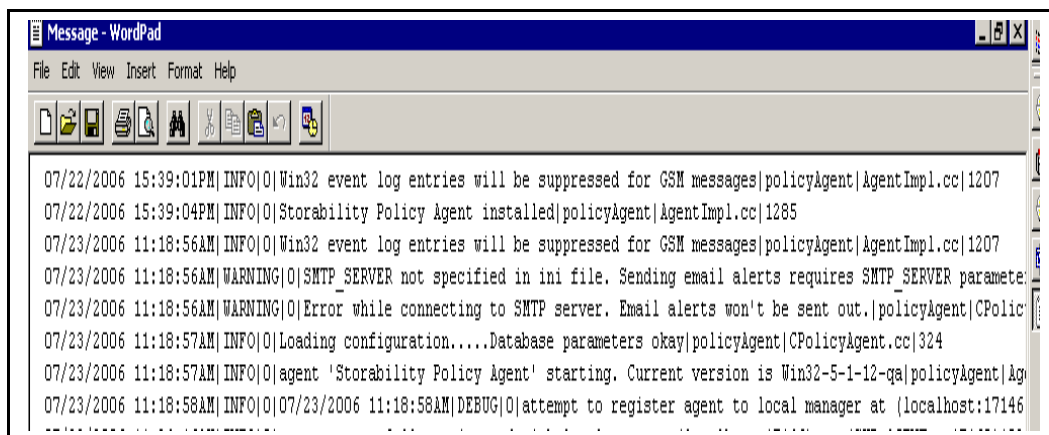
4. For **Local Manager**, identify the Local Manager by IP address or host name to be contacted for agent auto registration. The default value is localhost.
5. For **Local Manager Registration Port**, specify the port number that the Local Manager uses for agent auto registration. The default port number is 17146.
6. In the **ODBC DSN Name** input box, identify the ODBC System Data Source Name the Scheduler will use to access the database. The default value is *atlantis*.
7. In the **Database Server IP** input box, specify the IP address (or network resolvable host name) of the Central Manager database server.
8. The database name for polling schedules is "portal" (default value).
9. In the **Database Login Name** field, accept the default value of "assured".
10. Accept the default password for the assured database user in the **Database Password** field.
11. Click **Show Advanced Settings** to review/modify:
  - **Enable Auto Registration** – Turns agent auto registration on (default) or off.

- **Portal Database Name** – Is *portal*.
  - **Allow GSM Upstream Messaging** – Turns on (true) or off (false) having this agent publish the **gsa\_message** object, used for communication between Storability agents on the Central Manager. This value must be true (enabled) for the Storability Data Polling Agent.
12. With the "Save Configuration Settings" check box enabled, select **File->Save** and confirm your changes to the storability.ini file.
  13. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.

## Configure Policy Agent

The Policy Agent is responsible for executing the actions related to policy alerting. Besides specifying auto registration information and an ODBC System DSN to access the Sun StorageTek Business Analytics database, you will enter SMTP client configuration settings if the email functionality of Policy Alerting is to be used.

**Note:** The Policy Agent will start successfully if there is no valid SMTP Server specified in its section of the storability.ini file. This configuration is suited for customers who will use only the Database Batch Job (and no Policy Alerting) features that the Policy Agent supports. The Policy Agent will, however, log warning message entries in its message log, similar to the ones shown in Figure 41 – Policy Agent Warning Message Entries.



**Figure 41 - Policy Agent Warning Message Entries**

Policy alerting is configured using the Management Console's **Policy Alerting** menus; the database batch jobs are defined using the Management Console's **DB Batch Jobs** menus. These menu selections are accessed under the **Tools** menu options.

Proceed as follows to configure this agent:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**.
3. Click the **Policy Agent** tab. The Policy Agent configuration window, with Show Advanced Settings turned on, appears below.

storability.ini

Routing Agent License Agent Host Agent Policy Agent Scheduler Agent DataAggregator Agent DataPolling Agent

☐ Save Configuration Settings

New Parameters

Local Manager localhost OK

Local Manager Registration Port 17146 OK

Central Manager localhost OK

Central Manager Port 17130 OK

Email Address of Policy Alert Sender OK

SMTP Server IP OK

SMTP Server Port 25 OK

ODBC\_DSN atlantis OK

Database Server IP OK

Database User assurent OK

Database Password \*\*\*\*\* OK

Comments

Hide Advanced Settings

Advanced Settings : New Parameters

Enable Auto Registration true OK

Enable Upstream Messaging true OK

SMTP server login OK

SMTP server password OK

Scheduler Agent Password OK

**Figure 42 - Policy Agent Configuration Window**

4. For **Local Manager**, identify the Local Manager by IP address or host name to be contacted for agent auto registration. The default value is localhost.
5. For **Local Manager Registration Port**, specify the port number the Local Manager uses for agent auto registration. The default port is 17146.
6. For **Central Manager**, enter the Central Manager's network resolvable host name or IP address; default value is local host.
7. For **Central Manager Port**, identify the port on which the Central Manager's Routing Agent publishes its objects. The default port number is 17130.
8. In the **Email Address of Policy Alert Sender** input box, enter the email address that will be used to send emails containing policy execution results.
9. In the **SMTP Server IP** input box, specify the IP address of the SMTP Mail server used to send emails, if policy alerting is to be utilized.
10. In the **SMTP Server Port** input box, specify the SMTP server port used for sending emails. The default SMTP server port number is 25.
11. In the **ODBC DSN Name** input box, specify the ODBC System Data Source Name the Policy Agent will use to access the database. The default value is "atlantis".
12. In the **Database Server IP** input box, specify the IP address of the Central Manager database server.
13. The database name for polling schedules is "portal" (default value).
14. In the **Database Login Name** field, accept the default value of "assurent" as the database user ID.
15. Accept the default password for the assurent database user.
16. Click **Show Advanced Settings** to review/modify:
  - **Enable Auto Registration** – Turns auto registration on (true) or off (false). Auto registration is enabled (true) by default.
  - **Enable GSM Upstream Messaging** – Turns on (true) or off (false) having this agent publish the **gsa\_message** object, used for communication between Storability agents on the Central Manager. This setting must be set to true for the Storability Policy Agent.

- **SMTP server login** – Specify a valid SMTP server login if the SMTP server requires authentication.
- **SMTP server password** – Enter the SMTP user's password.
- **Scheduler password** – Encrypted Scheduler agent password (if applicable).
- **Portal Database Name** – Is "portal" by default.
- **Assurent Database Name** – Is "assurent" by default.

17. With the "Save Configuration Settings" check box enabled, select **File->Save** and confirm your changes to the storability.ini file.
18. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.

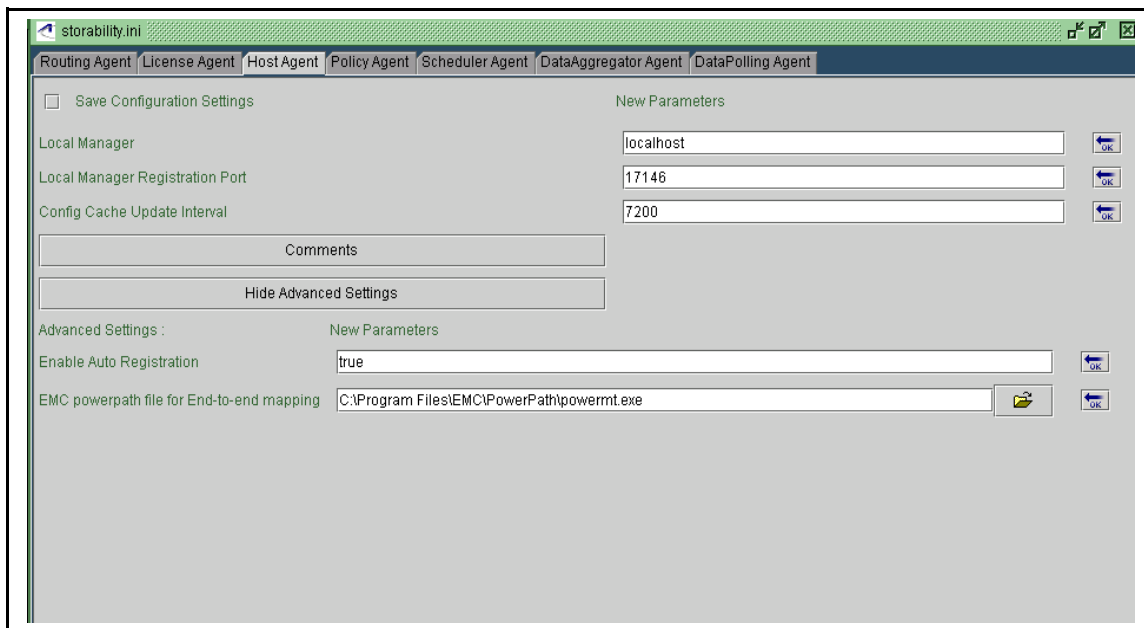
### Configure Host Agent

The Host Agent reports configuration information as well as file system, physical volume, and logical volume information for Windows, Solaris, IBM AIX, HP-UX, VMWare, and Linux platforms. The Host Agent is automatically started after it is installed.

If you change any configuration settings, such as the location of the EMC *powermt* program, restart the Host Agent to have the changes take effect.

Proceed as follows to configure this agent on the Sun StorageTek Business Analytics Central Manager:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**.
3. Click the **HostAgent** tab.



**Figure 43 - Host Agent Configuration Window**

4. In the **Local Manager** field, type the network resolvable host name or IP address of the Local Manager to be contacted for agent auto registration. The default value is "localhost". In this case, keep in mind that the Central Manager is also a Local Manager as it runs a Routing Agent.
5. In the **Local Registration Manager Port** input box, specify the port number that the Routing Agent uses for agent auto registration. The default port is 17146.

6. In the **Config Cache Update Interval** input box, review/modify how long the agent caches configuration data. The default value is 7200 seconds.
7. Click **Show Advanced Settings**.
8. Review/modify the **Enable Auto Registration** configuration setting that turns auto discovery on (true) or off (false). The default value of "true" will cause the agent to attempt to register with the Local Manager at start up. If registration fails, the agent will re-attempt registration every five minutes. If registration succeeds, the agent will "refresh" its registration every twenty-four (24) hours.
9. Review/modify the **EMC powerpath file for End to end mapping** setting. If the host server has EMC PowerPath software installed, use the **Browse** icon to locate and specify the location of the **powermt.exe** file.
10. With the "Save Configuration Settings" check box enabled (check mark), click **File->Save** and then confirm saving the storability.ini file.
11. Click **File->Exit** to close the Configuration Tool.
12. Use the Windows **Services** panel to restart the Host Agent if you have made any configuration changes.

## Configure SRM Agent

You may have selected to install the SRM Agent using the **Custom** Installation Type. The SRM Agent classifies files by type, size, owner, and access patterns.

Proceed as follows:

1. Launch the Configuration Tool.
2. Select **File->Edit->Smart Agent Configuration**.
3. Click the **SRM Agent** tab in the main configuration window.

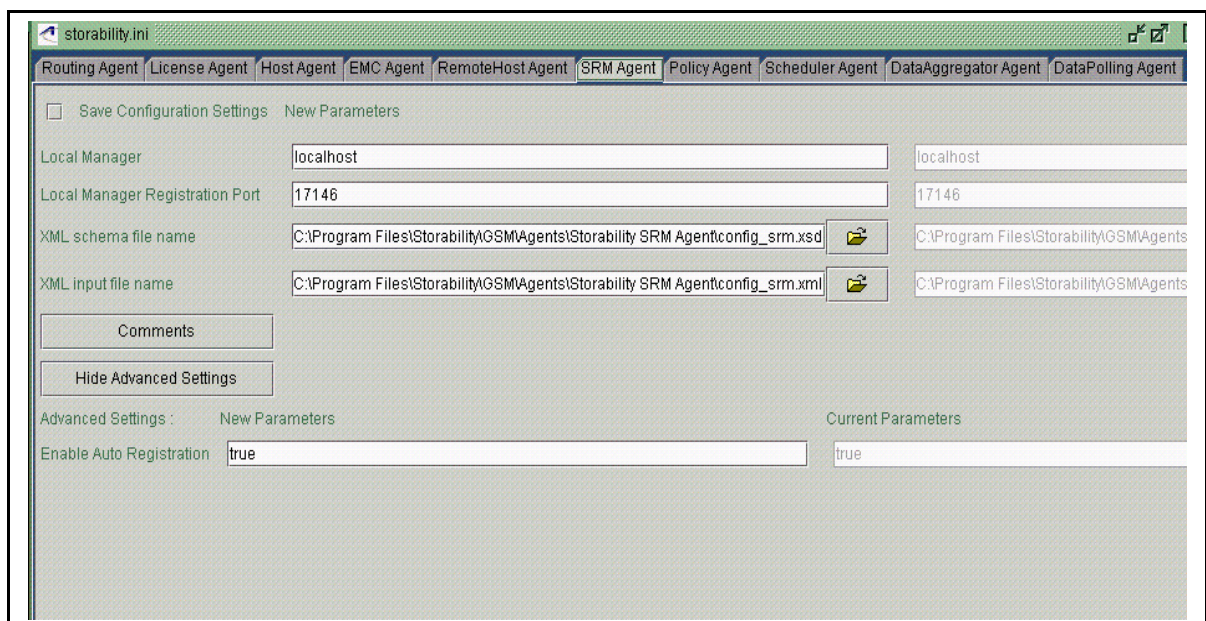


Figure 44 - SRM Agent Configuration Window

4. In the **Local Manager** field, specify the IP address or host name of the Local Manager to be contacted for agent auto registration. The default value is "localhost".

5. In the **Local Manager Registration Port** field, specify the TCP port number the Local Manager uses for agent auto registrations. The default port number is 17146.
6. For the **XML schema file name**, setting click the **Folder** icon and browse to the folder where the config\_srm.xsd file is installed. The default location is c:\Program Files\Storability\Agents\Storability SRM Agent.
7. Select the file and click **Open**.
8. For the **XML input file name** setting, the **Folder** icon and browse to the folder where the config\_srm.xml file is installed. The default location is c:\Program Files\Storability\Agents\Storability SRM Agent.
9. Select the file and click **Open**.
10. Click **Advanced Settings** to review/modify the "Enable Auto Registration" configuration setting, which turns agent auto registration on or off. Unless you want to disable agent auto registration (false), accept the default setting of true.
11. With the "Save Configuration Settings" check box enabled (check mark), click **File->Save** and then confirm saving the storability.ini file.
12. Select **File->Exit** to close the Configuration Tool.

If you installed the optional SNMP Proxy Agent, refer to the subsequent "Installing SNMP Proxy Agent on Windows" section to obtain instructions on configuring and verifying this agent. The *Remote Host Agent Installation Guide* provides instructions on configuring and verifying this agent.

## Remote Share Configuration Tool for SRM Agent

The following sections describe the Remote Share Configuration Tool (RSCT). The RSCT makes it easier for you to maintain entries in the SRM agent's configuration file, config\_srm.xml, that control the optional scanning of remote file systems by the SRM Agent.

The RSCT supports the following basic functions that will be subsequently described in more detail:

- Add
- Validate
- Delete
- Change Credentials

## Installation Requirements

The RSCT tool must run on a Windows Central Manager equipped with the cm-get utility. In addition, Perl version 5.6.1 must be installed and available in the PATH environment variable.

## Communications

The RSCT does not communicate directly with a NAS agent. It is designed to communicate with a Central Manager Routing Agent (CMRA, which in turn communicates with all the necessary NAS agent(s) installed in the environment. Using the RSCT Command Line Interface (CLI), you specify the IP address to communicate with:

- The Central Manager Routing Agent (CMRA)
- NAS Agent(s) on that server

RSCT supports two Business Analytics NAS Agents, which are the NetApp Agent and the EMC Celera Agent. RSCT expects share names to contain an IP address only; node name (host name) in the share path is not supported. This restriction results from a limitation in the way different NAS Agents report share data.

## Required cm-get Utility

The RSCT uses the 'cm-get' utility to perform agent-to-agent communication while retrieving up-to-date share information. To work correctly, the cm-get utility must be located in the directory in which the RSCT tool is run. The installation of the Central Manager creates the <drive>:\Program Files\Storability\GSM\Utilities\Storability Central Manager Utilities folder where the cm-get utility (cm-get.exe) is installed.

Refer to the subsequent Central Manager cm-get Utility section of this chapter to obtain additional information on the use of the cm-get utility.

## Updating the config\_srm.xml File

RSCT assumes it can access the config\_srm.xml file. For certain commands (e.g., Add, RSCT updates the section of the config\_srm.xml file between the <remote\_filesystems> and </remote\_filesystems> tags in the file. The tool assumes that no multi-line comments exist between these tags. If so, the RSCT will not maintain these multi-line comments and the state of the file is undefined.

The SRM Agent Configuration File, named config\_srm.xml, adheres to the schema defined in the config\_srm.xsd document. This document is not required or supplied with the RSCT; RSCT works as an independent tool.

The remote share information is encapsulated in XML tags in the following format:

```
<remote_filesystems>
  <filesystem_def>
    <share_name>\\server1\share1</share_name>
    <auth_username>username</auth_username>
    <auth_password>password</auth_password>
  </filesystem_def>
  <filesystem_def>
    <share_name>\\server1\share2</share_name>
    <auth_username>username</auth_username>
    <auth_password>password</auth_password>
  </filesystem_def>
  <filesystem_def>
    <share_name>\\server2\share1</share_name>
    <auth_username>username</auth_username>
    <auth_password>password</auth_password>
  </filesystem_def>
</remote_filesystems>
```

Where:

- server# is typically the NAS system IP.
- share# is the share exposed on the server that is scanned by the SRM Agent.
- username and password indicate the credentials required to authenticate with the server. Be aware that the password must be encrypted in the config\_srm.xml file to support remote file system scanning by the SRM Agent.
- Each matching <remote\_filesystems>, </remote\_filesystems> tag pair represents all NAS filesystems that are scanned by the SRM Agent. It contains the necessary information to connect to the various NAS systems and initiate the remote share scan.
- Each matching <filesystem\_def>, </filesystem\_def> tag pair represents a single share in a single NAS filesystem. The <filesystem\_def> tag is part of the <remote\_filesystems> tag.

## The ~config\_srm.xml file

In conjunction with some commands, RSCT will create a ~config\_srm.xml file. This backup file is created whenever the commands Add, Delete and Change Credentials are run. The file contains the original contents of the config\_srm.xml file before it is

modified. As a result, it will have the same format (described above) as the config\_srm.xml file.

The default name for the backup file is the output file name with a "~" prep-ended to it. In other words, the original config\_srm.xml file is saved as "~config\_srm.xml". However, if a "-o" flag is specified when one of the above commands is run, the contents of the output file name, which is specified after the flag, will be backed up.

**Note:** This file is not cleaned up automatically. It is overwritten every time the command is run with a given .xml file specified as input.

### The "NLSV" File

An NLSV file can be created in either of the following ways:

- By redirecting the output of the Validate command to a user-defined file or:
- By creating the file manually and having each line of the file represent one share.

Any NLSV file can be used as the input file for the Validate/Change Credentials/ Delete commands when used with the -f option.

- **Change Credentials** - When the NLSV file is used as the input file for the Change Credentials command, all shares that are listed in the NLSV file are matched against the shares in the config\_srm.xml file. Depending upon the match criteria, the credentials for such matching shares are updated with the new credentials. If the command is used with the -o option, the changes will be saved to a new user defined file, and the config\_srm.xml file will remain unchanged.
- **Delete** - When the NLSV file is used as input file for the Delete command, all shares listed in the NLSV file are matched against the shares in the config\_srm.xml file. The shares, which match the criteria, are deleted from the config\_srm.xml file. If the command is used with the -o option, the changes will be saved to a new user defined file, and the config\_srm.xml file will remain unchanged.
- **Validate** - In conjunction with the Validate command, you can either use the config\_srm.xml or a NLSV file (using the -f option) as the input file. In either case, RSCT will again redirect/pipe the output to a new NLSV file.

### Relationship between the Intermediate Files

The config\_srm.xml contains information about (apart from other things) the shares on a NAS system that are configured to be scanned by the SRM Agent. These shares are identified under the <remote\_filesystems> tab and each share is represented by a <filesystem\_def> tag.

Each <filesystem\_def> tag contains the following information about the share:

- Node name of the NAS system.
- Share name
- Authentication parameters (username and encrypted password) to access that particular share on the NAS system.

The information is present in XML format as shown below:

```
<remote_filesystems>
<filesystem_def>
    <share_name>\\server1\share1</share_name>
    <auth_userName>username</auth_userName>
    <auth_password>password</auth_password>
</filesystem_def>
<filesystem_def>
    <share_name>\\server1\share2</share_name>
```

```

        <auth_userName>username</auth_userName>
        <auth_password>password</auth_password>
    </filesystem_def>
    <filesystem_def>
        <share_name>\\server2\share1</share_name>
        <auth_userName>username</auth_userName>
        <auth_password>password</auth_password>
    </filesystem_def>
</remote_filesystems>

```

Here 'server1' is the node name of the NAS system and 'share1' is the share name for the share on that system that is to be scanned. The 'username' and 'password' are the authentication parameters to access that particular share. Similarly, 'server2' would correspond to a node name of another NAS system.

For each share on a NAS system that is configured for scanning, there would be one corresponding entry of <filesystem\_def> tag, as shown above.

The NLSV file contains the information about the IP of the NAS system and the shares exposed by that NAS system, such as:

```

server1\share1
server1\share2
server2\share1
server2\share2

```

Again, 'server1' is the node name of the NAS system and 'share1' is the share name for the share on that system that is to be scanned. Similarly, 'server2' would correspond to the node name of another NAS system.

Each line represents a combination of IP of the NAS system and the shares exposed for scanning. Authentication parameters for that share are not stored in the NLSV file.

An NLSV file can be created by redirecting the output of Validate command to a user-defined file. This is similar to redirecting (piping) output of any command that is run on a command prompt. The NLSV file may also be created manually, by having each line of the file represent one share as shown in the above example. Any NLSV file created as described can also be used as an input file (for Validate/Change Credentials/ Delete commands) when used with the optional -f option.

### Functional Description – Add (alias: ad)

The Add command adds to the config\_srm.xml file any shares that are exposed by the specified NAS Agent and that are not already present in the config\_srm.xml file. If the shares exposed by the NAS agent are already present in the config\_srm.xml file, RSCT will check if the existing credential information is different to the newly collected information. If so, RSCT will update the shares with this new credential information.

To retrieve the list of shares, RSCT communicates with the NAS Agent(s) via a Central Manager Routing Agent. This list is compared with the shares present in the config\_srm.xml file. In addition, the two lists are merged and all duplicate entries (shares with the same credentials) are discarded.

The share entries in the config\_srm.xml file are added or updated but are never removed and, therefore, the name "Add".

### Format(s)

1. `perl srmcfg.pl add <config_srm.xml> <Routing agent IP> <NAS agent IP> [-o <Output.xml>] <auth_user> <auth_pass>`

where:

- `config_srm.xml` - Input XML file containing the SRM Agent configuration parameters.
- Routing agent IP - IP address of the server on which the Central Manager Routing agent is running.
- NAS Agent IP - IP address of the server on which the NAS agent is running.
- `Output.xml` - The optional `Output.xml` file will contain the shares already present in the existing `config_srm.xml` file plus the additional new shares that were added as a result of executing the Add command.
- `auth_user` - Username credential to be applied to all shares exposed by a NAS Agent.
- `auth_pass` - Encrypted password credential to be applied to all shares exposed by a single NAS Agent. By encrypting the password using `inicypt`, you provide a valid password when the remote share configuration is used by the SRM. As shown in the examples, however, RSCT will accept a plain text password.

### Example(s)

1. `perl srmcfg.pl add config_srm.xml 192.168.200.100 192.168.200.200 Nancy Drew123`

This example represent the use case where:

- The list of shares reported by the NAS agent(s) at the location 192.168.200.200 is retrieved. RSCT communicates with the NAS Agent through the CMRA running on the 192.168.200.100 server.
- RSCT attempts to add all shares exposed by the NAS Agent(s), running on the 192.168.200.200 server, to the `config_srm.xml` file.
- All shares already present in the `config_srm.xml` file are compared with the newly obtained credential information to ensure that they have the most up to date credentials.
- Any share that does not match the credentials, "Nancy/Drew123 ", will be updated with this new information.
- Shares that are not exposed by the NAS Agent, running on 192.168.200.200 server, will not be changed in the file.
- Since the optional parameter (`-o <Output.xml>`) has not been supplied, the input file `config_srm.xml` will be backed up to `~ config_srm.xml` before any modifications occur.

2. `perl srmcfg.pl add config_srm.xml 192.168.200.100 192.168.200.200 -o Output.xml Nancy Drew123`

This example represent the use case where:

- The list of shares reported by the NAS agent, located at 192.168.200.200, is retrieved. RSCT communicates with this NAS Agent through the routing agent located at 192.168.200.100.
- RSCT attempts to add all shares exposed by the NAS Agent running on 192.168.200.200 to the `config_srm.xml` file.
- All shares already present in the `config_srm.xml` file are compared with the newly obtained credential information to ensure that they have the most up to date

credentials. Any share that does not match the credentials, "Nancy/Drew123 ", will be updated with this new information.

- Shares that are not exposed by the NAS Agent, running on 192.168.200.200, will not be affected.
- Since the optional parameter (-o Output.xml) has been supplied, the input file config\_srm.xml will be backed up to the file, named Output.xml, before any modifications occur.

### Validate (alias va)

The Validate function validates the contents of a config\_srm.xml file or an NLSV file against a NAS Agent. Specifically, this function validates that the shares currently specified in the config\_srm.xml file are still valid. The validation is performed by verifying that the NAS Agent still reports on these shares.

The output from the Validate command can be in treated in two ways:

- If no output file is specified, the command prints a list of shares in *servername\sharename* format on the screen.
- If a NLSV file is specified, the list will be "piped" to the specified output file and, thereby, create a NLSV file.

RSCT communicates with the specified NAS Agent via a Central Manager Routing Agent. It reads the shares in the input file, compares them to those retrieved from the NAS agent, and prints the share names not found in the list retrieved from the NAS Agent on the screen.

The config\_srm.xml file is not modified by this operation. If there are multiple NAS agents, the Validate command needs to be run against all of them iteratively to get the final list of invalid shares. In this case, a resulting NLSV file will become the input to all "Validate" commands that occur after the first Validate command has completed.

This process can be explained using the following scenario:

Since RSCT does not know which NAS Agent actually reports on which shares, it uses a process of elimination when shares are validated. Assume that there are three NAS Agents. In this scenario, it is necessary to validate the contents of the config\_srm.xml file against all three NAS Agents - one by one - to correctly determine all the invalid share entries.

This process should be done in a recursive manner. For example:

1. The config\_srm.xml file is used as the input to the Validate command run against NAS Agent #1. The output may be piped to an output file, called "file1.NLSV".
2. The "file1.NLSV" file will be the input to the Validate command run against NAS Agent #2. The output may be piped to an output file, called "file2.NLSV".
3. The "file2.NLSV" file will be the input to the Validate command run against NAS Agent #3. The output may be piped to an output file, called "file3.NLSV".
4. The resulting "file3.NLSV" file will contain all shares that RSCT was unable to validate. These are our invalid shares.

Whenever there is only one NAS agent in the environment and the config\_srm.xml file contains the share information for a single NAS system, the Validate command needs to be run only once.

### Format(s)

1. `perl srmcfg.pl va <config_srm.xml> <Routing Agent IP> <NAS Agent IP>`
2. `perl srmcfg.pl va -f <NLSV file> <Routing Agent IP> <NAS Agent IP>`

where:

- config\_srm.xml - Input XML file containing the SRM Agent configuration parameters to be validated against the NAS system on <NAS Agent IP>.
- NLSV file - Input file containing new-line separated value list of remote shares to be validated against the NAS system on <NAS Agent IP>.
- Routing agent IP - IP Address of the server on which the Central Manager Routing Agent is running.
- NAS Agent IP - IP Address of the server on which the NAS agent is running.

### Example(s)

```
1. perl srmcfg.pl validate config_srm.xml 192.168.200.100
   192.168.200.200
```

This example represent the use case where:

- The list of shares reported by the NAS agent, running on the 192.168.200.200 server, is retrieved. RSCT communicates with this NAS Agent through the Central Manager Routing Agent that is running on the 192.168.200.100 server.
- RSCT attempts to validate all shares exposed by the NAS Agent, running on 192.168.200.200 server, against the contents of the config\_srm.xml file.
- Since the output of this command is NOT piped to a NLSV file, any share that could not be matched with the output of the NAS agent will be written to the screen.
- Shares present in the config\_srm.xml file but not exposed by the NAS Agent, running on 192.168.200.200 server, will be printed to the screen.
- Shares present in the config\_srm.xml file that are also exposed by the NAS Agent, running on the 192.168.200.200 server, will not be printed to the screen.
- Shares not present in the config\_srm.xml file but exposed by the NAS Agent, running on the 192.168.200.200 server, will not be printed to the screen.

**Note:** Errors, if any, are written to the screen

```
2. perl srmcfg.pl validate config_srm.xml 192.168.200.100 192.168.200.200
   > NLSVfile.txt
```

This example represent the use case where:

- The list of shares reported by the NAS agent, located at 192.168.200.200, is retrieved. We communicate with this NAS Agent through the CMRA that is running on the 192.168.200.100 server.
- We attempt to validate all shares exposed by the NAS Agent, running on 192.168.200.200 server, against the contents of the config\_srm.xml file.
- Since the output of this command is piped to a NLSV file, any share that could not be matched with the output of the NAS agent will be written to this file.
- Shares present in the config\_srm.xml file but are not exposed by the NAS Agent, running on the 192.168.200.200 server, will be written to NLSVfile.txt.
- Shares present in the config\_srm.xml file, which are also exposed by the NAS Agent running on the 192.168.200.200 server, will not be written to NLSVfile.txt.
- Shares not present in the config\_srm.xml file but are exposed by the NAS Agent, running on the 192.168.200.200 server, will not be written to NLSVfile.txt.

**Note:** Errors, if any, are written to the NLSVfile.txt file.

```
3. perl srmcfg.pl validate config_srm.xml 192.168.200.100 192.168.200.200
   >> NLSVfile.txt
```

This example represent the use case where:

- The list of shares reported by the NAS agent, located at 192.168.200.200, is retrieved. We communicate with this NAS Agent through the CMRA, which is located at 192.168.200.100.
- We attempt to validate all shares exposed by the NAS Agent, running on 192.168.200.200, against the contents of the config\_srm.xml file.
- Since the output of this command is appended to a NLSV file, any share that could not be matched up with the output of the NAS agent will be appended to this file. We are assuming the NLSV file already exists. In other words, a previous "Validate" command has already occurred.
- Shares present in the config\_srm.xml file but are not exposed by the NAS Agent, running on 192.168.200.200, will be appended to NLSVfile.txt.
- Shares present in the config\_srm.xml file, which are also exposed by the NAS Agent running on 192.168.200.200, will not be appended to NLSVfile.txt.
- Shares not present in the config\_srm.xml file but are exposed by the NAS Agent, which is running on 192.168.200.200, will not be appended to NLSVfile.txt.

**Note:** Errors, if any, are appended to the NLSVfile.txt file.

4. `perl srmcfg.pl validate -f NLSV_file.txt 192.168.200.100 192.168.200.200`

This example represents the use case where:

- RSCT is validating the shares exposed by the NAS agent, which is running on the 192.168.200.200 server, with the contents of NLSV\_file.txt. The file, named NLSV\_file.txt, is the output from the execution of a previous Validate command. The results will be printed to the screen.
- The list of shares, which are reported by the NAS agent running on the 192.168.200.200 server, is retrieved. RSCT communicates with this NAS Agent through the CMRA that is running on the 192.168.200.100 server.
- RSCT attempts to validate all shares exposed by the NAS Agent, which is running on the 192.168.200.200 server, against the contents of NLSV\_file.txt.
- Since the output of this command is NOT piped to a NLSV file, any share that could not be matched against the output of the NAS agent will be printed to the screen.
- Shares present in the NLSV\_file.txt file but are not exposed by the NAS Agent, running on the 192.168.200.200 server, will be printed to the screen.
- Shares present in the NLSV\_file.txt file, which are exposed by the NAS agent running on the 192.168.200.200 server, will not be printed to the screen.
- Shares not present in the NLSV\_file.txt file but are exposed by the NAS Agent, running on the 192.168.200.200 server, will not be printed to the screen.

```
5. perl srmcfg.pl validate config_srm.xml 192.168.200.100 192.168.200.200
   > NLSVfile.txt

perl srmcfg.pl validate -f NLSVfile.txt 192.168.200.100 192.168.200.201
   > NLSVfile2.txt

perl srmcfg.pl validate -f NLSVfile2.txt 192.168.200.100
192.168.200.202 > NLSVfile3.txt
```

This example represents the use case where you use RSCT to validate the shares exposed by multiple NAS agents located at 192.168.200.200/2001/2002. As described above, this an iterative process.

- a. In the first Perl statement, note that:
  - The list of shares reported by the NAS agent, running on 192.168.200.200, is retrieved. RSCT communicates with this NAS Agent through the CMRA, running on 192.168.200.100.

- RSCT attempts to validate all shares exposed by the NAS agent, running on 192.168.200.200, against the contents of the config\_srm.xml file.
  - Since the output of this command is piped to a NLSV file, any share that could not be matched against the output of the NAS agent will be printed to the NLSVfile.txt file.
  - Shares present in the config\_srm.xml file but are not exposed by the NAS Agent, running on 192.168.200.200, will be printed in NLSVfile.txt.
  - Shares present in the config\_srm.xml file that are also exposed by NAS Agent, running on 192.168.200.200, will not be printed in NLSVfile.txt.
  - Shares not present in the config\_srm.xml file but are exposed by the NAS Agent, running on 192.168.200.200, will not be printed in NLSVfile.txt
- b. In the second Perl statement:
- The list of shares reported by the NAS agent, running on 192.168.200.201, is retrieved. RSCT communicates with this NAS Agent through the CMRA that is running on 192.168.200.100.
  - RSCT attempts to validate all shares exposed by the NAS agent, running on 192.168.200.201, against the contents of the NLSVfile.txt file. This is the output file created by the first Perl statement.
  - Since the output of this command is piped to a NLSV file, any share that could not be matched against the output of the NAS agent will be printed to the NLSVfile2.txt file.
  - Shares present in the NLSVfile.txt file but are not exposed by NAS Agent, running on 192.168.200.201, will be written to the NLSVfile2.txt.
  - Shares present in the NLSVfile.txt file that are also exposed by NAS Agent, running on 192.168.200.201, will not be written to the NLSVfile2.txt.
  - Shares not present in the NLSVfile.txt file but are exposed by NAS Agent running on 192.168.200.201 will not be written on NLSVfile2.txt
- c. In the third Perl statement, note that:
- The list of shares reported by the NAS agent, running on 192.168.200.202, is retrieved. RSCT communicates with this NAS Agent through the Central Manager Routing Agent that is running on 192.168.200.100.
  - RSCT attempts to validate all shares exposed by the NAS Agent, running on 192.168.200.202, against the contents of the NLSVfile2.txt file. This is the output file from the first Perl statement.
  - Since the output of this command is "piped" to a NLSV file, any share that could not be matched against the output of the NAS agent will be printed to this NLSVfile3.txt file.
  - Shares present in the NLSVfile2.txt file but are not exposed by the NAS Agent, running on 192.168.200.202, will be written on NLSVfile3.txt.
  - Shares present in the NLSVfile2.txt file that are also exposed by the NAS Agent, running on 192.168.200.202, will not be written to the NLSVfile3.txt.
  - Shares not present in the NLSVfile2.txt file but are exposed by the NAS Agent, running on 192.168.200.202, will not be written to the NLSVfile3.txt file.

The end result is that NLSVfile3.txt will contain a subset of all shares present in the config\_srm.xml file that are not exposed by any of the NAS agents running on IP 192.168.200.200, 192.168.200.201 and 192.168.200.202. These are the **invalid** shares.

### Delete (alias de)

The Delete command will delete all shares that match a specified criterion from the SRM configuration file. This command supports changes at the NAS Agent level. In other words, RSCT can specify a criterion where by all shares that a single NAS agent exposes

and that match the criterion will be deleted. The size of the config\_srm.xml file generally shrinks at the end of a successful execution of the Delete command.

### Format(s)

1. `perl srmcfg.pl de <config_srm.xml> -f <NLSV File> [-a <Routing agent IP> <NAS agent IP>] [-o <Output.xml>]`
2. `perl srmcfg.pl de <config_srm.xml> -u <find_auth_user> [-o <Output.xml>]`

Where:

- config\_srm.xml - Input XML file containing the SRM Agent configuration parameters.
- NLSV File - Input file containing new-line separated value list of remote shares to be deleted if found in the <config\_srm.xml> file.
- Routing agent IP - IP of the server on which the Central Manager Routing Agent is running.
- NAS Agent IP - IP of the server on which the target NAS agent is running.
- find\_auth\_user - User-name whose shares are to be deleted in the <config\_srm.xml> file.
- Output.xml - New output XML file not containing the deleted shares.

**Note:** The first option above is a potentially expensive operation

### Example(s)

1. `perl srmcfg.pl delete config_srm.xml -f NLSVfile.txt`

This example represent the use case where:

- Since no output file has been specified, the files will be deleted directly from the config\_srm.xml.
  - Shares listed in the NLSVfile.txt file are removed from the config\_srm.xml file.
  - Share listed in NLSVfile.txt file but not present in the config\_srm.xml file are ignored.
2. `perl srmcfg.pl delete config_srm.xml -f NLSVfile.txt -a 192.168.200.100 192.168.200.200`

This example represent the use case where:

- Since no output file has been specified, the files will be deleted directly from the config\_srm.xml file.
- Shares, which are listed in both the NLSVfile.txt file and the config\_srm.xml file, are deleted from the config\_srm.xml file.
- The NLSVfile.txt file may be created from the output of an earlier Validate command. This file contains the list of invalid shares.
- Shares, which are listed in the NLSVfile.txt file and that match with at least one aliased IP's of the NAS box shares in the config\_srm.xml file, are removed from the config\_srm.xml file.
- A share, which is listed in the NLSVfile.txt file but does not match any aliased IP in the config\_srm.xml file, will be ignored.
- Shares, which are present in the config\_srm.xml file but are not listed in the NLSVfile.txt file, remain unaffected.

3. `perl srmcfg.pl delete config_srm.xml -u Nancy`

This example represent the use case where:

- Since no output file has been specified, the shares will be deleted directly from the config\_srm.xml file.
- Shares containing <auth\_usr> tag value as "Nancy" are removed from the config\_srm.xml file.

- Shares containing <auth\_usr> tag value other than "Nancy" are not modified.

4. `perl srmcfg.pl delete config_srm.xml -u Nancy -o Output.xml`

This example represent the use case where:

- Since the output file, Output.xml, has been specified, the original config\_srm.xml file is NOT modified.
- Shares having a <auth\_usr> tag value other than "Nancy" are copied to the output file, Output.xml.
- Shares having a <auth\_usr> tag value of "Nancy" are not copied to the output file, Output.xml.
- The user is responsible for backing up the original config\_srm.xml file and renaming the new file Output.xml to config\_srm.xml.

### Change Credentials (alias chngcred or cc)

This function will change the username and password, or both, of shares matching certain criterion. RSCT will update shares in the config\_srm.xml file with new credential pair information that matches the criterion specified on the command line interface.

Several entries in the config\_srm.xml file may be updated with a new set of credentials specified on the CLI. However, the number of entries in the config\_srm.xml file remains the same.

### Format(s)

1. `perl srmcfg.pl cc <config_srm.xml> -f <NLSV File> [-a <Routing agent IP> <NAS agent IP>] [-o <Output.xml>] <auth_user> <auth_pass>`
2. `perl srmcfg.pl cc <config_srm.xml> -u <find_auth_user> [-o <Output.xml>] <auth_user> <auth_pass>`

Where:

- config\_srm.xml - Input XML file containing the SRM Agent configuration parameters.
- NLSV File - Input file containing new-line separated value list of remote shares to be updated with new credentials if found in <config\_srm.xml> file.
- Routing agent IP - IP of the server on which the Central Manager Routing Agent is running.
- NAS Agent IP - IP of the server on which the NAS agent is running.
- find\_auth\_user - User-name whose shares are to be updated with new credentials in the <config\_srm.xml> file.
- Output.xml - New output XML file containing shares updated with new credentials.
- auth\_user - This is the user name to replace the existing user name for shares that qualify for an update based on the criterion.
- auth\_pass - This is the password to replace the existing password for <auth\_user>.

**Note:** The first option above is a potentially expensive operation

### Example(s)

1. `perl srmcfg.pl changecredentials config_srm.xml -f NLSVfile.txt Joe Blogg123`

This example represent the use case where:

- Since no output file has been specified the shares will be deleted directly from the config\_srm.xml.

- Shares listed in NLSVfile.txt that are present in the config\_srm.xml file are updated with the <auth\_usr> and <auth\_pass> tag values "Joe/Blogg123".
- Shares listed in NLSVfile.txt and not present in config\_srm.xml file are not modified.
- Shares listed in config\_srm.xml file not present in NLSVfile.txt are not modified.
- The contents of config\_srm.xml file are changed to reflect the updated values.

2. `perl srmcfg.pl changecredentials config_srm.xml -u Nancy Joe Blogg123`

This example represents the use case where:

- Since no output file has been specified, the shares will be deleted directly from the config\_srm.xml.
- Shares having a <auth\_usr> tag value of "Nancy" will have their <auth\_usr> and <auth\_pass> tag values updated to "Joe/Blogg123" in the config\_srm.xml file.
- A share containing <auth\_usr> tag value other than "Nancy" is not modified.
- The contents of config\_srm.xml file get changed to reflect the updated values.

3. `perl srmcfg.pl changecredentials config_srm.xml -f NLSVfile.txt -a 192.168.200.100 192.168.200.200 Joe Blogg123`

This example represent the use case where:

- Since no output file has been specified, the shares will be deleted directly from the config\_srm.xml
- Shares listed in NLSVfile.txt and present in config\_srm.xml file will have their <auth\_usr> and <auth\_pass> tag values updated to "Joe" and "Blogg123" in the config\_srm.xml file
- The list of shares reported by the NAS agent, running on 192.168.200.200, is retrieved. RSCT communicates with this NAS Agent through the CMRA that is running on the 192.168.200.100 server.
- RSCT attempts to match all shares exposed by the NAS Agent, running on the 192.168.200.200 server, against the contents of the NLSVfile.txt file.
- Shares, which match with at least one of the aliased IP addresses for the NAS system in the config\_srm.xml file, are updated with Joe/Blogg123 username/password pair in the config\_srm.xml file.
- Shares, which are listed in NLSVfile.txt but that do not match with an aliased IP lookup in the config\_srm.xml file, will not modified
- The contents of config\_srm.xml file are changed to reflect the updated values.

4. `perl srmcfg.pl changecredentials config_srm.xml -u Nancy -o Output.xml Joe Blogg123`

This example represent the use case where:

- Since an output file has been specified, the config\_srm.xml file will not be modified. The output file contains the same data as the original config\_srm.xml file but with the changes implemented.
- Shares containing a <auth\_usr> tag value of "Nancy" will be copied to the output file "Output.xml" with their <auth\_usr> and <auth\_pass> tag values updated to "Joe" and "Blogg123", respectively.
- Shares containing <auth\_usr> tag value other than "Nancy" will be copied to the output file "Output.xml" without any modification to their <auth\_usr> and <auth\_pass> tag values.
- The contents of config\_srm.xml file will remain unchanged.
- The user is responsible for backing up the original config\_srm.xml file and renaming the new file Output.xml to config\_srm.xml.

## Start Central Manager Agents

The Windows administrator can use the Windows **Services** panel to start, stop, or restart the agents installed on the Central Manager. Be sure to start the Routing Agent first and then allow time for each agent to auto register before you verify agent functionality.

**Note:**

If you restart the database server, you also must restart the Central Manager agents in the following order:

1. Use the Windows **Services** panel to start the agents installed on the Sun StorageTek Business Analytics Central Manager in the following order:
  - a. Routing Agent.
  - b. License Agent.
  - c. Scheduler Agent.
  - e. Data Polling Agent.
  - f. Data Aggregator
2. Use the Windows **Services** panel to start or restart the remaining Central Manager agents (i.e. Policy Agent, Host Agent, SRM Agent, SNMP Proxy Agent, Remote Host Agent,).

The following section describes how to verify the Central Manager agents have started and registered successfully.

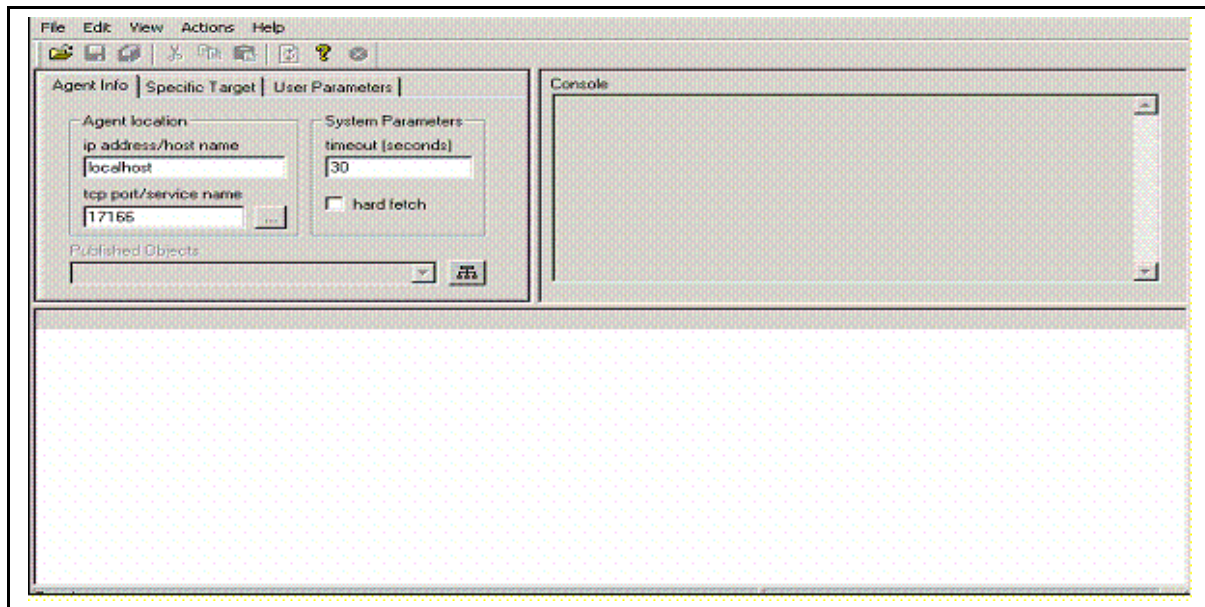
## Business Analytics Agent Diagnostic Tool

The Sun StorageTek Business Analytics Agent Diagnostic Tool is installed in the Storability Local Manager **Utilities** folder as part of the Local Manager and Central Manager during software installation. It represents the primary tool to verify agent functionality once it is configured and started.

You can use this agent diagnostic tool to:

- Communicate directly with a Smart Agent by specifying its IP address/nodename and TCP/IP port Number.
- Communicate directly with a Local Manager or Central Manager.
- Collect any object that the Smart Agent publishes.
- Save a file if requested by a support representative.

The **Agent Info** tab is displayed when you run it, which is installed by default in the <drive>:\Program Files\Storability\GSM\Utilities\Local Manager Utilities folder.



**Figure 45 – Business Analytics Agent Diagnostic Tool Main Window**

To collect an agent's objects (or tables), proceed as follows:

1. Type the IP Address or network resolvable node name in the **ip address/host name** box.
2. Click the button associated with the tcp port/service name input box and a list box is displayed with agent names.
3. Select the desired agent from the list box and the appropriate port number is automatically put into the input box.
4. In the timeout input box, specify a timeout or accept the default (30 seconds).
5. Click the **Get Object List** button, whose icon is shown below.



6. If the client can collect the tables successfully, the **Published Objects** list box is enabled.

The following figure shows an example of the main window after the host configuration (**gsa\_host\_config**) object has been requested.

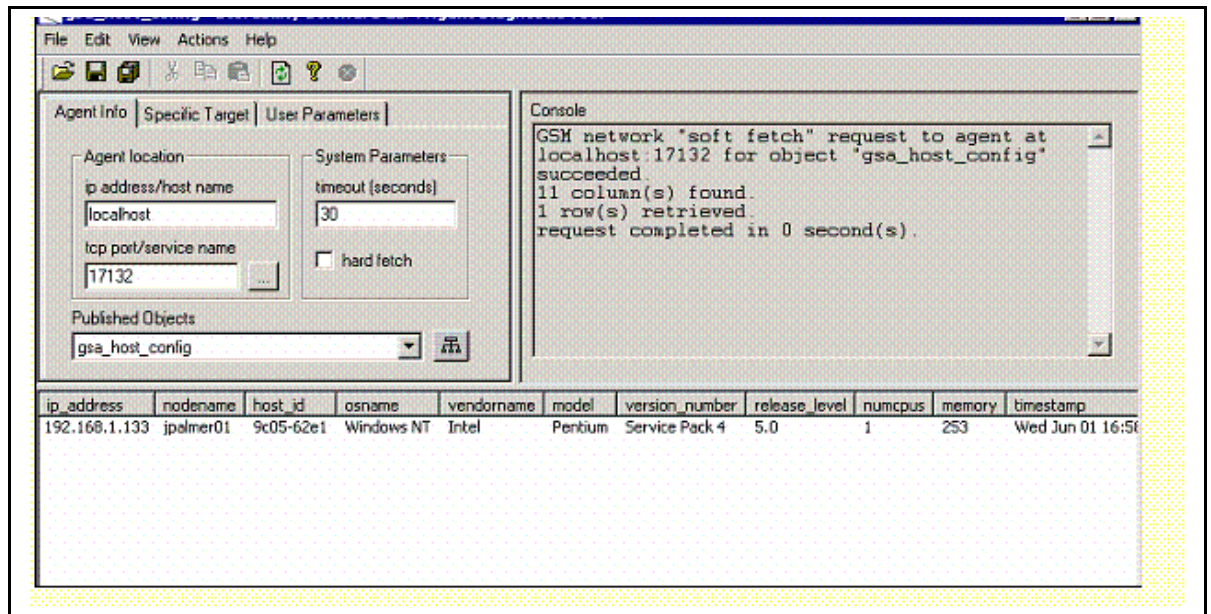


Figure 46 - Sample gsa\_host\_config Object

After you select **File**, a menu selection list appears that allows you to:

- **Save** - Save a particular collected object's data to a user-specified file. The default file extension is .gsm.
- **Save All** - Save the output from collecting all the objects that the agent publishes to a single file.

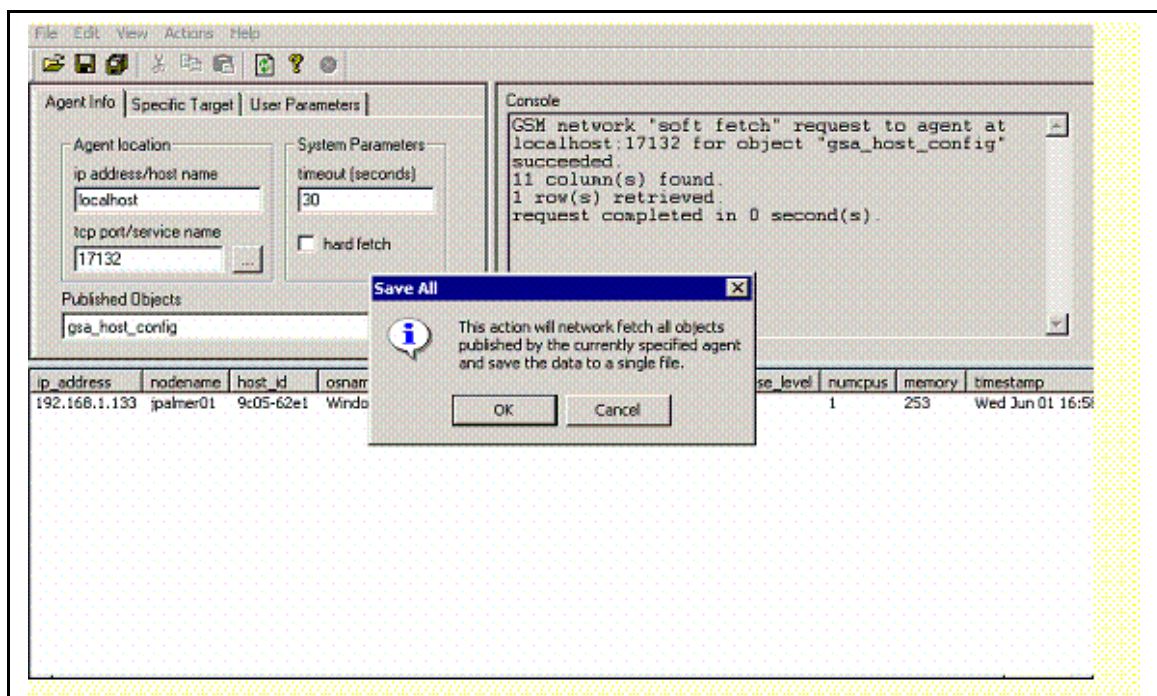


Figure 47 – Save All Option

After you highlight data in the window, the Cut, Copy, and Paste menu selections under **Edit** are enabled. There is no longer password protection enforced on the copy operation.

## Central Manager cm-get Utility

The <drive>:\Program Files\Storability\GSM\Utilities\Storability Central Manager Utilities directory contains the **cm-get** utility, which provides similar agent verification functionality to that of the Business Analytics Agent Diagnostic Tool (gsmdiag.exe). However, cm-get differs from the Business Analytics Agent Diagnostic Tool in that it will only work against a Central Manager Routing Agent (CMRA). That is, the cm-get utility cannot be used to collect data directly from an agent or Local Manager Routing Agent (LMRA), whereas the Business Analytics Agent Diagnostic Tool supports both of these operations. If either operation is attempted using cm-get, the "authorization failed" message is returned as the output.

The usage for **cm-get** is described below.

```
C:\Program Files\Storability\GSM\Utilities\Storability Central Manager Utilities>cm-get -H
Usage: cm-get [-sh] <cm_host_ip> <port> <target> [timeout] [arg]
       where target ::= <object name>[<ip>][<port>][<rid>]

Examples: cm-get 127.0.0.1 17130 gsa_agent_version 30 null
          cm-get 127.0.0.1 17130 gsa_agent_version 30 "<name1><value1>"
          cm-get 127.0.0.1 17130 gsa_host_config:17132x101 30 "<n1><val1><n2><val2>"
```

### Legend:

-s - Soft fetch  
 -h - Hard fetch (default)  
 cm\_host\_ip - Central Manager IP Address  
 port - TCP port number to communicate with the agent (e.g., 17132)  
 object\_name - Agent object name (e.g., gsa\_agent\_version-2\_0)  
 timeout - Execution timeout in seconds  
 arg - Optional arguments (e.g., \_passwd0=password)  
 rid - Routing ID assigned to the Routing Agent (e.g., 300)

A sample collection of the **gsa\_agent\_register** object is shown the following figure.

```
C:\Program Files\Storability\GSM\Utilities\Storability Central Manager Utilities>cm-get -s 127.0.0.1 17130 gsa_agent_register 30
First response in 1 seconds

Object name: gsa_agent_register
Object fields: 13
Object records: 8
```

rid	ra_host	ra_info_port	index	type	port	peer_list	active_peer	last_freshened	when_a
ctivated	application_status	network_status	last_error						
302	192.168.1.12	17146	0	AUTO_NET	17132	instructor3w2k	192.168.1.12	Tue Feb 28 08:01:39 2006	Tue Nov 22 16:44
:07	2005	ACTIVATED	up						
302	192.168.1.12	17146	1	STATIC	17146	192.168.1.12	192.168.1.12	Tue Feb 28 13:18:02 2006	Tue Feb 28 13:18
:02	2006	ACTIVATED	up						
302	192.168.1.12	17146	2	AUTO_NET	17148	instructor3w2k	192.168.1.12	Tue Feb 28 07:57:02 2006	Tue Nov 22 16:39
:30	2005	ACTIVATED	up						
302	192.168.1.12	17146	3	AUTO_NET	17152	instructor3w2k	192.168.1.12	Tue Feb 28 07:57:03 2006	Tue Nov 22 16:39
:27	2005	ACTIVATED	up						
302	192.168.1.12	17146	4	AUTO_NET	17155	instructor3w2k	192.168.1.12	Tue Feb 28 08:04:34 2006	Tue Nov 22 16:39
:56	2005	ACTIVATED	up						
302	192.168.1.12	17146	5	AUTO_NET	17156	instructor3w2k	192.168.1.12	Tue Feb 28 07:57:07 2006	Tue Nov 22 16:39
:35	2005	ACTIVATED	up						
300	192.168.1.3	17146	0	AUTO_NET	17130	INSTRUCTOR3W2K	192.168.1.12	Tue Feb 28 13:22:54 2006	Tue Feb 28 13:22
:54	2006	ACTIVATED	up						
300	192.168.1.3	17146	1	STATIC	17146	192.168.1.3	192.168.1.3	Tue Feb 28 13:22:27 2006	Tue Feb 28 13:22
:27	2006	ACTIVATED	up						

Figure 48 - Sample cm-get Output

# Verify Central Manager Agent Functionality

The Sun StorageTek Business Analytics Diagnostic Tool should be used to verify that the Central Manager agents have started and have registered with their configured Local Manager. Keep in mind that a Central Manager is also considered a Local Manager because it too runs a unique instance of a Routing Agent.

Proceed as follows:

1. Select **Launch Agent Diagnostic Tool** from the program folder you specified during installation.

## Verify Routing Agent

2. Wait approximately 30 seconds after the Routing Agent has started to allow it to initialize before querying it with the Business Analytics Agent Diagnostic Tool.
  - a. On the **Agent Info** window, enter the IP Address or network resolvable Host Name of the server where the agent is installed in the **ip address/host name** input box.
  - b. Set the port to 17146 (or select the Routing Agent from the drop down list of service names).
  - c. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.
  - d. Select the **gsa\_alerts-3\_1** object and examine the columns for warnings or errors. If errors are displayed, open the Routing Agent's **Message** log to further investigate the error.
  - e. Select the **gsa\_agent\_version-2\_0** object to verify the agent's software release level.
  - f. Select the **gsa\_ini\_control-2\_0** object and verify the agent's configuration settings you configured using the Configuration Tool. See Figure 38.
  - g. Select the **alerts-3\_1** object and examine the columns for warnings or errors.
  - h. Verify the other objects the agent publishes.

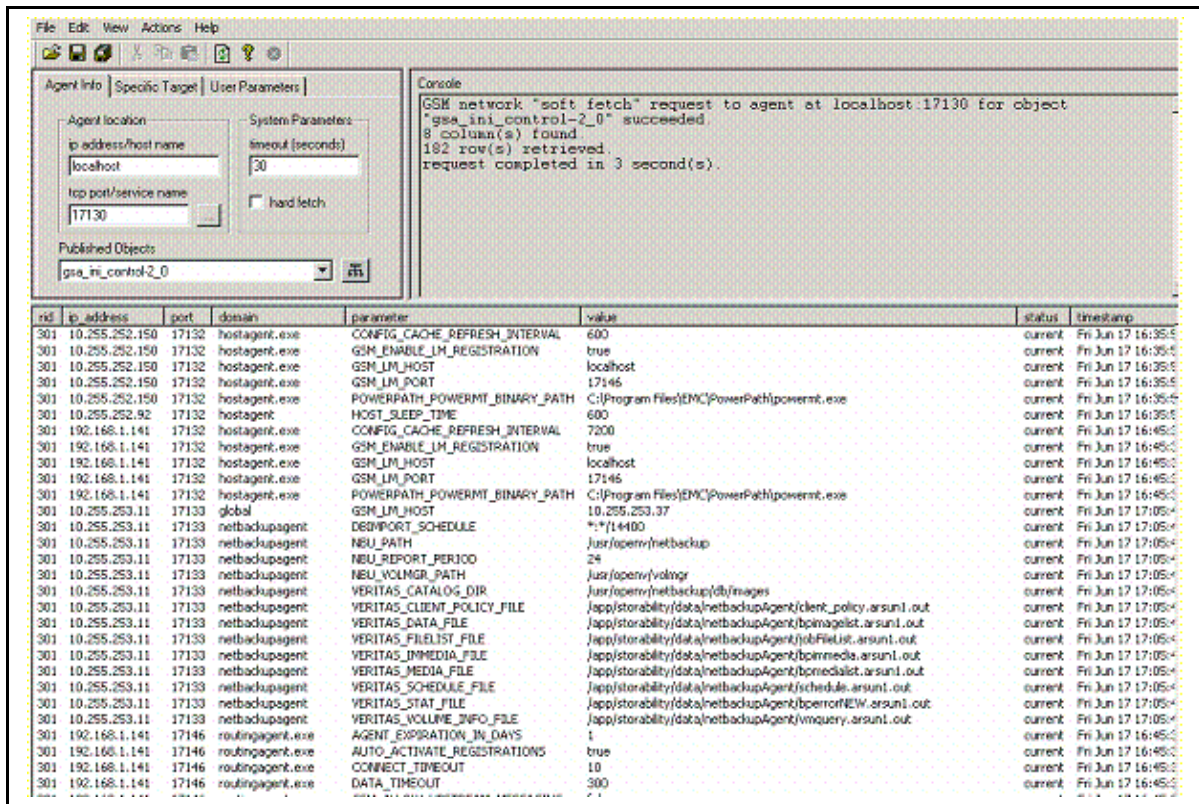


Figure 49 - Sample gsa\_ini\_control Object for Routing Agent

#### Verify License Agent

3. Wait approximately 30 seconds after the License Agent has started to allow registration and agent initialization to occur.
  - a. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the Central Manager/Local Manager in the **ip address/host name** input box.
  - b. Set the port to 17130 (or select Local Manager/Central Manager from the drop down list of service names).
  - c. Click the **Get Object List** button and you should receive a list of objects published by the License Agent.
  - d. Collect the **gsa\_ini\_control-2\_0** object and verify the agent's configuration settings you configured using the Configuration Tool.
  - e. Select the **gsa\_agent\_version-2\_0** object and verify the rid, port number, and version of the License Agent. Use the port number in the next step.

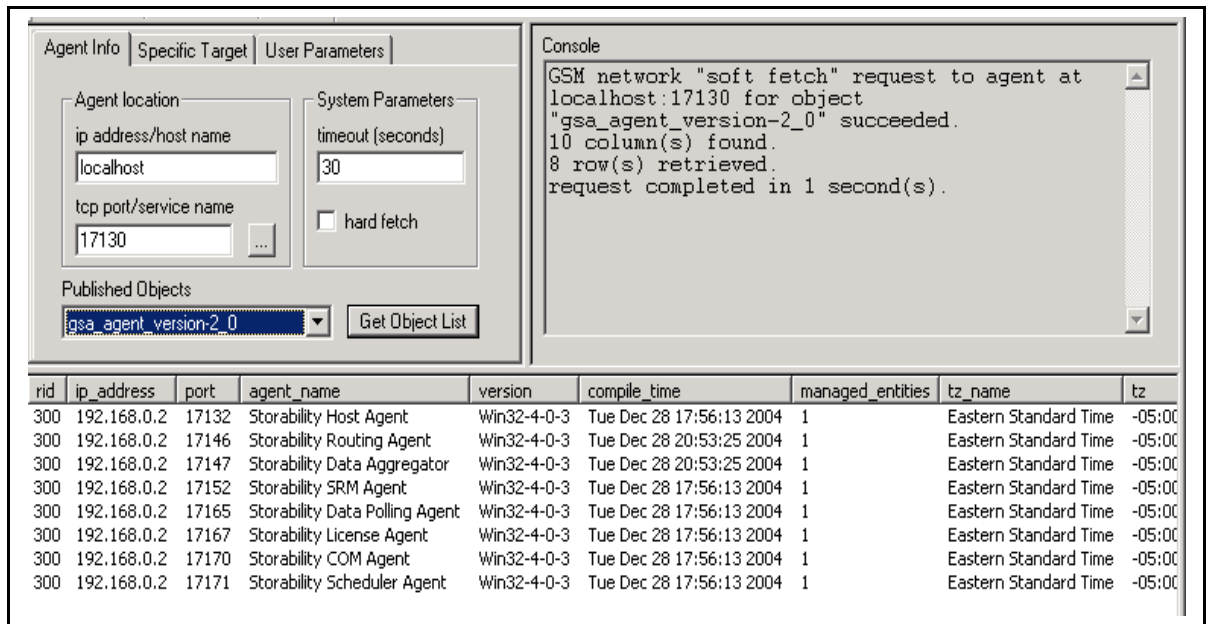


Figure 50 - Verify License Agent

#### Verify Scheduler Agent

4. Wait approximately 30 seconds after the Scheduler Agent has started to allow registration and agent initialization to occur.
  - a. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the Local Manager/Central Manager in the **ip address/host name** input box.
  - b. Set the port to 17130 (or select Local Manager/Central Manager from the drop down list of service names).
  - c. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.
  - d. Select the **gsa\_agent\_version-2\_0** object and verify the rid, port number, and version of the Scheduler agent. Its default port number is 17171.

#### Verify Storability Data Polling Agent

5. Wait approximately 30 seconds after the Data Polling Agent has started to allow registration and agent initialization to occur.
  - a. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the Local Manager/Central Manager in the **ip address/host name** input box.
  - b. Set the port to 17130 (or select Local Manager/Central Manager from the drop down list of service names).
  - c. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.
  - d. Select the **gsa\_agent\_version-2\_0** object and verify the rid, port number, and version of the Scheduler agent. Its default port number is 17165.

#### Verify Storability Data Aggregator Agent

6. Wait approximately 30 seconds after the Storability Data Aggregator Agent has started to allow registration and agent initialization to occur.

- a. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the Local Manager/Central Manager in the **ip address/host name** input box.
- b. Set the port to 17130 (or select Local Manager/Central Manager from the drop down list of service names).
- c. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.
- d. Select the **gsa\_agent\_version-2\_0** object and verify the rid, port number, and version of the Data Aggregator agent. Its default port number is 17147.

#### Verify Host Agent

1. Wait approximately 30 seconds after the Host Agent has started (or restarted) on the Central Manager to allow it to initialize before querying it with GSMdiag.
  - a. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the server where the agent is installed in the ip address/host name input box.
  - b. Set the port to 17132 (or select the Host agent from the drop down list of service names).
  - c. Click the **Get Object List** button and you should receive a list of objects published by the Host Agent.
  - d. Select the **gsa\_host\_config** object and it should list the IP address, node name, host ID of the host server as well as additional fields.
  - e. Verify all other objects published by the agent.
2. To verify the Host Agent has registered successfully with its configured Local Manager:
  - a. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the Local Manager in the ip address/host name input box and set the port to 17130 (or select Local Manager/Central Manager from the drop down list of service names).
  - b. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.
  - c. Select the **gsa\_agent\_version-2\_0** object and verify the rid, port number, and version of the Host Agent.

At this point, the Central Manager agents are running and registered with their Local Manager.

## SNMP Proxy Agent on Central Manager

The SNMP Proxy Agent is used to forward alerts to one or more trap receivers. The agent configuration is stored in the Proxy Configuration (proxy.cfg). If you installed the SNMP Proxy Agent on the Central Manager through the use of the **Custom** installation type, proceed as follows to configure the agent.

1. Select **Start->Programs->Storability->Launch Configuration Tool**.
2. Click **File, Edit**.
3. Click **Proxy Configuration**.
4. Click **Add**.
5. Set the IP address of the trap receiver in the **IP Address** column.
6. Set the TCP port number in the **Port** column.

7. Click **Submit**.
8. Repeat Steps 4 through 7 for each trap receiver.
9. Click **Show Advanced Settings** to review or edit these configuration settings.
10. If there is a peer to this proxy agent, set the **PEERADDR** value with the IP address of the peer. Make sure the **IS\_SECONDARY** value is set appropriately (0 for false and 1 for true) on both machines.
11. Click **File, Save** on the Configuration Tool main menu and confirm saving the configuration settings.
12. Close the proxy configuration file.
13. View and then close the readme.txt file and click **Finish**.
14. Use the Windows **Services** panel to start the agent.

## Management Console

The following sections describe how you install, configure, and verify the Sun StorageTek Business Analytics Management Console. The Management Console is supported both on Windows 2000 and Windows 2003 servers as well as on a VMWare instance.

### Install/Verify Microsoft IIS Server IIS 5.0

The Management Console is supported using IIS 5.0. The following section outlines its installation for reference if it is not already configured and running on the Windows 2000/2003 server.

1. Insert the Windows 2000 installation CD in the CD-ROM drive.
2. Select **Start-> Settings>Control Panel**.
3. Select **Add/Remove Windows Components**.
4. Follow the on-screen instructions to install IIS.
5. Verify the **World Wide Web Publishing** and Simple **Mail Transport Protocol (SMTP)** Services are running before you install Management Console. Open Internet Explorer on the server you will use for the Management Console and enter <http://localhost>. If the IIS default page is not returned, IIS is not running, or more likely not installed.
6. During the installation, follow the on-screen instructions to install SMTP Services that work in conjunction with IIS. You can view the product documentation by typing: file:\\%systemroot%\help\mail.chm in the browser address bar and pressing **Enter**.

### Install/Verify Microsoft IIS Server IIS 6.0 for Windows 2003

The Sun StorageTek Business Analytics Management Console is supported on a Windows 2003 server running IIS 6.0. There are several ways to install IIS 6.0, which is shipped with Windows 2003. The following procedure summarizes its installation using the **Add/Remove Programs** option from the Control Panel:

1. From the **Start** menu, click **Control Panel**.

2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the **Components** list box, click **Application Server**.
5. Click **Details**.
6. Click **Internet Information Services Manager**.
7. Click **Details** to view the list of IIS optional components.
8. Select all the optional components you wish to install. **Note:** The World Wide Web Publishing Service optional component includes important subcomponents like the **Active Server Pages** component and Remote Administration (HTML). To view and select these subcomponents, click **World Wide Web Publishing Service** and then click **Details**.
9. Click **OK** until you are returned to the **Windows Component Wizard**.
10. Click **Next** and complete the **Windows Component Wizard**.

Refer to your Microsoft documentation for additional details on installing Microsoft IIS 6.0.

### Additional Configuration Settings for Windows 2003 SP1

The Management Console requires that the **Active Server Pages** option is enabled on the Windows 2003 server.

1. Click **Start -> Administrative Tools -> IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).
2. Go to the **Web Service Extensions** tab.
3. Click **Active Server Pages**, and then press the **"Allow"** button on the left. Active Server Pages should now work.
4. To prevent IIS from timing out before Management Console, perform the following procedure:
  - a. Open the Properties on the Default Web Site.
  - b. On the first tab (Web Site), change the Connection Timeout to 900 seconds, which is the setting used in IIS 5.0.

### Problems Running on Windows 2003 SP1

On a computer that is running Microsoft Windows Server 2003 Service Pack 1 (SP1), programs that use DCOM do not work correctly. The Management Console "gsmcom" uses DCOM. With this condition, the COM Agent is unable to communicate to the License agent but is registered with the Routing Agent.

This issue occurs because the default Component Object Model (COM) permissions are changed in Windows Server 2003 SP1. The new COM permissions restrict remote calls that are not authenticated. The COM program may work locally, but the remote calls that are not authenticated fail. By default, only members of the Administrators group have the Remote Activation permission and the Launch permissions. This change prevents user accounts that do not belong to the Administrators group from starting COM components.

To resolve the permissions issue after a first time installation or upgrade of the Management Console, proceed as follows:

1. Click **Start**, point to **Control Panel, Administrative Tools**, and then click **Component Services**.
2. Expand the Component Services\Computers container.
3. Expand **My Computer**, click and expand DCOM Config.

4. In the right pane, locate the program called "gsmcom"
5. Right click the "gsmcom", and then select **Properties**.
6. On the **Security** tab, in the Launch and Activation Permissions group box, select **Customize**, and then click **Edit**.
7. Add Internet Guest Account "**IUSR\_Server\_Name**".
8. Click and highlight the "**IUSR\_Server\_Name**" account and then click **Allow** for the **Local** and **Remote Access** permissions.
9. Click **OK** two times to accept the changes. Then, try to Launch the Management Console.

This issue may not occur if SP1 is installed after the Management Console has been installed.

## Management Console Installation

This section describes the installation process for the Sun StorageTek Business Analytics Management Console.

**Note:** If the installation program detects that an existing Management Console has already been installed, you are prompted to uninstall the Management Console and its source files. If you select to delete the currently installed Management Console, you must run the Setup (setup.exe) from the installation media after it has been uninstalled.

The Management Console installation installs the Storability COM Agent. The default installation path is the <drive:>\Program Files \Storability\GSM\Agents\Storability COM Agent folder. The storability.ini is created and saved in the COM agent folder. If an existing storability.ini file is found, the install will rename the existing copy as "storability.ini.old + current time in milliseconds" before creating a new Storability.ini file.

1. Insert the Sun StorageTek Business Analytics Management Console Installation CD into the CD-ROM drive. **Note:** If the Setup program does not auto-run after you insert the CD into the drive, run setup.exe from the installation media to start the InstallShield Wizard.
2. Click **Next>** to continue on the **Installation Welcome** screen.
3. Click **Yes** to accept the Software License Agreement.

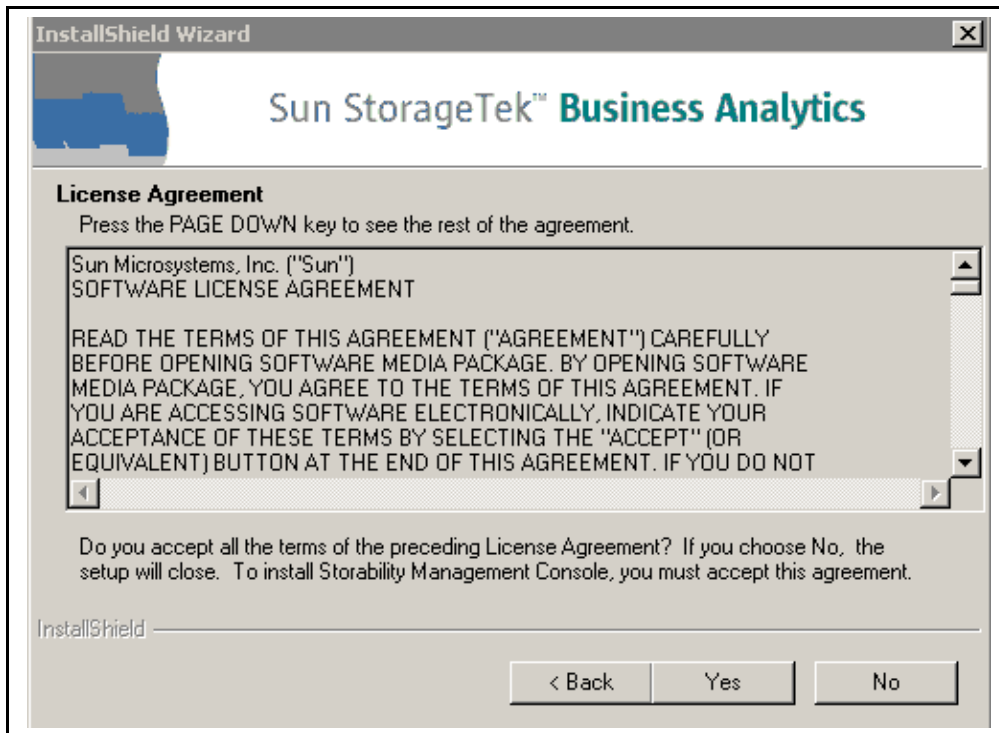


Figure 51 - Software License

4. Select **Typical** on the **Setup Type** screen and click **Next>**. The Choose Destination Location dialog is displayed. **Note:** The **Typical** setup type should be used for first-time installation of the Management Console. The **Custom** setup type can be used to install individual components, such as an upgraded version of the Storability COM Agent.
5. Specify an installation destination folder or accept the default destination location (C:\Program Files\Storability\Storability Management Console) and click **Next>**. The Storability COM Agent dialog appears.

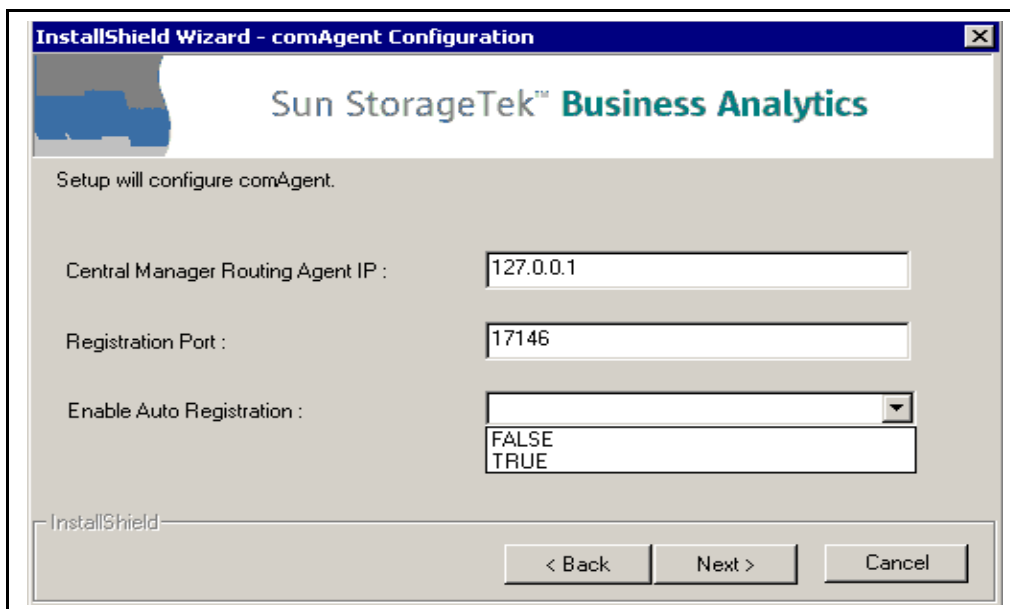


Figure 52 - Storability COM Agent Configuration Dialog

6. In the respective input boxes, enter the following:

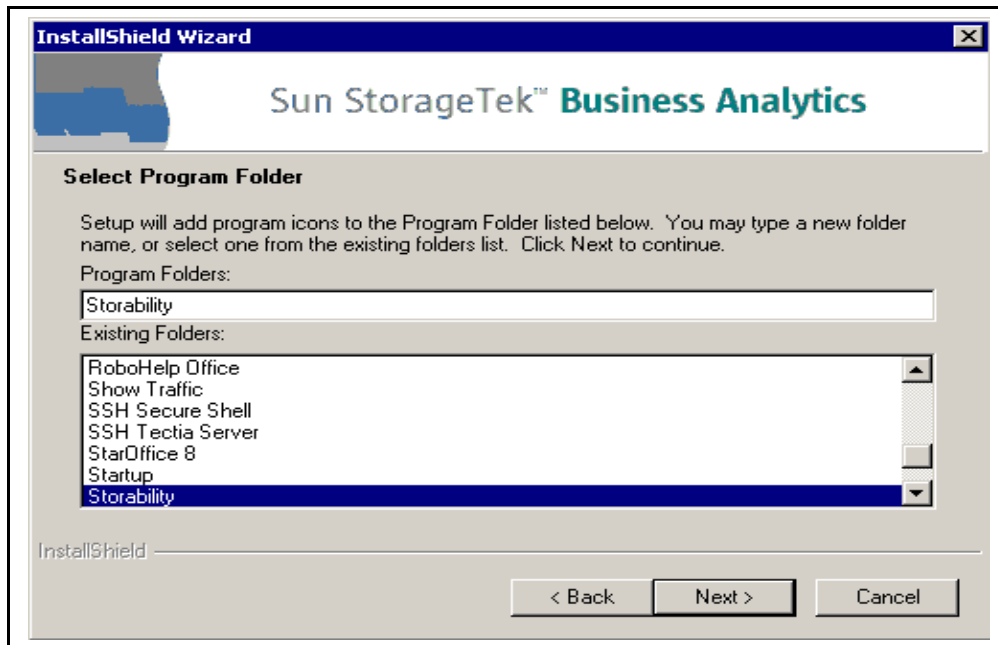
- **Central Manager Routing IP** – Specify the IP Address or network resolvable host name for the Local Manager to be contacted for auto registration. The default IP address is localhost (127.0.0.1) and will need to be changed if the Local Manager/Central Manager is not running on the Management Console server.
- **Registration Port** – Central Manager Routing's Agent's port used for agent auto registration. The default port is 17146.
- **Enable Auto Registration** – Using the selection list box, set this parameter to TRUE and allow the COM Agent to use agent auto registration, or set it to FALSE to disable auto registration for the COM Agent.

7. Click **Next>** to continue and the "Setup will configure System DSN" dialog appears.

The screenshot shows a Windows-style dialog box titled "InstallShield Wizard". The main heading is "Sun StorageTek™ Business Analytics". Below this, a message states: "Setup will configure System DSN. Please enter IP address and port number of the Microsoft SQL Server where GSM Databases are located". There are three text input fields: "System DSN:" containing "atlantis", "IP Address:" containing "127.0.0.1", and "Port:" containing "1433". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted.

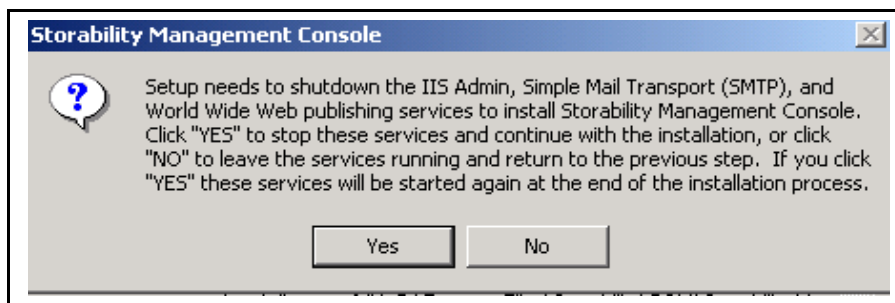
**Figure 53 - Configure System DSN**

8. Review/modify the configuration settings for the System DSN (atlantis) to be used to communicate with the Central Manager database server:
- **IP Address** – Specify the IP address of the Central Manager
  - **Port** – Specify the TCP port of the database instance; the default SQL Server port is 1433.
9. Click **Next>** to continue.
10. Specify the Program Folder to be updated with the Management Console option.



**Figure 54 - Select Program Folder**

11. Click **Next>** to continue and the Current Settings dialog appears. Review the current settings and click **Next>** to continue or **<Back** to make any changes to the listed configuration settings.
12. After you click **Next>**, the installation displays a dialog that warns you that IIS must be stopped. Click **Yes** to continue.



**Figure 55 - Shutdown IIS Informational Dialog**

13. The **Setup Status** splash box will display and will update you through the status bar on the progress of the installation.

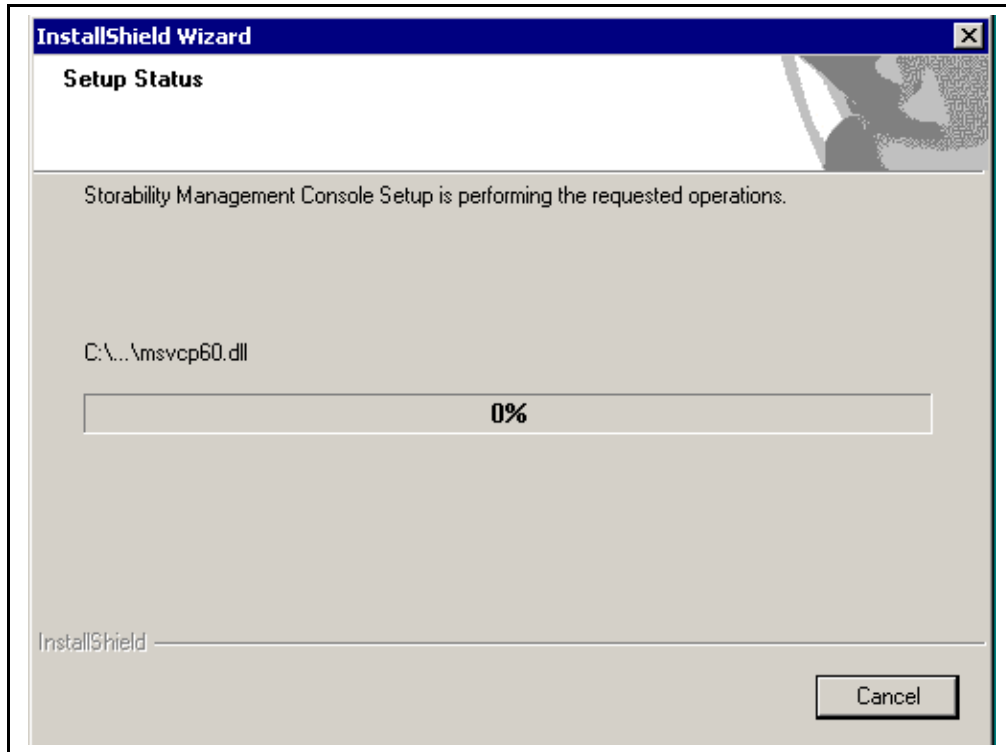


Figure 56 - Setup Status

13. The InstallShield Installation Complete dialog appears. Click **Finish** to complete the installation procedure.

#### Running Install from Network Drive

For Sun StorageTek Business Analytics 5.0 Management Console installation, the installation has no problem if installed locally. However, if installing through a network mapped drive or through a network location for a computer not having a CD-ROM drive, the IISMGr.exe throws an exception.

The manual procedure to circumvent this problem is described as follows:

1. Copy the entire contents of MC Installation CD to a local directory.
2. Install the Management Console from the local directory.
3. Manually create the virtual directory using the instructions below. **Note:** Different versions of Windows may differ slightly.
4. Right-click My Computer, then click Manage from the shortcut menu. The Computer Management window appears.
5. Expand the Services and Applications option, and then expand the Internet Information Services option until you see the default web site.
6. Right-click the default web site, point to New, and then click Virtual Directory from the shortcut menu. A Virtual Directory Creation Wizard launches to direct you through the creation of the new virtual directory.
7. Click Next. The Virtual Directory Alias panel appears. You specify the name (vir) of your virtual directory here.
8. Click Next. The Web Site Content Directory panel appears.
9. Click Browse and choose <drive>:\Program Files\Storability\GSM\Storability\Management Console\Source\portalsource\vir and click Next.

10. The Access Permissions panel appears. Manually configure your virtual directory permissions (enable Read and Run scripts (such as ASP)).
11. Click Next. The Confirmation that you have successfully completed the Virtual Directory Creation Wizard appears.
12. Click Finish. The virtual directory (vir) has now been created.

## Management Console Configuration

This section covers the steps that you can use to set up and then verify your Management Console functionality using the Central Manager's Host Agent. After you verify the Management Console using this simple configuration, you can proceed to add your additional Local Managers/Sites, dashboards, views, users, and polling schedules to the Sun StorageTek Business Analytics application.

### Launch Management Console

1. Select **Start->Programs->Storability-> Launch Management Console**. The Sun StorageTek Business Analytics Management Console Login window appears.
2. Log in using the default administrative account, gsmuser, as both the username and password.

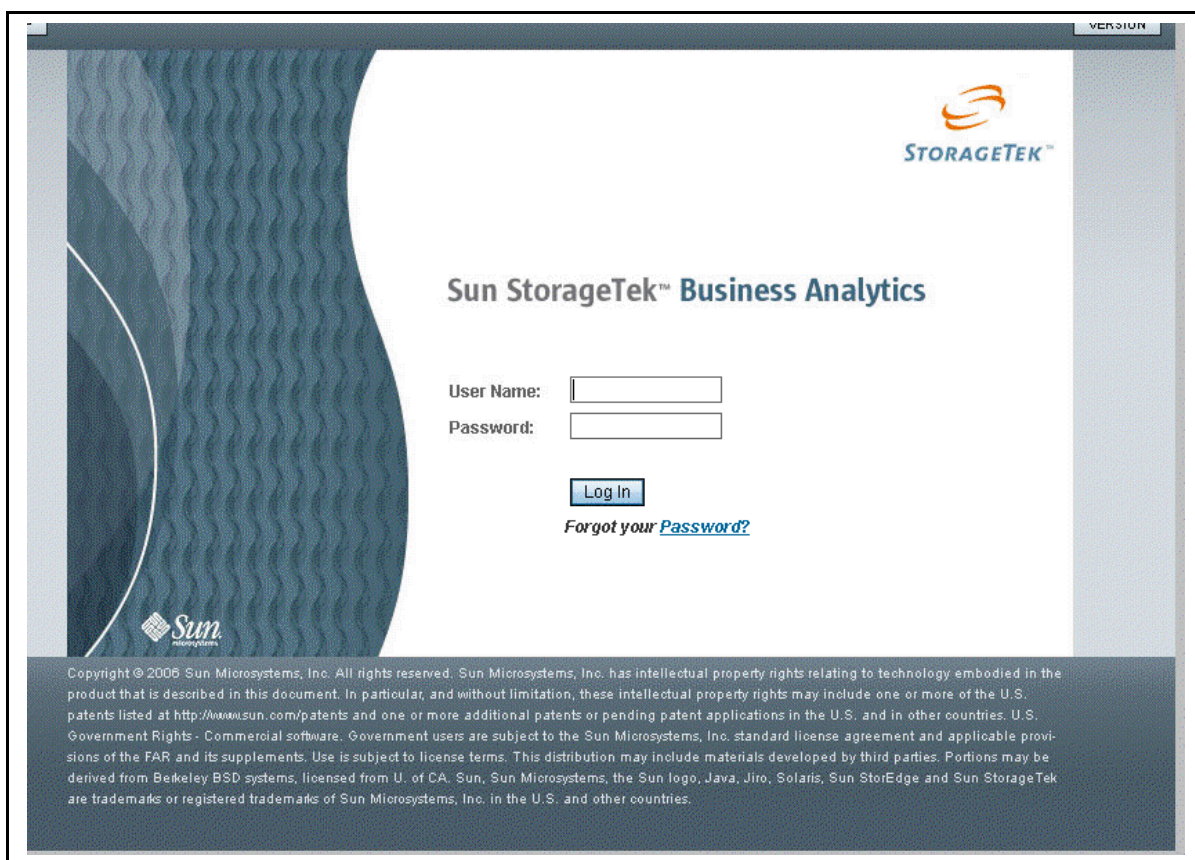


Figure 57 - Management Console Login Window

3. After a successful log in to the application, the Management Console Home Page appears. The home page is blank with the words "No Default View" displayed in the upper right corner. As soon as a view is created in the system and is used by the gsmuser, "No Default View" will disappear off of the home page.

## Customize the Default Local Manager and Default Site

### 4. Customize the default Local Manager:

- a. Select **Tools** -> **Site/Local Manager Administration**.



Figure 58 - Site and Local Manager Listing

- b. Click the Default Local Manager link displayed in the **Site/Local Manager Listing** window.
- c. Customize the default name to suit your company and to accommodate the Central Manager that you are setting up as a Local Manager. Remember that the Central Manager also functions as a Local Manager because it runs a unique instance of the Routing Agent. The Central Manager Routing Agent supports the top level of the messaging infrastructure.
- d. Modify the **Name** to suit your application/company.
- e. Modify the **Short Name** or alias for the Local Manager to suit your application/company.
- f. Update the **IP Address** of the Central Manager to its actual IP address.
- g. Click **Save** and click **OK** on the confirmation dialog box to update the Local Manager.

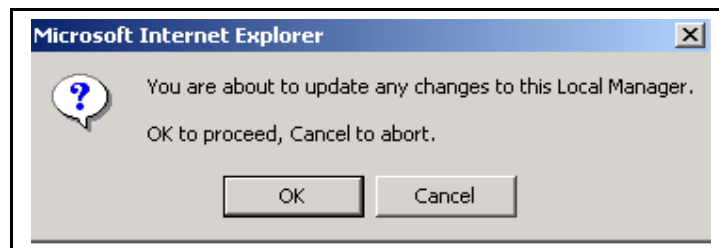


Figure 59 - Update Changes to Local Manager

### 5. Customize the default Site:

- a. Click the **Default Site** link for the listed default site.
- b. Enter a **site name** and **location** to suit your company's implementation.
- c. Click **Save** and confirm the changes, when prompted.

- d. Close the window.

## Create View and Assign to User

### 6. Create a View:

- a. Select **Tools -> View Administration** and the Views wizard appears.

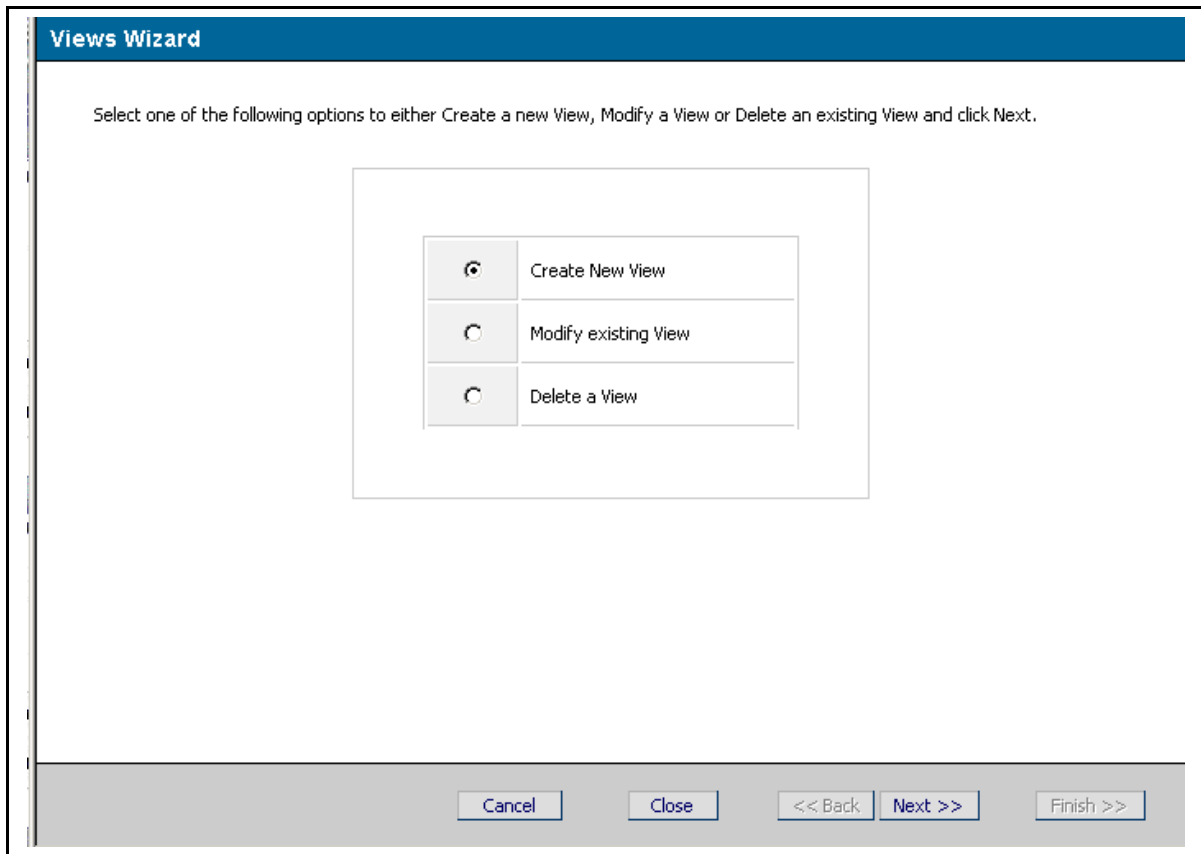


Figure 60 - Views Wizard

- b. Select **Create New View** (default) and click **Next >>** to continue.
- c. In the **Create View** window, enter the name of your enterprise as the name of the view.
- d. Use the **View Type** list box to select **Asset View** (do not specify Composite View).

**Create View**

**View Definition**

Name:

View Type:

Description: Maximum 255 characters are allowed.

**Figure 61 - Create View**

- e. Click **Next>>** and the **Add Assets to View** window appears for your new view.
- f. Select the "What type of asset do you wish to add to this view?" list box and select Sites. Only sites may be added until agent data collection has been completed successfully.
- g. Click the **List** button and the site(s) you created will appear.
- h. Click the **Select** check box to choose the site and then click the **Add to View** button.

**View Administration: Add Assets to View**

**Add Assets to View ACME Corporation**

What type of asset do you wish to add to this view?

Sites

<input checked="" type="checkbox"/>	Asset Type	Name	Location	Description
<input checked="" type="checkbox"/>	site	Headquarters	Headquarters Boston, MA	*All Assets at this Site*

Figure 62 - Add Assets to View

- i. Click **Next>>**. The "Site assets added successfully." text message appears on the **Add Assets to View** window to confirm adding the site to the view.
- j. Click **Next>>** and the **Add Users to View <View Name>** window appears.
- k. Use the checkbox to choose the (GSMuser) and click **Add to View**. The "Users Added Successfully" message is displayed in the Add Users to View window.
- l. Click **Next>** and the **Create View – Summary** window appears.

**Create View - Summary**

Printer Friendly Page

View 'ACME Corporation' created successfully.

<b>Name</b>	:	ACME Corporation
<b>View Type</b>	:	Asset View
<b>Description</b>	:	

**Asset List**

Asset Type	Name	Location	Description
site	Headquarters	Headquarters Boston, MA	*All Assets at this Site*

**User List**

User Name	First Name	Last Name
GSMUser	G	SMUser

Cancel << Back Next >> Finish >>

Figure 63 - Create View - Summary

- m. Review the information on the new asset view, including its status ("<view\_name> created successfully."), View Type, and Asset List. You can optionally click the **Printer Friendly Page** button and then **Print** to print the Create View – Summary information on a local or network printer.
- n. Click **Finish>>** and you are returned to the **Views Wizard** window.
- o. Click **Close** to close the Views Wizard.

## Dashboard Administration

7. Create Dashboard:
  - a. Select **Tools->Dashboard Administration->Manage Dashboards**.
  - b. Click **Create New**.
  - c. Type a meaningful name for the dashboard.
  - d. Use the **dashboard type** list box to choose the dashboard security of public or private. Assign public to allow any Business Analytics user to choose the dashboard. Select private to restrict its use to its creator.
  - e. Optionally enter a description.
  - f. Beside the "Components in the layout:" heading, click each type of pane (Storage, etc.) you want to be included. In this example, minimally click Server. A check appears in the selection box for each component you select.
  - g. Click **Save**.
  - h. Close the window.
8. Change Dashboard:
  - a. Select **Tools->Dashboard Administration->Change Dashboard**.
  - b. Use the radio button to select the dashboard you created.
  - c. Click **Set as current dashboard** and click **OK** to confirm.

- d. Verify the Home Page appears displaying the **Host Filesystem Utilization** pane (as pane well as any other selected panes in the dashboard you created). **Note:** Because you have not yet collected agent data using the Data Polling Schedules functionality, no data appears in the dashboards.

## Data Polling Schedules

9. Review/use the default polling schedules for the Configuration Type of Host:
  - a. Select **Tools -> Data Polling Schedule**.
  - b. The **Polling Schedules** window is displayed. The default polling schedules in the database, which were automatically created at installation time, include three schedules for Host. These have a Collection Metric of Configuration, FileSystem, and Logical VM (Volume Manager).
  - c. You are now ready to collect the Host Agents' data for all sites. You can later repeat this procedure for the other Collection types after your Smart Agents (fabric, array, etc.) have been deployed.
  - d. Click the **Collect Now** button for the Collection Type of **Host** and the Collection Metric of **Configuration**.
  - e. Wait approximately thirty seconds and click the **Collect Now** button for the Collection Type of Host and the Collection Metric of **Filesystem**.
  - f. Wait approximately thirty seconds and click the **Collect Now** button for the Collection Type of Host and the Collection Metric of **Logical VM**.
  - g. Verify the Central Manager server appears in the **Host Filesystem Utilization** dashboard. If so, the Management Collection is now ready for data collection.

**Note:** You must utilize the Refresh Homepage Cache menu under Database Administration to refresh the table cache before you will see any newly collected data in the Host Filesystem Utilization dashboard pane.

## Installing the Management Console to a Non-Default Web Site

The Management Console installation normally updates the default web site. If the default web site cannot be updated, proceed as follows to manually install the Management Console to a non-default web site.

1. Run Management Console installation.
2. Accept the license agreement.
3. In the Setup type selection dialog, choose the Custom installation option.
4. Specify the destination location (e.g., c:\Program Files\GSM\Storability Management Console).
5. On the "Select Features to be Installed" dialog, uncheck the IIS Settings option. Leave the other features enabled (check mark) to be installed.
6. In the dialog to configure the COM Agent, specify:
  - Central Manager Routing Agent IP Address: IP address to contact.
  - Registration Port – Accept the default port number of 17146.
  - Enable Auto Registration – Use the pull down list box to enable (TRUE) or disable agent auto registration for the COM Agent.
7. Accept the default DSN to connect to the Central Manager databases if the Management Console is being installed on the Central Manager. Otherwise, specify the following:
  - System DSN – atlantis
  - IP Address – IP address of the Central Manager
  - Port – Port number to connect to SQL Server running on the Central Manager.The default SQL Server port number is 1433.
8. Specify the Program Folder to be updated.

9. Review the Current Settings and then continue if the information is correct.
10. When prompted that installation will need to stop IIS, choose YES to allow the installation to proceed.
11. Using Internet Information Services, select your computer and right click.
12. Choose New->Web Site.
13. Type a description and click Next>.
14. In the Web Site Creation Wizard Dialog, specify the following:
  - Do Not Change the Default
  - TCP Port – Specify the port number (default is 80 and may be in use).
  - Do Not Change the Default
15. In the Web Site Home Directory dialog, use the Browse button to select the fully qualified path to the Management Console's sourcepriv folder.
16. Click OK and then Next> to continue.
17. In the Web Site Access Permissions dialog, accept the default web site permissions of "Read" and "Run scripts".
18. Click Next> and then Finish> to complete the wizard script used to create a web site.
19. Right click on the new web site and choose New-> Virtual Directory.
20. Click Next> in the Welcome dialog to continue.
21. In the Virtual Directory Alias dialog, type the alias name of vir and click Next>.
22. In the Web Site Content dialog, use the Browse button to select the fully qualified path to the Management Console's vir folder.
23. Click Next and review the enabled access permissions, which should be "Read"
24. Click Next> and then Finish to complete the wizard script used to create the virtual directory.
25. Reboot to restart all the services.
26. Test your Management Console install by pointing to http://localhost:<port number>.

## Local Manager

The Sun StorageTek Business Analytics Local Manager consists of the Routing Agent and a set of utilities. Each Local Manager is added to the application using the Management Console's **Site/Local Manager Administration** menus. The Local Manager ID is configured as the Local Manager's Routing ID in the storability.ini file. Each Local Manager must specify a parent Local Manager in its configuration settings to allow the messaging infrastructure to work properly.

The SNMP Proxy Agent may optionally be installed on a Windows or Solaris Local Manager.

### Add the Local Manager Using the Management Console

1. Select **Start->Programs->Storability-> Launch Management Console** from the **Start** menu. The Sun StorageTek Business Analytics Management Console Login window appears.
2. Log in using an administrative account (e.g., gsmuser).
3. Create the Local Manager:
  - a. Select **Tools -> Site/Local Manager Administration -> Add New Local Manager**.
  - b. Enter a name for the Local Manager in the **Name** field.

- c. Enter a **Short Name** or alias for the Local Manager.
- d. Enter the **IP Address** of the server where you will install the Local Manager.
- e. Select an existing site (or leave the Local Manager unassigned until you've created a site).

**Note:** These instructions assume that you have selected an existing site.

- f. Click **Save** and click **OK** on the confirmation dialog box to create the Local Manager and assign it to the selected site.
- g. When the Modify/Delete Site screen appears, review the information on the site and Local Manager.

**Notes:** The Local Manager Routing ID is generated when the new Local Manager is created using the Management Console application. You will specify this unique identifier when you configure the Local Manager Routing Agent. Be aware that Local Manager ID, Routing ID (RID) and acom\_id (in the database) are different terms for the same entity.

## Installing Local Manager – Windows

1. Insert the Sun StorageTek Business Analytics Local Manager Windows Installation CD into the CD-ROM drive.
2. Click **Next** on the **Welcome** menu to continue the installation.
3. Click **Yes** to accept the terms of the software license agreement.
4. Click **Next**.
5. Review/modify the User Name and Company Name and click **Next>**.
6. A screen appears that allows you to select Smart Agents. Select (check) the **Routing Agent** under the Local Manager heading.

**Notes:** If you are running the installation after previously agents, the installation screen contains check marks in the check boxes for the installed agents. You are prompted to uninstall and then reinstall each installed agent if you do not remove the check marks.

7. Click **Next>** to continue with the installation.
8. Review and verify the agents to be installed and click **Next>** to continue.
9. Click **Next>** to accept the default destination folder and click **Next>** to continue.
10. When the **Configuration Tool** is launched, configure the Local Manager:
  - a. Select **File->Edit->Smart Agent Configuration**.
  - b. Click the **Routing Agent** tab.
  - c. In the Routing Agent ID input box, enter the unique integer value to identify the Local Manager. Be sure that this RID matches the Local Manager ID (e.g., 301) that was created using the **Management Console's Site/Local Manager Administration** menus.

- d. In the **Parent Routing Agent IP** input box, specify the IP address of the Central Manager/Local Manager that will collect the agent data. This is a required parameter for a Local Manager.
- e. For **Port used to publish tables**, specify the TCP port number the Local Manager uses to publish its objects. The default TCP port number is 17130.
- f. For **TCP Connect Timeout**, accept the default time interval (10 seconds) to connect to an agent, which should be fine for most TCP environments.
- g. For **Data Timeout**, this parameter is generally ignored because this value is over-ridden by a system parameter passed to the Routing Agent by Sun StorageTek Business Analytics clients. The default value is 300 seconds.
- h. If your Local Manager will collect agent data from statically registered agents, proceed as follows:
  - i. Click **Change Option Values** button beside the **Static Sub Agent** heading. The Enter Static Sub Agent Registrations dialog box appears.
  - ii. Type the port number and IP address pair or the port number and server name pair to identify each sub agent.
  - iii. Click **Submit** after you have completed all the static agent registrations.
- i. Click **Show Advanced Settings** to review/modify the following configuration parameters:
  - **Allow GSM Upstream Messaging** – Turns on (true) or off (false) the capability to exchange messages with upstream agents. For the Routing Agent, set this variable to "false", which is the default value.
  - **Auto Activate Registration** – Turns on (true) or off (false) auto registration for this agent. The default value is "true" (enabled).
  - **Specific Network Interface to Bind to** - The value may be an IP address, specified in standard Internet dot ("x.x.x.x ") notation, or a name service resolvable hostname. This option allows you to bind the Routing Agent to a specific network interface in a dual-homed computer, for example. If you do not bind the Routing Agent to a specific network interface, the Routing Agent will bind to all available local interfaces.
  - **Maximum Number of Incoming Threads** – Is used to control the limited pool of threads that handle the incoming connections for agent registrations. The Routing Agent receives registrations on port 17146. The default value is 10.
  - **ALLOW\_DYNAMIC\_HOST\_RESOLUTION** – Specifies whether dynamic host resolution can be performed using Dynamic Name Resolution (DNS). The default value is true. If host name resolution fails because the host has been removed from DNS because of an administrative error, for example, the value can be set to false to avoid a valid partial data set from not being returned.
  - **Max. Number of Threads** – Specify the number of threads to be spawned. A rule of thumb is to set this value to one half the number of immediate sub-agents (number of rows in the gsa\_agent\_register table where rid = RID).

This should be set no lower than five (5) and no higher than fifty (50). The default value is ten (10).

- **Number of Days Agents Remain Registered** - Specifies the maximum number of days an agent can be down and remain registered. Its purpose is to provide a simple mechanism for removing records of agents that are no longer installed. When expired, the sub-agent registration is removed. However, the agent can always re-register if it ever comes back online.
- **Agent Registration Cache File** - Is <drive>:\Program Files\Storability\Agents\Storability Routing Agent\ardb.dat by default. The Routing Agent creates the agent registration cache file you specify at start up.
- **License File Name** - Is not applicable for a Local Manager.
- **License Audit Frequency** - Is not applicable for a Local Manager.
- **Interval to Poll Agent Meta Table** - Specifies how often in seconds to gather agent objects from the configured sub agents.

11. Select **File->Save** and confirm your changes to the storability.ini file.
12. Select another agent tab to review/modify its configuration settings or click **File->Exit** to close the Configuration Tool.
13. View and then close the **Readme** file and click **Finish**.
14. Use the Windows **Services** panel to start the Routing Agent before you verify agent functionality
15. Proceed to the **Verifying Local Manager** section.

## Installing SNMP Proxy Agent on Windows Local Manager

You may optionally install the SNMP Proxy Agent on a Windows Central Manager/Local Manager. Proceed as follows.

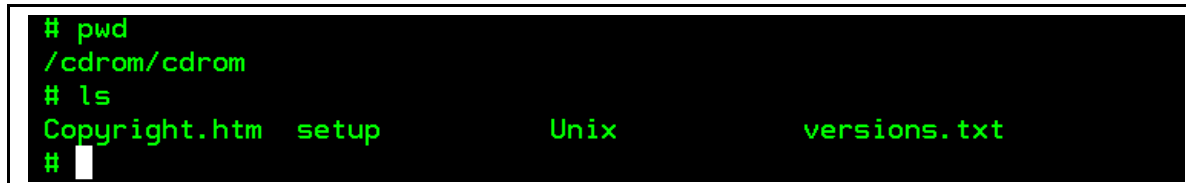
1. Insert the Sun StorageTek Business Analytics Local Manager Installation CD into the CD-ROM drive.
2. Click **Next** on the Welcome menu to continue the installation.
3. Click **Yes** to accept the terms of the software license agreement.
4. Click **Next**.
5. Review/modify the User Name and Company Name and click **Next**.
6. Select (check) the **Proxy Agent** checkbox on the screen that allows you to select Sun StorageTek Business Analytics Agents.
7. Review the settings and click **Next** to continue.
8. After the SNMP Proxy Agent is installed, the **Configuration Tool** is automatically launched.
9. Click **File, Edit**.

10. Click **Proxy Configuration**.
11. Click **Add**.
12. Set the IP address of the trap receiver in the **IP Address** column.
13. Set the TCP port number in the **Port** column.
14. Click **Submit**.
15. Repeat Steps 14 through 15 for each trap receiver.
16. Click **Show Advanced Settings** to review or edit these configuration settings.
17. If there is a peer to this proxy agent, set the **PEERADDR** value with the IP address of the peer. Make sure the **IS\_SECONDARY** value is set appropriately (0 for false and 1 for true) on both machines.
18. Click **File, Save** on the Configuration Tool main menu and confirm saving the configuration settings.
19. Close the proxy configuration file.
20. View and then close the readme.txt file and click **Finish**.
21. Use the Windows **Services** panel to start the agent.

## Solaris Local Manager Installation CD Setup Script

The setup script on the Solaris Local Manager Installation CD provides the following features:

- Provides a command line interface for the user to perform Business Analytics Local Manager (Solaris) installation.
- Validates that the user is root to perform the installation.
- Validates that the Solaris server is equipped with a supported Operating System, which includes Solaris 5.7 through Solaris 5.10 for certain agents.
- Provides a list the agents available, depending on the platform, for the user to choose to install or uninstall (setup -u).
- Performs agent installation depending on the user's selection.
- Performs agent upgrade for existing SUNWbizan packages.



```
# pwd
/cdrom/cdrom
# ls
Copyright.htm  setup          Unix          versions.txt
#
```

Figure 64 - Installation Directory for Solaris Local Manager

## Business Analytics Solaris Base Software and Utilities

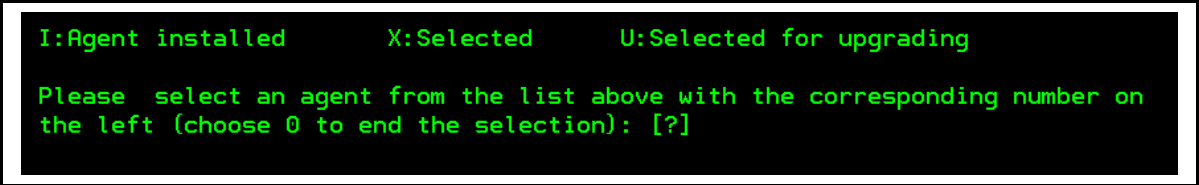
The Solaris Base Package (SUNWbizanbase) must be installed prior to the installation of any additional Business Analytics software. The Local Manager Utilities provide a set of utilities that include the optional agent monitor that can be used to automatically restart stopped agents. The installation script will automatically install one or both of these software components as required to support selected device agents.

1. Mount the installation CD on the Solaris server. For example:

```
mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /mnt
```

2. Change directory to the mounted CDRom drive (e.g., cdrom0).
3. To display the installation main menu that lists the available agents you can choose to install or upgrade, type:

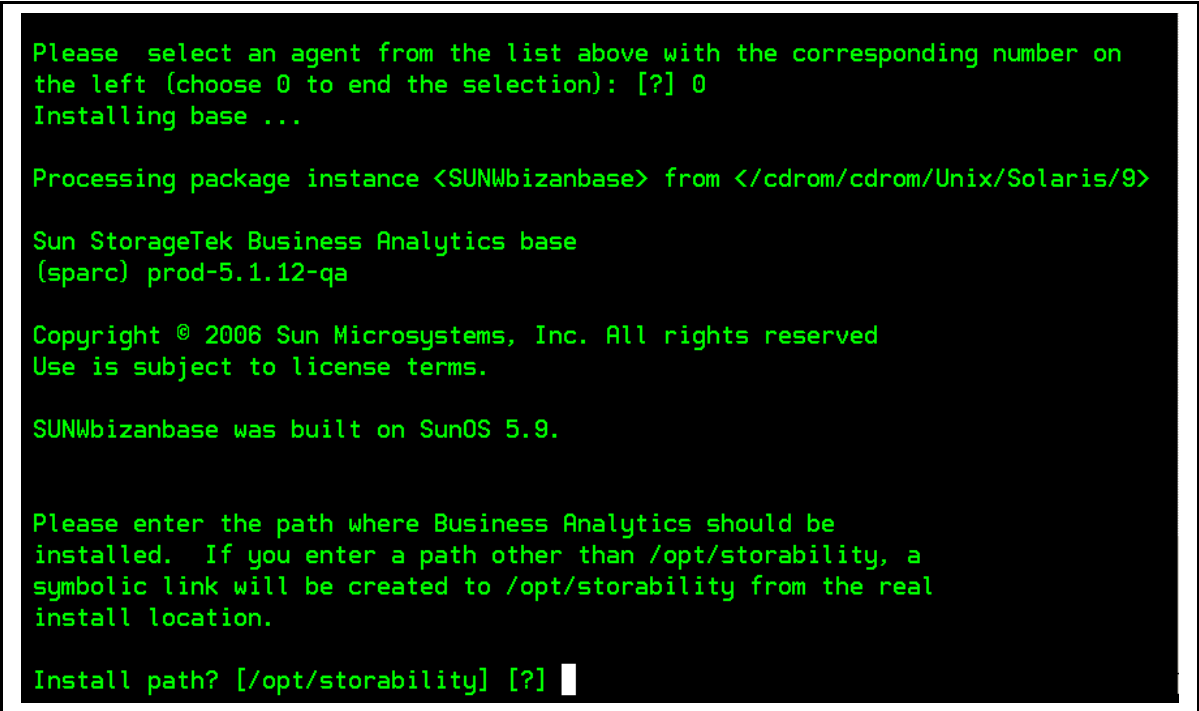
```
. /setup
```



```
I:Agent installed      X:Selected      U:Selected for upgrading

Please select an agent from the list above with the corresponding number on
the left (choose 0 to end the selection): [?]
```

4. As prompted, type the number associated with the agent that you want to install and press Enter.
5. The installation script menu displays a pair of brackets [] to the left of each listed agent and indicates the selection status as follows:
  - The letter, I, indicates the agent is already installed.
  - The letter, U, indicates that the agent will be upgraded.
  - The letter, X, indicates that the agent will be newly installed.
6. Type zero (0) and press Enter to complete the selection. The setup script checks to see if SUNWbizanbase is installed. If not, the installation automatically begins.



```
Please select an agent from the list above with the corresponding number on
the left (choose 0 to end the selection): [?] 0
Installing base ...

Processing package instance <SUNWbizanbase> from </cdrom/cdrom/Unix/Solaris/9>

Sun StorageTek Business Analytics base
(sparc) prod-5.1.12-qa

Copyright © 2006 Sun Microsystems, Inc. All rights reserved
Use is subject to license terms.

SUNWbizanbase was built on SunOS 5.9.

Please enter the path where Business Analytics should be
installed. If you enter a path other than /opt/storability, a
symbolic link will be created to /opt/storability from the real
install location.

Install path? [/opt/storability] [?] █
```

Figure 65 - SUNWbizanbase Installation

7. Press Enter to accept the default install path (/opt/storability).

8. If you want subsequently installed agents to "Enable Auto Registration Prompt?" Otherwise, type y (default) and press Enter at the . Otherwise, type n and press Enter.
9. At the "Local Manager address for auto registration?" prompt, press Enter to accept the local host. If the Routing Agent to contact is located on a different host, type the host's IP Address or network resolvable name
10. Press Enter to accept the default TCP agent registration port (17146) and continue.

```

Enable automatic agent registration? [y] [y,n,?]

Local Manager address for agent registration? [localhost]

TCP port for agent registration? [17146] [?]

Agents which do not require root privileges will be run under a dedicated
account (by default, username gsm, group gsm).

That user account need not be set up yet, but the group ownership of all
the Business Analytics files requires that the group exist.

```

Figure 66 -SUNWbizanbase Installation Advanced Settings

11. Press Enter to accept the default group agents that do not require root permissions run under or enter another group name and press Enter.
12. Type y and press Enter to have the group created or type n (default) and press Enter to not have it created.
13. Press Enter to accept the default group ID (GID) of 1090 or enter another one.
14. Read the information on agent monitor that can be used to restart agents that have been detected as stopped.
15. Type y and press Enter to have the agent monitor used to restart stopped agents or simply press Enter to not have it used (default).
16. The installation of the SUNWbizanbase package completes and the installation of SUNWbizanlmutil begins.
17. Press Enter to accept the default user (GSM) or enter a different user name.
18. Press y and press Enter to have the user automatically created or press Enter to not have the user created (default).
19. If creating the user, press Enter to accept the default UID of 1090 or enter a different one. The installation of the local manager utilities completes.

## Installing Local Manager – Solaris

The Solaris Local Manager (Routing Agent) is installed using the installation setup script (setup). The installation script will check and, if not already installed, first install the SUNWbizanbase and SUNWbizanlmutil packages. The following procedure is based on the assumption these packages have already been installed.

The Sun StorageTek Business Analytics Local Manager consists of the Routing Agent and a set of utilities. Each Local Manager is added to the application using the Management Console's **Site/Local Manager Administration** menus. The Local Manager ID is configured as the Local Manager's Routing ID in the storability.ini file. Each Local Manager must specify a parent Local Manager in its configuration settings to allow the messaging infrastructure to work properly.

The SNMP Proxy Agent may optionally be installed on a Windows or Solaris Local Manager.

1. Mount the installation CD on the Solaris server. For example:

```
mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /mnt
```

2. Type:

```
. /setup
```

and press **Enter** to launch the installation script. The installation script main menu appears. This screen allows you to select an agent to be installed or upgraded.

3. Type the number (e.g., 3) that is associated with the installing (or upgrading) the Routing Agent and press Enter.
4. The installation script menu displays a pair of brackets [] to the left of each listed agent and indicates the selection status as follows:
  - The letter, I, indicates the agent is already installed.
  - The letter, U, indicates that the agent will be upgraded.
  - The letter, X, indicates that the agent will be newly installed.
5. Type the number of the zero (0) and press Enter to proceed with the new or upgrade installation of the Business Analytics Routing Agent.
6. When prompted, enter the unique integer value to identify the Local Manager. Be sure that this RID matches the Local Manager ID (e.g., 301) that was created using the Management Console's Site/Local Manager Administration menus.
7. When prompted, type n and press Enter to specify this is not a Central Manager.
8. When prompted, specify the IP address of the Central Manager/Local Manager that will collect the agent data. This is a required parameter for a Local Manager.
9. For Port used to publish tables, specify the TCP port number the Local Manager uses to publish its objects. The default TCP port number is 17130.
10. For TCP Connect Timeout, accept the default time interval (10 seconds) to connect to an agent, which should be fine for most TCP environments.
11. For Data Timeout, this parameter is generally ignored because this value is overridden by a system parameter passed to the Routing Agent by Sun StorageTek Business Analytics clients. The default value is 300 seconds.
12. Type y and press Enter to view/modify the Advanced Settings, which all have reasonable default values:
  - Allow GSM Upstream Messaging – Turns on (true) or off (false) the capability to exchange messages with upstream agents. For the Routing Agent, set this variable to "false", which is the default value.

- Auto Activate Registration – Turns on (true) or off (false) auto registration for this agent. The default value is "true" (enabled).
- Specific Network Interface to Bind to - The value may be an IP address, specified in standard Internet dot ("x.x.x.x ") notation, or a name service resolvable hostname. This option allows you to bind the Routing Agent to a specific network interface in a dual-homed computer, for example. If you do not bind the Routing Agent to a specific network interface, the Routing Agent will bind to all available local interfaces.
- Maximum Number of Incoming Threads – Is used to control the limited pool of threads that handle the incoming connections for agent registrations. The Routing Agent receives registrations on port 17146. The default value is 10.
- ALLOW\_DYNAMIC\_HOST\_RESOLUTION – Specifies whether dynamic host resolution can be performed using Dynamic Name Resolution (DNS). The default value is true. If host name resolution fails because the host has been removed from DNS because of an administrative error, for example, the value can be set to false to avoid a valid partial data set from not being returned.
- Max. Number of Threads – Specify the number of threads to be spawned. A rule of thumb is to set this value to one half the number of immediate sub-agents (number of rows in the gsa\_agent\_register table where rid = RID). This should be set no lower than five (5) and no higher than fifty (50). The default value is ten (10).
- Number of Days Agents Remain Registered - Specifies the maximum number of days an agent can be down and remain registered. Its purpose is to provide a simple mechanism for removing records of agents that are no longer installed. When expired, the sub-agent registration is removed. However, the agent can always re-register if it ever comes back online.
- Agent Registration Cache File – The Routing Agent creates the agent registration cache file you specify at start up.
- License File Name – Is not applicable for a Local Manager.
- License Audit Frequency – Is not applicable for a Local Manager.
- Interval to Poll Agent Meta Table - Specifies how often in seconds to gather agent objects from the configured sub agents.

13. When prompted, confirm the installation of the Routing Agent.

14. The installation of the Routing Agent completes and returns you to the command line.

## Verify Local Manager Functionality

The Sun StorageTek Business Analytics Agent Diagnostic Tool should be used to verify the Local Manager. Proceed as follows:

1. Select Launch Agent Diagnostic Tool from its program folder.
  - a. Wait approximately 30 seconds after the Routing Agent has started to allow it to initialize before querying it with the agent diagnostic tool.

- b. In the **Agent Info** window, enter the IP Address or network resolvable Host Name of the server where the agent is installed in the **ip address/host name** input box.
- c. Set the port to 17146 (or select the Routing Agent from the drop down list of service names).
- d. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.
- e. Select the **gsa\_alerts-3\_1** object and examine the columns for warnings or errors.
- f. Collect the **gsa\_agent\_version-2\_0** object to verify the agent's software release level. Be aware that the output below is for illustrative purposes only; your agent version, time zone, and time zone offset to GMT will be current to your Sun StorageTek Business Analytics software release and geographical location

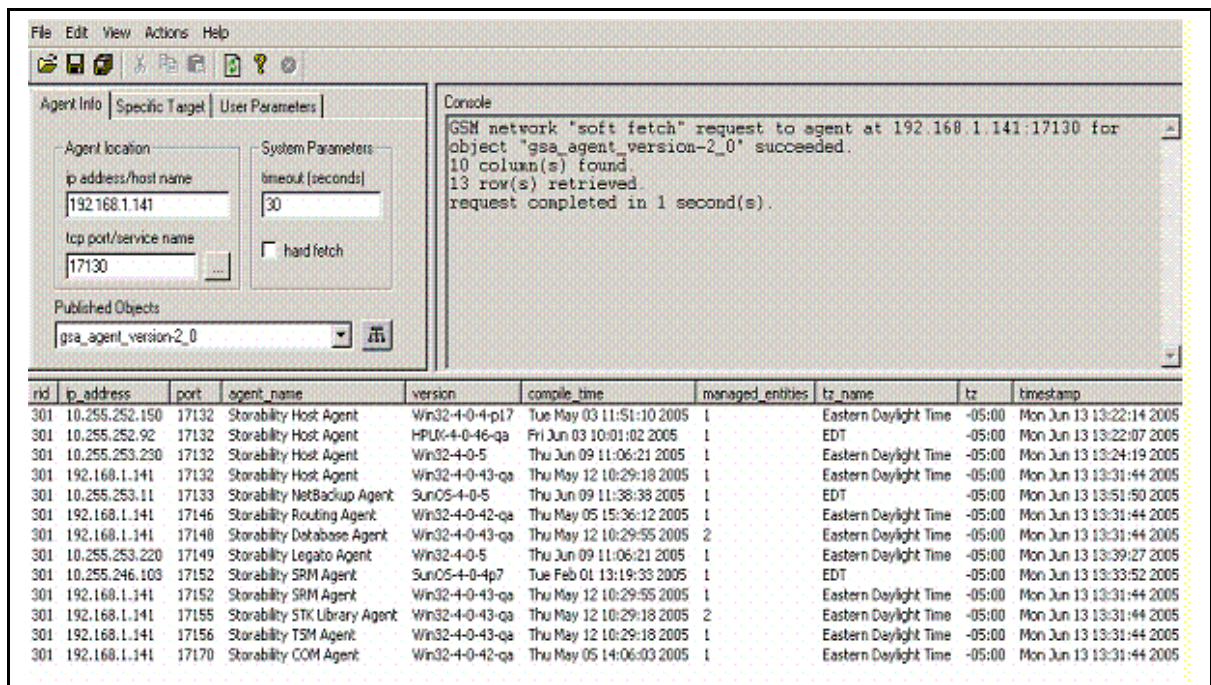


Figure 67 - gsa\_agent\_version-2\_0 Object

- g. Collect the **gsa\_ini\_control-2\_0** object and verify the agent's configuration settings (e.g., RID).

At this point, you may install device (e.g., array) and application agents on the Local Manager. Refer to the Sun StorageTek Business Analytics Agent Installation documentation for instructions on installing different types of Sun StorageTek Business Analytics agents, including the Host Agent, SRM Agent, Array Agents, Backup Agents, Library Agents, and Database Agent.

## Installing the SNMP Proxy Agent on Solaris Local Manager

You may optionally install the SNMP Proxy Agent on a Solaris Local Manager or other Solaris server. Proceed as follows:

1. Open a terminal window on the desktop of the Sun host.
2. Mount the Installation CD in your CD-ROM drive.

3. Change directory to the mount point.
4. Change directory (cd) to the directory corresponding to the host's Operating System. For example: cd /mnt/Unix/Solaris/8.
5. Run the **setup** command to access the main package installation main menu.
6. Select the **SUNWbizanproxy** agent and type 0 to complete the selection.
7. Enter the **IP address** of the SNMP framework system to which SNMP traps will be sent or press **Enter** to specify no additional addresses will be entered.
8. Enter **y** if the system has a peer; enter **n** if it does not have a peer.
9. Enter **y** to modify the administrative settings or **n** to accept the default values. You can modify the UDP timeout value and the retry count used to control attempts to contact the server.
10. Enter a proxy log file name or press **Enter** to accept the default log file name (proxyagent.log).
11. Enter **y** if a NIS master or slave will be contacted for name service lookups or enter **n** to not contact a NIS system.
12. Enter **y** to start agents after the installation.
13. Enter **y** and press Enter to continue installing the Proxy Agent.
14. The installation will complete and return you to the main package installation menu
15. Enter the number for any other package you wish to install, or **q** to quit.

## Agent Monitor

On a Solaris server, the SUNWbizanlmutil package includes the Business Analytics Agent Monitor. The SUNWbizanbase installation script provides the following description of the agent monitor functionality:

*"The agentMonitor script is run from cron to ensure that all configured agents are running. If an agent is down, it will generate an SNMP trap and restart it. If desired, the automatic restart can be suppressed by default or agent by agent."*

Some characteristics of the agent monitor functionality are summarized as follows:

- Is intended to ensure that all configured agents are running.
- Is disabled by default (Automatically restart stopped agents by default? [n] [y,n,?]).
- Checks monitored agents every five minutes if enabled.
- If a monitored agent is down, will attempt to restart that agent and send an SNMP trap to configured SNMP destinations.
- agents files contains list of agents to be monitored and OIDs for SNMP traps
- The monitor.cfg file must be manually edited to set SNMP trap destinations

During the SUNWbizanbase installation, the prompt, "Automatically restart stopped agents by default? [n] [y,n,?]" , is presented. The value (yes/no) you specify becomes

the default “auto restart by Agent Monitor” setting for all subsequently installed Storability agents.

The SUNWbizanlmutil package installation is recorded below.

```
...
SUNWbizanlmutil was built on SunOS 5.9.

...
Agents which do not require root privileges will be run under a dedicated
account (default username gsm, group gsm).
Username for GSM files? [gsm]
user 'gsm' does not yet exist

Automatically create account? [n] [y,n,?] y

UID for gsm? [1090] [?]
Using </app/storability> as the package base directory.
## Processing package information.
## Processing system information.
   8 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <SUNWbizanlmutil> [y,n,?] y

Installing Sun StorageTek Business Analytics <SUNWbizanlmutil>

## Executing preinstall script.
passwd: password information changed for gsm
user 'gsm' created
## Installing part 1 of 1.
/app/storability/bin/bulkAll
/app/storability/bin/inicrypt
/app/storability/bin/trapgen
/app/storability/gsm/.cshrc
/app/storability/gsm/.profile
[ verifying class <none> ]
Modifying /app/storability/bin/agentMonitor
Modifying /app/storability/bin/gsmHB
Modifying /app/storability/etc/monitor.cfg
[ verifying class <build> ]
[ verifying class <cron> ]

Installation of <GSMlmutil> was successful.
```

## Local Manager Utilities Install – crontab Entries

The crontab is updated by the installation of the Local Manager Utilities (SUNWbizanlmutil) as shown below.

```
root@sbolabsol03# crontab -l
#ident  "@(#)root      1.19    98/07/06 SMI"    /* SVr4.0 1.1.3.1    */
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * 0,4 /etc/cron.d/logchecker
10 3 * * 0    /usr/lib/newsyslog
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
# GSM 4.0 Fabric Performance Testing (Paul Kendall)
#0 0,3,6,9,12,15,18,21 * * * /var/tmp/kendall/performance/brcd-to-mcdata.sh
#0,5,10,15,20,25,30,35,40,45,50,55 0,3,6,9,12,15,18,21 * * *
/var/tmp/kendall/performance/brcd-to-brcd.sh
```

```
#0,10,20,30,40,50 1,4,7,10,13,16,19,22 * * * /var/tmp/kendall/performance/brcd-to-
brcd.sh
#30 22 * * 4 /usr/lib/acct/dodisk

# GSMLmutil -- start (do not delete this line)
# Storability agent monitor
#
0,5,10,15,20,25 * * * * /app/storability/bin/agentMonitor > /dev/null 2>&1
30,35,40,45,50,55 * * * * /app/storability/bin/agentMonitor > /dev/null 2>&1
# GSMLmutil -- end (do not delete this line)
```

The crontab is not updated after this initial entry.

## Monitor Configuration

The installation of the local manager utilities creates the monitor.cfg file. The contents of this file are displayed below. This file can be manually edited to set up SNMP trap destinations.

```
root@sbolabsol03# more /app/storability/etc/monitor.cfg
#!/bin/sh
#
# File contains hard coded configuration for agentMonitor script
#
# Parameters include the IP Address to which SNMP traps should be directed
# and an OID entry for each Storability agent process
#
# Created 05/15/01 by P. Cane
# Updated 06/08/01 by D. Butts
#

# Define these here, since multiple scripts use them.
#
snmpTrap () {

SEV=''
if [ -n "$3" ]; then SEV="-s $3" ; fi

for DEST in ${SNMP_DEST_LIST} ; do
    /app/storability/bin/trapgen -d ${DEST} -o "$2.0.1" -v "$2.1" STRING "$1"
${SEV}
done

}

HB_OID=.1.3.6.1.4.1.7509.101.1.3.8
HB_PERIOD=14400
SNMP_DEST_LIST="" ; export SNMP_DEST_LIST
TRAP_HB=""
```

## Agents File

The agents file after the installation of the SUNWbizanlmutil package appears below.

```
root@sbolabsol03# more agents
# Sun StorageTek Business Analytics Agent startup/monitoring configuration
#
# binary          rc-file          OID          AUTO-RESTART    order
```

This file will be updated for each agent that will be monitored.

## Monitor Log

The monitor log file name has the following syntax: monitor.log.yyyymmdd (e.g., monitor.log.20050921). The following sample logged entries show the agent monitor is checking the status of the host agent every five minutes.

```
09/21/2005 09:30:00|7412|hostAgent is running.
09/21/2005 09:35:01|7457|hostAgent is running.
09/21/2005 09:40:00|7480|hostAgent is running.
09/21/2005 09:45:00|7500|hostAgent is running.
09/21/2005 09:50:00|7551|hostAgent is running.
```



## Chapter 2: Upgrading Infrastructure Components

### Upgrade/Uninstall Infrastructure Components

This chapter covers the upgrade installation of the infrastructure components, including the Sun StorageTek Business Analytics Central Manager, Management Console, and Local Manager. When deploying Sun StorageTek Business Analytics Release 5.1 in an existing environment, you must upgrade the following software components:

- Sun StorageTek Business Analytics Management Console
- Sun StorageTek Business Analytics Central Manager Databases

When considering the upgrade of an agent to its latest version, you upgrade agents based on:

- A problem has been fixed in the particular component
- Recommendation by your Sun representative

### Upgrade Central Manager Database

All database upgrade scripts in Sun StorageTek Business Analytics Version 5.1 are written to handle the upgrade from Business Analytics Version 5.0 Service Pack 1 (SP1) to Business Analytics Version 5.1. If you have an installed version of Business Analytics prior to 5.0 SP1, you perform the following two-step procedure:

1. Upgrade the installed databases to Business Analytics Version 5.0 SP1.
2. Upgrade the Business Analytics Version 5.0 SP1 databases to Business Analytics Version 5.1.

#### Notes

- Sun StorageTek Business Analytics was previously called Global Storage Manager (GSM).
- Terminate running all virus scan software before you install the Business Analytics Central Manager, Management Console, or Local Manager software.

### Infrastructure Components Upgrade Summary

Follow these steps:

1. Backup the assurent and portal databases, storability.ini, and config\_srm.xml files.
2. Insert the Central Manager CD and select a Custom Installation. Choose Database setup and the Smart Agents to be installed. When prompted, select Upgrade Database.
3. Reconfigure the SRM agent using the Configuration Tool.
4. Manually copy any customized SRM files back into the Storability SRM Agent directory
5. On the Management Console machine, backup any files that may have been customized.
6. Uninstall Management Console.
7. Insert the Management Console CD into the CDRom drive and install the Sun StorageTek Business Analytics 5.1 version of Management Console.
8. Update device Smart Agents as required.

9. Configure/verify the database batch jobs (e.g., Extract, Transform, and Load or ETL) in DB Batch Jobs under Database Administration.

**Note:** If an SRM agent was installed from the Central Manager Installation CD, you should uninstall the SRM Agent and reinstall it using the Sun StorageTek Business Analytics Release 5.1 Central Manager Installation CD.

## Central Manager Software Upgrade Summary

To upgrade the Central Manager, proceed as follows:

**Notes:** Please make sure you have a backup of your existing database before running the Sun StorageTek Business Analytics Central Manager Database Upgrade.

1. Create a temporary "Backup" directory and backup the following configuration files to the directory:
  - storability.ini
  - ardb.dat (GSM 4.0/5.0 to Sun StorageTek Business Analytics 5.1 upgrade only)
  - aggregator.conf (GSM 3.x upgrade only)
  - queryAgent.conf (GSM 3.x upgrade only)
  - license.txt
  - config\_srm.xml (GSM 4.x upgrade only)
2. If applicable, uninstall the Sun StorageTek Business Analytics Central Manager Agents. As previously stated, you only need to reinstall a Central Manager Agent if a program has been fixed or a new, desired feature is provided. Otherwise, proceed directly to the next step in the procedure.
  - a. Select **Start->Programs->Storability->Uninstall->Uninstall Central Manager**. The InstallShield Uninstall Wizard is launched and a dialog box appears allowing you to select agents to be uninstalled.
  - b. Click the selection box for each listed agent you want to uninstall. A check mark appears in each selection box you choose.
  - c. Click **Next>** after you have selected the agents to uninstall. The Question "Do you want to continue with the Uninstall?" dialog appears.
  - d. Click **Yes** to continue (or No to terminate the uninstall procedure). After you choose **Yes** on the agent to uninstall dialog, a splash box will appear informing you of each selected agent that is being uninstalled.
  - e. When the **Maintenance Complete** dialog appears, click **Finish**.
3. Backup the Database Files:
  - a. Stop MSSQL Server Service using the Windows Control Panel **Services** interface.
  - b. For SQL 2000 Server, locate <drive>: x:\Program Files\Microsoft SQL Server\MSSQL\Data\.
  - c. Copy the following to the temporary "Backup" directory:
    - assurent.mdf
    - assurent\_log.ldf
    - portal.mdf
    - portal\_log.ldf

4. Start MSSQL Server Service using the Windows Control Panel **Services** interface.
5. Insert the Sun StorageTek Business Analytics 5.0 Central Manager Installation media into the CD-ROM drive.  
**Note:** If the Setup program does not auto-run after you insert the CD into the drive, run **setup.exe** from the installation media to start the InstallShield Wizard.
6. The Software License Agreement Dialog Box appears.
7. Accept the terms of the License agreement by clicking **Yes** to continue.
8. The **User Name** and **Company Name** screen appears. Review/change the informational User Name and Company Name fields and click **Next>** to continue.
9. Click **Next>** to install Central Manager to the default Destination Folder (or click **Browse** to change to where the previous GSM installation is located).
10. On the **Setup Type** dialog, use the radio button to choose **Custom**. A menu appears that allows you to customize the components you upgrade.
11. On the "Select features to be installed" dialog, select the GSM Application Component and the features to be installed and click **Next>** to continue.

**Note:** If you are upgrading from an installed GSM 4.0/5.0 version to Sun StorageTek Business Analytics 5.1, you only need to upgrade software components to fix problems or add features.

The **Typical** installation option installs/upgrades the following components:

- **Database Setup** – Creates the Business Analytics databases, tables, and installed procedures for first-time installation.
- **Aggregator Agent** – Aggregates collected data from Smart Agents into the assured database.
- **Routing Agent** – Uses the agent registration table to allow it to activate, deactivate, and collect data from configured GSM Smart Agents. For an upgrade, the Routing Agent's selection box is disabled as the agent must be installed/upgraded.
- **Scheduler Agent** – Is used to support the scheduling of data collection from the deployed agents and policy execution.
- **Data Polling Agent** – Validate data collection schedules and works with the Scheduler Agent to support data polling.
- **Policy Agent** – Executes policies that are configured and scheduled through the Management Console's **Policy Alerting** menus. In addition, the Policy Agent is responsible for the execution of the DB Batch Jobs, such as the ETL process that updates the tables used by the Storage Wizards.
- **Host Agent** – Provides information on host servers, including HBA configuration, operating system, and file system details.
- **Remote Host Agent** – Provides information on remote host servers supporting either the WMI or WBEM protocols.
- **Scheduled Jobs** – Adds the GSM scheduled job to the Windows Scheduler. This option should be selected if you also selected **Database Setup**.
- **License Agent** – Installs the License Agent used to support the audit license report.

The **Custom** installation allows you to additionally install/upgrade the following agent(s) by clicking on their respective selection box:

- **SRM Agent** – Provides disk usage statistics about volumes, files, and directories on a host; option is disabled unless the Host Agent has been selected.

- **Proxy Agent** – Supports sending/receiving SNMP traps; is required to utilize the Real Time Events report in conjunction with the Storability NetBackup Agent.
  - **Remote Host Agent** - Provides an interface to collect data from different Windows servers through the Windows Management Instrumentation (WMI)/Web Based Enterprise Management (WBEM) protocol.
12. Review the Components to be installed in the **Current Settings** dialog.
  13. If you want to review or change any settings, click **<Back**. If you are satisfied with the settings (selected features), click **Next>** to continue.
  14. Choose the "Upgrade Existing GSM Databases and Users?" option on the installation type dialog.
  15. Click **Next>** to continue with the GSM Database upgrade.
  16. The **Enter Database Connection Details** dialog appears. Review/modify the following:
    - **User ID**: Specify a database user/administrator ID that possesses administrative privileges to the assured and portal databases.  
**Note:** If the Database Administrator has removed permissions from the account (e.g., assured), the upgrade can fail because of insufficient database access permissions.
    - **Password** – Enter the above user's password.
    - **IP Address** - Review/modify the IP address of the database server. The default IP Address of the SQL database server is 127.0.0.1 (loopback).
    - **Port** – Review/modify the TCP port number to connect to Microsoft SQL Server . The default TCP Port Number is 1433.
  17. Click **Next>** to continue and the "GSM Database Portal, Assured, and their Schemas are currently present" dialog appears.
  18. Select "Upgrade the Existing GSM Database and Users? " and click **Next>** to continue.
  19. The GSM Database Upgrade version check dialog appears. It shows the currently installed database version and the database version associated with your Sun StorageTek Business Analytics Central Manager. Click **Yes** to continue with the upgrade or **No** to quit installation.
  20. The upgrade installation proceeds. A status command window appears to show the progress of the upgrade installation. An example is shown in the following figure.

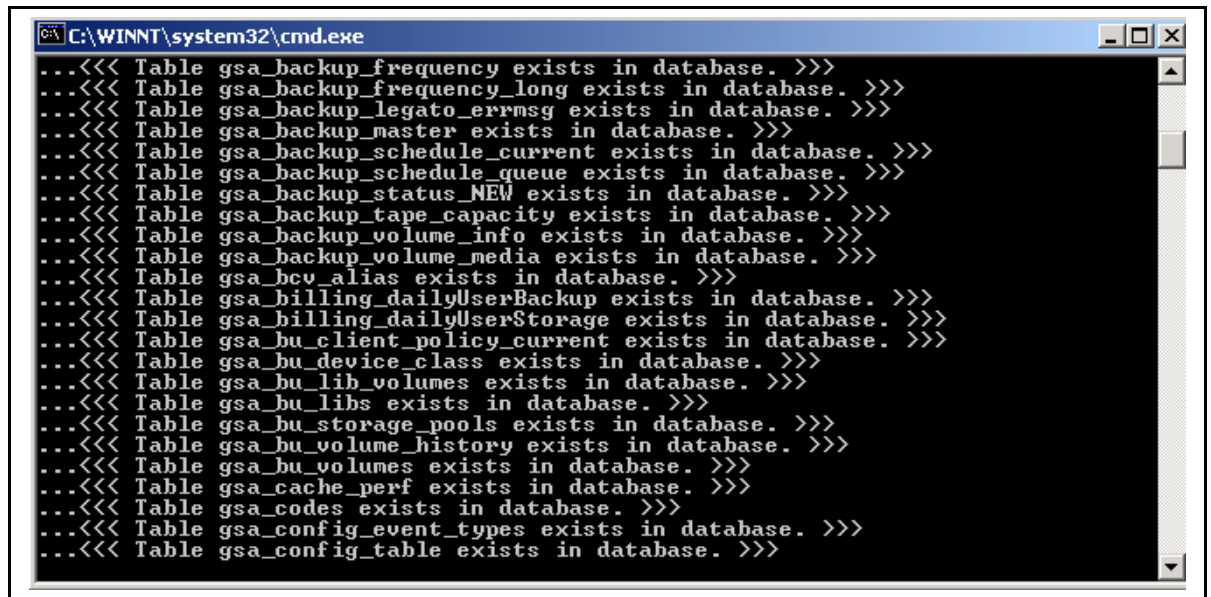


Figure 68 – Database Upgrade Messages Command Window

21. After the database setup has completed, the Scheduled Jobs are being installed dialog appears.
22. The Central Manager message/log files were located dialog appears. It prompts you to specify whether (yes/no) to have the installation delete these files?

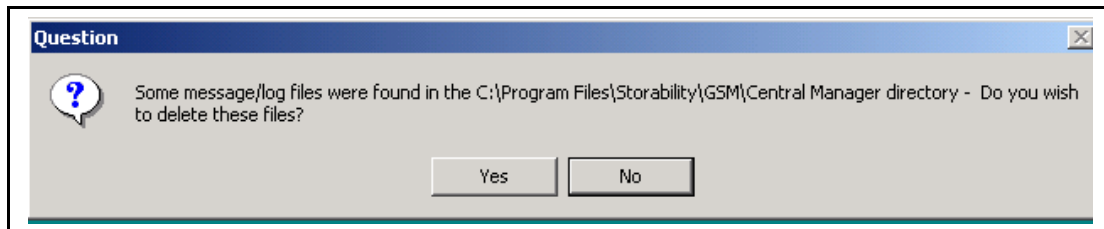


Figure 69 - Delete Central Manager Message/Log Files

23. Click **Yes** to allow the files to be deleted or **No** to retain them and the installation continues.
24. The Upgrade Aggregator Agent Upgrade Dialog Box appears. Click **OK** to upgrade the Aggregator Agent. If running, a dialog appears that specifies it will be stopped.
25. The Delete Previous Aggregator Message/Log files dialog appears. Click **Yes** to allow the files to be deleted or **No** to retain them and the installation continues.
26. The installation will prompt with a splash box as each Central Manager agent is installed. For example, the installation splash box for the License Agent appears below.

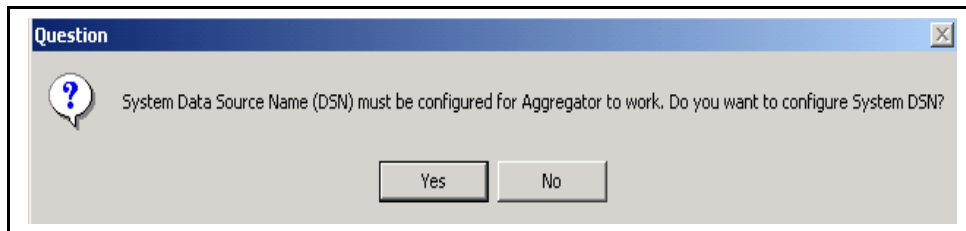


Figure 70 - Installing License Agent Splash Box

27. The Microsoft Disk Management Diagnostic Utility (DMDiag.exe) dialog appears as part of the Host Agent installation. Click **OK** to acknowledge the informational dialog box regarding the Microsoft Disk Management Diagnostic (DMDiag.exe) utility and to

continue. Reporting on dynamic disks only is affected by the availability of this Microsoft disk utility.

28. The Host Agent Upgrade Dialog Box appears, if applicable. Click **OK** to upgrade the Host Agent.
29. The Delete Previous Routing Agent Message/Log files dialog appears. Click **Yes** to delete these files.
30. The Installing SRM Agent pop-up dialog box appears (if you selected to optionally install this agent on the Central Manager).
31. The Install Configuration Tool dialog appears. The Configuration Tool is installed and minimized on your desktop.
32. The Create System Data Source (DSN) for the Aggregator to work dialog appears. Click **Yes** to create the System Data Source that the Aggregator uses to connect to the database. The System Data Source Name is atlantis.



**Figure 71 - System Data Source Name for Aggregator**

33. When the "What type of Central Manager GSM Database are you using?" dialog appears, choose the Database Type (default is SQL) that you previously installed and click **Next>** to continue.
34. The "Where is your GSM Database located?" dialog box appears. The values are described as follows:
  - DSN Name: atlantis
  - UserID: User ID of SQL Server administrator
  - Password: Above user's password (appears as asterisks)
  - IP Address: IP address of database server; the default value is 127.0.0.1
  - Port: SQL Server Port Number; default value is 1433
35. Click **Next>** to continue.
36. Click **OK** when the informational Dialog Box appears indicating the System DSN Configuration is complete.
37. Click **Finish** in the InstallShield Wizard Complete for Central Manager dialog box. The Readme file will be briefly displayed and minimized, if the check mark in the "Launch the Readme" checkbox was not removed before you clicked **Finish**.
38. The Configuration Tool is opened. You can proceed to configure your Central Manager Agents or select **File->Exit** to close the Configuration Tool. Refer to the *Configure the Central Manager Agents* section in **Chapter 1: Installing GSM Infrastructure Components** to obtain instructions on configuring the Central Manager Agents (e.g., Routing Agent).

### Using the aggconvert Utility

The aggConvert Utility (aggConvert.exe) is run after a successful database upgrade from GSM Release 3.6.x to GSM Release 4.0. Unless you are updating a GSM 3.x installation, you can skip this step.

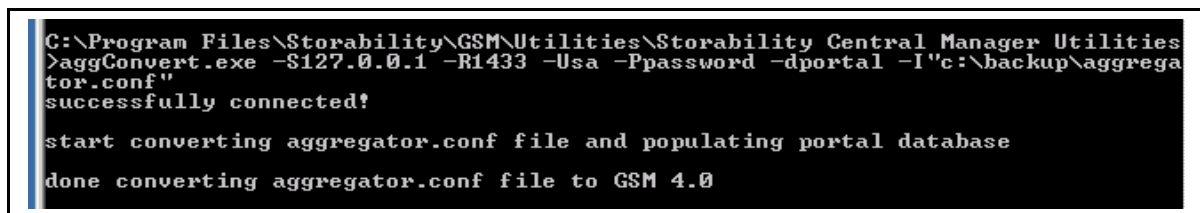
This utility reads and parses a specified GSM Release 3.6.x Aggregator Configuration file (aggregator.conf), and then it uses its configuration settings (e.g., Frequency) to populate four tables in the portal database:

- gsa\_jobs
- gsa\_job\_steps
- gsa\_job\_schedule
- gsa\_time

These tables are empty (no seed data) after the database upgrade has completed successfully. The command syntax for running aggConvert.exe is described as follows:

```
aggConvert -S {sql server ip} -R {Port Number} -U{user name} -P  
{password} -d portal -I{path_to_aggregator.conf}
```

An example of running the aggConvert utility is shown below.



```
C:\Program Files\Storability\GSM\Utilities\Storability Central Manager Utilities  
>aggConvert.exe -S127.0.0.1 -R1433 -Uasa -Ppassword -dportal -I"c:\backup\aggrega  
tor.conf"  
successfully connected!  
  
start converting aggregator.conf file and populating portal database  
  
done converting aggregator.conf file to GSM 4.0
```

Figure 72 - Running Aggregator Convert Utility

The quotation marks are required when you specify the fully qualified path to the Aggregator Configuration file (aggregator.conf).

To convert your GSM Release 3.6.x Aggregator Configuration file, proceed as follows:

1. Copy your Aggregator Configuration file (aggregator.conf) to the location of the aggConvert utility.
2. From a DOS command prompt, run aggConvert using the following syntax:

```
aggConvert -S {sql server ip} -R {Port Number} -U{user name} -P  
{password} -d portal -I{path_to_aggregator.conf}
```

3. Using ISQL utility or other SQL Query interface, verify the following tables in the portal database have been updated with new rows:

- gsa\_jobs
- gsa\_job\_steps
- gsa\_job\_schedule
- gsa\_time

Using gsa\_proc\_views\_users\_40\_upg.sql

**Note:** Unless you are updating a GSM 3.x installation, you can skip this step.

**If the GSM upgrade was from GSM 3.x to GSM 4.0,** use

"gsa\_proc\_views\_users\_40\_upg.sql", which is located on the Windows Central Manager installation media under Win32\dbSchema\assurent\reportsp to perform the following:

- Convert the existing 3-6 groups into 4-0 views

- Look up the current site allocation for these groups and add them to the appropriate views
- Look up the current shared host and backup client allocation, and add these records to the allocation tables
- Upgrade the 3-6 users into 5-0 users, and based on their 3-6 group (and child groups), allocate the appropriate views.

**Note:** To undo the database changes this script makes, use the command:

```
"exec gsa_proc_views_users_40_upg 'UNDO' "
```

The undo command will remove all views, view\_allocation and views asset allocations created by the script. However, it will not undo the changes made to the 3-6 portal user table, as the old records are permanently saved in portal.Users\_oldtable.

To use this function, issue the following command on the assurent database:

```
"exec gsa_proc_views_users_40_upg".
```

**Note:** Refer to the Administration chapter to obtain information on the administrative menus used to fully configure a Sun StorageTek Business Analytics deployment, including dashboards and policy alerting.

## Uninstall Central Manager

The “UnInstall Central Manager” functionality is used to remove any or all Central Manager Software components off of the Central Manager. The procedure will remove the agent’s Windows Registry settings as well as the agent itself.

1. Select **Start->Programs->Storability->Uninstall->Uninstall GSM Central Manager**. The Install Shield Uninstall Wizard is launched and a dialog box appears.
2. Click the selection box for a listed Central Manager agent you want to uninstall. A check mark appears in each selection box you choose.
3. Click **Next>** after you have selected the agents to uninstall. The Question “Do you want to continue with the Uninstall?” dialog appears.
4. Click **Yes** to continue (or **No** to terminate the uninstall procedure).
5. After you choose **Yes** on the agent to uninstall dialog, a splash box will appear informing you of each selected agent that is being uninstalled.
6. When the Maintenance Complete dialog appears, click **Finish**.

## Uninstall Database Setup

The “Uninstall Database Setup” functionality removes the Central Manager databases (assurent and portal) and their features from Microsoft SQL server. Sun StorageTek recommends that you have a current backup of these databases before you proceed.

1. Use the Windows Services panel to stop all services that access the databases.
2. Select **Start > Programs -> Storability -> Uninstall -> Uninstall GSMDatabaseSetup**.
3. The “Do you want to remove GSM Data Setup and all its features?” dialog appears.
4. Click Yes to proceed (or No to abort the procedure) and the Enter Database Connection Details dialog box appears.

Review/modify the following:

- **User ID:** Specify a database user/administrator ID that possesses administrative privileges to the assured and portal databases. The default user is assured. The assured user's password is st0rage.
- Note:** If the Database Administrator has removed permissions from the account (e.g., assured), the upgrade can fail because of insufficient database access permissions.
- **Password** – Enter the above user's password. The default password for the assured user is "st0rage".
  - **IP Address** - Review/modify the IP address of the database server. The default IP Address of the SQL database server is 127.0.0.1 (loopback).
  - **Port** – Enter the TCP port number for the Microsoft SQL Server database. The default TCP Port Number is 1433.

5. Click **Next>** to continue.

6. The un-installation of the Sun StorageTek Business Analytics databases and features proceeds. A command window opens and provides information on the progress of the operation.

7. When the Maintenance Complete dialog appears, click **Finish**.

## Upgrade Management Console

Proceed as described below to upgrade a previous version of the Management Console. As previously described, observe the following guidelines:

- You must upgrade a GSM 3.x or 4.x Management Console to Sun StorageTek Business Analytics Release 5.1 to use its new report functionality.
- You upgrade an existing GSM 4.x Management Console to the latest Sun StorageTek Business Analytics Release 5.1 version if it fixes a problem or if recommended by your Sun support representative.

**Note:** When the Management Console is uninstalled, the procedure will remove the System DSN, atlantis. When the Management Console was installed on a Central Manager, you need to create the DSN manually to allow the Central Manager agents to use the ODBC System DSN. The ODBC System DSN should be configured as follows:

- DSN Name: atlantis
- Server: 127.0.0.1
- Authentication: SQL Server authentication using login ID and password
- Login ID: assured
- Password: st0rage
- Default database: assured

Proceed as follows:

1. Insert the Management Console Installation media into the CD-ROM drive on the Windows server. If the Setup program does not auto-run after you insert the CD into the drive, run **setup.exe** from the installation media to start the Install Shield Wizard.
2. The Management Console Uninstallation dialog is displayed.

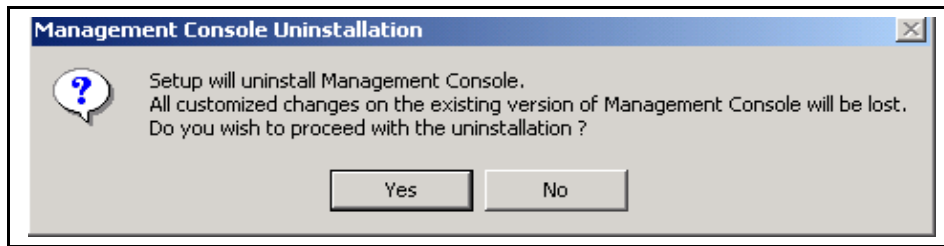


Figure 73 - Management Console Uninstallation Dialog

**Note:** When the Management Console is uninstalled, all customized changes to the existing Management Console are lost.

3. Click **Yes** to continue the uninstallation.
4. The Setup Status splash box appears to show the progress of the operation.

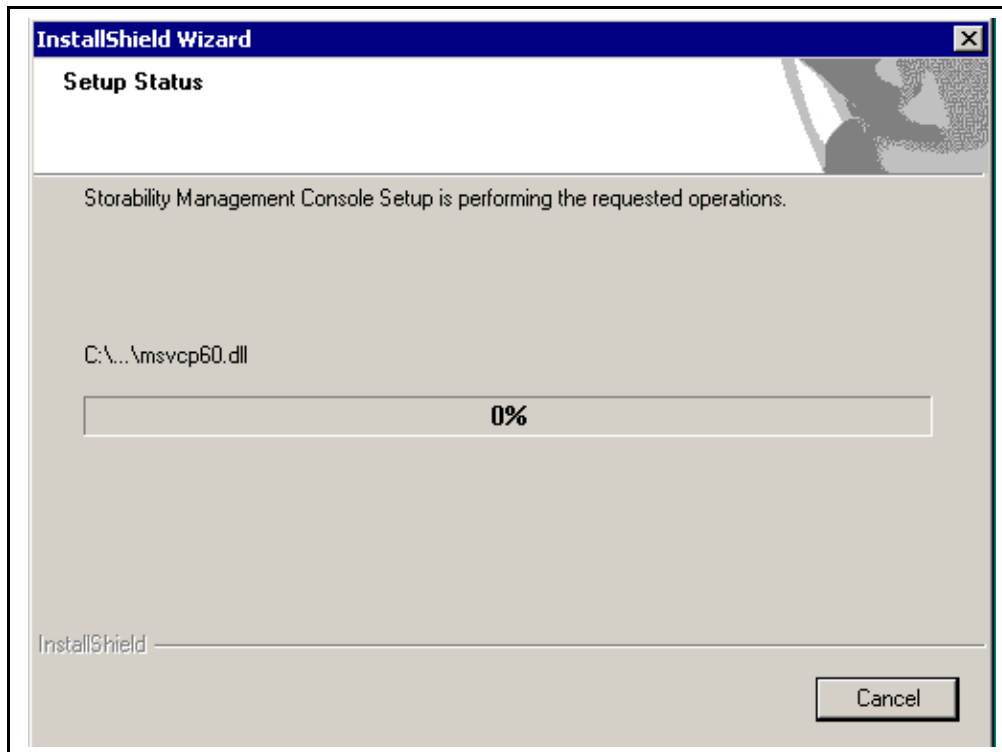


Figure 74 - Management Console Uninstallation Setup Status

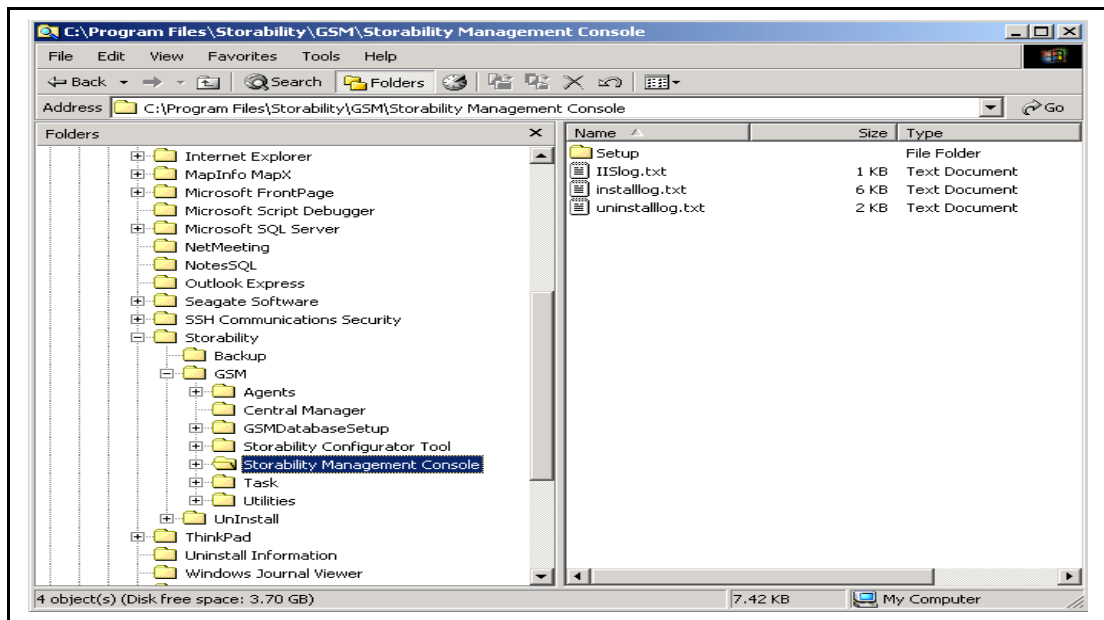
5. When the Install Shield Complete dialog appears, click **Finish**. At this point, you can rerun the Management Console Installation and perform essentially a first-time installation of the Sun StorageTek Business Analytics Management Console.

## Uninstall Management Console

Proceed as described below to uninstall a previous version of the Management Console.

1. Select **Start > Programs -> Storability -> Uninstall -> Uninstall Management Console**. The InstallShield wizard is launched that will guide you through the uninstallation.
2. The Management Console Uninstallation dialog appears. As it indicates, the Management Console Uninstallation removes any existing customized changes to the Management Console.
3. Click **Yes** to proceed or **No** to abort the uninstallation.
4. to continue.

5. If you choose to continue, the **Setup Status** dialog appears. It informs you of the progress of the Management Console.
6. The "InstallShield Uninstall Wizard is complete" dialog appears. Click **Finish** to continue.
7. After the Management Console has been uninstalled, you must manually delete the previously installed version of the Management Console folder/directories.
  - .a Open a **Windows Explorer** window.
  - .b Locate <drive\_letter>:\Program Files\Storability\GSM\Storability Management Console.
  - .c In Windows Explorer, select **File->Delete** to remove the Management Console folder.
  - .d Click **Yes** to continue the Storability Management Console Directory deletion. If a file in use message appears and you are unable to delete the folder, stop IIS and repeat the deleting the folder.



**Figure 75 - Storability Management Console Directory Deletion**

8. A Warning Dialog Box appears. Click **Yes** to continue and confirm the Storability Management Console Folder deletion.

## Upgrade Local Manager – Windows

This section describes how you uninstall a Windows Local Manager in preparation to upgrade that Windows Local Manager to the latest Sun StorageTek Business Analytics software release.

**Warning:** Uninstalling a Local Manager can seriously impact your Sun StorageTek Business Analytics Reporting Implementation. A Local Manager should not be deleted/removed from the application without your fully understanding the consequences to reporting.

1. Select **Start > Programs -> Storability -> Uninstall -> Uninstall Local Manager**. The Install Shield wizard is launched that will guide you through the uninstallation.

2. When the "Select the Agents that you want to uninstall" dialog appears, click (enable) the selection box for the Query Agent or Routing Agent. A check mark appears in the selection box for each agent you have selected.
3. Click **Next>** to continue and the "Do you wish to continue with the uninstall" dialog appears.
4. Click **Yes** to confirm the uninstallation (or No to abort the procedure).
5. Click **Finish** in the Install Shield Wizard Complete dialog to complete the uninstallation.

## Upgrade Local Manager – Solaris

A Local Manager has an installed Routing Agent. If you are not planning to install a new version of the Routing Agent, you may remove the Routing Agent's required packages, GSMbase and GSMImutil (pre V5.1) or SUNWbizanbase and SUNWImutil (V5.1 or higher), as well. If you are removing Sun Business Analytics 5.1 or higher, the "GSM" prefix has been replaced with "SUNWbizan" and the installation script (setup -u) is used instead of the pkgrm command.

**Warning:** Uninstalling the Local Manager Routing Agent can seriously impact your reporting implementation. The Local Manager Routing Agent should not be deleted/removed without fully understanding the consequences to reporting.

1. Create a temporary "Backup" directory on the Solaris server.
2. Copy the Storability Agent Configuration File (storability.ini) to the "Backup" directory.
3. Copy the /<install\_dir>/storability/bin/ardb.dat (agent registration cache file) to the "Backup" directory. It is now available to be restored after the uninstall/re-install procedure for the Local Manager Routing Agent has been completed.
3. Type the following command to remove the Routing Agent package:

```
pkgrm GSMroute (pre Business Analytics 5.1)
setup -u (Business Analytics 5.1 or greater)
```

and press **Enter**.

4. For the pkgrm command, the Currently Installed Package prompt appears. Type **y** and press **Enter** to confirm removing the package. For the **setup -u** command, type the number of the Routing Agent from the list of installed agents and then 0 to specify you have completed agent selection.

The Routing Agent is removed off of the Solaris server. The package removal script completes and returns to the command line.

## Chapter 3 – Troubleshooting

The following sections provide some guidelines for troubleshooting problems with your Business Analytics implementation.

### Device/Application Agents

Proceed as follows.

1. Verify the pre-requisites for the agent have been met. To do so, consult the latest version (exact version including Service Pack) of the Sun StorageTek Business Analytics Support Matrix to verify requirements, pre-requisites, and other notes.
  2. Verify the agent's configuration data is correct, such as the Local Manager IP address, path to required files, and so forth.
    - Windows: Run the Configuration Tool and select the tab for that agent.
    - UNIX: Using a system editor, open the `/opt/storability/etc/storability.ini` file.
  3. Make sure agent has been restarted and is running.
    - Windows: Open the Windows Services panel.
    - UNIX: Run the process status command, `"ps -ef |grep storability"`.
    - Management Console: From Tools, select the Agent Status report under Application Status.
- Note:** The Agent Status alert under Policy Alerting can be used to quickly identify when an agent is not running.
4. By using the Agent Diagnostic Tool and specifying the agent location, verify that the agent is collecting correct information. Agents publish a set of objects that should be populated with data. If the agent's objects are not populated with rows:
    - a. Check the agent's Message.log for CRITICAL, ERROR, and WARNING entries.
    - b. Verify the above Step 1, 2, and 3 are correct.
  5. If there are CRITICAL, ERROR, and WARNING entries but those entries do not on't pinpoint the problem, enable debug mode for the agent to collect more data.
    - a. Add `"LOG_SEVERITY = debug"` between the `# agent start` and `# agent end` section within the `storability.ini` file.
    - b. Restart the agent.
    - c. Allow the agent to run until the problem reoccurs.
    - d. Re-examine the Message.log, which will contain debug entries, prior to the CRITICAL, ERROR, and WARNING entries for detail.
    - e. Re-evaluate whether the agent configuration is correct. If not, verify Step 1, 2, and 3 are correct.
    - f. If data are collected from the agent, verify the messaging infrastructure is working correctly.

# Message Infrastructure

The IP-based, message infrastructure allows agent data to be collected by Local Managers from the device/application agent and forwarded to the Central Manager. Ultimately, the Central Manager Routing Agent provides the collected data to the Aggregator, which is responsible for data insertion into the Central Manager database.

Each Local Manager (including the Central Manager) is a unique instance of a Routing Agent. Proceed as follows.

1. Using the Agent Diagnostic Tool, verify the Local Manager is collecting the agent objects and that they are populated with data. To do so, specify the Local Manager/Central Manager in the ip address/hostname field and port 17130. When examining the returned rows, ensure the rid column contains the expected value (e.g., 301).
2. If the agent objects are empty, proceed as follows:
  - a. Gather and review the Routing Agent Message.log whose default install directory is C:\Program Files\Storability\GSM\Agents\Storability Routing Agent on a Windows server. On UNIX, a single message log is shared by all installed agents.
  - b. Verify the network port is not blocked. Use 'telnet <ip address> <port>'. Verify there aren't any other network issues.
  - c. Verify the Routing Agent has a STATIC/AUTO registration entry for the agent in its gsa\_register object.
3. If the agent objects are populated, move up the messaging infrastructure to the next Local Manager until the Central Manager Routing Agent is reached.
4. If the Agent Diagnostic Tool returns data when pointing to the Central Manager, verify data insertion into the Central Manager database.

## Central Manager Database

The Central Manager Scheduler Agent requests agent objects are collected by the Aggregator Agent. Data collection can occur on a one time (e.g., Collect Now) or scheduled basis. The Aggregator publishes a data collection statistics object (gsa\_data\_collection\_stats) that can be used to verify that (a) agent objects were received and (b) that the appropriate stored procedures successfully updated the database.

1. By using the Business Analytics Agent Diagnostic Tool and specifying the agent location of the Aggregator Agent, collect and then open the gsa\_data\_collection\_stats object. For the agent objects, verify the following:
  - a. Object name
  - b. Target site ID, rid, or host and port
  - c. Date and time of the data request
  - d. Date and time of the data arrival
  - e. Number of rows
  - f. Errors
2. To manually test data collection, proceed as follows:
  - a. Log in to the Management Console.
  - b. Select Tools->Data Polling Schedule to open the Polling window.
  - c. Click the 'Collect Now' button to collect agent objects.
  - d. Repeat the above Step 1 to verify data collection and insertion into the database.

3. If errors are indicated in the rows, there may be a problem with the stored procedure or the database.
  - a. Make sure the database is not suspect or down.
  - b. If you are investigating a performance or blocking issue with the assured database, gather the output for the following SQL commands
 

```
exec sp_who2
exec sp_lock
select id, type, name from sysobjects where type in ('U', 'V') order by id
```
3. If Step 2 works, it's likely to be a report issue. Some checks include:
  - Does the user's current view allow seeing information on the asset (e.g., storage array)?
  - Has the homepage cache been refreshed since the data collection occurred when data is not appearing in a dashboard pane?

## Central Manager Disaster Recovery

It is recommended that you implement a database backup maintenance procedure immediately after you deploy Business Analytics. The Business Analytics databases consist of the assured (report data) and portal (permissions, policies, and schedules) databases.

After a catastrophic failure, a Disaster Recovery procedure for the Central Manager may include the following steps:

1. Re-install the Central Manager using the first time installation procedure that is previously described in the manual.
2. Copy the latest backup of your software license (license.txt) to the Storability Routing Agent folder.
3. Copy the latest backup of the storability.ini file to the <drive>:\Program Files\Storability\GSM\Agents folder.
4. Copy the latest backup of the agent registration database (ar.db.dat) to the Storability Routing Agent folder.
5. If the SRM Agent is installed, copy the latest backup of the config\_srm.xml file to the SRM Agent folder.
6. Run MS SQL Query Analyzer and login as "sa" using sa password.
7. Remove the newly installed assured and portal databases.

```
sp_dbremove 'assured'
```

8. Restart SQL Server so that no users are using the database.

```
sp_dbremove 'portal'
```

9. If the database files, .mdf and .ldf, did not get removed, manually delete these files.
10. Unzip or copy the assured and portal database from your backup directory (e.g., c:\save) to C:\Program Files\Microsoft SQL Server\MSSQL\Data.
11. Attach the assured and portal databases.

```
sp_attach_db 'assured', 'C:\Program Files\Microsoft SQL
Server\MSSQL\Data\assured.mdf', 'C:\Program Files\Microsoft SQL
Server\MSSQL\Data\assured_log.ldf'
```

```
sp_attach_db 'portal','C:\Program Files\Microsoft SQL
Server\MSSQL\Data\portal.mdf','C:\Program Files\Microsoft SQL
Server\MSSQL\Data\portal_log.ldf'
```

## Appendix A: Agent Auto Registration Special Considerations

This appendix explains special considerations related to agent auto registration.

### Auto Registration – Special Considerations for Multi-homed Hosts

One of the features of Sun StorageTek Business Analytics agents is their ability to automatically register themselves with their associated Local Manager. This removes the previously required task of maintaining a list of IP address and port pairs in a configuration file on the Local Manager host machine for each agent. Instead, each agent adds the location of its local manager in its own storability.ini file by using the **GSM\_LM\_HOST** and **GSM\_LM\_PORT** settings and by also setting the **GSM\_ENABLE\_LM\_REGISTRATION** to true.

For example:

```
:hostagent
GSM_LM_HOST = localhost
GSM_LM_PORT = 17146
GSM_ENABLE_LM_REGISTRATION = true
```

When an agent starts up, it will immediately attempt to register itself based on these settings by passing special parameters to the Local Manager Routing Agent (LMRA) via the **gsa\_agent\_register** object published on its upstream port (17146 by default). It will also re-register once every 24 hours.

If the agent's host has multiple network interfaces (is multi-homed), the agent will, by default, bind its data port to all interfaces including the loopback. This does not cause any problems with the auto registration process since the LMRA will register the agent using the interface that the registration request originated from. The Routing Agent does not randomly decide which interface to register.

Although not necessary, forcing the agent to bind only to the interface it needs to communicate with the LMRA can avoid confusion. This is done using the **GSM\_LISTEN\_INTERFACE** ini setting. This configuration setting accepts a resolvable host name or IP address in standard dotted (x.x.x.x) notation:

```
:hostagent
GSM_LISTEN_INTERFACE = 192.168.0.2
```

This configuration setting guarantees that all successful data collections will happen through this interface exclusively, and it ensures that the generic ip\_address field found in many agent objects always contains the same value for the multi-homed host. It will also prevent the agent from binding to the loopback interface, so that data requests using the localhost name are no longer possible. There is also the added benefit of reducing the risk of duplicate host data in the Business Analytics database that is caused by a static SUB\_AGENT setting in a rogue LMRA for one of the other interfaces.

While setting the `GSM_LISTEN_INTERFACE` is generally a good idea for an agent configuration on a multi-homed host, it is most likely not what you want to configure for the Routing Agent. When the LMRA or Central Manager Routing Agent (CMRA) is installed on a multi-homed host, both interfaces are probably needed to route to all sub agents, since agents which share a LMRA do not necessarily need to be on the same subnet.

However, a host may have a second interface for a very specific purpose that is not intended for use by Business Analytics. An administrator may want to make sure that agents do not bind to this interface. In this case, it makes sense to set the `GSM_LISTEN_INTERFACE`. It should be set to the address of the interface used to connect to the LMRA's parent. In the case of a CMRA, it needs to be set to the address of the interface that the Data Aggregator is configured to find it. Unfortunately, there is not a way to bind to a list of interfaces using `GSM_LISTEN_INTERFACE`. It is either all or one. If the bind is restricted to a single interface on a Routing Agent host (LMRA or CMRA), the interface obviously must be the only interface needed for Business Analytics component inter-communication.

## Auto Registration – Special Considerations for Network Address Translation (NAT)

Network Address Translation (NAT) is an IETF standard that allows an organization to present itself to the Internet with far fewer IP addresses than there are nodes on its internal network. The NAT technology, which is implemented in a router, firewall or PC, converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. It changes the packet headers to the new address and keeps track of them via internal tables that it builds. When packets come back from the Internet, NAT uses the tables to perform the reverse conversion to the IP address of the client machine.

The auto-registration completely supports situations where agents live on a different NAT layer than the CMRA or other LMRA. However, there is an important restriction. When using agent->LMRA auto-registration, both MUST be in the same NAT layer. The LMRA of any agent must be on the same side of the NAT layer as itself.

However, there is no such restriction for the Routing Agent. A LMRA and its parent LMRA or CMRA may be separated by a NAT layer without issue. In this case, when there is a registration request from a sub-LMRA, the parent will register the LMRA's downstream port (which defaults to 17130) using the NAT router's address. All agents in this situation will report their NAT address in the generic `ip_address` field of their objects, not the router's address. Also, any NAT layers within a single Business Analytics implementation must have a unique site id. This is why the global agent uniqueness key consists of: IP address, port and site since two NAT layers may have the same address range.

Other questions may include:

- How does the Routing Agent register itself up out of a NAT layer?
- What address should it use for `RA_PARENT`, the router's?
- What if I have a very conservative network administrator?

The NAT layer LMRA should use the parent's normal interface address, not the router's address. Of course, the network administrator of the NAT router needs to allow IP traffic to flow up from the NAT layer to the LMRA or CMRA on the upstream port (which defaults to 17146). If the network administrator does not want to allow this, auto registration needs to be turned off on the NAT layer LMRA (by commenting out the

RA\_PARENT ini setting). In turn, the parent LMRA or CMRA needs to be configured for a static SUB\_AGENT using the NAT layer LMRA's downstream port and the NAT router's address. Unfortunately, this will cause a periodic warning in the NAT layer LMRA's log suggesting that it has no parent and is an orphan. In short, if the network administrator agrees to open the upstream ports, it will make everybody's life easier. However, it is not absolutely required.

**Auto Registration - Special Considerations for Virtual Private Networks (VPNs)**

The administrative considerations for Virtual Private Networks (VPNs) are very similar to those described for NAT layer. Business Analytics works fine with VPN's with the restriction that only the Routing Agents should communicate across them. An agent and its LMRA should not be separated by a VPN. Unlike NAT, VPNs by their nature give hosts an address in the same range as the parent network (unless NAT is also being used, in which case you need to follow those rules), so there is no site id restriction. Also, the VPN needs to be connected before the LMRA is started.