Sun StorageTek™ Business Analytics Installation Guide

Release 5.0 SP1

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6243-10
March 2006, Revision A

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

COPYRIGHT

English:

French:

TABLE OF CONTENTS

CHAPTER 1: INSTALLING INFRASTRUCTURE COMPONENTS

Introduction 4
Central Manager Installation 4
Central Manager Prerequisites 4
Installing Microsoft SQL Server on a Windows Central Manager 6
Installing SQL Server 2000 Service Pack 3 10
Central Manager Installation 13
Install the Software License 21
Configure the Central Manager Agents 21
Smart Agent Configuration 22
Start Central Manager Agents 38
Agent Diagnostic Tool 39
Central Manager Agent Diagnostic (cm-get) Application 41
Verify Central Manager Agent Functionality 42
SNMP Proxy Agent on Central Manager 45
Management Console 46
Install/Verify Microsoft IIS Server IIS 5.0 46
Additional Configuration Settings for Windows 2003 SP1 47
Management Console Configuration 53
Local Manager 60
Add the Local Manager Using the Management Console 60
Installing Local Manager - Windows 61
Installing SNMP Proxy Agent on Windows Local Manager 65
Installing Local Manager - Solaris 66
Installing the SNMP Proxy Agent on Solaris Local Manager 73
Procedure Summary to Upgrade from a Previous GSM Version 77
Central Manager Software Upgrade 78
Using the aggconvert Utility 85
Using gsa_proc_views_users_40_upg.sql 85
Uninstall Database Setup 87
Upgrade Local Manager - Windows 90
Upgrade Local Manager - Solaris 91

APPENDIX A: AUTO REGISTRATION SPECIAL CONSIDERATIONS 90

Introduction

This manual describes the procedures to install, configure, and verify installation of Sun StorageTek Business Analytics 5.0 software infrastructure. There are two types of deployments:

- First time deployment of Sun StorageTek Business Analytics Release 5.0 SP1 software components
- Upgrade deployment of software components from GSM Release 3.6 ,3.8, or 4.0 to Sun StorageTek Business Analytics Release 5.0 SP1

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. The functionality of Business Analytics is identical to GSM, only the name has changed.

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 Storability agents.
- Install the Windows Configuration Tool.

Central Manager Prerequisites

Verify the Central Manager's hardware and software prerequisites that are described in the *Infrastructure Planning Guide.* Your Sun representative can provide the current version of this document.

Note: 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.

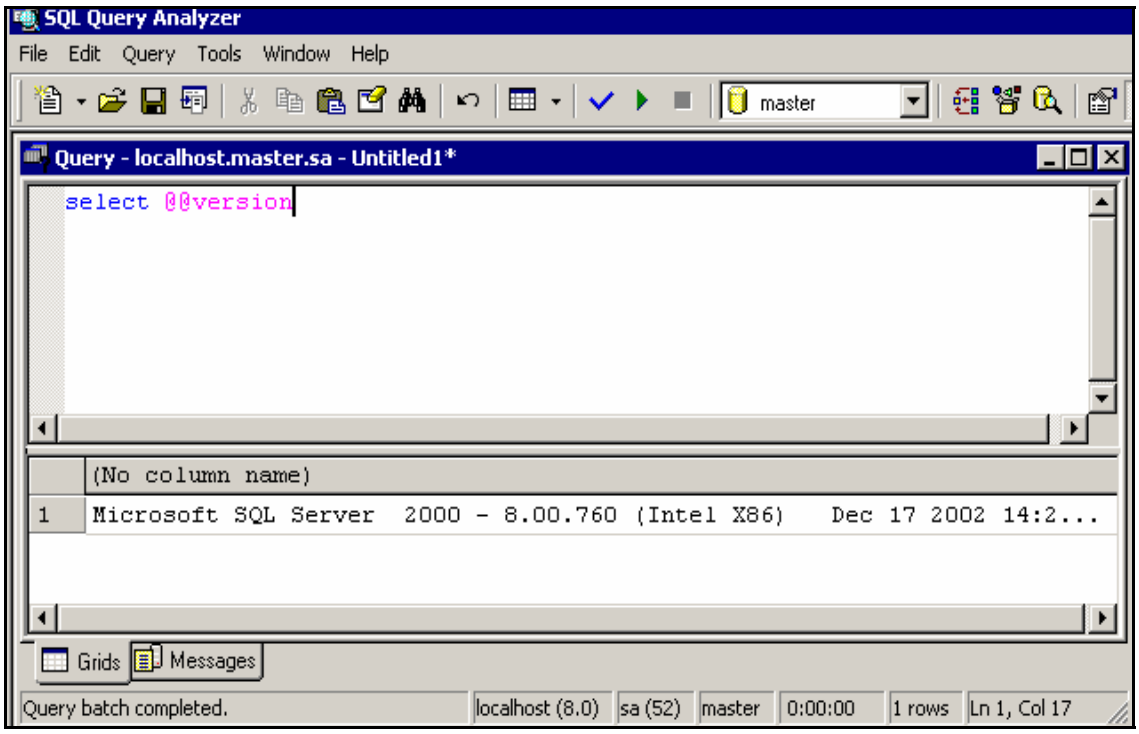


Figure 1 - select @@version

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

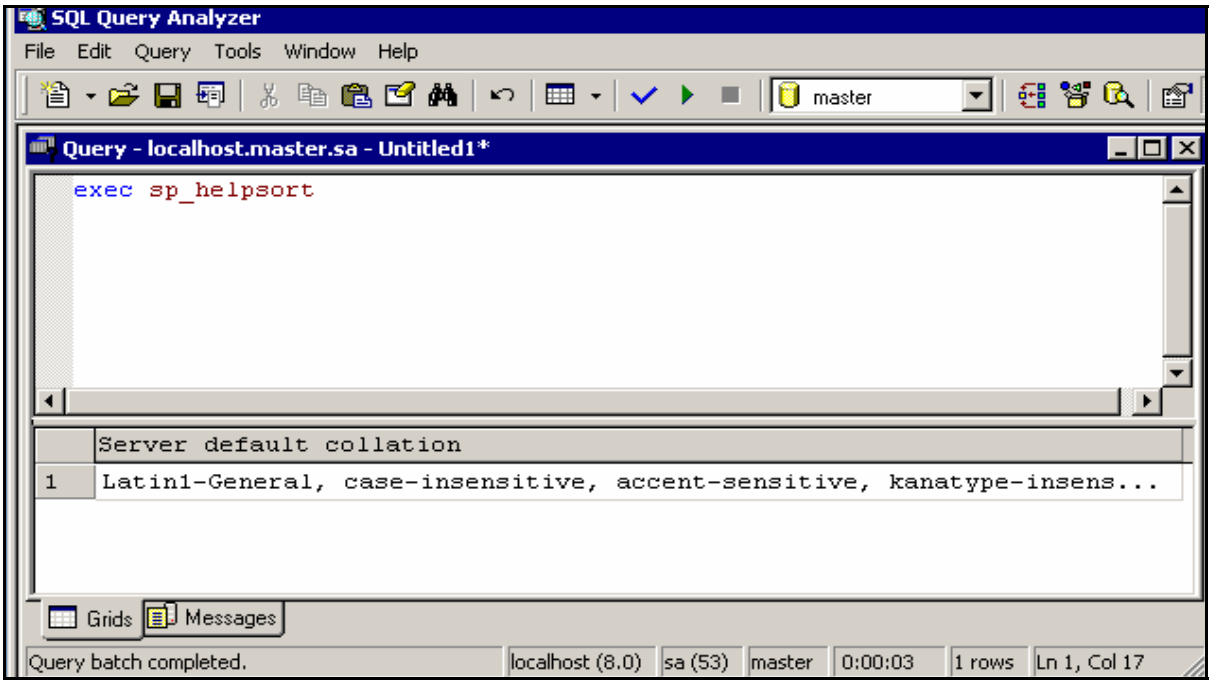


Figure 2 - exec sp_helpsort

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 uses 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.**

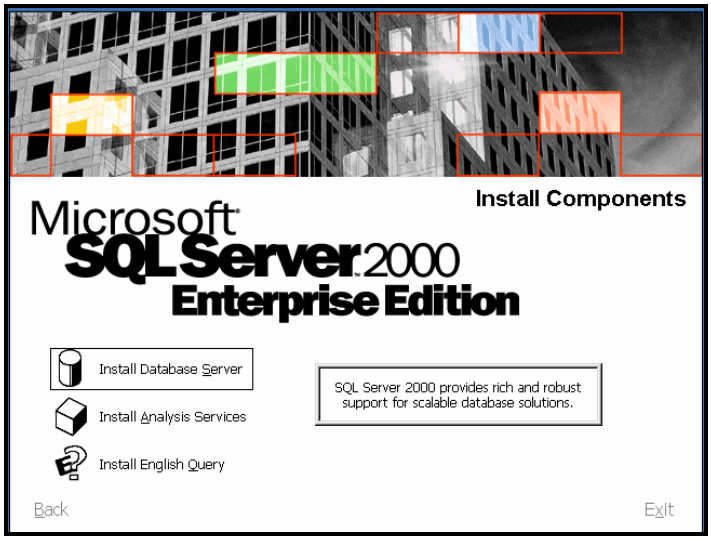


Figure 3 - Install Components Dialog Box

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.

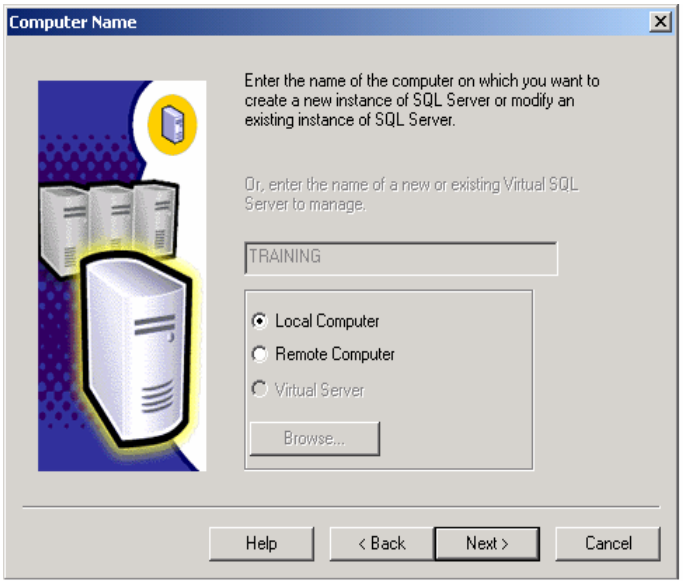


Figure 4 - Computer Name Dialog Box

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

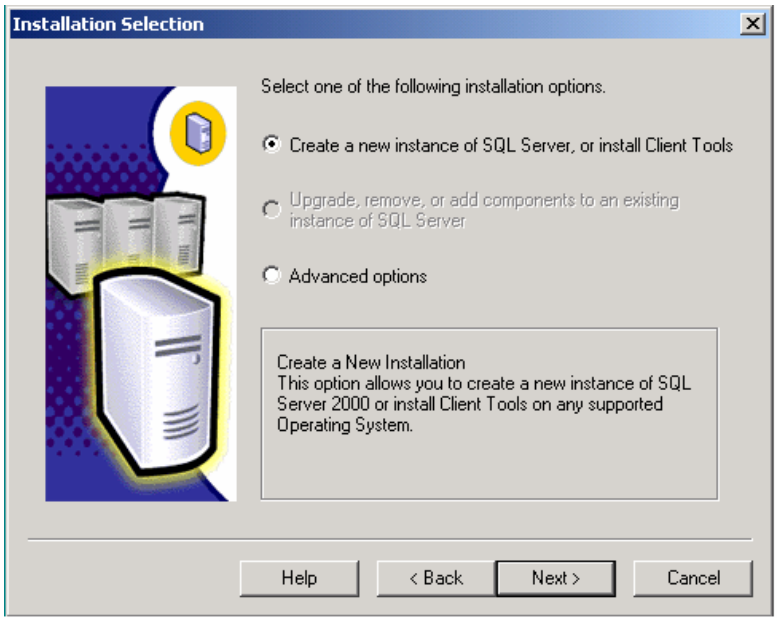


Figure 5 - Installation Selection Dialog Box

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.

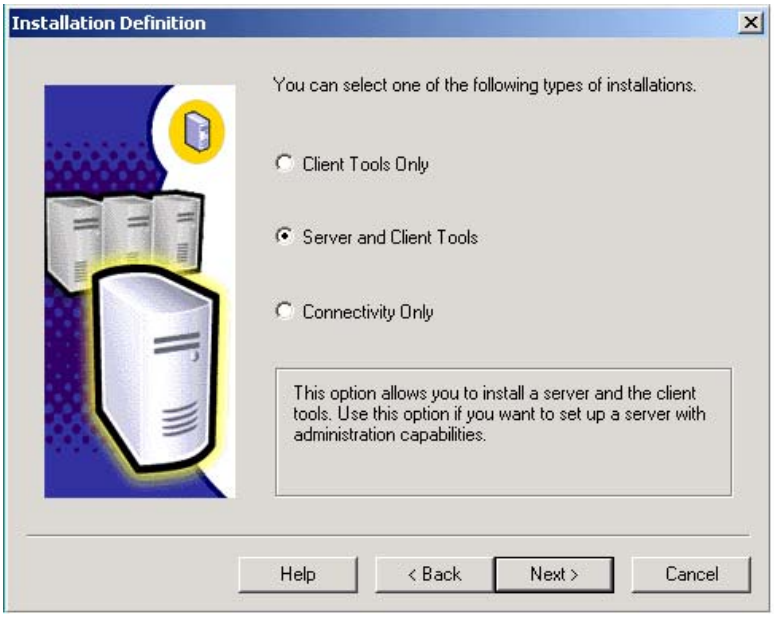


Figure 6 - Installation Definition Dialog Box

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.

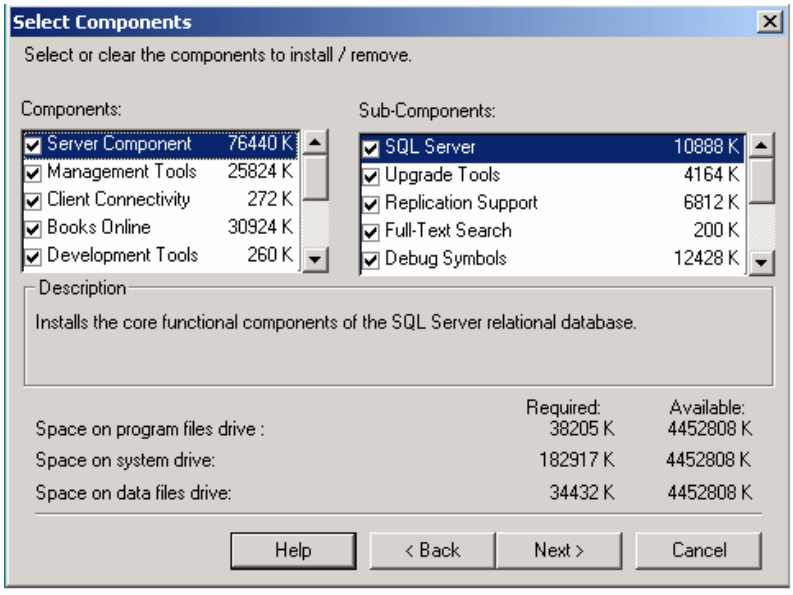


Figure 7 - Select Components Dialog Box

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.

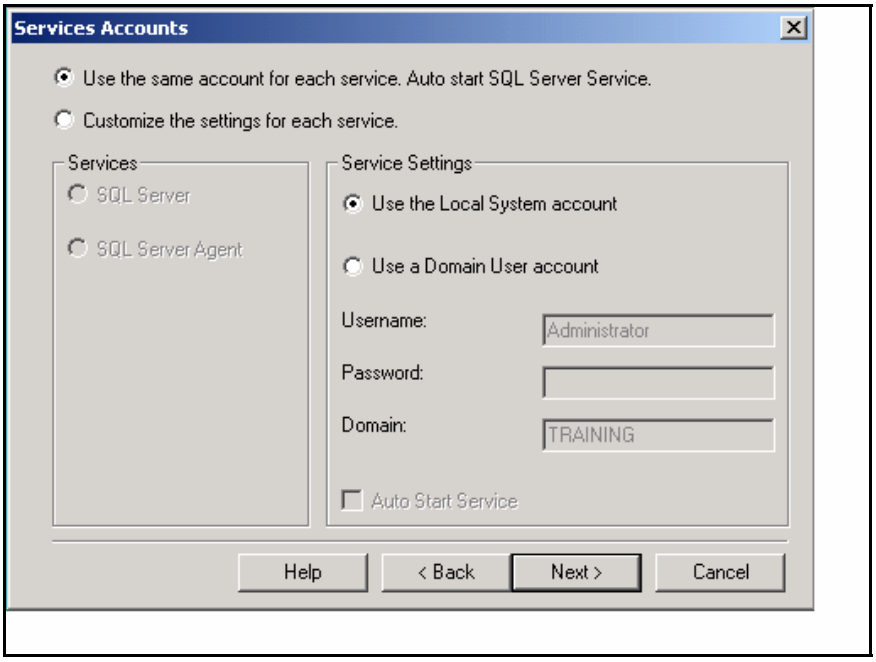


Figure 8 - Service Accounts Dialog Box

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.

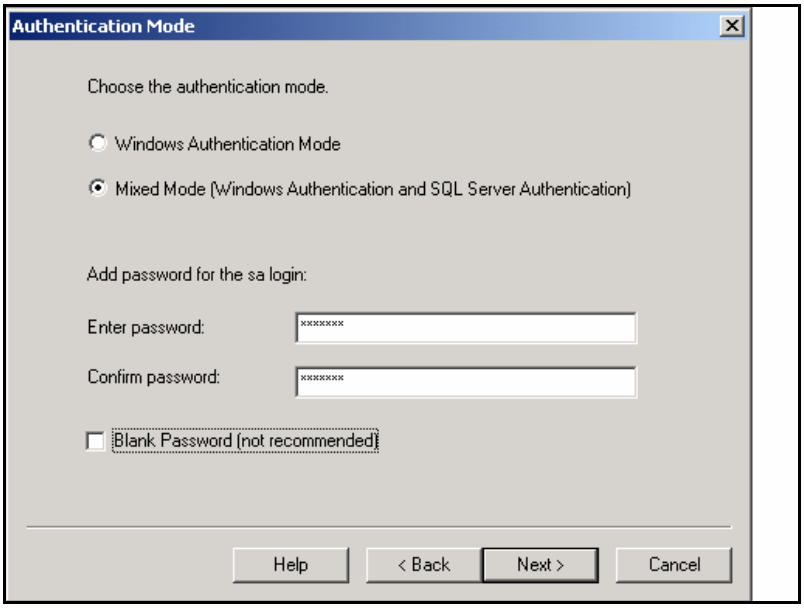


Figure 9 - Authentication Mode Dialog Box

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.

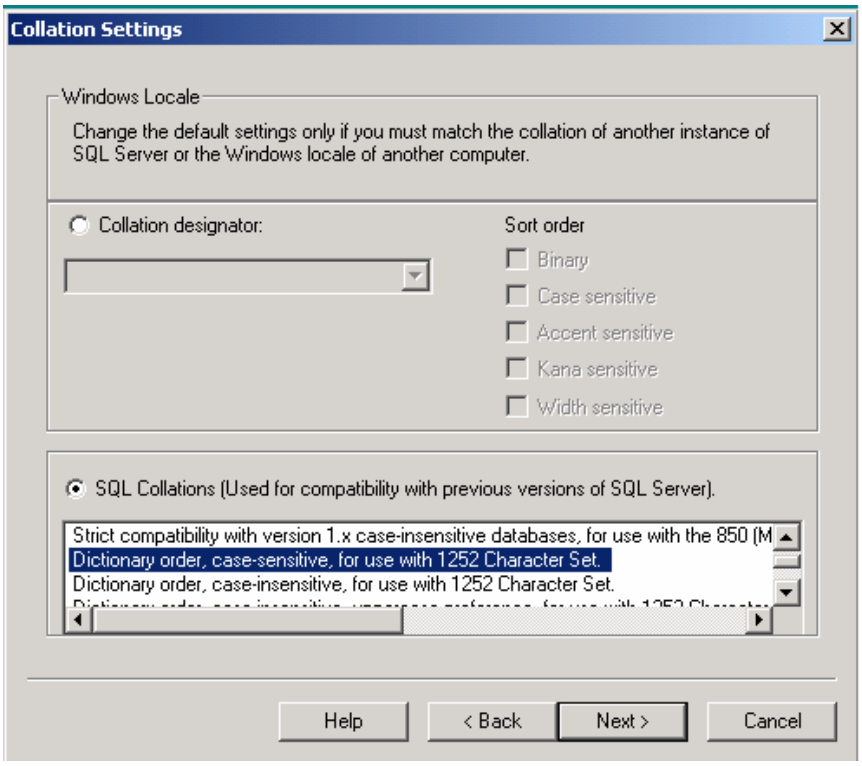


Figure 10 - Collation Settings Dialog Box

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

Table 1 - 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

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.

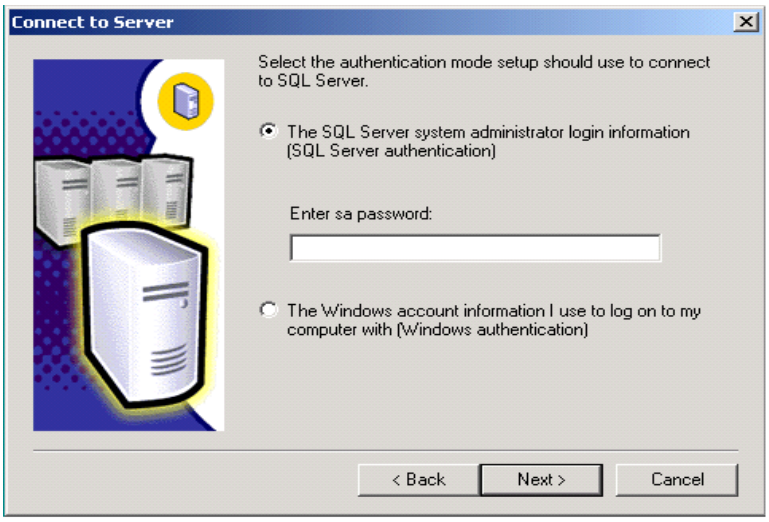


Figure 11 - Connect to Server Dialog Box

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 12 - 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.

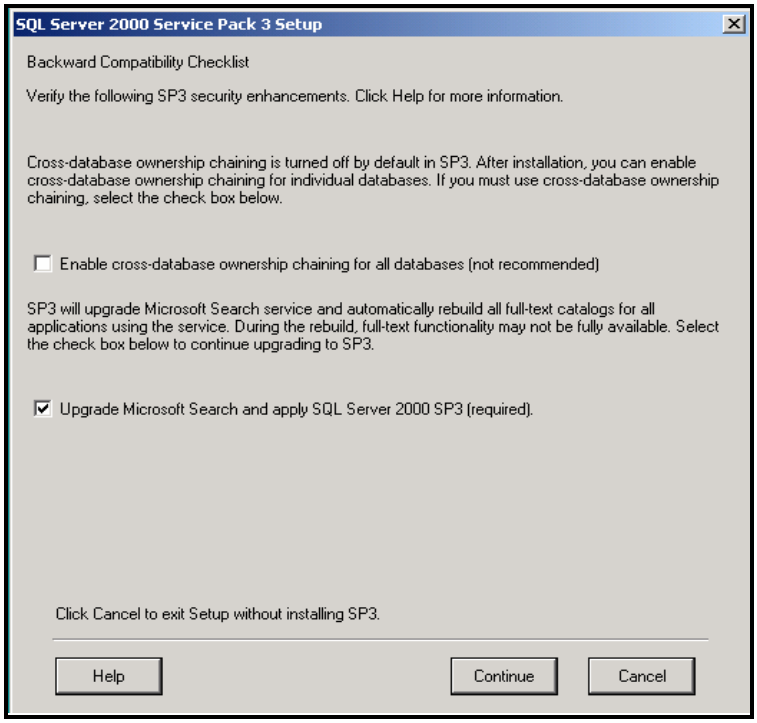


Figure 13 - SQL Server SP3 Setup Dialog Box

6. 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.

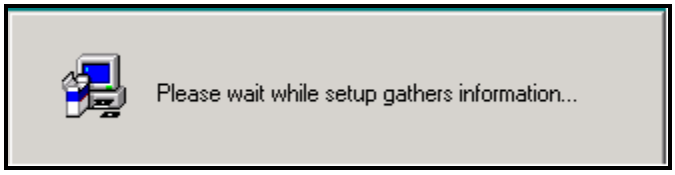


Figure 14 - Gathering Information Dialog Box

7. 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.

8. 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.
9. Reboot the Windows 2000 Server.

Central Manager Installation

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

1. 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.

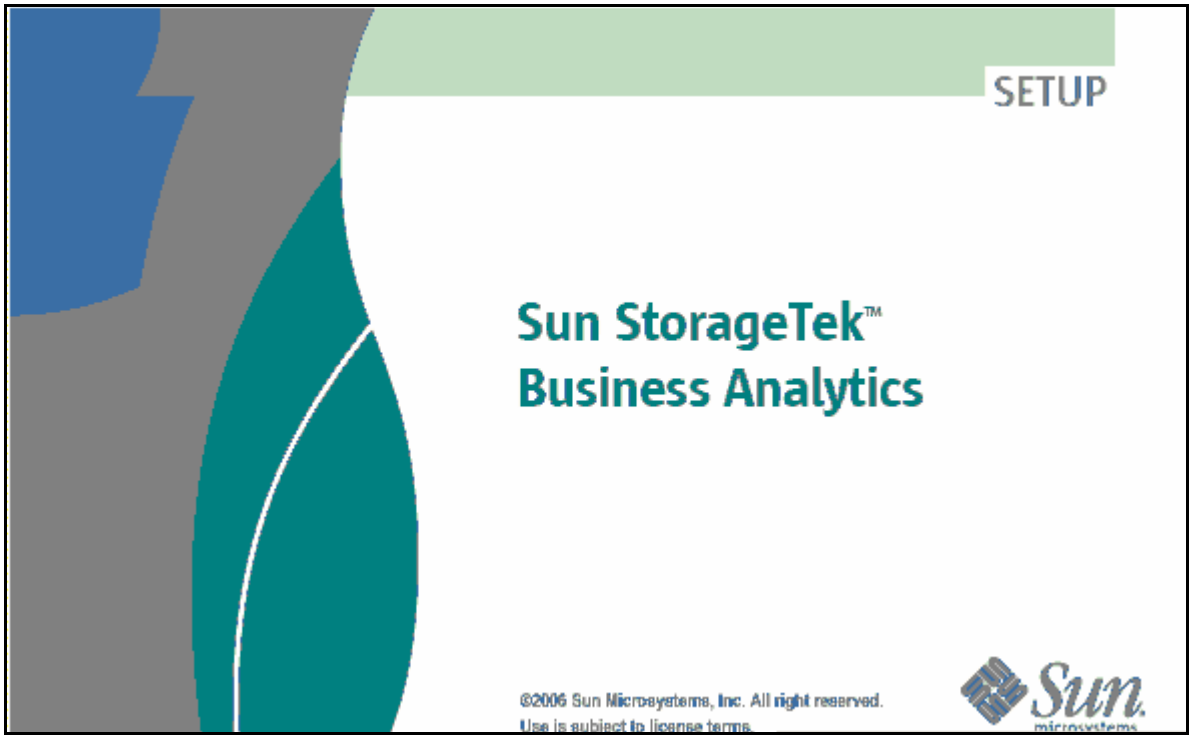


Figure 15 - Central Manager Installation Splash Screen

2. Click **Yes** to accept the terms of the software license agreement.

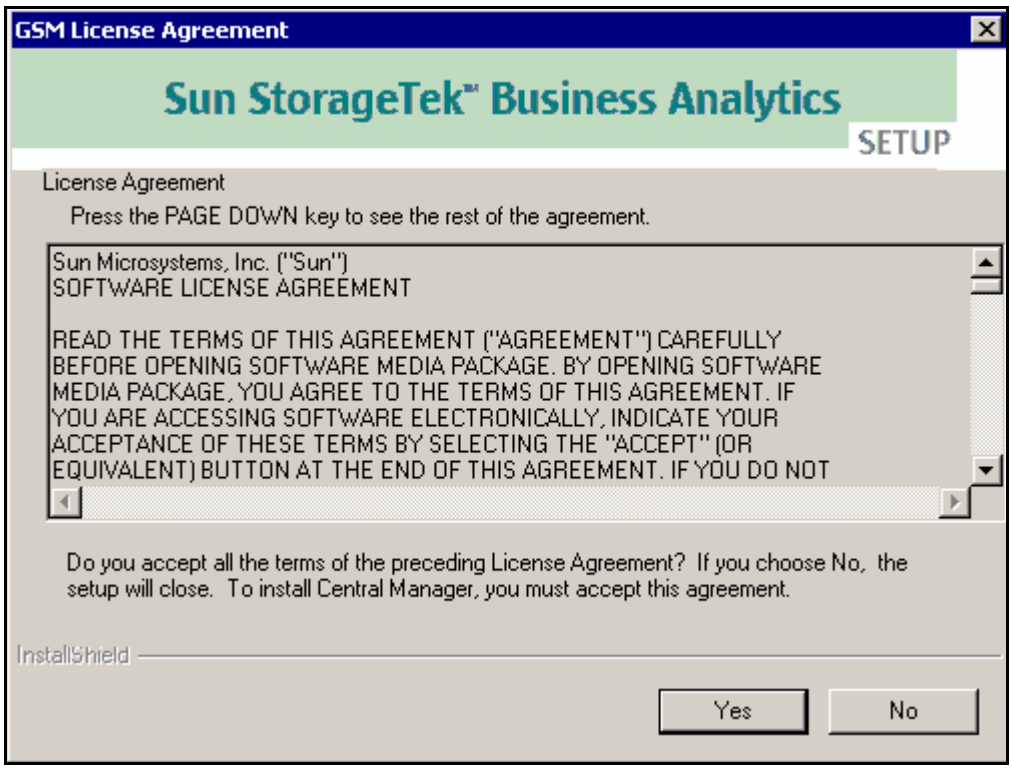


Figure 16 - Software License Agreement

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).

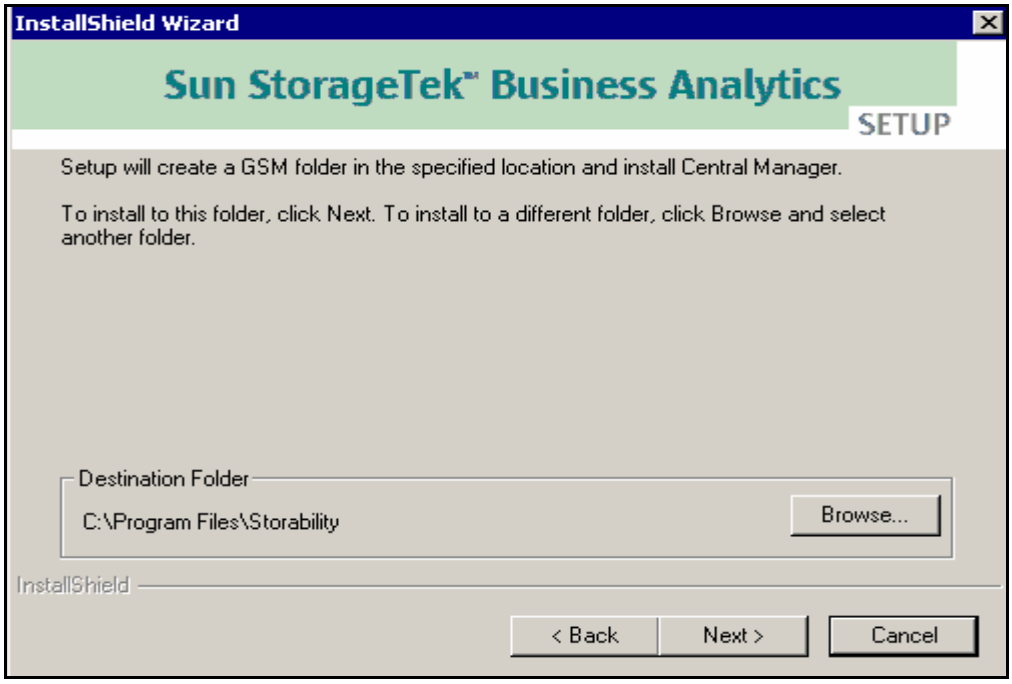


Figure 17 - Select Destination Folder

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

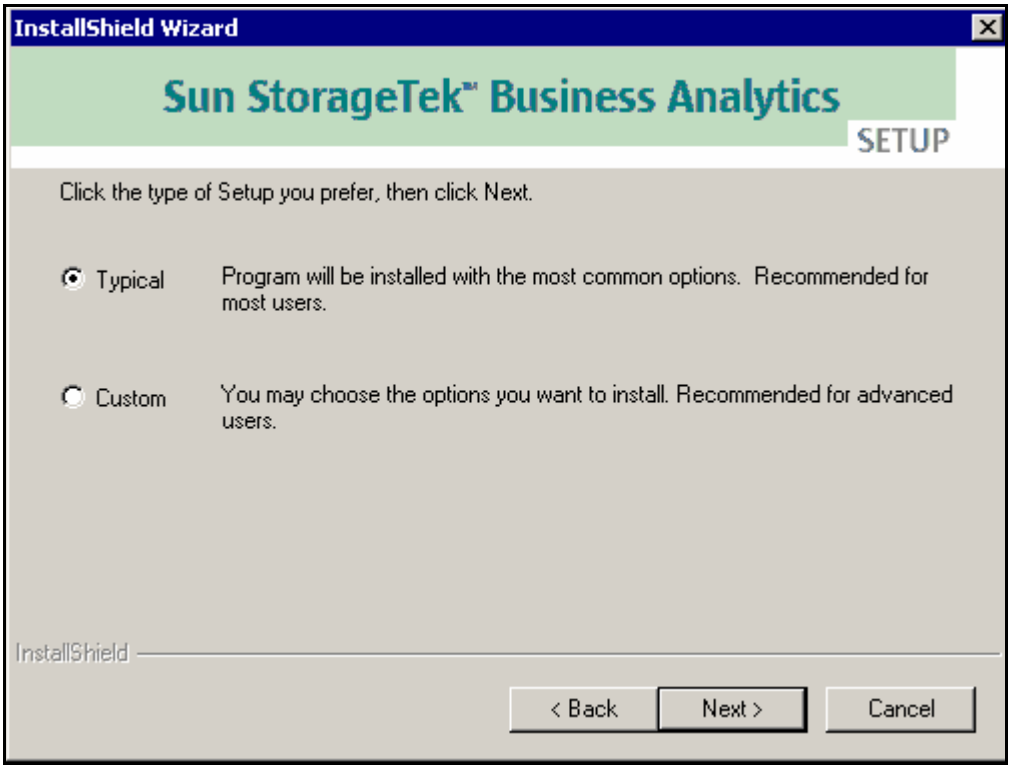


Figure 18 - Setup Type

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 assurent 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.
   - **GSM Scheduled Jobs –** Adds the GSM 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.

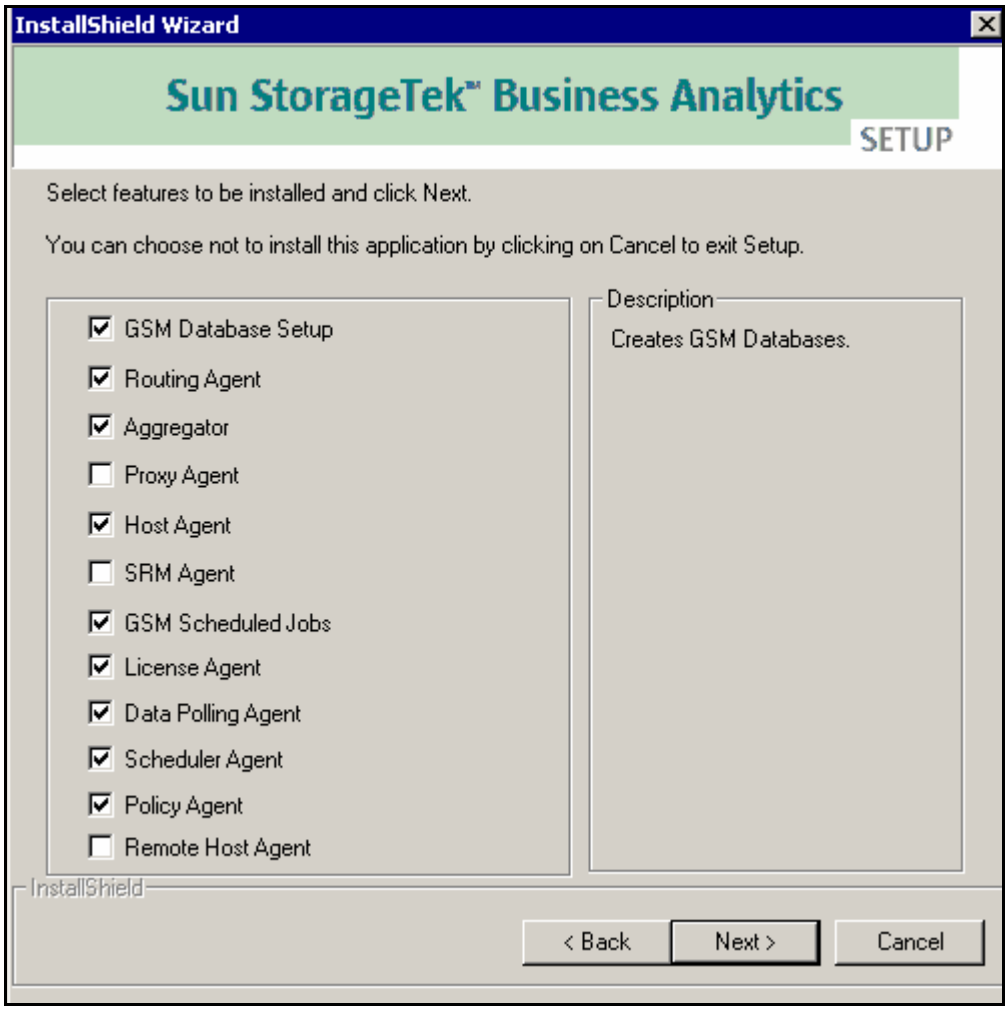


Figure 19 - Custom Install Dialog

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

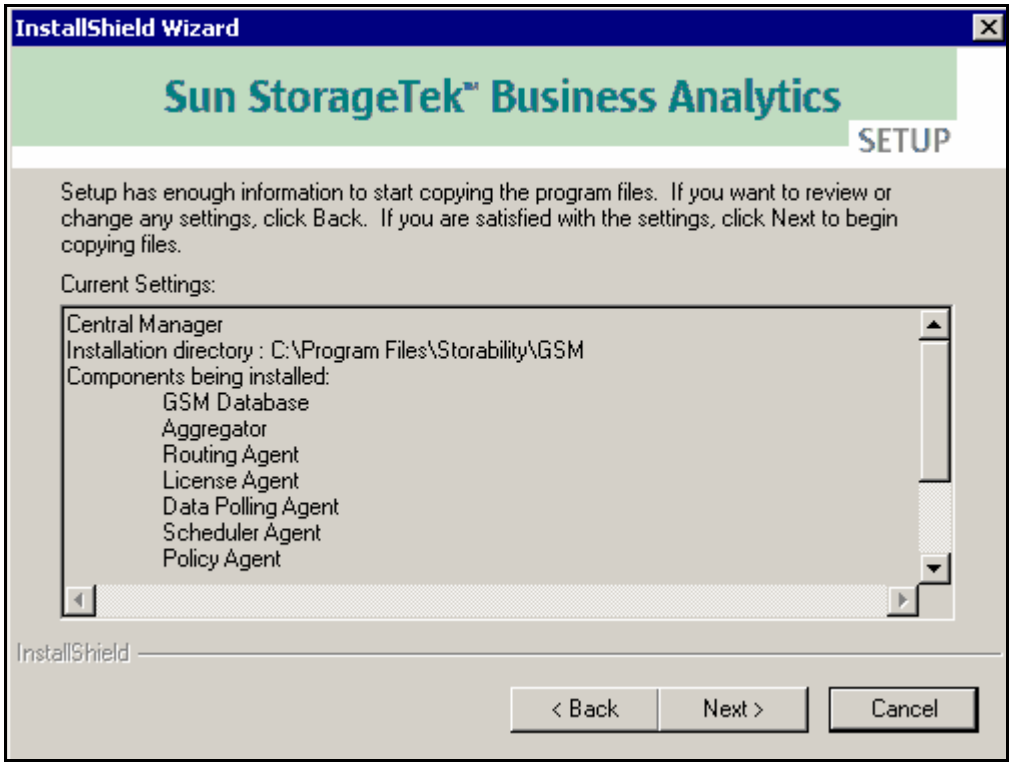


Figure 20 - Current Settings

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.

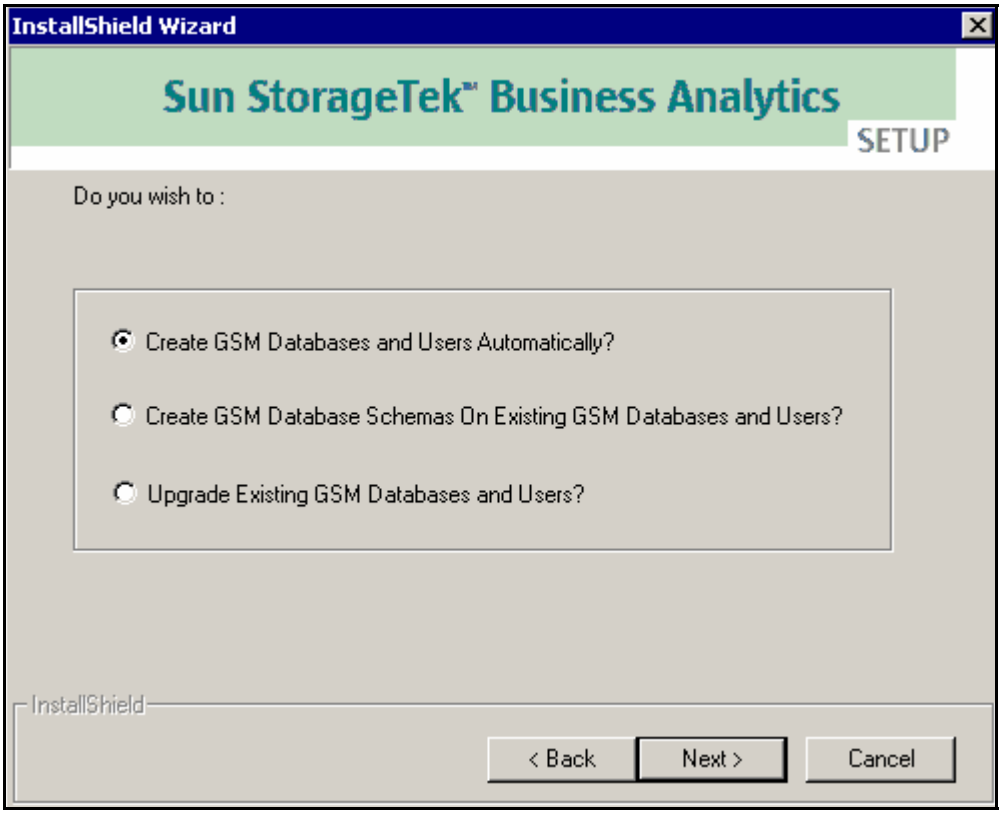


Figure 21 - Desired Database Setup

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.

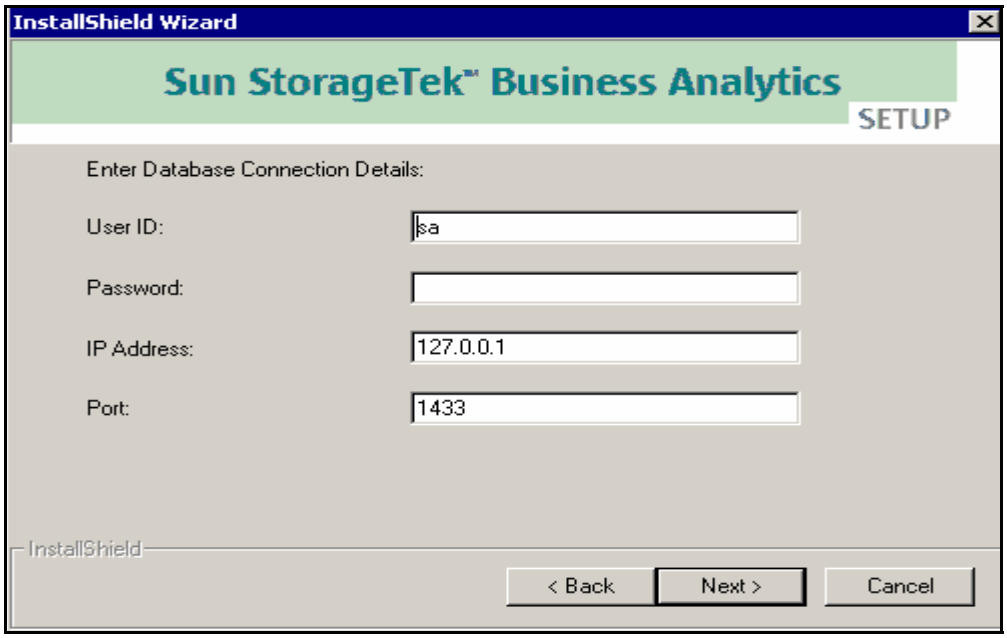


Figure 22 - Database Connection Details

10. The Sun StorageTek Business Analytics Database Setup creates the assurent 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.

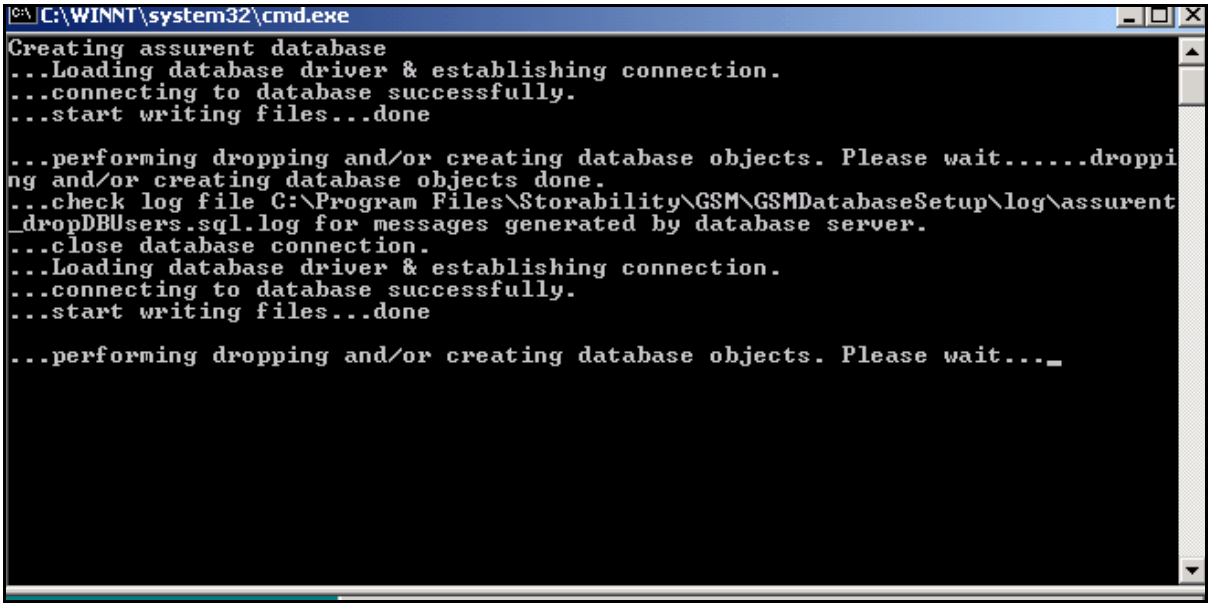


Figure 23 - Sample Database Setup Status

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.

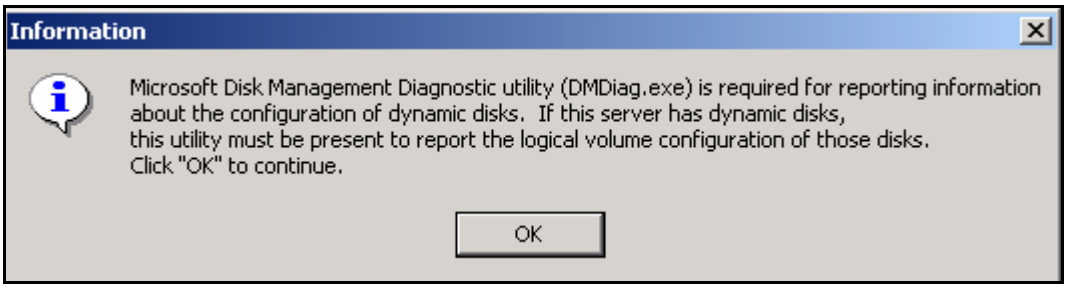


Figure 24 - Host Agent Information

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.

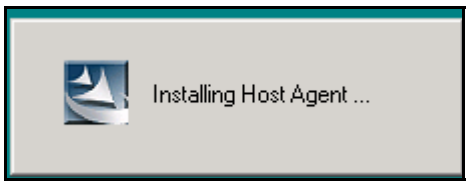


Figure 25 - Host Agent Install Splash Box

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.

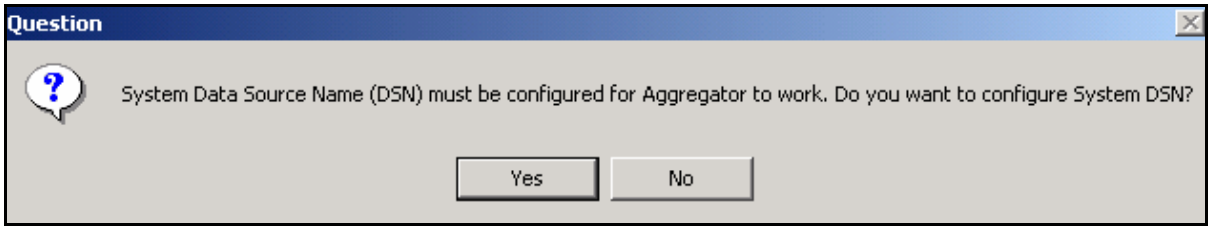


Figure 26 - Create System Data Source?

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.

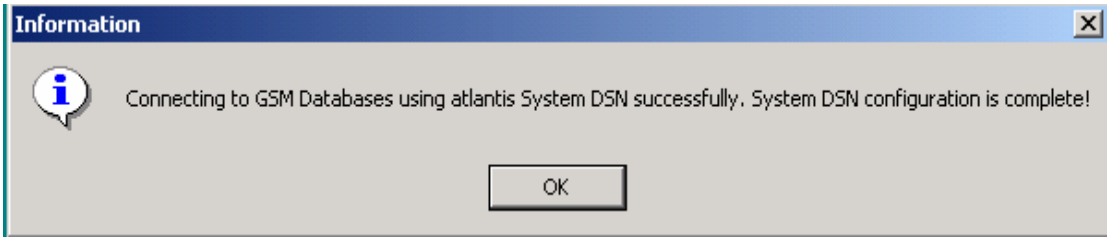


Figure 27 - System DSN configuration is complete!

18. Click **Finish** in the InstallShield Wizard Complete for Central Manager dialog box. The Readme file will be displayed in a system text editor (e.g., Wordpad) if the check mark in the **Readme** checkbox was not removed on the previous screen.

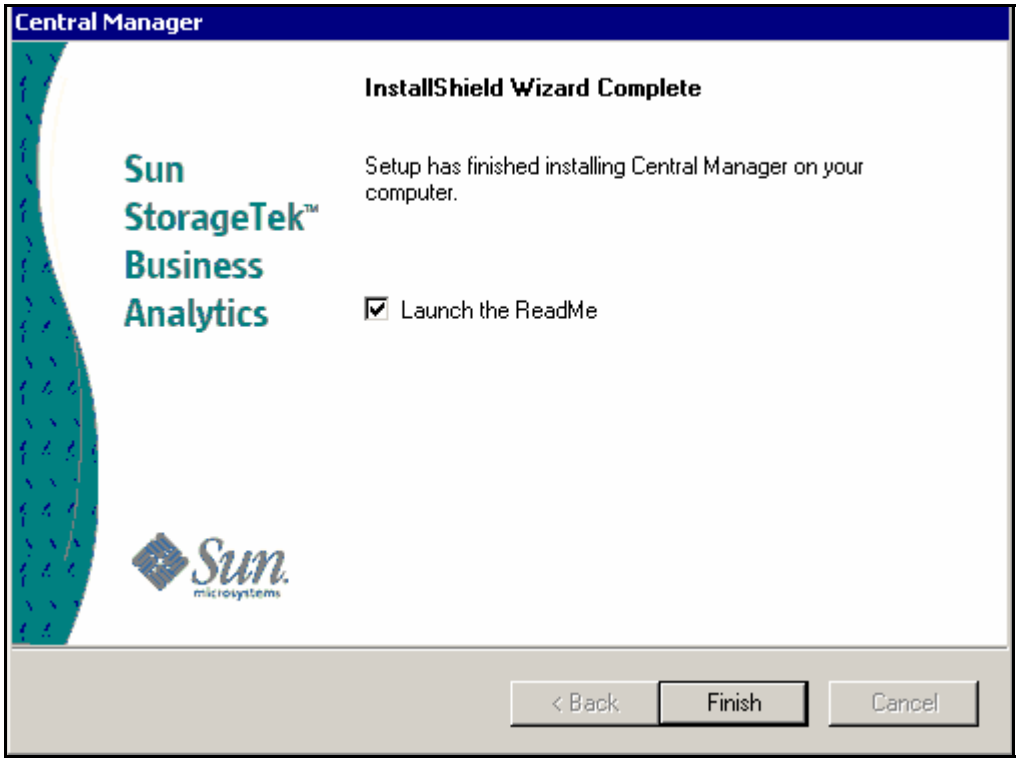


Figure 28 - InstallShield Wizard Complete

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 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.

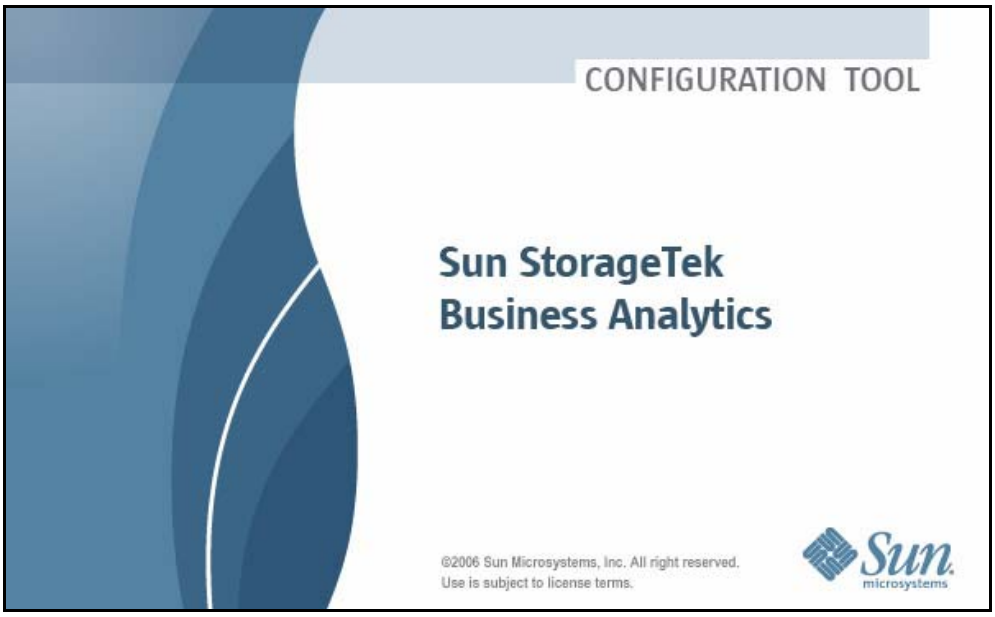


Figure 29 - Configuration Tool Splash Screen

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.

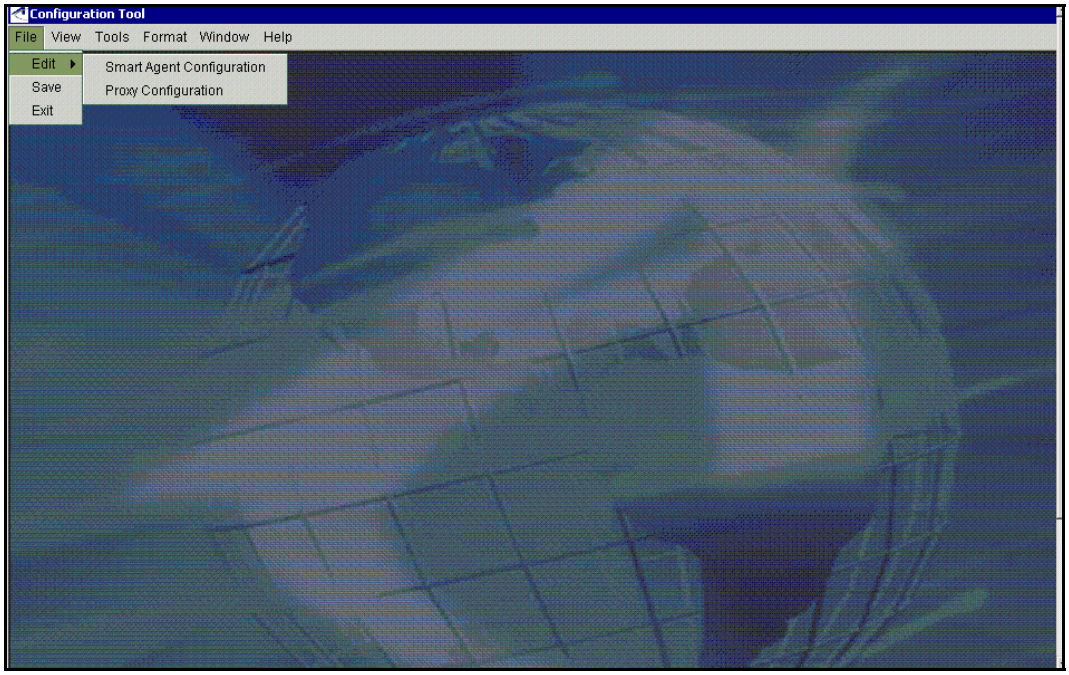


Figure 30 - Configuration Tool Main Menu

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

Table 2 - 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.

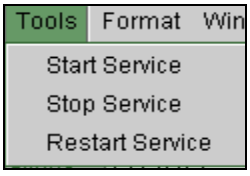


Figure 31 - Tools Menu in Configuration Tool

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.

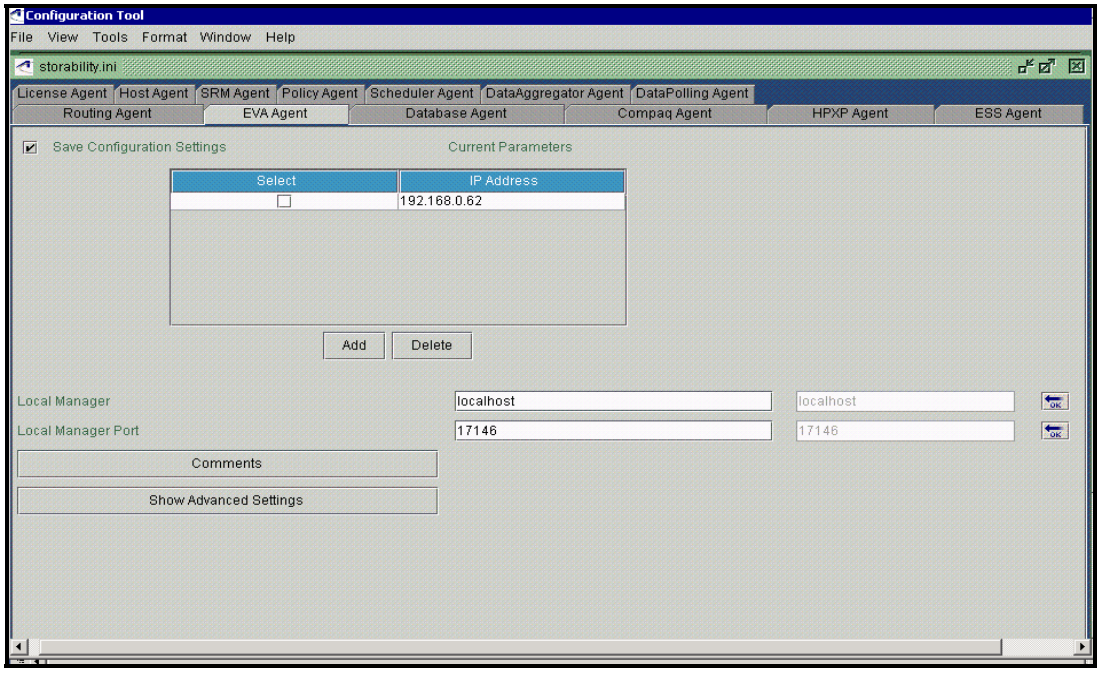


Figure 32 - Smart Agent Tabs in Configuration Tool

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.

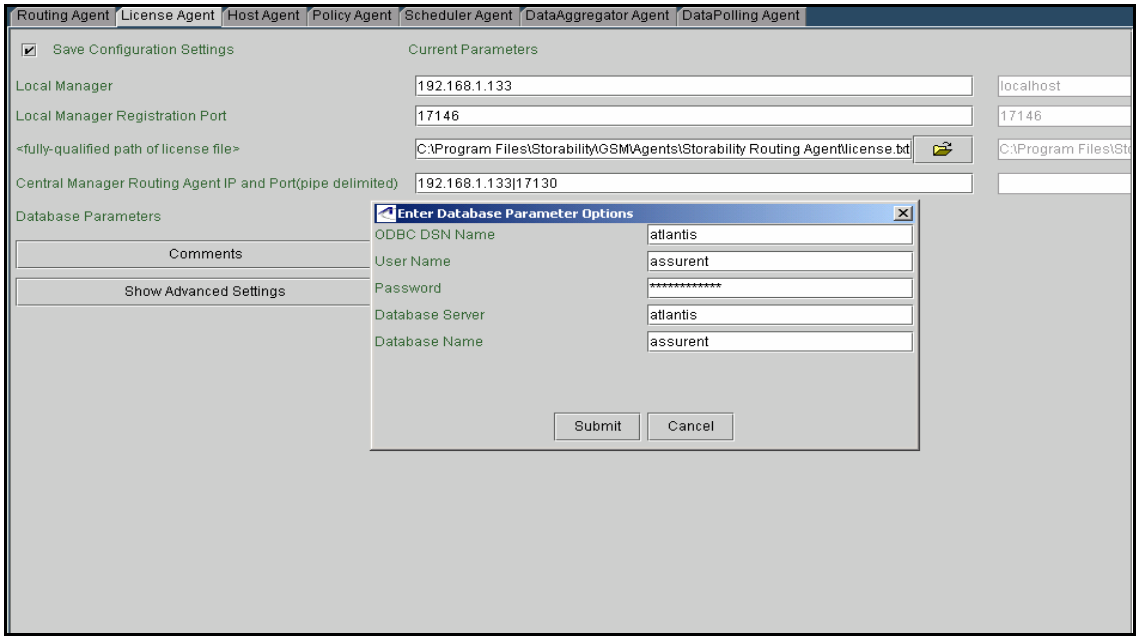


Figure 33 - License Agent Configuration Window

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.

LAUNCH THE CONFIGURATION TOOL

1. Select **Start->Programs->Storability->Launch Configuration Tool** on the Central Manager.
2. Select **File->Edit->Smart Agent Configuration**. The Smart Agent configuration main window is displayed, similar to the one shown below that has the License Agent tab enabled.

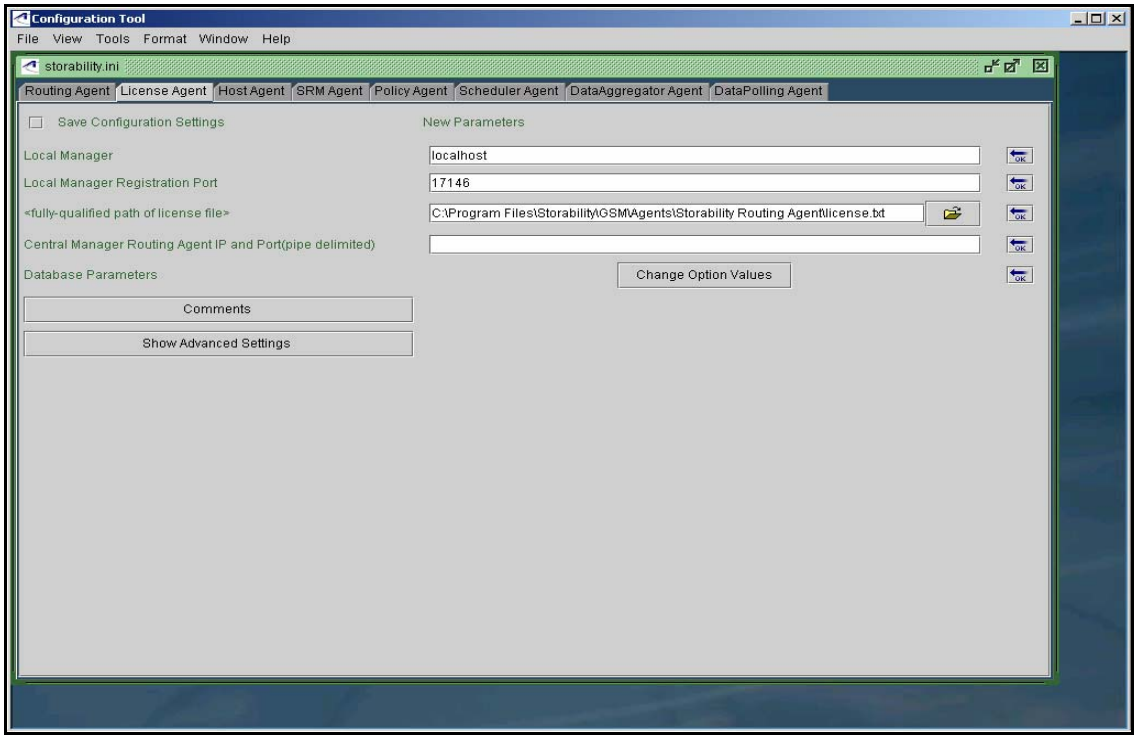


Figure 34 - Storability License Manager Configuration Window

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.

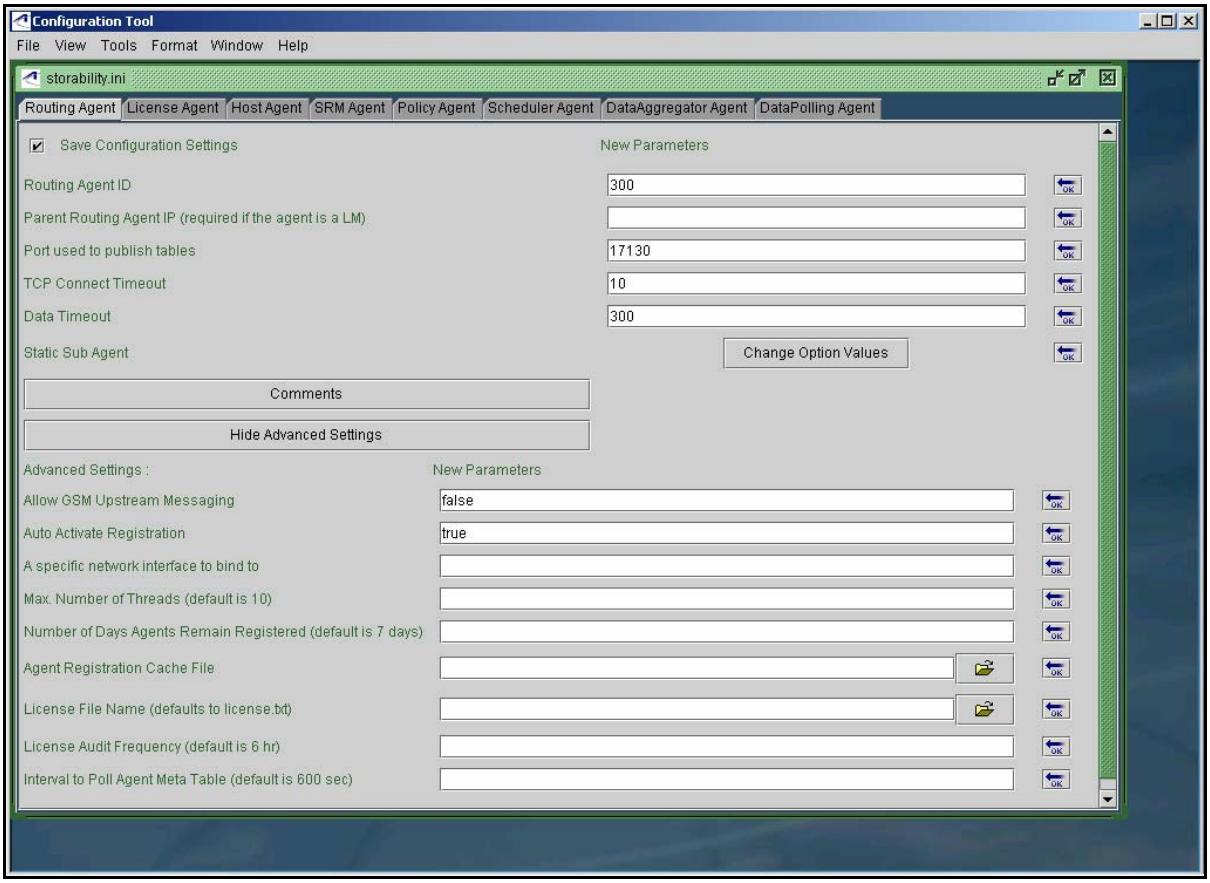


Figure 35 - Routing Agent Configuration Window

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 over-ridden 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.

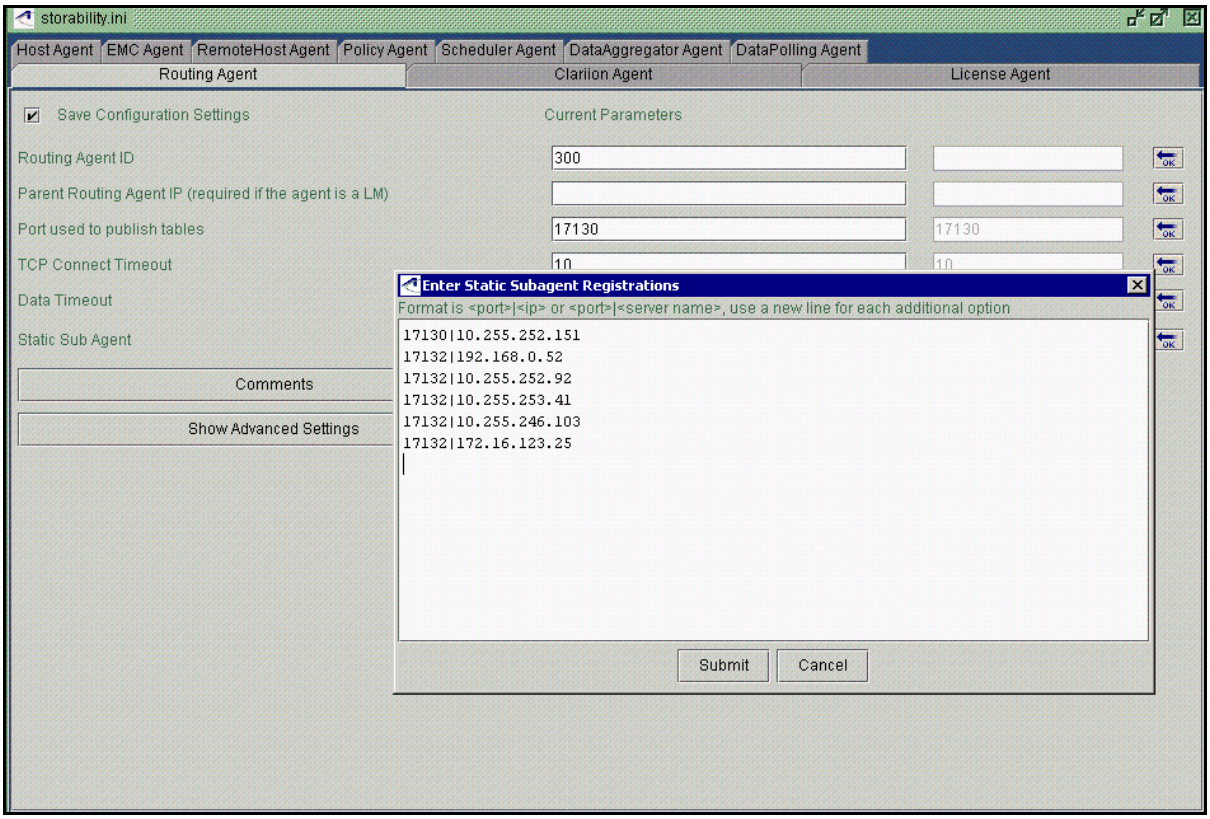


Figure 36 - Enter Static Subagent Registrations

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.
- **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.

- **Agent Registration Cache File –** Is <drive>:\Program Files\Storability\Agents\Storability Routing Agent\ardb.dat by default. The agent registration cache file (e.g., ardb.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.

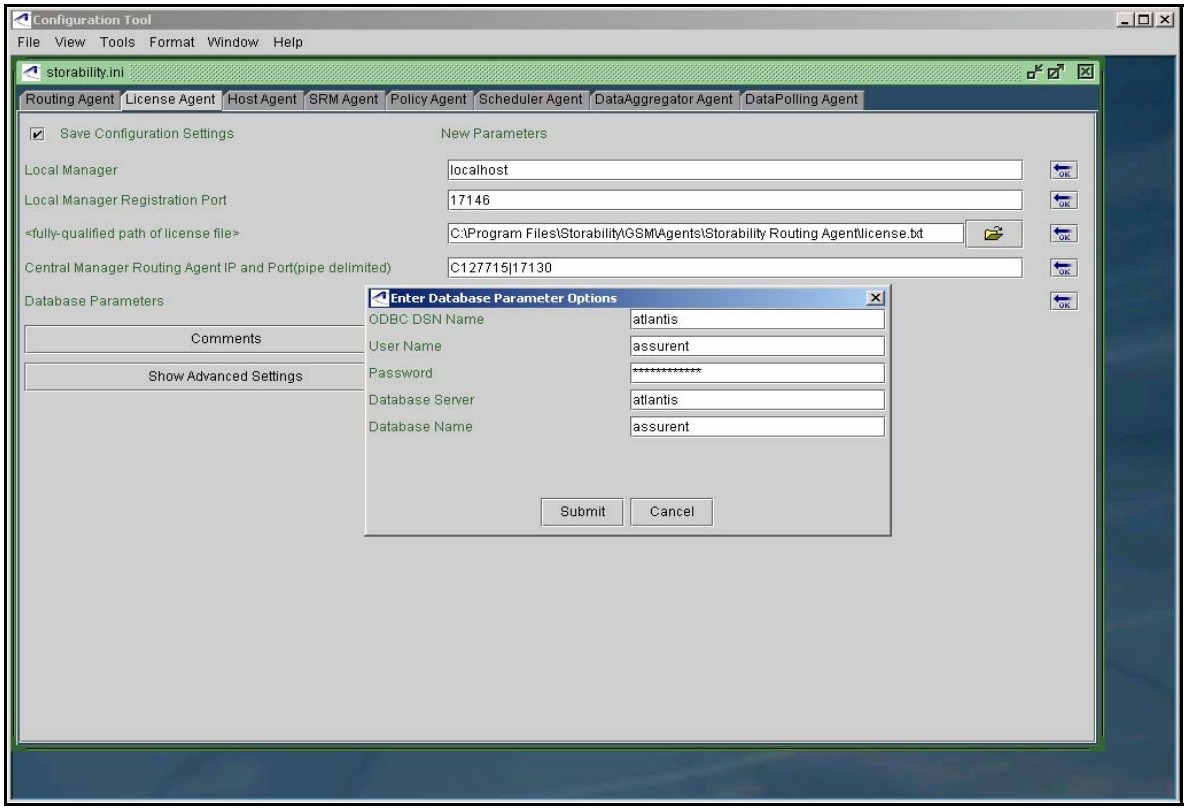


Figure 37 - License Manager Database Parameter Options

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 assurent 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 assurent 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.

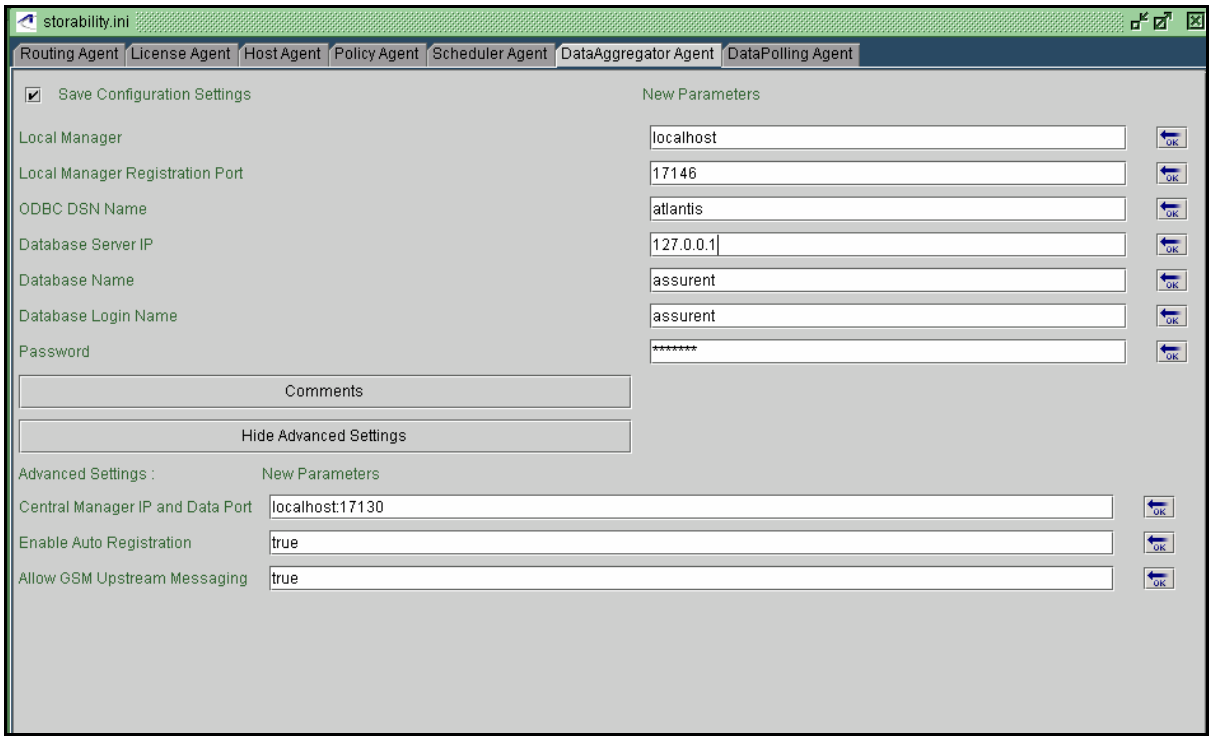


Figure 38 - Data Aggregator Configuration Window

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.

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.

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.

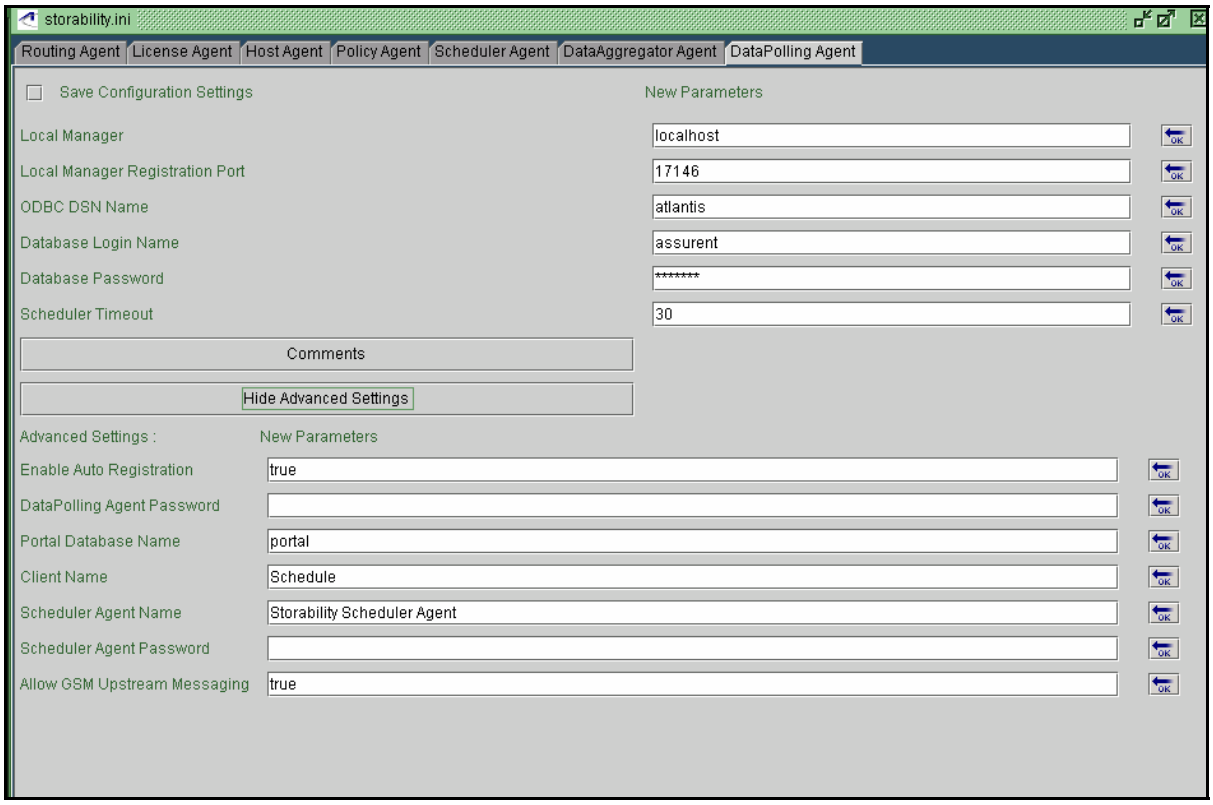


Figure 39 - Data Polling Agent Configuration Window

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.

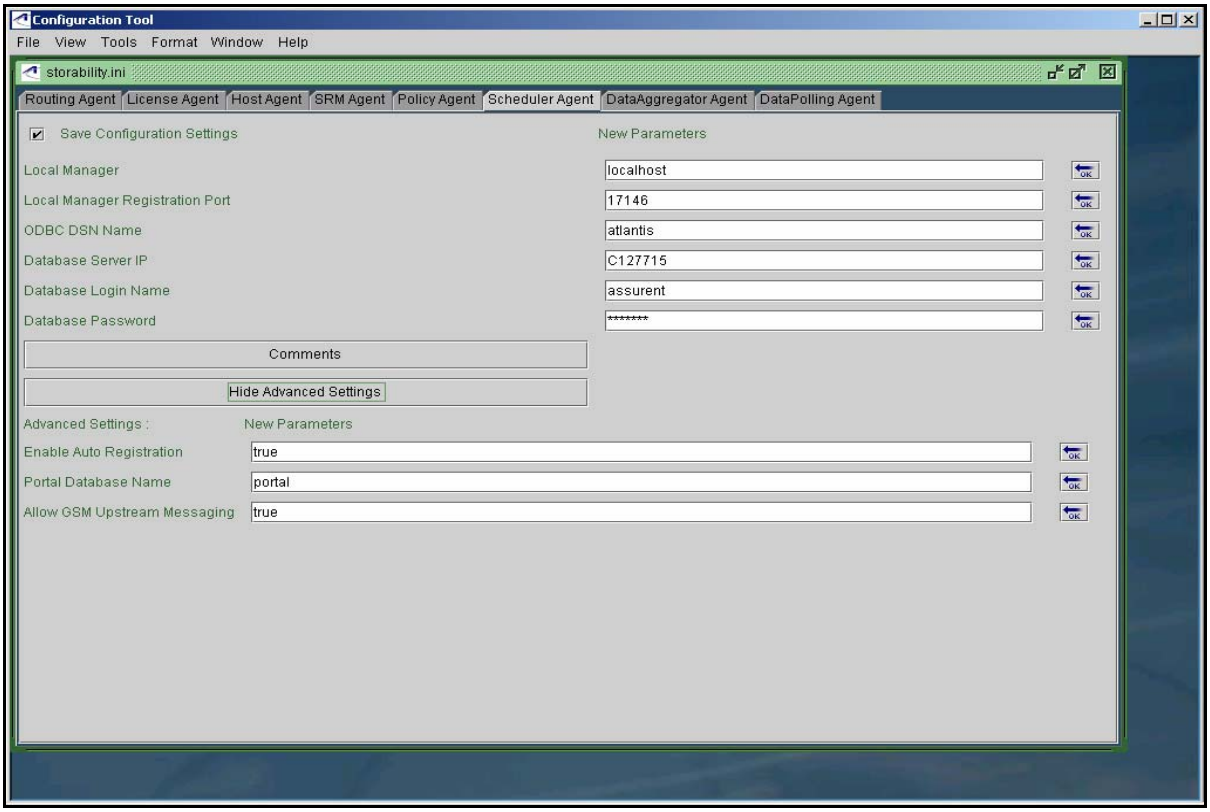


Figure 40 - Scheduler Agent Configuration Window

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 "assurent".
10. Accept the default password for the assurent 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 management. 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.

Note: The Policy Agent will not start successfully unless there is valid SMTP Server configuration details stored in its section of the storability.ini file.

The policies are defined using the Management Console's **Policy Alerting** menus. You must start the Policy Agent to use these menus.

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.

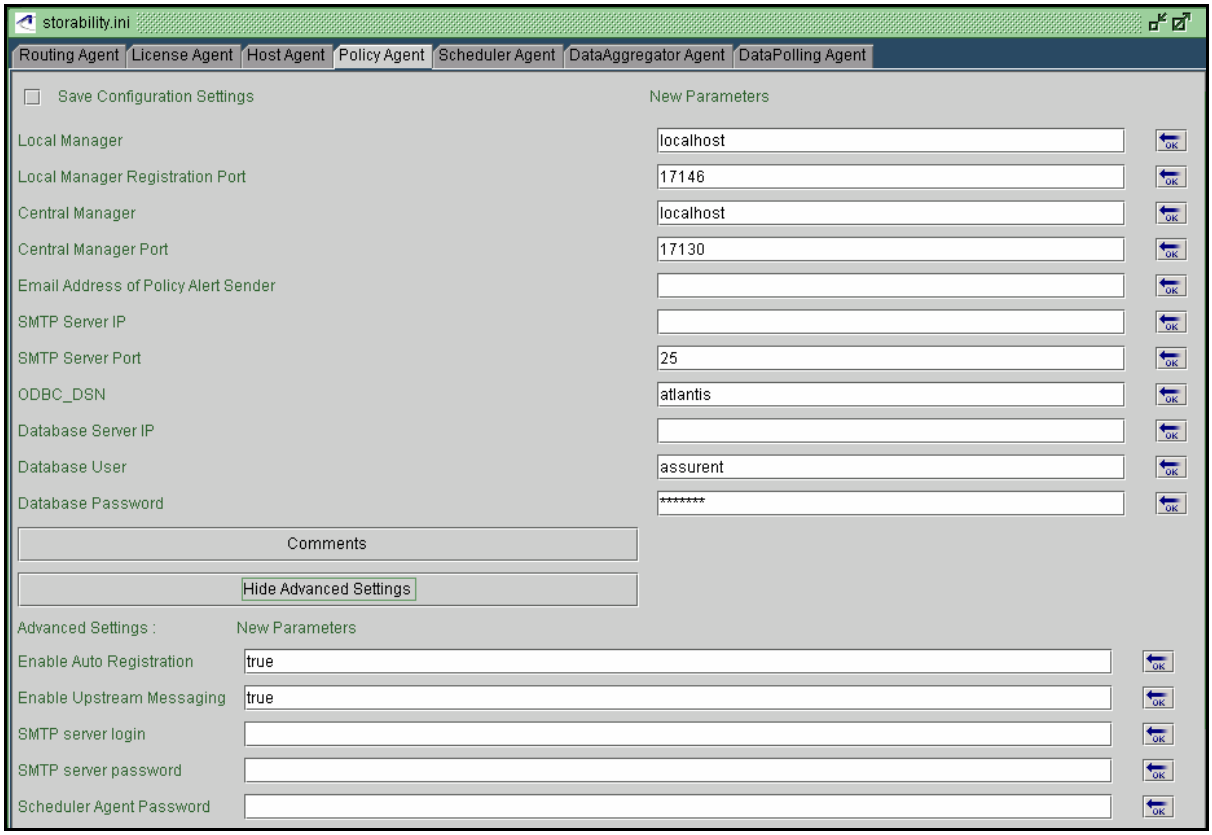


Figure 41 - Policy Agent Configuration Window

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.
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.

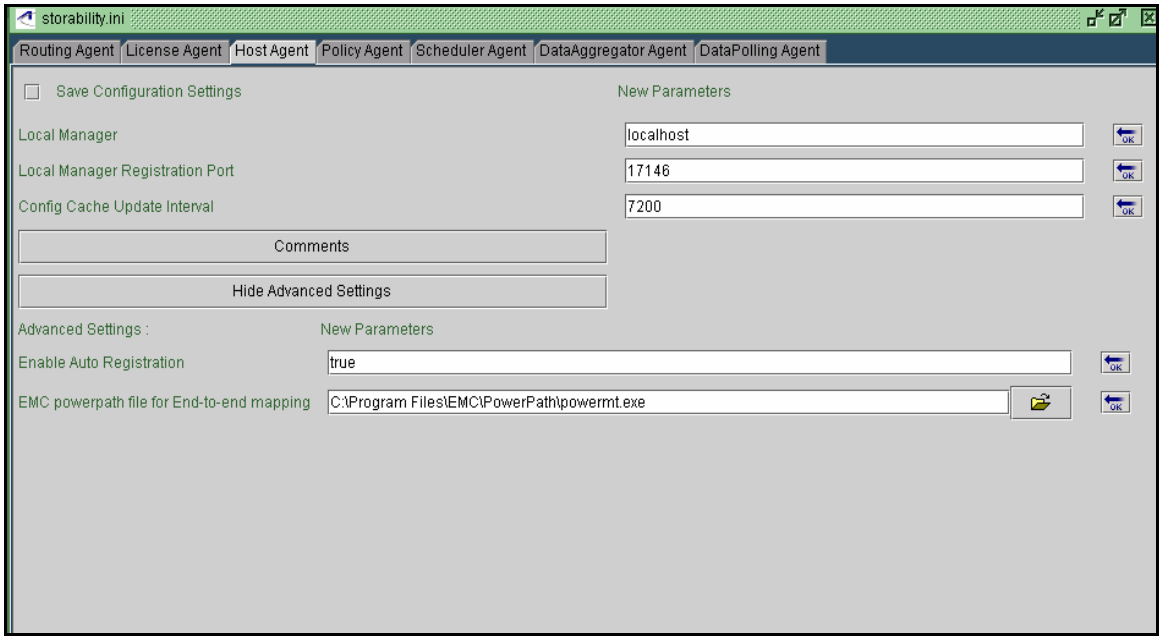


Figure 42 - Host Agent Configuration Window

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.

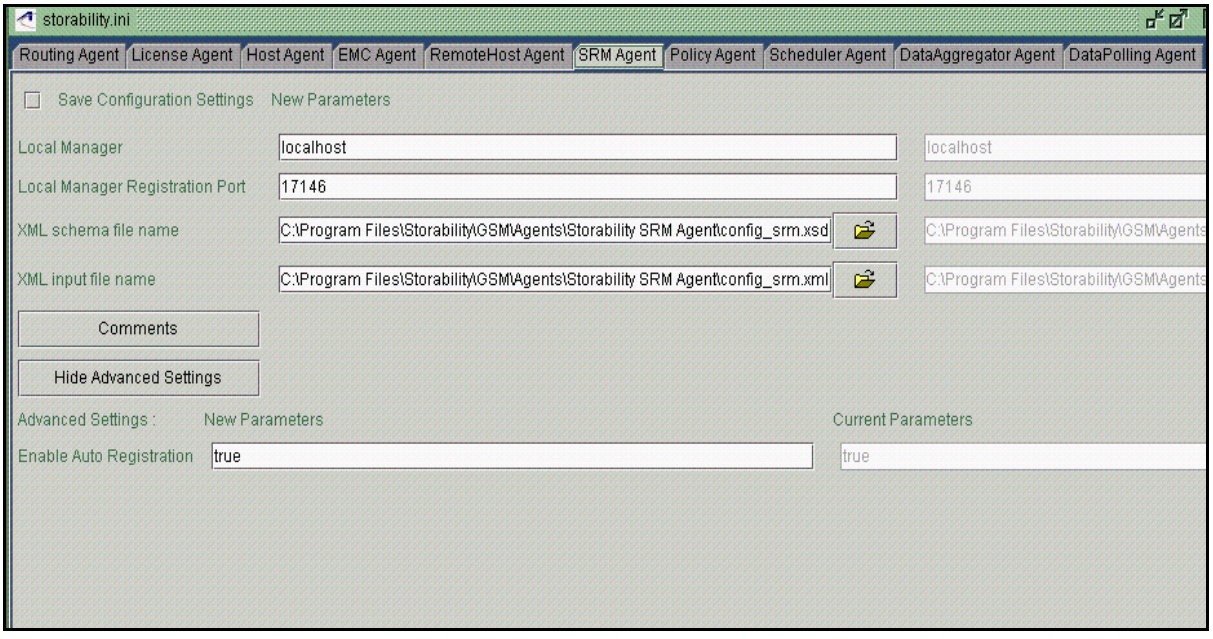


Figure 43 - SRM Agent Configuration Window

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 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.

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.

AGENT DIAGNOSTIC TOOL

The Agent Diagnostic Tool (gsmdiag.exe) is installed in the Storability Local Manager **Utilities** folder as part of the Local Manager and Central Manager for Windows installation procedures. It represents the primary tool to verify agent functionality once it is configured and started.

You can use GSMdiag 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 utility's (gsmdiag.exe) **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.

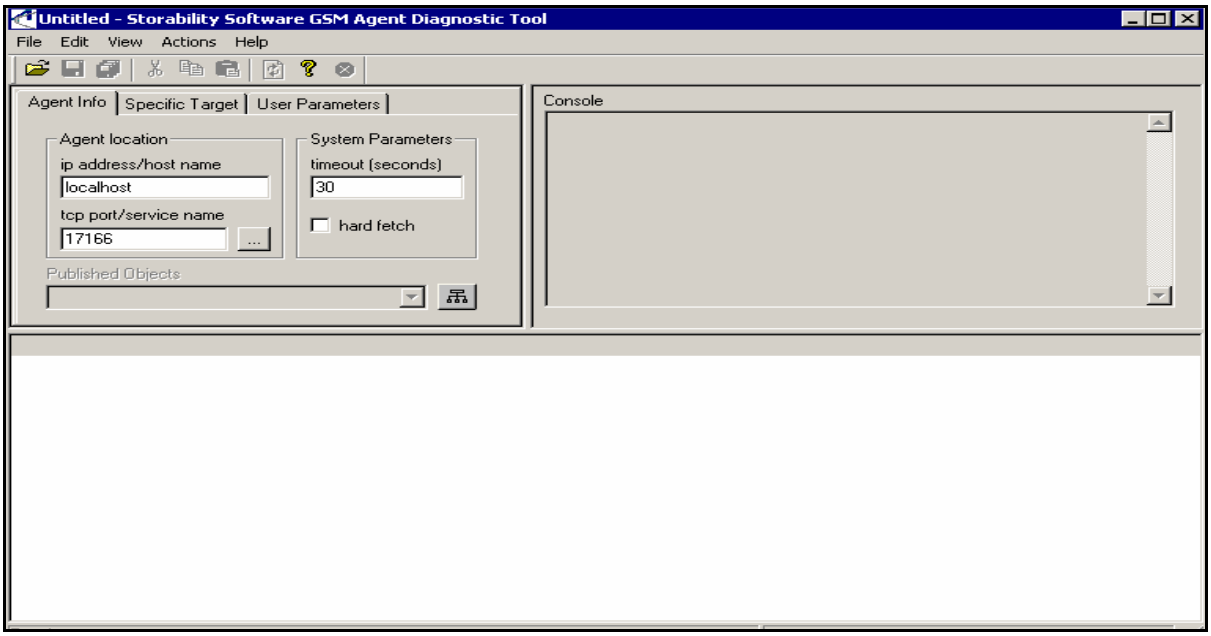


Figure 44 - GSM Agent Diagnostic Tool Main Window

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 (GSMdiag) can collect the tables successfully, the **Published Objects** list box is enabled.

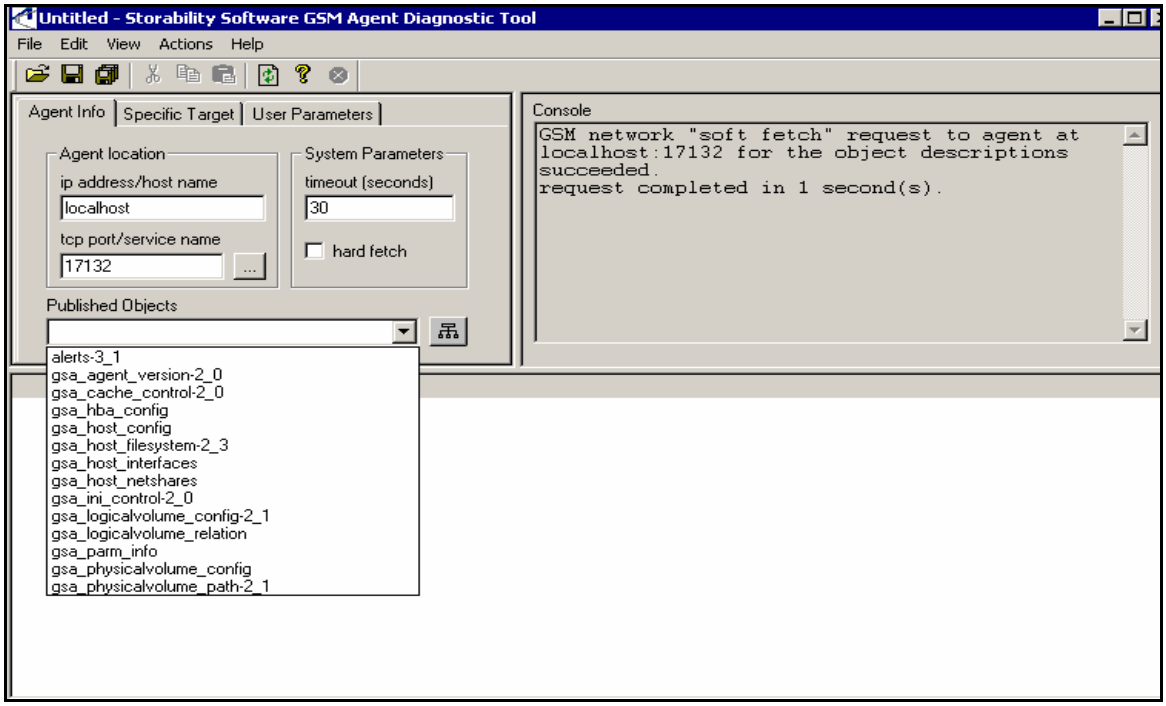


Table 3 - Sample Published Objects List

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

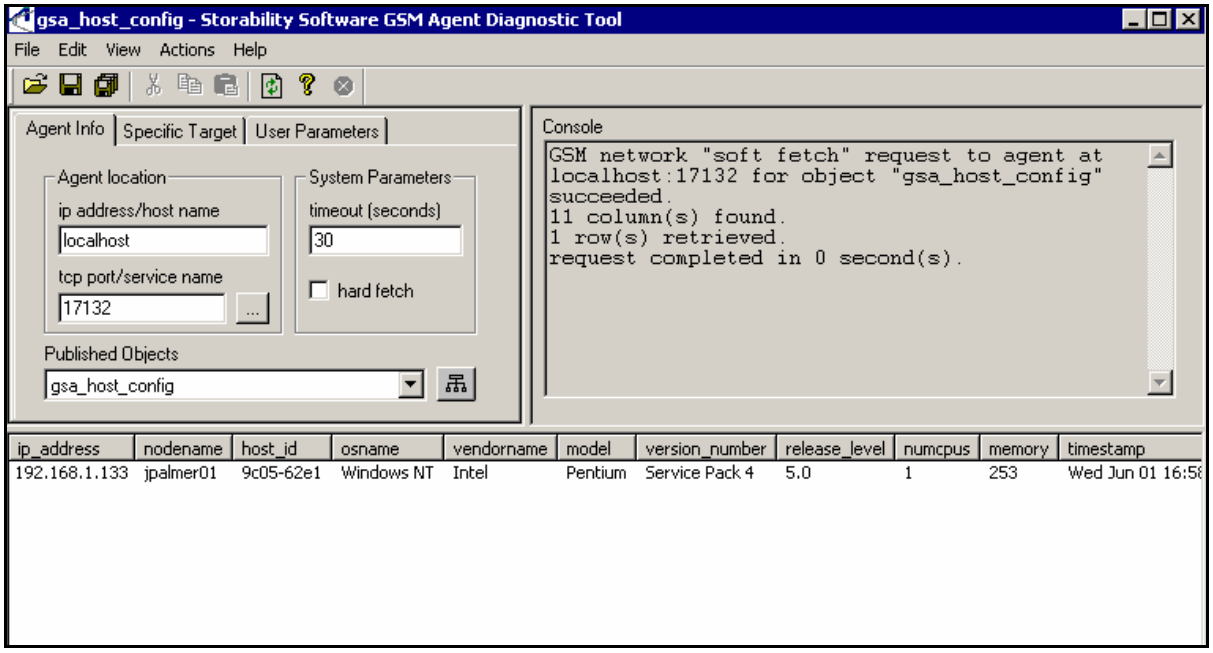


Table 4 - Sample Host Configuration

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.

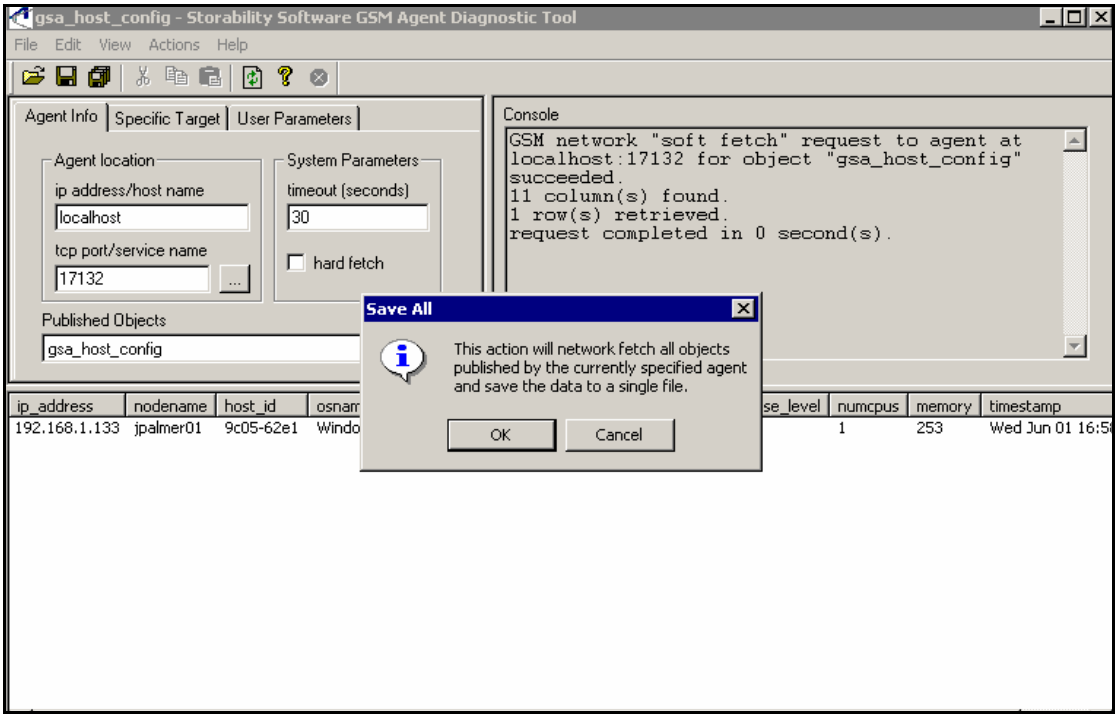


Table 5 – Save All Option

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 GSM Agent Diagnostic Tool (gsmdiag.exe). However, cm-get differs from the GSM 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 GSM 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:17132%101  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_reg
ister 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 45 - Sample cm-get Output

VERIFY CENTRAL MANAGER AGENT FUNCTIONALITY

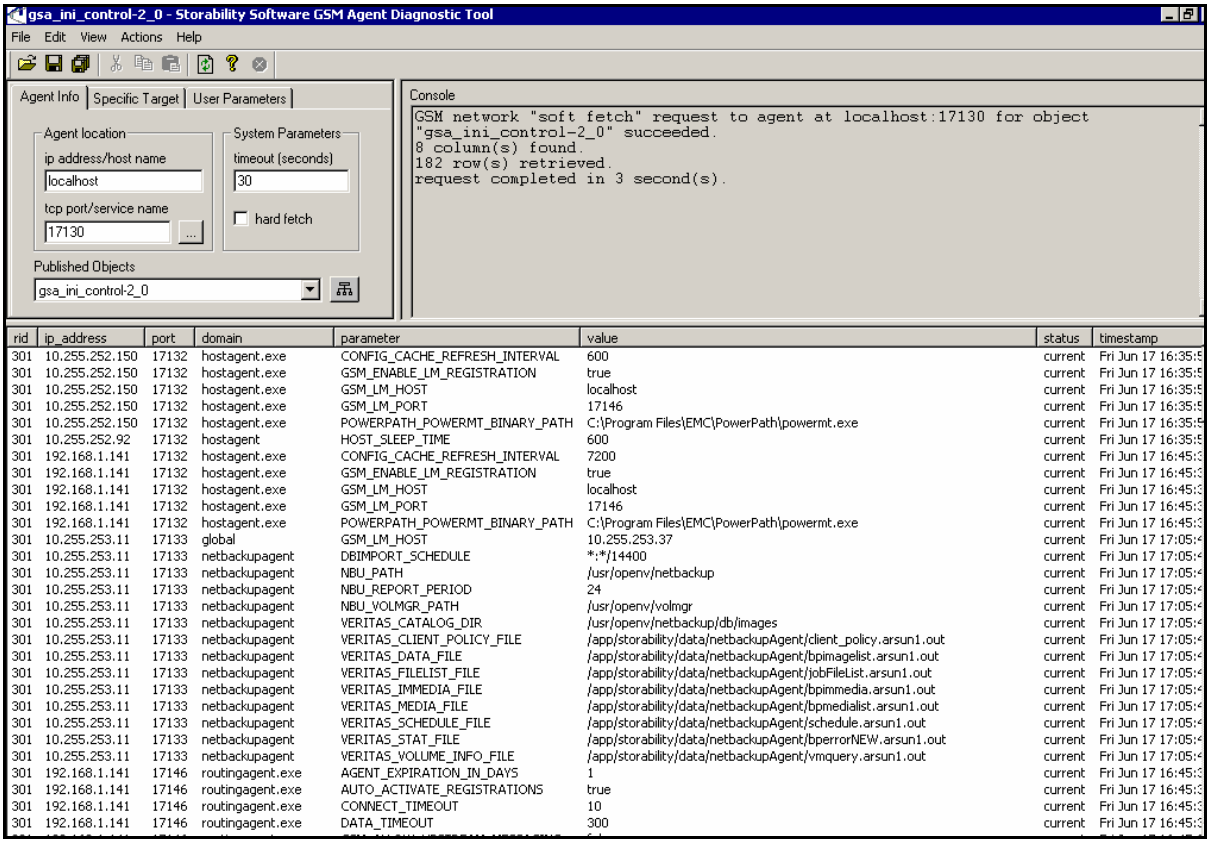
The Agent Diagnostic (gsmdiag.exe) utility should be used to verify the Central Manager agents have started and are registered with their configured Local Manager.

Proceed as follows:

1. Select **Start->Programs-> Storability->Launch GSM Agent Diagnostic Tool**.

Verify Routing Agent

2. Wait approximately 30 seconds after the Routing Agent has started to allow it to initialize before querying it with the GSM 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.

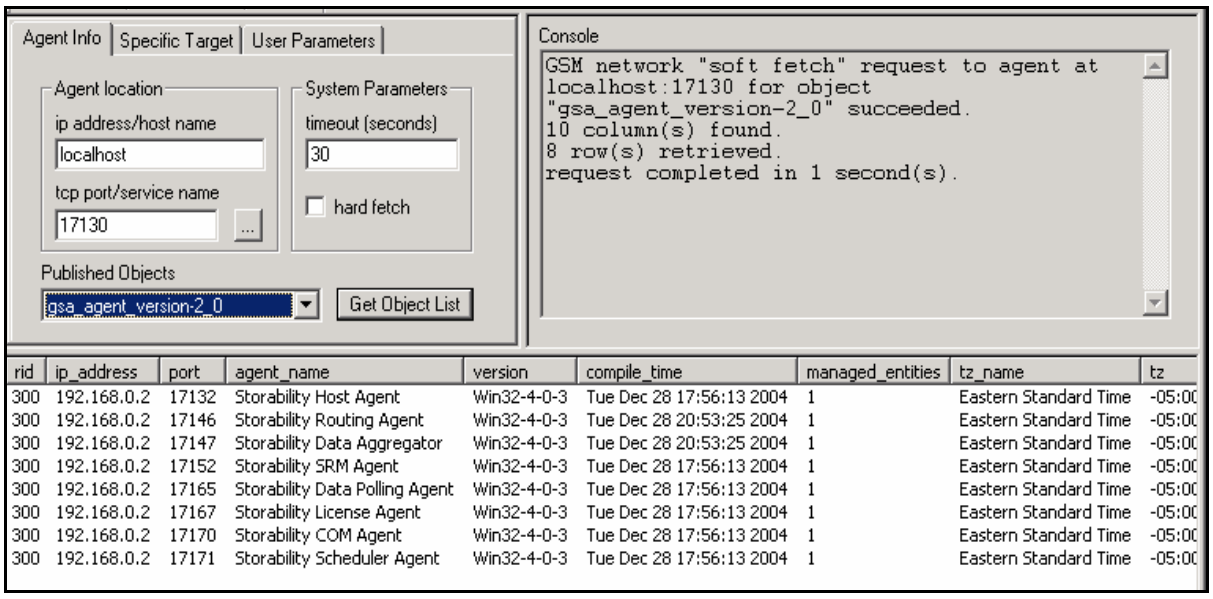


rid	ip_address	port	domain	parameter	value	status	timestamp
301	10.255.252.150	17132	hostagent.exe	CONFIG_CACHE_REFRESH_INTERVAL	600	current	Fri Jun 17 16:35:5
301	10.255.252.150	17132	hostagent.exe	GSM_ENABLE_LM_REGISTRATION	true	current	Fri Jun 17 16:35:5
301	10.255.252.150	17132	hostagent.exe	GSM_LM_HOST	localhost	current	Fri Jun 17 16:35:5
301	10.255.252.150	17132	hostagent.exe	GSM_LM_PORT	17146	current	Fri Jun 17 16:35:5
301	10.255.252.150	17132	hostagent.exe	POWERPATH_POWERMT_BINARY_PATH	C:\Program Files\EMC\PowerPath\powermt.exe	current	Fri Jun 17 16:35:5
301	10.255.252.92	17132	hostagent	HOST_SLEEP_TIME	600	current	Fri Jun 17 16:35:5
301	192.168.1.141	17132	hostagent.exe	CONFIG_CACHE_REFRESH_INTERVAL	7200	current	Fri Jun 17 16:45:3
301	192.168.1.141	17132	hostagent.exe	GSM_ENABLE_LM_REGISTRATION	true	current	Fri Jun 17 16:45:3
301	192.168.1.141	17132	hostagent.exe	GSM_LM_HOST	localhost	current	Fri Jun 17 16:45:3
301	192.168.1.141	17132	hostagent.exe	GSM_LM_PORT	17146	current	Fri Jun 17 16:45:3
301	192.168.1.141	17132	hostagent.exe	POWERPATH_POWERMT_BINARY_PATH	C:\Program Files\EMC\PowerPath\powermt.exe	current	Fri Jun 17 16:45:3
301	10.255.253.11	17133	global	GSM_LM_HOST	10.255.253.37	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	DBIMPORT_SCHEDULE	*:*/14400	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	NBU_PATH	/usr/openv/netbackup	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	NBU_REPORT_PERIOD	24	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	NBU_VOLMGR_PATH	/usr/openv/volmgr	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_CATALOG_DIR	/usr/openv/netbackup/db/images	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_CLIENT_POLICY_FILE	/app/storability/data/netbackupAgent/client_policy.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_DATA_FILE	/app/storability/data/netbackupAgent/bpimagelist.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_FILELIST_FILE	/app/storability/data/netbackupAgent/jobFileList.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_IMMEDIA_FILE	/app/storability/data/netbackupAgent/bpimmedia.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_MEDIA_FILE	/app/storability/data/netbackupAgent/bpmedialist.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_SCHEDULE_FILE	/app/storability/data/netbackupAgent/schedule.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_STAT_FILE	/app/storability/data/netbackupAgent/bperrorNEW.arsun1.out	current	Fri Jun 17 17:05:4
301	10.255.253.11	17133	netbackupagent	VERITAS_VOLUME_INFO_FILE	/app/storability/data/netbackupAgent/vmquery.arsun1.out	current	Fri Jun 17 17:05:4
301	192.168.1.141	17146	routingagent.exe	AGENT_EXPIRATION_IN_DAYS	1	current	Fri Jun 17 16:45:3
301	192.168.1.141	17146	routingagent.exe	AUTO_ACTIVATE_REGISTRATIONS	true	current	Fri Jun 17 16:45:3
301	192.168.1.141	17146	routingagent.exe	CONNECT_TIMEOUT	10	current	Fri Jun 17 16:45:3
301	192.168.1.141	17146	routingagent.exe	DATA_TIMEOUT	300	current	Fri Jun 17 16:45:3

Figure 46 - 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.



rid	ip_address	port	agent_name	version	compile_time	managed_entities	tz_name	tz
300	192.168.0.2	17132	Storability Host Agent	Win32-4-0-3	Tue Dec 28 17:56:13 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17146	Storability Routing Agent	Win32-4-0-3	Tue Dec 28 20:53:25 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17147	Storability Data Aggregator	Win32-4-0-3	Tue Dec 28 20:53:25 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17152	Storability SRM Agent	Win32-4-0-3	Tue Dec 28 17:56:13 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17165	Storability Data Polling Agent	Win32-4-0-3	Tue Dec 28 17:56:13 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17167	Storability License Agent	Win32-4-0-3	Tue Dec 28 17:56:13 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17170	Storability COM Agent	Win32-4-0-3	Tue Dec 28 17:56:13 2004	1	Eastern Standard Time	-05:00
300	192.168.0.2	17171	Storability Scheduler Agent	Win32-4-0-3	Tue Dec 28 17:56:13 2004	1	Eastern Standard Time	-05:00

Figure 47 - 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. Refer to the S*un StorageTek Business Analytics Infrastructure Planning* document for additional information on these supported platforms. Your Sun representative can provide you with the current version of this document.

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. Verify the platform requirements specified in the S*un StorageTek Business Analytics Infrastructure Planning* document for Microsoft IIS 5.0 Server.
2. Insert the Windows 2000 installation CD in the CD-ROM drive.
3. Select **Start-> Settings>Control Panel**.
4. Select **Add/Remove Windows Components**.
5. Follow the on-screen instructions to install IIS.
6. 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.
7. 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. In this case, 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, 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

Before you proceed, refer to the *Sun StorageTek Business Analytics Infrastructure Planning Guide* to verify the Management Console's requirements. Your Sun representative can provide the current version of this document.

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.

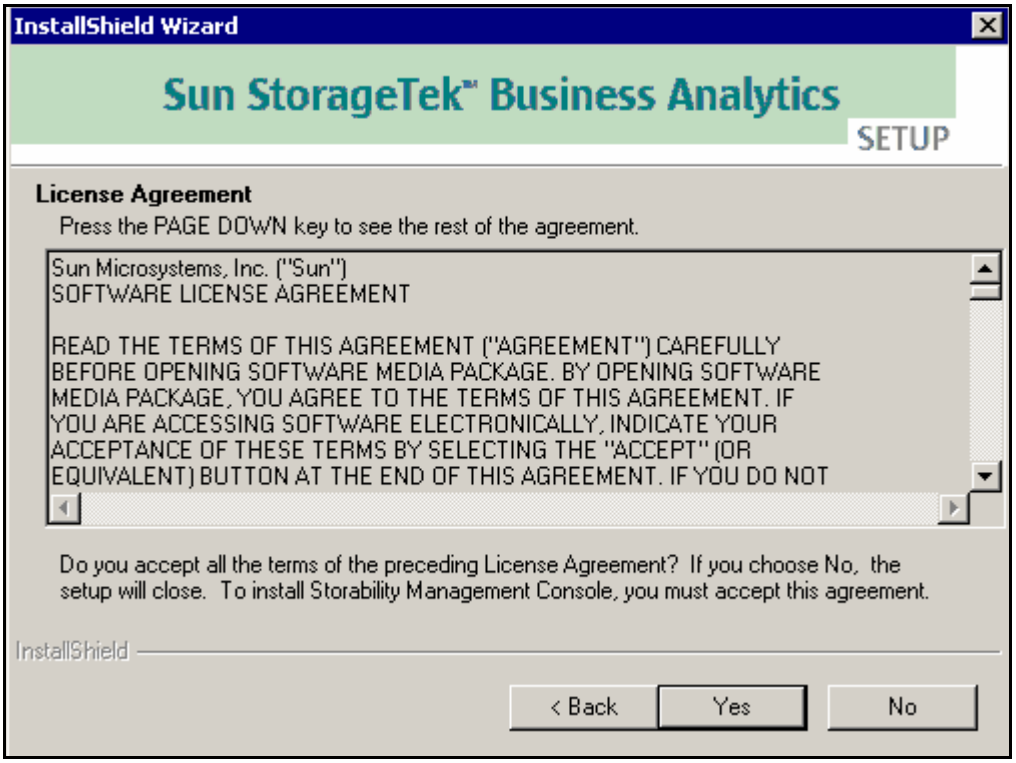


Figure 48 - Software License

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:\Progam Files\Storability\Storability Management Console) and click **Next>**. The Storability COM Agent dialog appears.

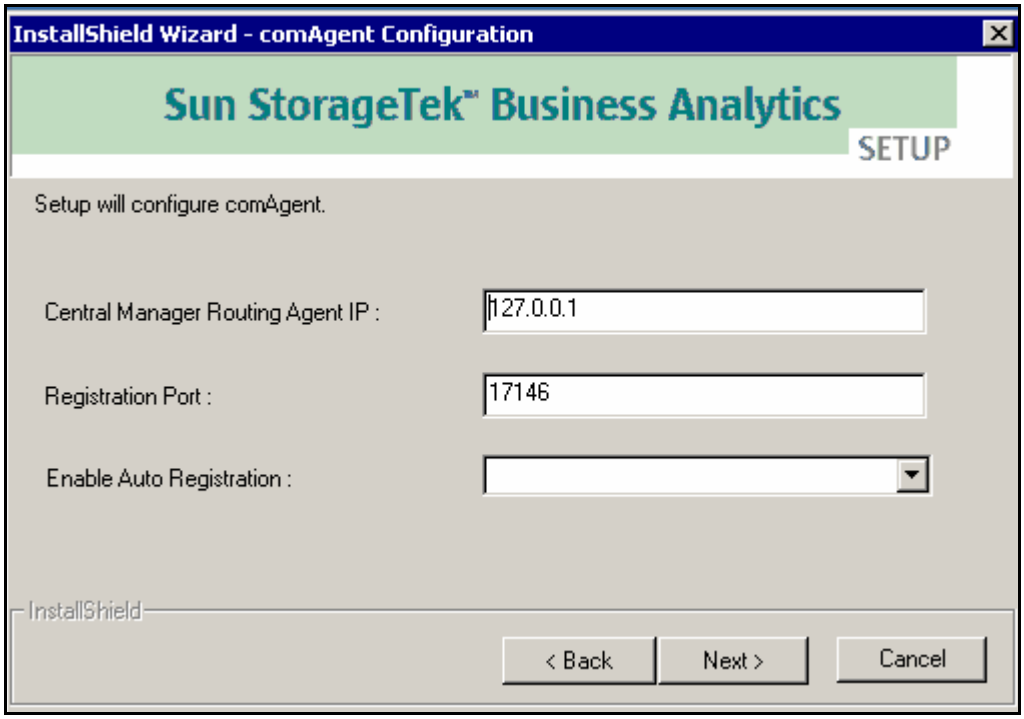


Figure 49 - Storability COM Agent Configuration Dialog

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

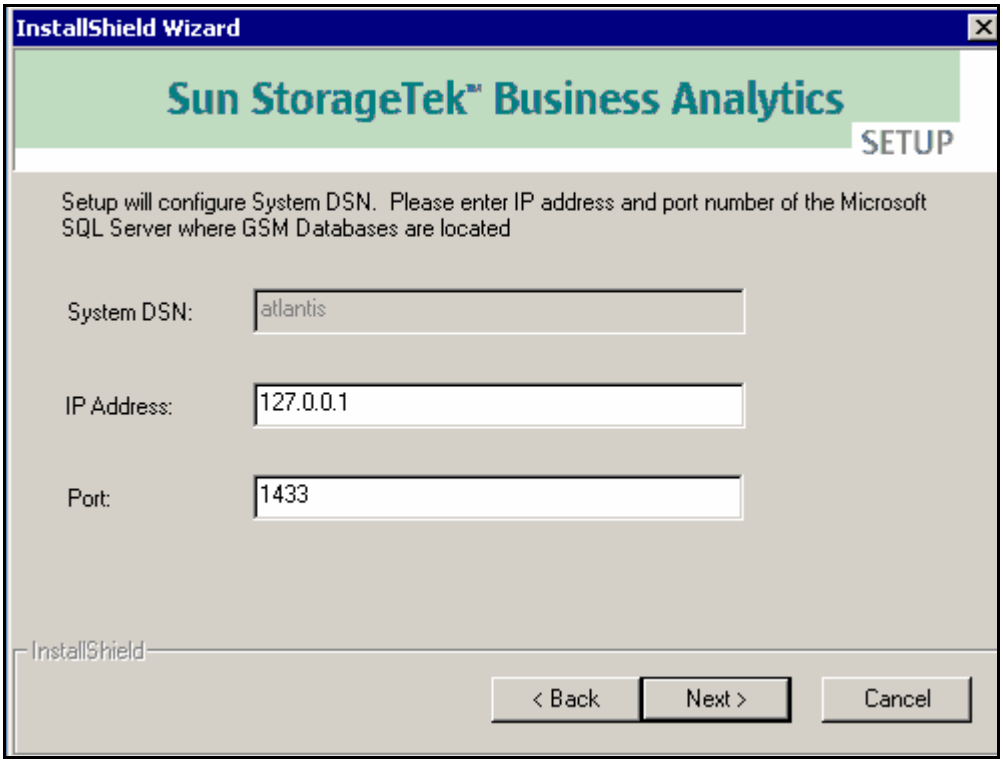


Figure 50 - Configure System DSN

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.

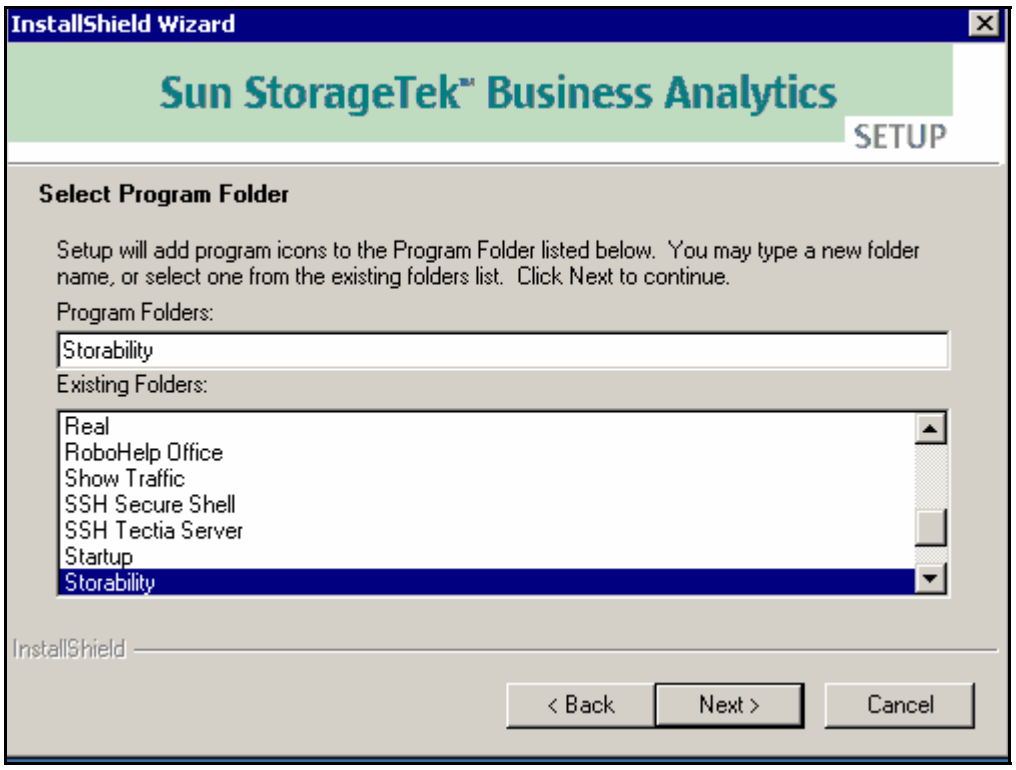


Figure 51 - Select Program Folder

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.

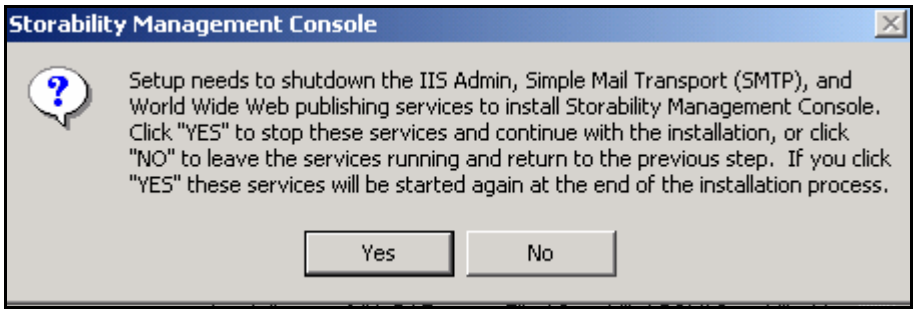


Figure 52 - Shutdown IIS Informational Dialog

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

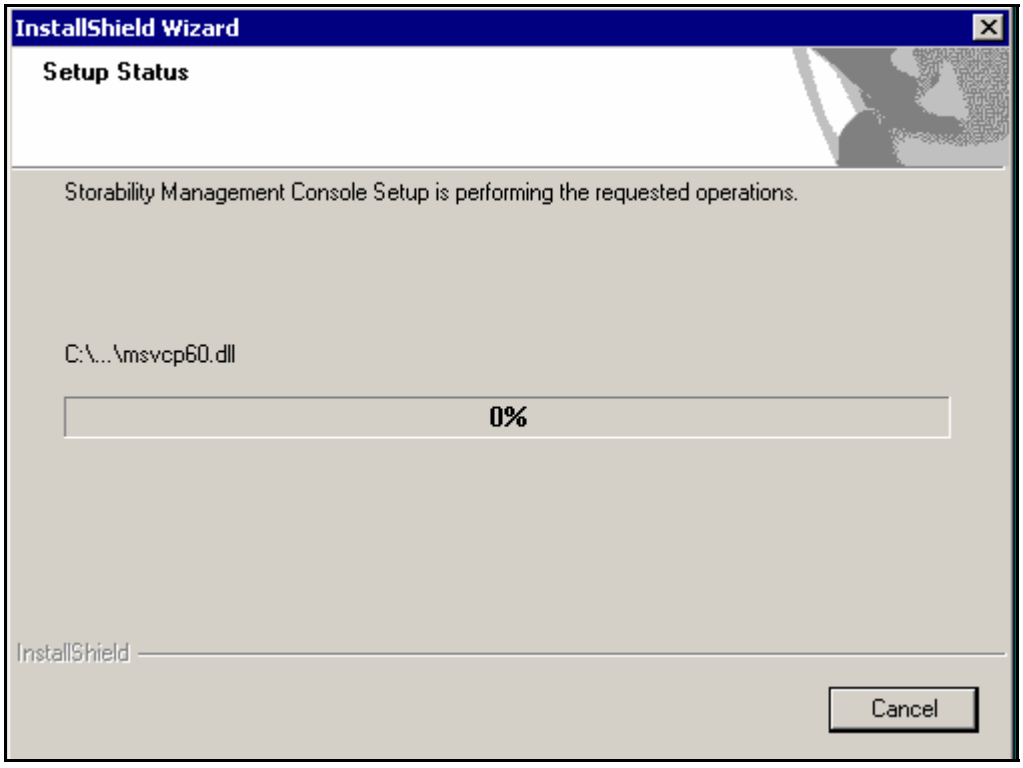


Figure 53 - Setup Status

13. The InstallShield Installation Complete dialog appears. Specify whether or not to view the **Readme** file and click **Finish**.

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**.

2. The Sun StorageTek Business Analytics Management Console Login window appears.
3. Log in using the default administrative account, gsmuser, as both the username and password, as shown in the Management Console Login window that appears below.

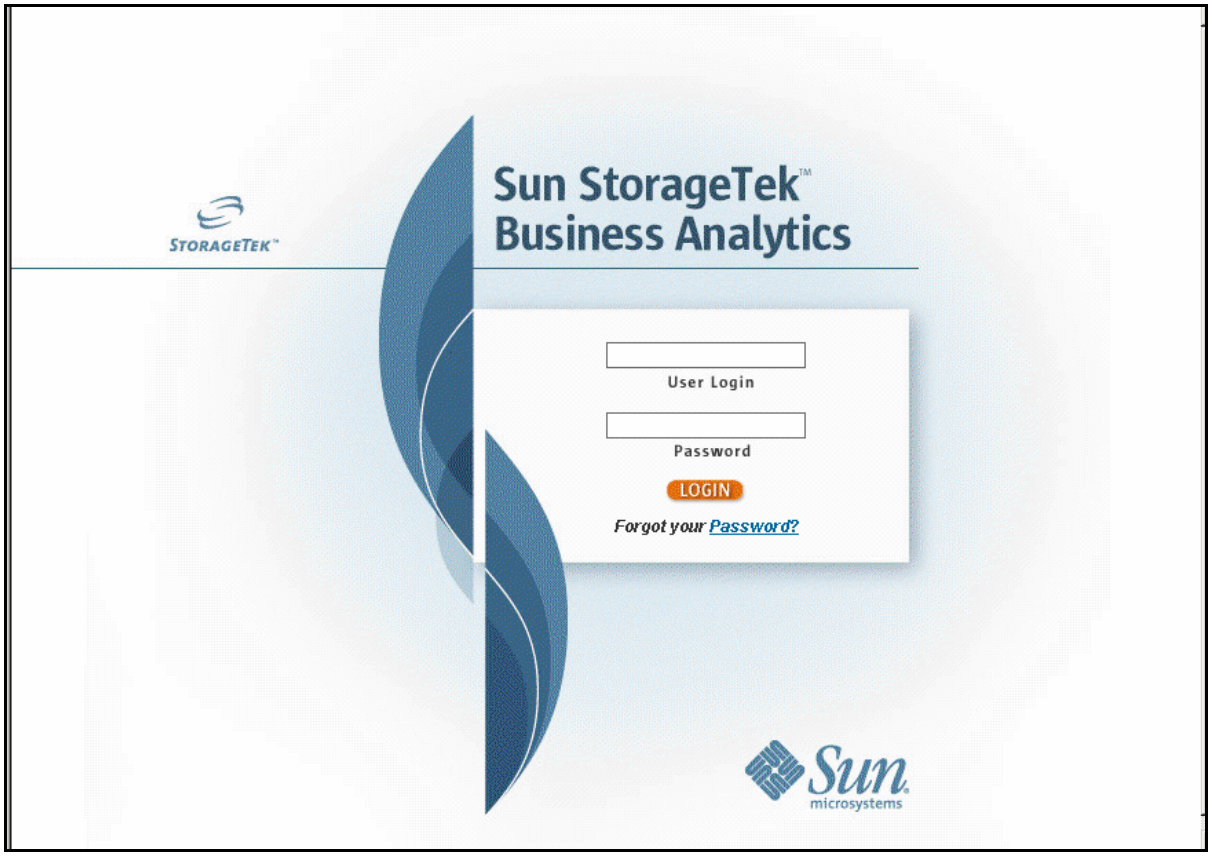


Figure 54 - Management Console Login Window

4. 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

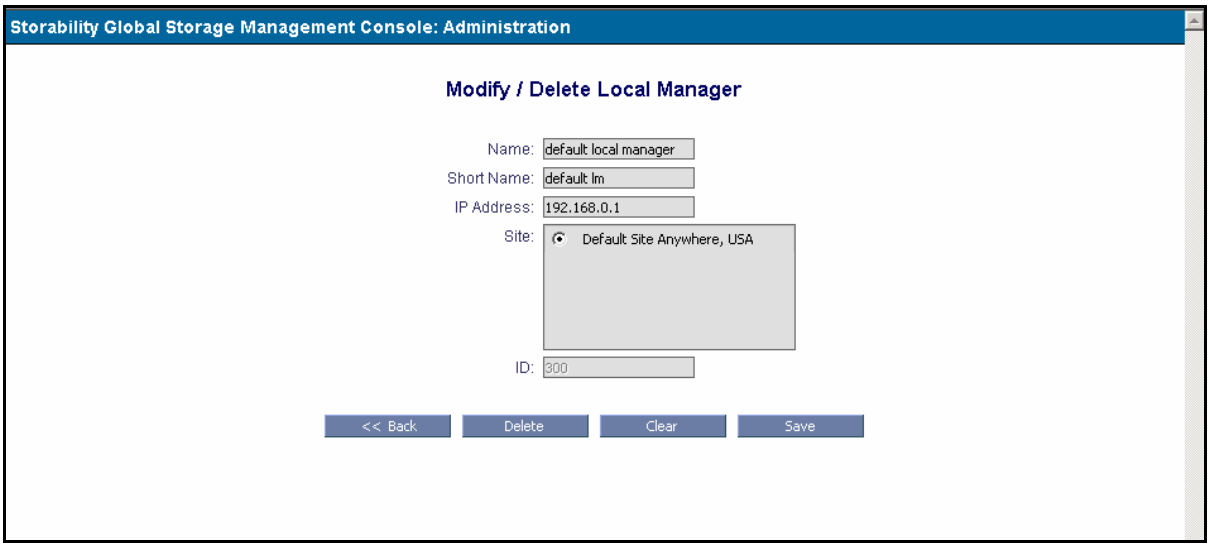
5. Customize the default Local Manager:
   a. Select **Tools** -> **Site/Local Manager Administration**.

Figure 55 - 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.

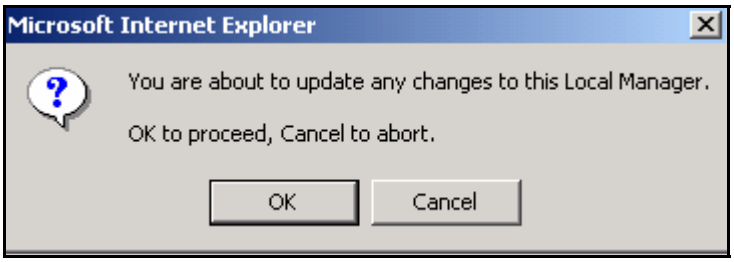


Figure 56 - Update Changes to Local Manager

6. 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

7. Create a View:

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

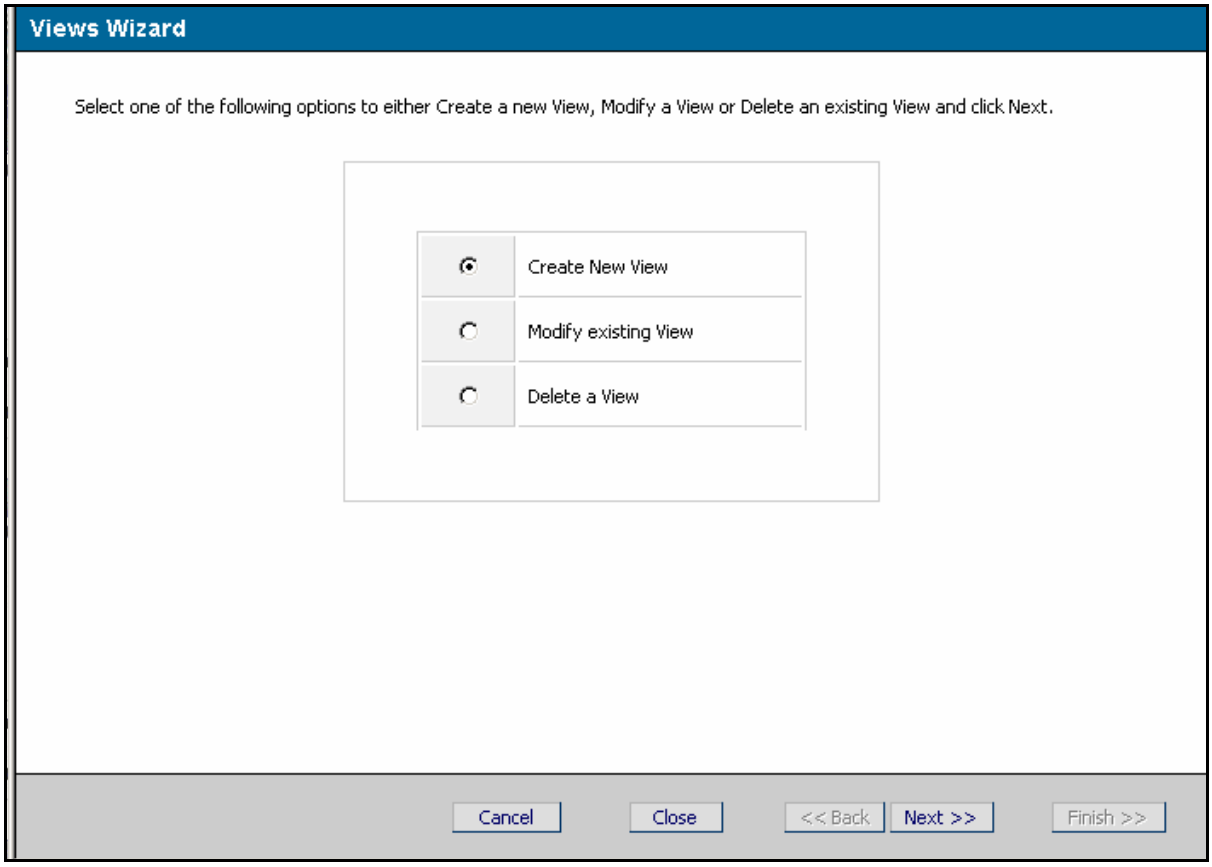


Figure 57 - Views Wizard

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).

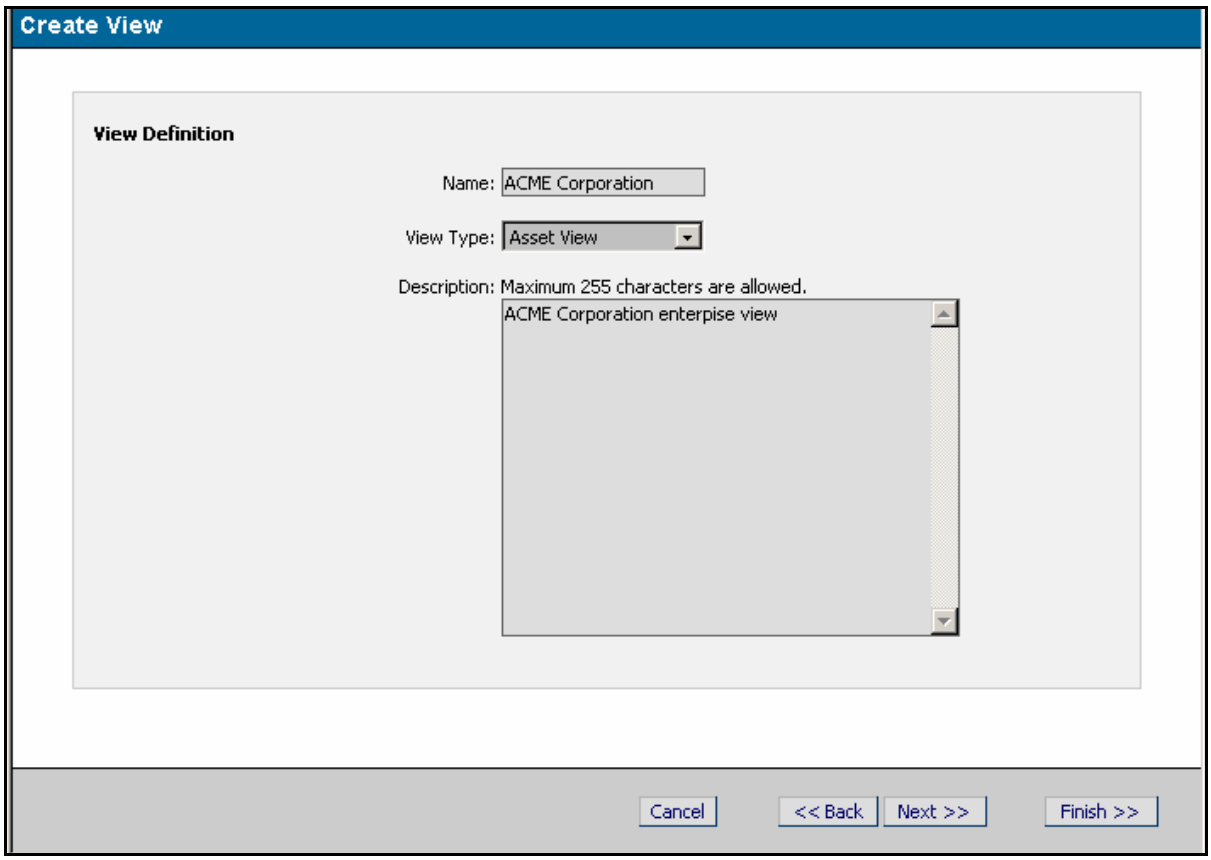


Figure 58 - Create View

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.

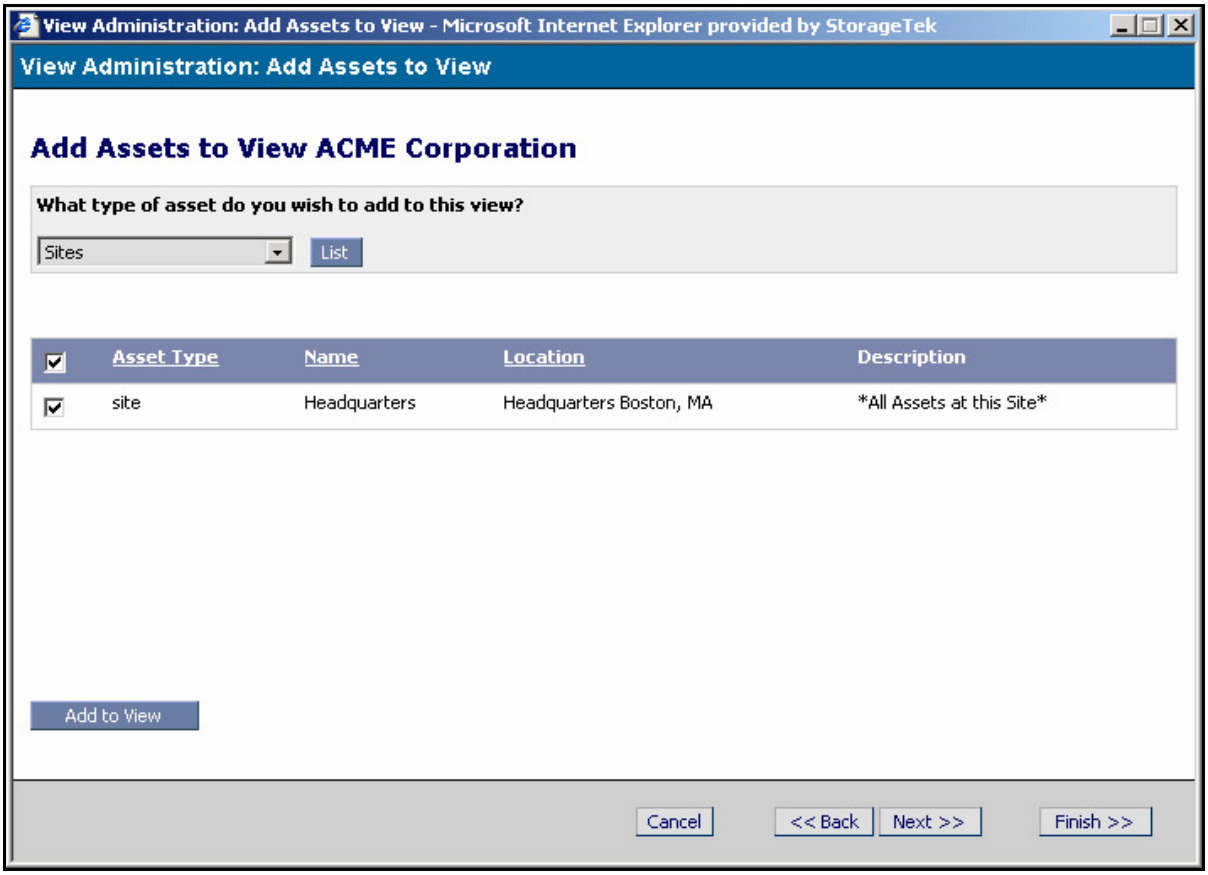


Figure 59 - Add Assets to View

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.

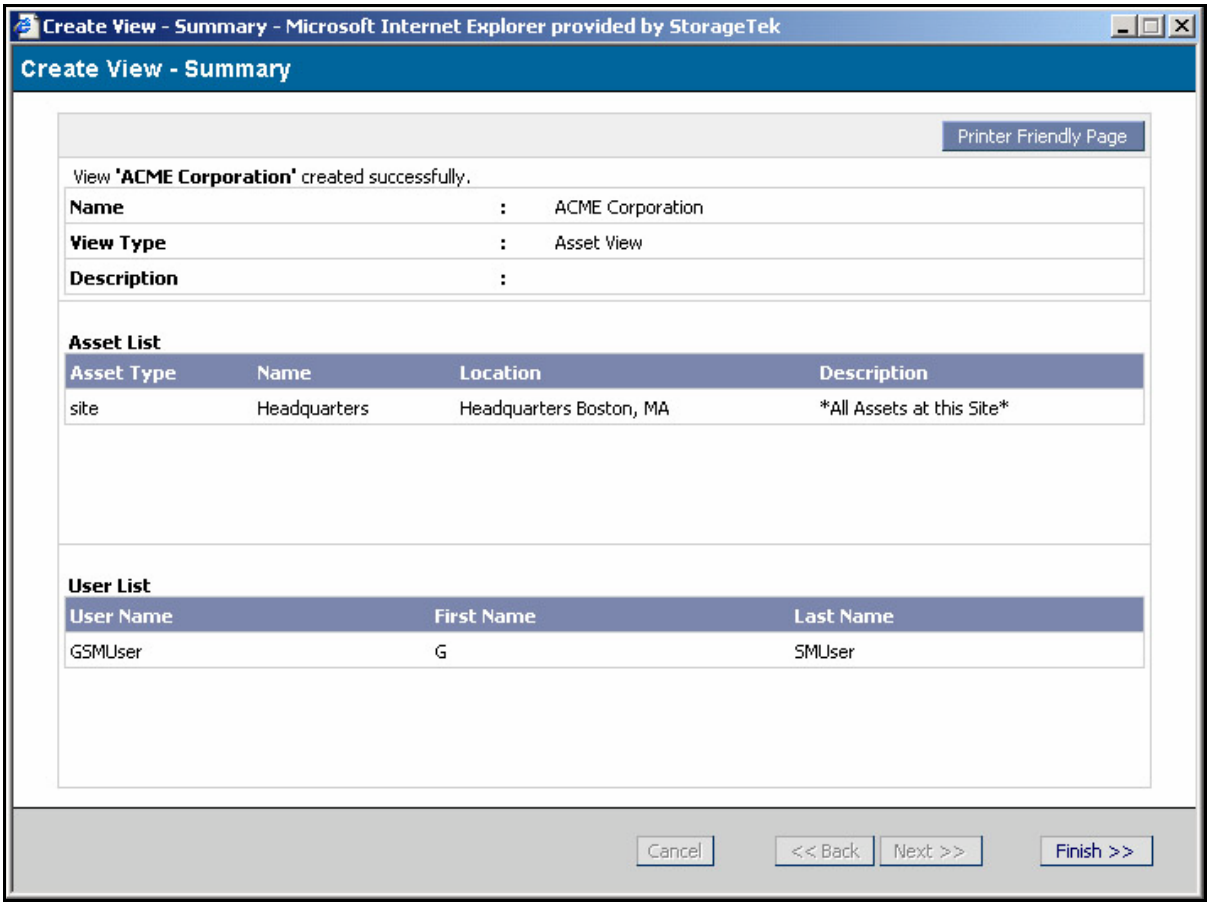


Figure 60 - Create View - Summary

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

8. 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.
9. 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 panes.

DATA POLLING SCHEDULES

10. 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 Storability 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 **Filesystyem**.
    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.

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.

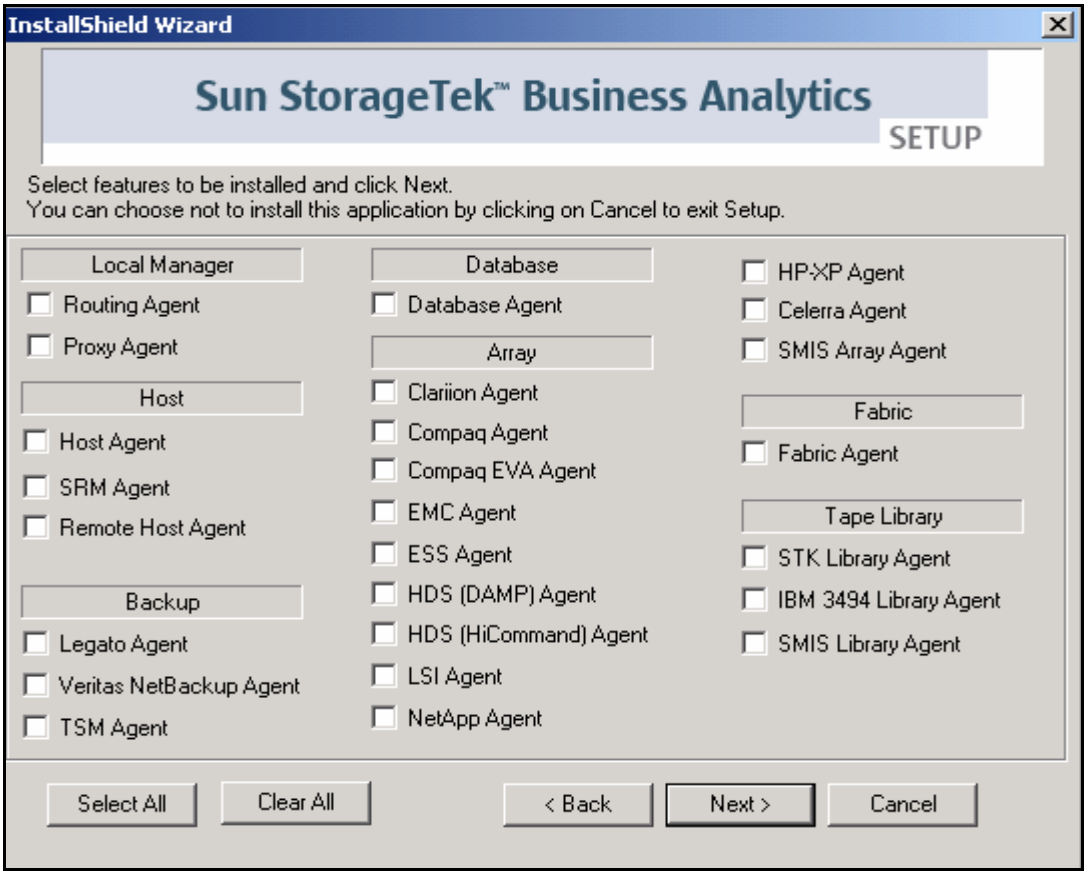


Figure 61 - Select Features To Be Installed

Notes: If you are running the installation after previously agents, the installation screen contains check marks in the checkboxes 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.

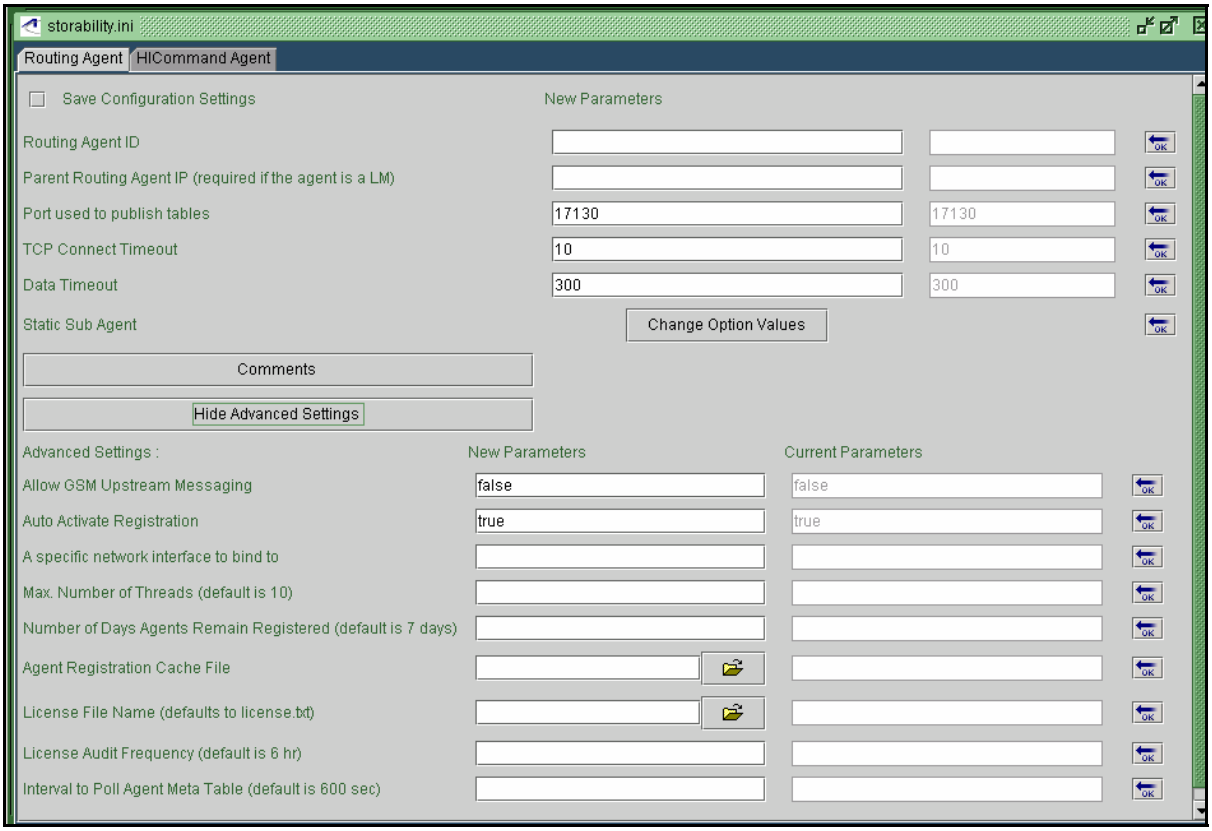


Figure 62 - Routing Agent Configuration Tool Window

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 Local Manager/Central Manager that will collect the agent data.

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.

- **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.

INSTALLING LOCAL MANAGER - SOLARIS

This section describes installing the Sun Storagetek Business Analytics Local Manager packages on a Solaris server, including GSMbase, GSMlmutil, and GSMroute. During the installation of GSMbase and GSMlmutil, you can optionally specify a user account for the agents that do not require root privilege to run under and for the required group ownership of GSM files. The default values are:

- The user name is gsm.
- The group name is gsm.
- The Group ID is 1090.

The GSMbase and GSMlmutil packages must be installed on the Local Manager (or other server platform) before specific Smart Agents (e.g., Fabric Agent) are installed.

1. Insert the Sun StorageTek Business Analytics Installation CD for Solaris into the CDROM drive.
2. Mount the CD using the following command, for example:

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

3. Change directory to the directory corresponding to the host's Solaris Operating System version. Display the /etc/release file if the Operating System version information is not available.

4. Type the following command to install GSMbase, GSMlmutil, and GSMroute.

```
pkgadd –d . GSMbase GSMlmutil GSMroute
```

5. Enter a different installation directory or press **Enter** to accept /opt/storability as the installation directory.

```
root@symmsun01# pkgadd -d . GSMbase GSMlmutil GSMroute

Processing package instance <GSMbase> from </jp/Unix/Solaris/8>

Storability GSM base
(sparc) prod-4.0.3
Copyright (c) 2002 Storability, Inc
All Rights Reserved

This is licensed software.  By installing this software you agree
to the terms of the license agreement included with the package in
/opt/storability/GSM-license.txt

GSMbase was built on SunOS 5.7.


Please enter the path where Global Storage Manager 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? [/app/storability] [?]

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

Local Manager address for agent registration? [localhost]

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

Figure 63 – GSMbase Package Installation

6. For "Enable automatic agent registration? [y] [y,n,?]", simply press **Enter** to accept that agent auto registration is turned on or type **n** and press **Enter** to disable it.

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

   If you press **Enter** to accept the default value, the GSM_LM_HOST value will not be created in a GSMBase section of the storability.ini file. If you type the IP Address, that IP address becomes the default Local Manager value for agent auto registration when you subsequently install other agents. The IP address will appear enclosed in brackets beside the Local Host prompt to show it is the default value during the installation of subsequent agents.

8. For "Local Manager port number", press **Enter** to accept the default TCP port number (17146) the Local Manager uses for agent auto registration (or specify a different port number if you know the default port number was changed when the agent was started).

9. The installation next prompts you for the group name to be used by agents not required to run as root. If the group does not exist, the package installation (pkgadd) will prompt you whether (y/n) to create it.

```
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 GSM files requires that the group exist.

Group name for GSM files? [gsm]

group 'gsm' does not yet exist.

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

GID for gsm? [1090] [?]

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.
```

Figure 64 - GSM Account Information

10. Press **Enter** to accept the default GID of1090, or set the identifier to a different, unique integer value for your UNIX environment.

11. Read the informational text on the Agent Monitor. Specify (y/n) whether to have the agent restarted if down using the Agent Monitor.

```
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.

Automatically restart stopped agents by default? [n] [y,n,?]
```

Figure 65 - Agent Monitor

12. Press **Enter** to accept the default (no) or enter **y**.

13. Specify whether (y/n) to allow the installation directory to be created, if prompted.

14. When prompted, enter **y** to allow the installation of GSMbase to continue. The installation proceeds and returns you to the main package installation menu. You can next choose to install the required Local Manager Utilities.

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

Installing Storability GSM base as <GSMbase>

## Executing preinstall script.
group 'gsm' created
## Installing part 1 of 1.
/app/storability/GSM-license.txt
/app/storability/etc/agents
/app/storability/lgpl-license.txt
/app/storability/lib/libgcc_s.so.1
/app/storability/lib/libstdc++.so.5 <symbolic link>
/app/storability/lib/libstdc++.so.5.0.0
/app/storability/openssl-license.txt
/app/storability/pcre-license.txt
/app/storability/pegasus-license.txt
/app/storability/snia-license.txt
/app/storability/snmp++-license.txt
/app/storability/xercesc-license.txt
[ verifying class <none> ]
/opt/storability <symbolic link>
[ verifying class <dirlink> ]
Modifying /etc/init.d/storabilityAgents
[ verifying class <build> ]
/etc/rc0.d/K07storabilityAgents <symbolic link>
/etc/rc1.d/K07storabilityAgents <symbolic link>
/etc/rc3.d/S93storabilityAgents <symbolic link>
/etc/rcS.d/K07storabilityAgents <symbolic link>
[ verifying class <blink> ]
/app/storability/etc/storability.ini:   updated.
[ verifying class <ini> ]

Installation of <GSMbase> was successful.

Processing package instance <GSMlmutil> from </jp/Unix/Solaris/8>
```

Figure 66 - GSMBase Install Completed

Install Local Manager Utilities (lmutil)
The lmutil package installs the Local Manager utilities, including the inicrypt program for password encryption and the bulkall utility to test access to a SNMP MIB.

15. The Local Manager Utilities (GSMlmutil) package is processed after the GSMbase installation has completed.

16. Press **Enter** to accept the default account name for Business Analytics agent files, or specify a different user account.

17. If the user account does not exist, enter **y** to let the script create it or **n** to not have it automatically created.

18. Press **Enter** to accept the default account name, gsm, or specify a different account name.

19. Press **Enter** to accept the default UID of 1090, or set the UID to the desired integer value.

20. When prompted, enter **y** to continue with the installation. The installation proceeds and the **GSMroute** package is next processed.

```
Installation of <GSMlmutil> was successful.

Processing package instance <GSMroute> from </jp/Unix/Solaris/8>

Storability GSM Routing Agent
(sparc) prod-4.0.3
Copyright (c) 2002 Storability, Inc
All Rights Reserved

This is licensed software.  By installing this software you agree
to the terms of the license agreement included with the package in
/opt/storability/GSM-license.txt

GSMroute was built on SunOS 5.7.


Unique routing ID?  [?] 302

Is this system a central manager? [n] [y,n,?] n

Central manager address? [done] 192.168.1.2

CM registration port? [17146] [?]

Central manager address? [done]
```

Figure 67- GSMroute Package Configuration

21. For "Unique Routing ID", enter the unique **Routing ID** to match the one generated when you added this Local Manager to the Sun StorageTek Business Analytics application using the Management Console's **Site/Local Manager Administration** menus.

22. For "Is this system a Central Manager", enter **n** and press **Enter** to specify this is NOT a Central Manager.

23. For Central manager address", enter the IP address or network resolvable host name of the Local Manager/Central Manager that will collect the agent data and press **Enter**. This is a required configuration setting (RA_PARENT) for all Local Managers.

24. For "CM Registration Port" specify the TCP port number the Central Manager/Local Manager (Parent RA) uses for agent auto registration. The default port number is 17146.

25. On a blank "Central Manager address" line, press **Enter** to specify you have completed these configuration settings.

26. Type **y** and press **Enter** to review/modify the **Advanced Settings**.

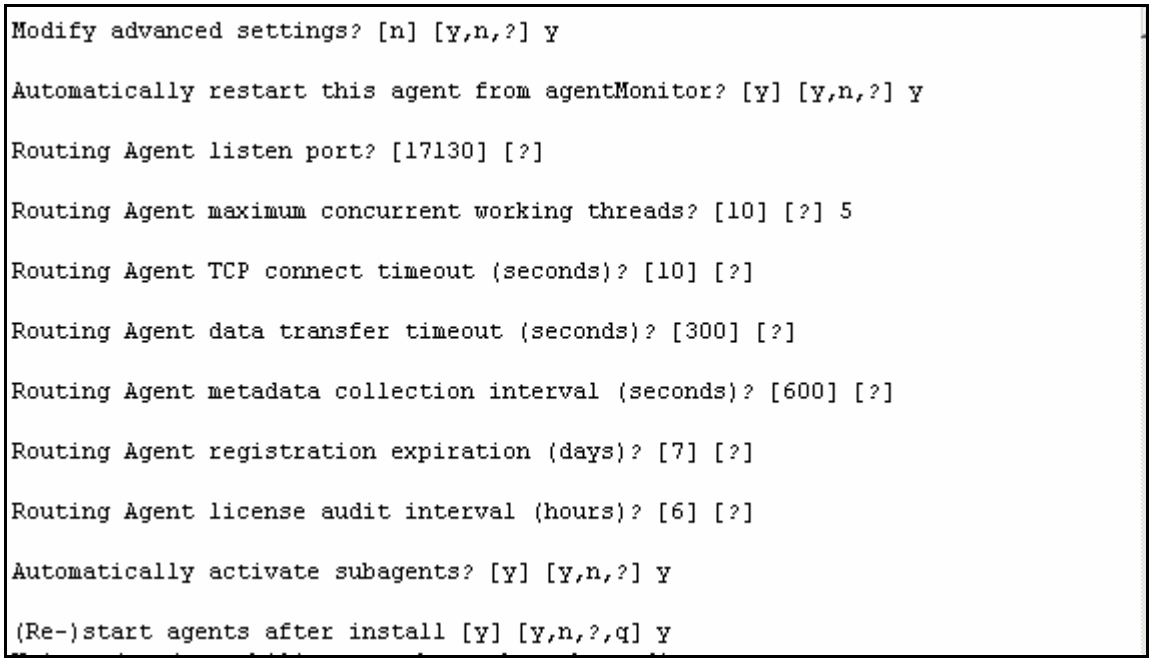


Figure 68 - Routing Agent Advanced Settings

- AgentMonitor – Specify **n** (no) unless you enabled the Agent Monitor during the base package installation.
- The Routing Agent "listen" port is 17130 by default.
- The default **TCP Connect Timeout** time interval (10 seconds) to connect to an agent should be fine for most TCP environments.
- The **data transfer timeout** is generally ignored because the 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.
- The **metadata collection interval** specifies how often in seconds to gather object schemas from sub agents; the default value is 600 seconds.
- **Agent registration expiration** 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.
- The **license audit interval** specifies how often to perform license audit; is not applicable for Local Manager.
- The **automatically activate registration** setting turns on or off the capability to automatically register agents.
- By default, the agents will be automatically restarted after installation is complete.

  Note: If you plan to manually add agent data collection configuration settings for GSM 3.x agent(s), you may want to wait and restart the agents after you have completed this task.

27. After you have reviewed/modified the **Advanced Settings** the installation prompts you to continue with the installation of the Routing Agent. Type **y** and press **Enter** to continue.

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

Installing Storability GSM Routing Agent as <GSMroute>

## Executing preinstall script.
## Installing part 1 of 1.
/app/storability/bin/routingAgent
/app/storability/etc/agents-registry
[ verifying class <none> ]
Modifying /etc/init.d/routingAgent
[ verifying class <build> ]
/app/storability/etc/agents:    updated.
[ verifying class <cfg> ]
/app/storability/etc/storability.ini:   updated.
[ verifying class <ini> ]
/app/storability/data/Message.log
/app/storability/data/ardb.dat
[ verifying class <touch> ]
## Executing postinstall script.
Storability agent startup:
Starting Storability routing agent:             routingAgent started
Storability agent startup complete.

Installation of <GSMroute> was successful.
```

Figure 69 - Routing Agent Advanced Settings

The installation of the Routing Agent completes and you are returned to the command line.

28. Use a system editor (e.g., vi) to add SUB_AGENT entries for agents not using agent auto registration, if any. For example:

```
SUB_AGENT=17152|192.255.252.70
```

29. Restart the Routing Agent if it is not running.

```
/etc/init.d/routingAgent start
```

30. Use the process status (ps) command to verify the Routing Agent is started before you proceed to verify agent functionality. A sample command output when the Routing Agent is running follows. Note that it was started using the default user account, gsm.

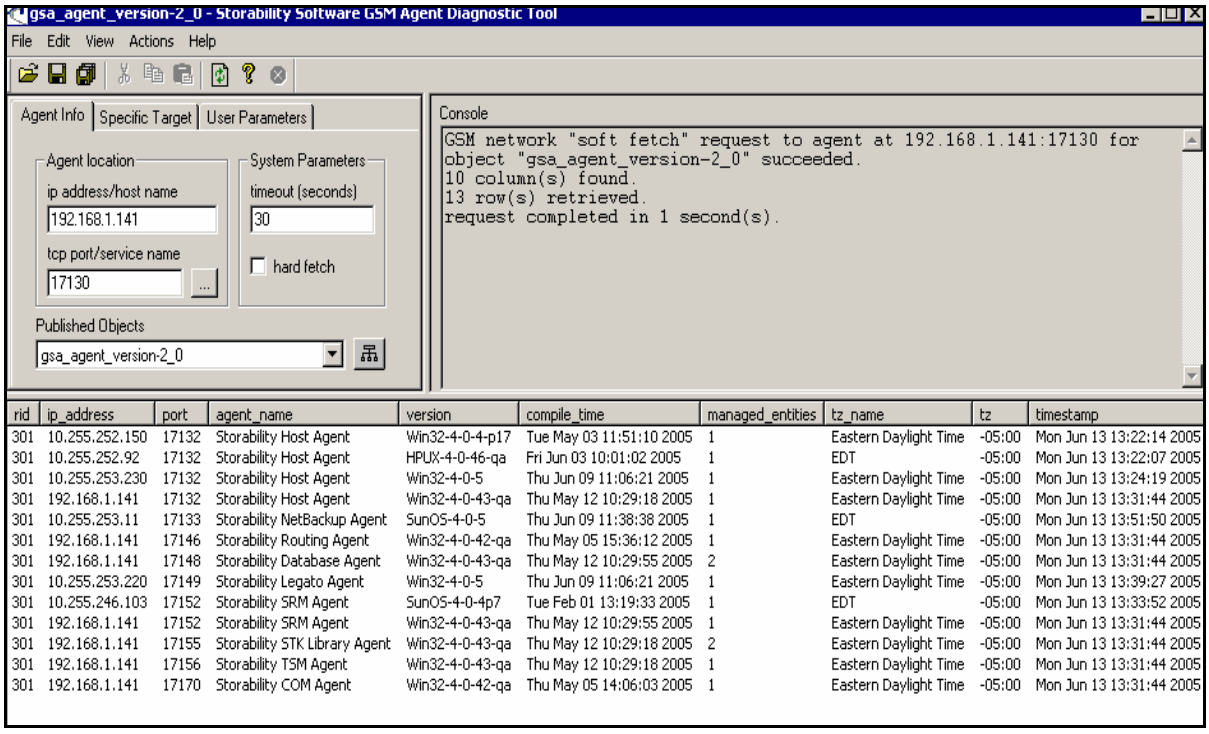
```
Last login: Wed Oct 27 08:50:01 2004 from 192.168.1.136
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
root@symmsun01# ps -ef | grep storability
    gsm 26128     1  0 18:15:28 ?        0:10 /app/storability/bin/routingAgent
 -w /app/storability/bin -msgdir /app/storabil
root@symmsun01#
```

Figure 70 - Verify Routing Agent Running

VERIFY LOCAL MANAGER FUNCTIONALITY

The Agent Diagnostic Tool (gsmdiag.exe) should be used to verify the Local Manager. Proceed as follows:

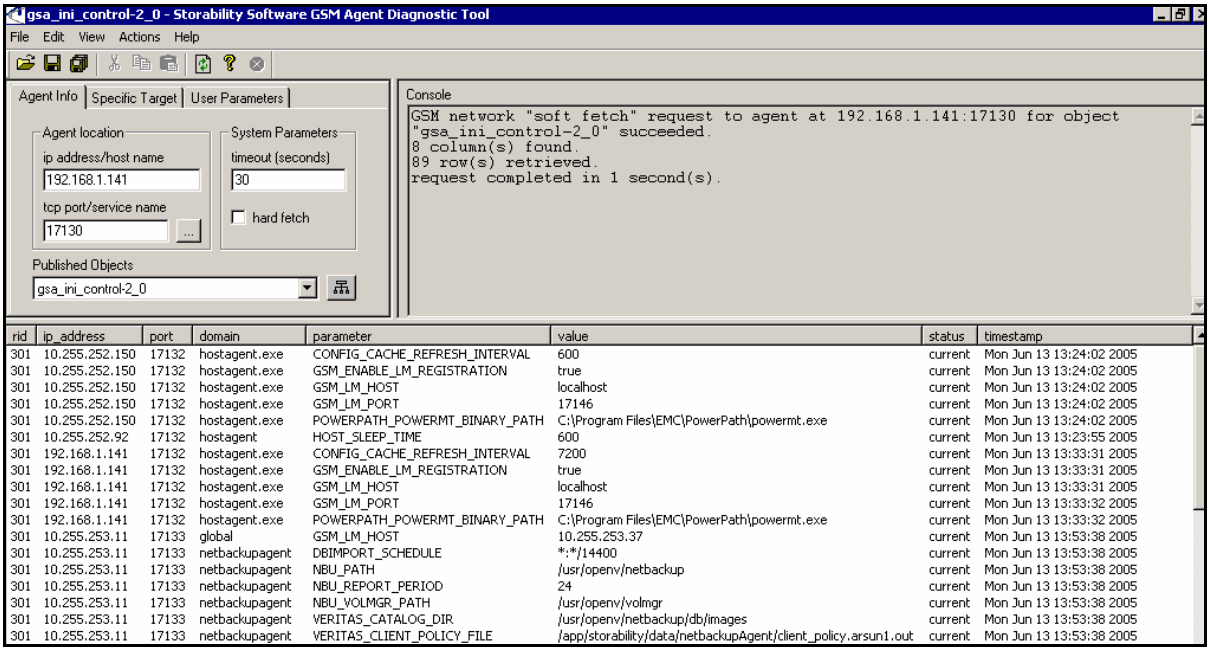
1. Using **Windows Explorer**, launch gsmdiag.exe that is located in the <drive>:\Program Files\Storability\GSM\Utilities\Storability Local Manager folder on Windows Local Managers and the Central Manager.
   a. Wait approximately 30 seconds after the Routing Agent has started to allow it to initialize before querying it with GSMdiag.
   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



rid	ip_address	port	agent_name	version	compile_time	managed_entities	tz_name	tz	timestamp
301	10.255.252.150	17132	Storability Host Agent	Win32-4-0-4-p17	Tue May 03 11:51:10 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:22:14 2005
301	10.255.252.92	17132	Storability Host Agent	HPUX-4-0-46-qa	Fri Jun 03 10:01:02 2005	1	EDT	-05:00	Mon Jun 13 13:22:07 2005
301	10.255.253.230	17132	Storability Host Agent	Win32-4-0-5	Thu Jun 09 11:06:21 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:24:19 2005
301	192.168.1.141	17132	Storability Host Agent	Win32-4-0-43-qa	Thu May 12 10:29:18 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005
301	10.255.253.11	17133	Storability NetBackup Agent	SunOS-4-0-5	Thu Jun 09 11:38:38 2005	1	EDT	-05:00	Mon Jun 13 13:51:50 2005
301	192.168.1.141	17146	Storability Routing Agent	Win32-4-0-42-qa	Thu May 05 15:36:12 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005
301	192.168.1.141	17148	Storability Database Agent	Win32-4-0-43-qa	Thu May 12 10:29:55 2005	2	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005
301	10.255.253.220	17149	Storability Legato Agent	Win32-4-0-5	Thu Jun 09 11:06:21 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:39:27 2005
301	10.255.246.103	17152	Storability SRM Agent	SunOS-4-0-4p7	Tue Feb 01 13:19:33 2005	1	EDT	-05:00	Mon Jun 13 13:33:52 2005
301	192.168.1.141	17152	Storability SRM Agent	Win32-4-0-43-qa	Thu May 12 10:29:55 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005
301	192.168.1.141	17155	Storability STK Library Agent	Win32-4-0-43-qa	Thu May 12 10:29:18 2005	2	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005
301	192.168.1.141	17156	Storability TSM Agent	Win32-4-0-43-qa	Thu May 12 10:29:18 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005
301	192.168.1.141	17170	Storability COM Agent	Win32-4-0-42-qa	Thu May 05 14:06:03 2005	1	Eastern Daylight Time	-05:00	Mon Jun 13 13:31:44 2005

Figure 71 - GSMdiag: 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).



rid	ip_address	port	domain	parameter	value	status	timestamp
301	10.255.252.150	17132	hostagent.exe	CONFIG_CACHE_REFRESH_INTERVAL	600	current	Mon Jun 13 13:24:02 2005
301	10.255.252.150	17132	hostagent.exe	GSM_ENABLE_LM_REGISTRATION	true	current	Mon Jun 13 13:24:02 2005
301	10.255.252.150	17132	hostagent.exe	GSM_LM_HOST	localhost	current	Mon Jun 13 13:24:02 2005
301	10.255.252.150	17132	hostagent.exe	GSM_LM_PORT	17146	current	Mon Jun 13 13:24:02 2005
301	10.255.252.150	17132	hostagent.exe	POWERPATH_POWERMT_BINARY_PATH	C:\Program Files\EMC\PowerPath\powermt.exe	current	Mon Jun 13 13:24:02 2005
301	10.255.252.92	17132	hostagent	HOST_SLEEP_TIME	600	current	Mon Jun 13 13:23:55 2005
301	192.168.1.141	17132	hostagent.exe	CONFIG_CACHE_REFRESH_INTERVAL	7200	current	Mon Jun 13 13:33:31 2005
301	192.168.1.141	17132	hostagent.exe	GSM_ENABLE_LM_REGISTRATION	true	current	Mon Jun 13 13:33:31 2005
301	192.168.1.141	17132	hostagent.exe	GSM_LM_HOST	localhost	current	Mon Jun 13 13:33:31 2005
301	192.168.1.141	17132	hostagent.exe	GSM_LM_PORT	17146	current	Mon Jun 13 13:33:32 2005
301	192.168.1.141	17132	hostagent.exe	POWERPATH_POWERMT_BINARY_PATH	C:\Program Files\EMC\PowerPath\powermt.exe	current	Mon Jun 13 13:33:32 2005
301	10.255.253.11	17133	global	GSM_LM_HOST	10.255.253.37	current	Mon Jun 13 13:53:38 2005
301	10.255.253.11	17133	netbackupagent	DBIMPORT_SCHEDULE	*:*/14400	current	Mon Jun 13 13:53:38 2005
301	10.255.253.11	17133	netbackupagent	NBU_PATH	/usr/openv/netbackup	current	Mon Jun 13 13:53:38 2005
301	10.255.253.11	17133	netbackupagent	NBU_REPORT_PERIOD	24	current	Mon Jun 13 13:53:38 2005
301	10.255.253.11	17133	netbackupagent	NBU_VOLMGR_PATH	/usr/openv/volmgr	current	Mon Jun 13 13:53:38 2005
301	10.255.253.11	17133	netbackupagent	VERITAS_CATALOG_DIR	/usr/openv/netbackup/db/images	current	Mon Jun 13 13:53:38 2005
301	10.255.253.11	17133	netbackupagent	VERITAS_CLIENT_POLICY_FILE	/app/storability/data/netbackupAgent/client_policy.arsun1.out	current	Mon Jun 13 13:53:38 2005

Figure 72 - Sample Routing Agent Configuration Settings

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 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 **pkgadd** command to access the main package installation main menu. See Figure 1.

6. Select the **GSMproxy** agent.

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 GSMlmutil package includes the Storability Agent Monitor. The GSMbase 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

GSMbase Installation

During the GSMbase 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.

GSMlmutil Installation

The GSMlmutils package installation is recorded below.

```
root@sbolabsol03# pkgadd -d . GSMlmutil

Processing package instance <GSMlmutil> from </gsmcd/Unix/Solaris/8>

Storability GSM Local Manager utilities
(sparc) prod-4.0.4p7
Copyright (c) 2002 Storability, Inc
All Rights Reserved

This is licensed software.  By installing this software you agree
to the terms of the license agreement included with the package in
/opt/storability/GSM-license.txt

GSMlmutil was built on SunOS 5.7.


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 <GSMlmutil> [y,n,?] y

Installing Storability GSM Local Manager utilities as <GSMlmutil>

## 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.
```

GSMlmutil Install – crontab Entries

The crontab is updated by the installation of the local manager utilities (GSMlmutil) 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 lmutil package appears below.

```
root@sbolabsol03# more agents
# Storability GSM Agent startup/monitoring configuration
#
# binary        rc-file         OID                             AUTO-RESTART    order
```

This file will be updated for each Storability 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 5.0 in an existing GSM Release 4.x environment, you must upgrade the following software components:

- GSM Management Console
- GSM 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 as described in the Release Notes
- Recommendation by your Sun representative

Currently, the upgrade from GSM 3.x to Sun StorageTek Business Analytics Version 5.0 is a two-step procedure:

a. Upgrade GSM 3.x to GSM 4.0
b. Upgrade GSM 4.0 to Sun StorageTek Business Analytics Release 5.0

Notes

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

Procedure Summary to Upgrade from a Previous GSM Version

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 5.0 version of Management Console.
8. Update device Smart Agents as required.
9. Configure/verify Extract, Transform, and Load (ETL) data loading process in Policy Alerting. Check to ensure the policy is enabled and that the email recipient is an appropriate user.

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 5.0 Central Manager Installation CD.

CENTRAL MANAGER SOFTWARE UPGRADE

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. Sun StorageTek Business Analytics was previously called Global Storage Manager (GSM).

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 5.0 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. Otherwise, proceed directly to the step in the procedure.
   a. Select **Start->Programs->Storability->Uninstall->Uninstall GSM 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 t**o 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.

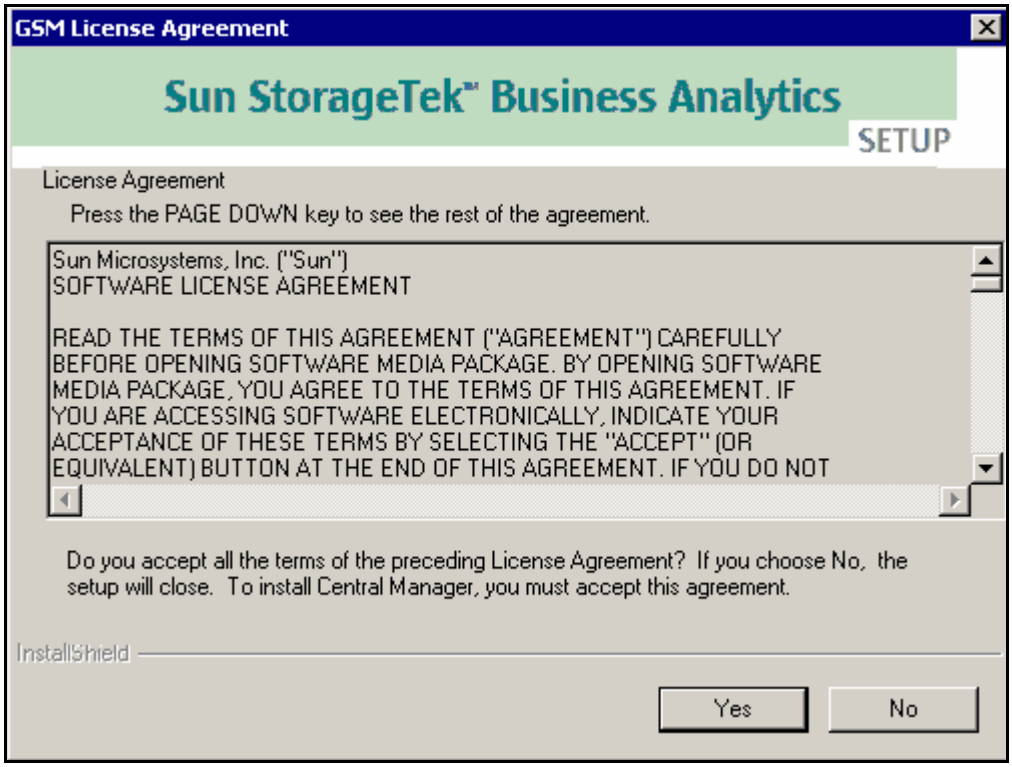


Figure 73 – GSM License Agreement

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.

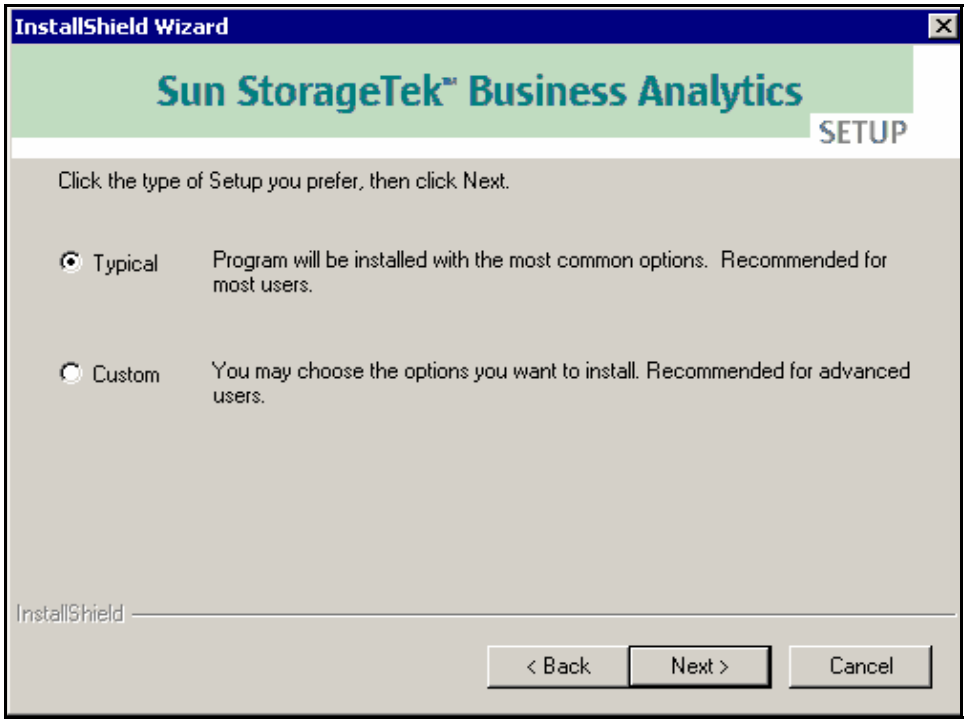


Figure 74 - Setup Type

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 5.0, you only need to upgrade software components to fix problems or add features that are stated in the Release Notes or advised by your Sun representative.

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

- **GSM Database Setup** – Creates GSM databases, tables, and installed procedures for first-time installation.
- **Storability Data Aggregator** – Aggregates collected data from Smart Agents into the assurent database.
- **Storability 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.
- **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.
- **Storability Remote Host Agent** – Provides information on remote host servers supporting either the WMI or WBEM protocols.
- **GSM Scheduled Jobs –** Adds the GSM scheduled job to the Windows Scheduler. This option should be selected if you also selected **GSM Database Setup**.
- **Storability 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:

- **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/receiving SNMP traps; is required to utilize the Real Time Events report in conjunction with the Storability NetBackup Agent.
- **Storability 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.

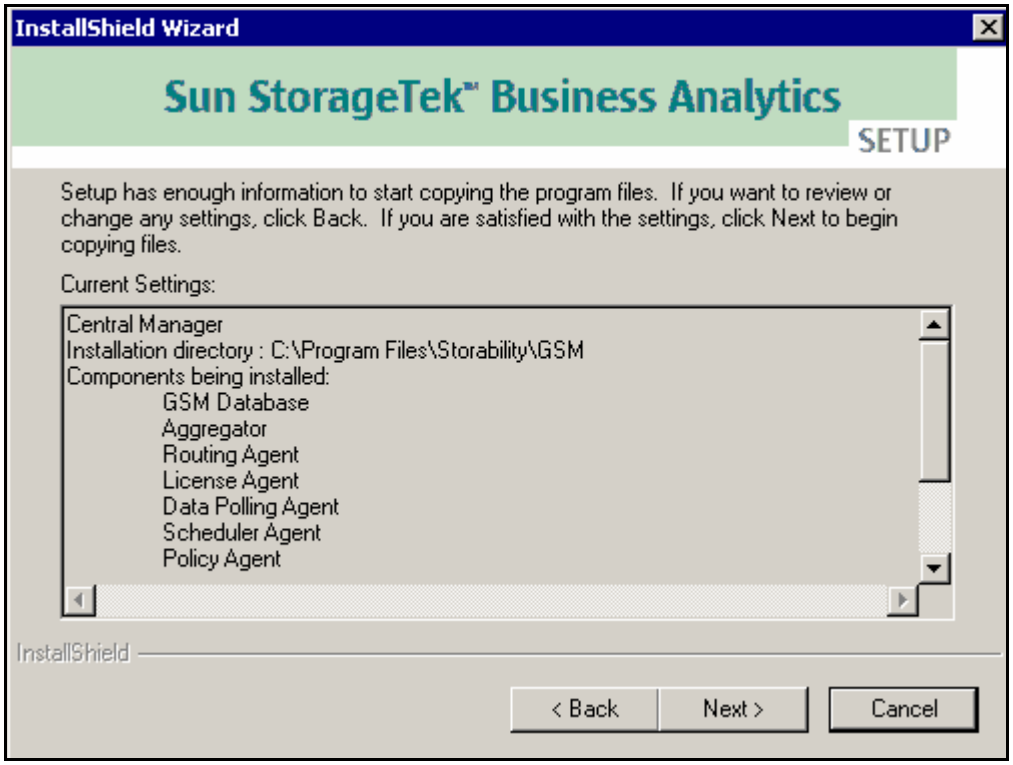


Figure 75 - Current Settings

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.

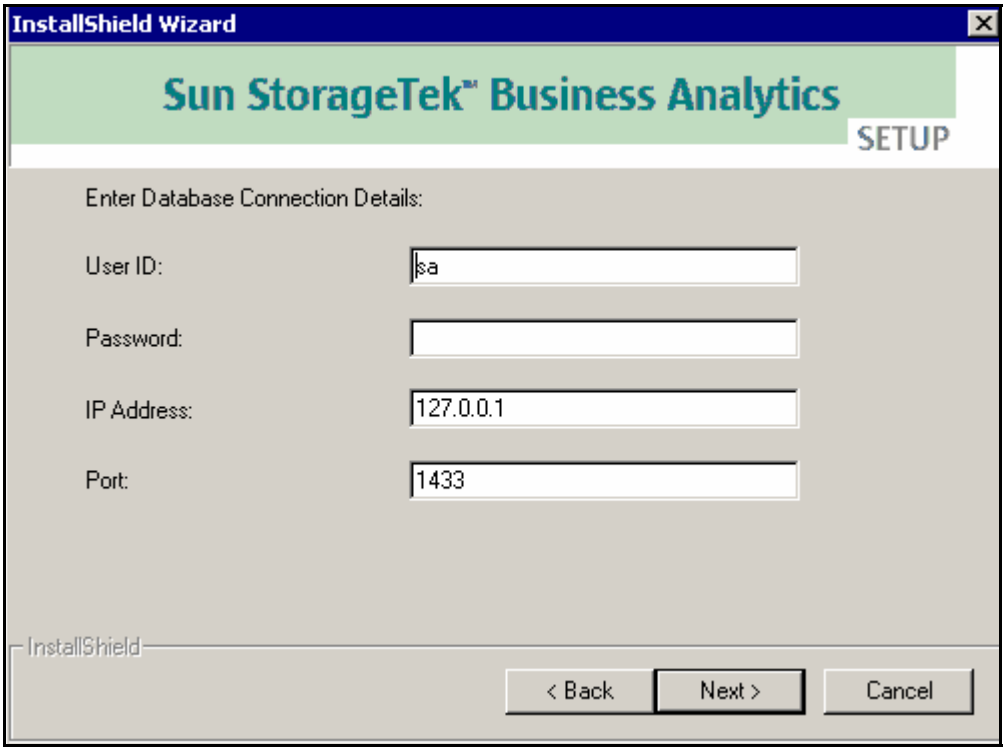


Figure 76 - Database Connection Details

17. Review/modify the following:
    - **User ID**: Specify a database user/administrator ID that possesses administrative privileges to the assurent and portal databases.

      Note: If the Database Administrator has removed permissions from the account (e.g., assurent), 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.
18. Click **Next>** to continue.
19. The "GSM Database Portal, Assurent, and their Schemas are currently present" dialog appears.
20. Select "Upgrade the Existing GSM Database and Users? "and click **Next>** to continue.
21. 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.
22. 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.

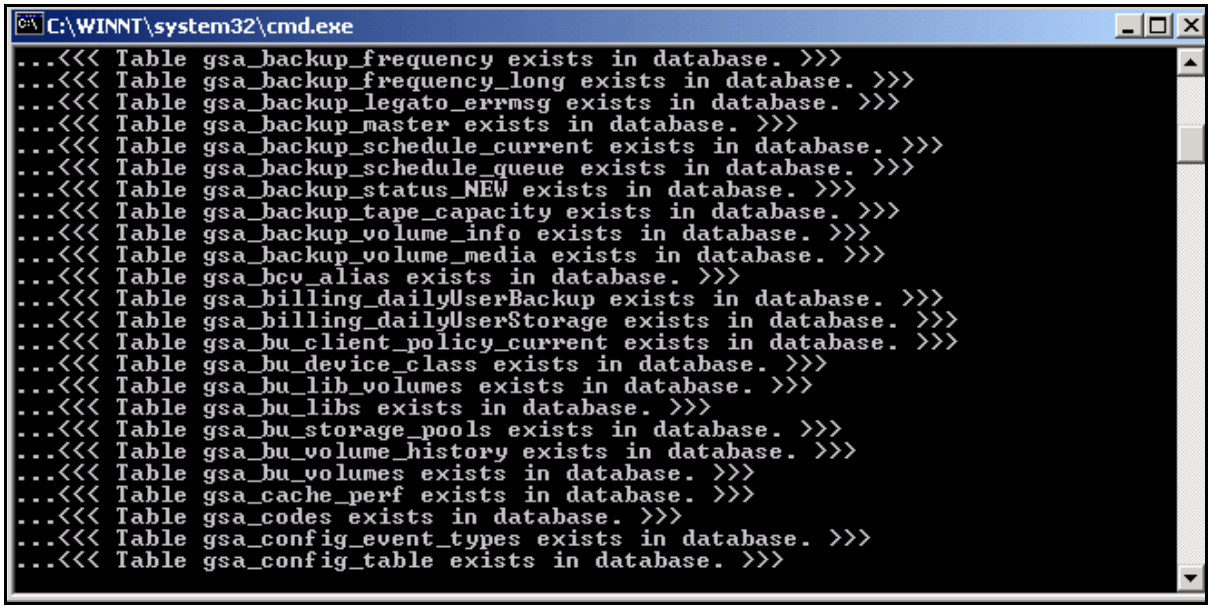


Figure 77 – Database Upgrade Messages Command Window

23. After the database setup has completed, the Scheduled Jobs are being installed dialog appears.
24. 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?

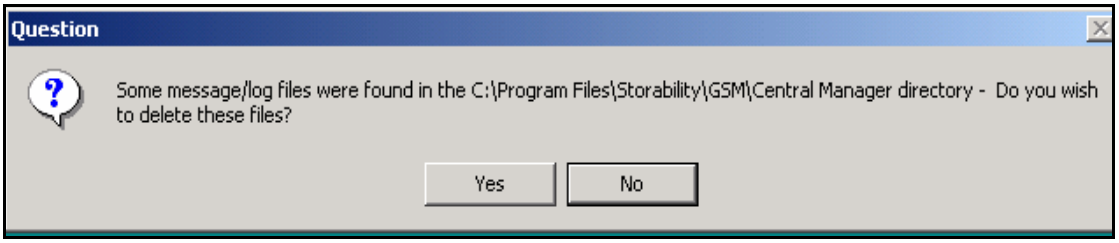


Figure 78 - Delete Central Manager Message/Log Files

25. Click **Yes** to allow the files to be deleted or **No** to retain them and the installation continues.
26. 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.
27. The Delete Previous Aggregator Message/Log files dialog appears.
28. Click **Yes** to allow the files to be deleted or **No** to retain them and the installation continues.
29. 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 79 - Installing License Agent Splash Box

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

Figure 80 - System Data Source Name for Aggregator

36. 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.
37. 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
38. Click "**Next>** to continue.
39. Click **OK** when the informational Dialog Box appears indicating the System DSN Configuration is complete.
40. 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**.
41. 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 GSM aggConvert Utility (aggConvert.exe) is run after a successful database upgrade from GSM Release 3.6.x to GSM Release 4.0.
Note: This utility is not run if you are updating a previous GSM 4.x or GSM 5.x release to the latest Sun StorageTek Business Analytics software release.

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 -Usa -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
```

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: This utility is not run if you are updating a previous GSM 4.x release to Sun StorageTek Business Analytics Release 5.0.

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 InstallShield Uninstall Wizard is launched and a dialog box appears similar to the one shown below

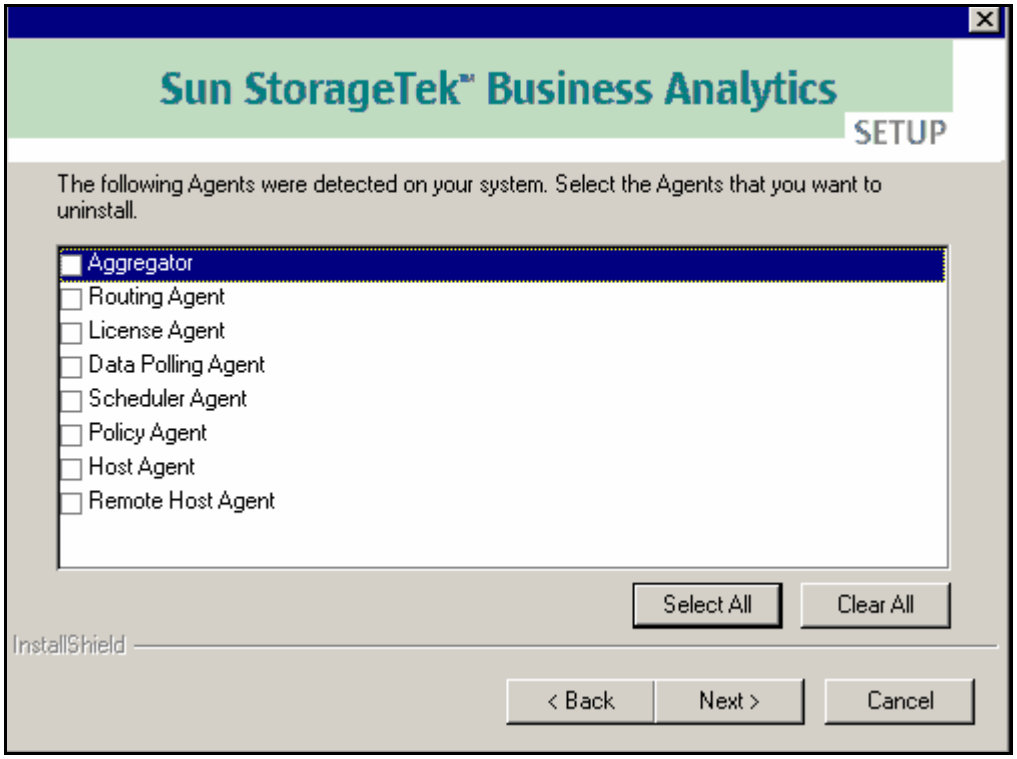


Figure 81 - Select the Agents to Uninstall

2. Click the selection box for a listed Storability 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.

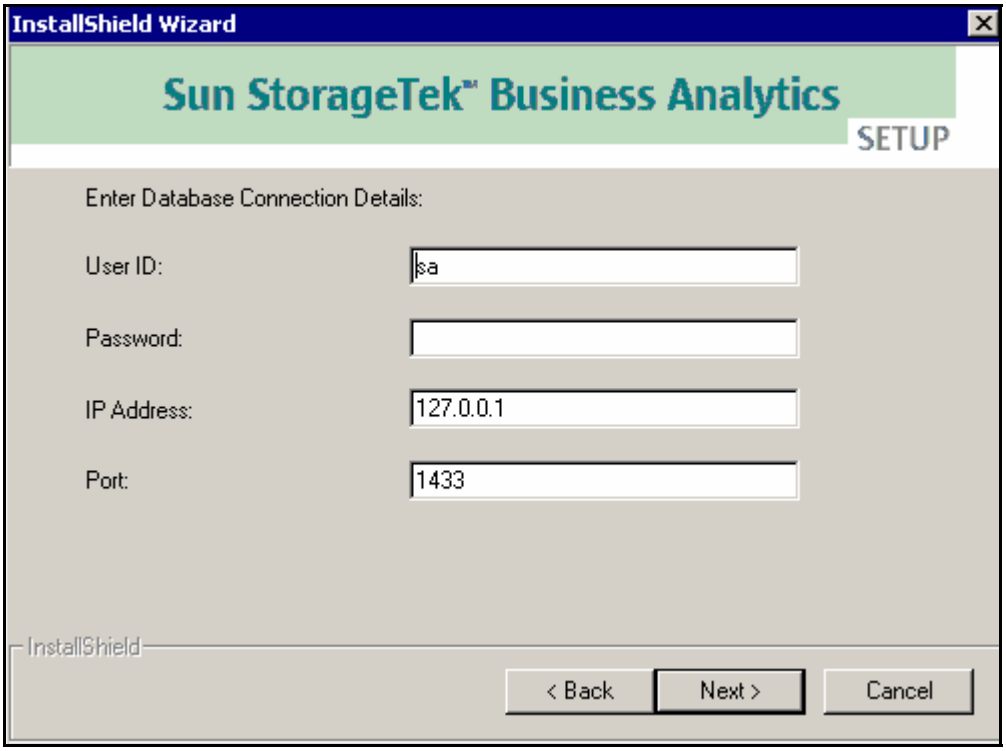


Figure 82 - Enter Database Connection Details

Review/modify the following:

- **User ID**: Specify a database user/administrator ID that possesses administrative privileges to the assurent and portal databases. The default user is assurent. The assurent user's password is st0rage.

  Note: If the Database Administrator has removed permissions from the account (e.g., assurent), the upgrade can fail because of insufficient database access permissions.

- **Password** – Enter the above user's password. The default password for the assurent 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 uninstallation 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.x to use its new report functionality.
- You upgrade an existing GSM 4.x Management Console to the latest Sun StorageTek Business Analytics Release 5.x version if it fixes a problem, as described in the Release Notes, or if recommended by Sun.

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 InstallShield Wizard.
2. The Management Console Uninstallation dialog is displayed.

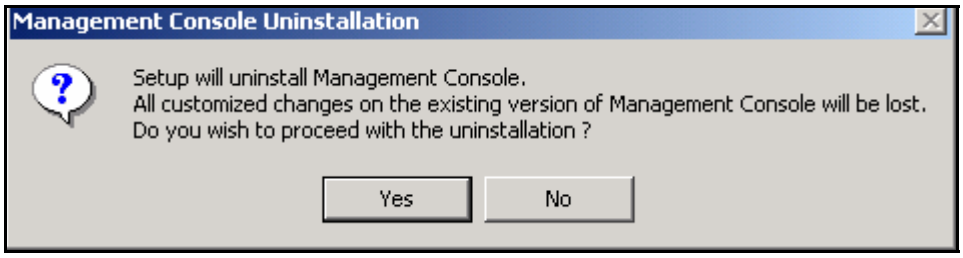


Figure 83 - Management Console Uninstallation Dialog

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.

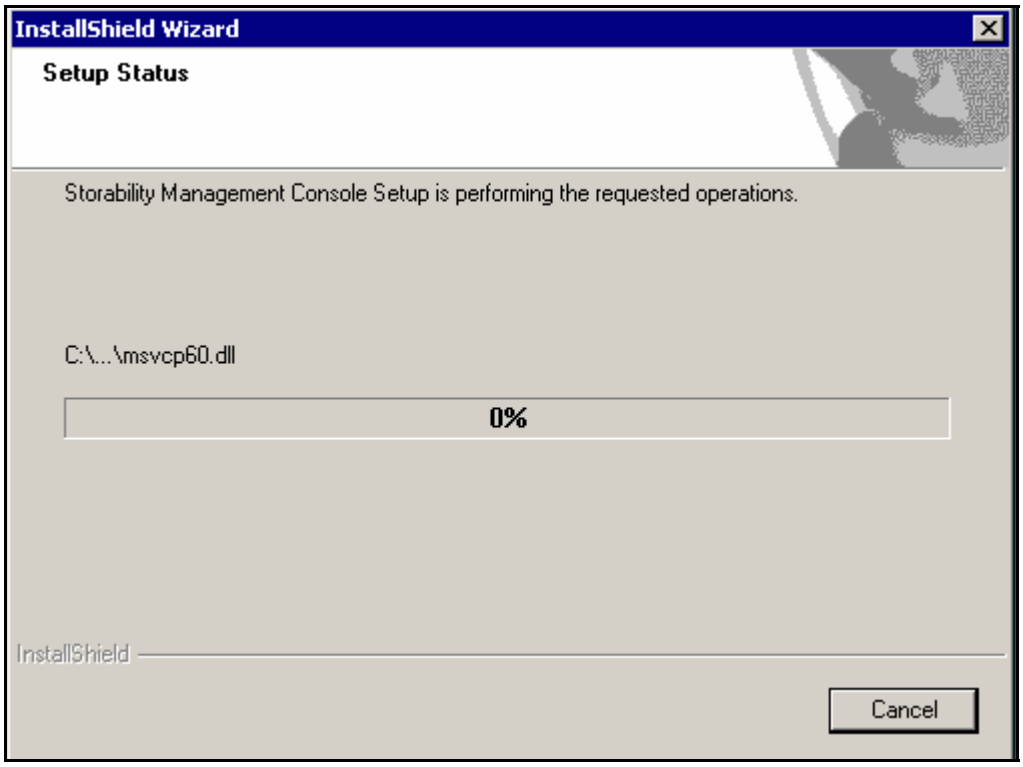


Figure 84 - Management Console Uninstallation Setup Status

5. When the InstallShield 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.

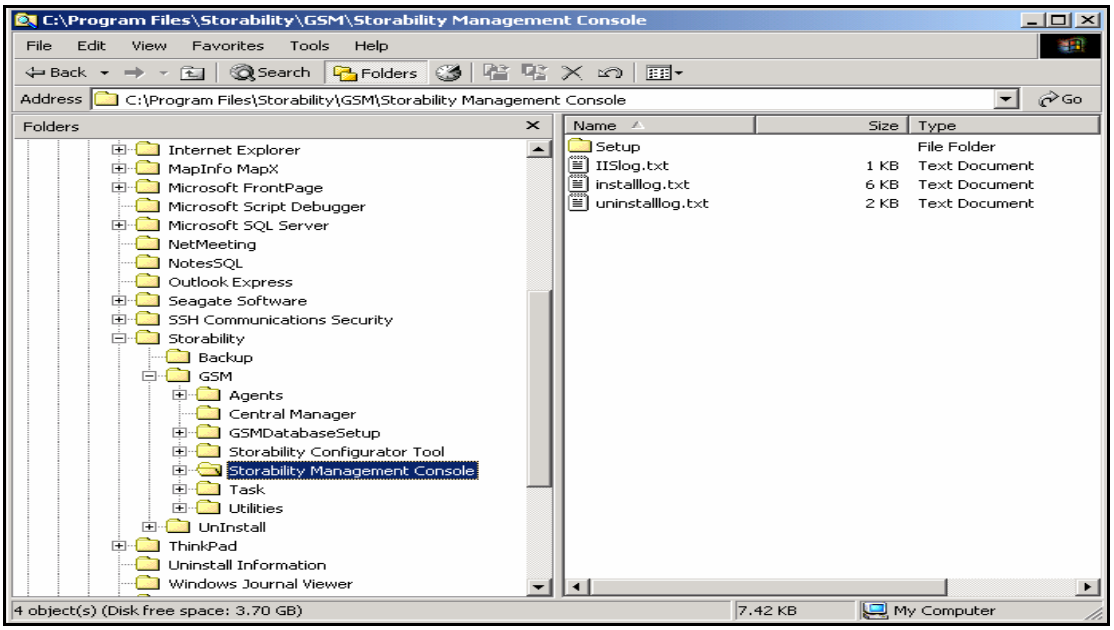


Figure 85 - Storability Management Console Directory Deletion

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 Release 5.0 version. A previously installed GSM Local Manager has either an installed Query Agent (3.x) or Routing Agent (4.x/5.x).

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 InstallShield 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 InstallShield Wizard Complete dialog to complete the uninstallation.

UPGRADE LOCAL MANAGER - SOLARIS

A Local Manager has an installed Routing Agent or Query 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 GSMlmutil, as well.

Use the package remove (pkgrm) command to remove the existing versions of GSMbase, GSMlmutil (if installed), and GSMquery or GSMroute before you proceed to upgrade to the latest version of Sun StorageTek Business Analytics.

Warning: Uninstalling the Local Manager Routing Agent can seriously impact your reporting implementation. This 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
```

   and press **Enter.**

4. The Currently Installed Package prompt appears. Type **y** and press **Enter** to confirm removing the package.

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

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 GSM 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 GSM. An administrator may want to make sure that GSM 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 GSM 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.

GSM 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 GSM 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. GSM 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.