



**IBM Electronic Service Agent for pSeries and
RS/6000**

User's Guide

SC38-7105-07

Eighth Edition (December 2005)

This edition applies to standalone AIX version 3.3 of Electronic Service Agent for pSeries and RS/6000 and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation. 2000, 2005. All Rights Reserved.

Before using this information and the product it supports, read the Notices and Trademarks information in Appendix G - Notices and Trademarks on page 143.

Note to U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GS ADP Schedule Contract with IBM Corp.

Table of Contents

CHAPTER 1. ABOUT THIS GUIDE	8
WHO SHOULD READ THIS GUIDE?	8
CONVENTIONS USED IN THIS GUIDE	8
TERMINOLOGY	8
CHAPTER 2. UNDERSTANDING SERVICE AGENT	9
WHAT IS SERVICE AGENT?	9
WHAT DOES “SERVICE AGENT FOR AIX ON pSERIES” SUPPORT?.....	9
WHAT’S NEW FOR SERVICE AGENT 3.3.0.0?	9
HOW DOES SERVICE AGENT WORK?	10
INVENTORY COLLECTION / VPD.....	11
PERFORMANCE MANAGEMENT (PM/AIX).....	11
SIMPLE NETWORK MANAGEMENT PROTOCOL SUPPORT (SNMP).....	11
WORKING WITH THE GATEWAY MACHINE (SERVER) AND THE CENTRAL DATABASE.....	13
UNDERSTANDING COMMUNICATION AND TCP/IP ADDRESSING	14
UNDERSTANDING THE MONITORING SYSTEM	14
<i>Electronic Server System (ESS) process</i>	15
<i>On Demand Server (ODS) process</i>	16
<i>Service Agent Connection Manager (SACM) process</i>	17
<i>Basic and advanced Graphical User Interfaces</i>	18
<i>Basic and advanced text user interfaces</i>	18
<i>PC interfaces</i>	18
CHAPTER 3. PLANNING	19
CHAPTER 4. PREREQUISITES	22
BASIC STEPS.....	22
MODEM COMMUNICATION STEPS	23
SETTING UP YOUR IBM MODEM FOR SERVICE AGENT	25
<i>Configuring the 7852-400 Modem</i>	25
<i>Configuring the 7857-017 or 7858-336 Modem</i>	26
CHAPTER 5. OBTAINING SERVICE AGENT	28
OBTAINING SERVICE AGENT FROM THE IBM ELECTRONIC SERVICES WEB SITE USING YOUR BROWSER	28
OBTAINING SERVICE AGENT FROM THE FTP.SOFTWARE.IBM.COM SITE USING YOUR BROWSER	28
OBTAINING SERVICE AGENT FROM THE FTP.SOFTWARE.IBM.COM SITE USING FTP	29
CHAPTER 6. INSTALLING SERVICE AGENT	30
INSTALLING SERVICE AGENT FROM SMIT.....	30
INSTALLING SERVICE AGENT FROM A COMMAND LINE	31

SETTING UP FOR REMOTE INSTALLATION OF MONITORED MACHINES USING SECURE SHELL (SSH).....	31
WHAT TO DO IF SERVICE AGENT INSTALLATION FAILS	33
<i>Analyzing installp faults</i>	33
<i>Installing Service Agent Code Manually</i>	34
<i>Manually installing Service Agent client from install media</i>	35
<i>Installing Service Agent Client using mksaclient</i>	35
<i>Manually installing Service Agent client without using mksaclient</i>	36
CHAPTER 7. ACTIVATING SERVICE AGENT	37
STEP 1: START CONNECTION MANAGER	38
STEP 2: START SA GATEWAY	40
STEP 3: INSTALL AND CONFIGURE SA CLIENT ON CLIENT HOST	42
CHAPTER 8. INITIAL SETUP: BASIC USER INTERFACE	44
ACCESSING THE BASIC USER INTERFACE	44
<i>Understanding the Basic User Interface Panel</i>	46
PERFORMING BASIC SERVICE AGENT DATA ENTRY	47
<i>Network Properties</i>	47
<i>Gateway Properties</i>	48
<i>CallController Properties</i>	49
<i>ConnectionManager Properties</i>	50
<i>Dialer Properties</i>	51
<i>Enroll Properties</i>	52
<i>CallLog Properties</i>	53
CHAPTER 9. LEARNING ABOUT THE ADVANCED USER INTERFACE.....	54
ACCESSING THE ADVANCED SERVICE AGENT USER INTERFACE	54
<i>Logging in</i>	55
<i>No Password Prompt</i>	55
<i>Basic Data Entry</i>	56
UNDERSTANDING THE ADVANCED CONFIGURATION PANEL	57
<i>Navigation Pane</i>	57
<i>Detail Viewing Pane</i>	59
<i>Category Selectors</i>	59
<i>View/Edit Properties button</i>	59
<i>View Error Events button</i>	60
<i>View Service Agent Internal Errors button</i>	62
<i>View Licensing Information button</i>	63
CHAPTER 10. ADVANCED CONFIGURATION TASKS	66
HOW TO PERFORM CONNECTIVITY TASKS.....	66
<i>How to set up SA CM to use Dialer</i>	66
<i>How to set up SA to use an Internet connection</i>	66
<i>How to set up a master gateway</i>	67
<i>How to set up a slave gateway</i>	67
<i>How to set up to a remote Connection Manager</i>	67

<i>How to set up to a secondary Connection Manager</i>	67
<i>How to change connection manager listening port</i>	68
HOW TO ADD OR CREATE ADDITIONAL CONFIGURATION ENTRIES	68
<i>How to create a department of monitored machines</i>	68
<i>How to add SP Nodes</i>	69
<i>How to add a machine</i>	70
<i>How to control dispatching for a machine supported by a different branch office..</i>	70
<i>How to install Service Agent code only on a monitored machine</i>	71
<i>How to specify the physical location of a machine</i>	71
<i>How to specify Cluster details</i>	71
<i>How to define resource filters</i>	72
<i>How to specify thresholds</i>	72
<i>How to add an e-mail address for a monitored client</i>	72
<i>How to configure for Performance Management</i>	73
<i>How to send Performance Management Data</i>	73
<i>How to add an SNMP Notification</i>	73
<i>How to lock out Service Agent on a machine</i>	74
<i>How to add an e-mail Alert</i>	74
HOW TO REMOVE OR DELETE CONFIGURATION ENTRIES.....	75
<i>How to remove a machine</i>	75
<i>How to remove an SNMP Notification</i>	75
<i>How to remove all nodes from a 9076 (SP)</i>	75
<i>How to remove Service Agent code only from a monitored machine</i>	75
<i>How to remove Cluster details</i>	76
HOW TO TEST CONFIGURATION ENTRIES.....	76
<i>How to send a test PMR to IBM</i>	76
<i>How to send a test e-mail</i>	76
<i>How to send a test SNMP Notification</i>	77
HOW TO PERFORM OTHER SERVICE AGENT FUNCTIONS	77
<i>How to determine your Service Agent version</i>	77
<i>How to manually transmit Vital Product Data (VPD) to IBM</i>	77
<i>How to clean up (remove some data from) monitored logs</i>	77
<i>How to clear pending requests to IBM</i>	78
CHAPTER 11. SERVICE AGENT SECURITY	79
TRAVERSING SECURE BOUNDARIES.....	79
SECURITY AND THE SERIAL INTERFACE	79
CHAPTER 12. CONTACTING CUSTOMER SUPPORT.....	80
ENTITLEMENT TO AUTOMATIC PROBLEM SUBMISSION	80
CONTACTING SUPPORT	80
WEB SITES	80
APPENDIX A - BASIC UI CONFIGURATION DETAILS.....	81
NETWORK PROPERTIES	81
GATEWAY PROPERTIES	82
CALL CONTROLLER PROPERTIES	83

CONNECTION MANAGER PROPERTIES	84
DIALER PROPERTIES	85
ENROLL PROPERTIES.....	86
CONNECT PROPERTIES	86
CALL LOG PROPERTIES	87
ERROR LOG PROPERTIES	87
APPENDIX B – ADVANCED UI CONFIGURATION/PROPERTY DETAILS	89
CATEGORY SELECTORS.....	89
NETWORK FOLDER.....	89
<i>Using the Add button from the Network folder</i>	90
ADDING ADDITIONAL SYSTEM INFORMATION USING FORMS.....	91
<i>Department Template</i>	91
<i>Node Info Template</i>	92
<i>Available Forms</i>	92
GATEWAY FOLDER	94
<i>Gateway Node Info</i>	94
<i>Call Controller Template</i>	95
<i>Connection Manager Template</i>	96
<i>Dialer Template</i>	97
<i>Environment Template</i>	98
<i>Data Folder</i>	99
<i>Enrollment Folder</i>	99
<i>Hardware Service Template</i>	99
<i>PMR Folder</i>	100
<i>Performance Management Template</i>	102
<i>SNMP Notification Template</i>	103
<i>Software Service Template</i>	104
ADDITIONAL MACHINE TEMPLATES	105
<i>E-mail Alert Template</i>	105
CLIENT MACHINES FOLDER	107
<i>Node Info Template</i>	107
<i>Call Controller Template</i>	107
CALL LOG FOLDER	108
ADMINISTRATION FOLDER.....	109
<i>Enroll Template</i>	109
<i>(Un) Install Template</i>	110
<i>Manage Cluster IDs</i>	111
<i>Add 9076 (SP) Nodes template</i>	111
<i>Data Compression Cycles Template</i>	112
<i>Import / Export Template</i>	113
<i>Lockout Machines Template</i>	114
<i>Purge Data Template</i>	114
<i>SA Access Template</i>	115
ALERTS FOLDER	115
FILTER LIST FOLDER.....	116
<i>Resource Filters Template</i>	116

<i>Thresholds Template</i>	117
MANUAL TOOLS FOLDER.....	118
<i>Connect Template</i>	118
<i>PMR Template</i>	119
<i>Performance Data Template</i>	119
<i>SNAP Template</i>	120
<i>Send VPD Template</i>	121
TEST TOOLS FOLDER	122
<i>Test E-mail</i>	122
<i>Test PMR</i>	122
<i>Test SNMPTrap</i>	122
APPENDIX C – ACCESSING SERVICE AGENT FROM A PC	123
<i>Creating the PC User Interface</i>	123
<i>Troubleshooting</i>	124
APPENDIX D – SERVICE AGENT ASCII USER INTERFACES	125
ACCESSING ASCII FROM SMITTY.....	125
<i>Basic ASCII Password</i>	127
<i>Basic ASCII Welcome Panel</i>	127
NAVIGATION IN THE BASIC ASCII USER INTERFACE.....	129
<i>Flow through the Basic ASCII User Interface</i>	130
<i>Basic ASCII CallController and SACM</i>	131
<i>Basic Dialer template</i>	132
<i>Basic ASCII Import / Export</i>	133
NAVIGATION IN THE ADVANCED ASCII USER INTERFACE	133
<i>Getting started using the Advanced ASCII User Interface</i>	134
<i>Menu Key Definitions</i>	135
<i>Machine template</i>	136
<i>Manual Tools template</i>	137
<i>Administration template</i>	137
<i>Using Help</i>	138
APPENDIX E - SNMP NOTIFICATION EXAMPLES	139
APPENDIX F – LIST OF ACRONYMS AND TERMS	140
ACRONYMS	140
TERMS	141
APPENDIX G - NOTICES AND TRADEMARKS.....	143
NOTICES.....	143
TRADEMARKS	144
INDEX.....	145

Chapter 1. About this guide

This guide provides overview information, setup or prerequisite information, installation instructions, and user operational information for Electronic Service Agent for pSeries and RS/6000, which is referred to as “Service Agent” or “SA” for the remainder of this document.

Who should read this guide?

This document is intended for use by pSeries and RS/6000 system administrators who are familiar with, or have a working knowledge of, AIX and RISC architecture as it pertains to basic operation of IBM RISC pSeries and System/6000®. You should also understand AIX system commands, System Management Interface Tool (SMIT), SMIT fast path, or smitty) for installation and running of SA.

Conventions Used in This Guide

This guide uses several typeface conventions for special terms and actions, as follows:

Bold

Commands and other controls, keywords, and other information you should use literally appear in **bold**.

Italics

Variables that you must provide appear in *italics*.

Monospace

Examples of code or text you should type appear in `monospace`.

Terminology

For a list of terms and acronyms used in this manual, please see **Appendix F, List of Acronyms, on page 139**.

Chapter 2. Understanding Service Agent

What is Service Agent?

Service Agent is a no-charge application program that operates on pSeries machines; monitors for hardware errors, sends automatic service request to IBM with no customer intervention, and collects machine inventory.

IBM does entitlement checking each time a service request is sent to IBM. Only machines on IBM Warranty or maintenance agreement (MA) can successfully submit service requests using Service Agent.

Service Agent does not replace the pSeries Maintenance Package. All SSRs should start with the standard Maintenance Package. Service Agent is used as an additional service tool for the system.

What does “Service Agent for AIX on pSeries” support?

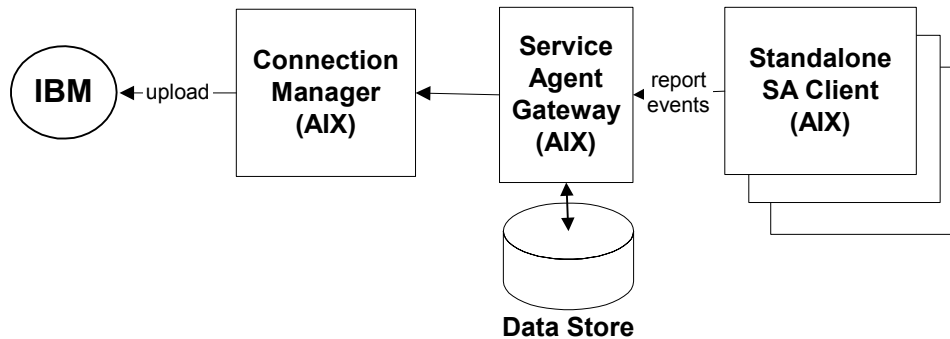
Service Agent supports all pSeries, pSeries p5 and most RS/6000 machine types, including the 9076 (SP) or cluster configurations, that have concurrent diagnostics installed, and are not under control of an HMC (Hardware Management Console). The application will run on HMC-controlled partitions but will not send Problem Management Reports (PMRs) or Vital Product Data (VPD). It will collect Performance Management (PM) data related to AIX and software inventory information. All machines must have valid RETAIN profiles to be able to open PMRs.

Service Agent supports AIX version 4.3.3 ML 11 and greater.

What’s New for Service Agent 3.3.0.0?

- Simple Network Management Protocol (SNMP) Trap Notification support has been added. See “How to add an SNMP Notification” on page 73, “How to remove an SNMP Notification” on page 75, “How to send a test SNMP Notification” on page 77, and “Appendix E - SNMP Notification Examples” on page 139.
- The SUMA_SOFT package, which collects software and fix inventory in an XML file, is being utilized..
- For INSTFIX and LSLPP functions, instead of sending all software and fix inventory data, only the data that has changed is sent.
- A tool is provided that lets users and support staff view the contents of the queues.
- Transactions are being prioritized on outgoing queues. For example, PMRs that are in the queue will be sent before inventory data.
- An extended logging system is provided that makes it easier for users to log data.
- SNAP data is periodically sent to IBM. See “SNAP Template” on page 120.

How does Service Agent work?



Automatic Service Request process:

Machines are defined and Service Agent installed by using the Service Agent user interface. After machines are defined, they are enrolled with IBM and assigned an electronic key. The key becomes part of your resident Service Agent code database.

- The key is used to enable error detection of the monitored host. Once enabled SA will monitor the error log for error labels and diagnostics for valid Service Request Numbers (SRNs).
- Each time Service Agent places an automatic service request, a check is made of the current customer support contract status from the IBM entitlement database.
- If the machine is covered, a PMR is created and the PMR number is returned to the customer's SA database. This will be reflected as an *OPEN* status under the failing machine's PMR folder.

If the entitlement check reveals that the host is not on Warranty or MA, then the service request is refused and posted back via e-mail internal notification if E-mail Alert is configured. See “How to lock out Service Agent on a machine

The Lockout Machines template allows turning off or locking out Service Agent on an individual machine or machines.

CAUTION: The locked out system will not report any errors until the lock is removed. Be sure to unlock the system after all maintenance work is performed.

1. Under the Administration folder, click **Lockout Machines**.
 2. From the detail pane, select the monitored machine or machines on which you want to lock out Service Agent.
 3. Click **lock**.
 4. To verify the lockout, click the **Network** folder, then click the **Padlock** icon to display status. The machine's status should show a red X, indicating it is locked.
 5. Repeat steps 1 and 2, and then click **unlock**.
- How to add an e-mail Alert” on page 74.

- If the current service request shows that the MA Expiry (Maintenance Agreement Expiration) date is greater than the local key indicates, then the key is extended to the new expiration date and you are sent a message indicating extension of service coverage if E-mail Alert is configured.

Inventory Collection / VPD

Service Agent collects hardware and software inventory data from your monitored machines on a periodic basis.

If you are concerned about whether this information is sensitive to your business, you can review the actual data that is being sent to IBM using the Service Agent User Interface or from the command line using file display programs. A WEB browser may be used to view any xml files that are generated. All customer data is fully encrypted during the transmission to IBM and until used by an authorized party.

The commands used to collect the information:

- Hardware: *invscout* program or *lscfg*, *lsyvd* commands for older systems
- Software: commands *suma_swinv -f xml* or *lslpp -hcq*, *suma_fixinv -f xml* or *instfix* and *snap -g* may be used.
- Extended Error Data (EED): *snap* command

You can run the commands on a system to view the information.

Note: You can prevent the collection and submission of this information using the Service Agent user interface. Additional transmissions will only occur if data changes.

Performance Management (PM/AIX)

Performance Management gathers data on an AIX system's performance and capacity, then returns the information to IBM for analysis and report building. Service Agent is the delivery method to IBM. After analysis of the data, reports are created and are available for viewing using several web sites. PM/AIX collects information daily from midnight to midnight. The SA collection time of PM/AIX information files can be configured on SA Performance Management template for each monitored machine.

PM/AIX is a separate product from Service Agent. It must be obtained, installed, and configured using Performance Management documentation. Additional information is available online at <http://perf.services.ibm.com/pmweb>

Simple Network Management Protocol Support (SNMP)

Service Agent generates SNMP notification traps for hardware problems and internal errors and sends them to the Management application of your choice. Some examples of Management applications are:

- Tivoli Enterprise Console
- HP Openview
- BMC Patrol

Service Agent generates the traps based on the '**ibmServiceAgent.mib**' module. Locate this MIB module in the **/usr/svcagent/lib** directory and import it into your Management application.

These notification types are supported:

- `ibmSaInternalError`
- `ibmSAHwErrorDetected`
- `ibmSaTestEvent`

For more information, see “Appendix E - SNMP Notification Examples” on page 139.

Working with the gateway machine (server) and the central database

When you install the Service Agent server package on a machine, that machine by default becomes a Service Agent gateway. The configured hostname of the machine becomes the default gateway machine name for Service Agent and is configured to be the reporting contact point for all communication interfaces. The communication interface that the hostname points to becomes the designated interface for all communications with Service Agent gateway server. The hostname can be configured to a different communication hostname before Service Agent is started. The Service Agent gateway registers TCP/IP port 1199 as the Java Remote Method Invocation (RMI) direct contact port on that named interface.

All configuration and setup data for monitored systems is maintained on the Service Agent gateway within a central Java database. All monitored machines and Service Agent user interfaces are attached and use that central database via Java-to-Java RMI communication over the default interface.

The following diagram illustrates a typical Service Agent monitored network and how it relates to IBM.

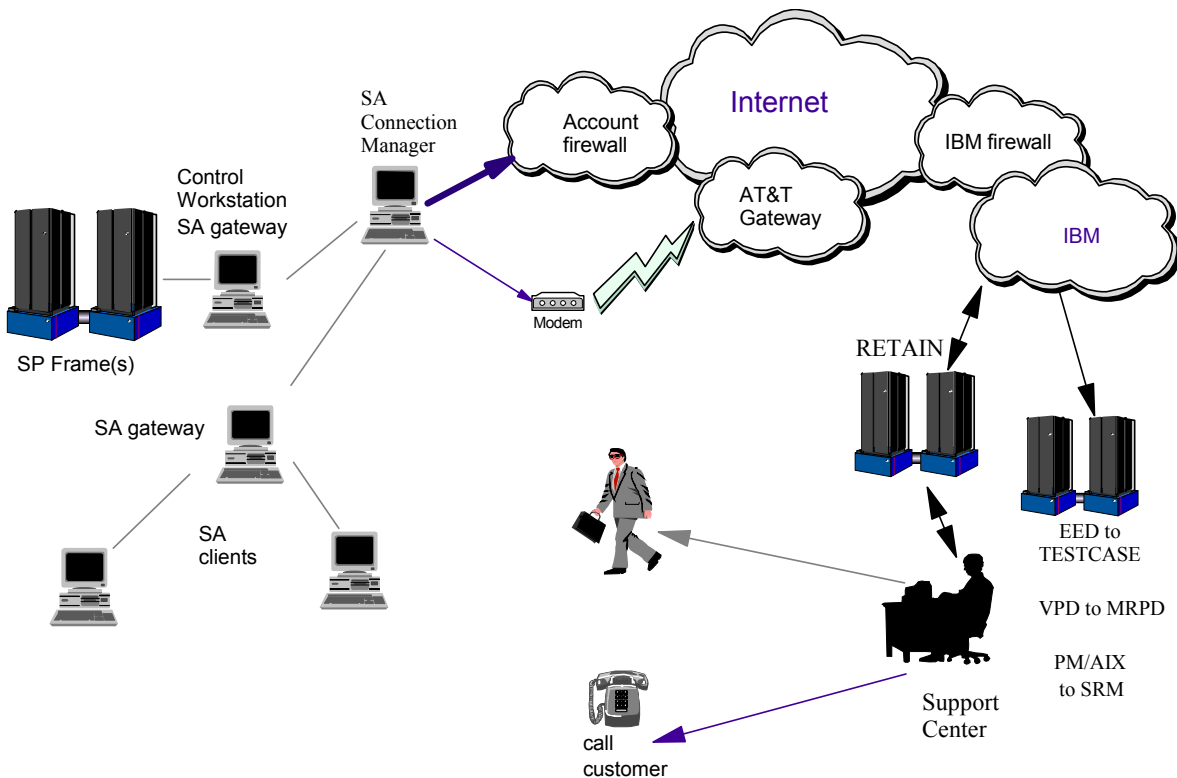


Figure 1 - Service Agent for AIX Monitored Network

Understanding communication and TCP/IP addressing

The Service Agent Connection Manager (SACM) can communicate with IBM using the Internet or a modem. The SACM can handle input from multiple SA gateways. A single Internet connection or modem is all that is needed to support a complex SA configuration. Redundancy can be achieved by defining a secondary SACM as backup. For instance, a primary Internet connection to IBM could be backed up with a secondary modem connection on another host running SACM.

If your TCP/IP installation permits direct connection to the Internet, you don't need a modem. If you want a modem setup, the SACM must have a modem attached to its serial port. This will allow the SA dialer to utilize a local call to connect to the AT&T Service Provider and in turn access IBM. "Setting up your IBM modem for Service Agent" on page 25 shows the proper basic modem setup for some IBM modems. Be sure that you configure the modem correctly using either the SA Basic or Advanced User Interfaces. Then test the modem setup using the **Connect** action described in Appendix B. Advanced UI Configuration/Property Details, "Connect Template" on page 118.

Service Agent uses TCP/IP addressing to communicate with its managed systems. Using IP addressing Java-to-Java direct connect RMI, the SA gateway receives information from its managed systems. The direct connect RMI is the fastest communication from the client SA to the SA gateway, but it cannot pass a secure firewall environment.

In order to support an internal customer firewall, communication between the Service Agent gateways and the Service Agent Connection Manager uses the HTTPS protocol over default TCP/IP port 1198. A customer Network Administrator will only need to write one firewall rule for the gateway to communicate with the SACM over port 1198. Service Agent also supports HTTPS and SOCKS proxies for Internet access.

Dial-up access to IBM requires that customer network administrators install the Point-to-Point Protocol (PPP) on the server that runs the SACM. The PPP must be properly configured with an available client interface. The dialer template must be properly configured to define the TTY port and modem type and the designated local AT&T phone number. Once connection is made to the AT&T gateway, the transmission is the same as on the Internet; it is just that AT&T is the Internet Service Provider (ISP).

Understanding the monitoring system

Four major components or processes make up the Service Agent application:

- Electronic Server System (ESS) process running only on the gateway
- On Demand Server (ODS) process running on both the gateway and monitored machines
- Service Agent Connection Manager process
- User Interfaces (Basic or Advanced, Text or GUI)

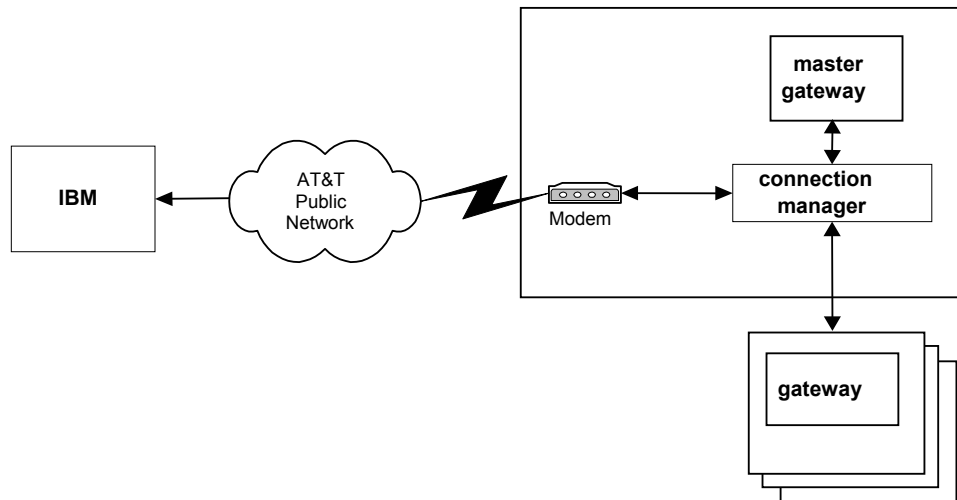
Electronic Server System (ESS) process

The ESS process runs only on SA gateway servers and handles all requests for data input and retrieval from the centralized database. The ESS registers the RMI direct connect socket 1199 for the ODS or User Interfaces applications to connect to the database.

Master gateways provide an SA Administrator the ability to update the Connection Manager configuration. The master gateway provides this function via an Advanced User Interface connected to it.

Slave gateways are not capable of updating the Connection Manager configuration. They are only capable of submitting requests to the Connection Manager for transmission to IBM.

Example Master gateway and Connection Manager configuration:



On Demand Server (ODS) process

The On Demand Server (ODS) runs on all hosts defined including the gateways, and handles all Service Agent monitoring and communication activities for that host. The ODS retrieves and sends data to the ESS process as necessary.

Any actual work or running of commands is done from the ODS. When the ODS initializes, it connects to the ESS using Java RMI, and this communication link is maintained on a secondary available socket for the duration of the ESS. If communication is lost with the ESS, the ODS will automatically abort and try to establish the connection again. If a second or third SA gateway server is configured, the ODS will attempt to connect to the first configured. If a timeout occurs on the first server, the ODS will attempt to connect to the next and keep cycling until a connection is established. Once established, the ODS will continue to communicate to the connected server until that secondary connection is lost.

Within the ODS, Service Agent automatically monitors and reports major events back to IBM, including:

- Serviceable events determined by Service Agent to be valid
- General Health Check, a transaction that reports the heartbeat of each client.
- Changes in the hardware inventory

Some of these events are reported to IBM directly using the Connection Manager. If no problems are reported to IBM during the Health Check interval, Service Agent initiates a transaction to IBM. The date stamp ensures that the machine is activated and is not having a system or communication problem.

When Service Agent detects a supported serviceable event, it starts actions to prepare and send a request for service. It logs the event and reports the problem to the IBM Problem Management system on RETAIN for remote analysis and action. If communications to RETAIN have been successful, a Problem Management Record (PMR) number is returned and logged in the database with an Open status. If the monitored AIX system has Extended Error Data (EED) capabilities, the EED information is sent to IBM. The associated file names are placed in the PMR for reference. You must define the machines you want Service Agent to monitor to enable error detection. If dynamic enrollment does not occur for the monitored machine, Service Agent will not capture serviceable events.

Additionally, Service Agent can send e-mail messages to contacts relating all or limited machine problem information. The e-mail notification functions must be configured by the customer or by an SSR before they become active. See the e-mail tasks in Chapter 10, Advanced Configuration Tasks, on page 66.

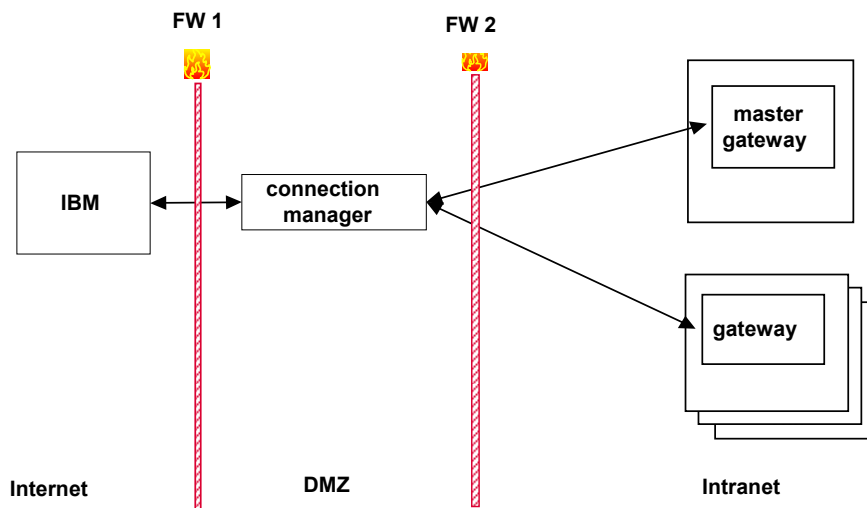
Service Agent Connection Manager (SACM) process

SACM provides the following services:

- Ensures Inter-enterprise (IES) compliance
- Utilizes industry standard HTTPS protocol
- Serves as a client side proxy to IBM
- Retrieves static content from IBM web site
- Provides location independence for Service Agent connectivity component
- Executes on any EServer p5 or pSeries system with a modem or an Internet accessible LAN adapter
- Utilizes PPP link layer for modem support
- Utilizes Java connection pooling in order to simultaneously support multiple gateways
- Provides a comprehensive logging facility for troubleshooting

SACM is a standalone process that can be configured by a customer or SSR to communicate with IBM using an existing Internet connection or modem. It may exist on any EServer p5 or pSeries in your environment and can support multiple SA gateways concurrently.

Example Connection Manager configuration with a DMZ:



Basic and advanced Graphical User Interfaces

The Graphical User Interfaces (GUI), Basic and Advanced, let you set up and define Gateway hosts or machines that Service Agent monitors. GUIs can run on an EServer p5 or pSeries installed with X11 or installed and run from a Windows-based PC.

The Basic User Interface is designed to allow a first-time user to configure the Service Agent system with as little user input as possible, utilizing predefined defaults for a single level network environment. The Advanced User Interface is used for advanced functions and customization of the system as well as configuration for complex systems and multilevel networks.

Both interfaces utilize a logon password (the default password is “password”) and are NLS enabled.

See Chapter 10, “Advanced configuration tasks,” on page 66 for more information.

Basic and advanced text user interfaces

These two ASCII interfaces provide the same function as the graphical user interfaces described previously. Both are NLS compliant.

The main difference between these interfaces is that the Text interfaces are not dependent on a graphical-capable terminal, but may be run from any type including the most basic ASCII terminal. The help panels can usually be selected from each displayed template, and they give detailed information of each item on the template.

Navigation is done completely by keyboard data entry instead of the clicking and scrolling prevalent in the GUI interfaces. Usually a single keystroke is all that is required to move through the various menus. These key functions are defined within the help menus.

See “Appendix D. Service Agent ASCII User Interfaces” on page 125 for information on how to access and use the ASCII interfaces.

PC interfaces

You can access Service Agent from a PC using either the Basic or Advanced Graphical User Interfaces once the initial SA gateway is configured. See “Appendix C – Accessing Service Agent from a PC” on page 123 for details.

Chapter 3. Planning

Early planning may save you valuable time and prevent aggravation later. This section provides information to help customers and SSRs set up Service Agent components to provide the best coverage for customer systems. Some of the basic questions about SA are addressed to assist in decision-making and placement of the SA components.

One should consider the following questions:

- What communication method should be used? If there is an existing high-speed Internet access available, that method is preferable. All communication between the SA gateway and IBM is encrypted and is secured using Java SSL no matter which communication method is selected. Using the dialer structure makes AT&T the Internet Service Provider (ISP), and the modem connection is a much slower network.
- Which host would best support the Service Agent Connection Manager (SACM)?
 - SACM can be installed on any pSeries AIX or Linux host. It does not have to be an SA gateway.
 - SACM can be controlled by a designated Master SA gateway, which is protected by a changeable password. This prevents different gateways that are using SACM from changing the communications method set from the master gateway.
 - Communication to and from the SACM host can pass through secure firewalls.
 - SACM uses HTTPS POST for secure transfers, which is slower but more secure. This communications method can pass secure firewalls, proxies, and use of Network Address Translation (NAT) devices to obtain access to an available high-speed Internet path.
 - Primary and Secondary SACM hosts can be used as backups, one for Internet, one for Dial.
 - SACM can support up to 15 SA gateways with default configuration. Five gateways are supported at the same time with up to ten queued waiting for service.
- How many SA gateways need to be set up to provide coverage for your network of monitored machines?
 - A gateway SA host can support up to 256 directly attached SA clients. See Service Agent Readme, “Tips on Large Environments.”
 - A direct attachment through port 1199 provides the quickest access between a client and gateway. The secondary communication port stays active for the duration of the ESS database process to the client ODS process.
 - Multiple SA gateways can support client machines for backup.
 - When the client host is defined, the backup Gateway hostname should be entered.

- Client host can be installed manually from media or remotely via the Advanced User interface. Once a client establishes communications with an SA gateway database, it will be automatically added to that gateway's database configuration.
 - All client configurations must exist in their respective SA gateway databases. Build the first SA gateway and export its database, then import the database to a second or third gateway to clone the first gateway if you want two or three gateways.
 - An SA Gateway host cannot report to any other SA gateway.
 - An SA Call Controller can be set up to use backup Connection Manager.
 - Only one SA gateway should be set up as a master gateway for each SACM.
- How should the client be set up, and what is the function of the On Demand Server (ODS)?
 - The ODS is the workhorse application; it does all of the local commands and data collection and sends the information to the SA gateway database. This same client process is busy on the SA gateway doing the same job for that host.
 - This client process is what monitors the host for errors, and it is activated once the host is enrolled and obtains a valid key.
 - SA uses the "errpt -c -g -s(timestamp)" command to continuously in-gate the error log to the ODS application. It takes the error labels and compares them to the defined error labels (See /usr/svcagent/README) and if these match, SA does the assigned action.
 - Most of SA fault detection is a follow-up of the diagnostics. If diagnostics produce an SRN, then SA will capture the results and call them in. Newer levels of diagnostics, at bos.diag.rte 5.1.0.35 or 5.2, will use a diagnostic Application Program Interface (API) to post results directly to SA.
 - SA normally exports the client portion of the Service Agent program from the SA gateway machine to monitored machines. This is done using FTP or remote commands, and requires root access to a client. If you have network security considerations that do not allow this distribution method, client code can be installed and configured from the client host. If secure shell (SSH) is installed on the Gateway host, it may also be selected for the distribution method. The openssh is the only secure shell that was tested with SA, and not all SSH commands may work.
 - Multiple SA Gateway hosts can provide backup for client communications. Initial direct contact is attempted to the first server and, if unsuccessful, the client will attempt to contact the second and third enabled servers. Once contact is established, communication will continue with that SA gateway server until the link is lost.

- What is the firewall impact?
 - We used to have a secure side and an unsecured side, but now most firewalls are secure on both sides. SA uses two different Java RMI (Java remote procedure call) processes to communicate at the different points in the Service Agent infrastructure.
 - The first Java RMI, and the fastest communication means from the SA Client ODS to SA gateway ESS (database), is direct contact on 1199. This direct contact is established and then maintained on an available secondary port between the two SA processes as long as they are active. If broken, the ODS process will abort and try to reestablish itself, always starting from the client end to the gateway. If the SA gateway is on the unsecured side of a firewall so the secure client hosts can see all of the SA gateway ports above 1000, then SA will work. But this will not work through a secure firewall. The SA client host must be able to see the secondary port issued by the SA gateway direct contact on port 1199. The SA application on the gateway has no control over the next available port request from the Java RMI direct contact code. So it cannot be predicted which port will be available to the client.
 - The second Java RMI is the secure POST, which will pass the most secure proxy firewalls. This method allows secure SA gateways to pass internal firewalls to the SACM, and allows SACM to pass account and IBM secure firewalls.
- What planning should be done for the High Availability (HA) environment?
 - HA machines are easy to support if they are defined as SA client machines.
 - HA hosts configured as SA Gateway hosts become much more difficult to configure. These SA gateways must all have identical SA configurations for full fallover support.
 - SA inittab entries are inserted two positions up from the bottom of the file to prevent interference with HA required last entry.

Chapter 4. Prerequisites

This chapter presents prerequisite activities that need to be verified or completed prior to installing Service Agent.

Basic steps

1. Review Chapter 3. Planning
2. Ensure your pSeries or RS/6000 is at AIX Version 4.3.3 ML-11 with diagnostics for problem reporting.
3. Ensure your pSeries or RS/6000 machine Type-Model-Serial has been defined within the RETAIN machine profile database so that PMRs can be created. This is an automatic process in most countries, but you may need IBM Service to verify with the local IBM Support group. This is usually the problem if you get the following message, "**FAILED Country, Type or Serial not available**" on a Test PMR.
4. Ensure the administrator installing Service Agent has root authority on has root authority on the gateway machine. This person must have access to a root-authorized window during installation of SA.
5. Ensure your gateway server has remote command capabilities (rsh, dsh) or REXEC and FTP capabilities to all monitored machines (other pSeries, RS/6000s, or nodes). If kerberos is on SA gateway server, make sure there is a valid root ticket. In some cases you may also need a valid ticket created for svcagent UID. If you have network security considerations, you may want to use the Secure SHell option (SSH) to send the code to your monitored machines. The SSH will require a secure key from the gateway svcagent UID on the client.
6. Ensure IBM diagnostics are installed on every monitored machine. Error logging and error log analysis must be enabled.
Tip: To determine if diagnostics are loaded, type **diag** on the command line. Then press **Enter** key and take *Task Selection* option of diagnostics. Scroll the task list until you find and can **select Periodic Diagnostics**. Press **Enter** on **Periodic Diagnostics Service Aid** main menu to get to the service aid list. The last entry will show the status of *Automatic Error Log Analysis* and will allow you to switch states, make sure it is **ENABLED**.
7. Ensure that Integrated Diagnostics and Extended Error Data are installed: Integrated diagnostics is available only for AIX 5.1 and above. SA needs the bos.diag.com packages to be above 5.1.0.35. EED is supported only on levels 5.1.0.50 and above (for 5.2 it is 5.2.0.10 and above).
Tip: Type the command. **lslpp -l bos.diag.com**
8. Ensure that Java is installed on all monitored machines. Java for AIX 4.3.3 and later is on the system disk. Java versions supported are 1.1.8 to 1.4.x, with the later version displaying a much better performance characteristic. Once SA is installed, its path statement will attempt to use the highest installed level of Java.
Tip: Type the command **lslpp -l Java*** This command displays the install level of Java. If Java is not installed, you receive a message back indicating so.

9. Prepare for e-mail alerts. The host that the E-mail Alert is placed under must have e-mail service available locally or via network. E-mail Alerts can be configured using the Advanced Service Agent configuration interface. See Chapter 10. Advanced Configuration Tasks, “How to add an e-mail alert,” on page 74.
10. Service Agent will define the svcagent user ID to be used by the application. If you have strict controls of machine UIDs, \$HOME directories, or other requirements, then the svcagent ID must be created before code is installed:

```
mkuser pgrp='system' gecos='Service Agent Administration' login='false'  
rlogin='false' svcagent
```

It is **extremely important** that the local System Administrator define the svcagent correctly. Otherwise problems will occur during attempted execution of SA binaries.

11. If you are using an existing Internet connection, you have completed the prerequisites. If you are using a modem, continue with “Modem Communication Steps.”

Modem communication steps

1. Ensure your SACM server has an available serial port. For a serial port, a TTY device must be available and configured on the CM system. If a TTY must be added, just take the default options that are automatically added.
2. An asynchronous modem with a minimum communications speed of 9600 baud and error correction (in the United States) is required. Please set the highest possible baud rate for your modem. Refer to local procedures in your country to see what the modem requirements are for Service Agent. If you are using an IBM modem, see “Setting up your IBM modem for Service Agent” on page 25 prior to using Service Agent.
3. The modem and phone should be connected and operational. Check the physical connections to determine this. Remember the physical port the modem is attached to does not equate to the assigned TTY port. Check TTY configuration to associate physical port to proper TTY.
4. On your SACM server, ensure Point-to-Point Protocol (PPP) is installed and configured. PPP is only required if a modem is going to be used for error reporting to IBM. Following are the PPP Link configuration parameters with general minimum values. These values only take into consideration Service Agent by itself. They may have to be adjusted depending on any additional connections configured.

For older levels of AIX, there might be an available 0.0.0.0 interface after pppcontrold has been started. To prevent the setup_server command from posting an error message, the 0.0.0.0 IP should be defined in /etc/hosts or DNS. This interface will not be present in AIX 5.3 or above. (or AIX 5.x with the latest fixes)

Tip: Type the command **ps -ef | grep ppp**. Look for pppcontrold. If you find this, PPP is installed, configured and running. Skip to the next step, Check and check diagnostics.

If you cannot locate pppcontrold, type **lspp -l bos.net.ppp**. This command indicates if the PPP file set is installed. If not installed, you need to install the code from the AIX media. Return here and complete the following steps when PPP is installed:

- 1) Type **smit**.
- 2) Select **Communications Applications and Services**.
- 3) Select **PPP**.
- 4) Select **Link Control Configuration**.
- 5) Select **Change/Show a Link Configuration**.

If a configuration is displayed, then return to PPP and select **Start PPP**. If an error occurs, it means there is no link configured. Follow these steps:

- 1) Cancel out of Change/Show a Link.
- 2) Select **Add a Link Configuration**.
- 3) If the menu contains the properties listed below, fill these in as follows:
 - PPP Subsystem name = PPP
 - max server connections(num) = 0
 - max client Connections(Num) = 1
 - max demand connections(Num) = 0
 - max IP interfaces(num) = 1
 - max async hdlc attachments(num) = 545
 - mru(Num) = 1500
 - async character map (Hex) = 454
 - transmit async character map (Hex) = 343Accept the remaining defaults, click **OK**, and skip the next step
- 4) If the menu instead contains these properties (AIX 5.3), fill these in as follows::
 - PPP Subsystem name = PPP
 - max server connections(num) = 0
 - max client Connections(Num) = 1
 - max demand connections(Num) = 0
 - max IP interfaces(num) = 1
 - Max IPv6 interfaces = 0
 - Max IP & IPv6 interfaces = 0
 - max async hdlc attachments(num) = 545
 - mru(Num) = 1500Accept the remaining defaults and click **OK**.
- 5) Return to PPP and select **Start PPP**.

Setting up your IBM modem for Service Agent

IBM ships the following modem types for use with Service Agent on some products.

- 7852 Model 400
- 7857-017 or 7858-336

Remember, these modems are considered to be assigned to the product serial number. If the machine moves, the modem must go with it.

Configuring the 7852-400 Modem

The 7852 Model 400 is one of the modems of choice for Service Agent. From the factory, there are DIP switches on the side of the modem that need to be set to make the asynchronous mode the default mode. Switch 12 needs to be set to the off (down) position for asynchronous mode. Switch 5 needs to be set to the off (down) position to disable auto-answer to meet the security requirement that modem will not answer. See the diagram below for proper settings of switches if necessary.

To set up and initialize the 7852-400 for operation:

1. Set switches 5 and 12 to the down (off) position.
2. Connect the RS232 cable to the modem and to a serial port.
3. Connect the telephone cable (sent with the modem) to the modem connector labeled LINE (middle connector), and to the telephone wall jack.
4. Connect the modem power cable to the modem and the transformer to the building power.
5. Power-on the modem (switch in rear).

Up	++	++	+	+	+	+										
Down	- - -	- -	- -													
Switch	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

7852-400 Service Agent DIP Switch Settings

Configuring the 7857-017 or 7858-336 Modem

The 7857 is another one of the modems of choice for Service Agent. The 7858-336 is the replacement modem for the 7857. These procedures are here to aid in the proper configuration of the 7857-017 or 7858-336, or to set a known configuration state.

To set up and initialize the 7857-017 or 7858-336 for operation:

1. Connect the RS232 cable to the modem and to a serial port.
2. Connect the telephone cable (sent with the modem) to the modem connector labeled PSTN, and to the telephone wall jack.
3. Connect the modem power cable to building power.
4. Power-on the modem.
5. Wait for the main display panel.

Use the following procedure to place the modem in a known configuration.

After the modem is powered on and local tests have completed, there should be two lines of configuration information displayed on the modem LCD panel.

At this time:

1. Press the down arrow key 12 times until the CONFIGURATIONS message is displayed.
↓ CONFIGURATIONS D12
 Press →
2. Press the right arrow key until the Select Factory message is displayed.
→ CONFIGURATIONS D12
 Select Factory_
3. Press the Enter key to select the Factory configuration option.
 - a. Press the up arrow key until 0 is displayed.
↑ CONFIGURATIONS D12
 Select Factory 0
4. Press the Enter key to load the predefined factory configuration 0.
IBM 7857 AT CMD aa ■
td_rd_dsr_ec ■ ll_
5. Press the down arrow key 7 times until the S-REGISTER message is displayed.
↓ S-REGISTER D7
 Press →
6. Press the right arrow key until the message Ring to answ. on is displayed.
→ S-REGISTER D7
 Ring to answ. On=2_
7. Press the Enter key to select Ring to answ. on.
S-REGISTER D7
 Ring to answ. On=_
8. Press the up arrow key until 0 is displayed.

↑ S-REGISTER D7
Ring to answ. On=0

9. Press the Enter key to set Auto Answer to 0.

S-REGISTER D7
Press →

10. Press the down arrow key 5 times until the CONFIGURATIONS message is displayed.

↓ CONFIGURATIONS D12
Press →

11. Press the right arrow key 3 times until the Store User Conf. message is displayed.

→ CONFIGURATIONS D12
Store User Conf._

12. Press the Enter key to select the Store User Configuration option.

Press the up arrow key until 0 is displayed

↑ CONFIGURATIONS D12
Store User Conf. 0

13. Press the Enter key to select location 0.

14. Press the Enter key to save current configuration into User 0 .

CONFIGURATIONS D12
Press →

15. Press the Enter key to return to main display panel.

IBM 7857 AT CMD aa_
td_rd_dsr_ ec ■ ll_ ■ = Shows LCD as on.

The above setup places the 7857 or 7858 modem into the proper configuration for use with the Dialer that is used for Service Agent pSeries or RS/6000.

Notes:

1. The modem initialization strings provided are on an AS IS basis. Although they have been tested in a typical environment, they may have to be modified depending on the actual setup and configuration of your environment.
2. If modem configuration assistance is required, you should contact the modem vendor for assistance. Information regarding modem standards, general modem setup, and specific configuration tips for IBM Asynchronous Adapters can be found in the MODEMS PACKAGE on AIXSERV
3. Assistance with IBM modem configuration issues can be obtained for a fee. Please check with your local IBM Support Center for more details.

Chapter 5. Obtaining Service Agent

The latest level of Service Agent is available from either the IBM Electronic Services Web site using your browser or via File Transfer Protocol (FTP) from the [ftp.software.ibm.com](ftp://ftp.software.ibm.com) site.

Note: If using ftp, “tmp” is the directory or folder name in which to save or transfer the Service Agent program. It is possible you will need to move the Service Agent packages for the gateway and/or Connection Manager to their designated target machines after obtaining the code.

Obtaining Service Agent from the IBM Electronic Services Web site using your browser

1. On the Electronic Services Web site (www.ibm.com/support/electronic) select the Electronic Service Agent category from the left navigation pane.
2. Select pSeries AIX Service Agent.
3. Select the version of Service Agent code you are downloading and press Enter. You see a panel similar to the one below.
Error! Objects cannot be created from editing field codes.
4. Select Save. You see a panel asking where (in which directory) you want to store the file.
5. Enter the directory name.
6. Click OK to transfer the file to your designated pSeries system.

Obtaining Service Agent from the [ftp.software.ibm.com](ftp://ftp.software.ibm.com) site using your browser

Complete the following steps to obtain the Service Agent program using a browser:

1. Using your browser, type in this URL:
`ftp://ftp.software.ibm.com/aix/service_agent_code/AIX`
2. Select the `svcagent.tar` file.
3. Click **File** and then click **Save As**.
4. Save the file as a `.tar` file. In this example, **tmp** is the folder in which to save the file.
5. Select the `svcUG.pdf` file to download the Acrobat image of the documentation.
6. Transfer the file in binary mode:

- On the gateway server, type **mkdir /tmp/svcagent** to make the svcagent directory if it does not already exist.
 - Move the **svcagent.tar** to **/tmp/svcagent** directory on the gateway server using ftp.
7. Untar the **svcagent.tar** file. You have successfully obtained the Service Agent program.

Obtaining Service Agent from the ftp.software.ibm.com site using FTP

Complete the following steps to obtain the Service Agent program using FTP:

1. Log in (or su) to root if on a pSeries.
2. Type **mkdir /tmp/svcagent** to make the svcagent directory if it does not already exist.
3. Type **cd /tmp/svcagent** to access the /tmp/svcagent directory.
4. Type **ftp ftp.software.ibm.com** .
5. Type **anonymous** as your login name (user ID).
6. Type your **e-mail address** as your Login password.
7. Type **bin** to set the file transfer type to binary.
8. Type **cd /aix/service_agent_code/AIX** to access the path where the SA code is stored.
9. Type **get svcagent.tar** to retrieve the Service Agent code.
10. Type **get svcUG.pdf** to retrieve the Acrobat format of the Service Agent User's Guide.
11. Type **quit** to end your FTP session.
12. Transfer the file, in binary if necessary, to the machine that you want to be the Service Agent gateway server.
13. **svcagent.tar** file into the directory you want to install from. You have successfully obtained the Service Agent program.

Note: When using ftp, “tmp” is the directory or folder name in which to save or transfer the Service Agent program. It is possible you will need to move the Service Agent packages for the gateway and/or Connection Manager to their designated target machines after obtaining the code.

Chapter 6. Installing Service Agent

There are two methods to install Electronic Service Agent for pSeries or RS/6000. They are:

- Installp from System Management Interface Tool (SMIT). Go to “Installing Service Agent from SMIT.”
- Installp from command line. Go to “Installing Service Agent from a command line.”

Notes:

- You can install this release of Service Agent over previous versions. **On an upgrade you must install svcagent.cm last, after you have first installed the other modules.** Your machine list, communications files, and database will remain the same. If you are migrating from SA release 2.4 or older, please utilize the following clean install procedure.

To make for an easier configuration after a clean install, first export the old SA database, then import it back in after a clean install is completed.

- You must install the correct svcagent.msg module to make application NLS compliant.

Installing Service Agent from SMIT

1. Log on to the gateway server as root or sign on using a root-authorized user ID.
2. If not using install media, type **inutoc /tmp/svcagent** (the directory where SA was saved).
3. Type **smiit** (in lowercase) to activate the System Management Interface Tool.
4. Select **Software Installation and Maintenance**.
5. Select **Install and Update Software**.
6. Select **Install and Update from Latest Available Software**.
7. Type **/tmp/svcagent** in the INPUT device/directory for software field, or select install media.
8. Click **OK**.
9. From the SOFTWARE to install field, select **svcagent** to do a complete install. Or select the appropriate module if doing a selective manual install.
10. Click **OK**. A prompt saying ARE You SURE? is displayed.
11. Click **OK**.
12. Check the installp *Summary message results* column to ensure it indicates SUCCESS. If failure is indicated, conduct an analysis. See “Analyzing installp faults” on page 33.

Installation Summary

Name	Level	Part	Event	Result
svcagent.cm	3.2.1.x	USR	APPLY	SUCCESS
svcagent.cm	3.2.1.x	ROOT	APPLY	SUCCESS
svcagent.client	3.2.1.x	USR	APPLY	SUCCESS
svcagent.client	3.2.1.x	ROOT	APPLY	SUCCESS
svcagent.help.en_US	3.2.1.x	USR	APPLY	SUCCESS
svcagent.msg.en_US	3.2.1.x	USR	APPLY	SUCCESS
svcagent.server	3.2.1.x	USR	APPLY	SUCCESS

13. Select **DONE** after the Service Agent program installs.
14. Select **CANCEL** to return to the System Management screen.

Installing Service Agent from a command line

1. Log on to the gateway server as root or sign on using a root-authorized user ID.
2. If not using install media, type **inutoc /tmp/svcagent** (the directory where you saved SA).
3. Type **installp -acXYd /tmp/svcagent all** (If this is a new install). Or replace "all" with the individual module name if doing an upgrade or selective manual install.
module names: *svcagent.client svcagent.help.en_US svcagent.msg.en_US svcagent.server svcagent.cm*

NOTE: If **installp** was not loaded into the **/tmp/svcagent** directory, use the directory name it was loaded into in place of **/tmp/svcagent**.

4. Check the *installp Summary message result column* to ensure it indicates SUCCESS. If failure is indicated, continue with “Analyzing installp faults” on page 33.

Setting up for remote installation of monitored machines using Secure SHell (SSH)

Service Agent provides the ability to remotely install new monitored machines from within the SA Advanced User Interface using the SSH protocol. The receiving host root ID must have a valid public from the SA gateway svcagent ID.

Only openssh has been tested in this operation. Here are some Q&As on openssh.

Q) Where do I get the openssh and opensll packages required by Service Agent for ssh?

A) You obtain these packages and more information from these sites:

<http://sourceforge.net/projects/openssh-aix>

http://www-128.ibm.com/developerworks/eserver/articles/openssh_aix.html

Note: Remote installation with SSH requires that remote SSH commands can be executed in non-interactive mode (without being asked for password/pass phrase).

Q) How can I check whether SSH commands can be executed in non-interactive mode?

A) Type the following command from the SA gateway machine as user svcagent.

```
prompt>$ whoami
svcagent
prompt>$ ssh -l root remote_host_address
remote_host_address:~ $
```

Replace *remote_host_address* with the actual address of the remote machine.

The system should not ask for password, pass phrase or anything else. The command should return immediately without requesting any input from the user.

If the system asks for password or pass phrase, or says that authenticity of the host can't be established and requires any input in order to continue, SSH is not configured for non-interactive mode.

Q) How can I configure SSH in non-interactive mode?

A) You need to generate public/private key pair as user svcagent and transfer the public key to the remote machine.

1. Log on to gateway as **su - svcagent**.

2. Generate public/private key pair.

Type **ssh-keygen -t rsa** from the SA gateway machine.

The output should look like the text below.

Accept all default values by pressing

.

```
prompt>$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/svcagent/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/svcagent/.ssh/id_rsa.
Your public key has been saved in /home/svcagent/.ssh/id_rsa.pub.
The key fingerprint is:
4c:c8:c2:de:1d:f6:e0:ca:c8:84:ff:b9:77:06:6e:f5 svcagent@hostname
```

3. Transfer gateway machine's public key to the remote client with one of these methods:

Method 1 - secure copy *authorized_keys* to remote host

Type:

```
prompt>$ scp /home/svcagent/.ssh/id_rsa.pub
root@remote_host_address:/home/svcagent/.ssh/authorized_keys
Password:
id_rsa.pub 100% 221 0.2KB/s 00:00
```

Replace *remote_host_address* with the actual address of the remote machine.

You will be asked for root's password on the remote host.

Method 2 - edit authorized keys on remote host and enter the key

4. Check whether SSH commands can be executed in non-interactive mode.

Type

```
prompt>$ ssh -l root remote_host_address  
remote_host:~ # whoami  
root
```

Replace *remote_host_address* with the actual address of the remote machine. The system should not ask for password, pass phrase or anything else. The command should exit almost immediately without requesting any input from the user.

What to do if Service Agent installation fails

If Service Agent installation fails, you can analyze the faults shown on the failed report.

Analyzing installp faults

You are in this analysis because the Service Agent installp process failed to post SUCCESS. You can determine the corrective action needed to recover SA to install. The installp process will attempt to uninstall the SA code if a fault occurs during the install. In order to properly analyze the initial fault, you must find the first failing message.

The SMIT window automatically starts from the beginning of the installp process. If you are in a scrollable window using a bottom line command, please scroll back to the installp command. If you are using a non-scrollable window and cannot see the initial failure but only the summary failure messages, run the listed cleanup command and reprocess the installp command using SMIT.

1. Review the installp messages for the first failing message posted.
2. If the problem has to do with prerequisites, insufficient core, or items that the system administrator can correct, fix the problem that has caused installp to fail.
3. If the problem is in the making of the svcagent user ID, the system administrator may create the svcagent user ID manually and installp will bypass the step on the next install. This ID will need to be created on all of the monitored client machines also.
4. If a problem occurs within User or Root configuration routines that cannot be corrected by the system administrator, capture the messages and open a PMR against Service Agent with the support group. If a problem has to do with security or certain functions within the complex, record the concern in the PMR. In some cases the application may not be able to properly exist on a customer complex. In all cases, do the cleanup steps and do not continue with the Service Agent install process until the condition is resolved.
5. If the uninstalled function of the installp also failed, run one of these installp cleanup function as follows before reinstalling code again:
 - Type **installp -C /tmp/svcagent.module_name svcagent**

- Replace "svcagent" with the individual module name if doing a selective manual clean. module names: *svcagent.client*, *svcagent.help.en_US*, *svcagent.msg.en_US*, *svcagent.server*, *svcagent.cm*
6. Return to your selected installp process and re-install Service Agent or just the failing module

Installing Service Agent Code Manually

Service Agent uses FTP or remote commands to send its client code to machines that you want to monitor. The client code attempts to use the selected "type of install" when you identify that machine using the "add machine" function. The automatic FTP process requires Service Agent to use the root password or a root-authorized password.

If your network security configuration does not allow root FTP access to machines or RSH/DSH access, and you elect not to install SSH, you can manually install the SA client code using one of the following methods:

- Install Service Agent Client using install media CD
- Install Service Agent Client Software using mksaclient
- Manually install Service Agent client software without using mksaclient

Before you execute a selected method you must:

- 1) Ensure the Service Agent program (*svcagent.server*) is installed on the machine you intend to use as your gateway machine. (This should be done if you followed the previous instructions in this chapter.)
- 2) Ensure the installp image */usr/svcagent/lib/svcagent.client* is present. If not, locate the *svcagent.client* package and copy as */usr/svcagent/lib/svcagent.client*

command: *cp <location>/svcagent.client /usr/svcagent/lib/*

- 3) Add the monitored machine or machines to the gateway Service Agent database. For monitored machine ODS to function it must first be defined in the ESS database. See "How to add a machine" on page 70.
- 4) Select one of the following installation methods.
 - SA client from install media or client installp file, configure and start from client smit
 - SA client using mksaclient
 - SA client without mksaclient

Manually installing Service Agent client from install media

The multi-part Service Agent code is available on the AIX Expansion Bonus pack, and the client code may be selected if client has ability to read the media. Or you can use the `svcagent.client` module to install from if you are using the `svcagent.tar` file.

Once code is installed you may use the SMIT Service Agent menu to configure and start the client SA and it will be automatically be added to the gateway configuration if it does not already exist in the configuration. If client host is already in SA gateway database, then no additional action will be taken and client will be active.

- 1) Log in as root or su to root on the client host machine.
- 2) Use “Installing Service Agent from SMIT” on page 30 and select the `svcagent.client` module and the help module.
- 3) After code is successfully installed, activate SA on client using SMIT - Manage SA Client.
- 4) First configure the client’s hostname (auto filled) and then the Gateway hostname that this client will use. Correct Type-Model-Serial if not auto-filled correctly, enter department if needed, and be sure to enter the correct password used for gateway SA UI access.

```

                                     Configure Service Agent Client
Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Client Host Name          [Client2]
Primary Gateway            [Gateway]
Secondary Gateway          [ ]
Tertiary Gateway           [ ]
Password                   [password]
* Machine Type              [7013]
* Machine Model             [J40]
* Machine Serial Number    [0044447]
Department Name            [ ]

```

- 5) Finally, start the SA Client configuration processes. Try not to do more than 20 clients at the same time or you may overburden the gateway processes.

Installing Service Agent Client using `mksaclient`

A script named `mksaclient` is provided with the Service Agent software to set up the environment and FTP the client host software. This script prompts for a user ID and password for getting the `svcagent.client` file from the gateway. The `root` or `svcagent` user ID can be used to do this. (A password can be assigned to the user ID `svcagent` on the gateway, if you plan to use the `svcagent` user ID.) If no FTP daemons are running on the gateway, this step can be avoided by copying the `svcagent.client` file to the `/tmp` directory.

To use `mksaclient`, do the following:

- 1) Ensure the file `/usr/svcagent/lib/svcagent.client` is present on the gateway. If not, locate the `svcagent.client` package and copy as `/usr/svcagent/lib/svcagent.client`.

command: `cp <location>/svcagent.client /usr/svcagent/lib/`

Be sure also that `/usr/svcagent/lib/svcagent.client` has at least 640 permissions.

- 2) Log in as root or su to root on the client machine.
- 3) Obtain and store `mksaclient` on the client host machine. Obtain `mksaclient` script from the gateway (it is stored at: `/usr/svcagent/bin/mksaclient`).
- 4) Type **chmod u+x mksaclient** to give `mksaclient` run permissions.
- 5) Type **./mksaclient** and press **Enter**. Follow the instructions provided by the script.

You will need to input the name of the gateway machine and the name of the client host machine.

Manually installing Service Agent client without using mksaclient

- 1) Ensure the file `/usr/svcagent/lib/svcagent.client` is present on the gateway. If not, locate the `svcagent.client` package and copy as `/usr/svcagent/lib/svcagent.client`.

command: `cp <location>/svcagent.client /usr/svcagent/lib/`

Be sure also that `/usr/svcagent/lib/svcagent.client` has the at least 640 permissions.

- 2) Log in as root or su to root on the client host machine.
- 3) Obtain the client host software from the gateway machine. The client host software is located in `/usr/svcagent/lib/svcagent.client` on the gateway machine.
Make sure to use the binary mode (for example, `bin`) to transfer the file.

- 4) Set `SvcAgentHOST` and `SvcAgentGATEWAY` to the following values:

```
export SvcAgentGATEWAY=<Gateway hostname>
export SvcAgentHOST=<client hostname>
```

- 5) Install the client host software in the usual manner. You can use either SMIT or an installation command on the command line.

Chapter 7. Activating Service Agent

The Service Agent processes are not active when initial installation is complete. Service Agent must be manually activated after installation.

Once the application has been successfully installed, the various processes have to be manually configured and started. This only occurs after the initial or new installation. The upgrade process does not require this step because SA is already running.

Determine what has to be configured and started. This depends on what has been installed.

- Full install making a new SA gateway.

Do steps 1 and 2.

- Install just SA Client code on client host.

Do step 3.

- Install just SA gateway code on slave gateway.

Do step 2.

- Install just SA Connection Manager.

Do step 1 only.

After the required steps are completed, you should be able to continue the configuration of Service Agent information by selecting one of the SA User Interfaces.

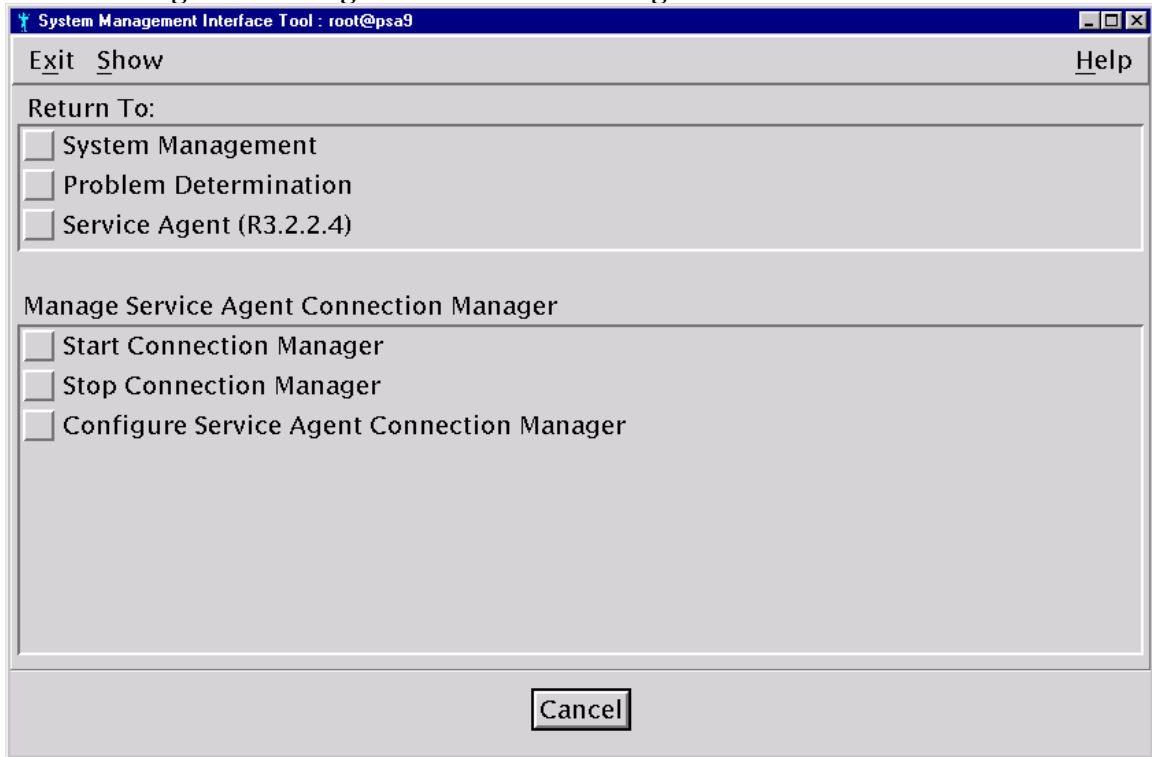
Use the following to get to the correct SMIT menu for SA.

1. Type **smitty** (in lowercase) to activate the System Management Interface Tool.
2. Select **Problem Determination**.
3. Select **Service Agent** (revision level).
4. Select the appropriate menu item to complete the step.
5. Click **Done** when action is completed.
6. Click **Cancel** to return to the SA menu to do other steps.

Check the status of SA using Display Service Agent Status. This will show which processes are active on that host.

Step 1: Start Connection Manager

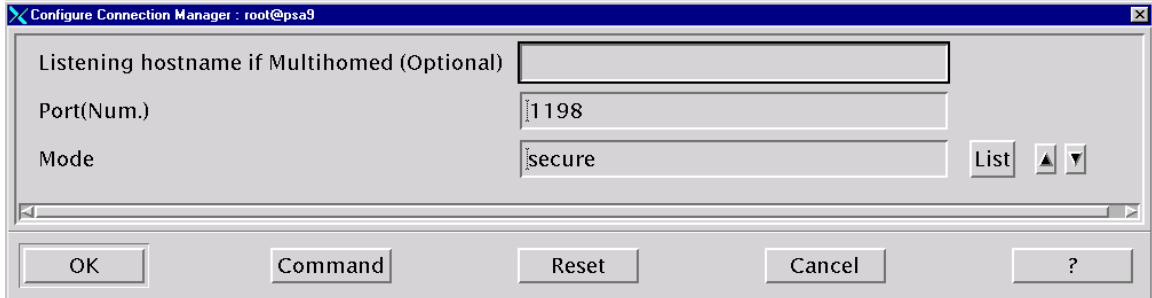
1. Verify the default configuration of SACM to the hostname and secure 1198 port if SACM is on the SA gateway server (loopback if blank may be used for efficiency).
2. Select **Manage Service Agent Connection Manager**.



3. Select **Start Service Agent Connection Manager** if using default configuration or go to item 5 if you need to change SACM default configuration.
4. The standalone SACM installation is completed. For full installation, continue with the

Step 2: Start SA gateway **on page 40**.

5. Select **Configure Service Agent Connection Manager** if you need to verify or change configuration.

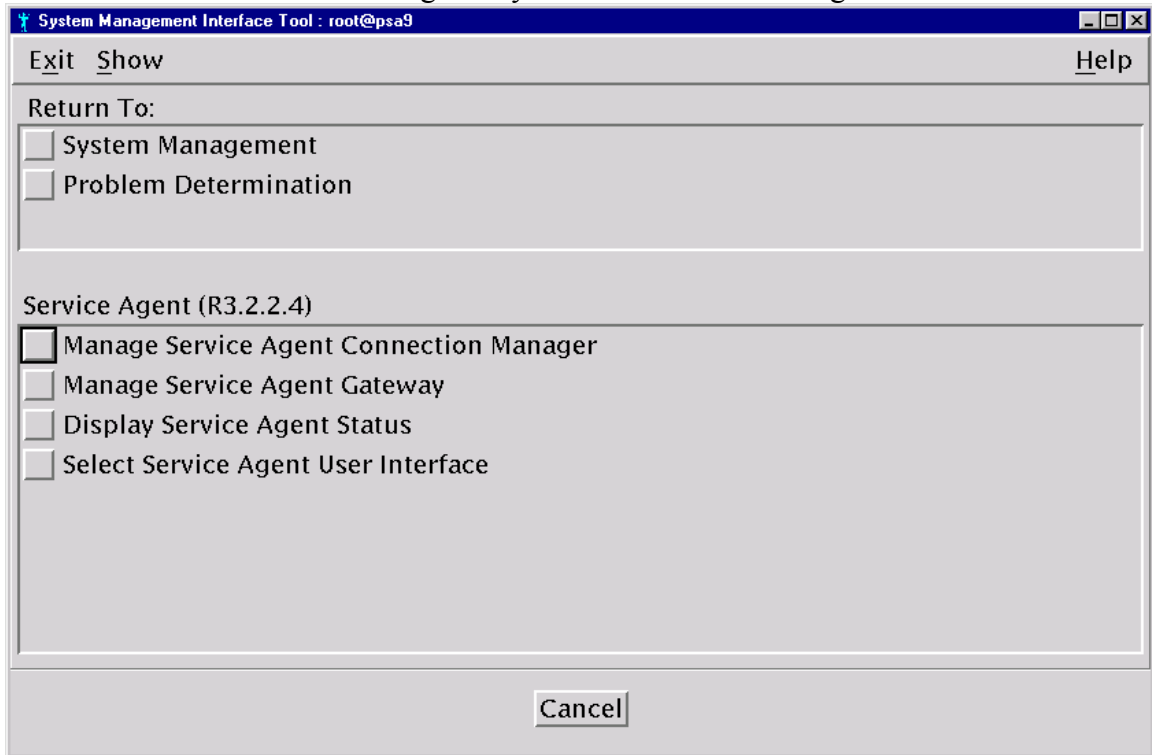


The screenshot shows a dialog box titled "Configure Connection Manager : root@psa9". It has three input fields: "Listening hostname if Multihomed (Optional)" which is empty, "Port(Num.)" which contains "1198", and "Mode" which contains "secure". To the right of the "Mode" field are a "List" button and two arrow buttons. At the bottom of the dialog are five buttons: "OK", "Command", "Reset", "Cancel", and "?".

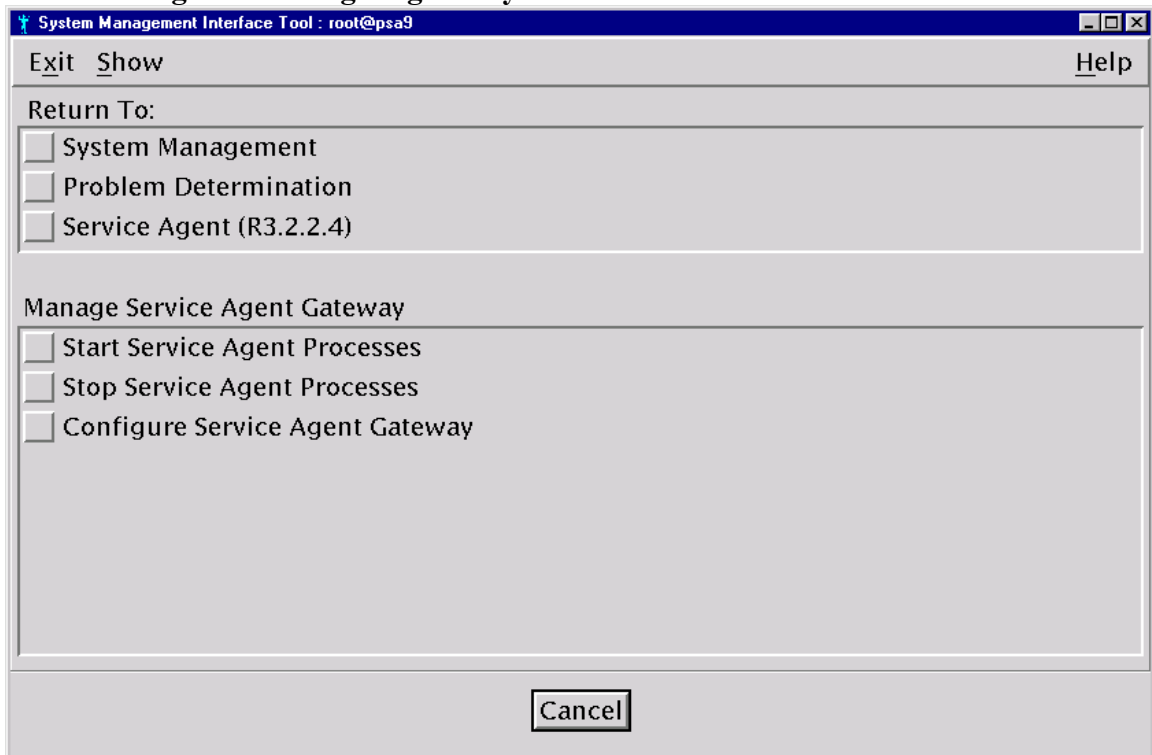
6. The Listening Host Name is blank on initial startup, and if it is left blank, the CM will start on loopback or localhost (127.0.0.1) port 1198 and will listen on all network interfaces that allow automatic loopback.
7. If an account requires connection to listen to a unique interface, insert correct hostname that points to the correct interface. You need to configure SACM to the correct interface and port, and define secure or unsecured assignment if SACM is installed on a standalone AIX host. If there is no need to go through a secure firewall to get to the CM, then you may want to use the unsecure assignment because access will be faster. You will need to change the CallController URL2CM to match interface, port, and security setting.
8. Click **OK**.
9. Click **Done**.
10. Click **Cancel**
11. Once configuration is acceptable, the SACM process must be started using the **Start Service Agent Connection Manager** go back to item 3 and start. Start will add the inittab entries for Connection Manager.

Step 2: Start SA gateway

1. The default hostname of the SA gateway server will be the configured host name.



2. Select **Manage Service Agent gateway**.



3. Select **Configure Service Agent gateway** to initially configure and start the gateway or to define a different hostname.

Enter Machine Type-Model-Serial data entry here (or you will be prompted for it later during SA data entry and definitions). Enter alpha characters in these fields in upper case only.

The screenshot shows a configuration window titled "Service Agent Gateway Configuration [R3.2.2.4] : root@psa9". It contains four input fields with the following values:

Field	Value
* Host Name	psa9.raleigh.ibm.com
* Machine Type(Num.)	7028
* Machine Model	6C1
* Machine Serial Number	103DD6A

At the bottom of the window are five buttons: "OK", "Command", "Reset", "Cancel", and "?".

Auto discovery may have filled in these fields if successful. The machine type is 4 characters, model is 3 characters, and the serial number is 7 characters (in USA, this is 00 followed by the last 5 characters of serial Number).

4. Click **OK**. The configuration and start of the SA gateway processes, add inittab entries for database and ODS scripts.
5. Click **Done**.
6. Click **Cancel** to return to SA main menu.
7. You can now continue with Chapter 8. Initial setup: basic user interface on page 44 to configure SA required data or go to the Chapter 9. Learning about the Advanced User Interface on page 54.

Step 3: Install and configure SA Client on client host

The account security does not allow or support the SA application distribution options, or you wish to install svcagent.client code on the client machines manually, use this procedure. Move the svcagent.client code to the remote client host or distributed filesystem following local account procedures.

1. Use Manually installing Service Agent client from install media on page 35 to install code.
2. The client host may be configured and started, using SMIT - Manage Service Agent Client. The host client may already be in SA database, if host name is not found in the database it will automatically be added.

Configure the client first, hostname is default, change if different hostname is in database. Enter the password to match the SA gateway password no action will be executed if password is wrong or omitted.

The screenshot shows a graphical user interface window titled "Configure Service Agent Client : root@psa9". The window contains a list of configuration fields with corresponding input boxes:

- * Client Host Name: psa9.raleigh.ibm.com
- Primary Gateway: (empty)
- Secondary Gateway: (empty)
- Tertiary Gateway: (empty)
- Password: (empty)
- * Machine Type(Num.): 7028
- * Machine Model: 6C1
- * Machine Serial Number: 103DD6A
- Department Name: (empty)

At the bottom of the window, there are five buttons: "OK", "Command", "Reset", "Cancel", and "?".

3. If the Department Name is in the SA database, the host will be placed under that department name. If Department Name does not exist it will be added to the database first then local client host will be placed under that department name.
4. Define the Primary (required), Secondary, and Tertiary server hostnames.

5. Check the Machine Type-Model-Serial data to be sure it has been properly filled by the auto discovery process.
6. If Client Host Name is already in the database, the entry here will be ignored.
7. If password does not match the SA gateway user interface password this entry will be ignored.
8. Click **OK**.
9. Click **Done**.
10. Click **Cancel** to either end SMIT or make UI selection.
11. Continue to next client host and repeat as often as necessary to enable all of your client hosts.
12. Continue with the Advanced User Interface to Client host information. Then check to see that there is an active Heartbeat from all manually installed client hosts.

Chapter 8. Initial setup: basic user interface

There are multiple NLS enabled interfaces available for configuring Service Agent. You have Graphical or ASCII versions of these interfaces available:

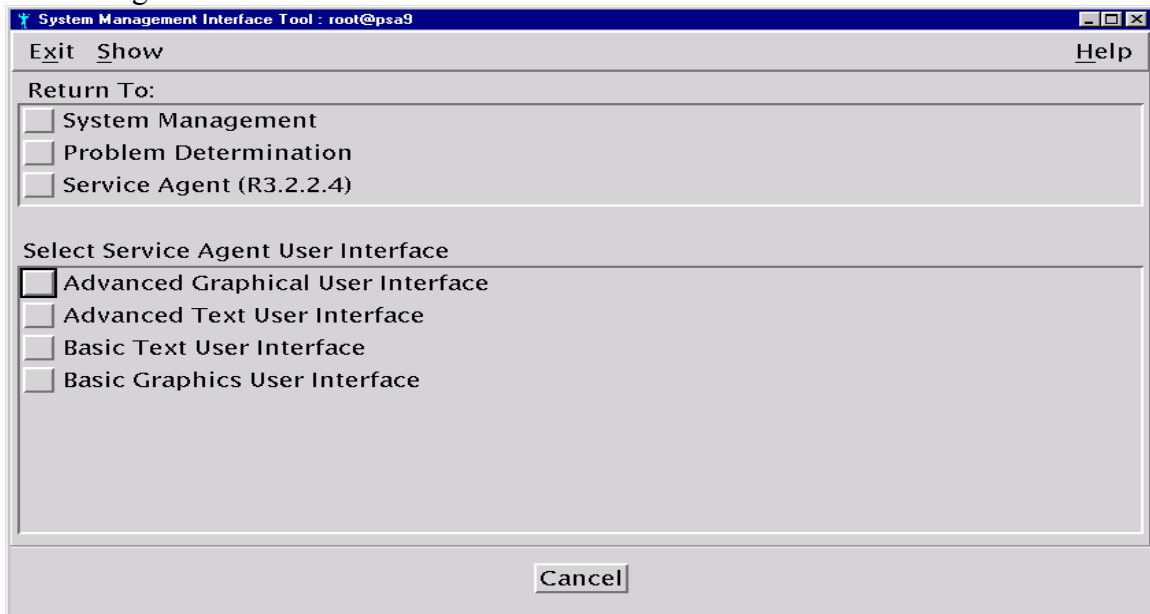
- **Basic Service Agent configuration**
Used for initial guided, simple network client machines; can address SA gateway directly.
- **Advanced Service Agent configuration**
Used for complex configurations and customization of parameters. This is the primary user interface for working with the Service Agent program. For example, this interface must be used to perform a test call to IBM or test e-mail.

Note: The first time you configure Service Agent you can go through the Basic user interface and complete the network and gateway server required fields.

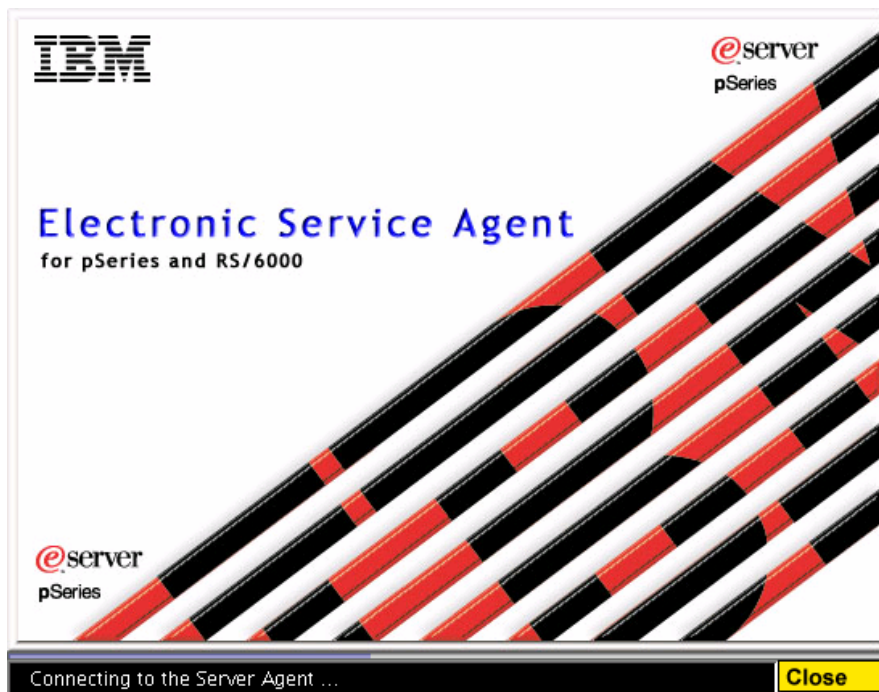
Accessing the basic user interface

Use the basic interface on accounts where all the client machines report to the SA gateway (no complex networks) and the Internet or dialer/modem configuration will be connecting to IBM. This interface will guide the installer through all the steps necessary to set up the correct SA environment.

1. Type **smit** (lowercase) from the command line. Click **Problem Determination**.
2. Click **Service Agent**.
3. Click **Select Service Agent User Interfaces**. The following screen illustrates the Service Agent User Interfaces selection.



4. Click **Basic Graphical User Interface**. (If you want to use the Service Agent program's ASCII Interface version, go to Appendix D – Service Agent ASCII user interfaces on page 125.)
5. The SMIT menu posts *User Interface will appear shortly*. SMIT is finished, and you may exit it at this point. You may elect to return only to the SMIT Service Agent menu for additional selections later.
6. The standalone Service Agent Basic window appears, posting *Connecting to Server*.



This is where the user interface is establishing communications with the ESS on the gateway server. If password prompt does not appear within a minute or two, check Service Agent Status from SMIT menu to verify that the server processes are running. If password prompt does not appear on the SA splash, then the user interface is having problems connecting to the database process.

7. Once the connection is established, a new window appears with a Password prompt. Select the text area and type the password. The default password is **password** in lowercase.

Note: The password can be changed later by going to the **Administration** folder in the Advanced user interface and selecting the **SA access** property. If the password has been changed, it will now carry the old password to the new level of SA. To restore to default password, SA must be reinstalled.

8. The Basic Service Agent configuration screen appears.

Understanding the Basic User Interface Panel

- The far left area (extending from top to bottom) is the Properties area. Within this area is a column of buttons that lets you go from one property folder to another. An auto-prompt feature is incorporated that takes you to the next logical properties folder when an update has taken place.
- The upper section of the far right area of the screen is a static area containing brief help information related to the currently selected property folder and its parameters.
- The lower right area contains the parameter update, selection and display fields. Depending up the actual folder button selected, you can change individual entries by clicking on the areas to be changed and typing in new data. If an exclamation mark (!) precedes the parameter name, that parameter is required. If an icon in the shape of a padlock precedes a parameter, that parameter cannot be changed.
- After all the data has been typed, click **OK** (located at the bottom of the screen) to save the data.
Note: Depending upon which user interface (Basic or Advanced) you are in, some parameters and their fields may have a lock on them in one case and not in the other.

Performing Basic Service Agent Data Entry

Network Properties

Electronic Service Agent for pSeries and RS/6000 R3.2.2.4

File Help

NETWORK SCREEN HELP

Fields with a ! before the titles must be filled out before continuing.
Please Enter the Customer Contact information as required below.
Click OK Button to Accept Data.
See Service Agent Help for additional details.

Customer, IBM Support May Contact

! Name
John Doe

! Phone Number
1234567

! Email (user@server.domain)
jdoe@us.ibm.com

eService Information

IBM Common Registration UserID

Address

! Queue Country / Region
UNITED STATES

Organization

Organizational Unit

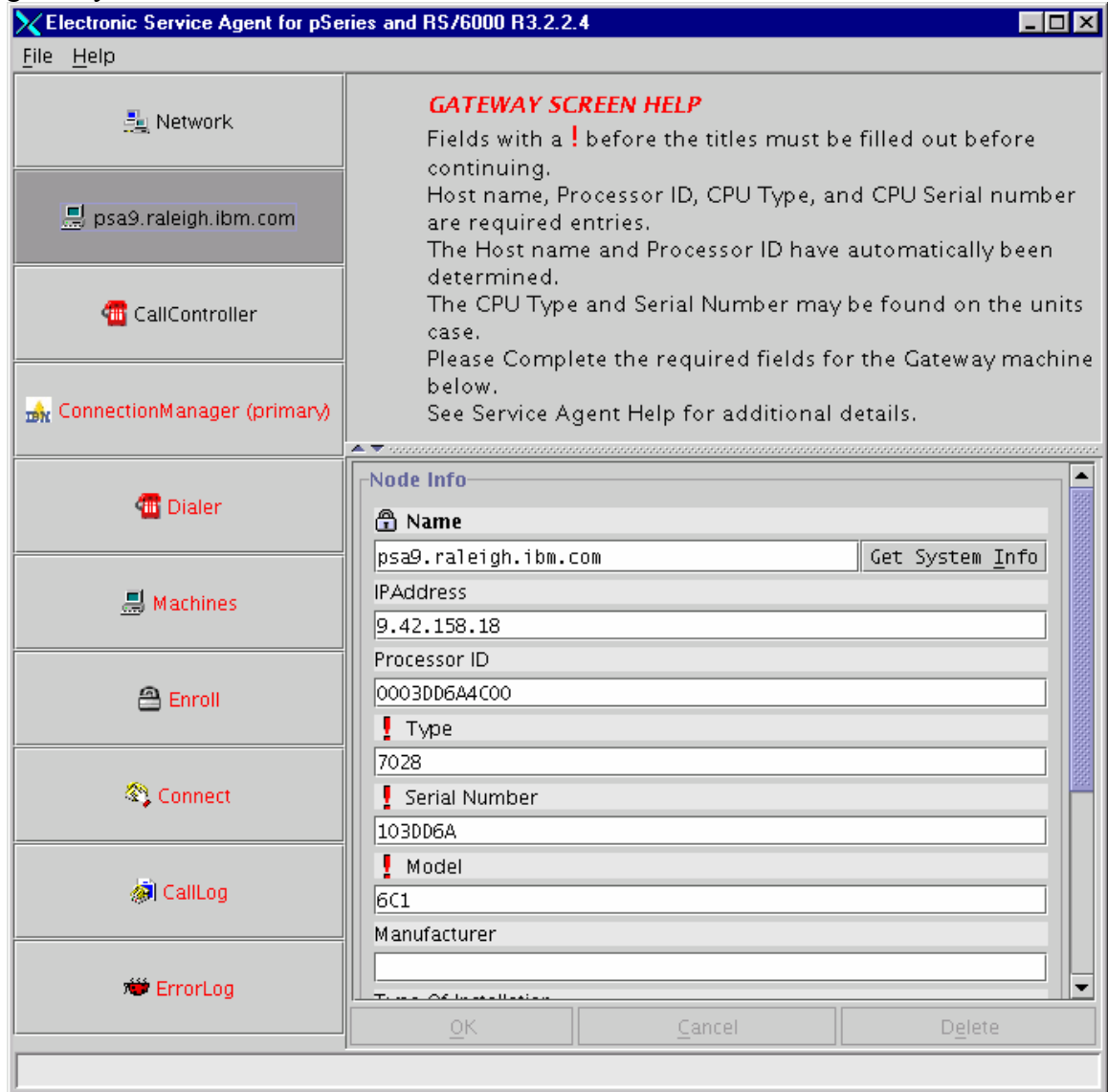
OK Cancel Delete

Country / Region [163 / 173]

1. Type the *Name*, *Phone Number*, and *E-mail* fields of the Local Customer Contact IBM may contact in the Customer IBM May Contact category. The E-mail field is not for e-mail notification, which must be configured with an E-mail Alert. See "How to add an E-mail Alert" on page 74.
2. From the *Queue Country/Region* field in the *Address* category, select from the pull-down menu the **Country** where your machines reside.
3. Complete as many of the fields as possible, to better define account information. The "Telephone Number" will be used for primary contact if entered, instead of the "Contact Phone Number." The "Comments" will be added to all PMR data records.
4. Click **OK**. You see the gateway Properties folder.

Gateway Properties

1. The **gateway** properties folder should appear automatically with most of the *Node Info* category complete. If it doesn't, click the second box that shows your gateway's hostname.



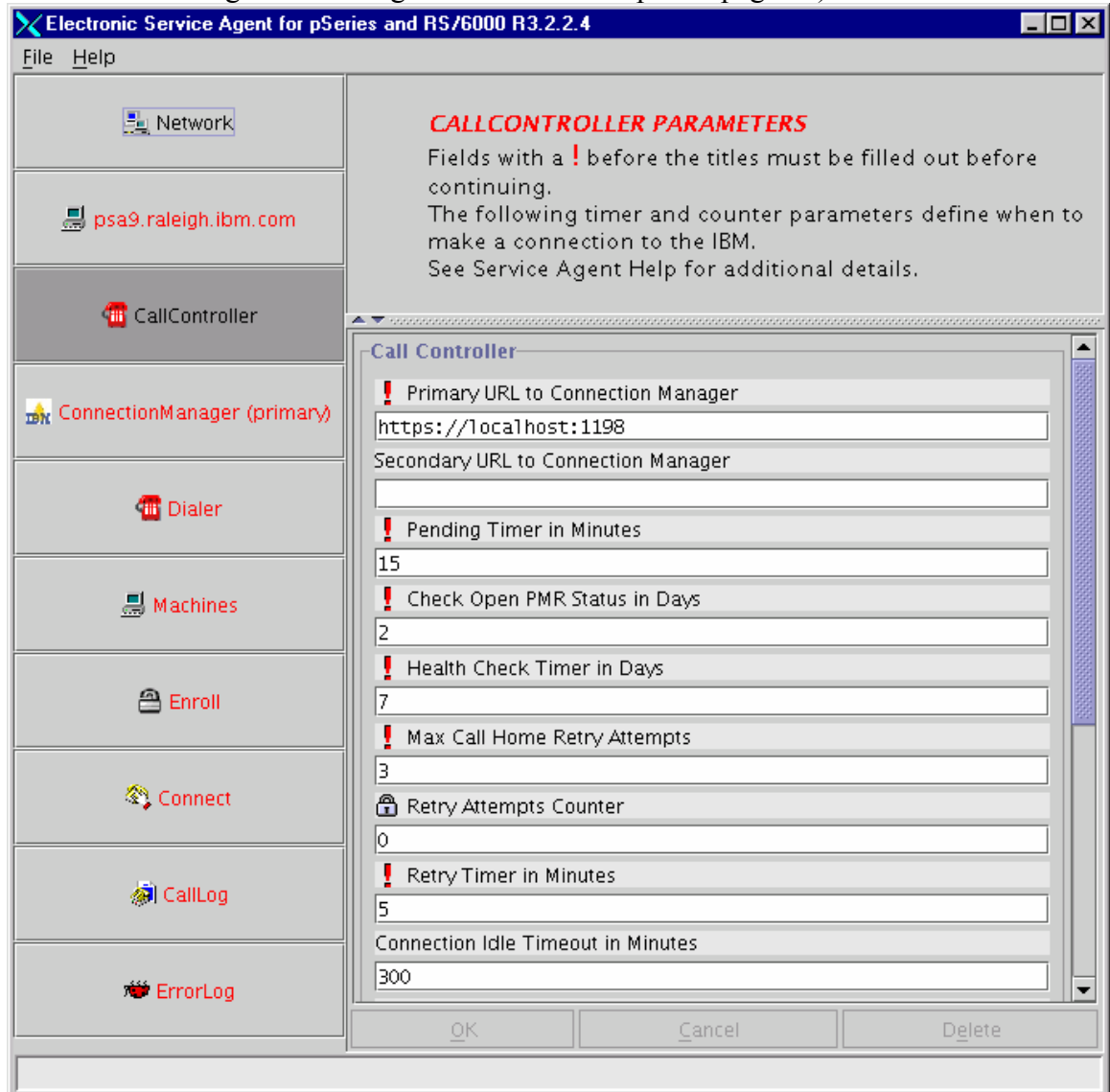
2. The gateway properties folder is labeled with the gateway server's Hostname. The *Node Info* category contains the name, IP address, and processor ID fields. Validate these for accuracy.
3. Enter the machine type (4 characters), serial number (7 characters), and model number (3 characters) in the appropriate fields. Alpha characters must be in UPPER CASE.
Note: If the gateway machine is a 9076 Control Work Station (CWS) use the 9076 type, serial number, and model information instead of the CWS local

machine information. You may have to correct the auto-discovery fields if they do not contain the 9076 information for the CWS.

4. Click **OK**. You see the CallController Properties folder.

CallController Properties

1. Verify the Primary URL to ConnectionManager field. This defaults to localhost, which is appropriate if the CM Listening Host Name was left blank. If the CM host is a different host or if listening hostname is unique to a communications adapter, then update the URL to reflect the correct hostname (the hostname that Connection Manager was configured with from Step 6 on page 39).

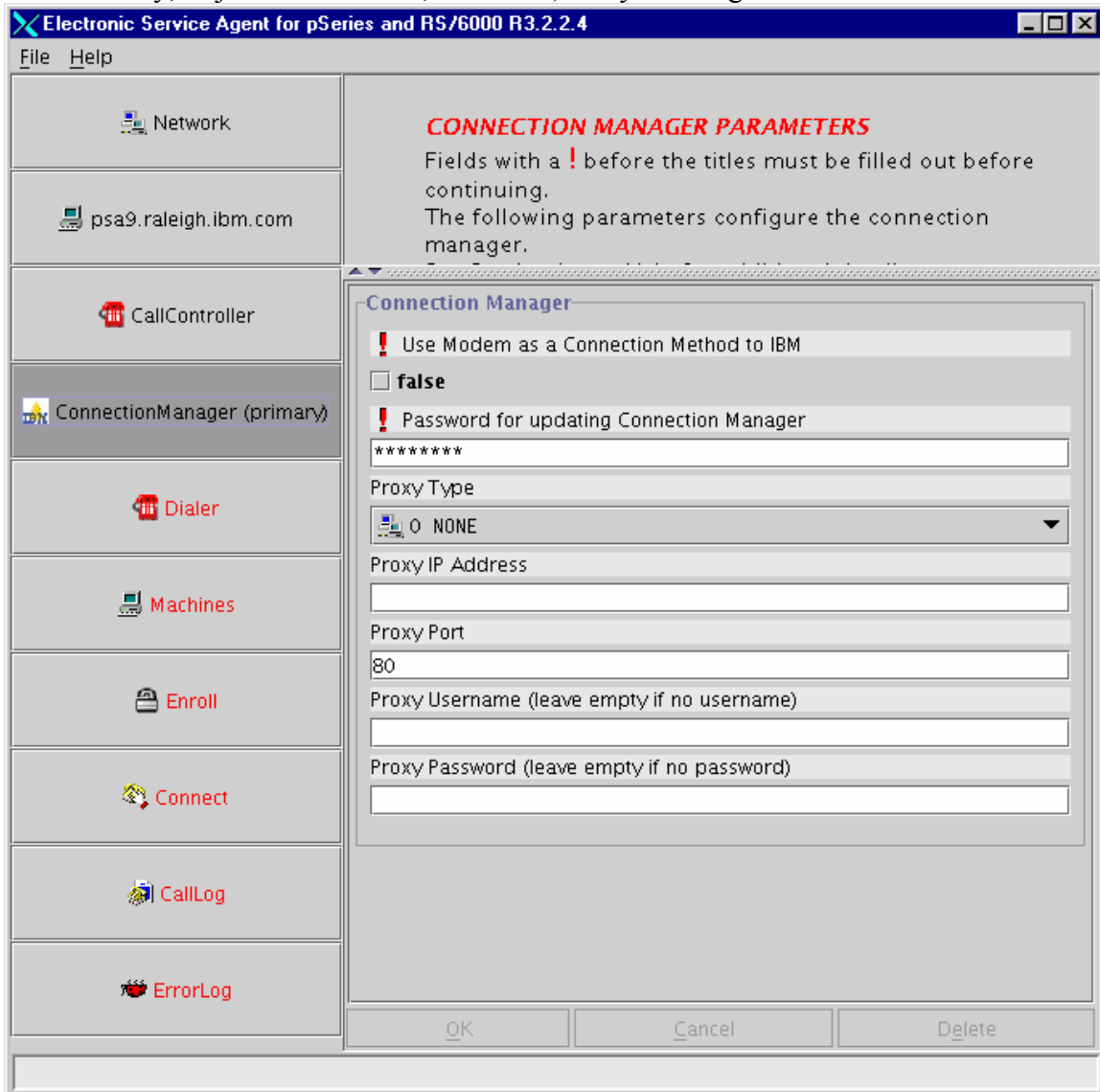


2. If port was not defaulted to 1198, correct the port number.
3. If Proxy is required to connect to Connection Manager, you must update the Proxy fields. The proxy must be able to pass port 443 to allow proper connection.
4. Click **OK**. You see the Connection Manager Properties folder.

ConnectionManager Properties

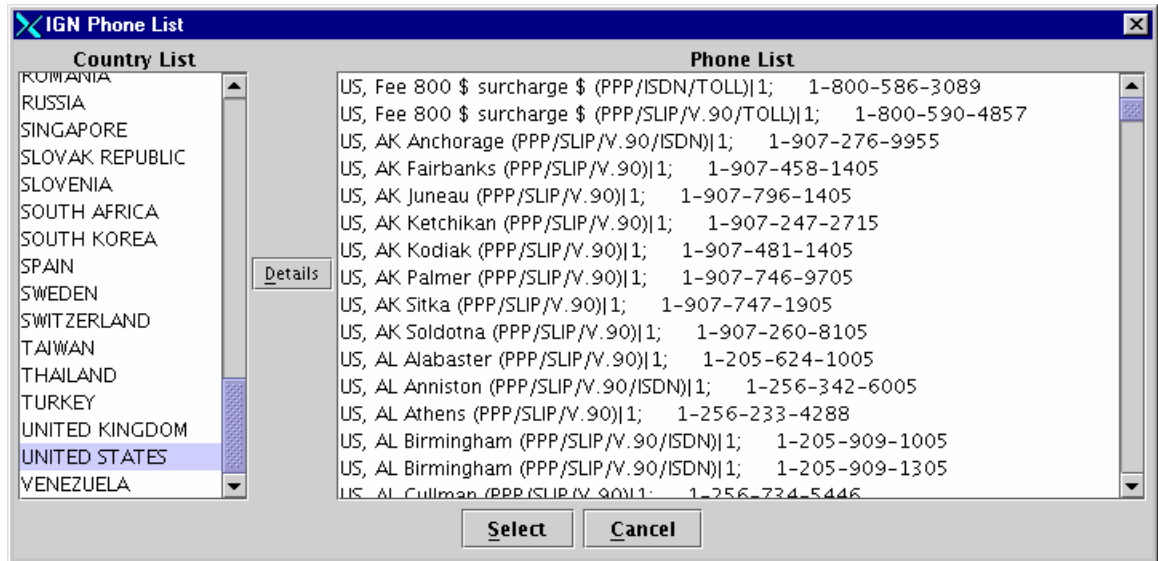
This folder lets you select your machines' method of communication with IBM.

- If you're using a Modem, choose **true**, click **OK**. You see a prompt asking *Configure Modem Now?* Click **Yes**. You see the Dialer Properties folder.
- If you're using an Internet connection, enter proxy type and any needed proxy data if necessary, or just choose **false**, click **OK**, and you will go to the Enroll folder.



Dialer Properties

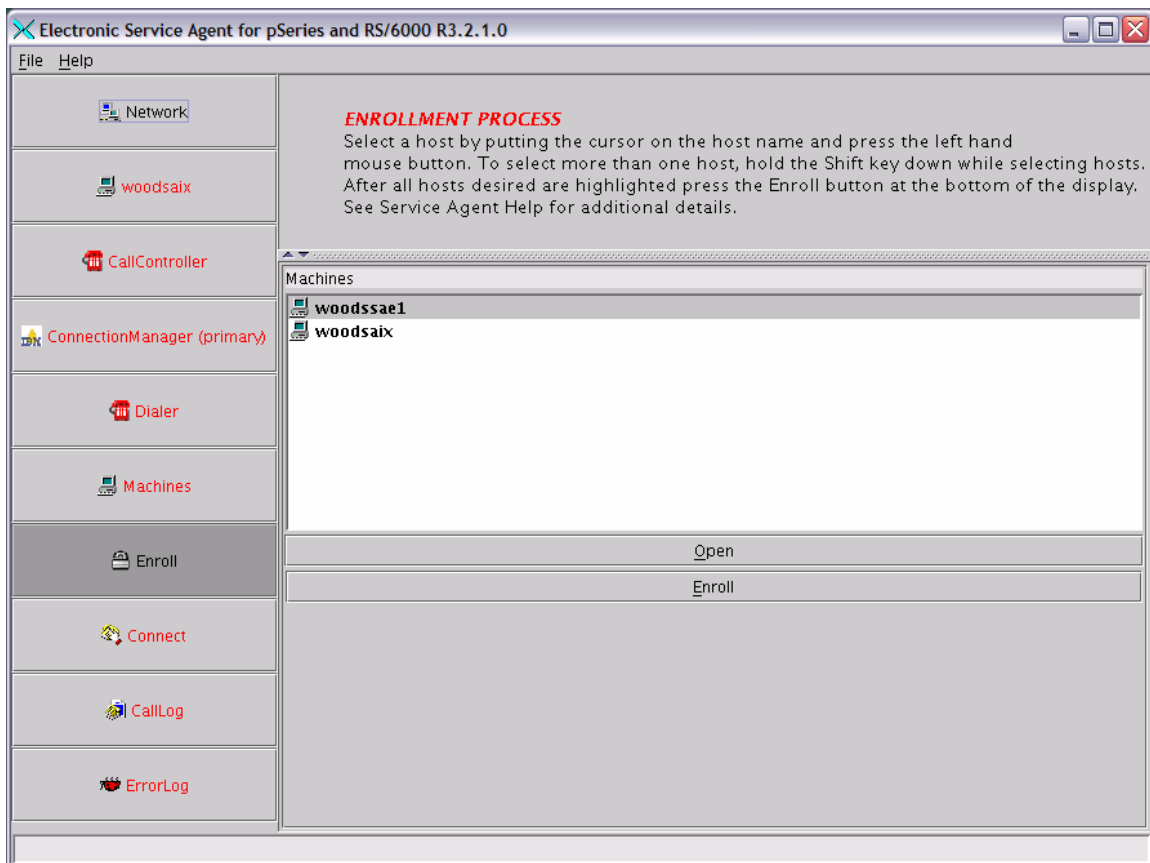
1. From the Location field, above the primary phone number, select the phone list browse box. This will post the Phone List with the country and city the modem calls to.



2. Open the *Location field*, select the proper *country*, then click **Details**. Select *city* and *local phone number*. Additional fields within the Dialer property are filled in for you.
3. Check the *Primary Phone Number* field and make sure it is filled in and correct. Depending on the local phone exchange, this number may need to be modified to utilize your outgoing number and area code requirements.
4. Check the *Secondary Phone Number* field to make sure it is filled in and correct..
5. The *Account*, *User ID*, and *Password* fields are automatically filled in and should not require changing or alterations.
6. Click the **TTY # dropdown**. Select the TTY # (number) of the serial port into which the modem is plugged.
 - The modem, by default, has to be attached to the Connection Manager server to establish communication with IBM.
 - If the TTY port number selected is in use with a process that is logged on to it, SA will reset the port number and take control when it accesses the port.
Attention! Do **NOT** select the same TTY port number that the boot console is using. The terminal will be reset and unpredictable results may occur.
7. If the default modem does not match your attached modem, click the **Modem dropdown** box. Select the Modem that matches the one installed to your gateway server. See “Modem communication steps” on page 23 for more information. Selecting a modem produces the values used in the Reset String and Init String fields. These modem strings are on an AS IS basis. They may need to be modified depending on the environment setup of your system.
8. If you have a rotary or pulse phone system, click the **Dial Type dropdown**. Select the *dial type (pulse)* to match the type of phone line.

9. Click the **Baud Rate dropdown**. Select the highest *baud rate* that your TTY uses. Selecting a baud rate greater than the modem supports could cause the dial-out process to fail. The flag entry *Verify Baud Rate Before Dialing* is defaulted to True. This feature, starting with the baud rate you types, attempts to find the correct baud rate setting for the TTY automatically.
10. If necessary, modify the default *reset and init strings* to work with the modem.
11. Click **OK** to save your Dialer property configuration data. Click **Yes** to go to the Enroll folder.

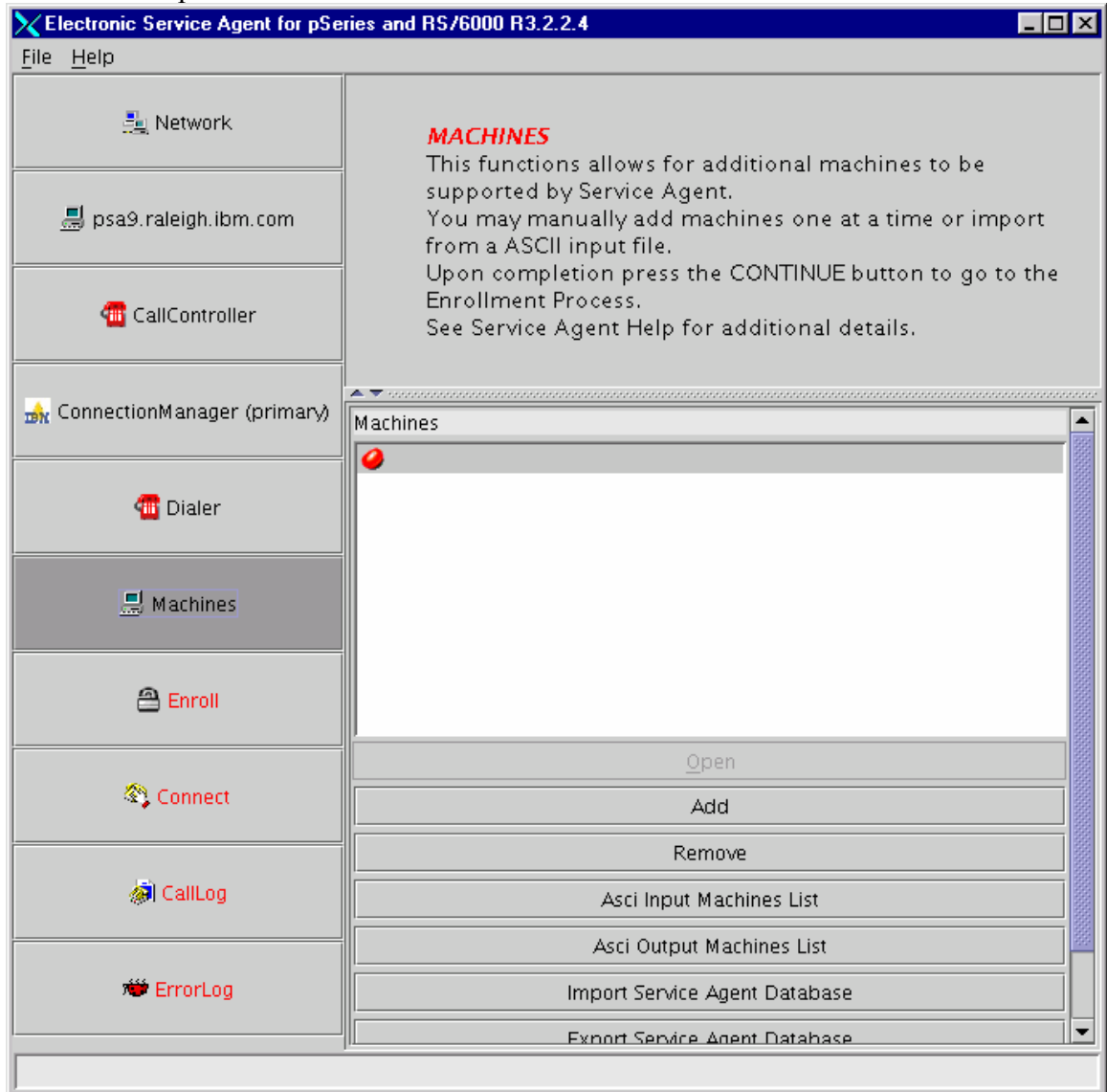
Enroll Properties



1. Select the **machines** you want to enroll by highlighting one or more of them. Holding down the shift key while selecting the second machine will allow a range to be selected.
2. Click **Register** or **Enroll**.
3. From the *Would you like to Connect to IBM Now?* prompt, click **Yes**. This action takes you to the CallLog properties folder.

CallLog Properties

1. Check the description column to determine if your call to register a system was successful or failed. See “Call Log Properties” on page 87 for a description of the CallLog fields.
2. If you are only installing Service Agent on a single machine, you have completed Basic Service Agent configuration. To exit the Basic Service Agent configuration interface select **File** and then click **Exit**.
3. If there are other monitored client hosts you want to add at this time, use the Machines template.



4. If you want to add more monitored machines, customize those monitored machines, or configure SP nodes, see “How to add or create additional configuration entries” on page 68.

Chapter 9. Learning about the Advanced User Interface

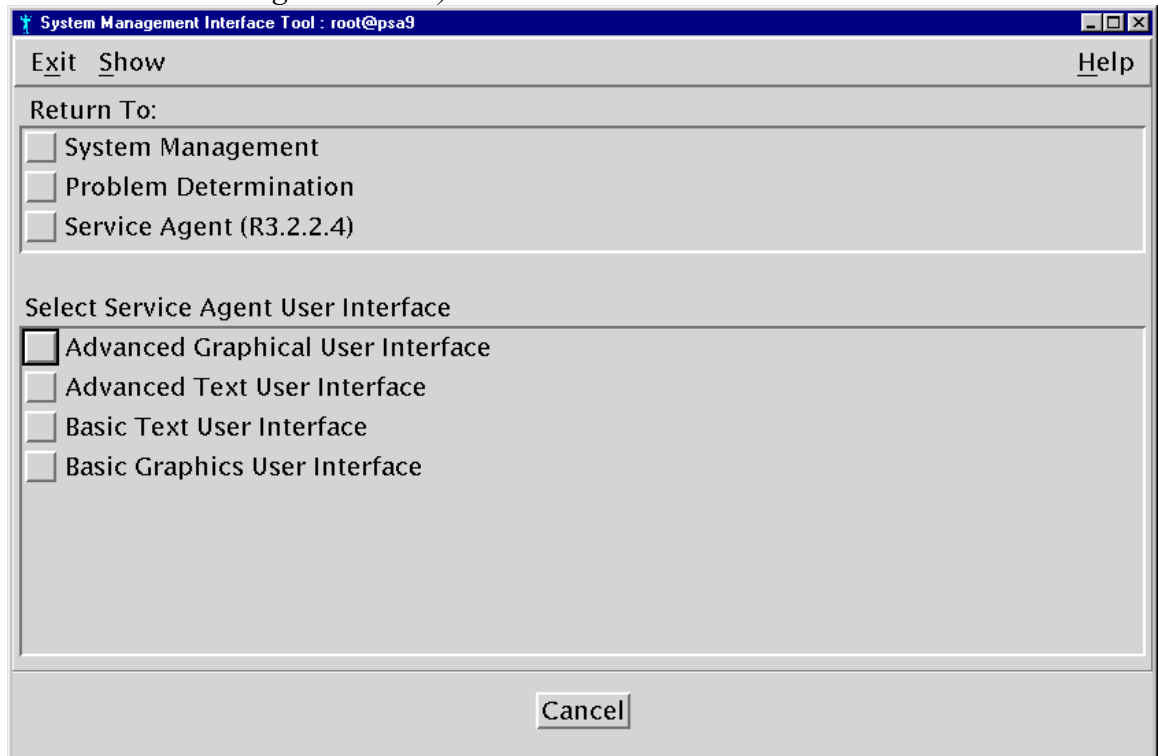
The Advanced User Interface is used for advanced functions and is National Language Support (NLS) enabled. Use this chapter to familiarize yourself with the user interface, but use the next chapter for guided steps on how to do functions.

You can use this interface anytime after the gateway server host type and serial number fields have been defined. All functions available within the basic interface are a subset of the functions available in the Advanced interface.

For later releases of the application, the Advanced interface can be used initially, and basic data will be prompted. You must remember to fill in additional account information and, if using a modem to access IBM, complete the Dialer template.

Accessing the Advanced Service Agent User interface

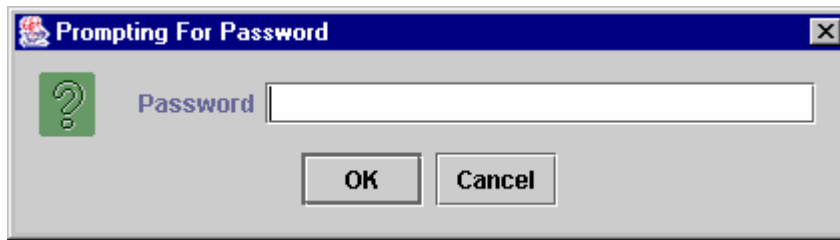
1. Type **smit** (lowercase) from the command line.
2. Click **Problem Determination ->Service Agent gateway-> Select Service Agent User Interfaces -> Advanced Service Agent User Interface**. (or use this command : `/usr/svcagent/bin/saui`)



3. If you want to use the Service Agent program's ASCII Interface version, go to "Appendix D – Service Agent ASCII User Interfaces" on page 125. You can execute this command for ASCII: `/usr/svcagent/bin/sauiascii`

Logging in

The Advanced Configuration interface requires a password to gain access to the system. The initial default password is **password**.



The administrator should change this password to one that is unknown to anyone but himself and/or authorized personnel to protect the Service Agent configuration setup from unauthorized modifications. Review the README file for the various passwords used within Service Agent.

- While Service Agent is waiting for input and matching the password a *Prompting for Password* progress window is displayed. After a successful password match, the user interface is displayed.
- Typing a wrong password causes an error message to be displayed indicating the password entered does not match the one expected. If the error message comes up, click **OK** and retype your entry to try again.
- You have up to six chances to type the password correctly. On the sixth mismatch, the logon quits and you must select the Advanced Configuration interface from SMIT again.

No Password Prompt

If hang occurs at this point, when you are expecting to get the password prompt, the User Interface is not connecting to the ESS database process on the SA gateway.

- Check that the `/var/svcagent/properties` file is pointing to the correct server.
- Check that the ESS process is running on the server with `ps -ef |grep svca` command.
- Use `netstat -a|grep 1199` to see if the direct connect port has been properly registered.

If these things check out, but the prompt is still not appearing, activate logging for the ESS and ODS scripts (See the Readme file for activating logging).

Basic Data Entry

If you entered the Advanced UI without first doing Basic UI, the following data entry prompt is displayed.

Please enter the following required data

Customer, IBM Support may contact

Name John Doe

Phone Number (845) 498-3334

Email (user@server.domain) jdoe@us.ibm.com

Queue Country / Region UNITED STATES

Gateway

Type 7028

Serial Number 103DD6A

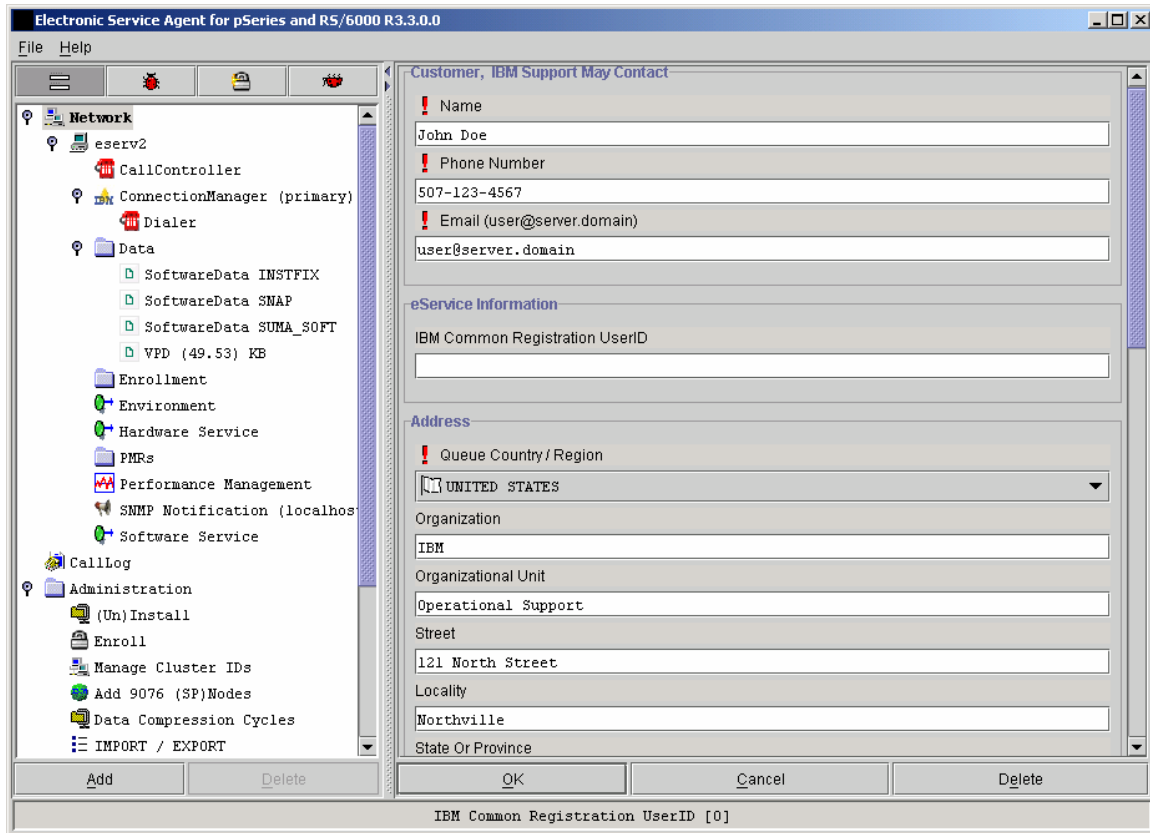
Model 6C1

Continue **Exit**

1. Fill in the customer information.
2. Select the correct country from the pull-down window.
3. If not filled in already by auto-discovery, enter Machine Type-Model-Serial data entry here
 - The machine type is 4 characters, model number is 3 characters, and the serial number is 7.
 - Enter any alpha characters in these fields in UPPER CASE only.
 - **Note:** The machine data must match the RETAIN customer profile data exactly. If not, when you try to create a Test PMR, you will see this message: "FAILED Country, Type or Serial not available or error in Local MPI database." You will need to check with the local country Remote Support group to correct the problem.
4. Click **Continue**. You see the Advanced Configuration panel.

Understanding the Advanced Configuration panel

The Advanced user interface is divided vertically into two panes – a navigation pane on the left and a detail-viewing pane on the right.

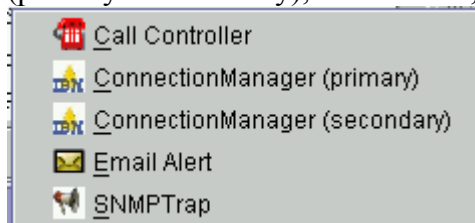


→ **Navigation Pane** ← | → **Detail Viewing Pane** ←

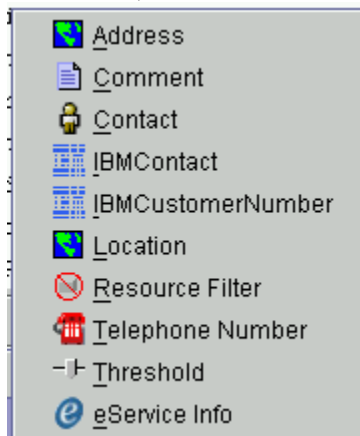
Navigation Pane

- File and Help buttons are located in the Menu bar. Click the File drop-down to enable the Exit option. Click the Help drop-down to see Help and About options.
- Category selector icons, at the top of the navigation pane, are used to select these types of information: Properties, Error Events, Licensing Information, and Internal Errors. See “Category Selectors” on page 59.
- Properties selectors are listed below the category selectors.
 - Click any property selection to see corresponding information in the detail pane on the right or additional function selections in the navigation pane.
 - If a property selection has a key pointing to the right, there is another level of detail below it. Click the key to expand the view.
 - A key pointing down indicates that all lower levels are displayed. To hide that level, click the key again. You can use this hierarchy to view information at different levels; for example, you can view data for the entire network, for a department, or just for an individual machine.

- The **Network** property selection is considered the main infrastructure property of the Service Agent system. This property displays the hierarchy tree used to view and configure information for individual machines and groups and includes these areas of information for each server you are monitoring: CallController, Connection Manager, Dialer, Data, Enrollment, Environment, Hardware Service, PMRs, Performance Management, SNMP Notification, Software Service, and CallLog. For information about each of these areas, see “Appendix B – Advanced UI Configuration/Property Details” on page 89.
 - The **Administration** property selection lets you choose these areas of information: Register, (Un) Install, Enroll, Manage Cluster IDs, Add 9076 (SP) Nodes, Data compression Cycles, Import/Export, Lockout Machines, Purge Data, Remove Sub-Net Machines, SA Access, and SA Update.
 - **Alerts** shows you the alerts you have set.
 - **Filter Lists** shows you Resource Filters and Thresholds.
 - **Manual Tools** lists tools that can be installed manually: Connect, Microcode, PMR, Performance Data, SNAP, and VPD.
 - **Test Tools** includes Test Email, Test PMR, and Test SNMPTrap.
- **Add button** at the bottom of the navigation pane, when enabled, offers these choices:
 - **Child:** lets you select these additions: Call Controller, ConnectionManager (primary or secondary), E-mail alert, SNMPTrap.



- **Forms:** lets you select these additions: Address, Comment, Contact, IBM Contact, IBM Customer Number, Location, Resource Filter, Telephone Number, Threshold, eService info.



- **Delete button** at the bottom lets you delete data displayed in the detail pane.
- Chapter 10. Advanced Configuration Tasks, explains how to use the features of the Advanced Configuration panel for individual procedures.

Detail Viewing Pane

- To edit the detail information to the right, click in a field and make the necessary changes.
- Mandatory fields are indicated by an exclamation mark; fields that cannot be changed are flagged with a padlock.
- If you are selecting an item from a list, you can type the first letter of the item you want to move quickly through the list.
- Click **OK** to save your changes, or click **Cancel** to abandon your changes. If you fail to click **OK** before switching to a different panel, your changes are not saved.
- For output fields like errors that are displayed:
 - You can scroll right to see all fields, or you can drag column titles to other positions. However, your changes will not last into the next session.
 - To see additional details about an error event, click on it. The details are displayed in the bottom right pane.

Category Selectors

There are four category selectors available to determine the type of information displayed in the detail window when you select a properties folder.

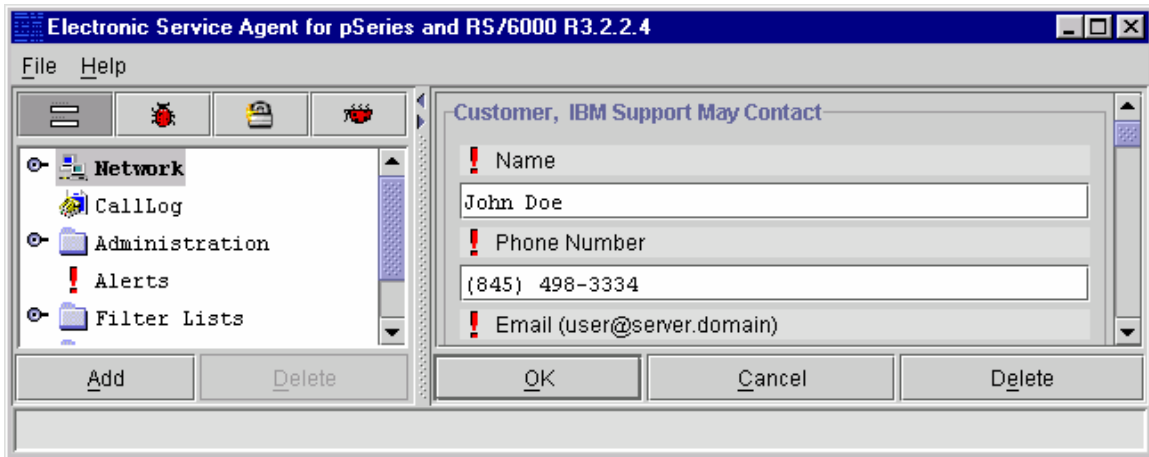


In many cases, the right detail panel may be blank. This is because the selected category may not have any information available.

View/Edit Properties button



The View / Edit Properties button is identified by the icon that looks like an equals (=) mark. While you select this category, all the Properties buttons described above are active and available, and you can see information about any property in the Detail Pane. .

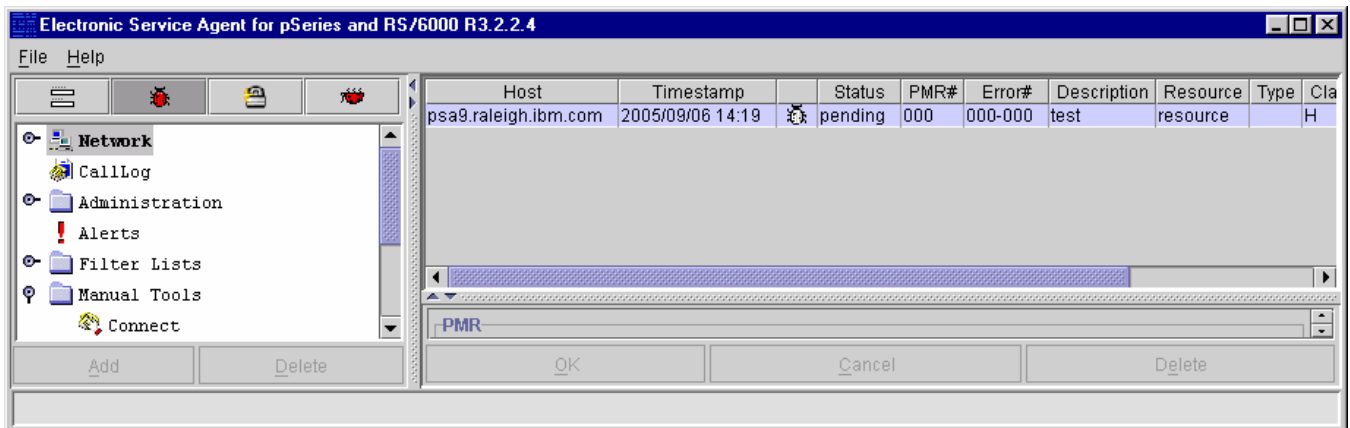


View Error Events button



To view error events:

1. Click the **View Error Events** icon (red bug).
2. Click the **Network** properties button.
3. Select an individual machine, such as eserv2.
4. Select an area of information. Some areas may be blank.



You may see the error details listed below, or a subset of these details.

- Host** The name of the machine for which information is being displayed.
- Timestamp** The year, month, day, and time the Error Event occurred.
- Icons** Quick indicators of error status.
- Status** The current state of a selected error. Possible states are:

Pending

Indicates an entry that is ready to be sent to the IBM Service Data Receiver (SDR). If the status is some other state, setting it to Pending again causes the entry to be resent.

held

Indicates that the Error Event was held rather than reported to IBM.

open

Indicates that the Error Event was sent to IBM and a Problem Management Report (PMR) was generated.

duplicate

Indicates an attempt was made to open a PMR that was already opened. If the same Type, Serial number, Description, and error number are opened before a previous PMR with the same error is closed, a duplicate status is returned.

failed

Indicates that the Error Event failed in the attempt to open a Problem Management Report (PMR); this will also be an internal SA error.

closed

Indicates that the Error Event previously opened with IBM has been closed.

PMR# (PMR Number)

PMR stands for Problem Management Report. The number in this field is the PMR number returned from IBM when an Error Event or problem is opened.

Status Details

Contain results of transmission attempts to IBM for specific error event or PMR entry.

When Status Checked

Last time the opened status of a specific error event was checked for closure.

Description

Error description that was generated.

Resource

The logical resource name of the component that failed.

Type

Describes the severity of the error that has occurred. Following are the definitions for the error types:

PERF

Condition where the performance of the device or component has degraded below an acceptable level (performance).

PERM

Condition from which there is no recovery (permanent).

PEND

Condition signifying that the loss of availability of a device or component is imminent (impending).

TEMP

Condition that was recovered from after a number of unsuccessful attempts (temporary).

UNKN

Condition where it is not possible to determine the severity of the error (unknown).

INFO

Condition for informational error log entry.

Class

Describes whether the error occurred in hardware or software, is an operator message, or is undetermined. Following are the definitions for the class descriptors:

H Indicates the error is a hardware failure.

O Indicates the error is an operator message.

S Indicates the error is a software failure.

U Indicates the error is undetermined.

Dups

Counter of duplicated error events that occurred since the original entry was generated and opened.

Last

Last time the Error Event occurred.

Error Details

Contains specific details for the error that occurred.

Status Details

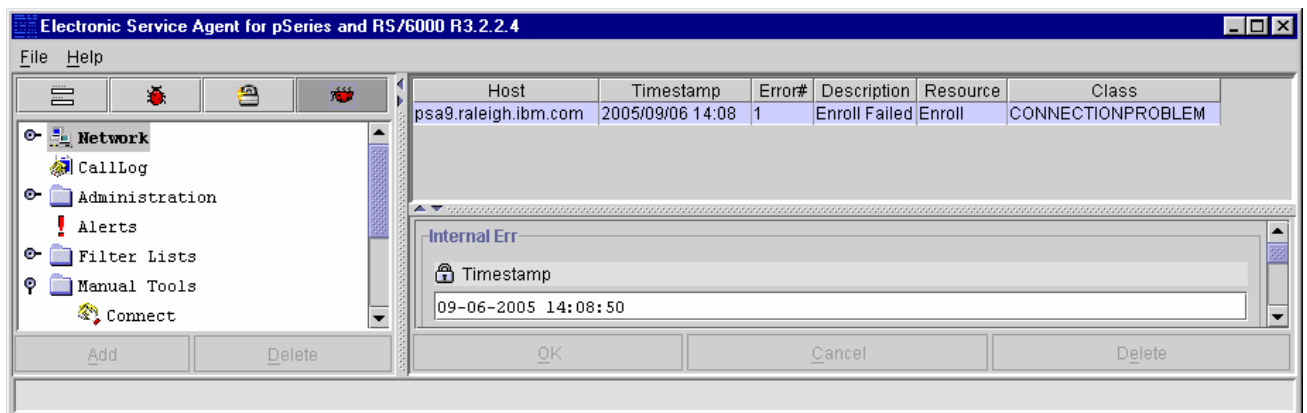
Contain results of transmission attempts to IBM for a specific error event or PMR entry.

View Service Agent Internal Errors button



To view internal error events:

1. Click the **View Internal Errors** icon (red bug on its back).
2. Click the **Network** properties button.
5. Select an individual machine, such as eserv2.
3. Select an area of information. Some areas may be blank.



You may see this internal error information:

Host

The name of the machine for which information is being displayed.

Timestamp

The year, month, day, and time the error occurred.

Error# (Error Number)

The number the system uses to identify the type of error generated.

Error Details

Contains specific details of error that occurred.

Status Details

Contains results of transmission attempts to IBM for a specific error event or PMR entry.

When Status Checked

Last time the opened status of a specific error event was checked for closure.

Details

Displays any appropriate error information about the internal error if available.

ID

Internal identification number. Typically “-1”.

Description

Description of the error that was generated.

Resource

The logical resource name of the program component that failed.

Class / Error Class

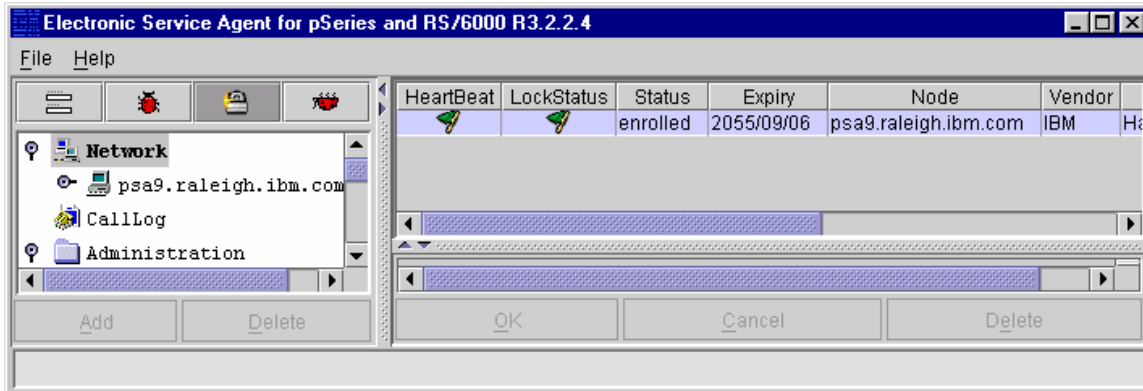
Typically this field indicates “none”.

View Licensing Information button



To view internal error events:

1. Click the **View Licensing Information** icon, which resembles a padlock.
2. Click the **Network** properties button.
3. Select an individual machine, such as eserv2.
4. Select an area of information. Some areas may be blank.



You may see the licensing information listed below.

HeartBeat

The HeartBeat status indicates whether a monitored machine has reported into the gateway within the defined time limit. A successful HeartBeat is indicated by a Green Flag. A missing HeartBeat is indicated by a Red X, indicating that the client is not communicating with the gateway within the specified time limit. Some causes for missing the HeartBeat are:

- Different version levels between the gateway and the monitored machine
- The Client code (On Demand Server) not running or needs to be restarted
- Possible slow network delays causing the client to miss its HeartBeat window
- The node is down
- The wrong time zone is set on either the gateway server or a client node.

To adjust the HeartBeat window: go into the Hardware Service template on the individual machine and change the HeartBeat and/or the HeartBeat Delay accordingly. To be notified when a machine misses a HeartBeat, you can set the heartbeat flag in the e-mail Notification template.

LockStatus

Indicates whether a system has been locked out and all errors detected are ignored or whether it is unlocked and the machine is being monitored. A Green Flag indicates the system is unlocked and is being monitored. A Red X indicates the machine is locked out and is being ignored.

If you want to run diagnostic tests on a machine's lockout capability:

1. In the Navigation Pane, click **Administration**.
2. Click **Lockout Machines**.
3. Click the machine whose lock status you want to change.
4. Click **Lock**. The LockStatus changes to a Red X.
5. Repeat the first three steps.
6. Click **Unlock**. It is essential that you return the machine to an unlocked status.

Status

Indicates the Hardware Service Template status of the machine. See “Hardware Service Template” on page 99 for detailed explanation of the Status.

Expiry

The date when the enable license expires.

Node

The name of the machine for which information is being displayed.

Vendor

The name of the company that manufactured the selected machine or device.

Module

The name of the Module or Template that is licensed. An example of this is the Hardware Service template.

Comment

A general comment field containing additional information pertaining to the licensed template.

Chapter 10. Advanced Configuration Tasks

This chapter contains instructions for various Advanced Configuration tasks that you can perform from within the Advanced User Interface. The tasks are grouped into the following categories:

- How to perform connectivity tasks
- How to add or create additional configuration entries
- How to remove or delete configuration entries
- How to test certain configuration functions
- How to perform other Service Agent functions

How to perform connectivity tasks

How to set up SA CM to use Dialer

If you want to use modem connection, as opposed to an Internet connection, perform these steps.

1. Click **Network**.
2. Click **Gateway host**.
3. Click **Connection Manager**.
4. Click **Use Modem as a Connection Method to IBM** check box to **true**.
5. Click **OK**.
6. Click **Dialer** if displayed.
7. If Dialer icon is not displayed, with CM selected click **Add->Child->Dialer**.
8. Complete the steps described in “Dialer Properties” on page 51.

How to set up SA to use an Internet connection

If you want to switch from using a modem connection to using an Internet connection, perform these steps. Internet connection is the default configuration.

1. Click **Network**.
2. Click **Gateway host**.
3. Click **Connection Manager**.
4. Click **Use Modem as a Connection Method to IBM** check box to **false**.
5. Click **OK**.
6. Click **Dialer**.
7. Click **Delete**. (bottom of left pane)
8. Click **OK** to the fail-safe prompt. (Deletes this server Dialer which will not be used)

How to set up a master gateway

By default all gateways when installed are master gateways. A master gateway by definition is one that contains a Connection Manager object.

How to set up a slave gateway

Slave gateways are not capable of updating the Connection Manager configuration. They are only capable of submitting requests to the Connection Manager for transmission to IBM.

Perform these steps to make a gateway become a slave gateway.

1. Click **Network**.
2. Expand **Gateway host**.
3. Click **Connection Manager**.
4. Click **Delete** (bottom of left pane). You see a fail-safe prompt.
5. Click **OK**. (Delete this server's SACM because it will not be used)
6. Click **Dialer**.
7. Click **Delete** (bottom of left pane).
8. Click **OK** to the fail-safe prompt. (Deletes the server Dialer because it will not be used)
9. Click **CallController**.
10. Enter the qualified hostname of the SACM server in the **Primary URL**.
(YourMaster.SACM.Server.Hostname:1198)
11. Click **OK**.

How to set up to a remote Connection Manager

If you want to utilize a remote Connection Manager not installed on the gateway itself but this host will be the master gateway, perform these steps.

1. Start **Advanced UI** for this gateway.
2. Click **Network**.
3. Click **Gateway host**.
4. Click **CallController**.
5. Enter the qualified hostname of the SACM server in the **Primary URL**.
(YourMaster.SACM.Server.Hostname:1198)
6. Click **OK**.

How to set up to a secondary Connection Manager

If you want to utilize a secondary Connection Manager as a backup, perform these steps.

1. Install svcagent.cm package on secondary Connection Manager
2. Start Connection Manager using smit on secondary host

3. Start **Advanced UI** for this gateway.
4. Click **Network**.
5. Click **Gateway host**.
6. Click **Add->Child->Connection Manager Secondary**
7. If a dialer is required for this CM, click **Add->Child->Dialer**, configure the dialer, and click **OK**.
8. Configure the secondary Connection Manager as required.
9. Click **OK**.
10. Click **CallController**
11. Populate the URL to Secondary Connection Manager properties.

How to change connection manager listening port

If you want to change the listening port for the Connection Manager, perform these steps. The Connection Manager default port is 1198.

1. Log into the CM machine as root.
2. Stop the CM using SMIT.
3. Edit `/var/svcagent/locks/lock.cm` and change the port number.
4. Save the file.
5. Restart the CM using SMIT

How to add or create additional configuration entries

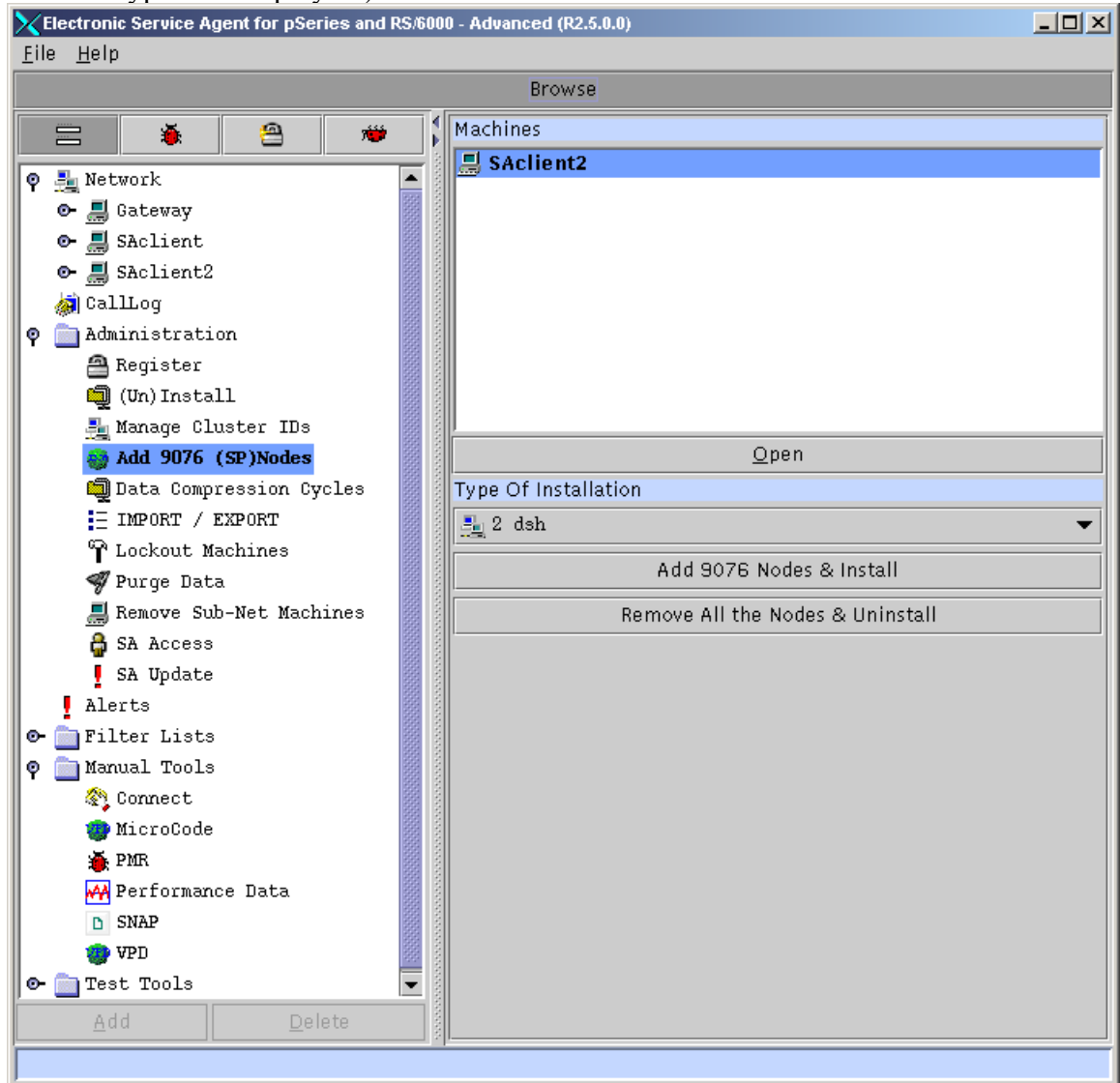
How to create a department of monitored machines

If you want to create a group of client machines under a department, you need to add the department name first. Then client machines can be created under that heading.

1. Click **Network**.
2. Click **Add**.
3. Click **Child**.
4. Click **Department**.
5. Type the **name** you want to use to describe this department or group. (This example uses DEPT1 as the department name.)
6. Click **OK**.
7. Click **DEPT1** (or the name you used to create your department).
8. Click **Add**.
9. Click **Child**.
10. Click **Machine**.
11. Fill out the *Node Info* template and click **OK**. This new monitored machine (designated by the name you give it) appears indented under the DEPT1 department name.

How to add SP Nodes

1. Expand the **Administration** property.
2. Click **Add 9076 (SP) Nodes**.
3. Select the 9076 host to which you want to add nodes. (Only hosts with 9076 machine types are displayed.)



4. Select **FTP, DSH, or RSH protocol option** from the *Type of Installation* table.
5. Click **Add 9076 Nodes & Install**.
6. When you use the FTP protocol, the *Enter the User ID and Password* window appears. Type the password for root. If you cannot use root and the root password, you can change the User ID field to a root-authorized user ID and use that ID's password.
7. Click **OK**.
8. Monitor the window that appears with messages indicating the install process to ensure it is successful.
9. Reply **OK** to the summary window.

10. Right-click on the **Network property** and click **refresh**. You should see the added SP nodes listed under the 9076 host.
11. **Note:** If you use the RSH protocol option to add 9076 nodes and kerberos security is not implemented on your 9076 system, you must add the following lines to your client machine's `/.rhosts` files to enable the gateway machine access. If necessary, after the code is installed, the entries in the `/.rhosts` files may be removed. With kerberos, you only need a valid ticket for root.

`<Gateway hostname> root`

`<Gateway hostname> svcagent`

Where `<Gateway hostname>` is the name of the machine where the SA program is installed. For example: if the Gateway hostname was Kansas City1 the two entries in the managed machine's `/.rhosts` file would be:

Kansas City1 root

Kansas City1 svcagent

How to add a machine

1. Select **Network** property.
2. Click **Add**.
3. Click **Child sub-menu**.
4. Click **Machine entry** of the Child sub-menu.
5. Complete all the required fields for the selected machine.
6. Select **FTP, DSH, or RSH protocol option** from the Type of Installation table.
7. Click **OK** to save the data.
8. If you use the FTP protocol, the Enter the User ID and Password Window appears. Type the password for root. If you cannot use root and the root password, you can change the User ID field to a root-authorized user ID and use that ID's password

How to control dispatching for a machine supported by a different branch office

In the Navigation Pane, select the machine supported by a different IBM branch office. For example, your gateway machine might be in Minneapolis and this monitored machine might be in Cedar Falls (also remember you have global users, not just USA users).

1. Click **Add**.
2. Select **Form**.
3. Click **Telephone Number**.
4. Add the proper contact telephone number for the machine located in Cedar Falls.
5. Click **OK**.

The new telephone number will appear in the Telephone Number parameter of this machine's Node Info template. Make sure this phone number is located in the first tab position (you can have more than one phone number listed). Service Agent uses the telephone number in tab position one (1) to dispatch SSR support.

How to install Service Agent code only on a monitored machine

1. Expand the **Administration** property.
2. Click **(Un)Install**.
3. Select a host or a range of hosts on which want you to install code.
Note: Select first host, scroll the range, hold the shift key and select ending host.
4. Click **Install**.

If you use the FTP protocol, the Enter the User ID and Password Window appears. Type the password for root. If you cannot use root and the root password, you can change the User ID field to a root-authorized user ID and use that ID's password.

How to specify the physical location of a machine

Specifying the physical location of a machine helps service representatives provide prompt, quick service to monitored machines.

1. Click the **Network** property folder.
2. Click **Add**.
3. Click **Form**.
4. Click **Location**.
5. Type the correct data in the Location template.
6. Click **OK**.
7. Scroll the details pane to verify that the Location template was completed.

How to specify Cluster details

Cluster information is needed for proper routing of problems on RETAIN.

1. Expand the **Administration** property.
2. Click **Manage Cluster IDs**.
3. Select the machines for which you want to add Cluster IDs.
4. Click **Append Cluster ID to the Machines**.
5. A window appears for adding Cluster Type, Serial & Model.
6. Enter the details and click **OK**.

Note: If the selected system already has cluster information, a warning appears. You can keep the existing information or overwrite it with the new details.

Adding the cluster information is a manual process, and this has to be done for every individual system. In the case of an SP system, if the Cluster details are added to a CWS before the "Add 9076 Nodes" function is called, the function will automatically add the cluster details to every individual node. If the cluster details are defined after the SP Nodes are added, it has to be done for each individual node that is part of the cluster.

How to define resource filters

Resource filters allow you to specify certain devices so that they are not reported to IBM. This is particularly needed if a non-IBM device is not covered under warranty or a maintenance agreement (MA). You can define resource filters for your network or for specific monitored machines. This example uses a specific monitored machine.

1. Click on a specific monitored machine.
2. Click **Add**.
3. Click **Form**.
4. Click **Resource Filter**
5. Type the name of the resource to filter or a range of resources.
6. Click **OK**.
7. Verify your Resource Filters by locating the Resource Filter template in the details pane.

How to specify thresholds

Thresholds provide you with a way to prevent certain errors (for a network view or a monitored machine view) from being reported by Service Agent to “IBM” (customers don’t need to know the term “SDR”).

See Appendix B. Advanced UI Configuration/Property Details, “Thresholds Template” on page 89 to see how to determine errors (their ID or number) that you can then use in defining thresholds.

1. Select either the Network folder or a monitored machine.
2. Click **Add**.
3. Click **Form**.
4. Click **Threshold**.
5. Type the correct data into the Threshold template.
6. Click **OK**.
7. To verify your Threshold entry, scroll the details pane to the Filter Lists folder, click **Thresholds**, and scroll until you locate the error that you just added.

How to add an e-mail address for a monitored client

This function provides the ability to transmit an e-mail address to IBM for a monitored client. IBM will use the e-mail address supplied here to register machines to your account on the PM pSeries web site.

1. Select the Network folder.
2. Select the appropriate monitored machine.
3. Click **Add**.
4. Click **Form**.
5. Click **IBM Contact**.
6. Populate the name, phone number and E-mail fields.
7. Click **OK**.

This new contact information will be sent to IBM and associated with this machine in the IBM service database.

How to configure for Performance Management

You must have Performance Management for AIX product installed in order to perform configuration. If the *Performance Management for AIX Installed?* parameter value is No, you do not have the product installed.

1. Under the machine folder, click **Performance Management**.
2. From the Browse pane, fill in the parameter values for the Performance Management template.

See Appendix B. Advanced UI Configuration/Property Details, “Performance Management Template” on page 102 for complete descriptions of the template parameters.

How to send Performance Management Data

If you want to manually send the Performance Management data to IBM, Service Agent provides this function. PM/AIX must be installed on the monitored system. This function will send all available Performance Management data for this monitored client.

1. Click **Manual Tools**
2. Click **Performance Management**.
3. Select the machines for which you want to send Performance Management data. The machine list appears in the Browse pane.
4. Click **Send Performance Management to IBM**.
5. Respond Yes or No to the Connect pop box.

To confirm whether the Performance Management data was sent to IBM, access the CallLog and review the entries in the CallLog.

How to add an SNMP Notification

1. Select the network folder.
2. Select the appropriate monitored machine.
3. Click **Add**.
4. Click **Form**.
5. Click **SNMPTrap**.
6. Modify the **Target Network Manager Host**, **SNMP Port Number** and **Community** as appropriate for your environment.
7. Set the remaining Send Trap fields to **TRUE** for each notification type you want to receive at the SNMP target host.
8. Click **OK**.

How to lock out Service Agent on a machine

The Lockout Machines template allows turning off or locking out Service Agent on an individual machine or machines.

CAUTION: The locked out system will not report any errors until the lock is removed. Be sure to unlock the system after all maintenance work is performed.

6. Under the Administration folder, click **Lockout Machines**.
7. From the detail pane, select the monitored machine or machines on which you want to lock out Service Agent.
8. Click **lock**.
9. To verify the lockout, click the **Network** folder, then click the **Padlock** icon to display status. The machine's status should show a red X, indicating it is locked.
10. Repeat steps 1 and 2, and then click **unlock**.

How to add an e-mail Alert

1. Select a monitored machine for which you want to create an E-mail Alert folder. (E-mail Alert is common for all the SA clients on the same gateway, and is not dependent on where we add the E-mail alert mechanism)
2. Click **Add**, Click **Child sub-menu**, Click **E-mail alert**.
3. Change the default e-mail address to one or more addresses you want this e-mail sent to. Separate multiple e-mail addresses with a comma. For example, joe@host.companyname.com, carol@abcit.com, jill@companyname.com .
4. If the selected host has a different Mail Server, type the name of that server as the value for E-mail Server. (The default name may be used if appropriate.)
5. Change the *E-mail Wait Time in Minutes* field to a number lower than 15 if you want to check the function or receive notification sooner than 15 minutes. You may not use a value of 0.
6. Set to True the types of alerts for which you want to be notified. (See Appendix B. Advanced UI Configuration/Property Details, "E-mail Alert Template" on page 105 for more information and a description of the alert types.)
7. Click **OK**.

Note: Different e-mail alerts can be customized for particular users. For example, you may want employee A to be notified of CAUTIONS and employee B to be notified of INTERNAL ERRORS. Only one E-mail Alert is normally needed for any events that might happen on any of the systems using this gateway. Adding E-mail Alerts to individual nodes does not provide details specific to that node.

How to remove or delete configuration entries

How to remove a machine

1. Select **Network** property.
2. Select the **machine** to remove.
3. Click **Delete**.
4. Click **Yes** to complete the removal.

Note: This uninstalls the code on the machine and removes the machine from the Service Agent configuration.

How to remove an SNMP Notification

1. Select the **Network** folder.
2. Select the **machine**.
3. Select the **SNMP Notification** you want to remove.
4. Click **Delete**.
5. Click **Yes** to complete the removal.

How to remove all nodes from a 9076 (SP)

1. Expand the **Administration** property.
2. Click **Add 9076 (SP) Nodes**.
3. Select the 9076 host you want to remove nodes from.
4. Select **Using FTP**. Deselect (make false) the choices you do not want to use.
5. Click **removeNodes**.
6. Right-click on the Network property to refresh. You should see that the SP nodes have been removed.

How to remove Service Agent code only from a monitored machine

1. Expand the **Administration** property.
2. Click **(Un)Install**.
3. Select a host or a range of hosts from which you want to remove Service Agent code.
Note: Select first host, scroll the range, hold the shift key and select ending host.
4. Click **Uninstall**

If you use the FTP protocol, the Enter the User ID and Password window appears. Type the password for root. If you cannot use root and the root password, you can change the User ID field to a root-authorized user ID and use that ID's password.

How to remove Cluster details

1. Expand the **Administration** property.
2. Click **Manage Cluster IDs**.
3. Select the machines to remove Cluster ID.
4. Click **Remove Cluster ID from Machines**.
5. A confirmation is requested and if the user selects “YES,” the cluster information from the selected machines will be removed.

Note: Cluster information is needed for proper routing of the problem on IBM RETAIN. If the cluster details are invalid, the normal details (System type, serial, and model) will be used.

How to test Configuration entries

How to send a test PMR to IBM

1. In the Test Tools folder, click **TestPMR**.
2. Select a machine and click **Generate** to create and send a test PMR to the IBM.
3. Reply Yes to the prompt of whether to connect to IBM now or later.
4. Click the **Callog** property to monitor the TestPMR progress for success or failure.
5. Look for the Red Bug icon beneath the monitored machine property. It should be prefaced by the error string 000-000.

How to send a test e-mail

You need to have an e-mail alert defined prior to sending a test e-mail. See “How to add an e-mail alert” on page 74. The e-mail test alert instructs the recipient to contact the system administrator.

1. Select a monitored machine for which you want to create a Test E-mails folder. You must expand the view of the monitored machine by clicking the key next to the machine name.
2. Click **E-mail alert** icon.
3. Scroll to Test E-mails Enabled field.
4. Click the **Test E-mails Enabled** check box to toggle the value to **True**.
5. Click **OK**.
Repeat steps 1 through 5 to send the test E-mails to other E-mail addresses.
6. Expand the **Test Tools** property.
7. Click the **Test E-mail** icon.
8. Click **Send**. **Note:** E-mail is sent after the time-delay (set when creating the e-mail alert) expires.
9. Scroll (while in the E-mail folder) to Test E-mails Enabled and click the **Test E-mails Enabled** check box to toggle the value to **False**.
10. Check with the persons who are designated to receive the E-mail Alerts to see if they did receive the alerts.

How to send a test SNMP Notification

1. Select the Test Tools.
2. Click **Test SNMPTrap**.
3. Click **Generate**.

How to perform other Service Agent functions

How to determine your Service Agent version

1. From the Service Agent interface, click **Help**.
2. Click **About**. This displays the Service Agent version number.

Note: This displays the level of code installed on the gateway server. Selecting the Environment item under the expanded node shows the Service Agent code level for that machine.

How to manually transmit Vital Product Data (VPD) to IBM

1. From the Manual Tools folder, click **Send Manual VPD**
2. Select a monitored machine for which you want to transmit Manual VPD.
3. Click **send Manual VPD** to send VPD to IBM at the next regularly scheduled time, or click **send Manual VPD Immediately to IBM** to transmit VPD as soon as the option is clicked.

How to clean up (remove some data from) monitored logs

You may want to clean up monitored logs because they are getting too large or you only want to keep certain data.

1. Expand the **Administration key**.
2. Select **Purge Data**.
3. Toggle to **True** the data you want to purge:
 - **CallLog data:**
All entries posted to the CallLog. For example, when a call is made to IBM, a record is created in the CallLog; this would be removed. This function removes ALL data in the CallLog.
 - **Purge Error Warning:**
Any warning messages, non-error messages (yellow triangles) are purged.
 - **Purge Internal Errors:**
Any errors with the upside-down Red Bug icon posted are purged.
 - **Closed PMRs:**
Purges any PMR marked as closed.
 - **All The PMRs:**
Purges all PMRs.
4. Click **Purge** to purge all data marked as True.

Note: A large quantity of data to purge will take some time to complete. You will not see any panel updates while this activity takes place.

How to clear pending requests to IBM

Normal workings of Service Agent can create requests to IBM. These requests can be queued for immediate or later processing. To clear any current or pending requests follow the steps below:

1. Click the **Administration** property folder.
2. Click **Purge**.
3. Toggle **The OutGoing Queue** to **True**.
4. Click **Purge**.

Note: You will not see any panel updates while this activity takes place.

Chapter 11. Service Agent Security

This chapter discusses how security for Service Agent works with the following areas:

- IBM using HTTPS
- SA Connection Manager
- Global Dialer and Network
- Modem security

Access to the latest Service Agent security information resides at this URL:

www.ibm.com/support/electronic

- Select a **Country**
- Select **Electronic Service Agent**™
- Under **Resources** expand General information
- Select the latest transmission security document for Internet and AT&T modem connection.

Traversing Secure Boundaries

An Inter-Enterprise Service (IES) activity is the IT process of providing access to proprietary IT Resources. To provide that access, the secure boundary of IT infrastructure must be traversed. Each communication path brings its own security requirements.

The SA application was designed to be IES compliant. It utilizes an HTTPS connection to IBM to ensure your data is transmitted securely.

The SA gateway will need to provide to IBM all the information it knows about a given system during enrollment. This information can be pulled from the Node Info associated with the machine in question. This applies to both communication methods available from SA, namely the Internet or the Dialer connection methods.

Security and the Serial Interface

The TTY port and modem security are both configured to NOT auto-answer the modem or allow login access from the TTY port. Service Agent only allows outbound calls to be created from the customer's location.

Chapter 12. Contacting Customer Support

Entitlement to Automatic Problem Submission

You are entitled to automatic problem submission from IBM only if your systems are under warranty and/or your organization has a maintenance agreement with IBM Service. This service program is not intended for customers who have a third party maintaining the pSeries servers. IBM's standard warranty response time is the next business day unless you have purchased an upgrade to the service level agreement.

Contacting Support

If you encounter problems or have technical questions regarding Service Agent, you should call your nearest IBM support center. You can obtain support center contact details that are appropriate for your country/region from the following web site:

www.ibm.com/planetwide/

Web Sites

IBM pSeries Support and Information

<http://www.ibm.com/servers/eserver/support/pseries>

IBM Support Center contact information

<http://www.ibm.com/planetwide/>

Electronic Service Agent installation package

<http://www.ibm.com/support/electronic>

Appendix A - Basic UI Configuration Details

Network Properties

The Network Properties function lets you update the contact information for callback from the local IBM Support Center. The Name, Phone Number, E-mail address of the contact, and Country where the gateway server is located are required fields. After you finish the data entry, click **OK** to save the data.

Network Properties:

Property	Description
IBM Contact	
Name	IBM may contact for PMR discussions. (Required)
Phone Number	Phone number of contact. (Required)
E-mail	Internet e-mail address of contact. (Required)
eService Information	
IBM Common Registration UserID	Your IBM Registration ID is your single point of access to IBM web applications that use IBM Registration. You need just one IBM ID and one password to access any IBM Registration based application. http://www.ibm.com/account
Address	
Queue Country	Physical Country Location of the systems where PMRs will be opened. This is generally the same country the contact person resides in. If different, the country where the Service Agent network is located should be used. (Required)
Organization	Name of company. (Optional)
Organizational Unit	Name of group or division (Optional)
Street	Street location where Service Agent Network is installed. (Opt)
Locality	City, Town, or Village where SA Network is installed. (Opt)
State Or Province	State/Province where Service Agent Network is installed. (Opt)
Postal Code	Zip or postal code where Service Agent Network is installed. (Opt)
Customer Number	
Customer Number	IBM customer number. (Optional)
Standard Template Settings Parameter	
Err Lease - Days, Hours, Minutes, Seconds	This timer determines how long to keep and maintain host-detected error entries generated by Service Agent.
Telephone Number	
Number	Additional Telephone Number (Optional) Will become primary contact phone number if different from initial phone number.
Contact Context	
Comment	Any comments that may help in communication between the company and IBM concerning support for the SA monitored hosts.

Note: The country value selected is utilized to properly identify the systems and open Problem Management Reports (PMRs) based on country codes. The country selected must match that identified with the IBM customer number. If the country is incorrect, the PMR will be rejected or sent to an incorrect queue.

Note: Use the additional telephone number for the IBM Support center contact point if the phone number is different from the initial contact phone number. If the first phone number is for the central complex contact, but you want the IBM Support center to contact a different telephone number, enter the second number under the additional telephone number parameter.

Gateway Properties

Gateways are named for their host servers. For example, if Service Agent were installed on a machine called ABC, the second property button down from top would be labeled "ABC." The required fields for the Node Info parameter are the hostname, Processor ID, Type, Serial number, and Model of the local machine. The hostname and Processor ID are not modifiable and are retrieved automatically along with the gateway server's IP address. The Type, Serial number, and Model are required input and must be accurate. If an error is made in one of the locked fields after clicking OK, Service Agent must be removed and reinstalled to correct the mistake. The auto discovery or "Get System Info" property should aid in getting this data correctly, but it still must be validated for accuracy.

Do not confuse the 3-digit model number with the new pSeries Server nomenclature that contains 4 characters like p650. Model number may be corrected if initially entered incorrectly.

After you have entered the data, click **OK** to save the data.

Property	Description
Name	Locked for Hostname of gateway system. This field entry may be updated when an additional host is added.
Get System Info	Auto discovery pushbutton - gets Type/Model/Serial for named machine.
IP address	If entered must be in proper IP number format #####.#####.#####.#####
Processor ID	Locked, uname -m number of local host.
Type	Required input- 4 digit brass tag number located on exterior of unit.
Serial number	Required - Brass tag serial number located on exterior of unit. Do NOT include dash or spaces that may be shown in serial number, Capitalize alphabetic characters. In United States, only the last 5 digits are used for IBM reporting, so 00 may be added in place of plant code, for example, 00123AB
Model	Required - Model number of unit, 3 characters like H80, not P670
Manufacturer	Optional - Manufacturer name of unit.
Type of Installation	Not applicable on a gateway server.
Primary Server Secondary Server Tertiary Server	These fields are locked on the gateway host and cannot be modified.

Call Controller Properties

Properties for the Call Controller:

Property	Description
Primary URL to Connection Manager	This entry is the hostname or IP address and Port number of the SACM primary server. This value was defined by the SMIT Manage SACM configuration options. If hostname:socket was configured at that time the default localhost:1198, value should be corrected to correct hostname:socket.
Secondary URL to Connection Manager	The URL of the secondary SACM for your environment. Empty by default.
Pending Timer In Minutes	When an event or problem is detected, its status is set to Pending. The value specified for the Pending Timer determines how many minutes to wait for additional events to be generated before taking action and attempting to make an external connection to the IBM SDR. For example, if an error is detected at 1:00 PM, SA will wait until 1:15 PM before taking action.
Check Open Status In Days	When an error event is set to an OPEN status, the value specified in this field determines how many days to wait before checking the status of the PMR .
Health Check Timer In Days	The value specified in this field determines how often (in days) SA should call into the IBM SDR for a Health Check. The Health Check indicates that everything is OK including the communication. The countdown for this timer is reset whenever a good connection is made to the SDR
Max Retry Attempts	This value determines how many times Service Agent will attempt to make a connection to the IBM SDR before giving up and setting the FAIL status of the event.
Retry Attempts Counter	This value indicates the current connection attempt the CallController is on with the CM. When this count equals the Max Attempts count, then the status is set to FAIL.
Retry Timer In Minutes	This value determines how many minutes to wait before making the next connection attempt. If the Max Attempts is set to 3 and the Retry Timer is set to 5, then the CallController sleeps between each attempt for 300 seconds until the Max Attempts value is reached.
Connection Idle Timeout in Minutes	This value determines how long a connection can be idle (no activity) before a time-out condition is posted back to the CallController, breaking the connection to the Connection Manager. The default timeout is 5 hours
Use HTTP Proxy between SA Server and SACM	When set to true, the Call Controller uses an HTTP Proxy to access the SACM. Default = false. Note: SOCKS is not supported.
HTTP Proxy IP Address	The IP Address of the Proxy to connect to the SA Connection Manager. Leave Blank if Proxy is not used
HTTP Proxy Port	The IP Address of the Proxy port number to access the SA Connection Manager. Default = 80
HTTP Proxy Username	The username for the HTTP proxy in Strict mode. Leave Blank if Proxy is not used
HTTP Proxy Password	The password for HTTP proxy in Strict mode. Leave Blank if no Proxy is used
Download ConnectManager Configuration Timer in Hours	This the interval at a Master gateway will request the Connection Manager configuration in hours The gateway provides the configuration for presentation in the UI's. Default = 24 hours

Available buttons for the Call Controller:

Button	Description
OK	This button, located at the bottom of the detail pane, is active once data has been entered or changed in a field. Click this button to save all data.
Cancel	Click Cancel to cancel the current operation. Screen is refreshed to original data.
Delete	This button, located at the bottom of the detail pane, becomes active when an entry in the detail pane is selected. Click this button to delete a selected entry.

Connection Manager Properties

Connection Manager Properties:

Property	Description
Use modem as connection method to IBM	This check mark when set to true indicates that the dialer will be used to contact the IBM Service Data Receiver. When set to false, SACM will expect to use an existing Internet connection. Default = false
Password for updating Connection Manager configuration	Default = password
Proxy IP Address	Populate with IP address of proxy server (leave empty if no proxy)
Proxy Port	default port = 80
Proxy Username	(leave empty if no user name)
Proxy Password	(leave empty if no password)
Use Socks Proxy	Set to true means you must use proxy to access. Default = false

Available buttons for Connection Manager template:

Button	Description
OK	This button, located at the bottom of the detail pane, is active once data has been entered or changed in a field. Click this button to save all data.
Cancel	Click Cancel to cancel the current operation. Screen is refreshed to original data.
Delete	This button, located at the bottom of the detail pane, becomes active when an entry in the detail pane is selected. Click this button to delete a selected entry.

You are then prompted to configure the Dialer properties. Click **Yes** to begin configuring the Dialer. Selecting **No** allows you to configure the Dialer at a later time.

Dialer Properties

Dialer properties allow you to define modem parameters and account values for communication to IBM. In this entry, required fields are marked by the “!” character as in other panels within Service Agent. However, there is no verification of required fields for the modem parameters since a modem is not required for local setup of the rest of the Service Agent system.

See “Setting up your IBM Modem for Service Agent” on page 25 for modem initialization and setup if you need additional information.

After you enter the data, click **OK** to save it. The system then prompts you to access registration properties. If you click the Yes button, you are taken to the *Enroll* panel by clicking the **Machines** button. If you click the No button, you are taken to the Machines button. Following are the Dialer parameters and field descriptions:

Dialer Properties:

Property	Description
Location	The country/city the modem is dialing. This value can be modified by opening this table and selecting the country, then Detail. Finally, select the town phone number closest to your location. Additional fields will be filled automatically.
! Primary Phone Number	The telephone number the modem is dialing. This number is populated according to the location selected. Change only if needed. Note: Depending upon the local phone exchange, this number may need to be modified to utilize your outgoing number and area code requirements.
Secondary Location	The second or backup country/city the modem is dialing.
Secondary Phone Number	The telephone number the modem uses to call in the event the primary phone number fails.
! Account	The Service Agent network login account assigned by IBM. May vary with location. Auto-filled; do not change.
! User ID	The Service Agent network login user ID. May vary with location. Auto-filled; do not change.
! Password	The Service Agent network login password. May vary with location. Auto-filled; do not change.
! TTY #	The available port number to which the modem is physically connected.
Modem	The modem’s reset and initialization string values. These are populated according to the modem selected. Change these values only if needed. Tip: Type the first letter of the name to move quickly through the list.
Init String	The modem’s reset string values, populated according to the modem selected. Change these values only if needed.
Baud Rate	The maximum value the TTY modem will be set at for connection. See * below.
! Dial Type	Select the dial type of this modem (i.e., tone or pulse).
Verify Baud Rate Before Dialing	Flag to verify baud rate selected works with the modem. If the baud rate fails, the program attempts to select the next best baud rate that works. Default is True. If the flag is set to False, no checking is done prior to running.
Max Retry Attempts	Maximum number of times the dialer will attempt to get a good connection to AT&T gateway. The default is 3.
Retry Timer In Seconds	The time (in seconds) the dialer will wait before attempting to retry. The default is 60.

* Baud rate

0	1,200	2	4,800	4	9,600	6	28,800	8	38,400
1	2,400	3	9,600	5	19,200	7	33,600	9	56,000

Enroll Properties

The Enroll Properties function displays a list of all machines that have been recognized by the gateway. At the bottom of this list are the Open and Enroll buttons. Prior to clicking a button, you must select one of the machines in the list by highlighting it. To highlight an entry, put the mouse pointer on the entry and click the left mouse button. To select multiple entries, hold down the **Ctrl** key while making selections. After all selections have been highlighted, click either **Open** or **Enroll**. Clicking the Open button displays the node information for the selected machine. Clicking the Enroll button allows you to enroll your machine with IBM.

Enroll Properties:

Property	Descriptions	
Open	This button displays the node info for the highlighted host. See Gateway Properties on page 82 for field details. Open will only display the first entry of a highlighted list.	
Enroll	After selecting one or more machines to register and clicking Enroll , a (Yes, No) prompt is displayed. This prompt allows the option to either attempt to connect to the IBM SDR immediately or to wait until the timer for the Pending process is triggered.	
Enroll Prompt Selections		
	No	If No is selected, the connection is attempted within the time frame specified for the Pending timer. The display is returned to the Enrollment panel.
	Yes	If Yes is selected, the connection is attempted immediately. The user is taken to the CallLog Properties display where real time status of the connection being made is displayed. See CallLog Properties on page 87 for details.

Connect Properties

The Connect Properties function provides for immediate connection to the IBM without waiting for any outstanding timer processes or the cancellation of the currently active connection. Upon connection, all entries in the queue for transmission to IBM are sent.

Connect Properties:

Property	Description
Connect	Clicking Connect causes the program to attempt connection immediately. The user is referred to the CallLog properties panel where the real time status of the connection being made is displayed. See CallLog Properties on page 87 for details.
Disconnect	Clicking Disconnect causes the program to cancel the current connection process and clear out all queues. All queued entries are set to a Failed status if appropriate. The CallLog property shows Canceled in the transmission description.

Call Log Properties

The CallLog Properties function displays a table of all calls made (or attempted) to IBM.

CallLog Properties:

Property	Description
Start Time Stamp	Time Stamp for the beginning of the transmission.
Description	Displays real time connection updates as the connection is made. Once the connection has ended, the final Success/Fail results are logged here.
Try	Displays how many times or retries it took to make the connection
TTY Baud	If a baud rate is established, shows the posted connect speed or <none>
Snd	This column is not used.
Rcy	This column is not used.
Status	Icon status of transmission, Green Flag = OK
Type	Type of call, LIC (padlock), PMR (bug), VPD (Heart) Icon symbols
End Time Stamp	Time Stamp for the end of the transmission

Error Log Properties

The ErrorLog Properties function displays a summary list of all exceptions Service Agent detected while running. Both internal program exceptions and external access failures for host creation or program events are displayed.

ErrorLog Properties:

Property	Description
Host	Host on which the error occurred
Timestamp	Time the error occurred
Error#	Error number
Description	Description or results of the error
Resource	Name of the resource on which the error occurred
Class	Name of error class

Associated with each entry in the table is a detail log containing additional information specific to the entry. This information is displayed on the bottom section of the panel by highlighting an entry in the table.

The log entry detail information contains the following:

Internal Error Properties:

Property	Description
Timestamp	Time the error occurred
Details	Additional details pertaining to error
Description	Description or results of the error
Error Class	
ID	Error ID
Resource	Name of the resource on which the error occurred

Appendix B – Advanced UI Configuration/Property Details

Category Selectors

There are four category selectors available to determine the type of information displayed in the detail window when a properties button is selected. These are:

- View / Edit Properties
- View Error Events
- View Licensing Info
- View Internal Errors

Note: The right hand detail panel may be blank if the selected category does not have information available.

This information is presented in the Advanced Configuration sequence in the user interface under the View / Edit Properties selection. The three remaining View templates are summary data of the information shown under the Properties templates.

- Network
- Gateway server
- Monitored machines
- Administration
- Filtering
- Manual tools
- Test tools

Starting with the folder level, show any detail templates that could exist under that folder. If a template is the same as a previously described template, the detail template may not be shown. For example, the "Node Info template" for a monitored client is the same and only the first instance is shown. If you do not find a template where you might expect it to be, then you may have to look for a higher template within the Network tree structure.

Network folder

The Network folder allows you to update the contact information for callback from the IBM Support Center for problems that are received. The *Name*, *Phone Number*, and *E-mail* address of the contact are required. In addition, the *Queue Country* where the gateway server is located is also required. After the data has been typed, click **OK** to save the data.

Note: The country value selected is utilized to properly identify the systems and open Problem Management Reports (PMRs) based upon internal country codes. The country selected must match that identified with the IBM customer number. If the Country code is incorrect, the PMR is either rejected or sent to an improper queue.

Network Properties:

Property	Description
IBM Contact	
Name	Customer employee that IBM can contact for PMR discussions. (Required)
Phone Number	Phone number of contact. (Required)
E-mail	Internet e-mail address of contact. (Required)
eService Information	
IBM Common Registration UserID	Your IBM Registration ID is your single point of access to IBM web applications that use IBM Registration. One IBM ID and one password (per person) to access any IBM Registration based application. http://www.ibm.com/account
Address	
Queue Country	Physical Country Location of the systems where PMRs will be opened . This is generally be the same country in which the contact resides. However, if different, the country where the Service Agent network is located should be used. (Required)
Organization	Name of company. (Optional)
Organizational Unit	Name of group or division (Optional)
Street	Street location where Service Agent Network is installed. (Optional)
Locality	City, Town, or Village where SA Network is installed. (Optional)
State Or Province	State/Province where Service Agent Network is installed. (Optional)
Postal Code	Zip or postal code where Service Agent Network is installed. (Optional)
Customer Number	
Customer Number	IBM customer number. (Optional)
Standard Template Settings Parameter	
Err Lease - Days, Hours, Minutes, Seconds	Default Template settings used across all monitored systems. Due to processing and system differences in a network, all times indicated are approximate execution times. This timer determines how long to keep and maintain host-detected error entries generated by Service Agent.
Telephone Number	
Number	Additional Telephone Number (Optional) Will become the primary contact phone number if different from the initial phone number.
Contact Context	
Comment	Any comments that may help in communication between the company and IBM concerning support for the SA monitored hosts.

Using the Add button from the Network folder

When the Network folder is selected, you can add additional information about your Network to the Service Agent program using the *Add* button. Departments, Machines, or Sub-Nodes can be added under the *Child* selection. Additional information can be added to the base Network Template with the *Forms* options. Additional comments, locations, telephone numbers, and other items will add tabs to the base template.

View pane control buttons:

Button	Description
Add	Will allow secondary selection of Child or Forms pull downs.
Delete	Will delete any selected template when selection is valid.

Adding additional system information using forms

Additional information may be added to a machine's node information by selecting the Add button and then the Form button at the bottom of the navigation pane and making a selection.

The following selections may take effect across the whole network hierarchy, department or on individual machine bases, depending upon the Property selection made. Forms added to a Machine take priority over a Department grouping and Forms added to a Department take priority over the Network.

Department Template

The Department template will allow you to group added machines under different names. This grouping allows for better or easier viewing of machines from a user interface. It will also allow additional information to be applied to a group of machines instead of at machine or network levels.

When client machines are added from the client local install referencing a department name, then the machine should be added under the selected Department.

Department Properties:

Property	Description
Name	Will allow a name to be added to the Department Group. If no name is added the department group will show as <new> under Network.
Button	
OK	The OK button is active once data has been typed or changed in a field. Click this button to save all data into database.
Cancel	Click Cancel to cancel the current operation.

Node Info Template

The Node Info template allows you to define specific information about new machines that you want to add to your network of monitored machines.

Node Info Properties:

Property	Description
Name	Locked for Hostname of gateway system. This field entry may be updated when an additional host is added.
Get System Info	Auto discovery pushbutton - gets Type/Model/Serial for named machine.
IP address	If entered, must be in proper IP number format (auto filled)
Processor ID	CPU type of local host. (auto filled)
Type	Required input- 4 digit brass tag number located on exterior of unit.
Serial number	Required - Brass tag serial number located on exterior of unit. Do NOT include dashes or spaces that may be shown in the serial number. Alphabetic characters should be capitalized.
Model	Required - Model number of unit; 3 characters like H80 not P670
Manufacturer	Optional Manufacturer name of unit.
Type of Installation	Determines the type of protocol used to distribute the client portion of the Service Agent program to selected monitored machines. FTP FTP prompts for a root authority ID and password. It will use the supplied password for transferring files using Java FTP protocol and running installation processes using the rexec program.
Primary Server (Locked)	Used for internal functions within Service Agent for gateway and sub-host communication. Indicates the primary host to which sub-hosts report. This field is locked on the Gateway host and should not be modified.
Secondary Server	Indicates the secondary host sub-hosts report to in case of <u>primary</u> failure. Initially same as Primary, but may be manually updated to point to secondary SA gateway server if configured.
Tertiary Server	Indicates the third host to which sub-hosts report in case of <u>secondary</u> failure. Initially the same as the Primary, but may be manually updated to point to third SA gateway server if configured.

Available Forms

Address

Select this form to add additional address information to the Network, Department, or Machine.

Comment

Select this form to add additional comment information to the Network, Department, or Machine.

Contact

Select this form to add additional comment information to the Network, Department, or Machine.

Location

Select this form to add additional location information to the Network, Department, or Machine as to the physical location of the system. Specific entries available are Building, Floor, and Room locations.

Resource Filter

You can define resources for which you do not want to report errors. For example, a hard disk that is not under an IBM warranty or maintenance agreement. Generally, resource filters are defined at the machine level but they can also be set at the network and department level. Enter the logical resource name of the device to be ignored. Add one resource form per device or range of devices. For example, (“hdisk0, hdisk1, tok0, tok1”).

Note: Services performed by IBM personnel on systems and products not on IBM warranty or maintenance agreement may be subject to time and material charges.

Threshold

Select the *Threshold* form to add additional error thresholds to the Network, Department, or Machine. Error events detected by Service Agent use internal threshold levels, defined by IBM, which must be exceeded before an action is taken (Ignore, Create Pending, or Create Held). In some cases, false error events may be detected due to system configuration or unusual process activities that give false returns. If this happens, thresholds can be added for the specific error Thresholds Property Selection.

Available Threshold Properties:

Property	Description	
Error ID	The Error ID can be a SRN number generated by the Diagnostics, a system error log error identifier, or a system error log error label. The Error ID or SRN number will be displayed in the “Error Number” field of the “Error Event” if available. Note: A threshold Error ID or SRN must be an exact match. If the Error ID detected by Service Agent contains upper or lower case characters, the same characters must be entered for the thresholds. All characters displayed in the Error ID of a PMR entry must be typed as the Threshold error. This would include any hex notation such as <i>0x</i> if present.	
Action	Action to be taken when this error occurs:	
0	Create Pending	Create error event to be transmitted to IBM
1	Create Held	Create an error event with Held status so it does not send to IBM. You would then have to manually update the status to Pending to send it or delete it if you were not interested in it.
2	Ignore	Ignore this error; do not report it.
Count	The number of occurrences of the error before the action is taken.	
Days/Hours/Minutes	The frequency of the count; for example, you might only want to act on the error after it happens 3 times in 1 day, or 2 times in 45 minutes.	

Settings

Select the *Settings* form to add additional Standard Template Settings entries to the Network, Department, or Machine.

Telephone Number

Select the *Telephone Number* form to add additional phone number information to the Network, Department, or Machine.

This additional information can be viewed, through the Network folder's detail list.

Following is a description of the *OK*, *Cancel*, and *Delete* buttons available when in the Network folder view detail or summary views are in the right pane.

Detail view pane control buttons:

Button	Description
OK	The OK button is active once data has been typed or changed in a field. Click this button to save all data into database.
Cancel	Click Cancel to cancel the current operation.
Delete	Will delete any selected additional added section to base template.

Gateway Folder

Gateway Node Info

The Node Info template for the gateway server allows you to define specific information needed to complete the definition of the gateway node. The Name, IP, and Processor ID are all automatically filled in with the correct information gathered during the initial configuration process. Although the "Type of Install" field exists, it does not apply to the Gateway host at the current time because of base install. Since this is the Primary Server, the hostname is auto filled and locked to all three server options; this gateway can not currently address a backup server.

The assumption is that is that the Machine Type, Machine Serial Number, and Machine Model is correct for this Gateway host. If any of these fields are incorrect, the only valid way to correct is to uninstall SA and then install it again and correct gateway data.

Gateway Node Info Properties

Property	Description
Name	Locked for Hostname of gateway system.
Get System Info	Auto discovery pushbutton - gets Type/Model/Serial for the machine.
IP address	If the IP address
Processor ID	Locked, CPU Type of local host.

Type	Required input- 4 digit brass tag number located on exterior of unit.
Serial Number.	Required input - brass tag serial number located on exterior of unit.
Model	Model number of unit (required). 3 chars after the "Type - xxx"
Manufacturer	Optional Manufacturer number of unit.
Type of Installation	Not applicable on gateway
Primary Server Secondary Server Tertiary Server (Locked)	Indicates primary host report to. This field is locked on the Gateway host and should not be modified. Currently gateway cannot utilize additional SA gateway servers.

Call Controller Template

The Call Controller template contains the entries and timers used to coordinate the call notification and external communication attempts among the monitored machines when an event or error is detected.

CallController Properties:

Property	Description
URL to Primary Connection Manager	The URL of the primary SACM for your environment. Defaults to https://<gateway.hostname>:1198
URL to Secondary Connection Manager	The URL of the secondary SACM for your environment. Empty by default.
Pending Timer In Minutes	When an event or problem is detected, its status is set Pending. The value specified for the Pending Timer determines how many minutes to wait for additional events to be generated before taking action and attempting to make an external connection to the IBM SDR. For example, if an error is detected at 1 PM, SA will wait until 1:15 PM before taking action.
Check Open Status In Days	When an error event is set to an OPEN status, the value specified in this field determines how many days to wait before checking the status of the PMR on the IBM Problem Management side.
Health Check Timer In Days	The value specified in this field determines how often (in days) SA should call into IBM for a health check. It indicates that everything is OK including the communication. The countdown for this timer is reset whenever a good connection is made to IBM
Max Retry Attempts	This value determines how many times Service Agent attempts to make a connection to IBM before giving up and setting the FAIL status of the events.
Retry Attempts Counter	This value indicates the current connection attempt the CallController is on with the Connection Manager. When this count equals the Max Attempts count then FAIL status is set.
Retry Timer In Minutes	This value determines how many minutes to wait before making the next connection attempt. If the Max Attempts is set to 3 and the Retry Timer is set to 5, then the CallController sleeps between each attempt for 300 seconds until the Max Attempts value is reached.
Connection Idle Timeout in	This value determines how long a connection can be idle (no activity) before a time-out condition is posted back to the CallController and breaking the connection to the

Minutes	Connection Manager. Default 5 hours
Use HTTP Proxy between SA Server and SACM	When set to true, the Call Controller will utilize a HTTP Proxy to access the SACM. The default value is false. NOTE: SOCKS is not supported.
HTTP Proxy IP Address	IP Address of the Proxy to connect to the Connection Manager. Leave Blank if Proxy is NOT used
HTTP Proxy Port	IP Address of the Proxy port number to access SA Connection Manager. Default = 80
HTTP Proxy Username	Username for HTTP proxy in Strict mode. Leave Blank if Proxy is NOT used
HTTP Proxy Password	Password for HTTP proxy in Strict mode. Leave Blank if No Proxy used
Download ConnectManager Configuration Timer in Hours	This the interval at a master gateway will request the Connection Manager configuration in hours The gateway provides the configuration for presentation in the UI's. Default = 24 hours

Available buttons for CallController template:

Button	Description
OK	This button located at the bottom of the detail pane is active once data has been entered or changed in a field. Click this button to save all data.
Cancel	Click Cancel to cancel the current operation.
Delete	This button, located at the bottom of the detail pane, becomes active when an entry in the detail pane is selected. Click the Delete button to delete a selected entry.

Connection Manager Template

Connection Manager Properties:

Property	Description
Use modem as connection method to IBM	This check mark when set to true will use the dialer to contact the IBM Service Data Receiver. When set to false, SACM will expect to use an existing Internet connection. Default = false
Password for updating Connection Manager configuration	Default = password
Proxy IP Address	Populate with IP address of proxy server (leave empty if no proxy)
Proxy Port	default port = 80
Proxy Username	(leave empty if no user name)
Proxy Password	(leave empty if no password)
Use Socks Proxy	Set to true means you must use proxy to access; the default is false

The Connection Manager template contains the entries and timers used to coordinate the call attempts to IBM. There should be only one Connection Manager for an account complex; all other CMs that might be available should be deleted. There may be a backup or secondary Connection Manager if high availability is required.

Available buttons for Connection Manager Template:

Button	Description
OK	This button located at the bottom of the detail pane is active once data has been entered or changed in a field. Click this button to save all data.
Cancel	Click Cancel to cancel the current operation. The panel is refreshed to display its original data.
Delete	This button, located at the bottom of the detail pane, becomes active when an entry in the detail pane is selected. Click the Delete button to delete a selected entry.

Dialer Template

The dialer allows you to define the modem parameters and field values for communication to IBM. In this template, required fields are marked by the “!” character as in other panels within Service Agent. However, there is no verification of required fields for the modem parameters since a modem is not required for local setup of the rest of the Service Agent program. It is highly recommended to configure the modem from within the Basic interface at the time of installation.

Dialer Template Properties: Property	Description
Location	The country/city the modem is dialing This value can be modified by opening this table and selecting the country, then Detail. Finally, select the town phone number closest to your location. Additional fields will be filled automatically.
! Primary Phone Number	The phone number the modem dial is populated according to the location selected. Change this phone number only if needed. Note: Depending upon the local phone exchange, this number may need to be modified to utilize your outgoing number and area code requirements.
Secondary Location	The second or backup country/city the modem is dialing.
Secondary Phone Number	The phone number the modem uses to call in the event the primary phone number fails.
! Account	The Service Agent network login account assigned by IBM. May vary depending upon location. Auto-filled; do not change.
! User ID	The Service Agent network login user ID. May vary depending upon location. Auto-filled; do not change.
! Password	The Service Agent network login password. May vary depending upon location. Auto-filled; do not change.
! TTY #	The available port number to which the modem is physically connected.
Modem	The modem’s reset and initialization string values are populated according to the modem selected. Change these values only if needed.

	Tip: Type the first letter of the name to move quickly through the list.
Init String	The modem's reset string values are populated according to the modem selected. Change these values only if needed.
Baud Rate	The maximum value the TTY modem will be set at for connection. See * below.
! Dial Type	Select the dial type of this modem (i.e. tone or pulse).
Verify Baud Rate Before Dialing	Flag to verify baud rate selected works with the modem. If the baud rate fails, the program attempts to select the next best baud rate that works. Default is True. If the flag is set to False, no checking is done prior to running.
Max Retry Attempts	Maximum number of times the dialer will attempt to get a good connection to AT&T gateway. The default is 3.
Retry Timer In Seconds	The time (in seconds) the dialer will wait before attempting to retry. The default is 60.

*Baud rate

0	1,200	2	4,800	4	9,600	6	28,800	8	38,400
1	2,400	3	9,600	5	19,200	7	33,600	9	5,600

Environment Template

The Environment template displays the various environments and revision levels of the supporting system and execution files on the machine. The revision level information is gathered every time the ODS process is started on the machine. The Environment information is transmitted with each connection to IBM for error analysis and update notification. These entries are locked and cannot be modified. If this template is empty then the ODS has never established communication with this gateway server database. The following values are included in the template:

- Java Vendor
- Java Version
- Operating System
- OS Version
- OS Release
- System Architecture
- Language
- Service Agent Version
- ODS Version
- Performance Management Version
- Logical Partition
- Lockout
- Whether controlled by HMC

Data Folder

A common grouping area that holds:

- Software Data
- Performance Data
- VPD Data (Hardware Inventory)

Enrollment Folder

The Enrollment Folder holds IBM enrollment information for this host.

Hardware Service Template

The Hardware Service template contains values used to control hardware monitoring operations. If the system is not enrolled, hardware monitoring functions are not enabled.

Hardware Service Properties:

Property	Description
Status	<p>This entry displays the enrollment status of the hardware template. This entry could be one of five different status states:</p> <p>0 Proposed - This state is the initial default state of a newly defined machine indicates the system is only proposed and not enrolled. No action will be taken until the status is set to Pending.</p> <p>1 Pending - This state indicates the system is staged to be enrolled. Upon the next connection to IBM, an enrollment request will be made for this host.</p> <p>2 Expired - This state indicates the maximum enrollment date has passed and the enrollment is expired. Reregister the system to get a new enrollment status. Functions requiring enrollment are disabled. When a system is expired, Service Agent automatically connects and requests a new license.</p> <p>3 Corrupt - This state indicates the license status is corrupt or damaged. For example if the return from License request was a bad transmission, the status will be set to corrupt. Re-enroll the system to get a clean enrollment status. Functions requiring enrollment are disabled with this status.</p> <p>4 Enrolled - This state indicates the machine is enrolled. All functions requiring enrollment are activated.</p> <p>5 Denied - This state indicates enrollment of the system was denied for some reason and a license to activate this template was refused. All functions requiring enrollment are disabled. Refer to the template comment field or the specific calllog entry for details. You must remove and redefine the machine to remove the Denied status state.</p>
Expiry	This is the date when the enrollment expires.

License	This the unique license number associated with the machine. This license number will not work with any other defined host.
Comment	General status response comments from IBM.
Heart Beat - Days, Hours, Minutes, Seconds	This is the timer to determine how often the gateway should expect a heartbeat from the host. If the host misses, a heartbeat a notification is sent. Actual time is an approximate value of Heart Beat + Delay.
Heart Beat Delay in Minutes	Value added to the heartbeat to compensate for Network delays and differences in systems. Minimum value is 2 minutes.
VPD Enabled	Enables or disables Vital Product Data (VPD) gathering on machine. True value indicates Enabled. See results in Data folder.
VPD Interval- Days, Hours, Minutes, Seconds	This timer determines how often to check for Changes in the Vital Product Data on a host. This data is then transmitted to IBM SDR for diagnostic and error analysis.
Err Enable	Flag to determine if system Error Log entries should be monitored for supported errors by the Service Agent. The Hardware Template must be enabled for this to be active.
Diag Enable	Flag to determine if the concurrent diagnostic information should be monitored by the Service Agent. The Hardware Template must be licensed for this to be active.
Diag Interval - Days, Hours, Minutes, Seconds	This timer determines how often to check for errors or problems detected by the Concurrent Diagnostics.
Enable the Automatic transmission of EED	Flag to determine if the Extended Error Data should be automatically sent with PMR data. AIX must be EED capable.

Available Buttons for Hardware Service Template:

Button	Description
OK	This button located at the bottom of the detail pane is active once data has been entered or changed in a field. Click this button to save all data entered.
Cancel	Click this button to cancel the current operation.
Delete	This button is located at the bottom of the detail pane and becomes active when an entry that can be deleted in the detail pane is selected.

PMR Folder

When Service Agent detects a valid Error Event, it puts the event in a PMR folder beneath the host (as viewed using the Service Agent interface) on which it was detected. This PMR grouping will make the user interface a more flexible tree structure. It will consolidate all the different error events for the host under a single keyed item.

Error Event template

This template appears when viewing an expanded machine Error Event. Templates are indicated by an icon in the shape of a bug along with the SRN or error number of the event and its description. Selecting an individual error template displays its

contents in the detail pane to the right. The information defined in this template is used to open an IBM PMR and to maintain its returning status and PMR number. These entries are removed when the “Err Lease” value specified in the detail pane of the “Network” selection is reached.

PMR Template Properties:

Property	Description
Timestamp	Time stamp when Error Event was first created
PMR Number	Problem Management Report (PMR) number returned from IBM.
Status	<p>This field depicts the status of the Error Event and the results of the PMR request. This field can be set to any of the entries in the status table.</p> <p>0 Pending This status indicates an entry that is set to be sent to IBM. It is the initial status state that triggers the Service Agent CallController to connect to IBM. If the status is some other state, setting it to Pending again causes the entry to be resent.</p> <p>1 Open This status indicates a PMR was opened in IBM RETAIN.</p> <p>2 Closed This status indicates a PMR was closed in IBM RETAIN.</p> <p>3 Held This status indicates the Error Event entry was held. No connection to IBM was made for this status state. Held status entries are general information entries not generally considered hard errors or valid errors.</p> <p>4 Duplicate This status indicates an attempt was made to open a PMR that was already opened. If the same Type, Serial number, Description, and error number is opened before a previous PMR with the same error is closed a Duplicate status is returned.</p> <p>5 Failed This status indicates an attempt to open a PMR with IBM failed for some reason. See the Status Details field for specific details on the error.</p>
Error Number	The Error Number is the actual error number found in the error log or the SRN (###-###) number generated by the concurrent diagnostics on the machine.
Description	This is the short verbal description of the error indicated from the system error log or the diagnostic data files.
Resource	This is the name of the resource where the error occurred.
Duplicate Count	This count indicates how many times the error has occurred since it was originally opened. Every time a duplicate error occurs, a check is made to see if the original creation date of the OPENED PMR is greater than 24 hours. If so, then the local status of the PMR is set to <i>PENDING</i> and an attempt is made to contact IBM again. If the PMR was closed at IBM, a new PMR number will be generated replacing the original one. If the PMR is still open, then the local status will be reset to <i>OPEN</i> and the original PMR number will be maintained. For tracking purposes, the original PMR number is appended to the Details text of the PMR when the PMR is replaced.
Last Occurrence	This is the time stamp of the last occurrence of the Error Event.

Error Details	This field contains the detail description of the Error Event that occurred. The complete diagnostic result file or the actual error log entry as seen in errpt.
Status Details	This field contains the detail description of the status results. If the status is set to FAIL due to some communication problem with the SDR this field would contain the associated error message. If PMR cannot be created because of an entitlement problem, that should be described here.
Last Check For Open Status	This is the time stamp of the last status check of the Open Error Event. This interval can be configured on Call Controller template. Default is every 2 days.
Error Class	Locked field showing what class the error event is posted as. H - Indicates the error is a hardware failure. S - Indicates the error is a software failure. U - Indicates the error is undetermined.
Type	The machine type configured for this monitored host.
Serial	The machine serial number configured for this monitored host.
Model	The machine model configured for this monitored host.
Cluster Type	The machine cluster type configured for this monitored host if part of cluster.
Cluster Serial	The machine cluster serial number configured for this host if part of cluster.
Cluster Model	The machine cluster model configured for this host if part of cluster.
Partition	Logical partition number.
Partition Name	Name of logical partition on which the fault was detected.
Special Handling	Locked field, any special handling instructions placed against this client machine, reference Forms added to monitored machine.
RefCode	Any Reference Code posted for this type fault.

Performance Management Template

The *IBM Performance Management for AIX* product must be installed on each machine for Service Agent to send the performance data to IBM. If any of the monitored machines do not have the properly installed version of *IBM Performance Management for AIX*, Service Agent sends no performance data for that machine.

The *IBM Performance Management for AIX* product, installed on the AIX system, gathers the following system statistics:

- Disk usage; a summary of disk usage of physical volumes and space on the file system
- IO data; Input/Output statistics for disks and CD-ROMs
- Networking data; network statistics for defined interfaces
- Virtual memory and CPU statistics

The Performance Management support in Service Agent helps gather the data from the defined clients, sends the data to the gateway machine, and then to IBM for further analysis.

Performance Manager Template Properties:

Property	Description
Is Performance Management package installed?	<p>The value of this parameter guides the user as to where to look for the Performance Management installation information. If it is not installed, this field would display information regarding the IBM site from which the <i>IBM Performance Management for AIX</i> software can be obtained.</p> <p>Yes - For version information, see the Environment panel for this system's definition.</p> <p>No - The default values will be displayed for all other fields; however, no performance data will be collected, since performance collection code is not installed.</p> <p>For more information on obtaining Performance Management monitoring and code, visit: http://perf.services.ibm.com/pmweb</p>
Enable performance data transmission for this machine?	<p>This parameter enables or disables the collection of performance data that is created by the <i>IBM Performance Management for AIX</i> product. If <i>Enable gathering of statistics about this system</i> is set to true for that monitored machine, performance data is collected from the specified directory at the specified time and sent to the gateway machine. If it is set to false, no performance data is sent to the gateway machine. The default value is true:</p> <p>true - Performance data is collected.</p> <p>false - No performance data is collected.</p>
Time to transmit data [12 hr (AM/PM) or 24 hr time format]	<p>This parameter is required for specifying the time at which the transfer of Performance Data should take place from the client machine to the gateway machine. The default value is a random time between midnight and 5 AM. You can set this value to your preference. The time can be specified either in 12 hour format (for example: 7 AM) or 24 Hr (e.g. 18:30) format.</p>
Performance data directory	<p>This parameter specifies the directory where the <i>Performance Management for AIX</i> product puts all the above mentioned system-related data into this directory. By default, this directory location is always <i>/var/adm/perfmgr/daily/[hostname]</i>. <i>[hostname]</i> = the hostname of the system being monitored</p> <p>Note: You can change the location value to your preference. However, if you change this location, ensure that <i>Performance Management for AIX</i> puts the data in the changed directory.</p>

SNMP Notification Template

The SNMP Notification function sends an SNMP trap notification to a network manager host.

By adding an SNMP Notification template, Service Agent will send an SNMP Notification to the machine(s) of your choosing. Multiple SNMP notifications can be added for a single host.

SNMP Notification Template Properties:

Properties	Description
Target Network Manager Host	Specify the Target Network Manager host that will be receiving the SNMP Trap Notification.
Community	Specify the Community (default is public).
SNMP Port Number	Specify the SNMP port number on the Target Network Manager.
Send Trap for PMRs with Pending Status	Set to TRUE, if you want an SNMP Trap sent PMRs in the “pending” state.
Send Trap for PMRs with Held Status	Set to TRUE, if you want an SNMP Trap sent PMRs in the “held” state.
Send Trap for Internal Errors	Set to TRUE, if you want an SNMP Trap sent for Service Agent internal errors.

Available buttons for the SNMP Notification template:

Button	Description
OK	The OK button located at the bottom of the detail pane is active once data has been typed or changed in a field. Click OK to save all data typed.
Cancel	Click Cancel to cancel the current operation.

Software Service Template

This template allows the SA administrator to enable/disable collection and adjust the collection interval for the selected monitored machine.

Software Service Template Properties:

Property	Description
Enable Regular Software Inventory Collection	Enable or disable Software Inventory collection for this machine.
Software Collection Interval in Days	Specify the frequency for Software collection in days. Default is 7 days. Minimum is 1 day.
Software Inventory Command	This field displays the command used to collect software inventory. The values will be either <code>/usr/bin/lslpp</code> or <code>/usr/suma/bin/suma_swinv</code> .
Enable Regular Fix Inventory Collection	Enable or disable Fix Inventory collection for this machine.
Fix Inventory Collection Interval in Days	Specify the frequency for Fix collection in days. Default is 30 days. Minimum is 7 day.
Fix Inventory Command	This field displays the command used to collect fix inventory. The values will be either <code>/usr/sbin/instfix</code> or <code>/usr/suma/bin/suma_fxinv</code> .
Enable Regular Fix	Enable or disable SNAP collection for this machine.

Inventory Collection	
Snap Collection Interval in Days	Specify the frequency for SNAP collection in days. Default is 90 days. Minimum is 30 day.
General Info	-g Gathers general system information.
Add Object Data Manager (ODM) files	-G Includes predefined Object Data Manager (ODM) files.
Add Security Info	-S Includes security files.
Add multicpu trace log files	-T Gathers all the log files for a multi-CPU trace.
Trace Filename	specify the trace filename
Gathers synchronous (TTY) info	-A Gathers asynchronous (TTY) information.
Gathers SSA info	-b Gathers SSA information.
Gathers dump & /unix info	-D Gathers dump and /unix information
Gathers file system info	-f Gathers file system information.
Gathers installation debug vital product data (VPD) info	-i Gathers installation debug vital product data (VPD) information.
Gathers kernel info	-k Gathers kernel information.
Gathers programming language info	-l Gathers programming language information.
Logical Volume Manager (LVM) info	-L Gathers LVM information.
Gathers Network File System (NFS) info	-n Gathers Network File System (NFS) information.
Gathers printer info	-p Gathers printer information.
Gathers System Network Architecture (SNA) info	-s Gathers Systems Network Architecture (SNA) information.
Gathers TCP/IP info	-t Gathers Transmission Control Protocol/Internet Protocol (TCP/IP) information.
Gathers WLM info	-w Gathers WLM information
Gathers ALL OF THE ABOVE	-a Gathers all system configuration information.

Additional Machine Templates

Additional templates can be added to every machine to provide various functions and options customizing Service Agent to the individual company's needs. In order to access these templates, select your gateway server or a monitored machine and click **Add** and then click **Child**.

E-mail Alert Template

By adding an E-mail Alert template, Service Agent can send an e-mail message to contacts relating all or limited machine problem information. You can define as many e-mail contacts as you require, but an e-mail server must be active and accessible.

E-mail Alert Properties:

Properties	Description
E-mail Address	The e-mail address of the contact you want to alert.
E-mail Subject	The default subject line for messages.
E-mail Server	The hostname name of the mail server to be used.
E-mail Wait Time In Minutes	This field determines how long to wait in order to gather any additional notifications that may be generated. When the time specified is reached, all notifications gathered are combined into one e-mail notification and sent to the e-mail address.
Enabled	Set the following Enabled and Urgent flags True/False accordingly.
Cautions	An <i>Error Event</i> occurred that is considered a cautionary or informational entry.
Failed	A <i>SA Error Event</i> transmission failed to open a PMR on the IBM SDR.
Held	A <i>Service Agent Error Event</i> entry was created and set to a Held status.
Pending	A <i>Service Agent Error Event</i> entry was created and set to a “pending status.
Opened	A <i>SA Error Event</i> transmission OPENED a PMR on the IBM SDR.
Closed	A <i>SA Error Event</i> transmission CLOSED a PMR on the IBM SDR.
Internal Errors	An internal operating problem has occurred (e.g. inability to read a required file, or run a command, or anything that is detected with the operation of SA).
Licensing	There is a change in the machine’s licensing information. Either a machine has been enrolled or it has expired.
Heart Beat	The machine failed a heartbeat.
Test E-mails	This contact should receive any test e-mails sent.
EED	Indicates a fault occurred while collecting or transmitting extended error data.

Available buttons for the E-mail template:

Button	Description
OK	The OK button located at the bottom of the detail pane is active once data has been typed or changed in a field. Click OK to save all data typed.
Cancel	Click Cancel to cancel the current operation.

Client Machines Folder

When a monitored machine is added to the network, the following templates are associated with that monitored machine.

Node Info Template

Properties	Description
Name	This field entry may be updated when an additional host is added.
Ip address	If entered, must be in proper IP number format ###.###.###.### (auto-filled)
Processor ID	Locked, CPU type of local host. (auto-filled)
Type	Required input- 4 digit brass tag number located on exterior of unit.
Serial number	Required - Brass tag serial number located on exterior of unit
Model	Required - Model number of unit, 3 characters like 672 <u>NOT</u> P670
Manufacturer	Optional Manufacturer name of unit.
Type of Installation	Determines the type of protocol used to distribute the client portion of the Service Agent program to selected monitored machines. The following are the available protocols: FTP FTP prompts for the a root authority ID and password. It will use the supplied password for transferring files using Java FTP protocol and running installation processes using the rexec program. SSH The SSH protocol must be configured to allow access as root from the Service Agent gateway to the client system.
Primary Server (Locked)	Used for internal functions within Service Agent for gateway and sub-host communication. Indicates the primary host to which sub-hosts report. This field is locked on the Gateway host and should not be modified.
Secondary Server	Indicates the secondary host to which sub-hosts report in case of <u>primary</u> failure. Initially the same as the Primary, but it may be manually updated to point to a secondary SA gateway server if configured.
Tertiary Server	Indicates the third host to which sub-hosts report in case of <u>secondary</u> failure. Initially the same as the Primary, but it may be manually updated to point to a third SA gateway server if configured.

Call Controller Template

The Call Controller template is installed by default on the gateway server for optimum performance of the Service Agent system. As a rule, the template should not be changed. However, if necessary for load balancing of the Network, any machine can run the Call Controller.

CAUTION: There should only be one Call Controller assigned within the Service Agent System. Do not operate with more than one template at a time. Results are undefined and could result in damaging the Service Agent databases.

Call Log Folder

The Call Log template displays the results of connections and transmissions to IBM. By viewing this log during the dialing or initial phase of a connection, real time updates are logged as the connection is made. Once connection is made and requests have been transmitted. A summary count of the request types and whether they were transmitted successfully are logged.

The summary counts overlay the description entries made during the connection phase. The Description field will hold the last posted message to the Call Log. If you are monitoring the Call Log, you will see a dynamic set of messages being posted. These messages will display the processes being communicated to IBM. The ending status messages that post (Success: #, Fail: #) entries show the transmission results of the communications session, not the function results.

Call Log Properties:

Properties	Description
Start Time Stamp	Time Stamp showing when the transmission started.
Description	Displays real time connection updates as the connection progresses. Once the connection has ended, final Success/Fail results are logged here.
Try	Displays how many times or retries it took to make the connection
TTY Baud	If a baud rate is established, this value represents the posted connect speed or <none>
Snd	This column is not used.
Rcy	This column is not used.
Status	Icon status of transmission; Green Flag = OK
Type	Type of call, LIC (padlock), PMR (bug), VPD (Heart) Icon symbols
End Time Stamp	Time Stamp of when the transmission ended

Check the following communications sample messages that one might see in the description:

```

Task: Ping...
Task: Ping: Connecting to https://localhost:1198
Task: Ping: sending request...
Task: Ping: FAILED: Unexpected end of file from server
Task: Ping: Connecting to https://localhost:1198
Task: Ping: FAILED: A remote host refused an attempted connect operation.
      ( above is a failed attempt to Connection Manager )
Task: Ping...
Task: Ping: Connecting to https://localhost:1198
Task: Ping: sending request...
Task: Ping: receiving response...
Task: Ping: finishing...
Task: EnrollUpdate...
Task: EnrollUpdate: Connecting to https://localhost:1198
Task: EnrollUpdate: sending request...
Task: EnrollUpdate: receiving response...
Task: EnrollUpdate: finishing...
Task: PMR...
Task: PMR: Connecting to https://localhost:1198
Task: PMR: sending request...
Task: PMR: receiving response...
Task: PMR: finishing...

```

Note: The summary counts only relate to whether the transmission was successful or not. It does NOT indicate whether the specific request was accepted or failed due to some internal process checking or rejection. To determine the results of a specific request, if available, you must look at the specific entry for the request in question. A successful result on the transmission does not necessarily indicate a positive reply for a specific request.

Administration Folder

Enroll Template

The Enroll template provides the capability of enrolling one or more defined machines. Holding the shift key while selecting the second machine will mark multiple machines for enrollment.

Within this template, a simple machine list is displayed, in the detail pane to the right, for selection and enrollment.

When the Enroll selection in the Navigation pane is highlighted, the Add and Delete buttons at the bottom are disabled.

Multiple machines may be selected for enrollment at any time. To select a range of machines select the first machine in the list, move to the last machine of the range and hold the Shift key down while selecting the second machine. The full range of machines should be highlighted.

Available Buttons for Enroll Template:

Button	Description
Open	Click Open to display node information of the selected machine. See section on Node Info for details.
Enroll	Click Enroll to enroll the selected machine(s) with IBM.

(Un) Install Template

The (Un) Install template provides the capability to install Service Agent client software on selected machines and to remove it as well. This selection comes into use when a machine is defined at the gateway and the automatic install feature fails or an upgrade of the code is necessary. Failure could be caused if the Remote Shell access is not set up properly or the system could not be found on the network at the time of install. For Service Agent to work on the remote machine the code must be there. The (Un) Install template allows the installation of the code after the machine has been defined. Any Service Agent code previously existing on the sub-host is overwritten with the new copy.

Additionally, the code from a sub-host may be removed or un-installed from the remote system. Selecting uninstall stops the Service Agent program and removes the Service Agent code and file structures from the system.

Available (Un) Install Properties:

Properties	Description
machine list	The name of the target machine on which Service Agent will be installed.

Available Buttons for (Un) Install Selection:

Button	Description
Install	Click Install to install the Service Agent program on the target machine. The transport protocol used to install the program on the target machine is determined by the machine's <i>Installation Type</i> selection (FTP, DSH, RSH).
UnInstall	Click UnInstall to remove the Service Agent program on the target machine. The transport protocol used to (un)install the code on the target machine is determined by the machine's <i>Installation Type</i> selection (FTP, DSH, RSH).

Manage Cluster IDs

This function allows the assignment or removal of Cluster Type, Serial, and Model information to selected machines.

Available Manage Cluster IDs Properties:

Parameters	Description
machine list	The name of the target machine the Cluster IDs will affect
Append	Append the Cluster information to selected machine or machines. Can apply the same cluster information to all machines contained within that cluster.
Remove	Remove Cluster ID from Machines, pushbutton will issue a Yes / No validation prompt. Pressing Yes will remove the cluster information from the selected machines. No will cancel operation with no action taken,

A cluster detail window will allow for the entry of cluster information, and whether you should override any detected cluster information.

Cluster Detail Properties:

Parameters	Description
Cluster Type	Enter 4-digit type assigned to cluster
Cluster Serial	Enter 7-digit serial number assigned to cluster
Cluster Model	Enter 3-digit model assigned (alpha in capitals)
Override detected Cluster Details	Check to override, only if Service Focal Point fails to detect the right cluster info.

Available Buttons:

Button	Description
OK	Saves entered cluster data
Cancel	Returns to previous menu, no action taken

Add 9076 (SP) Nodes template

The template labeled Add 9076 (SP) Nodes is designed specifically for the IBM SP system type 9076. It automatically queries the 9076 system selected, and installs Service Agent on all the nodes it has attached. The 9076 CWS must have already been installed using the 9076 type, serial number, and model number information.

Once the nodes are defined they can be located in the Network tree under a department, named after the machine that was originally selected. For example, if a 9076 machine was named *9076ABC* and was selected and then, upon completion of this process the entries for all nodes found would be under the department name of

9076ABE:SPNodes. At a later time, if additional nodes are added, you can either add them individually using the typical process or rerun this selection again.

Add 9076 (SP) Nodes template:

Parameters	Description
Type of Installation	<p>Determines the type of protocol used to distribute the client portion of the Service Agent program to selected monitored machines. The following are the available protocols:</p> <p>FTP prompts for the a root authority ID and password. It will use the supplied password for transferring files using FTP and running installation processes using the rexec command.</p> <p>RSH protocol must be configured to allow access for the svcagent user ID on the gateway system to access the client system. One way to do this is to add to the .rhost file in the root directory the entry “<gateway> svcagent” where “<gateway>” is the hostname of the gateway or forwarding system to which the client will be connecting.</p> <p>DSH protocol allows the gateway to create a node using the DSH system. Needs a valid kerberos ticket for root ID.</p>
Open	Click Open to see Node information details on the selected machine.
Add 9076 nodes & install	Click the Add 9076 nodes & install button to add the node and distribute the client portion of the Service Agent program.
Remove all the 9076 nodes & uninstall	Click the Remove all the 9076 nodes & uninstall button to remove all selected 9076 nodes and remove the client portion of the Service Agent program..

To monitor additional frames added to a 9076 group or to push a new version of the Service Agent program to the 9076 nodes. The template labeled *Add 9076 (SP)* can also be used. If the department name for the selected 9076 Control Work Station (CWS) has previously been created, you are prompted to select Yes or No to the *Retain Network Group* prompt. Pressing the Yes button puts the Service Agent program on any new nodes it finds and adds those nodes to the existing group. Pressing the No button puts the Service Agent program on all nodes (existing nodes) in the group as well as any new nodes it finds.

Data Compression Cycles Template

The Data Compression Cycles template allows for the automatic saving and restoration of the SA gateway database. The ESS database is maintained within the Java ESS daemon memory space and is saved and restored daily. Old or unused data is purged automatically from memory during this cycle if compression is enabled. Compression should always be enabled to keep the daemon running as smoothly as possible. If daily compression does not occur, then the **sares** process will force an ESS daemon restart.

Data Compression Cycles Properties:

Properties	Description
Next Compression Date	Locked entry showing the date and time the next scheduled compression cycle will occur.
Enter Time	A new cycle time may be set by entering the desired time in either 12 or 24 hour format. This is activated by pressing Set The Timer For Data Compression push button. <i>Tip:</i> Use the format display at the bottom of the window to assist you in the correct format for entering the time setting.
Compression Enabled	Set to true to allow daily compression cycle to occur.
Push buttons	
Set The Timer For Data Compression	If entry is valid then the Next Compression Date will reflect the new time. If improper data entry is made, a RED Time error will be posted and date will not be adjusted.
Compress Data Now	Immediately invoke a compression cycle, where the ESS process will shutdown, restart the database. The Next Compression Date will be updated to the new daily cycle time in 24 hours from the current time.

Import / Export Template

The Import / Export template allows for the automatic addition of machines from a ASCII input file, the capability of saving existing machine entries to a ASCII output file, and exporting the defined database to a binary file and importing a previously exported database

Import ASCII Input File Format:

Each monitored machine to be added must be on a single line. Each line must contain the required machine data in the following order with comma separators and no spaces.

Note: Processor ID is obtained by executing /usr/svcagent/bin/processor-id on the physical host.

“Hostname”, “Type”, “Serial”, “ProcessorID”, “Model”

For example, the input file would contain:

```
sles1.austin.ibm.com,9111,011043515,POWER5,812  
rhel2.austin.ibm.com,7028,011099998,POWER4+,6H2  
....
```

Available Buttons for Import / Export Template:

Button	Description
ASCII Input Machine List	Click ASCII Input Machine List to enter a ASCII machine list. Type the location and name of the file at the selection window.
ASCII Output Machine List	Click ASCII Output Machine List to output an ASCII machine list of all defined Service Agent machines. Type the destination and name of the file at the selection window.
Export Service Agent Database	Click Export Service Agent Database to output the defined machine database to a file.
Import Service Agent Database	Click Import Service Agent Database to input a previously exported machine database.

Lockout Machines Template

The Lockout Machines template allows turning off or locking out Service Agent on an individual machine or group of machines.

This is useful when there is to be some type of system maintenance that could possibly cause Service Agent to pick up false errors; for example, if diagnostics are run on a system with known problems, and Service Agent is not locked out or turned off. Then when diagnostics find an error, Service Agent records and reports it.

In order to avoid confusion, lock out the system that you want to ignore prior to performing any activities that could cause false errors.

CAUTION: The locked out system will not report any errors until the lock is removed. Be sure to unlock the system after all maintenance work is complete.

Available Buttons for Lockout Machines Template:

Button	Description
Open	Click Open to see Node information details on the selected machine.
lock	Click lock to lock the machine and disable Service Agent reporting.
unlock	Click unlock to unlock the machine and enable Service Agent reporting.

Purge Data Template

The Purge data template allows you to purge all the data collected and placed in the CallLog folder. The CallLog folder is located beneath the Network folder in the Navigation Pane. It will clear PMR or error data that has accumulated under machine

folders. If repeated calls are being made to IBM every 15 minutes or so, there may be something stuck in the OutGoing Queue entry, which would be cleared.

Available Buttons for Purge Data Template:

Button	Description
Purge	Click Purge to clear away all the following data. Items set to true will be cleared. <ul style="list-style-type: none"> • CallLog Data - Clears the CallLog • Error Warnings - Clears accumulated Error Warnings • Internal Errors - Clears accumulated Internal Errors • Closed PMR - Clears PMRs with a Closed status • All PMR - Clears all PMRs from the database • Outgoing Queue - Removes pending entries in the outgoing queue and sets the status to Fail

SA Access Template

This template allows the assignment of a new password for Service Agent User Interface access.

Pressing the Change the Password pushbutton will bring up a window prompt where old and new password information can be entered. The keystrokes will be shown with * filled for keystroke verification.

SA Access Properties:

Properties	Description
Old Password	Enter the current SA access password
New Password	Enter the new password data
Verify New Password	Enter the new password again for verification
OK	Verifies and saves entered data
Cancel	Returns to previous menu, no password action taken

Alerts Folder

The Alerts template allows for panel display notification of alerts.

Alerts are generated by Service Agent when important events occur, such as status changes to PMRs or Service Agent internal errors. In addition to the E-mail alert notification, other alert methods can be displayed on the panel. As long as the selection is open, configured alerts are displayed and maintained in the detail pane window. When

the selection is closed and reopened, the panel is cleared for new alerts. By default, all alerts are enabled for display in the Alert selection. Specific alerts can be ignored by setting the associated toggle buttons to true.

Alert Template Properties:

Property	Description
Limit	Number of Alerts that are kept at one time. When the limit is reached, no more entries are displayed until the window is cleared or the limit is increased.
Alerts	This is the display capture window for Alerts. All alerts are displayed as they occur; uninteresting alerts are filtered out.
Open	To view details of an alert entry, select it from the Alert window and click Open .
Reset	To clear the list entries from the alert window press this button.
Ignore Items	
Cautions	To ignore "Cautions" alerts, set this toggle button to true.
Closed	To ignore "Closed" alerts, set this toggle button to true.
Failed	To ignore "Failed" alerts, set this toggle button to true.
Held	To ignore "Held" alerts, set this toggle button to true.
Internal Errors	To ignore "Internal Error" alerts, set this toggle button to true.
Opened	To ignore "Opened" alerts, set this toggle button to true.
Pending	To ignore "Pending" alerts, set this toggle button to true.

Filter List Folder

Resource Filters Template

The Resource Filters template works in conjunction with the Add / Forms / Resource Filter template.

Resource Filter Properties:

Property	Description
Resource or Start Range	Enter the resource name as it appears in errpt. This is the resource or starting resource name of items that should be ignored completely.
End Range	If you want to ignore a range of devices of the same type, enter the last device resource name.

Removal of a resource filter should be done on the information template where it was added. When a Resource Filter entry is selected on the detail pane, the **Delete** push button will be highlighted to show it is an active valid push button. Pressing the push button will give you a Yes/No question to prevent accidental removal.

When this Resource Filters template is selected, a display of all resources that have been configured to be ignored is displayed.

If this template is blank, then no resource filters have been added to the Service Agent Network.

For details on adding Resource Filters, see *How to define Resource Filters* on page 72.

Once resource filters have been defined, clicking on this template changes the detail pane into two sections. The upper section has a list of all of the resource filters indicating the Source or machine to which the resource filter has been added and the name of the resource that is being ignored.

The lower section displays the Node Information associated with the source or machine that to which the filter was added . The display will change depending upon which source or machine is selected.

Thresholds Template

The Thresholds template works in conjunction with the Add Form Threshold template. When added to the Network level, it is attached to the Network template and it is applied to all monitored machines. It can be added at department or machine levels, multiple thresholds will appear as tab items on associated information templates. When added to a client machine, it will be applied only to that machine.

To remove a previously added threshold template the appropriate info template must be selected and threshold entry selected. Once threshold entry is selected on the detail pane, the **Delete** push button will highlight to show it is an active valid push button. Pressing the push button will give you a Yes/No question to prevent accidental removal.

Threshold Properties:

Properties	Description
Error ID	The SRN as shown in the diagnostic results file. The majority of errors is detected in this manner or in the error log label of one the monitored resources. See the list of errors monitored <code>/usr/svcagent/README.TXT</code>
Action	This is a selection pull down for the action to be taken when Error ID occurs and threshold conditions are met. It is a required entry. 0 CREATE PENDING - Creates a pending call when threshold conditions are met. 1 CREATE HELD - Creates a call that will be held and not called in to IBM. 2 IGNORE - Completely ignores Error ID, no action taken.
Count	The number of times the error must occur before meeting the threshold timing condition defined by the following time settings.
Days	The number of days over which the count can occur.
Hours	The number of hours over which the count can occur.
Minutes	The number of minutes over which the count can occur.

When this Thresholds template is selected, all thresholds that have been configured are displayed. If the display of sourced thresholds are blank, no additional thresholds have been added to Service Agent. This blank condition is seen on all SA predefined thresholds that are applied to Network level. If a source shows an entry, then it reflects where the new threshold has been applied.

For details on adding Thresholds, see *How to specify Thresholds* on page 72.

Clicking the Threshold template makes the detail pane appear in two sections.

The upper section has a list of all of the thresholds with the specific configuration information set for each threshold.

The bottom section displays the information details of the machine to which the threshold was added, or the information details of the Network if the threshold was added to the network. In addition, there is an Overrides entry which displays the name of the source or machine this threshold overrides. If the override is on a predefined threshold the source is blank and therefore the override is blank.

For example, if threshold error 124-708 is added to the Network and the same threshold error number 124-708 is added to a specific machine with different configuration data, then the threshold added to the machine would take precedence over an override threshold configured for the Network when it occurs on that machine. If the error occurs on any other machine, then the threshold for the Network applies.

Manual Tools Folder

Connect Template

The Connect template provides the capability to connect to IBM immediately or force a current connection to be canceled. It can be used in situations where there are pending requests that should go out immediately or where there is a need to verify the external connection process is working properly.

When connection is made to IBM, any pending requests destined to be sent are handled. If there are no pending requests, then a simple handshake between Service Agent and the IBM is performed and the connection is ended.

Available Buttons for Connect Template:

Buttons	Description
Connect	Click Connect to initiate an immediate connection to IBM.
Disconnect	Click Disconnect to disconnect the current connection to IBM.

PMR Template

The Manual PMR allows the creation of a PMR for the selected machine and sends it to the IBM.

Initial selection of the machine where PMRs will be posted must be made and the *Generate* button activated. This will bring up a Manual PMR Generation window with fields for updating Error Number, Description, and Error Details. The Error Number field should adhere to the error field conventions, while the Description and Details are freelance input data that describe the fault.

PMR Template Properties:

Properties	Description
Error Number	Enter SRN or errpt error number or label.
Description	Enter a short description of error.
Error Details	Enter as much detail as required to describe the problem accurately. Window will add a scroll bar if needed.
Error Class	Hardware / Software pull down. Hardware Only at this time

Available Buttons for PMR Template:

Buttons	Description
Generate	Gives you a choice to dial immediately or submit a delayed request to the IBM SDR.
Cancel	Return to main Manual PMR window with no action taken.

Only Hardware PMRs may be created currently. The Software selection is for future requirements.

Performance Data Template

The Performance Data template provides the capability to manual send all performance data available on the system to IBM.

Available Buttons for Performance Data Template:

Buttons	Description
Select machine list	Select one or more machines from this list
Open	To view information about the machine selected.
Send Performance Management Data to IBM	This button sends all available performance data to IBM for the set of selected machines.

SNAP Template

“SNAP” stands for “system snapshot,” that is, it allows capture of the current system configuration. The SNAP template allows you to capture and send a SNAP file for the selected machine or machines to IBM. After data is collected, there will be an option to wait for the next time Service Agent calls IBM, or you can make a connection and send the file immediately. SA uses /var on the client to create the SNAP file and then transfers it to SA gateway /var/svcagent/machine/hostname/soft/ until the file is sent to IBM. Make sure /var filesystem has enough available space to hold a SNAP file on monitored host.

Manual SNAP template:

Properties	Description
Machines	List of available machines, one or more must be selected.
Check Options	-g is the default selected option
-g	Gather general information
-G	Include Pd* ODM files in general information.
-S	Include security files in general information.
-T	Captures a specific trace (specify full path name of the trcfile).
-A	Gather async (tty) information.
-b	Gather SSA Adapter/Disk information.
-D	Gather dump and /unix.
-f	Gather file system information.
-i	Gather Install information.
-k	Gather kernel information.
-l	Gather programming language information.
-L	Gather logical volume manager (LVM) information.
-n	Gather nfs information.
-p	Gather printer information.
-s	Gather TCP/IP information.
-w	Gather workload manager (wlm) information.
-t	Gather tcpip information.
-a	Gather all information.

Available Buttons for SNAP Template:

Buttons	Description
Open	To view information about the machine selected.
Collect Snap Data	Starts data collection and transmission to IBM.

Send VPD Template

The Send VPD template gathers the latest Vital Product Data (VPD) from the selected machine and sends it to IBM.

In those instances where the most current copy of VPD is needed by IBM support for problem analysis, this selection bypasses the VPD timer configuration. You have the option to wait for the next time Service Agent calls IBM, or you can make a connection and immediately send the VPD.

For information on configuring VPD template, see “How to send Manual VPD data” on page 77.

Save VPD data to file

Saving VPD data to a local file is possible using the *VPD* option under the *Manual Tools* folder.

Select the machine for which the VPD data needs to be saved and click .

A file save dialog box pops up. The VPD data can be saved in two formats.

1. Text Format - Choose the *Files of Type* as text files (*.txt) and choose the file name and click on **Save**.
2. ZIP Format - Choose the *Files of Type* as zip files (*.zip) and choose the file name and click on **Save**. The file will be in zip format with a .zip extension. Use *unzip -j* to unzip the file.

If the destination for the file is a diskette, the program may fail if the diskette is full and does not prompt for the next diskette to be inserted. Hence the save process stops in the middle.

The best way to copy the file to a diskette is to save the file to the local hard drive first, then go to the command line and tar the file and then copy it to a diskette using a separate command.

Test Tools Folder

Test E-mail

The Test E-mail template allows you to verify the proper operation of the E-mail Alert templates that have been added. This selection sends a test E-mail notification to all E-mail Alert templates that have the Test E-mail option turned on or set to TRUE. If an E-mail address should not get *Test Notifications*, this option should be switched to FALSE.

See section on “Adding E-mail Alert” templates for details. If an e-mail address fails to receive a test notification, check to make sure the E-mail alert and the Test E-mail check box are set to TRUE. If they are, then examine your local e-mail system configuration and set up to ensure it is working property. Service Agent sends e-mail notifications using the simple *sendmail* command as a typical client. All other aspects of the local mail system are under control and responsibility of the user or local administrator.

Test PMR

The Test PMR template sends a test Problem Management Report to IBM. Upon receiving this report, contact is made back to the customer indicating proper reception of the test PMR. This is used to verify the machine can properly open a PMR into the IBM system. If contact with IBM support is not made within a reasonable time after the PMR has been successfully opened, contact IBM support or your normal channel of access to verify its arrival. Be ready to supply the PMR#, machine type, and serial number of the machine against which the problem was opened.

Test SNMPTrap

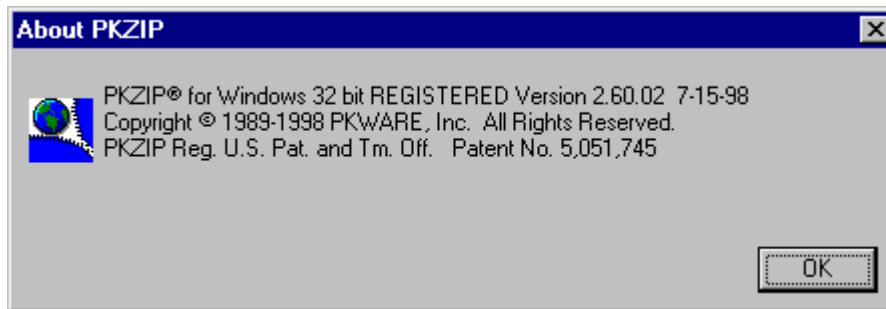
The Test SNMPTrap template sends a test SNMP event to all Service Agent clients configured to listen for the event. These Service Agent clients then in turn generate an SNMP trap notification and send it to their designated SNMP Target Host.

Appendix C – Accessing Service Agent from a PC

You can access Service Agent from a PC using either the Basic or Advanced Graphical User Interfaces. You must be using Windows 95, Windows 98, Windows NT (SP 4.0+), Windows 2000, or Windows XP.

Creating the PC User Interface

1. Log on to the gateway system.
2. Type `/usr/svcagent/bin/installnt`. Running `installnt` creates a tar file called `instui.tar` located in the `/tmp` directory.
3. Transfer the `instui.tar` file to the PC from which you want to run the Service Agent User Interface.
4. Unzip `instui.tar` using PKZIP or similar zip utility that supports tar format. About panel from the PKZIP for Windows used in testing:



5. The unzipped file contains a working directory called `svcagentui`. Open the `svcagentui` directory and you will find various scripts for starting the advanced or basic user interfaces. Depending on your PC environment, you can select one of the files to bring up the user interface remotely from a PC.

Advanced User Interface

- `startadvanced_java.bat` - use with Java 1.1
- `startadvanced_java2.bat` - use with Java 1.2 or higher
- `startadvanced_jre.bat` - use if you have JRE instead of Java

You can choose one from these three different scripts to bring up the advanced user interface. These commands expect Java or JRE (Java Runtime Environment) to be present on the system. To ensure, Java is present, run the following command from a DOS prompt.

```
java -version
```

If java is installed, this will display the level of Java on the panel. Depending on the java version, you can decide which script best suits your Java environment.

For example:

```
C:\>java -version
```

```
java version "1.3.1"
```

```
Java(TM) 2 Runtime Environment, Standard Edition (build 1.3.1)
```

```
Classic VM (build 1.3.1, J2RE 1.3.1 IBM Windows 32 build cn131-20031021
```

```
(JIT enabled: jitc))
```

This result illustrates a system installed with Java 2. Java level of 1.2 or above is considered to be Java 2. In this case you would run the “startadvanced_java2.bat” script.

If the Java level is 1.1 then use the startadvanced_java.bat script.

On older systems, instead of java, you may find a runtime version of Java installed on the system. If you have JRE on the system instead of java, you can try the third option to bring up the UI. To check if JRE is present on the system, run the command, “jre” and see if it returns a valid response. If jre is present, you may use the startadvanced_jre.bat file to bring up the advanced UI.

Basic User Interface

The same checks used for the Advanced User Interface apply to determining the version of the Basic User Interface appropriate for your system.

- startbasic_java.bat - use with Java 1.1
- startbasic_java2.bat – use with Java 1.2 or higher
- startbasic_jre.bat – use if you have JRE instead of Java

Troubleshooting

Password panel does not appear

The password panel may be hidden behind other windows. Try minimizing all windows.

UI does not appear

If the UI does not connect to the gateway the reason may be the properties file does not have a fully qualified name in it. You may need to edit the properties file located in the *svcagentui* directory and put in the fully qualified hostname of the gateway.

Appendix D – Service Agent ASCII User Interfaces

Before you can use the Service Agent ASCII user interfaces you will have had to install Service Agent on a machine chosen to be your gateway machine. Additionally, you will have to have an ASCII display attached to that machine.

You can manage Service Agent from an ASCII display as well as from a display capable of displaying graphics.

As with the graphical user interfaces (GUIs), there are two levels of ASCII interfaces:

- Basic
- Advanced

The ASCII User Interface has been internationalized and localized for most languages (i.e., NLS enabled) and is therefore capable of displaying characters in all UTF8 character sets. The term ASCII is a holdover from legacy versions of Service Agent.

Accessing ASCII from smitty

1. Access *smit* from an ASCII terminal or type **smitty** (lowercase) from the command line of a graphics terminal. You see the System Management panel. If you are already in *smit* or *smitty*, go to the next step.

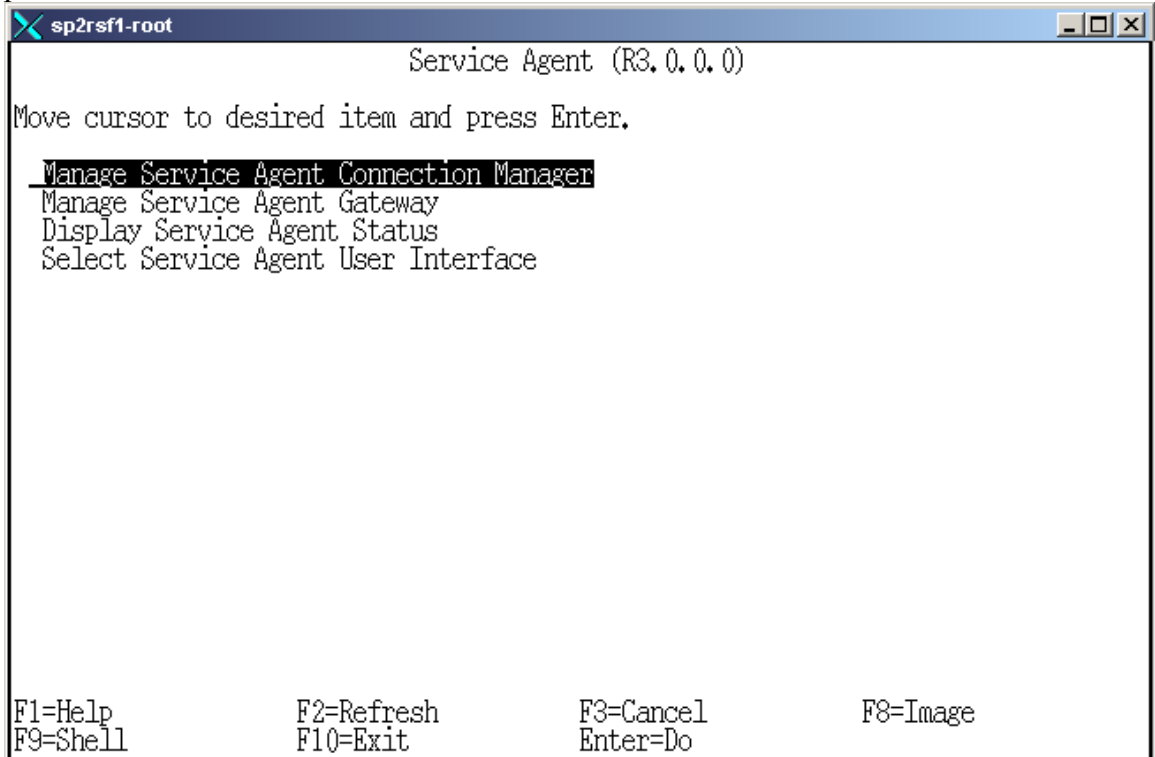
```
System Management

Move cursor to desired item and press Enter.

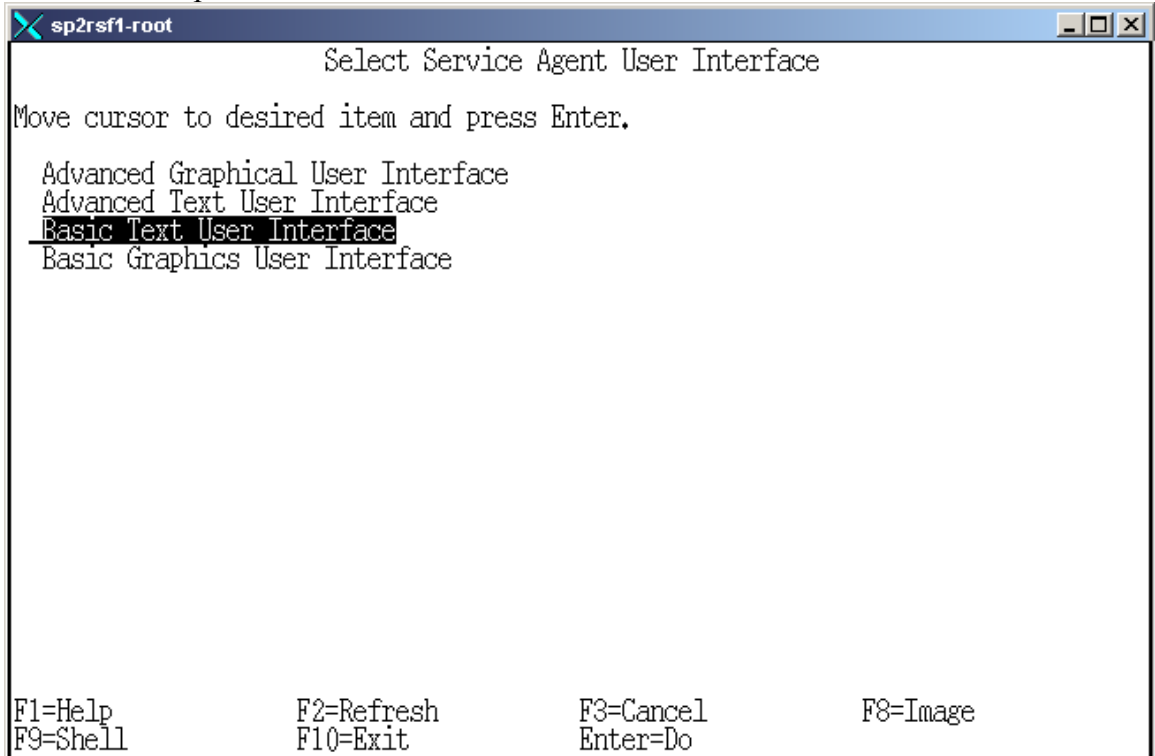
Software Installation and Maintenance
Software License Management
Devices
System Storage Management (Physical & Logical Storage)
Security & Users
Communications Applications and Services
Print Spooling
Problem Determination
Performance & Resource Scheduling
System Environments
Processes & Subsystems
Applications
Using SMIT (information only)
```

2. Select **Problem Determination** and press **Enter**. You see the Problem Determination panel.

3. Select **Service Agent gateway** and press **Enter**. You see the Service Agent panel.



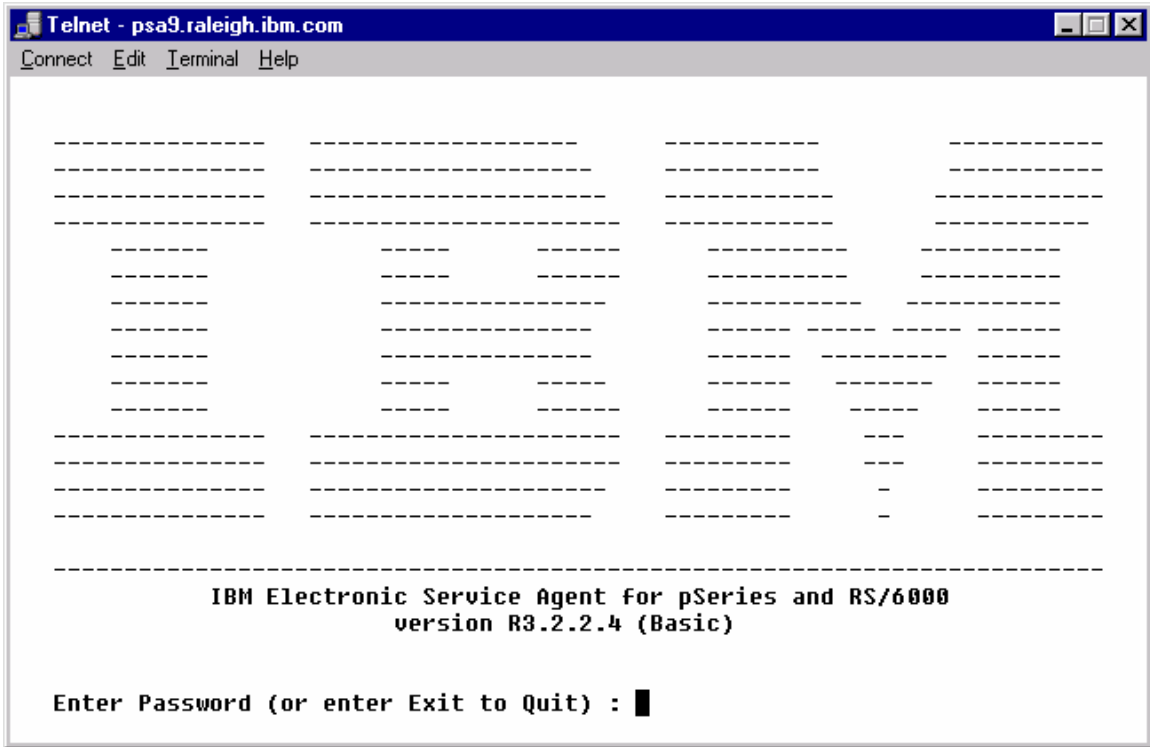
4. Select **Manage Service Agent Connection Manager**. You see the Service Agent User Interface panel.



5. Select either the Basic or Advanced User Interface.

Basic ASCII Password

You will be prompted for the password. The initial password is *password*. Type password and the following will be displayed:



Basic ASCII Welcome Panel

```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help

          IBM Electronic Service Agent for pSeries and RS/6000
          version R3.2.2.4 (Basic)
-----
| Welcome
----- screen 1 of 2 -----
|
| Use the Service Agent Basic ASCII Interface to define monitored machines
| and configure a communications link to IBM so that Service Agent data can
| be sent to IBM for problem analysis.
|
| You need to update (or take IBM-supplied defaults) to the following prompts
| in the Service Agent interface:
|
| Network
| Gateway
| CallController
| Connection Manager
| Dialer
| Machines
| Import/Export
|
|                                     [F <text>]-Find  [H]elp
|                                     [N [#]]-NextScreen [E]xit
-----
Would you like to continue? [Y/E] : █
```

Select “Y” to continue.

When you enter the ASCII interfaces the first time, you are prompted to complete certain required parameters and fields as shown in the following list:

- Customer, IBM Support May Contact > Name
- Customer, IBM Support May Contact > E-mail
- Customer, IBM Support May Contact > Phone Number
- Address > Queue Country
- gateway > Type
- gateway > Serial Number
- gateway > Model

The entries will automatically force data entry if fields are empty. Some fields may be automatically filled. You will see this panel.


```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Basic)
----- screen 1 of 1 -----
The Basic Service Agent found the following empty required fields:
1. Customer, IBM Support May Contact -> Name
2. Customer, IBM Support May Contact -> Email (user@server.domain)
3. Customer, IBM Support May Contact -> Phone Number
4. Address -> Queue Country / Region
[T]op Menu [H]elp
[E]xit
Please Enter "Name" : █
```

Navigation in the Basic ASCII User Interface

To navigate in an ASCII interface you must use commands and respond to prompts to:

- Move forward
- Move backward
- Select and change specific options
- Save changes
- Access Help
- Exit

Use the Help text associated with the Welcome panel (for the Basic ASCII interface) or the Main Menu panel (for the Advanced ASCII interface) to find descriptions of how the navigation commands work.

```

Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help

          IBM Electronic Service Agent for pSeries and RS/6000
          version R3.2.2.4 (Basic)
-----
| ./Help
|----- screen 1 of 9 -----
|
| (H070) ASCII Welcome
|
| The User Interfaces (Basic and Advanced) allow the
| user to setup and define hosts or machines that Service Agent
| monitors.
|
| The Basic User Interface is designed to allow an
| initial user to configure the Service Agent system with as
| little user input as possible, utilizing predefined defaults for
| a single level network environment.
|
| The Advanced User Interface is used for advanced
| functions and customization of the system as well as
| configuration for complex systems and multilevel networks.
|
|                                     [F <text>]-Find
| [T]op Menu [B]ack Menu             [N [#]]-NextScreen [E]xit
|-----
User Input: █

```

Flow through the Basic ASCII User Interface

The Basic ASCII interface is designed to let you work your way from the beginning to the end of the interface. The Basic ASCII interface has the following categories:

- Network
- gateway
- Call Controller
- Connection Manager
- Dialer
- Machines
- Import/Export
- Enroll
- Connection to IBM
- CallLog Information
- Error Log

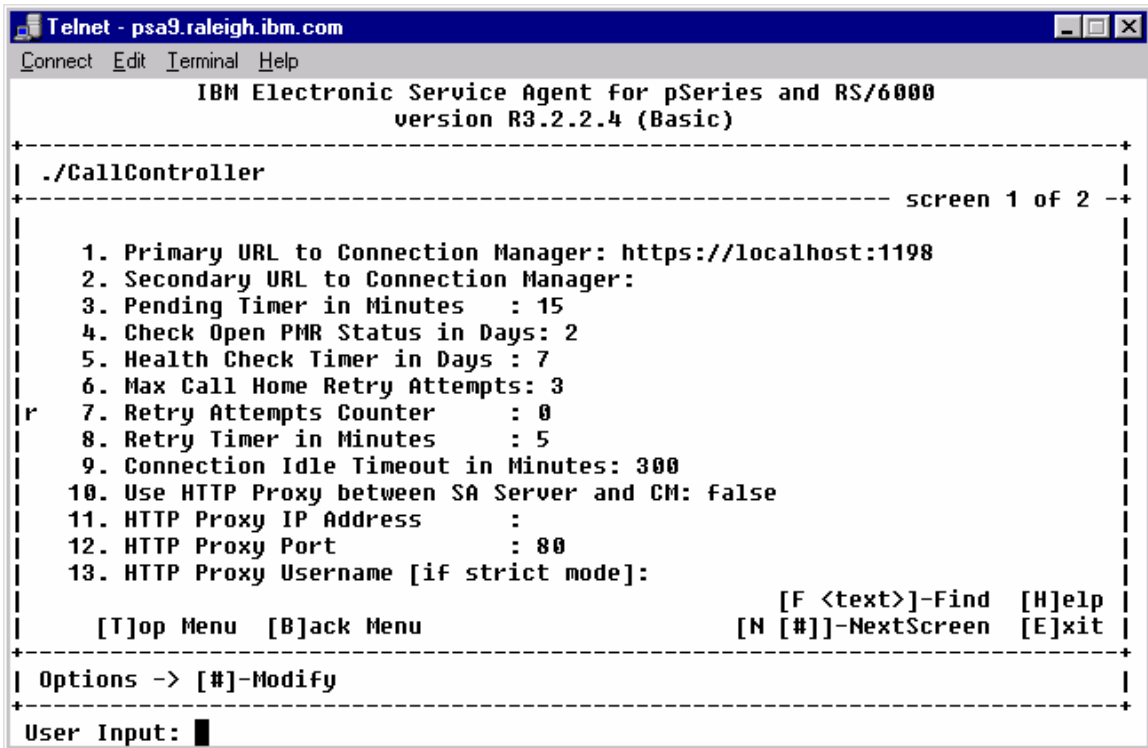
For example, if you were on the Network panel and wanted to get to the Machines panel, you would have to respond No to the *Would you like to update* prompt on the Network, gateway, Call Controller, Connection Manager, and Dialer panels. This flow should drive you through the basic setup of SA, when you complete and save a template, you will be linked to the next one in the flow.

You will probably find basic Network data filled in. You should add any additional information to define your account. The gateway information should be completely filled in with the auto discovery at configuration time, but please take a moment to verify the data.

Basic ASCII CallController and SACM

The Call Controller template only has to be entered if you expect to use some other host as the Connection Manager link to IBM. If that is the case, then you will be changing item # 9 to point at the SACM host that you expect to be using.

The next decision would affect the Connection Manager (if it is on this SA gateway); you must decide whether the SACM is going to use Internet access or take the default dialer. Using the first option will determine if the dialer is used; setting it to false will use an existing Internet connection.



```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Basic)
-----
| ./CallController |
|----- screen 1 of 2 -----|
|
| 1. Primary URL to Connection Manager: https://localhost:1198
| 2. Secondary URL to Connection Manager:
| 3. Pending Timer in Minutes : 15
| 4. Check Open PMR Status in Days: 2
| 5. Health Check Timer in Days : 7
| 6. Max Call Home Retry Attempts: 3
| 7. Retry Attempts Counter : 0
| 8. Retry Timer in Minutes : 5
| 9. Connection Idle Timeout in Minutes: 300
| 10. Use HTTP Proxy between SA Server and CM: false
| 11. HTTP Proxy IP Address :
| 12. HTTP Proxy Port : 80
| 13. HTTP Proxy Username [if strict mode]:
|
| [T]op Menu [B]ack Menu [F <text>]-Find [H]elp
| [N [#]]-NextScreen [E]xit
|-----
| Options -> [#]-Modify |
|-----
User Input: █
```

```

Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Basic)
-----
| ./ConnectionManager                               screen 1 of 1 |
|-----|
| 1. Use Modem as a Connection Method to IBM: false |
| 2. Password for updating Connection Manager: ***** |
| 3. Proxy Type : NONE |
| 4. Proxy IP Address : |
| 5. Proxy Port : 80 |
| 6. Proxy Username (leave empty if no username): |
| 7. Proxy Password (leave empty if no password): ***** |
|-----|
| [T]op Menu [B]ack Menu [H]elp [E]xit |
|-----|
| Options -> [#]-Modify |
|-----|
User Input: █

```

Basic Dialer template

If the dialer function is going to be used, then you must populate the Dialer template. Once the primary location is selected, most of the template will be automatically filled. You must modify the phone number to access the correct dial structure to match your location.

```

Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Basic)
-----
| ./Dialer Parameters                               screen 1 of 2 |
|-----|
| 1. Primary Location : . US, TX Austin (PPP/SLIP/U.90/ISDN)|1; |
|                    1-512-691-4485 |
| 2. Primary Phone Number : 1-512-691-4485 |
| 3. Secondary Location : |
| 4. Secondary Phone Number : |
| 5. Account : FAUN |
| 6. User ID : FRS6UN |
| 7. Password : as400t1 |
| 8. TTY # : tty0 |
| 9. Modem Type : IBM 7852-400 |
| 10. Baud Rate : 56000 |
| 11. Reset String : AT&F |
|-----|
| [T]op Menu [B]ack Menu [F <text>]-Find [H]elp |
| [N [#]]-NextScreen [E]xit |
|-----|
| Options -> [#]-Modify [S]-Save |
|-----|
User Input: █

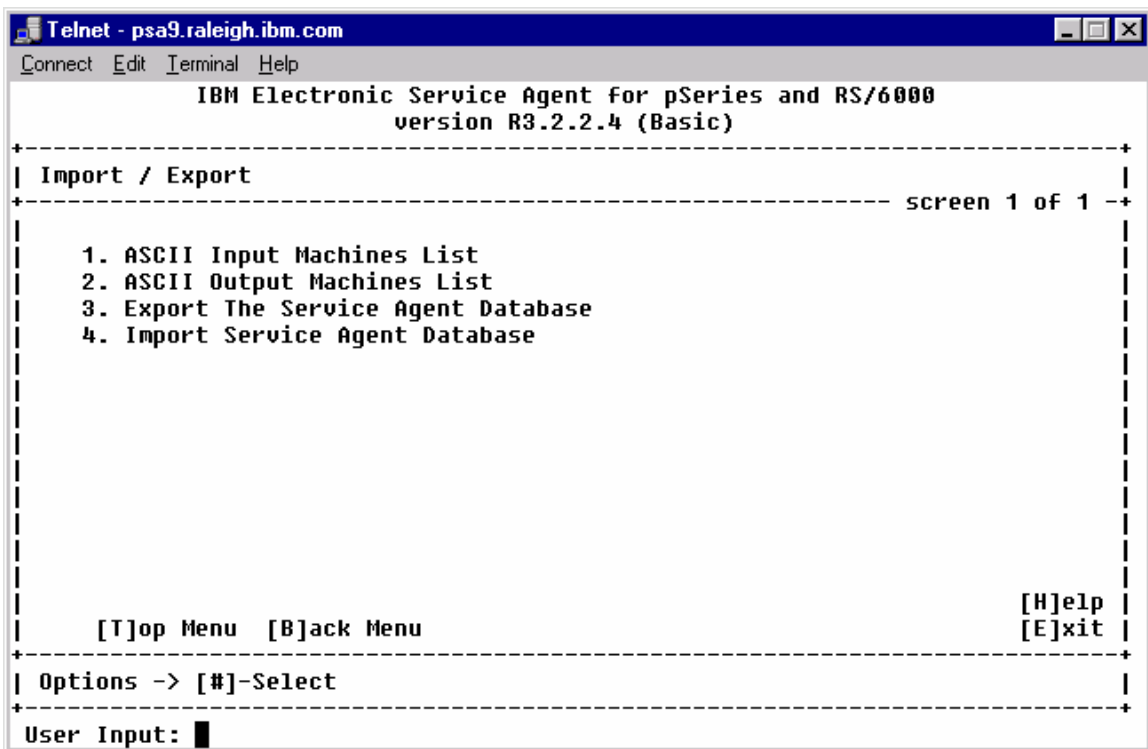
```

Then make sure correct tty port is selected from the available tty ports. Then check that the proper modem is selected and the init string entries look valid for your modem.

Basic ASCII Import / Export

Once you save the Dialer template, you have the option to test the configuration by enrolling the Gateway host. You may also elect to add more machines to this basic configuration, or to import a previously exported SA database, which would restore the full configuration that was in the exported data. With that option, the client code is not distributed and it must be installed on the clients manually. If you elect to import from a machine list or use the Machines template to add machines, the client code will be sent out and installed on the additional client machines.

Once you have finished adding machines you may elect to exit the Basic interface by entering an **E**, then respond with **Y** to the Yes/No prompt to really exit.



```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Basic)
-----
| Import / Export                                     screen 1 of 1 |
|-----|
| 1. ASCII Input Machines List                       |
| 2. ASCII Output Machines List                     |
| 3. Export The Service Agent Database               |
| 4. Import Service Agent Database                   |
|-----|
| [T]op Menu [B]ack Menu                            |
|                                                    |
| [H]elp                                           |
| [E]xit                                           |
|-----|
| Options -> [#]-Select                             |
|-----|
User Input: █
```

Navigation in the Advanced ASCII User Interface

The Advanced ASCII interface lets you choose options from a main menu. Available options are:

- Network
- CallLog
- Administration
- Alerts
- Filter Lists

- Manual Tools
- Test Tools

To access the Advanced ASCII User Interface from the command line, execute the command:

```
/usr/svcagent/bin/sauiascii
```

To advance to any option you type the option number on the command line and press Enter key.

Getting started using the Advanced ASCII User Interface

For example, to get to Test Tools, type 7 on the command line and press the Enter key. To return to the main menu, type T (for top or main menu) and press the Enter key.

After Service Agent has been configured, you can access the Advanced ASCII interface to configure such things as filters, alerts, e-mail alerts, and so on.

The Help menu is always available to assist you from any of the User Interface templates. The following list of menu keys and their definitions will aid you in moving through the various templates. If a menu key is active it will be displayed on the template.

```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Advanced)
----- current menu -----
| . |
----- screen 1 of 1 -----
|
| 1. Network
| 2. CallLog
| 3. Administration
| 4. Alerts
| 5. Filter Lists
| 6. Manual Tools
| 7. Test Tools
|
| [H]elp
| [E]xit
|
-----
| Options -> [#]-Select
|
-----
User Input: █
```

Menu Key Definitions

All key inputs accept both upper and lower case, when shown on menu.

[T]op Menu -

Used in the Advanced ASCII Interface. Pressing “T” when displayed will jump to the top menu selection list. In Basic ASCII Interface same as “B”.

[B]ack Menu -

Pressing “B” will take the user to the previous menu selection list.

[E]xit -

Pressing “E” will exit the program.

[F <text>] - Find -

Entering “f <some text>” will cause the interface to search for the text in the text file or list that is currently displayed. The text search is not case sensitive. The search starts from the current panel and stops at the first occurrence of the string or at the end of the file. After the first discovery is made entering “F” by itself will cause the display to go to the next entry found. Line containing text will be marked “>” in first column.

[F[U] <text>] - Find -

Entering “FU <some text>” will search UP the text file or list for the entered text. Search starts from current panel to beginning of file. Additional “fu” entries will continue the upward search.

[N [#]] - Next Panel -

Entering “N” will cause the next panel of information to be displayed. This operational mode becomes active when the displayed text exceeds the display area of the program. Entering “N <some number>” will jump the display window by the entered number.

[P [#]] - PrevPanel -

Entering “P” will cause the previous panel of displayed text to be shown. Entering “P <some number>” will jump the display text window by the entered number.

[#] - Select -

When active, allows the user to select a menu selection.

[#] - Modify -

When active, allows user to modify / update the displayed selection.

[D #] - Delete -

When active allows user to delete one of the entries displayed.

[S] - Save -

After modifying or updating an entry, you MUST select the “S” save option to have the data put into the Service Agent database. If the fields are changed but the “S” is not pressed then upon exit of the panel or interface a changed data reminder will be posted allowing you to return and save or exit and lose entered data.

Read Only & Mandatory

If the fields that are shown have the letter **r** at the beginning, it means that such fields are ‘read-only’ fields and that the user will not be allowed to modify them. If the fields have a ‘*’ at the beginning, such fields are mandatory fields. Such fields cannot be null or contain blanks. The ‘*’ is displayed as an indicator when the field is blank.

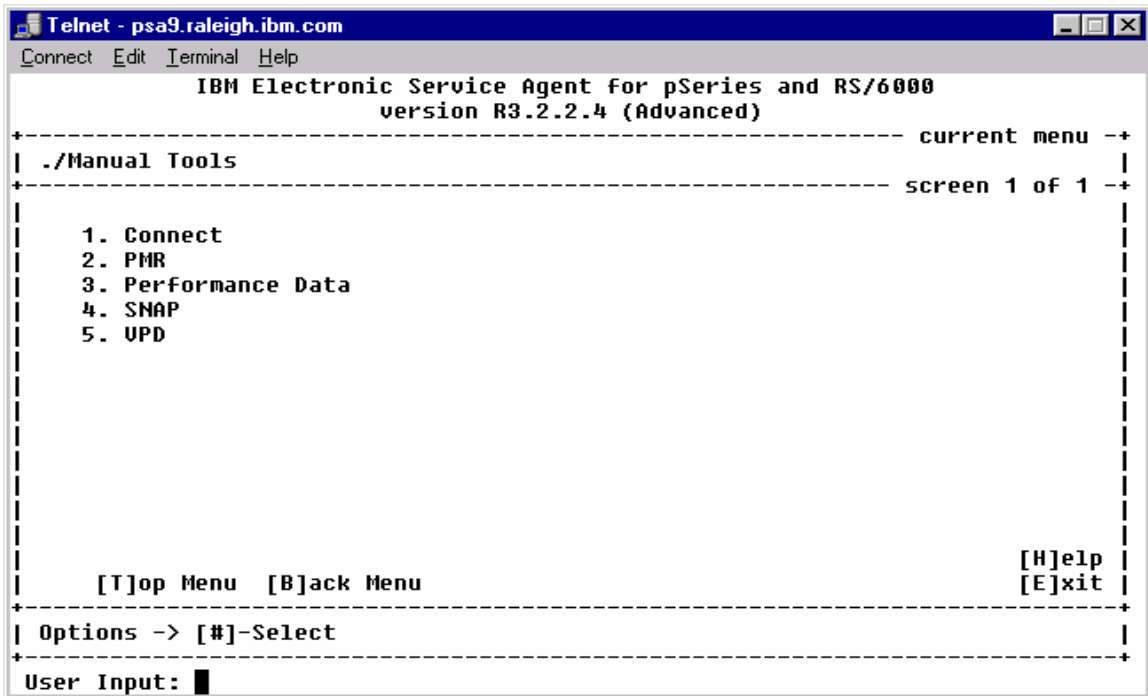
Machine template

To get to a machine information template, type 1 to select Network, and then type the number that selects the machine that you are interested in viewing. The information associated with that machine can be selected.

```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Advanced)
----- current menu --+
| ./Network/MACHINE - psa9.raleigh.ibm.com |
+----- screen 1 of 1 -----+
|
| 1. INFO of psa9.raleigh.ibm.com
| -----
| 2. Call Controller
| 3. Connection Manager - ConnectionManager (primary)
| 4. Folder - Data
| 5. Folder - Enrollment
| 6. Environment
| 7. Hardware Service Settings
| 8. Folder - PMRs
| 9. Performance Management
| 10. SNMP Trap Notification
| 11. Software Service Settings
|
| [T]op Menu [B]ack Menu [H]elp
| [E]xit
+-----+
| Options -> [#]-Select [A]-Add [D #]-Delete [R]-ErrEv [L]-License [I]-InErrs |
+-----+
User Input: █
```

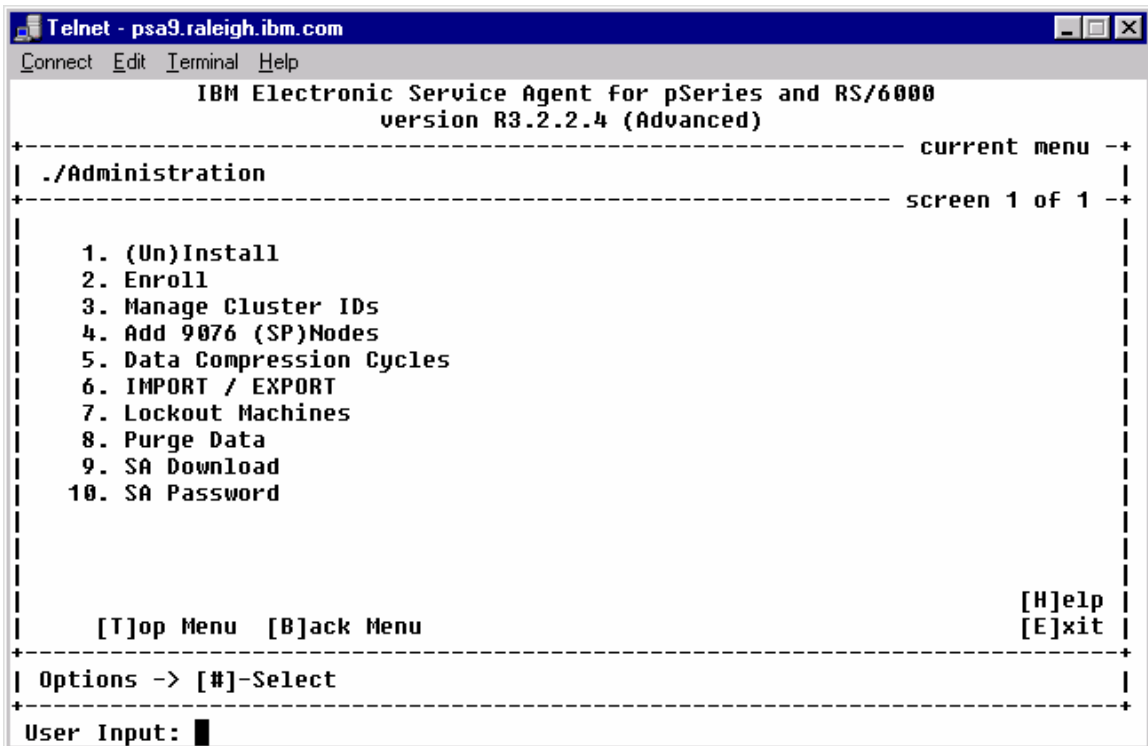
From the machine template, you can check the various options for that machine or add additional information to the template. You can check the Heart Beat and License status by typing **L** and pressing **Enter** key.

Manual Tools template



```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Advanced)
----- current menu --+
| ./Manual Tools |----- screen 1 of 1 --+
|
| 1. Connect
| 2. PMR
| 3. Performance Data
| 4. SNAP
| 5. UPD
|
| [T]op Menu [B]ack Menu [H]elp
| [E]xit
|-----
| Options -> [#]-Select
|-----
User Input: █
```

Administration template

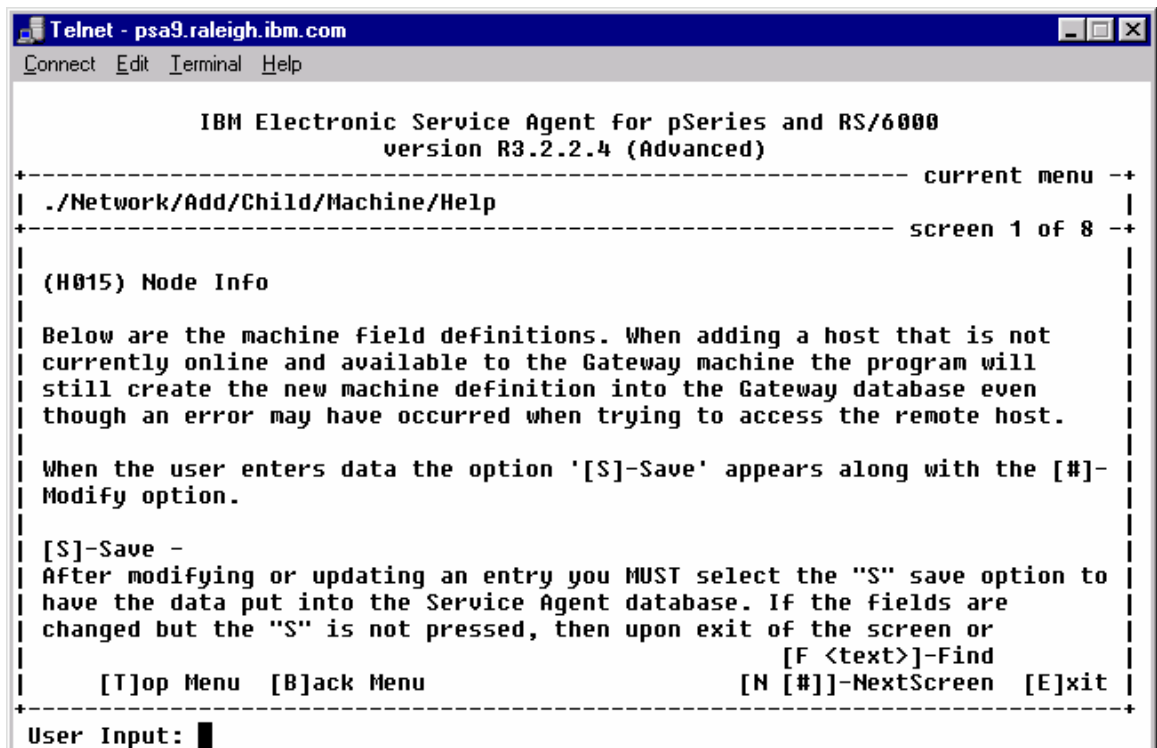


```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help
IBM Electronic Service Agent for pSeries and RS/6000
version R3.2.2.4 (Advanced)
----- current menu --+
| ./Administration |----- screen 1 of 1 --+
|
| 1. (Un)Install
| 2. Enroll
| 3. Manage Cluster IDs
| 4. Add 9076 (SP)Nodes
| 5. Data Compression Cycles
| 6. IMPORT / EXPORT
| 7. Lockout Machines
| 8. Purge Data
| 9. SA Download
| 10. SA Password
|
| [T]op Menu [B]ack Menu [H]elp
| [E]xit
|-----
| Options -> [#]-Select
|-----
User Input: █
```

Using Help

You can obtain descriptions of all the panels, options, parameters, and fields in the Help text.

Here is one of the help panels showing information about adding machine information after doing a Network - Add - Help selection.



```
Telnet - psa9.raleigh.ibm.com
Connect Edit Terminal Help

          IBM Electronic Service Agent for pSeries and RS/6000
          version R3.2.2.4 (Advanced)
----- current menu -----
| ./Network/Add/Child/Machine/Help |
----- screen 1 of 8 -----
|
| (H015) Node Info
|
| Below are the machine field definitions. When adding a host that is not
| currently online and available to the Gateway machine the program will
| still create the new machine definition into the Gateway database even
| though an error may have occurred when trying to access the remote host.
|
| When the user enters data the option '[S]-Save' appears along with the [#]-
| Modify option.
|
| [S]-Save -
| After modifying or updating an entry you MUST select the "S" save option to
| have the data put into the Service Agent database. If the fields are
| changed but the "S" is not pressed, then upon exit of the screen or
|                                     [F <text>]-Find
| [T]op Menu [B]ack Menu                [N [#]]-NextScreen [E]xit
-----
User Input: █
```

Appendix E - SNMP Notification Examples

Hardware Problem

Enterprise ibmSaNotifications (1.3.6.1.4.1.2.6.205) community public
generic trap:6 specific trap:2

Timestamp:1060369 Agentaddr:psa3.raleigh.ibm.com args(7):

[1] private.enterprises.ibm.ibmProd.205.2.1.0 (OctetString): Service Agent Call Placement Test

[2] private.enterprises.ibm.ibmProd.205.2.2.0 (OctetString): psa3.raleigh.ibm.com

[3] private.enterprises.ibm.ibmProd.205.2.3.0 (Integer): 2

[4] private.enterprises.ibm.ibmProd.205.2.4.0 (OctetString): 7026-B80_104A11F

[5] private.enterprises.ibm.ibmProd.205.2.5.0 (OctetString): disk0

[6] private.enterprises.ibm.ibmProd.205.2.6.0 (OctetString): pSeries Service Agent. Ver R3.3.0.0

[7] private.enterprises.ibm.ibmProd.205.2.7.0 (OctetString): AIX

Service Agent Internal Error

Enterprise ibmSaNotifications (1.3.6.1.4.1.2.6.205) community public
generic trap:6 specific trap:3

Timestamp:1082900 Agentaddr:psa3.raleigh.ibm.com args(4):

[1] private.enterprises.ibm.ibmProd.205.3.1.0 (OctetString): Enroll Failed - CONNECTIONPROBLEM -
Enroll

[2] private.enterprises.ibm.ibmProd.205.3.2.0 (OctetString): psa3.raleigh.ibm.com

[3] private.enterprises.ibm.ibmProd.205.1.6.0 (OctetString): pSeries Service Agent. Ver R3.3.0.0

[4] private.enterprises.ibm.ibmProd.205.1.7.0 (OctetString): AIX

Appendix F – List of Acronyms and Terms

Acronyms

Acronym	Definition
API	Application Program Interface
CE	Customer Engineer
DIP	p. 24
EED	Extended Error Data
ESS	Electronic Server System
FSP	Flexible Service Processor
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	High Availability
HMC	Hardware Management Console
HTTPS	Hypertext Transfer Protocol - Secure
HTTPS POST	Hypertext Transfer Protocol - Secure Program Operations Support Tool
IES	Inter-Enterprise Service
ISP	Internet Service Provider
LAN	Local Area Network
MIB	Management Information Block
MA	Maintenance Agreement
MA Expiry	Maintenance Agreement Expiration date
MTMS	Machine Type, Model, and Serial number
NAT	Network Address Translation
NLS	National Language Support
ODS	On Demand Server
PM	Performance Management
PMR	Problem Management Report
POST	p. 18
PPP	Point-To-Point Protocol
RETAIN	REmote Technical Assistance Information Network
RFS	Request For Service
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RPM	Redhat Package Manager
RSH/DSH	p. 34
SACM	Service Agent Connection Manager
SAUI	Advanced Service Agent User Interface
SDR	Service Data Receiver
SMIT	System Management Interface Tool
SNAP	System snapshot
SNMP	Simple Network Management Protocol

SOCKS	Software Common Knowledge IR System
SR	Service Request
SRC	System Resource Controller
SRN	Service Request Number
SSH	Secure SHell
SSR	Software Support Representative
SUMA	Service Update Management Assistant
TCP/IP	Transmission Control Protocol/Internet Protocol
TTY	Teletype
VPD	Vital Product Data
WAN	Wide Area Network

Terms

Service Agent Connection Manager (SACM)

The Service Agent Connection Manager (SACM) is a Java process, which runs on a designated system and manages connectivity to IBM. The SACM establishes a wide-area network (WAN) connection to IBM utilizing either an existing Internet connection or a modem attached to the TTY port of the system. The Service Agent gateway depends on the presence of the SACM in the environment for connectivity. The SACM can be installed on any eServer p5 or pSeries system in the target environment.

Service Agent gateway

The Service Agent gateway system is a designated system that contains the central database for a set of monitored machines (clients). The gateway controls the behavior of these clients through the Service Agent User Interface available to the system administrator. The gateway is responsible for initiating communication to IBM via the SACM and controls the flow of data sent to IBM.

Service Agent Client

A Service Agent Client (Client) is a machine that is monitored by a Service Agent gateway.

Enrollment

All monitored machines are enrolled with IBM using the machine type, model and serial number (MTMS). This enrollment is required to initiate the monitoring process and for security entitlement at IBM.

Resource filters

Resource filters allow you to specify that certain devices not be monitored by IBM. Resource filters are used to suppress submission of data from an IBM or non-IBM device that is not covered under warranty or a maintenance agreement (MA).

Thresholds

Thresholds are filters that can be applied to specific detected errors that can supersede the internal Service Agent error detection thresholds.

Heartbeat

Heartbeat transaction assures that each monitored machine is active. When the heartbeat function fails, the condition is NOT reported to IBM. Users can set up an E-mail Alert for notification of missing heartbeats.

Vital Product Data (VPD)

Vital Product Data (VPD) is the information Service Agent gathers, stores, and sends to IBM. The information gathered from this monitoring function is used for purposes of problem determination, assisting you with performance and capacity planning, assisting IBM to enhance IBM products and services, and notifying you of your system status and the solutions we have available.

Extended Error Data (EED)

Extended Error Data (EED) is additional information Service Agent gathers, stores, and then sends to IBM. IBM support uses extended error data for additional analysis of the fault condition. Service Agent transfers this data from your site to IBM and a reference to the data is placed in the call record.

Hardware Management Console

The Hardware Management Console (HMC) allows control of many hardware management tasks for your pSeries servers, including configuring logical and affinity partitions. In this environment, the HMC also does hardware data capture and additional data collection normally done by SA. The HMC performs problem collection and call home communications function via the modem attached to it.

Java RMI

gateway to Client (monitored machine) communication utilizes Java Remote Method Invocation (RMI). RMI allows one to write distributed objects using Java. At the most basic level, RMI is Java's Remote Procedure Call (RPC) mechanism.

Appendix G - Notices and Trademarks

Notices

IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could contain technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM international Program License Agreement or any equivalent agreement between us.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

IBM
RS/6000
Electronic Service Agent

Microsoft, Windows and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems

Other company, product, and service names may be trademarks or service marks of others.

Index

- Accessing Service Agent from a PC, 123
- Activating service Agent, 37
- Advanced Configuration panel, 57
- Advanced UI Details
 - (Un) Install Template, 110
 - Add 9076 (SP) Nodes template, 112
 - Add button from Network folder, 90
 - Adding additional system information using forms, 91
 - Additional Machine Templates, 105
 - Alert Template Properties, 116
 - Available Forms, 92
 - Available Threshold Properties, 93
 - Call Controller Template, 107
 - Call Log Properties, 108
 - CallController Properties, 95
 - Client Machines Folder, 107
 - Connect Template, 118
 - Connection Manager Properties, 96
 - Data Compression Cycles Template, 112
 - Data Folder, 99
 - Department Properties, 91
 - Dialer Template Properties, 97
 - E-mail Alert Properties, 106
 - Enroll Template, 109
 - Enrollment Folder, 99
 - Environment Template, 98
 - Hardware Service Properties, 99
 - Import / Export Template, 113
 - Lockout Machines Template, 114
 - Manage Cluster IDs Properties, 111
 - Network Properties, 89
 - Node Info Properties, 92
 - Performance Data Template, 119
 - Performance Manager Template Properties, 103
 - PMR Template, 119
 - PMR Template Properties, 101
 - Purge Data Template, 114
 - Resource Filter Properties, 116
 - SA Access Template, 115
 - Send VPD Template, 121
 - SNAP Template, 120
 - SNMP Notification Template Properties, 104
 - Software Service Template Properties, 104

- Test E-mail, 122
- Test PMR, 122
- Test SNMPTrap, 122
- Thresholds Template, 117
- Advanced User Interface
 - Accessing, 54
 - Basic data entry, 56
 - Category Selectors, 59
 - Configuration panel, 57
 - Detail Viewing Pane, 59
 - Heartbeat status, 64
 - View error events, 60
 - View licensing information, 63
 - View Service Agent internal errors, 62
 - View/Edit properties, 59
- ASCII User Interfaces, 125
- Basic UI Details
 - Call Controller Properties, 83
 - Call Log Properties, 87
 - Connect Properties, 86
 - Connection Manager Properties, 84
 - Dialer Properties, 85
 - Enroll Properties, 86
 - Error Log Properties, 87
 - Gateway Properties, 82
 - Network Properties, 81
- Basic User Interface, 47
 - Accessing, 44
 - CallController Properties, 49
 - CallLog Properties, 53
 - ConnectionManager Properties, 50
 - Dialer Properties, 51
 - Enroll Properties, 52
 - Gateway Properties, 48
 - Network Properties, 47
- Electronic Server System (ESS) process, 15
- Getting Service Agent
 - from the ftp.software.ibm.com site using FTP, 29
 - from the ftp.software.ibm.com site using your browser, 28
 - from the IBM Electronic Services Web site using your browser, 28
- Hardware Inventory Collection / VPD, 11
- Heartbeat status, 64
- How to
 - add a machine, 70
 - add an e-mail address for a monitored client, 72
 - add an e-mail Alert, 74

- add an SNMP Notification, 73
- add SP Nodes, 69
- change connection manager listening port, 68
- clear pending requests to IBM, 78
- configure for Performance Management, 73
- control dispatching for a machine supported by a different branch office, 70
- create a department of monitored machines, 68
- define resource filters, 72
- determine your Service Agent version, 77
- install Service Agent code only on a monitored machine, 71
- lock out Service Agent on a machine, 10, 74
- manually transmit Vital Product Data (VPD) to IBM, 77
- remove a machine, 75
- remove all nodes from a 9076 (SP), 75
- remove an SNMP Notification, 75
- remove Cluster details, 76
- remove Service Agent code only from a monitored machine, 75
- send a test e-mail, 76
- send a test PMR to IBM, 76
- send a test SNMP Notification, 77
- send Performance Management Data, 73
- set up a master gateway, 67
- set up a slave gateway, 67
- set up SA CM to use Dialer, 66
- set up SA to use an Internet connection, 66
- set up to a remote Connection Manager, 67
- specify Cluster details, 71
- specify the physical location of a machine, 71
- specify thresholds, 72
- IBM modem, setting up for Service Agent, 23, 25
- Installing Service Agent Code Manually, 34
- Installing Service Agent from a command line, 31
- Installing Service Agent from SMIT, 30
- installp faults, 33
- Modem communication steps, 23
- On Demand Server (ODS) process, 16
- Performance Management (PM/AIX), 11
- Planning, 19
- Prerequisites, 22
- RETAIN connection, 22
- SecureSHell (SSH), 31
- Service Agent Connection Manager (SACM), 141
 - Process, 17
- Simple Network Management Protocol Support (SNMP), 11
- SNMP Notification Examples, 139
- View Error Events, 60

View Licensing Information, 63
View Service Agent Internal Errors, 62
View/Edit Properties, 59