

SeeBeyond ICAN Suite

e*Gate Integrator SNMP Agent User's Guide

Release 5.0.5 for Schema Run-time Environment (SRE)



The information contained in this document is subject to change and is updated periodically to reflect changes to the applicable software. Although every effort has been made to ensure the accuracy of this document, SeeBeyond Technology Corporation (SeeBeyond) assumes no responsibility for any errors that may appear herein. The software described in this document is furnished under a License Agreement and may be used or copied only in accordance with the terms of such License Agreement. Printing, copying, or reproducing this document in any fashion is prohibited except in accordance with the License Agreement. The contents of this document are designated as being confidential and proprietary; are considered to be trade secrets of SeeBeyond; and may be used only in accordance with the License Agreement, as protected and enforceable by law. SeeBeyond assumes no responsibility for the use or reliability of its software on platforms that are not supported by SeeBeyond.

SeeBeyond, e*Gate, e*Way, and e*Xchange are the registered trademarks of SeeBeyond Technology Corporation in the United States and/or select foreign countries. The SeeBeyond logo, SeeBeyond Integrated Composite Application Network Suite, eGate, eWay, eInsight, eVision, eXchange, eView, eIndex, eTL, ePortal, eBAM, and e*Insight are trademarks of SeeBeyond Technology Corporation. The absence of a trademark from this list does not constitute a waiver of SeeBeyond Technology Corporation's intellectual property rights concerning that trademark. This document may contain references to other company, brand, and product names. These company, brand, and product names are used herein for identification purposes only and may be the trademarks of their respective owners.

© 2005 SeeBeyond Technology Corporation. All Rights Reserved. This work is protected as an unpublished work under the copyright laws.

This work is confidential and proprietary information of SeeBeyond and must be maintained in strict confidence.

Version 20051011102147.

Contents

Chapter 1

Introduction	5
Contents of This Guide	5
SeeBeyond Web Site	6
Supported Operating Systems	6

Chapter 2

Using SNMP to Manage e*Gate Schemas	7
The e*Gate SNMP Agent Model	7
About e*Gate SNMP Model Configurations	9
About the e*Gate MIB	10
Quick Start	11

Chapter 3

Installing the SNMP Agent	12
System Requirements	12
Installing the e*Gate SNMP Agent on Windows	12
Installing the Windows SNMP Service	12
Installing the e*Gate SNMP Agent	13
Installing the e*Gate SNMP Agent on UNIX	16

Chapter 4

Configuring e*Gate Schemas for SNMP Management	19
Creating SNMP Agent Components	19
Configuring SNMP Agent Components	20
Configuring Control Broker Notification Routing	22

Chapter 5

Managing e*Gate SNMP Agents	25
Managing the e*Gate SNMP Agent on Windows	25
Starting the e*Gate SNMP Agent	25
Configuring the e*Gate SNMP Startup Options	25
Stopping the e*Gate SNMP Agent	26
Enabling Logging	27
Specifying Communities	27
Managing the e*Gate SNMP Agent on UNIX	28
Starting the e*Gate SNMP Agent	28
Stopping the e*Gate SNMP Agent	28
Displaying the e*Gate SNMP Agent's Communities	29
Setting Up Communities	29
Enabling Logging	30
Reconfiguring Existing SNMP Agents	30
Changing the CB Port Number	31
Changing the Control Broker Wait Interval (CB Timer)	31
Changing the MIB II, STC, or SNMP Port Number	32
Changing the Trap Delimiter	32

Chapter 6

The e*Gate MIB	33
About the e*Gate MIB	33
e*Gate Managed Objects	34
e*Gate Trap Definitions	38

Chapter 7

Troubleshooting	43
Index	44

Introduction

This user guide describes how to install, configure, and use the e*Gate SNMP (Simple Network Management Protocol) Agent to monitor e*Gate schemas. This guide is intended for system administrators of e*Gate Integrator and SNMP management systems. This guide assumes that you are familiar with SNMP terminology and technology.

In This Chapter

- [“Contents of This Guide” on page 5](#)
- [“SeeBeyond Web Site” on page 6](#)
- [“Supported Operating Systems” on page 6](#)

1.1 Contents of This Guide

This guide provides the following information:

- [Chapter 1, “Introduction” on page 5](#) provides an overview of this guide, its contents, and writing conventions.
- [Chapter 2, “Using SNMP to Manage e*Gate Schemas” on page 7](#) describes the e*Gate SNMP Agent architecture and Management Information Database (MIB). This chapter also provides a “quick start” procedure.
- [Chapter 3, “Installing the SNMP Agent” on page 12](#) describes how to install the e*Gate SNMP Agent on Windows or UNIX.
- [Chapter 4, “Configuring e*Gate Schemas for SNMP Management” on page 19](#) describes how to configure e*Gate schemas to be monitored by the SNMP Agent.
- [Chapter 5, “Managing e*Gate SNMP Agents” on page 25](#) describes how to manage the e*Gate SNMP Agent, such as starting and stopping the SNMP Agent, and setting up communities for security. This chapter also describes how to reconfigure existing an SNMP Agent.
- [Chapter 6, “The e*Gate MIB” on page 33](#) provides details about the managed objects and trap notifications in the e*Gate MIB.
- [Chapter 7, “Troubleshooting” on page 43](#) provides guidelines for troubleshooting the SNMP Agent.

1.2 SeeBeyond Web Site

The SeeBeyond Web site is your best source for up-to-the-minute product news and technical support information. The site's URL is:

<http://www.seebeyond.com>

1.3 Supported Operating Systems

The e*Gate SNMP Agent is available for the following operating systems:

- Windows 2000, Windows XP, and Windows Server 2003
- HP Tru64 V5.1A
- HP-UX 11.0 and 11i (PA-RISC)
- IBM AIX 5L, version 5.1, 5.2, and 5.3
- Sun Solaris 8 and 9
- Japanese Windows 2000, Windows XP, and Windows Server 2003
- Japanese HP-UX 11.0 and 11i (PA-RISC)
- Japanese IBM AIX 5L, version 5.1, 5.2, and 5.3
- Japanese Sun Solaris 8 and 9

Note: *SeeBeyond only supports HP-UX running on 9000/8xx machines. 9000/800 is 64 bits, but can also run in 32 bit mode. To determine if the system is 32 or 64 bits, type: `getconf KERNEL_BITS`. This returns either 32 or 64.*

Using SNMP to Manage e*Gate Schemas

The e*Gate SNMP Agent enables you to manage e*Gate schemas using third-party SNMP management systems.

This chapter provides an architectural overview of the e*Gate SNMP Agent and its MIB. This chapter also includes a “quick start” procedure that provides a high-level overview of the steps you need to take to monitor e*Gate schemas using SNMP.

In This Chapter

- [“The e*Gate SNMP Agent Model” on page 7](#)
- [“About e*Gate SNMP Model Configurations” on page 9](#)
- [“About the e*Gate MIB” on page 10](#)
- [“Quick Start” on page 11](#)

2.1 The e*Gate SNMP Agent Model

The e*Gate SNMP Agent enables you to configure a third-party SNMP management system to monitor deployed e*Gate schemas running on Participating Hosts.

The SNMP Agent model includes the following components which enable the SNMP management system to send requests and receive responses and notification traps when a specified event occurs:

- **Control Broker**
This is the schema component that monitors and manages all other schema components such as e*Ways, IQ Managers, and Collaborations.
- **SNMP Agent component**
This is a schema component that must be added to a schema if it is to be monitored by the SNMP Agent. The SNMP Agent component defines the Control Broker wait interval, the user name, and the port through which the Control Broker and the e*Gate SNMP Agent communicate.
- **e*Gate SNMP Agent**
This is the Windows service or UNIX daemon through which the e*Gate schema and the SNMP management system communicate. The SNMP Agent includes the e*Gate MIB. This database defines the schema components that can be monitored as managed objects. The database also defines the trap notifications that the SNMP

management system can expect to receive for the managed objects. For more information about the e*Gate MIB, refer to **“About the e*Gate MIB” on page 10.**

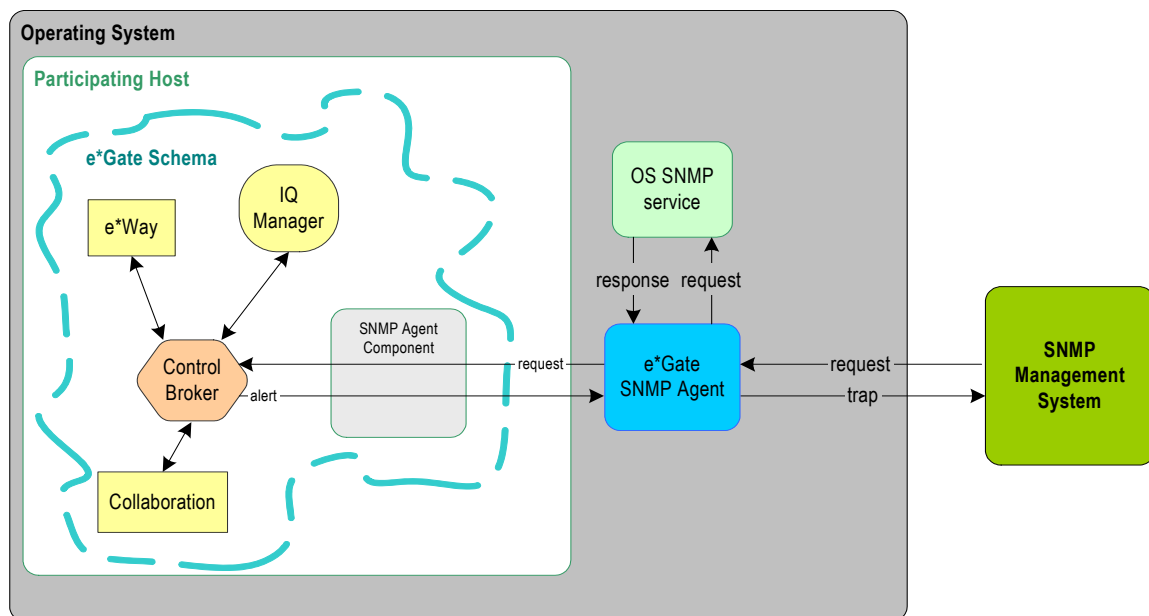
▪ **Operating system SNMP service**

Both UNIX and Windows systems provide operating system SNMP services. To run the e*Gate SNMP Agent on Windows, the Windows OS SNMP service must be installed. The e*Gate SNMP Agent uses the same community configurations as the Windows SNMP service. For information, refer to **“Installing the Windows SNMP Service” on page 12.**

On UNIX, installing the UNIX SNMP daemon is optional. If it is installed, the e*Gate SNMP Agent attempts to parse the OS SNMP configuration file and use its community settings. You can also define the communities for the e*Gate SNMP Agent in case the OS SNMP configuration file cannot be parsed or located. For information, refer to **“Setting Up Communities” on page 29.**

The diagram below shows the components in the e*Gate SNMP Agent model:

Figure 1 The e*Gate SNMP Agent Model



As Figure 1 shows, the e*Gate SNMP Agent communicates with the Control Broker using configuration settings set up on the SNMP Agent component, which is a schema component. The Control Broker monitors the status of its schema components such as e*Ways, IQ Managers and Collaborations.

If an event is detected, for example, if an e*Way is down, the Control Broker forwards the alert to the e*Gate SNMP Agent. The SNMP Agent then sends a trap notification to the SNMP management system via trap port 162.

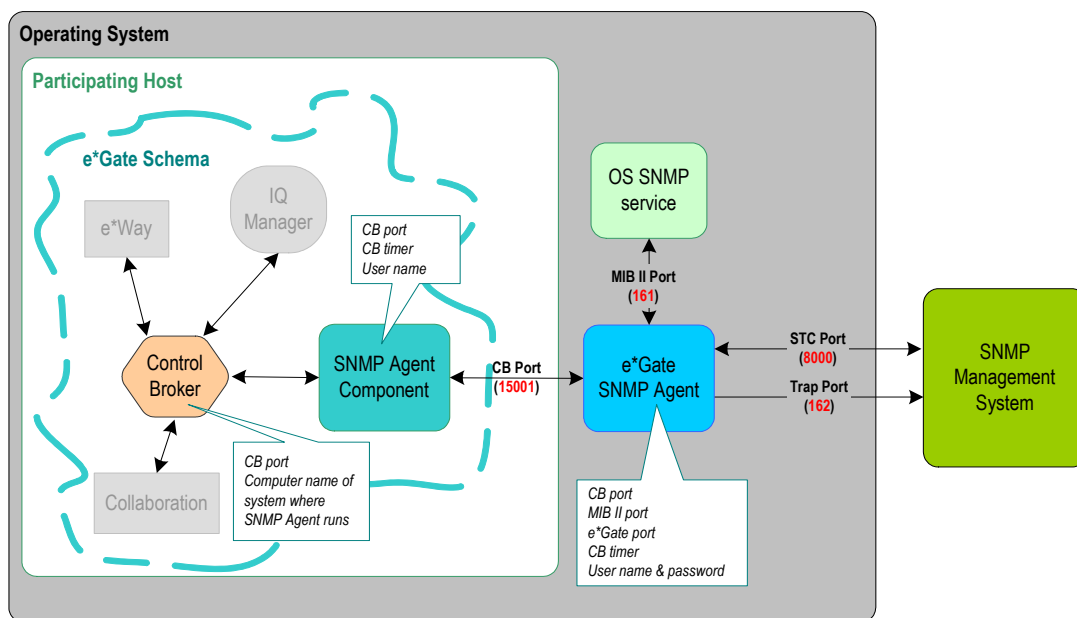
The SNMP management system sends requests directly to the e*Gate SNMP Agent. When the SNMP Agent receives a request (such as restart a down e*Way), it forwards the request to the Control Broker. The Control Broker then restarts the e*Way.

Alternatively, the SNMP management system can send requests to the e*Gate SNMP Agent to search the OS SNMP MIB. The SNMP Agent forwards those requests to the OS SNMP service or daemon.

2.2 About e*Gate SNMP Model Configurations

The components in the e*Gate SNMP model communicate with each other via port configurations. The diagram below shows the names of the ports and the default port number in red in parentheses. For each component, the diagram shows which configurations you must specify.

Figure 2 e*Gate SNMP Component Configurations



The diagram above shows the three ports that are used in the e*Gate SNMP model:

- CB port**
 This is the port where the Control Broker in the e*Gate schema listens for requests forwarded by the e*Gate SNMP Agent. This is also the port where the Control Broker forwards responses and alerts to the e*Gate SNMP Agent.
- STC port**
 This is the port where the e*Gate SNMP Agent listens for requests from the SNMP management system, and also where the e*Gate SNMP Agent forwards responses to the SNMP management system. This port is also referred to as the SNMP port on UNIX and in the e*Gate SNMP Agent configuration file.
- Trap port**
 This is the port where the e*Gate SNMP Agent forwards trap notifications. This port is set to 162 and cannot be changed.

- **MIB II port**
This is the port where the e*Gate SNMP Agent forwards requests from the SNMP management system to search the OS SNMP MIB. The OS SNMP service sends responses to this port, which the e*Gate SNMP Agent then forwards on to the SNMP management system. This enables the SNMP management system to manage the OS SNMP service via the e*Gate SNMP Agent rather than another SNMP configuration to work with the OS SNMP service.

For each e*Gate SNMP model component, the diagram shows the configurations you set up:

- **Control Broker**
For the Control Broker, you specify the CB port number and the computer name of the system where the e*Gate SNMP Agent runs. This can be a remote system. You set these configurations in the e*Gate schema in the Control Broker Notification script as described in [“Configuring Control Broker Notification Routing” on page 22](#).
- **e*Gate SNMP Component**
This component’s function is to enable you to specify additional configurations for the Control Broker. For this component, you specify the CB port, the CB timer, and the user name used to authorize with the Control Broker. The CB timer is the wait interval for the SNMP Agent to wait before finding the Control Broker unresponsive. You specify these configurations after you have created the e*Gate SNMP component for the schema you want the SNMP management system to manage. For information, refer to [“Configuring SNMP Agent Components” on page 20](#).
- **e*Gate SNMP Agent**
For the SNMP Agent, you specify all ports, the CB timer, and the user name and password to authorize with the Control Broker. You specify these configurations during the installation process of the SNMP Agent as described in [“Installing the SNMP Agent” on page 12](#).

2.3 About the e*Gate MIB

The e*Gate SNMP Agent provides the e*Gate MIB which defines the e*Gate trap notifications as well as the objects that can be managed in e*Gate schemas. The e*Gate MIB uses Abstract Syntax Notation One (ANS.1), which is industry standard for MIBs.

The e*Gate MIB, `stc_mib.txt`, is located in the `<eGate\client>\bin` directory, where `<eGate\client>` is the directory where you installed e*Gate Participating Host.

The e*Gate MIB objects can be found under the following node:

1.3.6.9.4.1.1351.1.1.1

For details about the e*Gate MIB objects and traps, refer to [Chapter 6, “The e*Gate MIB” on page 33](#).

2.4 Quick Start

The following is a broad overview of the steps to be taken to monitor an e*Gate schema with the e*Gate SNMP Agent:

- 1 Install the Windows SNMP service if you are installing the SNMP Agent on Windows and the Windows SNMP service is not present. For information, refer to [“Installing the Windows SNMP Service” on page 12](#).
- 2 Install the e*Gate SNMP Agent. You can install the SNMP Agent on the system that hosts the Participating Host where the schema runs that it will be monitoring, or you can have it monitor schemas remotely. For information, refer to [Chapter 3, “Installing the SNMP Agent” on page 12](#).
- 3 Add an SNMP Agent component to the e*Gate schema under the Participating Host in the e*Gate Schema Designer. The SNMP Agent component defines the Control Broker wait interval, the user name, and the port through which the Control Broker and the e*Gate SNMP Agent communicate. For information, refer to [“Creating SNMP Agent Components” on page 19](#).
- 4 In the Schema Designer, configure the Control Broker Notification script to indicate to the Control Broker on which local or remote system the SNMP Agent resides and which port to use to communicate with the SNMP Agent. For information, refer to [“Configuring Control Broker Notification Routing” on page 22](#).
- 5 Load the e*Gate MIB into the third-party SNMP management system.
- 6 If necessary, define the community information for the SNMP Agent. For information, refer to [“Managing e*Gate SNMP Agents” on page 25](#).
- 7 Start the schema and start the e*Gate SNMP Agent as described in [“Managing e*Gate SNMP Agents” on page 25](#).

Installing the SNMP Agent

This chapter describes how to install the e*Gate SNMP Agent on Windows and UNIX systems. The e*Gate SNMP Agent is installed as an e*Gate Integrator add-on.

In This Chapter

- [“System Requirements” on page 12](#)
- [“Installing the e*Gate SNMP Agent on Windows” on page 12](#)
- [“Installing the e*Gate SNMP Agent on UNIX” on page 16](#)

3.1 System Requirements

To use the e*Gate SNMP Agent, you need the following:

- An e*Gate Participating Host, version 5.0 SRE or later.
- The e*Gate Registry (which need not be located on the same system where the SNMP Agent resides).
- A TCP/IP network connection.
- At least 16 MB of free disk space and at least 8 MB of memory.

3.2 Installing the e*Gate SNMP Agent on Windows

This section describes how to install the SNMP Agent on a system that runs Windows 2000. The SNMP Agent runs as a standard Windows service in conjunction with the Windows operating system SNMP service.

3.2.1 Installing the Windows SNMP Service

Before you install the e*Gate SNMP Agent, the Windows SNMP service must be installed. If it is not installed, follow the procedure below.

The e*Gate SNMP Agent uses the same community settings as the Windows SNMP service. When you configure the e*Gate SNMP Agent, you define the MIB II port for the SNMP Agent to forward requests to the Windows SNMP service. This allows the SNMP management system to search the Windows operating system MIB. For

information about port configurations, refer to [“About e*Gate SNMP Model Configurations” on page 9.](#)

To install the Windows SNMP service

- 1 In the Windows Control Panel, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
- 2 Click **Management and Monitoring Tools** and click **Details**.
- 3 Select **Simple Network Management Protocol**, click **OK**, and click **Next**.

It is advisable to set up communities for the Windows SNMP service for security reasons. The e*Gate SNNMP Agent adopts the same communities as those set for the Windows SNMP service.

3.2.2 Installing the e*Gate SNMP Agent

You can install the e*Gate SNMP Agent on the system with the Participating Host with the e*Gate schema to be monitored—or you can install the SNMP Agent on any other system and monitor e*Gate schemas remotely.

For an SNMP management system to be able to manage an e*Gate schema via the SNMP Agent, the schema must be configured for SNMP monitoring. For information, refer to [“Configuring e*Gate Schemas for SNMP Management” on page 19.](#)

The SNMP Agent installation installs the following files in the `<eGate\client>\bin` directory, where `<eGate\client>` is the directory where the e*Gate Participating Host is located:

Table 1 e*Gate SNMP Agent Files (Windows)

File	Description
stcsnmpa.exe	The e*Gate SNMP Agent. This runs as a Windows service.
javai.dll	e*Gate DLL to support the e*Gate SNMP Agent.
stc_mib.txt	The e*Gate MIB. For information, refer to “About the e*Gate MIB” on page 10.
stcsnmpa.conf	The configuration file for the e*Gate SNMP Agent. For information, refer to “Managing the e*Gate SNMP Agent on Windows” on page 25.

The SNMP Agent installation also installed the file **snmpagent.jar** in the `<eGate\client>\classes` directory, where `<eGate\client>` is the directory where the e*Gate Participating Host is located.

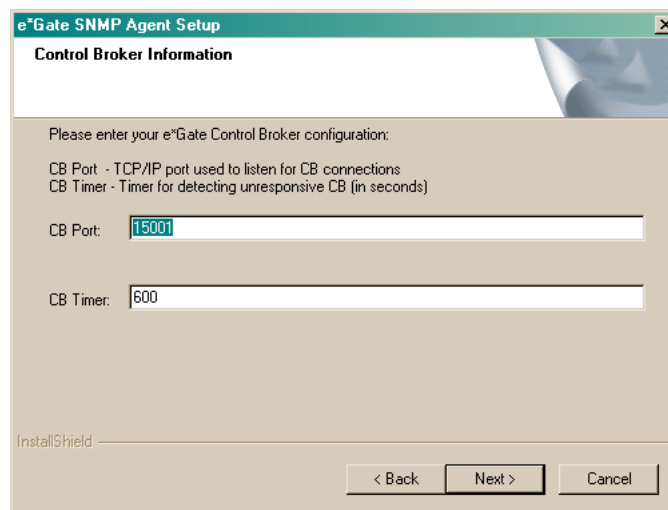
After installing the SNMP Agent and configuring the e*Gate schema, you load the e*Gate MIB into the SNMP management system. You can then start the SNMP Agent, which runs as a standard Windows service. For information, refer to [“Starting the e*Gate SNMP Agent” on page 25.](#)

To install the e*Gate SNMP Agent on Windows

- 1 Close all Windows applications, including any anti-virus applications, and stop all e*Gate services.
- 2 Follow the instructions for installing add-ons in the *e*Gate Integrator Installation Guide*.
- 3 From the list of available add-ons, select **SNMP Agent**, and click **Next**.
- 4 Follow the on-screen instructions.

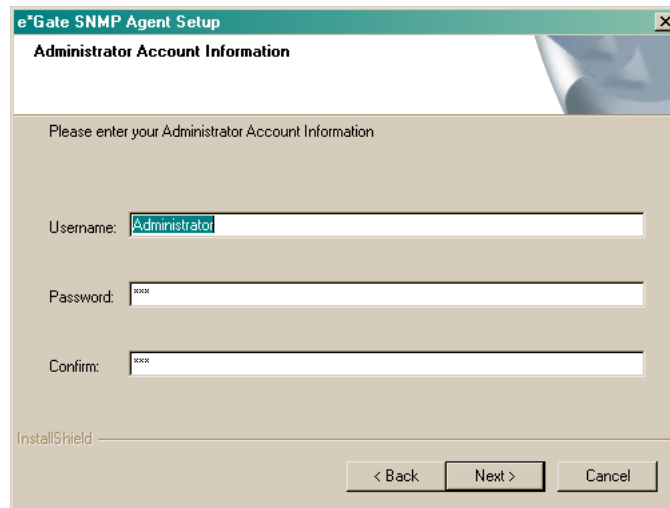
After the files are copied, the **Control Broker Information** dialog box appears as shown below.

Figure 3 Control Broker Information Dialog Box



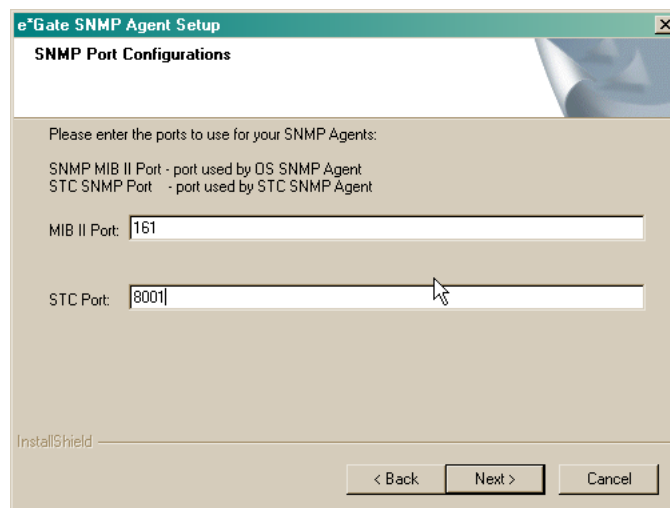
- 5 In the **CB Port** box, enter the number for the TCP/IP port that the e*Gate SNMP Agent uses to listen for Control Broker alerts and responses. This port must be a unique number not used by any other service. The default is 15001.
After the installation, you must specify this same port number for the e*Gate SNMP Agent component and the Control Broker Notification script as described in [Chapter 4](#).
- 6 In the **CB Timer** box, enter the number of seconds for the SNMP Agent to wait for a response from the Control Broker before considering the connection unresponsive. The default is 600 seconds (10 minutes).
After the installation, you must specify this the same wait interval for the e*Gate SNMP Agent component as described in [Chapter 4](#).
- 7 Click **Next**. The **Administrator Account Information** dialog box appears.

Figure 4 Administrator Account Information Dialog Box



- 8 Enter the user name and the password to authenticate with the Control Broker. Enter the password twice (both entries must be identical) and click **Next**. The **SNMP Port Configuration** dialog box appears.

Figure 5 SNMP Port Configuration Dialog Box



- 9 In the **MIB II Port** box, enter the number for the port where the e*Gate SNMP forwards requests from the SNMP management system under the MIB II subtree to the OS SNMP service. This enables the SNMP management system to send requests to search the OS SNMP service MIB via the e*Gate SNMP Agent. For Windows, the OS SNMP service must be present to run the e*Gate SNMP Agent. UNIX does not require the presence of the UNIX SNMP daemon. For more information, refer to **"Installing the Windows SNMP Service" on page 12**.

The default port number is 161. Unless you have specifically changed this port number in your operating system, do not change the default value.

- 10 In the **STC Port** box, enter the number for the port where the e*Gate SNMP Agent forwards responses to the SNMP management system. This is also the port where

the e*Gate SNMP Agent listens for requests from the SNMP management system. This port must be a unique number not used by any other service. The default port number is 8000.

11 Follow the on-screen instructions to complete the rest of the installation.

After the installation, you must modify the schema to be monitored by the e*Gate SNMP Agent in the Schema Designer. For a schema to be monitored, you must create an e*Gate SNMP Agent component in your schema and modify the Control Broker Notification Routing script as described in [Chapter 4, “Configuring e*Gate Schemas for SNMP Management” on page 19](#).

Once you have configured the schema for SNMP monitoring and are ready to run and monitor the schema, you must manually start the SNMP Agent as described in [“Starting the e*Gate SNMP Agent” on page 25](#). The e*Gate SNMP Agent installation configures the e*Gate SNMP Agent as a “manual” service; you must start the service manually before Windows can load it.

3.3 Installing the e*Gate SNMP Agent on UNIX

This section describes how you install the SNMP Agent on a UNIX system.

If you are installing the SNMP Agent on a system that hosts other e*Gate components, install the e*Gate Registry and Participating Host under a non-root account.

You can install the e*Gate SNMP Agent on a system with the Participating Host with the e*Gate schema to be monitored—or you can install the SNMP Agent on any other system and monitor e*Gate schemas remotely.

For an SNMP management system to be able to manage an e*Gate schema via the SNMP Agent, the schema must be configured for SNMP monitoring. For information, refer to [“Configuring e*Gate Schemas for SNMP Management” on page 19](#).

The SNMP Agent installation installs the following files in the `<eGate/client>/bin` directory, where `<eGate/client>` is the directory where the e*Gate Participating Host is located:

Table 2 e*Gate SNMP Agent Files (UNIX)

File	Description
<code>stc_mib.txt</code>	The e*Gate MIB. For information, refer to “About the e*Gate MIB” on page 10 .
<code>stcsnmpa.conf</code>	The configuration file for the e*Gate SNMP Agent. For information, refer to “Managing the e*Gate SNMP Agent on Windows” on page 25 .

The SNMP Agent installation installs the e*Gate SNMP Agent application as the shell script `S99stcsnmpdx`, which starts the SNMP Agent as a daemon, in the following directories depending on the type of UNIX system you are using:

Table 3 e*Gate SNMP Agent Shell Script Location

Platform	Directory
Solaris	/etc/rc3.d
UNIX	/sbin/rc3.d
AIX	/etc

The SNMP Agent installation also installed the file **snmpagent.jar** in the *<eGate/client>/classes* directory, where *<eGate/client>* is the directory where the e*Gate Participating Host is located.

After installing the SNMP Agent and configuring the e*Gate schema, you load the e*Gate MIB into the SNMP management system. You can then start the SNMP Agent, which runs as a UNIX daemon. For information, refer to [“Managing the e*Gate SNMP Agent on UNIX” on page 28](#).

To install the e*Gate SNMP Agent on UNIX

- 1 Verify that you are logged in as the **root** user.
- 1 Stop all e*Gate services.
- 2 Follow the instructions for installing add-ons in the *e*Gate Integrator Installation Guide*.
- 3 From the list of available add-ons, select **Agents**. Press **Enter** to begin installation and then follow the on-screen instructions.

After the files are copied, enter the information to configure the SNMP Agent’s properties.

- 4 Enter the port number for the OS SNMP service. The e*Gate SNMP Agent forwards requests to the OS SNMP service through this port. The default is 161. **Unless you have specifically changed this port number in your operating system, do not alter the default value.**

```
Please enter your SNMP MIB II port. This is the port your OS SNMP
agent will listen to for incoming requests.
SNMP II MIB Port [161]:
```

- 5 Enter the port number of the port on which the e*Gate SNMP Agent listens for requests from the SNMP manager. This port must be a unique number not used by any other service. The default is 8000.

```
Please enter your e*Gate SNMP port. This is the port used by the
e*Gate SNMP agent.
e*Gate SNMP Port [8000]:
```

The installation verifies if the port is available. If the port is in use, you are prompted for another port number. If you are using Solaris with the Network Information Service (NIS), you must register the e*Gate SNMP port.

Note: This port is referred to as the STC port in this guide and for Windows installations.

- 6 Enter the port number for the port that the e*Gate SNMP Agent uses to communicate with the Control Broker. The default is 15001.

```
Please enter the TCP/IP port used to listen for Control Broker
connections
CB Port [15001]:
```

- 7 Enter the timer the e*Gate SNMP Agent uses for detecting an unresponsive Control Broker, if no connection has been made during that time.

```
Please enter the timer for detecting unresponsive Control Broker
(in seconds)
CB Timer [600]:
```

- 8 Enter the location of the Java Runtime Environment (JRE).

```
Please enter the location of your Java Runtime Environment (JRE)
JRE Home directory [/opt/java/jre]:
```

- 9 Follow the on-screen instructions to complete the rest of the installation.

After the installation, you must modify the schema to be monitored by the e*Gate SNMP Agent in the Schema Designer. For a schema to be monitored, you must create an e*Gate SNMP Agent component in your schema and modify the Control Broker Notification Routing script as described in [Chapter 4, “Configuring e*Gate Schemas for SNMP Management” on page 19](#).

Once you have configured the schema for SNMP monitoring and are ready to run and monitor the schema, you must manually start the SNMP Agent as described in [“Starting the e*Gate SNMP Agent” on page 28](#). The e*Gate SNMP Agent installation configures the e*Gate SNMP Agent as a “manual” daemon; you must start the daemon manually before UNIX can load it.

Configuring e*Gate Schemas for SNMP Management

For an SNMP management system to be able to manage an e*Gate schema via the e*Gate SNMP Agent, the schema must be configured for SNMP monitoring. To enable a schema for SNMP monitoring, you create and configure an e*Gate SNMP schema component, and configure the Control Broker to forward and receive SNMP messages.

This chapter describes how to create and configure the e*Gate SNMP Agent component and how you edit the Control Broker Notification script. The Control Broker Notification script indicates to the Control Broker on which system the SNMP Agent runs and which port to use for SNMP notifications.

In This Chapter

- [“Creating SNMP Agent Components” on page 19](#)
- [“Configuring SNMP Agent Components” on page 20](#)
- [“Configuring Control Broker Notification Routing” on page 22](#)

4.1 Creating SNMP Agent Components

For the Control Broker in a schema to connect to the SNMP Agent, you need to create e*Gate SNMP Agent components in the schema to be monitored.

You create an SNMP Agent component in the e*Gate Schema Designer. You can create only one SNMP Agent component per schema.

To create SNMP Agent components


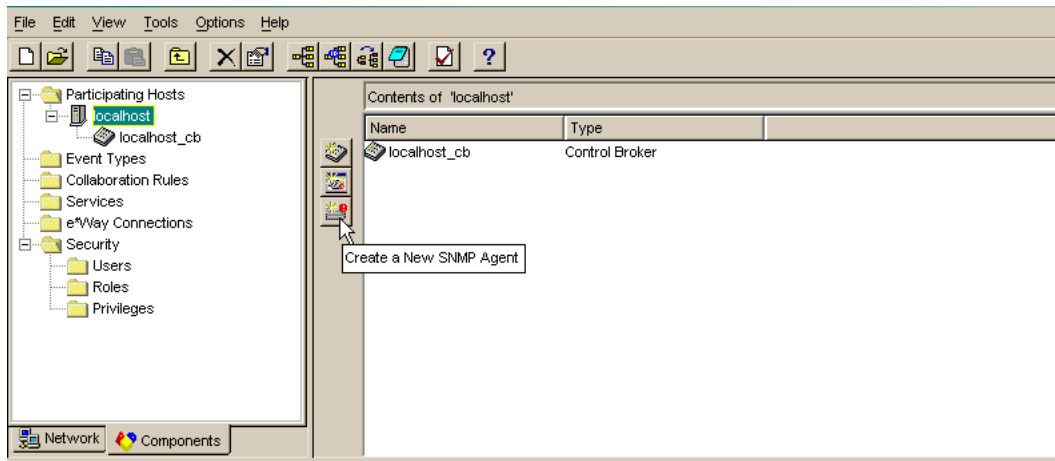
- 1 Start e*Gate Schema Designer and open the schema to be monitored by the e*Gate SNMP Agent.
- 2 Click the **Components** tab.
- 3 Expand the **Participating Host** folder and click the Participating Host where the schema runs.
- 4 Click **Create a New SNMP Agent**  to display the **New Monitor SNMP Agent Component** dialog box.

Figure 6 Creating an e*Gate SNMP Agent Component



- 5 Enter the name of the SNMP Agent component and click **OK**.

This adds the SNMP Agent to the Contents pane for the Participating Host. You can now configure the SNMP Agent component as described below.

4.2 Configuring SNMP Agent Components

After creating the e*Gate SNMP component as described in [“Creating SNMP Agent Components” on page 19](#), you must configure the component so that its properties match that of the SNMP Agent configuration file.

The configuration settings of the SNMP Agent component must always match the settings in the SNMP Agent configuration file. If there is a need to reconfigure the SNMP Agent, changes must be made to the e*Gate SNMP Agent component as well as the SNMP Agent configuration file and the Control Broker Notification script. For more information, refer to [“Reconfiguring Existing SNMP Agents” on page 30](#).

For information about the port configurations in the e*Gate SNMP model, refer to [“About e*Gate SNMP Model Configurations” on page 9](#).

To configure SNMP Agent components

- 1 If you do not know the port, timer, and user name settings for the SNMP Agent that were specified during the SNMP Agent installation, open the `stcsnmpa.conf` file.

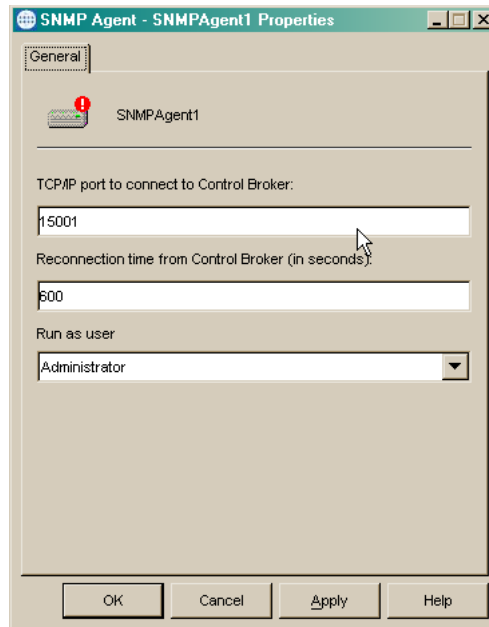
This file is located on the system where the SNMP Agent is installed. The file resides in the `<eGate\client>\bin` directory, where `<eGate\client>` is the directory where you installed the e*Gate Participating Host.

Make a note of the following configuration settings:

- ◆ CB_PORT
- ◆ CB_TIMER
- ◆ USERNAME

- 2 Log into the e*Gate Schema Designer and open the schema to be monitored.
- 3 Click the **Components** tab.
- 4 Expand the **Participating Host** folder and click the Participating Host with the SNMP Agent component.
- 5 In the Control Broker Contents pane, double-click the SNMP Agent component to display the **SNMP Agent Properties** dialog box.

Figure 7 SNMP Agent Properties Dialog Box



- 6 In the **TCP/IP port to connect to Control Broker** box, enter the port number listed as **CB_PORT** in the SNMP Agent configuration file. This is the port on which the SNMP Agent listens for Control Broker connections.
- 7 In the **Reconnection time from Control Broker** box, enter the number of seconds listed as **CB_TIMER** in the SNMP Agent configuration file. This is the number of seconds for the SNMP Agent to wait for a response from the Control Broker before considering the connection unresponsive. The default is 600 seconds (10 minutes).
- 8 In the **Run as user** list, click the user listed as **USERNAME** in the SNMP Agent configuration file. This is the e*Gate user name under which the SNMP Agent runs. Users are defined in the Schema Designer Users folder.
- 9 Click **OK**.

The e*Gate SNMP Agent component is now configured to match the properties in the SNMP Agent configuration file. Now you must configure the Control Broker for SNMP notification routing. For information, refer to [“Configuring Control Broker Notification Routing” on page 22](#).

4.3 Configuring Control Broker Notification Routing

After you have configured the SNMP Agent component in Schema Designer as described in “[Configuring SNMP Agent Components](#)” on page 20, you must configure the Control Broker to send and receive SNMP messages. To do this, you edit the Control Broker Notification script. This script, **Notification.tsc**, indicates to the Control Broker on which Participating Host the SNMP Agent runs, and to what port to forward SNMP notifications. Follow the procedure below to edit the **Notification.tsc**.

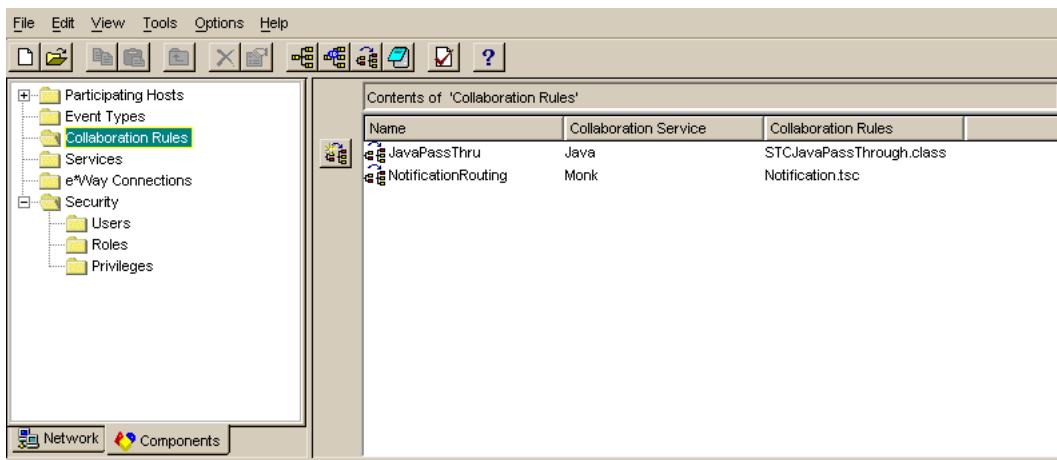
To configure Control Broker notification routing

- 1 Start the Schema Designer and open the schema to be monitored by the SNMP Agent.
- 2 Click the **Components** tab.
- 3 If you do not know the Participating Host name and port number specified for the SNMP Agent component, expand the **Participating Host** folder, click the hosts until you see the one that has an the SNMP Agent component.

To see the port number, double-click the SNMP Agent component to display its properties.

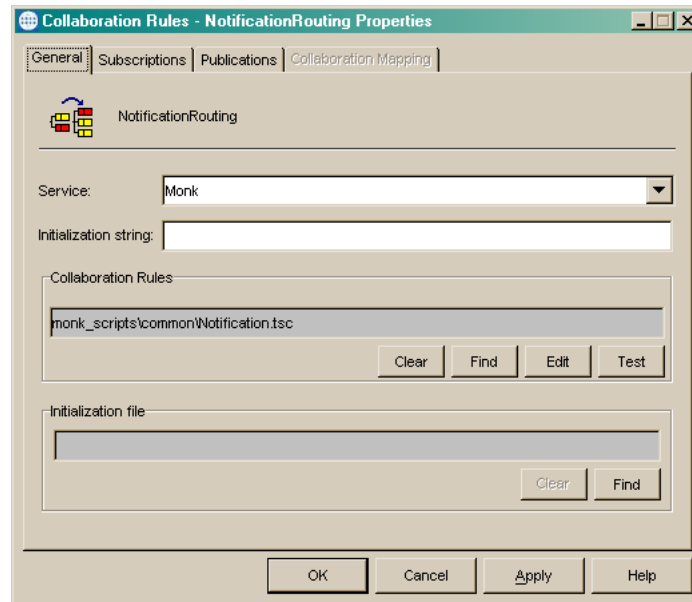
- 4 Click **Collaboration Rules**. The Collaboration Rules pane shows the Control Broker Notification script, **Notification.tsc**.

Figure 8 Notification Script



- 5 Double-click **Notification.tsc**. The **NotificationRouting Properties** dialog box appears.

Figure 9 NotificationRouting Properties Dialog Box



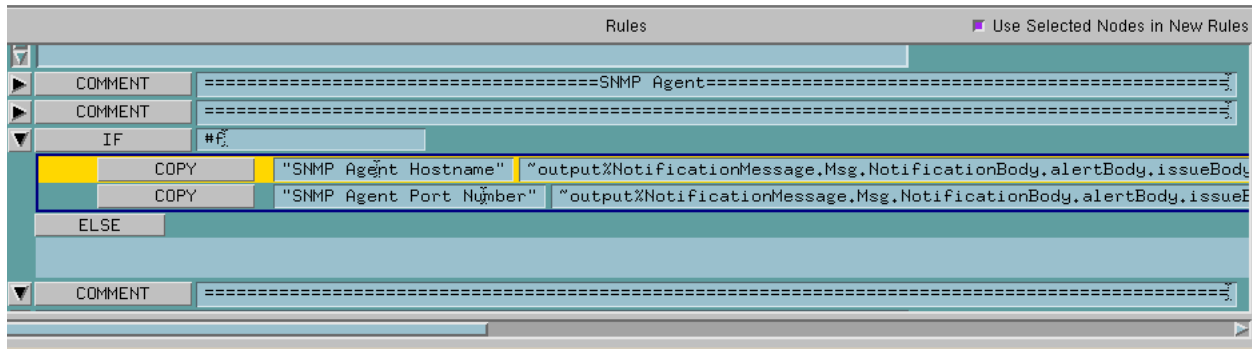
- 6 Click **Edit**. The **Monk Collaboration Rule Editor** window appears.
- 7 In the Rules pane, scroll down to the SNMP Agent section as shown below.

Figure 10 SNMP Agent Section in the Notification Script



- 8 In the SNMP Agent section, click the arrow in front of the IF statement. The IF statement shows the SNMP Agent settings as shown below.

Figure 11 SNMP Agent Settings in the Notification Script



- 9 Scroll to the end of the COPY statements where you see:

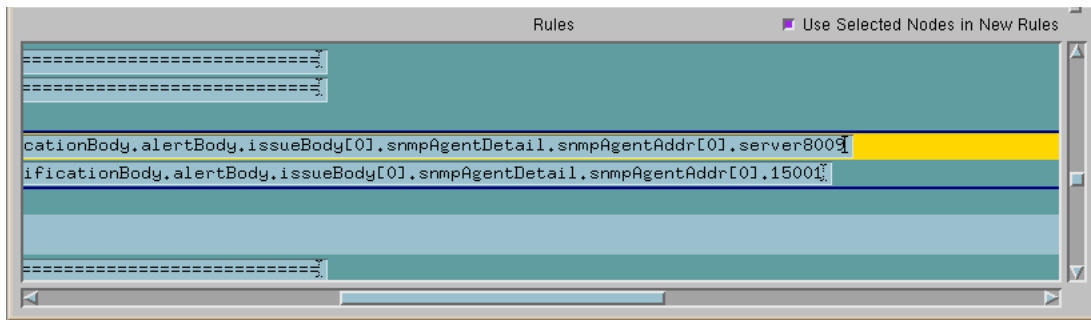
```
snmpAgentDetail.snmpAgentAddr[0].hostName
snmpAgentDetail.snmpAgentAddr[0].port
```

- 10 Replace **hostName** with the computer name of the system where the SNMP Agent runs.

The host name can be the name of a remote system where the SNMP Agent resides if this schema is monitored remotely.

- 11 Replace **port** with the port number where the Control Broker forwards SNMP alerts. This is the same port number defined during the SNMP Agent installation as the CB Port and the e*Gate SNMP Agent component configuration as TCP/IP port (page 21).

Figure 12 SNMP Agent Notification Configured



- 12 On the **File** menu, click **Save**.

Managing e*Gate SNMP Agents

This chapter describes how to manage the e*Gate SNMP Agent service on Windows, and the daemon on UNIX.

In This Chapter

- [“Managing the e*Gate SNMP Agent on Windows” on page 25](#)
- [“Managing the e*Gate SNMP Agent on UNIX” on page 28](#)
- [“Reconfiguring Existing SNMP Agents” on page 30](#)

5.1 Managing the e*Gate SNMP Agent on Windows

This section describes how you manage the e*Gate SNMP Agent on Windows, such as starting and stopping the service, configuring its startup options, and enabling logging.

5.1.1 Starting the e*Gate SNMP Agent

After the e*Gate SNMP Agent installation, the e*Gate SNMP Agent is configured as a “manual” service; you must start the service manually before Windows can load it as described below.

To change the e*Gate SNMP Agent startup options, refer to [“Configuring the e*Gate SNMP Startup Options” on page 25](#).

To start the e*Gate SNMP Agent using Windows

- 1 On the Windows desktop, right-click **My Computer** and click **Manage**.
- 2 Double-click **Services and Applications**.
- 3 Click **Services** in the left pane. The right pane shows the available services for the system.
- 4 Right-click **eGate SNMP (stcsnmpa)** and click **Start**.

5.1.2 Configuring the e*Gate SNMP Startup Options

After the e*Gate SNMP Agent installation, the e*Gate SNMP Agent is configured as a “manual” service; you must start the service manually before Windows can load it.

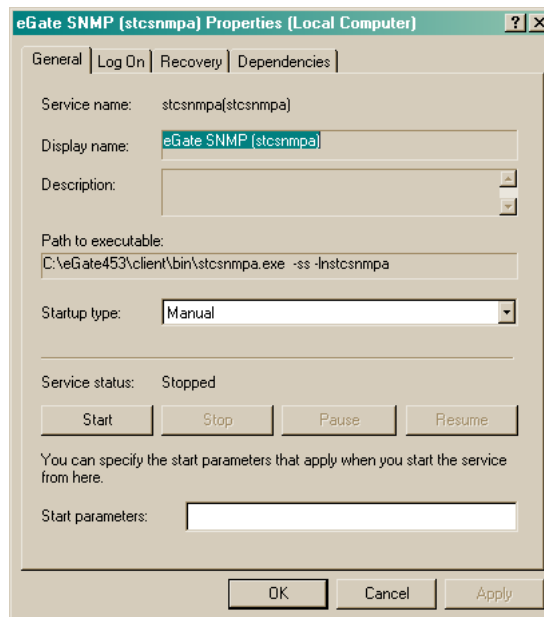
To change the e*Gate SNMP Agent startup options, follow the procedures below. You can use the command line utility or Windows to specify startup options.

When you configure a service as automatic, the service start automatically when the system starts or when the service is called for the first time. If a service is set to disabled, you cannot start it manually or automatically.

To configure the e*Gate SNMP Agent startup options using Windows

- 1 On the Windows desktop, right-click **My Computer** and click **Manage**.
- 2 Double-click **Services and Applications**.
- 3 Click **Services** in the left pane. The right pane shows the available services for the system.
- 4 Double-click **eGate SNMP (stcsnmpa)** to display the **eGate SNMP Properties** dialog box.

Figure 13 eGate SNMP Properties Dialog Box



- 5 In the **Startup Type** box, click **Automatic** to have the SNMP Agent start up automatically when the system boots up. Click **Manual** to start the service manually as described in [“Starting the e*Gate SNMP Agent” on page 25](#).

5.1.3 Stopping the e*Gate SNMP Agent

To stop the e*Gate SNMP Agent

- 1 On the Windows desktop, right-click **My Computer** and click **Manage**.
- 2 Double-click **Services and Applications**.
- 3 Click **Services** in the left pane. The right pane shows the available services for the system.

- 4 Right-click **eGate SNMP (stcsnmpa)** and click **Stop**.

5.1.4 Enabling Logging

You can enable logging by editing the e*Gate SNMP Agent configuration file as described below.

To enable logging using the SNMP Agent configuration file

- 1 Stop the SNMP Agent if it is currently running.
- 2 Open the SNMP Agent configuration file (**stcsnmpa.conf**) in the **<eGate\client>\bin** directory, where **<eGate\client>** is the directory where the Participating Host is installed on the system where the SNMP Agent resides.
- 3 Change **DEBUG false** to **DEBUG true** and save the file.
- 4 Restart the SNMP Agent.

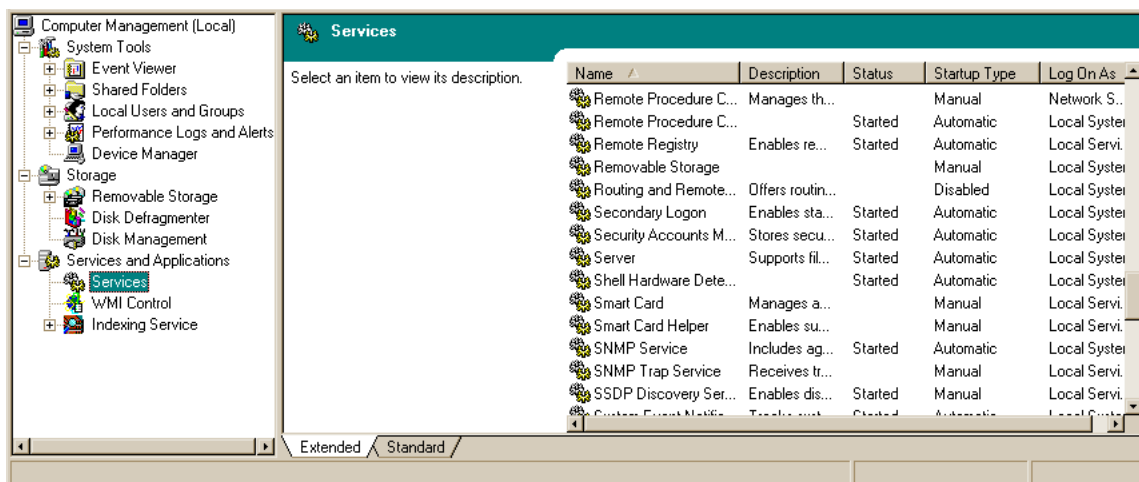
5.1.5 Specifying Communities

The e*Gate SNMP Agent automatically uses the same communities as those set up for the Windows SNMP service. To specify communities for the Windows SNMP service, follow the procedure below:

To specify communities

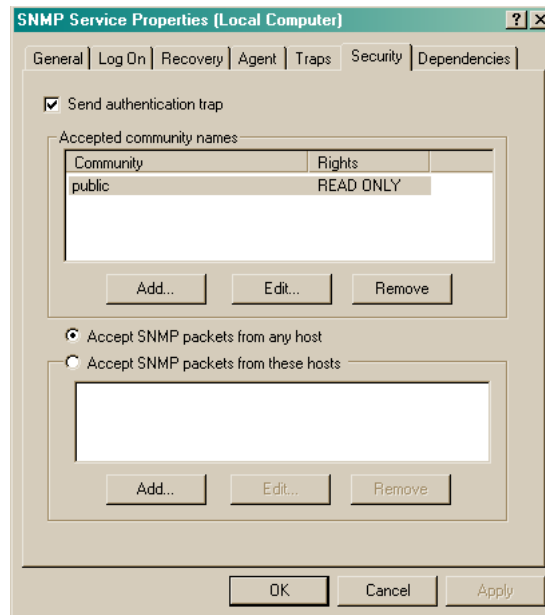
- 1 On the Windows desktop, right-click **My Computer** and click **Manage**.
- 2 Double-click **Services and Applications**.
- 3 Click **Services** in the left pane. The right pane shows the available services for the system.

Figure 14 Windows SNMP Service Configuration



- 4 In the right pane, double-click **SNMP Service** to display the **SNMP Service Properties** dialog box appears.
- 5 Click the **Security** tab. The current community settings appear as shown below.

Figure 15 Windows SNMP Service Security



- 6 Add or edit community names as necessary and click **OK**.

5.2 Managing the e*Gate SNMP Agent on UNIX

The e*Gate SNMP Agent runs on UNIX as a daemon and is started and stopped with a shell script. The sections below describe how you start and stop the SNMP Agent, and how you can display and configure the SNMP Agent's community settings for security purposes.

5.2.1 Starting the e*Gate SNMP Agent

To start the e*Gate SNMP Agent

- Type the following command:
S99stcsnmpdx start

5.2.2 Stopping the e*Gate SNMP Agent

To stop the e*Gate SNMP Agent

- Type the following command:
S99stcsnmpdx stop

5.2.3 Displaying the e*Gate SNMP Agent's Communities

To display the e*Gate SNMP Agent's communities

- Type the following command:
S99stcsnmpdx show

5.2.4 Setting Up Communities

When the SNMP Agent starts on UNIX, it attempts to locate and parse the OS SNMP configuration file (**snmpd.conf**) to use its community properties.

The parsing performed is simple; complex configuration files such as the AIX SNMP configuration file are not parsed. If the file cannot be parsed or found, communities are not set up to secure SNMP traffic, leaving e*Gate schema components vulnerable to security risks. It is therefore advisable to verify the community settings once the SNMP Agent has started, and change the community settings if necessary.

To show the current community settings, type the following in the **<eGate/client>/bin** directory, where **<eGate/client>** is the directory where the e*Gate Participating Host is located on the system with the SNMP Agent:

```
S99stcsnmpdx show
```

To change the settings displayed, follow the procedure below.

To change community settings

- 1 Stop the SNMP Agent if it is running.
- 2 In a shell script editor, open the file **S99stcsnmpdx** located in the **<eGate/client>/bin** directory, where **<eGate/client>** is the directory where the e*Gate Participating Host is located on the system with the SNMP Agent.
- 3 Enter the following information:

For this setting	Enter
MANAGERS	Name of hosts that can send SNMP queries to the e*Gate SNMP Agent, separated by spaces. The default is all.
READ_COMMUNITY	Name for the community that has read access to the e*Gate MIB.
WRITE_COMMUNITY	Name for the community that has read and write access to the e*Gate MIB.
TRAP_COMMUNITY	Name for the community under which trap notifications are sent.
TRAP_HOSTS	Host names of the hosts to which trap notifications are forwarded. The default is localhost.
TRAP_LIST	List of host^community pairs for sending traps. Separate each item with (pipe character).

- 4 Save the file and restart the SNMP Agent.

5.2.5 Enabling Logging

You can enable logging by starting the SNMP Agent using the debug parameter in the SNMP configuration file. When logging is enabled, the SNMP Agent logs errors in the **snmpa.log** file located in the `<eGate/client>/logs` directory where `<eGate/client>` is the directory where the e*Gate Participating Host is installed.

To enable logging

- 1 Stop the SNMP Agent if it is running.
- 2 Open the SNMP Agent configuration file (**stcsnmpa.conf**) in the `<eGate/client>/bin` directory, where `<eGate/client>` is the directory where the Participating Host is installed on the system with the SNMP Agent.
- 3 Change **DEBUG false** to **DEBUG true** and save the file.
- 4 Restart the SNMP Agent.

5.3 Reconfiguring Existing SNMP Agents

The SNMP Agent configuration consists of the combination of three components; the configuration for the following:

- The SNMP Agent itself
- The SNMP Agent component in the e*Gate schema
- The Control Broker Notification script

All three components contain all or some of the following settings that must match when you reconfigure settings:

- The computer name of the system where the SNMP Agent is installed.
- The port number indicating the TCP/IP port through which the SNMP Agent, the schema, and the Control Broker communicate (CB port).
- The number of seconds for the SNMP Agent to wait for a response from the Control Broker before considering the connection unresponsive if there has been no interaction during that time (CB timer).
- The user name to use to authorize with the Control Broker.

The table below lists the configuration for each component and how they match settings of other components. For example, the **CB_PORT** setting in the SNMP Agent configuration file must match the setting entered for the TCP/IP port property for the SNMP Agent component in the schema.

Table 4 e*Gate SNMP Agent Configurations

SNMP Agent	SNMP Agent Component	Notification Routing script
Installed on system	n/a	Computer name
CB_PORT	TCP/IP port to connect to Control Broker	Port
CB_TIMER	Reconnection time from Control Broker	N/A
USERNAME	Part of the Schema Managed by the Control Broker	N/A

5.3.1 Changing the CB Port Number

To change the port number for the CB port through which the Control Broker and the e*Gate SNMP Agent communicate, you must change the CB port settings for the SNMP Agent, the SNMP Agent component, and the Control Broker.

To change the CB port number

- 1 Stop the e*Gate SNMP Agent and all modules in the schema.
- 2 Edit the Control Broker notification script as described in [“Configuring Control Broker Notification Routing” on page 22](#).
- 3 Configure the SNMP Agent for the new CB port number by entering the number in the **TCP/IP port to connect to Control Broker** box as described in [“Configuring SNMP Agent Components” on page 20](#).
- 4 Open the SNMP Agent configuration file (`stcsnmpa.conf`) in the `<eGate/client>/bin` directory, where `<eGate/client>` is the directory where the Participating Host is installed on the system with the SNMP Agent.
- 5 Change the port number for the `CB_PORT` setting and save the file.
- 6 Restart all modules in the schema and start the SNMP Agent.

5.3.2 Changing the Control Broker Wait Interval (CB Timer)

To change the Control Broker wait interval (the CB timer), you must change the CB timer settings for the SNMP Agent component and the SNMP Agent. For an overview of the ports in the e*Gate SNMP model, refer to [“About e*Gate SNMP Model Configurations” on page 9](#).

To change the Control Broker wait interval (CB timer)

- 1 Stop the e*Gate SNMP Agent and all modules in the schema.
- 2 Configure the SNMP Agent for the new wait interval by entering the number of seconds in the **Reconnection time from Control Broker** box as described in [“Configuring SNMP Agent Components” on page 20](#).

- 3 Open the SNMP Agent configuration file (**stcsnmpa.conf**) in the `<eGate\client>\bin` directory, where `<eGate\client>` is the directory where the Participating Host is installed.
- 4 Change the number of seconds for the **CB_TIMER** setting and save the file.
- 5 Restart all modules in the schema and start the SNMP Agent.

5.3.3 Changing the MIB II, STC, or SNMP Port Number

You can change the port numbers for the MIB II port, the STC port and the SNMP port in the SNMP Agent configuration file as described below. The STC port and the SNMP port are the same port. During the Windows installation it is called the STC port; during the UNIX installation it is referred to as the SNMP port. For an overview of the ports in the e*Gate SNMP model, refer to [“About e*Gate SNMP Model Configurations” on page 9](#).

To change the MIB II, STC, or SNMP port number

- 1 Stop the e*Gate SNMP Agent.
- 2 Open the SNMP Agent configuration file (**stcsnmpa.conf**) in the `<eGate/client>/bin` directory, where `<eGate/client>` is the directory where the Participating Host is installed on the system with the SNMP Agent.
- 3 To change the MIB II port number, change the number for the **SNMP_MIB_II_PORT** setting.
- 4 To change the STC or SNMP port number, change the number for the **SNMP_PORT** setting.
- 5 Save the file and restart the SNMP Agent.

5.3.4 Changing the Trap Delimiter

The e*Gate SNMP Agent uses `\n` as its default trap delimiter. To change this character, follow the procedure below.

To change the trap delimiter

- 1 Stop the e*Gate SNMP Agent.
- 2 Open the SNMP Agent configuration file (**stcsnmpa.conf**) in the `<eGate/client>/bin` directory, where `<eGate/client>` is the directory where the Participating Host is installed on the system with the SNMP Agent.
- 3 Change the character to be used as a delimiter for the **SEPARATOR** setting.
- 4 Save the file and restart the SNMP Agent.

The e*Gate MIB

This chapter describes the e*Gate MIB provided with the SNMP Agent. You load this MIB into your SNMP management system to enable it to communicate with the e*Gate SNMP Agent.

In This Chapter

- [“About the e*Gate MIB” on page 33](#)
- [“e*Gate Managed Objects” on page 34](#)
- [“e*Gate Trap Definitions” on page 38](#)

6.1 About the e*Gate MIB

The e*Gate SNMP Agent provides the e*Gate MIB which defines the e*Gate trap notifications as well as the objects that can be managed in e*Gate schemas. The e*Gate MIB uses Abstract Syntax Notation One (ANS.1), which is industry standard for MIBs.

The e*Gate MIB, `stc_mib.txt`, is located in the `<eGate>\client\bin` directory, where `<eGate>` is the directory where you installed e*Gate Integrator. Do not modify this file.

The e*Gate MIB objects can be found under the following node as relative OIDs:

```
1.3.6.9.4.1.1351.1.1.1
```

In details, this node consists of the following object identifiers (OIDs):

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).stc(1351).
products(1).software(1).egate(1)
```

Certain objects may be duplicated because they form part of a group of objects associated with a certain module. For example, if a schema contains multiple Control Brokers there will be multiple `cbEntry` nodes and multiple set of Control Broker objects. The first Control Broker will be assigned the location `1.1.1.x` where `x` is a Control Broker object (such as `cbState`). The second Control Broker will be assigned the location `1.1.2.x`, and so forth.

The components which are monitored by the Control Broker, such as e*Ways, are contained in the data process table, `dtable`.

Entries are indexed by Control Broke and data process. For example, `1.3.6.1.4.1.1351.1.1.1.2.1.4.1.2` contains the `dCurState` of the 2nd module in the first Control Broker.

6.2 e*Gate Managed Objects

Table 5 e*Gate Managed Objects

Object	OID	Possible Values	Permissions	Description
Cbs	1	N/A	not accessible	The Control Broker (CB) tree.
CbTable	1.1	N/A	not accessible	A list of CB entries.
cbEntry	1.1.1	N/A	not accessible	A CB entry containing objects for a particular CB.
cbIndex	1.1.1.1	Integer	not accessible	This is a CB index.
cbName	1.1.1.2	String (0-255)	read-only	The logical name for this CB. The logical name is unique per host.
cbCurState	1.1.1.3	0=unknown 1=up 2=down	read-only	This is the state of the CB.
cbReqState	1.1.1.4	2=down	read/write	Allows you to issue a SET command that will shut down the CB. Note that you can only perform a GET operation after the parameter is SET.
cbHostName	1.1.1.5	String (0-255)	read-only	The host name for this CB.
cbLastUpdateTime	1.1.1.6	TimeTicks	read-only	The last update time for this CB.
cbStartupTime	1.1.1.7	TimeTicks	read-only	The startup time for this CB.
cbSharedDataDir	1.1.1.8	String (0-255)	read-only	The shared data directory for this CB.
cbControlPort	1.1.1.9	Integer	read-only	The CB's control port.
cbNumDRows	1.1.1.10	Integer	read-only	The number of rows of all data processes.
cbNumQRows	1.1.1.11	Integer	read-only	The number of rows of all the queues.
dTable	1.2	N/A	not accessible	A list of data processes in a particular CB. Data processes include server module, communication client, communication client proxy, e*Ways, and external processes. The cbIndex is used to identify a particular e*Gate environment.

Table 5 e*Gate Managed Objects

Object	OID	Possible Values	Permissions	Description
dEntry	1.2.1	N/A	not accessible	A data process entry containing objects for a particular data process.
dIndex	1.2.1.1	Integer	not accessible	This is a SeeBeyond data process index.
dName	1.2.1.2	String (0-255)	read-only	Logical name of a SeeBeyond data process. This name is unique within a CB environment.
dType	1.2.1.3	0=Unidentified Element 1=BOB 2=e*Way 3=IQMgr	read-only	This object is used to differentiate between the various types of SeeBeyond data processes.
dCurState	1.2.1.4	0=Unknown 1=up 2=down 3=suspended 4=reloaded 5=removed	read-only	This is the current state of the data process.
dReqState	1.2.1.5	1=up 2=down 3=suspended 4=reloaded	read/write	This object is used to request a change of state for a data process. It is mainly used by the SET command to change the state of an existing data process. It is not meant to allow the SNMP manager to create new data processes. Note that you can only perform a GET operation after the parameter is SET.
dHostname	1.2.1.6	String (0-255)	read-only	The host name for this data module.
dLastUpdateTime	1.2.1.7	TimeTicks	read-only	The last update time of this module.
dStartupTime	1.2.1.8	TimeTicks	read-only	The startup time of this module.
dSharedDataDir	1.2.1.9	String (0-255)	read-only	The shared data directory for this module.
dControlPort	1.2.1.10	Integer	read-only	The CB control port for this data process.
dLastActionTime	1.2.1.11	TimeTicks	read-only	The last action time of this data process. <i>Reserved for future use.</i>

Table 5 e*Gate Managed Objects

Object	OID	Possible Values	Permissions	Description
dLastActionName	1.2.1.12	String (0-255)	read-only	The last action name of this data process. <i>Reserved for future use.</i>
dLastPutTime	1.2.1.13	TimeTicks	read-only	Time of the last put operation. <i>Reserved for future use.</i>
dLastPutMsgType	1.2.1.14	TimeTicks	read-only	Time of the last put Event type. <i>Reserved for future use.</i>
dLastPutSeqNum	1.2.1.15	TimeTicks	read-only	Time of the last put sequence number. <i>Reserved for future use.</i>
dLastGetTime	1.2.1.16	TimeTicks	read-only	Time of the last get operation. <i>Reserved for future use.</i>
dLastGetMsgType	1.2.1.17	TimeTicks	read-only	Time of the last get Event type. <i>Reserved for future use.</i>
dLastGetSeqNum	1.2.1.18	TimeTicks	read-only	Time of the last get sequence number. <i>Reserved for future use.</i>
dLastMsgReceivedFromExtTime	1.2.1.19	TimeTicks	read-only	Time of the last Event received from the external. <i>Reserved for future use.</i>
dLastMsgSentFromExtTime	1.2.1.20	TimeTicks	read-only	Time of the last Event sent from the external. <i>Reserved for future use.</i>
dExtSeqNum	1.2.1.21	Integer	read-only	External sequence number. <i>Reserved for future use.</i>
dExtRetryCount	1.2.1.22	Integer	read-only	External retry count. <i>Reserved for future use.</i>
dExtState	1.2.1.23	0=Unknown 1=Communicating 2=Not Communicating	read-only	This is the state of the external process to which this data process connects. <i>Reserved for future use.</i>
qTable	1.3	N/A	not accessible	A list of queue entries in a particular CB.
qEntry	1.3.1	N/A	not accessible	A queue entry containing objects for a particular queue.
qIndex	1.3.1.1	Integer	not accessible	This is e*Gate's queue index.

Table 5 e*Gate Managed Objects

Object	OID	Possible Values	Permissions	Description
qName	1.3.1.2	String (0-255)	read-only	The logical name of the queue. This name is unique per CB.
qCurState	1.3.1.3	0=Unknown 1=Attached 2=Detached	read-only	This is the current state of the queue.
qReqState	1.3.1.4	1=Attached 2=Detached	read/write	Allows you to issue a SET command that will alter the queue's state. Note that you can only perform a GET operation after the parameter is SET.
qHostname	1.3.1.5	String (0-255)	read-only	The host name for this queue.
qLastUpdateTime	1.3.1.6	TimeTicks	read-only	The last update time of this queue.
qStartupTime	1.3.1.7	TimeTicks	read-only	The startup time of this queue.
qNumOfRevealedMsgs	1.3.1.8	String (0-255)	read-only	The number of revealed Events for this queue. <i>Reserved for future use.</i>
qNumOfUnRevealedMsgs	1.3.1.9	Integer	read-only	The number of unrevealed Events for this queue. <i>Reserved for future use.</i>
qNumOfExpiredMsgs	1.3.1.10	Integer	read-only	The number of expired Events for this queue. <i>Reserved for future use.</i>
qNumOfJournalledMsgs	1.3.1.11	Integer	read-only	The number of journaled Events for this queue. <i>Reserved for future use.</i>
qLastTimePublished	1.3.1.12	TimeTicks	read-only	Time of the last Event published to this queue. <i>Reserved for future use.</i>
qSizeInBytes	1.3.1.13	Integer	read-only	The size of this queue. <i>Reserved for future use.</i>
qSizeMsgCount	1.3.1.14	Integer	read-only	The size of the Event count. <i>Reserved for future use.</i>
stcReleaseVer	2	String (0-255)	read-only	Version number of the MIB table (the default value is: "version 4.0").
stcTraps	3	N/A	not accessible	Object identifier. The trap entries are shown on a separate table below.

Table 5 e*Gate Managed Objects

Object	OID	Possible Values	Permissions	Description
moduleName	4	String (0-255)	not accessible	This object is used for a trap that has a monitor name or module name when the e*Gate SNMP Agent does not have that information.
genericComments	5	String (0-255)	not accessible	This object is used along with most of the traps as a reason for trap generation. The content will be changed as a new trap is generated, it has no significant meaning by itself.

6.3 e*Gate Trap Definitions

Table 6 e*Gate Trap Notifications

Trap Name	Location	Variables	Description
SMNPALossConnectionToCb	3.1	cbName	The e*Gate SNMP Agent detects a lost connection to a Control Broker (CB).
SNMPADetectsCbUnresponsive	3.2	cbName	The e*Gate SNMP Agent detects an unresponsive CB.
SNMPADetectsCbResponded	3.3	cbName	The e*Gate SNMP Agent detects that a CB responded after it had been unresponsive.
cbDetectsSNMPAResponded	3.4	cbName	A CB detects that an element responded.
cbConnectedToSNMPA	3.5	cbName	A CB connects to the e*Gate SNMP Agent.
cbDetectsDiskUsageAbove Threshold	3.6	cbName, genericComments	A CB detects an out-of-disk space problem. Disk sector and other useful information are concatenated in the genericComments string.
timerEvent	3.7	cbName, genericComments	A timer event in a CB is triggered to signal the CB to perform certain tasks. A genericComments string will contain the notification name and other information.

Table 6 e*Gate Trap Notifications

Trap Name	Location	Variables	Description
cbCantGetStatus	3.8	cbName, moduleName, genericComments	A CB cannot get status from a module.
cbCantStartModule	3.9	cbName, moduleName, genericComments	A CB cannot start a module.
cbLostConnectionToM	3.10	cbName, moduleName, genericComments	A CB lost its connection to the monitor.
cbDetectsMUnresponsive	3.11	cbName, moduleName, genericComments	A CB detects an unresponsive monitor element.
cbDetectsMResponded	3.12	cbName, moduleName, genericComments	A CB detects that a monitor element responded.
monitorConnectedToCb	3.13	cbName, moduleName, genericComments	A monitor connected to the CB. <i>(Not implemented.)</i>
userAuthenticationFailure	3.14	cbName, moduleName, genericComments	A CB failed to authenticate a module.
alertDeliveryFailure	3.15	cbName, moduleName, genericComments	A CB cannot send an Alert to a certain monitor agent(s) or an agent cannot deliver the Alert. The list of alert agent(s) will be concatenated with the reason in the genericComments string.
dInputAboveThreshold	3.16	dName, genericComments	Data process input coming into an element above the threshold.
dInputBelowThreshold	3.17	dName, genericComments	Data process input coming into an element below the threshold.
dOutputAboveThreshold	3.18	dName, genericComments	Data process output from an element above the threshold.
dOutputBelowThreshold	3.19	dName, genericComments	Data process output from an element below the threshold.
dDownFatal	3.20	dName, genericComments	A data process is down for an unknown reason (for example, data process crashed or was shut down by a KILL command).
dDownControlled	3.21	dName, genericComments	A data process is shut down due to lack of memory.

Table 6 e*Gate Trap Notifications

Trap Name	Location	Variables	Description
dDownUser	3.22	dName, genericComments	A data process is shut down gracefully and status is sent to a CB.
dUp	3.23	dName	A data process is up and status is sent to a CB.
cbDetectsDUnreponsive	3.24	dName, genericComments	A data process does not respond to a CB.
cbDetectsDReponed	3.25	dName, genericComments	A CB detects a module responded after being unresponsive.
dCantConnectToExternal	3.26	dName, genericComments	A data process cannot connect to an external system. <i>(Not implemented.)</i>
dConnectedToExternal	3.27	dName, genericComments	A data process has connected to an external system. <i>(Not implemented.)</i>
dLostConnectionExternal	3.28	dName, genericComments	A data process lost connection to an external system.
dNotConnectedToExternal	3.29	dName, genericComments	A data process is not connected to an external system.
dDeliveryFailure	3.30	dName, genericComments	Data process got a failure from external procedure.
unUsableMessageCantId	3.31	dName, genericComments	This notification is generated when a message fails all ID tests.
messageContentOfInterest	3.32	dName, genericComments	A message of the element matches the requirement for which the element is looking.
unQueueableMessage	3.33	dName, genericComments	A message is unqueueable.
userDefined	3.34	dName, genericComments	An Event defined by a user for a certain data process.
queueMessageExpired	3.35	qName	A message has expired.
iqLimitExceeded	3.36	qName, genericComments	A queue has exceeded its limit.

Table 6 e*Gate Trap Notifications

Trap Name	Location	Variables	Description
CBConnectedToRegistry	3.37	cbName	The CB has connected to the e*Gate Registry. <i>(Not implemented.)</i>
CBLostConnectionToRegistry	3.38	cbName	The CB has lost its connection to the e*Gate Registry.

Troubleshooting

Follow the procedure below if the e*Gate SNMP Agent does not appear to function correctly.

- For the Windows e*Gate SNMP Agent, enable logging to track debug information, as described in [“Enabling Logging” on page 27](#).
- Verify that SNMP Agent section of the Control Broker Notification script (**notification.tsc**) has been modified to send notifications to the SNMP Agent. For information, refer to [“Configuring Control Broker Notification Routing” on page 22](#).
- Verify that the Control Broker log file is sending out notifications.
- If notifications are sent to the e*Gate SNMP Agent, verify the Control Broker log file for a “connected to SNMP Agent” message.
- Check the SNMP Agent log file to verify it has received trap notifications.
- Verify that there is a trap for each notification in the e*Gate MIB.
- In the SNMP trap notification, check for 1351 in OID. The OID identifies SeeBeyond SNMP trap notifications. For more information, refer to [“About the e*Gate MIB” on page 10](#).
- Verify that the e*Gate SNMP Agent is configured to forward trap notifications to the correct STC port for the SNMP management system. For information, refer to [“About e*Gate SNMP Model Configurations” on page 9](#).
- Verify that the SNMP management system expects the community name of the e*Gate SNMP Agent. On UNIX, you can display the SNMP community settings as described in [“Displaying the e*Gate SNMP Agent’s Communities” on page 29](#).
- Verify that the user name and password combination is correct.

Index

A

Administrator Account Information dialog box 15

C

CB port 17
 changing 31
 overview 9
 CB Timer 14, 18, 31
 communities 8
 UNIX 29
 Windows 27
 component, SNMP Agent 7
 configuring
 CB port 31
 CB timer 31
 Control Broker 14
 e*Gate SNMP Agent 30
 MIB II port 32
 SNMP Agent component 20
 SNMP port 32
 SNMP Agent startup options 25
 STC port 32
 Control Broker
 configuring 14
 overview 7
 port 9, 14, 17, 31
 timer 14, 18, 31
 wait interval 31
 Control Broker Information dialog box 14

D

DEBUG setting 27, 30
 delimiter, trap 32

E

e*Gate SNMP Agent
 communities, Windows 27
 configurations 9
 installing, UNIX 16
 installing, Windows 12
 log file 30

 logging 27, 30
 model 7
 overview 7
 platform support 6
 reconfiguring 30
 starting on UNIX 28
 starting on Windows 25
 STC port 9, 17
 stopping on UNIX 28
 stopping on Windows 26
 trap definitions 38
 UNIX shell script 16
 enabling
 logging, UNIX 30
 logging, Windows 27

F

file, log 30

I

installing
 SNMP Agent, UNIX 16
 SNMP Agent, Windows 12
 Windows SNMP service 12

L

logging
 enabling, UNIX 30
 enabling, Windows 27
 verbose 27

M

MIB file 38
 MIB II port 15, 17
 changing 32
 overview 10
 MIB objects 34, 38
 model, e*Gate SNMP Agent 7

O

organization of information, document 5
 OS SNMP service 8

P

platform support 6
 ports
 15001 9, 17, 31

Index

- 161 10, 17
- 162 9
- 8000 9, 17
- Control Broker (CB) 9, 14, 17, 31
- MIB II 10, 15, 17, 32
- SNMP 9, 17, 32
- STC 9, 15, 17, 32
- trap 9

S

- S99stcsnmpdx 16
- security 8
 - UNIX 29
 - Windows 27
- SeeBeyond Web site
 - technical support 6
- separator, trap 32
- shell script 16
- SNMP Agent component
 - CB port 9, 17, 31
 - CB Timer 14, 18, 31
 - configuring 20
 - overview 7
- SNMP Agent configuration file
 - CP_PORT 31
 - CP_TIMER 31
 - DEBUG 27, 30
 - SEPARATOR 32
 - SNMP_MIB_II_PORT 32
 - SNMP_STC_PORT 32
- SNMP Agent, see *e*Gate SNMP Agent*
- SNMP port 17
 - changing 32
 - overview 9
- SNMP Port Configuration dialog box 15
- SNMP service
 - Windows 12
- starting
 - SNMP Agent startup options 25
 - SNMP Agent, UNIX 28
 - SNMP Agent, Windows 25
- STC port 15, 17
 - changing 32
 - overview 9
- stc_mib.txt 38
- stcsnmpa.config see *SNMP configuration file*
- stopping
 - SNMP Agent, UNIX 28
 - SNMP Agent, Windows 26
- system requirements 12

T

- technical support 6
- timer 31
- trap port 9
- traps
 - delimiter 32
 - e*Gate trap definitions 38
- Troubleshooting 43

U

- UNIX SNMP service 8
 - MIB II port 17
- Username 21

V

- verbose logging 27

W

- wait interval, Control Broker 14, 18, 31
- Windows SNMP service 8, 12
 - MIB II port 10