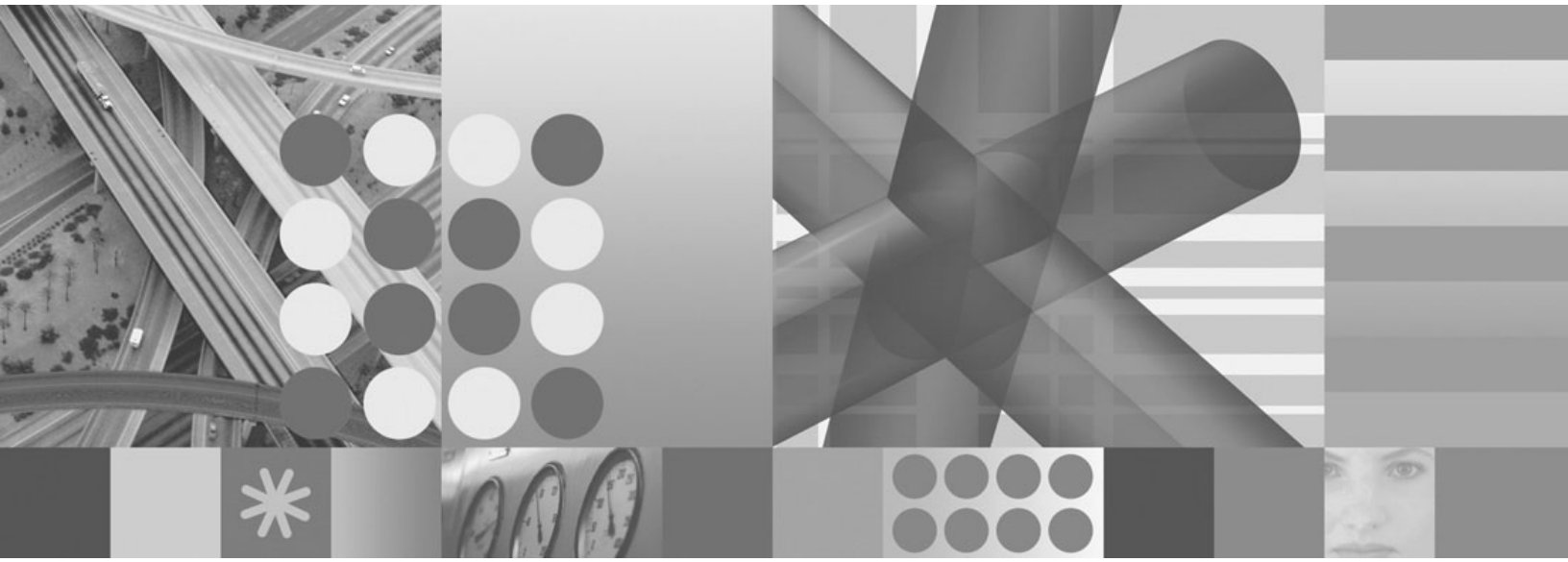
Tivoli® System Automation for Integrated Operations Management

User's Guide

SC23-6113-01

Tivoli® System Automation for Integrated Operations Management



User's Guide

SC23-6113-01

Note:
Before using this information and the product it supports, be sure to read the general information in Notices.

This edition applies to version 2.1 of IBM Tivoli System Automation for Integrated Operations Management (5724-L47) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures . . . . . **xiii**

Tables . . . . . **xv**

About This Document . . . . . **xvii**
Who should read this document xvii
How this document is organized xvii
Notices and statements used in this document xvii
Using the documentation xviii
Printing this document xviii
Printing problems? xviii
Contacting Adobe xviii
Adding annotations to PDF files xix

New in this release . . . . . **xxi**
New product name xxi
Alert escalation feature xxi
REXX enhancements xxi
Security enhancements xxi
Other enhancements xxii
Documentation changes xxii

Part 1. Getting started **1**

Chapter 1. Learning About SA IOM **3**
SA IOM overview 3
SA IOM and the client/server model 4
How SA IOM works 5
Host system connectivity 5
Client connectivity 5
Peer connectivity 6
Automation and notification 6
Message Collector capability 6
REXX-based extensibility 7
SA IOM features 7
Emulation features 7
REXX scripts 8
Additional security features of SA IOM servers and clients 8

Chapter 2. Planning your SA IOM configuration **11**
Planning overview 11
Client and server security and Windows 12
SA IOM and Windows security 12
Windows Service security considerations 12
Software requirements 14
Software requirements for the server 14
Software requirements for the client 14
Software requirements for the Web-based user interface 14
Software requirements for the database 14
Description of installation components 15
The SA IOM installation program 15
SA IOM executable programs 15
Web-based user interface and database software (optional) 16
Encryption software 17

Unicode software . . . 17
Support DLLs and drivers . . . 17
System DLLs . . . 17
README file . . . 17
Default configuration and log files . . . 17
Sample REXX programs . . . 17
TCP/IP considerations . . . 18
SA IOM TCP/IP port usage . . . 18
SA IOM server and client TCP/IP KEEPALIVE support . . . 19
About modems . . . 19
About configuring modems . . . 20
Using modems for SA IOM client/server communication . . . 20
Using modems for other SA IOM purposes . . . 20
Modem recommendations . . . 20
About direct connections . . . 20
Direct connection requirements . . . 21
About hardware adapters . . . 21
TN3270E connections . . . 21
Voice adapters . . . 21
LAN adapters . . . 21
Serial port expansion adapters . . . 21
3270 adapters (deprecated) . . . 22
REXX support requirements (optional) . . . 22
About REXX on Windows . . . 22
Supported software for REXX support . . . 22
Making Object REXX available to users running SA IOM server . . . 23
TN3270E operational environment . . . 23
About the TN3270E environment . . . 23
3270 emulation requirements (deprecated) . . . 24
About 3270 emulation adapters . . . 24
Supported 3270 emulation adapters . . . 24
Voice control requirements (optional) . . . 24
Beeper paging and time acquisition requirements (optional) . . . 25
Beeper paging requirements . . . 25
Time acquisition requirements . . . 25
Beeper paging and time acquisition can share a port . . . 25
SA IOM as a Windows Service . . . 25
Windows Services . . . 25
Client/Server compatibility considerations . . . 26
Where to go from here . . . 26

Chapter 3. Installing and configuring SA IOM . . . 27
Installing and verifying SA IOM . . . 27
Installing SA IOM . . . 27
Installing SA IOM sample scripts . . . 30
Verifying SA IOM installation . . . 30
Client and server profile parameters . . . 31
Locating new client and server profile parameters . . . 31
Logging on to SA IOM the first time . . . 31
Logging on to the server from a local client . . . 31
Renaming the server . . . 32
Uninstalling SA IOM (optional) . . . 32
Installing modems . . . 33
Adding modems to the Windows environment . . . 33
Testing modems . . . 34

Chapter 4. Starting and stopping SA IOM . . . 35
Starting and stopping the server . . . 35
Starting the server . . . 35
Stopping the server . . . 36

Connecting to a server from a configured client . . . 38
Before you start . . . 38
Logging on . . . 38
Configuring the client . . . 39
Before you start . . . 39
Defining a server connection . . . 39
Difficulty connecting . . . 39
Defining general properties of the client . . . 39

Part 2. "Classic" user and administrator tasks. . . . 41

Chapter 5. About the user interface . . . 43
About the SA IOM server . . . 44
Server component states . . . 44
About the SA IOM client . . . 45
Client control window panels . . . 46
Controlling scripts . . . 47
Script information . . . 47
Starting scripts . . . 47
Stopping scripts . . . 48
Viewing script output . . . 49
Authority and the Scripts panel display . . . 49
Managing users . . . 49
List of users . . . 50
Disconnecting users . . . 50
Sending messages . . . 51
Authority and the Users control panel . . . 51
Using Help . . . 51
Other types of help . . . 51
Recommendation . . . 52
Messages . . . 52
About SA IOM Service Manager . . . 52
SA IOM Service Manager . . . 52
Service Manager property pages . . . 52

Chapter 6. Administering SA IOM software . . . 55
Performing configuration tasks . . . 55
User authority required . . . 55
System administrator tasks . . . 55
System administrator responsibilities . . . 56
Defining general properties . . . 56
How to define general properties . . . 56
Defining host sessions . . . 57
Defining a Message Collector session . . . 57
Defining a TN3270E session . . . 58
Defining a 3270 session using the Attachmate IRMA 3270 PCI adapter . . . 58
Defining a Glass Teletype session (example) . . . 59
Defining user groups . . . 60
Default user groups . . . 60
Read Only sessions . . . 60
Defining new user groups . . . 61
Defining session classes . . . 62
Defining a new session class . . . 62
Configuring beeper paging . . . 63
Setting up beeper paging . . . 63
Defining users . . . 63
Adding users . . . 63
Defining client connections . . . 64
Setting up client connections . . . 64
Defining peer connections . . . 65

Setting up peer connections . . . 65
Defining service logging and recovery options . . . 66
Defining SA IOM Service log properties . . . 66
Defining SA IOM Service Manager log properties . . . 66
Specifying server shutdown and recovery options . . . 67

Chapter 7. Remote client/server connections . . . 69
Connecting clients and servers . . . 69
Methods of connecting client to server . . . 69
Authority required . . . 70
About instructions in these sections . . . 70
Client/server TCP/IP communications . . . 70
Prerequisites . . . 70
Tasks on the server . . . 70
Tasks on the client . . . 71
Client/server modem communications . . . 71
Prerequisites . . . 71
Tasks on the server . . . 71
Tasks on the client . . . 72
Client/server serial communications . . . 72
Prerequisites . . . 72
Tasks on the server . . . 72
Tasks on the client . . . 73

Part 3. "Classic" features . . . 75

Chapter 8. Message collector . . . 77
Controlling message processing . . . 77
SA IOM's implementation . . . 77
Sending messages from your application to SA IOM . . . 78
Uses of the Message Collector . . . 78
Consolidating messages to a single console display . . . 78
Interacting with the Message Collector . . . 79
Server-to-server messaging . . . 79
SA IOM to SA IOM network connections . . . 79
Sharing system resources using the Message Collector . . . 80
Sending a message to a Message Collector . . . 80
Before you start . . . 80
Sending the message . . . 80
Monitoring the Message Collector session . . . 80
REXX functions to use with the Message Collector . . . 81
Message Collector logging . . . 81
MSGCLECT.LOG file example . . . 81
Message Collector sample programs . . . 81
Windows . . . 81
UNIX . . . 84

Chapter 9. Peer-to-peer communications . . . 85
TCP/IP-based peer-to-peer communications . . . 85
"Types" of peer-to-peer communication . . . 85
Peer functions . . . 86
AF-to-AF usage scenarios . . . 87
Scenario 1 . . . 87
Scenario 2 . . . 87
Scenario 3 . . . 88
Scenario 4 . . . 88
About "non-AF" peer conversations . . . 88
About "non-header" peer conversations . . . 89
Peer communications protocol . . . 90
Peer-to-peer communications protocol language . . . 90

Peer-to-peer message packet format 91
Linkid or Message Token parameter 91
Data Type parameter 92
Reply Data Length parameter 94
Send Data Length parameter 94
Send Data parameter 95

Chapter 10. Beeper paging 97
Sending optional text 97
Optional message text 97
Touch-tone versus modem paging 97
Touch-tone paging requests 98
Modem paging services 98
Tuning for modem-to-modem paging 99
Automatic paging 99
What triggers automatic beeper paging 99
Fine-tuning a touch-tone WTOR 101
Initial procedure 101
Testing procedure 101
Calculating delays 102

Chapter 11. Voice control 103
Controlling a voice adapter 103
Installing Dialogic voice adapters 103
Text-to-speech support 104
Installation 104
Configuration notes 105
Configuring the SA IOM server for voice adapter use 105
Creating voice applications 106
Voice functions 106
Recording messages 106
Getting listener responses 107
Beeper paging with a voice adapter 107
Voice diagnostic and debugging facilities 108
Recovery and error processing 108
Voice operation diagnostic logging information 109

Chapter 12. SA IOM Hardware Management Console interface 111
HMC interface overview 111
Description of HMC network components 111
S/390 PTS configuration with SA IOM 111
Configuring the SA IOM HMC interface 112
SA IOM server configuration 112
Configuring the z9-109 HMC for use with SA IOM 113
HMC console configuration (OS/2 Warp Connect 4.0) 113
Testing and verification 114
Connecting the SA IOM HMC interface PC to the HMC 115
Using the SA IOM HMC interface 116
Navigation commands 116
How to navigate 116
Action commands 117
Action command syntax 117
Operating system commands 117
Additional commands 118
Status conditions 118
Modes 118
HMCACT.REX automation interface program 119
HMCACT.REX 119
Format 119
Example 120

Return codes 120

Chapter 13. Configuring TN3270E sessions 121
Configuring TN3270E support in SA IOM. 121
Configuring the TN3270E server 122
Configuring SA IOM session definitions 122
IBM 2074 connection considerations 125
Configuring MVS MCS console definitions with the IBM 2074 Console Support Controller 126
MVS TCP/IP configuration issues 126
Copying and pasting in TN3270E sessions. 127
Consolidating 3270 Sessions using SLF 128

Chapter 14. SA IOM problem determination 133
Begin by checking available logs 133
Format of log files. 134
Configuration errors 134
Network errors. 134
Hardware errors 134
Acquiring STATE-level logs. 135
Modem connection problems and documentation needed by IBM 136
Direct serial client/server connection problems 137
3270 Coax PCI connection problems. 138

Chapter 15. Utility programs 139
RpLogRd.exe 140
RpRunRex.exe 142
RpSend.exe 144
RpSesClr.exe. 146

Part 4. Alert escalation feature 149

Chapter 16. Administrator tasks for alert escalation 151
Post-installation administrator tasks 151
Access roles for SA IOM alert escalation 152
Creating user groups in Integrated Solutions Console 153
Assigning access roles to user groups in ISC 154
Creating users in Integrated Solutions Console 154
Assigning users to groups in Integrated Solutions Console 155
Administering users and user groups in Integrated Solutions Console 155
Changing passwords for users in Integrated Solutions Console. 155
Deleting user IDs in Integrated Solutions Console 156
Deleting groups in Integrated Solutions Console. 156
Administering the alert escalation database 156
Changing alert escalation passwords on the database side 157
Changing the rpweb to database password 158
Changing the SA IOM server to database password 159
Starting and stopping WebSphere Application Server on Windows 159
| Netcool/OMNIbus integration 160
| Configure ad hoc notification 161
| Set up a new peer-to-peer address 161
| Set up SA IOM servers 161
| Changing the DBNotify database. 162

Chapter 17. Alert escalation 163
Using the Web interface 163
Logging on 163
About 164
Manage policies 164
Manage alerts 174

| Ad hoc alert escalation 177
Defining a policy 180
Testing a policy. 181
Stopping escalation 182
Acknowledging an alert 182
Disabling an alert escalation policy 184
Alert status 185
Level of escalation. 186
Notification 186
E-mail notification. 186
Pager notification 187
Script notification 187
SMS notification 188
Voice notification 188
| Ad hoc notification 189
| Multiple server support 189
Helper scripts 189
Schedules 192
Automatically starting escalation 193
Display problems 193
Filtering, searching, and sorting tables 194
Configuring your Web browser 195
Troubleshooting SA IOM alert escalation 196

Part 5. Deprecated features 197

Chapter 18. Connecting to host systems 199
Setting up mainframe 3270 hosts 199
IBM and Amdahl 3270 ports 199
Configuring IBM and Amdahl 3270 ports 200
Cabling IBM and Amdahl 3270 ports 200
Configuring MVS on IBM/Amdahl mainframes 200
Amdahl 5995M support 200
Serial ports 200
Configuring serial ports 200
Cables and connectors 201
Cabling terms you should know 201
Cabling serial ports 202
Telnet and SA IOM 203
Testing TCP/IP Telnet on Windows 203

Chapter 19. Installing 3270 Emulation Adapters. 205
Setting up 3270 adapters for SA IOM 205
Summary of installing 3270 adapters 205
Supported 3270 adapters 205
Installing adapters in an ISA bus machine 206
Summary of steps 207
Notes about ISA 3270 adapters 207
IBM 3270 adapters (ISA bus) 208
Attachmate advanced 3270 adapters (ISA bus) 208
IRMA 3t adapters (ISA bus) 210
IRMA 3t adapters in IRMA mode (ISA bus) 210
IRMA 3t adapters in IBM mode (ISA bus) 210
Installing adapters in a PCI bus machine 211
Installing Attachmate IRMA PCI adapters 212
Configuring 3270 PCI adapters for SA IOM 213
How SA IOM assigns PCI slots to 3270 sessions. 213
Physical versus detected PCI slot order. 214
Determining the detected PCI slot order 216
Additional notes 217

Problem resolution 217

Chapter 20. Keyboard Support 219
Windows NT 122-key keyboards 219
122-key keyboard layout DLLs 219
122-key keyboard features 219
Japanese 106-key keyboard support 220
Configuring 122-key keyboards 220
Configuring SA IOM client to use 122-key keyboard 220
TN3270E keyboard support. 221

Part 6. Appendixes 223

Appendix A. SA IOM sample scripts 225

Appendix B. Client profile 231
Enforcing single client execution 231
Remapping the Enter key for 3270 sessions 231
Remapping the DUP key for 3270 sessions 232
Additional information on keyboard remapping. 232
Enabling or disabling 3270 console alarm beep 233
Disabling selected client pop-up messages. 233
Enabling serial com port journaling 233
Enabling cursor blink and block 234
Adjusting compatibility to an older server. 234

Appendix C. Server profile. 235
Enabling duplicate logon support 236
Enabling the Telnet server 236
Compressing TCP/IP client-server data. 237
Appending to a log rather than restarting it 238
Modifying the disconnect time interval. 238
Setting the server log trace level 238
Selecting VT emulation function key maps 239
Changing the default SA IOM keyboard mapping 240
Disabling selected server pop-up messages 243
Configuring a "non-header" peer communication port. 243
Extended voice return codes 244
Multiplexing direct serial client/server connections. 244
Enable serial com port journaling. 245
AFR_SEND_3270 keyboard delay parameter 245
Controlling initialization and termination behavior of Object REXX RXAPI.exe 245
Message Collector options 247
TN3270E EBCDIC code page assignment 247
TN3270E bind-image feature 248
Password validation 248
User change password during logon 249
AFR_USER REXX functions 249
AFR_NOTIFY REXX functions and alert escalation options 249
Encryption options 250
| Enable IPv6 support 250
| Audit log support 250

Appendix D. TN3270E operational information 251
TN3270E color support 251
With the 3270 Extended Data Stream option 251
Without the 3270 Extended Data Stream option 252
OIA status indicators 252
OIA Status indicators in SA IOM. 252

What these symbols mean 252
Other symbols 253
Reporting problems to IBM. 253

Appendix E. TCP/IP error codes 255
Common TCP/IP error codes 255

Appendix F. Messages 257

Index 273

Notices 279
Copyrights 280
Trademarks 280

Figures

1. Typical connection using an IBM 2074 console support controller 121
2. Wiring Diagram, DB-25 to DB-25 null modem pin-outs 202
3. Wiring Diagram, DB-9 to DB-9 null modem pin-outs 203
4. Wiring Diagram, DB-9 to DB-25 null modem pin-outs 203
5. Wiring Diagram, DB-9 to DB-25 adapter cable 203

Tables

1. SA IOM makes the following default port assignments 18
2. Windows Service - start server methods 35
3. Windows Service - stop server methods 36
4. Server subsystem/component states 45
5. Client Control window panels 46
6. REXX script states 47
7. User status values 50
8. Message Collector Functions 79
9. Comparison of touch-tone and modem paging 98
10. SA IOM 2.1 is installed with the following set of executable files and their associated logs 133
11. SA IOM configuration files 134
12. SA IOM 2.1 utility programs, summarized 139
13. Status modes of an alert 185
14. Alert escalation notification methods and associated helper script names. 190
15. The standard input parameters passed to notification helper scripts 190
16. Additional input parameters passed to notification helper scripts 191
17. Version A, IBM 3278/79 adapter sample switch settings (ISA bus) 208
18. Version B, IBM 3278/79 adapter sample switch settings (ISA bus) 208
19. Configuration settings for IBM (ISA bus) 208
20. Attachmate adapter sample switch settings (ISA bus) - "newer" 209
21. Attachmate adapter sample switch settings (ISA bus) - previous 209
22. DIP switch functions for Attachmate (ISA bus) 209
23. Configuration settings for Attachmate (ISA bus) 210
24. IRMA 3t adapter switch settings (ISA bus) 210
25. IRMA 3t adapter sample switch settings-alternate (ISA bus) 211
26. Configuration settings for IRMA 3t in IBM mode (ISA bus) 211
27. 3270 key assignments in TN3270E emulation mode 221
28. Default Enter key behavior 231
29. Keys on your keyboard 232
30. Keys on a 3278 keyboard 232
31. Customization options available in the server profile, rpsvrprf.txt 235
32. Remappable keys 240
33. TN3270E supported color 252
34. TCP/IP Error Codes 255

About This Document

This guide explains how to customize and operate IBM® Tivoli® System Automation for Integrated Operations Management (SA IOM).

Who should read this document

This guide is intended for users who are familiar with IBM PC-compatible computers, Windows® operating systems, and the hardware and software of the host computer systems that will be connected to SA IOM.

How this document is organized

This document contains the following sections.

- Part 1, “Getting started,” on page 1 provides an overview of what the product does, information to help you plan your SA IOM configuration, product installation details, how to log on for the first time as a system administrator, and how to start and stop the server and client components.
- Part 2, “"Classic" user and administrator tasks,” on page 41 describes some of the basic SA IOM operations including an overview of the SA IOM Client and Server control windows, how to configure the client and server for your site, and guidelines for establishing connections between clients and servers using the remote connection methods.
- Part 3, “"Classic" features,” on page 75 provides detailed information about the Message Collector, peer-to-peer communications, beeper paging, voice control (using adapters), the SA IOM HMC interface, configuring TN3270E sessions, and various logs and utility programs that can aid you in debugging your configuration of these.
- Part 4, “Alert escalation feature,” on page 149 describes the configuration, and user and administrator tasks of this most advanced optional feature of SA IOM.
- Part 5, “Deprecated features,” on page 197 describes physically connecting to Host Systems using coaxial cables that attach to the SA IOM server, installing 3270 emulation adapters in the SA IOM server, and the keyboards supported by the coaxially-connected host systems.

Notices and statements used in this document

The following types of notices and statements are used in this document:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.

- **Danger:** These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure step or situation.

Using the documentation

IBM provides the following set of documentation for v2.1:

- *System Automation for Integrated Operations Management User's Guide*
- *System Automation for Integrated Operations Management REXX Functions Reference*
- *System Automation for Integrated Operations Management Quick Start Guide*

These documents are available as PDF files on the product media.

Printing this document

IBM supplies documentation in the Adobe® Portable Document Format (PDF). The Adobe Acrobat Reader will print PDF documents with the fonts, formatting, and graphics in the original document. To print a document, do the following:

1. Specify the print options for your system. From the Acrobat Reader Menu bar, select **File > Page Setup** and make your selections. A setting of 300 dpi is highly recommended, as is duplex printing if your printer supports this option.
2. To start printing, select **File > Print** on the Acrobat Reader Menu bar.
3. In the Print window, select one of the **Print Range** options for:
   - All
   - Current page
   - Pages from: [ ] to: [ ]
4. (Optional.) Select the Shrink to Fit option if you need to fit oversize pages to the paper size currently loaded on your printer.

Printing problems?

The print quality of your output is ultimately determined by your printer. Sometimes printing problems can occur. If you experience printing problems, potential areas to check are:

- Settings for your printer and printer driver. (The dpi settings for both your driver and printer should be the same. A setting of 300 dpi is recommended.)
- The printer driver you are using. (You may need a different printer driver or the Universal Printer driver from Adobe. This free printer driver is available at www.adobe.com.)
- The halftone/graphics color adjustment for printing color on black and white printers (check the printer properties under **Start > Settings > Printer**). For more information, see the online help for the Acrobat Reader.
- The amount of available memory in your printer. (Insufficient memory can cause a document or graphics to fail to print.)

For additional information on printing problems, refer to the documentation for your printer or contact your printer manufacturer.

Contacting Adobe

If additional information is needed about Adobe Acrobat Reader or printing problems, see the Readme.pdf file that ships with Adobe Acrobat Reader or contact Adobe at **(www.adobe.com)**.

Adding annotations to PDF files

If you have purchased the Adobe Acrobat application, you can add annotations to IBM documentation in .PDF format. See the Adobe product for instructions on using the Acrobat annotations tool and its features.

New in this release

This section lists the changes that were made to this version and release of IBM Tivoli System Automation for Integrated Operations Management (SA IOM).

New product name

This product, IBM Tivoli System Automation for Integrated Operations Management (SA IOM), has been re-branded. The previous product version was known as "IBM Tivoli AF/REMOTE®".

Alert escalation feature

The alert escalation feature provides the ability to notify a sequence of individuals about an alert based upon criteria that you define. For any particular alert, you define the person or persons to contact, and how such persons will be contacted. Schedules can be used to specify who to call, or who not to call, at dates and times that you define. You can optionally define levels of escalation for each alert. For more information about using the feature, see Part 4, “Alert escalation feature,” on page 149.

The alert escalation notification data and policies are stored in a DB2® database that is created for you at installation time. A Web interface based on the IBM Integrated Solutions Console (ISC) is used to interact with the database. The alert escalation feature and the "classic" product (the SA IOM server and client components running on Windows) communicate with each other using TCP/IP and the REXX™ programming language. For more information about software associated with this feature, see Chapter 2, “Planning your SA IOM configuration,” on page 11.

REXX enhancements

- SA IOM V2.1 supports Open Object REXX.

  For details see “REXX support requirements (optional)” on page 22.
- There are additional REXX functions in this release.

  For details see the *System Automation for Integrated Operations Management REXX Functions Reference*.

Security enhancements

- "Secure TSO Terminal" is added to the list of types of emulation sessions you can configure on the SA IOM server. If your emulation session is configured as "Secure TSO Terminal", and you forget to log off from your session, SA IOM will automatically log off for you when you close the session window in the SA IOM client.

The following security enhancements are implemented as server profile parameters.

- You can optionally configure user data encryption between server and client.
- You can optionally specify that Windows security will authenticate logons to the SA IOM server, or specify that only the SA IOM server will authenticate logons to the SA IOM server.

- You can optionally allow these same options to be specified using REXX.
- You can optionally allow SA IOM users to change their own passwords during the logon process.
- You can optionally allow SA IOM users to change their own passwords using REXX.

Other enhancements

- You can copy and paste within a TN3270E emulation session. This is described in “Copying and pasting in TN3270E sessions” on page 127.
- Peer-to-peer communications can be configured to allow one special peer session per SA IOM server that does not include the binary header information. This is described in “About "non-header" peer conversations” on page 89.

Documentation changes

This section describes the changes to the documentation.

The documentation more accurately reflects the product.

User comments and suggestions have been incorporated.

Technical documents (such as "DCF Technotes") have been incorporated.

Index entries have been improved.

This book has been divided into parts to draw attention to deprecated features.

Part 1. Getting started

Chapter 1. Learning About SA IOM 3
SA IOM overview 3
SA IOM and the client/server model 4
How SA IOM works 5
Host system connectivity 5
System consoles 5
What is a host? 5
Client connectivity 5
Peer connectivity 6
Automation and notification 6
Message Collector capability 6
REXX-based extensibility 7
SA IOM features 7
Emulation features 7
Hardware Management Console emulation support 7
Telnet 3270 terminal emulation 7
Telnet terminal emulation 7
Serial terminal emulation 7
3270 terminal emulation using 3270 adapters (deprecated) 7
REXX scripts 8
Additional security features of SA IOM servers and clients 8

Chapter 2. Planning your SA IOM configuration 11
Planning overview 11
Client and server security and Windows. 12
SA IOM and Windows security 12
Windows Service security considerations . . . 12
Software requirements. 14
Software requirements for the server 14
Software requirements for the client 14
Software requirements for the Web-based user interface 14
Software requirements for the database 14
Description of installation components 15
The SA IOM installation program. 15
SA IOM executable programs 15
Server program 15
Service program. 15
Service Manager program 16
Client program 16
Web-based user interface and database software (optional) 16
Encryption software 17
Unicode software 17
Support DLLs and drivers 17
System DLLs 17
README file. 17
Default configuration and log files. 17
Sample REXX programs 17
TCP/IP considerations. 18
SA IOM TCP/IP port usage. 18
SA IOM server and client TCP/IP KEEPALIVE support. 19
About modems 19
About configuring modems 20
Using modems for SA IOM client/server communication 20
Using modems for other SA IOM purposes . . 20
Modem recommendations 20
About direct connections 20
Direct connection requirements. 21
About hardware adapters. 21
TN3270E connections 21
Voice adapters 21
LAN adapters 21
Serial port expansion adapters 21
3270 adapters (deprecated) 22
REXX support requirements (optional) 22
About REXX on Windows 22
Supported software for REXX support 22
Making Object REXX available to users running SA IOM server 23
TN3270E operational environment. 23
About the TN3270E environment 23
3270 emulation requirements (deprecated) 24
About 3270 emulation adapters. 24
Supported 3270 emulation adapters 24
Voice control requirements (optional). 24
Beeper paging and time acquisition requirements (optional) 25
Beeper paging requirements. 25
Time acquisition requirements 25
Beeper paging and time acquisition can share a port 25
SA IOM as a Windows Service. 25
Windows Services 25
Client/Server compatibility considerations 26
Where to go from here 26

Chapter 3. Installing and configuring SA IOM . . 27
Installing and verifying SA IOM 27
Installing SA IOM 27
Installing SA IOM sample scripts 30
Verifying SA IOM installation 30
Client and server profile parameters 31
Locating new client and server profile parameters 31
Logging on to SA IOM the first time. 31
Logging on to the server from a local client . . 31
Renaming the server 32
Uninstalling SA IOM (optional) 32
Installing modems 33
Adding modems to the Windows environment 33
Testing modems. 34

Chapter 4. Starting and stopping SA IOM . . . 35
Starting and stopping the server 35
Starting the server 35
Stopping the server. 36
Connecting to a server from a configured client . . 38

Before you start 38
Logging on 38
Configuring the client 39
Before you start 39
Defining a server connection 39
Difficulty connecting 39
Defining general properties of the client 39

Chapter 1. Learning About SA IOM

This chapter provides an overview of SA IOM.

Topics in this chapter

The following topics are discussed in this chapter:

- "SA IOM overview"
- "How SA IOM works" on page 5
- "SA IOM features" on page 7

SA IOM overview

SA IOM is a client/server application that assists you in performing host systems management tasks from either a local or remote location, using a comprehensive set of emulation, access, screen analysis, and notification tools.

Using SA IOM, you can:

- Access and control your mainframe and distributed systems by connecting to the SA IOM server from your personal computer or laptop, which may be located in your office, a different data center, or even your home.
- Monitor the status of distributed point-of-sale systems through SA IOM's Message Collector facility.
- Monitor and maintain your environment control systems, such as the Liebert SITESCAN system.
- Use the REXX programming language and a library of special SA IOM functions to automate practically any task you do manually. You can IPL a mainframe, perform complicated beeper paging scenarios, or synchronize all your mainframes to a national time service as easily as you can start a REXX program.

  With the addition of a supported voice adapter, you can create event-driven applications that call a person, play prerecorded voice messages, and act upon touch tone responses.
- Use SA IOM's peer-to-peer communication services to send messages to and receive messages from other TCP/IP hosts, including other SA IOM systems, Tivoli AF/OPERATOR® systems, and any other socket-connected applications.
- SA IOM using the IBM Integrated Solutions Console (ICS) and using other components described later in this book, provides an alert escalation feature that can notify a predefined list of subject matter experts in case a computer center application problem occurs.

When used as a standalone product, SA IOM allows remote access from LAN- or modem-based connections to a large family of systems and service consoles. Through its REXX-based automation capabilities, event trapping and notifications are also supported.

When integrated with other IBM products, such as IBM Tivoli AF/OPERATOR, SA IOM provides REXX-based console message analysis and actioning capabilities

that amplify the automation functions of the IBM product family and extend its reach to midrange computers, and environment control platforms not normally supported by other IBM products.

SA IOM and the client/server model

SA IOM is based on a standard client/server application model, which allows any authorized user to log on from the SA IOM client to one or more SA IOM servers. Once the client/server connections are established, you use the client to interact with connected SA IOM servers.

All activities, with the exception of initially starting and stopping the server, are performed from the SA IOM client. You use the client to view and interact with active sessions on the server, to manage the log, and to perform server configuration. If you need to update the server configuration, you can automatically restart the server from the client and then log back on.

You can install the SA IOM server either as a Windows Service or as a Start Menu application. When installed as a Windows Service, the SA IOM server process starts at system-boot time and runs in the background until someone logs onto the Windows system, at which time the server status window becomes visible. Starting SA IOM as a Windows Service simplifies remote management of the server and is particularly useful for unattended data centers.

How SA IOM works

This section describes the SA IOM functional capabilities.

Host system connectivity

The SA IOM server can connect to more than one host system at a time, and these host sessions can be distributed to multiple clients.

System consoles

System consoles, also called operator consoles, are specialized interactive components of system applications used to monitor and control the application. An MVS™ operator console is an example of a system console, with SA IOM providing the session emulation.

You can view and manipulate system consoles from any authorized SA IOM client, with SA IOM supporting the required special control keys and escape sequences.

What is a host?

In SA IOM, a host is any source of information delivered into the SA IOM system. Host information is presented to SA IOM clients as *host sessions*.

SA IOM supports the following kinds of host sessions:

- 3270 terminal emulation sessions using two distinct methods:
  - Telnet 3270 Enhanced sessions (for example, to connect to the IBM OSA Integrated Console Controller)
  - 3270 coax sessions (for example, using a supported 3270 emulation adapter to connect to a 3270 coaxially-connected server)[1]
- Direct Serial sessions
- Message Collector sessions
- Telnet sessions
- REXX sessions

Client connectivity

When a client is installed on the same PC as a server, that client is the server's *local client*, and the server, in relation to the client, is the *local server*. This is the typical installation on a server, as you use the client to interact with the server.

When the client resides on a remote PC connected through a LAN, modem, or serial port, it is called a *remote client*.

Remote LAN-connected, modem-connected, and serial-connected SA IOM clients are equivalent in capability to the local client.

Note: Server modem configuration can only be performed from the local client.

With SA IOM:

- You can access multiple servers from one client.
- Multiple users on different clients can view the same session and interact with each other.

1. Note the older 3270 adapter-based connection method is deprecated as IBM no longer makes 3270 coaxial controllers or 3270 emulation adapters. These belong to a previous generation of technology.

Peer connectivity

Using this product's peer communication services, your REXX scripts running under SA IOM can send messages to and receive messages from a different SA IOM system, a Tivoli AF/OPERATOR system, a legacy Tivoli AF/REMOTE system, or any TCP/IP host.

If you have implemented Tivoli AF/OPERATOR, then you can use AF/OPERATOR to trap messages and then notify SA IOM to perform a paging or other notification action. In this fashion, you can avoid writing screen trapping logic in REXX scripts under SA IOM.

If your site runs multiple SA IOM servers, you can implement one SA IOM as a notification server. That is, you can set up the alert escalation feature or concentrate voice cards and outgoing telephone lines under *one* server, and have other SA IOM servers send notification requests, thus decreasing the overall implementation cost.

Each SA IOM server is protected against unauthorized peer access. The SA IOM server will accept messages only from approved peer addresses.

Automation and notification

SA IOM supports triggered notification processes using its REXX script interface.

This means that you can use SA IOM external REXX functions to write REXX programs that perform any action that a live operator at a console might perform.

Many of the automation functions are driven by SA IOM's trap management facility. The SA IOM trap manager allows search conditions to be defined for text appearing in the host session screen output. When the search text matches, the supplied function reacts. We call this *trapping* on a message.

The ability to trap on a message and the ability to forward the message or to start a process using a REXX script, makes many things possible. For example, you can create simple or complex notification scenarios to contact a person using a variety of notification methods such as e-mail, pager, phone, and so on. With the addition of the alert escalation feature, you can automatically notify an alternative person in the reporting chain if a critical notification message has not been acknowledged within a predefined time period.

Message Collector capability

SA IOM supports TCP/IP-based application message collection.

Through the Message Collector, messages sent by remote systems over a TCP/IP link can be searched for trap conditions and accessed by external applications. Messages sent to a specified server port are gathered and presented to the SA IOM client as a host session. Messages are streamed through the trap processing and client session presentation facilities, as if the message stream constituted a TCP/IP-connected host.

You can send status messages to a Message Collector session using a variety of methods that are described in Chapter 8, "Message collector," on page 77.

REXX-based extensibility

SA IOM includes:

- An interface to the REXX programming language
- SA IOM REXX functions
- IBM-provided sample scripts

With the addition of REXX, you have the tools to program new SA IOM operations or customize existing ones to your needs. Though some effort is required to learn to customize REXX scripts, the value of being able to adjust operations to suit your environment will become evident the more you use the product.

The ability to customize SA IOM is a key feature, and a strength.

SA IOM features

This section describes key features of SA IOM.

Emulation features

With SA IOM, you can emulate hardware consoles and terminals for both IBM and non-IBM mainframe computer systems.

Hardware Management Console emulation support

The optional SA IOM Hardware Management Console (HMC) interface allows you to remotely monitor and manage resources in the IBM zSeries® HMC environment.

Telnet 3270 terminal emulation

SA IOM supports Telnet 3270 (TN3270) terminal emulation, which means that SA IOM TN3270 and Telnet 3270 Enhanced (TN3270E) host sessions can be configured and connected to MVS consoles and VTAM® applications. With TN3270E terminal emulation, SA IOM can operate with the IBM OSA Integrated Console Controller.

Telnet terminal emulation

With SA IOM, you can establish sessions using Telnet connections to access other host systems through the TCP/IP network. For example, by emulating Telnet in ANSI or VT 100 mode, you can access other host systems like UNIX®, or other Windows host systems that are connected through the TCP/IP network.

Serial terminal emulation

SA IOM supports the use of up to 32 serially connected hosts using VT100, VT220, VT420, HP2392, ANSI, and ASCII terminal emulation. Serial hosts are directly connected to the SA IOM server.

3270 terminal emulation using 3270 adapters (deprecated)

SA IOM supports 3270 terminal emulation using its own 3270 device drivers, which support ISA and PCI 3270 emulation adapters.

Notes:

1. The addition of a supported adapter is a requirement for 3270 terminal emulation using adapters. The modern method of emulating a 3270 terminal is to use Telnet 3270 Enhanced (TN3270E) terminal emulation.
2. The supported 3270 adapters are no longer produced by IBM or Attachmate.

SA IOM can support up to twelve 3270 adapters. (The actual number of emulation adapters that can be supported depends on the number of available internal and external expansion slots on the SA IOM server, and the amount of real and virtual memory.)

You can run as many separate 3270 emulation sessions as you have available expansion slots in the server. These sessions can all be on one mainframe or on different mainframes.

Each session can emulate the following console or terminal types.

- Hardware consoles for zSeries and many legacy mainframe models, such as: IBM 3090™, 308x, 43xx, ES/9000® (water cooled), Amdahl 5880, Amdahl 5890, Hitachi EX/CF, and so on.
- MVS operating system consoles
- OMEGAMON® consoles
- VTAM terminals
- Standalone application terminals
- Any other IMS™ console or VM or VSE terminal

REXX scripts

SA IOM is designed to make full use of the REXX programming language. The product supports customized REXX scripts.

In SA IOM, REXX scripts are used to:

- Select and interact with connected host sessions
- Interact with connected users
- Activate traps and process their results
- Drive user-defined notification (beeper, voice, e-mail) functions
- Interface with external, non-SA IOM applications

SA IOM features complete control of REXX scripts from within SA IOM.

In SA IOM, an active REXX script functions as a REXX:

- Host application that can request input and generate output like other connected hosts.
- Emulator capable of presenting screen output to attached client sessions like other host emulators.
- User session capable of receiving generated data, sending new data, and defining and acting on trap conditions.

Additional security features of SA IOM servers and clients

In addition to Windows security, the "classic" SA IOM server and client components provide their own user authorization and resource access controls.

To access the SA IOM server, a user must provide a user ID and password. SA IOM can be configured to use either its own user authentication method or to rely on the Windows environment to provide user authentication. This is a server customization option. SA IOM configuration files are fully encrypted. User authentication parameters are fully encrypted. The ability to encrypt all communication between SA IOM clients and servers is a server customization option.

A given user can be restricted to using the SA IOM client application only from a designated “call back” telephone number or from a designated TCP/IP domain name (or IP address). In addition, depending on the user group to which a user is assigned, a user’s access to REXX scripts and to the sessions of other SA IOM users can be controlled.

Default user groups are provided so that the roles and authorities of different SA IOM users can be easily defined.

Access to host sessions can be restricted by assigning a session class. You can control which user groups can access which classes of host sessions.

Access to a particular host session can be further secured by defining the 3270 Emulation Properties of the session itself to have a **Usage** of "Secure TSO Terminal".

Only SA IOM peers at specified IP addresses may access a given SA IOM server. Client/server connection time-outs can be defined, so the server connection will be automatically closed if not used. All user connection attempts to the server are logged for auditing purposes.

Chapter 2. Planning your SA IOM configuration

This chapter provides information to help you plan your SA IOM configuration.

Topics in this chapter

The following topics are discussed in this chapter:

- "Planning overview"
- "Client and server security and Windows" on page 12
- "Software requirements" on page 14
- "Description of installation components" on page 15
- "TCP/IP considerations" on page 18
- "About modems" on page 19
- "About direct connections" on page 20
- "About hardware adapters" on page 21
- "SA IOM as a Windows Service" on page 25
- "REXX support requirements (optional)" on page 22
- "TN3270E operational environment" on page 23
- "3270 emulation requirements (deprecated)" on page 24
- "Voice control requirements (optional)" on page 24
- "Beeper paging and time acquisition requirements (optional)" on page 25
- "Client/Server compatibility considerations" on page 26
- "Where to go from here" on page 26

Planning overview

Before you install and configure SA IOM, you need to determine the needs of your site. This includes:

- Determining your SA IOM server's hardware and software requirements
- Reviewing the concepts presented in this chapter

SA IOM is easy to install because it uses a standard InstallAnywhere application. Subsequent configuration can be either a short or a lengthy process depending on the types of optional hardware and software that your network requires.

SA IOM supports many hardware and software configuration options and many optional features.

The foremost optional feature is the SA IOM Alert Escalation feature. SA IOM Alert Escalation uses a Web browser interface which is administered using the IBM Integrated Solutions Console (ISC). ISC uses its own security features which are part of its Web application server.

This document uses the following terms:

1. The "console" to refer to ISC.
2. The "admin console" to refer to the Administration console of ISC.
3. "Server" to refer to the SA IOM server, and "client" to refer to the SA IOM client–both of which run in a "classic" Windows environment.

4. “Classic SA IOM” in conjunction with the server and client if necessary to distinguish these required product components from the optional Web-based components.
5. MVS to refer to the z/OS® operating system.

Client and server security and Windows

This section provides information about SA IOM server and client security in the Windows environment.

The "classic" SA IOM server and client components rely on Windows security and conform to it.

Note: SA IOM also provides an additional level of security as described previously in “Additional security features of SA IOM servers and clients” on page 8.

SA IOM and Windows security

Your Windows security implementation effects your implementation of the SA IOM server and client components. As a Windows application, SA IOM operates in the Windows security environment, therefore

- Access to all Windows resources, including files and processes, is controlled, with access controls associated with individual users or named groups of users. You can use the Windows NTFS file system to control access to configuration files, REXX scripts, or the SA IOM server program itself. (FAT file system configurations are also supported.)
- Windows users must uniquely identify themselves at login-time to access system functions. The SA IOM server can be accessed only by Windows users who have either local or network login access to the PC that runs the SA IOM client. By default, SA IOM users do not require a Windows login to the PC that runs the SA IOM server. However, the product can be customized to verify logins to the SA IOM server using only Windows security, instead of using SA IOM security.
- The SA IOM client should be installed using the authority of the person who will be using it to access the SA IOM server. For example, if the SA IOM client is installed with administrator authority then administrator authority will be required to access the client application. (This may not be as you intended.)
- Memory is protected such that it cannot be read after it is freed by a process. SA IOM runtime data, including user security data, cannot be accessed by non-SA IOM applications.
- Windows security-related events are logged and access to this information is limited to authorized Windows administrators.

Note: You can use the Event Viewer, available from Windows Administrative Tools, to interrogate these events.

Windows Service security considerations

When the SA IOM server is installed as a Windows Service, SA IOM operators must have Windows Administrator or Windows Power User authority to be able to start and stop the SA IOM Service.

Authorized SA IOM operators can use the Windows Services applet or the SA IOM Service Manager to perform the start and stop functions and to view the

current status of the SA IOM Service.

Software requirements

This section lists basic requirements for the SA IOM server, the SA IOM client, and the components used to support the optional SA IOM alert escalation feature. Additional hardware and software requirements depend on your choice of optional features. Take special note of "REXX support requirements (optional)" on page 22.

Software requirements for the server

These are the software requirements for installing the SA IOM server in a Windows environment.

Component	Software Requirements
SA IOM server	One of the following Windows versions: • Windows Vista Enterprise or Business 32 bit • Windows XP Professional Edition, with Service Pac 2 or above • Windows 2003 Professional server or workstation And, the SA IOM server must be installed on a Latin-1 configured windows machine.

It is recommended that you dedicate the PC that runs the SA IOM server to the task of running SA IOM.

Software requirements for the client

These are the software requirements for installing the SA IOM client in a Windows environment.

Component	Software Requirements
SA IOM client	One of the following Windows versions: • Windows Vista Enterprise or Business 32 bit • Windows XP Professional Edition, with Service Pac 2 or above • Windows 2003 Professional server or workstation And, the SA IOM client must be installed on a Latin-1 configured windows machine.

Software requirements for the Web-based user interface

These are the software requirements for installing the Web-based user interface in a Windows environment.

Component	Software Requirements
"Web-based UI"	One of the following Windows versions: • Windows Vista Enterprise or Business 32 bit • Windows XP Professional Edition, with Service Pac 2 or above • Windows 2003 Professional server or workstation

Software requirements for the database

These are the software requirements for installing the database component in a Windows environment.

Component	Software Requirements
"Derby"	One of the following Windows versions: • Windows Vista Enterprise or Business 32 bit • Windows XP Professional Edition, with Service Pac 2 or above • Windows 2003 Professional server or workstation

Description of installation components

The SA IOM installation media contains all prerequisite software *except REXX*. The following software components are *briefly* described in this section:

- The installation program
- SA IOM server and client executable programs
- Web-based user interface and database software (optional)
- Encryption software
- Unicode software
- Support DLLs and drivers
- System DLLs
- README file
- Default configuration and log files
- Sample REXX programs

The SA IOM installation program

The SA IOM installation program is a standard InstallAnywhere application that guides you through installation of SA IOM and optional features.

SA IOM executable programs

As part of SA IOM installation, a server program is installed on each SA IOM server and a client program is installed on each SA IOM client. The installation default is to install a client program on the same PC as the SA IOM server, where it runs as a local client.

The SA IOM server can be installed as either a Start Menu application or as a Windows service. When installed as a Windows service, an intermediate service process, `rpsvrsvc.exe`, starts the SA IOM server process `rpserver.exe`, which then executes in its standard manner. In addition, the SA IOM Service Manager component, `rpsvcmgr.exe`, is installed to support the Windows service interface and configuration.

Server program

The SA IOM server executable program, `rpserver.exe`, runs on the server PC.

When the `rpserver.exe` software is running, a small window, called the Server Control Window, is displayed to show the status of the SA IOM server. This also provides the mechanism to start and stop the server.

Service program

The Windows Service executable program, `rpsvrsvc.exe`, runs on the server PC.

In a Windows Service environment the `rpsvrsvc.exe` software starts the service, which then starts the server process `rpserver.exe`. When Windows is first booted,

the service status window displays. After you log on, the service status window will be hidden and the Server control window will display the status of the SA IOM server.

Service Manager program

The SA IOM Service Manager executable program, `rpsvcmgr.exe`, runs on the server PC.

The Service Manager program provides an interface to start and stop the server and modify various service parameters.

When the `rpsvcmgr.exe` program is running, the SA IOM Service Manager window is displayed.

Client program

The SA IOM client executable program, `rpclient.exe`, provides the interface for all SA IOM user interactions with the server program.

When the `rpclient.exe` program is running, the Client Control Window is displayed.

Web-based user interface and database software (optional)

The SA IOM installation default is to install the software required by the alert escalation feature onto the same PC as the SA IOM server. This ensures that the feature's best performance is achieved. The feature takes up very little space, as delivered.

However the two separately-installable components, one identified in the installation as the Web-based user interface, `rpweb.exe`, and the other identified as Derby, can each be installed on separate PCs if desired.

The "Web-based UI" component installs the following software.

IBM Integrated Solutions Console Advanced Edition 7.1
: The Integrated Solutions Console (ISC) administers different IBM products using a single Web-based console. It includes an embedded version of IBM WebSphere® Application Server, V6.1. The SA IOM installation program installs ISC and the "SA IOM Alert Escalation" console module, which is a Web application that is accessed from ISC.

IBM DB2 Run-Time Client 8.2 for Windows
: This is the prerequisite database component necessary to access the alert escalation database.

The "Derby" component installs the following software.

Apache Derby 10.2.2.0
: An included version of Apache Derby is used to manage the alert escalation database. Apache Derby, an Apache DB subproject, is an open source relational database management program implemented entirely in Java™. If you want additional information about Apache Derby, see the Apache Derby Web site at the following address.

  `http://db.apache.org/derby`

Encryption software

Encryption is provided by the included IBM Crypto for C (ICC) package. ICC uses the Advanced Encryption Standard (AES) cryptographic algorithm with a 128 bit key as the crypto type. This server prerequisite is automatically installed. All message traffic between this product's client and server can be encrypted. (This is an optional server profile customization.)

Unicode software

International Component for Unicode (ICU) is a server prerequisite and is automatically installed.

Support DLLs and drivers

SA IOM uses dynamic load libraries (DLLs) on the server and client to implement the serial and modem communication protocols, as well as the VT, HP, 3270, and ASCII emulation protocols. A REXX supported DLL is used when REXX access is necessary. HMC Interface DLLs are used when HMC access is necessary.

A device driver, `rp3270.sys`, is installed to manage communication with 3270 COAX devices.

System DLLs

SA IOM requires the following system DLLs, which are copied during product installation to your Windows system directory if they do not already exist, or if they are more current than the versions you already have.

Component	Description
COMCTL32.DLL	WIN32 Common Controls
INETWH32.DLL	WIN32 WinHelp Internet Access
MFC90.DLL	Microsoft® Foundation Class Library 9.0
MFCM90.DLL	Microsoft Foundation Class Managed Library 9.0
MSVCRT.DLL	Visual C Run Time Library
PSAPI.DLL	WIN32 System Functions Access

README file

The README.TXT file contains the latest information about SA IOM, which may not be included in this guide. Read this file before you begin using SA IOM.

Default configuration and log files

User and system default configuration files are included so that SA IOM system administrators can initialize SA IOM and define additional SA IOM users.

Empty log files are provided so that a subsequent uninstall of SA IOM will identify them as installed files and delete them.

Sample REXX programs

Sample REXX scripts are provided with SA IOM. All sample programs are commented to assist customization.

See Appendix A, "SA IOM sample scripts," on page 225 for more information about SA IOM sample scripts.

TCP/IP considerations

SA IOM uses the TCP/IP communications protocol via the Windows Winsock facility for several key functions:

- TCP/IP Client/Server Connections
- Host session connections via Telnet
- Host session connections via TN3270E
- Message Collector
- Integrated Telnet Server Support
- Peer-to-Peer Communications Support
- Network Messaging REXX APIs, such as AFR_SEND_MESSAGE and AFR_SEND_RPAGE

To ensure correct operation of SA IOM functions using TCP/IP, it is important to consider the TCP/IP address (or hostname) and the port number assignments so that conflicts with other system and application functions do not occur. Also, consider TCP/IP configuration parameters, typically defined in the Windows registry.

SA IOM uses fixed hostnames or IP addresses and does not provide special firewall support.

SA IOM TCP/IP port usage

Table 1. SA IOM makes the following default port assignments

Port number	**SA IOM Assignment**
1035	TCP/IP client connections
1040	TCP/IP peer connections (standard)
1090	Message collector
Note the port assignments cannot use the same number.	

Default port assignments used by SA IOM may also be used by other processes running on the SA IOM server or client machine. By design, SA IOM reuses port connections, and as a consequence may be unable to detect that a port previously used, is currently in use by a different process. This can result in unpredictable behavior affecting TCP/IP and local client connections. It can also affect the ability of the SA IOM server to gracefully shutdown, which it must do when recycling after a configuration edit. When the SA IOM server does not cleanly shutdown, new client network connections may fail or hang.

To ensure best operation of SA IOM, select port assignments for SA IOM functions that do not conflict with port assignments used by other applications and services. Be aware that many port assignments, such as those acquired by the operating system for network file system mounts, are variable and may change across an operating system restart or a file mount/dismount. Often, a conflicted port shows its effect, not when the current SA IOM instance shuts down, but when the following instance shuts down.

To understand port usage on your SA IOM machine, open a Command Prompt and execute the Windows netstat command shown below. In this example, the output of the netstat command is written to the file, NetStatResults.txt:

```
netstat -a  >  NetstatResults.txt
```

When SA IOM has cleanly shutdown and is no longer running, the ports used by it should not show netstat entries or should show themselves in a TIME_WAIT state. A port used by SA IOM that remains in a LISTENING state when the SA IOM process is not running may indicate an unsound Winsock environment. SA IOM usually restarts and continues to work satisfactorily, however, you may decide to reboot the SA IOM machine before restarting SA IOM.

SA IOM server and client TCP/IP KEEPALIVE support

By design, TCP/IP does not guarantee immediate or timely notification to a TCP/IP peer that a network availability problem has occurred, or that a connected peer application or machine is no longer available. Although different TCP/IP stack implementations can vary, under Windows a delay of up to two hours can occur before a peer is notified of a problem so that it can cleanly shutdown its TCP/IP (Winsock) connection.

The principal TCP/IP parameter governing the size of this interval in Windows is the TCP/IP KEEPALIVE parameter. The KEEPALIVE parameter, specified in the Windows registry of a peer machine, defines the interval at which TCP/IP "heartbeat" packets are sent from the peer to other connected peers. As mentioned, the Windows default for this parameter is two hours, the value used when a KEEPALIVE parameter is not defined.

The KEEPALIVE setting affects all applications using TCP/IP running on the SA IOM machine, and may cause degraded performance due to the additional network traffic. However, average network speeds have improved to the point where client-side KEEPALIVE is reasonable.

SA IOM, defines at install-time a KEEPALIVE interval of 20 seconds in its server and client installs. On the server side, the SA IOM server is notified by the TCP/IP stack (Winsock) of the loss of client connection within about 20 seconds of the occurrence. This notification allows the TCP/IP stack to clean up its client connection and release the information it holds on the logged-in user. On the client side, the SA IOM client recognizes an SA IOM server crash or a network outage within about 20 seconds.

Note: After the initial server and client installation, you must fully power down the machine and then power up to ensure full physical re-initialization of the network card/router connection. Only when this step is performed can a new KEEPALIVE setting become completely activated.

Modification of the TCP/IP KEEPALIVE parameter is a non-configurable function performed when the SA IOM server or client is installed. Only under atypical circumstances should this parameter need to be modified or disabled.

About modems

This section provides information about configuring and using modems.

The server and client can be configured to communicate with each other remotely, using modems. In this case, the Windows Telephony Service is used to control the modems.

SA IOM also makes use of modems to support the beeper paging notification and time acquisition features. In this case, the SA IOM server controls these features using REXX.

About configuring modems

Like other pieces of hardware, modems can only be configured from the physical location where they are installed.

For this reason, we highly recommend you follow instructions for "Installing modems" on page 33 so that you will not need to return to an installation site to re-configure a modem at a later time. Server modems must be configured using a local client.

Using modems for SA IOM client/server communication

When the server and client use modems to communicate with each other, both modems use the Windows Telephony Service.

Using modems for other SA IOM purposes

When the SA IOM server uses modems for other supported features, such as beeper paging notification and time acquisition, the modems are controlled using the SA IOM REXX serial communication functions. The Windows Telephony Service is not used.

Modem recommendations

IBM makes no specific recommendations for modems.

However both serial and USB modems by USRobotics are successfully used at existing customer sites.

Choose modems supported by Windows. Modems must be recognized by the Windows environment before they can be configured for SA IOM use.

You might want to consider the future growth of your SA IOM system. The optional hardware you can install on the server is limited by the number of internal expansion slots available in the server PC. If your server's modem is one of the internally installed types, it will occupy one of a limited number of internal expansion slots that could be used for one of the adapters discussed in "About hardware adapters" on page 21.

About direct connections

This section provides information about direct connections.

The server and client can be configured to communicate with each other remotely, using direct connections. SA IOM also makes use of direct connections to host systems that support:

- HP 2392 emulation
- VT protocol emulation (VT100, VT220, VT420)
- Glass Teletype (an unspecified ASCII device)

A direct connection means to directly cable a serial communications port on the server to the serial communications port of another computer. This other computer can be another PC or any host computer with an RS-232C serial communications port.

Direct connection requirements

Direct connections require:

- An RS-232 serial communications cable.

  You will need to build or purchase a null modem cable that can support full handshaking of the control lines.
- Close physical proximity of the server and the other computer.

  We recommend that installed RS-232 serial communication cables not exceed a maximum of 50 feet. Exceeding this length can cause random data errors as the capacitance of the cable increases with its length. The recommended maximum length also depends on the baud rate. Using a baud rate of 38,400 bps the length of the installed serial communication cable should not exceed 25 feet.

About hardware adapters

This section **briefly** describes the optional hardware adapters you might use in an SA IOM configuration. These adapters fit into the internal expansion slots on the SA IOM server PC.

TN3270E connections

SA IOM includes support for the TN3270E protocol using the IBM OSA Integrated Console Controller.

This requires a LAN adapter which is compatible with your specific OSA ICC configuration. See “TN3270E operational environment” on page 23.

Voice adapters

With a supported **voice adapter**, you can use REXX to write event-driven voice applications. See “Voice control requirements (optional)” on page 24 for more information about voice adapters.

You can also use a supported voice adapter for non-critical beeper paging applications. Chapter 10, “Beeper paging,” on page 97 discusses the advantages and disadvantages of using a voice adapter for touch-tone paging.

LAN adapters

With a LAN adapter, you can:

- Provide SA IOM clients with TCP/IP LAN access to the SA IOM server.
- Emulate Telnet sessions.
- Allow TCP/IP access to the Message Collector.

IBM provides no recommendations for LAN adapters.

Serial port expansion adapters

Serial port expansion adapters emulate serial ports. You can use adapters of this type to increase the number of available serial communication ports (COM ports) on the server PC.

The server uses serial communication ports for:

- Attaching external modems, which can be used for
  - Modem connections with clients
  - Beeper paging
  - Time acquisition
- Attaching null modem cables which can be used for
  - Direct serial connections with clients
  - Direct serial connections with host systems

If your server supports REXX, as described in "REXX support requirements (optional)," serial ports on the server can be configured for script use. This gives the SA IOM REXX functions access to the serial port. Serial ports configured for script use are used for beeper paging, time acquisition, communications port functions, and modem functions.

3270 adapters (deprecated)

One way that the SA IOM server can control supported mainframe models is by emulating a 3278/79 model 2 or model 4 terminal. And one way to do this is using a variety of supported 3270 emulation adapters which, for simplicity, are called **3270 adapters** in this guide.

See "3270 emulation requirements (deprecated)" on page 24 for more about 3270 adapters.

REXX support requirements (optional)

This section provides information on REXX support requirements.

SA IOM requires REXX to be installed on the server in order to provide:

- Automation of tasks on server-connected hosts.
- Notification by pager, e-mail, or voice application.
- Support for the alert escalation feature.
- Support for the peer-to-peer communication feature.
- Trapping of host session information.
- Support for the HMC Interface feature.
- Support for you to customize or develop new REXX programs.

About REXX on Windows

The supported software to enable REXX support is Open Object REXX. (This is an Open Source Project. See below.)

IBM Object REXX for Windows is no longer available for sale. (However, if you already have a supported version installed, SA IOM will use it. See below.)

Supported software for REXX support

SA IOM supports the following software to provide REXX support on Windows.

Component	Software Requirements
SA IOM server with REXX support	The requirements listed in "Software requirements for the server" on page 14 and **one** of the following: • Open Object REXX Version 3.1.2 Available for download from the following Web site.`http://www.oorexx.org/` • IBM Object REXX for Windows Development Edition, Version 2.1.3 Note: If both Open Object REXX and IBM Object REXX are installed on the same machine unpredictable results may occur.

Making Object REXX available to users running SA IOM server

To use the REXX automation feature of SA IOM, you must install one of the supported REXX products listed above. However, the IBM Object REXX installation program does not require the user performing the install to have Windows administrator privileges. Therefore, the Object REXX product does not have the All Users attribute of common products.

As a result, it is possible for IBM Object REXX for Windows to be installed but not available to the user who is running the SA IOM server. This situation will be detected during SA IOM server initialization, generating an error message that indicates the REXX Management component failed to initialize.

To remedy this problem, do one of the following:

- Log on as the user who installed IBM Object REXX and start the SA IOM server from that user ID.
- Add the IBM Object REXX directory to your system path, so that its modules will be available to all Windows user IDs.
- Reinstall IBM Object REXX from the user ID that will be starting SA IOM.

TN3270E operational environment

This section describes the operational requirements for TN3270E, which requires an IBM OSA Integrated Console Controller. For further information on configuring TN3270E support, see Chapter 13, "Configuring TN3270E sessions," on page 121.

About the TN3270E environment

SA IOM's TN3270E feature supports MVS MCS console sessions, TSO/ISPF, CICS®, IMS, and VM. While other applications may operate successfully, the testing, configuration, and problem determination of other session types are not currently supported by IBM. SA IOM's TN3270E support operates with a LAN adapter in the SA IOM server, connected to a TN3270E server which completes the host access.

In comparison to earlier and now deprecated methods of 3270 support in SA IOM, TN3270E support replaces a specialized 3270 adapter card and special coaxial cable connection with a generic LAN adapter and general-purpose cabling. The host access in previous 3270 support was provided by an IBM 3174 controller (or

equivalent). TN3270E support relies on a TN3270E server attached to the network to transport and transform information for host access. SA IOM continues to support 3270 coax connections via 3270 hardware adapters. An SA IOM server can have both 3174-connected coax and TN3270E-based connections.

Note: IBM does not make specific recommendations regarding your LAN adapter, but the TN3270E server may have specific requirements in this area.

3270 emulation requirements (deprecated)

This section provides information on the optional 3270 emulation requirements. SA IOM requires the addition of a supported 3270 adapter to provide this type of 3270 emulation.

Notes:

1. 3270 emulation using adapters is not the preferred method.
2. TN3270E is the modern method. For information on TN3270E requirements, see "TN3270E operational environment" on page 23.

About 3270 emulation adapters

Optional 3270 emulation adapters fit into expansion slots in the SA IOM server. The 3270 emulation adapters are physically connected to 3270 host systems using coaxial cables, so close physical proximity between a 3270 host and the SA IOM server is required.

Supported 3270 emulation adapters

SA IOM supports 3270 emulation adapters of the following types.

- **On the ISA bus:**
  - Attachmate Advanced 3270 Adapter/2
  - IBM 3270 Connection (Version A and B)
  - IRMA 3t 3270 Coax Adapter
- **On the PCI bus:**
  - Attachmate IRMA PCI adapter (CIP-based)

Note: If you use Extra Version 6.2 for emulation on the SA IOM server, and Extra is already configured to use Attachmate 3270 ISA adapters or IBM 3270 ISA adapters, and you then install the Attachmate IRMA PCI adapter (CIP-based), Extra will stop working. This is a problem known to Attachmate and occurs whether or not SA IOM is present.

Voice control requirements (optional)

This section provides information on voice control requirements.

The ability to create voice recording and playback applications, such as voice notification, using the SA IOM REXX functions requires:

- A Dialogic voice adapter installed and configured on the SA IOM Server PC

  Note: These adapters are no longer in production, see the list in Chapter 11, "Voice control," on page 103.
- REXX support, see "REXX support requirements (optional)" on page 22
- A serial communication port configured for script use

To learn more about what is involved in setting up voice control see Chapter 11, “Voice control,” on page 103.

Beeper paging and time acquisition requirements (optional)

This section provides information on the beeper paging and time acquisition requirements.

Beeper paging requirements

The server’s ability to perform automated beeper paging notification requires:

- A modem

  Note: For non-critical beeper paging applications, a supported voice adapter could be used instead of a modem. Chapter 10, “Beeper paging,” on page 97 discusses the advantages and disadvantages of using a voice adapter for touch-tone paging.
- A paging service provider, see Chapter 10, “Beeper paging,” on page 97
- REXX support, see “REXX support requirements (optional)” on page 22
- A serial communication port configured for script use

Time acquisition requirements

The server’s ability to perform time acquisition, which means automatically updating the clock on the server PC, requires:

- A modem
- REXX support, see “REXX support requirements (optional)” on page 22)
- A serial communication port configured for script use

Beeper paging and time acquisition can share a port

Because the time acquisition and beeper paging features both use a COM port infrequently, they can share a COM port configured for script use.

Both features will wait for the COM port to become available.

SA IOM as a Windows Service

This section provides information about running SA IOM as a Windows service.

Windows Services

A Windows Service is a user-mode process registered with the Windows environment that has the ability to be automatically started at system-boot time. Windows Services can be referred to as background processes. Services do not require a user logon to execute and they can span user logons and logoffs.

Service programs use functions that connect to the Windows Service Control Manager (SCM) and send status to the SCM. The SCM starts services and has the ability to command a service to stop, pause, or continue its operation.

You can interactively manipulate services from the Administrative Tools **Services** applet. From this Services applet you can:

- View the status of the service
- Stop and start the service

- View and modify service parameters

You can also administer services from the Administrative Tools **Computer Management** applet, where other useful administrative applications, such as the Device Manager, can be found.

Client/Server compatibility considerations

An SA IOM client can communicate with an AF/REMOTE server and vice versa.

As a rule, always edit the server configuration using a client at the same level as the server or at a later level than the server.

The configuration parameters can effect client/server compatibility. For example, the server can be configured to reject client connections from clients that do not support encryption.

Where to go from here

Once you have determined your hardware and software needs, you need to:

1. Install SA IOM. See Chapter 3, "Installing and configuring SA IOM," on page 27.
2. Configure SA IOM servers, sessions, and users. See Chapter 6, "Administering SA IOM software," on page 55.

Chapter 3. Installing and configuring SA IOM

This chapter explains how to install SA IOM and logon for the first time as a system administrator.

This chapter assumes that you are familiar with the Windows environment and that your Windows network is already operational.

Topics in this chapter

The following topics are discussed in this chapter:

- "Installing and verifying SA IOM"
- "Client and server profile parameters" on page 31
- "Logging on to SA IOM the first time" on page 31
- "Uninstalling SA IOM (optional)" on page 32
- "Installing modems" on page 33

Installing and verifying SA IOM

This section describes how to install SA IOM and verify its installation.

Installing SA IOM

SA IOM uses the InstallAnywhere program by Macrovision Corporation for installation. InstallAnywhere provides you with a series of step-by-step dialog boxes to guide you through installation. Once you make your selection in a dialog box, click **Next** to go to the next dialog. You can click **Previous** to go to back and change your choices any time before you click **Install** to download files.

Important:

1. The JAVA_HOME environment variable is extremely important to the install process.
2. The installation will fail with unpredictable results when the JAVA_HOME environment variable is present but the Java component is not installed. Therefore, delete the JAVA_HOME environment variable if there is no Java installed on the target PC.
3. If the JAVA_HOME environment variable is present and is set to a valid bin directory of a preinstalled version of Java, then the installation will use the indicated version of Java that is already installed on the target PC.
4. If the JAVA_HOME environment variable is not present, the install process installs a version of Java, sets the JAVA_HOME environment variable accordingly, then proceeds.

Follow these instruction to install SA IOM using default values:

1. Insert the program media into a suitable drive. If the program does not start automatically, you may need to go to the Control Panel to install and configure system components.

   Result: The SA IOM installation program displays the Introduction panel. Click Next.
2. The License Agreement displays. you must accept the terms to proceed with installation. Click Next.

3. The Choose Product Features panel displays. In general, InstallAnywhere distinguishes between these "Install Sets"

   Full Install
   Installs all components. This is the default.

   Selective Install
   Install selected components. Deselect components that you do not want to install. The installable component choices are: Server, Client, Web interface (including prerequisites, for the SA IOM alert escalation feature), and Derby (the alert escalation database component). The online instructions provide a brief description of each selection.

   Choose what you would like to install, then click **Next**.

The following instructions assume that you took the default, Full Install. If you did not, ignore instructions for panels that are not presented to you.

4. The Choose Install Folder panel displays. The default installation destination is *C:\Program Files\IBM\SA IOM*, but you have the option to change the destination. Click Next.
5. At this point, the installation program checks for dependencies and may display an Information panel. For example, if an installation of IBM REXX is found on the target machine, it may be used for REXX services. Otherwise, you are prompted to download ooRexx to be used for REXX services. Follow the suggested instructions on any Information panel that may display at this point. To proceed with product installation, click **Next**.

The following panels prompt you for several sets of user IDs and passwords that are needed to configure the SA IOM alert escalation feature. You may find it convenient to print out this section to keep track of the password values that you supply here.

6. The Derby Administrator Configuration panel prompts you for the following values.

```
Derby Server Connection Port         1527

Derby Administrator User ID         rpadmin

Derby Administrator User ID Password

Please confirm the password
```

   You have the option to change the default "Derby Server Connection" port and "Derby Administrator" user ID values. These default to 1527 and rpadmin. You must supply a password in the field provided. Confirm the password by supplying it again in the next field. Click **Next**.

7. The RpServer to Derby Connection Configuration panel prompts you for the following values.

```
RPServer to Derby DB Connection User ID     rpserver

RPServer to Derby DB Password

Please confirm the password
```

You have the option to change the default "RpServer to Derby DB Connection" user ID value. The default is rpserver. You must supply a password in the field provided. Confirm the password by supplying it again in the next field. Click **Next**.

8. The Web interface to Derby Connection Configuration panel prompts you for the following values.

```
Web interface to Derby Connection User ID    rpweb

Web interface to Derby Password

Please confirm the password
```

You have the option to change the default "Web interface to Derby Connection" user ID value. The default is rpweb. You must supply a password in the field provided. Confirm the password by supplying it again in the next field. Click **Next**.

9. The Embedded WebSphere Web interface Configuration panel prompts you for the following values.

```
Web interface Profile Name           AppSvr01

Web interface Server Name           server1

Web interface Administrator User ID      iscadmin

Web interface Administrator Password

Please confirm the password
```

You have the option to change the default "Web interface Profile" name and "Web interface Administrator" user ID values. These default to AppSvr01 and iscadmin. The name of the Web interface Server, server1, is fixed and can not be modified. You must supply a password in the field provided. Confirm the password by supplying it again in the next field. Click **Next**.

10. At this point, if the installation program detects it, you may be prompted as follows:

```
The installer detected an old installation of AFRemote.
Do you want to copy config files of the old installation for RPServer and RPClient?
```

The **Copy files to new product installation** checkbox is selected by default.

- If you want to copy your existing AF/REMOTE configuration files to your vanilla SA IOM installation, click **Next**.
- If you do not, then first deselect the checkbox, then click **Next**.

11. The RpServer Service Configuration panel displays.

The **Start RpServer as Service** checkbox is selected by default.

Starting SA IOM as a Windows Service simplifies remote management of the server and is particularly useful for unattended data centers. Otherwise, the server will be executed as a Start Menu application (and someone will have to start it).

Note: If this is a reinstall over an existing server installation, you cannot change the server's installation mode from Start Menu application to

Windows Service or vice-versa. To change the startup mode, you must first uninstall the server.

Click **Next**.

12. The Icon and Menu Configuration panel displays. It indicates that Desktop icons, Quick launch icons, and Start Menu application listings will be created by default. Deselect any of these that you do not want to install, otherwise you get them all. Click **Next**.
13. The Pre-Installation Summary displays installation information for you to review. Ensure that the information is as you intended, and that there is sufficient disk space for you to install the components you selected. If not, you can go back and change your choices before you download any software. When you are ready to proceed, click **Install** to begin copying files.
14. While the various installation component files download, the Installing IBM Tivoli System Automation IOM v2.1 panel displays. Various status messages and a moving status bar indicate the progress of the installation process.
15. When the installation process has finished correctly, the Installation Log can be found in *C:\Program Files\IBM\SA IOM\install\logs*.
16. If you installed components that included the server, you are asked if you want to restart Windows now or later.

    Note: You must restart Windows to implement the SA IOM device driver. We also recommend you restart Windows if you have installed or reinstalled the server as a Windows Service.

Installing SA IOM sample scripts

When SA IOM server is installed for the first time, the SA IOM sample scripts are installed into the `\scripts` subdirectory.

When an existing SA IOM installation is updated, existing REXX script files in the \scripts subdirectory are not overlaid with the same-named scripts copied from the installation CD. This step is taken to protect any modifications customers may have made to their SA IOM-supplied scripts. Instead, the latest versions of the SA IOM-supplied sample scripts are always installed into the `\scripts2` subdirectory. We therefore recommend that after you install a new SA IOM maintenance level, that you inspect the script files in the `\scripts2` subdirectory to identify possible changes. If there are updated sample scripts, you may want to incorporate them into the versions you execute out of the `\scripts` subdirectory.

Verifying SA IOM installation

Follow these steps to verify that SA IOM is installed:

1. Click the Start button on the Task Bar to display the Start menu. Select **Programs** to display the Programs menu.
2. From the Programs menu, select **IBM Tivoli System Automation IOM v2.1**. You should see menu items for the components you selected to install. For example, the **SA IOM Client** and the **SA IOM Server**. If you chose to install the server as a Windows Service, you will see the **SA IOM Server Service Manager** menu item. If you chose Full Install, you will also see Start and Stop menu items for the Web-based user interface and database components used by the alert escalation feature.
3. You can use the **IBM Tivoli System Automation IOM v2.1** menu items to run any of the product components that you installed.

Client and server profile parameters

Client and server profiles contain parameters that customize some SA IOM functions, for example: mapping the keyboard and allowing duplicate logons. In general, the parameter defaults are set to provide backwards compatibility with previous versions.

At installation time, you might consider modifying client and server parameters to:

- Enforce single client execution
- Allow duplicate logons
- Enable a Telnet server
- Compress TCP/IP client-server data

To consider all the parameters that you can modify, see Appendix B, "Client profile," on page 231 and Appendix C, "Server profile," on page 235.

Note: Profile parameters can be modified at any time, however you must restart the server or client to implement them.

Locating new client and server profile parameters

If you are installing a new SA IOM maintenance level on top of an existing installation, there is already a copy of the server profile file, `rpsvrprf.txt`, and client profile file, `rpcliprf.txt`, in your `\config` subdirectory (assuming you have both the server and client components installed).

Because customers often modify these profile files, the installation script does not overlay existing copies of the files. As a result, you will not find the newest profile parameters in your `\config` subdirectory if you are installing on top of an existing SA IOM installation.

The latest versions of `rpsvrprf.txt` and `rpcliprf.txt` are always installed into the `\config2` subdirectory. To make use of a new profile parameter, you must first locate the relevant parameter statements in the `\config2` version of the profile file, and then copy and uncomment those statements in the `\config` subdirectory version of the profile file. SA IOM client and server startup only read the copy of the profile file that is found in the `\config` subdirectory.

Logging on to SA IOM the first time

Before you can configure SA IOM for other users, you need to log on to SA IOM using a default Administrator account and perform your first configuration task, renaming the server.

Logging on to the server from a local client

Follow these steps to log on to the server from the local client:

1. Start the SA IOM server and client programs from the Windows Start Menu. If the server was installed as a service, then you can also start the server by starting the **SA IOM Service**.
2. Open the SA IOM server and client control windows.

   Note: The SA IOM server control window will already be open if you selected Windows Service as the start mode.

3. From the Client control window, on the Servers and Sessions panel, select (double-click) the **SAIOM1** server entry in the list.

   Result: The SA IOM Logon to Server SAIOM1 panel displays.

4. In the **User ID** field, type Administrator. In the Password field, type password (all lowercase) and then click **OK**.

   Result: SA IOM should display a message indicating that the logon was successful to server SAIOM1. You are now logged on to the server and have full system administrator authority. By selecting the Config menu option on the SA IOM client, you can define other user IDs, add host sessions, and perform all server configuration tasks.

To safeguard the security of your system, it is recommended that you define a new administrative password immediately. It is also recommended that your first task on each server you install, should be to change the server name from "SAIOM1" to a unique server name that is consistent with your SA IOM network plan. A properly configured server has a unique server name.

Renaming the server

To rename the server, proceed as follows:

1. From the **Config** pull-down on the SA IOM client, select **Server**, and then select **SAIOM1**.

   Result: The Server Configuration Properties dialog displays.

2. Select **General** to display the General page.
3. In the **Server Name** field, replace the name "SAIOM1" with a new server name.
4. When you are finished, click **OK** to complete the server configuration.
5. When prompted to save all changes, select **Yes**.
6. When prompted to restart the server, select **Yes**.

   Result: The Server Configuration Properties dialog closes. The server re-initializes and the new server name is visible in the **Server control** window at the top of the Server Status display. (Select **OK** to each Informational message. These messages are duplicated in the server log.)

Other server configuration tasks, such as adding users, are described in Chapter 6, "Administering SA IOM software," on page 55.

Notice that the name that appears in the client control window on the **Servers and Sessions** panel did not change. The name that appears on the **Servers and Sessions** panel is called the *server connection name*. This name is an alias for the server name. You supply the server connection name as part of client configuration, which is described in "Configuring the client" on page 39.

Uninstalling SA IOM (optional)

This section describes how to remove SA IOM from your system.

Make sure that the server and client, and any other installed components, are *not* running before you uninstall them.

To uninstall SA IOM, use the Control panel Add/Remove Programs interface that Windows provides.

You can choose between a complete or a selective uninstall process. If you want to uninstall the whole product, choose **Complete Uninstall**. Otherwise choose **Uninstall Specific Features** to select the specific component or components that you want to uninstall.

If you have added any files to the directories and subdirectories where SA IOM was installed, such as new REXX script files, then the Uninstall process will complete without removing all the files and directories associated with SA IOM.

The report, which the Windows interface produces, will show that the directories and subdirectories containing the newly added files could not be removed. This is a normal expected result since the Uninstall process can only know about, and delete, files that it copied during installation.

To complete the uninstallation and removal of all SA IOM directories, you need to manually delete any new files you added.

Notes:

1. The uninstallation of the SA IOM server can also complete with errors if the IBM Object REXX API process, `RXAPI.EXE`, holds a lock on the `\bin` directory from where the SA IOM server was executed. The symptom of this problem is that the `\bin` directory will not be removed even though every file in it is gone. If this occurs, you will need to terminate the `RXAPI.EXE` process in order to remove the SA IOM `\bin` directory.
2. DB2 lite is not removed when you remove SA IOM. Use the Control panel Add/Remove Programs interface that Windows provides to uninstall DB2 lite.
3. The JRE is not removed when you remove SA IOM. You can delete the JRE manually.

After uninstall, accept the reboot option to finish.

Installing modems

This section describes how to install modems.

If you will be using modems with SA IOM, set them up and verify their operation as described in this section. Modems must be recognized by the Windows environment before they can be used by SA IOM.

Adding modems to the Windows environment

Install a modem on a server or client PC as follows:

1. Stop and close all SA IOM components before installing a modem.
2. The Windows Telephony Service uses a driver called **TAPI Kernel-Mode Service Provider**. Check to make sure this driver is installed on your PC by selecting Phone and Modems Options from the Windows Control Panel. If the TAPI driver is not already listed on the Phone and Modem Options Advanced page, add it to your Windows configuration. (This is a Windows configuration option. No additional software is required.)
3. Add modems to your computer setup by selecting Add Hardware from the Windows Control Panel. The Add Hardware Wizard will guide you through the Install New Modem process. If you have a modem problem, refer to the Windows Help topic: Modem troubleshooter.

Note: After you have successfully installed the modem, you can adjust, if necessary, each modem's properties for baud rate, data bits, parity, and stop bits from the Phone and Modems Options, Modem, Properties dialog.

SA IOM will ignore any Dialing Properties you supply to the Windows Telephony Service. Numbers to be "dialed" by the modem must be supplied to the SA IOM configuration.

Once a modem is properly configured in the Windows environment, it is considered a valid device and will be added to the configurable SA IOM modem list.

Testing modems

To test the ability of each installed modem to dial out, use the HyperTerminal application available from the Accessories menu.

Chapter 4. Starting and stopping SA IOM

This chapter explains how to start and stop SA IOM, by starting and stopping SA IOM's server and client components.

Topics in this chapter

The following topics are discussed in this chapter:

- "Starting and stopping the server"
- "Connecting to a server from a configured client" on page 38
- "Configuring the client" on page 39

Starting and stopping the server

This section describes how to start and stop the server.

Starting the server

If you have selected to run the server as a Start Menu application, the server starts if you select it from the Windows Start Programs option.

Windows Vista

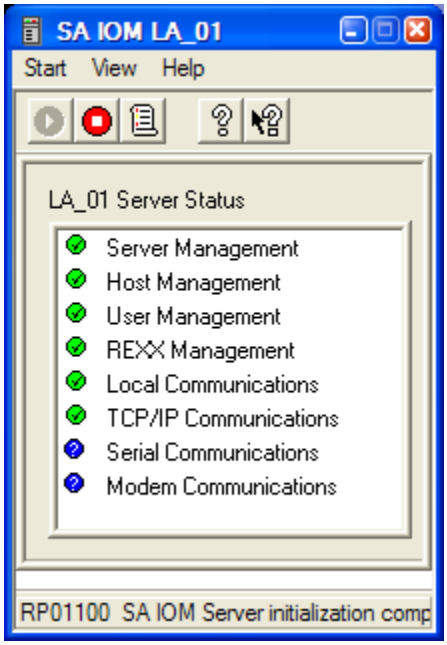
Set the server to "run as administrator" to ensure that it operates correctly when running under Vista.

If you have selected to run the server as a Windows Service, the server can be started in one of the following ways:

Table 2. Windows Service - start server methods

Start Method	Description
Automatically when Windows boots	If installed as an "automatic" mode Windows Service, the server is started automatically by the SA IOM Service after service initialization is complete. The Windows Service Control Manager (SCM) insures that all prerequisite services and drivers are started before the SA IOM Service is started. You can change the start mode using the SA IOM Service Manager or the Windows Services applet.
Manually using the SA IOM Start menu	If installed as a "manual" mode Windows Service, the user must take some explicit action to start the SA IOM Service. Selecting the **SA IOM Server** option from the SA IOM Start menu, causes the SA IOM Service to be started and the service will then start the server.
Manually using the SA IOM Service Manager application	You can start the SA IOM server from the SA IOM Service Manager. Selecting the **Start** button on the Service page of the SA IOM Server Manager, causes the SA IOM Service to start and the service will then start the server.
Manually using the Windows Control Settings Services applet	From the Windows Services applet, you can pick the service and then select the **Start** button. This will cause the SA IOM Service to start and the service will then start the server.

Result: The Server control window opens. Here is a Server control window for the successfully started server named LA_01.



The Server Status panel displays green check marks next to any components that started successfully. For a description of the other Server Status states, see "Server component states" on page 44.

Stopping the server

If you have selected to run the server as a Start Menu application, to stop the server you can select **Stop Server** from the Start menu in the Server control window or select the Stop Server icon from the Toolbar.

If you have selected to run the server as a Windows Service, the server can be stopped in one of the following ways:

Table 3. Windows Service - stop server methods

Stop Method	Description
Automatically when Windows shuts down	If installed as an "automatic" mode Windows Service, the server will be stopped automatically by the SA IOM Service when it gets a shutdown request from the Windows Service Control Manager (SCM), using one of the shutdown options defined below. The SA IOM Service will then allow itself to exit.
Manually using the SA IOM Service Manager application	You can stop the SA IOM server from the SA IOM Service Manager. Selecting the **Stop** button on the Service page of the SA IOM Server Manager, causes the SA IOM Service to stop the server, using one of the shutdown options defined below. The SA IOM Service will then allow itself to exit.
Manually using the Windows Control Settings Services applet	From the Windows Services applet, you can pick the service and then select the **Stop** button. This will cause the SA IOM Service to stop the server, using one of the shutdown options defined below. The SA IOM Service will then allow itself to exit.

The SA IOM Service supports the following shutdown options:

Normal shutdown	The server closes just as if you selected **Stop Server** on the Server control window.
Fast shutdown	The server terminates immediately.

The default option is **Normal shutdown**.

You can set the shutdown option using the SA IOM Service Manager. The option parameter is maintained in the Windows registry space for the service.

Result: The Server control window remains open. The Server Status panel displays blue question marks next to any components that stopped successfully. Any connected clients were disconnected when the server stopped. Here is a Server control window for the successfully stopped server named LA_01.

Connecting to a server from a configured client

This section describes how to log on to SA IOM as a user.

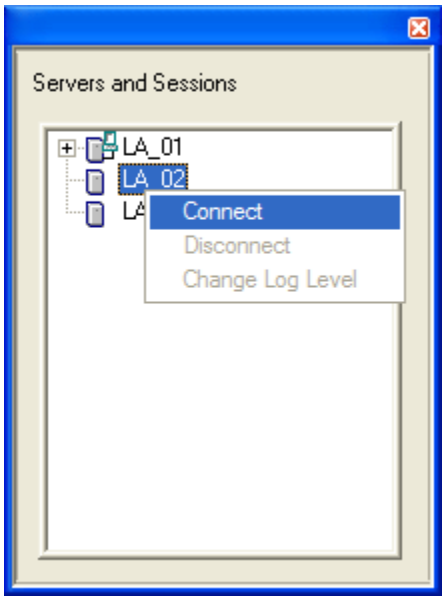
Before you start

Contact your system administrator for your user ID and password.

Logging on

Follow these steps to log on from a configured client:

1. Open the SA IOM Client control window.
2. On the Servers and Sessions panel, select the name of the server that you will connect to.
   (If the name of the server is not listed, you need to configure the client).



. To connect to the server, either double-click the server name, or right-click and choose Connect.

   Result: The Logon to Server panel displays.
3. In the **User ID** field, type your user ID.
4. In the **Password** field, type your password.
5. In the **New Password** field:
   - If you want to change your password, type a new one here, and reenter it in a subsequent **Confirm New Password** field that will be presented when you click OK.
   - If you do not want to change your password, leave the **New Password** field blank.
   - If the **New Password** field is gray or does not appear on the Logon to Server panel, it has possibly been disabled by the administrator of the SA IOM server.
6. Click **OK**.

   Result: SA IOM displays a message indicating that you are successfully connected to the server.

Configuring the client

This section describes how to configure the client. You must define a server connection before you can connect to a server. Any user who can access and execute the SA IOM client can configure the client.

Before you start

You may need to consult a system administrator to obtain the information required to establish the server connection.

Defining a server connection

Follow these steps to define a server connection.

1. From the **Config** pull-down on the SA IOM client, select **Client**.

   Result: The Client Configuration Properties dialog displays.
2. Using the mouse, right click and select **Add** from the menu to display the Server Connection page.
3. Supply information about the server:
   - Type a server connection name and optional description.
   - Select the connection method for communicating with the server. For example, if the method is modem-connected, specify which modem on the client PC to use to contact the server.
   - If you are communicating via TCP/IP with the IPV6 protocol, select the **Use IP V6** check box.
   - Specify the location where the server can be reached. For example, the phone number of the server's modem.
4. To enable the automation features (Auto Connect, Auto Logon, and Auto Select), select the appropriate check boxes.
5. When you are finished, you can choose to:
   - Continue with defining the general properties of the client.
   - Complete client configuration by selecting **OK**.

   Result: The server is added to the Servers and Sessions list and the Client Configuration Properties dialog closes.

Difficulty connecting

Configuration on the server is also required for communicating with clients. See Chapter 7, "Remote client/server connections," on page 69 for all the steps to connect the client and server using various remote connection methods.

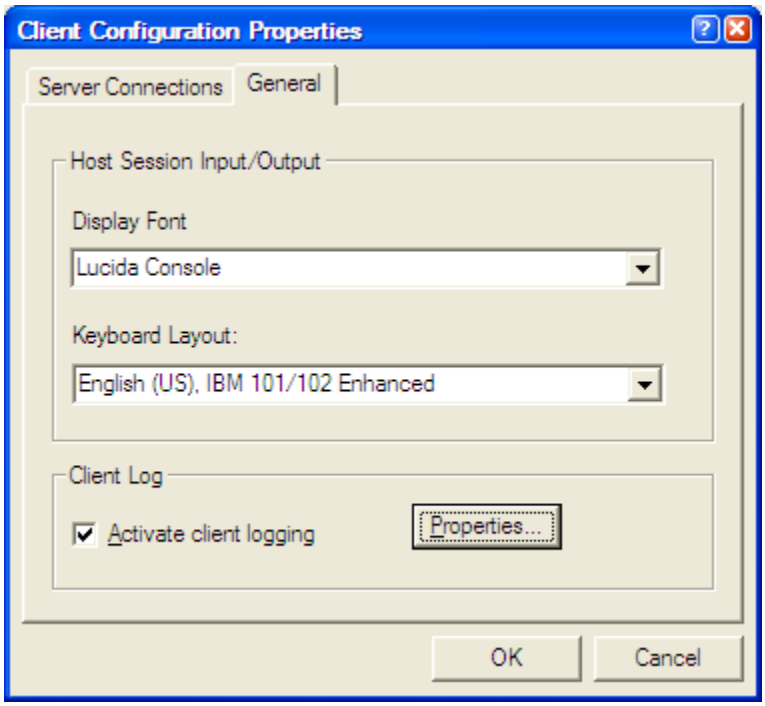
Defining general properties of the client

You can define certain client properties, including the display font and keyboard type, and you can specify the client log properties.

Follow these steps to define general client properties:

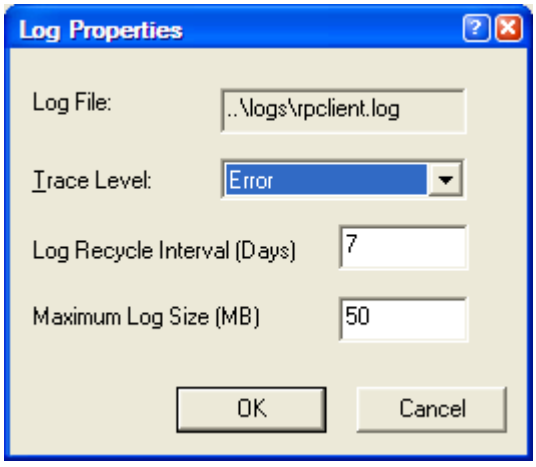
1. From the **Config** pull-down on the SA IOM client, select **Client**.

   Result: The Client Configuration Properties dialog displays.
2. Select **General** to display the General page.



3. Specify the display font for your host system. Or accept the preselected default.
4. Specify the keyboard type for your host system. Or accept the preselected default.
5. Activate client logging. By default, logging is active.
6. Click on **Properties**.

   Result: The Log Properties dialog displays.



7. You have the option of changing the defaults for Trace Level, Log Recycle Interval in days, and Maximum Log Size in MB. Accept the defaults, or change them as you like, and click **OK**.
8. When you are finished, you can choose to:
   - Continue with defining the Server Connections.
   - Complete client configuration by selecting **OK**.

   Result: The Client Configuration Properties dialog closes.

Part 2. "Classic" user and administrator tasks

Chapter 5. About the user interface 43
About the SA IOM server 44
Server component states 44
About the SA IOM client 45
Client control window panels 46
Controlling scripts 47
Script information 47
Starting scripts 47
Stopping scripts 48
Viewing script output 49
Authority and the Scripts panel display 49
Managing users 49
List of users 50
Disconnecting users 50
Sending messages 51
Authority and the Users control panel 51
Using Help 51
Other types of help 51
Recommendation 52
Messages 52
About SA IOM Service Manager 52
SA IOM Service Manager 52
Service Manager property pages 52

Chapter 6. Administering SA IOM software . . . 55
Performing configuration tasks 55
User authority required 55
System administrator tasks 55
System administrator responsibilities 56
Defining general properties 56
How to define general properties 56
Defining host sessions 57
Defining a Message Collector session 57
Defining a TN3270E session 58
Defining a 3270 session using the Attachmate IRMA 3270 PCI adapter 58
Defining a Glass Teletype session (example) . . 59
Defining user groups 60
Default user groups 60
Read Only sessions 60
Defining new user groups 61
Defining session classes 62
Defining a new session class 62
Configuring beeper paging 63
Setting up beeper paging 63
Defining users 63
Adding users 63
Defining client connections 64
Setting up client connections 64
Defining peer connections 65
Setting up peer connections 65
Defining service logging and recovery options . . . 66
Defining SA IOM Service log properties 66
Defining SA IOM Service Manager log properties 66
Specifying server shutdown and recovery options 67

Chapter 7. Remote client/server connections . . 69
Connecting clients and servers 69
Methods of connecting client to server 69
Authority required 70
About instructions in these sections 70
Client/server TCP/IP communications 70
Prerequisites 70
Tasks on the server 70
Tasks on the client 71
Client/server modem communications 71
Prerequisites 71
Tasks on the server 71
Tasks on the client 72
Client/server serial communications 72
Prerequisites 72
Tasks on the server 72
Tasks on the client 73

Chapter 5. About the user interface

This chapter describes some of the basic SA IOM operations, including:

- An overview of the SA IOM client and server control windows
- Information about online help and messages

Topics in this chapter

The following topics are discussed in this chapter:

- "About the SA IOM server" on page 44
- "About the SA IOM client" on page 45
- "Controlling scripts" on page 47
- "Managing users" on page 49
- "Using Help" on page 51
- "Messages" on page 52
- "About SA IOM Service Manager" on page 52

About the SA IOM server

This section describes the SA IOM server.

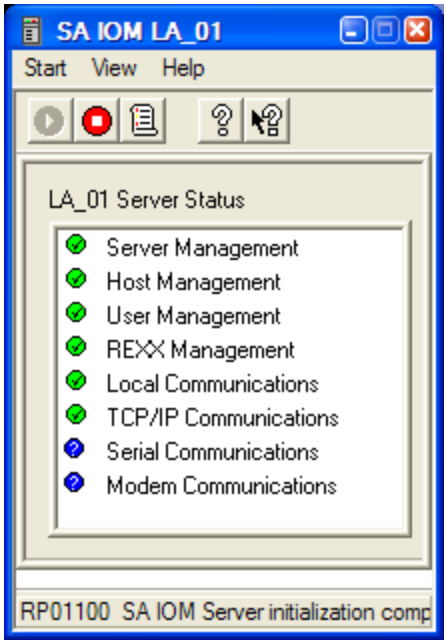
After successfully installing SA IOM, you must start the SA IOM server to initialize all host connections you have defined. See Chapter 6, "Administering SA IOM software," on page 55.

When the server is started, the initialization process begins, which includes connecting all enabled host systems and invoking startup time REXX scripts.

Note: Only one server can execute on a given machine at one time. If a server is in execution when you attempt to start another, the second startup will fail.

The Server control window contains the Server Status display which resembles a list.

Each item in the Server Status display represents one of the SA IOM server subsystem or communication components. Each component is preceded by an icon indicating component status.



. The Server Status display occupies most of the Server control window.

Server component states

Once started, SA IOM reports the state of each of the server subsystems/components as follows:

Table 4. Server subsystem/component states

State	Icon	Description
Undefined	Blue question mark	The initial state of all server components. If this icon does not change upon completion of server initialization, the subsystem/component is not part of the configuration.
Success	Green check mark	Initialization of the component is successful.
Warning	Yellow exclamation point	A minor problem was encountered, but initialization was performed.
Error	Red exclamation point	An error condition exists that prevented initialization of a component configured to initialize.

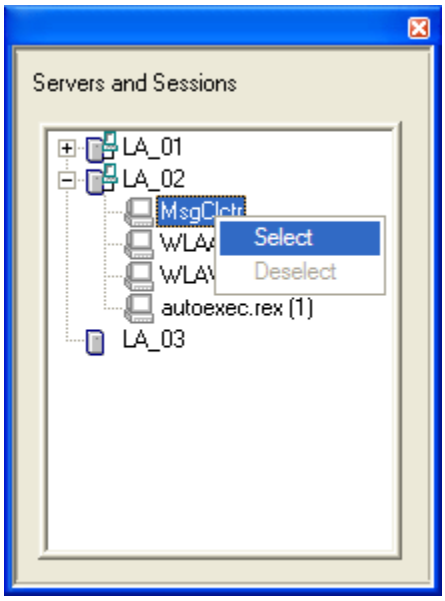
Whenever a component state changes, you can obtain information about the change by looking in the Server log. For example, if the Host Management status icon changes to an error status, an error message is written to the log. You can use the Server log to help determine the necessary corrective action. To view the server log, click the View Log icon in the Toolbar. To stop the server, click the **Stop** icon.

About the SA IOM client

This section describes the SA IOM client.

After successfully installing the SA IOM client on the Client workstation, you can start the client. The Client control window performs all SA IOM functions except starting and stopping the server. All SA IOM server configuration is performed using the client. Specifically, you use the Client control window to:

- Connect to one or more SA IOM servers
- Select host sessions supported by a connected SA IOM server



. The Message Collector and REXX scripts are also supported as selectable sessions.

- Observe the status of each connected server
- Configure the client, including server definitions
- Send messages to one or more currently connected clients

If you are authorized to do so, you can also

- View, start and stop REXX scripts on connected servers
- Configure connected servers
- Disconnect another SA IOM user connected to the same server

Client control window panels

The **Client control** window contains one or more of the following control panels. You control the number and type of control panels displayed using the **View Menu** commands on the **Client control** window.

Table 5. Client Control window panels

Control Panel	Purpose
Servers and Sessions	Displays the available servers to which this client can connect. After the client has connected to a server, this panel will also display the available sessions for each server.
Scripts	Displays the status of REXX scripts available on a server. At any point, multiple REXX scripts can be running on a server. Use this panel to start and stop scripts, and to display script status.
Server Status	Displays the status of SA IOM subsystems and components on a connected server. Use this panel to inspect the server state.
Users	Displays all users who are connected to an SA IOM server. Use this panel to disconnect users and to send messages to other SA IOM users.

The **Client control** window starts up with the default client panel, however you can modify this with one or more of the command line parameters, as follows:

-a Attach the specified session to an RpClient that is already running.

-c*uuu* Where *uuu* is the user ID that is configured in the RpServer.

-h*hhh* Where *hhh* is the name of the RpServer that you want to connect to. Note that it must have been previously configured in the RpClient.

-p*www*
Where *www* is the password for the user ID. You are prompted for the password if it is omitted.

-r*xxx* Where *xxx* is the REXX script that you want to start after logon.

-s*ttt* Where *ttt* is the session that you want to select or open.

For example:

```
RpClient -hSAIOM1 -cUser1 -pSecret -sTSO -rMyStart.rex parm1 parm2
```

Controlling scripts

This section provides information on controlling scripts.

The Scripts panel displays REXX scripts available on a server and their status.

If you are authorized to do so, you can start and stop, or view the status of, all scripts on a connected server.

Script information

For each script the following information is displayed:

- A status icon and a state description, as shown in the following table.

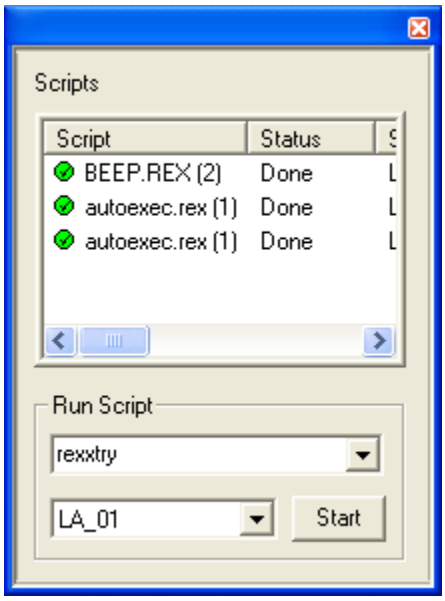
Table 6. REXX script states

State	Icon	Description
Running	Check mark in a green circle	The REXX script is running.
Stopping	Triangle in a red circle	The REXX script is in the process of halting.
Done	Check mark in a green circle	The REXX script is done.
Halted	Exclamation point in a yellow triangle	The REXX script is halted (stopped before completion).
Failed	An 'X' in a red circle	The REXX script failed.

- The name of the script and a script ID number
- The name of the server on which the script resides
- Script parameters
- Owner of the script
- Start and stop times of the script

Starting scripts

To start a script from the Scripts panel, you must be logged on to the server on which the script resides and you must be authorized to start scripts on that server.



. The Scripts panel of the SA IOM client.

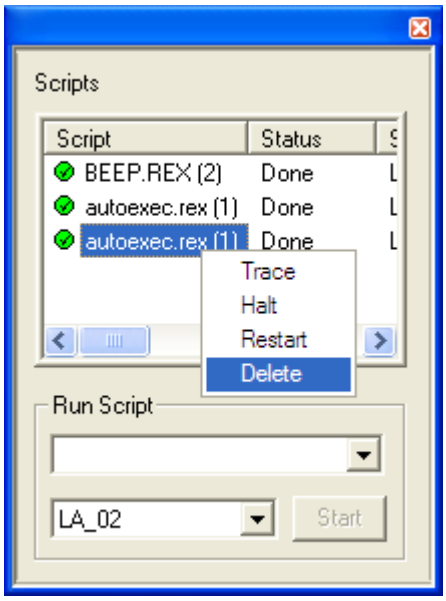
Locate the **Run Script** area, type the name of the script to run, select the name of the server on which is resides, and press **Start**. Once the script is started it will be displayed in the **Servers and Sessions** panel. You can view the script by selecting the session.

Scripts can also be started automatically. See the topic on automatically executing scripts at startup in *System Automation for Integrated Operations Management REXX Functions Reference*.

Stopping scripts

Use the pop-up menu that is associated with the **Scripts** panel to initiate the following activities.

Trace	Turns Trace on (or turns Trace off) a running script. This operation is only valid for a script whose status is Running.
Restart	Restarts a script.
Halt	Ends the script execution. This operation is only valid for a script whose status is Running.
Delete	Delete the selected script from the list area of the Scripts panel. This operation is only valid for a script whose status is Halted, Done, or Failed.



. How to select a script and delete it from the Scripts panel.

You must have ownership of a script in order to halt it, delete it, or restart it. For slightly more detail see "the REXX script owner" in the *System Automation for Integrated Operations Management REXX Functions Reference*.

Viewing script output

To view a script's output, select the session from the **Servers and Sessions** panel.

Result: The session window associated with your script displays.

If your script is interactive, you can type input to the script from its session window.

Authority and the Scripts panel display

What you see on the Scripts panel, depends on your user authority. In general:

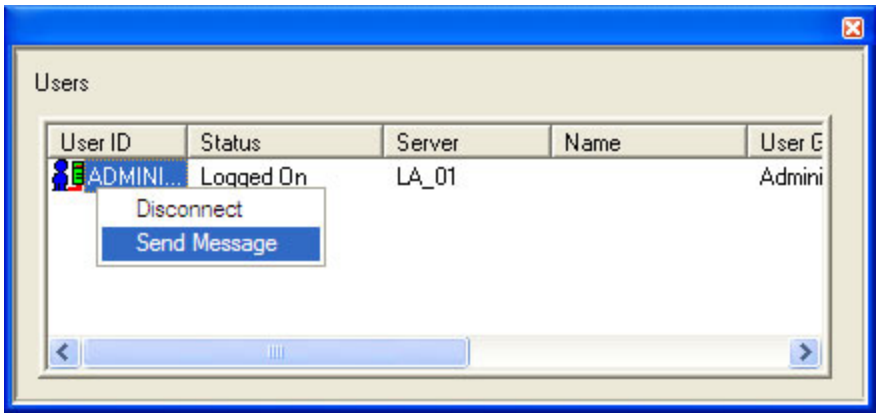
- If you belong to a user group with script user authority, your **Scripts** panel lists only those scripts that you started (those scripts that you own). It does not list scripts that were started by others.
- If you belong to a user group with script management authority, your **Scripts** panel lists all submitted scripts on all connected servers on which you have script management authority.

Managing users

This section provides information on managing client users.

The **Users** control panel displays a list of users who are logged on to an SA IOM server. You must be connected to a server in order to view that server's list of users.

In addition to viewing the list of users, you can send a message to a specific user or send a broadcast message to all logged-on users. If you are authorized to do so, you can disconnect a user from the server.



List of users

All users currently logged on to a server display on the **Users** control panel. For each user the following information is displayed:

- The name of the user and the user ID
- The name of server that the user is connected to
- The current status of the user, as follows:

Table 7. User status values

Status	Description
Connected	User is connected to the server.
Dialback	The user connection is awaiting completion of the modem dialback operation.
Editing configuration	The user connection is in the process of modifying the server configuration.
Logging on	The user is in the process of connecting to the server.
Logging out	The user is in the process of disconnecting from the server.

- The type of connection, such as Local, TCP/IP, Serial, or Modem
- The name of the user group that the user belongs to
- The time when the connection was made

Disconnecting users

To disconnect a user from the **Users** control panel, you must be logged on to the same server as the user and you must be authorized to logoff users on that server.

To disconnect a user, right-click the user from the list of active users, and click **Disconnect**.

Result: The **Confirm User Disconnect** window opens. From here you can confirm or cancel the disconnect request.

You can also select multiple users from the list and disconnect them all in one step.

When an SA IOM server receives a request to disconnect a user, the server sends a disconnect warning message to the user and starts a timer. The default disconnect time interval is 15 seconds. The disconnect time interval allows the user to save any configuration changes, host session edits, and so on, before the disconnect

takes effect. For more information on modifying the default disconnect time interval see Modifying the disconnect time interval.

Sending messages

To send a message to one or more users, select the users from the list of active users, right-click the selection and click **Send Message**.

Result: The **Send Message** window opens. From here you can specify the text of your message, modify the message distribution list as needed, and then send the message.

You can send a broadcast message, by selecting all the users connected to a particular server from the list of users on the **Users** control panel.

The **Send Message** window will open on your desktop when you receive a message from another user. After reading the message you can either close the window or you can send a reply to that user or any other active user.

Note: The Send Message function allows simple e-mail-type communication between SA IOM client users. However, a cumulative history of messages between users is not shown in the **Send Message** window, only the message last received.

Authority and the Users control panel

To disconnect a user from a server, you must be authorized to logoff users on that server.

For users who do not have logoff users authority, the User Group, Type, and Location fields on the Users control panel will be blank for all user IDs except their own.

Using Help

This section provides information on using the Help system.

The **Status Bar** on an SA IOM control window or session panel provides abbreviated help messages.

Other types of help

The classic SA IOM Windows interface supports two additional types of help:

- Online help. To view the Help system Table of Contents and search for help using a Help index, use either the Help pull-down from the menu bar or the documentation help icon in the Toolbar (the button with a question mark).
- Context-sensitive help. For help specific to a field, click on the context-sensitive icon in the Toolbar (the button with an arrow and question mark).

Windows Vista

No context-sensitive help is available when running under Vista.

The alert escalation feature has its own help system which uses Eclipse-plug-ins.

Recommendation

Use the help system whenever possible to learn more information about whatever task you need to complete. Most procedures and all the menu fields are explained in the help.

Messages

All messages are logged to the server or client log. Messages from the prior execution of the server and client are maintained in backup log files. Processing and help messages are displayed in the Status Bar on the Server control and Client control windows. Processing and error messages can also be displayed in message windows.

If the state of a subsystem or component changes to error, the icon for the appropriate subsystem/component turns to red. In this case, a message window will always open.

Message windows are modal. You may need to click **OK** on a displayed message window, to see the window that is underneath.

For detailed explanations of numbered product messages, see Appendix F, “Messages,” on page 257.

About SA IOM Service Manager

If, at install time, you successfully installed SA IOM as a Windows Service, then you can:

- Access the SA IOM Service Manager from the SA IOM **Start** menu.
- Use the SA IOM Service Manager to configure and manage the SA IOM Service and the SA IOM server that runs underneath it.

SA IOM Service Manager

When you install the SA IOM server as a Windows Service, SA IOM provides an SA IOM Service Manager that allows you to configure and manage the SA IOM Service and the server that runs under it.

Using the SA IOM Service Manager you can:

- Set controls to start and stop the SA IOM Service and server.
- Define SA IOM Service and Service Manager log properties.
- View the SA IOM Service and Service Manager logs.
- Specify server shutdown and recovery options.

The SA IOM Service moving window, which opens when SA IOM is running as a Windows service and a user is not currently logged in to Windows, can be disabled. To do this, start the SA IOM Service Manager, then select the **Disable Service popup** check box. The SA IOM server must be restarted for this option to take effect.

Service Manager property pages

The SA IOM Service Manager contains the following property pages:

Service	Configure and manage controls and parameters for the SA IOM Service, including: • Starting and stopping the SA IOM Service and server • Defining SA IOM Service Log parameters • Defining server shutdown and recovery options
General	Manage the controls and parameters for the SA IOM Service Manager Log.

Chapter 6. Administering SA IOM software

This chapter explains how to configure SA IOM client and server software for your site.

This chapter assumes that you:

- Have read and understand the concepts presented in Chapter 3, "Installing and configuring SA IOM," on page 27
- Can access the Client control window and connect to a running SA IOM server

Topics in this chapter

The following topics are discussed in this chapter:

- "Performing configuration tasks"
- "System administrator tasks"
- "Defining general properties" on page 56
- "Defining host sessions" on page 57
- "Defining user groups" on page 60
- "Defining session classes" on page 62
- "Configuring beeper paging" on page 63
- "Defining users" on page 63
- "Defining client connections" on page 64
- "Defining peer connections" on page 65
- "Defining service logging and recovery options" on page 66

Performing configuration tasks

This chapter is designed so that you can perform each configuration task independently. The tasks you perform depend greatly on how you have configured your SA IOM system.

Most of the procedures in this chapter start from the Config pull-down on the SA IOM Client. When you are using the manual to perform various tasks from the Server Configuration Properties dialog, you can skip to Step 2 in each procedure to avoid closing and opening the server configuration window repeatedly.

The Defining Service Logging and Recovery Options procedure starts by opening the SA IOM Service Manager dialog.

User authority required

You must have **Modify Server Config** authority to configure the server.

System administrator tasks

This section lists the system administrator tasks.

There are some tasks that you, the SA IOM system administrator, must complete to use SA IOM. Of course, these tasks vary from site to site, and depend on how you define authorities for other users.

System administrator responsibilities

The system administrator has the authority to perform the tasks listed below. The list also provides references to where you can go to receive more information about a particular task.

Task	For more information, see:
Define general properties	"Logging on to the server from a local client" on page 31.
Define host sessions	"Defining host sessions" on page 57.
Define user groups	"Defining user groups" on page 60.
Define session classes	"Defining session classes" on page 62.
Configure notification	"Configuring beeper paging" on page 63.
Add users	"Defining users" on page 63 and Chapter 7, "Remote client/server connections," on page 69.
Set up client connections	"Defining client connections" on page 64 and Chapter 7, "Remote client/server connections," on page 69.
Define peer connections	"Defining peer connections" on page 65.
Define service log properties and recovery options	"Defining service logging and recovery options" on page 66.

Defining general properties

This section describes how to define general properties.

You can define certain properties that affect all the sessions you define.

These include:

Setting this property	Allows you to:
Message of the Day	Define a message that will display at the logon prompt. (Optional)
Script COM Ports	Assign shared serial ports for scripts, so you can run multiple scripts on a port. For example, you can assign one port for both time acquisition and beeper paging. (Optional)
System Log	Activate system logging, and choose the type of message severity (warning, information, and so on) you want to be logged. (Optional)
Time Acquisition	Automatically acquire the most accurate time available to update your server's clock. (Optional)
Server Name	Defines the name of the server. (Required)

How to define general properties

Follow these steps to define general properties:

1. From the **Config** pull-down on the SA IOM Client, select **Server** then select which server to configure.

   Result: The Server Configuration Properties dialog displays.

2. Select **General** to display the **General** page.
3. Complete the fields for the properties you want to set.
4. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

   Result: The Server Configuration Properties dialog closes.

Defining host sessions

This section explains how to define some of many possible host sessions:

- Message Collector session.
- TN3270E session (using the IBM OSA Integrated Console Controller).
- 3270 session (using an Attachmate IRMA 3270 PCI Adapter).
- Glass Teletype session.

Note that since all configuration is performed using the client, you need to be connected, client to server, before you can define a server's host sessions.

After you have configured a server connection, you can start to define its sessions. A server manages connections between SA IOM and host systems, including emulation and access control.

In the Server Configuration Properties dialog, the Host Sessions page displays the name, state, type, and connection type for each host session which is already defined.

Defining a Message Collector session

Follow these steps to define a Message Collector session.

1. Connect to the server on which you will define the session. From the Config pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Host Sessions**. In the Host Sessions list area, right-click and select **Add**. The Session Properties dialog displays.
3. Complete the following fields:
   - Provide a name for the session, for example, MsgClctr.
   - Select **Message Collector** as the session type.
4. Click **Properties**. The Message Collector Properties panel displays.
5. Complete the following field:

   Port Select the TCP/IP port number that the server will use to listen for incoming Message Collector traffic.

   Pick a number that is not reserved or used in a daemon mode by another program. The default is 1090.
6. Click **OK**. Click **OK** on the remaining panel to accept the settings.

   Result: The Message Collector session is added to the **Host Sessions** list.
7. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

Results: Click Yes to confirm the update to the server configuration. The Server Configuration Properties dialog closes. Click Yes to complete the configuration process by restarting the server. Click OK to clear informational messages that display.

Defining a TN3270E session

Follow these steps to define a TN3270E emulation session. This type of session uses the IBM OSA Integrated Console Controller.

1. Connect to the server on which you will define a session. From the Config pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Host Sessions**. In the Host Sessions list area, right-click and select **Add**. The Session Properties dialog displays.
3. Complete the following fields:
   - Provide a name for the session.
   - Select **TN3270E Protocol** as the session type.
4. Click **Properties**.

   Result: The TN3270E Emulation Properties panel displays.
5. Complete the following fields:
   - **Language**, **Usage** and **Screen Size** settings appropriate to the host system to which you are connecting.
   - **Beeper Console** and **OIA Line**. These fields are optional. The Operator Information Area (OIA) is a status line at the bottom of the screen that communicates system status and error conditions. See the appendix Appendix D, “TN3270E operational information,” on page 251 for more information.
6. Click on **Connection**.

   Result: The **Telnet 3270E Connection** panel displays.
7. Complete the following fields:
   - **Host Name**, **Port** and **Resource/Device Name**. You can type either the host name or the IP address of the host session to which to connect. The port is the TCP/IP port through which the connection operates, and the resource/device name is the LU name.
8. Click **OK**.

   Result: The TN3270 session is added to the **Host Sessions** list.
9. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Defining a 3270 session using the Attachmate IRMA 3270 PCI adapter

Follow these steps to define a 3270 emulation session using the Attachmate IRMA 3270 PCI adapter:

1. Connect to the server on which you will define a session. From the Config pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.

2. Right click **Host Sessions** and click **Add**.

   Result: The **Session Properties** panel opens.
3. Complete the following fields:
   - Provide a name for the session.
   - Select **3270 Emulation** as the session type.
4. Click on **Properties**.

   Result: The **3270 Session Properties** panel opens.
5. Complete the following fields:
   - Select **Usage**, **Language**, and **Screen Size** settings appropriate to the host system to which you are connecting. Online information is available for every configuration field. Click on the question mark in the upper right of the window, and then click on the field for which you want help.
   - Select **Attachmate IRMA 3270 PCI Adapter** for the 3270 adapter.
6. Click on **Connection**.

   Result: The **Attachmate IRMA 3270 PCI Adapter Properties** panel displays.
7. Select the appropriate PCI slot and click on **OK**. Select **OK** on all the remaining panels to accept the settings.

   Result: The 3270 session is added to the Host Sessions list.
8. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Defining a Glass Teletype session (example)

Follow these steps to create a Glass Teletype session:

1. Connect to the server on which you will define a session. From the Config pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Right click **Host Sessions** and click **Add**.

   Result: The Session Properties dialog displays.
3. Complete the following fields:
   - Provide a name for the session.
   - Select **Glass Teletype** for the session type.
4. Click on **Properties**.

   Result: The Glass Teletype Properties panel displays.
5. Select **Direct Serial Connection** as the connection type and click on **Properties**.

   Result: The Serial Properties panel displays.
6. Complete the fields according to your hardware configuration and select **OK**. Select **OK** on all the remaining panels to accept the settings.

   Result: The Glass Teletype session is added to the Host Sessions list.
7. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Defining user groups

This section describes how to define user groups. User groups are a convenient way to organize and control the authorities granted to SA IOM users. You can think of a user group as a collection of authorities.

Users who become members of a user group inherit the authorities of the group. For example, you may have just a small group of users, named Administrators, who are authorized to configure the server.

Default user groups

SA IOM provides these default authority groups.

If you are assigned to the default authority group:	You can:
Administrators	• Modify server configuration • Respond to client messages • Manage others scripts • Use scripts • Log off other users
Operators	• Respond to client messages • Manage others scripts • Use scripts • Log off other users
Users	• Use scripts
Read Only	• Not use scripts or input data to sessions

Notes:

1. A user who is not assigned to a user group has the following default authorities:
   - Use scripts
   - Access to public sessions only (those with no session class)
2. The default authority groups do not have associated session classes since default classes are not provided. As you define session classes, associate them with user groups to control access of users to sessions. Note that host sessions without a session class are considered public and can be selected and viewed by any user.

Read Only sessions

SA IOM includes a facility to limit keyboard access of specified user groups. This security feature allows a group of users to display console and emulator session information, but not to enter keyboard commands, or commands from a command dialog (such as 3270 Special Keys).

This facility is specified using the Authorities tab of the User Group Properties dialog box. If this feature is desired for a particular user group, it can be specified at the end of the third step of “Defining new user groups” on page 61. This authority is mutually exclusive of all other authorities. If other authorities are

checked, the dialog disallows the read-only check. This authority should be contained in a group created for that purpose.

For fresh installations, there is a predefined read-only user group with the read-only authority checked. For installations with a pre-existing user configuration, there will not be a read-only user group. Additionally, all of the other user groups will have the read-only authority set. If necessary, the check box can be cleared. Then, if the administrator attempts to again check the box, it will be disallowed.

If a user who is a member of a read-only user group attempts to enter a command in a client session, a message window appears and any keystrokes are ignored.

Defining new user groups

Follow these steps to define user groups:

1. From the **Config** pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.

2. Select **User Groups**.

   Result: The default user groups are displayed.

3. You can:
   - Duplicate the properties of a default group (Administrators, Operators, or Users) by right-clicking the default group you want to copy, then clicking **Duplicate**.

     Note: When you duplicate a user group, the users from the original group are not included in the new group. Duplicating a user group copies the existing group's authority settings only. A user can only be a member of a single group at a time.

     Result: The **User Group Properties** dialog for the default group you chose is displayed.
   - Create a new user group by right-clicking and clicking **Add**.

     Result: The **User Group Properties** dialog displays without default values.

4. Complete the following fields:
   - Provide a new name for the group.
   - If this a new group that is not based on a default group, select the authorities that you want to apply to this group.
   - Click on **Members**.

     Result: The **Members** page displays the users you can add to the group.
   - Highlight the name of the user you want to add to the group and click on **Add**.

     Result: The user you chose is moved to the group member list.

5. Continue adding members until you are finished.

   Note: You can also assign a session class to a user group from the **Classes** tab. For more information on session classes, see "Defining session classes" on page 62. Click on **OK**.

   Result: The group you defined is added to the group list.

6. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.

- Complete server configuration by selecting **OK**.

  Result: The Server Configuration Properties dialog closes.

Defining session classes

This section describes how to define session classes.

You can define session classes that are associated with host sessions and user groups for this server. Session classes are a convenient way to control access by users to individual host sessions.

Session classes function as a bridge between user groups and host sessions. Each host session can belong to at most one session class. Each user group can be associated with zero or more session classes. A user in a given user group can select and view any host session belonging to a session class associated with that user group.

A host session that is not assigned to a session class is considered a public session. Public sessions can be viewed by all users.

A session is assigned to a session class in the **Host Sessions Property** page, and session classes are assigned to user groups in the **User Groups Property** page.

Where possible, you should organize your host sessions into logical groupings based on their security restrictions, the types of users who need access to the session, and so on. These logical groupings of sessions can be used to implement a system of session classes which provide both security and flexibility. For example, your MVS hosts could form one group of host sessions, which all belong to a session class that only the System Operators and Administrators user groups have access to.

Defining a new session class

Follow these steps to define session classes:

1. From the **Config** pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Right-click **Session Classes** and click **Add**.

   Result: The class properties dialog displays.
3. Type a name and description for the new class. When you are finished, click on **OK**.

   Result: The new session class is added to the class list.

   Note: As host sessions are assigned to this new class, and user groups are associated with the class, the Associated Sessions and Associated Groups lists will automatically get updated on the Class properties dialog to reflect the new associations.
4. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Configuring beeper paging

This section describes how to set up beeper paging.

For more information on beeper paging, see Chapter 10, “Beeper paging,” on page 97.

Setting up beeper paging

Follow these steps to set up beeper paging:

1. From the **Config** pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Notification** to display the **Notification** page.
3. To activate beeper paging notification, click on **Begin beeper paging notification at server startup**. Online information is available for every configuration field. Click on the question mark in the upper right of the window, and then click on the field for which you want help.
4. Complete the fields identifying REXX scripts and the trigger text (or take the defaults). Click on **Communication**.

   Result: The **Serial Properties** dialog displays.
5. Complete the fields and click on **OK**.
6. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Defining users

This section describes how to define users.

A user is a person authorized to use the SA IOM server. Each SA IOM server maintains a list of users. From the Users control panel, you can

- View the list of users
- Use the Location column to identify remote modem and TCP/IP clients
- Disconnect one or more users
- Send broadcast messages to users

See “Managing users” on page 49 for more information on the **Users** control panel.

Users have different levels of authority depending on their user group membership. The user inherits the authorities of the user group. See “Defining user groups” on page 60 for more information about user groups.

Adding users

Follow these steps to add users to an SA IOM server.

1. From the Config pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Users**. Right click and select **Add**.

   Result: The User Properties dialog displays.

3. Complete each field by entering the requested information about the user. You can also:
   - Define user-specific restrictions by clicking on **Restrictions**. Restrictions and time-outs become considerations if the user will be logging on from a remote location. See Chapter 7, "Remote client/server connections," on page 69.
   - Assign the user to one of the existing user groups by selecting a **Group Membership**.

   When you have finished defining a user, click **OK** until you reach the **User** page again.

   Result: The user you defined is added to the user list.
4. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Defining client connections

This section describes how to define client connections.

You can manage the connections between SA IOM servers and SA IOM clients. The Client Connections Property page allows you to define local, TCP/IP, modem and serially-connected clients.

Note: Connections between SA IOM servers and host systems are defined in the Host Sessions Property page.

Setting up client connections

Follow these steps to set up client connections:

1. From the **Config** pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Client Connections** to display the **Client Connections** page.
3. You can:
   - Define TCP/IP client connections. Check the **TCP/IP** box (it should already be checked by default), and choose the port number you want the server to use to listen for incoming TCP/IP-connected clients. The default is 1035. See "Client/server TCP/IP communications" on page 70 for all the steps to connect the client and server using TCP/IP.
   - Define modem client connections. Right-click in the modem window and click **Add** to display the **Client Modem Connection** panel. Follow the instructions to add a modem and click **OK**. See "Client/server modem communications" on page 71 for all the steps to connect the client and server using modems.
   - Define serial client connections. Right-click in the serial window and click **Add** to display the **Serial Properties** panel. See "Client/server serial communications" on page 72 for all the steps to connect the client and server using direct connections.
4. Complete the fields according to your hardware configuration and select **OK**. Select **OK** on all the remaining panels to accept the settings.

   Result: The **Client Connections** page displays the connections you defined.
5. When you are finished, you can choose to:

- Continue server configuration by selecting another tab.
- Complete server configuration by selecting **OK**.

  Result: The Server Configuration Properties dialog closes.

Defining peer connections

This section describes how to define peer connections.

Setting up peer connections

Follow these steps to set up peer connections.

1. From the **Config** pull-down on the SA IOM Client, select **Server** and then select the server you want to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Peers** to display the Peers page.
3. To define peer connections, check the **Peer Connections** box and then choose the port number you want the server to use to listen for standard incoming peer connections. The default is 1040.
4. You can:
   - Add a new peer connection by right-clicking and clicking **Add**.

     Result: The **Peer Properties** dialog displays.
   - Duplicate the properties of another peer connection by right-clicking the DNS name or IP address you want to copy and clicking **Duplicate**.

     Result: The **Peer Properties** dialog for the peer connection you chose is displayed.
5. Provide a DNS name, or an IP address (or a range of IP addresses), and an optional description. When specifying IP address ranges, use a single "-" to indicate a subrange. For example, "100.200.100.50-60" is a valid entry for the IP address field. Use "*" to indicate the entire range from 0-255.

   Notes:

   a. The peers listed here represent systems which are authorized to open peer connections to the SA IOM server, and not systems which this server is authorized to connect to. Each "AF" peer system, or other peer system, must have its own list of authorized inbound connections.

   b. The peers listed here must include every peer that will attempt to connect, including (if applicable) the PC that the SA IOM server is running on.

   c. Depending on the server and client build level, IP addresses that are entered as a range are still entered into the configuration individually (and must be deleted individually).
6. Click **OK**.

   Result: The **Peers** page displays the DNS name or IP address (or IP addresses) for the peer connection you defined.
7. When you are finished, you can choose to:
   - Continue server configuration by selecting another tab.
   - Complete server configuration by selecting **OK**.

     Result: The Server Configuration Properties dialog closes.

Defining service logging and recovery options

This section describes how to define properties for the SA IOM Service and SA IOM Service Manager logs, and specify the server shutdown and recovery options.

Defining SA IOM Service log properties

The SA IOM Service has a separate log file, `rpsvc.log`.

Follow these steps to define the properties of the SA IOM Service log:

1. From the SA IOM Start menu, select **SA IOM Service Manager**.
   Result: The **SA IOM Service Manager** dialog displays.
2. Select **Service** to display the Service page.
3. Under **SA IOM Service Log**, complete the following fields as needed.
   - Define the volume and degree of detail for messages written to the log by indicating the **Trace Level**.
   - Specify how often you want the log to be automatically recycled, by entering a value for the **Log Recycle Interval**.
   - Specify the **Maximum Log Size** allowed for the log. If the maximum log size is exceeded, the log will be automatically recycled.
   - Indicate whether you want to activate service logging and append to an existing service log.
4. When you are finished, you can choose to:
   - Apply the values you defined for the log by selecting **Apply**.
   - Continue SA IOM Service Manager configuration for other properties on the **Service** page or by selecting the **General** tab.
   - Complete SA IOM Service Manager configuration by selecting **OK**.
     Result: The SA IOM Service Manager dialog closes.

Defining SA IOM Service Manager log properties

The SA IOM Service Manager has a separate log file, `rpsvcmgr.log`.

Follow these steps to define the properties of the SA IOM Service Manager log:

1. From the SA IOM Start menu, select **SA IOM Service Manager**.
   Result: The SA IOM Service Manager displays.
2. Select **General** to display the General page.
3. Under **SA IOM Service Manager Log**, complete the following fields as needed.
   - Define the volume and degree of detail for messages written to the log by indicating the **Trace Level**.
   - Specify how often you want the log to be automatically recycled, by entering a value for the **Log Recycle Interval**.
   - Specify the **Maximum Log Size** allowed for the log. If the maximum log size is exceeded, the log will be automatically recycled.
   - Indicate whether you want to activate service logging and append to an existing service log.
4. When you are finished, you can choose to:
   - Apply the values you defined for the log by selecting **Apply**.
   - Continue SA IOM Service Manager configuration for other properties on the **General** page or by selecting the **Service** tab.

- Complete SA IOM Service Manager configuration by selecting **OK**.

  Result: The **SA IOM Service Manager** dialog closes.

Specifying server shutdown and recovery options

Follow these steps to define the SA IOM server shutdown and recovery options:

1. From the SA IOM Start menu, select **SA IOM Service Manager**.

   Result: The SA IOM Service Manager displays.
2. Select **Service** to display the Service page.
3. Under **Shutdown and Recovery**, complete the following fields as needed.
   - Specify whether you want a **Normal** or **Fast** shutdown of the server.
   - Choose a recovery option for when the SA IOM Service terminates the server abnormally.
4. When you are finished, you can choose to:
   - Apply the values you defined for shutdown and recovery, by selecting **Apply**.
   - Continue SA IOM Service Manager configuration for other properties on the **Service** page or by selecting the **General** tab.
   - Complete SA IOM Service Manager configuration by selecting **OK**.

     Result: The SA IOM Service Manager dialog closes.

Chapter 7. Remote client/server connections

This chapter provides guidelines for establishing connections between clients and servers using the remote connection methods.

Connecting to the server using a local client is described in "Logging on to SA IOM the first time" on page 31 and is already configured if you installed the Client and Server option at installation time.

Topics in this chapter

The following topics are discussed in this chapter:

- "Connecting clients and servers"
- "Client/server TCP/IP communications" on page 70
- "Client/server modem communications" on page 71
- "Client/server serial communications" on page 72

Connecting clients and servers

This section describes the methods of connecting the SA IOM client to the SA IOM server.

Methods of connecting client to server

You can connect the SA IOM client to the SA IOM server using any of the following **connection type** methods. Each method has its own requirements.

- Local

  This method requires that the server and client reside on the same machine. This allows them to communicate with each other using local communications, which means they use a shared memory area to communicate.
- TCP/IP

  This method requires that your TCP/IP network is installed and operational.
- Modem

  This method requires that the Windows environment recognize the modems that you install on the client and server machines, and that at least one modem is configured for use by the client and at least one modem is configured for use by the server.
- Direct Connect (serial communications)

  This method requires that COM ports on the client and server computers be connected by a null-modem cable.

More detailed requirements for each connection method are described in this chapter and can be used as a detailed checklist or a troubleshooting guide for client/server communication.

Note to the system administrator: For testing purposes, a client and server that are installed on the same PC can be configured to communicate with each other using any of the methods listed above, provided that they meet all of the requirements. However, this is not the recommended method for normal use because a server can have only one connection to a given client or PC instance at a time.

Authority required

Server configuration tasks require **Modify Server Config** authority.

Configuring a client requires no special authority.

About instructions in these sections

Steps are written at a level of detail to guide you to the appropriate configuration panel and accomplish the task at hand. If you want to know more about a particular SA IOM server or client configuration panel, click on the context-sensitive help icon (the button with the question mark and the arrow) for field level explanations.

Client/server TCP/IP communications

This section explains how to configure the server and client to communicate with each other using TCP/IP connections.

Prerequisites

Before you configure the server and client to communicate using TCP/IP connections:

1. You should have already installed the server and client components on the PCs that you will use as the server and client PCs. This is described in Chapter 3, “Installing and configuring SA IOM,” on page 27.
2. Your TCP/IP network should already be in place, and TCP/IP should already be configured on the PCs that you will use as the server and client PCs.
3. Validate the ability of the PCs to communicate using TCP/IP. The server and client PCs should be able to ping themselves and each other. For example, from a Command Prompt, enter the following, where *hostname* is the TCP/IP host name of the server or client PC:

   ```
   PING hostname
   ```

Tasks on the server

The system administrator should verify the following modifications to the server configuration to support TCP/IP-connected clients.

- Client Connections page

  Verify that TCP/IP client connections are allowed on the server, and select the port number that the server will use to listen for incoming TCP/IP-connected clients.

- Users page

  Add or modify a user definition for each user who will be allowed to access the server using a TCP/IP-connected client. Consider adding TCP/IP restrictions to each user. Users may be restricted to logging on from a particular DNS name, or IP address (or a range of IP addresses). To specify an IP address range, use a single "-" to indicate a subrange. For example, "100.200.100.50-60" is a valid entry for the IP address field. Use "*" to indicate the entire range from 0-255.

  There is a TCP/IP-connected timeout restriction associated with each user. You can choose to accept the default timeout, adjust the timeout, or eliminate the timeout for each user.

Tasks on the client

Consult the system administrator to obtain the server's IP address and port number. Update the client configuration to include a server connection definition to the server using TCP/IP.

On the Server Connections page:

1. Supply a server connection name.
2. Click **TCP/IP Communication**, and then enter the server's IP address and port number.
3. Select the **Use IP V6** check box to communicate with the IPV6 protocol.

Client/server modem communications

This section explains how to configure the server and client to communicate with each other using modems.

Setup for this connection method involves both hardware and software configuration at the sites where the server and client are installed.

Prerequisites

Before you configure the client and server to communicate using modems:

1. You should have already installed the server and client components on the PCs that you will use as the server and client PCs. This is described in Chapter 3, "Installing and configuring SA IOM," on page 27.
2. You should have already installed and verified the operation of at least one modem on the server PC and at least one modem on the client PC. This is described in "Installing modems" on page 33.

   Note: If you want to test modem-communication between a server and client that are installed on the same PC, you will need to install a least two modems on the PC (one for the server and one for the client).

Tasks on the server

The system administrator should verify the following modifications to the server configuration to support modem-connected clients.

- Local client logon

  Important: The server must be configured to recognize a modem using a local client. This means the client communicates with the server using the local communication method. If you access the server using another client connection method, the pop-up menu choice to **Add a modem** is not available.

- Client Connections page

  In the **Modem Client Connections** area, right click and select **Add** to specify which modem (or modems) will be used for communicating with clients.

  Notes:

  1. If the Add action on the pop-up menu is not available, logon to the server using a local client.
  2. If no modems appear in the list, cancel out of Server Configuration, stop the server, go to ("Installing Modems" on page 78) and repeat the procedure on the server PC.

- Users page

Add or modify a user definition for each user who will be allowed to access the server using a modem-connected client.

A call back restriction is the default option for users of modem-connected clients. To maintain logon security, as part of the logon process the server hangs ups and then "calls back" the user's client. To complete the user definition, either enter the telephone number of the user's modem-connected client PC, or exempt the user from the call-back restriction.

Recommendation: While testing the modem-connected client/server communication setup, do not require a call-back. Later, after successfully connecting, implement the call-back restriction to maintain the security of your SA IOM system.

There is a modem-connected time-out restriction associated with each user. You can choose to accept the default time-out, adjust the time-out, or eliminate the time-out for each user.

Tasks on the client

Consult the system administrator to obtain the telephone number of the server's modem. Update the client configuration to include a server connection definition to the modem-connected server.

On the Server Connections page:

1. Supply a server connection name.
2. Select **Modem Communication**, and then enter the telephone number of the modem on the server PC
3. Press the button to the right of the **Modem** field to select which modem to use for communicating with the server.

   Note: If no modems appear in the list, Cancel out of Client Configuration Properties, stop the client, go to "Installing modems" on page 33 and repeat the procedure on the client PC.

Client/server serial communications

This section explains how to configure the server and client to communicate with each other using direct serial connections.

Prerequisites

Cables should already be in place. See "About direct connections" on page 20.

Tasks on the server

Verify the following modifications to the server configuration to support serially-connected clients.

- Client Connections page

  In the **Serial Client Connections** area, right click, select **Add**, then supply the serial properties information. Double-check the COM port number that you specify. The baud rate specification for this COM port must be set to the same baud rate used on the client.

- Users page

  Add or modify a user definition for each user who will be allowed to access the server using a serially-connected client.

Tasks on the client

Update the client configuration to include a server connection definition to the server using serial communication.

On the Server Connections page:

1. Supply a server connection name.
2. Select **Serial Communication**, press **Properties**, and then supply the serial properties information. Double-check the COM port number that you specify. The baud rate specification for this COM port must be set to the same baud rate used on the server.

Part 3. "Classic" features

Chapter 8. Message collector 77
Controlling message processing. 77
SA IOM's implementation 77
Sending messages from your application to SA IOM 78
Uses of the Message Collector 78
Consolidating messages to a single console display 78
Interacting with the Message Collector 79
Server-to-server messaging 79
SA IOM to SA IOM network connections 79
Sharing system resources using the Message Collector 80
Sending a message to a Message Collector 80
Before you start 80
Sending the message 80
Monitoring the Message Collector session 80
REXX functions to use with the Message Collector 81
Message Collector logging 81
MSGCLECT.LOG file example 81
Message Collector sample programs 81
Windows 81
UNIX 84

Chapter 9. Peer-to-peer communications 85
TCP/IP-based peer-to-peer communications . . . 85
"Types" of peer-to-peer communication 85
Peer functions 86
AF-to-AF usage scenarios. 87
Scenario 1 87
Scenario 2 87
Scenario 3 88
Scenario 4 88
About "non-AF" peer conversations 88
About "non-header" peer conversations 89
Peer communications protocol 90
Peer-to-peer communications protocol language 90
Peer-to-peer message packet format 91
Linkid or Message Token parameter 91
Data Type parameter 92
Reply Data Length parameter 94
Send Data Length parameter 94
Send Data parameter 95

Chapter 10. Beeper paging 97
Sending optional text 97
Optional message text 97
Touch-tone versus modem paging 97
Touch-tone paging requests 98
Modem paging services 98
Tuning for modem-to-modem paging. 99
Automatic paging 99
What triggers automatic beeper paging 99
Fine-tuning a touch-tone WTOR 101
Initial procedure 101
Testing procedure 101
Calculating delays. 102

Chapter 11. Voice control 103
Controlling a voice adapter. 103
Installing Dialogic voice adapters. 103
Text-to-speech support 104
Installation 104
Configuration notes 105
Configuring the SA IOM server for voice adapter use 105
Creating voice applications 106
Voice functions 106
Recording messages 106
Getting listener responses 107
Beeper paging with a voice adapter 107
Voice diagnostic and debugging facilities 108
Recovery and error processing. 108
Voice operation diagnostic logging information 109

Chapter 12. SA IOM Hardware Management Console interface 111
HMC interface overview. 111
Description of HMC network components . . . 111
S/390 PTS configuration with SA IOM 111
Configuring the SA IOM HMC interface 112
SA IOM server configuration 112
Configuring the z9-109 HMC for use with SA IOM 113
HMC console configuration (OS/2 Warp Connect 4.0) 113
Testing and verification 114
Testing at the HMC console (OS/2 Version) 115
Testing at the SA IOM server 115
Connecting the SA IOM HMC interface PC to the HMC 115
Using the SA IOM HMC interface 116
Navigation commands 116
How to navigate 116
Action commands 117
Action command syntax. 117
Operating system commands 117
Additional commands 118
Status conditions 118
Modes. 118
HMCACT.REX automation interface program 119
HMCACT.REX 119
Format 119
Example 120
Return codes 120

Chapter 13. Configuring TN3270E sessions . . 121
Configuring TN3270E support in SA IOM. . . . 121
Configuring the TN3270E server 122
Configuring SA IOM session definitions . . . 122

IBM 2074 connection considerations 125
Configuring MVS MCS console definitions with the IBM 2074 Console Support Controller . . . 126
MVS TCP/IP configuration issues 126
Copying and pasting in TN3270E sessions. 127
Consolidating 3270 Sessions using SLF 128

Chapter 14. SA IOM problem determination . . 133
Begin by checking available logs 133
Format of log files. 134
Configuration errors 134
Network errors. 134
Hardware errors 134
Acquiring STATE-level logs. 135
Modem connection problems and documentation needed by IBM. 136
Direct serial client/server connection problems . . 137
3270 Coax PCI connection problems. 138

Chapter 15. Utility programs. 139
RpLogRd.exe 140
RpRunRex.exe 142
RpSend.exe 144
RpSesClr.exe. 146

Chapter 8. Message collector

This chapter provides information about the SA IOM Message Collector.

Topics in this chapter

The following topics are discussed in this chapter:

- "Controlling message processing"
- "Uses of the Message Collector" on page 78
- "SA IOM to SA IOM network connections" on page 79
- "Sending a message to a Message Collector" on page 80
- "Monitoring the Message Collector session" on page 80
- "Message Collector logging" on page 81
- "Message Collector sample programs" on page 81

Controlling message processing

The SA IOM Message Collector is a versatile tool that allows you to collect and filter message input from distributed or mainframe systems. You only need a TCP/IP LAN connection between the distributed systems and SA IOM to send messages from your application to the SA IOM Message Collector.

If you need to view application messages using a central console, but you do not want to define the application as an SA IOM session, you can modify your application to send messages to the SA IOM Message Collector. The messages can then be monitored by your operations staff. If your application is not readily modifiable, you can develop your own utility to read the application log as it is written and send the desired log entries to SA IOM. All that is required is that the host system on which the application executes is TCP/IP-connected to the SA IOM server.

If you need to concentrate message input from geographically distributed systems, such as outlying business offices or retail point-of-sale systems, you can send status messages from the remote sites to a central SA IOM console. You can then use SA IOM trapping functions and message line retrieval functions to access and respond to messages. Using Windows Remote Access Services (RAS), the outlying sites can communicate with the SA IOM server over standard telephone lines. You can write SA IOM scripts to recognize critical messages and page support personnel or conduct automated voice communications.

If you need to monitor other REXX scripts running under SA IOM, you can use the Message Collector as a central point for script status messages. You can write a REXX script to monitor the Message Collector session for messages indicating REXX script failures. Your script can detect the failure and take appropriate action. You have full control over the rules governing message processing.

SA IOM's implementation

SA IOM Message Collector session implementation relies on the underlying TCP/IP services your network provides. One Message Collector session can be established on each SA IOM server through the TCP/IP network.

The Message Collector is presented to you as a special type of SA IOM host session. It is implemented as a line-mode (scrolling) console which accepts multiple connections simultaneously. The status line of the Message Collector session shows status information for these connections.

Since the SA IOM Message Collector uses VT emulation, you can use escape sequences in your message to define message display characteristics, such as foreground and background color. This allows you to visually distinguish high priority messages.

Sending messages from your application to SA IOM

To send information from your application to SA IOM, you must first understand how your application performs its logging function.

If you have only one target application, and if your application supports logging to a console, you may prefer defining the console to SA IOM as an attached Telnet or serial session instead of using the Message Collector.

If the Message Collector use is indicated, then determine if your application supports log-time exits. That is, determine if the application provides an exit whereby your own program logic is given each message as it is logged. If such an exit exists, simply send the message using a Sockets send call to SA IOM.

If a log-time exit does not exist, then you must implement "log scraping" logic which reads the application log, either as it is written or at suitable intervals. In this case, you must insure that the application log can be accessed in a shared mode.

Uses of the Message Collector

This section provides information on using the Message Collector.

You can use a Message Collector session to receive and log messages from diverse operating systems (such as UNIX, Windows, and so on) that support TCP/IP socket applications. The Message Collector session receives messages from any TCP/IP program that can send messages through the TCP/IP network.

If your SA IOM Server supports REXX (see "REXX support requirements (optional)" on page 22), you can trap on messages, and then once Message Collector data is trapped it can be used for automation and notification purposes.

Consolidating messages to a single console display

A common use of the SA IOM Message Collector is to consolidate high priority messages from a set of MVS Consoles defined as SA IOM sessions.

By running a trapping REXX script on each attached MVS Console, you can retrieve high priority WTO and WTOR messages and consolidate them on a single console. For example, if you have four SA IOM servers each supporting four MVS consoles, then you can designate one of your SA IOM Message Collectors as a "master" console that collects specific messages from the 16 MVS consoles. Or, each SA IOM server can have its own consolidating Message Collector, and a fifth SA IOM server can have its own Message Collector that consolidates the four others.

Interacting with the Message Collector

You can use the following REXX functions to programmatically interact with a Message Collector session running on your SA IOM server.

Table 8. Message Collector Functions

AFR_MC_LASTMSGNUM	Retrieves the number of messages sent to the Message Collector.
AFR_MC_LASTMSGTEXT	Retrieves the last message received by the Message Collector.
AFR_MC_LASTMSGTIME	Retrieves the time of the last message received by the Message Collector.
AFR_MC_LOGSIZE	Retrieves the number of bytes in the Message Collector log.
AFR_MC_REOPEN_LOG	Reallocates the current Message Collector log under a specified name extension and starts a fresh log.
AFR_MC_SEND	Use this function to send a message to the Message Collector.

For details about each Message Collector function, see the *System Automation for Integrated Operations Management REXX Functions Reference*.

Server-to-server messaging

If you have two or more SA IOM servers that support REXX, then you can send messages from one SA IOM server to another using the AFR_SEND_MESSAGE function.

See "Sharing system resources using the Message Collector" on page 80.

SA IOM to SA IOM network connections

This section provides information on SA IOM to SA IOM network connections.

The SA IOM server can take advantage of all PC resources (for example, optional adapters). Resource use is restricted, however, by hardware limitations.

Usually a PC has, at most, only 8 internal expansion slots available for optional adapters. To increase SA IOM capabilities and performance, consider connecting one SA IOM server PC to another using their Message Collectors to share data and resources.

You can connect two or more SA IOM servers together to create a network of SA IOMs. A sample scenario follows.

Note: REXX support is required in order to network SA IOM servers as described here (see "REXX support requirements (optional)" on page 22).

You can also use SA IOM's peer-to-peer feature to send messages or trigger REXX script execution between SA IOM servers.

Sharing system resources using the Message Collector

You can use the Message Collector with the AFR_SEND_MESSAGE function to exchange messages between two SA IOM servers.

For example, if you want two SA IOM servers to have voice or beeper notification capabilities, but you have only one voice adapter or modem (or a limited number of telephone lines), you can make use of the following technique to share resources.

1. Using the AFR_SEND_MESSAGE REXX function, SA IOM Server 1 sends a message to SA IOM Server 2 with a request to start a REXX program (for example, for beeper service).
2. SA IOM Server 2
   - Receives the message
   - Traps the message
   - Parses the message
   - Executes the program, obtaining data or return codes
3. Once SA IOM Server 2 completes execution, it sends the results back to SA IOM Server 1, using the same mechanism.

Sending a message to a Message Collector

This section describes how to send a message to a Message Collector session.

You can send a message to a Message Collector session *on another SA IOM server* using any of the following methods:

- Use the AFR_SEND_MESSAGE function.
- Use any TCP/IP socket application.
- Use Windows Remote Access Services (RAS).
- Use the RpSend.exe utility program.

Before you start

Collect the following information

- The TCP/IP domain name of the target message collector
- The message collector port number of the target Message Collector

Sending the message

To send messages from your application to SA IOM

- If the application is a REXX script running under SA IOM, then all you have to do is call AFR_SEND_MESSAGE from your script, designating the SA IOM IP host name, port number, and the message.
- If your application is a REXX script running outside of SA IOM, all you need to do is use REXX's Sockets support. (Note sockets support is also generally available in many UNIX or Windows environments.)
- If yours is a Windows environment, consider using the RpSend.exe utility program for testing purposes while you are developing your application. For details see RpSend.exe.

Monitoring the Message Collector session

This section provides information about monitoring the Message Collector.

Using the SA IOM REXX programming API, you have complete control over the selection criteria for messages and the actions taken in response to them.

REXX functions to use with the Message Collector

To create a REXX automation program to read and take action on incoming messages, use the following REXX functions.

- AFR_SELECT
- AFR_GET_LINE
- AFR_LOAD

Note: The REXX script that detects incoming Message Collector traffic must be started on your SA IOM server before messages are sent to the Message Collector session. Otherwise, the messages will not be detected.

Message Collector logging

This section provides information on Message Collector logging.

The SA IOM server creates a log file in the `\logs` directory called `MsgClect.log`. All Message Collector activity is logged to this file.

MSGCLECT.LOG file example

A typical example of a Message Collector log follows.

```
04/09/07 10:54:04 Message Collector Log Initialization
```

Message Collector sample programs

This section contains sample programs that you can use to send data, by using a TCP/IP socket connection, to the Message Collector from the following platforms

- Windows
- UNIX

Note: These programs are samples only.

Windows

The following sample demonstrates how to send data through TCP/IP from a Windows environment.

```
/* Socket connection to SA IOM Message Collector using Windows Visual C++ */
#include <string.h>
#include <stdio.h>
#include <winsoc.h> /* remember to add wsock32.lib to link list */
main()
{
struct sockaddr_in sinAddr; /* endpoint address, Internet format */
SOCKET skt; /* socket descriptor */
char chAddr[] = "129.0.99.99"; /* end-point address in
** dotted format
*/
char msg[] = "SA IOM Message Collector Test\n";
/* sample message */
WSADATA wsaData; /* stores version data returned by WSAStartup */
WORD wVerReq = MAKEWORD(2,0); /* requested version of Windows
** socket DLL
** sample version = 2.0
*/
/*
** Start up winsock interface and check version levels
*/
if ( WSAStartup( wVerReq, &wsaData ) !=0 )
{
printf( "\nCouldn't find a useable winsock.dll.\n" );
WSACleanup();
exit(1);
}
```

```
/*
** Initialize socket Internet address
*/
memset( (char *) &sinAddr, 0, sizeof(sinAddr) );
sinAddr.sin_family = AF_INET; /* specify internet address family */
sinAddr.sin_port = htons( (unsigned short)1090 ); /* sample port = 1090
*/
sinAddr.sin_addr.s_addr = inet_addr( chAddr ); /* convert character string
representing
** internet dot notation to usable
format
*/
/*
** Create socket with PF_INET (internet protocol family) and SOCK_STREAM (tcp) flags
*/
if ( (skt = socket( PF_INET, SOCK_STREAM, 0 )) == INVALID_SOCKET )
{
printf( "\nFailed to create socket.\n" );
WSACleanup();
exit(1);
}
/*
** Connect the socket to the specified end-point, sinAddr
*/
if ( connect( skt, (struct sockaddr *) &sinAddr, sizeof(sinAddr) ) ==
SOCKET_ERROR )
{
printf( "\nFailed to connect.\n" );
WSACleanup();
exit(1);
}
/*
** Send message to end-point through the socket
*/
if ( send( skt, msg, strlen(msg), 0 ) == SOCKET_ERROR )
printf( "\nFailed to write.\n" );
/*
** Close the socket
*/
if ( closesocket( skt ) == SOCKET_ERROR )
printf( "\nFailed to close.\n" );
/*
** Deregister from DLL and free resources
*/
WSACleanup();
printf( "Message,\"%s\" , successfully sent.\n", msg );
}
```

UNIX

The following sample demonstrates how to send data through TCP/IP from UNIX.

```
/* Socket connection to SA IOM Message Collector using UNIX C */
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/socketvar.h>
#include <netinst/in.h>
#include <netdb.h>
extern int errno;
extern char *sys_errlist[];
main()
{
struct sockaddr_in sinAddr; /* endpoint address, Internet format */
int skt; /* socket descriptor */
char chAddr[] = "129.0.99.99"; /* end-point address in
** dotted format
*/
char msg[] = "SA IOM Message Collector Test\n";
/* sample message */
/*
** Initialize socket Internet address
*/
bzero( (char *) &sinAddr, sizeof(sinAddr) );
sinAddr.sin_family = AF_INET; /* specify internet address family */
sinAddr.sin_port = htons( (unsigned short)1090 ); /* sample port = 1090 */
sinAddr.sin_addr.s_addr = inet_addr( chAddr ); /* convert character string
** representing internet dot
** notation to usable format
*/
/*
** Create socket with PF_INET (internet protocol family) and SOCK_STREAM (tcp) flags
*/
if( (skt = socket( PF_INET, SOCK_STREAM, 0 )) < 0 )
{
printf( "\nFailed to create socket: %s\n", sys_errlist[errno] );
exit(1);
}
/*
** Connect the socket to the specified end-point, sinAddr
*/
if ( connect( skt, (struct sockaddr *) &sinAddr, sizeof(sinAddr) ) < 0 )
{
printf( "\nFailed to connect: %s\n", sys_errlist[errno] );
exit(1);
}
** Write with the socket descriptor as you would with a file descriptor
*/
if ( write( skt, msg, strlen(msg) ) < 0 )
{
printf( "\nFailed to write: %s\n", sinAddr.sin_addr.s_addr, sys_errlist[errno] );
exit(1);
}
/*
** Close the socket as you would with a file descriptor
*/
close( skt );
printf( "Message, \"%s\", successfully sent.\n", msg );
}
```

Chapter 9. Peer-to-peer communications

This chapter provides information about peer-to-peer communications.

Topics in this chapter

The following topics are discussed in this chapter:

- "TCP/IP-based peer-to-peer communications"
- "AF-to-AF usage scenarios" on page 87
- "About "non-AF" peer conversations" on page 88
- "About "non-header" peer conversations" on page 89
- "Peer communications protocol" on page 90
- "Peer-to-peer message packet format" on page 91

TCP/IP-based peer-to-peer communications

SA IOM provides an open, TCP/IP-based peer-to-peer feature which enables communication with any other platform supporting TCP/IP. Connectivity between and among SA IOM servers, Tivoli AF/OPERATOR address spaces, and other TCP/IP based applications is vital if you want to automate distributed enterprises spanning multiple platforms.

In any peer-to-peer connection, there is an originating peer which initiates and names the connection and a listening peer which accepts the connection. After a connection has been accepted, the listening peer does not need to initiate a second connection back to the originating peer, because once a connection has been established it is available for 2-way communication. Just as either peer can initiate a connection, either peer can terminate a connection.

"Types" of peer-to-peer communication

The different types of peer-to-peer communication supported by this product are, all of the following.

- Multiple simultaneous standard peer conversations to "AF" peers. Both sides of the conversation use IBM product-provided REXX functions. You can have as many of these conversations as you want. This is the peer interface described in this book, unless a section is specifically labeled otherwise.
- Multiple simultaneous peer conversations to "non-AF" peers. The SA IOM side of the conversation uses IBM product-provided REXX functions, the "non-AF" peer side of the conversation must be programmed to implement the protocol described in "Peer communications protocol" on page 90.
- One special "non-header" peer connection per SA IOM server.

Each type is discussed in turn below.

Standard peer conversations use the standard peer-to-peer configuration controls provided with this product. These standard peer conversations use IBM product-provided REXX peer functions to communicate on both sides of the conversation. (Internally, these implement the protocol described in "Peer communications protocol" on page 90 so that you do not have to implement it.) The term "AF" peer is used to describe another peer system that also implements

the protocol just mentioned. An example of an "AF" peer system is another SA IOM system (or a Tivoli AF/OPERATOR system, or a legacy AF/REMOTE system—historically these products were closely related.) You may need to consult the documentation of the other IBM product to determine if it implements the protocol described in “Peer communications protocol” on page 90.

The PEERSTRT.REX sample script is a working SA IOM REXX script that starts multiple peer-to-peer links to other "AF" peer systems. As a convenience, PEERSTRT.REX could be called during AUTOEXEC.REX processing to establish several long-term, frequently used conversations. The PEERSTRT.REX script is included in the SA IOM sample scripts directory.

Note: TCP/IP-based peer-to-peer communication between SA IOM and a mainframe "AF" peer, requires REXX to be installed both on the SA IOM server PC, and on the z/OS TCP/IP product to be installed and configured on the system where the "AF" peer runs.

Peer functions

In SA IOM there are a group of REXX peer functions that utilize TCP/IP. These functions can be divided into the following categories:

- Connection management (AFR_PEER_OPEN and AFR_PEER_CLOSE)
- Data transmission (AFR_PEER_SEND, AFR_PEER_SENDRCV, and AFR_PEER_RCV)
- Status reporting (AFR_PEER_GETLASTERROR and AFR_PEER_QUERY)

A typical SA IOM REXX script which makes use of these peer functions would begin with a call to AFR_PEER_QUERY to determine whether a particular link is active. If it is not active, an AFR_PEER_OPEN call would be made to start a conversation with the peer. This would be followed by one or more data transmission calls, such as AFR_PEER_SEND, to transmit data or REXX execs, or both, to the peer system. The script might then conclude with a call to AFR_PEER_CLOSE or it might leave the link active for subsequent REXX scripts to use.

For programming details about each Peer function, see the *System Automation for Integrated Operations Management REXX Functions Reference*.

AF-to-AF usage scenarios

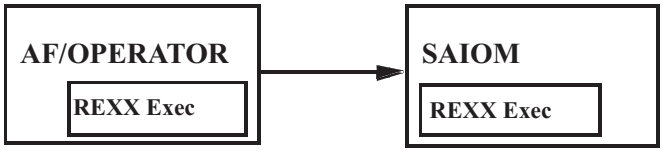
This section presents several high-level, peer-to-peer scenarios that describe possible conversations that can be established between Tivoli AF/OPERATOR and SA IOM.

These scenarios illustrate the diversity of application uses for the peer-to-peer feature. For simplicity, the diagrams only show different types of one-to-one relationships between peers. However, the architecture fully supports one-to-many connections, in which a single SA IOM (or AF/OPERATOR) can have multiple, simultaneous conversations active with multiple peers.

Note: One scenario not shown here is of an SA IOM REXX script opening a peer connection to another REXX script running on the same SA IOM server. The peer-to-peer feature does not support inter-REXX script communication within a single SA IOM server. You can use the REXX Queue functions to accomplish this type of communication.

Scenario 1

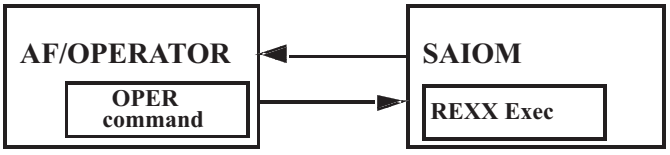
This scenario illustrates a REXX exec running under AF/OPERATOR, that sends input data to an SA IOM REXX exec that is waiting for data to arrive from the AF/OPERATOR peer.



In this case, the data might consist of a critical WTO message that was trapped by AF/OPERATOR, and the waiting SA IOM REXX exec would then receive the message and generate a beeper page or some other form of notification.

Scenario 2

This scenario illustrates an SA IOM REXX exec, that sends an MVS operator command to be issued by AF/OPERATOR and requests response data back from AF/OPERATOR.



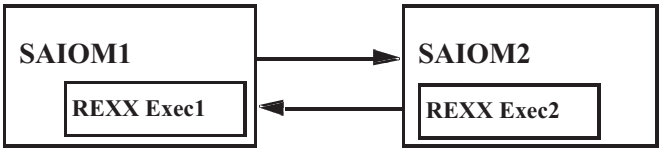
The returned MVS command output can then be stored in a local variable for the SA IOM REXX exec to scan through or parse as needed.

The SA IOM REXX exec implements the scenario by opening a connection to the listening AF/OPERATOR peer. If the connection succeeds, SA IOM sends the text of an MVS OPER command to execute along with the number of bytes of response data to send back, and then waits a specified amount of time for the data to arrive.

The PEERSEND.REX sample script is an example of an SA IOM script that sends an MVS operator DISPLAY command to an AF/OPERATOR peer system for execution, and then receives the DISPLAY output. The PEERSEND.REX script is included in the SA IOM sample scripts directory.

Scenario 3

This scenario illustrates a REXX exec running on one SA IOM server that causes a REXX exec to start running on another SA IOM server, and then waits for response data to be sent back by the triggered REXX exec.

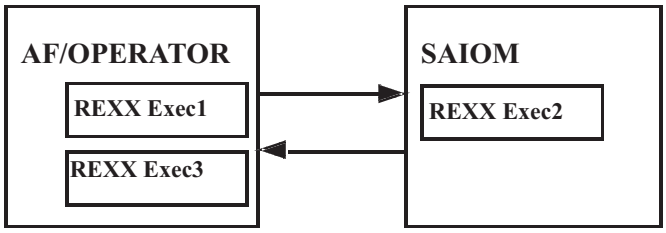


This scenario is logically the same as Scenario 1, except that both participants in the conversation are SA IOM servers.

Note: Multiple exchanges back and forth across the same link can be performed by two SA IOM REXX programs. This exchange could be repeated multiple times without the need to stop and restart the two REXX programs in order to transmit and receive additional messages.

Scenario 4

This scenario illustrates a dual conversation.



One AF/OPERATOR REXX exec initiates a conversation to an SA IOM REXX exec. The SA IOM exec then triggers a different exec to start running under AF/OPERATOR.

About "non-AF" peer conversations

Each SA IOM server can have multiple simultaneous "non-AF" peer conversations using this product's standard peer communications. This method uses IBM product-provided REXX peer functions to communicate on the SA IOM side of the conversation. On the "non-AF" side of the conversation, this method requires you to code the information described in “Peer communications protocol” on page 90. You can have as many peer conversations of this type as you want.

These are the requirements for the "non-AF" side of this product's standard peer communications.

1. TCP/IP connectivity. We don't care what type of Operating System the non-AF peer is running as long as it has TCP/IP connectivity with an SA IOM peer

system. For example, Linux® systems or mainframe z/OS systems can establish peer-to-peer conversations with an SA IOM peer system.

2. REXX is not required on the non-AF peer. However if you don't have REXX then you need *something else* to control the conversation over TCP/IP. You are responsible for coding the necessary peer communications protocols on the non-AF peer side of the peer communication.
3. The IP address of the non-AF peer client application must be authorized to the targeted SA IOM peer system and the **Peer Connections** checkbox must be selected, as described in Defining peer connections.
4. Non-AF applications that start conversations with SA IOM peers must send an ID record as their first data transmission after the TCP/IP peer-to-peer connection has been accepted. For more detail, begin with section "Peer communications protocol" on page 90.

About "non-header" peer conversations

One "non-header" peer session can be established on each SA IOM server through the TCP/IP network. The special "non header" peer conversation frees you from having to program your non-AF peer application to use the same TCP/IP-based communications protocols that AF peers use. Instead, on the other ″non-AF″ side of the conversation, you use standard TCP/IP calls to communicate with SA IOM. There are no headers or link IDs, only data is transmitted.

This method is based on the product's standard peer communications implementation. It uses the same peer functions on the SA IOM side of the conversation, which you use in the same way with a special link ID keyword. The "non-header" peer session uses its own special TCP/IP listening port number, that you must customize using the server profile. The incoming peer communication goes through the same authentication as for AF peers before automatically starting a REXX script to handle the conversation.

The PeerNSvr.rex and PeerNCli.rex sample scripts demonstrate how to quickly and easily get the SA IOM server communicating with peer "non-AF" systems using this method.

Here are all the steps to set up "non-header" peer communications.

1. TCP/IP connectivity must be in place. We don't care what type of Operating System the other peer side is running as long as it has TCP/IP connectivity with an SA IOM peer system.
2. Use the server profile configuration parameter PEER_PORT_NON_AFPACKET to define a special TCP/IP listening port that is dedicated to listening for incoming peer communications of this type, as described in Server Profile. On the next server restart, the special listening port for non-header peer conversations will be created. When a caller on this port is authenticated the REXX script PeerNSvr.rex will be started.
3. In order to successfully authenticate, the incoming peer must be defined in the peer connections section of the server configuration (as described in Defining peer connections). The **Peer Connections** checkbox must be selected, but the port used will be the special one you specified in the server profile configuration. Define all the peers that are allowed to connect to the server using the **Peer Properties** dialog.
4. Modify the REXX sample script PeerNSvr.rex to suit the needs of the communication. This script is automatically started when the incoming non-header peer has connected and is authenticated.

Note: Only one "non-header" peer session per SA IOM server is allowed. If this session type is already active the text "PEERNSVR BUSY" is returned and the new connection is closed.

5. Outbound connections are started from any script using the AFR_PEER_OPEN API with the data type parameter of 'USRDATA' and the special link ID keyword "NONAF". For an example of how to start an outbound non-header peer session see the REXX sample script PeerNCli.rex.
6. For programming details about each Peer function, see the *System Automation for Integrated Operations Management REXX Functions Reference*.

Peer communications protocol

This section describes the peer-to-peer communications protocol language that is used by SA IOM (and Tivoli AF/OPERATOR). It is intended only for users who want to create non-AF peer applications which will communicate with SA IOM *by using the same TCP/IP-based communications protocols that AF peers use*.

Peer-to-peer communications protocol language

As a rule, both SA IOM and Tivoli AF/OPERATOR require all peer-to-peer data transmissions to begin with a LINKID parameter.

The LINKID is a 1-to-8 byte, alphanumeric character string, that is specified in AF/OPERATOR LINK commands, the COMSDRCV REXX API, and SA IOM peer function calls. The originating peer which initiates the conversation (either with an AF/OPERATOR LINK DEFINE command, an SA IOM AFR_PEER_OPEN call, or a non-AF peer's transmission of an ID record) assigns the LINKID, which uniquely identifies the conversation.

It is essential that LINKIDs be kept unique since an AF peer can have multiple conversations active at the same time. To ensure that sends and receives are done on the correct link, each AF peer maintains a lookup table of LINKID names.

In addition to the LINKID parameter, all outbound data transmissions require a DATATYPE parameter to signify the type of message being sent. DATATYPE can have one of the following string values:

ID
Indicates that the send buffer contains peer attributes or descriptors. ID records allow a peer to identify attributes about itself, such as whether it will send ASCII or EBCDIC data. By default, SA IOM sends ASCII data (and AF/OPERATOR sends EBCDIC data).

Note: This record is *only required for non-AF peers starting conversations with AF peers.* In this case, the ID record must always be the first message sent. AF peers internally generate ID records when starting conversations with each other.

EXEC
Indicates that the send buffer contains an operator command or REXX program which is to be executed on the peer system.

DATARPLY
Indicates that the send buffer contains response data which was requested by the peer system. It should only be used if the other peer issued a SENDRCV call and is waiting for a response.

USRDATA Indicates that the send buffer contains user-specified data, such as input to a REXX program running on a connected peer, or some other type of conversational data. It should only be used if the other peer is in a "receive" state (for example, waiting for data using an AFR_PEER_RCV function call).

With the exception of the "ID" record, these DATATYPE values correspond to the ones supported by AF/OPERATOR's COMSDRCV REXX API functions. See "Understanding the Communications Environment" in the **AF/OPERATOR Command Reference Manual** for more information on establishing TCP/IP connections and using the COMSDRCV REXX API.

Peer-to-peer message packet format

The following figure presents a diagram of the internal message packet format which is used by SA IOM (and Tivoli AF/OPERATOR) for all of their standard TCP/IP-based conversational data transmissions.

Linkid or Message Token	Data Type	Reply Data Length	Send Data Length	Send Data
8 Byte String or Integer	8 Byte String	2 Byte Integer	2 Byte Integer	32K max

Note: The SA IOM (and Tivoli AF/OPERATOR) peer REXX functions already implement this internal message packet format, so you do not need to code to this specification if you are simply planning to use the existing product-provided peer REXX functions. Only non-AF peers that want to communicate with SA IOM *by using the same TCP/IP-based communications protocols that AF peers use* must adhere to the message packet format shown above.

If you want to create non-AF peer applications such as C/C++/Java/Visual Basic programs or REXX scripts that use native REXX socket code, it is essential that you know the details of the message packet format, and the order and restrictions for sending different types of peer records. By following this format, a REXX script using native REXX socket code or a C/C++/Java/Visual Basic program making socket calls, can establish TCP/IP-based peer communications with SA IOM, provided that the non-AF peer is running on a client machine whose IP address has been authorized to the targeted AF peer system. An additional requirement is that non-AF applications that start conversations with AF peers must send an ID record as their first data transmission after the TCP/IP connection has been accepted. (AF peers automatically send ID records to each other.) If the IP address of the non-AF peer has not been included in the AF peer's trusted hostname list, or if the ID record is missing or incorrectly coded, the conversation will not get started.

The `PEERSOCK.REX` sample script is an example of a native REXX socket program that uses the peer-to-peer message packet format to communicate with SA IOM. This script is included in the SA IOM sample scripts directory.

Linkid or Message Token parameter

The Linkid/Message Token parameter in the message packet has dual uses. It is normally the place where the linkid is stored. The linkid is the 1-to-8 character, alphanumeric string assigned by the originating peer to name the conversation. It

should be left justified so that it begins in position 1, and is blank padded to fill all 8 bytes. The linkid must be present in the first message sent, which is always an ID message.

Once a conversation has been established, this 8-byte field can be reused as a message token. Tokens are used to associate response data received from a peer system, with the particular REXX script or program which requested the response data. Tokens are helpful if multiple requests for data have been sent out and the order of receipt is unpredictable. In this situation, the sending peer should supply a unique integer token in the first 8 bytes of the message. The peer system is then obligated to return the token in the first 8 bytes of its message, along with the response data it is returning.

If message tokens are not being used, then each message should begin with the conversation linkid.

Data Type parameter

The Data Type parameter in the message packet must be a known data type, such as EXEC or DATARPLY. Unknown data types will be rejected. The Data Type must begin in the ninth position of the peer-to-peer message packet.

The Data Type parameter should reflect the contents of the send buffer, which is in the fifth parameter of the message packet format. The following topics provide some additional details about the contents of the send data buffer for each valid peer-to-peer data type.

Data Type Values	Description
ID	For non-AF peers, this record must be the first message packet sent in a new peer connection. The send data buffer should contain information about the connecting peer, such as its name, whether it will send ASCII or EBCDIC data, and the version information. Following is an example of a typical ID message sent to an SA IOM peer: **RPLINK ID** **0041NAME=MYAPP;VERSION=1;DATA=ASCII;REPLY=YES** In this example, a new connection called RPLINK is being established. The send data buffer is 41 bytes in length and the reply data length is 0. **Note:** The Reply Data Length and Send Data Length parameters are both 2-byte short integer fields, not text representations of integers. Also, there are byte ordering differences to be aware of when transmitting integer values between heterogeneous peer systems. By default, mainframe peers such as AF/OPERATOR send integers in "big-endian" order (the most significant byte first), whereas Intel-based peers such as SA IOM send integers in "little-endian" order (the least significant byte first and the most significant byte last). For example, if you were building this ID record string in a REXX program, you could code the length fields as follows: **sendstring = "RPLINK ID ",** **|| D2C(0) || D2C(0) || D2C(41) || D2C(0) ||,** **"NAME=MYAPP;VERSION=1;DATA=ASCII;REPLY=YES"** When a non-AF peer initiates a conversation to an AF peer, it must specify REPLY=YES on its ID record. If the ID record is accepted, the AF peer will return an ID record with REPLY=NO specified. When a non-AF peer receives an ID record from an AF peer requesting that a conversation be started, it must specify REPLY=NO on its acknowledging ID record. **Note:** Position matters in all peer messages. If a linkid is less than 8 characters in length, it must be blank padded to fill its allotted 8 bytes. The same is true for the data type parameter.
EXEC	The send data buffer should contain the name of a REXX script (along with one or more optional script arguments) or an MVS operator command, which is to be executed on the target AF peer system. Following is an example of a typical EXEC message sent to an SA IOM peer: **LINK1 EXEC 0010EX ABC.REX** In this example, the message packet will cause a REXX script named ABC.REX to begin executing on the connected SA IOM peer. No reply data has been requested because the reply length is 0.

Data Type Values	Description
DATARPLY	The send data buffer will contain whatever reply data is being returned, up to the length specified in the reply data length parameter that was in the initiating request. Following is an example of a typical DATARPLY message sent to an SA IOM peer: **RPLINK1 DATARPLY0036HERE IS THE REPLY DATA YOU REQUESTED** In this example, the message packet will return 36 bytes of reply data to the peer system, which is connected on the linkid named RPLINK1. No reply data has been requested because the reply length is 0. In SA IOM-to-SA IOM peer-to-peer conversations, it is possible to request reply data in a DATARPLY message by coding a non-zero reply length. The other SA IOM peer can do the same and this back-and-forth conversation can be repeated indefinitely. However, AF/OPERATOR does not support multiple DATARPLY messages being sent on the same linkid, without first stopping and restarting the connection.
USRDATA	The send data buffer can contain any user-defined data, such as error text captured on the peer system, a phone number to page, a broadcast-type message to be read or acted upon by the receiving peer, and so on. This data type will normally be received by a blocking SA IOM REXX script, which is waiting for input data. Following is an example of a typical USRDATA message sent to an SA IOM peer: **PRODSYS USRDATA 0038SA IOM System A is shutting down!!!** In this example, the message packet sends a broadcast message to the peer system, which is connected on the linkid named PRODSYS.

Reply Data Length parameter

The Reply Data Length parameter in the message packet should be coded as 0 if no reply data is expected or needed. Otherwise, specify from 1 to 32K of reply data as required. This parameter must begin in the seventeenth position of the message packet.

The AF peer which receives a message packet with a non-zero reply length will only send the amount of reply data requested, even if there is more data that could be sent.

Send Data Length parameter

The Send Data Length parameter in the message packet indicates the length of the send data buffer and can be any integer less than or equal to 32K. This parameter must begin in the nineteenth position of the message packet.

It is important that the send data length value be accurate, because it determines how much data will be read and processed by the AF peer. If the send data length is smaller than the send buffer, the AF peer system will truncate the message. If

the send data length is larger than the send buffer, the AF peer system could hang while it waits for the remaining data to arrive.

Send Data parameter

The Send Data parameter in the message packet is the send data buffer itself.

The first four parameters represent the header portion of a peer-to-peer message packet, which must be 20 bytes in length. The data being transmitted is expected to begin in the twenty-first position.

Chapter 10. Beeper paging

This chapter provides information about the SA IOM beeper paging feature.

Topics in this chapter

The following topics are discussed in this chapter:

- "Sending optional text"
- "Touch-tone versus modem paging"
- "Automatic paging" on page 99
- "Fine-tuning a touch-tone WTOR" on page 101

Sending optional text

The SA IOM beeper paging feature automatically pages support technicians whenever specified events occur on the mainframe host. If their beepers support alphanumeric message display, SA IOM can also send optional text describing the nature of the problem.

Optional message text

The number of characters of optional message text that can be sent depends on:

- The message area available on the MVS screen.

  This is controlled, in MVS, by the MFORM() keyword of the **K S** command. For example, changing **MFORM=(T,S,J)** to **MFORM=(T)** would increase the available message text by 13 characters. Any adjustments to the message display attributes of the console assigned to the SA IOM port should be specified in an MVS startup file.
- The size of your modem's dial-string command buffer, if you are doing DTMF (Touch Tone) paging.
- Any size limitations of your beeper paging service.

Note: If your host PC has a supported voice adapter installed, and you plan to perform only touch-tone paging, you do not need a serial port for beeper paging. Voice adapters are described in Chapter 11, "Voice control," on page 103.

Touch-tone versus modem paging

This section compares touch-tone and modem paging services.

SA IOM can use both touch-tone and modem paging services. For example, a given WTOR on the MVS Console/Beeper session may generate a touch-tone page to technician A, while another problem might generate a modem page to technician B. There are distinct pros and cons to both types of paging services. Understanding the differences can help you decide which type to use in a given situation.

The following table compares the relative advantages and disadvantages of both paging service types.

Table 9. Comparison of touch-tone and modem paging

Service Type	Advantages	Disadvantages
Touch-tone	• Less expensive • Unlimited vendor support • Can use a voice adapter, which provides greater reliability and frees up a serial port for other uses	• Less reliable • More difficult to use • Beepers display only numeric data • Modem used may limit display to 10 digits or less
Modem	• More reliable • Easier to use • Beepers display both numbers and letters • Can display long messages	• More expensive • Limited vendor support

Touch-tone paging requests

You may want to use touch-tone paging requests with a voice adapter rather than using a modem to generate the tones.

Voice adapters help you achieve more reliable touch-tone pages because they can recognize some line conditions that modems cannot. You can write a program that can indicate when it has successfully connected to the paging service. You do not have to estimate the necessary delays.

Touch-tone paging through a serial communications port is less reliable than touch-tone paging with a voice adapter. The problem lies in the fact that once a call to the paging service is generated, it can take a variable length of time to actually connect to the paging service computer. And since the touch-tone paging service does not transmit a modem carrier signal, modems for this kind of service cannot tell when they have connected.

To generate a successful touch-tone page from a serial port, therefore, you must code extra delays into the phone number and pager ID numbers that SA IOM sends to the paging service. If the delays don't exactly match the response time of the phone company switching system and the paging service computer, the page will fail.

Modem paging services

Modem-to-modem paging requests are the most reliable, and should be used in critical situations. Modem-based systems allow SA IOM's modem to call the paging service's modem to establish a communications link with error notification. The REXX script, BEEPCALL.REX, included with SA IOM, provides this function using a standard Telocator Alphanumeric Protocol (TAP) to communicate with the service.

If your paging service uses a different protocol, you will need to modify BEEPCALL.REX. Most major modem paging services support the TAP protocol.

Paging services using the IXO protocol (a precursor to the TAP protocol) should also work successfully with SA IOM, but if the service has made any modifications to the protocol you may experience problems.

It is recommended that the following procedure is used when shopping for a compatible modem paging service vendor:

1. Contact the sales representative and ask to speak with a technician.
2. Explain that you are looking for a modem paging service to support a program that can connect, using a modem, to their paging computer and initiate alphanumeric beeper pages using the TAP protocol. Does their service support this protocol? (Most likely only a technician will be able to answer this question.)
3. After you are in contact with a person who understands the question, some things you need to know are
   - Recommended baud rate
   - Recommended data bits/byte
   - Recommended parity
   - Stop bits

   Example values are respectively: 2400, 7, E, and 1.
4. If you decide this is the paging service for you, you will need the modem access number (the number that your modem will dial to connect with the modem on the paging service's computer).

Tuning for modem-to-modem paging

To generate a successful, consistent modem-to-modem page, you may need to spend time tuning and experimenting with various baud rates for each modem, due to:

- Differences between SA IOM's modem and the paging services's modem
- The relative quality of the phone line
- The robustness of the paging service software

It is recommended that you start at the highest baud rate supported by both SA IOM's modem and the paging services's modem (not faster than 28.8, however, for simple paging). You can then evaluate the results and, if necessary, lower the baud rate until consistent success is achieved.

Automatic paging

This section provides information on automatic paging.

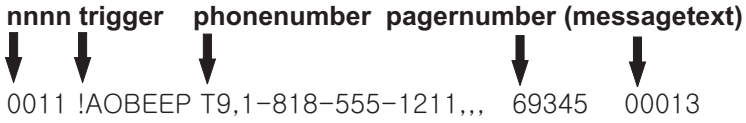
Automatic paging works by monitoring message traffic on the MVS/Beeper consoles for a WTOR that begins with a specified trigger pattern. When the trigger is detected, the program parses the remainder of the WTOR for the paging parameters such as phone number, pager number, and so on. The program returns a response to the WTOR and may also display a message on the host PC's display screen. The possible WTOR responses are:

Responses	Descriptions
Y	Page successful
N	Page aborted

What triggers automatic beeper paging

There are two events that trigger automatic beeper paging:

1. AF/OPERATOR (Versions 210 and later) or OG/MVS (Versions 100 and later) generates a BEEP command.
2. Any other mainframe program generates a WTOR with the proper syntax, as described below:



See the description of `messagetext` for a discussion of issues related to message length.

Syntax	Description
nnnn	The WTOR response sequence number.
trigger	The pattern denoting a beeper request. This string can be up to 20 characters in length and can include imbedded blanks. AF/OPERATOR's or OG/MVS's BEEP command always generates !AOBEEP as its trigger. When configuring SA IOM's beeper paging parameters, you specify which trigger pattern to act upon.
phonenumber	A string of up to 30 characters that can contain digits and selected non-numeric characters. These other characters are the letters M and T, the comma (,), the hyphen (-), and parentheses (). The first item in the string must be a single character specifying the type of paging service being used. The character M denotes an asynchronous modem-to-modem paging service, and the character T denotes a touch-tone paging service. Any other character in the first position is illegal. The phone number of the paging service immediately follows this first character and can contain parentheses and hyphens to enhance readability. When using a touch-tone paging service, insert commas as needed to force a delay. Each comma gives you a two second delay, and you can string commas together to produce longer delays. When using a modem paging service, however, you should never use commas to force delays because they are unnecessary with modem protocols. Inserting commas may cause the paging service computer to time out, resulting in premature hang-up or protocol failure.
pagernumber	A number required by some paging services to specify the person to whom the page is directed. This number can be up to 8 digits long. This field must contain at least 1 digit. Use the number 0 if the paging service does not require a pager number. If you want to call more than one person, separate the pager numbers with a comma, or specify the name of a file that includes a list of pager numbers. When specifying a file name, prefix it with **0** (zero). SA IOM then looks for a file name that ends with the extension **.PID**. For example, when the pager number **01234** is passed, SA IOM looks for a file named **1234.PID**. **Note:** In the file, specify one pager number per line.

Syntax	Description
(messagetext)	An optional string of characters to be transmitted for display on the target person's beeper. Since the WTOR text parsed by SA IOM resides on one 80-character line, the maximum length of the message text string is 80 minus the number of characters used for the WTOR response sequence number, the trigger, the phonenumber, the pagernumber, the 6 characters used by the beeper paging feature for modem control characters and default delays, and the spaces used to separate the fields. The message text string may contain any printable ASCII character, including spaces. Due to the limitations of telephone keypads, most touch-tone paging services will accept only digits in this field. Once a non-numeric character is encountered, the paging service drops that character and any following characters, transmitting only the digits received prior to that. The handshaking protocol used in a modem page allows you to keep a connection open long enough to send up to 80 characters of optional message text. Because a touch-tone page does not use protocols, the number of characters you can send is therefore dependent on the command buffer size of the modem being used.

Fine-tuning a touch-tone WTOR

This section provides information on fine-tuning a touch-tone WTOR.

When testing WTORs used for touch-tone pages, it is helpful to first call the paging service yourself with a stopwatch and time the delays between the audio prompts for the pager number and optional message digits. You can then approximate the number of commas to insert at the appropriate spots.

If the page fails, add or subtract commas until you get a successful page. You may find it easier to determine where to put the commas if you listen to your modem as it calls the paging service.

There are no exact guidelines to follow when tuning the WTOR, it is largely a matter of trial and error. The procedure below should help you get started. Call IBM Support if you need assistance.

Initial procedure

Before testing WTORs for touch-tone pages:

1. Turn up the volume on your external modem so you can hear the phone line activity.
2. Make sure you have one of the paging service's beepers close at hand. You will need to know when a page is successful.
3. Make sure you have a stopwatch handy. You will need to time responses lasting only seconds.

See the sample REXX script `Beepcall.REX` for an example.

Testing procedure

To test WTORs for touch-tone pages:

1. Listen carefully to the phone line activity. When you hear the paging service answer the line, start the stopwatch.
2. When the paging service gives you the cue to enter the pager number, note the elapsed time on your stopwatch. Write this time down and call it “cue one.” If applicable, listen further and note the elapsed time when you hear the cue for optional text. Call this “cue two.”
3. If the page is successful, your beeper is activated. Run the page again several times to check the consistency of the phone system and paging service response times.

   Once you have a successful page, combine the fields of the dialog box to assemble the WTOR. The message that’s generated each time you use the PAGE option also shows the appropriate WTOR string.

Note: As described in “Touch-tone versus modem paging” on page 97, touch-tone pages by nature are not always reliable. Even though the page may be successful on most occasions, it may occasionally fail.

Calculating delays

If the page is not successful, you need to calculate the needed delays.

1. Look at your elapsed time for cue one. If it is greater than 2 seconds, subtract 2 seconds and then divide the result by 2. The final product is the number of commas you must place at the end of the **Phone Number** field. If there is a remainder of 1, add another comma to the field.
2. If applicable, look at the elapsed time for cue two. Subtract cue one from cue two to determine the number of seconds that elapsed between the request for pager number and the request for optional text. Divide the result by 2. The product is the number of commas you must place at the end of the **Pager Number** field. If there is a remainder of 1, add another comma.
3. Re-edit the dialog box fields, adding the requisite commas in the **Phone Number** and **Pager Number** fields.
4. Try the page again (see “Testing procedure” on page 101), reiterating the steps until you get a consistently successful page.

Chapter 11. Voice control

This chapter provides information on voice control.

Topics in this chapter

The following topics are discussed in this chapter:

- "Controlling a voice adapter"
- "Installing Dialogic voice adapters"
- "Creating voice applications" on page 106
- "Beeper paging with a voice adapter" on page 107
- "Voice diagnostic and debugging facilities" on page 108

Controlling a voice adapter

SA IOM provides several external REXX functions that can control a voice adapter.

These REXX voice control functions allow you to create event-driven voice applications. You can use REXX to write scripts that perform automatic dialing, answering, recording or playing a message, beeping sequences, and tone detection. Specifically, you can use the voice adapter with touch-tone paging which results in more reliable paging than is possible when using a modem to perform touch-tone paging.

Note: If you have not already done so, see ("Touch-Tone Versus Modem Paging" on page 137).

Installing Dialogic voice adapters

This section provides information on installing Dialogic voice adapters.

Supported voice adapters are listed here. Note these adapters are no longer in production.

SA IOM supports the following types of Dialogic voice adapters to perform voice functions and beeper paging functions only. That is, functions such as dialing, answering, recording or playing a message, beeping sequence, and tone detection.

Adapter type	Model	Description
ISA bus adapter Note: ISA bus adapters are configured using Dialogic software that came with the adapter.	D/21D	Provides support for up to two telephone lines.
ISA bus adapter	D/41D	Provides support for up to four telephone lines.
PCI bus adapter	D/ESCEuro	
PCI bus adapter	D/4PCI	Provides support for up to four telephone lines.

Adapter type	Model	Description
PCI bus adapter Note: PCI bus adapters are also known as plug and play	D/4CIU	This card will work in earlier versions of Windows but is required for Windows XP and Windows 2003. There are two paths of required support software available from Dialogic Either use: Intel(R) Dialogic(R) System Release 6.0 for Windows *) Or use: Intel(R) Dialogic(R) System Release 5.1.1 for Windows, upgraded with both of the following: SR 5.1.1 Feature Pack 1 *) SR 5.1.1 Feature Pack 1 Service Update 15 *) separately purchased product See the Intel® Dialogic Web site for further information.

Text-to-speech support

Only the ISA bus Dialogic voice cards listed above support the ability to process a text file into spoken text. This capability ***is not supported*** by the D/ESCEuro or the D/4PCI and D/4CIU cards listed above.

Installation

Perform the following steps to install an **ISA bus card**:

1. Read the hardware installation literature and obtain a list of port and memory addresses to which the card may be configured.
2. Referring to the Configuration notes below, determine which port and memory addresses will not conflict with those ports already used by other installed devices.
3. Configure the card referring to the hardware instruction manuals and the information gathered in the above steps.
4. Power OFF the PC and install the card.
5. Use the software supplied with the Dialogic board to configure the card for operation.

Perform the following steps to install a **PCI bus card**:

1. Disconnect the power source from the PCI bus.

   Attention: Do not merely Power OFF the PC because this is not sufficient. Current® PCs have power to the motherboard even when the power is turned off.
   When you are certain that the power to the PCI bus is off, install the card in an available PC slot.
2. Restart your PC.
3. Configure using the DCM.

These installation instructions apply to both of the PCI voice cards.

Configuration notes

Before configuring the SA IOM server for voice adapter use

1. Check your current system configuration before you power down the PC.
   - Use Windows Diagnostics to check the IRQ levels and memory addresses that are in use on your system. Bring up the Windows Diagnostics program, available from the Administration Tools menu, and select the **Resources** tab. Examine the information displayed, first when the IRQ button is pressed, and again when the Memory button is pressed.

Button	Description
IRQ	The numbers listed under IRQ are interrupt requests used by devices on your system. Write down the IRQ numbers. Later, the Dialogic Board Configuration Utility will prompt you to select an IRQ value that is not used by another device.
Memory	The numbers listed under Address are memory address ranges (for example, D0000 - D2000, which is the default) used by devices on your system. Write down the memory address ranges. Later, the Dialogic Board Configuration Utility will prompt you to select a memory address (for example, D0000) that does not overlap into a memory address range used by another device.

   - The Dialogic voice adapter requires the Streams Environment Network Protocol. (This is a Windows configuration option, no additional software is required.) From the Windows Control Panel, select Network, then Protocols. If **Streams Environment** is not listed, Add it.
2. Set the jumpers and switches on the Dialogic adapter to an IRQ number and a memory address that are not in conflict with other devices on your PC. Note the IRQ number and the memory address you use.
3. Install the Dialogic software using the Dialogic installation program. This program will copy files, update the registries, and eventually start the Dialogic Board Configuration Utility. You will be prompted to select the type of voice adapter you are using, the IRQ number, and the memory address.
4. Shutdown and reboot the PC. After Windows is started, go to the new Dialogic System Software folder and manually start Dialogic Services.
5. If an error occurs starting Dialogic Services, try using different IRQ and memory address settings for the Dialogic Adapter. Shutdown the machine then repeat from step 2.

   You can check the Event Viewer System Log for additional information. Event Viewer is available from the Administration Tools menu.
6. When all Dialogic Services initialization processes are successfully completed, you can set Dialogic Services for automatic startup mode.
7. Verify the adapter is operating correctly by trying some of the Dialogic demonstration sample programs. Make sure the adapter is operational before proceeding. The adapter should be operational without using SA IOM.

Configuring the SA IOM server for voice adapter use

You will need to supply information on the appropriate SA IOM Server Configuration properties pages. The information you supply will depend on whether you are using the voice adapter for beeper paging, voice applications, or a combination of both.

Creating voice applications

This section provides information about creating voice applications.

Voice applications generally take the form of an event-driven program that waits for a certain condition to occur and then generates a phone call to a human. If a human voice answers the call, the application plays a prerecorded message that asks listeners to respond by pressing the touch-tone keys on their telephone keypad. The application then takes different courses of action based on the listener's responses.

In addition to asking for touch-tone responses, voice applications may also record verbal responses from listeners for later playback to other listeners. Telephone messaging systems are a common example of voice applications that utilize both touch-tone and verbal responses from listeners.

Voice functions

The external REXX functions provided with SA IOM that control the supported voice adapters are as follows:

REXX functions	Descriptions
AFR_VOICEANSWER	Waits for an incoming call.
AFR_VOICEBEEP	Generates a beep tone to provide audio cues for listeners.
AFR_VOICEDIAL	Dials a specified phone number.
AFR_VOICEGETTONES	Reads the touch-tone responses generated by listeners.
AFR_VOICEHANGUP	Terminates a phone call.
AFR_VOICEINIT	Tests if the server's voice adapter is accessible.
AFR_VOICERECORD	Records a voice message.
AFR_VOICESPEAK	Plays a prerecorded voice message for the listener. Messages are digitized samples stored in a server PC file.
AFR_TTS_FILE	Speaks the text contained in a file to a user dialed into a Dialogic voice card.
AFR_TTS_STRING	Speaks the text contained in a string to a user dialed into a Dialogic voice card.

Recording messages

Voice messages are digitized and stored in files on your SA IOM server. Each file contains a single message.

You will use the following functions:

- AFR_VOICEINIT
- AFR_VOICEDIAL
- AFR_VOICERECORD
- AFR_VOICEHANGUP

The basic procedure for recording messages you will use in a voice application is as follows.

1. Use the VOICEINIT and VOICEDIAL functions to generate a call to the phone at your own desk.

2. Use the VOICERECORD function to record your message. The VOICERECORD function will generate a beep to prompt you to begin speaking. The VOICERECORD function stops recording at the number of seconds specified by the length parameter, so give yourself plenty of time. The function will automatically stop recording once it detects a few seconds of silence, thereby minimizing file size.
3. When you have finished recording, use the VOICEHANGUP function to terminate the phone call.

Getting listener responses

User responses can be either touch-tones generated by the listener's telephone keypad or verbal messages recorded by the listener.

You will use the following functions.

- AFR_VOICESPEAK
- AFR_VOICEGETTONES
- AFR_VOICERECORD
- AFR_VOICEHANGUP

The basic procedure you will use to obtain user responses is as follows.

1. Once the voice adapter has connected to a human listener, use the VOICESPEAK function to play a message describing the range of responses the listener can make.
2. If you have asked the listener to make touch-tone responses, use the VOICEGETTONES function to capture the responses.

   If you have asked listeners to make verbal responses, use the VOICERECORD function to record their message.

   The VOICERECORD function will generate a beep to prompt the listener to begin speaking.

Beeper paging with a voice adapter

This section describes how to perform a touch-tone page using a voice-adapter. A good starting point is to first go through the DTMF (Dual-Tone Multi-Frequency), also known as TouchTone paging. The sequence goes something like this:

1. Take phone offhook.
2. Dial the number.
3. Number called answers with:
   a. A voice
   b. Two or three beeps, approximately 1000 cycles (C above middle C)
4. Enter numeric data to be sent terminated with the # key.
5. Hangup (replace phone on hook).

Same steps using AFR_VOICE APIs

1. Ret = AFR_VOICEDIAL(line, phoneno, rings).
2. When AFR_VOICEDIAL() returns evaluate Ret.
3. Return code is:
   a. 0 - voice answered
   b. When the VOICEDIAL function returns 0 (voice detected) or -7 (ring back stopped), use the VOICEDIAL function again to play the tone comprising

the phone number to be transmitted. Note that the call should always return a 0 since the connection is already established. All other return codes would indicate an error. Return code 0 or -7, send numeric data to the paging service terminated with a # sign.

4. Hangup the phone.

Voice diagnostic and debugging facilities

This section provides information on voice diagnostic and debugging facilities, error processing, and recovery.

Recovery and error processing

Following is information to help you with error processing and recovery.

- Voice cards cannot detect when the person called hangs up the phone. Hang-up can occur during playback, record, dial, or during any voice function. IBM has implemented some special, extended return codes for conditions that may occur when using the REXX Voice functions. To use these extended return codes you must uncomment the following profile entry `REXX_VOICE_VERSION = 2` in the server profile configuration file. For specific extended return codes returned by a Voice function, see the description of the individual function in the *System Automation for Integrated Operations Management REXX Functions Reference*.

  Note: Notify IBM if these special return codes cause more problems than they correct or if other conditions exist that you would like to detect.
- Your REXX scripts may experience ringback stopped (return code -7) from AFR_VOICEDIAL. This return code is returned after ten seconds if it cannot assign a more specific return value. Some of the reasons for this happening: Answered with a single frequency tone (a voice answering is detection of broad spectrum signal), answered with silence. How you respond depends on the application. If you are calling a DTMF or Touchtone-based beeper paging service, then -7 is most likely just as legitimate a return code as a zero.
- Your REXX scripts should always call AFR_VOICEHANGUP to close a line when you encounter errors that you don't want to correct, cannot seem to correct, or do not expect. When exiting a REXX script, AFR_VOICEHANGUP should be the last function called before the return. Be careful to always hang up the correct line. AFR_VOICEHANGUP will abort any active voice requests and close the Dialogic Voice channel.
- Dialogic voice lines cannot be shared by multiple scripts. Once a REXX script begins to use a line, another script must not use it until the first script has completed its voice activity and hung up the phone using AFR_VOICEHANGUP. Improper sharing or line mixing among scripts may crash REXX Management (red light) on the SA IOM server.
- AFR_VOICESPEAK can complete normally with return code 0 or 20. Return code 20 indicates that the person who answered the phone pressed a key on the key pad to terminate the playback of the message. You can use AFR_VOICEGETTONES to retrieve the key that was pressed. If AFR_VOICESPEAK ends with return code 3 (error playing message) or return code 21 (noise on playback), this may indicate that the phone was hung up during playback.
- If AFR_VOICERECORD completes with return code 18, your record time may be too short or the phone may have been hung up during the record. If you make sure your records have adequate time for the message to be recorded, you can then assume that return code 18 means the phone was hung up. There still may be a recording followed by silence.

Voice operation diagnostic logging information

Any diagnostic information is logged into the RpServer.log according to the currently selected Trace Level. At the default Error level, logging is limited to actual failures such as initialization. For diagnostics in greater detail, you must raise the level to at least the Trace level. This logging information is mixed in with all of the other logging information produced by other components of RpServer.

You can extract this diagnostic data using a filter such as Windows Find.exe, a filter program that is run from a Command Prompt.

1. Navigate to the Program Files\IBM\SA IOM\logs directory.
2. Enter the following command.

   ```
   Find "::Voice" RpServer.log >temp.txt
   ```

3. Now you can view the output with notepad.

Alternatively, you can use the Log Reader program described in Utility Programs to filter on the "::Voice" text in the RpServer.log.

Chapter 12. SA IOM Hardware Management Console interface

This chapter provides information on the SA IOM Hardware Management Console (HMC) Interface.

Topics in this chapter

The following topics are discussed in this chapter:

- "HMC interface overview"
- "Configuring the SA IOM HMC interface" on page 112
- "Using the SA IOM HMC interface" on page 116
- "HMCACT.REX" on page 119

HMC interface overview

The SA IOM HMC Interface allows you to remotely monitor and manage resources in an IBM zSeries Hardware Management Console (HMC) environment.

From an SA IOM session, you can

- Issue commands to Central Processing Complexes (CPCs) and their associated software images
- Monitor the operating status of HMC hardware and software resources

Description of HMC network components

The HMC is a workstation, connected to a private LAN, that provides the means to configure and manage zSeries resources. It does this through a resident application called the Hardware Management Console Application (HWMCA). Each HMC runs its own copy of HWMCA. Therefore, if you want to use SA IOM to manage multiple HMCs, you must configure each HMC's HWMCA separately.

Each SE is a dedicated PC hardwired to one CPC. It controls that CPC and its associated images. The standard communication protocols between the HMC and the SEs are SNA (LU6.2), TCP/IP, and NETBIOS (used for heartbeat checking).

S/390 PTS configuration with SA IOM

The figure in this section shows a typical S/390® PTS configuration, consisting of

- One or more HMCs
- CPCs and their Service Elements (SEs)
- A private LAN connecting the HMC and SEs

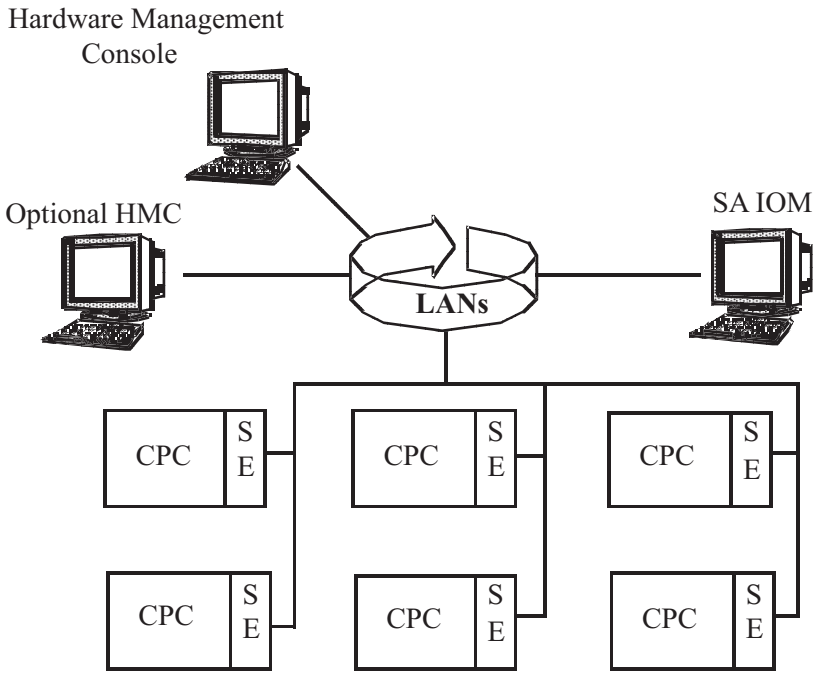
The figure also showsthe SA IOM HMC Interface using TCP/IP to communicate with an HMC.

This allows for a number of possible network configurations in connecting the SA IOM server to the HMC, including

- SLIP (Serial Line Interface Protocol) and a modem
- SLIP and a null modem cable
- Adding a router/bridge on the LAN

- Adding the SA IOM server to the LAN

The following figure illustrates these configurations:



Configuring the SA IOM HMC interface

This section describes how to configure the HMC Interface.

TCP/IP and SNMP must be setup correctly on both the SA IOM server and the HMC PC for the connection to be successful.

The following TCP/IP information is used throughout this section for example purposes.

HMC Console	Example Value	Your Value
IP Address	9.130.1.3	
Community Name	HOSTHMC1	
Subnet Mask	255.255.255.0	

The HMC Console IP address will already be set up. Obtain the IP address of your HMC console.

SA IOM server:	Example Value	Your Value
IP Address	9.130.1.7	
Community Name	SAIOMPC1	
Subnet Mask	255.255.255.0	

SA IOM server configuration

To configure the SA IOM server:

1. The HMC has two DLLs which the SA IOM HMC Interface requires, these are named HWMCAWIN.DLL and HWMCAORX.DLL. These files are distributed with the SA IOM installation media, and should already be in the bin directory where the SA IOM server executable files are installed.

   If these files are not present, copy these two HMC DLLs from the SA IOM installation media to the SA IOM server bin directory.

   Note: Be sure that both HWMCAWIN.DLL and HWMCAORX.DLL are copied again if software upgrades are made to the HMC. Problems can occur if the SA IOM server has different versions of these DLLs than the HMC, as these provide access to the API functions used by SA IOM REXX scripts. The most up to date copies of these files are also available on Resource Link™ at http://www.ibm.com/servers/resourcelink. Click on Services, and then Click API.
2. Perform SA IOM SNMP setup.
   - From the Windows Control Panel, select **Network**.
   - Select the **Services** tab.

     If the SNMP Services tab has not already been added to the SA IOM server, add it at this time. Be sure to fill in the Contact Location entry fields on the first property page.
3. Shutdown and reboot the SA IOM server.

Go to Control Panel/Services, which lists all services started on the PC and verify that the SNMP Service is activated at startup.

Configuring the z9-109 HMC for use with SA IOM

Starting with the z9-109 server, the HMC has been redesigned. It is Linux based. The following configuration changes are necessary to configure the z9® HMC for SA IOM use.

1. Logon to the HMC in Administrator mode and select Console Actions. Right click and navigate to the **Customize API Settings** task.

In the task Window:

2. Select the **Enable SNMP APIs** checkbox.
3. Empty the SNMP agent parameters field. The API will not communicate with the HMC if there is a value in this field.
4. Disregard SNMPv3 Users settings
5. Fill in Community Names you need for SA IOM (same as with the old HMC)
6. Fill in Event Notification information you need for SA IOM (same as with the old HMC)

Click the **Apply** button

7. An SNMP Configuration window will pop up, telling you that the HMC needs to be restarted to activate the changes.
8. Restart the HMC to activate the changes.

HMC console configuration (OS/2 Warp Connect 4.0)

The HMC needs three distinct components to be enabled: the HMC API, TCP/IP and SNMP. The following steps combine the setup procedures for a HWMCA running on OS/2® Warp Connect 4.0.

1. Logon to the HWMCA as user ACSADMIN.

   The local IBM representative (or your HMC specialist) may need to supply the password for this user, as it is a special ID that allows configuration changes.

It is highly unlikely that any existing user logons at your site will have the equivalent authority levels of ACSADMIN.

2. Select the **Console Actions** view.
3. Select the **Hardware Management Console Settings** task.
4. Select the **Network** page to verify the HMC's own IP address.
5. Check the **Enable the Hardware Management Console Application Program Interface** box.
6. Specify the community name to be used by the HMC itself. For example:

   ```
   HOSTHMC1
   ```

7. Under the Event Notification section, select **New** to create an entry for each PC which will communicate with the HMC. Include entries for the HMC and for one or more SA IOM servers. For each entry, check all of the HMC events boxes.
8. Specify any parameters that should be used when the HMC automatically starts the SystemView® Agent for OS/2. At the very least, you must specify the `-transport udp -dpi tcp` parameters.
9. Press the **Apply** button to apply the changes that have been made.

   Note: For any changes to the HMC settings to take effect, you must stop and restart the HWMCA. You can do this either by rebooting the HMC, or by logging off and pressing Cancel on the logon panel. You can then restart the HWMCA by starting the Hardware Management Console Application icon from the desktop.
10. Select the **SNMP Configuration** task.
11. Select the **Communities** tab.

    Enter the community name of each PC which will use SNMP to remotely communicate with the HMC. For example, your entries might be:

    ```
    Protocol        UDP
    Name            SAIOMPC1
    Address         9.130.1.7
    Network Mask    255.255.255.255
    Access Type     read/write
    ```

12. Include an entry for the HMC itself. For example, your entries might be:

    ```
    Protocol        UDP
    Name            HOSTHMC1
    Address         9.130.1.3
    Network Mask    255.255.255.255
    Access Type     read/write
    ```

13. Select the **MIB Variables** tab.

    Enter the description, contact, name, and location of the HMC. These are required fields that should contain meaningful values.
14. To complete the configuration process, close the SNMP configuration notebook and select **OK** to save the changed settings.

    Note: For any changes to the SNMP configuration notebook to take effect, you must stop and restart HWMCA as described in step 9.

Testing and verification

The following steps should be performed to verify that all of the components are in place. Run these steps prior to attempting to run the HMCSTAT.REX and HMCONS.REX programs from SA IOM. If any step fails, correct that item before proceeding to the next step.

Testing at the HMC console (OS/2 Version)

Perform the following tests at the HMC console.

1. In an OS/2 window on the HMC PC, enter the `ping` command followed by the IP address of the SA IOM server, for example:

   ```
   ping 9.130.1.7
   ```

   This should return messages indicating that packets were sent and received successfully. This step verifies the TCP/IP connection to the SA IOM server.

2. Issue a SNMPGRP command similar to the following example:

   ```
   SNMPGRP -h 9.130.1.3 -c HOSTHMC1 sys
   ```

   The `-h` signifies the HMC's hostname and the `-c` its community name. Be sure that the community name is entered in the proper case.

   This should return with the SNMP Contact Name and System Location data that you entered earlier. This step verifies the HMC's local SNMP environment is active and setup correctly.

   Change the prompt to the D: drive and change the directory to TOOLKIT. Run the IBM-provided sample REXX script, HWMCARX.CMD. Enter the IP address of the HMC and the Community Name of the HMC (case sensitive).

   This should display CPC data and list actions that could be taken. This step verifies that the HMC's API is enabled correctly. Exit from this program.

3. If all tests were successful, proceed to testing on the SA IOM server.

Testing at the SA IOM server

Perform the following tests at the SA IOM server.

1. At a command prompt on the SA IOM server, enter the `ping` command followed by the IP address of the HMC PC, for example:

   ```
   PING 9.130.1.3
   ```

   This should return messages indicating that packets were sent and received successfully. This verifies that TCP/IP can communicate with the HMC PC.

2. If all tests were successful, you are ready to run HMCSTAT.REX and HMCONS.REX.

Connecting the SA IOM HMC interface PC to the HMC

The final configuration task is to establish the connection between the PC running the SA IOM HMC Interface and the HMC. Before you begin, you must:

- Be logged onto SA IOM
- Have successfully enabled the HMC SNMP component and configured the HWMCA APIs as described previously
- Make sure the following two SA IOM HMC Interfaces for SA IOM REXX scripts are installed on the SA IOM server:

HMCSTAT.REX	Controls status monitoring and commands. Allows you to monitor the status of CPCs and their associated images, and issue commands to them. This script can be run in the SA IOM environment or outside directly by using the REXX command. It has an example of using AFR_SAY and AFR_CLS while running under SAIOM and using CHAROUT and SysCls when running directly under REXX.
HMCONS.REX	Event console. Lets you view HMC hardware messages, software messages, and status changes.

When you are ready, perform these steps on the SA IOM server running SA IOM HMC Interface to establish a connection with the HMC.

1. In SA IOM, start the REXX exec HMCSTAT.REX.
2. The **SA IOM HMC Interface** prompts you for the host name. After the **Host Name** prompt, type the IP address of the HMC you want to monitor and press Enter.
3. The **SA IOM HMC Interface** prompts you for the community name. After the **Community Name** prompt, type the community name of the SA IOM server defined to the HMC that you want to monitor and press Enter.
4. Start the REXX exec HMCONS.REX.
5. Repeat steps 2 and 3.
6. You are now ready to use the **SA IOM HMC Interface**.

Sample scripts are described in "HMCACT.REX automation interface program" on page 119.

Using the SA IOM HMC interface

This section provides information on using the HMC Interface.

Once you have successfully configured the SA IOM HMC Interface feature, you can gather information about the functioning of the S/390 PTS resources using a basic set of commands provided by the interface. These commands allow you to:

- Navigate between levels of HMC resources (CPC and CPC image)
- Perform actions and obtain status information on an HMC resource
- Execute operating system commands
- Obtain help

Navigation commands

There are two navigation commands, **(U)p** and **(D)own**. They allow you to move between the CPC and CPC image levels.

How to navigate

When you first connect, SA IOM HMC Interface displays status information:

```
Host: abchmc
Date: 20 September 1999
Time: 14:49:42

          ********************************************************
          *              Defined CPC status information          *
          ********************************************************

1) CEC01               Status=Operating              Mode=LPAR
2) CEC02               Status=Operating              Mode=LPAR
3) CEC03               Status=Not Operating        Mode=Coupling Facility


Enter (U)p. E(X)it, or object number followed by (D)own or Command Name.
Enter ? for Help.
```

The information displayed includes a list of the HMC's CPCs, and their status and mode. If a CPC is in LPAR mode, you can examine the status of its images by selecting its number and typing a **D** (for Down a level) on the command line (where the cursor is blinking).

For example, to examine the images of the CPC labeled CEC02 (listed above), enter:

```
2 D
```

You then receive a display of CEC02's images similar to the following:

```
1) CEC02 SPE10  Status=Operating          Mode=LPAR
2) CEC02 SPE11  Status=Operating          Mode=LPAR
3) CEC02 SPE12  Status=Operating          Mode=LPAR
```

To return to the CPC level, type **U** for Up.

Action commands

You can use the SA IOM HMC Interface feature to perform the following actions on HMC resources:

Command	Description
Activate	Activates a CPC or CPC image. Activate may also perform the following functions: • Power on the system hardware • Power-on reset • Activate partitions • Load the operating system When you issue the Activate command, you are prompted for the activation profile that you want to use. If you want to use the current profile, press Enter. If you want to change your IPL activation profile, type the new profile name and press Enter.
Deactivate	Deactivates a CPC or CPC image.
Start	Starts a CPC image.
Stop	Stops a CPC image.
ResetNormal	Performs a system reset on a CPC image.
PSWRestart	Performs a PSW restart on a CPC image.
Send_OpSys, or SO	Sends an operating system command to a CPC image.

Action command syntax

The syntax for issuing an action on an HMC object (CPC or CPC image) is as follows:

```
ObjectNumber action
```

where `ObjectNumber` is the number of the HMC object at the current level (CPC or CPC image) and `action` is the action you want to take on the object.

For example, to deactivate CPC image 2, type the following command:

```
2 deactivate
```

Operating system commands

The SA IOM HMC Interface lets you send operating system commands to HMC resources.

The syntax is:

```
ObjectNumber SO Command
```

where `ObjectNumber` is the number of the CPC or CPC image as listed in the SA IOM HMC Interface table, `SO` indicates an operating system command, and `Command` is the actual text of the command.

For example, to send a JES2 command to CPC image number 3, enter:

```
3 SO $DA
```

Additional commands

Some additional commands you can use are:

?	Displays help for SA IOM HMC Interface commands.
X	Exits SA IOM HMC Interface
U	Refreshes HMC data. **Note:** HMC data is automatically refreshed at CPC level.

Status conditions

The following table describes possible CPC or CPC image status conditions.

Status	Description
Operating	All systems are operational, and normal processing of instructions is taking place.
Not operating	The system is not processing instructions. Although system power is complete, power-on reset is not.
No power	The system has not been powered on.
Exceptions	For this system, one or more, but not all channels are in a Not Operational state.
Status check	A communication failure between this system and one of its constituent systems (for example, between the CPC and the CPC image) has occurred.
Service	The channel path to the CPC is in single channel service mode. Operator action is required to place the channel path in a standby state.
Link not active	The CPC is not currently active.
Power save	A reduced power state, usually caused by a main power failure.
Not activated	The system has been defined by the input/output configuration dataset used to perform a power-on reset of the CPC in LPAR mode, but the system has not been activated. Its operating mode has not been defined.

Modes

The following table describes possible CPC or CPC image modes.

Mode	Description
LPAR	Logical Partition mode. Can have multiple images running under a single CPC.
ESA 390	Native ESA without multiple images.
ESA 390 TPF	ESA running the TPF operating system.

Mode	Description
Coupling Facility	The hardware is a 9674 device.
UNKNOWN	The mode cannot presently be determined.

HMCACT.REX automation interface program

The HMCACT.REX Automation Interface sample program is included with the product media. A description of the program follows.

HMCACT.REX

HMCACT.REX creates an interface between an automation script running under SA IOM and the IBM HMC API interface functions provided by the HWMCAWIN.DLL. Call this function program to perform activities with the Hardware Management Console (HMC).

Format

The format for HMCACT.REX is:

```
rc = HMCACT(hostname communityname CPCname LPARID aname action
[systemcommand])
```

or

```
call HMCACT hostname communityname CPCname LPARID aname action
[systemcommand]
```

where:

hostname The name specified in the SNMP setup on the HMC. It can be an alias (for example, WLKHMC) or a TCP/IP node (for example, 130.1.1.9).

communityname The name assigned to the PC node that will be issuing commands. It is defined in the SNMP setup on the HMC.

CPCname The target image for which the command is intended.

LPARID The target LPAR for which the command is intended.

aname Any one of the following:

- The name of the profile to be used for the IPL
- The POR name
- A space-holding literal during the SYSRESET action

action Any of the following actions that the function is being asked to perform:

- Activate (POR)
- Deactivate (POFF)
- Activate an image (IPL)
- Reset normal (SYSRESET)
- Send operating system command (SO or SEND_OPSYS). Use this action with the **systemcommand** parameter.

systemcommand This optional parameter lets you send a command to the system. If you have selected SO or SEND_OPSYS as your action parameter, enter the command in quotes at the end of the string.

Example

In the following examples, if a parameter is case-sensitive, it is enclosed in quotes. Within the SA IOM HMC Interface, parameters without quotes are changed to uppercase.

The following example performs an IPL from a **down** LPAR, with IPLPROD as a defined profile on the target HMC:

```
rc = HMCACT(9.130.1.1 JMC CPC00 PROD IPLPROD 'IPL')
```

The following example starts SYSRESET from a **down** LPAR:

```
rc = HMCACT(9.130.1.1 JMC CPC00 PROD "*" 'SYSRESET')
```

The following example performs a Power Off from a **down** LPAR:

```
rc = HMCACT(CANPROD JMC CPC00 PROD PORCPC000 'POFF')
```

The following example performs a Power On from a **down** LPAR using the CALL command syntax:

```
call HMCACT CANPROD JMC CPC00 PROD PORCPC000 'POR'
```

The following examples send the operating system command `$DA` to an **up** LPAR. In the first example, the `communityname` 'jmc' is enclosed in quotes because the parameter is case-sensitive:

```
rc = HMCACT(CANPROD 'jmc' CPC00 PROD PORCPC000 'SO' '$DA')
```

or

```
rc = HMCACT(CANPROD JMC CPC00 PROD PORCPC000 'SO' '$DA')
```

Return codes

The return codes for HMCACT.REX are:

0 The program executed successfully

8 The program did not execute successfully.

Chapter 13. Configuring TN3270E sessions

This chapter explains how to configure support for Telnet 3270 Enhanced sessions. For information on implementing IBM 3270 emulation adapters with coaxial cable connections, see Chapter 19, "Installing 3270 Emulation Adapters," on page 205.

Topics in this chapter

The following topics are discussed in this chapter:

- "Configuring TN3270E support in SA IOM"
- "Configuring the TN3270E server" on page 122
- "Copying and pasting in TN3270E sessions" on page 127
- "Consolidating 3270 Sessions using SLF" on page 128

Configuring TN3270E support in SA IOM

Configuring a TN3270E session is a three-step process:

1. Configure the TN3270E server to include sessions for SA IOM.
2. Configure the session definitions in the SA IOM server.
3. Add or update console definitions within MVS to define MVS MCS consoles to match the SA IOM TN3270E sessions.

Each of these steps is explained in subsequent sections.

The following diagram depicts a connection using an IBM 2074 console support controller.

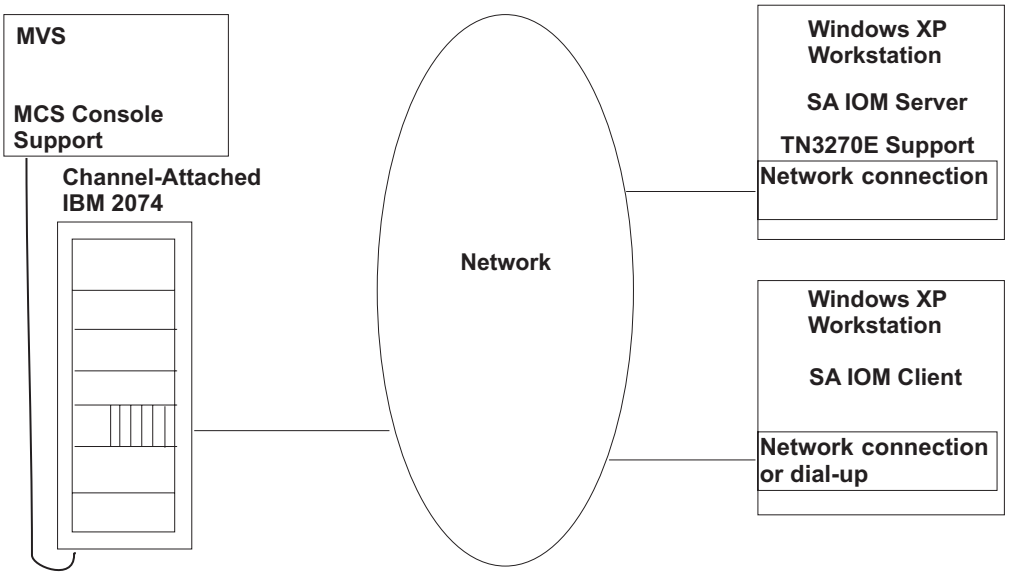


Figure 1. Typical connection using an IBM 2074 console support controller

In this illustration, general purpose network cabling connects the IBM 2074 to the LAN and the SA IOM server connects to the LAN using a general-purpose LAN adapter.

Configuring the TN3270E server

The TN3270E server currently supported by SA IOM is the IBM OSA Integrated Console Controller. The configuration process for this device is described in IBM redbook *OSA-Express Integrated Console Controller Implementation Guide*, document number SG24-6364.

The TN3270E server previously supported was the IBM 2074 Console Support Controller. (The 2074 is now quite old, however examples of connecting to it are retained in this book.) The configuration process for this device is described in IBM manual *2074 Console Support Controller Configuration Guide*, document number SC28-6806.

Configuring SA IOM session definitions

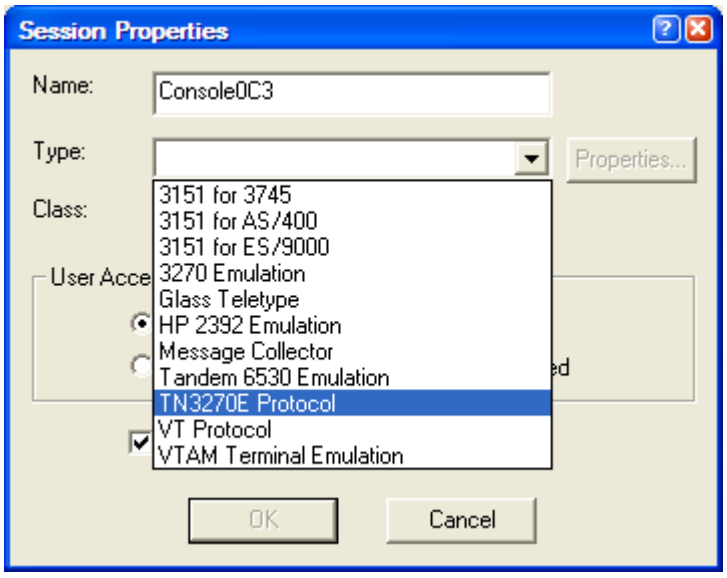
Adding a new session, or changing an existing session, for TN3270E MVS console support is similar to updating any other type of SA IOM session. Before starting, ensure that the configuration information from the TN3270E server, for example IBM OSA Integrated Console Controller, is readily available. Also, verify that any other existing console sessions or other sessions can be stopped and restarted.

Note: Adding the TN3270E session requires stopping and starting the SA IOM server, which is an unacceptable disruption in some production environments.

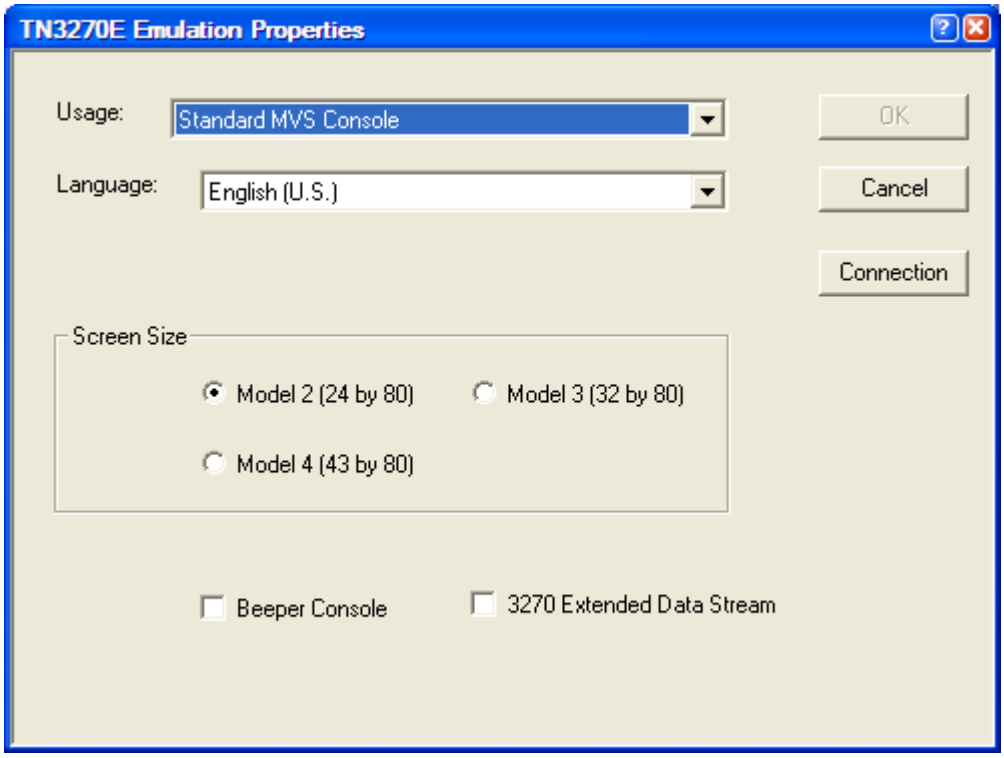
To start the configuration process, follow the steps below:

1. Connect to the server on which you will define a session. From the Config pull-down on the SA IOM Client, select **Server** and then select which server to configure.

   Result: The Server Configuration Properties dialog displays.
2. Select **Host Sessions**. In the Host Sessions list area, right-click and select **Add**. The Session Properties window displays.
3. Complete the following fields:
   - Provide a name for the session.
   - Select **TN3270E Protocol** as the session type. (The **Type** drop-down list contains all the valid session types permitted in SA IOM.)



4. Click **Properties**.
5. On the TN3270E Emulation Properties window,

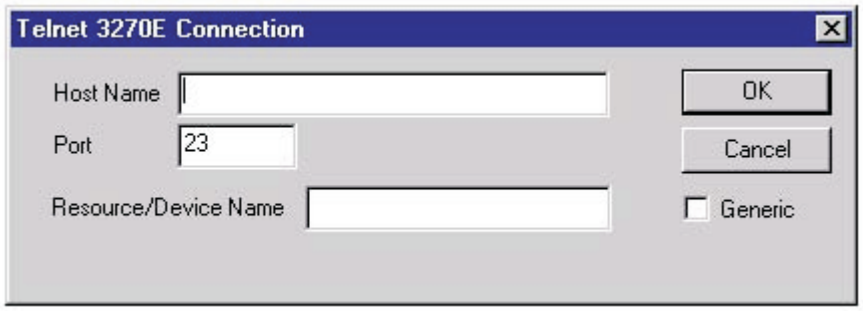


make the following choices:

- **Language** - as desired.
- **Usage** - Select the usage that best represents how you intend to use this console. (The default is usage for TN3270E is Standard MVS console.)
- **Screen Size** - Select the appropriate screen size. The 3278 models 2 (24 lines and 80 columns), 3 (32 lines and 80 columns), and 4 (43 lines and 80 columns) are supported.

- **Beeper Console** - Check this box if this console is used for beeper messages.
- **3270 Extended Data Stream** - This option enables support for extended highlighting and eight colors.

6. Click **Connection**.
7. On the Telnet 3270E Connection window,



add the following information:

Host name - Supply the TCP/IP address of the TN3270E server (for example, OSA Integrated Console Controller). You can supply either the DNS name or the address can be in dotted-decimal form (192.168.1.2).

Port - The TCP/IP port assigned to incoming TN3270E connection requests on the TN3270E server. This usually will take one of the values as shown below:

TN3270E Server	TCP/IP Connection Port Value
OSA Integrated Console Controller	3270
IBM 2074 (channel adapter 0)	3270
IBM 2074 (channel adapter 1)	3271
IBM MVS TCP/IP server	23
Other TN3270E servers	23

Resource/Device Name - The name assigned to the connection in the TN3270E server. (This may also be called the **TN3270E LU Name** in some documentation.) For the IBM 2074 Console Support Controller, this is the value specified in the **/R=** keyword for the session during configuration of the IBM 2074.

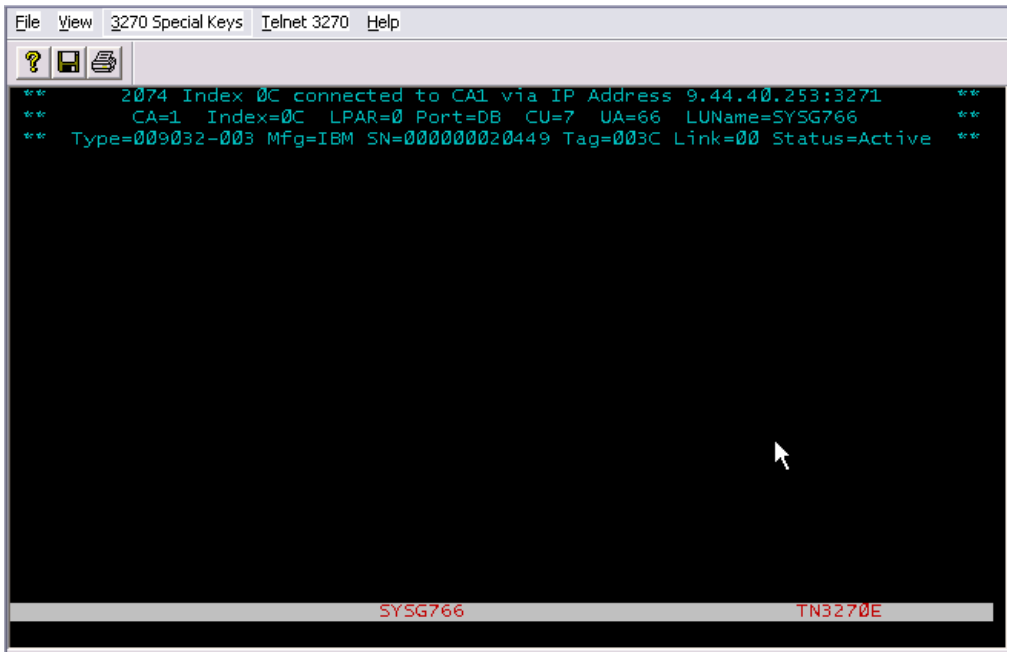
Generic - This indicates whether SA IOM should accept another Resource/Device Name (TN3270E LU Name) from the TN3270E during session setup negotiations. Normally, this should not be chosen for MVS console support since a specific console connection is usually required. It is intended for situations where SA IOM is to connect to a pool of sessions, and any session is acceptable. An example would be connecting to TSO. In this scenario, the Resource/Device Name is usually left blank and the Generic option is chosen.

8. When finished entering the connection data, click **OK**. As the display reverts to the TN3270E Emulation Properties and Session Properties windows, click **OK** in each. The display then reverts to the Server Configuration Properties window.
9. Verify that the name chosen for the new session is correctly shown on the Server Configuration Properties window. Click **OK** if it is, and follow the server restart process as displayed in the windows that subsequently open.

After the server has restarted, the new session should be active if the configuration selections were accurate and the TN3270E server is active. To display the session screen, double-click on the session name in the **Servers and Sessions** pane of the SA IOM Client window.

IBM 2074 connection considerations

For the IBM 2074, initial connection usually results in a display, similar to the following, within your SA IOM emulation session.



This display indicates that the connection to the IBM 2074 Console Support Controller is working, but that the host MVS console is not active. Note that some versions of the 2074 also display the SA IOM TCP/IP address and port number. At this point, the MVS console can be varied online with MVS commands.

The recommended sequence during initial testing of the SA IOM-to-IBM 2074 interface is to use the following commands. (The examples assume an SA IOM session mapped to unit address 00CC by the IBM 2074.)

```
D U,,,00CC,1
```

Display the unit address to be used for the console session. If it is not online, this may indicate a 2074 or MVS configuration or operational problem.

```
V PATH(00CC,nn),ONLINE
```

Vary the channel path online. This step is required by some levels of 2074 support for sessions defined with the 3270 Extended Data Stream. In the above message, `nn` represents the channel path. This can be determined by issuing the `D M=DEV(00CC)` command. (To determine other devices on the channel path, issue the `D M=CHP(nn)` command.)

```
V 00CC,ONLINE
```

Vary the unit address online. This is only necessary when the prior command showed that the unit address was offline. If the Vary command fails, this may indicate a 2074 or MVS configuration or operational problem.

```
V CN(console_name),ONLINE
```

Activate the MVS console. Note that the console_name is defined by the host MVS systems programmer, and may have no relationship to the unit address configured by the 2074.

If all the commands execute successfully, the SA IOM Client window should now be able to issue console commands, depending upon its definition in the MVS host.

In a production environment, normally only the last command (`V CN(console_name), ONLINE`) should be necessary to start or restart a console session. However, the longer **V PATH** sequence is recommended for diagnostic purposes.

Configuring MVS MCS console definitions with the IBM 2074 Console Support Controller

The SA IOM session's console definition may be configured using any typical options. The actual definition must be placed in a CONSOLxx member in the MVS SYS1.PARMLIB data set. When coding the SYS1.PARMLIB console entry, the following restrictions should be observed:

- The SA IOM TN3270E facility supports IBM 3278 model 2, 3, or 4 screen sizes. Coding 3270-X is also acceptable. Coding a different unit type within SYS1.PARMLIB will lead to initialization errors or other unpredictable results.
- If the SA IOM TN3270E session does not specify the 3270 Extended data stream option, commands such as Read Partition Query will fail. Coding the value 3270-X for the CONSOLE's UNIT parameter will generate errors during initialization, such as message IEE936I CONSOLE INITIALIZATION ERROR, and the session will be limited to four-color support.

A coded sample of the SYS1.PARMLIB CONSOLxx member data for an SA IOM MVS console session is shown in the figure below.

```
/*--------------------------------------------------------------------*/
/*                CONSOLE                                             */
/*--------------------------------------------------------------------*/
CONSOLE DEVNUM(0C3)
        UNIT(3278-2)
        NAME(CMD0C3)
        ALTERNATE(0C0)
        AUTH(SYS,IO,CONS)
        ROUTCODE(3,5,15)
        CON(N) SEG(19) DEL(R) RNUM(19) RTME(1) MFORM(J,T) AREA(NONE)
        MONITOR(JOBNAMES-T)
        MSCOPE(*)
        CMDSYS(*)
```

MVS TCP/IP configuration issues

SA IOM will connect and operate properly with standard IBM MVS TCP/IP configurations. However, it is possible to configure the MVS TCP/IP Telnet options in such a way as to prevent SA IOM from connecting successfully. This involves a conflict with an older protocol at some installations.

The older version of TN3270E is TN3270. TN3270 is adequate for some users, as using it eliminates the need for upgrades to the 3270 client emulator programs.

However, many older 3270 emulator programs do not negotiate service correctly with the MVS TCP/IP TN3270E server, and may fail to connect. To avoid this problem, some installations may specify the NOTN3270E option in their MVS TCP/IP TELNETPARMS to disable the TN3270E function at the server. If this option is selected, SA IOM cannot successfully connect to MVS TCP/IP.

Copying and pasting in TN3270E sessions

You can copy and paste within a TN3270E emulation session using the mouse to highlight an area then using Ctrl-C and Ctrl-V (in the usual Windows manner). A double-click sets the session cursor.

You may notice that the copy and paste behavior of this product within a TN3270E emulation session differs from the behavior you may be used to when using IBM Personal Communications Session Manager for terminal emulation. However, be aware that SA IOM copy and paste within a TN3270E emulation session is working as designed. To elaborate, be aware of the following differences in behavior.

Notes:

1. SA IOM pastes copied text, from the copied buffer, to the input areas on the emulation session screen as if the text is being typed in. Text is allowed to skip to the next input field if the pasted area happens to be larger than the input area. This behavior permits line commands to be issued. For example, if you are pasting text into an ISPF edit session and the line numbers are showing, SA IOM recognizes two active input areas in the ISPF session. One is on the left side of the screen–the line number area (ISPF users may enter line commands here). The second is on the right side of the screen–the text line area. SA IOM treats both these areas as input areas and anything pasted into the text line area may flow into the line number area if it is long enough. This behavior is different from Personal Communications Session Manager which pastes text in a rectangular area that helps avoid pasting text into the line number area if a start point for the paste action is suitably selected.
2. If you copy several lines of text, SA IOM also copies the CRLF character, at the end of each line, to the destination. Personal Communications Session Manager possibly removes CRLF characters. The difference becomes evident if you attempt to paste more than one line at the TSO ready prompt. After the first line is pasted for SA IOM TN3270E emulation, TSO responds with 'INVALID COMMAND NAME SYNTAX' and the rest of the lines are discarded. While if you perform the same operation using Personal Communications Session Manager, multiple lines are pasted and, if you then press Enter, the command is sent for execution.
3. To paste a single long line of text into an ISPF edit session using SA IOM TN3270E emulation, first type 'TE' in the line number area to put the ISPF session into Text Entry mode. The text will be wrapped and will appear as several lines in the edited dataset or member. However if the source for paste consists of several lines of text terminated by CRLFs, only the first line is pasted. ISPF Text Entry mode ends when the first CRLF character is encountered.

Consolidating 3270 Sessions using SLF

Use the Subsystem Logging Facility (SLF) feature of AF/OPERATOR to consolidate multiple consoles (mainframe images) to one SA IOM session. The feature supports color coded filtering and command input to and from a large number of mainframe sessions. All involved host sessions and filters must be defined to AF/OPERATOR's Subsystem Logging Facility. Currently OMEGAVIEW® is required for display purposes. The only setup required on the SA IOM side is to configure a TN3270E session to the particular OMEGAVIEW session that is used for display.

Tip: When you configure the SA IOM TN3270E emulation session that displays the Subsystem Logging Facility log, select a Usage of **TSO terminal**.

To configure the Subsystem Logging Facility feature, you will need the following information. The following versions of mainframe software are supported.

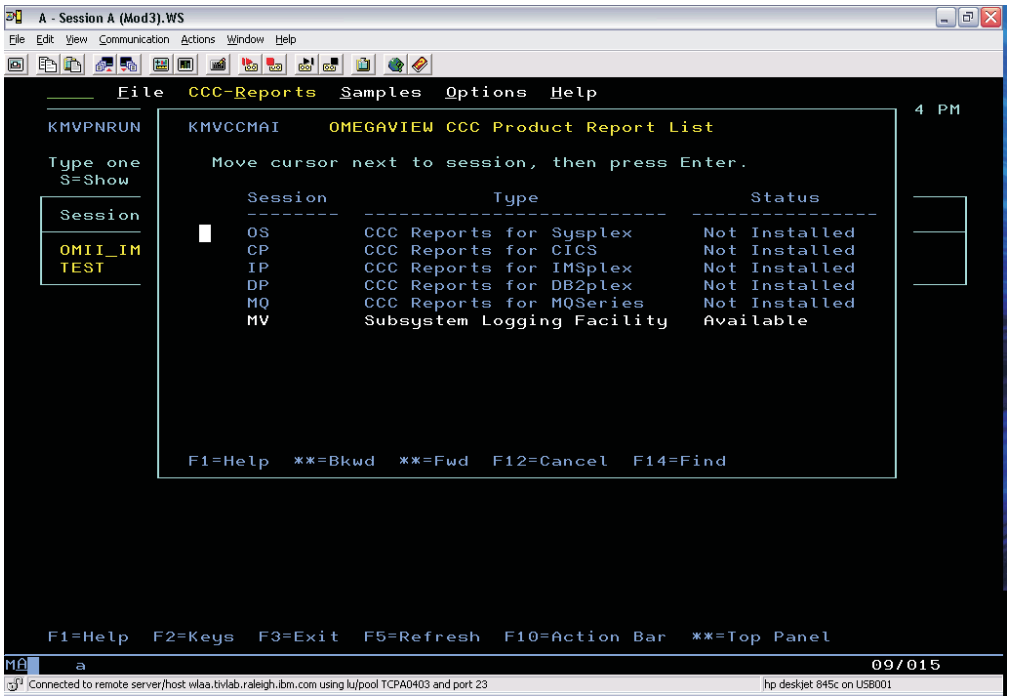
- AF/OPERATOR V320 or V340 or OMEGACENTER® GATEWAY V320 or V340
- OMEGAVIEW V300

Refer to one of the following manuals within the AF family of products for how to setup and use the Subsystem Logging Facility (SLF) with AF/OPERATOR or OMEGACENTER GATEWAY.

- *AF/OPERATOR: Using the Subsystem Logging Facility V340*, document number GC32-9143
- *OMEGACENTER GATEWAY: Using the Subsystem Logging Facility V340*, document number GC32-9232

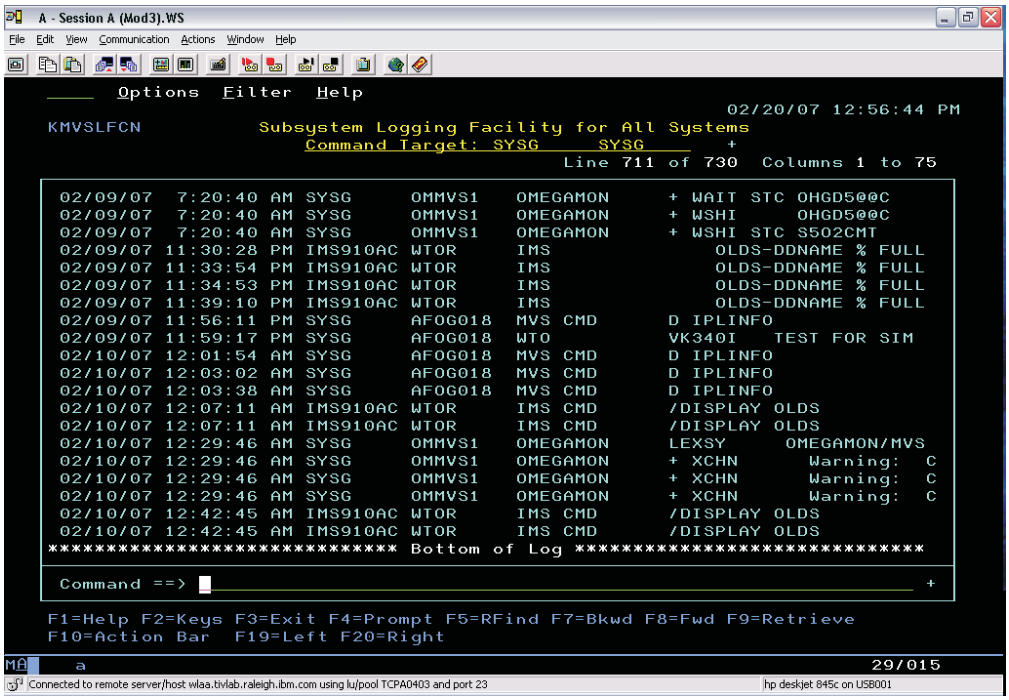
Access the Subsystem Logging Facility log from an OMEGAVIEW console, as follows.

1. From the OMEGAVIEW main panel Action Bar, select **CCC-Reports**. The OMEGAVIEW CCC Product Report List displays (as shown in the following illustration).



If CCC-Reports does not appear on your OMEGAVIEW main panel Action Bar at logon, that means the selection has not yet been authorized. To authorize the CCC-Reports selection, refer to the Assigning User Authorities chapter, Set CCC Report Authorities section within the manual *OMEGAVIEW Configuration and Customization V300*, document number GC32-9334.

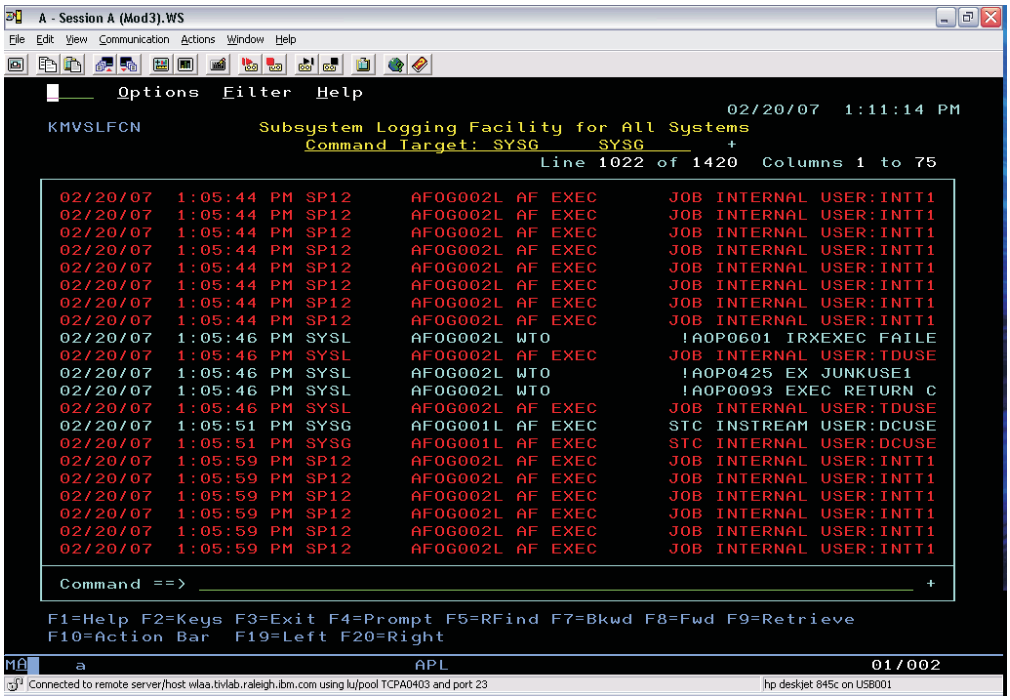
2. From the OMEGAVIEW CCC Product Report List, select the `MV` session of Type `Subsystem Logging Facility`. The Subsystem Logging Facility log displays. The log shown in the following illustration displays messages directed to it from a single system only.



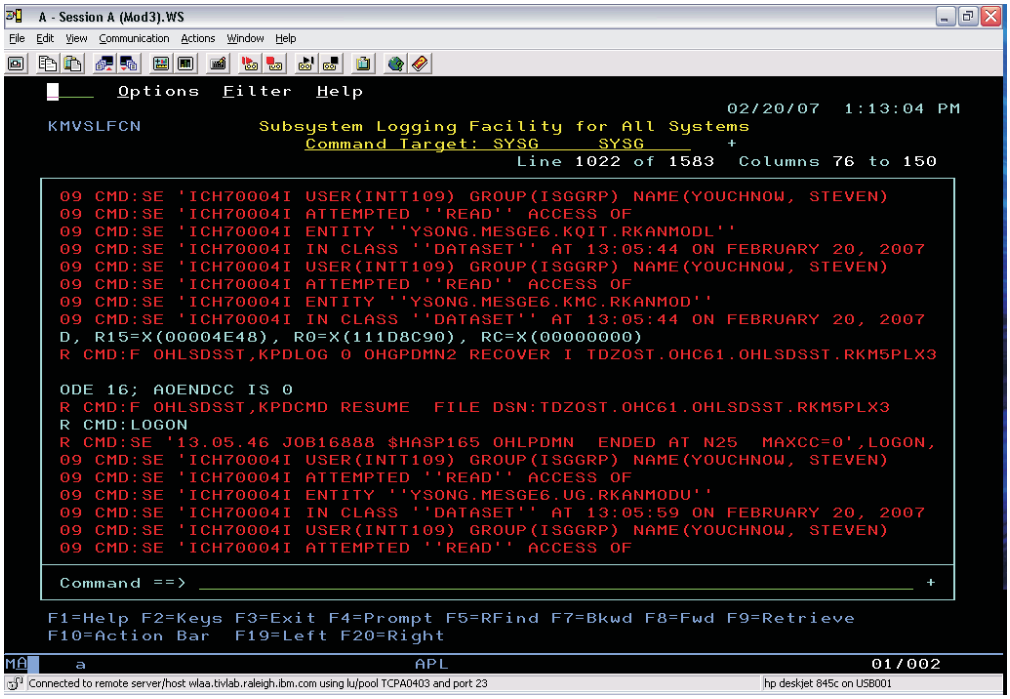
The Subsystem Logging Facility log can be used to consolidate and display selected messages from one or more systems. The messages are directed to the log from either AF/OPERATOR or OMEGACENTER GATEWAY. Sessions from multiple AF/OPERATOR systems or from multiple OMEGACENTER GATEWAY systems can feed data to one SLF log. The Subsystem Logging Facility manual referenced above contains the information necessary for you to choose and direct messages to this log.

Varying types of data can be included in the Subsystem Logging Facility log such as, OMEGAMON exception data, IMS messages and operator commands, and MVS messages and operator commands. Further, the data can be color coded, highlighted, reverse video or a number of other attributes.

The log shown in the following illustration contains RACF® and automation error messages from multiple systems.



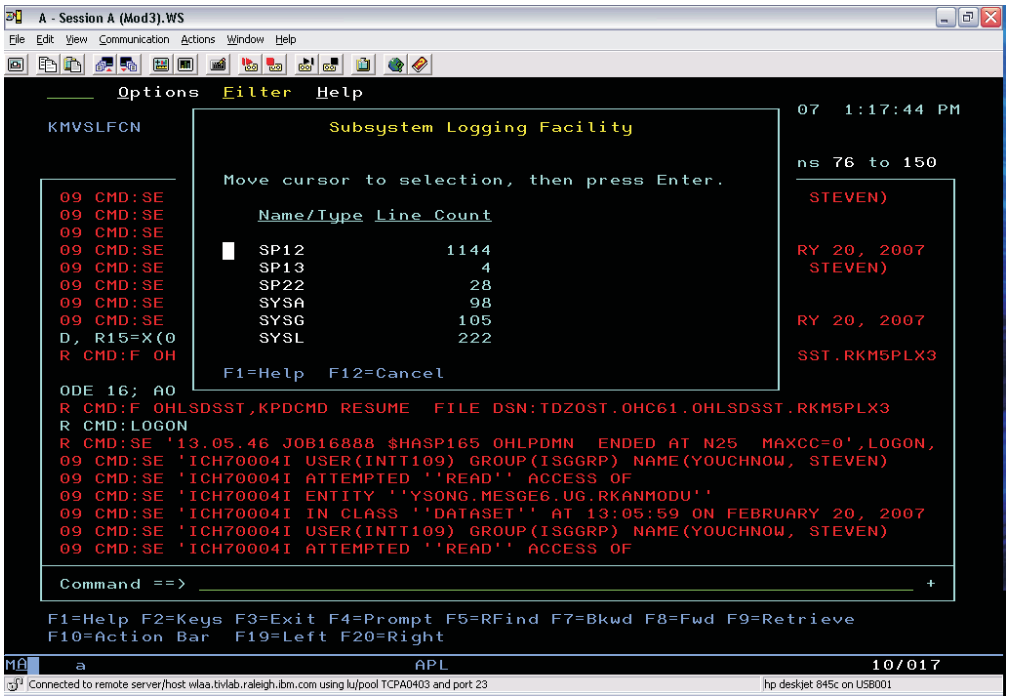
Paging to the right on the console reveals the text of the messages.



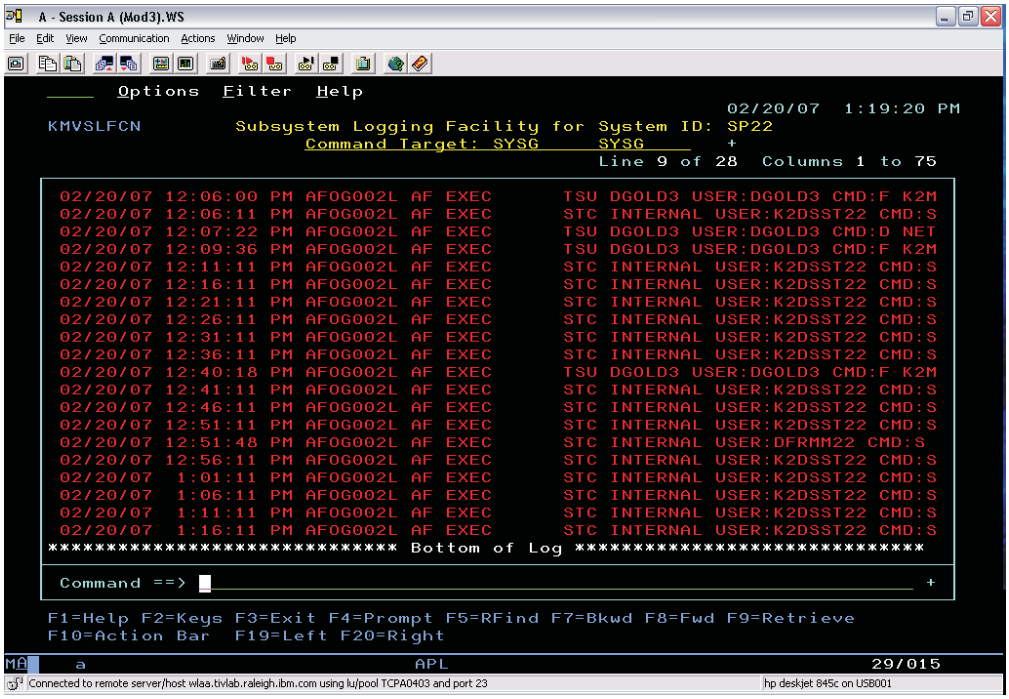
Options controls are available to tailor the display of the log, including the ability to display the timestamp in 12 hour or 24 hour format.

Filter controls are available to remove unwanted data from the display, leaving only that data of interest. Data can be filtered by origin, by jobname, or by system ID within the log.

For example, to filter by system ID, choose option 3 from the Filter menu then select your desired system ID from the subsequent panel (shown below).



The following illustration shows the filtered data that you would see if you selected system ID SP22 on the previous panel.



Chapter 14. SA IOM problem determination

This chapter provides SA IOM resources for problem determination.

Topics in this chapter

The following topics are discussed in this chapter:

- "Begin by checking available logs"
- "Modem connection problems and documentation needed by IBM" on page 136
- "Acquiring STATE-level logs" on page 135
- "Direct serial client/server connection problems" on page 137
- "3270 Coax PCI connection problems" on page 138

Begin by checking available logs

When working with SA IOM things may not always go as expected. A number of things can go wrong, from configuration errors, program and installation errors, to hardware errors. This chapter is intended as a guidance on how to go about debugging these kinds of situations.

The first question in most debugging situation is ″what are the symptoms?″ The answer to this can be anything from unexpected behavior to direct error messages. In almost all cases it is worthwhile to check the logs which often will give detailed information about an error, however most of the logs are level set so it may be necessary to repeat the situation with a more detailed log level.

Most of the logs are associated with an executable file and, in many cases, it is obvious which module is having problems. If this is the case, it is a good idea to scan all logs for unusual messages. The following is a list of most of the modules and logs that are installed with the product.

Table 10. SA IOM 2.1 is installed with the following set of executable files and their associated logs

Module name	Type	Description	Default log name & location
RpServer.exe	GUI	SA IOM's main module, it maintains connections to the hosts and clients and runs the REXX scripts. RpServer.log is a natural first place to look for errors.	logs\rpserver.log
RpClient.exe	GUI	Client module used to connect to RpServer.	logs\rpclient.log
RpSvrSvc.exe	background	Windows service module, used as a 'service wrapper' when RpServer is installed as a service.	rpsvc.log located in the windows service directory, often Windows\System32
RpSvcMgr.exe	GUI	The ″manager″ module for RpSvrSvc / RpServer when installed as a service.	logs\rpsvcmgr.log

Format of log files

The four main logs all have the same format with the message type as a one letter character in column 23 following the timestamp. For example:

```
06/03/07 18:06:29:796 E 496 [ CEmulTelnet3270::CommonTelnetOperation ] Failed to connect to Telnet host: local
```

The important code in this case is 'E' which stands for error. Not all error messages are signs of severe errors but they should always be examined. An easy way to do this is to use the RpLogRd utility and filter on errors.

Configuration errors

Many errors are disguised configuration errors, either as a result of an incorrect entry or due to a host or hardware change. If it isn't obvious what the error is, it is often a good idea to isolate the error by disabling parts of the configuration and retesting. It is easy to take a backup of a configuration files, the following table lists the ones in use.

Table 11. SA IOM configuration files

Configuration file name	Type	Description	Location
rpserver.dat	binary	RpServer host and connection data	config\rpserver.dat
rpsvrprf.txt	text	RpServer host and connection data	config\rpsvrprf.txt
rpclient.dat	binary	RpClient option and connection data	config\rpclient.dat
rpclirprf.txt	text	RpClient option and connection data	config\rpcliprf.txt
rpuser.dat	binary	RServer user data	config\rpuser.dat

Network errors

Some of the most common errors are caused by problems with the connecting network. Naturally this is not an issue for SA IOM only, but for installations that have a dedicated PC for RpServer this may be the first place such errors are encountered. It is a good rule to ensure availability of the external resources before digging too deep into any SA IOM debugging.

Hardware errors

Naturally hardware errors come in many shapes and forms. Many times the operating system will have detected the error before SA IOM, so in addition to the logs mentioned above it makes sense to check the system event logs.

Also, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected properly.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.

Acquiring STATE-level logs

The IBM Support representative for SA IOM often requests that you provide a detailed server or client log, or both, that captures an error that you have observed. You can dynamically change the level of a client log by editing the client configuration file and then saving it. The new log level takes effect immediately and does not require the client to be restarted.

You can also dynamically change the logging level of an SA IOM server without having to restart the server. The log level remains in effect until it is changed again or until the server is restarted. At this time the logging level reverts back to the permanent value stored in the server configuration.

To dynamically change the server log level, connect to a server and invoke that server's context pop-up menu. The modified pop-up menu contains the following options:

- Connect
- Disconnect
- Change Log Level

If you select "Change Log Level", you see a dialog entitled Server Log Level. It lists the currently active logging level, such as Error, Trace, State, etc., and allows you to select another value. Selecting OK activates the selected value.

If the SA IOM server crashes during startup, setting the RpServer log trace level to STATE to support problem diagnosis can be difficult. If the server crashes during startup, an SA IOM client cannot be connected to edit the server configuration or to temporarily set the log trace level to STATE. You may or may not be able to successfully edit the configuration using an SA IOM server at the same build level but on a different machine.

When no other options are available, override the configured SA IOM server trace level using the SERVER_LOG_TRACE_LEVEL keyword parameter with one of the following values:

CONFIG (Default. Use the configured value.)
PRIORITY
ERROR
WARNING
INFORMATION
TRACE
STATE

Set this keyword in the SA IOM server profile file, `rpsvrprf.txt`, in the SA IOM `\config` directory, for example:

```
SERVER_LOG_TRACE_LEVEL = STATE
```

You can also override the following SA IOM server parameter values:

Log Recycle Interval

Specify a value from 1 to 365 days. The default is 7 days. For example:

```
SERVER_LOG_RECYCLE_INTERVAL  =  7
```

Maximum Log Size

Specify a value in MB, from 1 to 25,000, depending on the build level. The default is 50 MB. For example:

```
SERVER_MAXIMUM_LOG_SIZE      =  50
```

To activate these overrides, you must stop and restart the SA IOM server. The new values are not stored in the SA IOM server configuration.

Modem connection problems and documentation needed by IBM

SA IOM does not use journaling to solve client/server modem connection problems. Instead, use the client log, server log, and Windows-generated modem logs.

To resolve SA IOM client/server modem connection issues, a Windows modem log and STATE-level logs from both the SA IOM server and client are needed. The client and server log levels are activated under the General tab during configuration of the client and server. The modem log can be requested by launching the Windows Control Panel and selecting the "Modems" icon. From here select the modem to log and press the **Properties** button. Select the **Connection** tab on the **Properties Window** and press the **Advanced** button. There is a checkbox for **Record a log file** on the bottom of the Advanced Connection Settings Window. Make sure it is checked. Click OK or Close to return to the Control Panel and close it.

The Windows-generated modem log files are named in the form MODEMLOG*.TXT.

Also send the MODEMDET.TXT file from both the server and client. These files contain the AT® commands issued by the Windows environment to setup or configure the modem and the responses received from the modem during configuration.

The generic unnamed modem settings for the Windows operating system cannot be used because they are not specific enough to allow the level of communication required by SA IOM. If a previously installed modem is shown on the Modem properties page in the control panel as standard modem, then it is recommended that the modem entry be removed, and the modem reinstalled. If after reinstalling, allowing the Operating System to search for the modem, the modem selected by the Operating System is Standard Modem, at that point, you have the option of changing the modem selected. Windows provides a very extensive list modems supported by make or manufacturer and model.

If you cannot find your exact model on the list, use a model with a somewhat slower speed. For example, if your modem is a US Robotics 56K, you may be able to use the settings for a US Robotics 33.8K fax modem just as well.

If the modem manufacturer is not in the list, the modem should come with a driver diskette or CD-ROM to identify the operating characteristics of the modem to the Windows operating system. Without that driver information, the operating system cannot configure the modem properly and since SA IOM uses the Operating System to communicate with the modem, SA IOM is unable to use the modem to communicate.

If the modem was pre-installed and appears to be configured with the correct make and model, but will not perform a client/server connection, uninstall the modem, reinstall it, ensuring that you end up configured for the proper make and model. Then restart the operating system before testing.

Direct serial client/server connection problems

If you have had difficulty connecting serial ports in a Direct Connect client/server connection through certain types of data multiplexers, it may be because these multiplexers use the Data Set Ready (DSR) control line to indicate multiplexer power on, rather than a signal that the remote device (the SA IOM client) wants to establish a connection.

Direct serial connection between a client and its intended server is governed by the state (level) of the Data Set Ready (DSR) lead at the computer. This is on pin 8 of a 25 pin connector. The server needs to see this signal transition from un-asserted (OFF) to asserted (ON) to start the connection process, or transition from asserted to un-asserted to start the disconnection process.

Some communication multiplexer vendors have decided to use the DSR line to indicate some other condition such as multiplexer powered ON. Therefore the line never changes state and the connect/disconnect processes are not started.

The DIRECT_CONNECT_CONTROL profile entry lets you change the control line to be monitored to establish a direct connect client/server connection. Use this feature in cases where a communications port is being used for client/server connection via a multiplexer or other dedicated line and IT IS NOT CONNECTING. If your connection is working, then you DO NOT need to modify its operation with this feature.

The following is an example for the discussion that follows:

DIRECT_CONNECT_CONTROL = DCD 1,2,4-6

The value assigned consists of two fields separated by one or more contiguous spaces. The first, which is DCD in the example above, indicates the control line to be monitored. Allowed values are:

DSR Data set ready, the default

DCD Data carrier detected

RLSD Receive line signal detected, a synonym for DCD

CTS Clear to send

These are not case sensitive.

The second field is a list that consists of port numbers (separated by commas), or ranges of ports (consisting of a starting port number followed by a hyphen followed by the ending port number), or a combination of these formats.

In the example provided above the DCD (RLSD) line is monitored on ports 1, 2, 4, 5, and 6.

Note: These settings are used only on those ports configured for direct connect client connections on the server.

If other ports need to be configured for direct connect client/server connection monitoring for another control signal, then another statement may be entered. It is not recommended that more than one line on a port be monitored.

3270 Coax PCI connection problems

The following possible problems related to a 3270 coax PCI connection have suggested fixes:

- You have an incorrect or non-supported cards (card identification)

  Presently, the only 3270 PCI card supported by SA IOM is the Attachmate 3270 PCI Rev B card. Attachmate had an earlier Rev A card which SA IOM has not ever supported. The easiest way to determine the revision level of a card is by physical inspection. The Rev A card is definitely rectangular in shape, the Rev B card is very nearly square in shape. Looking at the component side of the Rev B card the largest IC has “Plix Technologies” printed on it.

- You have the correct card, installed with the Attachmate device driver

  3270 PCI card installation on PCs running versions of the Windows Operating System that are `plug and play’ sensitive. That is, each time the machine is powered on, the bios produces a list of plug and play devices detected which is examined by the operating system. If a new device is encountered and there is not a device driver available then the operating system asks you to provide a device driver. Attachmate provides a device driver, that satisfies the operating system, but that driver supports only Attachmate emulation products. IBM provides its own device driver, a file name RP3270.sys, which is installed during the installation of the server portion of SA IOM. If the Attachment device driver is installed, the IBM device will fail initialization.

  The solution is to uninstall the Attachmate device driver, and when the operating system again asks for a device driver, point to IBM’s provided control file SAIOM3270.inf.

  Once the device driver is installed and RpServer has been restarted, you can complete the configuration of the cards.

  During the startup of the RpServer, a scan is made for all Attachmate 3270 cards, including those that may be installed in a PCI expansion chassis. The order in which the cards are found in the physical machine is determined by the bios program used by that particular machine’s vendor. Therefore, the card in position 7 may be the first card found and the card in position 2 may be the second found.

  The configuration dialogue for the Attachmate IRMA 3270 PCI Adapter Properties has a list of selectable cards. For example, if there are three cards then the list has entries for 1, 2, and 3. There is NO relationship between this number and its physical position within the PC or expansion chassis.

  Also, if additional Attachmate 3270 PCI cards are installed later, the association between a slot on the properties page and the physical card may change for one or more of the cards previous configured.

Chapter 15. Utility programs

SA IOM includes utility programs to aid you in performing the tasks summarized below.

Table 12. SA IOM 2.1 utility programs, summarized

Module name	Type	Description	Default location
RpLogRd.exe	GUI	Log viewer with filter options.	SA IOM\utils
RpRunRex.exe	cmd line	REXX scripts launcher.	SA IOM\utils
RpSend.exe	cmd line	Message submitter to Message Collector sessions.	SA IOM\utils
RpSesClr.exe	cmd line	Clear SA IOM Client session information.	SA IOM\utils

Each program is described in greater detail in the following section.

RpLogRd.exe

Purpose

The RpLogRd.exe utility program is a self-contained Windows application to aid you in examining SA IOM log files. It includes filtering and searching capabilities.

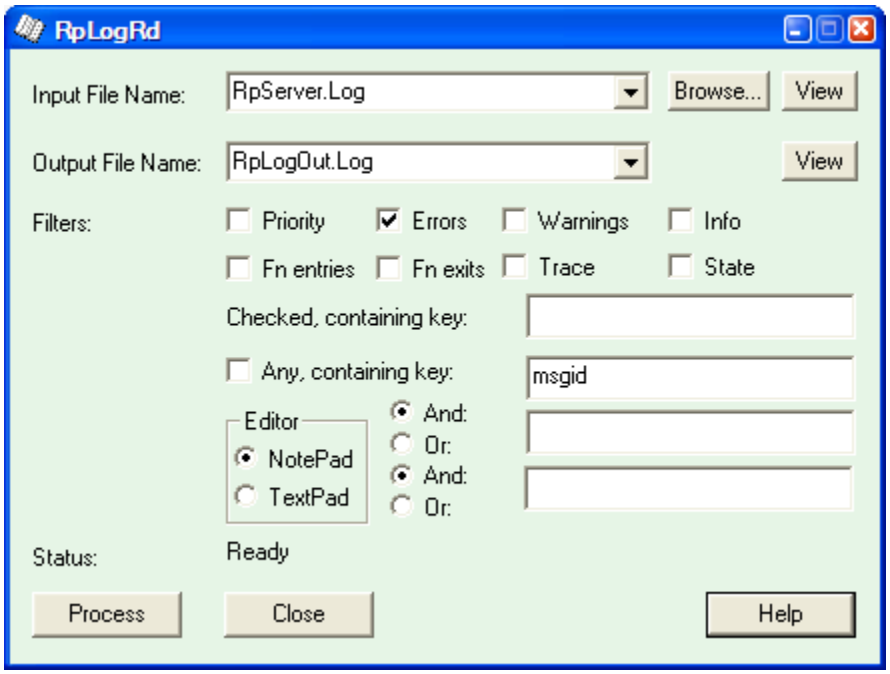
Context

No setup is required to make this utility operational. This program is located in the SA IOM\utils directory.

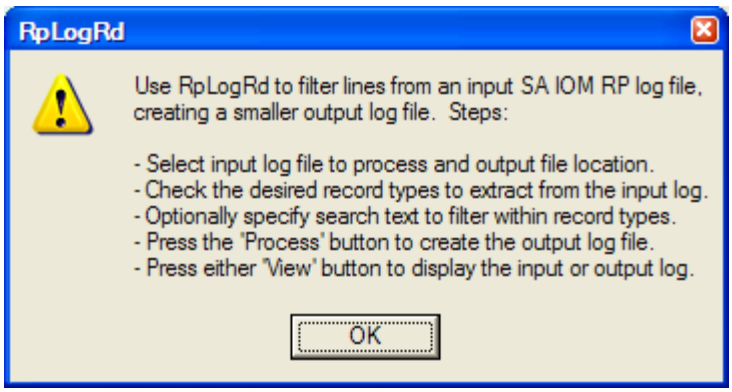
Usage

This Log Reader is a specialized debugging tool that is intended for filtering this product's trace logs, which can be very detailed. The Log Reader is designed for reading the following SA IOM log files: rpserver.log, rpclient.log, rpsvc.log, and rpsvcmgr.log. The default location of these log files is in the SA IOM\logs directory.

To start the program, from a command prompt in the SA IOM\utils directory, enter "RpLogRd" (or you can start this program using Windows Explorer). Here is a snapshot of the SA IOM Log Reader control window which illustrates its default contents and settings.



The SA IOM Log Reader program uses standard Windows controls in the usual manner. For example, click Close to end the Log Reader session. Click Help to display additional information. Basic instructions for use are there, as shown in the following illustration.



Examples

For example in SA IOM\logs\rpserver log, you can find all of the logged data from the AFR_LOG() API call by searching for the string AfrLog.

Note: The contents of the log file used for input depends on the Log Level or Trace Level setting that was used to create it. The Log Level or Trace Level defines the volume and degree of detail for messages written to the log. Levels from the least detailed to the most detailed, are: Priority, Error, Warning, Information, Trace, and State. These settings are cumulative–each level includes the previous level's messages. For example, an RpServer.log created at level Warning includes Priority, Error, and Warning messages. Log level State is equivalent to including all messages. Function entry and exit details can be captured at State level.

RpRunRex.exe

Purpose

The RpRunRex.exe utility program is a command line utility for starting an SA IOM REXX script on a specified SA IOM server that is TCP/IP connected. This program is located in the SA IOM\utils directory.

Context

The SA IOM server on which the REXX script runs must be configured to accept incoming peer messages from the PC on which this utility runs (and must be TCP/IP connected). For information on configuring to accept incoming peer messages see Setting up peer connections This program is located in the SA IOM\utils directory.

Usage

From a command prompt in the SA IOM\utils directory, enter "RpRunRex -?" to display program usage information.

```
RpRunRex version 5
purpose: Start specified REXX script inside SA IOM
usage:------------------------------------------------------------
RpRunRex [-?] [-debug] [-silent] [-loglevel=n] [-wait=n]
         host[:port] scriptname [parm-1] [parm-n]

        -? = This help text
    -debug = Display trace/debug information
   -silent = Only error messages will appear on the screen
 -loglevel : 0=none (default), 1=normal, 2=all. File = RpServer.log
      -wait: Seconds to wait for a response. The default is 0
             RpServer will repond when the script completes.
      host = PC with RpServer running
             Note: SA IOM must have peer enabled for this ip address
     :port = Specify if different from 1040
scriptname = Name of REXX script on the RpServer PC to be started
     parms = Optional parameters to the REXX script
------------------------------------------------------------------
For example: RpRunRex localhost MyScript.rex SYS1 "Device open error" ATTN

Licensed Materials - Property of IBM. Restricted Materials of IBM - 5724-L47.
(c) Copyright IBM Corp. 2001, 2007  All Rights Reserved
US Government Users Restricted Rights
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
```

Examples

For example, you have defined a new notification policy, MyEscalationID. This policy resides in your alert escalation database and you would like to test it. You have TCP/IP connectivity to the SA IOM server that has been configured for Alert Escalation. The SA IOM server has the sample program Escalation.rex installed in its scripts directory. The PC from which you run RpRunRex has been authorized to connect to the SA IOM server using a TCP/IP peer connection. Assume that the SA IOM server is using the default port number for incoming peer connections. All you need to know is: the host name (or IP address) of the SA IOM Server.

To test the new notification policy named MyEscalationID, on the SA IOM server with host name MYSERVER1, proceed as follows.

1. Open a command prompt on your PC and change to a directory that contains the rprunrex.exe utility program.
2. Issue the following command: "RpRunRex MYSERVER1 Escalation.rex MyEscalationID".
3. The SA IOM server uses the Escalation.rex script to start the MyEscalationID alert escalation policy.

RpSend.exe

Purpose

The RpSend.exe utility program is a command line utility for sending a message to the Message Collector.

Context

The SA IOM server to which you send the message must be configured to have a Message Collector session. For information on configuring the Message Collector see “Defining a Message Collector session” on page 57. This program is located in the SA IOM\utils directory.

Usage

From a command prompt in the SA IOM\utils directory, enter "RpSend -?" to display program usage information.

```
C:\Program Files\AFRemote\bin>rpsend -?
RpSend version 4
purpose: Send a text message to SA IOM's Message Collector
usage:---------------------------------------------------------------------
RpSend [-?] [-debug] [-silent] [-loglevel=n]
         host[:port] message

        -? = This help text
    -debug = Display trace/debug information
   -silent = Only error messages will appear on the screen
 -loglevel : 0=none (default), 1=normal, 2=all. File = RpSend.log
      host = PC with RpServer running
             Note: SA IOM must have a Message Collector session defined
     :port = Specify if different from 1090
   message = Text to send. Can contain Ansi escape sequences.
             - double quotes " must be specied as \"
             - to enter Esc from the command line use Ctrl[ or Alt27
             - See the SA IOM REXX manual for a list of Ansi sequences
         ~ = Will be replaced with Esc (hex 1B) in the message
---------------------------------------------------------------------------
Examples:
   RpSend localhost This is a test
   RpSend server1:12023 Look for \"SYS2 2031\"
   RpSend host  ~[2J~[HThis text will be the first line a blank screen
   RpSend host  "~[7mReverse video text"
   RpSend host  "~[0mReset all attributes"
   RpSend host -silent ~[33;44mYellow text on blue background

Licensed Materials - Property of IBM. Restricted Materials of IBM - 5724-L47.
(c) Copyright IBM Corp. 2001, 2007  All Rights Reserved
US Government Users Restricted Rights
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
```

Examples

For example, you would like to send a test message to an SA IOM server that has a Message Collector session running on it. You have TCP/IP connectivity to that SA IOM server. Assume that the Message Collector session is using the default port number. All you need to know is: the host name (or IP address) of the SA IOM Server.

To send a message to the SA IOM server with host name MYSERVER1, proceed as follows.

1. Open a command prompt on your PC and change to a directory that contains the rpsend.exe utility program.
2. Issue the following command: "RpSend MYSERVER1 This is a test message sent using rpsend".
3. The text "This is a test message sent using rpsend" displays in the Message Collector session window.

RpSesClr.exe

Purpose

The RpSesClr.exe utility program is a command line utility for clearing the positioning information about the SA IOM Client session windows from the Windows registry. (That is, the saved information about the size and placement of the emulation session windows, and if the Status and Tool bars are displayed.) Under normal circumstances, this utility program is not needed.

Context

No setup is required to make this utility operational. This program is located in the SA IOM\utils directory.

Usage

Use this program if you want to intentionally erase all the saved window position information about your SA IOM Client session windows. This program has no effect on the configuration settings for your SA IOM Client sessions.

From a command prompt in the SA IOM\utils directory, enter "RpSesClr -?" to display program usage information.

```
RpSesClr version 2
purpose: Lists the registry contents stored by RpClient on exit.
    These entries define the size and positioning of the displayed
    emulation sessions.  Appends the same information to a log file.
    By default the log file name is RpSesClr.log and the registry
    entries are deleted.
usage:-----------------------------------------------------------------
RpSesClr [-?] [-f<LogFileName>] [-t] [-c]
    -? = Or -h, produces this output and exits immediately.
    -f = Allows specification of log file with a different name.
    -t = Allows specifications of new, empty log.
    -c = Disables clearing of the registry entries.
-----------------------------------------------------------------------
For example: RpSesClr -c

Licensed Materials - Property of IBM. Restricted Materials of IBM - 5724-L47.
(c) Copyright IBM Corp. 2001, 2007  All Rights Reserved
US Government Users Restricted Rights
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
```

Examples

Here is an example of this program's output if you enter "RpSesClr" when no parameters are specified.

```
Server:LA_02
   Session:WLAVMXA-E
   Session:WLAA-E
   Session:TSOSEC
   Session:MsgClctr
   Session:Generic_REXX_Session
Server:LA_01
   Session:MsgClctr
   Session:Generic_REXX_Session
Server:Boeb_01
   Session:mc
   Session:Generic_REXX_Session
Sessions cleared:9
```

The list of sessions whose positioning information has been cleared is also output to the RpSesClr.log file which, by default, is located in the SA IOM\utils directory.

Part 4. Alert escalation feature

Chapter 16. Administrator tasks for alert escalation 151
Post-installation administrator tasks 151
Access roles for SA IOM alert escalation . . . 152
Creating user groups in Integrated Solutions Console 153
Assigning access roles to user groups in ISC . . 154
Creating users in Integrated Solutions Console 154
Assigning users to groups in Integrated Solutions Console 155
Administering users and user groups in Integrated Solutions Console 155
Changing passwords for users in Integrated Solutions Console 155
Deleting user IDs in Integrated Solutions Console 156
Deleting groups in Integrated Solutions Console 156
Administering the alert escalation database . . . 156
Changing alert escalation passwords on the database side 157
Changing the rpweb to database password . . 158
Changing the SA IOM server to database password. 159
Starting and stopping WebSphere Application Server on Windows 159
| Netcool/OMNIbus integration 160
| Configure ad hoc notification 161
| Set up a new peer-to-peer address 161
| Set up SA IOM servers 161
| Changing the DBNotify database. 162

Chapter 17. Alert escalation 163
Using the Web interface 163
Logging on 163
About 164
Manage policies 164
General settings 164
Persons 166
Groups 169
Escalations 171
Manage alerts 174
Alerts 174
Event history 176
| Ad hoc alert escalation 177
| Servers 177
| Notify user 178
| Notify group 179
| Notify by escalation 180
Defining a policy 180
Testing a policy. 181
Stopping escalation 182
Acknowledging an alert 182
Disabling an alert escalation policy 184
Alert status 185
Level of escalation. 186
Notification 186
E-mail notification. 186
Pager notification 187
Script notification 187
SMS notification 188
Voice notification 188
| Ad hoc notification 189
| Multiple server support 189
Helper scripts 189
Schedules 192
Automatically starting escalation 193
Display problems 193
Filtering, searching, and sorting tables 194
Configuring your Web browser 195
Troubleshooting SA IOM alert escalation 196

Chapter 16. Administrator tasks for alert escalation

This section lists the SA IOM alert escalation feature administrator tasks.

Post-installation administrator tasks

When the SA IOM alert escalation component is installed, only the user ID `iscadmin` is authorized for the Integrated Solutions Console, where it has unlimited authority. This topic describes how to create and authorize additional users.

the following gives an overview of how you create and authorize additional users of the Integrated Solutions Console (ISC).

1. Understand the access roles that are used for the SA IOM alert escalation view of ISC (these access roles begin with the letters ″AFI″).
2. In the administrative console of ISC, create user groups that correspond to the ″AFI″ access roles you will use.
3. In the administrative console of ISC, assign the appropriate ″AFI″ access role to each user group you created. For example, assign the access role AFIUser to the user group AFIUserGroup, and assign the access role AFIOperator to the user group AFIOperatorGroup.
4. In the administrative console of ISC, create users and assign the users to the user groups.

The following topics include the detailed information that you need to perform these tasks.

Related Concepts

“Access roles for SA IOM alert escalation” on page 152
Access roles determine which actions an SA IOM alert escalation user can perform. This topic describes the roles that are available for the SA IOM alert escalation view of the Integrated Solutions Console (ISC) and the recommended group names.

Related Tasks

“Creating user groups in Integrated Solutions Console” on page 153
In the administrative console of Integrated Solutions Console (ISC), create one user group for each access role that will be used. Note that the access roles are already defined; you do not need to define them.

“Assigning access roles to user groups in ISC” on page 154
After you have created user groups in the administrative console of Integrated Solutions Console (ISC), you must assign access roles to these groups. This will grant the members of a group all of the permissions the access role that is assigned to the group contains.

“Creating users in Integrated Solutions Console” on page 154
To create a user in Integrated Solutions Console (ISC), perform the following steps.

“Assigning users to groups in Integrated Solutions Console” on page 155
To assign a user to a group in the Integrated Solutions Console (ISC), perform the following steps.

Access roles for SA IOM alert escalation

Access roles determine which actions an SA IOM alert escalation user can perform. This topic describes the roles that are available for the SA IOM alert escalation view of the Integrated Solutions Console (ISC) and the recommended group names.

For each access role that will be used, you will create a user group in Integrated Solutions Console. Then, you assign access roles to the user groups.

When you create the groups, you should specify group names that are similar to the names of the corresponding access roles. Group name recommendations are provided in the rightmost column of the following table:

SA IOM alert escalation access roles	Description	Recommended group name
AFIAdmin	Can perform all operations and update any policy	AFIAdminGroup
AFIUser	Can view all policies but can only update a policy if they are its specified owner.	AFIUserGroup
AFIOperator	Can view the alert data base and acknowledge alerts.	AFIOperatorGroup
AFIViewOnly	Can only view the various escalation policies but not make any updates.	AFIViewOnlyGroup

Note: You can use different group names but the names should optimally be similar to the names of the access roles.

Detailed information about the access roles that are used for the SA IOM alert escalation view are provided in the following table. A user's access role determines which alert escalation activities the user is authorized to perform.

Activity	AFIAdmin	AFIUser	AFIOperator	AFIViewOnly
Create new escalation	yes	yes		
Update escalation, escalation level, schedule associated with escalation	yes	yes, if owner of escalation definition		
Delete escalation, escalation level, schedule associated with escalation	yes	yes, if owner of escalation definition		
Create group	yes	yes		
Delete group	yes	yes, if owner of group definition		
Update group settings	yes	yes, if owner of group definition		
Add or remove group members	yes	yes, if owner of group definition		

Activity	AFIAdmin	AFIUser	AFIOperator	AFIViewOnly
Create person object	yes	yes		
Delete person object	yes	yes, if owner of person definition		
Update person settings, notification details, schedule associated with person	yes	yes, if owner of person definition		
View alert database	yes	yes	yes	
View history	yes		yes	
Acknowledge alert	yes	yes	yes	
Close or clean up alerts	yes		yes	
View events	yes	yes	yes	
View escalation settings	yes	yes	yes	yes

Creating user groups in Integrated Solutions Console

In the administrative console of Integrated Solutions Console (ISC), create one user group for each access role that will be used. Note that the access roles are already defined; you do not need to define them.

About this task

To create the groups, perform the following steps:

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins). For how to get this far, see steps 1 and 2 of "Logging on" on page 163.
2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Expand the **Users and Groups** branch.
4. Select **Manage Groups**.
5. Click **Create**.
6. Type a unique user group name in the **Group name** field, supply an optional description of the group, click **Create** to create the group.
7. You can use the **Create Like** control to repeat the step (using a unique name) until you have created the groups AFIAdminGroup, AFIUserGroup, AFIOperatorGroup, and AFIViewOnlyGroup.
8. When you are finished creating groups, click **Close** to return to the Manage Groups page.

"Access roles for SA IOM alert escalation" on page 152
Access roles determine which actions an SA IOM alert escalation user can perform. This topic describes the roles that are available for the SA IOM alert escalation view of the Integrated Solutions Console (ISC) and the recommended group names.

Assigning access roles to user groups in ISC

After you have created user groups in the administrative console of Integrated Solutions Console (ISC), you must assign access roles to these groups. This will grant the members of a group all of the permissions the access role that is assigned to the group contains.

Before you begin

The following table shows how the access roles must be mapped to the user groups:

Role	Map to
AFIAdmin	AFIAdminGroup
AFIUser	AFIUserGroup
AFIOperator	AFIOperatorGroup
AFIViewOnly	AFIViewOnlyGroup

About this task

Perform the following steps to assign access roles to groups:

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins). For how to get this far, see steps 1 and 2 of "Logging on" on page 163.
2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Expand the **Users and Groups** branch.
4. Select **Administrative Group Roles**.
5. Select **Add**.
6. Enter a group that you have created in the previous step.
7. In Roles, select the role that corresponds to the group you entered. For example, if you enter AFIViewOnlyGroup then assign to this group the access role: AFIViewOnly.
8. Click **OK**.
9. If you have more than one group, then go back to step 5 and repeat these steps until all your user groups have roles assigned to them.
10. When you are complete, click **Save**.
11. Restart WebSphere Application Server to activate the new configuration.

What to do next

Now, you can define some users and assign them to these user groups in Integrated Solutions Console.

Creating users in Integrated Solutions Console

To create a user in Integrated Solutions Console (ISC), perform the following steps.

About this task

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins). For how to get this far, see steps 1 and 2 of "Logging on" on page 163.

2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Expand the**Users and Groups** branch.
4. Click **Manage Users**.
5. Click **Create**.
6. Enter the user ID and password, and the user's first name, last name, and e-mail address, and click **Create**.

What to do next

Now you can assign the user to one of the ISC user groups. You must assign each user you create in Integrated Solutions Console to at least one user group.

Assigning users to groups in Integrated Solutions Console

To assign a user to a group in the Integrated Solutions Console (ISC), perform the following steps.

Before you begin

You must assign each user you create in Integrated Solutions Console to at least one user group.

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins). For how to get this far, see steps 1 and 2 of "Logging on" on page 163.
2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Expand the **Users and Groups** branch.
4. Select **Manage Users**.
5. Select the user ID you want to modify (by clicking on the highlighted User ID).
6. In User Properties for the selected user, select the Groups page.
7. Search for, then Select the appropriate group, and click **Add**.

What to do next

If you want to add this user to additional groups, repeat steps 5 through 7.

Administering users and user groups in Integrated Solutions Console

The following sections describe how to modify and delete users and user groups that have already been defined in Integrated Solutions Console.

Changing passwords for users in Integrated Solutions Console

To change user passwords perform the following steps.

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins) For how to get this far, see steps 1 and 2 of "Logging on" on page 163.
2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Expand the **Users and Groups** branch.
4. Select **Manage Users**.

5. Select the user ID you want to modify (by clicking on the highlighted User ID).
6. Type the new password in the Password field, and type it again in the Confirm password field.
7. Click **OK**.

Deleting user IDs in Integrated Solutions Console

To delete users, perform the following steps.

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins) For how to get this far, see steps 1 and 2 of "Logging on" on page 163.
2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Select **Users and Groups**.
4. Select **Manage Users**.
5. Select the user ID that you want to delete.
6. Click **Delete**.

Deleting groups in Integrated Solutions Console

To delete groups, perform the following steps.

1. Log in to Integrated Solutions Console as administrator (default: user ID iscadmin, group iscadmins) For how to get this far, see steps 1 and 2 of "Logging on" on page 163.
2. In the navigation tree of Integrated Solutions Console, ensure that the **All tasks** view is selected.
3. Expand **Users and Groups**.
4. Select **Manage Groups**.
5. Click the **Delete** button for the group you want to delete.
6. Search for, then select the group.
7. Click **Delete**.

Administering the alert escalation database

The SA IOM Alert Escalation feature uses three sets of user IDs and passwords to establish communications between different parts of the SA IOM system. You are prompted for passwords, which must be supplied, at installation time. This section explains where, and how, to change the passwords post-installation.

Typical user IDs and passwords associated with the SA IOM alert escalation database are listed here.

User ID	Password (supplied at installation)	Description
rpserver	rpserver, for example	Used for communications between the SA IOM Server (the rpserver.exe program) and the SA IOM alert escalation database.

User ID	Password (supplied at installation)	Description
rpweb	rpweb, for example	Used for communications between Integrated Solutions Console (ISC) and the SA IOM alert escalation database.
rpadmin	rpadmin, for example	Used for administering connections to the SA IOM alert escalation database. For example: Connections during password changes. **Note:** If you change the rpadmin password, ensure that the connections for the SQL CONNECT statements in the SQL files you want to run are changed also.

To ensure the highest security, change the password for each user ID listed above. These changes are best done at installation time, as the different parts of the system need to be recycled after a password is changed. Ensure that you change the password on both sides of the communication connection. Start with the database side. Detailed instructions follow.

Changing alert escalation passwords on the database side

When you change the passwords that are associated with SA IOM alert escalation, start on the alert escalation database side, as described in this topic.

About this task

To change the passwords that components use to communicate with the alert escalation database, follow these steps.

1. First, use the text editor of your choice to edit the SAIOM_PWD_CHG.SQL file that is stored in the Utils directory of the PC that the alert escalation database is installed on. In this SQL file, the following three lines of text show the password values.

```
CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rpadmin','rpadmin');
CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rpserver','rpserver');
CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rpweb','rpweb');
```

2. The second parameter on each line is the password. Change each password as desired and make a note of the new values. Store your passwords in a safe place. These database passwords will be encrypted and cannot be easily recovered.
3. If you change the rpadmin password, ensure that the connections for the SQL CONNECT statements in the SQL files you want to run are changed also. For example, you connect to Derby using the rpadmin userid and the password, as shown in the CONNECT statement below.

```
-- SAIOM
-- DB Property file version 2.1

.
.
.

PROTOCOL 'jdbc:derby://localhost:1527//';
CONNECT 'DBNOTIFY;user=rpadmin;password=rpadmin';
```

4. Save and exit the SAIOM_PWD_CHG.SQL file.
5. Next, process the SAIOM_PWD_CHG.SQL file using the IJ.BAT file, as follows.
   a. Open a command prompt and navigate to this directory.

      ```
      \derby\frameworks\Networkserver\bin
      ```

   b. Start the `ij.bat` file.
   c. Type the following command.

      ```
      "run '\xxx\yyy\SAIOM_pwd_chg.sql';"
      ```

      Use the edited file in the \xxx\yyy location.
6. Finally, ensure that the SA IOM alert escalation database is running.

What to do next

Now that you have changed the passwords on the SA IOM alert escalation database side, next change the password that the console uses to communicate with the database.

Changing the rpweb to database password

To change the password that the SA IOM Alert Escalation component (rpweb) uses to communicate with the SA IOM alert escalation database, follow these steps.

1. Use the text editor of your choice to edit the AFISettings.properties file that is delivered in the RpWeb.war directory on the PC on which the Integrated Solutions Console (ISC) server is installed. Use the search command to find the file AFISettings.properties. Locate the following line in the PROPERTIES.

   ```
   com.ibm.saiom.db.password=rpweb
   ```

2. Change the password from `rpweb` to a new password that will be used by the SA IOM alert escalation interface to communicate with the alert escalation database.
3. Save and exit from the file.
4. Recycle the eWAS server.

What to do next

Now that you have changed the password on the SA IOM alert escalation interface side, next change the password that the SA IOM server uses to communicate with the alert escalation database.

Changing the SA IOM server to database password

To change the password that the SA IOM server (rpserver.exe) uses to communicate with the alert escalation database, follow these steps.

1. Use the text editor of your choice to edit the rpsvrprf.txt file that is located in the config directory on the PC on which the SA IOM server is installed. Locate the following line in the file.

   ```
   NOTIFY_ODBC1 = DBNOTIFY,rpserver,rpserver
   ```

   The third parameter is the password.
2. Change the password from `rpserver` to a new password that will be used by the SA IOM server to communicate with the alert escalation database.
3. Save and exit from the file.
4. Recycle the SA IOM server.

Starting and stopping WebSphere Application Server on Windows

The WebSphere Application Server instance for SA IOM is started in the same way as any other WebSphere Application Server instance. The following section describes the usual ways.

About this task

When you are running WebSphere Application Server on a Windows system, you usually start and stop WebSphere Application Server by clicking the relevant icons on your desktop. For this product, they are labeled **Start embedded WebSphere**, and **Stop embedded WebSphere**.

If the icons are not available, you can start and stop this instance of the server from the Windows Start menu:

Start > All Programs > IBM Tivoli System Automation IOM V2.1 > Start embedded WebSphere (or **Stop embedded WebSphere**).

What to do next

Alternatively, you can use the start and stop scripts that are available in the directory <*was_root*>\bin:

- To start the instance of WebSphere Application Server used by SA IOM, open a command prompt and issue the following command:`<was_root>\bin\startServer <server_name>`

  For example:

  ```
  C:\Program Files\IBM\SA IOM\ewas\bin\startServer server1
  ```
- To stop the instance of WebSphere Application Server used by SA IOM, open a command prompt and issue the following command:`<was_root>\bin\stopServer <server_name> -user <user_id> -password <password>`

Netcool/OMNIbus integration

Tivoli Netcool/OMNIbus collects and consolidates events and alarms and presents this information to IT executives and operations personnel in an intuitive, graphical console. Netcool/OMNIbus provides realtime monitoring, management, and event de-duplication and helps organizations proactively manage their IT infrastructures.

Tivoli Netcool/OMNIbus has automation functions that can perform intelligent processing on managed alerts. In order to manage operations environments effectively, Tivoli Netcool/OMNIbus customers require highly reliable interactive alerting capabilities. This ensures that the correct person gets to know the relevant information without delay.

The combination of the SA IOM and Netcool/OMNIbus provides you with an excellent solution for enabling service assurance and availability. It ensures that any service-affecting event is escalated appropriately.

Integration module

SA IOM provides an easy-to-use integration module that is a Java command that sends an alert to SA IOM via TCP/IP. SA IOM then forwards the alert to the appropriate recipients using their favored notification method.

You can invoke the Java command is as follows:

```
java -classpath ./afiextconn.jar com.ibm.afi.ext.connection.AFIIomConnector
               -s <server>  -p <port>  -t<timeout>
               -e <escalation>  -pr <priority>  -et <Alert text>
```

Where:

server This is the host name or IP address of the server that the RpServer component of SA IOM is installed on. The default is `localhost`. Contact your SA IOM administrator for the host name that has been given to the server.

port This is the port number that the RpServer is listening to. The default is 1040.

timeout
This is the maximum time in milliseconds that the command waits for a response from SA IOM. The default is 5000.

escalation
This is a notification policy that is defined in the alert escalation database in SA IOM. Note that the escalation ID is case-sensitive. The notification policy defines the rules for carrying out the alert. In principle, it defines who, when, and where to notify.

priority
This is a user-assigned decimal number, in the range 1 - 999, that expresses the relative importance of the alert.

Alert text
This is the message text to be passed to the recipient of the alert. Up to 240 characters can be specified.

Note: The maximum length of the message that can be forwarded using the various notification methods depends upon the hardware and service providers being used.

Enabling the integration module

To make use of the integration module, perform the following steps:

1. Transfer the file afiextconn.jar from in directory utils to the server that hosts Netcool/OMNIbus.
2. Create a BAT file that invokes the Java command that is supplied with SA IOM, for example:

   ```
   java -classpath ./afiextconn.jar com.ibm.afi.ext.connection.AFIIomConnector
        -s <server> -p 1040 -t 30000 -pr %1 -e %2 -et %3
   ```

   This BAT file accepts three parameters:
   - The priority of the alert
   - An escalation identifier
   - An alert message

   All other parameters that are required to invoke the AFIIomConnector command are hardcoded in the BAT file.
3. Define an *external procedure* (SendIOM) that invokes the BAT file.
4. Define a *database trigger* that invokes the external procedure, for example, at the 3rd occurrence of an event.

Configure ad hoc notification

If you plan to use the ad hoc notification feature of SA IOM you must set up a new peer-to-peer address on the SA IOM Client configuration panel and configure server IP addresses.

Set up a new peer-to-peer address

About this task

To set up a new peer-to-peer address on the SA IOM Client configuration panel:

1. Click **Config > Server > *your_rp_server_name* > Peers** and specify the IP address of the WebSphere Application Server where the RpWeb user interface application is installed in the accepted peer clients list. If you have several instances of the Web-based user interface, you should specify the IP addresses of all the WebSphere Application Servers.
2. Select the checkbox that allows clients to use the peer service on the appropriate port. For example, if the SA IOM server and eWAS are installed on the same machine, use 127.0.0.1 as the IP address and enter the port number 1040.

Set up SA IOM servers

To use the ad hoc notification feature of the SA IOM you must define at least one active SA IOM server that is enabled to process alerts. Use the Servers table from the Ad hoc notification branch of the SA IOM escalation navigation tree to create or modify the list of servers. See “Servers” on page 177 for more details.

Note: If you plan to use multiple server support, it is recommended that the alerting policy (escalations, user, groups, etc) is identical on all servers.

Changing the DBNotify database

This task shows you how to change the connection in the RpServer from one DBNotify database to another.

Before you begin

Carry out the following so that the Web server hosts a configured and ready-to-use RpWeb application that has been installed with the SA IOM installer. The installed Web server must point to the computer's IP address where the derby component runs.

1. Install and configure eWAS
2. Create the SA IOM databases using the bat files that are supplied with SA IOM

About this task

To change the connection in the RpServer from one DBNotify database to another, you need to change the name of the Web server that hosts the RpWeb user interface as follows:

1. Install the DB2 ODBC driver and light interface. This is required for PCs that are running RpServer and RpEvents.
2. Run DB2CLP.
3. Uncatalog the node DERBYNET
4. Catalog the tcpip node `DERBYNET remote 'new webservername or Iaddress' server 1527`. This changes the pointer to the new DBNOTIFY source in ODBC.
5. Locate the AFISettings.properties file in the eWAS directory.
6. To change the JDBC pointer (this is necessary to administer the DBNOTIFY database from the WebSphere server), edit the AFISettings.properties file and change the following line to the desired value:

   ```
   com.ibm.saiom.db.url=jdbc:derby://'derby database location IPaddress':1527//DBNOTIFY
   ```
7. Recycle eWAS.

Results

This changes the connection from the WebSphere server to the DBNotify database.

Chapter 17. Alert escalation

The SA IOM alert escalation feature provides the ability to automatically notify a sequence of individuals about an alert based upon criteria that you specify.

For any particular alert, you can define a person or group to notify, define the notification method, and define one or more levels of escalation. Using schedules, you can specify who to call, or who not to call, at dates and times that you define.

Alert escalation *policies* are used to store your definitions in an alert escalation database. You interact with the alert escalation database using a Web interface that is based on the IBM Integrated Solutions Console (ISC).

The SA IOM alert escalation components and the ″classic″ product components (the SA IOM server and client components running on Windows) communicate with each other using the REXX programming language.

The SA IOM alert escalation feature has its own security that is administered using the administrative console of ISC. Default user access roles are provided so that the roles and authorities of different SA IOM alert escalation users can be easily defined.

Using the Web interface

This section describes how to interact with the alert escalation database using a Web interface that is based on the IBM Integrated Solutions Console (ISC).

Logging on

To access SA IOM alert escalation, perform the following steps. The SA IOM alert escalation navigation tree and all its panels are described under this topic.

Before you begin

You may need to contact your administrator to obtain the correct hostname, port number, user ID, and password.

1. Open a Web browser window and type the address of Integrated Solutions Console in the Address field. The entry must have the following form:

   `http://<hostname>:<port>/ibm/console`

   where *<hostname>* is the name of the host on which the WebSphere Application Server is running and *<port>* is the port number of the WebSphere Application Server. The default port is 9060. The log in panel of Integrated Solutions Console is displayed in the browser window.
2. On the log in panel, specify your user ID and password. Both are case-sensitive. Then click **Log in**. The Welcome page of Integrated Solutions Console comes up.
3. In the navigation tree of Integrated Solutions Console, completely expand the **SA IOM Alert Escalation** view so that all items are visible. The navigation tree provides a method of organizing the various policy elements you will define.

   The SA IOM alert escalation navigation tree expands into the following nodes.

- SA IOM Alert Escalation
  - "About"
- Manage policies
  - "General settings" (Administrators only)
  - "Persons" on page 166
  - "Groups" on page 169
  - "Escalations" on page 171
- Manage alerts
  - "Alerts" on page 174
  - "Event history" on page 176 (Administrators and Operators only)
- Ad hoc notification
  - "Servers" on page 177
  - "Notify by escalation" on page 180
  - "Notify user" on page 178
  - "Notify group" on page 179

About

Select the **About** node from the **SA IOM Alert Escalation** navigation tree, to display release level information.

The About window shows the release level and build date of your product, and IBM copyright information, and the Java logo.

If you seek assistance from IBM support, you will be asked to supply the information you can read from this panel.

Manage policies

Use the Manage policies section to manage your SA IOM alert escalation policies.

General settings

Use the General settings window to display settings that apply to all SA IOM Alert Escalation policies.

To open the General settings window, from the **SA IOM Alert Escalation** navigation tree, select **General settings**.

Note: Administrator authority is required for access. If you do not have administrator authority, you will not see the **General settings** node in your **SA IOM Alert Escalation** navigation tree.

The following illustrates a General settings window with values filled in.

Product name	SA IOM
Product Version	2.1
Database Version	220
SMS service provider	212.215.24.38:2711
Phone prefix	
"From" E-Mail address	saiom@de.ibm.com
E-Mail server name / IP	relay.xde.ibm.com
Time zone of the SA IOM Server	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Retention period for schedules (Days)	2
Retention period for alerts (Days)	3
Last modified	thisadmin 13.04.2007 15:04:06

Notice that the **Phone prefix** field is blank. This site is not using telephones for notification. You only need to supply values for features that you use.

Changing general settings for policies:

Administrator authority is required to change general settings for policies. To do so, follow these steps.

1. From the General settings window, click **Modify**. The General settings window displays in edit mode.
2. Appropriate default settings are already filled in for required fields. Detailed information follows.

Field	Description
Product name	Automatically updated. Typical value: `SA IOM`
Product Version	Automatically updated. Typical value: `2.1`
Database Version	Automatically updated. Typical value: `220`
SMS service provider	(SMS notification is Optional) If you are using SMS for notification purposes, specify the contact information for the service provider that is used for all SMS type notifications. The format is the IP address of the service provider you have chosen, followed by a colon, followed by the port number; for example `212.215.24.38:2711`.
Phone prefix	(Pager notification is Optional) If you are using a pager for notification purposes, specify a telephone prefix number for reaching a public network. For example, in the USA it is common to dial the number 9 to reach an ″outside line″ from a business phone.
″**From**″ **E-Mail address**	(E-mail notification is Optional) If you are using e-mail for notification purposes, specify the e-mail address that is the ″issuer″ of e-mail notification messages.
E-Mail server name / IP	(E-mail notification is Optional) If you are using e-mail for notification purposes, specify the server name or IP address of the e-mail server. This is your site's Simple Mail Transfer Protocol (SMTP) server.
Time zone of the SA IOM Server	(Required) Select the name of a city to indicate the physical location of the SA IOM server. This is used to calculate the time zone of the SA IOM server.
Retention period for schedules (Days)	(Required) Specify the number of days to store schedule definitions in the alert escalation database. A schedule is eligible for automatic deletion when the retention period expires. The range is from 0 to 9999. If 0 is specified, outdated schedules are not automatically deleted. The default is 14 days.
Retention period for alerts (Days)	(Required) Specify the number of days to store alert definitions in the alert escalation database. Alerts in Closed status are eligible for automatic deletion when the retention period expires. The range is from 0 to 9999. If 0 is specified, alerts in Closed status are not automatically deleted. The default is 14 days.

3. When you are finished supplying information, click **OK** to save it. (Or click **Cancel** to exit without saving.)

Persons

Use the Persons table to view, create, or modify the list of users who are the recipients of alert escalation messages. Typically, users are authorized to create and modify their own definitions, thus they can keep their own contact information current. The ISC user ID is used to check if the user is allowed to modify the person settings. If the ISC user ID does not match the person ID, then the modification is not allowed unless the user has admin rights.

To open the Persons table, from the **SA IOM Alert Escalation** navigation tree, select **Persons**.

- Above the table, the following buttons typically display:

Refresh	Updates the display with the latest information from the alert escalation database (and deselects the selected row).
Create user	Click to define a person to be notified using the SA IOM alert escalation feature.
Delete user	Click to delete the selected user definition.

  Note: The *access role* assigned to your user ID determines whether or not some interface controls are available to you. In general, if you are not authorized to perform an action then the control is not available.
- Table controls are described in "Filtering, searching, and sorting tables" on page 194.
- Beneath the table, additional definition pages become available when you select a definition.

  Related Tasks

  "Creating or modifying person definitions"
  To define, or to edit information for, a user, follow these steps.

  "Notification page" on page 167
  Use this page to create, modify, or delete one or more methods of contacting this person. At least one method for contacting the person must be specified. You should also always specify a default notification method for the person.

  "Schedules page" on page 167
  Use this page to create, modify, or delete, one or more schedule definitions for a person, if desired. If no schedule is specified for the person, the person is considered active at all times.

  "Groups page" on page 168
  Use this page to add this person as a member of one or more groups, or to view which groups this person is a member of.

  "Deleting person definitions" on page 168
  To delete a recipient of alert escalation messages, follow these steps.

Creating or modifying person definitions:

To define, or to edit information for, a user, follow these steps.

1. From the Persons table
   - To define a new user, click the **Create user** button (above the table). If no **Create user** button is available, then you are not authorized to create one.
   - To edit a user, select the definition and, on the General page (beneath the table) , click **Modify**. If no **Modify** button is available then you are not authorized to modify this definition.

2. Supply or edit the following General information for the person.

Field	Description
User ID	(Required) Supply a maximum of 20 characters alphanumeric text. **Note:** The user ID is case-sensitive. If you are a user creating your own definition, supply the same user ID that you used when logging on to SA IOM alert escalation.
First name	This is the given name of the person.
Last name	This is the family name of the person.
Description	This field is intended for descriptive information about the person, for example: the person's department.
Time zone	(Required) Select the name of a city to indicate the physical location of the person to be notified.
Active	The Active checkbox indicates whether or not this definition is used. If you clear the checkbox, then this definition is ignored. The default is Active.

3. Click **OK**. The definition is listed in the Persons table and the definition is selected. Beneath the table, the information you supplied displays on the **General** page. The `Last Modified` field shows the user ID and time stamp of the person who last modified the definition.

What to do next

Additional definitions pages for a selected person are: **Notification**, **Schedules**, and **Groups**. These are described next.

Notification page:

Use this page to create, modify, or delete one or more methods of contacting this person. At least one method for contacting the person must be specified. You should also always specify a default notification method for the person.

About this task

To view or manage the information for how to notify a person, follow these steps.

1. From the Persons table, select the person definition.
2. Click the Notification tab (beneath the table). The Notification page displays. If the buttons for **Create**, **Modify**, **Set as default**, and **Delete** are not available, then you are not authorized to modify this definition.
3. On the Notification page
   - To define a new notification method, click **Create**.
   - To edit a notification method definition, select it and click **Modify**.
   - To make a notification method the default method, select it and click **Set as default**.
   - To delete a notification method definition, select it and click **Delete**.

   For more information see "Notification" on page 186

Schedules page:

Use this page to create, modify, or delete, one or more schedule definitions for a person, if desired. If no schedule is specified for the person, the person is considered active at all times.

About this task

To view or manage the schedules for a person, follow these steps.

1. From the Persons table, select the person definition.
2. Click the Schedules page (beneath the table). The Schedules page displays. If the buttons for **Create**, **Modify**, and **Delete** are not available, then you are not authorized to modify this definition. If there is more than one schedule, Priority numbers (starting with the number 1) indicate the order in which the schedules take precedence in case there is a time period when more than one schedule is defined.
3. On the Schedules page
   - To define a new schedule, click **Create**.
   - To edit a schedule definition, select it and click **Modify**.
   - If there is more than one schedule, priority numbers (starting with the number 1) indicate the order in which the schedules take precedence. To change the order, select a schedule and click **Move up** or **Move down** to change the priority numbers as you like them.
   - To delete a schedule definition, select it and click **Delete**. You are prompted to confirm the deletion. Click **OK** to completely delete the selected definition.

   For more information see “Schedules” on page 192

Groups page:

Use this page to add this person as a member of one or more groups, or to view which groups this person is a member of.

About this task

To view or manage the groups for a person, follow these steps.

1. From the Persons table, select the person definition.
2. Click the Groups page (beneath the table). The Groups page displays. If the buttons for **Add to**, **Remove from** are not available, then you are not authorized to modify this definition.
3. On the Groups page
   - Groups that the selected person is a member of, show a check mark in the **User's Membership** column.
   - To add the person to a group, select the group then click **Add to**.
   - To remove the person from a group, select the group then click **Remove from**.

Deleting person definitions:

To delete a recipient of alert escalation messages, follow these steps.

1. From the Persons table, select the person definition to delete.
2. Click **Delete user**. You are prompted to confirm the deletion. The detailed definition pages, such as schedules associated with this user, will also be deleted when you click OK. The user is also automatically removed as a member from any group, and from all associations with escalation policies.

3. Click **OK** to completely delete the selected definition.

Groups

Use the Groups table to view, create, or modify the list of groups whose members are potential recipients of alert escalation messages. Group definitions can simplify the task of maintaining your alert escalation policies. If your policy specifies to notify a group, then all persons who are members of that group are notified.

To open the Groups table, from the **SA IOM Alert Escalation** navigation tree, select **Groups**.

- Above the table, the following buttons typically display:

Refresh	Updates the display with the latest information from the alert escalation database (and deselects the selected row).
Create group	Click to define a group to be notified using the SA IOM alert escalation feature.
Delete group	Click to delete the selected group definition.

Note: The *access role* assigned to your user ID determines whether or not some interface controls are available to you. In general, if you are not authorized to perform an action then the control is not available.

- Table controls are described in "Filtering, searching, and sorting tables" on page 194.
- Beneath the table, additional definition pages become available when you select a definition.

Related Tasks

"Creating or modifying a group"
To define, or to edit the information for, a group, follow these steps.

"Members page" on page 170
Use this page to view, add, or remove, member definitions from the selected group. Each group should have at least one member.

"Schedules page" on page 170
Use this page to create, modify, or delete, one or more schedule definitions for a group, if desired. If no schedule is specified for the group, the group is considered active at all times.

"Deleting a group" on page 171
To delete a group definition, follow these steps.

Creating or modifying a group:

To define, or to edit the information for, a group, follow these steps.

1. From the Groups table
   - To define a new group, click the **Create group** button (above the table). If no **Create group** button is available, then you are not authorized to create one.
   - To edit a group, select the definition and, on the General page (beneath the table) , click **Modify**. If no **Modify** button is available then you are not authorized to modify this definition.

2. Supply or edit the following General information for the group.

Field	Description
Group ID	Specify a unique alphanumeric identifier of the group. The maximum length is 20 characters. **Note:** The group ID is case-sensitive.
Group owner	This is the person who is permitted to change the group settings. Only the owner of the group, or the SA IOM alert escalation administrator, is allowed to modify it or delete it. If no owner is specified, then all users with the AFIUser role are permitted to modify the settings.
Description	This field is intended for descriptive information about the group.
Active	The Active checkbox indicates whether or not this definition is active. If you clear the checkbox, then this definition is ignored by the software application. The default is Active.

3. Click **OK**. The definition is listed in the Groups table and the definition is selected. Beneath the table, the information you supplied displays on the **General** page. The `Last Modified` field shows the user ID and time stamp of the person who last modified the definition.

What to do next

Additional definitions pages for a selected group are: **Members** and **Schedules**. These are described next.

Members page:

Use this page to view, add, or remove, member definitions from the selected group. Each group should have at least one member.

About this task

To view or manage the members for a group, follow these steps.

1. From the Groups table, select the group definition.
2. Click the Members tab (beneath the table). The Members page displays. If the buttons for **Add** and **Remove** are not available, then you are not authorized to modify this definition.
3. On the Members page
   - Users that the selected group includes, show a check mark in the **Member** column.
   - To add the person to the group (that is already selected), select the user then click **Add**.
   - To remove the person from the group (that is already selected), select the user then click **Remove**.

Schedules page:

Use this page to create, modify, or delete, one or more schedule definitions for a group, if desired. If no schedule is specified for the group, the group is considered active at all times.

About this task

To view or manage the schedules for a group, follow these steps.

1. From the Groups table, select the group definition.
2. Click the Schedules tab (beneath the table). The Schedules page displays. If the buttons for **Create**, **Modify**, and **Delete** are not available, then you are not authorized to modify this definition.
3. On the Schedules page
   - To define a new schedule, click **Create**.
   - To edit a schedule definition, select it and click **Modify**.
   - If there is more than one schedule, priority numbers (starting with the number 1) indicate the order in which the schedules take precedence. To change the order, select a schedule and click **Move up** or **Move down** to change the priority numbers as you like them.
   - To delete a schedule definition, select it and click **Delete**. You are prompted to confirm the deletion. Click **OK** to completely delete the selected definition.

   For more information see "Schedules" on page 192

Deleting a group:

To delete a group definition, follow these steps.

About this task

The owner of the group has authority to delete it. So does the administrator. If the group has no owner listed, then any user ID with the AFIUser role is sufficiently authorized to delete it.

1. From the Groups table, select the group definition.
2. Click the **Delete group** button (above the table). If no **Delete group** button is available then you are not authorized to delete this definition.

Escalations

Use the Escalations table to view, create, or modify the list of alert escalation policy names.

To open the Escalations table, from the **SA IOM Alert Escalation** navigation tree, select **Escalations**.

- Above the table, the following buttons typically display:

Refresh	Updates the display with the latest information from the alert escalation database (and deselects the selected row).
Create escalation	Click to define a policy using the SA IOM alert escalation feature.
Delete escalation	Click to delete the selected policy definition.

Note: The *access role* assigned to your user ID determines whether or not some interface controls are available to you. In general, if you are not authorized to perform an action then the control is not available.

- Table controls are described in "Filtering, searching, and sorting tables" on page 194.

- Beneath the table, additional definition pages become available when you select a definition.

  Related Tasks

  "Creating or modifying an escalation"
  To define or edit the information for an escalation policy follow these steps.

  "Levels page" on page 173
  Use this page to specify at least one escalation level for your escalation policy. Each level includes a duration (in minutes) and at least one Member (the person or group to notify).

  "Schedules page" on page 173
  Use this page to create, modify, or delete, one or more schedule definitions for an escalation, if desired. If no schedule is specified for the escalation, the escalation is considered active at all times.

  "Deleting an escalation" on page 174
  To delete an escalation policy, follow these steps.

Creating or modifying an escalation:

To define or edit the information for an escalation policy follow these steps.

1. From the Escalations table
   - To define a new escalation, click the **Create escalation** button (above the table). If no **Create escalation** button is available, then you are not authorized to create one.
   - To edit an escalation, select the definition and, on the General page (beneath the table) , click **Modify**. If no **Modify** button is available then you are not authorized to modify this definition.
2. Supply or edit the following General information for the escalation.

Field	Description
Escalation ID	Specify a unique alphanumeric identifier of the escalation policy. The maximum length is 20 characters. **Note:** The escalation ID is case-sensitive.
Owner	This is the person who is permitted to change the escalation settings. Only the owner of the escalation, or the SA IOM alert escalation administrator, is allowed to modify it or delete it. If no owner is specified, then all users with the AFIUser role are permitted to modify the settings.
Description	This field is intended for descriptive information about the escalation policy.
Active	The Active checkbox indicates whether or not this definition can be used. If you clear the checkbox, the definition is ignored by the software application. The default is Active.

3. Click **OK**. The definition is listed in the Escalations table and the definition is selected. Beneath the table, the information you supplied displays on the **General** page. The `Last Modified` field shows the user ID and time stamp of the person who last modified the definition.

What to do next

Additional definitions pages for a selected escalation are: **Levels** and **Schedules**. These are described next.

Levels page:

Use this page to specify at least one escalation level for your escalation policy. Each level includes a duration (in minutes) and at least one Member (the person or group to notify).

About this task

To view or manage the information for the levels of a selected escalation, follow these steps.

1. From the Escalations table, select the escalation definition.
2. Click the Levels tab (beneath the table). The Levels page displays. If the buttons for **Create**, **Modify**, and **Delete** are not available, then you are not authorized to modify this definition.
3. On the Levels page
   - To define a new level, click **Create**. Specify its duration in minutes and its Members.
   - To edit a level definition, select it and click **Modify**. Specify its duration in minutes and its Members.
   - Notice each level you define has a section for Members. For each level you specify, make sure that at least one user or group is specified in the Members section. To do so, proceed as follows.
     a. In the Levels section of the Levels page, select the level definition.
     b. In the Members section of the Levels page
        – Users or groups that the selected level includes, show a check mark in the **Member** column.
        – To add a user or group definition, select it then click **Add**.
        – To remove a user or group definition, select it then click **Remove**.
   - If there is more than one level, level numbers (starting with the number 1) indicate the order in which the levels occur. To change the order, select a level and click **Move up** or **Move down** to change the level numbers as you like them.
   - To delete a level definition, select it and click **Delete**.

   For more information see “Level of escalation” on page 186

Schedules page:

Use this page to create, modify, or delete, one or more schedule definitions for an escalation, if desired. If no schedule is specified for the escalation, the escalation is considered active at all times.

About this task

To view or manage the schedules for an escalation, follow these steps.

1. From the Escalation table, select the escalation definition.
2. Click the Schedules tab (beneath the table). The Schedules page displays. If the buttons for **Create**, **Modify**, and **Delete** are not available, then you are not authorized to modify this definition.
3. On the Schedules page
   - To define a new schedule, click **Create**.
   - To edit a schedule definition, select it and click **Modify**.

- If there is more than one schedule, priority numbers (starting with the number 1) indicate the order in which the schedules take precedence. To change the order, select a schedule and click **Move up** or **Move down** to change the priority numbers as you like them.
- To delete a schedule definition, select it and click **Delete**. You are prompted to confirm the deletion. Click **OK** to completely delete the selected definition.

For more information see "Schedules" on page 192

Deleting an escalation:

To delete an escalation policy, follow these steps.

About this task

The owner of the escalation has authority to delete it. So does the administrator. If the escalation has no owner listed, then any user ID with the AFIUser role is sufficiently authorized to delete it.

1. From the Escalations table, select the escalation definition.
2. Click the **Delete escalation** button (above the table). You are prompted to confirm the deletion. Click **OK** to completely delete the selected definition.

Manage alerts

Use the Manage alerts section to view and manage SA IOM alert escalation messages.

Alerts

Use the Alerts table to view and modify the status of alert escalation messages. You can track the progress of an alert from this table. You can also close alert entries manually, or delete obsolete alert entries (clean them up) manually from this table.

To open the Alerts table, from the **SA IOM Alert Escalation** navigation tree, select **Alerts**.

- Above the table, the following buttons typically display:

Refresh	Updates the display with the latest information from the alert escalation database (and deselects the selected row).
Accept	Changes the status of the selected alert to **Accepted** and indicates that you are now the owner of the selected alert. The alert is successfully acknowledged when its status changes to **Accepted**. Alert escalation processing ends. The status change is logged.
Reject	Does not change the status of the selected alert, but indicates that you are unable or unwilling to be its owner. Alert escalation processing continues.
Receive	Does not change the alert status, but indicates that you received the alert message of the selected alert. Alert escalation processing continues.
Close	(Administrators and Operators only) Changes the status of the selected alert to **Closed**. You must set the status of an alert to closed to make the alert eligible to be automatically deleted when the retention period expires.

Clean up	(Administrators and Operators only) You can use the **Clean up** button to delete obsolete alert entries from the alert escalation database manually. This is an alternate method of maintaining the alert table at a reasonable size if you have disabled the control that automatically deletes closed alerts when the retention period expires. See "Deleting obsolete alert entries" on page 176 below.

Note: The *access role* assigned to your user ID determines whether or not some interface controls are available to you. In general, if you are not authorized to perform an action then the control is not available.

- Table controls are described in "Filtering, searching, and sorting tables" on page 194.
- Beneath the table, additional definition pages become available when you select a definition.

Viewing alert status information:

To view or modify the status of an alert, follow these steps.

1. From the Alerts table, select the alert.
2. On the alerts General page (below the table), you can view the General information about the selected alert. The following illustrates a typical alerts General page.

```
Alert ID                 2914                    WARNING!
Escalation ID            MVSALERT
RpServer ID              A
Message                  ING140I ALERT 'CS_PROBLEM' FOR
                         'OPCAO_TEST/APG' ON 'SAT1' AT 17:33:14
                         2007-03-09
Arrival time             09.03.2007 17:38:07
Priority                 1
Current escalation level 3

Status                   Exhausted
```

Note: All possible status values for an alert are described in "Alert status" on page 185.

3. Click the History tab (below the table) to view the alerts History page. Administrator authority is required to view the alerts History page.

Example

The alerts History page displays the following columns. Most are considered self-explanatory. The various events for the alert are listed in chronological order.

Column	Description
Time stamp	Typical value: `13.03.2007 19:19:59`
Event type	This column displays a message when the alert changes state. For example: `Escalation level start`
Information	This column contains freeform text that further describes the Event Type in the adjoining row of the table. If available, "keyword = value" details are displayed here. For example: `duration=30 minutes`

Deleting obsolete alert entries:

To delete obsolete alert entries from the alert escalation database manually, follow these steps.

Before you begin

Only an administrator or operator has authority to manually delete obsolete alert entries.

Important: Ensure that you choose a quiet period in which to delete entries from the alert escalation database. Database locks may prevent new alerts from being created.

1. From the **SA IOM Alert Escalation** navigation tree, select **Alerts**.
2. Click **Clean up** (this button is located above the table).
3. A dialog on which you can customize manual alert deletion criteria displays.
4. Specify a number of days in the **Delete alerts older than** field.
5. In the **Delete alerts in the following states** area, all possible states for an alert are listed. A checkbox precedes each state. By default, alerts in the Closed state are selected. However you can delete alerts in any state by selecting the checkbox next its state. Multiple states can be selected. All alerts in the indicated states will be deleted from the database when you click OK.
6. When you are sure that you want to delete all alerts in the states you have indicated, click **OK**.

Event history

Use the Event history table to display details for all SA IOM alert escalation events. The Event history table gives you a comprehensive view of what is going on.

To open the Event history table, from the **SA IOM Alert Escalation** navigation tree, select **Event history**.

Note: Administrator authority or Operator authority is required for access. If you do not have the necessary authority, you will not see the **Event history** node in your **SA IOM Alert Escalation** navigation tree.

- Above the table, the following button typically displays:

Refresh	Updates the display with the latest information from the alert escalation database (and deselects the selected row).

- Table controls are described in "Filtering, searching, and sorting tables" on page 194.

Tip: To see the usefulness of event history information, filter on the Condition ″numbers equal to″ for a specified Alert ID.

The Event history table displays the following columns. Most are considered self-explanatory. Each can be sorted in ascending or descending order.

Column	Description
Time stamp	Typical value: `13.03.2007 17:37:32`
Alert ID	numeric

Column	Description
Escalation ID	case-sensitive alphanumeric
Escalation level	numeric
Event type	This column displays a message when the alert changes state. For example: `Escalation level start`
Information	This column contains freeform text that further describes the Event Type in the adjoining row of the table. If available, "keyword = value" details are displayed here. For example: `duration=15 minutes`

Ad hoc alert escalation

Use the Ad hoc alert escalation section to manage SA IOM ad hoc alert escalation.

Servers

Use the Servers table to view, create, or modify the list of servers that are to process alerts.

If an alert is to be sent using ad hoc notification, the RpWeb application attempts to establish a connection to an active server, starting with the first active server in the list. The first server in the list is taken where the connection could be established. Bear in mind that the eWAS IP address must be defined in the accepted peer clients list on all SA IOM Servers that can be used to process alerts.

To open the Servers table, from the **SA IOM Alert Escalation** navigation tree, select **Servers**.

- Above the table, the following buttons typically display:

Refresh	Updates the display with the latest information from the alert escalation database (and deselects the selected row).
Create server	Click to define a server to be notified using the SA IOM alert escalation feature.
Delete server	Click to delete the selected server definition.
Move Up	Move the selected server up in the list.
Move Down	Move the selected server down in the list.

Notes:

1. The sequence of the servers defined in the list determines which server will be used to process an alert. If a server is not available, SA IOM attempts to process the alert on the next active server from the list.
2. The *access role* that is assigned to your user ID determines which interface controls are available to you. In general, if you are not authorized to perform an action the control is not available.

- Table controls are described in "Filtering, searching, and sorting tables" on page 194.
- Beneath the table, additional definition pages become available when you select a definition.

Related Tasks

"Creating or modifying server definitions" on page 178
To define, or to edit information for a server, follow these steps.

"Deleting server definitions"
To delete a server, follow these steps.

"Changing the sequence of servers"
To move a server in the list, follow these steps.

Creating or modifying server definitions:

To define, or to edit information for a server, follow these steps.

1. From the Servers table.
   - To define a new server, click the **Create server** button (above the table). If no **Create server** button is available, then you are not authorized to create one.
   - To edit a server, select the definition and, on the General page (beneath the table) , click **Modify**. If no **Modify** button is available then you are not authorized to modify this definition.
2. Supply or edit the following information for the server.

Field	Description
Host name	(Required) Host name or IP address of the SA IOM server, supposed to process alert notifications.
Port	(Required) Port used to connect to the server. Default value is 1040.
Timeout	(Required) The timeout value (in milliseconds) for the server connections. Default value is 5000 ms.
Description	This field is intended for descriptive information about the server, for example, the server's location.
Active	The Active checkbox indicates whether or not this definition is used. If you clear the checkbox, then this definition is ignored. The default is Active.

3. Click **OK**. The definition is listed in the Servers table and the definition is selected. Beneath the table, the information you supplied displays on the General page.

Deleting server definitions:

To delete a server, follow these steps.

1. From the Servers table, select the server definition to delete.
2. Click **Delete server**. You are prompted to confirm the deletion.
3. Click **OK** to completely delete the selected definition.

Changing the sequence of servers:

To move a server in the list, follow these steps.

1. From the Servers table, select the server definition to move.
2. Click **Move Up** or **Move Down**.

Notify user

Use the Notify user panel to notify one or more individuals based on the data configured in the alert escalation database.

About this task

Perform the following steps:

1. Select one or more users in the Persons table shown at the top of the panel.
2. Decide whether the user schedules should be taken into account for carrying out the notification. If not, the notification is done using the default notification method that is defined for the user.

   Note: Including the user schedule might result in non-delivery of the notification if the schedule defines an off-duty period.
3. Specify the alert priority. The priority is a user-assigned decimal number, in the range from 1 through 999, which expresses the relative importance of the alert.
4. Specify the message text to be passed to the recipients of the alert.
5. Click the **Send** button.

Results

If more than one person is selected, the alert is issueed for each person, resulting in multiple alert entries in the alert table.

Related Concepts

"Persons" on page 166
Use the Persons table to view, create, or modify the list of users who are the recipients of alert escalation messages. Typically, users are authorized to create and modify their own definitions, thus they can keep their own contact information current. The ISC user ID is used to check if the user is allowed to modify the person settings. If the ISC user ID does not match the person ID, then the modification is not allowed unless the user has admin rights.

"Schedules" on page 192
Schedules are used when you define SA IOM alert escalation policies. Schedules are used for determining "on duty" and "off duty" time periods, and for defining individual notification methods. This is a conceptual topic.

Notify group

Use the Notify group panel to notify one or more groups based on the data configured in the alert escalation database.

About this task

Perform the following steps:

1. Select one or more groups in the Group table shown at the top of the panel.
2. Decide whether the user schedules should be taken into account for carrying out the notification. If not, the notification is done using the default notification method that is defined for the user.

   Note: Including the user schedule might result in non-delivery of the notification if the schedule defines an off-duty period.
3. Specify the alert priority. The priority is a user-assigned decimal number, in the range from 1 through 999, which expresses the relative importance of the alert.
4. Specify the message text to be passed to the recipients of the alert.
5. Click the **Send** button.

Results

If more than one group is selected, the alert is issueed for each group, resulting in multiple alert entries in the alert table.

Related Concepts

"Groups" on page 169
Use the Groups table to view, create, or modify the list of groups whose members are potential recipients of alert escalation messages. Group definitions can simplify the task of maintaining your alert escalation policies. If your policy specifies to notify a group, then all persons who are members of that group are notified.

"Schedules" on page 192
Schedules are used when you define SA IOM alert escalation policies. Schedules are used for determining ″on duty″ and ″off duty″ time periods, and for defining individual notification methods. This is a conceptual topic.

Notify by escalation

Use the Notify by escalation panel to start an alert escalation process based on the data configured in the alert escalation database.

About this task

Perform the following steps:

1. Select the escalation ID to be used for deciding who to notify.
2. Specify the alert priority. The priority is a user-assigned decimal number, in the range from 1 through 999, which expresses the relative importance of the alert.
3. Specify the message text to be passed to the recipients of the alert.
4. Click the **Send** button.

Related Concepts

"Escalations" on page 171
Use the Escalations table to view, create, or modify the list of alert escalation policy names.

Defining a policy

A policy contains all the information needed by SA IOM to perform alert notification and, if desired, one or more levels of alert escalation. A policy has a name and specifies: by what notification method to send the alert, one or more time frames to associate with the alert, and to whom the alert will be sent. This topic provides a high level view of how to define an SA IOM alert escalation policy.

Before you begin

The following are prerequisites to defining a policy:

- The SA IOM alert escalation feature is installed, deployed, and configured.
- And one of the following describes your SA IOM alert escalation access.
  - You have Admin authority for the SA IOM Alert Escalation view of ISC, or you have sufficient authority to grant this to yourself.
  - You have User authority for the SA IOM Alert Escalation view of ISC, and any general settings that you need for your policy are already defined by the administrator.

About this task

Follow these steps to define a policy.

1. In the navigation tree of Integrated Solutions Console, completely expand the **SA IOM Alert Escalation** view so that all items are visible. Everything you need to define a policy is under the **Manage policies** branch of the tree. For how to get this far, see "Logging on" on page 163.
2. If you have Admin authority, select **General settings** and ensure that any service provider name (or email server name) needed by your policy is specified here. For more detail see "General settings" on page 164.
3. Specify who to notify and how to notify using the **Persons** node. For more detail see "Persons" on page 166.
4. Specify notification groups, if desired. For more detail see "Groups" on page 169.
5. Create a name for your escalation policy using the **Escalations** node. Also specify at least one escalation level for your escalation policy. Each level includes a duration (in minutes) and at least one Member (the person or group to notify). For more detail see "Escalations" on page 171.

What to do next

This concludes the task of defining an alert escalation policy. Make a note of the escalation ID, you will need it to start the notification process. Be aware that the escalation ID is case-sensitive. A programming best practice is to test your policy immediately to ensure that it works as you intended.

Testing a policy

You start alert escalation processing using the product-provided AFR_NOTIFY REXX functions. This topic describes how to run the escalation.rex sample script. This script demonstrates the simplest way to start your escalation policy, so that you can test it.

Before you begin

Before you can start escalation, an escalation policy must be defined and configured in the SA IOM alert escalation database. You need to know the escalation ID in order to start the escalation policy that you defined.

About this task

To manually start escalation, follow these steps.

1. Log on to the SA IOM server on which the alert escalation feature has been configured.
2. From the Scripts panel, run the escalation.rex sample script and provide the escalation ID of the policy that you want to start.
   a. For example, to start the escalation policy named TestPolicy1 you would type the following in the entry field on the Scripts panel. `escalation.rex TestPolicy1` and click **Start**. Note that the escalation ID is case-sensitive. A REXX session window named escalation.rex is listed on the Servers and Sessions panel beneath the server on which you started the session.
   b. Double-click on the escalation.rex session window to select it.

If no escalation ID is provided to the escalation.rex sample script, the script attempts to start the SampleEsc1 escalation policy.

3. The REXX session output is displayed in the session window.

Example

Example output to a REXX session window might look like this:

```
Escalation 'SampleEsc1' started, alert ID = 0000000001
done
```

What to do next

SA IOM tracks the progress of the alert using its alert ID. You can track the progress of the alert by logging on to the SA IOM alert escalation Web interface and viewing the Alerts table.

Stopping escalation

Stop alert escalation processing either by acknowledging the alert with an Accept, or by disabling the escalation policy in the SA IOM alert escalation database.

To stop escalation, use one of the following methods.

Acknowledging an alert

Acknowledging an alert is one way to stop the escalation process. If the alert is not successfully acknowledged then the escalation process continues. You can acknowledge an alert either using a Web browser or using a REXX script that runs under SA IOM control.

- If using a Web browser:
  1. Log on to the SA IOM alert escalation view of the console. For how to get this far, see "Logging on" on page 163.
  2. From the SA IOM Alert Escalation navigation tree, expand all nodes then select **Alerts**
  3. Select the Alert ID of the alert notification you want to acknowledge then click **Accept**. For more detail see "Alerts" on page 174.
- If using a REXX script that runs under SA IOM control:
  1. Use the AFR_NOTIFY_INIT() REXX function to initiate your log in to the alert escalation database.
  2. Use the the AFR_NOTIFY_ACK() function to specify the Alert ID of the message you are acknowledging, to specify the keyword ACCEPT, and to identify yourself as the acknowledging person.
  3. Use the AFR_NOTIFY_EXIT() REXX function to end your database session.

  Here is an example of a REXX script routine that acknowledges an alert.

```
/*****************************************************************************/
/*                                                                           */
/* Name:      Acknowledge                                                    */
/*                                                                           */
/* Function:  This routine acknowledges the alert notification.              */
/*                                                                           */
/* Input:         1)  alert id                                               */
/*                2)  ack level                                              */
/*                3)  user id                                                */
/*                4)  message                                                */
/*                                                                           */
```

```
/*********************************************************************************/

/*********************************************************************************/
/* Tell REXX which routine to call in case of an error...                        */
/* Programmer: Do not change the following code sequence.  This code block       */
/*             must be at the beginning of the script.                           */
/*********************************************************************************/
gbl. = ''                          /* no global variable set yet - done to avoid
                                      any no-value condition while accessing
                                      any of the global variables                */
gbl.0debug = 'Y'                   /* run in debug mode                          */

Signal On Syntax  Name RTN_Error; Signal On NoValue Name RTN_Error
Signal On Failure Name RTN_Error; Signal On Halt    Name RTN_Error

/*********************************************************************************/
/* Initialize a few variables...                                                 */
/*********************************************************************************/
dfltlvl = 'accept'
dfltuid = 'WAS'
dfltmsg ='ack response'

/*********************************************************************************/
/* Determine who we are                                                          */
/*********************************************************************************/
gbl.0me = 'Acknowledge(' || AFR_WHOAMI() || ')'

/*********************************************************************************/
/* Pickup input parameters....                                                   */
/*   1)  alert id                                                                */
/*   2)  ack lvel                                                                */
/*   3)  user id                                                                 */
/*   4)  comment message                                                         */
/*********************************************************************************/
Parse Arg alertid acklevel userid msg
if alertid = '' then
  do
    SAY 'Alert id missing'
    exit
  end
if acklevel = '' then acklevel = dfltlvl
if userid   = '' then userid   = dfltuid
if msg      = '' then msg      = dfltmsg
If gbl.0debug = 'Y' then
  SAY 'alert id is' alertid '- ack level is' acklevel

rc = AFR_NOTIFY_INIT()
If rc <> 0 then                    /* good completion ?                          */
  do                               /* ..No, report error                         */
    err_msg = 'Bad return code from AFR_NOTIFY_INIT, RC='rc
    If gbl.0debug = 'Y' then
      SAY err_msg
    rc = Afr_Log(gbl.0me':' err_msg)
  end

rc = AFR_NOTIFY_ACK(alertid,acklevel,userid,message)
If rc <> 0 then                    /* good completion ?                          */
  do                               /* ..No, report error                         */
    lrc = rc                       /* save return code from service              */
    err_msg = 'Bad return code from AFR_NOTIFY_SET_RESULT, RC='rc
    If gbl.0debug = 'Y' then
      SAY err_msg
    rc = Afr_Log(gbl.0me':' err_msg)
  end

rc = AFR_NOTIFY_EXIT()
If rc <> 0 then                    /* good completion ?                          */
```

```
  do                                /* ..No, report error                    */
    err_msg = 'Bad return code from AFR_NOTIFY_EXIT, RC='rc
    If gbl.0debug = 'Y' then
      SAY err_msg
     rc = Afr_Log(gbl.0me':' err_msg)
  end

exit                                /* and return to caller                  */

/*****************************************************************************/
/*                                                                           */
/* Name:      RTN_Error                                                      */
/*                                                                           */
/* Function:  This is the common error trap routine. The routine gets the    */
/*            error data, logs a message and exits the script.               */
/*                                                                           */
/* Global Input:  gbl.0me   - name of script where error occurred            */
/*                                                                           */
/* Output:        Not applicable                                             */
/*                                                                           */
/*****************************************************************************/
RTN_Error:
  Signal Off Syntax; Signal Off Failure;
  Signal Off Halt; Signal Off NoValue

  cond = condition('C')
  desc = strip(left(condition('D'),150))

  Select
    When cond = 'HALT' Then desc = 'SCRIPT HALTED'
    When cond = 'SYNTAX' Then desc = errortext(rc)
    Otherwise Nop
  End
  If cond = 'NOVALUE' | cond = 'HALT' Then rc = 'N/A'

  msg = cond 'condition trapped in script' gbl.0me 'Line:' sigl,
        'Code:' rc 'Description:' desc
  If gbl.0debug = 'Y' then SAY msg
  rc = AFR_LOG(gbl.0me':' msg)

  Exit                              /* and leave this script                 */
```

Results

Regardless of the acknowledgement method you use, the implications of your response are the same; as described in the following table.

Response	Result
Accept	Indicates you are now the ″owner″ of this alert. The alert is successfully acknowledged when its status changes to Accepted. Alert escalation processing ends.
Reject	Indicates you are unable or unwilling to be the owner of this alert. Alert escalation processing continues. **Note:** If all recipients at a particular level of escalation reject the alert, escalation proceeds immediately to the next level.
Receive	Indicates you received the alert message. Alert escalation processing continues.

Disabling an alert escalation policy

It may become necessary to disable an alert escalation policy if it is not working as intended. To do so, follow these steps.

1. Log in to Integrated Solutions Console (ICS).
2. Select the SA IOM Alert Escalation view and expand the **Manage Policies** branch.
3. Select the **Escalations** node. The Escalations table displays.
4. Select the escalation policy.
5. On the General page (beneath the table) , click **Modify**. If no **Modify** button is available then you are not authorized to modify this definition.
6. Clear the **Active** checkbox.
7. Click **OK**.

What to do next

No new instances of the selected escalation can be started unless the **Active** checkbox is selected.

Alert status

All possible status modes for an alert are described in this section.

Table 13. Status modes of an alert

Status	Description
Open	This is the first status given when an alert arrives in SA IOM.
Exhausted	This status is given when all defined escalation levels have run out, and the alert has not been acknowledged.
Error	An error occurred during escalation processing.
Accepted	The alert has been acknowledged by at least one recipient.
Disabled	The alert is blocked from being processed, for example the alert's escalation policy is marked inactive or the current schedule indicates an "off duty" period.
Closed	This is the final status meaning that the alert has been completely processed. The alert is eligible for becoming automatically deleted when the retention period expires. You must set the status of an alert to **Closed**; this is not automatic.

While it is being escalated, an alert has a status of **Open**.

Typically, the status of an alert traverses from **Open** through either **Accepted**, **Exhausted**, or **Error**, to the final status of **Closed**. The following diagram shows the flow of status transitions for an alert.

Important:

1. If the SA IOM server stops, either intentionally or unintentionally, while alerts are being processed then alerts may remain in unpredictable states. There is no ″clearing″ function that resumes processing when the server is restarted. For example, there is no function in the SA IOM server that examines all open alerts after a

restart and then resumes processing them. Therefore, when the server is restarted, all open alerts that were being processed before the server stopped, must be cleaned up manually.

2. Ensure that you choose a quiet period in which to delete entries from the alert escalation database. Database locks may prevent new alerts from being created.

Level of escalation

A *level* is a predefined time-period that you specify in the alert escalation policy. You must estimate the total length of time it takes to notify a specified person and to have that person acknowledge the alert. We don't know how long this time period should be; perhaps 30 minutes.

Each escalation level has a *duration* which is its specified maximum time-to-live, in minutes. (You will see this term on a panel when you are defining an escalation level.)

Each escalation level specifies one or more *groups* or *persons* to notify.

Time counting begins from the point in time when the alert is first *trapped* by SA IOM. At this point in time, the alert is in an open state and is at the first escalation level.

An escalation policy can have as many levels as you want. But as a practical matter perhaps two or three levels are sufficient. Your business may not have a large number of subject matter experts to whom a particular urgent technical problem can be escalated.

Escalation progresses to the next escalation level in these cases.

- None of the persons being notified ″accepts″ the alert within the specified time period.
- Every person being notified ″rejects″ the alert. (In this case the duration is ignored.)

Escalation is terminated when one of the persons being notified ″accepts″ the alert. This can be a person at the current level or any previous level.

Notification

Automatically send the alert to a designated person (or group), using any of the available notification methods. A user can define one or more notification methods for each defined person within the alert escalation database. This topic leads you to more detailed information about the supported SA IOM alert escalation notification methods, which are: E-mail, Pager, SMS, Script, and Voice.

E-mail notification

E-mail type notification requires an E-mail server. This service is not provided for you by IBM nor by the SA IOM alert escalation feature. This topic lists where, in the console interface, to supply the required E-mail information.

All Policies in the alert escalation database use the same email server and the same ″from″ address.

Specify the **E-Mail server name/IP** name and the **From** email name on the General Settings page. Administrator authority is required to edit the General Settings of the SA IOM Alert Escalation view.

Specify other e-mail settings on the Notification page of a **Persons** definition.

- E-mail address (Supply the address of the individual to be notified.)
- E-mail type (Choose one of: TO, CC, BCC)
- Optional parameter 1 (This optional parameter is provided to give your helper script more flexibility. The sample script does not use this parameter.)
- Optional parameter 2 (This optional parameter is provided to give your helper script more flexibility. The sample script does not use this parameter.)

When an alert notification message is sent using the information you supplied above, the REXX script identified in "Helper scripts" on page 189 is called.

Pager notification

Pager notification requires a paging service provider. This service is not provided for you by IBM nor by the SA IOM alert escalation feature. This topic lists where, in the console interface, to supply the required Pager information.

The paging service provider is reached using a phone number that you specify as part of a user definition. Therefore different policies in the alert escalation database can use different paging service providers.

Specify the **Phone prefix** that is used for all calls, for example 9, on the General Settings page. Administrator authority is required to edit the General Settings of the SA IOM Alert Escalation view.

Specify other pager settings on the Notification page of a **Persons** definition.

- Mobile phone number (Supply the phone number of the paging service provider here and the number that identifies the individual to be notified. Specification methods differ from provider to provider.)
- Optional parameter 1 (This field provides a place for passing additional information to your service provider, if needed.)
- Optional parameter 2 (This field provides a place for passing additional information to your service provider, if needed.)

When an alert notification message is sent using the information you supplied above, the REXX script identified in "Helper scripts" on page 189 is called.

Script notification

This topic lists where, in the console interface, to supply the required script information.

All Policies in the alert escalation database use the SA IOM server as the script notification service provider.

Specify other script settings on the Notification page of a **Persons** definition.

- Script name (Supply the number that identifies the individual to be notified.)
- Optional parameter 1
- Optional parameter 2

When an alert notification message is sent using the information you supplied above, the REXX script identified in “Helper scripts” on page 189 is called.

Note: Ensure that your script has a completion return code. Use a return code of 0 to indicate success. Any non-zero return code indicates an error occurred and the script failed. This is required for scripts that you start using the NotifyScript.rex program, and is a good programming practice for any REXX script.

SMS notification

Short Message Service (SMS) also known as Global Messaging Service (GSM) and as cellular phones. SMS type notification requires an SMS service provider. This service is not provided for you by IBM nor by the SA IOM alert escalation feature. This topic lists where, in the console interface, to supply the required SMS information.

All Policies in the alert escalation database use the same SMS service provider. Keep these things in mind when you choose a service provider. Ensure that the provider guarantees delivery of the SMS message. Free internet services may provide the SMS function but without a guarantee of delivery. Also, some service providers allow the recipient to ″acknowledge″ the alert by replying to the SMS message. The sample SMS helper script shows how this is accomplished using eCall as the service provider.

Specify the service provider you have chosen in the **SMS service provider** field on the General Settings page. The format is the IP address, followed by a colon, followed by the port number; for example `212.215.24.38:2711`. Administrator authority is required to edit the General Settings of the SA IOM Alert Escalation view.

Specify other SMS settings on the Notification page of a **Persons** definition.

- Mobile phone number (Supply the number that identifies the individual to be notified.)
- Optional parameter 1 (This field provides a place for passing additional information to your service provider, if needed. For example, an account number for the individual to be notified.)
- Optional parameter 2 (This field provides a place for passing additional information to your service provider, if needed. For example, a password for the individual to be notified.)

When an alert notification message is sent using the information you supplied above, the REXX script identified in “Helper scripts” on page 189 is called.

Voice notification

Voice notification requires the text to speech function to be provided by a voice service provider. The text to speech function is not provided for you by IBM nor by the SA IOM alert escalation feature. This topic lists where, in the console interface, to supply the required Voice notification information.

All Policies in the alert escalation database use the same voice service provider.

Specify other voice settings on the Notification page of a **Persons** definition.

- Mobile phone number (Supply the number that identifies the individual to be notified.)

- Optional parameter 1 (This field provides a place for passing additional information to your service provider, if needed.)
- Optional parameter 2 (This field provides a place for passing additional information to your service provider, if needed.)

When an alert notification message is sent using the information you supplied above, the REXX script identified in "Helper scripts" is called.

Ad hoc notification

Ad hoc notification is an extension of the alert escalation Web-based user interface. It allows an operator to manually issue an alert that is to be sent to a particular person, or group of persons as defined in an escalation policy.

You can use the Web-based user interface to inform subject matter experts about a particular situation without needing to know how to reach the expert or, in out of office situations, who is deputizing for them. Thus you are able to respond to situations that may not be dealt with by normal alert escalation policies.

When you issue an alert using ad hoc notification, you can send it to one of the following:

- One or more users, using the Notify user panel
- One or more groups of users, using the Notify group panel
- An escalation ID that determines which users should be notified, using the Notify by escalation panel

You can also specify a priority that indicates how important the alert is and a text message that is passed to the recipients of the alert.

Alert notification is thus evolving beyond being an add-on mechanism that is used to pass information to offsite personnel's mobile devices. Ad hoc alerting gives IT operations the ability to deliver real-time information and to control the amount of data that is reported, thus avoiding sending unimportant data.

Multiple server support

You can have number of SA IOM Servers that are enabled to process alerts.

If an alert is to be sent using ad hoc notification, the RpWeb application attempts to establish a connection to an active server starting with the first active server in the list. If the server is unavailable, the RpWeb application takes the next server from the list until a connection can be established. To use multiple server support, the alerting policy (escalations, user, groups, etc.) must be identical on all servers.

Helper scripts

A *helper script* is the bridge between the notify REXX function routine and the hardware used for carrying out the notification. Each of the notification methods is initiated using a REXX helper script that is called by SA IOM. SA IOM passes a standard parameter list to the notification helper script. Guidelines for helper scripts are also described in this topic.

The following table lists, for each supported notification method, the program that the SA IOM server attempts to execute when an alert notification message is sent.

Table 14. Alert escalation notification methods and associated helper script names

Notification method	Helper script program name
E-mail	NotifyEmail.rex
Pager	NotifyPager.rex
Script	NotifyScript.rex
SMS	NotifySMS.rex
Voice	NotifyVoice.rex

You will most likely need to customize the contents of the helper scripts that you use; since the protocol to be used varies from hardware to hardware, and the interface to interact with the various service providers varies from country to country. For example, consider the pager notification helper script, NotifyPager.rex. It uses a service provider called CITYRUF pager service which is available in Germany. A pager service provider available in Germany will most likely follow different rules than a pager service provider available in the USA or in the country where you happen to be.

Note: The names of the helper scripts *cannot* be changed; they are required to remain as listed in Table 14.

Standard parameter list for helper scripts

SA IOM passes a standard parameter list to each notification helper script. When passed, the various parameters are separated by the 'FF'x character. The standard input parameters are described in the following table.

Table 15. The standard input parameters passed to notification helper scripts

Parameter	Description
1. Alert ID	This is a unique positive number that is assigned by SA IOM and is used to track the alert message. This is returned by a successful AFR_NOTIFY function call.
2. Alert priority	This parameter is a user-assigned decimal number, in the range from 1 to 999, that is intended to express the relative importance of the alert. The alert priority parameter is passed in the AFR_NOTIFY function call.
3. Alert message	This parameter is the message text to be passed to the recipient of the alert. The maximum length of the message that can be forwarded using the various notification methods depends upon the hardware and service providers being used. The alert message is passed in the AFR_NOTIFY function call.
4. Escalation ID	This parameter identifies a policy that is defined in the alert escalation database. The escalation ID is passed in the AFR_NOTIFY function call.
5. Current escalation level	This parameter identifies the current escalation level of the policy that is defined in the alert escalation database.
6. Duration time of escalation level	This parameter identifies the duration time, in minutes, of the current escalation level of the policy that is defined in the alert escalation database.

Table 15. The standard input parameters passed to notification helper scripts (continued)

Parameter	Description
7. Service provider (or name of the email server)	This parameter identifies the name of the email server or the SMS service provider, or the paging service provider that is defined in the alert escalation database. These are specified by the Administrator when defining General settings for policies. This parameter is passed as an input to and is required by sample helper scripts NotifyEmail.rex, NotifyPager.rex, and NotifySMS.rex. This parameter is not passed as an input to sample helper scripts NotifyScript.rex and NotifyVoice.rex. The SA IOM server acts as the REXX service provider, so you do not specify it. And the assumption is that the telephone number is sufficient to identify and reach the service provider that you are using to provide text-to-speech services.
8. Optional parameter 1 (if more than one separated by semi-colon)	Optional parameters 1 and 2 may be specified with the Notification settings for a Person definition in the alert escalation database. These optional parameter fields are provided to give your helper scripts more flexibility, and they can be used in any of your helper scripts. It is your responsibility when customizing a script to define the meaning of these parameters. Optional parameters 1 and 2 are not used by sample helper scripts NotifyEmail.rex and NotifyScript.rex. **Note:** The options associated with the various recipients are separated by a semi-colon (;).
9. Optional parameter 2	
10. Process handle	This parameter is a handle that uniquely identifies this helper script invocation; it is passed by SA IOM on input to the helper script.
11. User ID (if more than one separated by semi-colon)	This parameter is the user ID that identifies a Person definition in the alert escalation database.

Additional required parameters vary by notification method as summarized in the following table.

Table 16. Additional input parameters passed to notification helper scripts

Notification method	Description of standard required parameters plus additional required parameters
E-mail	Standard parameters, plus 12 Sender email address 13 ″TO″ email addresses (if more than one, separated by semi-colon) 14 ″CC″ email addresses (if more than one, separated by semi-colon) 15 ″BCC″ email addresses (if more than one, separated by semi-colon)
Pager	Standard parameters, plus 12 Pager number (if more than one, separated by semi-colon)

Table 16. Additional input parameters passed to notification helper scripts (continued)

Notification method	Description of standard required parameters plus additional required parameters
Script	Standard parameters (except for 7 Service provider), plus 12 Script name (if more than one, separated by semi-colon)
SMS	Standard parameters, plus 12 Cellphone number (if more than one, separated by semi-colon)
Voice	Standard parameters, plus 12 Telephone number (if more than one, separated by semi-colon)

Guidelines for helper scripts

The best guides to writing your own helper scripts are to examine the helper script sample programs.

Here are some other points to guide you.

- The names of the helper scripts can **not** be changed; they are required to remain as listed in Table 14 on page 190.
- Ensure that your script resides in the script directory of the SA IOM server and that it ends with the .REX extension.
- Ensure that your script has a completion return code. Use a return code of 0 to indicate success. Any non-zero return code indicates an error occurred and the script failed. This is required for scripts that you start using the NotifyScript.rex program, and is a good programming practice for any REXX script.

Schedules

Schedules are used when you define SA IOM alert escalation policies. Schedules are used for determining "on duty" and "off duty" time periods, and for defining individual notification methods. This is a conceptual topic.

Theoretically, specifying a Schedule (using the Schedules tab of an Escalation, Group, or Person) is optional. If no schedule is specified for the escalation, group, or person; then the escalation, group, or person is considered to be active at all times.

A schedule is an "object" that you define and associate with another "object" in the SA IOM alert escalation database. For example:

- **An escalation can have a schedule.** Commonly, escalation schedules are used to specify when the escalation is **not** in effect, for example, Holidays or times when the system is down for maintenance upgrades. Specifying an "off duty" escalation schedule prevents the policy from being used during the specified time period.
- **A group can have a schedule.** A group schedule is used primarily to define "off-duty" time periods for the group. Specifying an "off duty" group schedule prevents persons in the group from being notified during the specified time period.
- **A person can have a schedule.** A person schedule is used to define "on duty" or "off duty" time periods. Each "on duty" schedule for a person specifies the notification method to use for that person during that time period.

Multiple schedules may be in effect. You can define as many schedules as you want. However, it is a programming best practice to avoid complexity when possible. Keep in mind that there are no special utilities included with this product that will help you in the event that you define multiple schedules that conflict with each other. You are on your own there.

Schedules are processed in the following order.
1. escalation schedules
2. group schedules
3. person schedules

If the escalation schedule indicates that this time period is an ″off duty″ period then processing stops. If a group schedule indicates that this time period is an ″off duty″ period then the entire group is ignored. All schedules in effect in a given time period have to be in agreement to create a notification.

Active schedules of the same type (escalation, group, or person) are processed in the order of their priority number. A schedule with priority number 1 is processed first, priority number 2 is processed next, and so on.

When defining the time period for your schedule, choose the ″Type″ option that best describes how the time period should be measured.

Range is characterized by one begin date and time, and one end date and time.

For example from 08:00 on 05/01/07 to 16:00 on 05/02/07 (Range is the default.)

Band is a repeating time pattern.

For example every Monday and Friday from 08:00 to 16:00 in the first 2 weeks of May, 2007 (05/01/07 until 05/14/07).

Automatically starting escalation

The goal is to configure your software solution in such a way that you are automatically alerted if a bad situation develops. You can then address the situation in time to prevent it from becoming an application-stopping problem.

Your site needs to determine alert conditions and then use the AFR_NOTIFY REXX functions to issue the alert.

You can use any of the following SA IOM features to initially gather the information for the alert message from your system or application:

- Any of the product provided REXX APIs traditionally used for trapping, such as AFR_ASYNC_WTOR, AFR_SET_TRAP, AFR_SET_WTOR, AFR_CHECK_TRAP, AFR_CHECK_WTOR, and the AFR_GET_LINE functions
- Message Collector
- Peer-to-peer communications, from a console that SA IOM is monitoring or from another peer system

Display problems

If you are unable to select or to find an SA IOM alert escalation item in one of the table displays, try using the **Refresh** button to update the display with the latest information from the alert escalation database. **Refresh** also deselects the selected table row.

Before you begin

Common table controls are described in "Filtering, searching, and sorting tables."

About this task

If refreshing the table did not solve the problem, try using the **Expand Table** button. This makes more entries visible.

If you still are unable to select or to find the item after expanding the table, use the **Clear All Sorts** and the **Clear All Filters** buttons.

To gain extra room to display more table entries

- If you previously turned them on, click the **Hide Filter Row** and **Hide find toolbar** buttons.
- If using Microsoft Internet Explorer, select **View > Full Screen F11**.

All entries in the table are now displayed. Depending upon your configuration, many pages of entries may now be available for display. If no table entries display, you need to Create some.

1. If you still have display trouble, try "Configuring your Web browser" on page 195 then return to this topic.
2. Are you able to log on? See "Logging on" on page 163.
3. Your user ID may not be authorized to perform the action you are attempting. See "Access roles for SA IOM alert escalation" on page 152

Example

Filtering, searching, and sorting tables

Describes the common controls for manipulating alert escalation table displays (such as the Persons, Groups, Escalations, Alerts, and Event history tables). Learning to use these controls is helpful if you have a large number of SA IOM alert escalation definitions of any type.

Buttons for performing table actions

Small ″table actions″ buttons are located just above the column headings. Table actions work on the table as a whole.

- **Show Filter Row**. Produces a dialog box for specifying the resources to view in the table. When you produce the dialog box, select the column to filter and enter the filter criteria.
  - **Column to filter** Select the column to filter from the drop-down list. When you apply the filter, only those items in the selected column that meet the filter criteria are displayed.
  - **Filter criteria** Alerts and events can be filtered by numbers and by dates. Or, you can enter a string that must be found in the name of an entry to qualify the entry to display in the table. The string can contain the Percent sign (%), Asterisk (*), or Question mark (?) wildcard characters.
- **Hide Filter Row**. Hides the dialog box for specifying the resources to view in the table.
- **Clear All Filters**. Clears all filter changes and restores the default table display.
- **Edit Sort**. Specify up to 3 columns from the list to sort the list by.
- **Clear All Sorts**. Clears all sort changes and restores the default table display.

- **Collapse Table**. Collapses all the table entries, so you can more easily work with the detailed definition pages that display beneath the table. For example, you may find it convenient to use this control after you have selected a definition to Modify (such as a Persons, Groups, or Escalations definition). This eliminates the need to scroll to the bottom of the display. When collapsed, the table displays only its status row, which indicates `Selected: 1`.
- **Expand Table**. Expands all the collapsed table entries.

Searching

Listed under the **Select Actions** control (to the right of the ″table actions″ buttons) are the same ″Table Actions″ that are available as buttons, plus one additional **Show find toolbar** control. It provides a fairly sophisticated search facility.

Select **Show find toolbar** then click **Go** to produce a dialog box in which you can specify the exact text to Search for, as well as these search criteria.

- Condition for matching the search text (such as: Contains, Starts with, Ends with, or Exact match.)
- Column in which to search, or search across all columns.
- Direction in which to search.
- Whether or not to Match case for the search.

Specify the search criteria, then click **Find** to highlight the first item that matches your search criteria. Click **Find** again to highlight the next match.

To make the find toolbar bar go away, select **Hide find toolbar** (listed under the **Select Actions** control) then click **Go**.

Sort toggle buttons

Where supported, the column headings in the table are followed by icons for sort ascending (^) and sort descending (v). By default, items such as names are sorted in descending order (alphabetically). To enable another sorting order, click the icons for the column that you want to sort. (If the numbers 1, 2, or 3 also appear in the columns headings, then the **Edit Sort** table action is in use.)

List navigation

The last line of the table allows navigation throughout the list by supporting:

- Next and previous buttons for moving through the list
- Going to a specific page in the list
- Running counts of entries indicate the number of Total entries, Filtered entries, Displayed entries, and Selected entries in the table.

Configuring your Web browser

To correctly display SA IOM alert escalation in your Web browser, the following settings are required:

- JavaScript™ must be enabled in all Web browsers.
- For Microsoft Internet Explorer, the following settings are required:
  - Set the security level to medium.

    Do not set the security level to high. If high security is required, ensure that the entry **ActiveX controls and plugins - Initialize and Script ActiveX**

controls not marked as safe on the Security settings page is set to **Enable**. Otherwise, the information displayed on the console is not updated automatically.

– Set **Scripting - Active Scripting** to **Enable** on the Security settings page. Otherwise, navigating the console is not possible.

Troubleshooting SA IOM alert escalation

To turn debug mode on or off, and read the trace log file for the SA IOM alert escalation feature, perform these steps.

1. Ensure that at least one of the SA IOM Alert Escalation User Interface panels was started within the ISC (that is, a page was requested from the ISC navigation menu). Otherwise the Application Server won't list the SA IOM Alert Escalation User Interface as a running component (see step 4)
2. Navigate to the Logging and Tracing page by clicking on the **Log and Trace** link within the Troubleshooting ISC menu item.
3. In the Server table select the appropriate server (for instance server1) and in the General Properties section click on the **Change Log Detail Levels** link.
4. Change to the Runtime tab where you should see a list of running components and the tree item `com.ibm.saiom.*` represents the SA IOM Alert Escalation User Interface. Click the latter with the left mouse button to obtain the following options from the context menu:
   - No Logging (simply turn of logging)
   - Messages Only (only messages are displayed in the log trace file)
   - All Messages and Traces (to gather all messages and traces this is the right option to select)
   - Message and Trace Levels (specify a certain message and trace level)
5. Click the **Ok** button to save the changes.
6. Finally change to the `<YOUR_EWAS_ROOT_DIR>\profiles\<YOUR_PROFILE_NAME>\logs\<YOUR_SERVER_NAME>` directory, which, per default is C:\Program Files\IBM\SA IOM\ewas\profiles\default\logs\server1 and open the `trace.log` file to see the log trace.

Part 5. Deprecated features

Chapter 18. Connecting to host systems . . . 199
Setting up mainframe 3270 hosts 199
IBM and Amdahl 3270 ports 199
Configuring IBM and Amdahl 3270 ports . . . 200
Cabling IBM and Amdahl 3270 ports 200
Configuring MVS on IBM/Amdahl mainframes 200
Amdahl 5995M support 200
Serial ports 200
Configuring serial ports 200
Cables and connectors 201
Cabling terms you should know 201
Cabling serial ports 202
Telnet and SA IOM 203
Testing TCP/IP Telnet on Windows 203

Chapter 19. Installing 3270 Emulation Adapters 205
Setting up 3270 adapters for SA IOM 205
Summary of installing 3270 adapters 205
Supported 3270 adapters 205
Which 3270 adapter should I use? 206
Extended attribute bytes. 206
Multiple logical terminals (MLT) 206
Installing adapters in an ISA bus machine 206
Summary of steps 207
Notes about ISA 3270 adapters 207
IBM 3270 adapters (ISA bus) 208
Attachmate advanced 3270 adapters (ISA bus) . . 208
IRMA 3t adapters (ISA bus) 210
IRMA 3t adapters in IRMA mode (ISA bus) . . 210
IRMA 3t adapters in IBM mode (ISA bus) . . . 210
Installing adapters in a PCI bus machine 211
Installing Attachmate IRMA PCI adapters . . . 212
Installation 212
Ordering of PCI cards 212
Configuring 3270 PCI adapters for SA IOM . . . 213
How SA IOM assigns PCI slots to 3270 sessions 213
Physical versus detected PCI slot order. . . . 214
Determining the detected PCI slot order . . . 216
Additional notes 217
Problem resolution 217

Chapter 20. Keyboard Support 219
Windows NT 122-key keyboards 219
122-key keyboard layout DLLs 219
122-key keyboard features 219
Japanese 106-key keyboard support 220
Configuring 122-key keyboards 220
Configuring SA IOM client to use 122-key keyboard 220
TN3270E keyboard support. 221

Chapter 18. Connecting to host systems

This chapter describes how to connect to host systems. Two main categories of hosts are IBM/Amdahl and non-IBM. Setting up either category requires you to attach cables or modems and to configure ports. Setting up IBM/Amdahl mainframes also requires you to configure MVS.

Topics in this chapter

The following topics are discussed in this chapter:

- "Setting up mainframe 3270 hosts"
- "Configuring MVS on IBM/Amdahl mainframes" on page 200
- "Amdahl 5995M support" on page 200
- "Serial ports" on page 200
- "Telnet and SA IOM" on page 203

Setting up mainframe 3270 hosts

This section describes how to set up mainframe 3270 hosts. SA IOM supports hardware consoles for the following mainframe models.

- IBM 3090
- IBM 308*x*
- IBM 43xx
- ES/9000 (water-cooled)
- Amdahl 5880
- Amdahl 5890
- Amdahl 5995M
- Hitachi EX/CF
- Any non-IBM computer that supports an ASCII terminal, HP 2392 terminal, VT100 terminal, VT220 terminal, VT420 terminal, or Telnet

Non-IBM computers communicate only through serial ports. The other IBM and Amdahl mainframes listed above communicate with SA IOM using 3270 adapters.

TN3270E connections such as those to the IBM 2074 Console Support Controller, are discussed in the chapter, Chapter 13, "Configuring TN3270E sessions," on page 121.

IBM and Amdahl 3270 ports

You can connect the server's 3270 adapters to any console or terminal port on the mainframe. Typically, there are 3270 adapters connected to the hardware console and the MVS console. Additional adapters may service VTAM applications or applications with dedicated terminals, such as OMEGAMON.

A typical server with four 3270 adapters may be connected to:

- A system hardware console (Session A)
- An MVS console (Session B)
- A VTAM application terminal (Session C)

- An OMEGAMON console (Session D)

Configuring IBM and Amdahl 3270 ports

When setting up mainframe ports for use with SA IOM, configure the port as if it were going to be attached to the type of console you are emulating, such as an MVS console. The port must be configured as a (327*x*) 3278 or 3279 Model 2 or Model 4 terminal in CUT mode. DFT mode is not supported.

Cabling IBM and Amdahl 3270 ports

Use 3278-type coaxial cables to connect the mainframe ports to the server's 3270 adapters.

Caution
SA IOM supports connecting or removing coaxial cables while the server is running, but make sure that you vary the terminal offline ("v term_id offline") before removing the coaxial connection. The manufacturers advise to always make sure the PC in which the adapters are installed is turned off, otherwise the emulation adapters may be damaged.

Connecting mainframe cables can be an involved process, so you should refer to your hardware documentation when doing this. If you have any doubts, consult your hardware support representative.

Configuring MVS on IBM/Amdahl mainframes

This section provides information on configuring MVS on IBM/Amdahl mainframes.

Set the MVS console ports used by SA IOM to roll-deletable display mode using the following command:

```
K S,DEL=RD,SEG=10
```

Refer to your mainframe documentation for details.

Amdahl 5995M support

This section provides special instructions on SA IOM's support of the Amdahl 5995M.

For model 4 support, the 5995M must use a 3270 adapter that supports extended attribute bytes (EABs). See "Extended attribute bytes" on page 206.

Serial ports

This section provides information on serial ports.

Serial ports on the server that are configured for use by SA IOM can be connected to any RS-232C serial port on the host computer. You can connect the ports either with modems or directly with a null-modem cable.

Configuring serial ports

An SA IOM serial port can support several values for the baud rate, parity, data bits, and stop bits.

When configuring your computer's serial ports to communicate with the SA IOM server, use any of the following values. The default SA IOM values are underlined:

Settings	Values
Baud Rate	1200, 9600, 14400, 19200, 38400, 57600, 115200
Parity	Even, Odd, Mark, Space, or None
Data Bits	7 or 8
Stop Bits	1 or 2
Flow Control Type	None, RTS/CTS (hardware handshaking), or XON/XOFF (software handshaking)

Cables and connectors

Cables are the most common source of modem connection problems with SA IOM. If you are having trouble with your modem connection, try replacing your cable with a known working cable, or check the signals with a breakout box.

Cabling terms you should know

You should be familiar with the following terms.

Cabling terms	Descriptions
DB-9 and DB-25	The connector for the serial communications cable, the computer, the modem, and any terminals will have either 9 or 25 pins, in two rows. You may also see the letters P or S, as in DB–25P. The letters stand for **pin** (male connector) or **socket** (female connector).
DTE	Data Terminal Equipment. The serial-communications device that sends data on Pin–2. The serial ports on most computers are configured as DTE, with either a 9–pin or 25–pin male connector.
DCE	Data Communications Equipment. The serial-communications device that sends data on Pin–3. Most modems are configured as DCE, with a 25–pin female connector. Normally one DTE device is connected to one DCE device. To connect two similar devices together, use a "null modem" cable or connector.
RS–232	The formal name (with associated electrical specifications) for a serial communications port.
RS–422	A serial communications protocol that can be converted to RS–232 with an inexpensive adapter. RS–422 supports much longer transmission wires than RS–232 does.

Wiring diagrams in this chapter use the following pin assignments.

Pin	Assignment
TD	Transmit Data, an outbound signal
RD	Receive Data, an inbound signal
DCD	Data Carrier Detect, an inbound signal
DTR	Data Terminal Ready, an outbound signal
RTS	Request to Send, an outbound signal
CTS	Clear to Send, an inbound signal
SG	Signal Ground, a reference signal
NC	No Connection
DSR	Data Set Ready, an inbound signal
RI	Ring Indicator, an inbound signal not used by SA IOM

Cabling serial ports

Your computer will have either a DB-9P or DB-25P connector (both male) for the serial port. The DB-25S (female) connector you may see is for the printer parallel port.

If you are directly cabling the server to a non-IBM computer, or if you are directly cabling two PCs together, you will need to build or purchase a null modem cable that can support full-handshaking of the control lines.

And you will probably also need to Enable the Telnet server as described in Server Profile.

The following diagrams show the wiring connections necessary for full-handshake null modem connectors of various types.

DB-25 Pin	Signal			DB-25 Pin
2	TD	-	RD	3
3	RD	-	TD	2
4	RTS	-	CTS	5
5	CTS	-	RTS	4
6,8	DCD	-	DTR	20
20	DTR	-	DCD	6,8
7	SG	-	SG	7

Figure 2. Wiring Diagram, DB-25 to DB-25 null modem pin-outs

DB-9 Pin	Signal			DB-9 Pin
2	RD	-	TD	3
3	TD	-	RD	2
1,6	DCD	-	DTR	4
4	DTR	-	DCD	1,6
7	RTS	-	CTS	8
8	CTS	-	RTS	7
5	SG	-	SG	5
9	NC	-	NC	9

Figure 3. Wiring Diagram, DB-9 to DB-9 null modem pin-outs

DB-9 Pin	Signal			DB-25 Pin
1	DCD	-	DTR	20
2	RD	-	TD	2
3	TD	-	RD	3
4	DTR	-	DCD	6,8
5	SG	-	SG	7
6	DSR	-	NC	
7	RTS	-	CTS	5
8	CTS	-	RTS	4
9	RI	-	NC	

Figure 4. Wiring Diagram, DB-9 to DB-25 null modem pin-outs

DB-9 Pin	Signal			DB-25 Pin
1	DCD	-	DCD	8
2	TD	-	TD	3
3	RD	-	RD	2
4	DTR	-	DTR	20
5	SG	-	SG	7
6	DSR	-	DSR	6
7	RTS	-	RTS	4
8	CTS	-	CTS	5
9	RI	-	RI	22

Figure 5. Wiring Diagram, DB-9 to DB-25 adapter cable

Telnet and SA IOM

This section provides information on SA IOM's support of Telnet sessions. The SA IOM server supports Telnet session types to connected host systems.

Testing TCP/IP Telnet on Windows

If you experience difficulty connecting the SA IOM server to a Telnet host, a good troubleshooting technique is to ensure that you can establish a Telnet session to the named host using the Windows Telnet Client.

Open a command prompt and enter "Telnet" then enter "?" for more about how to use this command line utility to supply the host name, then launch the session.

An inability to establish a session in this way may indicate that the Telnet host is not active or that your TCP/IP configuration is not complete or that there is a firewall between that is blocking communication.

Chapter 19. Installing 3270 Emulation Adapters

This chapter provides information on installing 3270 emulation adapters. For information on implementing TN3270E support, see the chapter entitled Chapter 13, "Configuring TN3270E sessions," on page 121.

Topics in this chapter

The following topics are discussed in this chapter:

- "Setting up 3270 adapters for SA IOM"
- "Installing adapters in an ISA bus machine" on page 206
- "IBM 3270 adapters (ISA bus)" on page 208
- "Attachmate advanced 3270 adapters (ISA bus)" on page 208
- "IRMA 3t adapters (ISA bus)" on page 210
- "Installing adapters in a PCI bus machine" on page 211
- "Configuring 3270 PCI adapters for SA IOM" on page 213

Setting up 3270 adapters for SA IOM

Installing 3270 emulation adapters in the server is one of the most involved parts of customizing SA IOM. You must install hardware, cable the PC to the mainframe host, and configure the server itself.

Due to the wide variety of hardware used and supported by SA IOM, it is not feasible to give detailed instructions about installing each item. Instead, this section covers only the information you will need to properly set up each item for use with SA IOM. You must refer to your hardware documentation for detailed instructions on installation.

Summary of installing 3270 adapters

Here's a summary of the steps involved to install 3270 adapters:

1. All 3270 emulation adapters use 3278-type coaxial cables to connect mainframe ports to the adapters installed on the server. These 3270 cables should already be connected at the mainframe end.
2. Turn off the server, open it up, and install all the 3270 adapters you plan to use. More detailed instructions are listed later in this chapter for the ISA bus type.
3. Connect the mainframe coaxial cables to the 3270 adapters.

   Note: When connecting or removing cables to 3270 adapters, the manufacturers advise to always make sure the server PC is turned off. Otherwise, the emulation adapters may be damaged. The same holds true for any mainframe consoles or terminals you may choose to disconnect.
4. Configure the SA IOM software following the steps described in Chapter 6, "Administering SA IOM software," on page 55.

Supported 3270 adapters

SA IOM supports 3270 emulation adapters of the following types.

- **On the ISA bus:**

  - Attachmate Advanced 3270 Adapter/2.
  - IBM 3270 Connection (Version A and B).
  - IRMA 3t 3270 Coax Adapter.
- **On the PCI bus:**
  - Attachmate IRMA PCI adapter (CIP-based)

Important: See "Which 3270 adapter should I use?"

Which 3270 adapter should I use?

Notes about the supported 3270 emulation adapters include:

- SA IOM supports up to eight 3270 coaxial connections. Some exceptions are noted in this chapter.
- The Attachmate - Advanced 3270 adapter (ISA bus) and the IBM 3270 adapter (ISA bus) are easier to install than the IRMA 3t (ISA bus) adapter because fewer settings and no vender-support files are required. The Attachmate IRMA PCI Adapter is the easiest adapter to install.
- To avoid hardware conflicts with other adapters, it is sometimes necessary to use a mix of vendors' adapters.
- IBM 3270 adapters and IRMA 3t adapters running in IBM mode do not support extended attribute bytes.

Extended attribute bytes

Extended attribute bytes (EABs) allow SA IOM user applications running on a PC to appear as if they were running on a 3179 terminal, making increased color combinations and reverse video data displays possible. The Attachmate Advanced 3270 Adapter/2, the IRMA 3t adapter, or the Attachmate IRMA PCI adapter is required for extended attribute support.

EAB detection is specified when you configure a 3270 emulation adapter. Automatic detection of EAB support and a 15-second delay (maximum) are the defaults.

Multiple logical terminals (MLT)

If you use multiple logical terminals (MLT) on one 3270 adapter, a menu pull-down control enables you to toggle between sessions.

- On the 3270 Special Keys menu pull-down, choose the **ChgSc** key to toggle between sessions.
- On an IBM 101-enhanced keyboard, the sequence is **Ctrl+PageUp.**

Installing adapters in an ISA bus machine

This section describes how to install adapters in an ISA bus machine.

An IBM PC/AT-compatible computer uses an industry-standard architecture (ISA) bus. Make sure that the adapters you are installing are designed for the ISA bus.

You will need the following items before you start:

- Documentation provided with your computer
- Adapters you plan to install
- Documentation provided with your adapters

Summary of steps

To install 3270 adapters in an ISA bus machine, you must perform the following steps. Refer to the documentation for your computer and each adapter for installation instructions. Also, you should carefully read the subsections following this summary, for special notes that affect operation with SA IOM.

Warning:
There are hazardous high-voltage areas inside the machine that can cause severe injury or death. Always unplug the computer before removing the cover.

1. Start the Windows NT® Diagnostics program, available from the **Administration Tools** menu, and select the **Resources** tab. Write down your I/O port and memory usage. Make sure all the dip switch settings you will set for your ISA adapters are not conflicting with the current system usage.

   SA IOM comes with a device driver `rp3270.sys`. This driver is installed in your Windows NT `system32` drivers directory. Use the **Devices** icon in the **Control Panel** to make sure `rp3270.sys` is installed and started properly.
2. Turn off the computer, unplug it, and remove its cover.
3. If needed, set switches on each adapter being installed.
4. Plug the adapters into the computer's expansion slots. The adapters do not have to be in any particular order.
5. Replace the computer's cover.

Notes about ISA 3270 adapters

All the ISA 3270 adapters use a set of switches to configure the adapter's port and register address. You need to manually set these switches so each adapter uses a different address.

IBM 3270 adapters (ISA bus)

This section provides information on the switch settings for IBM 3270 adapters.

Set the switches on each IBM 3278/79 adapter according to either Table 17 or Table 18. Older Version A IBM adapters have 8 dip switches, newer Version B adapters have 4 dip switches. It may help to mark each adapter with the numbers 1-4 before you change the switches. Also, you may have to use a razor knife to strip the cover off of the switch pack.

Table 17. Version A, IBM 3278/79 adapter sample switch settings (ISA bus)

Board	Switch Number							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	ON	ON	ON	OFF	ON	OFF	ON	ON
2	OFF	ON	ON	OFF	OFF	OFF	ON	ON
3	ON	OFF	ON	OFF	OFF	OFF	ON	ON
4	OFF	OFF	ON	OFF	OFF	OFF	ON	ON

Table 18. Version B, IBM 3278/79 adapter sample switch settings (ISA bus)

Board	Switch Number			
	1	**2**	**3**	**4**
1	ON	ON	OFF	ON
2	OFF	ON	OFF	ON
3	ON	OFF	OFF	ON
4	OFF	OFF	OFF	ON

The matching configuration settings for the IBM adapters in either of the previous tables are as follows:

Table 19. Configuration settings for IBM (ISA bus)

Board	Register Location	Memory Address
1	02D0 (IBM)	CE000
2	06D0 (IBM)	CA000
3	0AD0 (IBM)	CC000
4	0ED0 (IBM)	D0000

Attachmate advanced 3270 adapters (ISA bus)

This section provides information on switch settings for Attachmate Advanced 3270 adapters.

Set the switches on your Attachmate Advanced adapter according to one of the following two tables.

If you have a "newer" version of the Attachmate cards (shipped since April 1997), use Table Table 20 on page 209. If you have an earlier version of the Attachmate adapter, use Table 21 on page 209.

The "newer" version of the Attachment adapter has different DIP switch settings than earlier versions. Unlike previous versions whose RJ11 polarity is controlled by a slide switch, the "newer" version controls this function using DIP switch 1. The switch functions are different from previous versions. See Table 22 for the newer functions and the Attachmate documentation for more information.

Table 20. Attachmate adapter sample switch settings (ISA bus) - "newer"

Board	**Switch Number**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	OFF	OFF	OFF	OFF	OFF	ON	N/A	N/A	OFF	OFF
2	OFF	OFF	OFF	OFF	ON	ON	N/A	N/A	ON	OFF
3	OFF	OFF	OFF	ON	OFF	ON	N/A	N/A	ON	OFF
4	OFF	OFF	OFF	ON	ON	ON	N/A	N/A	ON	OFF

In Table 20 and Table 21, N/A means the switch does not affect SA IOM and can be set either to ON or OFF.

Table 21. Attachmate adapter sample switch settings (ISA bus) - previous

Board	**Switch Number**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	N/A	N/A
2	OFF	OFF	OFF	OFF	ON	OFF	ON	ON	N/A	N/A
3	OFF	OFF	OFF	ON	OFF	OFF	ON	ON	N/A	N/A
4	OFF	OFF	OFF	ON	ON	OFF	ON	ON	N/A	N/A

The functionality of DIP switches 6 through 10 is different for "newer" and older Attachmate models. Functions are shown in the following table:

Table 22. DIP switch functions for Attachmate (ISA bus)

New adapter	**Function**	**Old adapter**
Switch 1	RJ11 polarity control	Slide switch
Switch 2	Interrupt 2 enable	Switch 2
Switch 3	IBM function enable	Switch 3
Switch 4	IBM I/O register low	Switch 4
Switch 5	IBM I/O register high	Switch 5
Switch 6	IRMA function enable	Switch 8
Switch 7	IRMA I/O register low	Switch 9
Switch 8	IRMA I/O register high	Switch 10
Switch 9	Power up memory enable	Switch 7
Switch 10	Power up comm enable	Switch 6

The register and memory addresses for "newer" and older Attachmate models are shown in the following table.

Table 23. Configuration settings for Attachmate (ISA bus)

Board	Register Location	Memory Address
1	02D0 (Attachmate)	CE000
2	06D0 (Attachmate)	CA000
3	0AD0 (Attachmate)	CC000
4	0ED0 (Attachmate)	D0000

IRMA 3t adapters (ISA bus)

This section provides information on IRMA 3t adapters.

The example IRMA configurations that follow are a few of many possible setups. The switch settings for each IRMA adapter (which set the register location) must be unique. A legend of possible switch settings is in the manual that accompanies your adapter.

IRMA 3t adapters in IRMA mode (ISA bus)

The following is an example of IRMA 3t adapters running in IRMA mode on the ISA bus. To begin, set the switches on each adapter to set the register locations. An example is shown in Table 24.

Table 24. IRMA 3t adapter switch settings (ISA bus)

Board	Switch Number			
	1	**2**	**3**	**4**
1	ON	ON	ON	ON
2	ON	ON	ON	OFF
3	ON	ON	OFF	ON
4	ON	ON	OFF	OFF
5	OFF	ON	ON	ON
6	ON	OFF	ON	ON
7	OFF	ON	ON	OFF
8	OFF	ON	OFF	ON
9	OFF	ON	OFF	OFF
10	ON	OFF	ON	OFF
11	ON	OFF	OFF	ON
12	ON	OFF	OFF	OFF
Note: This sets adapters to register locations 280, 680, A80, E80, 2AO, 2C0, 6A0, AA0, EA0, 6C0, AC0, and EC0 respectively.				

The File field in the IRMA 3t configuration panel specifies a valid IRMA 3t microcode file `IRMA3t.dnl`. This file ships with the adapter installation diskette or you can download this file from the Attachmate Web site. You must specify the full path of this file. For example, `e:\winnt40\system32\irma3t.dnl`.

IRMA 3t adapters in IBM mode (ISA bus)

If necessary, and if your ISA bus machine's IBM registers are not already occupied by IBM emulation adapters, multiple IRMA 3t adapters can be accessed in IBM

mode through the SA IOM server configuration (though EABs are not supported in this mode). To access IRMA 3t adapters in IBM mode on an ISA bus machine, set the switches on each IRMA adapter to IBM register locations.

In the SA IOM IRMA 3t configuration, IBM Mode needs to be checked. IBM register locations are not documented by DCA, but the corresponding register locations are as follows:

Use IRMA adapter switch settings for:	To match IBM register:
280	2D0
680	6D0
A80	AD0
E80	ED0

Example switch settings for the IRMA adapters are shown in Table 25.

Table 25. IRMA 3t adapter sample switch settings-alternate (ISA bus)

Board	Switch Number			
	1	**2**	**3**	**4**
1	ON	ON	ON	ON
2	OFF	ON	ON	OFF
3	ON	ON	OFF	ON
4	ON	ON	OFF	OFF
Note: This sets adapters 1 through 4 to register locations 280, 680, A80, and E80 respectively.				

The last step to configure an IRMA 3t adapter in IBM mode on an ISA bus machine is performed on the IRMA 3t Convertible Properties panel in the SA IOM host session configuration. The corresponding configuration settings for the IRMA 3t adapter switch settings in Table 26 are as follows:.

Table 26. Configuration settings for IRMA 3t in IBM mode (ISA bus)

Board	Register Location	Memory Address
1	02D0 (IBM)	CE000
2	06D0 (IBM)	CA000
3	0AD0 (IBM)	CC000
4	0ED0 (IBM)	D0000

Installing adapters in a PCI bus machine

This section provides information on installing adapters in a PCI bus machine.

PCI stands for Peripheral Component Interconnect, a type of bus. The PCI bus is a newer design than the ISA bus.

PCI adapters choose an unused memory address for you, thus relieving you of this task.

SA IOM supports the Attachmate IRMA PCI adapter (CIP-based), a 3270 adapter made for the PCI bus.

Installing Attachmate IRMA PCI adapters

Older Attachmate IRMA PCI adapters use an API (Divine-based) that is not supported by SA IOM. Unfortunately, these older adapters have the same name as the supported (CIP-based) adapter. When ordering the PCI adapter, you should explicitly request the Revision B version, which has an SFS-prefixed serial number.

To verify that your Attachmate IRMA PCI adapter is supported by SA IOM, locate the serial number label on the outside of the finished product, on the top flap under the UPC code. The label will have a barcode and the words **Product SN (S) SFSE000000.**

Another method to determine if the correct board assembly was included, would be to check the date on the kit label on the bottom of the box. The third line is the date code: anything after August 22, 1997 includes the new assembly.

The software verification method is to check the PCI Configuration register "Device ID" (at PCI Configuration address 02h). The SA IOM-supported IRMA PCI (CIP-based) adapter returns a value of 0001h when queried.

Installation

All 3270 PCI interfaces are included with SA IOM. No additional software is required.

See the adapter product documentation for installation and basic configuration instructions. Read the adapter documentation before proceeding.

Ordering of PCI cards

The PCI slot number is the relative slot number occupied by a recognized 3270 PCI card. PCI slot assignments must be sequential beginning from 1, and they must reflect the relative ordering of recognized PCI 3270 cards in the machine.

In general, choose physical slot 1 to be the one closest to the CPU chip. However, the actual order is what the operating system delivers when you ask it for an enumeration of the PCI devices.

It is recommended that the PCI slots be filled in order without any physical gaps.

Following is an example that illustrates what can happen when multiple cards are installed.

Physical PCI Slot	Card Type PCI	Slot Number
1	Empty	-
2	3270 PCI card	1
3	Empty	-
4	3270 PCI card	2

If you install a third 3270 PCI card in physical slot 3, SA IOM will interpret the session order as follows:

Physical PCI Slot	Card Type PCI	Slot Number
1	Empty	-
2	3270 PCI card	1
3	New 3270 PCI card	2
4	3270 PCI card	3

SA IOM would expect the second card's host session to be assigned a PCI slot number of 2, and the PCI slot number of the third 3270 PCI card's host session to be changed from 2 to 3.

However, you can define the order as follows:

Physical PCI Slot	Card Type PCI	Slot Number
1	Empty	-
2	3270 PCI card	1
3	New 3270 PCI card	3
4	3270 PCI card	2

In this case, SA IOM will assign the new host session to the card in physical slot 4, and the host session that was previously mapped to the card in physical slot 4 will be mapped to the new card in physical slot 3.

Configuring 3270 PCI adapters for SA IOM

This section provides information on configuring PCI adapters, explaining how PCI slots are assigned by SA IOM and how to overcome problems you may encounter during configuration.

How SA IOM assigns PCI slots to 3270 sessions

The 3270 PCI adapters are conceptually simple to install because the adapters do not require memory addresses or device registers. However, you may encounter problems determining which adapters correspond with which 3270 sessions because of one or more of the following reasons.

- PCI adapters are sometimes assigned to SA IOM 3270 sessions in a non-intuitive order, due to the behavior of Windows NT and the underlying PCI BIOS.
- The physical order in which the adapters reside in the box is often not the same order in which SA IOM assigns 3270 sessions.
- Some vendors imprint numbering on the physical slots (especially for server-class PCs).
- SA IOM, in its configuration interface, asks you for the session's PCI slot number.

When SA IOM asks for the session's PCI slot number it is asking for the PCI detected slot number. It does not mean the actual physical slot number, although sometimes they are the same.

SA IOM has to query Windows NT to give it the installed PCI adapters one by one. The order that Windows NT returns each installed PCI adapter may or may not match the physical order of the PCI adapters in the box, and SA IOM has no way of guessing the relationship between the detected order and the actual physical order.

Following are steps that describe how SA IOM assigns PCI adapters to 3270 sessions.

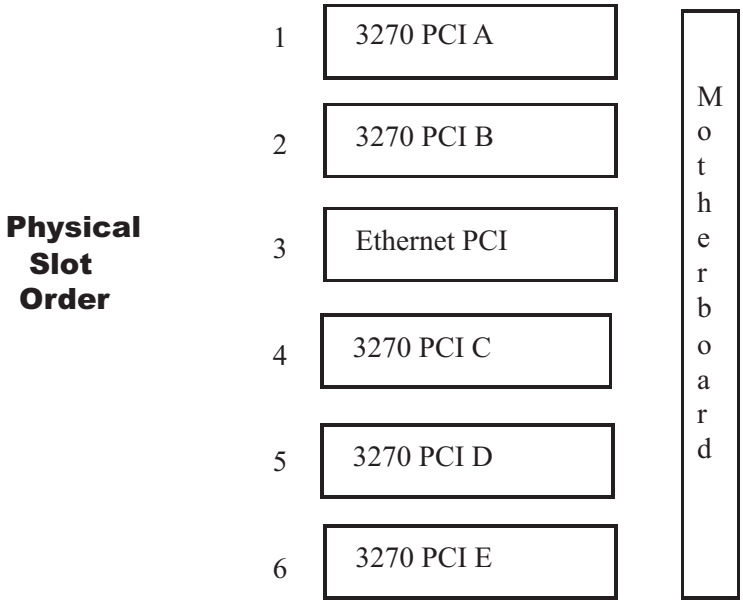
1. When the SA IOM server is started, it reads its server configuration data from *rpserver.dat*. The 3270 sessions are listed in the server configuration in the same order that they are defined and modified. When you modify the properties of a host session, it goes to the top of the list. This does not affect PCI assignment order.
2. When SA IOM starts a 3270 PCI session, it builds a list of 3270 PCI adapters by asking Windows NT to give it the first PCI device on PCI bus 0, then the second, the third, and so on until Windows NT tells it there are no more devices on PCI bus 0. It then does the same thing for PCI bus 1, PCI bus 2, and so on until Windows NT tells SA IOM there are no more PCI buses.

   When SA IOM gets back information about a PCI device, it checks to see if it is a supported 3270 adapter. If so, SA IOM adds it to a list it builds. Otherwise, it is discarded (this means you never have to worry about the order or placement of non-3270 PCI adapters in your box). The result of this detection process is that SA IOM has a list of 3270 PCI devices.
3. SA IOM starts its configured host sessions in the same order that they appear in the session list. For a given 3270 PCI host session, it takes the configured PCI slot number and then assigns the session to the adapter at that same position in the adapter list.

For example, if you assigned PCI slot 1 to the host session, then SA IOM would assign the session to the first PCI adapter in its list. If you assigned PCI slot 5 to the host session, then it would assign the session to the fifth PCI adapter in its list.

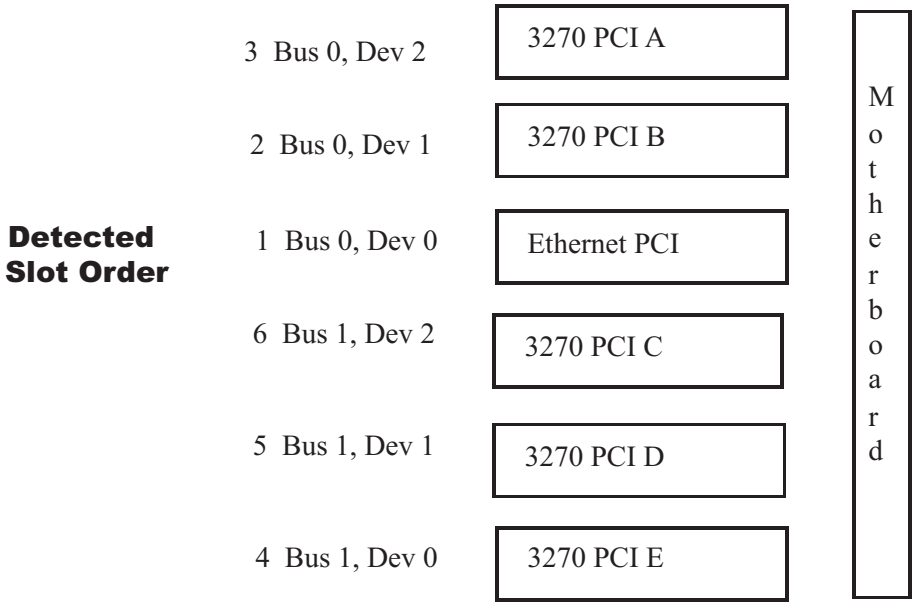
Physical versus detected PCI slot order

Following is an example showing a set of physical PCI slots.



In this example, assume that this is what the inside of your SA IOM server box looks like after you insert all of your 3270 PCI adapters. You would think that the PCI adapter in physical slot 1 (3270 PCI A) would be assigned to the host session you configured as PCI slot 1, the PCI adapter in physical slot 2 (3270 PCI B) would be assigned to the host session configured as PCI slot 2, and so on. However SA IOM does not assign PCI slots following physical slot order.

The following example shows how the PCI BIOS (and the Windows Hardware Abstraction Layer) might identify the adapters.



Following is the order the adapters are returned to SA IOM and what SA IOM does with each adapter.

- The first adapter returned is the one in physical slot 3 (Bus 0, Dev 0), the Ethernet PCI adapter. Since this is not a 3270 PCI adapter, SA IOM skips it.
- The second adapter returned is the one in physical slot 2 (Bus 0, Dev 1), the 3270 PCI B adapter. This is a 3270 PCI adapter, so SA IOM adds it as the first entry to its list of 3270 adapters. SA IOM does not know that the adapter is in physical slot 2, only that it is (Bus 0, Dev 1).
- The third adapter returned is the one in physical slot 1 (Bus 0, Dev 2), the 3270 PCI A adapter. This is also a 3270 PCI adapter, so SA IOM adds it as the second entry to its list of 3270 PCI adapters.
- The fourth adapter returned is the one in physical lot 6 (Bus 1, Dev 0), the 3270 PCI E adapter. It is added as the third entry in the 3270 PCI adapter list.

When the detection process completes, SA IOM has the following list of 3270 PCI adapters.

1. 3270 PCI B
2. 3270 PCI A
3. 3270 PCI E
4. 3270 PCI D
5. 3270 PCI C

Using this list, SA IOM takes the PCI slot number from the configured host session and assigns it to the corresponding 3270 adapter. For example, if you defined PCI slot 1 for a host session, it would be assigned to the adapter 3270 PCI B (which happens to be in physical slot 2). If you defined PCI slot 4 for a host session, it would be assigned to the adapter 3270 PCI D (which happens to be in physical slot 5).

Keep in mind that:

- Non-3270 PCI adapters are skipped, so it does not matter where you place them
- 3270 ISA adapters are handled separately, so it does not matter if you place them in shared ISA/PCI slots

Determining the detected PCI slot order

To determine the actual PCI slot order that SA IOM uses to assign host sessions, you can go to your vendor Web site and look to see if there is technical support information that describes the slot order (COMPAQ provides a white paper on the subject). Or you can experiment until you figure it out.

Use the following process to experiment and document how to determine SA IOM's actual PCI slot order.

1. Make sure you are satisfied with the PCI slot numbers you assigned to you 3270 host sessions. The slot numbers you assigned should be sequential, starting from 1.
2. Unload all the 3270 PCI adapters that you plugged into you box except one, which should be positioned at one extreme end of the physical slots or the other (ignoring non-3270 PCI adapters). You might choose the slot closest to the motherboard or to the CPU chip, or the slot physically labelled as the first slot.
3. Disable all 3270 host sessions in the SA IOM server configuration, except the one to which you assigned PCI slot 1. This will result in SA IOM only attempting to start one 3270 PCI session.
4. Attach a live coax cable to the single 3270 PCI adapter and boot the PC. Start the SA IOM server and client. Verify that the host session opened okay. If it didn't and you followed steps 1-3 correctly, then you have a hardware or 3270 device driver problem that you'll need to resolve. Do not continue with the additional boards.
5. If your host started okay, connect to the server from a client and select the host session. To get the first display buffer from the host 3270 controller, enter a keystroke (for example, the tab character). If the intended display does not appear, then you have a 3270 problem. Check to see that the 3270 connection is active.
6. If you have the first adapter working, try the second adapter. Enable the SA IOM host session to which you assigned PCI slot 2, save the confirmation, and then shutdown the machine. Insert the second adapter into the slot next to the first adapter (or the closest available slot). Reboot the machine and restart the server.
7. Select both sessions and inspect the display. See if the host session that originally appeared for the adapter assigned PCI slot 1 still remains, or if it was swapped with the second session. (If your machine is like the one in the above example, your sessions would be swapped.)
8. You now know the slot ordering for one of your PCI buses. Continue adding PCI adapters and enabling additional 3270 sessions one by one. At some point, you will span a PCI bus boundary and detect a new suborder.
9. Once you figure out and document the complete ordering sequence, edit the assigned PCI slot numbers for your configured 3270 sessions so that they correspond to the coax connections in the way you intended. To avoid confusion, wait and do this last so that you don't have to be continuously editing your PCI slot numbers.

Additional notes

Be careful when adding a new 3270 PCI card in between two other 3270 PCI cards or on a lower numbered bus. This will cause an insertion of the new adapter into the middle of the detected list of 3270 PCI adapters, and all the adapters following it in the list will be mapped to the wrong host sessions.

Problem resolution

If you need to contact IBM Support for help with a problem, you will need to collect the following information.

- PC vendor, make, and model
- The exact layout of adapters in the PC, including vendor, type, and so on
- SA IOM Server and Client version levels (from the **About** box)
- SA IOM Server STATE-level log capturing server startup

Also, you'll want to check that other PCI adapters installed on the machine work (modem, network, and so on). If they don't, it may mean that you have non-SA IOM-related problems due to faulty cables or due to a bad motherboard.

Chapter 20. Keyboard Support

This chapter provides information about SA IOM's support of 122-key keyboards and the Japanese 106-key keyboard.

Topics in this chapter

The following topics are discussed in this chapter:

- "Windows NT 122-key keyboards"
- "Configuring 122-key keyboards" on page 220
- "TN3270E keyboard support" on page 221

Windows NT 122-key keyboards

SA IOM supports four 122-key keyboards for Windows NT and the English (US) locale only.

- HOB Electronic Type 7
- IBM PC3270 #1393656 (old version, the top left keycap is "Help")
- IBM PC3270 #1397000 (newer version, the top left keycap is "Attn")
- Key Tronic KB3270PLUS

Note: This release does not support 122-key keyboards for Windows 95/98.

SA IOM supports the Japanese IBM 106-key keyboard.

122-key keyboard layout DLLs

For the IBM and Key Tronic keyboards, SA IOM provides keyboard layout DLLs for Windows NT on the SA IOM product CD.

HOB Electronic provides its own keyboard layout DLL for Windows NT, when you purchase the HOB keyboard.

Note: The HOB keyboard layout DLL is not supplied on the SA IOM product CD.

122-key keyboard features

The 122-key keyboards include the following features.

- The 122-key keyboard layout DLLs provide you with the full set of 3270 functions, when used with a 3270 session that SA IOM supports.
- The 122-key keyboard contains keycaps with multiple key functions. The black keycap legend is for 3270 emulation mode and the blue keycap legend is for Windows mode.
- You can continue to use the standard IBM-compatible 101/102-key Enhanced keyboard with SA IOM. The 101/102-key keyboard is defined as the default SA IOM client keyboard. No special configuration is required to use it.
- The keyboard gives standard Windows behavior when used with other Windows applications.

Japanese 106-key keyboard support

The Japanese 106-key keyboard type can be selected on the SA IOM Client Configuration Properties dialog.

The Japanese keyboard layout DLL is supplied as part of the Japanese version of Windows NT and should be installed using the keyboard applet in the Windows NT Control Settings panel.

Configuring 122-key keyboards

This section describes how to configure the SA IOM client to use a 122-key keyboard.

Configuring SA IOM client to use 122-key keyboard

When you install the SA IOM client, the keyboard layouts that SA IOM supplies are unloaded into a client subdirectory called `\keyboards`. As part of configuring the client to use the new keyboard, you install the keyboard layout into Windows using the Config Client dialog.

To configure your SA IOM client to use a 122-key keyboard, follow these steps:

1. Start Windows using your current keyboard.

   Note: You must logon to Windows as an administrator.
2. Open the SA IOM Client control window.

   You do not need to be connected to an SA IOM server to perform client configuration activities.
3. From the **Config** pull-down on the SA IOM client, select **Client**.

   Result: The **Client Configuration Properties** dialog displays.
4. Select the **General** tab to display the **General** page.
5. In the **Keyboard Layout** field, choose the desired keyboard layout from the pull-down list.

   The keyboard layout is a combination of a language locale and a physical keyboard type.
6. Click **OK** to save the client configuration changes.

   Result: Several confirmation and warning windows open.
7. Click **Yes** to all of the confirmations and warnings.

   Result: The keyboard layout DLL will be copied from the `\keyboards` subdirectory to the Windows NT system directory (usually `c:\winnt\system32`). The NT registry key for the English (US) locale will also be updated to point to this DLL.

   When the installation is complete, you will be notified to restart Windows NT. This will activate the keyboard layout DLL.
8. Power down your system and attach the 122-key keyboard. Depending on the keyboard connector style, you may need to use a PS/2-to-101 keyboard adapter.
9. Power up your system and log on.

   Result: When you log on, Windows determines the default locale from your personal preferences. Windows uses this information to locate and load your keyboard layout.

This installation does not affect your Windows Control Settings for keyboard type (under Keyboard) or input locale (under Keyboard or Regional Settings). The 122-key keyboards that SA IOM supports are compatible with your OEM-supplied keyboard.

You may reinstall your original 101/102 keyboard at any time, using the SA IOM Client Configuration Properties dialog.

TN3270E keyboard support

SA IOM's initial TN3270E support makes the following key assignments.

Table 27. 3270 key assignments in TN3270E emulation mode

3270 Key	**PC Keyboard Key**
Enter	Both the Enter key on the numeric keypad and the right Ctrl key may be used as the 3270 Enter key.
Erase EOF	The End key
Clear	See below
PA1	See below
PA2	See below
PA3	See below
Reset	The Esc key

For TN3270E implementation, the Clear, PA1, PA2, and PA3 keys should be invoked through the drop-down menu on the Client 3270 window. This is done with the menu item **3270 Special Keys**. The PA1 and PA2 keys may be mapped to specific keys by using the client profile, which is discussed in Appendix B, "Client profile," on page 231.

Part 6. Appendixes

Appendix A. SA IOM sample scripts

A number of SA IOM sample REXX programs and support subroutines are included with this application. These programs provide examples that demonstrate how to apply the IBM-supplied external REXX functions in programs that you develop. Some provide services, such as beeper paging and time acquisition. Others serve as coding examples only and are not supported as automation tools. These will be noted in the description.

In alphabetical order, the REXX scripts included with SA IOM are:

6530CONT.REX
6530CONT is an application-specific example of how to perform automation on a Tandem 6530 session. IBM does not support this program as an automation tool, it is an example program only.

AUTOEXEC.REX
This is a working program. AUTOEXEC is started by SA IOM automatically. It is normally used to perform product initialization services such as the following.

- Conditionally starts up a REXX program to automatically acquire accurate system time from the Automated Computer Telephone Service (ACTS), operated by the National Institute of Standards and Technology in Fort Collins, Colorado, USA. The default REXX program used here is TIME.REX, but you may substitute any other program when you configure the server.
- Conditionally starts up a program that may in turn initiate one or more occurrences of another program that scans host sessions defined as Beeper for WTORs generated by the Tivoli AF/OPERATOR BEEP command. When such a WTOR is encountered, this program generates a beeper page. The default REXX program used here is BEEP.REX, but you may substitute any other program when you configure the server.
- Looks for and, if found, calls the AUTOUSER.REX file. You should create a file called AUTOUSER.REX if you have custom initialization files or custom-made REXX scripts that you want to start at SA IOM startup.

  When AUTOEXEC.REX has completed these activities, it then terminates itself.

BEEP.REX
BEEP scans through all of the 3270-type emulation sessions searching for those which are specified as Beeper. For each of these an instance of WTORSCAN.REX is started. Once BEEP has completed these activities, it terminates.

BEEPCALL.REX
BEEPCALL monitors the progress of the current paging attempt. It attempts a beeper page up to 3 times.

BEEPQSHL.REX
The BEEPQSHL.REX script is a support subroutine that is required for some operating modes of WTORSCAN.REX. It is recommended that you do not make changes to this support subroutine.

Cursor.rex
The Cursor.rex script displays, for the selected emulator, the screen position of the cursor, the character at the cursor, and the color attribute of that screen position.

EmailReply.rex
The EmailReply.rex script is used by the SA IOM POP3 reader to reply to an e-mail.

Escalation.rex
The Escalation.rex script is a sample that demonstrates how to start an alert escalation using the SA IOM alert escalation feature. Note the alert escalation feature must be configured, and the escalation policy that you start using this sample must be defined and configured.

HMCACT.REX
This is a working program that performs activities with the Hardware Management Console (HMC). For a detailed description, see "HMCACT.REX automation interface program" on page 119. Scripts whose names begin with the letters HMC are described in Chapter 12, "SA IOM Hardware Management Console interface," on page 111.

HMCONS.REX
This is a working program that lets you view HMC hardware messages, software messages, and status changes. For more context, see Chapter 12, "SA IOM Hardware Management Console interface," on page 111.

HMCSTAT.REX
This is a working program that controls status monitoring and commands. It allows you to monitor the status of CPCs and their associated images, and issue commands to them. For more context, see Chapter 12, "SA IOM Hardware Management Console interface," on page 111.

INTERACT.REX
INTERACT demonstrates the use of a voice card as an interactive input device. (Interactive programs require keyboard input or input from another device.) The script waits for a specific message, then telephones a person, allowing that person to control the response interactively. The voice-assisted portion of this program requires installation of a supported voice card on the SA IOM server (see Voice Control).

INGRNIOM.REX
INGRNIOM receives a TCP/IP-based alert from a configured peer SA z/OS system. To receive such an alert, the SA IOM system must be configured as a peer also. Once INGRNIOM informs the calling program that it has received the alert, it terminates.

MCSSEND.REX

The MCSSEND.REX script is a support subroutine that is callable from another SA IOM script. It lets you send text strings to an MCS console session and ensures that the script is delivered free of errors. You can use this function instead of a call to AFR_SEND_3270() when the target of the string is an MCS console session.

- MCSSend guarantees delivery of text strings by monitoring the command line to make sure that it:
  - Contains an accurate copy of the command before emitting the HLLAPI code for SEND
  - Is cleared by the controller, indicating that the sent command was received by the controller

- If the command as displayed on the command line is corrupted, the MCSSend subroutine takes steps to correct, or clear and rewrite, the command before issuing the SEND HLLAPI code.
- The subroutine monitors the OAI line for various keyboard locked indicators. It then waits for the lock to clear or takes corrective action to clear the error locks.
- Assuming that all SA IOM REXX scripts use this script to provide the MCS command line interface, the subroutine serializes access to the MCS command line.

  An operator can restrict access to the REXX scripts by positioning the MCS command line cursor at least 1 space to the right or below the start of the first MCS command line. If the operator locks the console and forgets to unlock it, time-out logic allows the subroutine to eventually reclaim use of the command line.
- Programs using the AFR_SEND_3270 function calls include the various HLLAPI codes for pressing function keys, tabbing, SENDing, and so on. The subroutine removes those commands that are involved in cursor positioning and use of the SEND command because it uses those commands to manage the positioning of the cursor on the command line. Function key codes remain in use because they may be legitimate codes to be sent by the using program.
- MCSSend will reposition the cursor at the start of the command line if the cursor is positioned in the data display or scroll areas.
- The subroutine provides the following return codes:
  0 The command executed successfully.
  –1 Unable to clear the keyboard lock.
  –2 Serialization lockout.
  –3 The controller is not accepting the command.
  –4 The controller is not clearing the command.
- The script lets you call the program to modify the various default values for times to retry, delay times, screen size, and so on. It does this by issuing VALUE function calls before issuing the call to the routine.

MODSTAT.REX

The MODSTAT.REX script evaluates the status returned by the AFR_MODEMCALL, AFR_MODEMSTATUS, AFR_MODEMHANGUP, and AFR_MODEMANSWER external REXX functions.

MONTHLY.REX

You can use MONTHLY.REX to reallocate the server log file just after midnight on the first day of every month. After MONTHLY.REX reallocates the log, the extension on the old log file indicates the month it records. For example, on November 1, MONTHLY.REX would rename the October log as RPSERVER.OCT.

NETSAMP.REX

NETSAMP supports a Tivoli AF/OPERATOR demonstration of IBM's NetView® Interface. It is called by the program NETSCAN.REX. IBM does not support this program as an automation tool, it is an example program only.

NETSCAN.REX

This is a working program. NETSCAN monitors the MVS console for a trigger string, then calls the REXX script named in the WTOR (in this case, NETSAMP.REX). NETSCAN has two parameters: The name given to the

3270 session to be monitored (in this case, MVS-Console) and the trigger string to trap for (in this case, !ARNETV).

For example:

```
ret = AFR_START_PROGRAM( "NETSCAN MVS-Console !ARNETV" )
```

See the Tivoli AF/OPERATOR documentation for a complete description of IBM's NetView Interface. See AFR_SELECT in the *System Automation for Integrated Operations Management REXX Functions Reference* for details on selecting the 3270 session to monitor using SA IOM.

NotifyAck.rex
The NotifyAck.rex sample script is used by the SA IOM POP3 Reader to acknowledge an alert raised by the Alert Escalation.

NotifyEmail.rex
The NotifyEmail.rex sample script is an alert escalation feature helper script that demonstrates alerting one or more persons using e-mail.

NotifyGetAnswer.rex
The NotifyGetAnswer.rex sample script is called by the script NotifySMS.rex to lookup the answer of the sent SMS from the SMS service provider.

NotifyGetState.rex
The NotifyGetState.rex sample script is called by the script NotifyVoice.rex to lookup the state of the call from the Voice service provider.

NotifyPager.rex
The NotifyPager.rex is an alert escalation feature helper script that demonstrates alerting one or more persons using a paging device.

NotifyScript.rex
The NotifyScript.rex script is an alert escalation feature helper script that demonstrates how to execute one or more scripts, that you write, for alerting each person to be notified.

NotifySMS.rex
The NotifySMS.rex script is an alert escalation feature helper script that demonstrates alerting one or more persons using SMS. The service provider used in this sample is eCALL.

NotifyVoice.rex
The NotifyVoice.rex script is an alert escalation feature helper script that demonstrates alerting one or more persons using a telephone service provider that provides text-to-speech capabilities. The service provider used in this sample is eCALL.

PeerNCli.rex
The PeerNCli.rex script sample demonstrates the client side of the special type of peer-to-peer session that we are calling a "non-header" peer conversation. It shows how to start an outbound "non-header" peer conversation over the TCP/IP network.

PeerNSvr.rex
The PeerNSvr.rex script sample demonstrates the server side of the special type of peer-to-peer session that we are calling a "non-header" peer conversation. This program demonstrates the server side of the conversation that is initiated by an external peer over the TCP/IP network.

PEERSEND.REX
This is a working program. PEERSEND.REX sends a D TS, L operator

command to Tivoli AF/OPERATOR for execution and then waits for the command response data to be returned.

PEERSOCK.REX
This is a working program. PEERSOCK.REX is a REXX socket program which can converse with an SA IOM server. This program is designed so that it can be run either inside or outside SA IOM.

PEERSTRT.REX
This is a working program. PEERSTRT.REX starts up peer links to multiple Tivoli AF/OPERATOR and SA IOM peer systems. As a convenience, PEERSTRT.REX could be called during AUTOEXEC.REX processing to establish several long-term, frequently used conversations.

SKELETON.REX
SKELETON is an example of how to organize a REXX script. IBM does not support this program as an automation tool, it is an example program only.

SUBFUNCT.REX
The SUBFUNCT.REX script displays a subset of configuration parameters stored in the server configuration file.

TIME.REX
This is a working program. TIME.REX continually compares the current date and time with the following server values and targets the value that is later in time:

- The date and time specified for "Next Call"
- The date and time of the previous call plus the specified "Call Interval"

When the current system date and time is greater than the target value, the TIMECALL script is called.

TIMECALL.REX
This is a working program. TIMECALL contains the logic to initiate the call to the National Institute of Standards and Technology's Automated Computer Telephone Service (ACTS), interpret the data received, and update the system date and time accordingly.

VOICE.REX
VOICE is an interactive REXX script that provides a simple, menu-driven routine to exercise each of the voice functions individually. (Interactive programs require keyboard input or input from another device.) The user performs each action, such as initializing the voice card or dialing a number, by selecting that item from a list. Once completed, the user may then select another function. This program requires installation of a supported voice card on the SA IOM server (see Voice Control).

WTORSCAN.REX
This is a working program. WTORSCAN sets traps to look for the beeper trigger pattern defined during server configuration. The default value of the trigger pattern is !AOBEEP. If a WTOR trap is tripped, WTORSCAN retrieves the 80-character WTOR line, parses it, and passes it to BEEPCALL.REX. BEEPCALL.REX initiates a beeper page.
WTORSCAN.REX runs until either the server is shutdown or the system administrator terminates the program.

Appendix B. Client profile

Enforcing single client execution 231
Remapping the Enter key for 3270 sessions . . . 231
Remapping the DUP key for 3270 sessions . . . 232
Additional information on keyboard remapping 232
Enabling or disabling 3270 console alarm beep . . 233
Disabling selected client pop-up messages. . . . 233
Enabling serial com port journaling 233
Enabling cursor blink and block 234
Adjusting compatibility to an older server. . . . 234

This section provides information about using the SA IOM client profile, `rpcliprf.txt`, to customize aspects of product operation.

Enforcing single client execution

By default, it is possible to start multiple copies of the SA IOM client on the same PC. However, some customers may want to prevent this to avoid starting a second or third instance of the client. Instead, you can terminate additional client startups and automatically switch window focus to the copy of the client that is already executing.

To enforce single client execution, uncomment the following parameter in the client profile file, `rpcliprf.txt`:

```
ENFORCE_SINGLE_CLIENT = YES
```

The default setting for this parameter is NO.

Remapping the Enter key for 3270 sessions

The following table describes the default Enter key behavior for the SA IOM client for 3270 sessions.

Table 28. Default Enter key behavior

Key	Description of Behavior
ENTER key, Typewriter Keypad	Performs 3270 New Line cursor control function, (for example, moves the cursor key to the beginning of the next line, but does not return the current input to the host).
ENTER key, Numerical Input Keypad (NumPad)	Performs 3278 Enter function, (for example, returns current input to the host for processing).
RIGHT CONTROL key	No 3270 action.

The following procedure describes how to remap these keys using the `rpcliprf.txt` client-side profile.

1. Using a standard text editor, create a file named `rpcliprf.txt` in the SA IOM client's `\config` directory, or, if this file already exists, open it for modification.
2. To remap the Right Control key to perform a 3270 Enter, include the following entry in `rpcliprf.txt`:

   ```
   RIGHT_CONTROL_KEY = ENTER
   ```
3. To remap the Typewriter keypad's Enter key to perform a 3270 Enter, include the following entry in `rpcliprf.txt`:

   ```
   NEW_LINE_KEY = ENTER
   ```

Remapping the DUP key for 3270 sessions

On a 122-key IBM enhanced keyboard, a key commonly called the ″DUP″ key is present. When the ″DUP″ key is pressed unshifted, ″PA1″ is entered. When the key is pressed shifted, ″DUP″ is entered.

When used with an MVS console, entering a PA1 causes the last operator command to be retrieved to the command line. For this reason, the key is called ″DUP″ even though the actual key code sent is PA1.

On a 101/102-key Enhanced keyboard, or a Japanese 106-key keyboard, PA1 can be mapped to the PageUp key for 3270 sessions using the following entry:

```
PAGE_UP_KEY = PA1
```

Additional information on keyboard remapping

Not all keyboards have the same complement of keys. For example: A laptop with an 85-key keyboard will not have a keypad Enter key. This key is the key which is by default defined as the Enter key for 3270 sessions.

You can remap the following keys on your keyboard to perform as one of several other keys.

Table 29. Keys on your keyboard

RIGHT_CONTROL_KEY
This key is marked Ctrl on the bottom right of the typewriter keyboard, usually under the right Shift key.

NEW_LINE_KEY
This is the Enter key on the typewriter keyboard

ENTER_KEY
This is the Enter key on the numeric key pad.

PAGE_UP_KEY
This is the Page Up key.

You can remap the keys listed above to perform one of the following 3278 keyboard functions.

Table 30. Keys on a 3278 keyboard

ENTER
This is the Enter key on a 3278 keyboard.

NEW_LINE
This is the key marked with an arrow down and to the left on a 3278 keyboard. It moves the cursor to the first entry position on the next line.

RESET
Performs a keyboard reset on a 3270 session. By default, the key is assigned to the Left Ctrl key.

DUP
See remapping the DUP key for 3270 sessions, above.

HOME
Homes the cursor in 3270 and other emulations.

And these 3278 keys: **CURSOR_SELECT**, **FIELD_MARK**, **IDENT**, **PA1**, **PA2**, and **PA3**.

If you need to perform any special keyboard remapping on your SA IOM client PC, you can create parameters in this profile file in the form:

```
<name of new key function>  =  <name of key being remapped>
```

For example to make the PageUp and PageDown keys on your keyboard act like PA1 and PA2 (when you are in a 3270 emulation session) uncomment the following two lines.

```
PAGE_UP_KEY     =   PA1
PAGE_DOWN_KEY   =   PA2
```

Enabling or disabling 3270 console alarm beep

Prior releases do not support the detection and propagation of beeps (alarms) to 3270 client sessions. Two examples of these alarms are:

- MVS Master Consoles, when a WTOR is raised.
- VTAM consoles, when an invalid command is attempted.

In some environments a client user may not wish to be interrupted by incoming 3270 alarm beeps. Therefore a profile entry is provided to enable or disable the sounding of a beep when a 3270 alarm beep is detected. The setting applies to all 3270 sessions accessed by that client. Other sessions employing other emulations such as VT100 or HP will not be affected.

Alarm beeping is enabled by using the following entry:

```
ENABLE_3270_BEEP = YES
```

It may be disabled by either removing the entry, allowing the default to be taken, or by making the following entry:

```
ENABLE_3270_BEEP = NO
```

The default setting is disabled (NO) to be consistent with the behavior of previous releases of the product. All other values are diagnosed as in error.

Disabling selected client pop-up messages

Selected SA IOM client pop-up messages can be disabled via the client profile file. Certain pop-up messages can be unnecessary for some customers, and it is possible to disable their display. The message still appears on the status bar, but may be overwritten by a subsequent message.

In the SA IOM client profile, rpcliprf.txt, the following pop-up messages can be suppressed:

- RP06101 SA IOM Server logon in progress.
- RP06102 Logon successful. Dialback to xxx in progress.
- RP06103 Logon successful.
- RP06105 Client disconnected from Server.

To enable this feature, create one NODISP_MSG entry in the client profile file for each message to be suppressed. For example, to suppress the RP06101 and RP06102 messages, include the following entries:

```
NODISP_MSG = RP06101
NODISP_MSG = RP06102
```

Enabling serial com port journaling

For debugging purposes it can be useful to journal all com port data traffic. This feature is specified by port number and can be enabled with the following entry.

```
COMJOURNAL_PORT = 1
```

The journal file will be placed in the \journals\COMPORTn.JRN file. Only one port can be journaled at a given time.

Enabling cursor blink and block

Use the ENABLE_CURSOR_BLINK parameter to enable or disable the blinking behavior of the cursor in SA IOM host session windows. By default, cursor blinking is enabled. Disabling cursor blink may improve performance of some Windows graphical emulators by reducing the frequency of screen updates.

Use the ENABLE_CURSOR_BLOCK parameter to change the shape of the cursor in SA IOM host session windows.

```
ENABLE_CURSOR_BLINK = YES
ENABLE_CURSOR_BLOCK = YES
```

Adjusting compatibility to an older server

In SA IOM environments having a mixture of GA and post-GA clients and servers, post-GA clients will not successfully connect to an older GA level server. This is due to a change in the initial handshaking logic between the client and server involving character code pages.

For each GA-level server to which the post-GA client must connect, make the following profile entry:

```
SERVER_ACP_VERSION  =  saiom1::7
```

Where:

saiom1
: is the name of the GA server connection as it appears in the client's Servers and Sessions window. Note that this name cannot contain embedded blanks.

7
: refers to an internal messaging "ACP Version" number, not to the SA IOM build level. You can find the "ACP Version" number in the unfiltered header of the server's log file (rpserver.log).

Example:

```
SERVER_ACP_VERSION  =  HOUSTON_1::7
```

Multiple profile entries of this type can be made, but only one for each GA-level server connection.

Appendix C. Server profile

Enabling duplicate logon support 236
Enabling the Telnet server 236
Compressing TCP/IP client-server data. 237
Appending to a log rather than restarting it . . . 238
Modifying the disconnect time interval 238
Setting the server log trace level 238
Selecting VT emulation function key maps . . . 239
Changing the default SA IOM keyboard mapping 240
Disabling selected server pop-up messages . . . 243
Configuring a "non-header" peer communication port 243
Extended voice return codes 244
Multiplexing direct serial client/server connections 244
Enable serial com port journaling. 245
AFR_SEND_3270 keyboard delay parameter . . . 245
Controlling initialization and termination behavior of Object REXX RXAPI.exe 245
Message Collector options 247
TN3270E EBCDIC code page assignment 247
TN3270E bind-image feature 248
Password validation 248
User change password during logon 249
AFR_USER REXX functions 249
AFR_NOTIFY REXX functions and alert escalation options 249
Encryption options 250
| Enable IPv6 support 250
| Audit log support 250

This section provides information about using the SA IOM server profile, `rpsvrprf.txt`, to customize the application. Table 31 lists the parameters that you should use.

Table 31. Customization options available in the server profile, rpsvrprf.txt

To perform this server customization:	**Use:**
Enable duplicate logon support	ENABLE_DUPLICATE_LOGONS = YES
Enable the Telnet server	ENABLE_TELNET_CLIENT_CONNECTIONS = YES TELNET_SERVER_LISTENING_PORT = 23
Enable hotkeys with the Telnet server	TELNET_SERVER_HOTKEYA = <session name> TELNET_SERVER_HOTKEYB = <session name> TELNET_SERVER_HOTKEYC = <session name> TELNET_SERVER_HOTKEYD = <session name>
Compress TCP/IP client-server data	ENABLE_SVRTOCLI_TCPIP_COMPRESSION = YES
Append to a server log rather than restart it	SERVER_LOG_APPEND = YES
Modify the default disconnect time interval	USER_DISCONNECT_WARNING_TIMEOUT = 30
Set the server log trace level	SERVER_LOG_TRACE_LEVEL = CONFIG
Override the server Log Recycle Interval	SERVER_LOG_RECYCLE_INTERVAL = 7
Override the server Maximum Log Size	SERVER_MAXIMUM_LOG_SIZE = 50
Select the VT emulation function key map	VT_FUNCTION_KEY_MAP = <session name>::<map id>
Change the default SA IOM keyboard mapping	KEYBOARD_MAPPING_NAME = KBMAPEX1
Extended voice return codes	REXX_VOICE_VERSION = 2
Multiplexing direct serial client/server connections	DIRECT_CONNECT_CONTROL = DCD 1,2,4-6
Disabling selected server pop-up messages	NODISP_MSG = RP01100
Configuring a ″non-header″ peer communication port	PEER_PORT_NON_AFPACKET = 10018
Enable serial com port journaling	COMJOURNAL_PORT = 1
AFR_SEND_3270 keyboard delay parameter	SEND_3270_KEYBOARD_DELAY
Controlling initialization and termination behavior of Object REXX RXAPI.exe	RXAPI_TERMINATE_OPTION = IMPLICIT
Message Collector options	MSGCOLLECT_DISPLAYSIZE = MOD4 MSGCOLLECT_KEYS = YES

Table 31. Customization options available in the server profile, rpsvrprf.txt (continued)

To perform this server customization:	Use:
TN3270E EBCDIC code page assignment	TN3270E_EBCDIC_CODEPAGE_DEFAULT = 37
TN3270E bind-image feature	TN3270E_BIND_IMAGE_FEATURE = YES
Password validation	SERVER_CALLS_WINDOWS_LOGONUSER = YES
Specify the domain server for Password validation	PASSWORD_DOMAIN = JUPITER
User change password during logon	ALLOW_LOGON_CHANGE_PASSWORD = NO
AFR_USER REXX functions	ALLOW_AFR_USER_REXX = YES
AFR_NOTIFY REXX functions and options	NOTIFY_ODBC1 = DBNOTIFY,rpserver,rpserver NOTIFY_RPID = B NOTIFY_HISTORY_LEVEL = value NOTIFY_FLOOD_LEVEL = value
Encryption options	ENABLE_ENCRYPTION = YES REQUIRE_ENCRYPTION = YES
Enable IPv6 support	IPV6_CLIENT_PORT
Audit log support	SERVER_AUDIT_LOG_ENABLE = YES SERVER_AUDIT_LOG_RECYCLE_INTERVAL = 7 SERVER_MAXIMUM_AUDIT_LOG_SIZE = 50 SERVER_AUDIT_LOG_APPEND = YES

Important: When making changes to the server profile or to a keyboard mapping file, you must close the server application completely and restart it for the profile changes to take effect. Using the Stop and Start buttons on the server tool bar is insufficient, because certain profile parameters must be made available to the server when its process first starts.

Enabling duplicate logon support

By default, the same user ID cannot logon to the same SA IOM server multiple times to ensure the security and uniqueness of each client session. It also eliminates ambiguity when directing an operation at a particular user, for example, when sending a message or disconnecting another user.

However, for customers who need support for duplicate logons, the following parameter can be uncommented in the server profile file, `rpsvrprf.txt`:

```
ENABLE_DUPLICATE_LOGONS = YES
```

With this parameter enabled, it is possible for the same user to logon via TCP/IP from two different PCs or to logon from the same PC using, for example, TCP/IP for one client session and a modem or serial connection for the other client session.

Note: The same user cannot log on from the same client PC using the same communications method. This restriction is necessary because the difference in the location or type of connection, or both, allows the SA IOM server to distinguish between multiple client sessions with the same user ID.

Enabling the Telnet server

Connections to the SA IOM server are supported from native Telnet programs, whether running on a Windows platform or not. These Telnet clients only provide a subset of the functional capabilities available to Windows-based SA IOM clients. For example, Telnet clients cannot stop, start or view REXX scripts and they cannot

configure the SA IOM server. However, Telnet clients can view host sessions to which they are authorized and they can view a list of other active clients.

To enable the Telnet server feature, specify the following two parameters in the server profile file, `rpsvrprf.txt`:

```
ENABLE_TELNET_CLIENT_CONNECTIONS  =   YES
TELNET_SERVER_LISTENING_PORT   =   23
```

The presence of these two parameters in `rpsvrprf.txt` is all that is needed to enable the Telnet Server. The first parameter tells the SA IOM server that Telnet client connections are being accepted. It should be set equal to YES. The second parameter tells the SA IOM server the port number the Telnet Server is using to listen for client connections. This parameter can be set to any valid integer in the range from 1 to 32767. The example above assumes that the standard Telnet port number of 23 is being used.

There are four other optional parameters that can be used with the Telnet server feature to enable hotkey capability. Hotkey capability lets you configure hotkey letters A through D and assign them to particular host sessions. This allows Telnet clients to quickly toggle with Ctrl-A, Ctrl-B, and so on, to designated sessions.

To enable hotkey capability, you must uncomment some or all of the following parameters in the server profile file, `rpsvrprf.txt`:

```
TELNET_SERVER_HOTKEYA  =   <session name>
TELNET_SERVER_HOTKEYB  =   <session name>
TELNET_SERVER_HOTKEYC  =   <session name>
TELNET_SERVER_HOTKEYD  =   <session name>
```

Replace `<session name>` with the actual configured host session name exactly as it appears in the SA IOM Server Configuration Host Sessions list.

Note: Session names are case-sensitive. Also, if a session name contains one or more embedded blanks, the entire session name string must be enclosed in quotes.

If these hotkey parameters are not specified, then Telnet clients see all 3270-type host sessions listed first in their Sessions pull-down followed by any non-3270 sessions.

Compressing TCP/IP client-server data

Normally, messages from the SA IOM server to its TCP/IP-connected clients are not compressed. For slow LAN speeds, it may be beneficial to compress TCP/IP messages sent from the server to the client. For fast LAN speeds, the CPU cost of the compression and decompression may outweigh the benefit of sending smaller TCP/IP packets.

To enable TCP/IP message compression, make the following profile entry in the rpsvrprf.txt file:

```
ENABLE_SVRTOCLI_TCPIP_COMPRESSION  =  YES
```

Note: Older clients will continue to communicate with the server using the default non-compressed message mode. A server may simultaneously have new clients using the TCP/IP message compression feature, and some older clients not using the feature.

Appending to a log rather than restarting it

By default, when the SA IOM server process is started, the following logs are renamed to a backup file and then restarted from an empty state:

- The server log, rpserver.log
- The audit log, rpaudit.log, which contains messages that relate to a client connecting or a user logon and logoff as well as a user selecting a console
- The e-mail log, rpemail.log, which contains messages processed by the POP3 email server

Rather than restarting the log, you can append to the previous log. The following procedure describes how to append to a previous log by making an entry to the SA IOM `rpsvrprf.txt` server profile:

1. Using a standard text editor, create a file named `rpsvrprf.txt` in the SA IOM server's `\config` directory. Or, if this file already exists, open it for modification.
2. Add the following entries for the logs that you want to append:

```
AUDIT_LOG_APPEND  = YES
EMAIL_LOG_APPEND  = YES
SERVER_LOG_APPEND = YES
```

When the server is next started, new log messages will be appended to the bottom of the existing log. A backup of the log will not be made.

Note: The log configuration parameters defining the log recycle interval based on time or size will still be acted upon.

Modifying the disconnect time interval

The default disconnect time interval that the server process uses when it receives a request to disconnect a user is 15 seconds.

You can modify the default time interval by modifying a parameter in the SA IOM `rpsvrprf.txt` server profile.

1. Using a standard text editor, create a file named `rpsvrprf.txt` in the SA IOM server's `\config`. directory. Or, if this file already exists, open it for modification.
2. Uncomment the

   ```
   USER_DISCONNECT_WARNING_TIMEOUT
   ```

   parameter.
3. Change the time-out value of 15 seconds to the value you need.

The default time interval you specify displays in a warning message that the user being disconnected receives on their desktop.

Setting the server log trace level

If the SA IOM server crashes during startup, setting the `RpServer` log trace level to STATE to support problem diagnosis can be difficult. If the server crashes during startup, an SA IOM client cannot be connected to edit the server configuration or temporarily set the log trace level to STATE. It may or may not be possible to successfully edit the configuration using an SA IOM server at the same build level but on a different machine.

When no other options are available, you can override the configured SA IOM server trace level using the SERVER_LOG_TRACE_LEVEL keyword parameter with one of the following values:

CONFIG (Default. Use the configured value.)
PRIORITY
ERROR
WARNING
INFORMATION
TRACE
STATE

Set this keyword in the SA IOM server profile file, rpsvrprf.txt, in the SA IOM \config directory, for example:

```
SERVER_LOG_TRACE_LEVEL = STATE
```

You can also override the following SA IOM server parameter values:

Log Recycle Interval
Specify a value from 1 to 365 days. The default is 7 days. For example:

```
SERVER_LOG_RECYCLE_INTERVAL  =  7
```

Maximum Log Size
Specify a value in MB, from 1 to 25,000, depending on the build level. The default is 50 MB. For example:

```
SERVER_MAXIMUM_LOG_SIZE      =  50
```

To activate these overrides, you must stop and restart the SA IOM server. The new values are not stored in the SA IOM server configuration.

Selecting VT emulation function key maps

It is possible to assign one of four supported function key maps to individual host sessions employing VT serial or Telnet protocols. You can override the default function key escape sequence map used by SA IOM for host sessions using VT emulation.

Note: It is not possible to assign a customized mapping to an individual function key or to define new maps.

SA IOM supports the following hard-coded maps for defining VT function key escape sequences:

0: SA IOM Default Function Key Map

1: SA IOM Legacy Function Key Map

2: VT220 Terminal Function Key Map

3: AS400 Telnet Function Key Map

Maps can be assigned to individual SA IOM sessions using the following notation:

VT_FUNCTION_KEY_MAP = <session name>::<map id>

For example,

VT_FUNCTION_KEY_MAP = AS400_1::3

VT_FUNCTION_KEY_MAP = Central Park::1

VT sessions not explicitly specified use the SA IOM default function key map. Only sessions using VT emulation can be assigned function key maps. If the session name contains embedded blanks, the entire right-hand side expression should be enclosed with single or double quotes.

Changing the default SA IOM keyboard mapping

SA IOM supports a limited keyboard remapping facility, that is implemented using the `rpsvrprf.txt` server profile. To remap selected keys, include the following parameter in your server profile:

```
KEYBOARD_MAPPING_NAME = <filename>
```

For example, including the following profile parameter,

```
KEYBOARD_MAPPING_NAME = KBMAPEX1
```

causes SA IOM to load the file `kbmapex1.txt` from SA IOM's `\config` directory when the server process is started. This file contains definitions of remapped keys, as well as other parameters defining the individual sessions (or ALL sessions) to which the key mappings apply.

Note: See the sample `kbmapex1.txt` file installed in your `\config` directory for examples of remapped keys.

At this time, you cannot remap keys to escape sequences, macros, or keys not identified in the following table. Also, to exploit the keyboard mapping capability, both the SA IOM server and client must be at Build 23 or higher.

The following table lists the keys that you can remap.

Table 32. Remappable keys

0_KEY	ALT_0_KEY	CTRL_0_KEY
1_KEY	ALT_1_KEY	CTRL_1_KEY
2_KEY	ALT_2_KEY	CTRL_2_KEY
3_KEY	ALT_3_KEY	CTRL_3_KEY
4_KEY	ALT_4_KEY	CTRL_4_KEY
5_KEY	ALT_5_KEY	CTRL_5_KEY
6_KEY	ALT_6_KEY	CTRL_6_KEY
7_KEY	ALT_7_KEY	CTRL_7_KEY
8_KEY	ALT_8_KEY	CTRL_8_KEY
9_KEY	ALT_9_KEY	CTRL_9_KEY
NUMPAD_0_KEY	SHIFT_NUMPAD_0_KEY	CTRL_NUMPAD_0_KEY
NUMPAD_1_KEY	SHIFT_NUMPAD_1_KEY	CTRL_NUMPAD_1_KEY
NUMPAD_2_KEY	SHIFT_NUMPAD_2_KEY	CTRL_NUMPAD_2_KEY
NUMPAD_3_KEY	SHIFT_NUMPAD_3_KEY	CTRL_NUMPAD_3_KEY
NUMPAD_4_KEY	SHIFT_NUMPAD_4_KEY	CTRL_NUMPAD_4_KEY
NUMPAD_5_KEY	SHIFT_NUMPAD_5_KEY	CTRL_NUMPAD_5_KEY
NUMPAD_6_KEY	SHIFT_NUMPAD_6_KEY	CTRL_NUMPAD_6_KEY
NUMPAD_7_KEY	SHIFT_NUMPAD_7_KEY	CTRL_NUMPAD_7_KEY

Table 32. Remappable keys (continued)

NUMPAD_8_KEY	SHIFT_NUMPAD_8_KEY	CTRL_NUMPAD_8_KEY
NUMPAD_9_KEY	SHIFT_NUMPAD_9_KEY	CTRL_NUMdPAD_9_KEY
PA1_KEY	PA2_KEY	PA3_KEY
ALT_A_KEY	CTRL_A_KEY	
ALT_B_KEY	CTRL_B_KEY	
ALT_C_KEY	CTRL_C_KEY	
ALT_D_KEY	CTRL_D_KEY	
ALT_E_KEY	CTRL_E_KEY	
ALT_F_KEY	CTRL_F_KEY	
ALT_G_KEY	CTRL_G_KEY	
ALT_H_KEY	CTRL_H_KEY	
ALT_I_KEY	CTRL_I_KEY	
ALT_J_KEY	CTRL_J_KEY	
ALT_K_KEY	CTRL_K_KEY	
ALT_L_KEY	CTRL_L_KEY	
ALT_M_KEY	CTRL_M_KEY	
ALT_N_KEY	CTRL_N_KEY	
ALT_O_KEY	CTRL_O_KEY	
ALT_P_KEY	CTRL_P_KEY	
ALT_Q_KEY	CTRL_Q_KEY	
ALT_R_KEY	CTRL_R_KEY	
ALT_S_KEY	CTRL_S_KEY	
ALT_T_KEY	CTRL_T_KEY	
ALT_U_KEY	CTRL_U_KEY	
ALT_V_KEY	CTRL_V_KEY	
ALT_W_KEY	CTRL_W_KEY	
ALT_X_KEY	CTRL_X_KEY	
ALT_Y_KEY	CTRL_Y_KEY	
ALT_Z_KEY	CTRL_Z_KEY	
ALT_PF1_KEY	CTRL_PF1_KEY	
ALT_PF2_KEY	CTRL_PF2_KEY	
ALT_PF3_KEY	CTRL_PF3_KEY	
ALT_PF4_KEY	CTRL_PF4_KEY	
ALT_PF5_KEY	CTRL_PF5_KEY	
ALT_PF6_KEY	CTRL_PF6_KEY	
ALT_PF7_KEY	CTRL_PF7_KEY	
ALT_PF8_KEY	CTRL_PF8_KEY	
ALT_PF9_KEY	CTRL_PF9_KEY	
ALT_PF10_KEY	CTRL_PF10_KEY	
ALT_PF11_KEY	CTRL_PF11_KEY	
ALT_PF12_KEY	CTRL_PF12_KEY	

Table 32. Remappable keys (continued)

ALT_PF13_KEY	CTRL_PF13_KEY	
ALT_PF14_KEY	CTRL_PF14_KEY	
ALT_PF15_KEY	CTRL_PF15_KEY	
ALT_PF16_KEY	CTRL_PF16_KEY	
ALT_PF17_KEY	CTRL_PF17_KEY	
ALT_PF18_KEY	CTRL_PF18_KEY	
ALT_PF19_KEY	CTRL_PF19_KEY	
ALT_PF20_KEY	CTRL_PF20_KEY	
ALT_PF21_KEY	CTRL_PF21_KEY	
ALT_PF22_KEY	CTRL_PF22_KEY	
ALT_PF23_KEY	CTRL_PF23_KEY	
ALT_PF24_KEY	CTRL_PF24_KEY	
ALT_INSERT_KEY	CTRL_INSERT_KEY	
ALT_PAGE_UP_KEY	CTRL_PAGE_UP_KEY	
ALT_PAGE_DOWN_KEY	CTRL_PAGE_DOWN_KEY	
ALT_CURSOR_DOWN_KEY	CTRL_CURSOR_DOWN_KEY	
ALT_CURSOR_LEFT_KEY	CTRL_CURSOR_LEFT_KEY	
ALT_CURSOR_RIGHT_KEY	CTRL_CURSOR_RIGHT_KEY	
ALT_DELETE_KEY	CTRL_DELETE_KEY	
ALT_END_KEY	CTRL_END_KEY	
ALT_HOME_KEY	CTRL_HOME_KEY	
ALT_HOME_KEY	CTRL_HOME_KEY	
ALT_ESCAPE_KEY	CTRL_ESCAPE_KEY	
ESCAPE_KEY	SHIFT_ESCAPE_KEY	
PAUSE_KEY	SHIFT_PAUSE_KEY	
SCROLL_LOCK_KEY	SHIFT_SCROLL_LOCK_KEY	
ENTER_KEY	SHIFT_ENTER_KEY	
NUMPAD_PERIOD_KEY	SHIFT_NUMPAD_PERIOD_KEY	
INSERT_KEY	SHIFT_INSERT_KEY	
PAGE_UP_KEY	SHIFT_PAGE_UP_KEY	
PAGE_DOWN_KEY	SHIFT_PAGE_DOWN_KEY	
CURSOR_LEFT_KEY	SHIFT_CURSOR_UP_KEY	
CURSOR_RIGHT_KEY	SHIFT_CURSOR_DOWN_KEY	
CURSOR_TWO_LEFT_KEY	SHIFT_CURSOR_LEFT_KEY	
CURSOR_TWO_RIGHT_KEY	SHIFT_CURSOR_RIGHT_KEY	
END_KEY	SHIFT_END_KEY	
HOME_KEY	SHIFT_HOME_KEY	
DELETE_KEY	SHIFT_DELETE_KEY	
NEW_LINE_KEY	CTRL_NEW_LINE_KEY	
LEFT_CONTROL_KEY	RIGHT_CONTROL_KEY	
LEFT_CONTROL_MODIFIER_KEY	RIGHT_CONTROL_MODIFIER_KEY	

Table 32. Remappable keys (continued)

LEFT_BRACKET_KEY	RIGHT_BRACKET_KEY	
PRINT_122_KEY	DEVICE_CANCEL_KEY	
PERIOD_KEY	VERTICAL_BAR_KEY	
RESET_KEY	ATTN_KEY	
DUP_KEY	CLEAR_KEY	
ERASE_EOF_KEY	FIELD_MARK_KEY	
CENT_SIGN_KEY	INDENT_KEY	
SYSRQ_KEY	CURSOR_SELECT_KEY	

For example, to remap the Alt+F5 key on the IBM Enhanced 101/102 keyboard to perform a 3270 SYSRQ function, make the following entry in your keyboard mapping file:

```
ALT_PF5_KEY = SYSRQ
```

Notes:

1. To remap CTRL-modified keys using the Left Control key (on the IBM Enhanced 101/102 key keyboard), the following key mapping must be included:

   ```
   LEFT_CONTROL_KEY = LEFT_CONTROL_MODIFIER
   ```

2. Key mappings defined in the client profile (for example, ENTER_KEY) will be remapped by the keyboard mapping defined using the server profile. That is, the client-side mapping will be applied first and then the server-side mapping.

Disabling selected server pop-up messages

Selected SA IOM server pop-up messages can be disabled via the Server profile file. Certain pop-up messages can be unnecessary for some customers, and it is possible to disable their display. The message still appears on the status bar, but may be overwritten by a subsequent message.

In the SA IOM server profile, rpsvrprf.txt, the following message pop-ups can be suppressed:

- RP01100 SA IOM Server initialization completed successfully.
- RP01101 SA IOM Server shutdown completed successfully.
- RP01102 Server restart requested by user.
- RP01103 User configuration update requested by user.
- RP01104 Shutting down SA IOM due to Windows session shutdown.

To enable this feature, create one NODISP_MSG entry in the server profile file for each message to be suppressed. For example, to suppress the RP01100 and RP01001 messages, include the following entries:

```
NODISP_MSG = RP01100
NODISP_MSG = RP01101
```

Configuring a "non-header" peer communication port

You can customize each SA IOM server to have *one* TCP/IP port specifically listening for incoming peer-to-peer communications from peers that do not use the header information used by standard peer communications.

To enable non-header peers and have the SA IOM server listen for that type of connections, uncomment the following keyword line and specify the desired port number. In addition Peers must be enabled and configured in the SA IOM server configuration.

```
PEER_PORT_NON_AFPACKET = 10018
```

When enabled and a connection is made on the specified port, the SA IOM server will start the script named PeerNSvr.rex to handle the conversation.

See also Peer-to-Peer Communications.

Extended voice return codes

Voice cards cannot detect when the person called hangs up the phone. Hang-up can occur during playback, record, dial, or during any voice function. IBM has implemented some special, extended return codes for conditions that may occur when using the REXX Voice functions. To use these extended return codes you must uncomment the following profile entry

```
REXX_VOICE_VERSION  =  2
```

See also Voice diagnostic and debugging facilities.

Multiplexing direct serial client/server connections

This feature is applicable in those cases where a communications port is being used for client/server connection via a multiplexer or other dedicated line and IT IS NOT CONNECTING. If your connection is working, then you DO NOT need to modify its operation with this feature.

Direct serial connection between a client and its intended server is governed by the state (level) of the Data Set Ready (DSR) lead at the computer. This is on pin 8 of a 25 pin connector. The server needs to see this signal transition from unasserted (OFF) to asserted (ON) to start the connection process, or transition from asserted to unasserted to start the disconnection process.

Some vendors of communication multiplexers have decided to use the DSR line to indicate some other condition such as multiplexer powered on. Therefore the line never changes state and the connect/disconnect processes are not started.

The DIRECT_CONNECT_CONTROL profile entry allows you to change the control line to be monitored to establish a direct connect client/server connection.

The following is an example for the discussion that follows:

DIRECT_CONNECT_CONTROL = DCD 1,2,4-6

The value assigned consists of two fields separated by one or more contiguous spaces. The first, which is DCD in the example above, indicates the control line to be monitored. Allowed values are:

DSR Data set ready, the default
DCD Data carrier detected
RLSD Receive line signal detected, a synonym for DCD
CTS Clear to send

These are not case sensitive.

The second field is a list that consists of port numbers (separated by commas), or ranges of ports (consisting of a starting port number followed by a hyphen followed by the ending port number), or a combination of these formats.

In the example provided above the DCD (RLSD) line is monitored on ports 1, 2, 4, 5, and 6.

Note: These settings are used only on those ports configured for direct connect client connections on the server.

If other ports need to be configured for direct connect client/server connection monitoring for another control signal, then another statement may be entered. We do not recommend monitoring more than one line on a port.

Enable serial com port journaling

For debugging purposes it can be useful to journal all com port data traffic. This feature is specified by port number and can be enabled with the following entry.

```
COMJOURNAL_PORT = 1
```

The journal file will be placed in the \journals\COMPORTn.JRN file. Only one port can be journaled at a given time.

AFR_SEND_3270 keyboard delay parameter

You can introduce a delay between entering characters via the AFR_SEND_3270 function by setting the SEND_3270_KEYBOARD_DELAY parameter to a value between 0 and 2000 milliseconds. This parameter will affect all AFR_SEND_3270 calls. Use this parameter only if you experience ″too fast″ character entry and keyboard lockouts when sending strings to 3270 coax or TN3270E sessions.

The default keyboard delay used by SA IOM is zero milliseconds as SA IOM 3270 emulation normally senses keyboard availability.

```
SEND_3270_KEYBOARD_DELAY  =  0
```

Controlling initialization and termination behavior of Object REXX RXAPI.exe

If the SA IOM server is restarted multiple times, and if there is a REXX script that runs but fails each time the server is started, an Object REXX interface process, `RXAPI.exe`, may become damaged. In this case, the REXX Management component of SA IOM will not initialize successfully and will show a red light. The corrective action is to terminate the current `RXAPI.exe` process, and then restart the SA IOM server, causing a new `RXAPI.exe` process to be created. The RXAPI process can be terminated by a Windows Administrator using the operating system Task Manager.

When the SA IOM server is shutting down or recycling, the server releases Object REXX resources managed by `RXAPI.exe`. At this time, the `RXAPI.exe` process also shuts down if there are no other applications using it. Occasionally, RXAPI does not shut down cleanly, and an internal Object REXX thread running inside the SA IOM process space does not terminate before the SA IOM server process, `rpserver.exe`, terminates. In this case, the SA IOM server can crash.

Two SA IOM server profile parameters are provided that allow you to tune `RXAPI.exe` startup and termination, guarding against erratic RXAPI behavior from SA IOM:

RXAPI_TERMINATE_DELAY

RXAPI_TERMINATE_OPTION

Use these new profile options to help eliminate or greatly reduce repeated the number of RXAPI problems.

Set the RXAPI_TERMINATE_DELAY parameter to the number of seconds that the SA IOM server, when shutting down, should wait after releasing its Object REXX resources before continuing its shutdown. This interval allows Object REXX to shut down its RXAPI interface thread, which executes within the SA IOM server process space. You are allowed a value range of one to ten seconds.

RXAPI_TERMINATE_DELAY = 1 (1 second default)

Set the RXAPI_TERMINATE_OPTION parameter to the method to be used by SA IOM server when disconnecting from Object REXX:

RXAPI_TERMINATE_OPTION = IMPLICIT

Default option. RXAPI is allowed to terminate without special action from SA IOM.

Note: If other applications are using Object REXX at this time, RXAPI correctly continues running.

RXAPI_TERMINATE_OPTION = AT_SERVER_START

If RXAPI is running when SA IOM server starts, this instance is terminated by SA IOM so that a fresh instance can be started. Use this option if RXAPI does not exit when SA IOM shuts down, when the SA IOM server is the first or only application using Object REXX to be started.

RXAPI_TERMINATE_OPTION = AT_SERVER_STOP

If RXAPI is still running after the SA IOM server completes its termination delay wait (See RXAPI_TERMINATE_DELAY above), then it is terminated by SA IOM so that a fresh instance can be started when SA IOM next starts. Use this option if RXAPI does not exit when SA IOM shuts down, when the SA IOM server is the last or only application using Object REXX to be shut down.

RXAPI_TERMINATE_OPTION = AT_SERVER_START_AND_STOP

If RXAPI is still running after the SA IOM server completes its termination delay wait (See RXAPI_TERMINATE_DELAY above), then it is terminated by SA IOM so that a fresh instance can be started when SA IOM next starts. If RXAPI is running when SA IOM server starts, this instance is terminated by SA IOM so that a fresh instance can be started. Use this option if RXAPI does not exit when SA IOM shuts down, when the SA IOM server is the only application using Object REXX, and when an extra margin of safety is desired.

Message Collector options

There are two Message Collector customization options available from this profile:

1. Change the display size from MOD2 (24 lines by 80 columns) to MOD4 (43 lines by 80 columns)
2. Enable the Functions keys - currently only F5 is supported (clear screen)

To enable these functions, uncomment the following two statements:

```
MSGCOLLECT_DISPLAYSIZE = MOD4
MSGCOLLECT_KEYS = YES
```

TN3270E EBCDIC code page assignment

You can assign the EBCDIC code page to be used with TN3270E sessions using the following notation:

```
TN3270E_EBCDIC_CODEPAGE_DEFAULT  =  <code page number>
TN3270E_EBCDIC_CODEPAGE  =  <session name>::<code page number>
```

For example:

```
TN3270E_EBCDIC_CODEPAGE_DEFAULT  =  37
TN3270E_EBCDIC_CODEPAGE  =  SYSA::500
TN3270E_EBCDIC_CODEPAGE  =  "System B"::273
```

If the session name contains embedded blanks, the entire right-hand side expression should be enclosed with single or double quotes, as shown in the example for `"System B"`.

The following EBCDIC code pages are supported:

37 English US
273 Austrian/German
274 Belgian
277 Danish, Norwegian
280 Italian
284 Spanish
285 English UK
297 French
500 International
871 Icelandic

The EBCDIC default code page assignment is used for all TN3270E sessions for which a specific codepage is not defined. The hard-coded default EBCDIC codepage, if no profile EBCDIC keywords are set, is 37 (English US).

```
TN3270E_EBCDIC_CODEPAGE_DEFAULT  =  37
```

If all TN3270E sessions use the same EBCDIC code page, setting the TN3270E_EBCDIC_CODE_PAGE_DEFAULT parameter is sufficient. Individual TN3270E sessions do not require entries in this case.

The characters '¬' and '¢' exist on the 3278 keyboard but not the PC keyboard. By default, COAX 3270 sessions map the '¬', '¢' and '|' characters to the '^', '[' and ']' keys. By default, TN3270E sessions do not map these keys. You can have all TN3270E sessions behave as all COAX sessions do regarding these three keys by using the option:

```
TN3270E_MAP_KEYS_LIKE_COAX_FEATURE  =  YES
```

TN3270E bind-image feature

Before Build 95, TN3270E sessions did not request the Bind-Image feature. To support a number of VM hosts, support was added as the default as it did not seem to affect TSO or MVS Console use.

```
TN3270E_BIND_IMAGE_FEATURE  =  YES
```

This feature can be turned off for all sessions, returning usage as it was before Build 95, with:

```
TN3270E_BIND_IMAGE_FEATURE  =  NO
```

Individual sessions can be changed with:

```
TN3270E_BIND_IMAGE_SESSION  =  <session name>
```

If the session name contains embedded blanks, the entire right-hand side expression should be enclosed with single or double quotes, as shown below for ″System B″:

```
TN3270E_BIND_IMAGE_SESSION  =  SYSA
TN3270E_BIND_IMAGE_SESSION  =  "System B"
```

TN3270E_BIND_IMAGE_FEATURE will set the default for all sessions. Use as many TN3270E_BIND_IMAGE_SESSION over-rides as needed to change this default for the specified sessions.

Password validation

The default validation behavior of the SA IOM Server is to authenticate user IDs by checking each password internally against one saved with the User record. You can customize the SA IOM Server to use Windows password validation (the Windows LogonUser API) to authenticate user IDs (except for the user ID Administrator).

To use Windows validation instead of using the default SA IOM Server validation method, uncomment the following server profile entry:

```
SERVER_CALLS_WINDOWS_LOGONUSER  =  YES
```

Notes:

1. The validation is performed on the PC that is running the SA IOM Server. Each user defined to SA IOM in the User record must also be defined in Windows for the password validation.
2. The ″Administrator″ user is always validated locally to prevent the possibility of being locked out of the configuration.
3. Under Windows 2003, the SA IOM Server must be run as a System Service to avoid logon failure code 1314 (Privilege not held). Windows XP has fixed this limitation.

Use the following variable to specify the DOMAIN server for setting/changing Windows user passwords. For example, to pass a domain name of JUPITER, add the following server profile entry.

```
PASSWORD_DOMAIN = JUPITER
```

If PASSWORD_DOMAIN = xxxxx is enabled, the authenticating Windows machine may and may not be the PC RpServer is running on, this is all done by the same Windows API just passing in the domain name.

User change password during logon

To prevent the user from changing the password during logon, make the following profile entry change.

```
ALLOW_LOGON_CHANGE_PASSWORD = NO
```

AFR_USER REXX functions

To enable the AFR_USER functions, make the following profile entry change.

```
ALLOW_AFR_USER_REXX = YES
```

AFR_NOTIFY REXX functions and alert escalation options

Before the AFR_NOTIFY functions can be used the ODBC DS must be defined. This task is done for you by the installation program.

To enable the AFR_NOTIFY functions, activate the server profile entry of the following form, and change the appropriate values to those that were specified for the alert escalation "server to derby connection" configuration.

Format: NOTIFY_ODBC1 = ODBC dsn, user_id, password

For example, make the following profile entry change.

```
NOTIFY_ODBC1 = DBNOTIFY,rpserver,rpserver
```

When more than one RpServer is used in the same NOTIFY, the originator can be identified with the following event ID code (the default is 'A').

```
NOTIFY_RPID = B
```

The events from any alert are recorded in the alert escalation database. To control the detail level of these events, use the following keyword / value combination.

Format: NOTIFY_HISTORY_LEVEL = value

The default *value* is 3.

0 No history, no status updates
1 Minimal history, minimal status updates
3 Full history, full status updates (default)

For example, make the following profile entry change.

```
NOTIFY_HISTORY_LEVEL = 0
```

The maximum number of active alerts can be controlled with the following keyword / value combination:

Format: NOTIFY_FLOOD_LEVEL = value
The default *value* is 500.

For example, make the following profile entry change.

```
NOTIFY_FLOOD_LEVEL = 300
```

Encryption options

By default, messages between the SA IOM server and its clients are not encrypted.

To enable message encryption, make the following profile entry change.

```
ENABLE_ENCRYPTION  =  YES
```

To reject connections from clients that do not support encryption, make the following profile entry change.

```
REQUIRE_ENCRYPTION  =  YES
```

Setting the REQUIRE_ENCRYPTION entry implies that ENABLE_ENCRYPTION will also be set.

Enable IPv6 support

To enable IPV6 support uncomment the following keyword:

```
IPV6_CLIENT_PORT  =  YES
```

Audit log support

The audit log contains information about all events that occur in the RpServer, for example users logging on and off or entering input data. The log contains all relevant events regardless of the trace level. The events are stored in a separate file called RpAudit.log

To enable the audit log, uncomment the following server profile entry:

```
SERVER_AUDIT_LOG_ENABLE  =  YES
```

the default action if the audit log is not enabled is not to record audit events to the RpAudit.Log file.

You can also override the following audit log parameter values by changing the default values and uncommenting them:

Log Recycle Interval
Specify a value from 1 to 365 days. The default is 7 days. For example:

```
SERVER_AUDIT_LOG_RECYCLE_INTERVAL  =  7
```

Maximum Log Size
Specify a value in MB, from 1 to 25,000, depending on the build level. The default is 50 MB. For example:

```
SERVER_MAXIMUM_AUDIT_LOG_SIZE      =  50
```

If you do not want to append to the previous audit log when the SA IOM server process is started, you can uncomment the following server profile entry:

```
SERVER_AUDIT_LOG_APPEND  =  NO
```

To activate any of these changes, you must stop and restart the SA IOM server. The new values are not stored in the SA IOM server configuration.

Appendix D. TN3270E operational information

TN3270E supported colors and system status and error conditions are listed in this appendix. Also included is suggested materials you may need when reporting problems involving SA IOM TN3270E facilities. Specific information on customer support is contained in the *Software Support Handbook* on page 285, located http://techsupportservices.ibm.com/guides/handbook.html.

Topics in this appendix

The following topics are discussed in this appendix:

- "TN3270E color support"
- "OIA status indicators" on page 252
- "Reporting problems to IBM" on page 253

TN3270E color support

This section describes color support with and without the 3270 extended data stream option.

With the 3270 Extended Data Stream option

If selected during session configuration, the SA IOM TN3270E facility supports the IBM 3270 Extended Data Stream protocol. This includes graphics and support for eight colors. The eight colors included in the IBM 3270 Extended Data Stream are:

- Black
- Blue
- Red
- Pink
- Green
- Turquoise
- Yellow
- White

These may be used as both foreground and background colors. Highlighting options include:

- Blink
- Underscore
- Reverse video

These are in addition to intensified fields in the normal 3270 data stream.

The following 3270 Extended Data Stream features are not supported by SA IOM:

- Mandatory fill
- Mandatory entry
- Trigger fields
- Character set
- Field outlining
- Transparency

Without the 3270 Extended Data Stream option

Without the 3270 Extended Data Stream option, the SA IOM TN3270E support uses four colors:

Table 33. TN3270E supported color

Color	Designates
Green	Unprotected, normal intensity fields
Red	Unprotected, high intensity fields
Light Blue	Protected, normal intensity fields
White	Protected, high intensity fields

For MVS console operation, normal messages appear in light blue and action messages (WTORs) appear in white. Key input appears in green.

OIA status indicators

The IBM 3270 series of terminals includes an area at the bottom of the screen called the Operator Information Area (OIA). This area communicates system status and error conditions to the terminal user. Review the following table for explanations of the OIA status indicators that SA IOM displays. The IBM manual *IBM 3270 Information Display System Component Description*, order number GA27-2749-10, lists 135 unique status and error values that can be displayed.

OIA Status indicators in SA IOM

Symbol	Original 3270 Condition	Host Sense	SNA Sense	Reset Key?
X [\] 390	Parity error	N/A	N/A	No
X PROG 401	Invalid command received	CR	1003	Yes
X PROG 402	Invalid address	OC	1005	Yes
X PROG 403	Data after read, and so on	OC	1003	Yes
X PROG 404	Data too short	OC	1005	Yes
X Z 505	Session disconnected	N/A	N/A	No
XZ 510	Not active	N/A	N/A	No
X	Input inhibited	N/A	N/A	Yes
X >>	Field full (Insert mode)	N/A	N/A	Yes
X SYS	Transaction in progress	N/A	N/A	No

What these symbols mean

The following table describes what the status indicator symbols mean.

Symbol	Description
Z	Used in place of the special 3270 “Lightening Bolt” symbol to indicate communication problems.
Z 505	Displayed while TN3270E session negotiation is in progress.

Symbol	Description
X [\]	Used in place of the special 3270 “Broken Box” symbol. This symbol indicates severe errors. The session should be disconnected and reconnected, although a restart of the server may also be advisable if this symbol is displayed.
OC	Operation Check status. Presented to the host for data stream errors.
CR	Command Reject status. Presented to the host for data stream errors.
SNA Sense	Defines the SNA sense code associated with the problem. SNA sense data is not provided by SA IOM’s TN3270E facility. These values are listed for those readers experienced with SNA error reporting.
Reset key	Indicates if the client user can clear the condition with the reset key.

In addition to the above OIA line information, SA IOM also displays a connection type on the right-hand side of the status line. This contains one of three values:

Connection types	Descriptions
TN3270E	The SA IOM server successfully established a session with the TN3270E server.
Telnet	No sessions exist.
Blank	Some stage of session negotiations is occurring.

Other symbols

The following table describes other status indicator symbols and whether or not SA IOM provides such an indicator.

Symbol	Description
X Clock	Refers to a special symbol displayed on the 3270 OIA. It is displayed in the time between pressing a key for host transmission (for example Enter and PF keys) and the time the host actually reads the generated data stream. This is a very short interval in the SA IOM TN3270E implementation, and no separate symbol is provided for this state.
X-SYS (X system)	Indicates that the user’s data was sent to the host, but the host has not responded with a message to unlock the keyboard.
^ (Insert)	Displayed at position 52 of the OIA when the keyboard is in Insert mode.
Connection indicator	Displayed by the IBM 3270 at the left side of the OIA. SA IOM does not provide this.

Reporting problems to IBM

When you report problems involving the SA IOM TN3270E facilities to IBM Support, some additional material may be needed. Normally, IBM Support requests a copy of the client and server logs for the time period that the error arose, as well as copies of any REXX scripts involved. For the TN3270E facility, IBM Support may ask for the problem documentation listed here, depending on the type of problem. For more information on customer support, see the *Software Support Handbook* on page 285, located http://techsupportservices.ibm.com/guides/handbook.html.

Requested documentation - configuration problems

For problems where the configuration options in SA IOM are suspected as the cause of a connection problem, try to provide the following to IBM.

- SA IOM server log
- Screen prints of the configuration panels as you have completed them
- 2074 DEVMAP file

Requested documentation - connection problems

For problems where the 2074 does not connect successfully with the SA IOM server, provide the following.

- SA IOM server log
- Communications packet trace between the 2074 and the SA IOM server

The Windows Network Monitor tool may be used for the packet trace. If this is not installed or not available at your installation, contact IBM to discuss other alternatives. The IBM 2074 DEVMAP file may also be required in some instances.

Requested documentation - display problems

If problems involve how messages are displayed on the SA IOM TN3270E console session, provide the following.

- SA IOM server log
- Communications packet trace between the 2074 and the SA IOM server

If possible, screen prints of the display in question and a display of what the session should be doing are desirable for this type of problem.

Appendix E. TCP/IP error codes

This appendix lists the TCP/IP error codes that you may encounter when using IBM's REXX functions.

Common TCP/IP error codes

This section lists some of the most common TCP/IP error codes you may encounter.

Table 34. TCP/IP Error Codes

Error Code	Description
10037	An operation is already in progress with the specified TCP/IP socket. For example, a second connect was attempted on a socket that is already attempting to connect or a second close was attempted on a socket that is already in the process of closing.
10049	The specified host address is not valid. Verify that the address is defined in your TCP/IP network.
10051	The specified host address cannot be reached. This usually means that the local software knows no route to connect to the remote host system.
10053	An established connection was aborted by the software in your local machine, possibly due to a data transmission time-out or protocol error.
10054	An established connection was forcibly closed by the remote peer. This usually results if the remote application was suddenly stopped or the peer was rebooted.
10056	A connect request was made on a TCP/IP socket that is already connected.
10061	The connection request to the specified host address was refused. This usually results from trying to connect to an inactive peer.
10093	A valid Windows socket environment does not exist.

Appendix F. Messages

This section lists the SA IOM Web-based user interface messages.

AFI0001E **A critical error occurred at the database level.**

Explanation: The database server is probably offline.

System Action: The current task ends.

User Response: Check if the database server is working correctly. If not, contact your system administrator.

AFI0002E **The invoke() function of the User Task Manager failed with the following exception.**

Explanation: The application is trying to call the invoke function of the User Task Manager but failed with an exception.

User Response: Contact your system administrator.

AFI0004E **This action is not applicable for the current alert status.**

Explanation: A possible reason for the error: an another user performed a status change prior to you.

System Action: The view will now be refreshed.

User Response: Consult the documentation for the status state diagram.

AFI0005I **You should select an item before performing this action.**

Explanation: There is no item selected. Nothing will happen.

User Response: Make sure an item is selected.

AFI0006W **The selected item already has a membership.**

Explanation: This operation has no effect.

User Response: Perhaps you wanted to remove this item?

AFI0007W **The selected item doesn't have a membership.**

Explanation: This operation has no effect.

User Response: Perhaps you wanted to add this item?

AFI0008E **The item has been deleted or modified.**

Explanation: The action can't be performed because the item does not exist.

User Response: Perhaps it has been deleted or modified by a different user.

AFI0009W **Items have been deleted or modified.**

Explanation: The action can't be performed completely because one or more items were not found.

User Response: Perhaps items were deleted or modified by a different user.

This section lists the "classic" SA IOM messages.

RP00400 **Log Manager initialization successful.**

Explanation: The SA IOM server log file has been opened and server logging has successfully started.

System Action: The SA IOM server continues starting other components.

User Response: None. This is an informational message only.

RP01100 **SA IOM server initialization completed successfully.**

Explanation: All components of SA IOM server started successfully. All configured host sessions and communication ports were successfully opened.

System Action: The SA IOM server is ready for client connections.

User Response: None. This is an informational message only.

RP01101 **SA IOM server shutdown completed successfully.**

Explanation: All components of the SA IOM server shut down successfully. All configured host sessions and communication ports were successfully closed.

System Action: The SA IOM server is ready to be restarted.

User Response: None. This is an informational message only.

RP01102 **Server restart requested by user** *userid*

Explanation: The specified user requested the server to be restarted so that new server configuration changes can take effect.

System Action: The SA IOM server shuts down then restarts.

User Response: A consequence of the server shutting down, the user connection to the server is closed. The user must reconnect and logon again after the server has started.

RP01200 **Errors detected during server initialization.**

Explanation: One or more errors were reported by one or more server components as they were starting.

System Action: The server continues execution. Depending on the type of error, the server may be able to service client connections and may be able to serve some or all connected host sessions.

User Response: Inspect the Server Status Display and the server log to determine the errors that occurred. Perform corrective action specific to each error as defined by the error number.

RP01201 **Slow server shutdown detected**

Explanation: One or more server components was slow in shutting down or did not respond to the shutdown request. A slow server machine or one or more non-responding REXX scripts are main causes of this error. Server components shut down sequentially, so a non-responding component may cause delay in the shutdown of other components later in the shutdown sequence.

System Action: The server forces itself to shut down, potentially not releasing all system resources.

User Response: Consult the server log to determine if errors were reported that might be the cause of the shutdown delay. Close the server application completely before restarting it. If you use REXX scripts and, on restarting, the REXX Management component does not successfully initialize.

1. Close the server.
2. Terminate the RXAPI.EXE process using the operating system Task Manager.
3. Restart the server.

RP01202 **Server profile read error or invalid entry:** *text*

Explanation: The text displayed at the end of this message is a clue to help you solve the problem.

System Action: The entry is ignored.

User Response: Some possible reasons for receiving this message are:

- A setting in the server profile is not supported by the server.
- A setting in the server profile is not spelled correctly.

RP03200 **An error occurred during Host Management initialization. Server startup will continue.**

Explanation: The Host Management component of the server did not successfully open all configured and enabled host sessions.

System Action: The Host Management light on the Server Status display turns red, but the server continues execution. Depending on the type of error, the server may be able to service client connections and may be able to serve some, but not all, connected host sessions.

User Response: Consult the server log to determine which host sessions did not successfully open. Possible causes include:

- Invalid host session configuration data
- Incorrect communications adapter setup
- Serial or TCP/IP communications failures
- Host system failure

RP03202 **Failed to initialize 3270 device**

Explanation: The rp3270.sys device driver is not installed or running, or the correct version is not installed.

System Action: The Host Management light on the Server Status display turns red but the server continues execution. You cannot access any 3270 host sessions.

User Response: Use the Devices icon in the Control Panel to see if rp3270.sys is installed and started. If it is not listed in Devices, then this product is not properly installed. When rp3270.sys is installed, reboot and it will show up in Devices if it has been properly installed.

RP03400 **Host Management initialization successful**

Explanation: The Host Management component of the server started successfully. All configured and enabled host sessions were opened successfully.

System Action: The Host Management light on the Server Status display turns green, and the server continues starting other components.

User Response: None. This is an informational message only.

RP06101 **server** *servername* **logon in progress**

Explanation: A user ID and optional password were sent to the server, and the server is validating them.

System Action: The server validates the logon. If valid, the server returns the list of host sessions authorized for this user ID, or first performs a call back procedure. If invalid, the server returns an error message.

User Response: If the message remains and the logon is not established or denied, consult the system administrator for corrective action, if any, on the server. Then restart the client and repeat the logon procedure.

RP06102 **Logon successful. Dialback to** *phonenumber* **in progress.**

Explanation: The user ID and optional password have been validated. For security reasons, this user ID requires the server to call back the client to establish a client/server connection.

System Action: The server is attempting to communicate with the modem on the client machine. When the connection is made, the server returns the list of host sessions authorized for this user ID. If the call back is not completed successfully, the server terminates its connection to the client.

User Response: None. If the call back is not completed successfully, validate the correct operation of the client machine's modem and consult the system administrator for corrective action, if any, on the server. Validate the call back number for the telephone line connected to the client machine associated with this user. Then restart the client and repeat the logon procedure.

RP06201 **server** *servername* **logon unsuccessful.**

Explanation: The user ID and optional password have not been successfully validated. Possible causes include:

- User ID not defined in the user configuration data for the target server.
- User properties for this user are not enabled.
- Incorrect or missing password.
- The server is forwarding password authentication during logon to Windows.
- This user is restricted from connecting to the target server using the attempted method.

System Action: The server logs the invalid logon attempt and continues execution.

User Response: Check your password. It is case sensitive. If the problem persists, consult the system administrator to obtain a valid user ID, reset the current password, or modify other logon restrictions.

RP06202 **Script** *scriptname* **is still running. Script must be halted before it can be deleted**

Explanation: An attempt was made to delete a running REXX script. Only scripts which have been halted or scripts which have completed their execution can be deleted.

System Action: The server continues execution. The running REXX script is not affected.

User Response: Issue a Halt request or wait until the script is done before you delete it.

RP06203 **Script** *scriptname* **is still running. Script must be halted before it can be restarted**

Explanation: An attempt was made to restart a running REXX script. Only scripts which have been halted or scripts which have completed their execution can be restarted.

System Action: The server continues execution. The running REXX script is not affected.

User Response: Issue a Halt request or wait until the script is done before you restart it.

RP06204 **Script** *scriptname* **is not running. Script must be running before trace mode can be set or reset**

Explanation: An attempt was made to turn trace on or turn trace off of a REXX script that is no longer running. The Trace menu action only works on scripts which are running.

System Action: The server continues execution. The non-running REXX script is not affected.

User Response: Restart the script then issue the Trace request again.

RP06205 **Server version** *versionlevel* **does not support this client**

Explanation: The client attempted to connect to an incompatible server. The server is an older version that the client does not support.

System Action: The server and client continue execution.

User Response: The targeted server must be upgraded before this client can connect to it. Alternatively, a compatible version of the client can be used. Use the client About dialog to determine the client version level.

RP06206 **server** *servername* **logon unsuccessful. Invalid IP address.**

Explanation: The server, for this user ID, only allows client connections from a specific list of one or more IP addresses. The IP address used for this logon attempt is invalid.

System Action: The user is prevented from logging on to the server. The server logs the unsuccessful logon attempt and continues execution. The client continues execution.

User Response: Logon to the server from a client machine with a valid IP address, or logon to the server using a user ID for which this client IP address is valid. If these options are not possible, consult your system administrator to modify your user restrictions.

RP06207 **server** *servername* **logon unsuccessful. Only local connection is permitted**

Explanation: The server, for this user ID, only allows client connections from a client that is resident on the same machine as the server. This user cannot connect to the specified server from a remote machine.

System Action: The server logs the unsuccessful logon attempt and continues execution. The client continues execution.

User Response: Logon to the server from the server machine, or logon to the server using a user ID for which remote connection is allowed. If the options are not possible, consult your system administrator to modify your user restrictions.

RP06208 **client failed to receive dialback from server** *servername***.**

Explanation: There is a user restriction in effect on the indicated server, which specifies a "call back" phone number for the user. The server calls the client back as part of the logon validation process. This is a security feature. The "call back" phone number field in the indicated server's configuration for this user may be incorrect.

System Action: The user is prevented from logging on to the server.

User Response: This message may indicate a security violation. The system administrator of the indicated server can remove the user restriction, or correct the call back phone number for this user by reconfiguring the server.

RP06209 **Connection to server** *server_name* **already exists from this client**

Explanation: The client currently has an open connection to a server using the indicated server name. This is a name that appears in the Server Name control of the General property page in the Server Configuration dialog. By default, this name is set to SAIOM1. While a client can simultaneously have many connections to different servers, it cannot have two connections open to the same server, and it also cannot have two connections open to different servers which happen to use the same server name.

System Action: None. The attempted connection remains closed and the previous connection remains open.

User Response: Close the previous connection before attempting the new connection. If this is the second connection attempt to the same server, determine if there is a good reason why this client needs two separate server connection definitions to the same server. Two server connection definitions are necessary only if alternate client/server connection methods (such as TCP/IP and modem) are needed for testing or backup purposes. But if two server connection definitions to the same server are not necessary, then one of the definitions should be removed from this client's Servers and Sessions list to prevent this error from occurring. If the error was caused by a connection attempt to a different server which uses the same name as an already connected server, you should review your server configuration definitions to make sure that each server has a unique name.

RP06301 **Script** *scriptname* **is not running. Halt not performed.**

Explanation: The REXX script is either halted, done, in the process of stopping, or has failed. The Halt operation cannot be performed.

System Action: The halt request is ignored. The server and client continue execution.

User Response: Check the server log or the REXX session window, or both, to determine if the script should still be running but ended prematurely. If the script status is Halted, Done, or Failed it can be deleted using the Delete context menu function. If the script status is Stopping, and the status does not change, consult your operator for corrective action.

RP06302 **Server** *servername* **disconnected. Config changes cancelled**

Explanation: The indicated server stopped executing after the server configuration session had started. All changes made by the client and not saved are lost and must be reentered.

System Action: The server, if it is still running, allows its configuration to be accessed by other authorized clients or by the same client once a new connection is made.

User Response: Try to reconnect to the same server and reenter the configuration changes. If you cannot reconnect, contact your operator for server status information.

RP08400 **User Management initialization successful**

Explanation: The User Management component of the server started successfully. The user configuration file was successfully accessed.

System Action: The User Management light on the Server Status display turns green, and the server continues starting other components.

User Response: None. This is an informational message only.

RP10200 **An error occurred during REXX Management initialization. Server startup will continue**

Explanation: The REXX Management component of the server did not start successfully, due to a missing DLL or due to an inability to register with the REXX Interpreter. A frequent cause of this error is that the REXX Interpreter is in a damaged state and requires restarting.

System Action: The REXX Management light on the Server Status display turns red, and the server continues execution. The REXX API is disabled. Additional error messages providing more detail are written to the log.

User Response: Consult the server log to determine the cause of the initialization failure. Possible causes include:

- A missing or damaged REXX Support DLL or rprexxaf.dll
- A failure in starting the REXX Interpreter
- A failure in registering entry points

This problem can usually be corrected by these steps:

1. Close the server.
2. Terminate the RXAPI.EXE process using the operating system Task Manager.
3. Restart the server.

RP10201 **REXX Support DLL did not load. REXX facility disabled**

Explanation: The REXX Management component of the server did not start successfully, due to a missing or damaged dynamic link library, rprexxaf.dll. The installation is considered damaged.

System Action: The server continues initialization, but cannot execute autoexec.rex or other REXX scripts.

User Response: Backup the existing configuration files and reinstall the server to recover a fresh copy of the REXX Support DLL.

RP10202 **REXX Interpreter did not initialize. REXX facility disabled**

Explanation: The REXX Management component of the server did not start successfully, due to a failed REXX Interpreter initialization call.

System Action: The server continues initialization, but cannot execute autoexec.rex or other REXX scripts.

User Response: This problem can usually be corrected by these steps:

1. Close the server.
2. Terminate the RXAPI.EXE process using the operating system Task Manager.
3. Restart the server.

then starts a new invocation of the RXAPI.EXE process. REXX scripts running outside of SA IOM control should be exited before performing this action.

RP10203 **REXX API registration failed. REXX facility disabled**

Explanation: The REXX Management component of the server did not start successfully, due to a failed REXX API registration call.

System Action: The server continues initialization, but cannot execute autoexec.rex or other REXX scripts.

User Response: This problem can usually be corrected by these steps:

1. Close the server.
2. Terminate the RXAPI.EXE process using the operating system Task Manager.
3. Restart the server.

then starts a new invocation of the RXAPI.EXE process. REXX scripts running outside of should be exited before performing this action.

RP10204 **REXX Script Information did not initialize. REXX facility disabled**

Explanation: Internal information necessary to start autoexec.rex was not successfully created. The REXX facility is disabled because the same error occurs for all REXX scripts.

System Action: The server continues initialization, but cannot execute autoexec.rex or other REXX scripts.

User Response: This problem is usually caused by insufficient virtual memory. As a result, the server will most likely not complete its initialization phase. Correct the problem by increasing the amount of virtual memory for the system using the Windows NT Control Settings applet.

RP10205 **REXX environment not found in search path. REXX facility disabled**

Explanation: The REXX environment required by to execute REXX scripts could not be found. The REXX Interpreter cannot be accessed.

System Action: The server continues initialization, but cannot execute autoexec.rex or other REXX scripts.

User Response: Add the REXX environment to the system path using the Windows NT Control Settings applet. Note that this problem may indicate a damaged or failed Object REXX installation, and the installation of Object REXX may need to be repeated. This problem can occur if Object REXX was not installed by a person having NT administrator authority. In this case, reinstall Object REXX using the NT administrator logon ID.

RP10206 **The following script did not successfully start:** *scriptname*

Explanation: The specified script was not found or could not be loaded by the REXX Interpreter.

System Action: The server continues execution.

User Response: Verify that the name and location of the specified script is correct. If this information is correct, verify the correct behavior of the REXX Interpreter by executing the same script from a local client. Verify that the script file is not damaged and can be successfully edited. If all the above are satisfactory, attempt the execution of other scripts. If similar problems occur, then this problem may indicate a damaged or failed Object REXX installation, and the installation of Object REXX may need to be repeated.

RP10207 **REXX script** *scriptname* **terminated with an exception**

Explanation: The REXX script encountered an exception during execution.

System Action: The REXX script is terminated. The REXX Management light on the Server Status Display turns red and the server continues execution.

User Response: Examine the REXX script to find the cause of the exception. When REXX scripts terminate with an exception, system resources may not be released. If many such failures occur, the server may become damaged. After may REXX script failures, the server should be restarted.

RP10400 **REXX Management initialization successful**

Explanation: The REXX Management component of the server started successfully. The REXX Interpreter was successfully located and initialized, and the REXX API was successfully registered. The autoexec.rex script was successfully executed. Authorized clients can execute other REXX scripts.

System Action: The REXX Management light on the server status display turns green, and the server continues starting other components.

User Response: None. This is an informational message only.

RP12101 **Please wait while configuration file transfer is in progress.**

Explanation: The server configuration files are being transferred from the server machine to the client machine. This process may take several seconds, depending on the size of the configuration files.

System Action: The server continues sending its configuration files.

User Response: None. This is an informational message only.

RP12201 **Configuration transfer failure. Failed to transfer** *filename*

Explanation: A communications error occurred sending the specified server configuration file from the server to the client.

System Action: The configuration edit request is terminated. The server and client continue executing.

User Response: If other communication activities with the server are successful, repeat the configuration edit request. If the same error occurs, consult your systems administrator.

RP12202 **Configuration transfer failure. Failed to read** *filename*

Explanation: A file input error occurred when the server attempted to read the configuration file to satisfy the client's configuration edit request.

System Action: The configuration edit request is terminated. The server and client continue executing.

User Response: The specified configuration file may be damaged. Repeat the configuration edit request. If the same error occurs, consult your systems administrator.

RP12203 **Configuration transfer failure. Failed to open** *filename*

Explanation: The server could not locate the specified configuration file or the file was locked by a different application.

System Action: The configuration edit request is terminated. The server and client continue executing.

User Response: Verify that the specified configuration file is located in the server's `\config` subdirectory and is correctly named. If so, close all other applications running on the server machine. If access is still not possible, close the Server and reboot the NT operating system.

RP12204 **The server is currently being configured by** *userid*

Explanation: Only one client at a time can update the server configuration. Another client is currently editing the configuration file.

System Action: The attempt to update the server configuration file is blocked. The server and client continue executing.

User Response: Wait for the other client to complete the configuration edit activity. If this is not possible, restart the server, reconnect your client, and perform the configuration edit request.

RP12205 **You are not authorized to perform server configuration.**

Explanation: The current user ID does not have authorization to edit the configuration file for this server.

System Action: The attempt to update the server configuration file is blocked. The server and client continue executing.

User Response: Consult your system administrator to modify the authorizations for this user ID.

RP12400 **Configuration Manager initialization successful.**

Explanation: The Configuration Management component of the server started successfully. The configuration files were successfully loaded. No other components can successfully initialize if this first initialization step is not successful.

System Action: The Server Management light on the Server Status display turns green, and the server continues starting other components.

User Response: None. This is an informational message only.

RP16101 **server** *servername* **connection in progress via local connection**

Explanation: The client is currently connecting to the specified server from the same machine using a shared memory area for communication.

System Action: The server is preparing its support for a locally connected client.

User Response: None. This is an informational message only.

RP16102 **server servername connection timeout**

Explanation: The connection to the indicated server has timed out because no user input was detected in the specified time interval.

System Action: The client connection to the server is closed.

User Response: You can logon to the server again to reestablish the connection. The system administrator of the indicated server can remove or modify the idle timeout restriction for this user by re-configuring the server.

RP16103 **server** *servername* **logon timeout**

Explanation: A user attempting to logon to the indicated server did not enter a logon ID and password within 2 minutes.

System Action: No client connection to the indicated server is established.

User Response: Try logging on again.

RP16104 **Session input required in seconds on server** *servername* **to prevent timeout**

Explanation: This is a connection timeout warning. There is a user restriction in effect on the indicated server. This causes the client connection to disconnect if no user input is detected within a specified time.

System Action: If no input is detected within the indicated number of seconds, the client connection to the server is closed.

User Response: You can logon to the server again to reestablish the connection. The system administrator of the indicated server can remove or modify the idle timeout restriction for this user by re-configuring the server.

RP16201 **server** *servername* **not available via local connection**

Explanation: The server could not be accessed using the client running on the same machine. The server may not be running, or may not be ready to accept client connections.

System Action: No client connection to the indicated server is established. The client continues execution.

User Response: Make sure that the server has started successfully and repeat the client connection attempt. The Local Communications status light on the Server Status Display must be green.

RP16400 **Local Communications initialization successful**

Explanation: The component of the server that supports locally connected clients initialized successfully.

System Action: The server continues starting other components.

User Response: None. This is an informational message only.

RP16600 **Local communication functions are not available on this system.**

Explanation: A memory allocation error has occurred, or another locally connected client is executing. The local client will not be able to access the server using local communication.

System Action: System errors result when the server fails to create the named pipe that it uses for local communication. The local client will not be able to connect to the server.

User Response: Check to see if there is another process running on the server that is using local communication to the server, such as another locally connected client.

RP17101 **server** *servername* **connection in progress via TCP/IP**

Explanation: The client is currently connecting to the specified server using a TCP/IP connection, either across a LAN or on the same machine as the server.

System Action: The server is preparing its support for a TCP/IP-connected client.

User Response: None. This is an informational message only.

RP17200 **An error occurred during TCP/IP initialization. Server startup will continue**

Explanation: The TCP/IP Communications component of the server did not successfully start its listening function. The TCP/IP configuration on the server machine may not be functional.

System Action: The server continues execution. The server will not be able to service clients attempting to connect using TCP/IP.

User Response: Validate the server machine's ability to perform TCP/IP communications (for example, ping the server machine hostname), and correct problems encountered. Reboot the server machine, and restart the server.

RP17201 **server** *servername* **not available via TCP/IP connection**

Explanation: The indicated server is not configured to allow a TCP/IP connection.

System Action: The client cannot connect to the server.

User Response: Contact the system administrator who can use "Client Connections" in the server configuration to enable TCP/IP client connections.

RP17400 **Client TCP/IP Communications initialization successful**

Explanation: The server has successfully started its ability to service TCP/IP connections from clients across a LAN or on the same machine as the server.

System Action: The TCP/IP Communications light on the Server Status display turns green. The server continues starting other components.

User Response: None. This is an informational message only.

RP17401 **Message Collector TCP/IP Communications initialization successful**

Explanation: The server has successfully started its ability to service TCP/IP connections from other systems communicating to the Message Collector. This message only occurs if the Message Collector is configured as an enabled host session.

System Action: The server continues starting other components.

User Response: None. This is an informational message only.

RP17612 **TCP/IP functions are not available on this system**

Explanation: The TCP/IP port specified in the configuration for the client connection is not available. It is in use by another product.

System Action: A TCP/IP connection is not allowed, but the server continues execution.

User Response: Modify the client connection to specify another available port.

RP18101 **server** *servername* **connection in progress via direct serial connection**

Explanation: The client is currently connecting to the specified server using a direct serial connection.

System Action: The server is preparing its support for a serially connected client.

User Response: None. This is an informational message only.

RP18200 **An error occurred during initialization of serial communication. Server startup will continue**

Explanation: The communication port specified in the serial client connection configuration is not available.

System Action: The Serial Communications light on the Server Status display turns red, and the server continues execution. The server will not be able to service clients attempting to connect using a direct serial connection.

User Response: Validate the server machine's serial port definitions using the NT Control Settings applet. Reboot NT and restart the server.

RP18201 **server** *servername* **not available via direct serial connection**

Explanation: The client is failing to connect to the server using a serial port.

System Action: The client cannot connect to the server.

User Response: Make sure there is a null modem cable connection between the server and client COM ports. Check the server configuration and client configuration to make sure the Client Connections and Server Connections Serial Properties are correctly specified for the COM ports at both ends of the connection.

RP18400 **Serial Communications initialization successful**

Explanation: The component of the server that supports serially-connected clients and host systems initialized successfully.

System Action: The Serial Communications light on the Server Status display turns green. The server continues starting other components.

User Response: None. This is an informational message only.

RP18600 **Explanation: The `rpserial.dll` is missing in the server's bin directory or it is not the correct version.**

System Action: No serial communication between server and client is allowed, but the server continues execution.

User Response: Examine the `\bin` directory to be sure the `rpserial.dll` exists. If it is not in the `\bin` directory, then this product is not properly installed.

RP19101 **server** *servername* **connection in progress via modem connection**

Explanation: The client is currently connecting to the specified server using a modem connection.

System Action: The server is preparing its support for a modem-connected client.

User Response: None. This is an informational message only.

RP19200 **An error occurred during initialization of modem communication. Server startup will continue**

Explanation: The Modem Communications component of the server did not successfully open its configured modem.

System Action: The Modem Communications light on the Server Status display turns red, but the server continues execution. The server will not be able to service clients attempting to connect using a modem.

User Response: Validate the server machine's modem configuration. See "Installing modems" on page 33.

RP19201 **server** *servername* **not available via modem connection**

Explanation: The client failed to connect successfully to the server using a modem. The server may not be running or may not be ready to accept client connections through a modem.

System Action: The client cannot connect to the server.

User Response: Check to see that the server has the modem configured in the client connection. Check to see if the server phone number is correctly specified in the client configuration. Make sure the server has successfully started and then repeat the client connection attempt. The Modem Communications status light on the Server Status Display must be green.

RP19400 **Modem Communications initialization successful**

Explanation: The server has successfully started its ability to service modem-based connections from clients.

System Action: The Modem Communications light on the Server Status display turns green. The server continues starting other components.

User Response: None. This is an informational message only.

RP19600 **Modem functions are not available on this system**

Explanation: The modem is not recognized by the Windows environment.

System Action: The server continues to come up but the modem function for server/client communication is not operating.

User Response: Validate the server machine's modem configuration. See "Installing modems" on page 33.

RP19601 **Modem unable to dial back**

Explanation: The server made three attempts and was not able to successfully call back to the client.

System Action: The server modem line resumes its listening mode and is ready to accept a modem connection.

User Response: Check that the correct call back phone number is entered on the user restrictions panel associated with the user who was not able to successfully log on.

RP19602 **Unable to load `RpModem.DLL, rc=returncode`**

Explanation: The server cannot load the rpmodem.dll, because it is missing from the server's `\bin` directory. The return code states the error code returned by the system.

System Action: No modem communication between server and client is allowed, but the server continues execution.

User Response: Check the `\bin` directory to be sure the `rpmodem.dll` exists. If it is not in the bin directory, then this product is not properly installed.

RP19603 **Unable to load functions from `RpModem.DLL, rc=returncode`**

Explanation: The `rpmodem.dll` in the `\bin` directory is not the correct version.

System Action: No modem communication between server and client is allowed, but the server continues execution.

User Response: Check to see that this product is properly installed.

RP30600 **Telnet host telnethostname is unavailable**

Explanation: A timeout occurred while attempting to connect to the indicated Telnet host. This message is not logged.

System Action: Server and client operations continue.

User Response: Verify that the Telnet host name is spelled correctly and that it is up and available.

RP31601 **Failed to connect to Telnet host** *telnethostname*

Explanation: An error occurred while attempting to connect to the indicated Telnet host. This message is not logged.

System Action: Server and client operations continue.

User Response: Check the server log for more specific error information.

RP31602 **REXX script** *scriptname* **could not be started. REXX facilities are not available on the server**

Explanation: The server rejects any REXX script start request if the REXX Management component is in a damaged or inactive state. This message is not logged.

System Action: Server and client operations continue.

User Response: Check the server log for more specific error information as to why the REXX Management component failed to initialize.

RP31603 **REXX script** *scriptname* **could not be started. You are not authorized to start scripts**

Explanation: Your User ID is not associated with a user group that has Use Scripts authority. This message is not logged.

System Action: The attempt to start the indicated REXX script is blocked.

User Response: Contact your system administrator.

RP31604 **Operation on REXX script scriptname not authorized.**

Explanation: You do not have authority to perform the attempted operation on the script. This error occurs when your User ID is not associated with a user group that has "Manage Scripts" authority and you attempt to delete, halt, restart, or trace, a script started by someone else. This message is not logged.

System Action: The script is not operated upon.

User Response: None. This is an informational message only.

Index

Special characters

\config2 subdirectory 31
\scripts2 subdirectory 30

Numerics

122-key keyboards 219
3270 adapters
  connecting to mainframes 205
  installing 205
  supported 205
3270 adapters (deprecated)
  defined 22
3270 sessions, consolidating to one session 128
3270 terminal emulation using adapters (deprecated) 7
6530CONT.REX sample script 225

A

access roles
  AFI 151
  assigning to user groups in ISC 154
  SA IOM alert escalation 152
ad hoc notification 189
  configure server IP addresses 161
  setting up peer connections 161
adapters, emulation
  installing:Attachmate IRMA PCI 212
  verifying support for:Attachmate IRMA PCI 212
adapters, voice
  installing Dialogic 103
  supported types 103
AFI
  access roles 151, 152
  prefixed messages 257
alert escalation
  administrator tasks 151
  automatically starting 193
  change DBNotify database 162
  defining a policy 180
  helper scripts 189
  Netcool/OMNIbus integration 160
  overview 163
  schedules 192
  stopping 182
  testing a policy 181
  troubleshooting 196
  troubleshooting displays 194
  Web interface 163
alerts
  changing status of 174
  cleaning up manually 175
  closing 174
  deleting obsolete 176
  kicking off, automating 193
  status modes 185
  status, important points 185
  viewing history of 175
  viewing status of 174
Alerts table
  SA IOM alert escalation 174
Amdahl
  5995M support, instructions 200
  cable connections 200
  Model 2 and Model 4 terminals 200
Apache Derby 10.2.2.0 16
application model, client/server 4
Attachmate IRMA PCI adapter
  installing 212
authorities 60
authority, Modify Server Config 70
Auto Connect feature 39
Auto Logon feature 39
Auto Select feature 39
AUTOEXEC.REX sample script 225
automatic paging 99
automation
  features 39
  functions 6

B

baud rate
  configuring ports 201
beep, 3270 console 233
BEEP.REX sample script 225
BEEPCALL.REX sample script 98, 225
beeper paging 63
  automatic paging 99
  coding delays into a page 101
  commas, when/when not to use 100
  IXO modem protocol 98
  overview of 97
  paging services 98
  TAP modem protocol 98
  touch-tone versus modem paging 97
  trigger pattern 99
  tuning a touch-tone WTOR 101
  with a voice adapter 107
  WTOR syntax 99
BEEPQSHL.REX subroutine 225
browser
  configuring for Web-based user interface 195

C

cables
  3270 adapters 200
  directly connecting two computers 202
  mainframe ports 200, 205
  null modem pin-outs 202
  some terms you should know 201
change
  DBNotify database 162
clean up
  obsolete alerts manually 175
client 45
client com port journaling 233
client connections 64

client connectivity 5
client pop-up messages
  disabling 233
client profile
  defaults, in general 31
  detailed parameters information 231
client profile file
  locating new 31
client server connections
  serial 244
client, adjusting compatibllity 234
client, local client 5
client, remote client 5
client/server application model 4
client/server communication
  modem connections 71
  serial connections 72
  TCP/IP connections 70
client/server compatibility considerations 26
code pages
  assigning in TN3270E sessions 247
  supported in TN3270E sessions 247
colors for TN3270E 252
components of SA IOM
  3270 adapters (deprecated) 22
  voice adapter 21
compress TCP/IP client-server data 31
configuration
  ports:non-IBM mainframe 200
  ports:RS-232C serial port 200
configuration process, TN3270E 122
configure Telnet 3270E sessions 121
configuring
  beeper paging 63
  i2.the client 39
  modems 20
configuring SA IOM session definitions 122
connecting client to server 69
connecting SA IOM's
  scenario 79
connecting to a server 38
consoles, consolidating multiple 128
consolidate selected messages from one or multiple systems 130
consolidating messages 78
context-sensitive help under Vista 51
copy and paste 127
CPC 111
cursor blinking behavior 234
Cursor.rex sample script 226
CUT mode 200

D

DB-9 and DB-25 cables 201
DBNotify database, change 162
DCE cable 201
debugging
  alert escalation 196
debugging tools
  voice adapter 108
default user groups 60
defining
  3270 sessions 58
  client connections 64
  Glass Teletype sessions 59
  host sessions 57
defining *(continued)*
  peer connections 65
  recovery options 66
  service logging 66
  session classes 62
  user groups 60, 61
  users 63
delays between characters
  touch-tone paging service 98, 100
Deleting
  scripts 48
DFT mode not supported 200
Dialogic voice adapter
  installing 103
DIP switches
  3270 adapters 207
direct connections 20
DLLs
  SA IOM HMC Interface-required 113
  support 17
  system 17
drivers, devise
  rp3270.sys 207
DTE cable 201
DUP key, 3270 sessions 232
duplicate logon 236
duplicate logons 31
duration, of escalation level 186
dynamic load libraries 17

E

EABs 206
EBCDIC code pages
  assigning in TN3270E sessions 247
  supported in TN3270E sessions 247
EmailReply.rex sample script 226
emulation features 7
enable a Telnet server 31
enabling the Telnet server 236
encryption xxi, 8, 17, 26, 250
Enter key, 3270 sessions 231
error codes
  TCP/IP 255
error processing 52
escalation level 186
Escalation.rex sample script 226
Escalations table
  Alerts table
    troubleshooting 194
  SA IOM alert escalation 171
  troubleshooting 194
Event history table
  SA IOM Alert Escalation 176
  troubleshooting 194
extended attribute bytes 206

F

flow control 201
functional capabilities of SA IOM 5

G

General properties panel, description 56

General settings window
SA IOM alert escalation 164
Generic 124
Groups table
SA IOM alert escalation 169
troubleshooting 194

H

Halting
scripts 48
handshaking 201
hardware adapters 21
hardware components
3270 adapters (deprecated) 22
voice adapter 21
Help 51
helper scripts 189
history
alert status 175
detailed event history 176
HMC emulation support 7
HMC Interface
introduction 111
HMCACT.REX 119
HMCACT.REX subroutine 226
HMCONS.REX 115, 226
HMCSTAT.REX 115, 226
host sessions, defined 5
host system connectivity 5
HP 17, 20, 199
HWMCA 111

I

IBM 2074 connection 125
IBM 2074 Console Support Controller 121, 126
IBM Crypto for C (ICC) 17
IBM DB2 Run-Time Client 8.2 for Windows 16
IBM Integrated Solutions Console Advanced Edition 7.1 16
industry standard architecture (ISA) bus 206
INGRNIOM.REX sample script 226
installation
3270 adapters on server 205
3270 emulation adapters 205
verification 30
installing
SA IOM 27
installing modems 33
Integrated Solutions Console (ISC) 16
intellectual property 275
INTERACT.REX sample script 226
International Component for Unicode (ICU) 17
IP address, for peer connections 65
IP address, for TCP/IP connected clients 70
IPv6 support, enabling 250
ISA bus 206
IXO modem protocol
finding a compatible vendor 98
used by BEEPCALL.REX 98

K

keepalive support 19
Keyboard remapping, client 232
keyboard support
overview of 219
keyboard support for TN3270E 221

L

LAN adapters 21
level, of escalation 186
license, patents 275
licensing
address 275
Web address 275
local client, defined 5
local communications 69
local server, defined 5
log files
MSGCLECT.LOG 81
log level
client
dynamically changing 135
server
dynamically changing 135
Log Reader program, for RP logs 140
logging level 109
server log 135
logging on
alert escalation 163
to SA IOM server
first time, from a local client 31
from a configured client 38
Web-based user interface, alert escalation 163
logging overrides
server log 135

M

mainframes
3278 Model 2 and 4 terminals 200
5995M support, instructions 200
Amdahl 200
cable connections 200, 205
configuring:MVS display mode 200
non-IBM:port configuration 200
MCSSEND.REX subroutine 226
message collection 6
Message Collector
default port 18
logging 81
monitoring 80
sample programs 81
sample programs:UNIX sample 84
sample programs:Windows sample 81
scenario 80
sending a message 80
server profile customization options 247
using 78
Message Collector session
configuring 57
message of the day, defining 56
messages
error processing 52
prefixed with AFI 257
prefixed with RP 258
voice recording 106
MLT (Multiple Logical Terminals) support 206
Model 2 terminal 200

Model 4 terminal 200
modem communications 71
modem-to-modem paging 99
modems
  installing 33
  paging service types 97
  Telephony Service (TAPI) 33
  testing 34
  using with SA IOM 20
Modify Server Config authority 70
MODSTAT.REX sample script 227
MONTHLY.REX sample script 227
MVS
  configuring display mode 200
MVS console operation, colors 252
MVS MCS console definitions with the IBM 2074 126

N

Netcool/OMNIbus integration 160
NETSAMP.REX sample script 227
NETSCAN.REX sample script 227
network connections between servers 79
notices
  used in this document xvii
notification 186
  ad hoc 189
notification processes 6
NotifyAck.rex sample script 228
NotifyEmail.rex sample scripts 228
NotifyGetAnswer.rex sample script 228
NotifyGetState.rex sample script 228
NotifyPager.rex sample script 228
NotifyScript.rex sample script 228
NotifySMS.rex sample script 228
NotifyVoice.rex sample script 228
null modem cables, pin-outs 202

O

Object REXX 245
OIA status indicators 252
OMEGAVIEW 128
OMEGAVIEW CCC Product Report List 128
operator consoles 5
Operator Information Area (OIA) 252
OSA Integrated Console 122

P

paging services 98
password
  validation
    by SA IOM server 248
    by Windows LogonUser API 248
    specifying a Windows DOMAIN server 248
passwords
  for alert escalation database 156
  for users in ISC 155
patents 275
PCI bus 211
PDF files, adding annotations xix
peer connections
  default port 18
  defining 65
  for ad hoc notification 161
peer connectivity 6
peer-to-peer communications 18
  usage scenarios 87
PeerNCli.rex sample script 228
PeerNSvr.rex sample script 228
PEERSEND.REX sample script 228
PEERSOCK.REX sample script 229
PEERSTRT.REX sample script 229
performance 234
Peripheral Component Interconnect (PCI) bus 211
Persons table
  SA IOM alert escalation 166
  troubleshooting 194
pin-outs, null modem cables 202
policy
  defining 180
  disabling 185
  testing 181
port assignments, default 18
ports, configuring
  connecting to RS-232C serial ports 200
  non-IBM mainframes 200
printing problems xviii
profile files
  locating 31
profile parameters
  at installation time 31
  client profile, details 231
  restart Windows to implement 31
  server profile, details 235

R

recording messages 106
recovery options 66
release level and build date
  SA IOM alert escalation 164
remote client, defined 5
renaming the server 32
requirements
  beeper paging and time acquisition 25
requirements, software 14
Resource/Device Name 124
responsibilities
  performed by system administrator 55
Restarting
  scripts 48
REXX
  sample programs:HMC automation interface 119
REXX functions
  voice applications 106
REXX scripts 8
  BEEPCALL.REX 98
  descriptions of sample programs 225
  HMCACT.REX 119
REXX support
  required in order to 22
roll-deletable mode 200
RP
  prefixed messages 258
rp3270.sys 207
rpclient.exe 16
RpLogRd.exe utility program 140
RpRunRex.exe utility program 142
RpSend.exe utility program 144
rpserver.exe 15
RpSesClr.exe utility program 146

rpsvrmgr.exe 16
rpsvrsvc.exe 15
RS–232 201
RS–422 201

S

SA IOM
  client 45
  emulation features 7
  functional capabilities 5
  installation and verification 27
  logging on as user 38
  logging on the first time 31
  message collection 77
  overview 3
  security 12
  software requirements 14
  verifying installation 30
SA IOM HMC Interface
  components 111
  configuring 112
  required DLLs 113
  S/390 configuration 111
SA IOM network
  scenario 79
SA IOM Service Manager 52
sample REXX programs 225
sample scripts, installing 30
schedules 192
script com ports, defining 56
script management authority 49
scripts
  locating new 30
  stopping 48
scripts, helper 189
security
  considerations 12
  features, general description 8
  in relation to Windows 12
  session classes 62
  user groups 60
serial communications 72
serial ports
  cabling 202
  configuring mainframe ports 200
  expansion adapters 21
  handshaking 201
  on the server are used for 21
serial terminal emulation 7
server
  installing 3270 adapters 205
  IP addresses, configure 161
  starting 35
  starting under Vista 35
  stopping 36
  supported 3270 adapters 205
Server
  name, defining 56
server component states 44
server connection name, defined 32
Server control window 44
server log trace
  setting 238
server name, renaming 32
server pop-up messages
  disabling 243
server profile
  defaults, in general 31
  detailed parameters information 235
server profile file
  locating new 31
Server Status display 44
server, local server 5
service logging 66
session classes 62
session definitions, TN3270E MVS console support 122
Session Properties window 122
sessions
  read only 60
  toggling, MLT 206
setting up
  beeper paging 63
  client connections 64
single client execution 31, 231
SKELETON.REX sample script 229
SLF 128
SLIP 111
software requirements 14
start
  WebSphere Application Server 159
starting
  scripts, from the scripts panel 47
  scripts, with a utility program 142
  the server 35
  the server under Vista 35
status indicators, OIA 252
stop
  escalation 182
  WebSphere Application Server 159
stopping
  the server 36
SUBFUNCT.REX sample script 229
Subsystem Logging Facility (SLF) 128
summary of
  installing 3270 adapters 205
  installing 3270 adapters in an ISA bus machine 207
support, IPv6, enabling 250
supported
  file configurations on the server 12
  voice adapters 103
switch settings
  3270 adapters 207
system administrator
  list of tasks 56
  responsibilities 56
  role of 56
system consoles 5
system log, activating 56

T

Tandem 20, 225
TAP modem protocol
  finding a compatible vendor 98
  used by BEEPCALL.REX 98
TAPI, Windows Telephony Service
  used by client/server modems 33
tasks performed by system administrator 55
TCP/IP
  communications 70
TCP/IP client connections
  default port 18
TCP/IP client-server data, compressing 237

TCP/IP communications 18
TCP/IP error codes 255
TCP/IP keepalive 19
TCP/IP message compression 237
TCP/IP port 18
TCP/IP port assignments, default 18
TCP/IP port for TN3270E 124
Telnet 203
Telnet 3270 terminal emulation 7
Telnet 3270E Connection window 124
Telnet 3270E sessions, configure 121
Telnet server, enabling 236
Telnet terminal emulation 7
terminals
  3278 Model 2 and Model 4 200
testing
  alert escalation 181
  modems 34
  TCP/IP Telnet configuration on Windows 203
time
  delays between characters:touch-tone paging service 98, 100
time acquisition, setting 56
time, of escalation level 186
TIME.REX sample script 229
TIMECALL.REX sample script 229
TN3270E color support 251
TN3270E Emulation Properties window 123
TN3270E keyboard support 221
TN3270E operation requirements 23
TN3270E operational information 251
TN3270E, configuration process 122
trace level
  server log 135
Trace Level
  of rpsvc.log 66
  of rpsvcmgr.log 66
  server log 109
Tracing
  scripts 48
trap manager 6
trapping
  alert information 193
trapping, defined 6
trigger for beeper paging 99
troubleshooting
  alert escalation 196
  alert escalation displays 194
  cables 201
  client/server communication 69
  modems 34
tuning the modem 99

U

unicode 17
uninstalling
  DB2 lite 33
  JRE 33
  SA IOM 32
user groups 60
  default, classic 60
  defining 60
users 63
  alert escalation, creating 151
  assigning access roles to user groups in ISC 154
  assigning to groups in Integrated Solutions Console 155
users *(continued)*
  creating user groups in Integrated Solutions Console 153
  creating users and groups in ISC 154
  modifying users and groups in ISC 155
  overview of steps 151
using SA IOM 3
utility programs 139

V

verifying installation 30
Vista
  context-sensitive help 51
  starting the server 35
voice
  applications 106
  beeper paging 107
  functions 106
  getting listener responses 107
  recording messages 106
voice adapter
  configuring on the server 105
  controlling 103
  debugging 108
  defined 21
  touch-tone paging 98
VOICE.REX sample script 229

W

Web browser
  configuring 195
Web interface, alert escalation 163
Windows Service security considerations 12
Windows Telephony Service (TAPI) 33
wiring connections, diagrams of 202
WTOR
  syntax 99
  tuning for touch-tone pages 101
WTORSCAN.REX sample script 229

Z

z/OS images, consolidating to one session 128
zSeries HMC 111

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other 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 on 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, N.Y. 10504-1785
U.S.A.

For additional information, visit the Web at:
http://www.ibm.com/ibm/licensing/contact/

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

This information could include 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level

systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Copyrights

Trademarks

- Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, and service names may be trademarks or service marks of others.

Printed in USA

SC23-6113-01