

WebSphere® Partner Agreement Manager



# Administrator's Guide

*Version 2 Release 2*

**BIAAAB02**

**Note:** Before using this information and the product it supports, read the information in *Notices* on page 167.

### **Third Edition (July 2001)**

This edition applies to version 2, release 2 of WebSphere Partner Agreement Manager (product number 5724-A85) and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. You can make comments on this information via e-mail at [idrcf@hursley.ibm.com](mailto:idrcf@hursley.ibm.com).

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2000-2001. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# TABLE OF CONTENTS

	<b>WELCOME TO THE ADMINISTRATOR'S GUIDE</b>	<b>ix</b>
	Who should use this information	x
	Related information	x
	<b>SUMMARY OF CHANGES</b>	<b>xiii</b>
<b>CHAPTER 1</b>	<b>ADMINISTERING PARTNER AGREEMENT MANAGER</b>	<b>1</b>
	About Partner Agreement Manager	2
	About configuring Partner Agreement Manager	3
	About administering Partner Agreement Manager	4
<b>CHAPTER 2</b>	<b>ADMINISTERING THE PROCESS SERVER</b>	<b>7</b>
	About the Partner Agreement Manager operating environment	8
	About the Process Server	9
	Starting the Process Server	10
	Starting the Process Server on Windows	10
	Starting the Process Server on UNIX	11
	About the Process Server window	12
	Administering passwords	14
	Changing passwords from the Process Server	14
	Changing passwords from the Process Manager	15

Stopping the Process Server	16
Stopping the Process Server on Windows	17
Stopping the Process Server on UNIX	17
<b>CHAPTER 3 CONFIGURING PARTNER AGREEMENT MANAGER</b>	<b>19</b>
Setting up the Partner Agreement Manager Channel profile	20
Opening your Partner Agreement Manager Channel profile	21
Entering contact information	22
Setting up communications	24
Defining your security profile	33
Setting up certificates	36
Setting up Partner Agreement Manager users	44
About users	45
Setting up the Admin user	45
Adding a new user	47
Removing a user	48
Changing user information	49
Importing user information	50
Exporting user information	52
Setting up system error notifications	54
Specifying termination action reasons	55
Setting up the diagnostic monitoring system	56
About monitored resources	58
Monitored resources	58
About the Partner Agreement Manager SNMP agent	61
<b>CHAPTER 4 SETTING UP PARTNERS</b>	<b>63</b>
About setting up partners	64
Setting up a new Partner Agreement Manager Channel partner	66
Accepting new Partner Agreement Manager Channel partners	69
Updating partner information	75
Sending your channel profile to a specific partner	75
Sending your channel profile to all partners	76

<b>CHAPTER 5</b>	<b>ADMINISTERING THE ADAPTER SERVER</b>	<b>77</b>
	About the Adapter Server	78
	Starting the Adapter Server	80
	About the Adapter Server window	81
	About the Command toolbar	81
	About the status bar	82
	Starting the Adapter Server on Windows	83
	Monitoring operations and events	83
	Starting monitoring	84
	Stopping monitoring	84
	Testing the server connection	84
	Configuring the Adapter Server	85
	Stopping the Adapter Server on Windows	89
	Managing the Adapter Server on UNIX	89
<b>CHAPTER 6</b>	<b>MANAGING ADAPTERS</b>	<b>91</b>
	About managing adapters	92
	Starting the Adapter Manager	93
	Adding adapter instances	94
	Starting or stopping adapter instances	98
	Duplicating adapter instances	100
	Renaming adapter instances	100
	Exporting an adapter instance	101
	Importing an adapter instance	102
<b>CHAPTER 7</b>	<b>AUDITING PROCESSES</b>	<b>103</b>
	About auditing	104
	About Auditor folders	104
	About Auditor messages	105
	Finding an instance of a process	107
	Viewing process information	109
	Using the Process Audit window	110
	Marking an error as resolved	114
	Using the Trace window	115

Archiving and restoring process logs	117
Archiving process logs	117
Scheduling automatic archives	118
Restoring archived process logs	120
Exporting process logs	120
Importing process logs	123
Viewing system messages	124
Deleting system audit information	126
Extracting message information	126
<b>APPENDIX A</b>	<b>USING LDAP WITH PARTNER AGREEMENT MANAGER</b>
	<b>129</b>
About LDAP	130
User information overview	130
Before you install Partner Agreement Manager	132
Installing and configuring Partner Agreement Manager for LDAP	132
Mapping Partner Agreement Manager information to LDAP	133
Mapping user information	134
Mapping partner information	134
Setting up LDAP support after you install Partner Agreement Manager	135
Configuring the Partner.properties file	135
Storing the LDAP password in the MasterStore	136
Using Partner Agreement Manager with LDAP	137
Setting user permissions	137
<b>APPENDIX B</b>	<b>USING THE PAM PROXY SERVER</b>
	<b>139</b>
About the PAM Proxy Server	140
About inbound and outbound messages	141
Requirements	141
Configuring the PAM Proxy Server	142
Example Network Configuration	142
Sample Configuration File	146
Compiling the PAM Proxy Server	148
Running the Proxy Server as an NT service	150
Maintaining the PAM Proxy Server	150

<b>APPENDIX C</b>	<b>USING THE WEB PROXY</b>	<b>153</b>
	About the Web Proxy and the Proxy Broker	154
	Requirements	155
	Using the Web Proxy and the Proxy Broker	156
	Installing and using the Web Proxy	156
	Installing the Web Proxy on Windows NT	157
	Installing the Web Proxy on UNIX	157
	Using the Web Proxy	158
	About the integrated Proxy Broker	158
	Configuring Proxy Broker Properties	159
<b>APPENDIX D</b>	<b>USING THE OUTBOUND PROXY</b>	<b>163</b>
	Using an outbound proxy	164
	Configuring an outbound proxy	164
<b>APPENDIX E</b>	<b>CONFIGURING PAM FOR MQSERIES</b>	<b>165</b>
	About Partner Agreement Manager for MQSeries	166
	Configuring MQSeries for Partner Agreement Manager	166
	Setting transmission properties	167
	Installing an incoming service	169
<b>APPENDIX F</b>	<b>NOTICES</b>	<b>173</b>
	Trademarks	176
<b>GLOSSARY</b>		<b>177</b>
<b>INDEX</b>		<b>185</b>





# WELCOME TO THE ADMINISTRATOR'S GUIDE

This document describes WebSphere® Partner Agreement Manager and explains how to administer and configure Partner Agreement Manager, its servers, and its proxies.

**To administer and configure Partner Agreement Manager, follow these general steps:**

- Read the overview to administering and configuring Partner Agreement Manager. See *Administering Partner Agreement Manager* on page 1.
- Start the Process Server and change passwords as needed. See *Administering the Process Server* on page 7.
- Set up your Partner Agreement Manager profile, set up Partner Agreement Manager users, set system error notifications, specify reasons for termination actions, and set up diagnostic monitoring. See *Configuring Partner Agreement Manager* on page 19. If you are using LDAP, see *Using LDAP with Partner Agreement Manager* on page 129.
- Set up your Partner Agreement Manager partners. See *Setting up partners* on page 63. If you are using LDAP, see *Using LDAP with Partner Agreement Manager* on page 129. If you are using MQSeries® as a transport layer, see *Configuring PAM for MQSeries* on page 165.
- Start the Process Server and monitor operations and events. See *Managing adapters* on page 91.
- Audit running or completed processes. See *Auditing processes* on page 103.

- If you plan to use the Partner Agreement Manager Proxy, see *Using the PAM Proxy Server* on page 139. If you plan to use the Web Proxy, see *Using the Web Proxy* on page 153. To use an outbound proxy, see *Using the Outbound Proxy* on page 163.

## WHO SHOULD USE THIS INFORMATION

This information is for those who need to administer or configure Partner Agreement Manager, its servers, or its proxies.

## RELATED INFORMATION

For additional information see the following:

- The `readme.htm` file. This file may contain information that became available after this book was published. Before installation, the `readme.htm` file is located in the root directory of the product CD-ROM. After installation, the `readme.htm` file is located in the root directory of the Partner Agreement Manager installation.
- The `StartHere.htm` file. This file contains links to the Partner Agreement Manager `readme.htm` file and Installation Guide. Before installation, the `StartHere.htm` file is located in the root directory of the product CD-ROM. After installation, the `StartHere.htm` file is located in the root directory of the Partner Agreement Manager installation.
- The *Partner Agreement Manager Installation Guide*, form number GC34-5964-02, which describes how to install Partner Agreement Manager.
- The *Partner Agreement Manager User's Guide*, form number BIAAAC02, which describes how to start a Partner Agreement Manager session, design public and private processes, define element definition sets, create business objects, and manage process distribution.
- The *Partner Agreement Manager Adapter Developer's Guide*, form number BIAAAD02, which describes how to develop and administer adapters using the Partner Agreement Manager Adapter Development Environment.
- The *Partner Agreement Manager Script Developer's Guide*, form number BIAAAE02, which describes how to write scripts used in Partner Agreement Manager private processes and elsewhere.

- The *Partner Agreement Manager External API Guide*, form number BIAAAF02, which describes principles behind the Partner Agreement Manager External API. See also the Javadoc for the External API, which is installed in the Partner Agreement Manager Docs folder.
- The *Partner Agreement Manager Adapters for MQSeries User's Guide*, form number BIAAAG02, which describes how to install, configure, and run the Partner Agreement Manager Adapters for MQSeries.
- The *Partner Agreement View User's Guide*, form number GC34-5965-02, which describes how to install, configure, and use Partner Agreement View.





# SUMMARY OF CHANGES



This edition includes these changes since the previous, second, edition:

- *External APIs.* Partner Agreement Manager 2.2 provides added flexibility to external applications through additional APIs. These APIs let third-party applications take advantage of the Partner Agreement Manager partner management and process engine through programmatic access. The API is distributed as a set of Java classes that the external application can import. Communication between the API classes and the Process Server is through RMI, but in the future can be swapped out for HTTP or SOAP. Specifically, APIs have been added to the following functional areas:
  - Session Service API
  - Admin Service API
  - Document Service API
  - Partner Service API
  - Adapter Service API
  - Process Service API

- *LDAP Support.* Partner Agreement Manager 2.2 provides centralized user authentication and administration through an LDAP directory. Partner Agreement Manager can retrieve user information—such as name, e-mail address, phone, and fax—stored in an LDAP directory. Updating this information is done in a single place, through the LDAP management tool. Users are authenticated through the same directory, giving them single-sign-on capabilities across enterprise applications.
- *Double-byte character sets (DBCS) and National Language Support (NLS).* Double-byte character sets are now supported in Partner Agreement Manager 2.2. Double-byte and multibyte data can be transferred and operated on in business objects and adapters. NLS lets Partner Agreement Manager display user interface text in other languages.
- *Improved XML Support.* The Partner Agreement Manager 2.2 engine fundamentally changes the way it interacts with business objects by replacing proprietary parsers with a third-party parser. This simplifies support of DTD 1.0 and the support of XML Schemas when the standard is finalized.

The Business Object and Script API have been extended with new classes and methods. The new classes and methods let you work with business objects as W3C Documents.

- *Adapter Asynchronous Callback.* An additional Adapter API allows adapters to be more efficient with long-running adapter operations. The Asynchronous Callback method tells the Adapter Server that an operation will be long-running, that system resources should be freed while the adapter waits for a response from the end system, and that another method will be called when the response arrives. The Asynchronous Callback method frees the adapter developer from using the request-retry method that makes the Adapter Server responsible for polling the end system for the response.
- *Script API Changes.* The script API now provides access to the PartnerGroupContext and the Public and Private Process Contexts. Through these contexts, you can get information such as partner group binding, a reference to the process, inputs to the process (which contain a reference to the sender, the ID of the sending node, and the variable name), and unique node and loop IDs.

- *Certificate Support.* Partner Agreement Manager 2.2 is able to request and import certificates from certificate authorities like VeriSign. This lets organizations use their existing certificate, or request a new one if their partners do not accept self-signed certificates. Partner Agreement Manager 1.1 supported only self-signed certificates.
  - *Outbound Proxy Support.* Partner Agreement Manager 2.2 channels that use HTTP communication can work with outbound proxies that use authentication. Outbound proxy authentication is used within *internal* networks to ensure that only people and applications that are authenticated may communicate with an *external* network. Authentication in the outbound proxy is done with a standard user name and password combination. You can turn on the outbound proxy feature after installation. Thereafter, all outbound HTTP communication will use the same user name and password combination for the proxy.
- NOTE:** Note that this feature is only used by channels using HTTP communication; it does not apply to channels that use the built-in Partner Agreement Manager proxy.





# ADMINISTERING PARTNER AGREEMENT MANAGER

Welcome to WebSphere Partner Agreement Manager 2.2, the leading B2B software platform. Partner Agreement Manager is designed to create a seamless web of electronic communications and commerce between businesses over the Internet—helping you to work more closely and effectively with your partners, suppliers and customers.

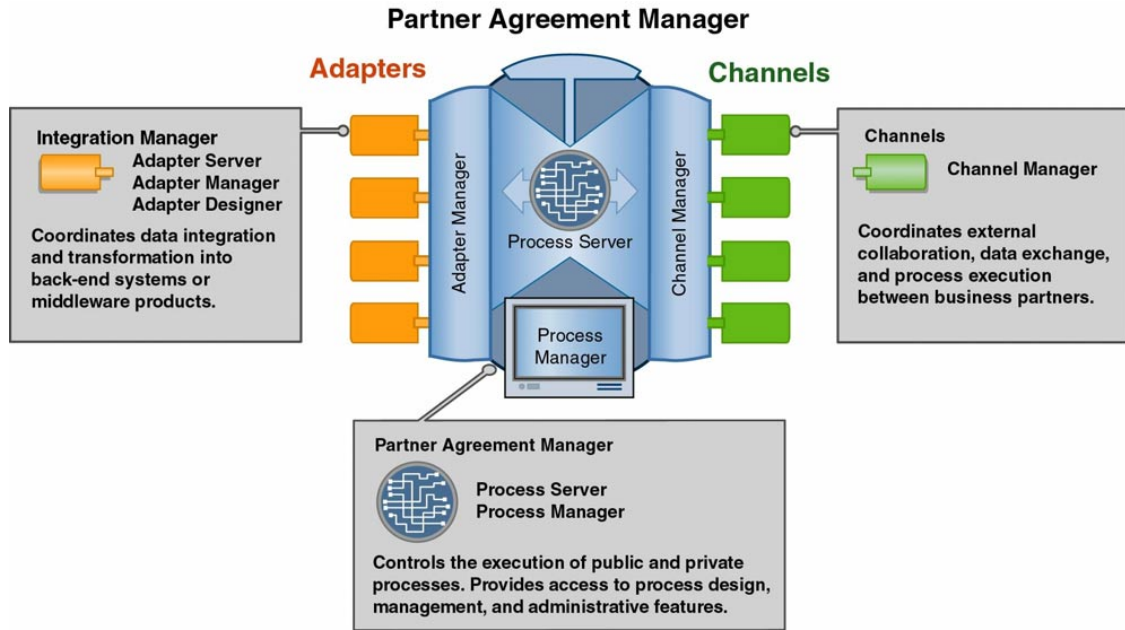
This book describes how to set up, configure, and administer your Partner Agreement Manager installation.

This introductory chapter is an overview that includes:

- *About Partner Agreement Manager* on page 2.
- *About configuring Partner Agreement Manager* on page 3.
- *About administering Partner Agreement Manager* on page 4.

# ABOUT PARTNER AGREEMENT MANAGER

Using Partner Agreement Manager, an enterprise can communicate with its business partners using fully integrated, real-time connections. Partner Agreement Manager facilitates the flow of business information between partners in a controlled, secure environment. You and your trading partners can work together effectively, yet maintain organizational independence when you need it.



The key components of Partner Agreement Manager are:

- Partner Agreement Manager (core) supports the execution of public and private processes. This is where you design processes and create business objects that manage the transfer of information. Within Partner Agreement Manager:
  - The Process Server is the engine that powers Partner Agreement Manager.

- You use the Process Manager to design public and private processes, design formats for sharing business information, and manage processes. You use the Public Process and Private Process windows to build public and private processes. Public processes define the flow of actions and information between partners. Private processes determine the actions that each partner takes for its step in the public process.

**NOTE:** In earlier releases of Partner Agreement Manager, the Process Manager window was called the Partner Agreement Manager window, or the Explorer window.

- The Integration Manager provides the connection and takes care of data transformation when you need to exchange information with back-end or other systems within your organization. Within the Integration Manager:
  - The Adapter Server is the engine that powers integration.
  - You use the Adapter Manager to add, remove, start, and stop adapters.
  - You use the Adapter Designer to create or modify adapter types that provide connectivity to end systems. Depending on the end system, you might also be able to use integration wizards to create adapters.
  - Individual adapters provide for integration with specific back-end systems. Examples are the adapters for MQSeries.
- The Channel Manager supports the configuration and management of the channels Partner Agreement Manager uses to connect you to your partners. Each channel has its own characteristics and capabilities. An example is Channel for RosettaNet.

## ABOUT CONFIGURING PARTNER AGREEMENT MANAGER

Here's a brief overview of the steps involved in configuring Partner Agreement Manager and where to locate information about each step.

- STEP 1** Install Partner Agreement Manager. (For more information, see the *Partner Agreement Manager Installation Guide*.)
- STEP 2** Start the Process Server and the Process Manager. (For more information, see *Administering the Process Server* on page 7.)
- STEP 3** Set up your Partner Agreement Manager Channel profile. (For more information, see *Configuring Partner Agreement Manager* on page 19.)

- STEP 4** Set up your Partner Agreement Manager users. (*Configuring Partner Agreement Manager* on page 19.)
- STEP 5** Set up your system error notifications, termination action reasons, and diagnostic monitoring system. (*Configuring Partner Agreement Manager* on page 19.)
- STEP 6** Set up your Partner Agreement Manager partners. (*Setting up partners* on page 63.)
- If you are setting up LDAP partners or users, see *Using LDAP with Partner Agreement Manager* on page 129.
  - If you are using the Partner Agreement Manager Proxy, see *Using the PAM Proxy Server* on page 139.
  - If you are setting up a partner channel that requires the Web Proxy, see *Using the Web Proxy* on page 153.
  - If your channel uses HTTP communication, you can use an outbound proxy for authentication. For more information, see *Using the Outbound Proxy* on page 163.
  - If you are using MQSeries as your transport layer, see *Configuring PAM for MQSeries* on page 165.
- STEP 7** Set up and configure your Adapter Server. (For more information, see *Administering the Adapter Server* on page 77.)
- STEP 8** After you have installed or created adapters, add adapter instances as needed. (For more information, see *Managing adapters* on page 91. For more information about adapters, see the documentation for each adapter. For more information about utility adapters and the Adapter Development Environment, see the *Partner Agreement Manager Adapter Developer's Guide*.)

## ABOUT ADMINISTERING PARTNER AGREEMENT MANAGER

Here's a brief overview of the steps involved in administering a Partner Agreement Manager installation and where to locate information about each step.

**STEP 1** Design your public processes and business objects. Distribute the public processes to your partners for approval. Design your private processes plus any private business objects you'll use to transfer information internally within a private process. (For more information, see the *Partner Agreement Manager User's Guide*.)

As part of a private process, you might need to include one or more adapters. (For more information about adapters in general and the Adapter Development Environment, see the *Partner Agreement Manager Adapter Developer's Guide*. For information about specific adapters, see the guides that accompany any adapters you might have already installed.)

The actions in your private processes will also include scripts. (For more information, see the *Partner Agreement Manager Script Developer's Guide*.)

**STEP 2** Install your processes and start running them. (For more information, see the *Partner Agreement Manager User's Guide*.)

**STEP 3** After you have created and installed processes, use the Auditor to track process instances. (For more information see [Auditing processes](#) on page 103.)



# ADMINISTERING THE PROCESS SERVER

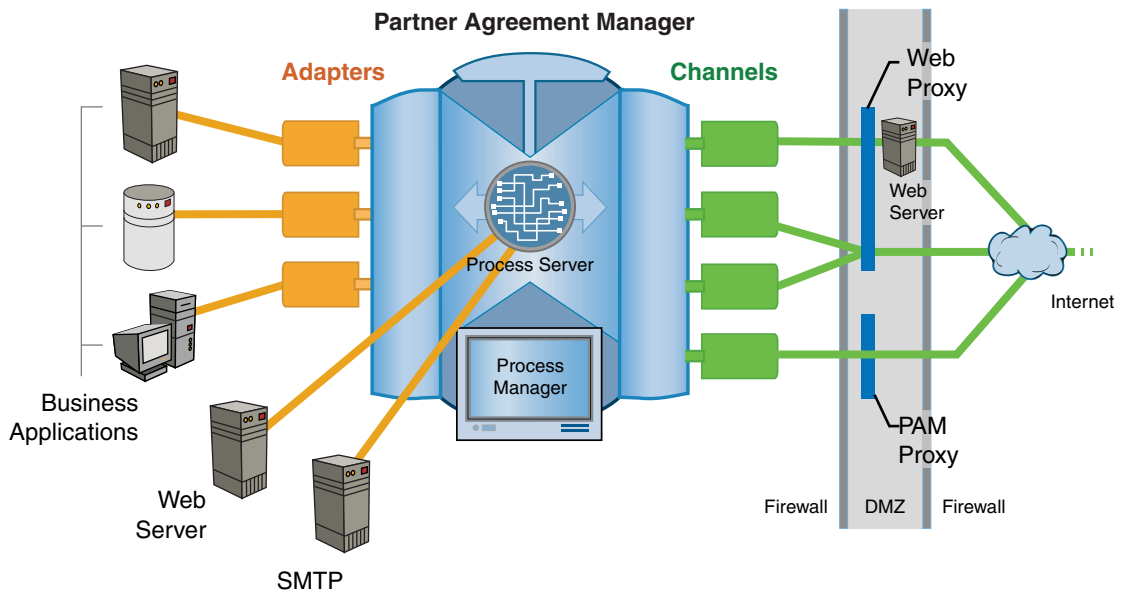
Read this chapter for information about starting and administering the Partner Agreement Manager Process Server, including starting and stopping the Process Server and administering passwords.

This chapter includes these sections:

- *About the Partner Agreement Manager operating environment* on page 8.
- *About the Process Server* on page 9.
- *Starting the Process Server* on page 10.
- *About the Process Server window* on page 12.
- *Administering passwords* on page 14.
- *Stopping the Process Server* on page 16.

# ABOUT THE PARTNER AGREEMENT MANAGER OPERATING ENVIRONMENT

Like most enterprise-wide applications, Partner Agreement Manager has a complex operating environment that extends beyond the boundaries of the Partner Agreement Manager software to include other software and hardware components—all of which can affect the success of a Partner Agreement Manager installation.



The Partner Agreement Manager operating environment includes these hardware and software components:

- **Partner Agreement Manager**

Partner Agreement Manager consists of components that communicate with each other over a distributed object framework. The information managers, transporter, execution engine, and database are referred to collectively as the Process Server. See *About the Process Server*, next.

- **Business applications**

Partner Agreement Manager can interact with a variety of additional applications that reside on the corporate network. These applications range from complex, multi-functional enterprise resource planning applications to simple spreadsheet applications.



- Mail and Web servers

Partner Agreement Manager interfaces with both an SMTP server and Microsoft's Internet Information Server (IIS) web server to execute notification and approval actions within a Partner Agreement Manager process. Notification actions send e-mail to a specified user. Approval actions pause a process and elicit input from a specified user before proceeding.

- Network communication and firewalls

Partner Agreement Manager relies on several networking components. Within the enterprise, Partner Agreement Manager uses the corporate internal network (intranet) for connections to business applications, SMTP servers, Partner Agreement Manager clients, and so forth. For communications between partners, Partner Agreement Manager can use the Internet, a dial-up connection, or message queuing (TCP/IP or dial-up). For security reasons, most companies implement a firewall to limit incoming and outgoing messages to and from the Internet. Therefore, the firewall must be configured (via a proxy server or other means) to allow your Partner Agreement Manager installation to communicate with other Process Servers outside the firewall. (For more information, see [Using the PAM Proxy Server](#) on page 139.)

- Hardware

The Process Server software usually resides on a single Windows server, although it is possible to split the Partner Agreement Manager components to run on more than one computer.

## ABOUT THE PROCESS SERVER

The Process Server is a collection of components that support your efforts as you design, test, deploy, maintain, and run extended enterprise processes. The Process Server also serves as the connection point for any Partner Agreement Manager clients that might be running. Different components can be run on single or multiple hosts.

Because it plays such a central role in providing Partner Agreement Manager functionality, the Process Server must be running whenever processes are being tested, deployed, or executed.

The Process Server consists of these elements:

- Information managers

Information managers control Partner Agreement Manager information, implement application logic, and ensure information consistency.

- Execution engine

The execution engine manages the set of installed processes (with the help of the Information Managers) and coordinates their execution.

- Transport manager

The transport manager manages communications and security between partners.

- Database

The database stores all Partner Agreement Manager data—process definition, process execution, and channel profiles—as well as audit information. It communicates through a Java Database Connectivity (JDBC) layer and is installed on the Microsoft SQLServer. Although the database typically resides on the same server as Partner Agreement Manager, it can be installed on another server as long as Partner Agreement Manager can connect to the database over an internal network.

## STARTING THE PROCESS SERVER

You start the Process Server the same way you do any other application. For security reasons, only the admin user can log in to the Process Server.

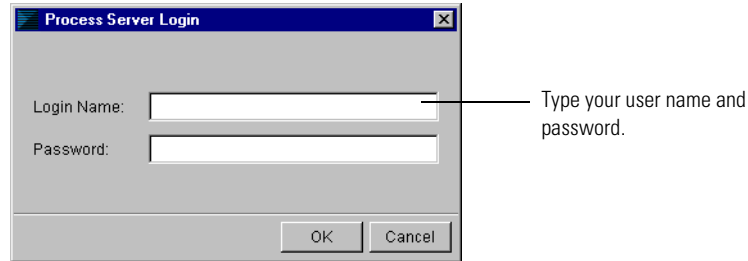
### STARTING THE PROCESS SERVER ON WINDOWS

**NOTE:** When you installed Partner Agreement Manager, you might have installed it to run as an NT service. If so, the Process Server automatically starts whenever you start the Process Server computer. You must start the Process Server before you can start any other Partner Agreement Manager component.

#### To start the Process Server:

- 1  Click Start>Programs>IBM WebSphere Business Integrator>Process Server (*partner name*).

The Process Server Login dialog box appears.



- 2 Type your Partner Agreement Manager user name (login name) and password. Click OK.

The preset user name for the admin user is `admin`. The password is set when you install Partner Agreement Manager. User names are not case-sensitive, but passwords are.

The Process Server window appears. See [About the Process Server window](#) on page 12.

## STARTING THE PROCESS SERVER ON UNIX

**NOTE:** When you installed Partner Agreement Manager, you might have installed it to run as an NT service. If so, the Process Server automatically starts whenever you start the Process Server computer. You must start the Process Server before you can start the Adapter Server.

### To start the Process Server:

- 1 Go to your Partner directory with the command:  

```
cd /YourPartner Agreement ManagerInstallDir/Partners/Partnernnn
```

where *YourPartner Agreement ManagerInstallDir* is where you installed Partner Agreement Manager and *nnn* is a placeholder for your Partner number.
- 2 Run the script to create the Process Server environment variables:  

```
. Scripts/setCEnv .
```

Note the spaces between the text and the dots.  
The second dot specifies the current directory.
- 3 Start the Process Server:  

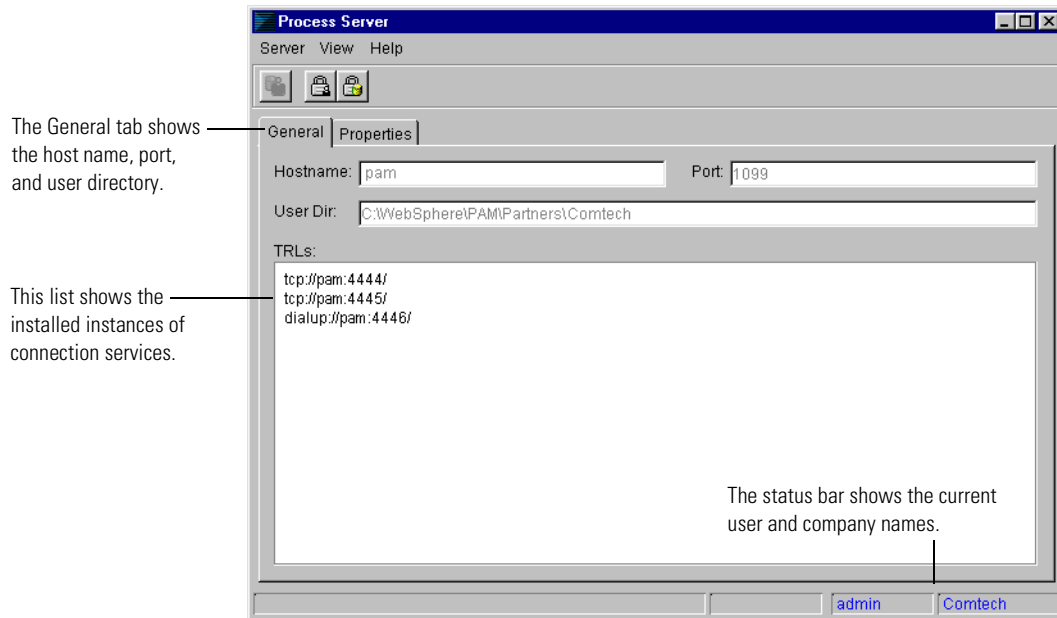
```
alliance -server 2>&1
```

The server will log output to `logs/Partner Agreement Manager.log`. As this file grows, you might want to look at the most recent output in that file with the command:

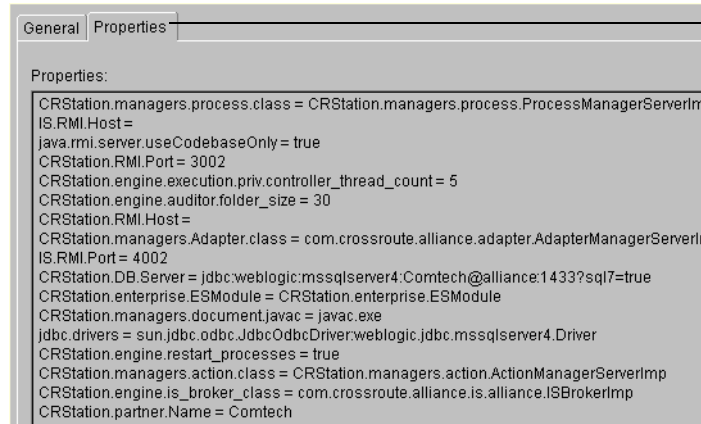
```
tail -f Partner Agreement Manager.log
```

## ABOUT THE PROCESS SERVER WINDOW

On Windows, the Process Server window displays information about the current Partner Agreement Manager installation (such as host name and port) and gives you access to configuration tasks. Using the Process Server, you can change the passwords for the Process Server or database modification. You can also import users. The Process Server window is not supported on UNIX.



The Properties tab shows the values from the various properties files that Partner Agreement Manager uses.



The Properties tab shows the current values gleaned from the properties files that Partner Agreement Manager uses.

Partner Agreement Manager uses these properties files to collect and store information about your Partner Agreement Manager installation. One group of properties files is located in the root folder. A second group is located in your partner folder. Collectively, they provide Partner Agreement Manager with the information it needs to identify your Partner Agreement Manager installation and to enable the various Partner Agreement Manager components to work together.

Partner Agreement Manager creates all of the properties files it requires during installation and populates them with the correct values based on the installation information you provide.

**NOTE:** In general, Partner Agreement Manager property files are not designed to be edited. If changes occur in your installation—such as new server host names or ports—please contact your IBM representative. The only file that you need to consider editing is the `partner.properties` file. See [Setting up system error notifications](#) on page 54.

# ADMINISTERING PASSWORDS

Partner Agreement Manager makes it easy to change or remove the passwords associated with the Partner Agreement Manager database and with enterprise systems that Partner Agreement Manager connects with. If you are the Partner Agreement Manager administrator, you can change passwords for a Process Server from either the Process Manager or the or the Process Server. For compatibility, if you are running the Process Server on UNIX, you must use the Process Manager provided with the UNIX server distribution. For information on installing the Process Manager, see the *Partner Agreement Manager Installation Guide*.

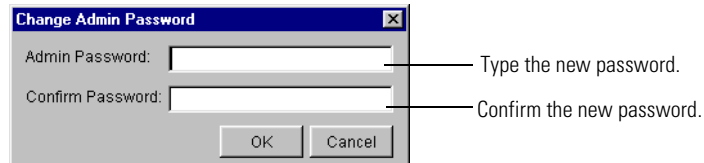
## CHANGING PASSWORDS FROM THE PROCESS SERVER

On Windows, you can use the Process Server window to change passwords. On UNIX, use the Process Manager to change passwords. From the Process Server, you can change either the administrator's password or the password associated with data modification for the Partner Agreement Manager database. The password for the Partner Agreement Manager database was established when the database was created.

### To administer passwords from the Process Server:

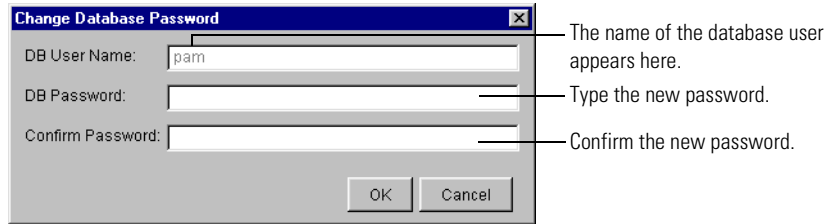
- 1 Choose a command from the Server menu.
  - To change the Partner Agreement Manager administrator's password, choose Change Admin Password.

The Change Admin Password dialog box appears.



- To change the database password for the data modification user, choose Change Database Password.

The Change Database Password dialog box appears.



- 2 Type a new password and confirm it. Click OK.

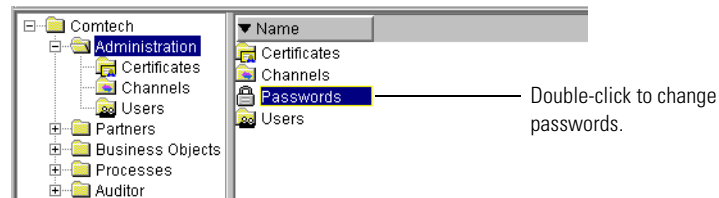
All future connections to the Partner Agreement Manager database will use the new password. The new admin password takes effect the next time you log in to the Process Server.

## CHANGING PASSWORDS FROM THE PROCESS MANAGER

From the Process Manager, you can change or remove passwords for databases and enterprise systems that Partner Agreement Manager connects with. You can use the Process Manager to change passwords for a Process Server, regardless of the platform the Process Server is running on.

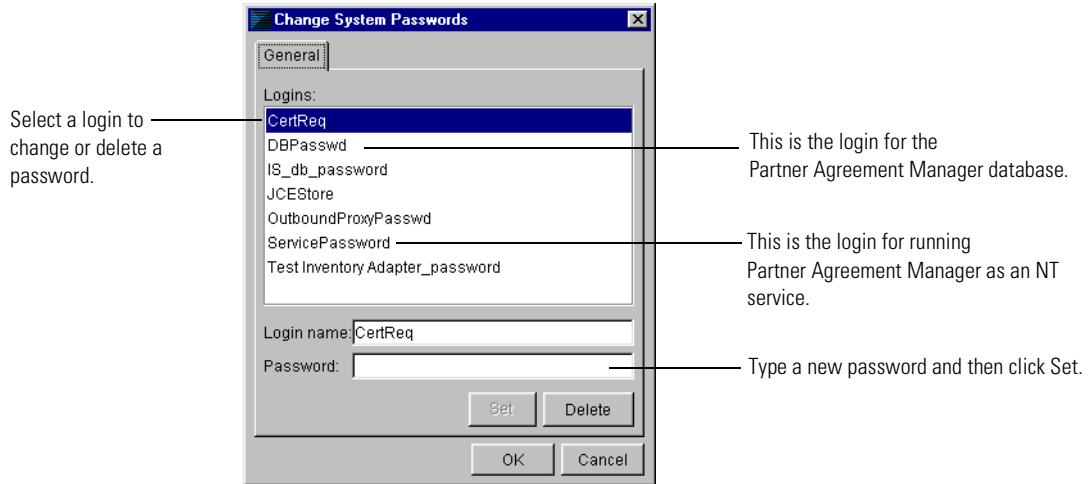
### To change passwords from the Process Manager:

- 1 Open the Administration folder in the Process Manager window.



- 2 Double-click the Passwords item.

The Change System Passwords dialog box appears.



- 3 Select a login name and make any necessary changes.
  - To change a password, type a new password, and click Set.
  - To delete a password, click Delete.
- 4 Click OK.

## STOPPING THE PROCESS SERVER

You can stop the Process Server as needed. As soon as you stop the Process Server, any processes that are currently running will be halted. Partner Agreement Manager notes the state of each running process so that each process can pick up where it left off when the server is restarted.

In addition, until the Process Server is restarted:

- no new processes can start.
- users can't create or modify private or public processes.

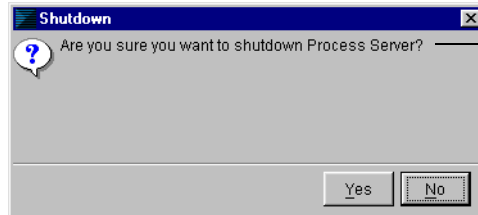


## STOPPING THE PROCESS SERVER ON WINDOWS

### To stop the Process Server:

- 1 Choose Exit from the Server menu.

Partner Agreement Manager asks you to confirm that you want to stop the server at this time.



Partner Agreement Manager asks you to confirm that you want to stop the Process Server.

- 2 Click Yes.

## STOPPING THE PROCESS SERVER ON UNIX

### To stop the Process Server:

- ▶ Stop the Process Server with the following command:

```
pam -stop -server
```

**NOTE:** UNIX might keep TCP ports in TIME\_WAIT state for up to 5 minutes. You can monitor port status with the command:

```
netstat -a
```

If you attempt to restart the Process Server before UNIX has released the ports, you will get a bind error because the ports are already in use.



## CONFIGURING PARTNER AGREEMENT MANAGER

Read this chapter for information about configuring Partner Agreement Manager, including setting up the Partner Agreement Manager Channel profile, setting up Partner Agreement Manager users, setting up system error notifications, and selecting a cryptographic service provider. For information on other supported channels (such as EDI, RosettaNet, or cXML), see the appropriate Partner Agreement Manager documentation for that channel.

You configure Partner Agreement Manager using the Process Manager, which you must install on a Windows system. For more information on installing the Process Manager, see the *Partner Agreement Manager Installation Guide*.

This chapter includes these sections:

- *Setting up the Partner Agreement Manager Channel profile* on page 20.
- *Setting up Partner Agreement Manager users* on page 44.
- *Setting up system error notifications* on page 54.
- *Specifying termination action reasons* on page 55.

# SETTING UP THE PARTNER AGREEMENT MANAGER CHANNEL PROFILE

Each company's Partner Agreement Manager provides the basis for exchanging information between business partners. A company channel profile includes four types of information:

- *Corporate information* includes information that was entered when you installed Partner Agreement Manager—partner name and ID, for example. It also includes information you enter when you set up your channel profile, such as contact information.
- *Contact information* identifies the primary person to contact for issues regarding Partner Agreement Manager. See [Entering contact information](#) on page 22.
- *Communication settings* specify the services you use to send information to, and receive information from, your partners. You can set up one or more Internet services to communicate via the Internet, extranet, or private networks. You can also set up dialup services to communicate with partners by modem, or message queueing services such as IBM's MQSeries (supported on UNIX and Windows). If you set up several services, you can specify the order in which Partner Agreement Manager uses them to send and receive information. See [Setting up communications](#) on page 24.
- Your *security profile* consists of policy options, cryptographic algorithms, and certificates that safeguard your communications with partners. See [Defining your security profile](#) on page 33.

**NOTE:** Only the admin user can initially set up or change the Partner Agreement Manager Channel profile. The admin user can then set up other users and give them permission to change the Partner Agreement Manager Channel profile. See [Setting up Partner Agreement Manager users](#) on page 44.

After setting up your Partner Agreement Manager Channel profile, you set up your Partner Agreement Manager partners and then exchange profile information with them to enable secure connectivity. See [About setting up partners](#) on page 64.

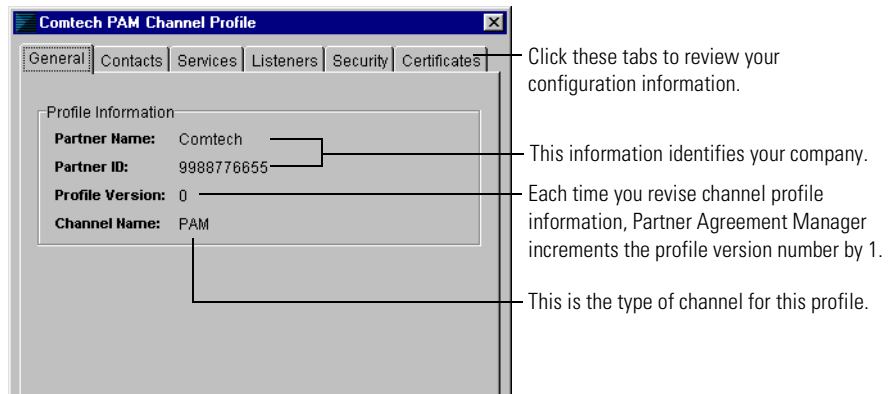
Each time you revise channel profile information—for example, to change a contact name, or to modify security information—Partner Agreement Manager increments the channel profile version number to help you and your partners synchronize channel profile information.

## OPENING YOUR PARTNER AGREEMENT MANAGER CHANNEL PROFILE

To open your Partner Agreement Manager Channel profile:

- 1 Open the Administration folder in the Process Manager window.
- 2 Open the Channels folder and double-click your Partner Agreement Manager Channel profile.

The Channel Profile dialog box appears, with the General tab selected. The General tab shows your corporate information.



The General tab shows the partner name and ID that was entered during Partner Agreement Manager installation. It also shows the version of the channel profile, which increments each time you revise profile information. The channel name shows the type of channel for this channel profile.

Use these tabs to enter channel profile information.

**Contacts** Enter information about your company and to identify the person at your company to contact with Partner Agreement Manager issues. See [Entering contact information](#) next.

**Services** Configure your installed communication services for transmissions to your partners. See [Setting up communications](#) on page 24 and [Setting up service types](#) on page 26.

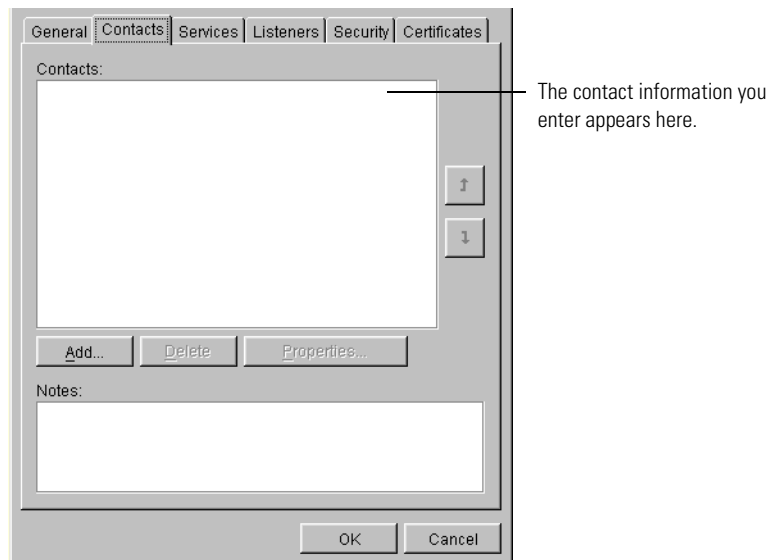
- Listeners** Set up services for incoming communications from your partners. See *Setting up communications* on page 24 and *Setting up a listener service* on page 29.
- Security** Define your security profile. See *Defining your security profile* on page 33.
- Certificates** Set up certificates. Certificates work with the security options during information exchange, to safeguard communications with your partners. See *Setting up certificates* on page 36.

## ENTERING CONTACT INFORMATION

Contact information includes information about your company and identifies the primary person to contact for issues regarding Partner Agreement Manager. Contact information also specifies the way to reach the contact person—for example, an e-mail address.

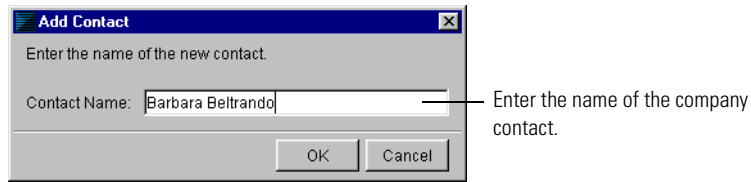
### To enter contact information:

- 1 Open the Admin\Channels folder and open your Partner Agreement Manager Channel profile by double-clicking its icon.  
The Partner Agreement Manager Channel Profile window appears.
- 2 Click the Contacts tab.



3 Click Add.

The Add Contact dialog box appears.



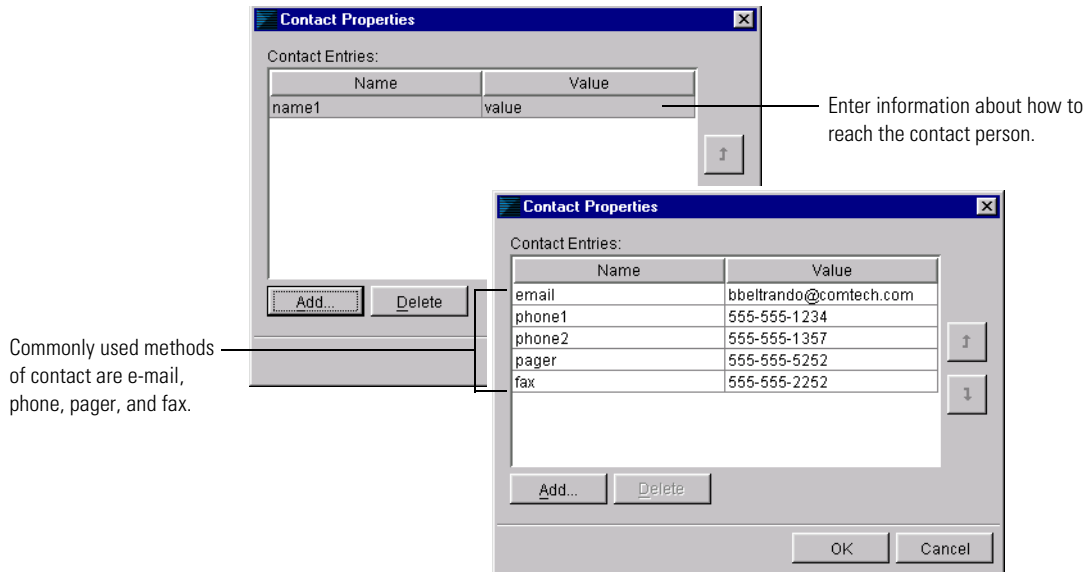
4 Type in the name of the company contact person and click OK.

The Contacts tab shows the name of the contact.

5 Click Properties in the Contacts tab.

Use the Contact Properties dialog box to specify how to reach the contact person.

6 Click Add.



7 Enter the contact method in the Name field and the appropriate matching information in the Value field.

For example, the Name field might specify “email” and the Value field specify the e-mail address for the contact person. Use the arrow keys to rearrange the entries if necessary.

8 Click OK.

## SETTING UP COMMUNICATIONS

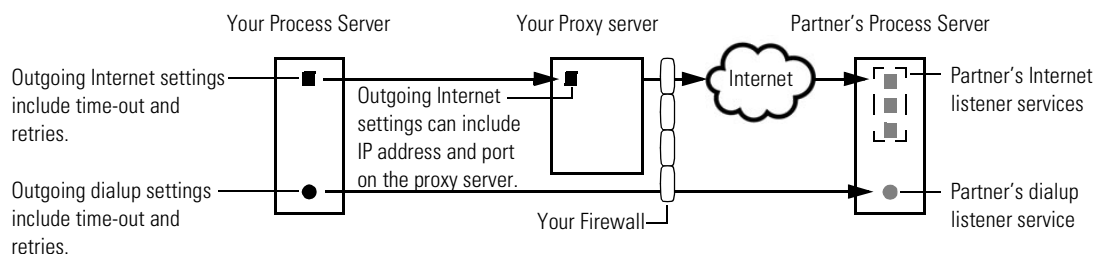
Partner Agreement Manager Channel supports three types of communication services—Internet, dialup, and message queueing services such as IBM’s MQSeries. Internet and dialup are synchronous communication services. With Internet services, you and your partners communicate via the Internet or a private network. With dialup services, you and your partners communication using a direct modem-to-modem connection.

A message queueing service is an asynchronous, application-independent method of network communication that is based on a message queueing model. MQSeries from IBM is supported on both the UNIX and Windows versions of Partner Agreement Manager. For more information on installing and configuring MQSeries, see the *Partner Agreement Manager Adapters for MQSeries User’s Guide*.

When you set up communication services, you configure the *service types*—Internet, dialup, or message queueing—that you use to send messages, and that your partners use to accept communications from you.

You set properties for your service types, including a time-out interval to specify the amount of time Partner Agreement Manager waits for a reply from your partner before cancelling a connection attempt. For synchronous services (Internet and dialup), you also specify the number of times to retry the connection.

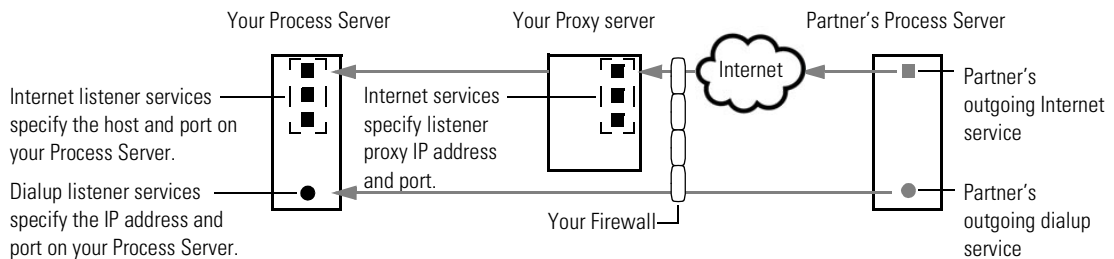
If Partner Agreement Manager needs to connect through a firewall, Internet service type settings must also include proxy settings for the IP address and port on the Partner Agreement Manager server side of the proxy server (as opposed to the Internet side). See [Setting up service types](#) on page 26 and [Setting up a listener service](#) on page 29. For more information on proxy servers, see [Using the PAM Proxy Server](#) on page 139 and [Using the Web Proxy](#) on page 153.





After setting up your service types, you specify at least one *listener service* for your partner's Process Server to communicate with when sending communications to you.

If Partner Agreement Manager is receiving messages on an Internet listener through a firewall, you can specify incoming proxy settings (IP address and port). The settings for dialup listener service include the telephone number, baud rate, and the host name and port on your Process Server. Settings for an MQSeries listener include queue manager, queue name, and error queue. See [Setting up a listener service](#) on page 29.



When you put it all together, a typical synchronous communication between partners might work like this:

- You start a Partner Agreement Manager process that sends a message to a partner.
- Partner Agreement Manager looks at your copy of the partner's channel profile and selects the first listener service listed by your partner—for example, Internet.
- Partner Agreement Manager then looks at your own transmission settings for the corresponding service type to see how long a time-out you set and how many retries you permit.
- If the selected service type is Internet and you entered proxy settings, Partner Agreement Manager gets the IP address and port for access to your proxy server.

- Partner Agreement Manager applies the appropriate security and tries to send the message. Assuming an Internet service, the message goes through your proxy server (if necessary) and via the Internet to your partner's proxy server (also if necessary). The proxy server reroutes it to the IP address for this partner's Process Server.
- If the first attempt times out, Partner Agreement Manager retries. If Partner Agreement Manager runs out of retries for the first service, it tries the second service on the partner's list. Partner Agreement Manager keeps trying until the message is received or until it runs out of time-outs, retries, and listener services.

### SETTING UP SERVICE TYPES

Partner Agreement Manager uses service properties to determine the time-out (for all services) and number of retries permitted for outgoing communications (synchronous services only). Time-out is the amount of time Partner Agreement Manager waits for a reply before cancelling a connection attempt. Retries specifies the number of times Partner Agreement Manager attempts to send a message before giving up.

**NOTE:** Because MQSeries is an asynchronous communication service, there are no Partner Agreement Manager retry properties to set. MQSeries manages message queueing and retries as needed.

For Internet service, additional settings let you connect through a proxy server. For more information on proxy servers, see *Using the PAM Proxy Server* on page 139, *Using the Web Proxy* on page 153, and *Using the Outbound Proxy* on page 163.

---

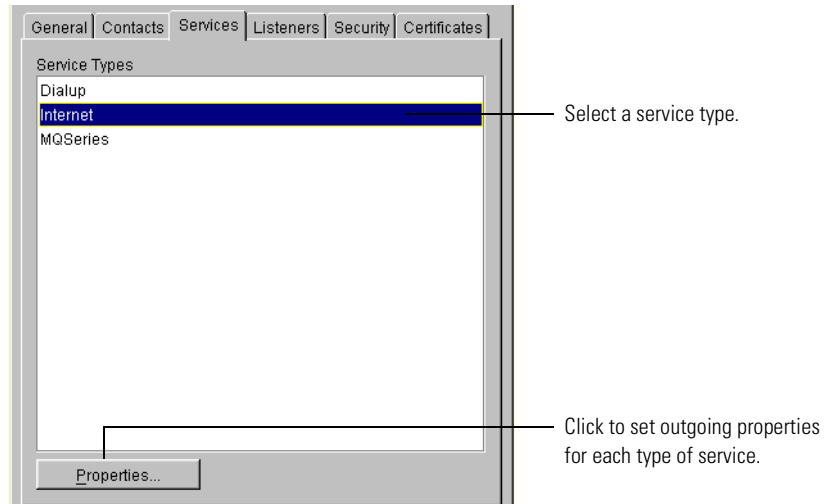
**IMPORTANT:** You must set up at least one valid internet or dialup service. These are synchronous services. Process Control Messages generated by Partner Agreement Manager require a synchronous transport. Queueing services such as MQSeries are asynchronous.

---

### To set up service types:

- 1 Open your Partner Agreement Manager Channel profile and click the Services tab.

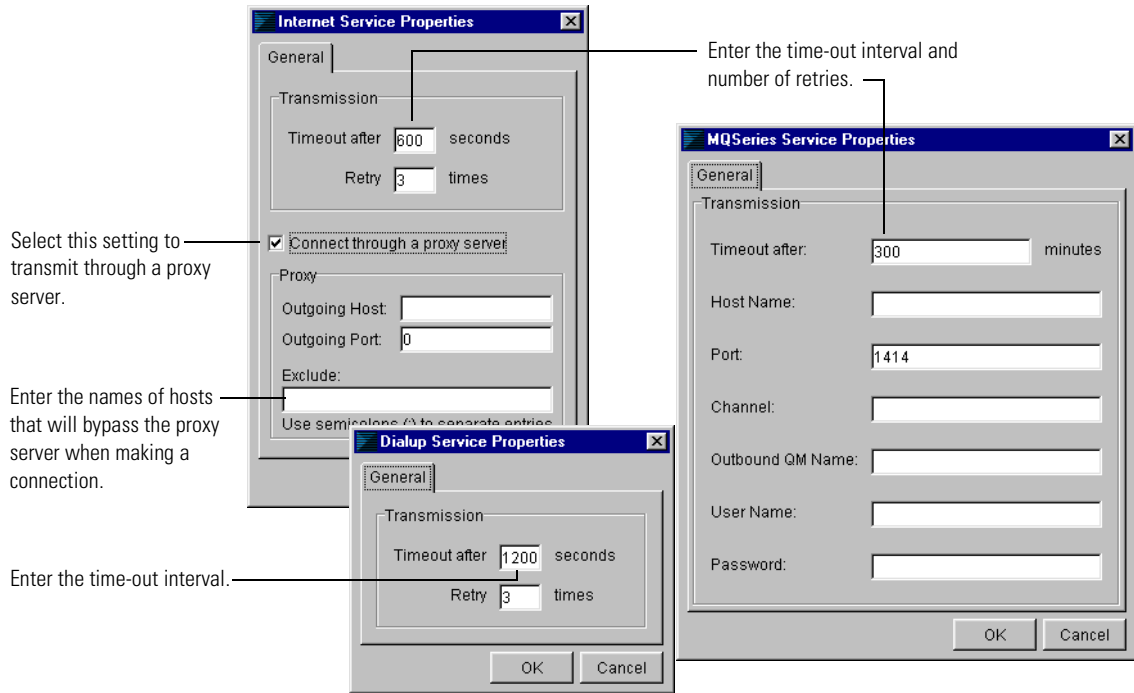
The Services tab appears.



- 2 Select a service type from the list, and click Properties to set the properties for that service type.

The Service Properties dialog box appears for the service type you selected.

Both Internet and dialup services use time-out and retry settings for outgoing transmissions. Internet services can also specify proxy server settings for communication with a proxy server. MQSeries service has only a time-out interval. For more information on proxy servers, see *Using the PAM Proxy Server* on page 139 and *Using the Web Proxy* on page 153.



### 3 Enter the appropriate information.

#### For this type of service

#### Do this

Internet

1. Enter the time-out interval and number of retries.
2. If you use a proxy server, turn on the Connect through a Proxy Server setting, enter the proxy server's outgoing IP address and port, and enter the names of hosts that bypass the proxy server. The outgoing IP address and port correspond to the OUTBOUND\_LISTENER directive in the proxy.cnf file.

Dialup

Enter the time-out interval and number of retries.

MQSeries

Enter the time-out interval, the host name, the MQSeries port, the channel, the outbound queue manager name, the user name and password.

**TIP:** You only need to set up properties for the service types you will use with your partners. For example, if your partners only accept incoming Internet connections, it is not necessary to set properties for dialup or message services.

- 4 Click OK in the Service Properties dialog box.

#### SETTING UP A LISTENER SERVICE

The settings for a Partner Agreement Manager listener service provide your partners with the information they need to communicate with you. Because reliable communication is important to running processes, Partner Agreement Manager lets you set up as many incoming services as you want—both synchronous (Internet or dialup) and asynchronous (MQSeries).

If your partner's Partner Agreement Manager is unable to connect using the first listener service listed in your channel profile, it tries the next service in the list, and keeps trying the services in the list until the message is received or until it runs out of time-outs, retries, and listener services.

**NOTE:** Partner Agreement Manager rolls over from one synchronous or asynchronous service to the next, but does not roll over between synchronous and asynchronous services.

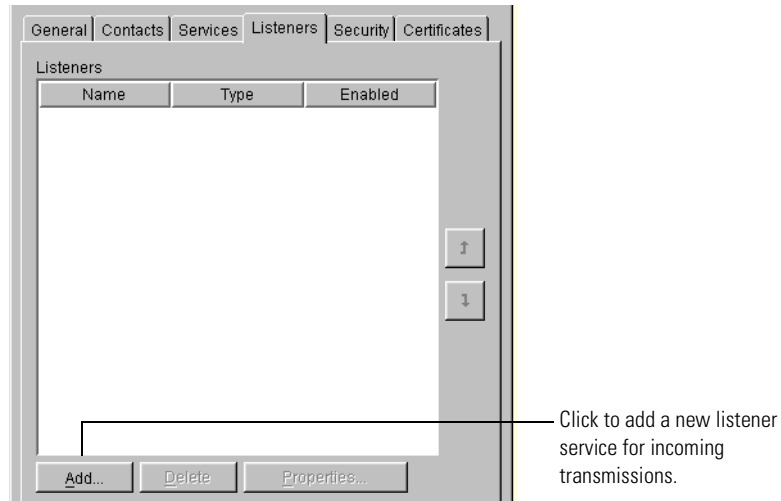
Your prioritized list of connection services is one of the items that you give to your partners when you exchange channel profile information. In return, you receive prioritized lists from your partners that tell you how to connect to their Process Servers.

To increase your processing flexibility, you can set up different types of synchronous services: Internet and dialup. For example, you can set up different Internet services for Internet, extranet, and private networks. If you prefer to have partners connect via a dialup connection, you could set up three different dialup services, each using a different phone number. Or you might use both types of services, with an Internet service as your main connection and dialup services as backup connections.

## To set up a listener service:

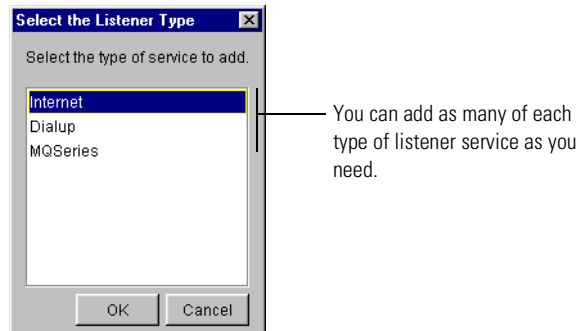
- 1 Open your Partner Agreement Manager Channel profile and click the Listeners tab.

The Listeners tab appears.



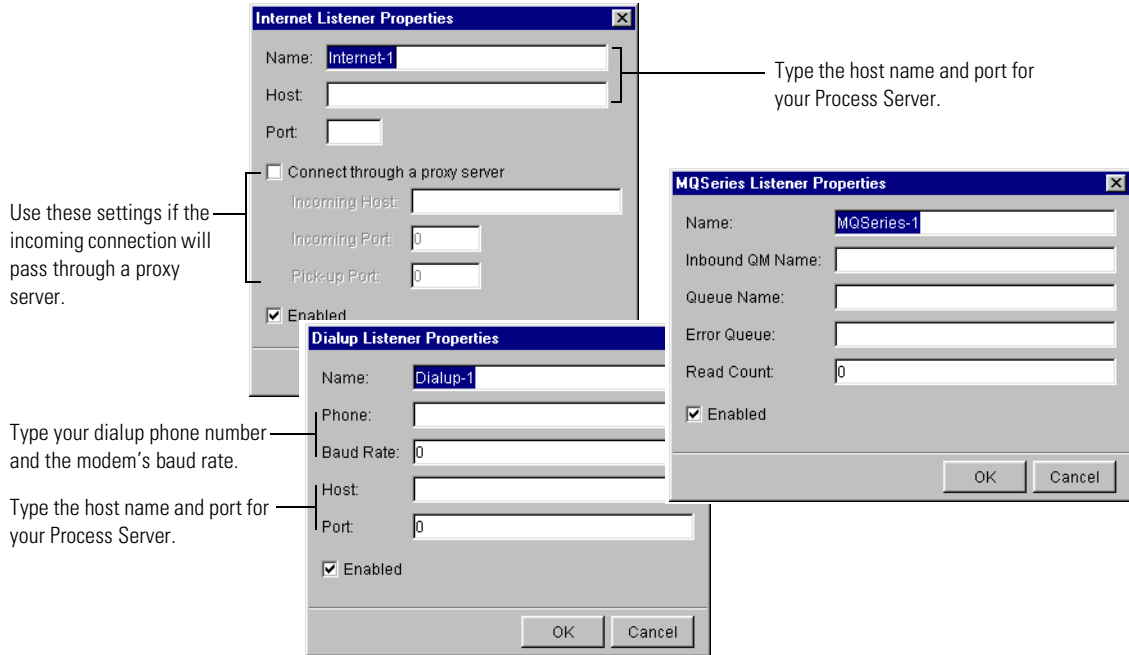
- 2 Click Add.

The Select the Listener Type dialog box appears.



- 3 Select the type of listener service to add and click OK.

The Listener Properties dialog box appears for the type of service you selected.



Partner Agreement Manager assigns a name to the listener service, based on the service type you selected—for example, if you select Internet, Partner Agreement Manager assigns the name Internet-1. If you add more than one listener service of the same type, Partner Agreement Manager increments the number when it assigns the name—for example, it assigns the name Internet-2 to the second Internet connection.

You can change the assigned name by selecting it and typing over it. If you change the name, it's a good idea to use a name that clearly identifies the service. For example, you might name your primary Internet service "Internet main," or your primary messaging service on UNIX "MQSeries main." The instance name you use does not need to be the same as the queue name. Each service name must be unique.

- 4 Enter the appropriate information for the listener service.

**For this type of listener**

**Do this**

Internet

1. Enter your Process Server's host name and port number.
2. If you use a proxy server, turn on the Connect through a Proxy Server setting, and enter the proxy server's listener incoming host, the incoming port, and the pick-up port where Partner Agreement Manager checks for incoming messages.

**NOTE:** Incoming port and pickup port are set differently, depending on whether you're using the proxy in active or passive mode. For passive mode, the `proxy.cnf` file uses the `PASSIVE_PROXY` directive, which defines two ports. The first port is the incoming port, and the second port is the pickup port. For active mode, the `proxy.cnf` file uses the `PROXY` directive, which has only one port. This port corresponds to the incoming port, and the pickup port is left blank.

Dialup

Enter the phone number and baud rate needed to make the connection, and the host name and port on your Process Server.

MQSeries

Enter the queue manager name, the queue name, and the error queue.

**NOTE:** For more information on configuring Partner Agreement Manager for MQSeries, see *Configuring PAM for MQSeries* on page 165.

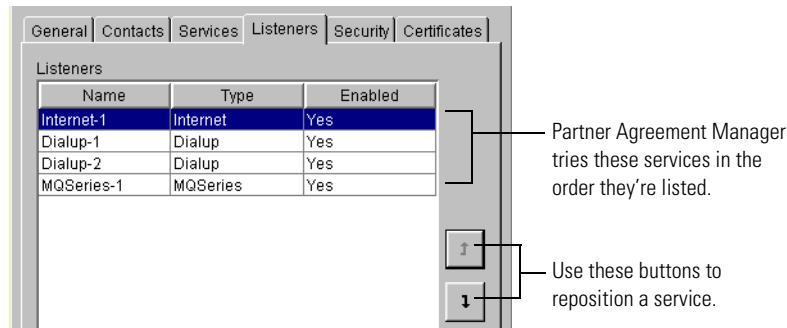
- 5 Click OK in the Listener Properties dialog box.
- 6 Repeat steps 2 - 5 to continue adding listener services as necessary.
- 7 Click OK, or click another tab in the Channel Profile dialog box to enter additional channel profile information.

### PRIORITIZING CONNECTION SERVICES

Your Partner Agreement Manager listens to all services, and your partner's Partner Agreement Manager manages your listener services like telephones in a telephone bank, rolling over from one listener service to the next until communication is successful. Partner Agreement Manager starts with the first service in the Listeners list and continues through the list in order as necessary.



Initially, Partner Agreement Manager lists connection services in the order that you install them, but you can use the up-arrow and down-arrow buttons to change the order of services in the list. For example, you can set Partner Agreement Manager to try all of your Internet connections first, followed by any dialup connections.



### To prioritize connection services:

- 1 Open the Partner Agreement Manager Channel profile and click the Listeners tab.
- 2 Select the listener service to reposition.
- 3 Click the up-arrow or down-arrow buttons to move the service up or down in the list.

## DEFINING YOUR SECURITY PROFILE

To ensure that your transactions with your partners are protected, Partner Agreement Manager uses a combination of security options that includes public key cryptography and other methods of encryption.

### ABOUT YOUR SECURITY PROFILE

Your security profile has three components—your standard policies, cryptography algorithms, and the certificates you define for authentication and encryption. These components work together to ensure the privacy and security of transmissions between partners.

You start defining your security profile by selecting the policy options to implement (there are four options, and you can select them in any combination). Each policy option you select uses its own combination of algorithms. Depending on the policy options you select, you can also prioritize different combinations of cryptography algorithms.

This table shows the algorithms used for the security policy options:

Partner Agreement Manager uses these algorithm types	And these algorithms	
	Base level	Enhanced level
Encryption	RC2_40	RC2_56, RC2_128, DES, DESEDE, DESEDE3
Key Exchange	RSA_512	RSA_768, RSA_1024
Signature	RSA_512 with SHA-1, RSA_512 with MD5, RSA_512 with MD2	RSA_768 with SHA-1, RSA_768 with MD5, RSA_1024 with SHA-1, RSA_1024 with MD2, RSA_1024 with MD5

### ABOUT POLICY OPTIONS

Partner Agreement Manager supports four types of security policy options: privacy, authentication, non-repudiation of origin, and non-repudiation of receipt. Your standard security policy can contain any combination of these options.

- **Privacy:** Partner Agreement Manager encodes the contents of a message in a way that can be decoded only by the intended recipient.
- **Authentication:** Partner Agreement Manager verifies the identity of the sender using the sender's signature certificate.
- **Non-repudiation of origin:** Partner Agreement Manager authenticates each message and maintains an audit record to verify that a message actually originated from the stated originator.
- **Non-repudiation of receipt:** Partner Agreement Manager authenticates each message and maintains an audit record to verify that a message was actually received by the intended recipient.

### ABOUT CRYPTOGRAPHY ALGORITHMS

Partner Agreement Manager uses three types of algorithms to implement the security policies you select: encryption, key exchange, and signature.

- **Encryption** uses two variable key-size ciphers: RC2, a variable key-size block cipher, and RC4, a variable key-size stream cipher.

- **Key Exchange** uses RSA cipher suites with key-exchange algorithm.
- **Signature** uses RSA cipher suites with hashing algorithms (SHA-1 or MD5), which create message digests, used to verify digital signatures.

## ABOUT CERTIFICATES

A certificate is a security document that binds a public or private encryption key to an organization or an individual. Partner Agreement Manager supports two types of certificates:

- **Self-signed certificates**, where the same person is both the principal and guarantor.
- **CA-issued certificates**, also known as third-party-signed or linked certificates, which are issued and guaranteed by a certificate authority (CA), such as Verisign or Thawte.

Each security certificate has a principal and a guarantor, effective and expiration dates, a serial number, and a fingerprint. After you create a certificate, you designate whether it will be used for encryption, signature authentication, or both.

**NOTE:** As part of the process of setting up Partner Agreement Manager partners, you must view your partners' certificates and designate them as trusted. See [Accepting new Partner Agreement Manager Channel partners](#) on page 69.

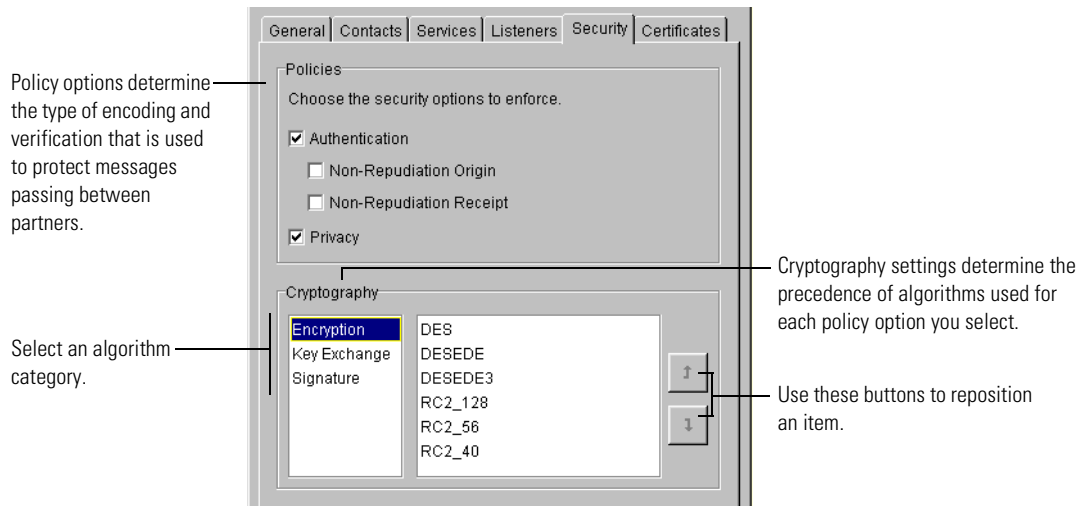
## SETTING UP SECURITY POLICY OPTIONS AND ALGORITHMS

When you set up the security portion of your Partner Agreement Manager Channel profile, you select the policy options to use and prioritize the available algorithms.

### To set up security policy options and algorithms:

- 1 Open the Partner Agreement Manager Channel profile and click the Security tab.

The Security tab appears.



**2** Select the security options to implement.

Partner Agreement Manager is preset with the Privacy and Authentication options turned on. These are the recommended minimum security level settings. See [About policy options](#) on page 34 for a description of each option.

**3** Select an algorithm category.

Partner Agreement Manager lists the algorithms available for the category. Partner Agreement Manager uses the first algorithm in the list to implement the security policies you defined.

To prioritize the order in which Partner Agreement Manager rolls over from one algorithm to the next, select an algorithm and use the up-arrow or down-arrow buttons to move it up or down in the list. See [About cryptography algorithms](#) on page 34 for a description of each algorithm.

**4** Click OK.

## SETTING UP CERTIFICATES

Partner Agreement Manager uses your certificates in combination with the security options during information exchange, to ensure the privacy and security of transmissions between partners.

When you set up a certificate, you decide how it will be guaranteed (self-signed or CA-issued), and bind the certificate to your Partner Agreement Manager Channel profile.

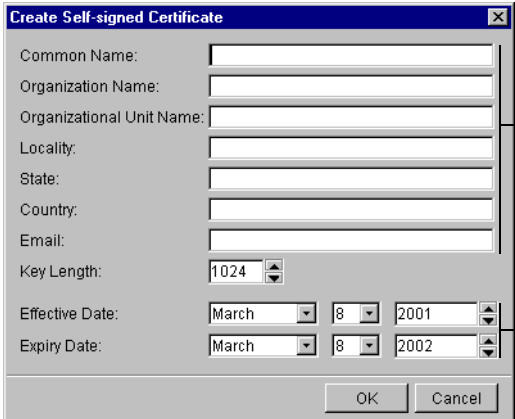
## CREATING SELF-SIGNED CERTIFICATES

When you create a self-signed certificate, you are the guarantor for the certificate. In other words, you verify the authenticity of the certificate to your partners.

### To create a self-signed certificate:

- 1 Choose New from the Actions menu, and Self-signed Certificate from the submenu.

The Create Self-signed Certificate dialog box appears.



Enter a certificate name and contact information for the person who is responsible for authentication.

Enter starting and ending dates for the certificate.

- 2 Enter information for setting up the certificate.

You can enter a common (certificate) name, organization name, organizational unit name, contact information for the person responsible for authenticating the certificate, and effective and expiration dates for the certificate. The required fields are common name and e-mail. The date fields have preset values: the current date for Effective Date and one year from the current date for Expiry (expiration) Date.

**NOTE:** The common name is usually the computer name. For more information, see your CA's documentation.

- 3 Click OK.

Partner Agreement Manager adds the signature certificate to the list.

After you create the certificate, you must bind it. See [Binding a certificate](#) on page 41.

## CREATING CA-ISSUED CERTIFICATES

When you create a CA-issued certificate, the certificate authority (CA) guarantees the certificate. You create a request and send it to your CA, usually via e-mail or a web page. The CA returns a signed certificate file, which you then import into Partner Agreement Manager.

---

**IMPORTANT:** Be sure to import the Certifying Authority certificate, also known as the *root* certificate, in addition to your own certificate.

---

### To set up a CA-issued or linked certificate:

- 1 Choose New from the Actions menu, and Certificate Request from the submenu.

The Create Certificate Request dialog box appears.

Enter a certificate name and contact information for the person who is responsible for authentication.

- 2 Enter information for setting up the certificate.

Enter a common (certificate) name, organization name, and organizational unit name and location information. The CA provides the effective and expiration dates.

- 3 Click OK.

The Save Certificate Request to File dialog box appears. Save your certificate as a text file to send to the CA.

- 4 Type a name for the file and click Save.
- 5 Send the certificate request file to your CA.

You can send it by e-mail or through a web site. Check with your CA for more information.

The CA returns a signed certificate file to you, which you must import into Partner Agreement Manager.

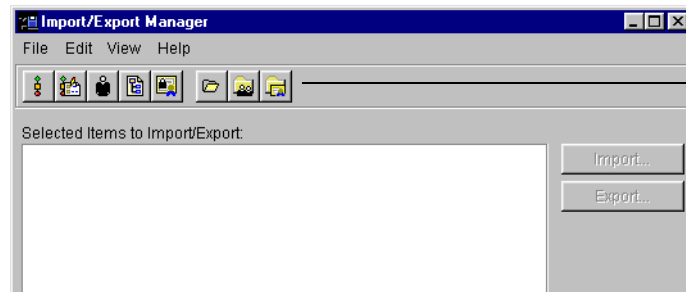
### To import a certificate file into Partner Agreement Manager:

- 1 Make sure you know the path of the signed certificate text file your CA sent you.



- 2 In the Process Manager window, click the Import/Export Manager button in the Command toolbar.

You can also choose Import/Export Manager from the Tools menu. The Import/Export Manager appears.

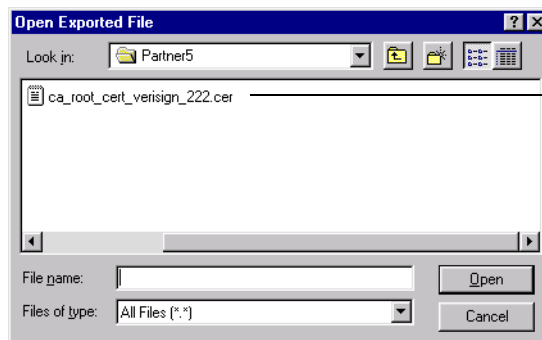


Use the toolbar button to select the certificate to import.



- 3 Click the Open Certificate File for Import button in the Command toolbar, or choose Open for Import from the File menu, and then choose Certificate File.

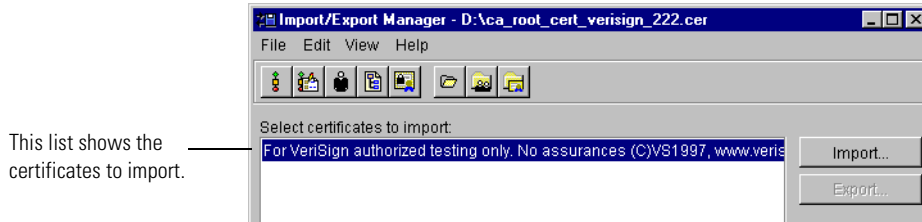
The Open Exported File dialog box appears.



This text file with a .cer extension contains signed certificate information.

- 4 Select the certificate file to import and click Open.

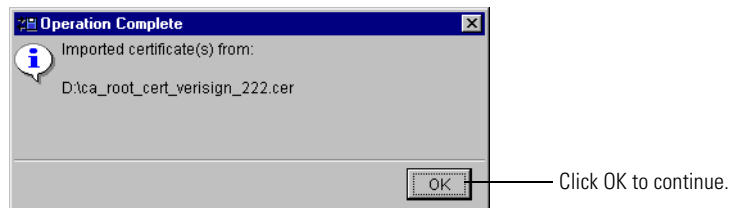
The Import/Export Manager shows all certificates in the file.



- 5 Select the certificates to import, and click Import or choose Import from the File menu.

Sometimes a certificate is multi-level and will include several files (including a root certificate), all necessary to the certificate. Select all the files at once to import.

When the import is finished, a dialog box appears.



- 6 Click OK in the Operation Complete dialog box.  
Partner Agreement Manager imports the certificates.
- 7 Close the Import/Export Manager.

If you import a certificate whose issuer is trusted, the certificate is auto-trusted (provided it has not expired or is otherwise invalid). If it is a root certificate, or is a multi-level certificate with an untrusted issuer in the chain, you will manually have to trust it. For more information, see See [Accepting new Partner Agreement Manager Channel partners](#) on page 69.

You can now bind the certificate to your profile. See [Binding a certificate](#), next.

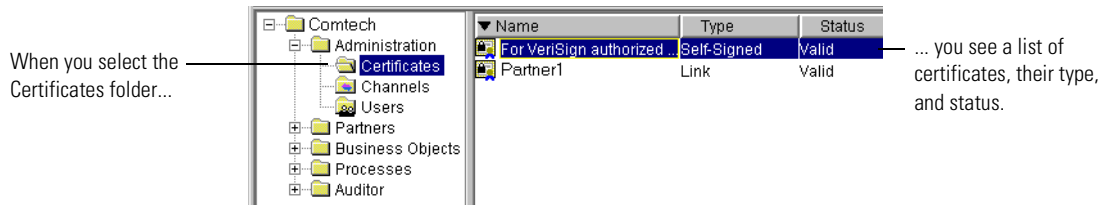
---

**IMPORTANT:** If you import and bind a certificate obtained from a CA and then later decide to delete the certificate, you will lose your private key. You cannot then re-import and re-bind the same certificate. You must get another certificate from your CA and import and bind it.

---



After you create certificates, you can view them in the Process Manager window. In the Process Manager window, select the Certificates folder to see the list of current certificates, along with their type (Self-Signed or Link) and status (Valid or Invalid).



## BINDING A CERTIFICATE

After you create a certificate, you specify how it is to be used by binding it to your Partner Agreement Manager profile.

During the binding process, you designate a protocol for the type of certificate—signature, encryption, or both.

- **Signature certificates** are used to sign messages when sending. They authenticate messages when bound with the S/MIME Signature protocol.
- **Encryption certificates** are used by your partner to encode a private message when bound with the S/MIME Encryption protocol.

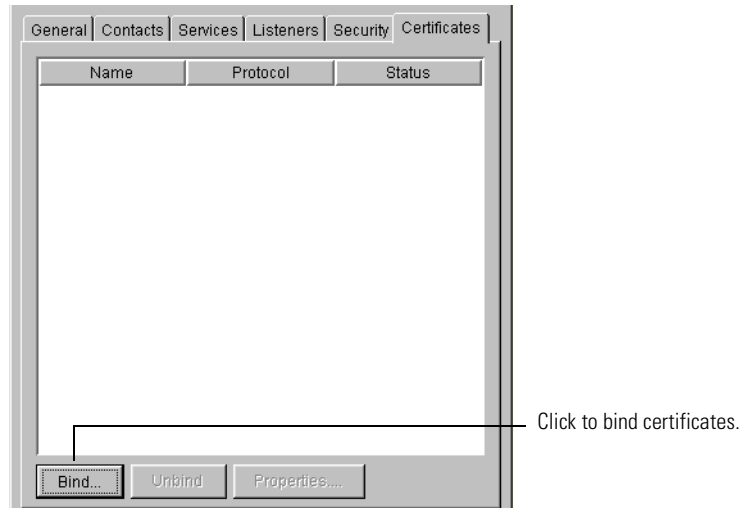
You must define a signature certificate and a encryption certificate before you can exchange information with your partners. You can use a single certificate for more than one purpose and bind it to more than one protocol (or the “Any” protocol).

### To bind a certificate:

- 1 Open the Partner Agreement Manager Channel profile and click the Certificates tab.

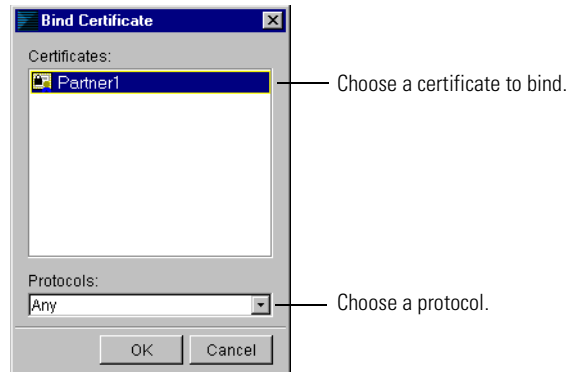
For more information on opening the channel profile, see [Opening your Partner Agreement Manager Channel profile](#) on page 21.

The Certificates tab appears.



- 2 Click Bind to add a new certificate.

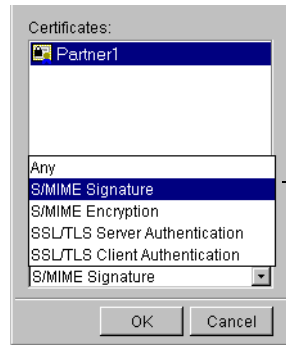
The Bind Certificate dialog box appears.



- 3 Choose a certificate, and choose a protocol from the dropdown list based on how the certificate will be used.

**NOTE:** You can use one certificate for more than one purpose. You can bind it to more than one protocol, or you can bind it to the “Any” protocol.

- **Signature certificates** are used to sign messages when sending. They authenticate messages when bound with the S/MIME Signature protocol.
- **Encryption certificates** are used by your partner to encode a private message when bound with the S/MIME Encryption protocol.



Choose a protocol based on how you want to use the certificate.

Use the information in this table to help you determine which protocol to specify.

Choose	To have a certificate
Any	Serve more than one purpose.
S/MIME Signature	Authenticate signed e-mail.
S/MIME Encryption	Encrypt messages.
SSL/TLS Server Authentication	Identify servers to clients for channels using SSL (Secure Sockets Layer).
SSL/TLS Client Authentication	Identify clients to servers for channels using SSL.

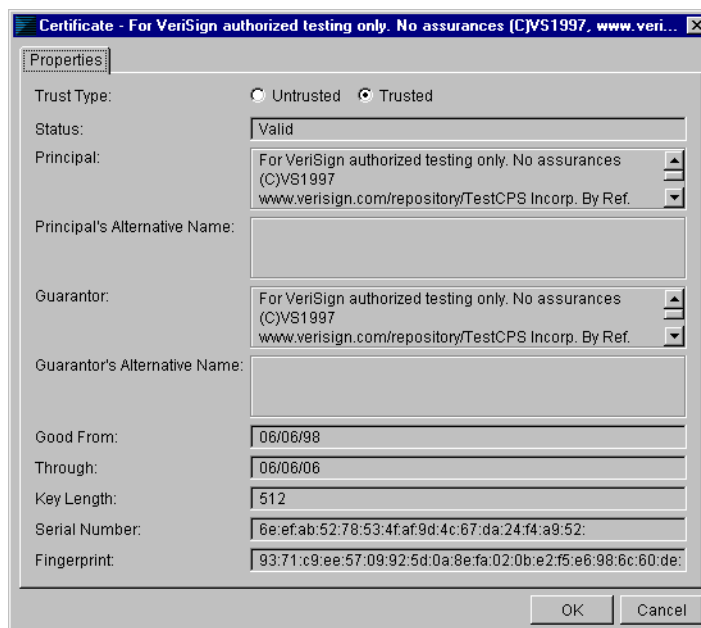
**4** Click OK.

Partner Agreement Manager binds the certificate.

### To review the properties of a certificate:

- ▶ On the Channel Profile dialog box, click the Certificates tab, select the certificate, and then click Properties.

The Certificate properties dialog box appears.



**NOTE:** As part of the process of setting up Partner Agreement Manager partners, you must view your partners' certificates and designate them as trusted. See [Accepting new Partner Agreement Manager Channel partners](#) on page 69.

## SETTING UP PARTNER AGREEMENT MANAGER USERS

Partner Agreement Manager users are people who have access to Partner Agreement Manager functions such as Channel profile administration or new process building. You typically set up Partner Agreement Manager users from within the Process Manager. You can also import selected user information from another source.

**NOTE:** Partner Agreement Manager now supports accessing users from an LDAP (Lightweight Directory Access Protocol) directory. For more information on setting up Partner Agreement Manager for LDAP, see *Using LDAP with Partner Agreement Manager* on page 129.

## ABOUT USERS

Partner Agreement Manager user profile consists of information about the user, such as name, e-mail address, and telephone number. It also includes access permissions that determine what Partner Agreement Manager functions the user can perform.

For each function, Partner Agreement Manager provides three types of user access: read, edit, and none. The Admin user is preset with edit access to all functions.

With read access, users can open folders and view their contents but not make changes. For example, a user with read access to processes can open the Process folder, open a public process in the Process window, and view the private processes for an action. The same user cannot make changes to either the public or private process.

With edit access, a user can both read and make changes in a Partner Agreement Manager function.

## SETTING UP THE ADMIN USER

As part of installation, Partner Agreement Manager creates a user named **admin**. This user is preset with edit access to Partner Agreement Manager functions, such as adding partners, creating business objects, and adding processes. The Admin user can also monitor running processes, audit completed ones, edit the company's Partner Agreement Manager Channel profile, and add other users.

Although you cannot change the Admin user's access settings, you can change the password or enter new contact information if you are logged on as the Admin user.

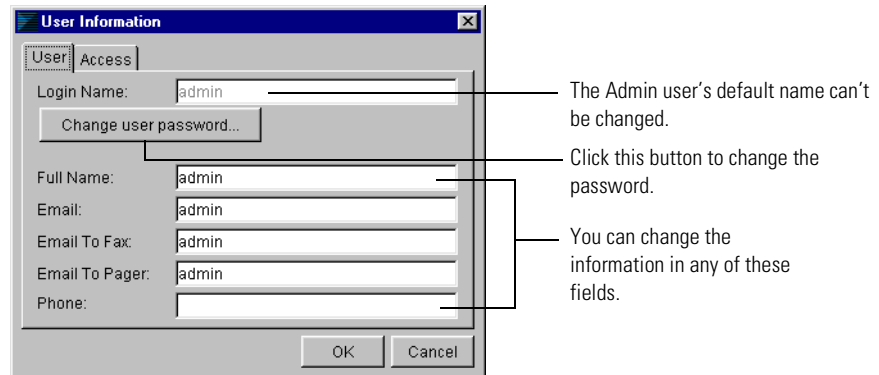
## To set up the Admin user:

- 1 Log in as the Admin user.

Only the Admin user can edit the Admin user's properties. You can also open the Administration folder in the Process Manager window, open the Users folder, and double-click the Admin user in the list.

- 2 Choose Current User from the Edit menu.

The User Information dialog box appears.

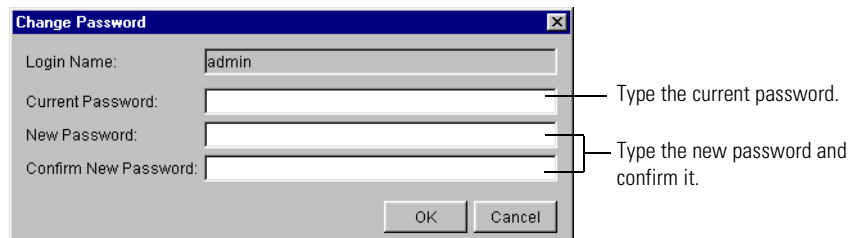


- 3 Enter the contact information.

If you have e-mail access to faxing and paging, you can include those e-mail addresses in the contact information. With Partner Agreement Manager, you can use this information when you address notification and approval actions.

- 4 To change your password, click the Change User Password button.

The Change Password dialog box appears.



- 5 Type your old password, and then a new password. Type your new password again to confirm it, and then click OK.
- 6 Click OK to close the User Information dialog box.

## ADDING A NEW USER

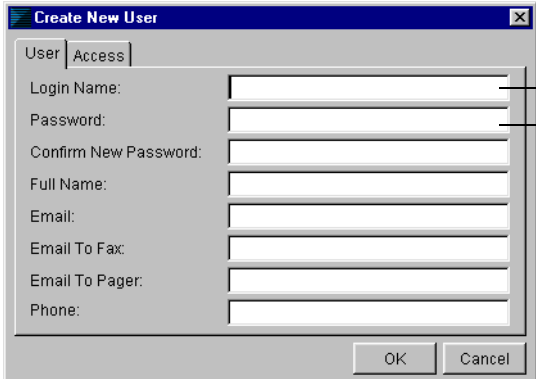
When you add a new Partner Agreement Manager user, you enter the user's login name, password, and contact information. You also assign the user access to different Partner Agreement Manager functions. Access levels are none, read, and edit. With read access, the user can view but not change material. With edit access, a user can both read and edit information.

You can add and remove Partner Agreement Manager users as you need them. If you plan to set up or modify several users, you might want to use the user import feature in the Process Server. See *Importing user information* on page 50.

### To add a new user:

- 1 Choose New from the Actions menu, and choose User from the menu that appears.

The Create New User dialog box appears.



— Login name and password are required. All other fields are optional.

- 2 Type a user name and password. Confirm the password.
- 3 Enter the user's full name and contact information.  
Partner Agreement Manager uses contact information when sending notifications.
- 4 Click the Access tab to give the new user access to different Partner Agreement Manager features.

The Access tab appears.

Partners: Read  
Business Objects: Read  
Processes: Read  
Auditor: Read  
Reports: None  
Users: Read  
Channels: Read

OK Cancel

You can select access levels for each Partner Agreement Manager component.

- 5 Assign an access level for as many areas as the user needs.
- 6 Click OK.

The new user appears in the Process Manager window.

Double-click a user in the list to change its settings.

Name	Phone	Email
admin	650-555-4556	admin@comtech.com
buyer	650-555-0344	buyer@comtech.com
libby	650-555-0355	libby@comtech.com

## REMOVING A USER

You can remove a user by deleting the user name from the Process Manager window.

**To remove a user:**

- 1 Open the Administration folder in the Process Manager window. Open the Users folder. Select the user name.

Name	Phone	Email
admin	650-555-4556	admin@comtech.com
buyer	650-555-0344	buyer@comtech.com
libby	650-555-0355	libby@comtech.com

-  2 Click the Delete button on the Command toolbar.

You can also press the Delete key or right-click the user name and choose Delete from the menu that appears.



## CHANGING USER INFORMATION

All Partner Agreement Manager users can change their own passwords, full names, and contact information. If you are the Admin user, you can assign new passwords to other Partner Agreement Manager users and change their user information. After you set up a user, the user's login name must remain the same.

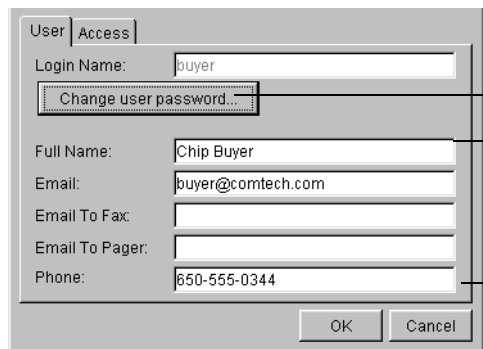
**TIP:** To change a user's login name, delete the user and create a new one.

### To change user information:

- 1 Open the Administration folder in the Process Manager window. Open the Users folder, and double-click a user profile in the list.

If you don't have access to the Users folder, choose Current User from the Edit menu to edit your own user information.

The User Information dialog box appears.



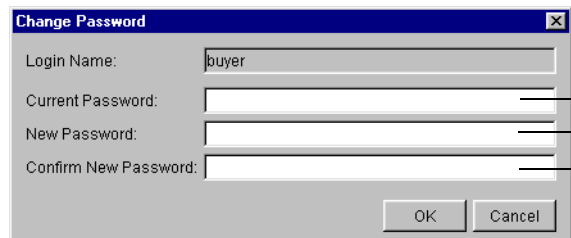
The User Information dialog box is shown with the 'User' tab selected. It contains the following fields: Login Name (buyer), Full Name (Chip Buyer), Email (buyer@comtech.com), Email To Fax, Email To Pager, and Phone (650-555-0344). A 'Change user password...' button is located below the Login Name field. The dialog also has 'OK' and 'Cancel' buttons at the bottom.

Click this button to change your password.

You can change any of this information.

- 2 Enter a new full name or contact information.
- 3 To change the password, click the Change User Password button.

The Change Password dialog box appears.



The Change Password dialog box is shown with the following fields: Login Name (buyer), Current Password, New Password, and Confirm New Password. The dialog also has 'OK' and 'Cancel' buttons at the bottom.

Type your current password.

Type your new password and confirm it.

- 4 Type your old password, and then your new password. Type your new password again to confirm it, and then click OK.

**NOTE:** If you're the Admin user and you are changing another user's password, you don't have to enter the current password. You can simply enter the new password and confirm it.

- 5 Click OK in the User Information dialog box.

## IMPORTING USER INFORMATION

If you have several users to set up or modify, consider using the Partner Agreement Manager user import feature. With the import feature, you can import a comma-delimited text file that contains the same user identity information as the User tab of the User Information dialog box.

You can use this feature to create new users or to update information for current users (for example, to update a group of phone numbers or e-mail addresses). You cannot import security information such as passwords or access. After you import users, you must therefore edit each user to set a password and access.

The fields in the text file are: Partner Agreement Manager user name (required), full name, e-mail address, e-mail to fax, e-mail to pager, and phone number. Each field must appear in the text file. If there is no data for a field, use a single blank space instead.

A typical entry might look like this:

					Blank space for E-mail to pager
<b>Al Frahm, Alfred L. Frahm, alfrahm@comtech.com, alifax@comtech.com, , 410-555-0288</b>					
_____	_____	_____	_____	_____	_____
PAM user name	Full name	E-mail address	E-mail to fax	Phone number	

---

**IMPORTANT:** Each Partner Agreement Manager user name must be unique within an import text file. If the text file contains the names of current Partner Agreement Manager users, Partner Agreement Manager uses the imported information to update name, address, and e-mail information.

---

## To import user information:

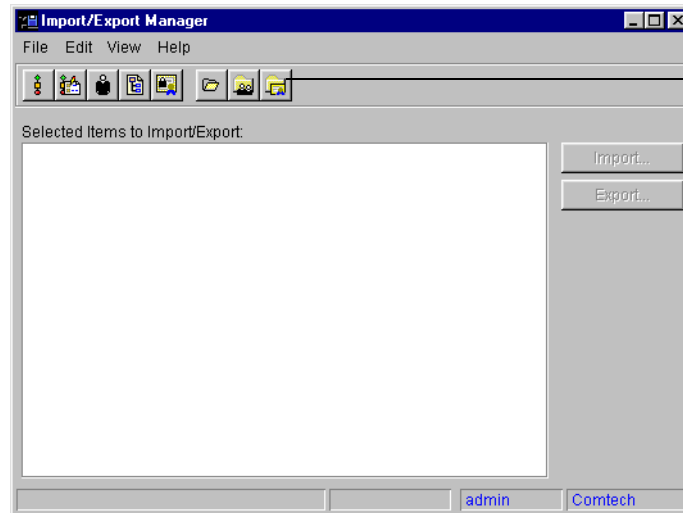
- 1 Create a text file that contains the information to import.

Each entry must be on its own line. Separate the fields in an entry by commas. Each field must appear in each entry in the text file. If there is no data for a field, enter a single, blank space.



- 2 Click the Import/Export Manager button in the Command toolbar.

You can also choose Import/Export Manager from the Tools menu. The Import/Export Manager appears.

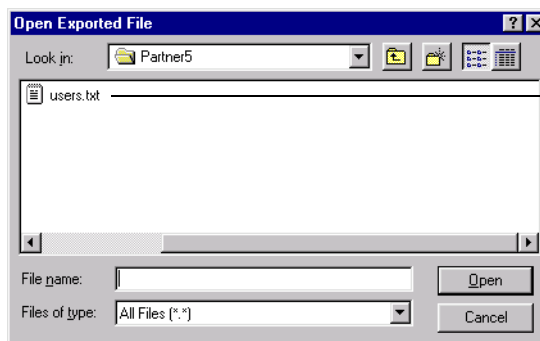


Toolbar buttons let you select the items to export, or the file to open for importing.



- 3 Click the Open User File for Export button in the Command toolbar, or choose Open for Import from the File menu, and then choose User File.

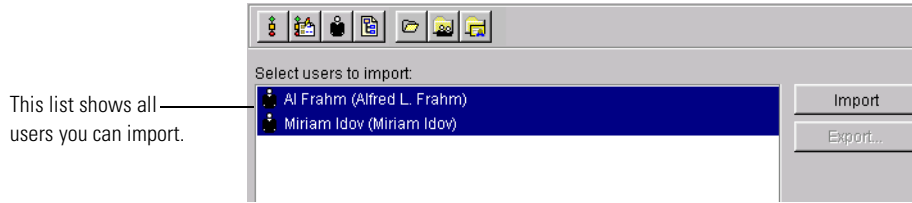
The Open Exported File dialog box appears.



This text file contains user information.

- 4 Select the file to import and click Open.

The Import/Export Manager shows all users in the file.



- 5 Select the users to import, and click Import or choose Import from the File menu.

Partner Agreement Manager imports the users and displays them in the Process Manager window. The imported users do not have passwords or access settings.

Name	Phone	Email
Al Frahm	410-555-0288	alfrahm@comtech.com
Miriam Idov	410-555-4444	midov@comtech.com
admin	650-555-4556	admin@comtech.com
buyer	650-555-0344	buyer@comtech.com

Information for these users was imported from a text file.

---

**IMPORTANT:** You must edit each new imported user to set a password and access.

---

- 6 Close the Import/Export Manager.

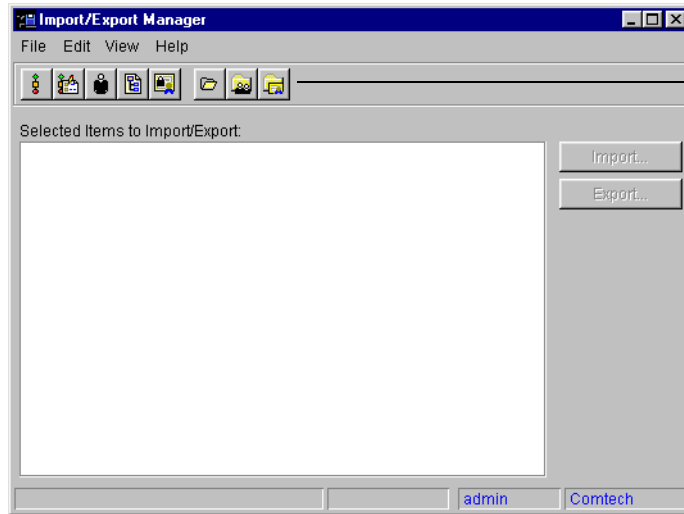
## EXPORTING USER INFORMATION

During the course of implementing Partner Agreement Manager, you might want to duplicate your Partner Agreement Manager environment on another system for testing purposes, or to move from testing to production systems. Because the users you have set up in Partner Agreement Manager are an important part of the environment, Partner Agreement Manager makes it easy to export users for import on another system. Exporting captures all user information, including access and passwords.

**To export user information:**

- 1 Click the Import/Export Manager button in the Command toolbar.

You can also choose Import/Export Manager from the Tools menu. The Import/Export Manager appears.

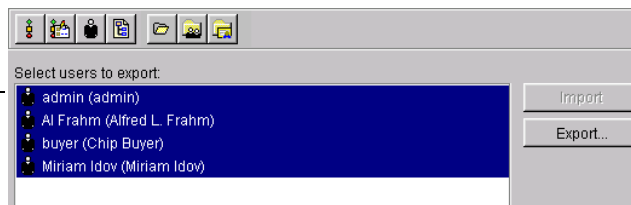


Toolbar buttons let you select the items to export, or the file to open for importing.



- 2 Click the Users button in the Command toolbar, or choose Select for Export from the File menu, and choose User from the menu that appears.

The Import/Export Manager shows all users set up in Partner Agreement Manager.



This list shows all users you can export.

- 3 Select the users to export, and click Export or choose Export from the File menu.

Partner Agreement Manager exports the users and alerts you when the export operation is complete.

- 4 Close the Import/Export Manager.

## SETTING UP SYSTEM ERROR NOTIFICATIONS

As the Process Server runs, errors might occur that are systemic instead of process-related. For example, there might be a connection failure, or a failure in some other system function. Partner Agreement Manager posts these types of errors in the Auditor System folders.

You can set Partner Agreement Manager to send e-mail to the Partner Agreement Manager administrator (or to other individuals), in addition to posting the errors in the Auditor System folders. This e-mail provides immediate notification when an error occurs.

The resulting error e-mail message includes the name of the component that failed and the full text of the error message. The information contained in this message can be very useful to your customer support representative.

This text also appears in a Partner Agreement Manager system error message.

```
From: pam@comtech.com    To: smodlin@comtech.com
Subject: Error: Event Manager

(80070002)80070002

java.lang.NullPointerException
at CRStation.engine.info.EngineInfoManager.getPublicProcessInfo(EngineInfoManager.java:580)
at CRStation.engine.info.EngineInfoManager.getPublicProcessInfo(EngineInfoManager.java:545)
at CRStation.engine.execution.pub.PublicController.startProcess(PublicController.java:818)
at CRStation.engine.execution.pub.PublicController.startProcess(PublicController.java:316)
at CRStation.engine.Engine.startProcess(Engine.java:473)
at CRStation.managers.event.Cron.execute(Cron.java:183)
at CRStation.managers.event.Scheduler.executeJobs(Scheduler.java:334)
at CRStation.managers.event.Scheduler.run(Scheduler.java:283)
at java.lang.Thread.run(Thread.java:466)
```

The information for system error notifications is in the **Partner.Properties** file, located in your partner folder. For example, if your partner name is Comtech, the location of the **Partner.Properties** file would be: `c:\WebSphere\PAM\Partners\Comtech\Properties\Partner.Properties`. You can edit this file using any standard text editor, such as Wordpad or Notepad.

A notification entry consists of a key name and a value. The key name is **Error.notification\_recipient** and the value is the e-mail addresses you enter (you can enter more than one). The **Partner.Properties** file contains a placeholder entry for the e-mail address. This entry is located in the **# Error notification e-mail** section.

```
#Error.notification_recipient=email_name; mode=server; type=string;
desc="Email account to which Partner Agreement Manager notifications are
sent"
```

### To set up system error notifications:

- 1 Use a text editor to open the `Partner.Properties` file.

On this platform	The file is located here
------------------	--------------------------

UNIX	Partner/Properties
------	--------------------

Windows	Partner\Properties
---------	--------------------

- 2 Scroll to the `# Error notification email` section at the end of the file.
- 3 Remove the `#` at the beginning of the `Error.notification_recipient` entry so that the entry becomes active.  
Partner Agreement Manager ignores any properties that start with a `#` (a comment character).
- 4 Select the text `email_name` and type one or more e-mail addresses.  
Use commas to separate multiple e-mail addresses. For example:  
`smodlin@comtech.com, alfrahm@comtech.com, msheehan@comtech.com`
- 5 Save the `Partner.Properties` file.
- 6 Restart the Process Server to let the new setting take effect.

## SPECIFYING TERMINATION ACTION REASONS

When a private process terminates abnormally, Partner Agreement Manager displays an error message and makes the reason for the termination available for troubleshooting or other audit purposes. Partner Agreement Manager is preset to include some of the most common reasons for terminating a private process: out-of-range or missing data, data format errors, or approval refusal. These reasons appear in the Termination Properties dialog box, in audit messages, and in the status field in the Partner Agreement Manager Auditor.

You can add other reasons that are specific to your PAM installation, or you can edit the wording for the default reasons that Partner Agreement Manager provides.

The reason codes are stored in a text file, `Terminate.Properties`. You can edit the contents of this file using a text editor such as Wordpad or Notepad.

Each reason has a code and description. Partner Agreement Manager uses the code internally and displays the corresponding reason when you set properties or view an audit item. User-defined reason codes are five-digit numbers starting with 32768 (Partner Agreement Manager reserves codes 0 through 32767). Both the codes and descriptions must be unique.

This is a sample section of the `Terminate.Properties` file.

```
#-----  
# The user-defined terminate reasons (> 32767)  
#-----  
32768=Missing Data In Business Object  
32769=Data Incorrectly Formatted  
32770=Data Value Out Of Range  
32771=Approval Denied
```

#### To include other termination reasons:

- ▶ Add as many reasons as you need to the list in `Terminate.Properties`, and be sure to save the file as a text file.

You must restart both the Process Server and client to display the new reasons in the Termination Properties dialog box.

**NOTE:** For more information about terminating a private process, see the *Partner Agreement Manager User's Guide*.

## SETTING UP THE DIAGNOSTIC MONITORING SYSTEM

Partner Agreement Manager provides a mechanism for administrators to monitor the health of the servers. It does this in two ways:

- through active traps then get thrown when events happen in the system.
- by providing access to resources that can be polled for information.

By monitoring resources like memory or thread pool size, an administrator can determine whether Partner Agreement Manager is operating correctly. This information is presented in the Partner Agreement Manager Auditor or by communicating to a network monitor through the Simple Network Management Protocol (SNMP).

**NOTE:** The `Alliance.mib` file (which supports SNMP version 1 and 2) is located in `PAM\Snmplib\Alliance.mib` and is distributed as a source that needs to be compiled.



The diagnostic monitoring system polls Partner Agreement Manager system resources such as available memory or the status of a process type. You can use the diagnostic monitoring system properties to set the threshold at which warning messages are posted. For example, you might set a percent usage of the Java Virtual Machine heap at which a message is sent.

The diagnostic monitoring system caches the most recent status of each polled resource and compares the new status with the cached information. If the diagnostic monitoring system detects a status change, it posts a message in the Auditor's System Messages folder.

The diagnostic monitoring system monitors both Partner Agreement Manager resources and Adapter Server resources. See [About monitored resources](#), next.

The information gathered by the diagnostic monitoring system can also be accessed by a network management application that uses SNMP, via the Partner Agreement Manager SNMP Agent. See [About the Partner Agreement Manager SNMP agent](#) on page 61.

You enable the diagnostic monitoring system during Partner Agreement Manager installation or upgrade. If you did not enable diagnostic monitoring during installation and you later decide to use it, or if you want to change the polling rate after installation, you can edit the `Partner.properties` file. After editing the file, you must restart Partner Agreement Manager for the new settings to take effect.

The `Partner.properties` file is in your PAM partner folder. For example, if your partner ID is 527, the location of the `Partner.properties` file would be: `c:\WebSphere\PAM\Partners\Partner527\Properties\Partner.properties`. You can edit this file using any standard text editor such as Wordpad or Notepad.

- To turn polling of monitored resources on or off, stop the Process Server and edit this line in your `Partner.Properties` file:

```
com.extricity.registry.polling=true ; mode=server ;  
type=boolean
```

- To specify the diagnostic monitoring polling rate, stop the Process Server and add this line:

```
com.extricity.registry.polling_rate=nm ; mode=server ;  
type=int
```

Set the `polling_rate` parameter to the number of seconds to poll.

The changes take effect after you restart the Process Server.

## ABOUT MONITORED RESOURCES

Process Server and Adapter Server monitored resources can be polled by the diagnostic monitoring system. See *Monitored resources*, next.

Each monitored resource gives its resource status when it is queried by either the diagnostic monitoring system or by a network management application that uses SNMP. The resource's status indicates whether the resource is in a normal range of operation (Informational), or in a Warning or Error state.

Each monitored resource has a set of properties that determine when a resource status changes. You can set property thresholds using a network management application that uses SNMP. Properties set via SNMP can modify system performance or status-reporting behavior without the need to restart Partner Agreement Manager. If you are not using an SNMP-based application, you can set the properties in the `Partner.properties` file, and then you must restart Partner Agreement Manager.

## MONITORED RESOURCES

These are the Partner Agreement Manager resources that are monitored. If Partner Agreement Manager is configured to be managed by an SNMP application, system messages that appear in the Auditor window are also sent as SNMP traps.

### SYSTEM AND APPLICATION MEMORY

These resources display information about available system and application memory, and let you set the percent of the Java Virtual Machine heap at which a warning is sent.

#### RESOURCE NAME

Memory: Process Server

Memory: Adapter Server <Adapter Server identification number>

#### PROPERTIES

- Percent usage of total heap at which a warning message is sent:

`HeapUsageThreshold="<integer percentage>"`

## STATUS

- Current Virtual Machine memory:

VMSize="<num bytes>"

- Current heap size:

HeapSize="<num bytes>"

- Total physical memory:

SystemPhysical="<num bytes>"

- Total virtual memory:

SystemVirtual="<num bytes>"

- Size of total available VM heap:

TotalHeap="<num bytes>"

- Percent of available heap currently in use:

HeapInUse="<integer>%"

## INSTALLED PROCESSES

Each installed process type is a monitorable resource. The execution state of the process type is displayed—installed test, installed production, or suspended. For more information about process types, see the *Partner Agreement Manager User's Guide*.

If the process type is suspended, the current number of queued events for the process type is displayed. You can set the number of queued events at which a warning message is sent.

If the process type is executable, the current number of running instances of this process type is displayed.

## RESOURCE NAME

Public Process:<process display name>

## PROPERTIES

- Length of the event queue at which a warning is sent:

EventQueueThreshold="<integer>"

## STATUS

- Current process install mode:

Mode="Test | Production"

- Whether this process type is suspended:

State="Active | Suspended"

- Number of process instances of this type currently executing (only displayed if the process is active):

InProgress="<integer>"

- Number of events queued for this process type (only displayed if the process is suspended):

EventsQueued="<integer>"

## THREAD POOLS

A thread pool allows Partner Agreement Manager to use threads more efficiently by providing a pool of threads that are managed by the system. There are thread pools for public processes, private processes, inbound Partner Agreement Manager communication, outbound Partner Agreement Manager communication, and non-Partner Agreement Manager communication.

Some thread pools in Partner Agreement Manager are monitorable resources. Because the number of threads indicates how many objects can run concurrently, monitor the thread pool for the number of waiting threads. If a thread pool is monitored, information about the thread pool load is displayed. You can change the size of the thread pool and set the number of waiting threads at which a warning message must be sent.

---

**IMPORTANT:** Contact Customer Support before modifying any thread-pool size. Increasing or decreasing thread-pool size might negatively affect performance.

---

## RESOURCE NAME

Thread Pool:<thread pool name>

## PROPERTIES

- Size of the thread pool:

ThreadPoolSize="<integer>"

- Number of waiting objects at which to send a warning message:

ObjectsWaitingThreshold="`<integer>`"

#### STATUS

- Current number of objects waiting for an available thread:

ObjectsWaiting="`<integer>`"

#### ADAPTER INSTANCES

Each installed adapter instance is a monitored resource. The name of the monitored resource is composed of the name of the adapter instance and the Adapter Server ID. The status displays the running state of the adapter instance—running, stopped, or suspended—and lists the current adapter property settings. For more information on adapter instances, see [Managing adapters](#) on page 91.

#### RESOURCE NAME

`<name of adapter instance> on IS Server <IS ID where the adapter is installed>`

#### STATUS

- Current running state:

State=`<"running" | "stopped" | "suspended">`

- Current adapter property settings.

## ABOUT THE PARTNER AGREEMENT MANAGER SNMP AGENT

The Simple Network Management Protocol (SNMP) is a set of network communication specifications that enable network applications to be managed remotely.

The Partner Agreement Manager SNMP Agent exposes the information gathered by the diagnostic monitoring system as SNMP objects and traps to network management applications that use SNMP—for example, HP OpenView or Tivoli NetView.

Partner Agreement Manager system messages that appear in the Auditor's System Messages folder also appear as SNMP traps in SNMP-based network management applications. You specified whether to use the SNMP Agent during installation.



**NOTE:** If you did not install the SNMP Agent during installation and later decide to use it, call Customer Support for information on how to set it up.

During installation, you also had the option to specify trap receivers. Trap receivers are computers on your network that use SNMP-based network applications to listen for Partner Agreement Manager system messages.

If you need to change or add to the list of computers that listen for Partner Agreement Manager system messages, stop the Process Server and edit this line in the **Partner.properties** file:

```
com.extricity.registry.SNMPTrapReceivers= ; mode=server ;  
type=string ; desc=space-separated list of SNMP trap receiver  
hostnames
```

The changes take effect after you restart the Process Server.

## SETTING UP PARTNERS

Read this chapter for information about setting up partners and updating partner information.

This chapter includes these sections:

- *About setting up partners* on page 64.
- *Setting up a new Partner Agreement Manager Channel partner* on page 66.
- *Accepting new Partner Agreement Manager Channel partners* on page 69.
- *Updating partner information* on page 75.

## ABOUT SETTING UP PARTNERS

Partner Agreement Manager is designed to facilitate the exchange of important business information between companies in a secure, automated fashion. The companies you exchange business information with via Partner Agreement Manager are your Partner Agreement Manager Channel partners. Each company's Partner Agreement Manager Channel profile provides the key for exchanging information securely.

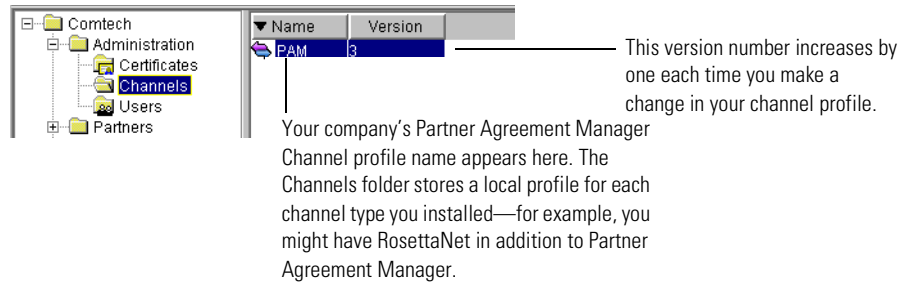
With WebSphere Partner Agreement Manager 2.2, you can implement different types of partner-to-partner communication channels. A channel encapsulates all the processing information needed to send Partner Agreement Manager *messages* to a partner's system, and to translate data from a partner into Partner Agreement Manager messages. All Partner Agreement Manager installations have the Partner Agreement Manager channel installed. Other available channels include RosettaNet and cXML.

**NOTE:** This guide describes setting up Partner Agreement Manager Channel partners only. For information about setting up all other types of partners, see the appropriate Partner Agreement Manager documentation.

Before you can add a Partner Agreement Manager Channel partner, each company must set up all three segments of its own Partner Agreement Manager Channel profile. A channel profile identifies a contact person at the company, establishes communication services, and defines the company's security profile.



When you set up another company as a Partner Agreement Manager Channel partner, you exchange channel profile information with your partner to ensure authenticity. Each time you revise channel profile information—to change a contact name, or to add security certificates, for example—Partner Agreement Manager increments the channel profile version number to help you and your partners synchronize channel profile information.



**NOTE:** Partner Agreement Manager now supports accessing user and partner information from an LDAP (Lightweight Directory Access Protocol) directory. For more information on setting up Partner Agreement Manager for LDAP, see [Using LDAP with Partner Agreement Manager](#) on page 129.

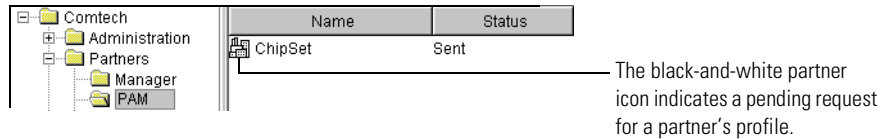
Setting up a Partner Agreement Manager Channel partner is a multi-step, interactive process. The process includes off-line communication as well as the exchange of Partner Agreement Manager Channel messages.

Use the telephone, e-mail, or fax to get this information before you begin setting up a partner:

- The name of your partner's Process Server.
- The port number of your partner's Process Server.
- The communication services your partner specifies for you to connect to when you send messages. Your partner might, for example, have three Internet services set up, but request that you use only two of them.

Either partner can start the process by adding the other. You begin by entering some basic information about the prospective partner so that you can send an initial message. Partner Agreement Manager sends a copy of your Partner Agreement Manager Channel profile to the prospective partner and requests a copy of the partner's Partner Agreement Manager Channel profile in return.

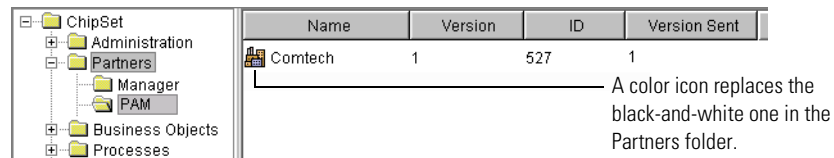
As soon as you send your request, Partner Agreement Manager displays a black-and-white icon for the partner in your Partner Agreement Manager channel folder, which is in the Partners folder. You can double-click the icon to see your request for information.



When you send your request, your partner's Process Manager window displays an action item in the Manager folder in the Partners folder. The partner reviews your channel profile, verifies your security certificates (usually over the phone), marks your certificates as "trusted," and accepts your channel profile.

When your partner accepts your channel profile, the partner's Partner Agreement Manager installation sends you the most up-to-date version of its Partner Agreement Manager Channel profile. It appears as an action item in your Partners\Manager folder, and it is now your turn to go through the steps of trusting certificates and accepting the channel profile. (See [Accepting new Partner Agreement Manager Channel partners](#) on page 69.)

When a partner accepts the other's channel profile, the partner's icon changes from black and white to color.



## SETTING UP A NEW PARTNER AGREEMENT MANAGER CHANNEL PARTNER

The first step in setting up a channel partner is to enter the information Partner Agreement Manager needs before it can send an initial message to your partner. Partner Agreement Manager then sends the latest valid version of your Partner Agreement Manager Channel profile to the partner for acceptance.

## To set up a new partner:



- 1 Click the New Partner button in the toolbar.

The New Partner Wizard appears.

A screenshot of the 'New Partner Wizard' dialog box. The title bar reads 'New Partner Wizard'. The main text says 'Enter the name of the new partner and select a channel.' Below this is a 'Partner Name:' label followed by an empty text input field. Underneath is a 'Channels:' label followed by a list box containing the text 'PAM'. At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Partner Agreement Manager lists the channel types you installed—for example, if you installed RosettaNet it would appear here, in addition to Partner Agreement Manager.

- 2 Type the partner's name and select a channel.

**NOTE:** You don't need to type the partner's full name. Partner Agreement Manager updates the name you enter with the partner's channel profile name when you receive your partner's channel profile.

- 3 Click Next to move to the next New Partner Wizard step.

A screenshot of the 'Service Types' dialog box. The title bar reads 'Service Types:'. The main text lists three options: 'Internet', 'Dialup', and 'MQSeries'. A horizontal line is positioned below the list.

The New Partner Wizard lists the communication service types that are available.

- 4 Select the type of communication service that the new partner uses and click Next.

You must select a synchronous service to exchange partner information.

The information needed depends on the type of service you selected—Internet or Dialup.

The image shows two overlapping dialog boxes. The background dialog box is titled "Internet" and contains two input fields: "Host:" and "Port:". The foreground dialog box is titled "Enter the communication service information." and contains a "Dialup" section with four input fields: "Phone:", "Baud Rate:", "Host:", and "Port:". Both dialog boxes have a "< Back" button and a "Next >" button at the bottom.

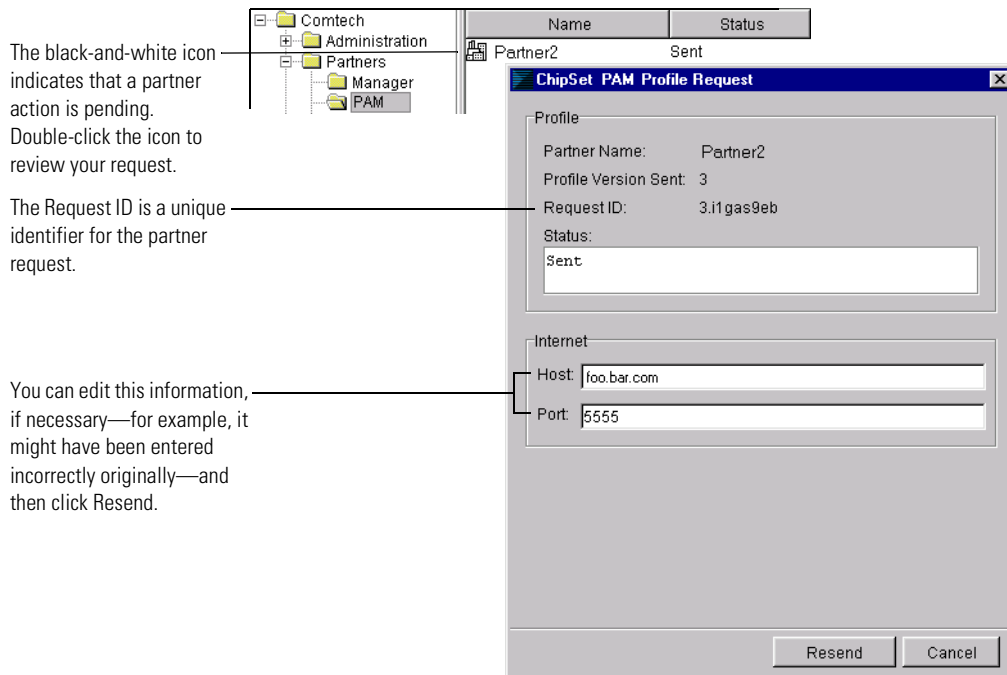
- 5 Type the information for the type of service you selected, to identify how the partner's Process Server will receive the messages you send. Contact the partner directly to get this information:
  - Internet: host and port
  - Dialup: phone, baud rate, host, and port
- 6 Click Next to review the properties you entered for the new partner.

The image shows a dialog box with the following text:  
Partner name: ChipSet  
Channel: PAM  
  
Communication Service:  
Name: Internet  
Type: Internet  
Host: foo.bar.com  
Port: 5555

A line points from the text "The properties you assigned to the new partner appear here." to the "Communication Service" section.

- 7 Click Finish to send a copy of your Partner Agreement Manager Channel profile to your partner and request a copy of the partner's Partner Agreement Manager Channel profile.

**TIP:** Partner Agreement Manager displays a black-and-white icon for the new partner request in your Partners\PAM folder. You can double-click the icon to see the status of your request for information.



## ACCEPTING NEW PARTNER AGREEMENT MANAGER CHANNEL PARTNERS

Partner Agreement Manager requires each prospective Partner Agreement Manager Channel partner to review the other's Partner Agreement Manager Channel profile, verify and trust the other's certificates, and accept the other's channel profile.

Before accepting a new partner:

- Review the partner's Partner Agreement Manager Channel profile and verify the security certificates it contains.
- Mark the partner's certificates as "trusted" after you are satisfied with their authenticity. You must trust at least one signature certificate and one encryption certificate. (For more information about certificates, see [Setting up certificates](#) on page 36.)

- Specify which of the partner's incoming communication services you will try to connect to when sending messages to the partner. You need to know the services to specify if, for example, the partner has set up three incoming Internet services but requests that you use only two of them. (See *Setting up communications* on page 24.)
- Accept the other partner's channel profile.

When another Partner Agreement Manager installation sets you up as a new partner, or when your partner has accepted your channel profile request, you receive a copy of that partner's Partner Agreement Manager Channel profile (it appears in the Manager folder in your Partners folder).

**NOTE:** The illustrations in this section show how one partner (ChipSet) responds when it receives a partner request from another partner (Comtech).

### To accept new partners:

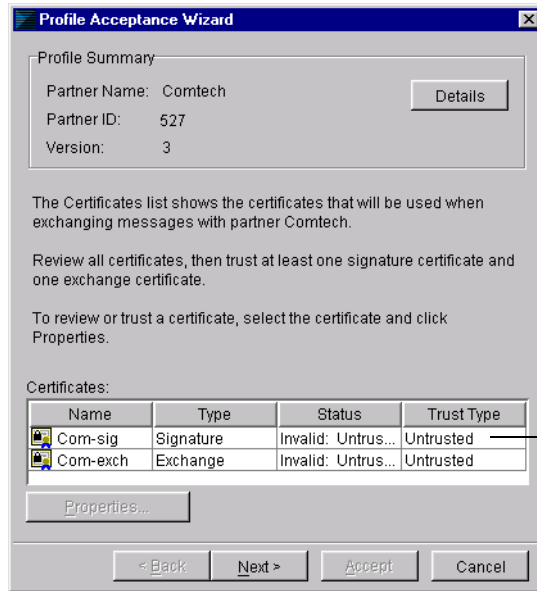
- 1 Open the Partners folder, open the Manager folder, and double-click the partner awaiting action.



The partner's Profile Request dialog box appears.



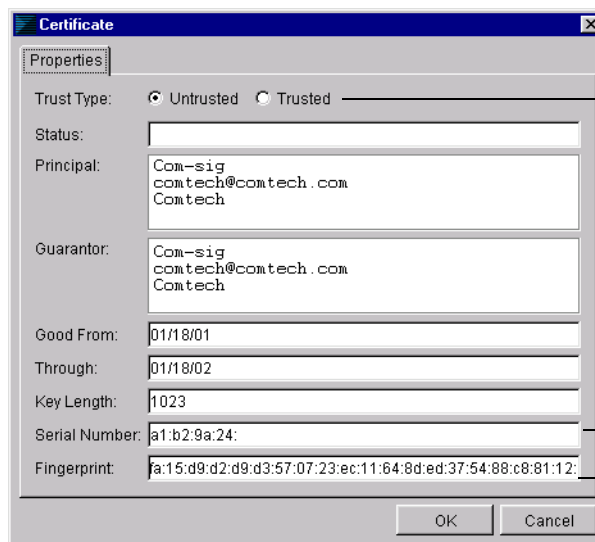
- 2 Ensure that the channel profile is from a known partner and click Continue. The Profile Acceptance Wizard appears.



Trust one signature and one encryption certificate before you exchange profiles with a partner.

- 3 Select a certificate to trust and click Properties (or double-click the certificate name).

The partner's Certificate dialog box appears.



Click to trust a partner's certificate.

An e-mail address doesn't appear if your certificates were created on UNIX.

The serial number and fingerprint uniquely identify the certificate as belonging to this partner.

4 Review the partner's information and confirm it by telephone, if necessary. The most important information to verify is the serial number and the fingerprint for each certificate.

5 Click Trusted to trust the certificate, and then click OK.

6 Continue validating and trusting certificates.

Before you can run a process with this partner, you must trust one signature certificate and one encryption certificate.

**NOTE:** You can accept a partner without trusting any certificates—for example, you might want to build processes using the partner but haven't yet validated the partner's certificates. You can build processes using the partner, but you cannot run the processes until you trust at least one signature certificate and one encryption certificate.

7 Click Next when you finish trusting your partner's certificates.

The Profile Acceptance Wizard lists the partner's incoming communication services. These are the services that are available for use during message exchange.

Profile Summary

Partner Name: Comtech

Partner ID: 527

Version: 3

The Services list shows the communication services that partner Comtech supports.

To disable services that will not be used, select the service and click Properties.

Services:

Name	Type	Enabled
Internet-1	Internet	Yes
Dialup Service-1	Dialup Service	Yes
Dialup Service-2	Dialup Service	Yes

These services are available during message exchange with this partner.

8 Disable any service that is not to be used by selecting the service and clicking Properties.



The properties dialog box for the service appears.

Click to disable the service.

- 9 Click the Enabled check box to remove the check mark and thus disable the service. Click OK.

The status of the connection changes to show the new setting.

Name	Type	Enabled
Internet-1	Internet	Yes
Dialup Service-1	Dialup Service	Yes
Dialup Service-2	Dialup Service	No

Partner Agreement Manager uses only the enabled connection services when you transmit messages to a partner.

10 Click Next to complete the channel profile acceptance process.



Click to accept the partner's channel profile.

11 Click Accept to accept the partner's channel profile.

When a partner is accepted, it appears in the Partners\PAM folder in the Process Manager window.

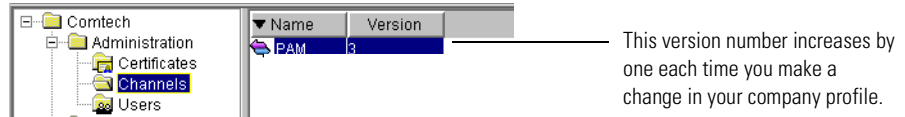
After you accept a new partner, its icon appears in color in your Partners\PAM folder.

Name	Version	ID	Version Sent
Comtech	3	527	5

Name	Status	Version	ID	V
ChipSet		5	555	-1

## UPDATING PARTNER INFORMATION

As you work with Partner Agreement Manager, you might need to change your company's Partner Agreement Manager Channel profile. You might, for example, need to change contact information, enable or disable connection services, or add or remove certificates. Each time you make a change in your channel profile, Partner Agreement Manager increases the version number by one.



Because your partners must be updated as soon as your Partner Agreement Manager Channel profile changes, Partner Agreement Manager lets you distribute new versions of your Partner Agreement Manager Channel profiles quickly. You can send the latest version of your channel profile to a specific partner, or you can send it to all partners at the same time.

### SENDING YOUR CHANNEL PROFILE TO A SPECIFIC PARTNER

You can send your channel profile to any partner you select.

#### To send your channel profile to a specific partner:

- 1 In the Process Manager window, open the Partners\PAM folder.
- 2 Right-click the partner's channel profile and choose Distribute from the menu that appears.

Partner Agreement Manager looks to see whether that partner has the most recent copy of your channel profile. If a newer channel profile exists, Partner Agreement Manager sends the new channel profile. The current version appears in the Version Sent column of the Process Manager window. If you are the partner receiving a new channel profile, you see the new channel profile information the next time you open the partner's Partner Agreement Manager Channel profile. Be sure to look for, verify, and trust any new security certificates.

## SENDING YOUR CHANNEL PROFILE TO ALL PARTNERS

You can also send your channel profile to all partners at once.

### To send your channel profile to all partners:

- 1 In the Process Manager window, open the Administration folder and the Channels folder.
- 2 Right-click your Partner Agreement Manager Channel profile and choose Distribute To All from the menu that appears.

Partner Agreement Manager sends the latest version of your channel profile to all Partner Agreement Manager Channel partners. You can verify that the Version Sent number has incremented in the Process Manager window.

# ADMINISTERING THE ADAPTER SERVER

Read this chapter for information about starting and administering the Adapter Server, including starting and stopping server components, testing your connection to a Process Server, and monitoring operations and events.

This chapter includes these sections:

- *About the Adapter Server* on page 78.
- *Starting the Adapter Server* on page 80.
- *About the Adapter Server window* on page 81.
- *Starting the Adapter Server on Windows* on page 83.
- *Monitoring operations and events* on page 83.
- *Testing the server connection* on page 84.
- *Configuring the Adapter Server* on page 85.
- *Stopping the Adapter Server on Windows* on page 89.
- *Managing the Adapter Server on UNIX* on page 89.

## ABOUT THE ADAPTER SERVER

The Adapter Server manages the execution of adapter interactions between Partner Agreement Manager private processes and your business systems. The Adapter Server supports:

- Execution of Partner Agreement Manager adapter operations.
- Archiving of adapter interactions.
- Creation of events from the business systems.
- Presentation of adapter properties to process designers.
- Registration and installation of adapters.

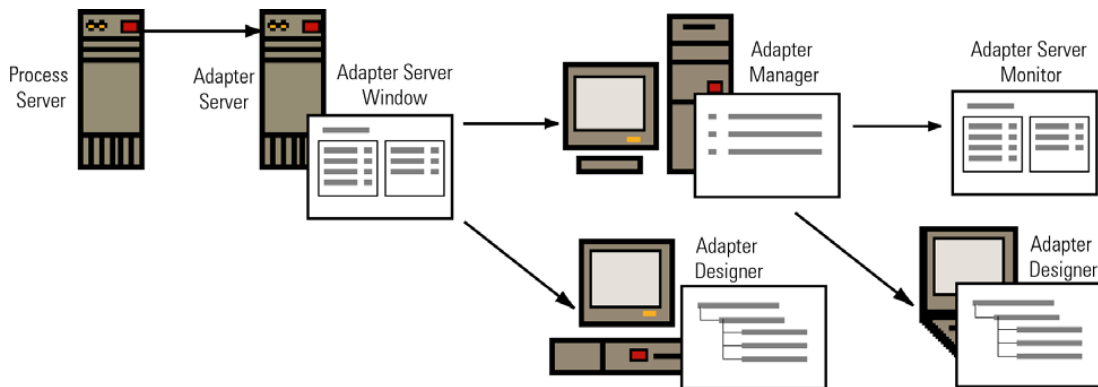
In addition, the Adapter Server acts as the connection point for any Adapter Server components that might be running.

---

**IMPORTANT:** The Adapter Server must be running whenever Partner Agreement Manager processes are being tested, deployed, or executed.

---

The Adapter Server is actually composed of several components: the Adapter Server window, the Adapter Manager, and the Adapter Designer.



## ■ Adapter Server

For an Adapter Server running on the Windows platform, you use the Adapter Server window to start and stop the Adapter Server, to configure the Adapter Server, and to monitor adapter operations and events. You can also launch the Adapter Manager and Adapter Designer from the Adapter Server window. The Adapter Server window runs only on the computer where the Adapter Server is installed.

For an Adapter Server running on the UNIX platform, you start and stop the Adapter Server from the command line. You can use the Adapter Manager to configure the Adapter Server, and to monitor adapter operations and events.

## ■ Adapter Manager

For an Adapter Server running on the Windows platform, you use the Adapter Manager (the Adapter Server client) primarily to add and remove adapters. You can also use it to start and stop the Adapter Server, to configure the server, and to display the Adapter Server Monitor (a display-only version of the Adapter Server window that shows information about operations and events). The Adapter Manager can be installed and run independently, or you can run it from the Adapter Server window. You can also run the Adapter Manager from a browser window. For more information about using the Adapter Manager, see the *Partner Agreement Manager Adapter Developer's Guide*.

For an Adapter Server running on the UNIX platform, you use the Adapter Manager to configure the Adapter Server, and to monitor adapter operations and events. For more information about using the Adapter Manager, see “Managing Adapters” in the *Partner Agreement Manager Adapter Developer's Guide*.

## ■ Adapter Designer

You use the Adapter Designer to develop new adapter types and implementations. You can also import and export adapters, or edit existing adapters. The Adapter Designer can also be installed and run independently, or if your Adapter Server is running on the Windows platform, you can run it from the Adapter Server window. For more information about using the Adapter Designer, see the *Partner Agreement Manager Adapter Developer's Guide*.

## STARTING THE ADAPTER SERVER

The Adapter Server window is supported only for Adapter Servers running on the Windows platform. For Adapter Servers running on the UNIX platform, use the Adapter Manager to configure the Adapter Server.

You start the Adapter Server the same way you do any other application: from a shortcut placed in your Start menu by the Partner Agreement Manager installer.

---

**IMPORTANT:** The Process Server must be running before you start the Adapter Server.

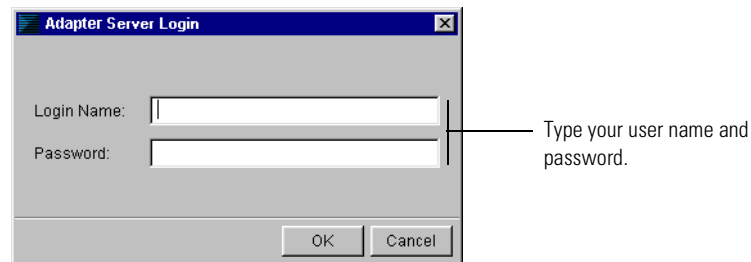
---

Unless you configure it to do so, the Adapter Server does not necessarily start when you open the Adapter Server window. Once you open the Adapter Server window, you can then start or stop the Adapter Server. The Adapter Server need not be running for you to open and use the Adapter Manager or Adapter Designer. However, you must start the Adapter Server before you can use it to monitor operations and events. See *Starting the Adapter Server on Windows* on page 83.

### To start the Adapter Server:

- 1 Click Start>Programs> IBM WebSphere Business Integrator>Adapter Server.

The Adapter Server Login dialog box appears.



- 2 Type your Partner Agreement Manager user name (login name) and password. Click OK.

The preset user name for the admin user is `admin`. The password is set when you install Partner Agreement Manager. User names are not case-sensitive, but passwords are.

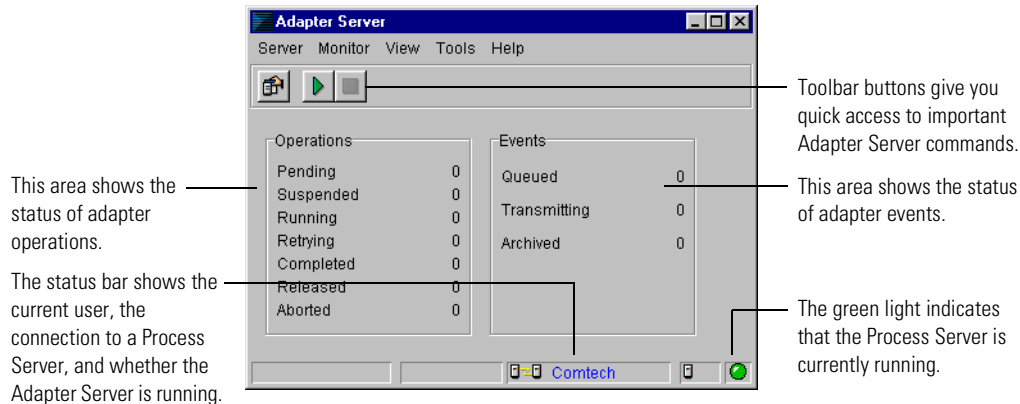


The Adapter Server window appears. See *About the Adapter Server window*, next.

**NOTE:** Initially, the Adapter Server is not preset to start when you open the Adapter Server window. However, you can configure the Adapter Server to start automatically. See *Configuring the Adapter Server* on page 85.

## ABOUT THE ADAPTER SERVER WINDOW

The Adapter Server window displays information about the current Partner Agreement Manager installation (such as host name and port) and gives you access to configuration tasks. Using the Adapter Server window, you can start and stop the Adapter Server, configure the Adapter Server, and monitor adapter operations and events. You can also launch the Adapter Manager and Adapter Designer from the Adapter Server window.



**NOTE:** The Adapter Server window is supported only on the Windows platform.

## ABOUT THE COMMAND TOOLBAR

With the buttons on the Command toolbar at the top of the Adapter Server window, you can configure the Adapter Server, start monitoring operations and events, and stop monitoring them.



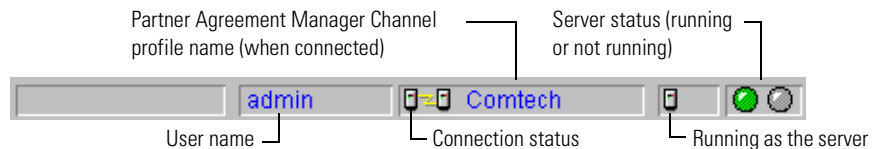
### To show or hide the toolbar:

- ▶ Choose **Toolbar** from the **View** menu.

A check mark indicates that the toolbar is currently displayed.

## ABOUT THE STATUS BAR

The status bar at the bottom of the Adapter Server window displays the name of the current user. If you are connected to a Process Server, a connection icon and the channel profile name appear. The status bar also shows if the Adapter Server is currently running and where you are running the Adapter Server from.



### This icon Indicates



The Adapter Server is connected to a Process Server.



The Adapter Server is not connected to a Process Server.



The Adapter Server is running (green).



The Adapter Server is stopped (red).



You are running the Adapter Server window from the computer where the Adapter Server is installed.



You are running the Adapter Server window from a different computer.

### To show or hide the status bar:

- ▶ Choose **Status Bar** from the **View** menu.

A check mark indicates that the status bar is currently displayed.

## STARTING THE ADAPTER SERVER ON WINDOWS

Partner Agreement Manager is preset so that opening the Adapter Server window does not automatically start the Adapter Server. This lets you to start the Adapter Server whenever you want. After the Adapter Server is started, you can also begin monitoring adapter operations and events.

### To start the Adapter Server:

- ▶ Choose Start from the Server menu.

A green indicator light appears in the status bar to indicate that the Adapter Server is running.

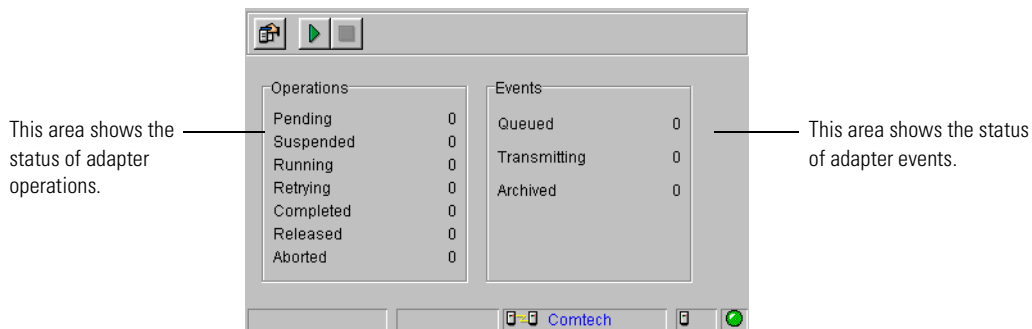


The green light indicates that the Adapter Server is running.

**NOTE:** You can configure the Adapter Server so that it starts automatically when you launch it. See *Configuring the Adapter Server* on page 85.

## MONITORING OPERATIONS AND EVENTS

When the Adapter Server is running, it can monitor the operations and events for any adapters that are also running. After you start the monitoring function, the Adapter Server window displays information about adapter operation and event status.




## STARTING MONITORING

### To start monitoring on an Adapter Server running on Windows:

-  In the Adapter Manager (the client for the Adapter Server), choose Start from the Monitor menu, or click the Start Monitor button in the Command toolbar.

### To start monitoring on an Adapter Server running on UNIX:

-  In the Adapter Manager, choose Adapter Server Monitor from the Tools menu. The Adapter Server Monitor appears. Choose Start from the Monitor menu or click the Start Monitor button in the Command toolbar to start monitoring.


The Adapter Server window immediately displays information about the number of operations that are pending, running, completed, and archived. For events, it monitors the number queued, sent, and archived.

## STOPPING MONITORING

### To stop monitoring on an Adapter Server running on Windows:

-  In the Adapter Manager, choose Stop from the Monitor menu, or click the Stop Monitor button in the Command toolbar.

### To stop monitoring on an Adapter Server running on UNIX:

-  In the Adapter Server Monitor, choose Stop from the Monitor menu, or click the Stop Monitor button in the Command toolbar.

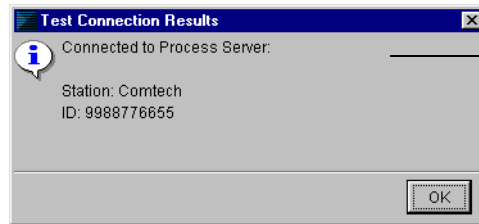
## TESTING THE SERVER CONNECTION

With Partner Agreement Manager, you can test the connection between the Adapter Server and the corresponding Process Server. In addition to displaying the Partner Agreement Manager Channel profile name of the Process Server you're connected to, testing the server connection also displays the partner ID of the Process Server.

For an Adapter Server running on Windows, use the Adapter Manager. For an Adapter Server running on UNIX, use the Adapter Manager. The following directions apply to both the Adapter Server administrator and the Adapter Manager.

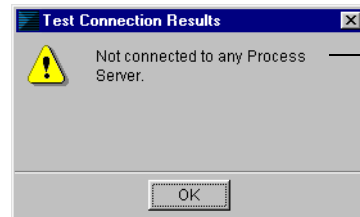
### To test the server connection:

- ▶ Choose Test Connection from the Server menu.
  - If you are connected to a Process Server, testing the connection displays this message.



This message shows the name of the Process Server you're connected to.

- If you are not connected to a Process Server, testing the connection displays this message.



This message indicates that you're not connected to a Process Server.

## CONFIGURING THE ADAPTER SERVER

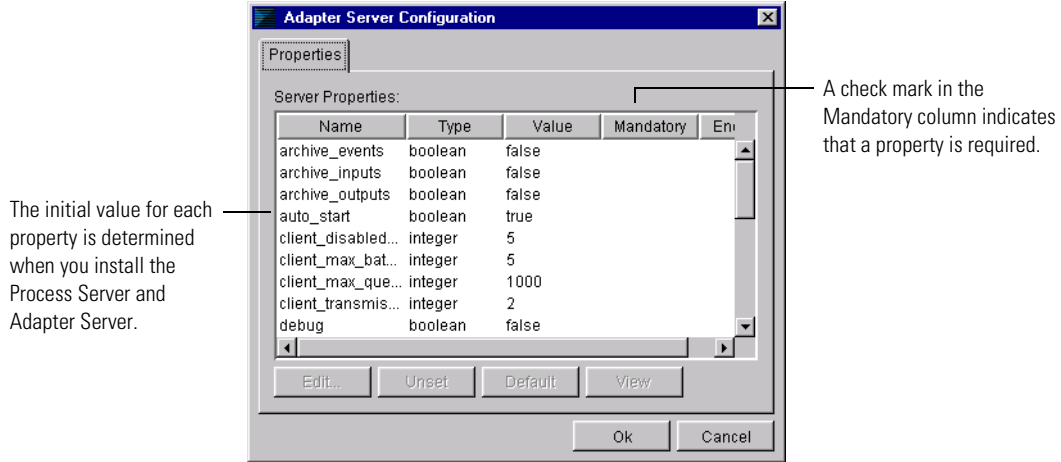
With Partner Agreement Manager, you can configure the Adapter Server to suit your environment. For an Adapter Server running on Windows, use the Adapter Manager. For an Adapter Server running on UNIX, use the Adapter Manager. The following directions apply to both the Adapter Server administrator and the Adapter Manager.

### To configure the Adapter Server:



- 1 Choose Configure Server from the Server menu, or click the Configure button in the Command toolbar.

The Adapter Server Configuration dialog box appears.

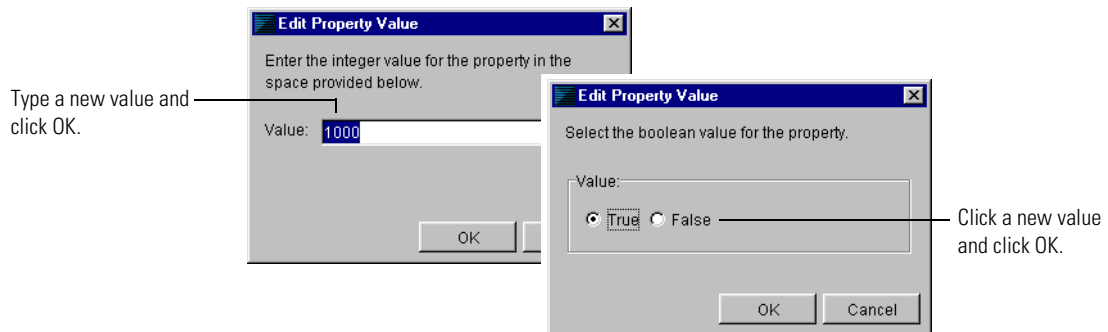


- 2 To remove the current setting for a property, select the property and click Unset.

If you unset the value for a mandatory property, Partner Agreement Manager alerts you that a value is required when you leave the Adapter Server Configuration dialog box.

- 3 To restore a property's default value, select the property and click Default.
- 4 To change the value for a property, double-click the property or select the property and click Edit.

The Edit Property Value dialog box appears.



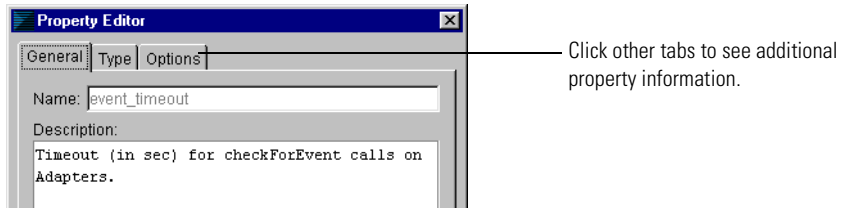
You can edit these Adapter Server settings.

<b>This property</b>	<b>Determines</b>
archive_events	Whether to archive events. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
auto_start	Whether the Adapter Server automatically starts when you launch it. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
client_disabled_sleep	The length of time the message dispatch thread waits before checking to see if the Adapter Server is running. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
client_max_queue_size	The maximum size of the message queue. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
data_release_interval	The number of seconds between attempts to clean up adapter operation data belonging to completed private processes. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
event_ceiling	The maximum number of events permitted for a single check for events call. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
event_timeout	How long the Adapter Server will wait for events calls to time out. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
exec_db_io	Execution data must be checkpointed in the database or in dynamic memory. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
is_id	The unique Adapter Server ID. This is preset to 1, and must remain 1 for the current Partner Agreement Manager release. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
is_server_host	The host name of the computer where the Adapter Server is running. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
is_server_port	The port number of the Adapter Server computer. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
max_adapter_errors	The maximum number of runtime errors that can occur before the Adapter Server prevents execution for an adapter. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.

This property	Determines
num_event_relay_threads	The number of threads in the event thread pool used to send events to the Process Server. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
num_executor_threads	The number of threads in the execution pool for concurrent execution. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
pending_queue_limit	The number of pending adapter operations to queue before beginning to back up the pending queue to the database. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
retry_check_interval	The number of seconds to wait before checking for retry operation requests. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
retry_queue_limit	The number of adapter operations to queue before beginning to back up the retry queue to the database. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
same_db	A flag that shows whether Partner Agreement Manager and the Adapter Server share the same database. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.
suspended_queue_limit	The number of suspended adapter operations to queue before beginning to back up the suspended operation queue to the database. You must stop and restart the Adapter Server after editing this setting for the changes to take effect.

- To view more detailed information about a property, select the property and click View.

The Property Editor dialog box appears. It displays the property's name and description, the type of value it requires, the default value and whether values are constrained to a list of predetermined values, and whether the property values is required or encrypted.



- Click OK when you finish editing properties.



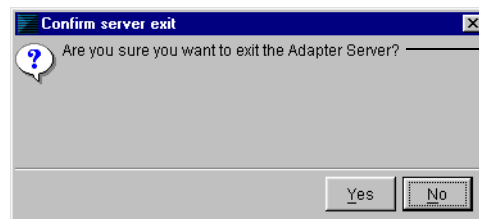
## STOPPING THE ADAPTER SERVER ON WINDOWS

You can stop the Adapter Server as needed. As soon as you stop the Adapter Server, any instances of installed processes that are currently running will be halted until you restart the Adapter Server. In addition, no new instances of processes can start until the Adapter Server is restarted. You might, for example, want to stop the Adapter Server so that you can update an existing adapter with new class files. Or you might want to stop the server to perform maintenance.

### To stop the Adapter Server:

- 1 Choose Exit from the Server menu.

Partner Agreement Manager asks you to confirm that you want to stop the server at this time.



Partner Agreement Manager asks you to confirm that you want to stop the Adapter Server.

- 2 Click Yes.

**NOTE:** UNIX might keep TCP ports in TIME\_WAIT state for up to five minutes. You can monitor port status with the command:

```
netstat -a
```

If you try to restart the Process Server before UNIX releases the ports, you will get a bind error because the ports are already in use.

## MANAGING THE ADAPTER SERVER ON UNIX

On UNIX, you manage the Adapter Server using the Adapter Server client. This client, like the Partner Agreement Manager client, runs on a Windows system. For more on installing the Adapter Server client (also referred to as the Adapter Manager), see the *Partner Agreement Manager Installation Guide*. For more on using the Adapter Manager, see the *Partner Agreement Manager Adapter Developer's Guide*.



## MANAGING ADAPTERS

Read this chapter for information about creating adapter instances, as well as starting, stopping, renaming, duplicating, importing, and exporting adapter instances.

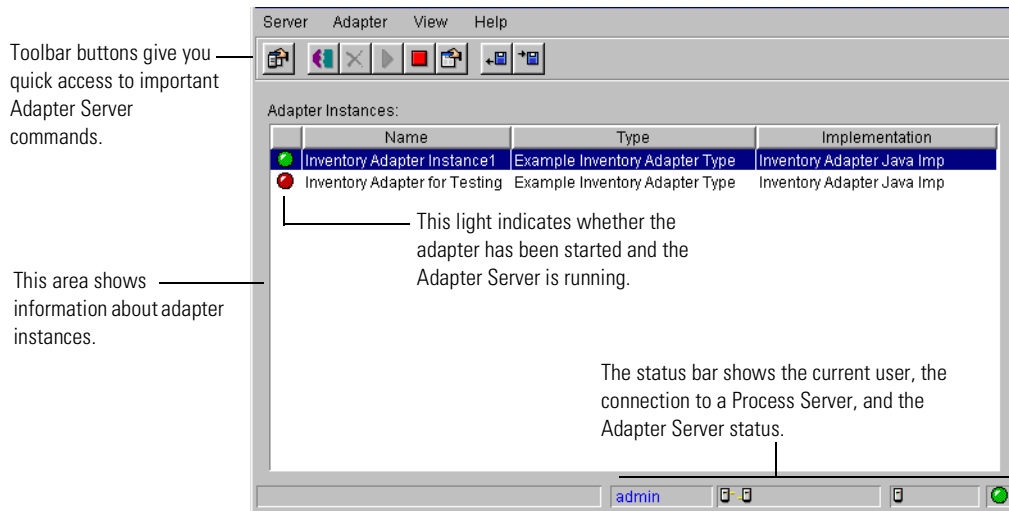
This chapter includes these sections:

- *About managing adapters* on page 92.
- *Starting the Adapter Manager* on page 93.
- *Adding adapter instances* on page 94.
- *Starting or stopping adapter instances* on page 98.
- *Duplicating adapter instances* on page 100.
- *Renaming adapter instances* on page 100.
- *Exporting an adapter instance* on page 101.
- *Importing an adapter instance* on page 102.

## ABOUT MANAGING ADAPTERS





After an adapter has been completed, you make it available to process designers by adding an instance. You can then start the adapter so that processes can use it to interact with business systems. You can also rename an adapter instance, duplicate it, remove it, or view its properties.

Use the Adapter Manager to add, remove, start, stop, and manage adapters. The Adapter Manager contains the same status bar as the Adapter Server window, but it has a different set of toolbar buttons.

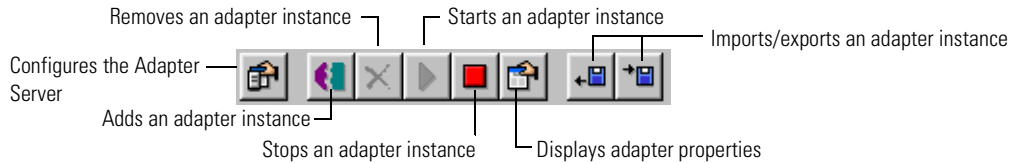


**TIP:** You can right-click items in the Adapter Manager window to display a context-sensitive menu of commands.

The light next to each adapter instance name indicates whether the adapter instance is started or stopped and whether the Adapter Server is running.

- A green light  indicates that the adapter instance is started and the Adapter Server is running.
- A red light  indicates that the adapter instance is stopped.
- An amber light  indicates that the adapter instance is started but the Adapter Server is not running.
- A blinking amber light  indicates that the adapter instance is suspended.

With the buttons on the Command toolbar at the top of the Adapter Manager, you can configure the Adapter Server window, add or remove adapter instances, start or stop an adapter instance, or display adapter instance properties.



## STARTING THE ADAPTER MANAGER

The Adapter Manager is an Adapter Server component that you can launch from the Process Server window or install as a client on another computer and connect to the Adapter Server over the network. You can also run the Adapter Manager from a browser window.

From the Adapter Manager, you can:

- start and stop the Adapter Server.
- configure the Adapter Server.
- add or remove adapter instances.
- start or stop adapter instances.
- change adapter instance properties.

Partner Agreement Manager provides two ways to start the Adapter Manager: from the Adapter Server window or from another computer where the Adapter Manager is installed as a client.

### To start the Adapter Manager:

- ▶ From the Adapter Server window, choose Adapter Manager from the Tools menu.

The Adapter Manager window appears.

- ▶ From a computer on which the Adapter Manager has been installed, click Start>Programs>IBM WebSphere Business Integrator>Adapter Manager. The Adapter Manager window appears.

## ADDING ADAPTER INSTANCES

Adapters must be added before process designers can include them in a private process. An adapter that has been added is called an instance. When you add an adapter instance, you provide a name and description, specify the adapter type and implementation declaration, turn event polling on or off, and provide values for the adapter instance's properties. You can add adapter instances based on the same adapter type as many times as you want—using different names and property settings.

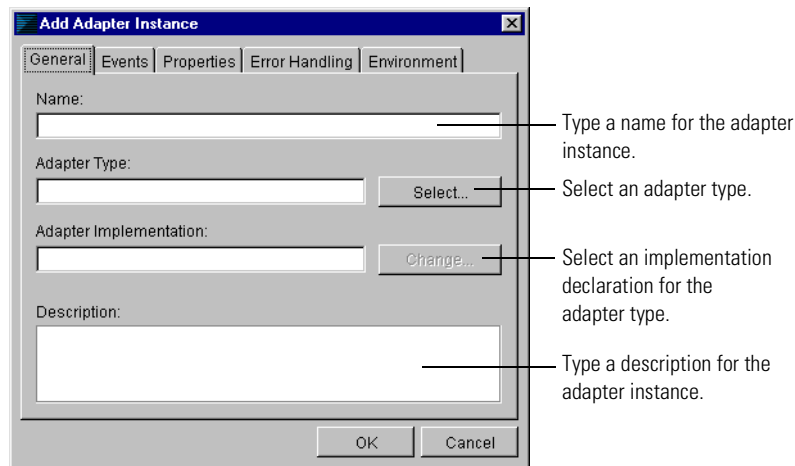
### To add an adapter instance:



- 1 Click the Add Adapter Instance icon in the Command toolbar, or choose Add from the Adapter menu.

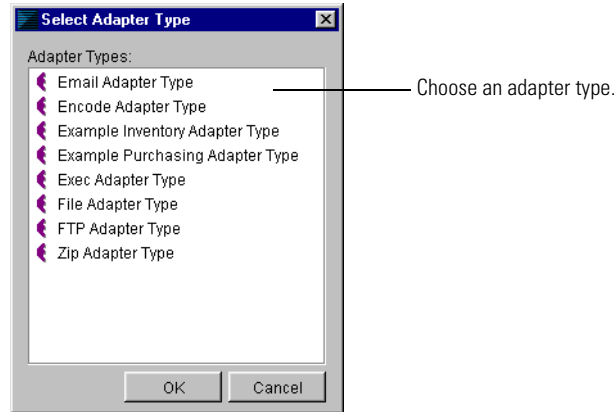
You can also right-click in the adapter list and choose Add from the menu that appears.

The Add Adapter Instance dialog box appears, with the General tab displayed.



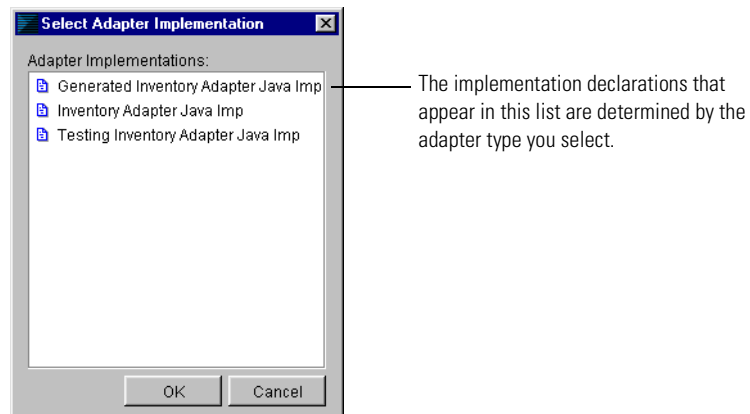
- 2 Type a name for the adapter instance and click Select to choose an adapter type.

The Select Adapter Type dialog box appears. It shows all available adapter types.



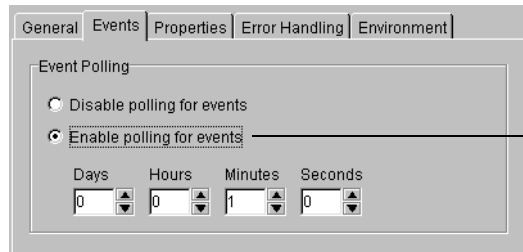
- 3 Choose an adapter type and click OK.
- 4 Click Change on the General tab to select an adapter implementation declaration.

The Select Adapter Implementation dialog box appears. It shows all implementation declarations for the adapter type you selected.



- 5 Select an adapter implementation declaration and click OK.
- 6 Click the Events tab and set event polling.

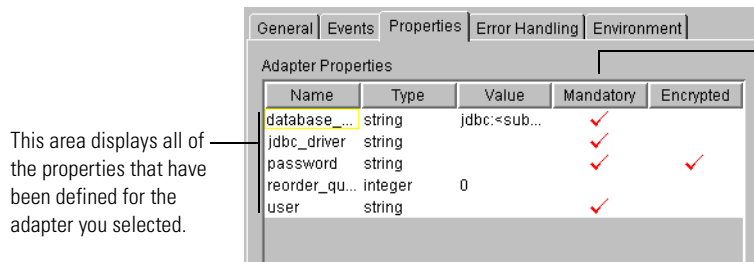
The Events tab appears. If you enable event polling, specify how often you want to poll for events.



If you turn on event polling, specify how often you want to poll for events.

- 7 Click the Properties tab to set values for the properties defined for this adapter type.

The Properties tab appears. This tab shows the default values for each property (if any), as well as whether each property is mandatory and encrypted (passwords, for example, usually are).

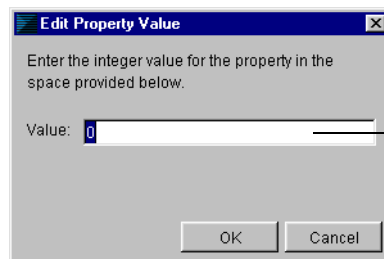


This area displays all of the properties that have been defined for the adapter you selected.

You must either use the default or enter a value for all mandatory properties.

- 8 Select the property you want to set and click Edit.

The Edit Property Value dialog appears.



Type a value for the property.



- 9 Type a value for the property and click OK. Edit other properties as necessary.

Click to remove the value for a selected property. Unset removes both edited and default values.

Name	Type	Value	Mandatory	Encrypted
database_...	string	jdbc:<sub...	✓	
jdbc_driver	string		✓	
password	string		✓	✓
reorder_qu...	integer	0		
user	string		✓	

Click to reset a selected property to its default value. If there is no default value defined in the adapter, the edited value remains as is.

Click to view property type and options such as mandatory and encryption.

- 10 Click the Error Handling tab to set values for error recovery and handling.

Set the maximum number of recovery attempts after suspension.

Click to suspend the adapter instance when it throws an EndSystemNotAvailableException exception. The Adapter Server will then attempt to recover.

Set the time between recovery attempts.

The Error Handling tab governs how the Adapter Server handles an `EndSystemNotAvailableException`. The startup method of your adapter should attempt all connections to business systems. The startup method must throw this exception if it fails to connect with a business system, such as a database.

If you enabled auto-recovery, the Adapter Server suspends the adapter. In the Adapter Manager, a suspended adapter is indicated by a blinking yellow light on the left. The Adapter Server waits the amount of time indicated by the recovery interval and then attempts to restart the adapter. The Adapter Server attempts to recover until the adapter does not throw `EndSystemNotAvailableException`, or until it has reached the maximum number of recovery attempts.

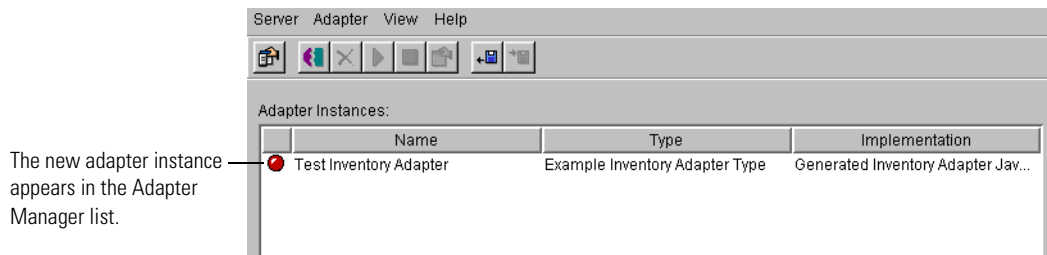
If it reaches the maximum number of recovery attempts, the Adapter Server stops the adapter and the extension action that called the adapter times out. When the extension action times out, the private process must handle the error appropriately.

- 11 Click the Environment tab to set the classloader for this adapter instance.

The preset classloader is the system's classloader. In the default case, the CLASSPATH is the same as the one the Adapter Server uses. If you choose to use another classloader, you need to make sure your adapter code is in the CLASSPATH.

**NOTE:** If you are running the Adapter Server on UNIX, remember that when setting your own CLASSPATH, the browse function will point you to the local client computer. You will need to add the adapter files on the UNIX computer to the CLASSPATH. You will need to consult with your system administrator to be able to view and browse those directories.

- 12 Click OK to add the new adapter instance.







## STARTING OR STOPPING ADAPTER INSTANCES

After an adapter instance is added, you must start the adapter instance so that processes can run against it. Process designers can work with a stopped adapter instance when they add Extension actions to a private process, but the process cannot call the adapter operation unless the adapter instance is also running.

You can start an adapter instance immediately after you add it, or you can start it later. Likewise, you can stop an adapter instance at any point. For example, you might want to stop an adapter instance and replace it with a newer version. If you stop an adapter instance that is currently executing, the adapter instance continues to run until all current executions have completed.

**NOTE:** When you stop an adapter instance, the Adapter Server queues all adapter operations on the adapter instance that is stopped. After you start the adapter, the Adapter Server runs the queued operations. Partner Agreement Manager processes that use the stopped adapter will continue to run, blocked at the Extension action until the adapter is restarted.

The light next to each adapter name indicates whether the adapter instance and the Adapter Server are started or stopped.

- A green light  indicates that both the adapter instance and the Adapter Server are started.
- A red light  indicates that the adapter instance is stopped.
- An amber light  indicates that the adapter instance is started but the Adapter Server is stopped.
- A blinking amber light  indicates that the adapter instance is suspended.

#### To start an adapter instance:



- ▶ Select the adapter instance and click the Start icon in the Command toolbar, or choose Start from the Adapter menu.

You can also right-click the adapter instance and choose Start from the menu that appears. If the Adapter Server is running, the adapter light changes from red to green. If the Adapter Server is not running, the adapter light changes to amber. (To start the Adapter Server, go to the Windows Start menu and choose Adapter Server from the IBM WebSphere Business Integrator menu. You will need to log in.)

#### To stop an adapter instance:



- ▶ Select the adapter instance and click the Stop icon in the Command toolbar, or choose Stop from the Adapter menu.

You can also right-click the adapter instance and choose Stop from the menu that appears. The adapter light changes from green or amber to red.

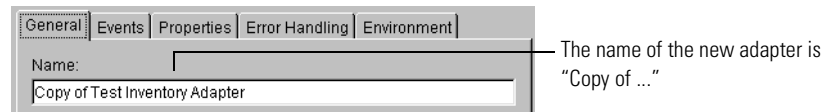
## DUPLICATING ADAPTER INSTANCES

Partner Agreement Manager makes it easy to add multiple similar instances of the same adapter type. You might, for example, want to add several nearly identical adapter instances that have slight variations in their property values. Or you might want to create an adapter instance that uses a different implementation, but uses the same property values. When you duplicate an adapter instance, the new instance is an exact replica of the existing instance. If you duplicate an adapter instance that has been started, the new adapter instance is created in a stopped mode.

### To duplicate an adapter instance:

- 1 Select the adapter instance you want to copy and choose Duplicate from the Adapter menu.

You can also right-click the adapter instance and choose Duplicate from the menu that appears. Partner Agreement Manager creates an exact copy of the current adapter instance and opens the Edit Adapter Instance dialog box.



- 2 Edit the new adapter instance as necessary and click OK.

## RENAMING ADAPTER INSTANCES

After an adapter instance is added, you can change its name. You might, for example, want to change an adapter instance name to make it more descriptive. The adapter instance must be stopped before you can change its name.

---

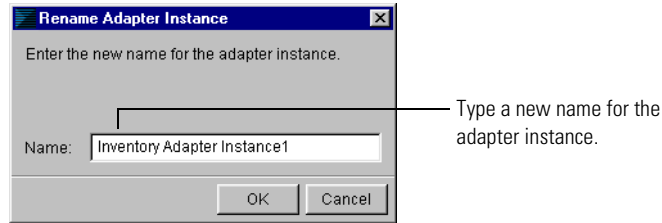
**IMPORTANT:** If a private process uses the adapter instance, you must revise the private process to reflect the new adapter instance name.

---

### To rename an adapter instance:

- 1 Select the adapter instance you want to rename, and choose Rename from the Adapter menu.

You can also right-click the adapter instance and choose Rename from the menu that appears. The Rename Adapter Instance dialog box appears.



- 2 Type a new name for the adapter instance and click OK.


## EXPORTING AN ADAPTER INSTANCE

To make it easier to work in multiple locations, Partner Agreement Manager lets you export adapters from one computer and import them elsewhere. You might, for example, develop adapters on a workstation for eventual installation on the computer that runs the Adapter Server. You can also develop an adapter on a desktop computer, export it, and continue development on any other computer where the Adapter Designer is installed.

You can export adapter instances as XML files. You can also export adapter types and implementation declarations.

**TIP:** Use file names for exported instances that make it easy to distinguish between them when you import them later.

### To export an adapter instance:

- 1 In the Adapter Manager, select the adapter instance you want to export.
- 2  Click the Export icon in the Command toolbar or choose Export from the File menu.

The Export Adapter Instance dialog box (a standard File dialog box) appears. The default name is that of the adapter instance.

- 3 Type a name for the exported adapter, select a location for it, and click Save. The Process Server writes an XML file for the adapter instance you selected.

---

**IMPORTANT:** If you export an adapter instance created by the Flat File Integration Wizard, you must also move the data format file.

---

## IMPORTING AN ADAPTER INSTANCE

After you export an adapter instance developed on a computer other than the one that runs the Adapter Server, Partner Agreement Manager makes it easy to import the adapter to the location you want. You must import an adapter type and implementation declaration before you can import any of its instances.

If you're importing adapters to a different Partner Agreement Manager instance (for example, if you are importing an adapter created by a third party), make sure that the business objects used by the adapter are available. If the underlying Process Server is the same, the business objects will already be available. Events are created on import.

### To import an adapter:



- 1 In the Adapter Manager, click the Import icon in the Command toolbar or choose Import Adapter Server from the Server menu.

An Import Adapter Instance dialog box (a standard File dialog box) appears.

- 2 Select the XML file to be imported and click Open.

The imported adapter instance appears in the Adapter Designer.

## AUDITING PROCESSES

Read this chapter for information about finding an instance of a process, monitoring a running process or auditing a completed process, and viewing system messages.

This chapter includes these sections:

- *About auditing* on page 104.
- *Finding an instance of a process* on page 107.
- *Viewing process information* on page 109.
- *Archiving and restoring process logs* on page 117.
- *Viewing system messages* on page 124.
- *Deleting system audit information* on page 126.
- *Extracting message information* on page 126.

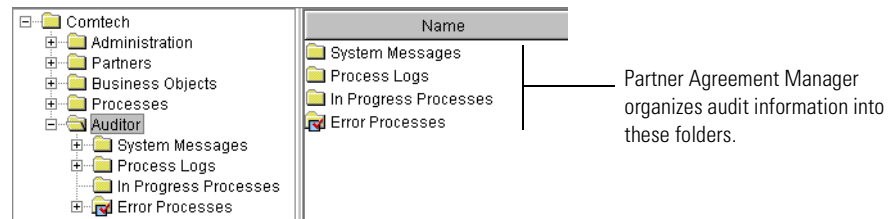
## ABOUT AUDITING

Each time you run a process, Partner Agreement Manager creates a new instance of the process and assigns it a unique ID. With the Partner Agreement Manager Auditor, you can monitor each instance as it runs, audit each completed instance, and view any error messages associated with each instance.

At any point while a process is running, you can display its current status in the Auditor. After a process terminates, you can use the Auditor to view the audit trail. For more information about the Process Audit window, see [Viewing process information](#) on page 109.

### ABOUT AUDITOR FOLDERS

Partner Agreement Manager divides messages in the Auditor folder into four main subfolders according to the message type.



- The System Messages folder contains an entry for each system event. A system event can be related to a process error, or to events that occur during normal Partner Agreement Manager operation, such as partner profile updates or process distribution. System events can also be generated when a monitored resource changes status.
- The Process Logs folder contains entries for each instance of a process that starts—whether it finishes running or not.
- The In Progress Processes folder lists the process instances that are currently running.
- The Error Processes folder contains entries for each process instance that generates an error.



Within each Auditor folder, Partner Agreement Manager organizes each day's messages into a separate subfolder. At the end of the month, it creates a folder to hold that month's daily folders. At the end of the year, Partner Agreement Manager creates a folder to hold the month folders for that year.

Name	Time
Feb 19, 2001	02/19/01 23:59:59
Feb 16, 2001	02/16/01 23:59:59
Feb 15, 2001	02/15/01 23:59:59
Feb 14, 2001	02/14/01 23:59:59
Feb 13, 2001	02/13/01 23:59:59
Feb 12, 2001	02/12/01 23:59:59
Jan 2001	01/31/01 23:59:59

## ABOUT AUDITOR MESSAGES

Partner Agreement Manager displays two types of audit information: system information and process information. System information consists of messages that describe system events, such as exceeding your communication time-out and retry limits. Other system messages give information about process distribution, partner exchange, scheduler failure, or server components being off-line, or the status of a monitored resource.

Each system message gives the time that the event occurred, the type of message, and the Partner Agreement Manager component that generated it.

Name	Time	Type	Source
Process Error for Comtech ...	02/19/0111...	Error	Engine Man...
Process Error for Comtech ...	02/19/0111...	Error	Engine Man...
Process Error for Comtech ...	02/19/0111...	Error	Engine Man...
Error while reading from tc...	02/19/0111...	Error	Transporter
Error while reading from tc...	02/19/0111...	Error	Transporter
Unable to receive from tcp/...	02/19/0111...	Error	Transporter
Unable to receive from tcp/...	02/19/0111...	Error	Transporter
Unable to send Distributio...	02/19/0111...	Warning	Transporter
Unable to send Distributio...	02/19/0111...	Warning	Transporter

Each time a process instance starts, Partner Agreement Manager assigns it a unique ID and logs a message in the In Progress Processes folder and the Process Logs folder. For each running instance of a process, the In Progress Processes folder shows the process name, the status, the start and end time, the owner, the version, the instance ID, and the execution mode (test or production).

Name	Status	Start Time	Owner	Version	ID	Execution
One-step ...	In Progress	02/19/01...	Comtech 2.2	0.hm7...	Test	
One-step ...	In Progress	02/19/01...	Comtech 2.2	0.hm7...	Test	
One-step ...	In Progress	02/19/01...	Comtech 2.2	0.hm7...	Test	
One-step ...	In Progress	02/19/01...	Comtech 2.2	0.hm7...	Test	

A check mark indicates there are In Progress messages. The check mark is removed when you mark all errors as resolved.

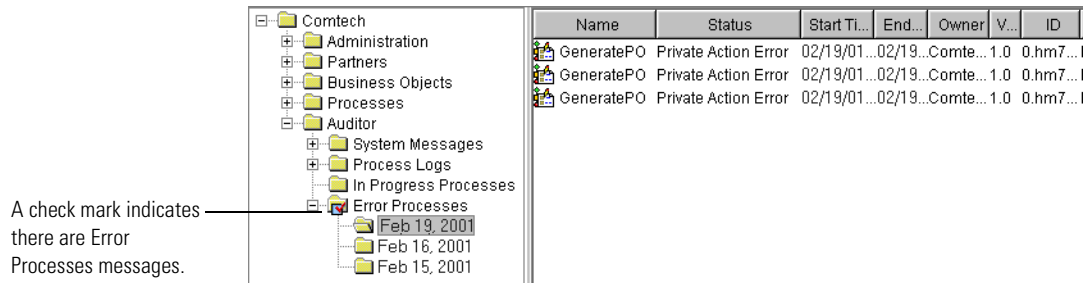
Entries in the Process Logs folder are initially listed according to start time, but you can sort them by name or any of the other columns that appear.

Process Logs are grouped by day.

Name	Status	Start	End	Owner	V...	ID	Execution
One-step...Complete...	Complete	02/19/...	02/19/...	Comtech 2.2	0.hm7ih...	Production	
One-step...Complete...	Complete	02/19/...	02/19/...	Comtech 2.2	0.hm7ih...	Production	
One-step...Complete...	Complete	02/19/...	02/19/...	Comtech 2.2	0.hm7ih...	Production	
Generate...Private Acti...	Private Acti...	02/19/...	02/19/...	Comtech 1.0	0.hm7io...	Production	
Generate...Private Acti...	Private Acti...	02/19/...	02/19/...	Comtech 1.0	0.hm7ip...	Production	
Generate...Private Acti...	Private Acti...	02/19/...	02/19/...	Comtech 1.0	0.hm7iq...	Production	
One-step...Complete...	Complete	02/19/...	02/19/...	Comtech 2.2	0.hm7ir...	Production	
One-step...Complete...	Complete	02/19/...	02/19/...	Comtech 2.2	0.hm7ir...	Production	
One-step...In Progress	In Progress	02/19/...		Comtech 2.2	0.hm7...	Test	
One-step...In Progress	In Progress	02/19/...		Comtech 2.2	0.hm7...	Test	
One-step...In Progress	In Progress	02/19/...		Comtech 2.2	0.hm7...	Test	
One-step...In Progress	In Progress	02/19/...		Comtech 2.2	0.hm7...	Test	

Process log messages show you the status of each instance of a Partner Agreement Manager process—whether it's in progress or completed, for example, and whether it generated any errors.

When a process instance finishes running, Partner Agreement Manager removes the In Progress message and updates the corresponding process log message to show that the instance has completed. If the instance generates an error, Partner Agreement Manager adds a message to the Error Processes folder.



The Error Processes folder contains a second set of entries for all completed process instances that generated error messages. As you fix the errors, you can mark them as resolved. When you resolve an error, Partner Agreement Manager removes it from the Error Processes folder, but not from the Process Logs folder.

---

**WARNING:** Deleting an item from the Error Processes folder also deletes it from the Process Logs folder as well, which might result in an incomplete audit trail. Therefore, it's a good idea to resolve errors instead of deleting them. See [Marking an error as resolved](#) on page 114.

---

## FINDING AN INSTANCE OF A PROCESS

Partner Agreement Manager assigns a unique ID to each process instance. If you wanted to locate a specific instance of a process, you might scan for its ID in the In Progress or Process Logs folders. Most users find it easier to think of process instances in terms of the information conveyed in their business objects. For example, a company typically differentiates between all of the purchase orders it sends or receives by looking at the PO number.

For this reason, Partner Agreement Manager lets you use the contents of a business object's key field value to locate the specific instance of a process. When you define a purchase order business object, for example, the logical choice for key field is the PO number. You can then locate a specific instance of a purchase order process by searching on the value in a PO number field. For information about designating a field as a key field, see the *Partner Agreement Manager User's Guide*.

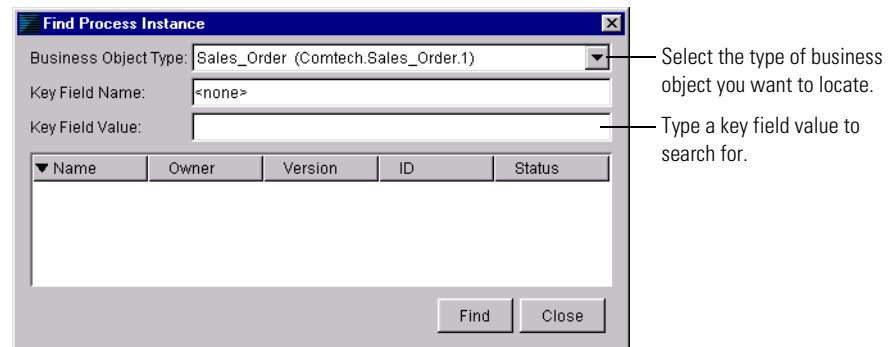
Based on the key field value you enter, Partner Agreement Manager searches through all instances of all processes and locates the process that contains the value you entered. Partner Agreement Manager then displays the process name, the owner, the version, the instance ID, and the instance status. You can also double-click an instance to examine it in the Process Audit window, where you can see any messages that it might have generated.

**NOTE:** If the key field value is not unique to a single instance, Partner Agreement Manager locates all instances that share a common key field value.

#### To find an instance of a process:

- 1 Click the Find Process Instance button in the Command toolbar.

The Find Process Instance dialog box appears.



- 2 Select the type of business object you want to locate.  
Partner Agreement Manager displays the name of the business object's key field.
- 3 Type the key field value that you want to locate.
- 4 Click Find.

Partner Agreement Manager displays the process instance that has a matching value, or, if none are found, Partner Agreement Manager displays a No Matches message.

Name	Owner	Version	ID	Status
GeneratePO	Comtech	1.0	0.hm7rpw16	Completed OK

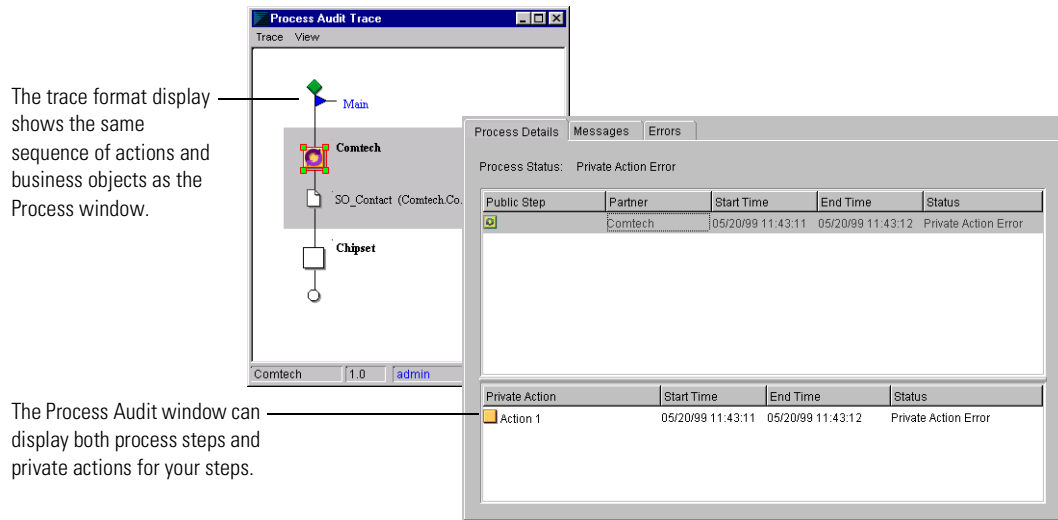
Partner Agreement Manager displays any matching process instances here. Double-click an instance to view it in the Process Audit window.

- 5 Double-click the process name to view it in the Process Audit window.

## VIEWING PROCESS INFORMATION

Partner Agreement Manager uses the Process Audit window to display information that lets you monitor a running instance of a process or audit a completed one. The Process Audit window displays three types of information: process details, business objects, and error messages.

You can also display audit information in a graphical format that lets you trace the flow of actions and business objects in each process instance. The trace view uses the same symbols and layout as the Public Process and Private Process windows.



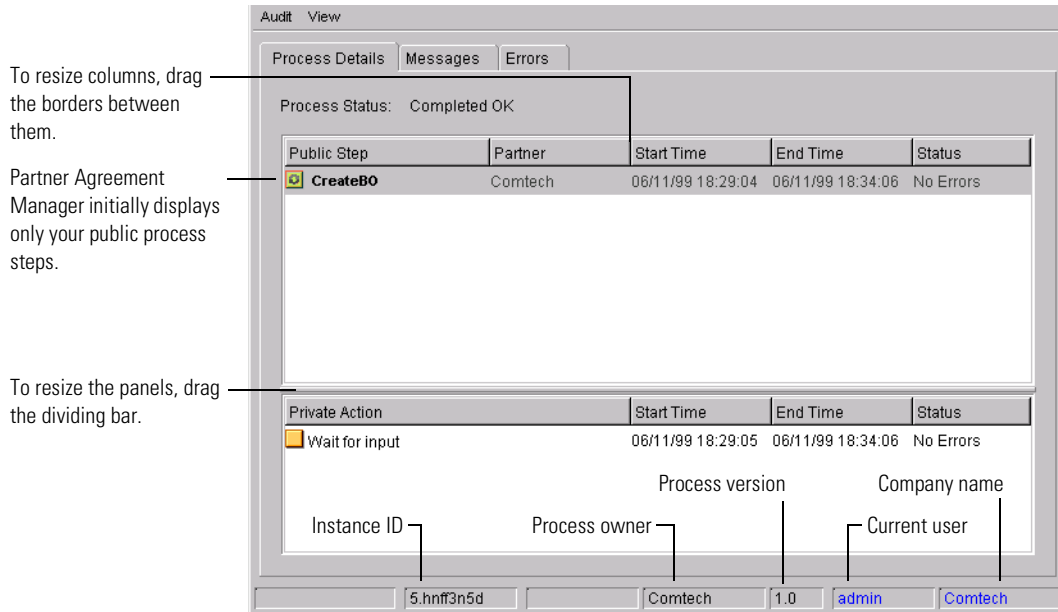
## USING THE PROCESS AUDIT WINDOW

Partner Agreement Manager uses the Process Audit window to audit a completed process or to display information like the current status of a running instance of a process. The Process Audit window displays three types of information: process details, business objects, and error messages.

- Process Details lists your steps in a public process and their private process actions. You can also add your partners' public process steps to the list (but not the partner's private process actions). In this view you can see the status of each step in a process.
- Messages include all business objects that have been sent so far in the process. Information includes the business object name and key element value, the sending and receiving companies, and the name of the path the business object is located on. In the business objects list, you can see which business objects have been exchanged.
- Errors are divided into three categories: overall process, public process steps, and private process actions. In the errors list, you can see any error messages that were generated at any level by the process.

**NOTE:** After you open an audit log, it is not refreshed. You must re-open it to view the ongoing process.

When you open the Process Audit window for a process instance, it displays only your steps in the public process.



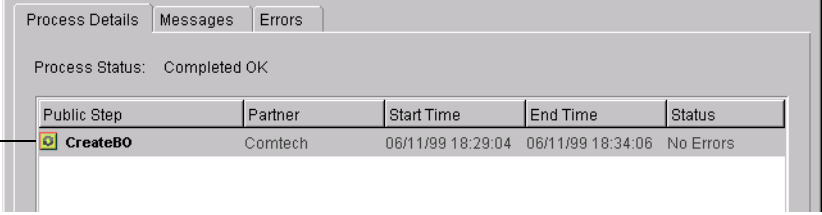
You can request and display public process information from your partners to get a more complete picture. You can also display the private process actions for any step that you own.

### To use the Process Audit window:


- 1 Open the Auditor module and select the process instance that you want to view.
  - To monitor a running process, open the In Progress Processes folder and double-click a process instance.
  - To audit a completed process, open the Process Logs folder, open a subfolder, and double-click the process instance.

The Process Audit window appears. It displays the status of your public process steps.

Only your public process steps appear initially.



The screenshot shows a window titled "Process Details" with tabs for "Messages" and "Errors". Below the tabs, it says "Process Status: Completed OK". A table lists public process steps:

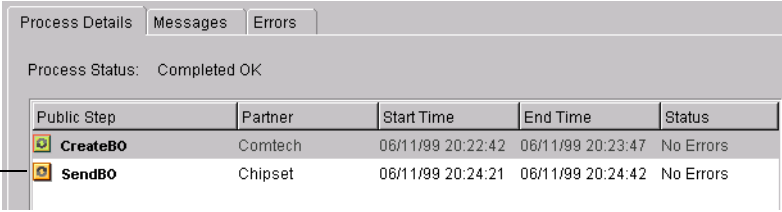
Public Step	Partner	Start Time	End Time	Status
 CreateBO	Comtech	06/11/99 18:29:04	06/11/99 18:34:06	No Errors

- 2 To display the status of your partners' public process steps, choose Get Remote Audit from the Audit menu.



**NOTE:** Choose Get Remote Audit after the process completes because there is a time-out period between remote audit requests. Requests issued before this time-out will wait until the time-out has expired.

Partner Agreement Manager polls your partners and adds entries for any executed public process steps to the display.

You can display public process steps for your partners.



The screenshot shows the same window as before, but with two rows in the table:

Public Step	Partner	Start Time	End Time	Status
 CreateBO	Comtech	06/11/99 20:22:42	06/11/99 20:23:47	No Errors
 SendBO	Chipset	06/11/99 20:24:21	06/11/99 20:24:42	No Errors

- 3 To view the private process status for one of your steps in the public process, select a step in the Public Step list.



Partner Agreement Manager displays the corresponding private process action status.

Process Details | Messages | Errors

Process Status: Completed OK

Public Step	Partner	Start Time	End Time	Status
CreateBO	Comtech	06/11/99 20:22:42	06/11/99 20:23:47	No Errors
SendBO	Chipset	06/11/99 20:24:21	06/11/99 20:24:42	No Errors

Private Action	Start Time	End Time	Status
Wait for input	06/11/99 20:22:43	06/11/99 20:23:46	No Errors
Action 2	06/11/99 20:23:46	06/11/99 20:23:46	No Errors

4 To view the business objects exchanged in the process, click the Messages tab.

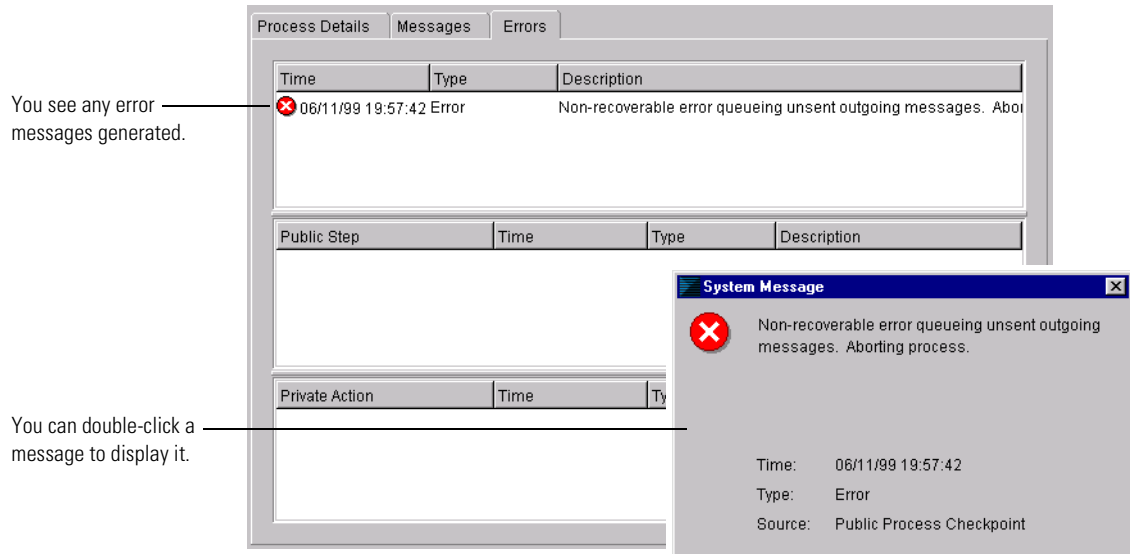
The Messages tab lists the business object name, the key element field value, the sending and receiving companies, the name of the path on which the business object is located, and the state of the message. It displays only the business objects you have sent or received. After you choose Get Remote Audit, the Messages tab displays all business objects that are part of the current public process instance.

Process Details | Messages | Errors

Name	Key Element	Sender	Receiver	Path	State
SO_Contact	Alfred L. Frahm	Comtech	Chipset	Main	Sent

5 To view any error messages generated by the process instance, click the Errors tab.

You can double-click a message to open it in its own window.



## MARKING AN ERROR AS RESOLVED

Any completed process instance that generates an error message appears in both the Completed and Error folders. It appears in both places to let you know that the instance ran to completion and that it generated an error.

If you want, you can mark errors as resolved, which allows Partner Agreement Manager to remove them from the Error folder. Resolved errors still appear in the Completed folder so that you always have a complete audit trail.

### To mark an error as resolved:

- 1 Open the Auditor module, open the Error Processes folder, open a subfolder, and select the process instance that you want to resolve.

The Process Audit window appears, displaying the error you selected.

- 2 Choose Error Status Resolved from the Audit menu.

A check mark appears to the left of the command when it's selected.

- 3 Close the Process Audit window.

Partner Agreement Manager updates the contents of the Error Processes folder and removes the resolved error. The resolved error still appears in the Process Logs folder.

**TIP:** To change the status of a resolved error back to unresolved (and to display it in the Error Processes folder again), open the error from the Process Logs folder and choose Error Status Resolved from the Audit menu again (the check mark disappears).

## USING THE TRACE WINDOW

The Trace window displays process status in a graphical format that looks exactly like the public process. It uses the same icons for steps and business objects and the same path as the public process. Color icons let you immediately see how much of a process has been completed. You can also drill down from the public process level trace to view a trace of your underlying private processes.

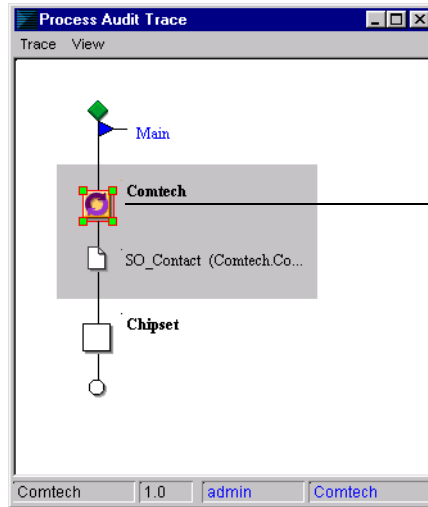
### To use the Trace window:

- 1 Open the public process instance that you want to view in the Process Audit window.
  - To get a snapshot of a running process, open the In Progress folder and double-click a process.
  - To audit a completed process, open the Completed folder or the Error folder, open one of the subfolders, and double-click the process.
- 2 Choose Trace View from the View menu.

The Process Audit Trace window appears. Color icons show how far the process has run. Icons for completed nodes and business objects that have been sent are in color. Otherwise they are white. If the process contains loops, steps appear in color after they have been executed once.

**NOTE:** Partner steps are not in color until you get a remote audit.

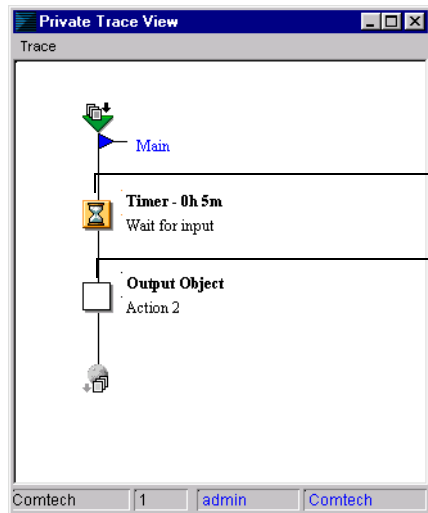
**TIP:** The Trace window skips the partner's node unless you choose Get Remote Audit from the Audit menu.



Color icons show how far the process has run. The icons for completed nodes and business objects that have been sent are in color. Otherwise, they are white.

- 3 To display the private process for any step you own in a trace window, select the step in the Process Audit Trace window and choose Trace View from the View menu.

The Private Trace View appears. The icons for completed actions are in color. Otherwise, they are white.



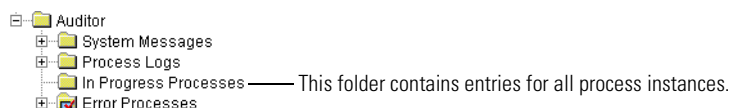
Color icons show how far the process has run.

White icons show an action that was not executed.

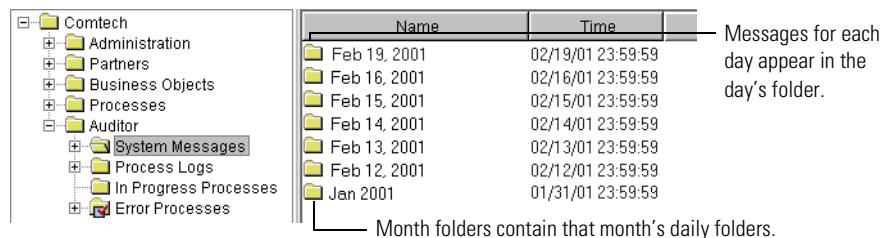
- 4 Choose Exit from the Trace menu to close the Private Trace View or Process Audit Trace window.

## ARCHIVING AND RESTORING PROCESS LOGS

Each time you run a process, Partner Agreement Manager creates a new instance of the process and assigns it a unique ID number. When the instance terminates, it appears in the Auditor's Process Logs folder. If the instance generates any errors, it also appears in the Error Processes folder.



Within each Auditor folder, Partner Agreement Manager organizes each day's messages into a separate subfolder. At the end of the month, it creates a folder to hold that month's daily folders. Similarly, at the end of the year it creates a folder that holds that year's monthly folders.



## ARCHIVING PROCESS LOGS

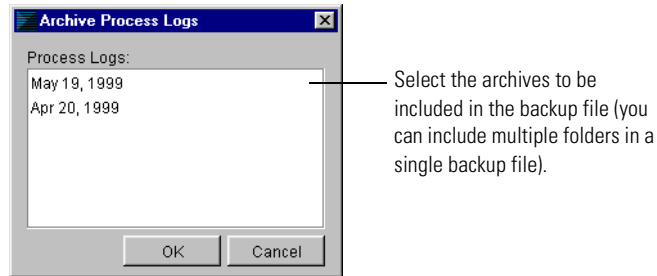
To help you manage the process instances generated by your processes, Partner Agreement Manager lets you archive daily Process Log folders. You can also schedule a backup for a later date and time and set Partner Agreement Manager to delete system messages at the same time. Partner Agreement Manager stores the archived logs in a backup file, which you can later use to restore the original archive folder.

**NOTE:** You can only archive and restore a single process log once. After a process log has been restored it can't be archived again.

### To archive process logs:

- 1 In the Process Manager window, choose Archive Process Logs from the Tools menu.

The Archive Process Logs dialog box appears. The Process Logs list shows the folders for all days prior to today.



- 2 Select the folders to be archived.  
Control-click to select multiple folders.
- 3 Click OK.

**TIP:** Archive files are located in the `Partner\Data\archive` directory on the Process Server computer. You might want to back these files up to tape and delete them to free disk space.

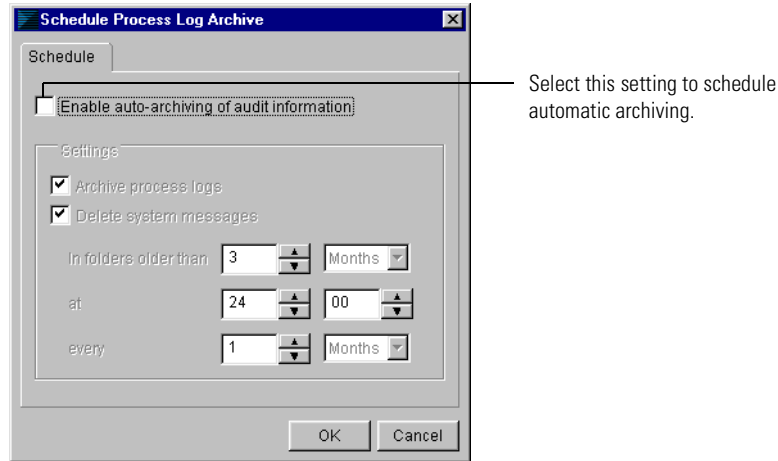
## SCHEDULING AUTOMATIC ARCHIVES

You can set Partner Agreement Manager to archive process logs or delete system messages on a regular basis. You can specify the age of the logs or system messages to be archived, the time that the archiving takes place, and the interval between archives. The more processes you run, the more often you will probably want to archive the process logs.

### To schedule automatic archives:

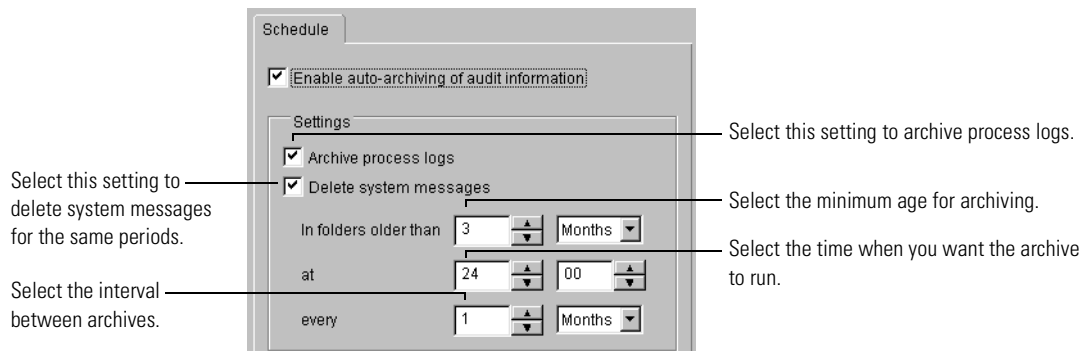
- 1 In the Process Manager window, choose Archive Scheduler from the Tools menu.

The Schedule Process Log Archive dialog box appears.



- 2 Turn on the Enable Auto-Archiving of Audit Information setting to allow Partner Agreement Manager to archive.

The other settings in the Schedule Process Log Archive dialog box become available.



- 3 Turn on settings for archiving process logs, deleting system messages, or both.

If you select both archiving and deleting, the timing settings you select apply to both actions.

- 4 Select the minimum age for process logs to be archived or system messages to be deleted.

Partner Agreement Manager will archive any process logs or delete systems messages that are older than the age you specify.

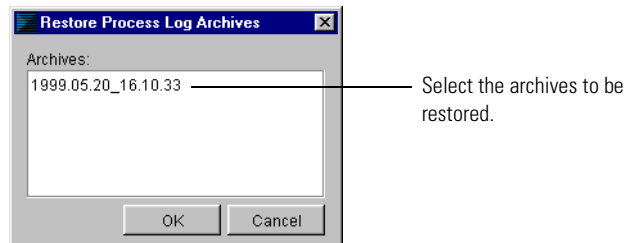
- 5 Select the time when you want the archiving to take place.  
Partner Agreement Manager uses a 24-hour clock for this setting.
- 6 Select the interval between archives.  
You can set the interval to be a number of days or months.
- 7 Click OK.

## RESTORING ARCHIVED PROCESS LOGS

When you archive process logs, Partner Agreement Manager stores the archived process instances in a backup file. You can use the backup to restore the original process log folders.

### To restore archived process logs:

- 1 In the Process Manager window, choose Restore Process Logs from the Tools menu.  
The Restore Process Logs dialog box appears. The Archives list shows all archived folders.



- 2 Select the folders to be restored.  
Control-click to select multiple folders.
- 3 Click OK.

**NOTE:** After you have restored an archived process log, you can't archive it again.

## EXPORTING PROCESS LOGS

With Partner Agreement Manager, you can export any process logs from today's folder or a single process log from any folder you want. You can then import the exported process logs if you want.



Exporting a process log creates an XML file that contains any combination of log entries from today's folder.

### To export process logs from today's folder:

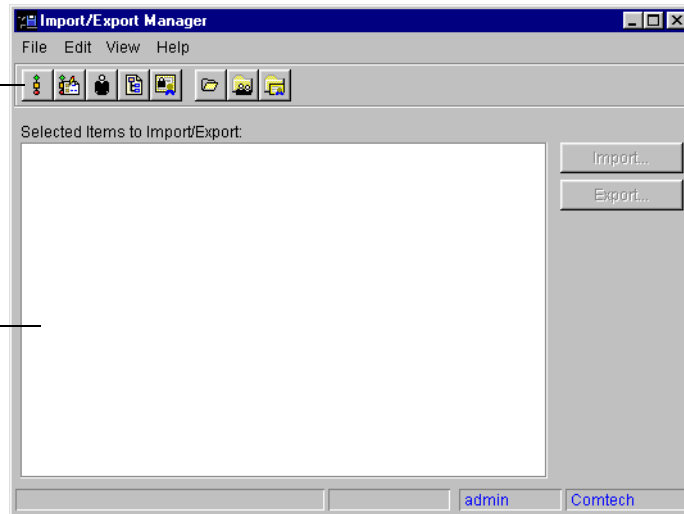


- 1 Click the Import/Export Manager button in the Command toolbar.

The Import/Export Manager appears.

Click to select a process to be exported.

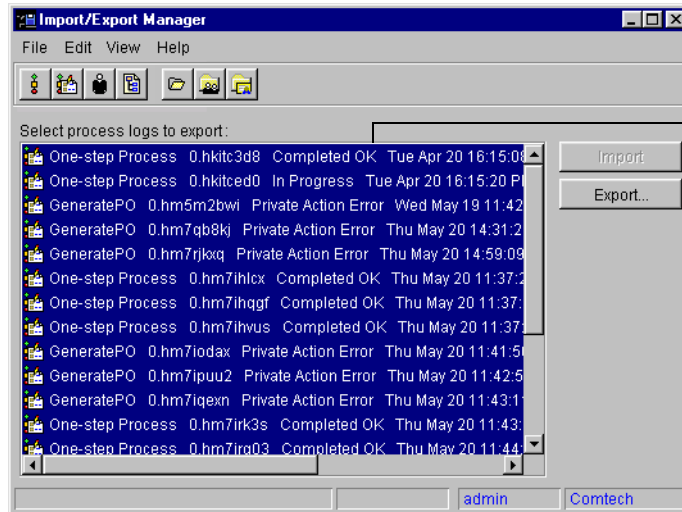
This area shows a list of the items in a pending import or export action.



- 2 Click the Select Process Logs to Export button in the Command toolbar.

You can also choose Select for Export from the File menu, and then choose Process Log from the menu that appears.

The Import/Export Manager lists the process log entries for today.



This list shows all available process log entries.

- 3 Select the items that you want to export and click Export.

You can also choose Export from the File menu. The Export to File dialog box appears.

- 4 Type a name, and then select the location where you want to save the export file.

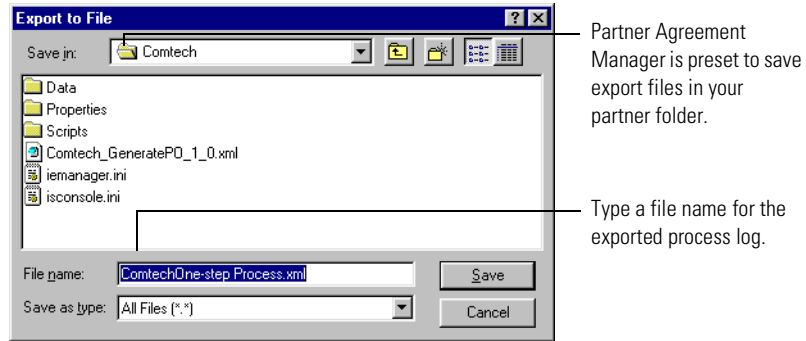
Partner Agreement Manager exports the items you selected and alerts you when the export is complete.

- 5 Close the Import/Export Manager.

#### To export a single process log entry:

- 1 In the Import/Export Manager, right-click the process log entry you want to export, and choose Export from the menu that appears.

The Export to File dialog box appears.




- 2 Type a name, and then select the location where you want to save the export file. Click Save.

Partner Agreement Manager exports the items you selected and alerts you when the export is complete.

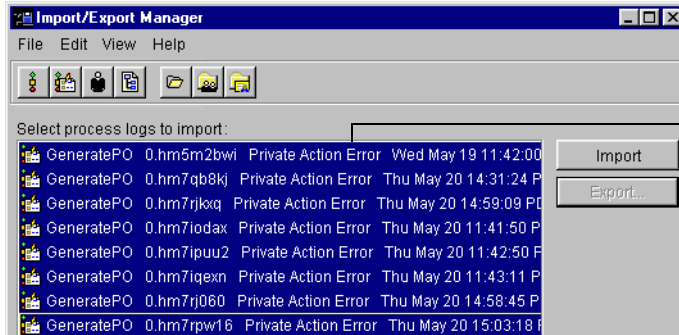
## IMPORTING PROCESS LOGS

When you import a process log, you can select the entries you want to import. For example, the import file might contain all of the log entries for a single day, but you can choose to import only those that produced error messages.

### To import processes:

- 1  Click the Import/Export Manager button in the Command toolbar.  
The Import/Export Manager appears.
- 2 Choose Open for Import from the File menu.  
The Open Exported File dialog box appears. You can select any export (XML) file.
- 3 Select the file you want to import and click Open.

The Import/Export Manager shows all available log entries in the file.



This list shows all available log entries you can import.

- 4 Select the entries you want to import, and then choose Import from the File menu or click Import.  
Partner Agreement Manager imports the items you selected and alerts you when the import is complete.
- 5 Close the Import/Export Manager.

## VIEWING SYSTEM MESSAGES

System messages, which provide information about Partner Agreement Manager events that are not related to the running of processes, are divided into three categories: Info, Warning and Error.

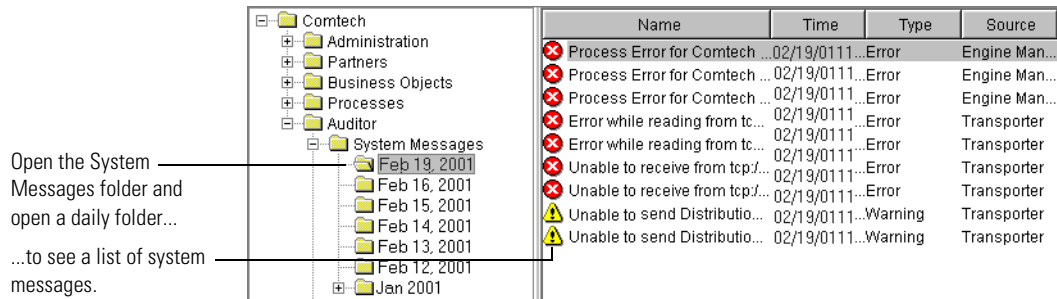
- Info messages provide information about status of a system function.
- Warning messages indicate unexpected system events that do not cause system failures.
- Error messages indicate the failure of a system function.

You can view system messages directly in the Process Manager window, or you can select a message and open it to see more detail.

**To view system messages:**

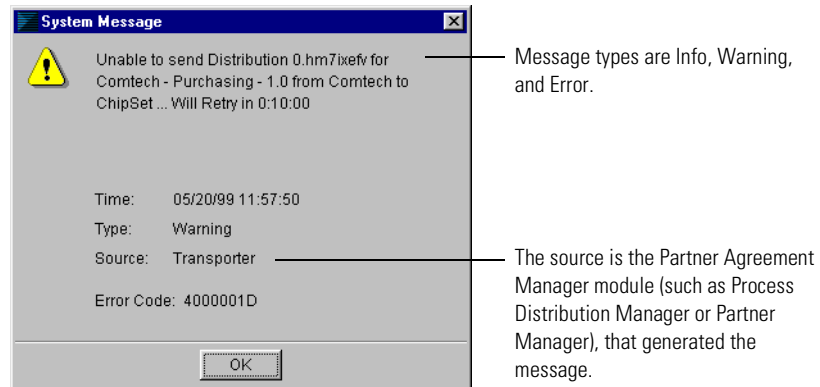
- 1 Open the Auditor module, open the System Messages folder, and open an archive folder by date.

The right panel of the Process Manager window displays all system messages. For each system message, Partner Agreement Manager displays the date and time the message was generated, the type of message, and the source (the Partner Agreement Manager module that generated the message).



**2** Double-click the message that you want to view.

The System Message dialog box appears. It shows the time that the message was issued, the type of message, and the source (the Partner Agreement Manager module that generated it). The full message text appears in the Description box.



**3** Click OK to close the System Message dialog box.

## DELETING SYSTEM AUDIT INFORMATION

You can delete archive folders of system error messages that you no longer need to view.

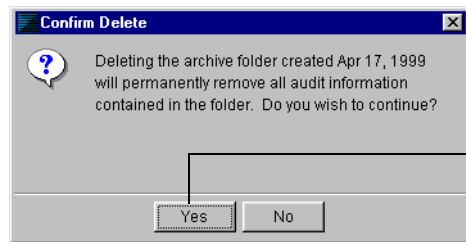
### To delete system audit information:

- 1 Open the Auditor's System Messages folder. Right-click the daily folder you want to delete and choose Delete from the menu that appears.



You can also select a folder and then press the Delete key or click the Delete button in the Command toolbar. You can't delete today's folder, and you can't delete individual system messages.

A confirmation message appears.



Confirm that you want to delete the archive folder.

- 2 Click Yes to confirm the deletion.

## EXTRACTING MESSAGE INFORMATION

With Partner Agreement Manager, you can extract both the contents of a message and proof that messages have been sent and received. Partner Agreement Manager extracts message contents to a text file. The proof of sending and receiving is in the form of an RSA-PKCS 7 file.

---

**IMPORTANT:** The non-repudiation settings for the process must be turned on for this information to be available. In addition, auditing must be enabled for the business object. See the *Partner Agreement Manager User's Guide*.

---

Although Partner Agreement Manager is preset to audit all business objects, you can disable auditing for individual business object types.

When auditing of the business objects used in a process is enabled, you can extract the contents of each message you send or receive in instances of that process.

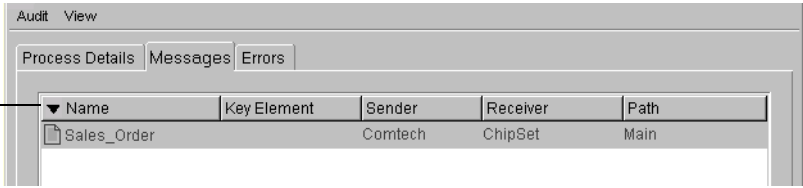
When non-repudiation and business object auditing are both enabled, you can extract non-repudiation information. This means that if you sent the message, you can also extract proof that the message was received. If you received the message, you can extract proof of the identity of the sender.

### To extract business object non-repudiation information:

- 1 Open the Auditor folder in the Process Manager window, open the Process Logs folder, and navigate to the process instance for which you want information.
- 2 Open the process instance and click the Messages tab.

The Messages tab shows all messages sent as part of this process.

This list shows all messages created in this process instance.



Name	Key Element	Sender	Receiver	Path
Sales_Order		Comtech	ChipSet	Main

- 3 Right-click the message for which you want information and choose a command from the menu that appears.
  - Choose Extract Content to create a text file that contains the message contents.
  - Choose Extract Receipt if you are the partner who sent the message. The resulting file contains electronic proof that the message was received by the designated partner.
  - Choose Extract Origin if you are the partner who received the message. The resulting file contains electronic proof that the message was sent by the originating partner.
- 4 Type a name and save the file that contains the extracted information.





# A

## USING LDAP WITH PARTNER AGREEMENT MANAGER

Partner Agreement Manager now supports accessing user and partner information from an LDAP (Lightweight Directory Access Protocol) directory. Read this chapter for information about using LDAP with Partner Agreement Manager.

This appendix includes these sections:

- *About LDAP* on page 130.
- *Installing and configuring Partner Agreement Manager for LDAP* on page 132.
- *Mapping Partner Agreement Manager information to LDAP* on page 133.
- *Setting up LDAP support after you install Partner Agreement Manager* on page 135.
- *Using Partner Agreement Manager with LDAP* on page 137.

## ABOUT LDAP

LDAP provides a standard method for accessing information from a central directory. A common use for LDAP is user authentication. After a user is set up in the LDAP directory, that user can log in to any application that supports the LDAP protocol with the same user name and password.

Partner Agreement Manager now includes support for LDAP. With LDAP support in Partner Agreement Manager, you can do the following tasks with an external LDAP directory:

- authenticate users.
- retrieve user information.
- store and retrieve partner information.

You can think of these tasks as grouped into two categories—operations related to user information (the most common use for LDAP) and operations related to partner information.

Because users should administer their account information from a central place, the following tasks are disabled in Partner Agreement Manager with LDAP support:

- creating new users.
- changing the properties of a user (except for permissions).
- deleting a user.

## USER INFORMATION OVERVIEW

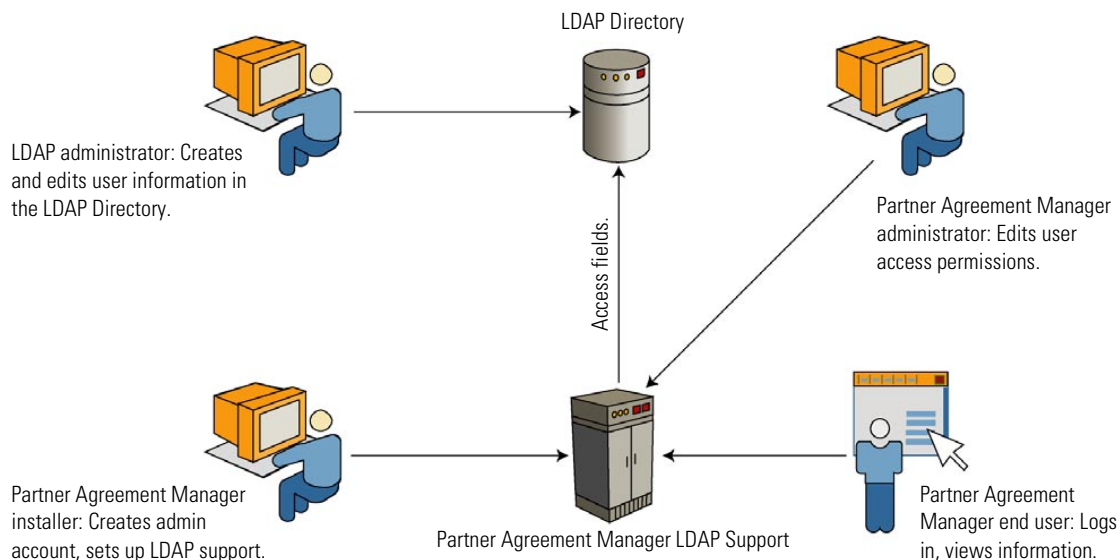
The following list includes the users of the LDAP feature in Partner Agreement Manager and this documentation:

- The *LDAP administrator* creates and modifies user information in the LDAP directory.
- The Partner Agreement Manager *installer* installs the Partner Agreement Manager products, creates the Partner Agreement Manager admin user account, and sets up LDAP support.

- The Partner Agreement Manager *administrator* (admin) configures other users' permissions in Partner Agreement Manager. When using Partner Agreement Manager with LDAP support, the admin is no longer permitted to create new users in Partner Agreement Manager. This task can be done only by the LDAP administrator in the LDAP directory.
- Partner Agreement Manager *end users*, who are any users with an LDAP user name and password. Although these users can log in to Partner Agreement Manager, they cannot access or modify any information until the Partner Agreement Manager admin grants them permission to do so.

The first three users must communicate closely to set up and use LDAP support in Partner Agreement Manager. Among these users, there is likely to be some overlap. That is, the Partner Agreement Manager installer and administrator might be the same person, or the LDAP administrator might also serve as the Partner Agreement Manager administrator.

The following illustration gives a picture of the different users and the tasks they perform.



## BEFORE YOU INSTALL PARTNER AGREEMENT MANAGER

Partner Agreement Manager requires an LDAP user account created specifically for it. This user account must include sufficient permissions for Partner Agreement Manager to read the user information it needs and sufficient permissions to read and write the partner information that it needs.

Before installation, the LDAP administrator and the Partner Agreement Manager installer must agree on these values:

- the DN (distinguished name) of the Partner Agreement Manager user (the DN is like a path; for example, `uid=PAM,ou=Special Users,o=Comtech.com`).
- the password for the Partner Agreement Manager user.
- the LDAP directory to connect to (for example, `ldap://ldap.comtech.com`).

The LDAP administrator creates the Partner Agreement Manager user account and gives the Partner Agreement Manager installer the DN and password of this account, as well as the LDAP directory URL. These values are used in the installation process, as described in the next section.

**NOTE:** If the Partner Agreement Manager configuration for LDAP isn't completed before Partner Agreement Manager is installed, you can create an LDAP user account for Partner Agreement Manager later in the LDAP directory. At that time, you can configure Partner Agreement Manager to use the LDAP user name and password and edit the `Partner.properties` file to support users and partners, as necessary. See *Setting up LDAP support after you install Partner Agreement Manager* on page 135.

## INSTALLING AND CONFIGURING PARTNER AGREEMENT MANAGER FOR LDAP

The Partner Agreement Manager installer:

- creates the Partner Agreement Manager admin user (for more information, see *Setting up the Admin user* on page 45).
- installs the Partner Agreement Manager Process Server, the Process Manager, and the Adapter Server (for more information, see the *Partner Agreement Manager Installation Guide*).

- configures Partner Agreement Manager to use LDAP by:
  - setting up the LDAP server and user information (during installation, as described later in this section).
  - mapping Partner Agreement Manager objects to LDAP objects (see *Mapping Partner Agreement Manager information to LDAP*, next).

During installation, the Partner Agreement Manager Installer wizard lets you choose whether you want to use LDAP for authorizing users, storing partner information, or both. If you choose one or both options, you must provide the LDAP provider host name and port number, as well as the user DN and password of the special account set up by the LDAP administrator.

## MAPPING PARTNER AGREEMENT MANAGER INFORMATION TO LDAP

LDAP support in Partner Agreement Manager requires mapping Partner Agreement Manager's objects to corresponding LDAP objects. For each object type, the mapping must match each Partner Agreement Manager field to a corresponding LDAP attribute.

The LDAP feature uses JNDI (Java Naming and Directory Interface) to access the LDAP directory indirectly. It doesn't change the values returned from the LDAP directory, but maps values between the Partner Agreement Manager schema and the LDAP directory schema as it retrieves the values.

Map these objects and fields in the following properties files:

- For mapping user information, edit  
PAM\CRStation\managers\security\UserLDAPMapper.properties.
- For mapping partner information, edit  
PAM\com\IBM\partner\mgr\PartnerLDAPMapper.properties.

The mapping files include comments on how the mapping works; that is, they are self-documenting. Before you begin editing the files, be sure you have a detailed understanding of the LDAP schema you're mapping.

## MAPPING USER INFORMATION

In most cases, the only change you need to make to the `UserLDAPMapper.properties` file is to indicate the correct search root and search filter for user objects, according to the layout of your LDAP directory. The file that ships with Partner Agreement Manager maps correctly for the `inetOrgPerson` schema, which is the standard user schema in LDAP. If you're using another schema for storing user information, follow the instructions in the file to modify the mapping.

The following examples show how to specify the search root, search filter, and object class for mapping Partner Agreement Manager field names to their counterparts in LDAP:

```
ldap.user.search_root="ou=People, o=Comtech.com"  
ldap.user.search_filter="(&(criterion) (criterion))"  
ldap.user.object_class=inetOrgPerson
```

The field names are `user_id`, `full_name`, `email`, `email_to_fax`, `email_to_pager`, and `phone`. Enter one line in the properties file for each Partner Agreement Manager field you want mapped, including the corresponding attribute in the LDAP directory. For example:

```
ldap.user.fields.user_id=uid  
ldap.user.fields.full_name=cn  
ldap.user.fields.email=mail  
ldap.user.fields.phone=telephoneNumber
```

## MAPPING PARTNER INFORMATION

Because partner information is more structured than user information, mapping partner information is more complex than mapping user information. For best results, we recommend using the Partner Agreement Manager partner LDAP schema:

(`PAM\com\IBM\partner\mgr\schema\AllianceSchema.ldif`).

### To enable Partner Agreement Manager to store partner information in LDAP:

- 1 Load the partner LDAP schema into the LDAP directory.
- 2 Create a new Group or Organizational Unit in the LDAP directory tree to hold the partner information.

- 3 Grant the Partner Agreement Manager LDAP account write permission for the new Group or Organizational Unit.
- 4 Edit `PartnerLDAPMapper.properties` to point each object class's search root to that new Group or Organizational Unit.

## SETTING UP LDAP SUPPORT AFTER YOU INSTALL PARTNER AGREEMENT MANAGER

To set up LDAP support in Partner Agreement Manager *after* you install Partner Agreement Manager, you need to:

- set up the LDAP user account for Partner Agreement Manager (see [Before you install Partner Agreement Manager](#) on page 132).
- edit `Partner.properties` (see [Configuring the Partner.properties file](#), next).
- store the LDAP password in Partner Agreement Manager's MasterStore library (see [Storing the LDAP password in the MasterStore](#) on page 136).
- map user and partner information as necessary (see [Mapping user information](#) on page 134).

---

**IMPORTANT:** Be sure to check your user information in Partner Agreement Manager after you set up support for LDAP.

---

### CONFIGURING THE PARTNER.PROPERTIES FILE

To configure LDAP support after an installation that didn't originally include LDAP support, the Partner Agreement Manager installer must edit the `Partner.properties` file (located in the `\Partners\Partner $nnn$ \Properties` folder, where  $nnn$  is your Partner Agreement Manager partner number). Use a standard text editor and add the required settings in a group at the end of the `Partner.properties` file.

For example, type the following lines in `Partner.properties` to specify the location of the LDAP server and the Partner Agreement Manager user account:

```
# LDAP Configuration
ldap.provider_url=ldap://<ldap_host>/
ldap.account_dn=<PAM_account_DN>
```

where *<ldap\_host>* is the name of the computer hosting the LDAP directory, and *<PAM\_account\_DN>* is the DN of the account set up for Partner Agreement Manager by the LDAP administrator.

The property settings are described in the following table.

To	Type this in the Partner.properties file
Get user information from the LDAP directory	<code>ldap.enable_user=true</code>
Get partner information from the LDAP directory	<code>ldap.enable_partner=true</code>
Specify the location of the LDAP server	The URL for the LDAP server; for example, <code>ldap.provider_url=ldap://ldap.comtech.com/</code>
Specify the DN of the Partner Agreement Manager user account in LDAP	For example, <code>ldap.account_dn="uid=pam, ou=Special Users, o=Comtech.com"</code>  <b>NOTE:</b> The password for the Partner Agreement Manager user account is stored in the Partner Agreement Manager MasterStore library under the key <code>ldap_user_dn</code> .
Set a time limit (in milliseconds) for the caching information from LDAP (if information isn't retrieved before the specified time limit, the information in the cache will be refreshed)	<code>ldap.cache_max_age=xxxxx</code> (for example, if <code>xxxxx=60000</code> , the time limit is one minute)
Set a time-out (in milliseconds) for the LDAP feature when it is waiting for the LDAP server to respond	<code>ldap.server_timeout=xxxxx</code> (for example, if <code>xxxxx=15000</code> , the time-out value is 15 seconds)

## STORING THE LDAP PASSWORD IN THE MASTERSTORE

The batch utility `initLDAP` stores the LDAP password in the Partner Agreement Manager MasterStore library. `initLDAP` is located in the `\PAM\Scripts` directory, but you must run it from your partner directory.



## To store the LDAP password for Partner Agreement Manager in the MasterStore:

- 1 Open a Partner Agreement Manager Diagnostic Shell.
- 2 Run the `initLDAP` batch utility, passing it the LDAP password.

For example:

```
initLDAP <password>
```

## USING PARTNER AGREEMENT MANAGER WITH LDAP

Users log in to Partner Agreement Manager with the LDAP feature in much the same way they do without LDAP. The end user logs in to Partner Agreement Manager with a user name and password—in this case, an LDAP user name and password. Behind the scenes, the Partner Agreement Manager authenticates the user through the LDAP server, and Partner Agreement Manager opens. The end user works in Partner Agreement Manager the same way as before.

### SETTING USER PERMISSIONS

When using the LDAP feature, LDAP users don't have permission to access or modify information in Partner Agreement Manager until the Partner Agreement Manager administrator grants them permissions. In other words, although any LDAP users can log in to Partner Agreement Manager, the Partner Agreement Manager admin must first set their permissions for them to be able to do anything useful.

Here are the steps required to set user permissions:

- log in to Partner Agreement Manager with the Admin user account.
- set access permissions for each LDAP user.

---

**IMPORTANT:** Remember that when using the LDAP feature, the Partner Agreement Manager administrator can set user access permissions but not create new users. Creating new users is possible only in the LDAP directory by the LDAP administrator.

---



## USING THE PAM PROXY SERVER

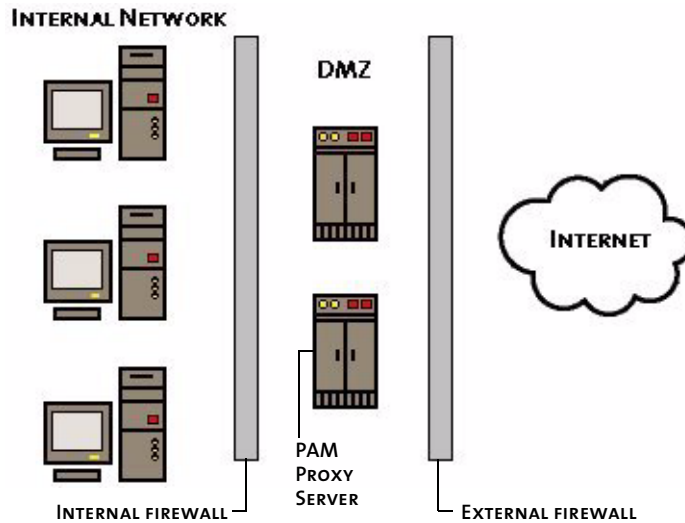
Read this chapter for information about using the PAM Proxy Server. The Proxy Server provides connectivity between Process Servers across firewalls without compromising network security policies.

This appendix includes these sections:

- *About the PAM Proxy Server* on page 140.
- *About inbound and outbound messages* on page 141.
- *Configuring the PAM Proxy Server* on page 142.
- *Sample Configuration File* on page 146.
- *Compiling the PAM Proxy Server* on page 148.
- *Running the Proxy Server as an NT service* on page 150.
- *Maintaining the PAM Proxy Server* on page 150.

## ABOUT THE PAM PROXY SERVER

The PAM Proxy Server is software that resides in the DMZ between an internal and an external firewall. The Proxy Server passes messages from a local Process Server to remote Process Servers outside the company, and passes inbound messages from a remote Process Server to the local Process Server.



The PAM Proxy Server functions as a mediator for connections between the internal system and external systems—its behavior is similar to that of a SOCKS server.

In addition to providing a virtual connection between Process Servers (through connection splicing), the PAM Proxy Server manages access control based on source and destination host addresses.

## ABOUT INBOUND AND OUTBOUND MESSAGES

In handling outbound and inbound messages, the PAM Proxy Server performs access control checks based on the information contained in its configuration file. If the access control checks succeed, the PAM Proxy Server establishes the appropriate connections and forwards the messages with no additional checks. Specifically:

- For outbound messages, the access control check is performed on the source address, which is contained in the Internet connection request, and on the destination address, which is contained in the message header. If the access control check succeeds, the PAM Proxy Server establishes a TCP connection to the destination address and forwards the entire message with no additional checks.
- For inbound messages, the access control checks are performed on the source, which is contained in the TCP connection request. If the access control check succeeds, the PAM Proxy Server forwards the entire message to the derived destination address with no additional checks.

## REQUIREMENTS

The PAM Proxy Server does not do any processing or inspection of data—it simply routes data from one socket to another if it is authenticated by the access control list. Because it does not do any processing, the hardware requirements are minimal. The proxy logs debugging information to a file on the hard disk, so you need to size the amount of disk space appropriately.

For example, 20,000 processes (independent of business object size) generate about 20 MB of debugging log information. Because you must shut the PAM Proxy Server down to rotate the log file, be sure you have enough disk space when you debug your network. The PAM Proxy Server code itself requires less than 1 MB of disk space.

In addition to the disk space, the PAM Proxy Server requires:

- 32 MB of memory for Windows
- 128 MB for UNIX
- any Pentium-class CPU for Windows
- any sparc class CPU for UNIX

## CONFIGURING THE PAM PROXY SERVER

You can configure the PAM Proxy Server to operate in either active or passive mode:

- In active mode, the PAM Proxy Server accepts a new connection from a remote Process Server and then establishes a new connection to the Process Server on the internal network.
- In passive mode, the PAM Proxy Server waits for the Process Server on the internal network to open a connection to the proxy's "reverse channel" port. The PAM Proxy Server accepts connections from a remote Process Server only when a connection exists between itself and the local Process Server.

**NOTE:** If your network security policy does not allow DMZ computers to initiate connections to the internal network, you must use the passive mode configuration.

For information on how to configure Partner Agreement Manager to use a proxy server, see *Setting up service types* on page 26 and *Setting up a listener service* on page 29.

### EXAMPLE NETWORK CONFIGURATION

This example of a PAM Proxy Server implementation is based on the following network configuration:

- An internal network that contains protected enterprise applications.
- A DMZ, which contains computers that have restricted access to the internal network, and that have restricted access to the external network.
- An external network /Internet that provides unrestricted access to the rest of the Internet.

This example is based on this TCP configuration:

MYCOMPANY.COM      Your company

---

MYPARTNER.COM      Your business partner

---

PAM.MYCOMPANY.COM

The Process Server on your internal network. It uses a random port above 1024 for outbound TCP connections, and it listens on a configurable port (10001 in this example) for TCP connections.

---

---

#### **PAM-PROXY.MYCOMPANY.COM**

The computer that hosts the PAM Proxy Server in the DMZ. It listens for outbound messages on a configurable port (8471 in this example), and it supports connections only from **PAM.mycompany.com**. It listens for inbound messages on a second configurable port (8481 in this example), and it only allows connections from computers specified by an **EXTERNAL=** directive in the proxy configuration file.

---

#### **INTERNAL-DMZ-FIREWALL.MYCOMPANY.COM**

The firewall that restricts the data flow between the internal network and the DMZ. It is configured for these rules:

---

In active mode:

Allow PAM.mycompany.com:(>1024) —> PAM-proxy.mycompany.com:8471

Allow PAM-proxy.mycompany.com:(>1024) —> PAM.mycompany.com:10001

---

In passive mode:

Allow PAM.mycompany.com:(>1024) —>PAM-proxy.mycompany.com:8471

Allow PAM.mycompany.com:(>1024) —>PAM-proxy.mycompany.com:10001

---

## DMZ-EXTERNAL-FIREWALL.MYCOMPANY.COM

The firewall that restricts the data flow between the DMZ and the Internet. It is configured for these rules:

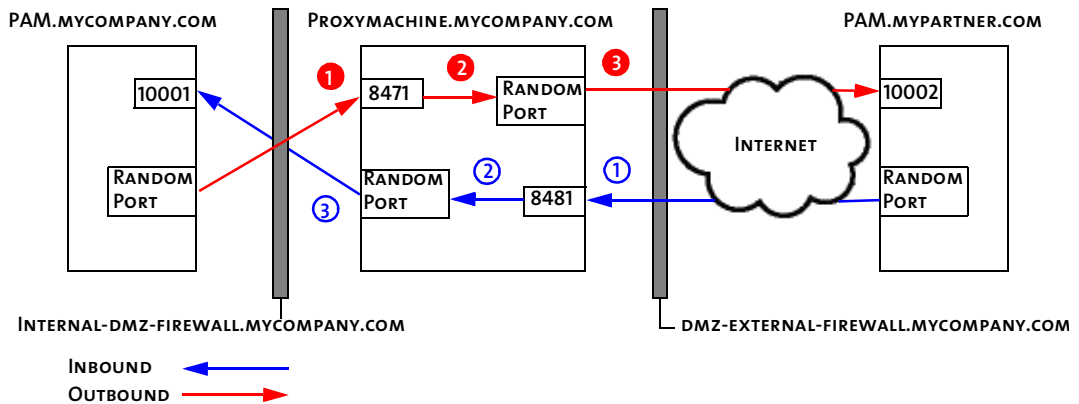
Allow connections from PAM-proxy.mycompany.com to an unrestricted set of hosts on the Internet. Alternatively, the connections allowed can be limited to just the set of known remote Process Servers.

Allow connections from an unrestricted set of hosts on the Internet to PAM-proxy.mycompany.com:8481. Preferably, the connections allowed can be limited to just the set of known remote Process Servers.

## PAM.MYPARTNER.COM

Your business partner's Process Server. It doesn't matter whether this is an actual Process Server, or the PAM Proxy Server running in mypartner.com's DMZ. If it is the proxy, it forwards the message to mypartner.com's internal Process Server.

## ACTIVE MODE PROXY EXAMPLE



The PAM Proxy Server performs these steps for outbound connections:

- 1 The PAM Proxy Server ensures that the source IP address of the incoming connection matches one of the IP addresses defined on the right side of the proxy directives in the *proxy* section of the configuration file.
- 2 The PAM Proxy Server ensures that the final destination requested in the message body matches one of the listed IP/port combinations defined in the *external* section of the configuration file.
- 3 If the message passes the first two tests, the PAM Proxy Server opens a new connection or retrieves one from the connection cache if one exists. The data in the message is transparently proxied over to the requested destination.

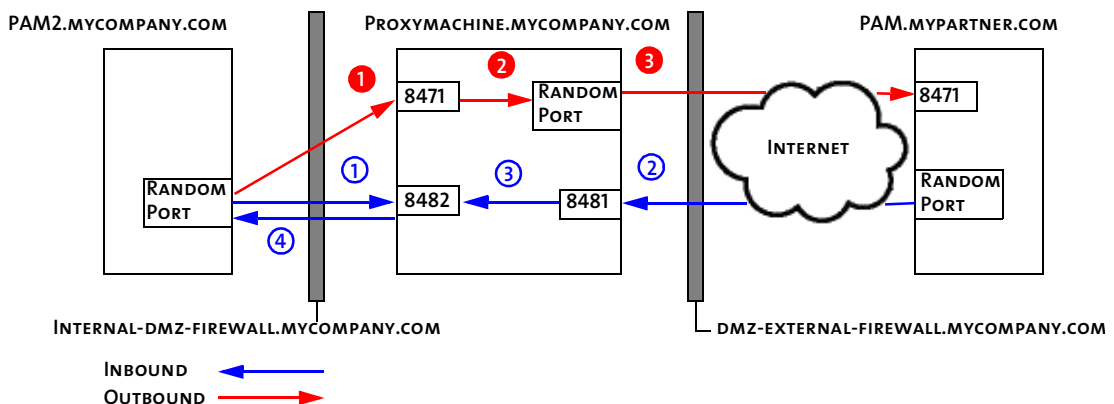


The PAM Proxy Server performs these steps for inbound connections:

- ① When a message from the remote host arrives, the PAM Proxy Server checks the source address against the known valid source IP addresses listed in the *external* section of the configuration file.
- ② Data is automatically transferred to the inbound port via a memory buffer.
- ③ The PAM Proxy Server transparently proxies all the bytes of the message to the host and IP address specified on the right side of a *proxy* directive in the configuration file. The directive used is determined by the port on which the request arrives. (If the request arrives on port 8481, it is proxied to PAM.mycompany.com:10001.)

### PASSIVE MODE PROXY EXAMPLE

In passive mode, the outbound flow is the same as in active mode. For the inbound flow, there is one additional step.



The PAM Proxy Server performs these steps for outbound connections:

- ① The PAM Proxy Server ensures that the source IP address of the incoming connection matches one of the IP addresses defined on the right side of the proxy directives in the *proxy* section of the configuration file.
- ② The PAM Proxy Server ensures that the final destination requested in the message body matches one of the listed IP/port combinations defined in the *external* section of the configuration file.
- ③ If the message passes the first two tests, the PAM Proxy Server opens a new connection or retrieves one from the connection cache if one exists. The data in the message is transparently proxied over to the requested destination.

The PAM Proxy Server performs these steps for inbound connections:

- ① The internal Partner Agreement Manager installation (PAM2.mycompany.com) connects to the proxy pickup port. The pickup port enables the internal Partner Agreement Manager installation to pick up messages from the proxy, instead of across the DMZ.  
Only the host specified on the right side of the *passive\_proxy* directive can connect to this port. The location of the proxy computer and the pickup port are specified in the partner's Internet Listener Properties.

---

- ② When a message from the remote host arrives, the PAM Proxy Server checks the source address against the known valid source IP addresses listed in the *external* section of the configuration file.

---

- ③ Data is automatically transferred to the inbound port via a memory buffer.

---

- ④ The PAM Proxy Server transparently proxies all the bytes of the message to the socket that is connected to the pickup port.

---

**NOTE:** If an access control check fails, the message is dropped and the connection attempt is logged in the log file.

## SAMPLE CONFIGURATION FILE

This is a sample of the configuration file used to configure the PAM Proxy Server.

```
# File for logging messages
LOGFILE=/home/proxy/proxy_log.txt

# Size of connection cache
CACHE_SIZE=64

# Number of seconds we wait before timing out a connection
IDLE_TIMEOUT=60

# listen for requests from internal machines on this port
OUTBOUND_LISTENER=PAM-proxy.mycompany.com:8471

# This is the list of valid proxies. It is of the form
# proxy_host:proxy_port->internal_host:internal_port
# You must have one PROXY= directive for each tcp listener
# that talks through a proxy.
```

```
PROXY=proxy_machine.mycompany.com:
8481->PAM.mycompany.com:10001

PASSIVE_PROXY=proxy_machine.mycompany.com:
8491->proxy_machine.mycompany.com:
8492->PAM2.mycompany.com:1

# the list of valid external ip addresses for acl purposes
EXTERNAL=PAM.mypartner.com:10002
EXTERNAL=PAM.external.com:10003
EXTERNAL=test_PAM.crossroute.com:8888
EXTERNAL=10.11.38.*
EXTERNAL=10.12.*.*
```

## Where:

### LOGFILE

Defines an output file for all error and status messages generated during proxy runtime. Because this directive sends all configuration file processing errors to the specified logfile instead of to the console, this must be the first directive in the configuration file.

---

### CACHE\_SIZE

Defines how many file handles the proxy will keep open per forked instance. Increasing this number reduces the number of times a new TCP connection needs to be established for a given remote host, but increases the amount of memory used by Partner Agreement Manager, and might reduce the number of file descriptors available to other processes on the system.

---

### IDLE\_TIMEOUT

Defines the number of seconds that the proxy waits after a given TCP connection goes idle before the proxy server forces the connection to close. If your connection is idle for long periods of time, you can use IDLE\_TIMEOUT to set up your proxy to close connections after they've been idle for a specified period of time.

**NOTE:** In a passive configuration, Partner Agreement Manager sends a bit of data (<16 bytes) every 30 seconds to keep the pickup channel open. If the IDLE\_TIMEOUT setting is less than 30 seconds, the connection is closed every 30 seconds. You might want to set the IDLE\_TIMEOUT to 300 seconds, to ensure that the pickup channel remains open.

---

### OUTBOUND\_LISTENER

---

Defines a host and port number on the proxy computer through which all outbound connections are channeled. All internal Partner Agreement Manager computers that send or receive messages through the proxy make outbound connections through this port. You might want to define this as an IP address rather than as a host name to protect the proxy from a DNS spoof. The outbound listener is a single process that can support only a single outbound message at a time.

---

#### EXTERNAL

Defines a valid external host/IP combination. This is used for authentication before allowing data through the proxy in either direction. For inbound connections, the proxy validates that the source IP address matches one of the IP addresses defined in the external section. For outbound connections, it verifies that the destination IP *and* port match one of the IP/port combinations specified in the external section. You can use wildcards to specify IP address ranges, if you prefer to limit connections using your firewall instead of the proxy software.

---

#### PROXY

Defines a transparent proxy from an IP/port combination on the proxy computer to an IP/port combination on another computer (usually an internal Partner Agreement Manager computer). You must supply multiple instances of this directive if you have multiple listeners defined on an internal Process Server, or if you have more than one internal Process Server running. A process will be forked to manage each transparent proxy. Each proxy can support only one message at a time.

**NOTE:** Only the IP addresses defined on the right side of the arrow can connect back to the outbound listener.

---

#### PASSIVE\_PROXY

PASSIVE\_PROXY directives define a triplet of host/port combinations. The first two combinations define a pair of listeners: an external listener and a pickup-port listener. The third host/port combination defines the destination host, which is the only host allowed to connect to the pickup port. The port of the destination host is currently ignored.

---

## COMPILING THE PAM PROXY SERVER

The Windows version of the PAM Proxy Server is already compiled and ready to use. You must compile the UNIX version before running it. The UNIX version of the Partner Agreement Manager Proxy Server includes a makefile and all source files. You can use any C compiler to compile the Partner Agreement Manager Proxy Server.

**NOTE:** If you change the built-in compiler options for the Windows version of the PAM Proxy Server, you must recompile it. The instructions in this section include notes about what you need to do to compile the Proxy Server on Windows.

### To compile the PAM Proxy Server:

- 1 Copy all source files into a directory on a computer with a C compiler installed.
- 2 Load the makefile into an editor and ensure that the basic settings are correct.

**NOTE:** If you are compiling the proxy on NT, check the `makefile.nt` file.

```
# set to your compiler
CC = gcc

# set to your preferred debug level .. 99 is max, 0 is min
DEBUG=0

# uncomment one of these lines ...
#BUILD_OS=LINUX
#BUILD_OS=SOLARIS
BUILD_OS=AIX

# if you're compiling solaris uncomment this line...
#LIBS=-lsocket -lnsl

#####
# change nothing below here
...
```

- 3 When the makefile settings are correct, type `make` (or `nmake /f makefile.nt` on NT systems) to compile the `PAM_proxy` executable.

### To test the PAM Process Server:

- 1 Type `PAM_proxy <proxy_config.cnf>` and ensure that it starts correctly.
- 2 Type Control-C to stop the PAM Proxy Server after it starts.

**TIP:** After testing, you might want to modify the `start_proxy` shell script and include it in your server boot script, so that the proxy server is automatically started when the proxy computer starts up.

## RUNNING THE PROXY SERVER AS AN NT SERVICE

If you are using Windows, you can run the PAM Proxy Server as a service.

---

**IMPORTANT:** Before you install the PAM Proxy Server as an NT service you must: 1) install `PAM_proxy.exe` in its permanent working directory before you run the `install` command, and 2) name the configuration file `PAM_proxy.cnf`, and install it in the same directory as `PAM_proxy.exe`.

---

**TIP:** Specify the `LOGFILE` directive at the top of the configuration file to ensure that any problems that might occur with the proxy are logged.

**To run the PAM Proxy Server as an NT service:**

- 1 Install `PAM_proxy.exe` by typing `PAM_proxy -install`.
- 2 Open the Control Panel and click Services. Select the service and click Start.

**NOTE:** When you install the proxy service it is set up so that you must start it manually. To start the proxy service automatically at system startup, open the Control Panel and click Services. Select the service, click Startup, and select the Automatic startup type.

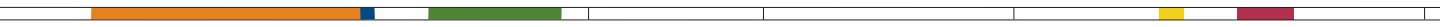
**To remove the PAM Proxy Server service:**

- 1 Stop the service in the NT Services control panel.
- 2 From the PAM Proxy Server working directory, type:

```
PAM_proxy -remove
```

## MAINTAINING THE PAM PROXY SERVER

The PAM Proxy Server is designed to run for long periods of time with little or no intervention on your part. The only output that the PAM Proxy Server generates is its log file, which grows over time—especially if debugging is turned on. After the PAM Proxy Server goes into production, decide how many days' worth of logs to save and weigh that against the amount of disk space that you can afford to allocate to log files. In most cases, many weeks' worth of logs can be saved with little risk.



Because there is no automated way to archive or delete a log file in the current version of the Proxy Server, the log file can get very big. One solution is to shut down the Proxy Server periodically and rename or delete the existing log file. When you restart the Proxy Server, it creates a new log file.





## C

## USING THE WEB PROXY

The Web Proxy enables communication with your partners across your company firewall without compromising the security of your internal network. The two key components are the Web Proxy and the Proxy Broker.

This appendix describes how to install and configure both the Web Proxy and the Proxy Broker.

This appendix includes these sections:

- *About the Web Proxy and the Proxy Broker* on page 154.
- *Using the Web Proxy and the Proxy Broker* on page 156.
- *Installing and using the Web Proxy* on page 156.
- *About the integrated Proxy Broker* on page 158.
- *Configuring Proxy Broker Properties* on page 159.

## ABOUT THE WEB PROXY AND THE PROXY BROKER

The Web Proxy serves as a sentry that collects incoming messages outside the firewall and notifies your Proxy Broker that they are available. The Proxy Broker then retrieves the waiting messages and forwards them to the Web server. With this configuration, your partners never have direct access to your internal network.

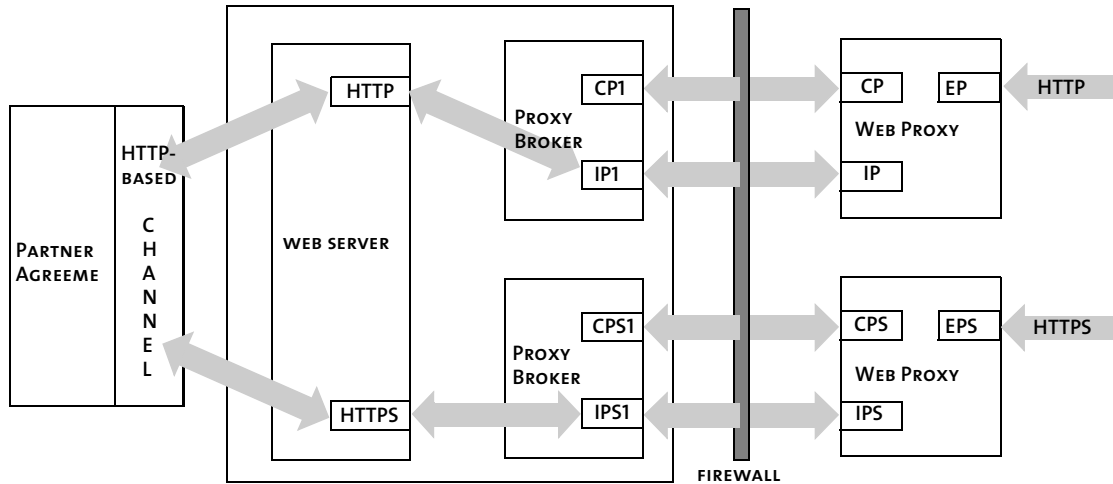
When you communicate with your partners using the Partner Agreement Manager protocol, you use the PAM Proxy. The Web Proxy is used for communications over a Web-based channel that uses the HTTP protocol. Both proxies enable inbound communications to pass through your network's firewall

The Web Proxy receives inbound messages that are intended for your Web server or Web application. The Web Proxy listens on its external data port for these messages and makes them available to the Proxy Broker on its internal data port. The Proxy Broker, which starts when the Web Proxy starts, then connects to the Web Proxy's internal data port, retrieves these messages, and forwards them to your Web server or Web application.

The Web Proxy runs outside the firewall. The Proxy Broker runs on the internal network and acts as a liaison between the Web Proxy and the Web server—the Web Proxy itself does not connect to the internal network.

The Proxy Broker is part of Partner Agreement Manager, and is active whenever Partner Agreement Manager is running.

As the following illustration shows, you must start separate instances of the Web Proxy to establish HTTP and HTTPS connections to the Web server. In this illustration, the Web Proxy ports EP (external data port), IP (internal data port), and CP (control port) are specified when you start the proxy; the IP and CP ports on the Proxy Broker are random ports.



**Tip:** When the Web Proxy is used for inbound SSL connections, the server certificate for the Web server must be created specifying the Web Proxy's IP address, because all inbound connections will be made to the Web Proxy. The certificate itself must be installed on the Web server, and the IP address must be the Web Proxy's IP address.

## REQUIREMENTS

The Web Proxy does not do any processing or inspection of data—it simply routes data from one socket to another if it is authenticated by the access control list. Because it does not do any processing, the hardware requirements are minimal. The proxy logs debugging information to a file on the hard disk, so you need to size the amount of disk space appropriately.

For example, 20,000 processes (independent of business object size) generate about 20 MB of debugging log information. Because you must shut the Web Proxy Server down to rotate the log file, be sure you have enough disk space when you debug your network. The Web Proxy code itself requires less than 1 MB of disk space.

In addition to the disk space, the Web Proxy requires:

- 32 MB of memory for Windows
- 128 MB for UNIX
- any Pentium-class CPU for Windows
- any sparc class CPU for UNIX

## USING THE WEB PROXY AND THE PROXY BROKER

The Web Proxy is for inbound communications only. Outbound messages can continue to use the HTTP proxy that you might already have established, to allow browser-based clients to communicate outside your firewall. To use your HTTP proxy, you must reconfigure it before attempting to send outbound messages through your Web-based channel. For more information, see *Using the Outbound Proxy* on page 163.

**NOTE:** If you already have a proxy solution that supports SSL connections to your Web server without message decryption, you do not need to install the Web Proxy.

## INSTALLING AND USING THE WEB PROXY

You can run the Web Proxy on Windows NT or on UNIX. This section gives you installation instructions for each operating environment.

**NOTE:** The Web Proxy supports one type of connection per instance of the proxy. Therefore, if you plan to run the Web Proxy for both HTTP and HTTPS connections simultaneously, you need to run two instances each of the Web Proxy and the Proxy Broker—one for HTTP and one for HTTPS.

## INSTALLING THE WEB PROXY ON WINDOWS NT

When you have completed the installation, you can run `webproxy.exe` from the command prompt to start the Web Proxy.

### To install the Web Proxy on Windows NT:

- 1 Extract the contents of the `Webproxy.zip` file into any directory you choose. It is a good idea to create a separate directory for the extracted files.
- 2 Set your `PATH` to include the `\release` subdirectory in the directory where you extracted the `Webproxy.zip` file.

For example, if you extracted the zip file to `c:\WebProxy`, set your `PATH` to include `c:\WebProxy\release`.

## INSTALLING THE WEB PROXY ON UNIX

When you install the Web Proxy on UNIX, you extract the contents of a `.tar` file and, depending on your platform, run the `Make` command to build the proxy.

### To install and build the Web Proxy on UNIX:

- 1 If you are running Solaris, extract the contents of the `webproxy.tar` file and place it into any directory you choose. Use the `tar -xf webproxy.tar` command.
- 2 If you plan to use the proxy on another UNIX platform, you must run the `Make` command to build the proxy:

```
make -f Makefile.os
```

where `os` is the OS-specific extension.

Example: `make -f Makefile.sun`

**TIP:** You can also start a fresh build by typing `make -f Makefile.os clean`

**NOTE:** If the appropriate `Makefile` does not exist, contact Software Support at <http://ps.software.ibm.com/pbin-usa-ps/getobj.pl?/pdocs-usa/phonenos.html>. You can create your `Makefile` from one of the existing `make` files, if you are familiar with the `Make` command.

When the build is complete, the executable `webproxy` appears in the `release` directory.

## USING THE WEB PROXY

The Web Proxy uses three ports on the proxy server:

- the control port; the default is 6000.
- the internal data port; the default is 6001.
- the external data port, on which the proxy server listens for incoming data; the default is 6002.

The Web Proxy command accepts either no arguments or three arguments. If arguments are specified, three are required: `proxy_control_port`, `proxy_internal_data_port`, and `proxy_external_data_port`. If no arguments are specified, the ports are set to their defaults (6000, 6001, and 6002).

To run the Web Proxy, do one of the following:

- ▶ Type this command from a Windows NT command prompt or from a UNIX shell: `webproxy`
- ▶ Type this command from a Windows NT command prompt or from a UNIX shell:

```
webproxy <proxy_control_port> <proxy_internal_data_port>  
<proxy_external_data_port>; for example, webproxy 6200 7200 8200.
```

This command	Does this
<code>webproxy</code>	Starts the Web Proxy and sets the Control Port to 6000, the Internal Data Port to 6001, and the External Data Port to 6002.
<code>webproxy 6200 7200 8200</code>	Starts the Web Proxy and sets the Control Port to 6200, the Internal Data Port to 7200, and the External Data Port to 8200.

**TIP:** To see various options, use `webproxy -help`.

## ABOUT THE INTEGRATED PROXY BROKER

If the Web Proxy is necessary for your configuration, you must set specific properties in the `Partner.properties` file. The next section describes these properties. (You do not need to install the Web Proxy if you already have a proxy solution that supports SSL connections to your Web server without message decryption.)

**NOTE:** The `Partner.properties` file is located in the `Partner\Partner\Properties` directory in your Partner Agreement Manager installation directory (where `nnn` corresponds to your partner ID).

## CONFIGURING PROXY BROKER PROPERTIES

All properties for HTTP and HTTPS protocols must be specified in `Partner.properties` file on your Process Server. Depending on your configuration, you might need to add a property definition. If a property line is not already there, you must add it to the properties file.

If there is a line for a property with values you need to modify, modify only the value that appears between the first equal (=) sign and the first semicolon (;). This is either your host name or a port number. The other values, such as `mode` and `type`, which you must also enter if you are adding a new property line, must be entered exactly as presented in the example below.

**NOTE:** Every host must have a corresponding control port number. The internal data port number defaults to control port + 1 if you specify the host and control port.

### To configure the Proxy Broker properties:

- 1 Stop the Process Server if it is running.
- 2 Open the `Partner.properties` file.
- 3 Modify or add the appropriate information.

Follow the format of the example below to enter your settings. Enter the host IP address and port numbers (in place of the text in the brackets). Enter the text string for `mode` and `type` exactly as it appears for each property line—HTTP Host, ControlPort, and DataPort and HTTPS Host, ControlPort, and DataPort:

Example:

```
WebProxy.HTTP.Host=<YourWebProxyHTTPHost>; mode=server; type=string;
WebProxy.HTTP.ControlPort=<YourWebProxyHTTPControlPort>; mode=server;
type=int;
WebProxy.HTTP.DataPort=<YourWebProxyHTTPInternalDataPort>; mode=server;
type=int;
```

```
WebProxy.HTTPS.Host=<YourWebProxyHTTPSHost>; mode=server; type=string;
WebProxy.HTTPS.ControlPort=<YourWebProxyHTTPSControlPort>; mode=server;
type=int;
WebProxy.HTTPS.DataPort=<YourWebProxyHTTPSInternalDataPort>;
mode=server; type=int;
```


As you can see in the example above, there are two sets of host and port properties—one set for each instance of the Web Proxy you might want to start. One set manages HTTP connections and the other handles the HTTPS connections. These settings are unique and you must specify them for your Proxy Broker configuration:

This setting	Specifies this
WebProxy.HTTP.Host	The IP address for your HTTP protocol. If this property is not specified, the broker instance for HTTP does not start.
WebProxy.HTTP.ControlPort	Your established control port for the HTTP Partner Agreement Manager. This property must be specified if the HTTP Host is specified. If you ran <b>webproxy</b> with defaults, then specify 6000 here for the control port.
WebProxy.HTTP.DataPort	The internal data port of your HTTP Web Proxy. If host and control port are specified and data port is not, it defaults to the Control Port value +1. If you ran <b>webproxy</b> and specified all three arguments, make sure the data port value here matches the internal data port number (the second parameter) you specified when you ran <b>webproxy</b> .
WebProxy.HTTPS.Host	The IP address for your HTTPS protocol. If this property is not specified, the broker instance for the HTTPS protocol does not start.
WebProxy.HTTPS.ControlPort	Your established control port for the HTTPS Web Proxy. This property must be specified if the HTTPS Host is specified.
WebProxy.HTTPS.DataPort	The internal data port of your HTTPS Web Proxy. If host and control port are specified and data port is not, it defaults to the Control Port value +1.

Example settings:

```
WebProxy.HTTP.Host=109.0.0.21; mode=server; type=string;
WebProxy.HTTP.ControlPort=6200 mode=server; type=int;
```





```
WebProxy.HTTP.DataPort=7200; mode=server; type=string;  
WebProxy.HTTPS.Host=109.0.0.21; mode=server; type=string;  
WebProxy.HTTPS.ControlPort=6443; mode=server; type=int;  
WebProxy.HTTPS.DataPort=6453; mode=server; type=int;
```

After adding these lines, press Enter before closing the properties file.

**NOTE:** If the control connection to the Web Proxy is broken, the control port logs exception messages to the System Messages audit folder. All exceptions are logged in this folder.

Stopping the Process Server also stops the Proxy Broker. Any changes in Proxy Broker settings *or* Process Server settings require the Partner Agreement Manager service to be restarted. Restarting Partner Agreement Manager also restarts the integrated Proxy Broker.



## D

## USING THE OUTBOUND PROXY

Partner Agreement Manager 2.2 channels that use HTTP or HTTPS communication can work with outbound proxies that use authentication. Outbound proxy authentication is used within *internal* networks to ensure that only people and applications that are authenticated may communicate with an *external* network.

This appendix describes how to use and configure the outbound proxy for Partner Agreement Manager.

This appendix includes these sections:

- *Using an outbound proxy* on page 164.
- *Configuring an outbound proxy* on page 164.

## USING AN OUTBOUND PROXY

Outbound HTTP and HTTPS proxy authentication is used within internal networks to ensure that only users and applications that are authenticated can communicate with an external network. Authentication in the outbound proxy is based on a standard user name and password combination.

You turn on the outbound proxy feature after you install Partner Agreement Manager. When you do, all outbound HTTP and HTTPS communication uses the same user name and password combination for the proxy.

**NOTE:** This is not an additional IBM proxy—it provides outbound proxy support for existing channels that use HTTP or HTTPS communication. Partner Agreement Manager-to-Partner Agreement Manager communication still needs to go through the Partner Agreement Manager Proxy.

## CONFIGURING AN OUTBOUND PROXY

If your network has an outbound proxy, you must configure Partner Agreement Manager to use it.

**To configure Partner Agreement Manager to use an outbound proxy for HTTP or HTTPS traffic:**

- ▶ Add or edit the Partner.properties in your partner directory:

Outbound.Http.Proxy.Host = <your\_outbound\_proxy\_host>

Outbound.Http.Proxy.Port = <your\_outbound\_proxy\_port>

You can tell if an outbound proxy is authenticating if your browser prompts you for a user name and password when you browse the Web.

**If the proxy is authenticating, also follow these steps:**

- 1 Edit Partner.properties:

Outbound.Proxy.User = <your\_proxy\_user>

- 2 In the Process Manager/System Passwords, update the Outbound Proxy Password to the proxy user's password.

See *Changing passwords from the Process Manager* on page 15.

# E

## CONFIGURING PAM FOR MQSERIES

Partner Agreement Manager supports MQSeries for asynchronous communication. This appendix describes how to configure Partner Agreement Manager for MQSeries.

This appendix includes these sections:

- *About Partner Agreement Manager for MQSeries* on page 166.
- *Configuring MQSeries for Partner Agreement Manager* on page 166.
- *Setting transmission properties* on page 167.
- *Installing an incoming service* on page 169.

## ABOUT PARTNER AGREEMENT MANAGER FOR MQSERIES

Partner Agreement Manager supports MQSeries for asynchronous communication. Before configuring Partner Agreement Manager for MQSeries, you must install MQSeries 5.1 for NT. You can install it either on the computer where Partner Agreement Manager is installed, or on another computer. After you configure Partner Agreement Manager to run with MQSeries, you can use MQSeries from within Partner Agreement Manager as a communication service.

**NOTE:** See *Setting up the Partner Agreement Manager Channel profile* on page 20 for more information on communications settings in general.

Depending on your company's communication needs, you can install as many of each type of service as you need. For example, if you have several inbound MQSeries queues, you might install a Partner Agreement Manager connection for each queue. This allows Partner Agreement Manager to try an alternate queue if the primary queue becomes unavailable.

Your prioritized list of connection services is one of the items that you give to your partners when you exchange channel profile information. In return, you receive prioritized lists from your partners that tell you how to connect to their PAM servers.

## CONFIGURING MQSERIES FOR PARTNER AGREEMENT MANAGER

The way in which you configure MQSeries communications depends on the version you're using. Consult your MQSeries documentation for more information.

Each MQSeries installation must have:

- a queue manager.
- a local queue.
- a transmission queue between each partner's MQSeries installation.
- a sender channel.
- a receiver channel.
- a SVRCONN channel.

After MQSeries is configured correctly, you start the MQSeries listener, and then you start the sender channel.

## SETTING TRANSMISSION PROPERTIES

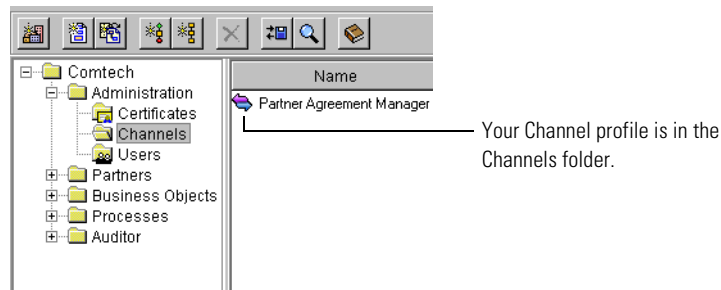
In Partner Agreement Manager, you must set transmission properties to specify the connection time-out interval—that is, the amount of time Partner Agreement Manager waits for a reply before cancelling a connection attempt. To set up MQSeries transmissions, you need to know:

- The name of the computer where MQSeries is installed.
- The port where the MQSeries server listens.
- The names of the channel and of the outbound queue manager.

The standard MQSeries configuration includes defining the queue manager and channel names. You also need to know whether MQSeries requires a user name and password for establishing communications.

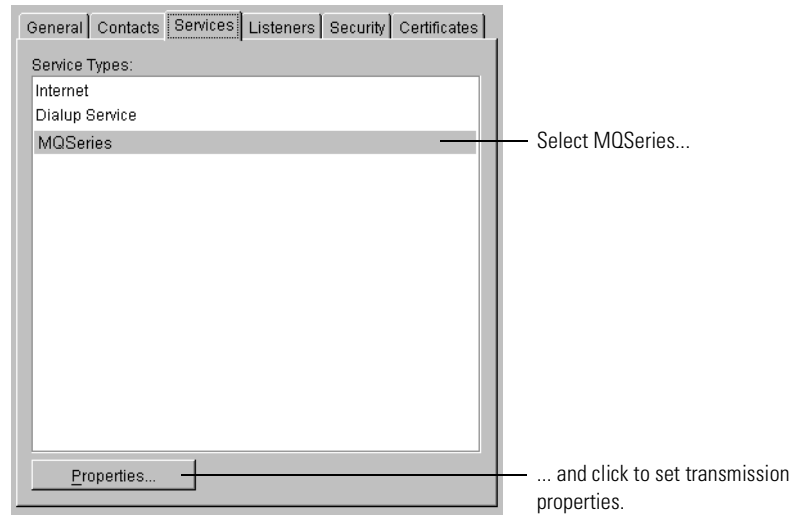
### To set transmission properties:

- 1 Open the Administration folder in the Process Manager window, and then open the Channels folder.



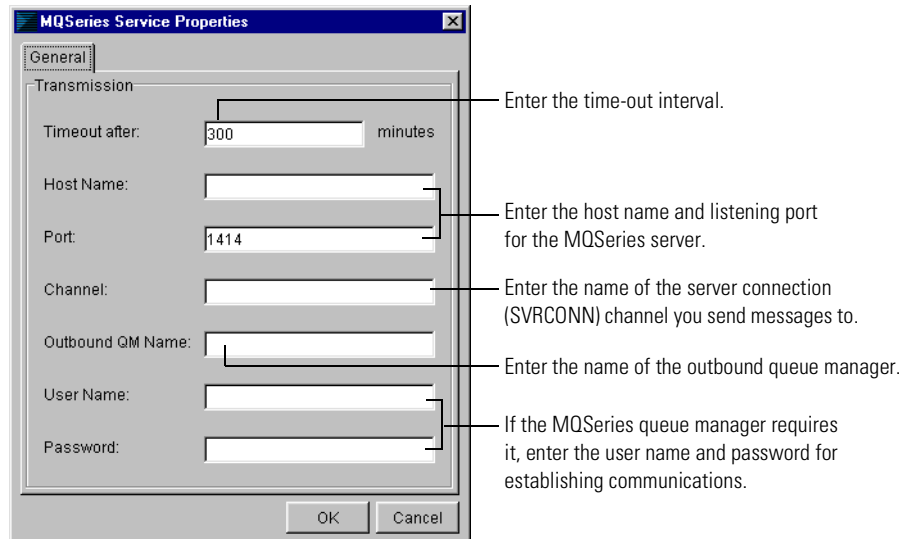
- 2 Double-click the Channel profile and click the Services tab.

The Services tab appears.



**3** Select MQSeries and click Properties.

The MQSeries Service Properties dialog box appears.





#### 4 Enter the appropriate information.

In this field	Enter this information
Timeout after	The time-out interval (in minutes).
Host Name	The name of the computer where MQSeries is installed.
Port	The port number where the MQSeries server listens. This port number corresponds to the port you are using for the MQSeries listener.
Channel	Name of the server connection channel to which you send messages.
Outbound QM Name	The name of the outbound queue manager (the queue manager for which you run a listener).
User Name	The user name MQSeries uses for establishing communications (if necessary).
Password	The password MQSeries uses to establish communications (if necessary).

#### 5 Click OK to save the MQSeries transmission properties.

**NOTE:** Because MQSeries is an asynchronous communication service, there are no Partner Agreement Manager retry properties to set. MQSeries manages message queuing and retries as needed.

## INSTALLING AN INCOMING SERVICE

The settings you specify for an incoming Partner Agreement Manager service provide your partners with the information they need before they can successfully communicate with you. Because reliable communication is important to running processes, Partner Agreement Manager enables you to set up as many incoming services as you need—both synchronous (Internet or dialup) and asynchronous (MQSeries).

If Partner Agreement Manager can't connect using the first incoming service listed in your channel profile, it rolls over to the next service listed, and so forth.

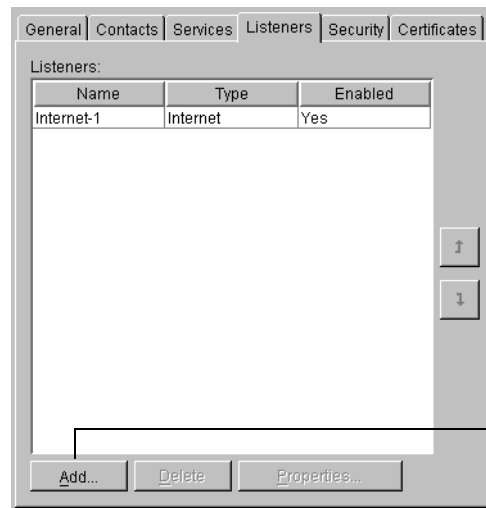
**NOTE:** Partner Agreement Manager rolls over from one synchronous or asynchronous service to the next, but does not roll over between synchronous and asynchronous services.

To install MQSeries as an incoming connection, you need to know the names of the inbound queue, the inbound queue manager, and the queue to which you want to send unreadable (error) messages. You can also set the read count, which determines the number of threads Partner Agreement Manager uses as it listens for incoming messages. The minimum number of threads is 1, but you can increase the number to 2 or 3 if you expect a higher volume of traffic.

### To install an incoming service:

- 1 Open your Channel profile and click the Listeners tab.

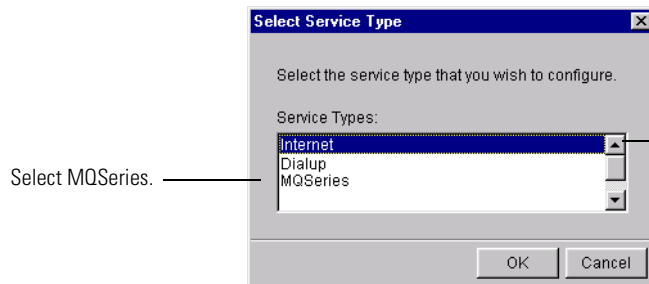
The Listeners tab appears.



Click to add a install a new service for incoming MQSeries transmissions.

- 2 Click Add to add a service for incoming MQSeries transmissions.

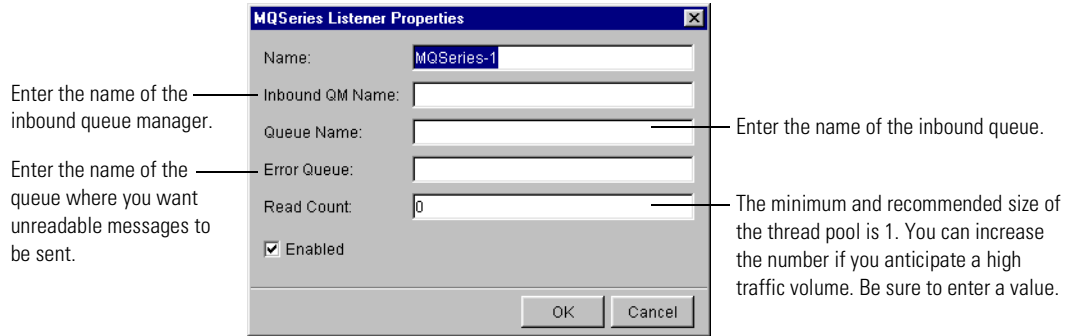
The Select Service Type dialog box appears.



The items that appear in this list vary, depending on the services available on your computer.

- 3 Choose MQSeries and click OK.

The MQSeries Listener Properties dialog box appears.



**4** Type a name for the incoming service.

Each service name must be unique. It's a good idea to use a name that clearly identifies the service. For example, you can give your primary MQSeries service a name like "MQSeries main." The name you use doesn't have to be the same as the queue name.

**5** Enter the appropriate information for the service.

In this field	Enter this information
Inbound QM Name	The name of the inbound queue manager
Queue Name	The name of the inbound queue
Error Queue	Name of the queue to which unreadable messages are transferred
Read Count	Number of threads that read messages (size of thread pool) <b>NOTE:</b> You can increase the number if you anticipate a high traffic volume. If you leave the default setting (0), you cannot use MQSeries service.
Enabled (checkbox)	When you are a partner, you can disable certain channels that you don't want to use to contact a particular partner. For example, if your partner sends a channel profile with: <ul style="list-style-type: none"> <li>■ TCP-1</li> <li>■ MQSeries-1</li> </ul> You can open that partner's channel profile and uncheck the Enabled check box so you will never attempt to send something over the MQSeries-1 channel.

**6** Click OK in the Listener Properties dialog box.

**7** Repeat steps 2 - 6 to continue adding services as necessary.

**8** Click OK, or click another tab in the Profile dialog box to enter additional information.



## F

## NOTICES

This information was developed for products and services offered in the United States. IBM may not offer the products, services, or features discussed in this information 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 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 information. The furnishing of this information does not give you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106, Japan

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information 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. Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM United Kingdom Laboratories,  
Mail Point 151,  
Hursley Park,  
Winchester,  
Hampshire,  
England  
SO21 2JN.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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

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.

## TRADEMARKS

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AIX  
DB2  
IBM  
MQSeries  
SupportPac  
WebSphere

Pentium is a registered trademark of Intel Corporation in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

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.



## GLOSSARY

**action**—a task performed as part of a private process. A private process action is the equivalent of a step in a public process. See the following terms in this glossary for more information about the action types you can include in a private process:

- approval action
- extension action
- mapping action
- notification action
- output object action
- script action
- subprocess action
- termination action
- timer action

See also *private process*.

**adapter**—the software bridge between Partner Agreement Manager processes and specific end-system and business-application interfaces. Adapters manage interactions between business applications and the Adapter Server. They allow private processes to interact with external business applications while a process is running, and they allow Partner Agreement Manager to start public processes based on events that occur in external business applications. See also *adapter implementation*, *adapter instance*, *adapter type*.

**adapter implementation**—the implementation declaration for an adapter type. It specifies the name and location of the Java source file that defines the application logic used to communicate with a specific end system through that end system’s interface. The application logic is specified in the form of properties. See also *adapter*, *adapter instance*, *adapter type*.

**adapter instance**—an instance of an adapter implementation. The adapter instance is used in a private process extension action and provides the specific values to be used for the properties declared in the adapter implementation. See also *adapter*, *adapter implementation*, *adapter type*, *extension action*.

**adapter type**—a definition that is stored in XML format and specifies the adapter’s properties as well as the operations and events it supports. A single adapter type can have multiple implementations, and each implementation can have multiple instances. See also *adapter*, *adapter implementation*, *adapter instance*.

**approval action**—a private process action that you use to ask for a response from a user before letting the process continue to run. You can use an approval action, for example, to ask for an OK when a purchase order exceeds a predetermined amount. See also *private process*.

**business object**—a message transmitted as part of a public process. Business objects take the form of purchase orders, acknowledgments, requests for clarification, and so on. See also *business object type*.

**business object type**—a definition that determines the types of information a message can contain. It has three properties: the top-level element in its element definition set, its key field, and whether instances of it return audit information for non-repudiation purposes. The name of the business object type is the name of the element you select as its top-level element. See also *business object*, *element definition set*, *non-repudiation*.

**business object variable**—one of the two types of variables used in Partner Agreement Manager to store information within a process. Business object variables create an instance of a business object type. They can be used to store, for example, the outputs from extension actions, the inputs for map actions, or the inputs and outputs for subprocesses. See also *business object*, *business object type*, *extension action*, *variant variable*.

CA—see *certificate authority*.

**certificate**—a security document that binds a public encryption key to an entity (an individual or organization) known as the principal. The security document (a digital certificate) is signed by another entity known as the issuer. A digital certificate for which both the principal and issuer are the same entity is known as a self-signed certificate. A certificate for which the principal and issuer are different entities is issued by a certificate authority (CA) like VeriSign and is known as a CA-issued (or third-party-signed) certificate. Partner Agreement Manager supports both self-signed and CA-issued certificates. PAM also supports the binding of certificates to be used for signature authentication, message encryption, and SSL authentication for channels other than Partner Agreement Manager. See also *certificate authority*, *SSL*.

**certificate authority**—a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the certificate authority, or CA, is to authenticate the entities (individuals or organizations) involved in electronic transactions. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be. See also *certificate*.

**channel**—a communications mechanism that encapsulates all the processing information needed to send messages to a partner's system, as well as to translate data received from a partner into Partner Agreement Manager messages. Partner Agreement Manager provides channels for RosettaNet, EDI, cXML, and other systems and protocols. See also *message*.

**digital certificate**—see *certificate*.

**DTD**—Document Type Definition. A type of file associated with SGML and XML documents that defines how the formatting tags should be interpreted by the application presenting the document. In Partner Agreement Manager, a DTD file contains the complete description of a business object type's element definition set. See also *business object*, *business object type*, *element definition set*.

**element definition set**—a collection of data fields (or elements) or groups of data fields that defines the structure and meaning of a business object type. See also *business object*, *business object type*.

**encryption certificate**—see *certificate*.

**event**—a piece of information that comes into Partner Agreement Manager as a message from another source (an enterprise system or business application, for example) and triggers a public process. See also *message*.

**event push**—a method that uses the HTTP POST mechanism to push events into Partner Agreement Manager as a way to trigger processes. A port on the Process Server is set to listen for events in the form of HTTP POST messages. When a message is detected, PAM uses the information in the message to generate an event. See also *event*.

**extended enterprise**—a business model under which companies that work together as partners function as efficiently as a single organization through the implementation of automated communication technologies.

**extension action**—a private process action that communicates via an adapter with an external application that is registered with Partner Agreement Manager. You can use an extension action, for example, to launch a spreadsheet application, perform calculations, and update the enterprise system, or to get information from an enterprise system or listen for an event in the enterprise system. See also *adapter, private process*.

**LDAP**—Lightweight Directory Access Protocol. LDAP provides a standard method for accessing information from a central directory. After user authentication is set up in the LDAP directory, applications that use the LDAP protocol can retrieve the information from that directory. An authenticated user can log in to any application that supports the LDAP protocol with the same user name and password.

**linked certificate**—see *certificate*.

**map**—a Java Script or VBScript that inserts data into fields in an output business object type generated by a private process. The map specifies which fields in the output business object type receive data, and it identifies the information source.

**map method**—a reusable logical block of code that inserts data into a particular type of element or element sequence in a business object type. Within a map method, you can write the expressions that map individual input and output fields in the sequence. Or you can create a submap and drag input fields to output fields and have Partner Agreement Manager create the appropriate mapping expressions. See also *map, submap*.

**mapping action**—a private process action that you use to call a map. The map specifies the fields in a business object type that will receive data extracted from another source. You use a mapping action when you want to extract data from one business object type and insert it in a different business object type. For example, you use a mapping action to transform a purchase order generated by your inventory system into a sales order in a format that your partner expects. See also *map, private process*.

**message**—a structured communication used to pass information and control to another partner in a public process. The action in the process passes to the partner who receives the message. The content of a message is determined by its business object type. A message can be transmitted via synchronous or asynchronous methods, as determined by its communication service type. See *business object type*.

**non-repudiation**—a business object security feature that authenticates instances of a business object type and maintains an audit record to verify that they were received by the intended recipient. For business object instances that you receive, Partner Agreement Manager authenticates each instance and maintains an audit record to verify that the instance actually originated with the stated originator. If you disable auditing for a business object type, non-repudiation support is disabled for all messages that contain instances of that business object type.

**notification action**—a private process action that you use to send an e-mail, fax, or pager message to addressees that you specify. You use a notification action to inform someone inside or outside your organization that an event has occurred. For example, you can use a notification action to alert the order entry department when a purchase order arrives from a customer. See also *private process*.

**output object action**—a private process action that you use to bind a business object to the expected output object and path in a public process. You use an output object action at the point in a private process when you are ready to send a business object to the associated public process. This is typically the last action in the private process. See also *private process*.

**partner group**—a group of partners that perform the same role in a process at different times. Instead of duplicating a public process and substituting a different partner name, you can set up a partner group for the public process and then designate a specific partner as the participant when you start an instance of the process. For example, you might design a generic purchasing process that works equally well with any of your suppliers and then designate the appropriate partner when you start the process.

**partner profile**—information that identifies an organization, specifies a contact person in that organization, lists the communication services the organization supports, and defines the organization's security profile. When partners agree to participate in a public process, they must exchange profile information as a way to ensure authenticity before they can proceed.

**PIP**—Partner Interface Process. RosettaNet PIPs are specialized system-to-system XML-based dialogs that define business processes between supply-chain partners and provide models and documents for the implementation of e-commerce standards. Each PIP includes a technical specification based on the RosettaNet Implementation Framework (RNIF), a message guideline document with a PIP-specific version of the business dictionary, and an XML message guideline document. See also *RosettaNet*.

**post method**—the last block of code that is executed when a mapping action runs. Its only parameter is the output business object. You use the post method when you need to perform post-processing on the output business object. For example, you might use the post method to set the value of a summary field based on the number of line items in the output business object, or to examine a range of dates in a repeated group, extract the most recent date, and post that date in a header field. See also *mapping action*, *pre method*.

**pre method**—the first block of code that is executed when a mapping action runs. The pre method's parameters are the map inputs. You use the pre method to access a map's inputs and set global variables based on their content. See also *mapping action*, *post method*.

**private process**—a task or set of tasks that business partners participating in a public process perform at points where they need to take action internally. Partners participating in a public process must implement a private process for each public process step that they own. A private process begins with input from the public process and ends with output that feeds back into the public process. The input can be the receipt of a business object from a partner, or it can be a triggering event from an internal system. The output is the business object that transfers control back to the public process. See also *action*, *process*, *public process*.

**private process action**—see *action*.

**process**—the flow of actions and the exchange of business information between partners in an extended enterprise. A process operates on two levels, public and private. See *extended enterprise*, *private process*, *public process*.

**public process**—the step-by-step flow of messages, events, and actions between two or more business partners. Public processes are set up by agreement between partners, and each step in a public process has a private process associated with it. A public process is developed by one partner, and all the partners who participate in it must review and approve it before it can be implemented. The partner who designs a public process is its owner. See also *private process*, *process*.

**RosettaNet**—a consortium of major information technology, electronic components, and semiconductor manufacturing companies that is working to create and implement industry-wide, open e-business process standards. See also *PIP*.

**script action**—a private process action that consists of a script written in VBScript or JavaScript and is designed to manipulate information or set up conditional actions based on input. You use a script to establish decision-making criteria for branches or loops, to set variables, or to calculate values that are used elsewhere in the private process. See also *private process*.

**security certificate**—see *certificate*.

**self-signed certificate**—see *certificate*.

**signature certificate**—see *certificate*.

**SSL**—Secure Sockets Layer. The SSL protocol is a security protocol that provides for communications privacy and reliability over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

**submap**—a secondary level map that is called by a map method to insert data into an output element other than the top-level element. See *map*, *map method*.

**subprocess action**—a private process action you use to call an existing public process. You can call any public process in which your organization owns the first partner action. For example, you can use a subprocess to get a quote approved by a third-party supplier before responding to a customer. See also *private process*.

**termination action**—a private process action that you use to stop a process at a predetermined point for a reason that you specify. You can use a termination action to deal with errors in data that might prevent a process from completing successfully. For example, you might want to stop a process in cases where an enterprise system passes incomplete or corrupted information to it. See also *private process*.

**third-party-signed certificate**—another name for a CA-issued certificate. See *certificate*.

**timer action**—a private process action that you use to insert a pause. You can use a timer action to specify the period of time you want to elapse before the next action in the process starts. See also *private process*.

**variant variable**—single field variables. Variant variables store text strings—the type of information contained in a single field element. You can use variant variables to store the input for actions, to set flags (such as the time-out flag for an approval action), to move information within scripts, or to store the results of an approval action. See also *business object variable*.





## A

## access

- assigning to users 47
- types, described 45
- See also* edit access; read access

## Adapter Designer, renaming adapter instances 100

## adapter instances

- adding 94
- duplicating 100
- enabling event polling 96
- exporting 101
- importing 102
- renaming 100
- specifying property values 96
- starting 98
- stopping 98
- See also* Adapter Manager

## Adapter Manager

- adding adapter instances 94
- described 92
- determining if Adapter Server is started 99
- duplicating adapter instances 100
- enabling event polling 96
- exporting adapter instances 101
- importing adapter instances 102
- specifying property values 96
- starting 93
- starting and stopping adapter instances 98
- toolbar 93
- window features 92

## Adapter Server

- determining if it is started 99
- managing on UNIX 89
- starting 80
- testing the connection 84

## Adapter Server Login dialog box 80

## Adapter Server window

- described 78, 81
- status bar 82
- toolbar 81

## adapter types, relationship to adapter instances 94

- Admin user
  - described 45
  - editing user information 46
  - role in LDAP 131
- algorithms
  - described 34
  - encryption 34
  - key exchange 35
  - prioritizing 36
  - selecting 36
  - signature 35
- archive folders, described 105, 117
- Archive Process Logs dialog box 118
- archives, backing up 117
- audit information
  - backing up 118
  - restoring archived 120
  - system, deleting 126
  - types 105
  - viewing 109
- Audit Trace window. *See* Process Audit Trace window
- authenticating outbound proxy 164
- authority, certificate 35
- B**
- batch utility for LDAP password 136
- Bind Certificate dialog box 42
- binding certificates 41
- business objects
  - extracting content 127
  - extracting origin information 127
  - extracting receipt information 127
- C**
- CA-issued certificates, described 35
- certificate authority 35
- certificate, for web server 155
- certificates
  - binding 41
  - CA-issued 35
  - described 35
  - encryption, described 41
  - importing 40
  - linked 35
  - reviewing properties 44
  - self-signed 35
  - signature, described 41
  - trusting partner's 72
- Certificates dialog box 42
- Change Admin Password dialog box 14
- Change Database Password dialog box 15
- Change Password dialog box 46
- Change System Password dialog box 16
- channels, described 64
- command toolbar, described 81
- communication services
  - disabling for partners 72
  - overview 24
  - prioritizing incoming 32
  - setting up incoming services 29
- Communication tab, Profile dialog box 27
- communications
  - in Partner Agreement Manager profile 24
  - inbound 156
  - outbound 156
  - See also* transmission services, incoming services
- configuring
  - the Adapter Server 85
  - Partner Agreement Manager for LDAP 132
  - Partner.properties file 135
  - the Proxy Server 142
- connection services. *See* communication services
- contact information, in Partner Agreement Manager profile 22, 23
- corporate information in company profile 21
- Create New User dialog box 47
- Create Self-signed Certificate dialog box 37
- cryptography algorithms. *See* algorithms

## D

- diagnostic monitoring system
  - described 57
  - enabling 57
  - monitored resources 58
- dialog boxes
  - Adapter Server Login 80
  - Archive Process Logs 118
  - Bind Certificate 42
  - Certificates 42
  - Change Admin Password 14
  - Change Database Password 15
  - Change Password 46
  - Change System Password 16
  - Create New User 47
  - Find Process Instance 108
  - Import/Export Manager 40, 52, 53, 121, 124
  - New Partner Wizard 67
  - Open Exported File 39, 51, 123
  - Process Server Login 11
  - Profile 21
  - Profile Acceptance Wizard 71
  - Profile Request 70
  - Restore Process Logs 120
  - Select File to Import 51
  - Service Properties 27
  - System Message 125
  - User Information 46
- dialup services
  - setting incoming properties 31
  - setting transmission properties 28
- DN (distinguished name) 132

## E

- edit access, described 45
- encryption certificates 41
- encryption certificates, described 41, 43
- encryption cryptography algorithms 34
- error messages, viewing 113
- errors, marking as resolved in the Auditor 114
- events, enabling polling 96
- Extension actions
  - starting and stopping adapters 98
  - updating adapter instance names 100

- External Data Port
  - function defined 154
  - role in using the Web Proxy 158

## F

- Find Process Instance dialog box 108
- firewall, using proxy with 153

## H

- HTTP and HTTPS connections to web server 155
- HTTP proxy 156
- HTTP proxy authentication. *See* outbound proxy

## I

- implementation declarations, relationship to adapter instances 94
- Import/Export Manager 40, 52, 53, 121, 124
- importing users 51
- importing, certificates 40
- inbound
  - messages 141
  - Proxy Server connections in active mode 145
  - Proxy Server connections in passive mode 146
- inbound communications 156
- incoming services
  - installing 29
  - prioritizing 32
  - setting Internet properties 31
- initLDAP batch utility 136
- installing
  - LDAP considerations before you install 132
  - Partner Agreement Manager for LDAP 132
- instances of Web Proxy 156
- integrated Proxy Broker 158
- Internal Data Port
  - function defined 154
  - setting for using the Web Proxy 158
- Internet services
  - described 24
  - setting incoming properties 31
  - setting transmission properties 28
  - transmission 24
- IP address, setting 159

- J
  - JNDI (Java Naming and Directory Interface) 133
- K
  - key exchange, cryptography algorithms 35
  - key fields
    - finding an instance of 107
    - searching on values 107
- L
  - LDAP
    - administrator user 130
    - before you install Partner Agreement Manager 132
    - configuring Partner Agreement Manager 132
    - described 130
    - directory tasks 130
    - DN 132
    - installing and configuring Partner Agreement Manager 132
    - retrieving user and partner information 130
    - setting up after you install Partner Agreement Manager 135
    - setting user permissions 137
    - storing the password in the MasterStore 136
    - user overview 130
    - using with Partner Agreement Manager 137
  - LDAP administrator 130
  - LDAP directory
    - described 130, 132
    - schema 133
  - linked certificates 35
  - linked certificates. *See* CA-issued certificates
  - listener services, Internet 25
- M
  - Make command 157
  - managing the Adapter Server on UNIX 89
  - mapping
    - Partner Agreement Manager information to LDAP 133
    - partner information for LDAP 134
    - user information for LDAP 134
  - maps, importing 40, 52, 53
  - MasterStore, storing the LDAP password 136
  - messages
    - extracting non-repudiation information 126
    - inbound 141
    - non-repudiation information 126
    - outbound 141
  - MQSeries
    - configuring Partner Agreement Manager 165
    - installing an incoming service 169
    - Service Properties dialog box 168
    - setting dialup service properties 171
    - setting incoming service properties 171
    - setting transmission properties 167
- N
  - New Partner Wizard 67
  - non-repudiation information, extracting 126
- O
  - Open Exported File dialog box 39, 51, 123
  - operating environment, for Partner Agreement Manager 8
  - outbound
    - communications 156
    - messages 141
    - Proxy Server connections in active mode 144
    - Proxy Server connections in passive mode 145
  - outbound proxy
    - authenticating 164
    - configuring 164
- P
  - PAM database, changing the password 14
  - Partner Agreement Manager
    - configuring for MQSeries 165
    - configuring to use outbound proxy 164
    - introducing 2
    - operating environment 8
    - overview of work flow 3, 4
    - schema 133
    - using with LDAP 137
  - Partner Agreement Manager client, changing passwords from 15
  - Partner Agreement Manager installer, role in LDAP 130

- Partner Agreement Manager profile
  - contents 20
  - setting security 35
  - setting up 20
  - setting up communications 24
- Partner Agreement Manager profiles
  - and partner setup 64
  - reviewing partner's 70
  - updating partner's 75
  - See also* security profile
- partner information, mapping from LDAP 134
- partner.properties
  - configuring 135
- Partner.properties, configuring 135
- PartnerLDAPMapper.properties file 133
- partners
  - accepting new 69
  - adding new 66
  - black and white icon 69
  - described 64
  - distributing updated information 75
  - new 66
  - setting up 66
  - setting up, described 65
  - updating information 75
  - verifying fingerprint 72
  - viewing new partner request 69
- passwords
  - admin, changing 14
  - system, changing 16
  - user, changing 46, 49
- path for Web Proxy install 157
- policy options
  - authentication 34
  - described 34
  - non-repudiation origin 34
  - non-repudiation receipt 34
  - privacy 34
- polling, diagnostic monitoring system 57
- port
  - Control Port 158
  - External Data Port 154, 158
  - Internal Data Port 154, 158
- ports for Web Proxy 155, 158
- private process status, viewing 112
- private processes
  - importing 40, 52, 53
  - starting and stopping adapters 98
  - updating adapter instance names 100
- Private Trace View, described 116
- Process Audit Trace window, described 115
- Process Audit window
  - described 110
  - opening 111
  - remote information 112
  - viewing private process status 112
- process information
  - described 106
  - in Process Audit window 111
  - viewing 109
- process logs
  - archiving 117
  - restoring from archive 120
- Process Server
  - changing passwords from 14
  - described 9
  - properties, described 13
  - starting 10, 11
  - stopping 16
  - window, described 12
- Process Server Login dialog box 11
- processes
  - auditing 104
  - Error status 107
  - finding an instance of 107
  - In Progress 106
  - viewing information about 109
- profile
  - accepting new partners 69
  - and partner exchange 65
  - distributing updated information 75
  - Profile Acceptance Wizard 71
- Profile dialog box
  - Certificates tab 41
  - General tab 21
  - Security tab 35
  - Services tab 27
- Profile Request dialog box 70

- properties
  - configuring for Proxy Broker 159
  - file 158
  - specifying values in adapter instances 96
- proxy
  - different types 154
  - HTTP 156
  - installing 156
- Proxy Broker function defined 154
- Proxy inbound connections in passive mode 146
- Proxy Server
  - about 140
  - active mode 142, 144
  - compiling 149
  - configuring 142
  - example network configuration 142
  - inbound and outbound messages 141
  - inbound connections in active mode 145
  - log file 151
  - maintaining 151
  - outbound connections in active mode 144
  - outbound connections in passive mode 145
  - passive mode 142, 145
  - running as NT service 150
  - sample configuration file 146
- proxy server settings
  - incoming services 32
  - transmission services 28
- public processes
  - archiving audit information 117
  - audit information, backup and restore 117
  - backing up audit archives 117
  - importing 40, 52, 53
  - restoring audit archives 117

## R

- read access, described 45
- remote audit information 112
- Restore Process Logs dialog box 120
- retrieving partner information, LDAP 130

## S

- schema, Partner Agreement Manager and LDAP 133
- security certificates. *See* certificates
- security profile
  - adding certificates 41
  - described 33
  - options, selecting 36
  - policy options, described 33
  - setting up 35
  - See also* algorithms, Partner Agreement Manager profile, certificates, policy options
- Security tab, Profile dialog box 35, 41
- Select File to Import dialog box 51
- Select Service Type dialog box 27
- self-signed certificates, described 35
- service types, setting properties 26
- setting user permissions for LDAP 137
- signature certificates 41
- signature certificates, described 41, 43
- signature cryptography algorithms 35
- SNMP Agent, described 61
- SSL connection 155, 156
- starting
  - the Adapter Server Administrator 80
  - the Adapter Server on Windows 83
  - monitoring 84
- status bar, described 82
- stopping
  - the Adapter Server on Windows 89
  - monitoring 84
- subprocesses, importing 40, 52, 53
- system audit information, deleting 126
- system information, described 105
- System Message dialog box 125
- system messages
  - described 105
  - viewing 124

## T

- testing the server connection 84
- third-party-signed certificates. *See* CA-issued certificates
- Trace window. *See* Process Audit Trace window
- transmission services
  - Internet 24
  - proxy server settings 28
  - setting dialup properties 28
  - setting Internet properties 28

## U

- User Information dialog box 46
- user information, mapping from LDAP 134
- user overview, LDAP 130
- user permissions, setting for LDAP 137
- user profile. *See* users
- UserLDAPMapper.properties file 133
- users
  - access levels 45
  - adding new 47
  - Admin user 45
  - assigning access 47
  - authenticating with LDAP 130
  - changing passwords 46, 49
  - deleting 48
  - editing information 49
  - importing 51, 52, 53
  - updating contact information 46

## W

- Web Proxy
  - function defined 153
  - installing 157
  - instances 156
  - running 158
- web server certificate 155
- Webproxy.zip 157
- Windows, installing the Web Proxy 157