iSoft®

iSoft Commerce Suite

Administration Guide

Document Edition 1.3
February 2003

Copyright

Restricted Rights Legend

Information in this document is subject to change without notice and does not represent a commitment on the part of iSoft Corporation. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, iSoft Corporation DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Trademarks or Service Marks

Contents

About This Document

1. Introduction to Commerce Suite

2. Starting and Stopping P2P Agent

3. Understanding Configuration and Work Order Files

4. Configuring Commerce Suite and Testing with iSoft

5. Configuring Commerce Suite for Load Balancing and Failover

6. Configuring Commerce Suite for Non-Database Remote Administration

7. Configuring Commerce Suite Database Remote Administration

8. Configuring Commerce Suite for Simple Database Connectivity

9. Configuring Commerce Suite for Inbound/Outbound MQSeries Interfacing

10.Server Administration

11.Trading Partner Administration

12.Certificate Administration

A. UNIX Configuration Information

B. Commerce Suite Firewall Configuration Considerations

C. Commerce Suite for OS/400 Reference

D. Commerce Suite for OS/390 Reference

E. IBM Federated Partner Profile Support

F. Commerce Suite Error Messages

Glossary

About This Document

This document introduces and outlines the iSoft Commerce Suite Commerce Suite features, services, and architecture.

- Chapter 1, “Introduction to Commerce Suite,” describes the Commerce Suite product and how it can benefit your business, introduces the command-line interface, and describes the Commerce Suite architecture.
- Chapter 2, “Starting and Stopping Commerce Suite,” describes how to start, stop, and check the status of the Commerce Suite application.
- Chapter 3, “Understanding Configuration and Workorder Files,” describes the `p2pagent.cfg` configuration file and the workorder (.wo) files that are loaded and read upon Commerce Suite application startup.
- Chapter 4, “Configuring Commerce Suite and Testing with iSoft,” describes how to install, configure, and test your Commerce Suite connectivity with iSoft.
- Chapter 5, “Configuring Commerce Suite for Load Balancing and Failover,” describes how to install and configure Commerce Suite router and transport agents for inbound load balancing and failover capabilities.
- Chapter 6, “Configuring Commerce Suite for Non-Database Remote Administration,” describes how to install and configure Commerce Suite router and transport agents for remote administration capabilities.
- Chapter 7, “Configuring Commerce Suite for Database Remote Administration,” describes how to install and configure Commerce

Suite router, transport, and admin agents for database remote configuration capabilities.

- Chapter 8, “Configuring Commerce Suite for Simple Database Connectivity,” describes how to configure Commerce Suite for use with a supported Relational Database Management System (RDBMS).
- Chapter 9, “Configuring Commerce Suite for Inbound/Outbound MQSeries Interfacing,” introduces the iSoft Commerce Suite for MQSeries(TM) (Commerce Suite/MQ) product and provides instructions for using existing Commerce Suite commands and new MQSeries-specific parameters to interface with the MQSeries product
- Chapter 10, “Server Administration,” describes how to define and manage servers using the Commerce Suite command line interface (CLI).
- Chapter 11, “Trading Partner Administration,” describes how to define and manage trading partners using the Commerce Suite command line interface (CLI).
- Chapter 12, “Certificate Administration,” describes how to define and manage certificates using the Commerce Suite command line interface (CLI).
- Appendix A, “UNIX Configuration Information,” describes how to run Commerce Suite in the background on a Linux server.
- Appendix B, “Commerce Suite Firewall Configuration Considerations,” provides the information needed to make the necessary firewall configuration changes to support communication with the Commerce Suite application.
- Appendix C, “Commerce Suite for OS/400 Reference,” explains how to install, configure, and use Commerce Suite for use with the OS/400 operating system.
- Appendix D, “Commerce Suite for OS/390 Reference,” explains how to install, configure, and use the Commerce Suite application for use with the OS/390 operating system.

- Appendix E, “IBM Federated Partner Profile Support,” explains how the Commerce Suite application interfaces with IBM Federated Partner profiles.
- Appendix F, “Commerce Suite Error Messages,” provides a description of error, informational, and warning messages that can be encountered while using the Commerce Suite software.
- Glossary, provides a listing of commonly used terms found in this document.

Audience

This document is intended primarily for use by iSoft Commerce Suite data administration personnel responsible for installation, configuration, maintenance, and use of the Commerce Suite system.

This document has been written with the assumption that iSoft Commerce Suite administrators and users have a general understanding of the following concepts and technologies:

- Your business application software and business practices
- Electronic Data Interchange over the Internet (EDI-INT)
- E-Commerce
- Uniform Code Council (UCC)
- Data types
- Transport protocols
- Security standards
- The Internet
- Windows operating systems
- UNIX operating system

How to Print the Document

You can open the PDF in Adobe Acrobat Reader and print the entire document (or a portion of it) in book format.

Adobe Acrobat Reader is available at no charge from the Adobe Web site at http://www.adobe.com.

Contacting iSoft

Refer to the following section for instructions on contacting various iSoft support departments.

For Customer Support

If you have any questions about this version of the iSoft Commerce Suite software, or if you have any problems installing and running iSoft Commerce Suite, contact iSoft Technical Support at **support@iSoft.com**.

When contacting Customer Support, be prepared to provide the following information:

- Your name, email address, phone number, and fax number.
- Your computer type, manufacturer, model, CPU, memory, disk space, and network environment.

- The name and version of the product you are using.
- A description of the problem and the content of any error messages.

If you are unable to resolve your problem, call us at 214-890-9988

For Sales Support

For Sales support, contact us at the following phone numbers and Email address:

- Phone: 214-890-9988
- Fax: 214-890-7686
- Email: **sales@iSoft.com**

For Documentation Support

Your feedback on the iSoft Commerce Suite documentation is important to us. Send us email at **docsupport@isoft.com** if you have questions or comments. Your comments will be reviewed directly by iSoft professionals who create and update the iSoft Commerce Suite documentation.

In your email message, please indicate that you are using the documentation for the iSoft Commerce Suite.

Documentation Conventions

The following documentation conventions are used throughout this document.

Convention	Meaning
bold	Names of fields, buttons, icons, and check boxes.
Italics	Words or phrases that you type. Options that you select.
{ }	Indicates a set of choices from which you must choose one.
`monospace text`	Code samples, commands and their options, directories, and file names and their extensions. Monospace text also indicates text that you enter from the keyboard.
`monospace italic text`	Variables in code Example: `String` *`Customername;`*
|	Separates two mutually exclusive choices in a syntax line. Type one of the choices, not the symbol.
parameters	Specifies a variable name or other information you must provide.
[ ]	Indicates optional parameters. You typically type only the information within the brackets, not the brackets.
...	Indicates that a parameter can be repeated several times in a command line. You enter only the information, not the ellipsis (...).

CHAPTER

1 Introduction to Commerce Suite

The following sections provide an overview of the Commerce Suite product.

- The Commerce Suite Solution
- The Commerce Suite Advantage
- Commerce Suite Architecture
- Commerce Suite Services Overview
- Understanding Commerce Suite Roles

The Commerce Suite Solution

Whether you are using private networks or the Internet, today's competitive business environment demands a secure and reliable solution for exchanging data between trading partners.

Building a successful Internet-based trading community requires a high performance, high availability e-business solution that enables businesses to connect simply and securely over public networks.

The iSoft Commerce Suite solution delivers the performance, scalability, reliability, and security necessary to manage your Internet-based trading community.

The iSoft Commerce Suite supports industry standards, enabling businesses to send and receive any type of data using multiple communication protocols and security models. Commerce Suite can be downloaded over the Internet and rapidly deployed to put your business in contact with it's trading partners.

The iSoft Commerce Suite enables your enterprise with the profile, communication, security, and rollout management necessary to ensure the integrity of your business partner relationships.

The iSoft Commerce Suite solution is certified by the Uniform Code Council (UCC) and is also in full compliance with the Internet Engineering Task Force (IETF) Electronic Data Interchange over the Internet (EDI-INT) specification.

Support for the EDI-INT specification ensures that EDI trading partners and user agents can use the Internet as a transport medium to conduct business between EDI systems and provide secure EDI over the Internet.

The Commerce Suite application provides your enterprise with the following business benefits:

- Supports multiple data types, transport protocols, and security standards.
- Supports a wide range of platforms.
- Utilizes high-performance technology to maximize throughput.
- Enables complete Privacy, Authentication, Integrity, and Non-Repudiation of all transactions.
- Supports certificates from all major security vendors and provides a Public Key Infrastructure (PKI) solution generating X.509 certificates.
- Offers high-availability failover and restart.

The Commerce Suite Advantage

iSoft Commerce Suite provides the required capabilities for managing the largest and smallest trading communities.

Supports the EDI-INT Specification

Full compliance with the Internet Engineering Task Force (IETF) Electronic Data Interchange over the Internet (EDI-INT) specification ensures that EDI trading partners and user agents can use the Internet as a transport medium to conduct business between EDI systems and provide secure EDI over the Internet.

Ensures Data Integrity and Confidentiality

Support for industry security standards ensures the integrity and confidentiality of data over the Internet or other public networks. iSoft's solution supports the creation and application of digital signatures and their verification to provide for non-repudiation of message origination and receipt.

Enables a High Performance, High Availability Trading Community

Commerce Suite utilizes high performance technologies to maximize throughput by implementing multi-threading and multi-tasking for scalable parallel processing. Support for data compression and platform-specific performance features enable you to fine tune options to optimize Commerce Suite compatibility with your network configuration.

Assure Reliable Trading Community Data Delivery

Commerce Suite assures reliable data delivery through session management and extensive recovery features and also provides automatic notification of transfer completion. These features, along with high-availability failover and restart capabilities enable load balancing between multiple computers ensuring data throughput.

Commerce Suite Architecture

The following sections discuss the principles of operation and the fundamental concepts underlying the Commerce Suite architecture.

- Multithreaded Execution
- Dynamic Scalability
- Failsafe Redundancy
- Data Asset Protection

Multithreaded Execution

To accomplish a broad variety of data-processing operations while maintaining an efficient and robust design, the major operations of the Commerce Suite application are executed as discrete services operating concurrently within a single process. For example, at any given moment, the Commerce Suite may be in the process of both receiving an inbound data stream and also preparing a file to be sent to a remote computer.

The integrity of each independent task being performed by the computer is essential. To protect each discrete operation and to more efficiently organize program logic, the Commerce Suite application executes its code in the context of multiple threads of execution within the overall application process. The operating system reserves time to execute each thread in a cooperative manner, switching between threads at regular intervals. Usually these thread-to-thread interruptions occur when a thread requests access to a system resource that would otherwise, in a single-threaded environment, impose a delay in processing due to media-access time. So, for example, while one thread is waiting for a disk or network event to complete, other threads may obtain CPU attention.

Commerce Suite Configuration

Prior to installation, configuration, and operation of the Commerce Suite application, careful consideration needs to be given to the quantity and characteristics of data to be interchanged between Internet hosts so that the Commerce Suite configuration will be optimal. To facilitate broad scalability in both processing and storage capacity, Commerce Suite operation is considered in terms of three basic roles that can be shared by a single process or divided among many cooperating host computers depending on resource requirements. The three basic roles are:

- Transport
- Router
- Admin (Administration)

Dynamic Scalability

One of the essential qualities of a real-time communications system is the ability to dynamically tune the performance of the system without requiring system down-time. A Commerce Suite configuration can be dynamically scaled by adding or removing Transport agents without shutting down any other agent in the configuration. When a new Transport agent is started and configured to participate in a Transport agent group, or pool, the Transport agent automatically notifies any Router or Admin agent on its local network segment of its presence by periodically sending a small Universal Datagram Protocol (UDP) packet.

Conversely, when a Transport agent is shut down, Router and Admin agent on the local network segment become aware of the removal of the Transport agent by detecting that UDP packets are no longer being transmitted by the Transport agent.

Failsafe Redundancy

Another essential quality of a robust software system is redundancy. A Commerce Suite configuration can be configured with multiple Router agents and multiple Admin agents in order to insure that the secure flow of business information is not interrupted, even if a Router or Admin agent is shut down. More than one Router agent can service the same Transport agent pool, since each inbound data connection is serviced by separate, dedicated threads in each agent. Likewise, more than one Admin agent can distribute data-transfers to the same pool of Transport agents.

Data Asset Protection

Data security is of prime importance for any business enterprise. The typical solution to avoid unauthorized access to computer systems connected to the Internet is the use of a firewall - hardware and software specifically designed to prevent certain network traffic. When one or more firewalls are used, it is critical that software systems avoid compromising the inherent security of the firewall by requiring that inbound connections be permitted through the firewall. To ensure firewall security, a Commerce Suite configuration option, known as Data Asset Protection (DAP), can be employed to guarantee that no Internet assailant can ever jeopardize the integrity of computing assets behind a firewall. To accomplish this, a Commerce Suite Enterprise Configuration employs one or more Admin agents to connect out from the inner Local Area Network (LAN) to the Transport agent pool to collect inbound data while it is still in its encrypted form. After the data is retrieved, the decryption of the data is accomplished within the secure inner LAN. In the Commerce Suite Enterprise Configuration with

DAP, the Transport agents may be equipped with two network interfaces each, ensuring that no sensitive data is exposed to a network segment that is publicly addressable.

When using DAP, the Admin agents do not listen for UDP notifications from the Transport agent pool. Instead, they remotely configure the Transport and Router agents themselves by connecting to a known set or IP addresses and sending configuration commands to setup and start each Transport and Router agent. Therefore, no configuration data need be present outside the secure inner LAN.

Commerce Suite Services Overview

Before configuring the Commerce Suite application, it is helpful to understand the operation of the various threads of execution that comprise the Commerce Suite process. A thread may be understood as a series of computer instructions executed within the context of a single machine state, that is, the set of internal registers managed by the computer's central processing unit (CPU). In a multi-threaded processing environment, such as UNIX or Windows NT, a single process may posses multiple independent threads executing machine instructions in various different parts of the program concurrently. The operating system divides its attention between threads by preemptively switching between machine states.

The Commerce Suite is written to take advantage of preemptive multitasking systems by devoting a thread to a particular purpose, such as listening for inbound connections or scanning for expiring certificates. Each of these threads may be thought of as providing an independent service.

The Commerce Suite process is divided into the following services:

- Console
- Serialization
- Control

- Outbound
- Inbound
- work order
- Beacon
- Router

Understanding the Console Service

The Console service performs the basic initialization, main logic loop, and finalization tasks for the application. This thread is the first application thread to be started by the operating system and the last thread to terminate when the application stops.

The initialization portion of this thread establishes communication with the underlying network communication layer. The main logic loop accepts operator input to manipulate application operation, manually initiate tasks, or initiate application termination. The finalization task gracefully terminates the application and releases allocated system resources. Operator access to the Console service is provided through the terminal at the host computer.

Understanding the Serialization Service

The Serialization service is started automatically during program initialization. This service manages access to file and memory resources that are shared between other threads. Although the Commerce Suite application operates as several independent threads, some resources such as disk files and common memory areas must be accessed by only one thread at a time. In order to ensure that each thread is able to complete its access to these shared resources before being interrupted by another thread, the Serialization service acts as a gatekeeper, allowing only one service to access shared resources at the same time.

Understanding the Control Service

The Control service actively listens for incoming connections on a TCP/IP port dedicated to receiving command messages from an Admin agent, that is, a Commerce Suite process configured for the Admin role. Admin agents regularly connect to Transport and Router agents to send configuration data and to receive status information and inbound data. These connections from the Admin agent are always made to the Transport or Router agent's Control port. By default, this port is the Internet Assigned Numbers Authority (IANA) -assigned Internet Protocol's Reserved Port for the isoft-p2p service (port 3501). However, alternate ports may be configured for this purpose. Note that an Admin agent always initiates control service connections. Transport and Router agents never connect directly to Admin agents. This design is to allow the Transport and Router agents to be located in relatively less secure network locations, such as DMZ's, whereas the Admin agent and associated databases could be located in a more secure location protected by a firewall disallowing inbound connections.

Understanding the Outbound Service

The Outbound service is responsible for preparing data for transmission, initiating and supervising the transmission of data to other computers, recording the result of the transmission, and rescheduling the transmission in the case of errors or as user preferences require. The Outbound service polls an outbound queue for outgoing data and creates session threads for each individual outbound send operation.

The outbound queue is a list of transactions that carry addressing and status information about the data to be sent. Two types of send operations are found on the outbound queue: single-send operations and recurring-send operations. The single-send operation is simply a send of a file from one location to another. The recurring-send operation represents any iterative event, typically either a periodic send (for example, a weekly status report) or a drop-box configuration wherein an outbox location is continuously scanned for outgoing data. Both single-send and recurring-send operations can be configured with retry parameters to handle the situation where a send operation fails.

Any send can be configured to be retried a configurable number of times at a configurable interval. When combined with the Router services ability to buffer and spool incoming data to a pool of Transport agents, both sending and receiving locations share in the responsibility of reliably transmitting data.

In a configuration where several Transport agents are receiving inbound data, the Admin agent will typically be the primary sending agent. In configurations that do not require an Admin agent, the Transport agent(s) may both send and receive data.

Understanding the Inbound Service

The Inbound service is responsible for receiving data being sent to the host computer, either directly from a remote host or from a Router agent, preparing and sending suitable responses or receipts to the sending host, properly terminating the inbound connection, delivering the received data to the proper location or service, and recording the result of the inbound operation. In fact, more than one distinct inbound service may be in operation at any given moment. Each instance of the inbound service is tailored to a specific network messaging protocol (for example, HTTP or HTTPS) and is assigned to a specific Internet protocol address and port on which to listen for incoming connections. Moreover, each Inbound Service instantiates an Inbound Session Thread for each concurrent inbound operation, isolating each independent inbound connection.

Understanding the Out-Beacon Service

Commerce Suite processes acting in the Transport role use the Beacon service. The Beacon service periodically emits a small packet of information using UDP. This packet is broadcast to the local network segment, informing any Router agent of the Transport’s existence on the network. Using this mechanism to advertise the Transport’s existence to the Router permits the Router to operate without explicit information of the Transports beforehand and the ad hoc addition or removal of Transport agents without having to reconfigure the Router. The packets of data broadcast by the Beacon service include the TCP/IP addresses and ports that the Transport agent is listening on for incoming data. The Router agent collects these addresses and ports into a dynamic list of servers to which incoming data can be sent to provide load-balancing. The packets also contain other information about the Transport including a routing group number to permit the configuration of several distinct load-balancing server groups on the same local network or the establishment of a hierarchical load-balancing configuration.

Understanding the Router Service

The Router service uses two or more threads of execution. First, one thread listens for incoming UDP broadcast packets from Transport agents advertising their presence to the Router agent. This thread collects the broadcast packets and maintains a linked-list of Transport agent records, which indicate which TCP/IP address should be connected-to when forwarding incoming data. Additionally, an inbound thread listens for incoming data for a particular Internet Protocol (HTTP or HTTPS). This thread is the first to receive incoming data from a remote host when the Router role is used in a multi-server configuration. This inbound thread logic differs from the Transport agent's inbound logic. The Router service does not expect to parse or decrypt incoming data. Therefore, the Router agent does not make assumptions or decisions relating to the processing of data based on the contents of the data.

The Router service is responsible, however, for ensuring that all data received from a remote host is delivered to a Transport agent for processing. To make this happen, the Router service queues incoming data while also forwarding it to a Transport agent. If the connection to the Transport agent is interrupted, the Router service will temporarily suspend receiving data from the remote host while it establishes a new connection to another Transport agent and forwards to it all data as yet received from the remote host. When all data is forwarded successfully, the Router will again attempt to receive more data from the remote host. The Router service does not disconnect from either the remote host or the Transport agent until one of the connections is terminated by the owning processes.

Under normal circumstances, each Router session will:

- Forward all incoming data from the remote host connection to the Transport agent.
- Forward all response data from the Transport agent to the remote host.
- Detect that the Transport agent has closed an inboard connection.
- Close the connection to the remote host.

Understanding Commerce Suite Roles

Commerce Suite operation is considered in terms of three basic roles, which can be shared by a single process, or divided among many cooperating host computers depending on resource requirements. The three basic roles are Transport, Router, and Administration.

Understanding the Transport Role

The Transport role combines the most fundamental operations of Commerce Suite: compression and decompression, encryption and decryption, digital signing and signature verification, and sending and receiving data.

With the decryption and signing operations being the most mathematically intensive operations performed by the Transport role, if large numbers of digitally signed and encrypted messages need to be sent between computers, it is recommended that the Transport role be divided across several processors to enhance throughput.

Understanding the Router Role

The Router role provides software-based load sharing between multiple computers providing the Transport role. The Router provides a single point of entry for data of a given Internet protocol that can then be distributed to one or many Transport agents for processing. The Router balances incoming data across a pool of Transport agents. The Router also provides a fail-safe mechanism against the eventuality of a Transport failure by buffering incoming data until an entire message can be safely delivered to a Transport agent.

Understanding the Admin Role

The Admin role provides several important services in a Commerce Suite configuration. One of these services is outbound distribution. This is the logical reverse of inbound load balancing performed by the Router. The Admin agent facilitates outbound load balancing by distributing the data-sending workload among a group of transport agents in the same way that the Router agent distributed inbound data-receiving workloads.

The Admin role also provides a Web-based user interface to support the definition and maintenance of data-interchange relationships. In the electronic commerce industry, such defined interchanges are often referred to as trading partner relationships. Such a relationship defines the Internet address of the participating computers, message delivery options, and data-security parameters such as the certificates to be used for signature creation and key-encryption. The Admin agent also is responsible for configuring the Transport and Router agents and for replicating configuration updates to these roles if they are being hosted on separate processors.

2 Starting and Stopping P2P Agent

This section describes how to use the iSoft P2P Agent command line interface (CLI) to start and stop the P2P Agent as well as check application status. The CLI is a simple text mode utility that provides a command line interface to the P2P Agent.

The command line interface provides a mechanism to manipulate application operation, manually initiate tasks, and initiate application startup and termination. Operator access to the P2P Agent command line interface is provided through the terminal at the host computer.

Starting the P2P Agent Application

Although it is not necessary to execute P2P Agent prior to setting up its configuration, you may run the program prior to its configuration to ensure that the P2P Agent executable has not been damaged or digitally altered.

Note: To demonstrate how to start and stop the P2P Agent application, this document will assume a Microsoft Windows operating system platform with a base directory named `c:\isoft\p2pagent`.

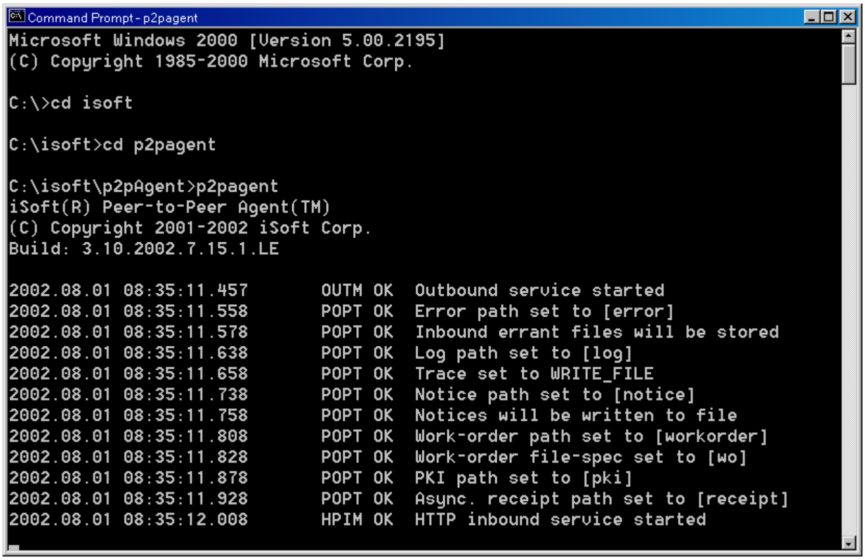
Perform the following steps to start the Commerce Suite application:

1. Open a command prompt console window.
2. Change your directory to the `c:\isoft\p2pagent` directory.

3. Type `p2pagent` and press Enter to execute and start the Commerce Suite application.

```
c:\isoft\p2pagent\p2pagent
```

Once the program properly initializes, a console window appears displaying the following information:



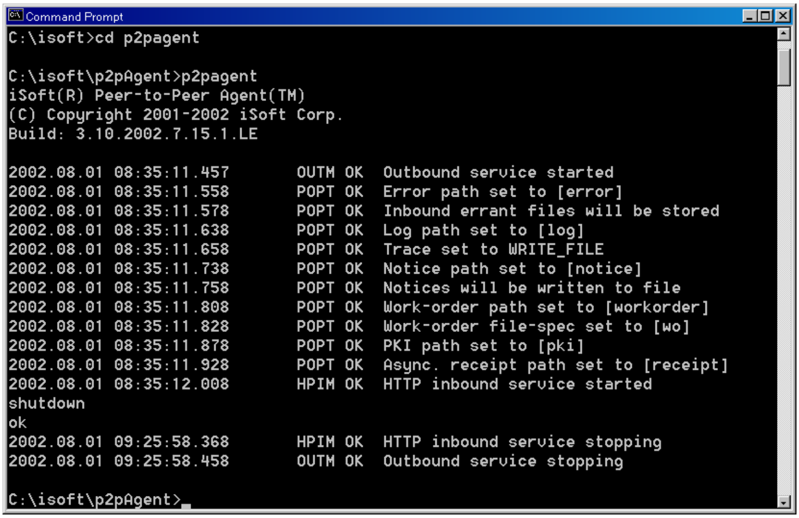
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd isoft

C:\isoft>cd p2pagent

C:\isoft\p2pAgent>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1.LE

2002.08.01 08:35:11.457       OUTM OK  Outbound service started
2002.08.01 08:35:11.558       POPT OK  Error path set to [error]
2002.08.01 08:35:11.578       POPT OK  Inbound errant files will be stored
2002.08.01 08:35:11.638       POPT OK  Log path set to [log]
2002.08.01 08:35:11.658       POPT OK  Trace set to WRITE_FILE
2002.08.01 08:35:11.738       POPT OK  Notice path set to [notice]
2002.08.01 08:35:11.758       POPT OK  Notices will be written to file
2002.08.01 08:35:11.808       POPT OK  Work-order path set to [workorder]
2002.08.01 08:35:11.828       POPT OK  Work-order file-spec set to [wo]
2002.08.01 08:35:11.878       POPT OK  PKI path set to [pki]
2002.08.01 08:35:11.928       POPT OK  Async. receipt path set to [receipt]
2002.08.01 08:35:12.008       HPIM OK  HTTP inbound service started
```

Once the program properly completes its initialization tasks, a blinking cursor appears below the title message. The P2P Agent application is now ready to accept commands from the local console.

Although the P2P Agent application can accept console command at any time, it may be more desirable to have P2P Agent read configuration commands from a configuration file. It is also possible to enter configuration commands as command-line arguments when the application is started.

Stopping the P2P Agent Application

To stop the P2P Agent application process, enter `shutdown` in the P2P Agent console window. The `shutdown` command gracefully terminates any operating thread within the process and then terminates the process itself. The following type of information displays.

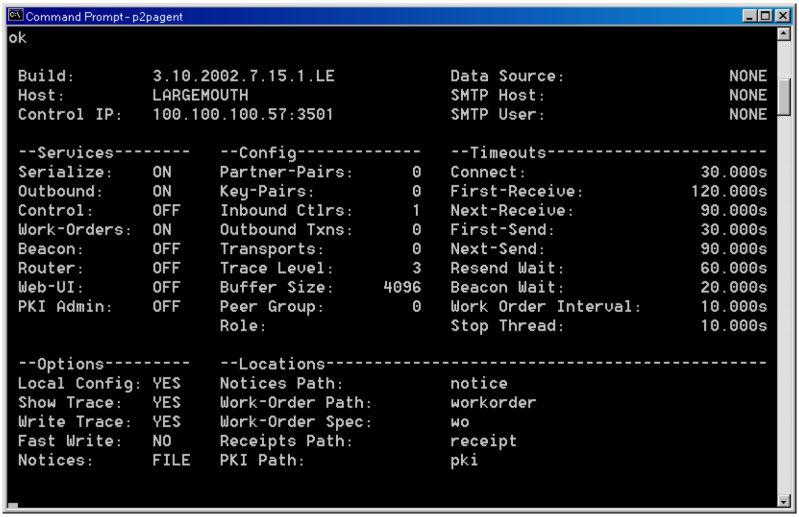


```
C:\isoft>cd p2pagent

C:\isoft\p2pAgent>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1.LE

2002.08.01 08:35:11.457       OUTM OK  Outbound service started
2002.08.01 08:35:11.558       POPT OK  Error path set to [error]
2002.08.01 08:35:11.578       POPT OK  Inbound errant files will be stored
2002.08.01 08:35:11.638       POPT OK  Log path set to [log]
2002.08.01 08:35:11.658       POPT OK  Trace set to WRITE_FILE
2002.08.01 08:35:11.738       POPT OK  Notice path set to [notice]
2002.08.01 08:35:11.758       POPT OK  Notices will be written to file
2002.08.01 08:35:11.808       POPT OK  Work-order path set to [workorder]
2002.08.01 08:35:11.828       POPT OK  Work-order file-spec set to [wo]
2002.08.01 08:35:11.878       POPT OK  PKI path set to [pki]
2002.08.01 08:35:11.928       POPT OK  Async. receipt path set to [receipt]
2002.08.01 08:35:12.008       HPIM OK  HTTP inbound service started
shutdown
ok
2002.08.01 09:25:58.368       HPIM OK  HTTP inbound service stopping
2002.08.01 09:25:58.458       OUTM OK  Outbound service stopping

C:\isoft\p2pAgent>_
```

Note that depending on the number of active threads, several seconds may elapse before the application terminates completely.

Checking P2P Agent Status

At any time during the execution of the application, the current general status of the application can be displayed at the host-computer's console by entering the `status` command. The application will display several lines of information representing the status of the application.



```
ok

 Build:        3.10.2002.7.15.1.LE          Data Source:                NONE
 Host:         LARGEMOUTH                   SMTP Host:                  NONE
 Control IP:   100.100.100.57:3501          SMTP User:                  NONE

 --Services--------    --Config------------   --Timeouts----------------------
 Serialize:    ON      Partner-Pairs:      0  Connect:                 30.000s
 Outbound:     ON      Key-Pairs:          0  First-Receive:          120.000s
 Control:      OFF     Inbound Ctlrs:      1  Next-Receive:            90.000s
 Work-Orders:  ON      Outbound Txns:      0  First-Send:              30.000s
 Beacon:       OFF     Transports:         0  Next-Send:               90.000s
 Router:       OFF     Trace Level:        3  Resend Wait:             60.000s
 Web-UI:       OFF     Buffer Size:     4096  Beacon Wait:             20.000s
 PKI Admin:    OFF     Peer Group:         0  Work Order Interval:     10.000s
                       Role:                  Stop Thread:             10.000s

 --Options---------    --Locations-------------------------------------------
 Local Config: YES     Notices Path:          notice
 Show Trace:   YES     Work-Order Path:       workorder
 Write Trace:  YES     Work-Order Spec:       wo
 Fast Write:   NO      Receipts Path:         receipt
 Notices:      FILE    PKI Path:              pki
```

CHAPTER

3 Understanding Configuration and Work Order Files

Configuring the Commerce Suite application is accomplished in several ways, through console commands, local configuration files, or by a remote Administrative Agent. The following section describe the `p2pagent.cfg` configuration file and the work order (.wo) files that are loaded and read upon Commerce Suite application startup.

- What is the p2pagent.cfg File?
- What are Work Order Files?

What is the p2pagent.cfg File?

The `p2pagent.cfg` file is a text file containing configuration commands that are loaded and read each time the application is started. This configuration file contains commands that enable a Commerce Suite instance to act as either a Transport, Router, or Administrative Agent. This file also contains trading partner information specifying inbound and outbound definitions, certificate assignments, and commands to invoke trading partners listeners on IP addresses and ports.

The `p2pagent.cfg` file is a text file using an XML command structure. As such, all configuration files must begin with a beginning xml tag (`<xml>`) and end with an xml tag (`</xml>`). Please note that it is not necessary to include a new-line or carriage-return and line-feed combination between commands. The `p2pagent.cfg` file is created using the following command categories:

- **Set**: updates the server variable
- **Addpair**: defines a new trading partner relationship
- **Importkey**: assigns certificates to be used for trading partner relationships
- **Start**: starts an inbound controller or service

The following code is a sample configuration file showing the four command categories being utilized.

Listing 3-1 Sample p2pagent.cfg Configuration File

```
<xml>
#
#    define transport for company “you”
#
<command>set -ca24.141.17.210 -cp3501 -gt -gp1 -nf -npnotice -
opworkorder -oswo -pppki -rpreceipt</command>
#
#    define transport for company “QA_a”
#
<command>addpair QA_b QA_a http://24.141.17.210:400080
http://24.141.17.13:40081 suser@myip.com inbox</command>
<command>addpair QA_a QA_b http://24.141.17.13:40081
http://24.141.17.210:40080 suser@myip.com inbox</command>
<command>importkey QA_b QA_a E -fCpki\devel.cer -
fKpki\test.prv</command>
<command>importkey QA_b QA_a J -fCpki\test.cer</command>
<command>importkey QA_a QA_b E -fCpki\devel.cer -
fKpki\test.prv</command>
<command>importkey QA_a QA_b J -fCpki\test.cer</command>
#
#    start services
#
<command>start http://24.141.17.210:8081</command>
<command>start http://24.141.17.210:40080</command>
</xml>
```

Editing the p2pagent.cfg File

iSoft recommends that you use a standard Windows text editor, such as Notepad or Wordpad to modify the `p2pagent.cfg` file.

Rules for Editing the p2pagent.cfg File

Consider the following issues before you edit the configuration file:

1. Always save your `p2pagent.cfg` file before editing it.
2. If you manually edit the configuration file while the Commerce Suite application is active, any changes you make will not be active until you restart the application. Furthermore, any changes made through console commands will not be made permanent unless they are added to the `p2pagent.cfg` file.
3. No validation or value checking occurs while you are editing the `p2pagent.cfg` file. Any errors detected will be displayed on the console as the application starts-up.

What are Work Order Files?

Work order files are XML-formatted text files containing valid Commerce Suite commands like those found in the `p2pagent.cfg` file. Work order files end with a `.wo` extension to designate them as work order files. A work order file provides an easy method for storing single or multiple commands used to process work.

The following example shows the contents of a sample work order file, `SendFile.wo`.

Listing 3-2 Sample SendFile.wo Workorder File

```
<xml>
<command>send http CompanyA CompanyB -fNtest.txt -n1</command>
</xml>
```

Commands listed in a work order file may be submitted to the Commerce Suite command queue in the following ways:

- Work order files can be opened and executed using the Commerce Suite `batch` command.

  For example: `batch testsend.wo`

- The `p2pagent.cfg` file can be edited so that the Commerce Suite will monitor a directory for the presence of work order files upon startup. When Commerce Suite detects a work order file, it places the workorder file in the Commerce Suite command queue.

  For example, the following entry in a `p2pagent.cfg` file will setup a work order directory that the Commerce Suite monitors for files having a .wo extension:

  ```
   <command>set -opworkorder -oswo</command>
  ```

CHAPTER

4 Configuring Commerce Suite and Testing with iSoft

This chapter describes how to install, configure, and test your Commerce Suite connectivity with iSoft.

This section contains the following sections:

- Performing a Basic Commerce Suite Configuration
- Conducting Connectivity Testing with iSoft

Performing a Basic Commerce Suite Configuration

This section describes the steps necessary to configure the Commerce Suite application as a stand-alone Transport agent using a configuration file that will be read by the application upon startup.

Perform the following steps to configure your Commerce Suite:

1. Create an iSoft directory on your local file system and copy the iSoft ZIP file you received into that directory.

2. Unzip the file and extract the iSoft Commerce Suite software files into the iSoft directory. The following files should be present after unzipping the file:

   - `Buildcfg.exe`
   - `ISOFTAS2TEST.CER`
   - `p2pagent.exe`
   - `Test.txt`
   - `Readme.txt`
   - `RelNotes.pdf`
   - `GetStart.pdf`
   - `Admin.pdf`

3. Start the Buildcfg application located in the iSoft root directory you created. This utility prompts you for the variables needed to create your initial configuration file.

   a. Select the platform type that Commerce Suite will run on. Your two options are:

      - Windows-based
      - UNIX or Linux-based

   b. Enter the Test AS2 Name you want associated with your business. This AS2 Name can be your business name, or any name that is meaningful to you. This AS2 Name value is a case-sensitive alphanumeric string with no spaces allowed. It should be descriptive and must be unique between the trading partners. (Example: ABCcompany)

   c. Specify your external address type. Your two options are:

      - IP Address
      - A DNS resolvable URL

      This external address is the Internet address to which trading partners send messages. If you are behind a firewall, your external address could be the firewall IP address. You need to understand your firewall configuration to correctly identify the external address. (Example: 127.0.0.1)

d. Enter your external address, either your IP address or DNS resolvable name.

e. Enter your external port number. The external port number is a specific communications end-point to a logical connection. Your trading partners will use this port when configuring for a AS2 connection to your server. (Example: 5080)

f. Specify your internal address type. Your two options are:

   - IP Address
   - A DNS resolvable URL

   The internal address is the physical address of the actual machine where the Commerce Suite application is installed and running. (Example: 127.0.0.1)

g. Enter your internal port number. (For example:5080)

h. Specify your notification address type. Your three options are:

   - IP Address
   - A DNS resolvable URL
   - Email address

i. Enter your notification address based on the address-type you specified in the previous step. The notification name will be used in sending asynchronous receipts.

j. Enter a certificate name that will be used for iSoft testing. This name should be a descriptive name indicating the trading partner relationship for which it was created. (For example: *yourname-iSoft*) This name is used to designate both the public and private certificate files created by the Buildcfg utility.

   Note: Only enter the descriptive file name. Do not include a file extension. The Buildcfg utility automatically adds `.cer` and `.prv` extensions to your entered file name when creating the two key pair files.

k. Enter a certificate name that will be used for Wal-Mart testing. This name should be a descriptive name indicating the trading partner relationship for which it was created. (For example: *yourname-walmart*) This name is used to designate both the public and private certificate files created by the Buildcfg utility.

Note: Only enter the descriptive file name. Do not include a file extension. The Buildcfg utility automatically adds `.cer` and `.prv` extensions to your entered file name when creating the two key pair files.

The following inputs are used to create descriptive information contained in the certificate.

l. Enter your two-letter state code.

m. Enter your city. Do not use any spaces between letters.

n. Enter your organization name. Do not use any spaces between letters.

Once you have entered your data using the Buildcfg utility, the application does the following:

- Creates an initial `p2pagent.cfg` file containing your enterprise-specific values.
- Creates the following required subdirectories for testing with iSoft. If the Buildcfg utility does not create these directories, you can create them manually.
  - `/error`
  - `/log`
  - `/notice`
  - `/pki`
  - `/receipt`
  - `/inbox`
  - `/inbox/`***`Name`***
  - `/inbox/0892548us00`
  - `/outbox/isoft`
  - `/workorder`

- Creates the following work order files required to support key generation and testing with iSoft:
    - `addkey1.wo`
    - `addkey2.wo`
    - `exportkey1.wo`
    - `exportkey2.wo`
    - `Test1.wo`
    - `Test2.wo`
    - `Test3.wo`
    - `Test4.wo`
    - `Test5.wo`
    - `isoft.wo`
    - `walmart.wo`

4. Open the `p2pagent.cfg` configuration file located in the `iSoft` root directory you created. The configuration file should contain the following text with items in bold replaced by the data you entered in the Buildcfg utility:

Listing 4-1 Sample p2pagent.cfg File

```
<xml>

#      configuration settings
<command>set -eperror -ef</command>
<command>set -lplog -lf</command>
<command>set -npnotice -nf-</command>
<command>set -opworkorder -oswo</command>
<command>set -pppki</command>
<command>set -rpreceipt</command>
<command>set -tr300s</command>

#      iSoft Testing
<command>addpair MyName ISOFTAS2TEST http://63.140.159.17:6080/
http://127.0.0.1:5080/ MyName inbox </command>

<command>addpair ISOFTAS2TEST MyName http://127.0.0.1:5080/   *
ISOFTAS2TEST inbox </command>
```

```
#      iSoft certificates and keys
<command>importkey MyName ISOFTAS2TEST E -fCpki/MyName-iSoft.cer
-fKpki/MyName-iSoft.prv</command>

<command>importkey MyName ISOFTAS2TEST J
-fCpki/ISOFTAS2TEST.cer</command>

<command>importkey ISOFTAS2TEST MyName E -fCpki/MyName-iSoft.cer
-fKpki/MyName-iSoft.prv</command>

<command>importkey ISOFTAS2TEST MyName J
-fCpki/ISOFTAS2TEST.cer</command>

#
#      Wal-Mart
<command>addpair MyName 08925485US00 http://161.165.202.30:5080/
http://127.0.0.1:5080/ MyName inbox/08925485US00</command>

<command>addpair 08925485US00 MyName http://127.0.0.1:5080/    *
08925485US00 inbox/08925485US00</command>
#

#      Wal-Mart certificates and keys
<command>importkey MyName 08925485US00 E -fCpki/MyName-Walmart.cer
-fKpki/MyName-Walmart.prv</command>

<command>importkey MyName 08925485US00 J
-fCpki/??Wal-Mart.cer{/command>

<command>importkey 08925485US00 MyName E -fCpki/MyName-Walmart.cer
-fKpki/MyName-Walmart.prv</command>

<command>importkey 08925485US00 MyName J
-fCpki/??Wal-Mart.cer{/command>

#
#      start services
<command>start http://127.0.0.1:5080/</command>

#
</xml>
```

Note: You will see initial errors on loading keys that have not been created. This is acceptable as you will create a certificate and private-key later in this procedure.

5. Start the Commerce Suite application and monitor your console output for any start-up error messages. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

6. Enter the `listpairs` command in the console. Output similar to the following example displays.

```
listpairs
ok

#         From       To        URL
0          Srvr1       Srvr2      www.myurl.com
```

7. Enter the `listinbound` command in the console. This command displays information about the address and ports listening for inbound connections. The following output displays.

```
ok
127.0.0.1:6080     HTTP
1 inbound controller(s)
```

Note: Enter the following console commands using the `batch` command. The `batch` command processes the specified work order file containing one or more console commands.

8. Create a self-signed X.509V3 certificate for iSoft testing. The associated Public/Private key pair is created in memory by entering the following command:

```
batch addkeys.wo
```

The `batch addkeys.wo` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing. This batch file enters the following command in the command queue for you.

```
addkeys Name ISOFTAS2TEST O 1024 self
C=US;S=TX;L=Dallas;O=iSoft;CN=Name
```

Note: Any work order (.wo) text file can be viewed using Notepad.

a. Export the generated keys into two files in the `iSoft` root directory by entering the following command:

```
batch exportkeys.wo
```

This batch work order file enters the following command in the command queue for you.

```
exportkeys Name ISOFTAS2TEST CertName.cer CertName.prv
```

9. Create a self-signed X.509V3 certificate for Wal-Mart testing. The associated Public/Private key pair is created in memory by entering the following command:

   ```
   batch addkeys.wo
   ```

   The `batch addkeys.wo` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing. This batch file enters the following command in the command queue for you.

   ```
   addkeys Name 0892548us00 O 1024 self
   C=US;S=TX;L=Dallas;O=iSoft;CN=Name
   ```

   a. Export the generated keys into two files in the `iSoft` root directory by entering the following command:

   ```
   batch exportkeys.wo
   ```

   This batch work order file enters the following command in the command queue for you.

   ```
   exportkeys Name 0892548us00 CertName.cer CertName.prv
   ```

10. Move all four created `.cer` and `.prv` key files from the `iSoft` root directory into the `/pki` subdirectory.

11. Move the `ISOFTAS2TEST.cer` key file from the `isoft` root directory into the `/pki` subdirectory.

12. Check the `/pki` subdirectory to verify that is has five files.

13. Exit the Commerce Suite application by entering the `shutdown` command at the console prompt.

    Once you have successfully completed configuring Commerce Suite, you are ready to begin testing your connectivity and ability to send and receive files. Refer to the following section for instructions on conducting connectivity testing with iSoft.

Conducting Connectivity Testing with iSoft

Perform the following steps to contact, schedule, and conduct connectivity testing with iSoft:

1. Send an email to iSoft Testing Support at **as2test@isoft.com** to request your iSoft trading partner configuration be tested. Ensure your email contains the following information and contents:

   a. Format the Subject line as follows: ***Company Name*:AS2 Testing Request**

   b. Include all your contact information:

      - Company Name
      - Primary Contact Name, E-mail address, and phone numbers
      - Secondary Contact Name, E-mail address, and phone numbers
      - Platform type

   c. Attach a copy of your `SendtoiSoftServer.cfg` file.

   d. Attach a copy of your public key file (*`CertName`*`.cer`) for use in the iSoft connectivity tests.

Do not send your `.prv` file to your trading partner. This is your private key file and should not be shared with anyone.

   Upon receiving your testing request, iSoft Testing Support will contact you to schedule the iSoft connectivity testing.

2. iSoft testing personnel will contact you by phone at the scheduled time of your testing to start your connectivity test.

3. Start the Commerce Suite application on your local machine.

Note: You will receive key import errors upon application startup. This is normal and does not necessarily indicate an application problem. This will continue until you receive the Wal-Mart `.cer` file.

4. Set the messaging level to INFO by entering the following command:

   ```
   set -m3
   ```

   This message level will display errors, warnings, and general information messages. These messages are written to the log.

   Note: This log file can be found in the `/log` folder created during installation. The log file uses the following naming convention: `P2P`*`YYYYMMDD`*`.log`. For example `P2P20020904.log`

5. iSoft Testing Support initiates testing by sending a series of files to your system that test the following iSoft functionality:

   - Connectivity
   - Receipts
   - Digital Signatures
   - Encryption
   - Compression

6. After receiving files from the iSoft server, you will continue testing by executing a series of work order files. These contain Commerce Suite commands that will send files to the iSoft server. The files you send will also test the same functionality iSoft tested in the previous step.

Note: Enter the following console commands using the `batch` command. The `batch` command processes the specified work order file containing one or more console commands.

7. Send an EDI-formatted file by entering the following command at the console prompt:

   ```
   batch Test1.wo
   ```

   The `Test1.wo` file contains the following command:

   ```
   send http Name ISOFTAS2TEST  -fNtest.txt -n1
   ```

   Monitor your console for output similar to the following sample:

Listing 4-2 Test1.wo Console Output

```
batch test1.wo
ok
2002.11.26 23:50:37.085 45754 HPOS OK  Outbound session started -
attempt=[1 of 1]

2002.11.26 23:50:37.105 45754 HPOS OK  Mailbox=[0]  Batch=[0]

2002.11.26 23:50:37.235 45754 HPOS OK  Outbound session stopping -
batch=[0]
```

8. Resend the same EDI-formatted file and request a receipt by entering the following command at the console prompt:

   `batch Test2.wo`

   The `Test2.wo` file contains the following command:

   send http **Name** ISOFTAS2TEST -fNtest.txt -nl -r

   Monitor your console for output similar to the following sample:

Listing 4-3 Test2.wo Console Output

```
batch test2.wo
ok
2002.11.26 23:55:34.542 61612 HPOS OK  Outbound session started -
attempt=[1 of 1]

2002.11.26 23:55:34.562 61612 HPOS OK  Mailbox=[0]  Batch=[0]

2002.11.26 23:55:34.733 61612 HPOS OK  Outbound session stopping -
batch=[0]
```

9. Resend the same EDI-formatted file with a digital signature by entering the following command at the console prompt:

   `batch Test3.wo`

   The `Test3.wo` file contains the following command:

   `send http Name ISOFTAS2TEST -fNtest.txt -n1 -sC -r1`

Monitor your console for output similar to the following sample:

Listing 4-4 Test3.wo Console Output

```
batch test3.wo
ok
2002.11.26 23:57:30.689 29938 HPOS OK  Outbound session started -
attempt=[1 of 1]

2002.11.26 23:57:30.709 29938 HPOS OK  Mailbox=[0]  Batch=[0]

2002.11.26 23:57:31.751 29938 VRFY OK  ** Signature verified **

2002.11.26 23:57:31.771 29938 PMDN OK  ** Original-Content-MIC
found in MDN **

2002.11.26 23:57:31.811 29938 HPOS OK  Outbound session stopping -
batch=[0]
```

10. Resend the same EDI-formatted file encrypted by entering the following command at the console prompt:

    ```
    batch Test4.wo
    ```

    The `Test4.wo` file contains the following command:

    ```
    send http Name ISOFTAS2TEST -fNtest.txt -n1 -sC -e -r1
    ```

    Monitor your console for output similar to the following sample:

Listing 4-5 Test4.wo Console Output

```
batch test4.wo
ok
2002.11.26 23:58:24.627 40044 HPOS OK  Outbound session started -
attempt=[1 of 1]

2002.11.26 23:58:24.647 40044 HPOS OK  Mailbox=[0]  Batch=[0]

2002.11.26 23:58:26.149 40044 VRFY OK  ** Signature verified **

2002.11.26 23:58:26.169 40044 PMDN OK  ** Original-Content-MIC
found in MDN **
```

```
2002.11.26 23:58:26.199 40044 HPOS OK  Outbound session stopping -
batch=[0]
```

11. Resend the same EDI-formatted file with compression by entering the following command at the console prompt:

    ```
    batch Test5.wo
    ```

    The `Test5.wo` file contains the following command:

    ```
    send http Name ISOFTAS2TEST -fNtest.txt -n1 -oZ -sC -e -r1
    ```

    Monitor your console for output similar to the following sample:

Listing 4-6 Test5.wo Console Output

```
batch test5.wo
ok
2002.11.26 23:59:17.052 53270 HPOS OK  Outbound session started -
attempt=[1 of 1]

2002.11.26 23:59:17.072 53270 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.26 23:59:18.454 53270 VRFY OK  ** Signature verified **
2002.11.26 23:59:18.474 53270 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.26 23:59:18.504 53270 HPOS OK  Outbound session stopping -
batch=[0]
```

12. The Buildcfg utility provides the commands necessary to create an automatic `outbox`. This outbox will send any file placed in it with an `.out` extension to the iSoft Test Server. Create the outbox by entering the following command at the command prompt:

    ```
    batch isoft.wo
    ```

    The `isoft.wo` file contains the following command:

    ```
    <xml>
    #
    #   start iSoft outbox
    <command> send http Test ISOFTAS2TEST -fPoutbox/isoft -fSout
    -fE.sent -tC30s -tE20031231000000 -sC -e -r1</command>
    </xml>
    ```

To test this outbox functionality for iSoft, perform the following steps:

a. Create a copy of the `test.txt` file in the `iSoft` root directory.

b. Rename the file to `test.out` and place it in the `outbox/iSoft` directory.

c. Monitor your Commerce Suite console output for the file to be sent. You should see some console output once the 30 second time interval listed in the `p2pagent.cfg` file has expired.

d. The `test.out` file will be renamed as `test.out.sent`.

13. To configure Commerce Suite for the same outbox upon startup, cut and paste the contents of the `isoft.wo` file in to your `p2pagent.cfg` file. Place the new text before the *`start services`* section and above the ending `</xml>` tag.

14. Exit the Commerce Suite application by entering the `shutdown` command at the console prompt.

Getting Ready to Test With Wal-Mart

Perform the following steps to prepare for testing with Wal-Mart:

1. Contact Wal-Mart and provide your AS2 name, external address and port, and a copy of your certificate. For example, *`MyName.cer`*.

2. Review the firewall considerations for Wal-Mart.

CHAPTER

5 Configuring Commerce Suite for Load Balancing and Failover

Once you have successfully performed a basic Commerce Suite configuration and conducted connectivity testing with iSoft, you are now ready to understand configuring Commerce Suite to enable load balancing and failover. If you have not performed a basic Commerce Suite configuration, refer to Chapter 4, *Configuring Commerce Suite and Testing with iSoft*.

This chapter describes how to install and configure Commerce Suite router and transport agents for inbound load balancing and failover capabilities. Detailed instructions on starting both agents and creating a Commerce Suite to act as a trading partner are also included.

Note: In order to test your Commerce Suite instances for load balancing and failover, it is recommended that you install each Commerce Suite instance on a separate machine.

Performing a load balancing and failover configuration requires a full licensed copy of the Commerce Suite software. The free Wal-Mart Commerce Suite copy does not support a load balancing and failover configuration.

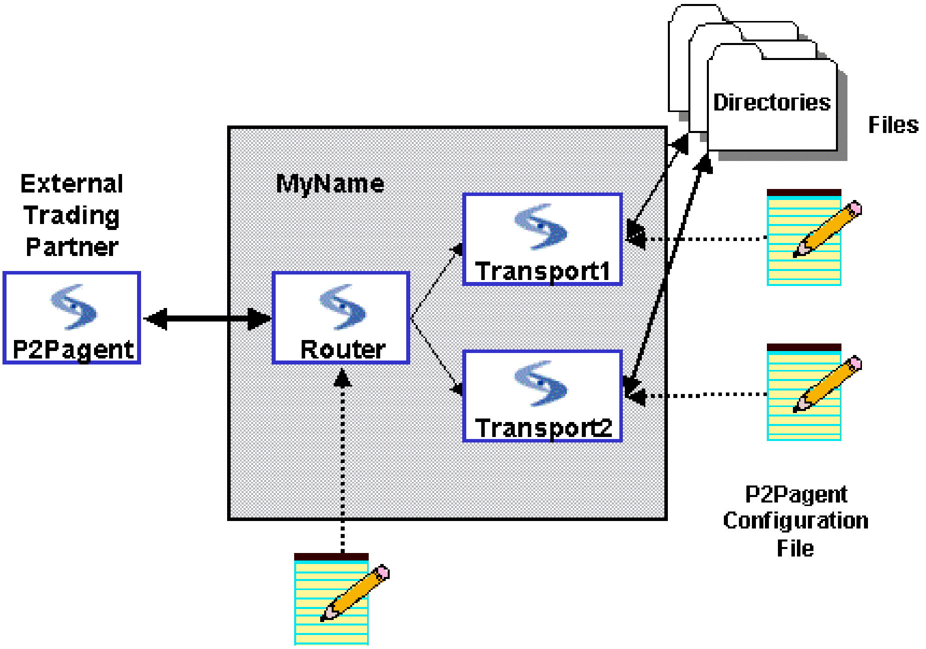
This section contains the following sections:

- Installing and Configuring a Router Agent

- Installing and Configuring Multiple Transport Agents
- Starting Your Router and Transport Agents
- Testing the Load Balancing and Failover Configuration

The following diagram illustrates how the Commerce Suite router and transport agents interact to enable load balancing and failover capabilities with an external trading partner.

Figure 5-1 Commerce Suite Load Balancing and Failover Capabilities



Installing and Configuring a Router Agent

This section describes the steps necessary to install and configure a Commerce Suite Router agent using a Commerce Suite text configuration file.

Note: Your Commerce Suite Router agent instance must be installed on a separate machine, referred to as the router machine, in order to perform load balancing and failover testing with other Commerce Suite instances.

Perform the following steps to install and configure your Commerce Suite Router agent:

1. On your router machine, create a separate `router` subdirectory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent.exe` file to the `router` subdirectory.
3. Create a `\log` subdirectory within the `router` subdirectory.
4. Create a `p2pagent.cfg` file in the `router` agent installation directory.
5. Cut and paste the sample router text in Listing 5-1 into the `p2pagent.cfg` file. Start with the `<xml>` tag and end with the `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 5-1 p2pagent.cfg Sample Router Text

```
<xml>
# The following commands configure your router agent
#
<command>set -gr</command>
```

```
<command>set -gp1</command>
<command>set -lplog</command>
<command>set -lf</command>
#
#  The following command enables the router to listen for client
   connections

<command>start rhttp://127.0.0.1:5080</command>
#
#  The following command enables the router to listen for transport
   broadcasts

<command>start router</command>
#
</xml>
```

Listing 5-1 p2pagent.cfg Sample Router Text Command Definitions

The following command definitions apply to the commands used in Listing 5-1 *p2pagent.cfg Sample Router Text*.

- The `set -gr` command configures the Commerce Suite to perform the software router mode.
- The `set -gp1` command assigns the router to peer group 1.
- The `set -lplog` command enables the writing of log information to a daily file and.
- The `-lf` command specifies the file-system directory location in which to store daily log files.
- The `start rhttp://127.0.0.1:5080` command starts the router on the configured address and port listening for a transport agent broadcasting it's presence for work.
- The `start router` command starts the Commerce Suite in the router mode.

Installing and Configuring Multiple Transport Agents

The following sections provide instructions on installing and configuring multiple transport agents for testing Commerce Suite's load balancing and failover capabilities.

- Installing and Configuring a Transport Agent
- Installing and Configuring a Second Transport Agent
- Creating a Stand-Alone Commerce Suite to Act as an External Trading Partner

Installing and Configuring a Transport Agent

This section describes the steps necessary to install and configure a Commerce Suite Transport agent using a Commerce Suite text configuration file.

Note: Your Commerce Suite Transport agent instance must be installed on a separate machine, referred to as the transport1 machine, in order to perform load balancing and failover testing with other Commerce Suite instances.

Perform the following steps to install and configure your first Commerce Suite Transport agent:

1. On your transport1 machine, create a separate `transport1` directory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent.exe` file to the `c:\isoft\transport1` subdirectory.
3. Create a `p2pagent.cfg` file in the `c:\isoft\transport1` subdirectory.
4. Cut and paste the sample transport text in Listing 5-2 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

Note: For testing purposes in the following code sample, the ***MyName*** variable is used as a placeholder to represent your AS2 name. You can change the ***MyName*** variable to a more meaningful name, however you must ensure that all ***MyName*** variable references in the `p2pagent.cfg` file are changed or else you may encounter errors.

All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 5-2 p2pagent.cfg Sample Transport1 Text

```
<xml>

#  The following commands configure your transport1 agent

<command>set -eperror</command>
<command>set -ef</command>
<command>set -gt</command>
<command>set -gp1</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -opworkorder</command>
<command>set -oswo</command>
<command>set -pppki</command>
<command>set -rpreceipt</command>
<command>set -tr300s</command>

#   The following commands define your trading partner relationships

<command>addpair ExtTP MyName http://127.0.0.1:5080/
mailto:as2@test.com as2@test.com inbox\ExtTP</command>

<command>addpair MyName ExtTP http://127.0.0.1:6080/
mailto:as2@test.com as2@test.com inbox\MyName</command>

#   The following commands import an X.509 certificate and
    corresponding private key for you and your trading partner.

<command>importkey MyName ExtTP E -fCpki\MyName.cer -fKpki\
MyName.prv</command>

<command>importkey MyName ExtTP J -fCpki\ExtTP.cer</command>
```

```
<command>importkey ExtTP MyName E -fCpki\MyName.cer -fKpki\
MyName.prv</command>

<command>importkey ExtTP MyName J -fCpki\ExtTP.cer</command>

#   The following start commands start the http listener at the
    specified address and port, and starts the outbound beacon
    service.

<command>start http://127.0.0.1:5080</command>
<command>start beacon</command>
#
</xml>
```

Listing 5-2 p2pagent.cfg Sample Transport1 Text Command Definitions

The following command definitions apply to the commands used in Listing 5-2 *p2pagent.cfg Sample Transport1 Text*.

- The `set -eperror` command sets the error recording path to `\error`.
- The `set -ef` command enables inbound and outbound files with errors will be written to an error directory.
- The `set -gt` command sets Commerce Suite to transport mode.
- The `set -gp1` command sets your Commerce Suite peer group number to 1.
- The `set -lplog` command sets the log path to `\log`.
- The `set -lf` command enables the writing of trace-log records set to a daily file.
- The `set -npnotice` command sets the notice record path to `\notice`.
- The `set -nf` command specifies for notices to be written to a file.
- The `set -opworkorder` command sets the work order path to `\workorder`.
- The `set -oswo` command sets the work order extension to `.wo`.
- The `set -pppki` command sets the PKI path to `\pki`.

- The `set -rpreceipt` command sets the asynchronous receipt path to `\receipt`.
- The `set -tr300s` command sets the first-receive interval to 300 seconds.
- The `addpair MyName` *`ExtTP`* `http://127.0.0.1:6080/ mailto:as2@test.com as2@test.com inbox\MyName` command defines a trading pair {*`AS2from`*][*`AS2to`*][*`external address`*][*`async receipt address`*][*`notfication name`*][*`inbox location`*].
- The `addpair` *`ExtTP`* `MyName http://127.0.0.1:5080/ mailto:as2@test.com as2@test.com inbox\YourName` command defines a trading pair {*`AS2from`*][*`AS2to`*][*`external address`*][*`async receipt address`*][*`notfication name`*][*`inbox location`*].
- The `importkey MyName` *`ExtTP`* `E -fCpki\MyName.cer -fKpki\MyName.prv` command imports a public/private key pair used for digital signatures in the [*`AS2from`*] to [*`AS2to`*] relationship.
- The `importkey MyName` *`ExtTP`* `J -fCpki\ExtTP.cer` command imports an public key used for encryption in the [*`AS2from`*] to [*`AS2to`*] relationship.
- The `importkey` *`ExtTP`* `MyName E -fCpki\MyName.cer -fKpki\MyName.prv` command specifies to sign and decrypt your public/private key-pair.
- The `importkey` *`ExtTP`* `MyName J -fCpki\ExtTP.cer` command specifies to encrypt and verify the public/private key pair signatures.
- The `start http://127.0.0.1:5080` command starts an http listener for the defined address and port.
- The `start beacon` command starts the outbound beacon service, which allows the transport to broadcast its presence.

5. Create the following subdirectories in the `c:\iSoft` installation directory:
   - `\error`
   - `\inbox\`*`ExtTP`*
   - `\inbox\`*`MyName`*

- `\log`
- `\notice`
- `\outbox`
- `\pki`
- `\receipt`
- `\workorder`

6. On your transport1 machine, start the Commerce Suite transport agent and monitor your console output for any start-up error messages. Refer to *Chapter 2, "Starting and Stopping P2P Agent,"* for instructions on starting the application. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

   Note: You will see initial errors on loading keys that have not been created. This is acceptable as you will create a certificate and private-key later in this procedure. You will also create an external trading partner certificate that will be required in a later step.

7. Create a self-signed X.509V3 certificate for load balancing and failover testing. The associated Public/Private key pair is created in memory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

```
addkey MyName ExtTP O 1024 self
C=US;S=TX;L=Dallas;O=iSoft;CN=MyName
```

   The `addkey` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing.

   a. Export the generated keys into two files in the `c:\isoft\transport1` root directory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

```
exportkey MyName ExtTP O MyName.cer MyName.prv
```

8. Move the *MyName*.cer and *MyName*.prv key files from the c:\isoft\transport1 root directory into the c:\isoft\transport1\pki subdirectory.
9. Exit the Commerce Suite application by entering the shutdown command at the console prompt.

Installing and Configuring a Second Transport Agent

This section describes the steps necessary to install and configure a second Commerce Suite Transport agent used in testing Commerce Suite load balancing and failover functionality.

Note: Your Commerce Suite Transport agent instance must be installed on a separate machine, referred to as the transport2 machine, in order to perform load balancing and failover testing with other Commerce Suite instances.

Perform the following steps to install and configure your Commerce Suite Transport agent:

1. On your transport2 machine, create a separate c:\isoft\transport2 directory within your existing c:\iSoft installation root directory.
2. Copy the p2pagent.exe file to the c:\isoft\transport2 subdirectory.
3. Create a p2pagent.cfg file in the c:\isoft\transport2 subdirectory.
4. Cut and paste the sample transport text in Listing 5-3 into the p2pagent.cfg file you created. Start with the <xml> and end with </xml> tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 5-3 p2pagent.cfg Sample Transport2 Text

```
<xml>

#  The following commands configure your transport2 agent

<command>set -eperror</command>
<command>set -ef</command>
<command>set -gt</command
<command>set -gp1</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -opworkorder</command>
<command>set -oswo</command>
<command>set -pppki</command>
<command>set -rpreceipt</command>
<command>set -tr300s</command>

#   The following commands define your trading partner relationships

<command>addpair ExtTP MyName http://127.0.0.1:5080/
mailto:as2@test.com as2@test.com inbox\ExtTP</command>

<command>addpair MyName ExtTP http://127.0.0.1:6080/
mailto:as2@test.com as2@test.com inbox\MyName</command>

#   The following commands import a X.509 certificate and
    corresponding private key for you and your trading partner.

<command>importkey MyName ExtTP E -fCpki\MyName.cer -fKpki\
MyName.prv</command>

<command>importkey MyName ExtTP J -fCpki\ExtTP.cer</command>

<command>importkey ExtTP MyName E -fCpki\MyName.cer -fKpki\
MyName.prv</command>

<command>importkey ExtTP MyName J -fCpki\ExtTP.cer</command>

#   The following start commands start the http listener at the
    specified address and port, and starts the outbound beacon
    service.

<command>start http://127.0.0.1:5080</command>
<command>start beacon</command>
#
</xml>
```

Note: Refer to Listing 5-2 for sample text command definitions.

5. Create the following subdirectories in the `c:\iSoft` installation directory:
   - `\error`
   - `\inbox\`*`ExtTP`*
   - `\inbox\`*`MyName`*
   - `\log`
   - `\notice`
   - `\outbox`
   - `\pki`
   - `\receipt`
   - `\workorder`
6. Copy the *`MyName`*`.cer` and *`MyName`*`.prv` files from the transport1 machine `c:\isoft\transport1\pki` subdirectory into the transport2 machine `c:\isoft\transport2\pki` subdirectory.

Creating a Stand-Alone Commerce Suite to Act as an External Trading Partner

This section describes the steps necessary to install and configure an external Commerce Suite trading partner used in testing Commerce Suite load balancing and failover functionality.

Note: Your stand-alone external Commerce Suite instance must be installed on a separate machine, referred to as the external trading partner machine, in order to conduct testing with the internal load balancing and failover configuration.

Perform the following steps to create a Commerce Suite to act as an external trading partner:

1. On your external trading partner machine, create a new `c:\isoft\ExtTP` subdirectory within your existing `c:\iSoft` installation root directory.

2. Copy the `p2pagent.exe` file into the `c:\isoft\ExtTP` subdirectory.
3. In the `c:\isoft\ExtTP` subdirectory, create a new `p2pagent.cfg` file.
4. Cut and paste the sample transport text in Listing 5-4 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 5-4 p2pAgent Trading Partner p2pagent.cfg File

```
<xml>
#  External Trading Partner config
<command>set -eperror</command>
<command>set -ef</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -opworkorder</command>
<command>set -oswo</command>
<command>set -pppki</command>
<command>set -rpreceipt</command>
<command>set -tr300s</command>
#
<command>addpair ExtTP MyName http://127.0.0.1:5080/
mailto:as2@test.com as2@test.com inbox\ExtTP1</command>

<command>addpair MyName ExtTP http://127.0.0.1:6080/
mailto:as2@test.com as2@test.com inbox\MyName</command>
#
<command>importkey ExtTP MyName E -fCpki\ExtTP.cer -fKpki\
ExtTP1.prv</command>

<command>importkey ExtTP MyName J -fCpki\MyName.cer</command>

<command>importkey MyName ExtTP E -fCpki\ExtTP.cer -fKpki\
ExtTP.prv</command>

<command>importkey MyName ExtTP J -fCpki\MyName.cer</command>
#
<command>start http://127.0.0.1:5080</command>
```

```
#
</xml>
```

Note: Refer to Listing 5-2 for sample text command definitions.

5. Start the stand-alone Commerce Suite and monitor your console output for any start-up error messages. Refer to *Chapter 2, "Starting and Stopping P2P Agent,"* for instructions on starting the application. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

   Note: You will see initial errors on loading keys that have not been created. This is acceptable as you will create a certificate and private-key later in this procedure. You will also create an external trading partner certificate that will be required in a later step.

6. Create a self-signed certificate for the external trading partner. The associated Public/Private key pair is created in memory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   addkey ExtTP MyName O 1024 self
   C=US;S=TX;L=Dallas;O=iSoft;CN=ExtTP
   ```

   The `addkey` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing.

   a. Enter the following command to export key files into the `ExtTP` root directory:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   exportkey ExtTP MyName O ExtTP.cer ExtTP.prv
   ```

7. Move the `ExtTP.cer` and `ExtTP.prv` key files from the `c:\isoft\ExtTP` root directory into the transport1 `c:\isoft\transport1\pki` subdirectory.

8. From the transport1 machine `c:\isoft\transport1\pki` subdirectory, copy the `MyName.cer` file and place a copy of it into the `c:\isoft\ExtTP\pki` subdirectory.

9. Copy the `MyName.cer` file from the transport1 machine `c:\isoft\transport1\pki` subdirectory and place a copy of it into the external transport machine `c:\isoft\extTP\pki`.

Starting Your Router and Transport Agents

This section details how to start your router and transport agents.

Starting the Router

Perform the following steps to start your router agent:

1. On your router machine, start the Commerce Suite application in the `c:\isoft\router` subdirectory of the router machine.

2. From within the `c:\isoft\router` directory, start the Commerce Suite application.

3. Monitor the console for the following output:

Listing 5-5 Commerce Suite Router Startup Console Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\ROUTER1>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1
```

```
2002.10.10 20:28:35.493    OUTM OK  Outbound service started
2002.10.10 20:28:35.563    POPT OK  Server is a router server
2002.10.10 20:28:35.583    POPT OK  Peer group set to [1]
2002.10.10 20:28:35.633    POPT OK  Log path set to [log]
2002.10.10 20:28:35.653    POPT OK  Trace set to WRITE_FILE
2002.10.10 20:28:35.723    RTRM OK  Router service started
2002.10.10 20:28:35.753    IBCM OK  Inbound beacon service started
```

4. Enter the command `set -m6` to set your trace level to debug.

Starting the First Transport

Perform the following steps to start the first Transport agent:

1. On your transport1 machine, start the Commerce Suite application in the `c:\isoft\transport1` subdirectory.
2. Monitor the transport console for the following representative significant output:

Listing 5-6 Commerce Suite Transport1 Startup Console Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\TRANPORT1>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1

2002.10.10 20:34:45.044       OUTM OK  Outbound service started
2002.10.10 20:34:45.154       POPT OK  Error path set to [error]
2002.10.10 20:34:45.174       POPT OK  Inbound errant files will
                                       be stored
2002.10.10 20:34:45.224       POPT OK  Server is a transport server
2002.10.10 20:34:45.244       POPT OK  Peer group set to [1]
2002.10.10 20:34:45.294       POPT OK  Log path set to [log]
2002.10.10 20:34:45.314       POPT OK  Trace set to WRITE_FILE
2002.10.10 20:34:45.365       POPT OK  Notice path set to [notice]
2002.10.10 20:34:45.385       POPT OK  Notices will be written
```

```
                                            to file
2002.10.10 20:34:45.435       POPT OK  Work Order path set
                                            to [workorder]
2002.10.10 20:34:45.455       POPT OK  Work Order file-spec set
                                            to [wo]
2002.10.10 20:34:45.505       POPT OK  PKI path set to [pki]
2002.10.10 20:34:45.555       POPT OK  Async. receipt path set
                                            to [receipt]
2002.10.10 20:34:45.605       POPT OK  First-receive interval
                                            set to [300000ms]
2002.10.10 20:34:46.216       HPIM OK  HTTP inbound service
                                            started
2002.10.10 20:34:46.276       OBCM OK  Outbound beacon service
                                                started
```

3. Enter the console command `set -m6` to set your trace level to debug.

4. Check the Commerce Suite router console on the router machine for the addition of the first transport agent.

   ```
   2002.10.10 20:34:46.967 PBCN OK peer 127.0.0.1:5081 http added
   ```

Starting the Second Transport

Perform the following steps to start the second Transport agent:

1. On your transport2 machine, start the Commerce Suite application in the `c:\isoft\transport2` subdirectory.

2. Monitor the transport console for the following representative significant output:

Listing 5-7 Commerce Suite Transport2 Startup Console Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\TRANSPORT2>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
```

```
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1

2002.10.10 20:34:45.044       OUTM OK  Outbound service started
2002.10.10 20:34:45.154       POPT OK  Error path set to [error]
2002.10.10 20:34:45.174       POPT OK  Inbound errant files will
                                       be stored
2002.10.10 20:34:45.224       POPT OK  Server is a transport server
2002.10.10 20:34:45.244       POPT OK  Peer group set to [1]
2002.10.10 20:34:45.294       POPT OK  Log path set to [log]
2002.10.10 20:34:45.314       POPT OK  Trace set to WRITE_FILE
2002.10.10 20:34:45.365       POPT OK  Notice path set to [notice]
2002.10.10 20:34:45.385       POPT OK  Notices will be written
                                       to file
2002.10.10 20:34:45.435       POPT OK  Work Order path set
                                       to [workorder]
2002.10.10 20:34:45.455       POPT OK  Work Order file-spec set
                                       to [wo]
2002.10.10 20:34:45.505       POPT OK  PKI path set to [pki]
2002.10.10 20:34:45.555       POPT OK  Async. receipt path set
                                       to [receipt]
2002.10.10 20:34:45.605       POPT OK  First-receive interval
                                       set to [300000ms]
2002.10.10 20:34:46.216       HPIM OK  HTTP inbound service
                                       started
2002.10.10 20:34:46.276       OBCM OK  Outbound beacon service
                                           started
```

3. Enter the console command `set -m6` to set your trace level to debug.

4. Check the router console on the router machine for the addition of the second transport agent.

```
2002.10.10 20:54:10.630 PBCN OK peer 127.0.0.1:5082 http added
```

Testing the Load Balancing and Failover Configuration

Perform the following steps to test your load balancing and failover configuration.

1. On your external trading partner machine, initiate a basic file send from the Commerce Suite application. Enter the following command to process a basic file send.

   ```
   send http ExtTP MyName -fNp2pagent.cfg -n1
   ```

   The command will not request a receipt, perform encryption, or any other options. Monitor the router and multiple transport consoles on their respective machines. You should see output similar to the following sample output for the router.

Listing 5-8 Commerce Suite Sample Router Console Output

```
2002.10.11 00:01:25.755 05884 RTRS OK  1498 bytes read from server
2002.10.11 00:01:25.785 05884 RTRS OK  1498 bytes written to client
2002.10.11 00:01:25.826 05884 RTRS OK  Server has disconnected
2002.10.11 00:01:25.856 05884 RTRS OK  Router session stopping
2002.10.11 00:04:10.032 43456 RTRS OK  Router session started
2002.10.11 00:04:10.052 43456 RTRS OK  Router client:127.0.0.1:1226
2002.10.11 00:04:10.102 43456 RTRS OK  1863 bytes read from client
2002.10.11 00:04:10.122 43456 RTRS OK  1863 bytes buffered
2002.10.11 00:04:10.142 43456 RTRS OK  1863 bytes written to server
2002.10.11 00:04:10.172 43456 RTRS OK  Timeout waiting for client
                                       data
..........
2002.10.11 00:04:10.793 43456 RTRS OK  178 bytes read from server
2002.10.11 00:04:10.813 43456 RTRS OK  178 bytes written to client
2002.10.11 00:04:10.843 43456 RTRS OK  Server has disconnected
2002.10.11 00:04:10.863 43456 RTRS OK  Router session stopping
```

You should see output similar to the following sample output for transport1 and transport2.

Listing 5-9 Commerce Suite Sample Transport1 and Transport2 Console Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\DEMO\FAILOVER\B\TRAN1>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1

2002.11.04 10:23:03.937       OUTM OK  Outbound service started
2002.11.04 10:23:04.057       POPT OK  Error path set to [error]
2002.11.04 10:23:04.077       POPT OK  Inbound errant files will be
                                       stored
2002.11.04 10:23:04.127       POPT OK  Server is a transport server
2002.11.04 10:23:04.147       POPT OK  Peer group set to [1]
2002.11.04 10:23:04.197       POPT OK  Log path set to [log]
2002.11.04 10:23:04.217       POPT OK  Trace set to WRITE_FILE
2002.11.04 10:23:04.327       POPT OK  Notice path set to [notice]
2002.11.04 10:23:04.347       POPT OK  Notices will be written to
                                       file
2002.11.04 10:23:04.397       POPT OK  Work Order path set to
                                       [workorder]
2002.11.04 10:23:04.418       POPT OK  Work Order file-spec set to
                                       [wo]
2002.11.04 10:23:04.468       POPT OK  PKI path set to [pki]
2002.11.04 10:23:04.518       POPT OK  Async. receipt path set to
                                       [receipt]
2002.11.04 10:23:04.568       POPT OK  First-receive interval set
                                       to [300000ms]
2002.11.04 10:23:05.159       HPIM OK  HTTP inbound service started
2002.11.04 10:23:05.189       OBCM OK  Outbound beacon service
                                       started
2002.11.04 10:23:35.834 14029 HPIS OK  HTTP inbound session started
2002.11.04 10:23:35.854 14029 HPIS OK  HTTP client: 127.0.0.1:1219
2002.11.04 10:23:36.315 14029 DECR OK  ** Content decrypted **
2002.11.04 10:23:36.385 14029 VRFY OK  ** Signature verified **
2002.11.04 10:23:37.016 14029 HPIS OK  HTTP inbound session stopping
```

2. To provide a work load, create a work order file that contains ten send commands.

3. Open Notepad or Wordpad on the external trading partner machine and cut and paste the following code sample into a new text file.

Listing 5-10 Commerce Suite Sample Work Order File

```
<xml>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

</xml>
```

4. Name the new text file `send10.wo` and place it in the `c:\isoft\ExtTP` subdirectory.

5. Enter the following command to initiate the `send10.wo` work order file.

```
batch send10.wo
```

You should see output similar to the following router command output code sample:

Listing 5-11 Commerce Suite Sample batch send.wo Router Command Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\DEMO\FAILOVER\B\ROUTER1>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1

2002.11.01 20:36:57.967       OUTM OK  Outbound service started
2002.11.01 20:36:58.037       POPT OK  Server is a router server
2002.11.01 20:36:58.057       POPT OK  Peer group set to [1]
2002.11.01 20:36:58.107       POPT OK  Log path set to [log]
2002.11.01 20:36:58.127       POPT OK  Trace set to WRITE_FILE

Note the following router startup and transport aquisition.

2002.11.01 20:36:58.197     RTRM OK  Router service started
2002.11.01 20:36:58.227     IBCM OK  Inbound beacon service started
2002.11.01 20:37:05.578     PBCN OK  peer 127.0.0.1:5081 http added
2002.11.01 20:37:10.946      PBCN OK  peer 127.0.0.1:5082 http added

Note the initiation and termination of the Router transport session

2002.11.01 20:37:29.163 07205 RTRS OK  Router session started
2002.11.01 20:37:29.343 06039 RTRS OK  Router session started
2002.11.01 20:37:29.513 57767 RTRS OK  Router session started
2002.11.01 20:37:30.645 12157 RTRS OK  Router session started
2002.11.01 20:37:30.755 16988 RTRS OK  Router session started
2002.11.01 20:37:32.938 25739 RTRS OK  Router session started
2002.11.01 20:37:33.309 16273 RTRS OK  Router session started
2002.11.01 20:37:33.509 47251 RTRS OK  Router session started
2002.11.01 20:37:35.072 07205 RTRS OK  Server has disconnected
2002.11.01 20:37:35.392 06039 RTRS OK  Server has disconnected
2002.11.01 20:37:35.813 07205 RTRS OK  Router session stopping
2002.11.01 20:37:36.193 06039 RTRS OK  Router session stopping
2002.11.01 20:37:36.614 39977 RTRS OK  Router session started
2002.11.01 20:37:36.824 31530 RTRS OK  Router session started
2002.11.01 20:37:36.924 57767 RTRS OK  Server has disconnected
2002.11.01 20:37:37.295 57767 RTRS OK  Router session stopping
```

```
2002.11.01 20:37:37.986 12157 RTRS OK  Server has disconnected
2002.11.01 20:37:38.236 16988 RTRS OK  Server has disconnected
2002.11.01 20:37:38.386 12157 RTRS OK  Router session stopping
2002.11.01 20:37:38.587 16988 RTRS OK  Router session stopping
2002.11.01 20:37:40.229 25739 RTRS OK  Server has disconnected
2002.11.01 20:37:40.389 25739 RTRS OK  Router session stopping
2002.11.01 20:37:40.530 16273 RTRS OK  Server has disconnected
2002.11.01 20:37:40.640 47251 RTRS OK  Server has disconnected
2002.11.01 20:37:40.720 16273 RTRS OK  Router session stopping
2002.11.01 20:37:40.820 47251 RTRS OK  Router session stopping
2002.11.01 20:37:41.431 39977 RTRS OK  Server has disconnected
2002.11.01 20:37:41.501 39977 RTRS OK  Router session stopping
2002.11.01 20:37:41.551 31530 RTRS OK  Server has disconnected
2002.11.01 20:37:41.581 31530 RTRS OK  Router session stopping
```

You should see output similar to the following Transport1 command output code sample:

Listing 5-12 Commerce Suite Sample batch send.wo Transport1 Command Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\DEMO\FAILOVER\B\TRAN1>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1
```

Transport startup

```
2002.11.01 20:37:03.845       OUTM OK  Outbound service started
2002.11.01 20:37:03.946       POPT OK  Error path set to [error]
2002.11.01 20:37:03.966      POPT OK  Inbound errant files will be
                                      stored
2002.11.01 20:37:04.016      POPT OK  Server is a transport server
2002.11.01 20:37:04.036       POPT OK  Peer group set to [1]
2002.11.01 20:37:04.086       POPT OK  Log path set to [log]
2002.11.01 20:37:04.106       POPT OK  Trace set to WRITE_FILE
2002.11.01 20:37:04.156       POPT OK  Notice path set to [notice]
2002.11.01 20:37:04.176       POPT OK  Notices will be written to
                                       file
2002.11.01 20:37:04.226       POPT OK  Work Order path set to
                                       [workorder]
2002.11.01 20:37:04.246       POPT OK  Work Order file-spec set to
                                       [wo]
2002.11.01 20:37:04.296       POPT OK  PKI path set to [pki]
2002.11.01 20:37:04.346       POPT OK  Async. receipt path set to
                                       [receipt]
2002.11.01 20:37:04.396       POPT OK  First-receive interval set
                                           to [300000ms]
2002.11.01 20:37:04.987      HPIM OK  HTTP inbound service started
2002.11.01 20:37:05.017       OBCM OK  Outbound beacon service
                                           started
```

Transport1 starts inbound sessions from the router and completes the required work

```
2002.11.01 20:37:29.513 64565 HPIS OK  HTTP inbound session started
2002.11.01 20:37:29.533 64565 HPIS OK  HTTP client: 127.0.0.1:1178
2002.11.01 20:37:29.563 37367 HPIS OK  HTTP inbound session started
2002.11.01 20:37:29.814 37367 HPIS OK  HTTP client: 127.0.0.1:1180
2002.11.01 20:37:31.366 64987 HPIS OK  HTTP inbound session started
2002.11.01 20:37:31.426 64565 DECR OK  ** Content decrypted **
2002.11.01 20:37:31.586 64987 HPIS OK  HTTP client: 127.0.0.1:1184
2002.11.01 20:37:32.378 64565 VRFY OK  ** Signature verified **
```

```
2002.11.01 20:37:32.558 37367 DECR OK  ** Content decrypted **
2002.11.01 20:37:33.149 37367 VRFY OK  ** Signature verified **
2002.11.01 20:37:34.341 20320 HPIS OK  HTTP inbound session started
2002.11.01 20:37:34.621 20320 HPIS OK  HTTP client: 127.0.0.1:1189
2002.11.01 20:37:34.701 64987 DECR OK  ** Content decrypted **
2002.11.01 20:37:35.222 64565 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:35.652 64987 VRFY OK  ** Signature verified **
2002.11.01 20:37:36.634 37367 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:37.535 60825 HPIS OK  HTTP inbound session started
2002.11.01 20:37:37.826 60825 HPIS OK  HTTP client: 127.0.0.1:1193
2002.11.01 20:37:37.886 20320 DECR OK  ** Content decrypted **
2002.11.01 20:37:38.156 20320 VRFY OK  ** Signature verified **
2002.11.01 20:37:38.386 64987 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:40.009 60825 DECR OK  ** Content decrypted **
2002.11.01 20:37:40.319 60825 VRFY OK  ** Signature verified **
2002.11.01 20:37:40.470 20320 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:41.471 60825 HPIS OK  HTTP inbound session stopping
```

You should see output similar to the following Transport2 command output code sample:

Listing 5-13 Commerce Suite Sample batch send.wo Transport2 Command Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\DEMO\FAILOVER\B\TRAN2>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1

Transport startup

2002.11.01 20:37:09.364       OUTM OK  Outbound service started
2002.11.01 20:37:09.444       POPT OK  Error path set to [error]
2002.11.01 20:37:09.464       POPT OK  Inbound errant files will be
                                          stored
2002.11.01 20:37:09.514       POPT OK  Server is a transport server
2002.11.01 20:37:09.534       POPT OK  Peer group set to [1]
2002.11.01 20:37:09.584       POPT OK  Log path set to [log]
2002.11.01 20:37:09.604       POPT OK  Trace set to WRITE_FILE
2002.11.01 20:37:09.654       POPT OK  Notice path set to [notice]
2002.11.01 20:37:09.674       POPT OK  Notices will be written to
```

```
                                         file
2002.11.01 20:37:09.724       POPT OK  Work Order path set to
                                         [workorder]
2002.11.01 20:37:09.744       POPT OK  Work Order file-spec set to
                                         [wo]
2002.11.01 20:37:09.794       POPT OK  PKI path set to [pki]
2002.11.01 20:37:09.844       POPT OK  Async. receipt path set to
                                         [receipt]
2002.11.01 20:37:09.894       POPT OK  First-receive interval set
                                         to [300000ms]
2002.11.01 20:37:10.485      HPIM OK  HTTP inbound service started
2002.11.01 20:37:10.515       OBCM OK  Outbound beacon service
                                             started
```

Transport2 starts inbound sessions from the router and completes the required work

```
2002.11.01 20:37:29.533 37972 HPIS OK  HTTP inbound session started
2002.11.01 20:37:29.553 37972 HPIS OK  HTTP client: 127.0.0.1:1179
2002.11.01 20:37:31.256 16388 HPIS OK  HTTP inbound session started
2002.11.01 20:37:31.426 16388 HPIS OK  HTTP client: 127.0.0.1:1183
2002.11.01 20:37:31.586 37972 DECR OK  ** Content decrypted **
2002.11.01 20:37:32.658 37972 VRFY OK  ** Signature verified **
2002.11.01 20:37:33.940 06508 HPIS OK  HTTP inbound session started
2002.11.01 20:37:34.341 06508 HPIS OK  HTTP client: 127.0.0.1:1188
2002.11.01 20:37:34.541 16388 DECR OK  ** Content decrypted **
2002.11.01 20:37:34.621 51933 HPIS OK  HTTP inbound session started
2002.11.01 20:37:34.941 51933 HPIS OK  HTTP client: 127.0.0.1:1190
2002.11.01 20:37:35.072 16388 VRFY OK  ** Signature verified **
2002.11.01 20:37:35.813 37972 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:37.375 06508 DECR OK  ** Content decrypted **
2002.11.01 20:37:37.776 06508 VRFY OK  ** Signature verified **
2002.11.01 20:37:37.936 48096 HPIS OK  HTTP inbound session started
2002.11.01 20:37:38.006 51933 DECR OK  ** Content decrypted **
2002.11.01 20:37:38.136 48096 HPIS OK  HTTP client: 127.0.0.1:1194
2002.11.01 20:37:38.326 51933 VRFY OK  ** Signature verified **
2002.11.01 20:37:38.587 16388 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:40.249 06508 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:40.369 48096 DECR OK  ** Content decrypted **
2002.11.01 20:37:40.500 51933 HPIS OK  HTTP inbound session stopping
2002.11.01 20:37:40.640 48096 VRFY OK  ** Signature verified **
2002.11.01 20:37:41.551 48096 HPIS OK  HTTP inbound session stopping
```

You should see output similar to the following External Trading Partner command output code sample:

Listing 5-14 Commerce Suite Sample batch send.wo External Trading Partner Command Output

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\ISOFT\DEMO\FAILOVER\B\TRAN2>p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.10.2002.7.15.1
```

Initiation of ten send commands

```
2002.11.01 20:36:53.640      HPIM OK  HTTP inbound service started
batch send10.wo
ok
2002.11.01 20:37:28.141 02930 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:28.161 02930 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:28.231 54553 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:28.252 54553 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:28.933 02020 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:29.063 02020 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:29.513 08664 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:29.533 50814 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:29.543 08664 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:29.553 50814 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:31.076 10947 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:31.256 56069 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:31.316 10947 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:31.406 12285 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:31.426 56069 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:31.506 12285 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:34.541 47075 HPOS OK  Outbound session started -
attempt=[1 of 1]
2002.11.01 20:37:34.661 47075 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:34.711 34920 HPOS OK  Outbound session started -
attempt=[1 of 1]
```

External trading partner receives the MDN and verifies the signature and original content.

```
2002.11.01 20:37:34.851 34920 HPOS OK  Mailbox=[0]  Batch=[0]
2002.11.01 20:37:35.352 02930 VRFY OK  ** Signature verified **
2002.11.01 20:37:35.773 02930 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:35.963 54553 VRFY OK  ** Signature verified **
2002.11.01 20:37:36.153 02020 VRFY OK  ** Signature verified **
2002.11.01 20:37:36.384 54553 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:36.524 02930 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:36.574 02020 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:36.844 54553 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:36.984 02020 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:38.066 08664 VRFY OK  ** Signature verified **
2002.11.01 20:37:38.186 08664 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:38.407 50814 VRFY OK  ** Signature verified **
2002.11.01 20:37:38.507 08664 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:38.587 50814 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:39.017 50814 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:40.309 10947 VRFY OK  ** Signature verified **
2002.11.01 20:37:40.349 10947 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:40.500 56069 VRFY OK  ** Signature verified **
2002.11.01 20:37:40.590 56069 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:40.650 12285 VRFY OK  ** Signature verified **
2002.11.01 20:37:40.680 10947 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:40.720 12285 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:40.780 56069 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:40.910 12285 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:41.471 47075 VRFY OK  ** Signature verified **
2002.11.01 20:37:41.501 47075 PMDN OK  ** Original-Content-MIC
found in MDN **
2002.11.01 20:37:41.561 34920 VRFY OK  ** Signature verified **
2002.11.01 20:37:41.581 47075 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.01 20:37:41.591 34920 PMDN OK  ** Original-Content-MIC
```

```
found in MDN **
2002.11.01 20:37:41.641 34920 HPOS OK  Outbound session stopping -
batch=[0]
```

6. You can conduct more comprehensive testing by using additional send parameters for encryption and digital signatures.
7. To test dynamic scaling, you can create additional transports by duplicating the configuration used to create your Transport2 agent and start them up after the work order file transfer starts. Once this happens, you should see additional transports picked-up by the router and start to receive work. Perform the following steps to create an additional transport agent:
   a. Create a third transport trading partner by following the steps in the “Installing and Configuring a Second Transport Agent,” section of this chapter.
   b. Using Notepad or Wordpad, cut and paste the contents of the `send10.wo` into a new text file and save it as `send50.wo`.
   c. Place the `send50.wo` in the `c:\isoft\transport3` subdirectory of the transport3 machine.
   d. Initiate the `send50.wo` file by executing the following command:

      ```
      batch send50.wo
      ```

   e. Start the transport3 trading partner by following the steps in the “Starting the Second Transport,” section of this chapter.
   f. Monitor the router console output for the addition of the transport3 trading partner.
   g. As soon as the transport3 trading partner is picked up by the router, the router will begin to send work to the transport3 trading partner.
   h. You can now monitor the activity of the transport3 trading partner.
8. To test for failover, shutdown a transport by closing the transport console window.

6 Configuring Commerce Suite for Non-Database Remote Administration

If you have not performed a basic Commerce Suite configuration, refer to Chapter 4, "Configuring Commerce Suite and Testing with iSoft."

This chapter describes how to install and configure Commerce Suite router, transport, and admin agents for non-database remote configuration capabilities. Detailed instructions on starting both agents and creating a Commerce Suite to act as a trading partner are also included.

Note: In order to test your Commerce Suite instances for remote configuration, it is recommended that you install each Commerce Suite instance on a separate machine.

Performing a remote configuration requires a full licensed copy of the Commerce Suite software. The free Wal-Mart Commerce Suite copy does not support a remote administration configuration.

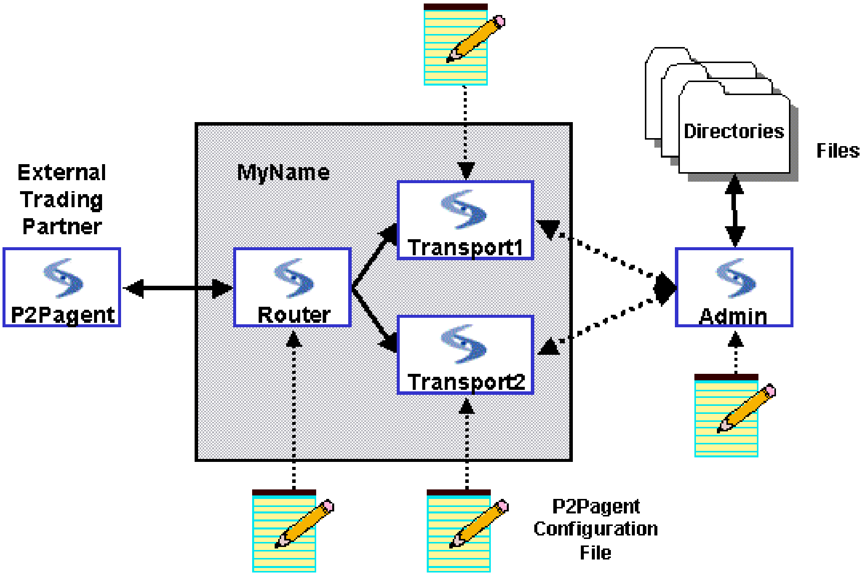
This section contains the following sections:

- Installing and Configuring a Router Agent for Remote Administration

- Installing and Configuring Multiple Transport Agents
- Installing and Configuring the Administration Agent
- Starting Your Remote Administration Cluster
- Starting the Administration Agent
- Testing the Remote Administration Configuration

The following diagram illustrates how the Commerce Suite router, transport, and admin agents enable remote administration capabilities with an external trading partner.

Figure 6-1 Commerce Suite Remote Administration Capabilities



Installing and Configuring a Router Agent

This section describes the steps necessary to install and configure a Commerce Suite Router agent using a basic Commerce Suite text configuration file.

Note: Your Commerce Suite Router agent instance must be installed on a separate machine, referred to as the router machine, in order to perform remote administration testing with other Commerce Suite instances.

Perform the following steps to install and configure your Commerce Suite Router agent:

1. On your router machine, create a separate `router` subdirectory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent.exe` file to the `router` subdirectory.
3. Create a `\log` subdirectory within the `router` subdirectory.
4. Open Notepad and create and save a file named `p2pagent.cfg` in the `router` agent installation directory.
5. Cut and paste the sample router text in Listing 5-1 into the `p2pagent.cfg` file you created. Start with the `<xml>` tag and end with the `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 6-1 p2pagent.cfg Sample Router Text

```
<xml>

# Router minimum remote admin start-up config
<command>set -ca127.0.0.1</command>
```

```
<command>set -cnR1</command>
<command>set -gr</command>
<command>set -gp1</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>start p2p://127.0.0.1:6081</command>
<command>start rhttp://127.0.0.1:5081</command>
<command>start router</command>

</xml>
```

Listing 6-1 p2pagent.cfg Sample Router Text Command Definitions

The following command definitions apply to the commands used in Listing 6-1 *p2pagent.cfg Sample Router Text*.

- The `set -ca` command sets the IP address to be used by the Commerce Suite to accept control messages from an Administrative Agent.
- The `set -cn` command sets the symbolic name to be used when referring to the Commerce Suite instance.
- The `set -gr` command sets Commerce Suite to act as a load balancing router for incoming data transfers.
- The `set -gp1` command assigns the router to peer group 1.
- The `set -np` command specifies the file-system location where Commerce Suite stores notice files.
- The `set -nf` command specifies for notice records to be written to a file.
- The `set -lplog` command enables the writing of log information to a daily file and.
- The `set -lf` command specifies the file-system directory location in which to store daily log files.The `set -gr` command configures the Commerce Suite to perform the software router mode.
- The `start p2p://` command specifies the control address for the remote agent.

- The `start rhttp://` command specifies the address for the remote agent.
- The `start router` command specifies to start the Commerce Suite router agent.

Installing and Configuring Multiple Transport Agents

The following sections provide instructions on installing and configuring multiple transport agents for testing Commerce Suite's load balancing and failover capabilities.

- Installing and Configuring a Transport Agent
- Installing and Configuring a Second Transport Agent
- Creating a Stand-Alone Commerce Suite to Act as an External Trading Partner

Installing and Configuring a Transport Agent

This section describes the steps necessary to install and configure a Commerce Suite Transport agent using a basic Commerce Suite startup text configuration file.

Note: Your Commerce Suite Transport agent instance must be installed on a separate machine, referred to as the transport1 machine, in order to perform remote administration testing with other Commerce Suite instances.

Perform the following steps to install and configure your first Commerce Suite Transport agent:

1. On your transport1 machine, create a separate `transport1` directory within your existing `c:\iSoft` installation root directory.

2. Copy the `p2pagent.exe` file to the `c:\isoft\transport1` subdirectory.
3. Open Notepad and create and save a `p2pagent.cfg` file in the `c:\isoft\transport1` subdirectory.
4. Cut and paste the sample transport text in Listing 6-2 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

   Note: For testing purposes in the following code sample, the ***MyName*** variable is used as a placeholder to represent your AS2 name. You can change the ***MyName*** variable to a more meaningful name, however you must ensure that all ***MyName*** variable references in the `p2pagent.cfg` file are changed or else you may encounter errors.

   All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 6-2 p2pagent.cfg Sample Transport1 Text

```
<xml>

# Transport 1 Minimum remote admin config
<command>set -ca127.0.0.1</command>
<command>set -cnT1</command>
<command>set -cp3501</command>
<command>set -gt</command>
<command>set -gp1</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>start p2p://127.0.0.1:6082</command>
<command>start beacon</command>

</xml>
```

Listing 6-2 p2pagent.cfg Sample Transport1 Text Command Definitions

The following command definitions apply to the commands used in Listing 6-2 *p2pagent.cfg Sample Transport1 Text*.

- The `set -ca` command sets the IP address to be used by the Commerce Suite to accept control messages from an Administrative Agent.
- The `set -cn` command sets the symbolic name to be used when referring to the Commerce Suite instance.
- The `set -cp` command sets the IP port to be used by the Commerce Suite to accept control messages from an administrative agent.
- The `set -gt` command sets the Commerce Suite is to act as a transport agent.
- The `set -gp` command sets the peer group to which the Commerce Suite instance belongs.
- The `set -np` command specifies the file-system location where Commerce Suite stores notice files.
- The `set -nf` command specifies for notice records to be written to a file.
- The `set -lplog` command enables the writing of log information to a daily file and.
- The `set -lf` command specifies the file-system directory location in which to store daily log files. The `set -gr` command configures the Commerce Suite to perform the software router mode.
- The `start p2p://` command specifies the control address for the remote agent.
- The `start beacon` command starts the outbound beacon service, which allows the transport to broadcast its presence.

5. Create the following subdirectories in the `c:\iSoft` installation directory:
   - `\error`
   - `\log`
   - `\notice`

6. On your transport1 machine, start the Commerce Suite transport agent and monitor your console output for any start-up error messages. Refer to *Chapter 2, "Starting and Stopping P2P Agent,"* for instructions on starting the application. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

Installing and Configuring a Second Transport Agent

This section describes the steps necessary to install and configure a second Commerce Suite Transport agent used in testing Commerce Suite remote administration functionality.

Note: Your Commerce Suite Transport agent instance must be installed on a separate machine, referred to as the transport2 machine, in order to perform remote administration testing with other Commerce Suite instances.

Perform the following steps to install and configure your Commerce Suite Transport agent:

1. On your transport2 machine, create a separate `c:\isoft\transport2` directory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent.exe` file to the `c:\isoft\transport2` subdirectory.
3. Create a `p2pagent.cfg` file in the `c:\isoft\transport2` subdirectory.
4. Cut and paste the sample transport text in Listing 6-3 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 6-3 p2pagent.cfg Sample Transport2 Text

```
<xml>

# Transport 2 Minimum remote admin config
<command>set -ca127.0.0.1</command>
<command>set -cnT2</command>
<command>set -cp3501</command>
<command>set -gt</command>
<command>set -gp1</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>start p2p://127.0.0.1:6083</command>
<command>start beacon</command>

</xml>
```

Note: Refer to Listing 6-2 for sample text command definitions.

5. Create the following subdirectories in the `c:\iSoft` installation directory:
   - `\error`
   - `\log`
   - `\notice`

Creating an Administration Agent

Creating a Commerce Suite Administrative Agent requires that the Commerce Suite instance be installed on a separate machine, referred to as the admin machine. This configuration enables you to perform remote configuration testing with other Commerce Suite instances.

Perform the following steps to install and configure your admin agent:

1. On your designated admin machine, create a separate `admin` subdirectory within your existing `c:\isoft` installation root directory.
2. Copy the `p2pagent.exe` file to the `admin` subdirectory.

3. Create a `\log` subdirectory within the `admin` subdirectory.
4. Create a `p2pagent.cfg` file in the admin agent installation directory.
5. Cut and paste the sample admin text in Listing 6-4 into the `p2pagent.cfg` file. Include the `<xml>` and `</xml>` tags when you cut and paste.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 6-4 p2pagent.cfg Sample Admin Text

```
<xml>

# Admin Config
<command>set -ca127.0.0.1</command>
<command>set -cnA1</command>

# Set P2Pagent Peer Group
# assign agent to a group and role
<command>set -gp1</command>
<command>set -ga</command>

<command>set -npnotice</command>
<command>set -nf</command>
<command>set -nd-</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>set -opworkorder -oswo</command>

# define servers
<command>addserver R1 1 R rhttp://127.0.0.1:5081
p2p://127.0.0.1:6081</command>

<command>addserver T1 1 T http://127.0.0.1:5082
p2p://127.0.0.1:6082</command>

<command>addserver T2 1 T http://127.0.0.1:5083
p2p://127.0.0.1:6083</command>

# define trading pairs

<command>addpair MyName  ExtTP  http://127.0.0.1:5081/
http://127.0.0.1:4080/ name@myname.com inbox</command>
```

```
<command>addpair ExtTP  MyName    http://127.0.0.1:5081/
http://127.0.0.1:5081/ name@myname.com inbox</command>

<command>remotepair T1 MyName  ExtTP  http://127.0.0.1:4080/
http://127.0.0.1:4080/ name@myname.com inbox</command>

<command>remotepair T1 ExtTP  MyName  http://127.0.0.1:4080/
http://127.0.0.1:5081/ name@myname.com inbox</command>

<command>remotepair T2 MyName  ExtTP  http://127.0.0.1:5081/
http://127.0.0.1:4080/ name@myname.com inbox</command>

<command>remotepair T2 ExtTP  MyName  http://127.0.0.1:4080/
http://127.0.0.1:5081/ name@myname.com inbox</command>

# define keys

<command>importkey ExtTP MyName  E -fCpki\MyName.cer
-fKpki\MyName.prv</command>

<command>importkey ExtTP MyName  J -fCpki\ExtTP.cer</command>

<command>importkey MyName  ExtTP E -fCpki\MyName.cer
-fKpki\MyName.prv</command>

<command>importkey MyName  ExtTP J -fCpki\ExtTP.cer</command>

<command>remotekey ExtTP MyName  E -fCpki\MyName.cer
-fKpki\MyName.prv</command>

<command>remotekey ExtTP MyName  J -fCpki\ExtTP.cer</command>

<command>remotekey MyName  ExtTP E -fCpki\MyName.cer
-fKpki\MyName.prv</command>

<command>remotekey MyName  ExtTP J -fCpki\ExtTP.cer</command>

</xml>
```

Listing 6-4 p2pagent.cfg Sample Admin Text Command Definitions

The following command definitions apply to the commands used in Listing 6-4 *p2pagent.cfg Sample Admin Text*.

- The `set -ca` command sets the IP address to be used by the Commerce Suite to accept control messages from an Administrative Agent.

- The `set -cn` command sets the symbolic name to be used when referring to the Commerce Suite instance.
- The `set -gp` command sets the peer group to which the Commerce Suite instance belongs.
- The set `-ga` command specifies that the Commerce Suite is the primary Administrative Agent for the Commerce Suite clustered configuration.
- The `set -np` command specifies the file-system location where Commerce Suite stores notice files.
- The `set -nf` command specifies for notice records to be written to a file.
- The `set -nd-` specifies that notice records are not to be written to the database.
- The `set -lplog` command enables the writing of log information to a daily file and.
- The `set -lf` command specifies the file-system directory location in which to store daily log files. The `set -gr` command configures the Commerce Suite to perform the software router mode.
- The `set -opworkorder` command specifies the file-system location where Commerce Suite searches for work orders.
- The `addservers` command specifies Transport or Router servers that are to be remotely configured by an Administrative Agent.
- The `addpair` command specifies trading partner relationships.
- The `remotepair` command replicates a public-key pair to a remote host.
- The `importkey` command imports an X.509 certificate and corresponding private-key.
- The `remotekey` command replicates a public-key pair to a remote host.

6. Create a self-signed certificate for the admin agent. The associated Public/Private key pair is created in memory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   addkey MyName ExtTP O 1024 self
   C=US;S=TX;L=Dallas;O=iSoft;CN=MyName
   ```

   The `addkey` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing.

   a. Enter the following command to export key files into the `Admin` iSoft installation root directory:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   exportkey MyName ExtTP O ExtTP.cer ExtTP.prv
   ```

7. Move the **`MyName`**`.cer` and **`MyName`**`.prv` key files from the `c:\isoft\Admin` root directory into the admin machine's `c:\isoft\admin\pki` subdirectory.

8. From the admin machine `c:\isoft\admin\pki` subdirectory, copy the **`MyName`**`.cer` file and place a copy of it into the `c:\isoft\ExtTP\pki` subdirectory.

Creating a Stand-Alone Commerce Suite to Act as an External Trading Partner

This section describes the steps necessary to install and configure an external Commerce Suite trading partner used in testing Commerce Suite load balancing and failover functionality.

Note: Your stand-alone external Commerce Suite instance must be installed on a separate machine, referred to as the external trading partner machine, in order to conduct testing with the internal load balancing and failover configuration.

Perform the following steps to create a Commerce Suite to act as an external trading partner:

1. On your external trading partner machine, create a new `c:\isoft\ExtTP` subdirectory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent.exe` file into the `c:\isoft\ExtTP` subdirectory.
3. In the `c:\isoft\ExtTP` subdirectory, create a new `p2pagent.cfg` file.
4. Cut and paste the sample transport text in Listing 6-5 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 6-5 Commerce Suite Trading Partner p2pagent.cfg File

```
<xml>
#  External Trading Partner config
<command>set -eperror</command>
<command>set -ef</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -opworkorder</command>
<command>set -oswo</command>
<command>set -pppki</command>
<command>set -rpreceipt</command>
<command>set -tr300s</command>
#
<command>addpair ExtTP MyName http://127.0.0.1:5080/
mailto:as2@test.com as2@test.com inbox\ExtTP1</command>

<command>addpair MyName ExtTP http://127.0.0.1:4080/
mailto:as2@test.com as2@test.com inbox\MyName</command>
#
<command>importkey ExtTP MyName E -fCpki\ExtTP.cer -fKpki\
ExtTP1.prv</command>

<command>importkey ExtTP MyName J -fCpki\MyName.cer</command>
```

```
<command>importkey MyName ExtTP E -fCpki\ExtTP.cer -fKpki\
ExtTP.prv</command>

<command>importkey MyName ExtTP J -fCpki\MyName.cer</command>
#
<command>start http://127.0.0.1:4080</command>
#
</xml>
```

Note: Refer to Listing 6-2 for sample text command definitions.

5. Start the stand-alone Commerce Suite and monitor your console output for any start-up error messages. You will see initial errors on loading keys that have not been created. This is acceptable as you will create a certificate and private-key later in this procedure. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

6. Create a self-signed certificate for the external trading partner. The associated Public/Private key pair is created in memory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   addkey ExtTP MyName O 1024 self
   C=US;S=TX;L=Dallas;O=iSoft;CN=ExtTP
   ```

   The `addkey` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing.

   a. Enter the following command to export key files into the `ExtTP` root directory:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   exportkey ExtTP MyName O ExtTP.cer ExtTP.prv
   ```

7. Move the `ExtTP.cer` and `ExtTP.prv` key files from the `c:\isoft\ExtTP` root directory into the admin machine's `c:\isoft\admin\pki` subdirectory.

8. From the admin machine `c:\isoft\admin\pki` subdirectory, copy the `MyName.cer` file and place a copy of it into the `c:\isoft\ExtTP\pki` subdirectory.

Starting Your Remote Administration Cluster

This section details how to start, monitor, and test your remote administration cluster.

Starting the Router

Perform the following steps to start your router agent:

1. On your router machine, start the Commerce Suite application in the `c:\isoft\router` subdirectory of the router machine.
2. Monitor the console for the following output:

Listing 6-6 Commerce Suite Router Startup Console Output

```
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
2002.11.23 17:42:57.124       POPT OK  Control address set to
                                       [127.0.0.1]
2002.11.23 17:42:57.154       POPT OK  Control name set to [R1]
2002.11.23 17:42:57.184       POPT OK  Server is a router server
2002.11.23 17:42:57.214       POPT OK  Peer group set to [1]
2002.11.23 17:42:57.244       POPT OK  Notice path set to [notice]
2002.11.23 17:42:57.274       POPT OK  Notices will be written to
                                       file
2002.11.23 17:42:57.304       POPT OK  Log path set to [log]
```

```
2002.11.23 17:42:57.335       POPT OK  Trace set to WRITE_FILE
2002.11.23 17:42:57.405       RTRM OK  Router service started
```

3. Enter the command `set -m6` to set your trace level to debug.

Starting the First Transport

Perform the following steps to start the first Transport agent:

1. On your transport1 machine, start the Commerce Suite application in the `c:\isoft\transport1` subdirectory.
2. Monitor the transport console for the following representative significant output:

Listing 6-7 Commerce Suite Transport1 Startup Console Output

```
Listing 5-8
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
2002.11.23 17:43:02.412      POPT OK  Control address set to
                                      [127.0.0.1]
2002.11.23 17:43:02.442      POPT OK  Control name set to [T1]
2002.11.23 17:43:02.472      POPT OK  Control port set to [3501]
2002.11.23 17:43:02.502      POPT OK  Server is a transport server
2002.11.23 17:43:02.532      POPT OK  Peer group set to [1]
2002.11.23 17:43:02.562      POPT OK  Notice path set to [notice]
2002.11.23 17:43:02.592      POPT OK  Notices will be written to
                                      file
2002.11.23 17:43:02.622      POPT OK  Log path set to [log]
2002.11.23 17:43:02.652      POPT OK  Trace set to WRITE_FILE
```

3. Enter the console command `set -m6` to set your trace level to debug.

Starting the Second Transport

Perform the following steps to start the second Transport agent:

1. On your transport2 machine, start the Commerce Suite application in the `c:\isoft\transport2` subdirectory.
2. Monitor the transport console for the following representative significant output:

Listing 6-8 Commerce Suite Transport2 Startup Console Output

```
Listing 5-8
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
2002.11.23 17:43:02.412      POPT OK  Control address set to
                                      [127.0.0.1]
2002.11.23 17:43:02.442      POPT OK  Control name set to [T2]
2002.11.23 17:43:02.472      POPT OK  Control port set to [3501]
2002.11.23 17:43:02.502      POPT OK  Server is a transport server
2002.11.23 17:43:02.532      POPT OK  Peer group set to [1]
2002.11.23 17:43:02.562      POPT OK  Notice path set to [notice]
2002.11.23 17:43:02.592      POPT OK  Notices will be written to
                                      file
2002.11.23 17:43:02.622      POPT OK  Log path set to [log]
2002.11.23 17:43:02.652      POPT OK  Trace set to WRITE_FILE
```

3. Enter the `listpairs` command to check for any active trading partner relationships. Your console output should look similar to the following.

Listing 6-9 Transport2 listpair Command Console Output

```
listpairs
ok

0 pair(s)
```

4. Enter the `listkeys` command to check for any active public-key pairs. Your console output should look similar to the following.

Listing 6-10 Transport2 listkeys Command Console Output

```
listkeys
ok

0 key(s)
```

Starting the Administration Agent

Perform the following steps to start the admin agent:

1. On your admin machine, start the Commerce Suite application in the `c:\isoft\admin` subdirectory.
2. Monitor the admin console for the following representative significant output:

Listing 6-11 Commerce Suite Admin Startup Console Output

```
iSoft(R) Peer-to-Peer Agent(TM) for MQSeries(R)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
2002.11.23 18:03:40.232       POPT OK  Control address set to
                                       [127.0.0.1]
2002.11.23 18:03:40.262       POPT OK  Control name set to [A1]
```

```
2002.11.23 18:03:40.292       POPT OK  Peer group set to [1]
2002.11.23 18:03:40.322     POPT OK  Server is PRIMARY admin server
2002.11.23 18:03:40.352       POPT OK  Notice path set to [notice]
2002.11.23 18:03:40.382       POPT OK  Notices will be written to
                                       file
2002.11.23 18:03:40.412       POPT OK  Notices will not be written
                                       to data-source
2002.11.23 18:03:40.442       POPT OK  Log path set to [log]
2002.11.23 18:03:40.472       POPT OK  Trace set to WRITE_FILE
2002.11.23 18:03:40.502       POPT OK  Work Order path set to
                                       [workorder]
2002.11.23 18:03:40.512       POPT OK  Work Order file-spec set to
                                       [wo]
2002.11.23 18:03:40.622 82048 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 5]
2002.11.23 18:03:40.692 35825 HPOS OK  Outbound session started
-mbox=[0] batch=[0] attempt=[1 of 5]
2002.11.23 18:03:40.752 82048 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.23 18:03:40.793 53520 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 5]
2002.11.23 18:03:40.823 31192 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 5]
2002.11.23 18:03:40.853 09632 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 5]
2002.11.23 18:03:40.933 31192 HPOS OK  Outbound session stopping -
batch=[0]
2002.11.23 18:03:41.013 15505 HPOS OK  Outbound session stopping -
batch=[0]
```

Verifying the Remote Configuration Process

The remote configuration process consists of adding servers to control, sending trading partner information to each server, and sending certificate information to each transport server.

Perform the following steps to start the remote configuration process:

1. Start the Commerce Suite admin agent.

2. Monitor your router console output after starting the admin agent by entering the following command.

```
set -m3
```

Your output should look similar to the following:

Listing 6-12 Router Console Output

```
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
2002.11.26 23:13:13.018     POPT OK  Control address set to
                                     [127.0.0.1]
2002.11.26 23:13:13.058     POPT OK  Control name set to [R1]
2002.11.26 23:13:13.098     POPT OK  Server is a router server
2002.11.26 23:13:13.138     POPT OK  Peer group set to [1]
2002.11.26 23:13:13.178     POPT OK  Notice path set to [notice]
2002.11.26 23:13:13.218     POPT OK  Notices will be written to
                                     file
2002.11.26 23:13:13.248     POPT OK  Log path set to [log]
2002.11.26 23:13:13.278     POPT OK  Trace set to WRITE_FILE
2002.11.26 23:13:13.368     RTRM OK  Router service started
2002.11.26 23:13:37.153     PBCN OK  peer 127.0.0.1:5082 http added
2002.11.26 23:13:43.311     PBCN OK  peer 127.0.0.1:5083 http added
```

3. On each transport agent, enter the `listpairs` command to display active trading partner relationships. The transport agent has received this trading partner information from the admin agent. The transport agent console output should display results similar to the following code sample.

Listing 6-13 Transport1 listpairs Command Console Output

```
listpairs
ok

From:         MyName
To:           ExtTP
URL:          http://127.0.0.1:4080/
Receipt:      http://127.0.0.1:4080/
Notify:       name@myname.com
```

```
Inbox:        *
Direction:    outbound
Params:

From:         ExtTP\
To:           MyName
URL:          http://127.0.0.1:5081/
Receipt:      http://127.0.0.1:5081/
Notify:       name@myname.com
Inbox:        *
Direction:    outbound
Params:

2 pair(s)
```

4. On each transport agent, enter the `listkeys` command to display the active public-key pairs. This key-pair information was received from the admin control agent. The console output should display results similar to the following code sample:

Listing 6-14 Sample Transport Agent listkeys Command Console Output

```
listkeys
ok

From:         ExtTP
To:           MyName
Usage:        E ( Sign Decrypt )
Cert File:
Key File:
Valid From:   020815192708Z
Valid To:     030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Serial No.:   20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:   604
```

```
From:         ExtTP
To:           MyName
Usage:        J ( Encrypt Verify )
Cert File:
Key File:
Valid From:   020815192708Z
Valid To:     030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@isf
t.com
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Serial No.:   20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:   604

From:         MyName
To:           ExtTP
Usage:        E ( Sign Decrypt )
Cert File:
Key File:
Valid From:   020815192708Z
Valid To:     030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Serial No.:   20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:   604

From:         MyName
To:           ExtTP
Usage:        J ( Encrypt Verify )
Cert File:
Key File:
Valid From:   020815192708Z
Valid To:     030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com\
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
```

```
ft.com
Serial No.:  20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:  604

4 key(s)
```

5. Monitor your first transport under admin control by going to the Transport1 console and enter the following command:

   ```
   set -m6
   ```

   The following code sample displays console output for the transport agent receiving control messages from the admin agent.

Listing 6-15 Transport Console Output

```
set -m6
ok
2002.11.18 22:28:49.947       POPT OK  Trace-level set to [DEBUG]
2002.11.18 22:28:49.957       PCMD OK  End of ProcessCommand
2002.11.18 22:28:59.070      OBCM OK  Ping: 7F 00 00 01 13 DA 03 31
2002.11.18 22:29:05.510 79556 CTLS OK  control client:
127.0.0.1:1575
2002.11.18 22:29:05.520 85681 CTLS OK  control client:
127.0.0.1:1576
2002.11.18 22:29:05.530 85681 CTLS OK  40 bytes read
2002.11.18 22:29:05.540 85681 PHDR OK  End of headers found
2002.11.18 22:29:05.550 85681 DCTL OK  Decomposing control message
2002.11.18 22:29:05.560 85681 DCTL OK  Control message decomposed
2002.11.18 22:29:05.580 85681 CTLS OK  19 bytes written
2002.11.18 22:29:05.590 79556 CTLS OK  120 bytes read
2002.11.18 22:29:05.600 79556 PHDR OK  HTTP protocol version is 1.0
2002.11.18 22:29:05.610 79556 PHDR OK
Content-Type=[isoftp2p/command]
2002.11.18 22:29:05.620 79556 PHDR OK  Content-Length=[27]
2002.11.18 22:29:05.630 79556 PHDR OK  End of headers found
2002.11.18 22:29:05.640 79556 DCTL OK  Decomposing control message
2002.11.18 22:29:05.650 79556 DCMD OK  Decomposing P2P command
2002.11.18 22:29:05.670 79556 DCMD OK  P2P command decomposed
2002.11.18 22:29:05.680 79556 DCTL OK  Control message decomposed
2002.11.18 22:29:05.690 79556 CTLS OK  19 bytes written
2002.11.18 22:29:05.710       PCMD OK  Start of ProcessCommand
2002.11.18 22:29:05.720       PSTR OK  Start of
                                       ProcessStartCommand()
```

```
2002.11.18 22:29:05.740      SINB OK  Inbound controller already
                                      started
2002.11.18 22:29:05.750      PSTR OK  End of ProcessStartCommand()
2002.11.18 22:29:05.760      PCMD OK  End of ProcessCommand
2002.11.18 22:29:09.145      OBCM OK  Ping: 7F 00 00 01 13 DA 03 31
```

Testing the Remote Administration Configuration

Testing your remote administration configuration consists of verifying the sending and receiving of files between Commerce Suite instances within the remotely configured cluster. To test your configuration, perform the steps in the following two sections:

- Receiving Files on the Remote Administration Cluster
- Sending Files From the Remote Administration Cluster

Receiving Files on the Remote Administration Cluster

Perform the following steps to test your remote administration configuration.

1. In the `c:\isoft\ExtTP` subdirectory of the ExtTP machine, open Notepad and create and save a file named `Send2.wo`.
2. Cut and paste the sample `Send2.wo` command text in Listing 6-16 into the `Send2.wo` file you created. Start with the `<xml>` and end with `</xml>` tag.

Listing 6-16 Send2.wo Sample File

```
<command>send http ExtTP MyName -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>
```

3. On your external trading partner machine, initiate a file send from the Commerce Suite application. Enter the following command to process a file send.

   ```
   batch send2.wo
   ```

   This command will send multiple files, perform encryption, and request a signed receipt. Monitor the router and multiple transport consoles on their respective machines.

4. Monitor the router agent console. You will see output similar to the following output sample on your cluster router.

Listing 6-17 Sample Router Console Output

```
2002.11.26 23:16:55.358 36177 RTRS OK  Router session started
2002.11.26 23:16:55.378 76850 RTRS OK  Router session started
2002.11.26 23:16:57.130 36177 RTRS OK  Server has disconnected
2002.11.26 23:16:57.150 36177 RTRS OK  Router session stopping
2002.11.26 23:16:57.210 76850 RTRS OK  Server has disconnected
2002.11.26 23:16:57.260 76850 RTRS OK  Router session stopping
```

5. Monitor the transport agent consoles. You will see output similar to the following output sample for both your transport agents.

Listing 6-18 Sample Transport1 and Transport2 Console Output

```
2002.11.26 23:13:33.888       HPIM OK  HTTP inbound service started
2002.11.26 23:16:55.388 41583 HPIS OK  HTTP inbound session started
2002.11.26 23:16:55.398 41583 HPIS OK  HTTP client: 127.0.0.1:1282
2002.11.26 23:16:56.249 41583 DECR OK  ** Content decrypted **
2002.11.26 23:16:56.329 41583 VRFY OK  ** Signature verified **
2002.11.26 23:16:57.150 41583 HPIS OK  HTTP inbound session stopping
```

6. View the contents of the transport agent's `/notice` subdirectory. The subdirectory will be populated with files received on the transport and waiting for admin pickup.
7. View the contents of the admin agent's `/inbox` subdirectory. The subdirectory should be populated with the files being pulled by the admin agent.

   As you watch both directories, you will see the files moving from one location to another.
8. To provide a larger work load, create a new work order file that contains ten `send` commands.
9. Open Notepad on the external trading partner machine and cut and paste the following code sample into a new `send10.wo` text file.

Listing 6-19 Commerce Suite Sample Work Order File

```
<xml>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>
```

```
<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

</xml>
```

10. Name the new text file `send10.wo` and place it in the `c:\isoft\ExtTP` subdirectory.

11. Enter the following command to initiate the `send10.wo` work order file.

    ```
    batch send10.wo
    ```

    Monitor the files moving from the transport directories to the admin agent inbox.

Sending Files From the Remote Administration Cluster

Perform the following steps to test your remote administration configuration.

1. In the `c:\isoft\admin` subdirectory of the admin machine, open Notepad and create and save a file named `Rsend2.wo`.

2. Cut and paste the sample `Rsend2.wo` command text in Listing 6-20 into the `Send2.wo` file you created. Start with the `<xml>` and end with `</xml>` tag.

Listing 6-20 Rsend2.wo Sample File

```
<command>send http MyName ExtTP -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>

<command>send http MyName ExtTP -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>
```

3. Monitor your admin agent console output by opening the admin console and entering the following command:

   ```
   set -m3
   ```

4. Monitor your transport agent's console output by opening both transport consoles and entering the following command:

   ```
   set -m3
   ```

5. Perform a remote send operation to the external partner by entering the following command at the admin agent console:

   ```
   batch rsend2.wo
   ```

6. Monitor the admin console output. It should look similar to the following output.

Listing 6-21 Admin Console Output

```
batch rsend2.txt
ok
2002.11.26 23:21:43.772 71834 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 5]

2002.11.26 23:21:43.832 71834 HPOS OK  Outbound session stopping -
batch=[0]

2002.11.26 23:21:43.842 67665 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 5]
```

```
2002.11.26 23:21:43.932 67665 HPOS OK  Outbound session stopping -
batch=[0]
```

7. Monitor the transport consoles for outbound transmissions.

   Your output should look similar to the following sample output.

Listing 6-22 Transport Outbound Transmission Output

```
2002.11.23 21:34:52.844 32174 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 1]

2002.11.23 21:34:54.266 32174 VRFY OK  ** Signature verified **

2002.11.23 21:34:54.316 32174 PMDN OK  ** Original-Content-MIC
found in MDN **

2002.11.23 21:34:54.396 32174 HPOS OK  Outbound session stopping -
batch=[0]
```

8. Monitor your external trading partner console to ensure the files are being received. Your output should look similar to the following sample output.

Listing 6-23 External Trading Partner Output

```
2002.11.23 21:34:53.385 35415 HPIS OK  HTTP inbound session started
2002.11.23 21:34:53.425 35415 HPIS OK  HTTP client: 127.0.0.1:1376
2002.11.23 21:34:53.505 35415 VRFY OK  ** Signature verified **
2002.11.23 21:34:53.936 98252 HPIS OK  HTTP inbound session started
2002.11.23 21:34:53.976 98252 HPIS OK  HTTP client: 127.0.0.1:1377
2002.11.23 21:34:54.056 98252 VRFY OK  ** Signature verified **
2002.11.23 21:34:54.266 35415 HPIS OK  HTTP inbound session stopping
2002.11.23 21:34:54.627 98252 HPIS OK  HTTP inbound session stopping
```

CHAPTER

7 Configuring Commerce Suite Database Remote Administration

If you have not performed a basic Commerce Suite configuration, refer to Chapter 4, *Configuring Commerce Suite and Testing with iSoft*.

This chapter describes how to install and configure Commerce Suite router, transport, and admin agents for database remote configuration capabilities. Detailed instructions on starting both agents and creating a Commerce Suite to act as a trading partner are also included.

Note: In order to test your Commerce Suite instances for remote configuration, it is recommended that you install each Commerce Suite instance on a separate machine.

Performing a remote database configuration requires a full licensed copy of the Commerce Suite software with database capability. The free Wal-Mart Commerce Suite copy does not support a remote administration configuration.

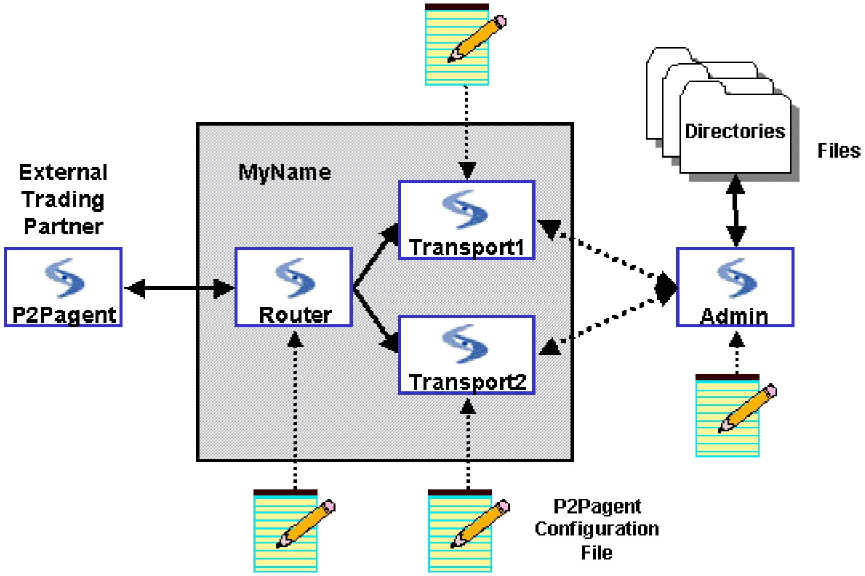
This section contains the following sections:

- Installing and Configuring a Router Agent for Remote Administration
- Installing and Configuring Multiple Transport Agents
- Starting Your Remote Administration Cluster

- Testing the Remote Administration Configuration

The following diagram illustrates how the Commerce Suite router, transport, and admin agents enable remote administration capabilities with an external trading partner.

Figure 7-1 Commerce Suite Remote Administration Capabilities



Installing and Configuring a Router Agent for Remote Administration

This section describes the steps necessary to install and configure a Commerce Suite Router agent using a basic Commerce Suite text configuration file.

Note: Your Commerce Suite Router agent instance must be installed on a separate machine, referred to as the router machine, in order to perform remote administration testing with other Commerce Suite instances.

Perform the following steps to install and configure your Commerce Suite Router agent:

1. On your router machine, create a separate `router` subdirectory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent_odbc.exe` file to the `router` subdirectory.
3. Create a `\log` subdirectory within the `router` subdirectory.
4. Open Notepad and create and save a file named `p2pagent.cfg` in the `router` agent installation directory.
5. Cut and paste the sample router text in Listing 5-1 into the `p2pagent.cfg` file you created. Start with the `<xml>` tag and end with the `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 7-1 p2pagent.cfg Sample Router Text

```
<xml>

#Router minimum remote admin start-up configuration
<command>set -npnotice</command>
<command>set -nf</command>
<command>start p2p://127.0.0.1:6081</command>
<command>start router</command>

</xml>
```

Listing 7-1 p2pagent.cfg Sample Router Text Command Definitions

The following command definitions apply to the commands used in Listing 7-1 *p2pagent.cfg Sample Router Text*.

- The `set -np` command specifies the file-system location where Commerce Suite stores notice files.
- The `set -nf` command specifies for notice records to be written to a file.
- The `start p2p://` command specifies the control address for the remote agent.
- The `start router` command specifies to start the Commerce Suite router agent.

Installing and Configuring Multiple Transport Agents

The following sections provide instructions on installing and configuring multiple transport agents for testing Commerce Suite's remote administration capabilities.

- Installing and Configuring a Transport Agent
- Installing and Configuring a Second Transport Agent
- Creating a Stand-Alone Commerce Suite to Act as an External Trading Partner

Installing and Configuring a Transport Agent

This section describes the steps necessary to install and configure a Commerce Suite Transport agent using a basic Commerce Suite startup text configuration file.

Note: Your Commerce Suite Transport agent instance must be installed on a separate machine, referred to as the transport1 machine, in order to perform remote administration testing with other Commerce Suite instances.

Perform the following steps to install and configure your first Commerce Suite Transport agent:

1. On your transport1 machine, create a separate `c:\isoft\transport1` directory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent_odbc.exe` file to the `c:\isoft\transport1` subdirectory.
3. Open Notepad and create and save a `p2pagent.cfg` file in the `c:\isoft\transport1` subdirectory.
4. Cut and paste the sample transport text in Listing 7-2 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

   Note: For testing purposes in the following code sample, the ***MyName*** variable is used as a placeholder to represent your AS2 name. You can change the ***MyName*** variable to a more meaningful name, however you must ensure that all ***MyName*** variable references in the `p2pagent.cfg` file are changed or else you may encounter errors.

   All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 7-2 p2pagent.cfg Sample Transport1 Text

```
<xml>

Transport1 Minimum database remote admin config
<command>set -npnotice</command>
<command>set -nf</command>

</xml>
```

Listing 7-2 p2pagent.cfg Sample Transport1 Text Command Definitions

The following command definitions apply to the commands used in Listing 7-2 *p2pagent.cfg Sample Transport1 Text*.

- The `set -npnotice` command specifies the file-system location where Commerce Suite stores notice files.
- The `set -nf` command specifies whether notice records are to be written to files.

5. Create the following subdirectories in the `c:\iSoft` installation directory:
   - `\error`
   - `\log`
   - `\notice`
6. On your transport1 machine, start the Commerce Suite transport agent and monitor your console output for any start-up error messages. Refer to Chapter 2, "Starting and Stopping P2P Agent," for instructions on starting the application. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

Installing and Configuring a Second Transport Agent

This section describes the steps necessary to install and configure a second Commerce Suite Transport agent used in testing Commerce Suite remote administration functionality.

Note: Your Commerce Suite Transport agent instance must be installed on a separate machine, referred to as the transport2 machine, in order to perform remote administration testing with other Commerce Suite instances.

Perform the following steps to install and configure your Commerce Suite Transport agent:

1. On your transport2 machine, create a separate `c:\isoft\transport2` directory within your existing `c:\iSoft` installation root directory.
2. Copy the `p2pagent_odbc.exe` file to the `c:\isoft\transport2` subdirectory.
3. Open Notepad and create a `p2pagent.cfg` file in the `c:\isoft\transport2` subdirectory.
4. Cut and paste the sample transport text in Listing 7-3 into the `p2pagent.cfg` file you created. Start with the `<xml>` and end with `</xml>` tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 7-3 p2pagent.cfg Sample Transport2 Text

```
<xml>
#Transport2 Minimum database remote admin config
<command>set -npnotice</command>
<command>set -nf</command>

</xml>
```

Note: Refer to Listing 7-2 for sample text command definitions.

5. Create the following subdirectories in the `c:\iSoft` installation directory:
   - `\error`
   - `\log`
   - `\notice`

Creating a Commerce Suite Administration Agent

Creating a Commerce Suite Administrative Agent requires that the Commerce Suite instance be installed on a separate machine, referred to as the admin machine. This configuration enables you to perform remote configuration with other Commerce Suite instances from configuration information stored in a database.

Perform the following steps to install and configure your admin agent:

1. On your designated admin machine, create a separate `c:\isoft\admin` subdirectory within your existing `c:\isoft` installation root directory.
2. Copy the `p2pagent_odbc.exe` file to the `admin` subdirectory.
3. Create a `\log` subdirectory within the `admin` subdirectory.
4. Open Notepad and create a `p2pagent.cfg` file in the admin agent installation directory.
5. Cut and paste the sample admin text in Listing 5-4 into the `p2pagent.cfg` file. Include the `<xml>` and `</xml>` tags when you cut and paste.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 7-4 p2pagent.cfg Sample Admin Text

```
<xml>

# Admin Config
<command>set -ca127.0.0.1</command>
<command>set -cnA1</command>
<command>set -nd-</command>
<command>set -df</command>
<command>set -lplog</command>
<command>set -lf</command>
```

```
<command>set -opworkorder -oswo</command>
#define servers
<command>getservers</command>
#define trading pairs
<command>getpairs</command>
#define keys
<command>getkeys</command>

</xml>
```

Listing 7-4 p2pagent.cfg Sample Admin Text Command Definitions

The following command definitions apply to the commands used in Listing 7-4 *p2pagent.cfg Sample Admin Text*.

- The `set -ca` command sets the IP address to be used by the Commerce Suite to accept control messages from an Administrative Agent.
- The `set -cn` command sets the symbolic name to be used when referring to the Commerce Suite instance.
- The `set -gp` command sets the peer group to which the Commerce Suite instance belongs.
- The set `-ga` command specifies that the Commerce Suite is the primary Administrative Agent for the Commerce Suite clustered configuration.
- The `set -np` command specifies the file-system location where Commerce Suite stores notice files.
- The `set -nf` command specifies for notice records to be written to a file.
- The `set -nd-` specifies that notice records are not to be written to the database.
- The `set -df` command specifies configuration updates made to local memory storage should be replicated immediately to the database.
- The `set -lplog` command enables the writing of log information to a daily file and.

- The `set -lf` command specifies the file-system directory location in which to store daily log files. The `set -gr` command configures the Commerce Suite to perform the software router mode.
- The `set -opworkorder` command specifies the file-system location where Commerce Suite searches for work orders.
- The `getservers` command reads server/protocol settings from the database. The `getservers` command retrieves all remote service and agent information from the database and populates the Commerce Suite memory with the material needed to remotely configure agents and issue remote commands.
- The `getpairs` command reads trading partner relationship data from the database. The `getpairs` command retrieves all trading partner relationship information from the database and populates the Commerce Suite memory with the configuration material needed to process message transfers.
- The `getkeys` command reads public key information from the database. The `getkeys` command retrieves all certificate and key material information from the database and populates the Commerce Suite memory with the security material needed to process message transfers.

6. Create a self-signed certificate for the admin agent. The associated Public/Private key pair is created in memory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   addkey MyName ExtTP O 1024 self
   C=US;S=TX;L=Dallas;O=iSoft;CN=MyName
   ```

   The `addkey` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing.

   a. Enter the following command to export key files into the `Admin` iSoft installation root directory:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   exportkey MyName ExtTP O ExtTP.cer ExtTP.prv
   ```

7. Move the **MyName**.cer and **MyName**.prv key files from the c:\isoft\Admin root directory into the admin machine's c:\isoft\admin\pki subdirectory.

8. From the admin machine c:\isoft\admin\pki subdirectory, copy the **MyName**.cer file and place a copy of it into the c:\isoft\ExtTP\pki subdirectory.

Creating a Stand-Alone Commerce Suite to Act as an External Trading Partner

This section describes the steps necessary to install and configure an external Commerce Suite trading partner used in testing Commerce Suite load balancing and failover functionality.

Note: Your stand-alone external Commerce Suite instance must be installed on a separate machine, referred to as the external trading partner machine, in order to conduct testing with the internal load balancing and failover configuration.

Perform the following steps to create a Commerce Suite to act as an external trading partner:

1. On your external trading partner machine, create a new c:\isoft\ExtTP subdirectory within your existing c:\iSoft installation root directory.

2. Copy the p2pagent.exe file into the c:\isoft\ExtTP subdirectory.

3. In the c:\isoft\ExtTP subdirectory, create a new p2pagent.cfg file.

4. Cut and paste the sample transport text in Listing 7-5 into the p2pagent.cfg file you created. Start with the <xml> and end with </xml> tag.

   Note: All IP addresses listed in the following code sample are placeholders for example purposes. You must replace these sample IP addresses with your actual IP addresses or you will experience errors when trying to send data.

Listing 7-5 Commerce Suite Trading Partner p2pagent.cfg File

```
<xml>
#  External Trading Partner config
<command>set -eperror</command>
<command>set -ef</command>
<command>set -lplog</command>
<command>set -lf</command>
<command>set -npnotice</command>
<command>set -nf</command>
<command>set -opworkorder</command>
<command>set -oswo</command>
<command>set -pppki</command>
<command>set -rpreceipt</command>
<command>set -tr300s</command>
#
<command>addpair ExtTP MyName http://127.0.0.1:5080/
mailto:as2@test.com as2@test.com inbox\ExtTP1</command>

<command>addpair MyName ExtTP http://127.0.0.1:4080/
mailto:as2@test.com as2@test.com inbox\MyName</command>
#
<command>importkey ExtTP MyName E -fCpki\ExtTP.cer -fKpki\
ExtTP1.prv</command>

<command>importkey ExtTP MyName J -fCpki\MyName.cer</command>

<command>importkey MyName ExtTP E -fCpki\ExtTP.cer -fKpki\
ExtTP.prv</command>

<command>importkey MyName ExtTP J -fCpki\MyName.cer</command>
#
<command>start http://127.0.0.1:4080</command>
#
</xml>
```

Note: Refer to Listing 7-2 for sample text command definitions.

5. Start the stand-alone Commerce Suite and monitor your console output for any start-up error messages. Refer to Chapter 2, “Starting and Stopping P2P Agent,” for instructions on starting the application. If any errors are detected, examine the configuration file for syntax, spelling, or case-matching errors.

Note: You will see initial errors on loading keys that have not been created. This is acceptable as you will create a certificate and private-key later in this procedure. You will also create an external trading partner certificate that will be required in a later step.

6. Create a self-signed certificate for the external trading partner. The associated Public/Private key pair is created in memory by entering the following command:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   addkey ExtTP MyName O 1024 self
   C=US;S=TX;L=Dallas;O=iSoft;CN=ExtTP
   ```

   The `addkey` command will return an `ok` status. Wait for the console to display the message `key pair generated` before continuing.

   a. Enter the following command to export key files into the `ExtTP` root directory:

   Note: The first line of the following code sample contains an alphabetic character O, not the number zero.

   ```
   exportkey ExtTP MyName O ExtTP.cer ExtTP.prv
   ```

7. Move the `ExtTP.cer` and `ExtTP.prv` key files from the `c:\isoft\ExtTP` root directory into the admin machine's `c:\isoft\admin\pki` subdirectory.

8. From the admin machine `c:\isoft\admin\pki` subdirectory, copy the `MyName.cer` file and place a copy of it into the `c:\isoft\ExtTP\pki` subdirectory.

Starting Your Remote Administration Cluster

This section details how to start, monitor, and test your remote administration cluster.

Starting the Router

Perform the following steps to start your router agent:

1. On your router machine, start the Commerce Suite application in the `c:\isoft\router` subdirectory of the router machine.
2. From within the `c:\isoft\router` directory, start the Commerce Suite application.
3. Monitor the console for the following representative output:

Listing 7-6 Commerce Suite Router Startup Console Output

```
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
2002.11.23 17:42:57.405 RTRM OK Router service started
```

Starting the First Transport

Perform the following steps to start the first Transport agent:

1. On your transport1 machine, start the Commerce Suite application in the `c:\isoft\transport1` subdirectory.
2. Monitor the transport console for the following representative significant output:

Listing 7-7 Commerce Suite Transport1 Startup Console Output

```
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
```

```
Authorized License
2002.11.23 17:42:57.405 RTRM OK Router service started
```

Starting the Second Transport

Perform the following steps to start the second Transport agent:

1. On your transport2 machine, start the Commerce Suite application in the `c:\isoft\transport2` subdirectory.
2. Monitor the transport console for the following representative significant output:

Listing 7-8 Commerce Suite Transport2 Startup Console Output

```
Listing 5-8
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Oct 28 2002 13:37:12]
Standard Edition
Authorized License
```

3. Enter the `listpairs` command to check for any active trading partner relationships. Your console output should look similar to the following.

Listing 7-9 Transport2 listpair Command Console Output

```
listpairs
ok

0 pair(s)
```

4. Enter the `listkeys` command to check for any active public-key pairs. Since the Commerce Suite admin has not pushed keys to the transports, your console output should look similar to the following:

Listing 7-10 Transport2 listkeys Command Console Output

```
listkeys
ok

0 key(s)
```

Starting the Administration Agent

Perform the following steps to start the admin agent:

1. On your admin machine, start the Commerce Suite application in the `c:\isoft\admin` subdirectory.
2. Monitor the admin console for output.

Verifying the Remote Configuration Process

The remote configuration process consists of adding servers to control, sending trading partner information to each server, and sending certificate information to each transport server.

Perform the following steps to start the remote configuration process:

1. Start the Commerce Suite admin agent.
2. Monitor your router console output after starting the admin agent by entering the following command.

   ```
   set -m3
   ```

3. On each transport agent, enter the `listpairs` command to display active trading partner relationships. The transport agent has received this trading partner information from the admin agent. The transport agent console output should display results similar to the following code sample.

Listing 7-11 Transport1 listpairs Command Console Output

```
listpairs
ok

From:        MyName
To:          ExtTP
URL:         http://127.0.0.1:4080/
Receipt:     http://127.0.0.1:4080/
Notify:      name@myname.com
Inbox:       *
Direction:   outbound
Params:

From:        ExtTP\
To:          MyName
URL:         http://127.0.0.1:5081/
Receipt:     http://127.0.0.1:5081/
Notify:      name@myname.com
Inbox:       *
Direction:   outbound
Params:

2 pair(s)
```

4. On each transport agent, enter the `listkeys` command to display the active public-key pairs. This key-pair information was received from the admin control agent. The console output should display results similar to the following code sample:

Listing 7-12 Sample Transport Agent listkeys Command Console Output

```
listkeys
ok
```

```
From:         ExtTP
To:           MyName
Usage:        E ( Sign Decrypt )
Cert File:
Key File:
Valid From:  020815192708Z
Valid To:    030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Serial No.:  20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:  604

From:         ExtTP
To:           MyName
Usage:        J ( Encrypt Verify )
Cert File:
Key File:
Valid From:  020815192708Z
Valid To:    030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@isf
t.com
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Serial No.:  20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:  604

From:         MyName
To:           ExtTP
Usage:        E ( Sign Decrypt )
Cert File:
Key File:
Valid From:  020815192708Z
Valid To:    030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
```

```
ft.com
Serial No.:  20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:  604

From:        MyName
To:          ExtTP
Usage:       J ( Encrypt Verify )
Cert File:
Key File:
Valid From:  020815192708Z
Valid To:    030815192708Z
X.509 Usage: E4
Subject:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com\
Issuer:
C=US;S=TX;L=Dallas;O=iSoft;OU=eCommerce;CN=as2test;E=dwalling@is
ft.com
Serial No.:  20 02 08 0F 13 1B 0A 03 14 99 8E FB 67 16 39 C7
Cert Length: 674
Key Length:  604

4 key(s)
```

5. Monitor your first transport console output by opening the transport console and entering the following command:

   ```
   set -m6
   ```

   The following code sample displays console output for the transport agent receiving control messages from the admin agent.

Listing 7-13   Transport Console Output

```
set -m6
ok
2002.11.18 22:28:49.947       POPT OK  Trace-level set to [DEBUG]
2002.11.18 22:28:49.957       PCMD OK  End of ProcessCommand
2002.11.18 22:28:59.070      OBCM OK  Ping: 7F 00 00 01 13 DA 03 31
2002.11.18 22:29:05.510 79556 CTLS OK  control client:
127.0.0.1:1575
2002.11.18 22:29:05.520 85681 CTLS OK  control client:
127.0.0.1:1576
2002.11.18 22:29:05.530 85681 CTLS OK  40 bytes read
```

```
2002.11.18 22:29:05.540 85681 PHDR OK  End of headers found
2002.11.18 22:29:05.550 85681 DCTL OK  Decomposing control message
2002.11.18 22:29:05.560 85681 DCTL OK  Control message decomposed
2002.11.18 22:29:05.580 85681 CTLS OK  19 bytes written
2002.11.18 22:29:05.590 79556 CTLS OK  120 bytes read
2002.11.18 22:29:05.600 79556 PHDR OK  HTTP protocol version is 1.0
2002.11.18 22:29:05.610 79556 PHDR OK
Content-Type=[isoftp2p/command]
2002.11.18 22:29:05.620 79556 PHDR OK  Content-Length=[27]
2002.11.18 22:29:05.630 79556 PHDR OK  End of headers found
2002.11.18 22:29:05.640 79556 DCTL OK  Decomposing control message
2002.11.18 22:29:05.650 79556 DCMD OK  Decomposing P2P command
2002.11.18 22:29:05.670 79556 DCMD OK  P2P command decomposed
2002.11.18 22:29:05.680 79556 DCTL OK  Control message decomposed
2002.11.18 22:29:05.690 79556 CTLS OK  19 bytes written
2002.11.18 22:29:05.710       PCMD OK  Start of ProcessCommand
2002.11.18 22:29:05.720       PSTR OK  Start of
                                       ProcessStartCommand()
2002.11.18 22:29:05.740       SINB OK  Inbound controller already
                                       started
2002.11.18 22:29:05.750       PSTR OK  End of ProcessStartCommand()
2002.11.18 22:29:05.760       PCMD OK  End of ProcessCommand
2002.11.18 22:29:09.145       OBCM OK  Ping: 7F 00 00 01 13 DA 03 31
```

Testing the Remote Administration Configuration

Testing your remote administration configuration consists of verifying the sending and receiving of files between Commerce Suite instances within the remotely configured cluster. To test your configuration, perform the steps in the following two sections:

- Receiving Files on the Remote Administration Cluster
- Sending Files From the Remote Administration Cluster

Receiving Files on the Remote Administration Cluster

Perform the following steps to test your remote administration configuration.

1. In the `c:\isoft\ExtTP` subdirectory of the ExtTP machine, open Notepad and create and save a file named `Send2.wo`.
2. Cut and paste the sample `Send2.wo` command text in Listing 7-14 into the `Send2.wo` file you created. Start with the `<xml>` and end with `</xml>` tag.

Listing 7-14 Send2.wo Sample File

```
<command>send http ExtTP MyName -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>
```

3. On your external trading partner machine, initiate a file send from the Commerce Suite application. Enter the following command to process a file send.

   ```
   batch send2.wo
   ```

   This command will perform encryption and request a receipt. Monitor the router and multiple transport consoles on their respective machines.
4. Open your router agent consoles to monitor their output. You will see output similar to the following output sample for both your transport agents.

Listing 7-15 Commerce Suite Sample Router Console Output

```
2002.11.26 23:16:55.358 36177 RTRS OK  Router session started
2002.11.26 23:16:55.378 76850 RTRS OK  Router session started
2002.11.26 23:16:57.130 36177 RTRS OK  Server has disconnected
2002.11.26 23:16:57.150 36177 RTRS OK  Router session stopping
2002.11.26 23:16:57.210 76850 RTRS OK  Server has disconnected
2002.11.26 23:16:57.260 76850 RTRS OK  Router session stopping
```

5. Open your transport agent consoles to monitor their output. You will see output similar to the following output sample for both your transport agents.

Listing 7-16 Commerce Suite Sample Transport1 and Transport2 Console Output

```
2002.11.23 21:33:22.444 HPIM OK HTTP inbound service started
2002.11.23 21:34:05.947 32483 HPIS OK HTTP inbound session started
2002.11.23 21:34:05.967 32483 HPIS OK HTTP client: 127.0.0.1:1345
2002.11.23 21:34:06.327 79372 HPIS OK HTTP inbound session started
2002.11.23 21:34:06.487 79372 HPIS OK HTTP client: 127.0.0.1:1349
2002.11.23 21:34:07.980 32483 DECR OK ** Content decrypted **
2002.11.23 21:34:08.240 32483 VRFY OK ** Signature verified **
2002.11.23 21:34:08.530 79372 DECR OK ** Content decrypted **
2002.11.23 21:34:08.711 79372 VRFY OK ** Signature verified **
2002.11.23 21:34:09.692 79372 HPIS OK HTTP inbound session stopping
2002.11.23 21:34:09.762 32483 HPIS OK HTTP inbound session stopping
2002.11.23 21:34:10.103 01977 HPIS OK HTTP inbound session started
2002.11.23 21:34:10.163 01977 HPIS OK HTTP client: 127.0.0.1:1353
2002.11.23 21:34:11.004 01977 DECR OK ** Content decrypted **
2002.11.23 21:34:11.465 01977 VRFY OK ** Signature verified **
2002.11.23 21:34:12.887 01977 HPIS OK HTTP inbound session stopping
2002.11.23 21:34:13.087 62188 HPIS OK HTTP inbound session started
```

6. View the contents of the transport agent’s `/notice` subdirectory. The subdirectory will be populated with files received on the transport and waiting for admin pickup.

7. View the contents of the admin agent's `/inbox` subdirectory. The subdirectory should be populated with the files being pulled by the admin agent.

   As you watch both directories, you will see the files moving from one location to another.

8. To provide a larger work load, create a new work order file that contains ten `send` commands.

9. Open Notepad on the external trading partner machine and cut and paste the following code sample into a new `send10.wo` text file.

Listing 7-17 Commerce Suite Sample Work Order File

```
<xml>
<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>

<command>send http ExtTP MyName -fNp2pagent.cfg -n1 -sC -e
-r1</command>
</xml>
```

10. Name the new text file `send10.wo` and place it in the `c:\isoft\ExtTP` subdirectory.

11. Enter the following command to initiate the `send10.wo` work order file.

    ```
    batch send10.wo
    ```

    Monitor the files moving from the transport directories to the admin agent inbox.

Sending Files From the Remote Administration Cluster

Perform the following steps to test your remote administration configuration.

1. In the `c:\isoft\admin` subdirectory of the admin machine, open Notepad and create and save a file named `Rsend2.wo`.

2. Cut and paste the sample `Rsend2.wo` command text in Listing 7-18 into the `Send2.wo` file you created. Start with the `<xml>` and end with `</xml>` tag.

Listing 7-18 Rsend2.wo Sample File

```
<command>send http MyName ExtTP -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>

<command>send http MyName ExtTP -fNoutbox\edix12.txt -cE -n1 -sC -e
-r1</command>
```

3. Monitor your admin agent console output by opening the admin console and entering the following command:

    ```
    set -m3
    ```

4. Perform a remote send operation to the external partner by entering the following command at the admin agent console:

```
batch rsend2.wo
```

5. Monitor the admin console output. It should look similar to the following output.

Listing 7-19 Admin Console Output

```
2002.11.23 21:33:22.444 HPIM OK HTTP inbound service started
2002.11.23 21:34:05.947 32483 HPIS OK HTTP inbound session started
2002.11.23 21:34:05.967 32483 HPIS OK HTTP client: 127.0.0.1:1345
2002.11.23 21:34:06.327 79372 HPIS OK HTTP inbound session started
2002.11.23 21:34:06.487 79372 HPIS OK HTTP client: 127.0.0.1:1349
2002.11.23 21:34:07.980 32483 DECR OK ** Content decrypted **
2002.11.23 21:34:08.240 32483 VRFY OK ** Signature verified **
2002.11.23 21:34:08.530 79372 DECR OK ** Content decrypted **
2002.11.23 21:34:08.711 79372 VRFY OK ** Signature verified **
2002.11.23 21:34:09.692 79372 HPIS OK HTTP inbound session stopping
2002.11.23 21:34:09.762 32483 HPIS OK HTTP inbound session stopping
2002.11.23 21:34:10.103 01977 HPIS OK HTTP inbound session started
2002.11.23 21:34:10.163 01977 HPIS OK HTTP client: 127.0.0.1:1353
2002.11.23 21:34:11.004 01977 DECR OK ** Content decrypted **
2002.11.23 21:34:11.465 01977 VRFY OK ** Signature verified **
```

6. Monitor the transport consoles for outbound transmissions by entering the following command at each transport console.

   ```
   set -m3
   ```

   Your output should look similar to the following sample output.

Listing 7-20 Transport Outbound Transmission Output

```
2002.11.23 21:34:52.844 32174 HPOS OK  Outbound session started -
mbox=[0] batch=[0] attempt=[1 of 1]

2002.11.23 21:34:54.266 32174 VRFY OK  ** Signature verified **

2002.11.23 21:34:54.316 32174 PMDN OK  ** Original-Content-MIC
found in MDN **

2002.11.23 21:34:54.396 32174 HPOS OK  Outbound session stopping -
batch=[0]
```

7. Monitor your external trading partner console to ensure the files are being received. Your output should look similar to the following sample output.

Listing 7-21 External Trading Partner Output

```
2002.11.23 21:34:53.385 35415 HPIS OK  HTTP inbound session started
2002.11.23 21:34:53.425 35415 HPIS OK  HTTP client: 127.0.0.1:1376
2002.11.23 21:34:53.505 35415 VRFY OK  ** Signature verified **
2002.11.23 21:34:53.936 98252 HPIS OK  HTTP inbound session started
2002.11.23 21:34:53.976 98252 HPIS OK  HTTP client: 127.0.0.1:1377
2002.11.23 21:34:54.056 98252 VRFY OK  ** Signature verified **
2002.11.23 21:34:54.266 35415 HPIS OK  HTTP inbound session stopping
2002.11.23 21:34:54.627 98252 HPIS OK  HTTP inbound session stopping
```

8 Configuring Commerce Suite for Simple Database Connectivity

This chapter provides information on creating the database tables required to support a database-enabled Commerce Suite environment. Database tables will hold trading partner configurations, server configuration, trading relationship information, certificates and key data, and transaction detail records.

This document provides your database administrator (DBA) with the information needed to create the necessary database environment and tables required for the P2Pagent application. It also provides information on configuring and accessing the information from the Commerce Suite application.

Creating Commerce Suite Database Tables

Perform the following steps to create Commerce Suite database tables:

1. Select the database that will be used with Commerce Suite.

The Commerce Suite supports ODBC and ESQL database access and connects to Oracle, Informix, and MS-SQL Server Relational Database Management Systems (RDBMS).

2. Create the necessary database files and tables required by the Commerce Suite application.

   This step will require coordination with your database administrator (DBA). The following listing provides the Commerce Suite basic table and field definition.

Listing 8-1 Commerce Suite Database Table Definitions

```
//The Server Table holds configuration data for P2PAgent instances.

CREATE TABLE server( agentname      CHAR(20)         NOT NULL,
                     Peergroup      CHAR(1)          NOT NULL,
                     Agentrole      CHAR(1)          NOT NULL,
                     url            VARCHAR2(255)    NOT NULL,
                     controlurl     VARCHAR2(255)    NOT NULL,
                     orgid          NUMBER           NOT NULL

 );

//The certkey table contains public key data.

CREATE TABLE certkey(certkeyid      NUMBER           NOT NULL,
                     validfrom      CHAR(14)         NOT NULL,
                     validto        CHAR(14)         NOT NULL,
                     keyusage       CHAR(1)          NOT NULL,
                     subjectname    VARCHAR2(512)    NOT NULL,
                     issuername     VARCHAR2(512)    NOT NULL,
                     serialnbr      VARCHAR2(256)    NOT NULL,
                     certdata       VARCHAR2(4000)   NOT NULL,
                     keydata        VARCHAR2(2000)

 );

//The relationship table holds trading pair communication parameter
data.

CREATE TABLE relationship(fromname     CHAR(32)         NOT NULL,
                          Toname       CHAR(32)         NOT NULL,
                          protocol     NUMBER           NOT NULL,
                          notifyname   CHAR(40)         NOT NULL,
                          inbox        CHAR(40)         NOT NULL,
                          tourl        VARCHAR2(255)    NOT NULL,
                          rcpturl      VARCHAR2(255)   NOT NULL,
                          sendparams   VARCHAR2(255)   NOT NULL,
                          hashoption   NUMBER          NOT NULL,
                          cipheroption NUMBER          NOT NULL,
                          compressionoption NUMBER     NOT NULL,
                          requestreceiptCHAR(1)        NOT NULL,
                          asyncreceipt CHAR(1)         NOT NULL,
                          receipthashoption NUMBER     NOT NULL,
                          fromorgid  NUMBER NOT NULL,
                          fromtpid   NUMBER NOT NULL,
                          toorgid    NUMBER NOT NULL,
                          totpid     NUMBER NOT NULL,
                          id         NUMBER NOT NULL  -- sequence

 );
```

//The Keypair Table contains public key certificate data.

```
CREATE TABLE keypair(    fromname   CHAR(32)       NOT NULL,
                         toname     CHAR(32)       NOT NULL,
                         keyusage   CHAR(1)        NOT NULL,
                         pending    CHAR(1)        NOT NULL,
                         encrypted  CHAR(1)        NOT NULL,
                         status     CHAR(1)        NOT NULL,
                         certkeyid  NUMBER         NOT NULL,
                         certfile   VARCHAR2(255)  NOT NULL,
                         keyfile    VARCHAR2(255)  NOT NULL,

 );
```

//The Workorder Table holds work order commands to be executed in batch.

```
CREATE TABLE workorder(  workorderid  NUMBER        NOT NULL,
                         fromname     CHAR(32)      NOT NULL,
                         toname       CHAR(32)      NOT NULL,
                         notifyname   CHAR(40)      NOT NULL,
                         status       CHAR(1)       NOT NULL,
                         statustime   CHAR(14)      NOT NULL,
                         begintime    CHAR(14)      NOT NULL,
                         endtime      CHAR(14)      NOT NULL,
                         batchnumber  NUMBER        NOT NULL,
                         command      VARCHAR2(255) NOT NULL

 );
```

//The Notice Table contains data related to all send attempts.

```
CREATE TABLE notice(   noticeid       CHAR(22)       NOT NULL,
                       opcode         CHAR(8)        NOT NULL,
                       fromname       CHAR(32)       NOT NULL,
                      toname         CHAR(32)        NOT NULL,
                      notifyname     CHAR(40)        NOT NULL,
                      msgid          CHAR(22)        NOT NULL,
                      subject        CHAR(64)        NOT NULL,
                      msgdigest      CHAR(28)        NOT NULL,
                      begintime      CHAR(14)        NOT NULL,
                      endtime        CHAR(14)        NOT NULL,
                      agentrole      CHAR(1)         NOT NULL,
                      batchnumber    NUMBER          NOT NULL,
                      bytesincount   NUMBER          NOT NULL,
                      bytesoutcount  NUMBER          NOT NULL,
                      errcode        NUMBER          NOT NULL,
                      filesize       NUMBER          NOT NULL,
                      srcipaddress   CHAR(15)        NOT NULL,
                      destipaddress  CHAR(15)        NOT NULL,
                      srcipport      NUMBER          NOT NULL,
                      destipport     NUMBER          NOT NULL,
                      attemptcount   NUMBER          NOT NULL,
                      attemptlimit   NUMBER          NOT NULL,
                      origfilename   VARCHAR2(255)   NOT NULL,
                      agentname      VARCHAR2(20)    NOT NULL,
                      sendparams     VARCHAR2(255)   NOT NULL,
                      errtext        VARCHAR2(255)   NOT NULL
 );

//The Route Table contains all route definitions us by P2PAgent.

CREATE TABLE p2proute(   fromname    VARCHAR2(64)    NOT NULL,
                         toname      VARCHAR2(64)    NOT NULL,
                         condition   VARCHAR2(255)   NOT NULL,
                         filter      VARCHAR2(255)   NOT NULL,
                         url         VARCHAR2(255)
 );
```

The certkey_sequence is the primary key for all certificates and keys.

The relationship_sequence is the primary key for all trading pairs.

3. Your DBA will create the necessary database tables and user logon IDs to enable database access. You can contact iSoft support to obtain SQL Scripts to assist in the automation of database table creation.

Testing Commerce Suite Database Environment

Perform the following steps to test your Commerce Suite database environment:

After the database is created, verify that the machine running the Commerce Suite can access the Commerce Suite database tables.

- Ensure the machine has the necessary ODBC connectivity software installed.
- Test connecting to the database by utilizing a SQL query tool like SQL Plus.
- Test the ability to use the login ID to insert records into the tables.
- Test viewing the records that you inserted.

Configuring Commerce Suite for Simple Database Connectivity

The Commerce Suite application supports two methods of connecting to the database.

- For ODBC databases, you must use the `p2pagent_odbc` version.
- For ESQL, you must use the `p2pagent_esql` version.

Note: Confirm you have the appropriate version for your Commerce Suite to work in your database environment.

Perform the following steps to configure Commerce Suite for simple database connectivity:

1. Modify the `p2pagent.cfg` file located in the `p2pagent` root directory by adding the additional database configuration commands shown in Listing 8-2. You must enter your database-specific information for the hostname, driver name, database name, user ID, and password.

Listing 8-2 P2Pagent Configuration File - Database Configuration

```
<xml>
<command>set -dhLAPTOP</command>
<command>set -ddSQL-Server</command>
<command>set -dnisoft</command>
<command>set -duisoft</command>
<command>set -dwisoft</command>
<command>set -df</command>
<command>set -nd</command>
<command>dbconnect</command>
</xml>
```

The commands used in the previous listing are defined as follows:

set -dhLAPTOP

specifies the database host name.

Note: Do not use this parameter to reference an external mailbox system. Refer to the set `-b*` series of commands for specifying external mailboxing systems.

set -ddSQL-Server

specifies the name of the ODBC driver manager being used.

set -dnisoft

specifies the name of the database used by Commerce Suite.

set -duisoft

specifies the user name used to connect to the database.

set -dwisoft

specifies the database login password.

set -df

specifies to immediately replicate configuration updates made to local memory to the database.

set -nd

specifies to write notice record to the database.

dbconnect

specifies to connect P2Pagent to a database.

2. Test the Commerce Suite database connection by performing the following steps:

   a. Start Commerce Suite by executing the `p2pagent.exe`.

Listing 8-3 Commerce Suite Startup Output

```
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.10.30.1 [Nov 18 2002 11:32:01]
Standard Edition
Authorized License
2003.01.18 19:58:33.456       POPT OK  Database name set to
[isoft]

2003.01.18 19:58:33.466       POPT OK  Database driver set
to [SQL~Server]

2003.01.18 19:58:33.476       POPT OK  Database host set to
[isoft]

2003.01.18 19:58:33.486       POPT OK  Database user set to
[isoft]

2003.01.18 19:58:33.496       POPT OK  Database password
set to [isoft]

2003.01.18 19:58:33.606       PTWC OK  Work Orders reset

2003.01.18 19:58:33.616       POPT OK  Notices will be
written to data-source

2003.01.18 19:58:33.626       DBCO OK  Connected to
database

2003.01.18 19:58:33.646       POPT OK  Peer group set to
[1]
```

```
2003.01.18 19:58:33.676       POPT OK  Server is a
transport server
```

b. Add a Commerce Suite server by executing the `addserver` command at the command prompt using the following syntax:

```
addserver <name> <group> <role> <url> <control-URL>
```

Code Example:

```
addserver Transport1 1 T 127.0.0.1:5080 127.0.0.6080
```

Refer to Appendix A, "Commerce Suite Command Reference," for additional information on using the `addserver` command.

c. Insert the newly created server into the database by executing the `insertserver` command at the command prompt using the following syntax:

```
insertserver <name> <group> <role> <url> <ctrlurl>
```

Code Example:

```
insertserver Transport1 1 T 127.0.0.1:5080 127.0.0.6080
ok
```

Refer to Appendix A, "Commerce Suite Command Reference," for additional information on using the `insertserver` command.

d. Define a new trading partner relationship by executing the `addpair` command at the command prompt using the following syntax:

```
addpair <from> <to> <to-URL> <rcpt-URL> <notify-name> <inbox>
[in|out][<send-parameters>]
```

Code Example:

```
addpair TP1 TP2 127.0.0.1:4080 127.0.0.1:5080 TP1 inbox
ok
```

Refer to Appendix A, "Commerce Suite Command Reference," for additional information on using the `addpair` command.

e. Insert a trading relationship pair into the database by executing the `insertpair` command at the command prompt using the following syntax:

```
insertpair <from> <to> <to-URL> <rcpt-URL> <notify-name>
<inbox> [<send-parameters>]
```

Code Example:

```
insertpair TP1 TP2 127.0.0.1:4080 127.0.0.1:5080 TP1 inbox
ok
```

Refer to Appendix A, "Commerce Suite Command Reference," for additional information on using the `insertpair` command.

f. Create key-material for data encryption and authentication purposes by executing the `addkey` command at the command prompt using the following syntax:

```
addkey <from> <to> <usage> <key-bits> <issuer> <subject>
```

Code Example:

```
addkey TP1 TP2 O 1024 self
C=US;S=TX;L=Dallas;O=iSoft;CN=iSoft
ok
2003.01.18 20:26:16.107       PAKC OK  Keypair generated
exportkey TP1 TP2 O isoft.cer isoft.prv
ok
2003.01.18 20:31:04.121       POKC OK  Key-pair exported
```

Refer to Appendix A, "Commerce Suite Command Reference," for additional information on using the `addkey` command.

g. Insert public-key information into the database by executing the `insertkey` command at the command prompt using the following syntax:

```
insertkey <from> <to> <usage> <certfile> <keyfile> [<encrypt>
[-p]]
```

Code Example:

```
importkey TP1 TP2 O -fCisoft.cer -fKisoft.prv
ok
```

Refer to Appendix A, "Commerce Suite Command Reference," for additional information on using the `insertkey` command.

h. Extract server information from the database by executing the getservers command at the command prompt using the following syntax:

```
getservers
listservers
```

Code Example:

```
getservers
ok
2003.01.18 20:44:11.583      PGSC OK  1 servers(s) read from
database
listservers
ok
Name:        Transport1
Group:       1
Role:        T
URL:         127.0.0.1:5080
Control URL: 127.0.0.16080

1 server(s)
```

i. Extract server information from the database by executing the `getservers` command at the command prompt using the following syntax:

```
getpairs
listpairs
```

Code Example:

```
getpairs
ok
2003.01.18 20:49:20.497      PGRC OK  1 relationship(s) read
from database
listpairs
ok

From:        TP1
To:          TP2
URL:         127.0.0.1:4080
Receipt:     127.0.0.1:5080
Notify:      TP1
Inbox:       inbox
Direction:   outbound
Params:

1 pair(s)
```

j. View the keys with the `listservers` command at the command prompt.

```
getkeys
listkeys
```

Code Example:

```
getkeys
ok
2003.01.18 20:51:55.413      PGKC OK  1 keypairs(s) read from
database

2003.01.18 20:51:55.443      PGKC OK  Certs and keys assigned
to relationships

listkeys
ok
From:        TP1
To:          TP2
Usage:       O ( Sign Encrypt Decrypt Verify )
Cert File:   isoft.cer
Key File:    isoft.prv
Valid From:  030119022607Z
Valid To:    040119022607Z
X.509 Usage: E4
Subject:     C=US;S=TX;L=Dallas;O=iSoft;CN=iSoft
Issuer:      C=US;S=TX;L=Dallas;O=iSoft;CN=iSoft
Serial No.:  20 03 01 13 02 1A 0F 38 E2 F8 DD C6 A8 E6 DC 86
Cert Length: 558
Key Length:  604

1 key(s)
```

CHAPTER

9 Configuring Commerce Suite for Inbound/Outbound MQSeries Interfacing

This chapter introduces the iSoft Commerce Suite for MQSeries(TM) (Commerce Suite/MQ) product and provides instructions for using existing Commerce Suite commands and new MQSeries-specific parameters to interface with the MQSeries product. This chapter contains the following sections:

- What is IBM MQSeries?
- How Does Commerce Suite Work With IBM MQSeries?
- Configuring Commerce Suite/MQ for Inbound/Outbound MQSeries Interfacing
- Commerce Suite/MQ Command Reference
- Accessing IBM MQSeries Documentation

What is IBM MQSeries?

MQSeries is a message-oriented communication system that provides assured, asynchronous, transactional, one-time delivery, message handling across a broad range of hardware and software platforms.

MQSeries messaging products enable application integration by helping business applications to exchange information across different platforms by sending and receiving data as messages.

Messages are grouped into units of work and either all or none of the messages in a unit of work are processed. MQSeries coordinates message work with other transaction work, like database updates, so data integrity is always maintained.

Messages, Queues, and Queue Managers

The three primary concepts in MQSeries that you need to understand in relation to Commerce Suite are the following:

- Messages
- Queues
- Queue Managers

Messages

A message is a string of bytes that has meaning to the applications that use it. Messages are used for transferring data from one application to another (or to different parts of the same application). The applications can be running on the same platform, or on different platforms. MQSeries messages have two parts:

- The application data

  The content and structure of the application data is defined by the application programs that use the data.

- A message descriptor

  The message descriptor identifies the message and contains other control information, such as the type of message and the priority assigned to the message by the sending application.

Queues

A queue is a data structure in which messages are stored. The messages may be put on, or received from, the queue by applications or by a queue manager as part of its normal operation.

Queues exist independently of the applications that use them. Each queue belongs to a queue manager, which is responsible for maintaining it. The queue manager puts the messages it receives onto the appropriate queue.

Applications send to, and receive messages from, queues. For example, one application can put a message on a queue, and another application can get the message from the same queue.

Queue Managers

A queue manager provides queuing services to applications, and manages the queues that belong to it. It ensures that:

- Object attributes are changed according to the details received.
- Special events (such as instrumentation events or triggering) are generated when the appropriate conditions are met.
- Messages are put on the correct queue, as requested by the application. The application is informed if this cannot be done, and an appropriate reason code is given.

Each queue belongs to a single queue manager and is said to be a local queue to that queue manager. The queue manager to which an application is connected is said to be the local queue manager for that application. For the application, the queues that belong to its local queue manager are local queues. MQSeries supports multiple queue managers on the same machine.

How Does Commerce Suite Work With MQSeries?

The iSoft Commerce Suite for MQSeries (Commerce Suite/MQ) product extends the connectivity between the Commerce Suite and external data sources by adding direct message retrieval and storage capabilities between Commerce Suite and IBM MQSeries 5.2 for Windows NT and Windows 2000.

This section contains the following topics:

- Commerce Suite/MQ and MQSeries Interfacing
- MQSeries Support Libraries
- Typical Commerce Suite/MQ and MQSeries Data Flow Scenario
- Inbound Message Processing
- Outbound Message Processing
- Supported URL Schemas
- Receipt Production and Delivery
- Notice Production and Delivery

Commerce Suite/MQ and MQSeries Interfacing

Commerce Suite/MQ enables the following interfaces to MQSeries:

- Retrieval of messages from MQSeries queues for AS2 delivery to a trading partner
- Storage of received AS2 messages in an MQSeries queue.
- Association of MQSeries queues to trading partners at the relationship level

- Designation of an MQSeries queue as a work order source location
- Designation of an MQSeries queue as a Notice output location
- Designation of an MQSeries queue as a Receipt output location
- Designation of an MQSeries queue as an Errors output location
- Designation of an MQSeries queue as a Recycle output location
- Support for multiple MQSeries Queue Managers as inbound data locations

MQSeries Support Libraries

The Commerce Suite/MQ product is linked with run-time MQSeries support libraries provided by IBM. The following IBM libraries are required by Commerce Suite/MQ and are usually installed in the `MQSeries\bin` directory when MQSeries 5.2 for Windows NT/2000 is installed:

- `mqm.dll`
- `amqxcs2.dll`
- `amqzst.dll`
- `amqldatn.dll`
- `amqzc.dll`
- `amqvwaa2.dll`
- `mqmvxd.dll`
- `amqmtmgr.dll`
- `amqztm.dll`
- `amqzsai.dll`

Typical Commerce Suite/MQ and MQSeries Data Flow Scenario

The following conditions and steps illustrate a typical movement of data between Commerce Suite/MQ, the supporting database, and the MQSeries repository.

1. Commerce Suite/MQ stores persistent data in a supported RDBMS using either an ODBC or ESQL/C programming interface to send commands (or Commerce Suite work orders) to the database. A copy of this persistent data is stored in memory by Commerce Suite/MQ.
2. Work orders are deposited by a client’s back-office application in an MQSeries Queue.
3. Commerce Suite/MQ polls a MQSeries work order queue, reads the work order from the queue, and removes it from the queue after processing the work order file.
4. After processing the work order, Commerce Suite/MQ stores a notice message on a separate MQSeries Queue indicating the result of the operation.
5. Only data that is pertinent to the transfer of data is passed to Commerce Suite/MQ. This pertinent data is stored both in the persistent RDBMS (in the relationship, keypair, and certkey tables) and in memory. In a clustered Commerce Suite configuration, the primary Commerce Suite/MQ Admin agent will replicate the configuration to downstream agents as is typical.
6. The work orders or commands passed to Commerce Suite/MQ contain basic syntax instructing Commerce Suite/MQ to add, update, or delete a trading partner profile. Each trading partner profile represents a complete bidirectional data traffic definition.
7. Responses that are passed from Commerce Suite/MQ to MQSeries contain basic syntax that reports the final disposition of a command or work order once its processing has completed.

Inbound Message Processing

Inbound data received by Commerce Suite/MQ is processed in the same way as Commerce Suite Standard Edition (Commerce Suite/SE). Messages intended to be delivered into a queue may be sent using either HTTP or HTTPS protocols. Inbound messages may be processed according to AS2, or other supported packaging styles.

Outbound Message Processing

Outbound data sent by Commerce Suite/MQ is processed in the same way as Commerce Suite/SE. Commerce Suite/MQ supports all modes of compression, authentication, and encryption supported by Commerce Suite/SE.

All outbound data transfers are processed as `send` commands. `send` commands are delivered to the Commerce Suite either directly, by means of *push* interfaces such as the operator's console or TCP/IP socket connections, or indirectly, by means of *pull* interfaces such as directory, database, or queue polling. No special initialization is required for *push* interfaces because the Commerce Suite normally exposes an operator console interface and a control-port listener. *Pull* interfaces (polling) do require some definition and initialization at Commerce Suite start-up time so that Commerce Suite knows which directories, databases, or queues to poll for outbound data.

It is common for a Commerce Suite configuration file to include a `send` command that is persistent. This means the `send` command is configured to persist in the Commerce Suite command queue and repeat at a specified interval to effectively poll a directory, database, or queue for outbound data. Since all `send` commands are directly related to a *Relationship*, destination and protocol for the send command is already predefined before any outbound data is found to transfer.

The options to request receipts for outgoing data transfers is specified in the *Relationship* definition, which may reside in configuration files or the database. These options may be overridden by send command parameters.

Notice records are also produced and stored for outbound data transfers including multiple notice records for single data transfers. Notice records generated and stored for outbound data transfers are stored in the same manner as they are for inbound data transfers.

Supported URL Schemas

The Commerce Suite/MQ application supports the following URL schemas:

Table 9-1 Supported Commerce Suite/MQ Schemas

Schema	Payload Storage Mechanism
None	Store data as an operating system file.
`file://`	Store data as an operating system file.
`mailto://`	Deliver payload using SMTP (email).
`mq://`	Deliver payload to an IBM MQSeries Queue.

The format of the URL that encapsulates the definition of an IBM MQSeries Queue for inbound payload delivery substitutes the Queue-Manager name for the host portion of the URL and Queue name for resource portion of the URL.

Receipt Production and Delivery

The production and delivery of receipts (for example, AS2 MDNs) is specified by the sender of the message. For all Commerce Suite editions, the receipt disposition must report the successful delivery of the payload to the intended storage media or mechanism. Therefore, the receipt is not constructed until after the result of storing the data to MQSeries is known. The delivery of inbound data to MQSeries is synchronous.

Once a receipt is generated, a copy of the receipt is stored in the location specified to hold returned receipts as defined in the Commerce Suite configuration. For example, `set -rp<url>`. Commerce Suite/MQ supports the `mq://extension` to the following recognized URL formats:

Table 9-2 Supported Commerce Suite/MQ Returned Receipt Storage Mechanisms

Schema	Payload Storage Mechanism
None	Store receipt to file if the `set -rp<`*`path`*`>` command is specified.
`file://`	Store receipt to file if the `set -rp<`*`url`*`>` command is specified.
`mailto://`	Deliver receipt using SMTP (email).
`mq://`	Deliver receipt to an IBM MQSeries Queue.

Notice Production and Delivery

The production and delivery of notices is extended for Commerce Suite/MQ to permit the specification of a queue to hold notices. Queues for receiving processing notices must be specified in the Commerce Suite configuration. For example, `set -np.` Commerce Suite/MQ supports the `mq://`*`extension`* to the following recognized URL formats:

Table 9-3 Supported Commerce Suite/MQ Notice/Alert Delivery Mechanisms

Schema	Payload Storage Mechanism
None	Store notice to file if the `set -nf` command is specified.
`file://`	Store notice to file if the `set -nf` command is specified.
`mailto://`	Deliver notice using SMTP (email).

Schema	Payload Storage Mechanism
`mq://`	Deliver notice to an IBM MQSeries Queue.

Configuring Commerce Suite/MQ for Inbound/Outbound MQSeries Interfacing

Perform the following steps to enable inbound and outbound interfacing between iSoft Commerce Suite and IBM MQSeries.

1. Create MQSeries queues for notices, work orders, and inbound and outbound data. Refer to IBM MQSeries documentation for instructions on creating MQSeries queues.
2. Defining an MQSeries Queue for Storage of Received AS2 Messages.
3. Defining an MQSeries Queue as a Notice Output Location.
4. Defining an MQSeries Queue as a Work Order Source Location.
5. Associating an MQSeries Queue to Trading Partners at the Relationship Level.
6. Defining an MQSeries Queue as a Receipt Output Location.
7. Defining an MQSeries Queue as an Errors output location.
8. Defining an MQSeries Queue as a Recycle output location.
9. Defining an queue for persistent polling.

Refer to the following sections for a detailed description of each step necessary to enable inbound and outbound interfacing between iSoft Commerce Suite and IBM MQSeries.

Step 1 - Creating MQSeries Queues for Notices, Work Orders, and Inbound and Outbound Data

Refer to IBM MQSeries documentation for instructions on creating MQSeries queues. Refer to “Commerce Suite/MQ Command Reference,” for a listing of IBM MQSeries documentation and the IBM MQSeries web site address.

Step 2 - Defining an MQSeries Queue for Storage of Received AS2 Messages

IBM MQSeries is now recognized as a supported external mailboxing system in the same way as Connect:Enterprise. As such, you must edit the `p2pagent.cfg` configuration file to define an MQSeries Queue Manager as an external mailbox.

The `-bh` parameter identifies the home MQSeries Queue Manager that will be used when extracting messages to be sent to trading partners.

The external mailbox hostname `-bh<`*`hostname`*`>` parameter of the `set` command can be edited to include an MQSeries Queue Manager hostname within the parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
set -bh[<scheme>://]<hostname>
```

Example

```
set -bhmq://QM_polaris
```

Step 3 - Defining an MQSeries Queue as a Notice Output Location

The notice path `-np<path>` parameter of the `set` command can be edited to include a URL, allowing for MQSeries notice queues to be defined within the notice path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
set -np<url|path>
```

Example

```
set -npmq://QM_polaris/notices -nf
```

The `-nf` switch enables/disables notice storage to the notice *path*.

If no scheme is defined within the notice path parameter, then the value is interpreted as a relative path.

Step 4 - Defining an MQSeries Queue as a Work Order Source Location

The work order path `-op<path>` parameter of the `set` command can be edited to include a URL, allowing for MQSeries work order queues to be defined within the work order path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
set -op<url|path>
```

Example

```
set -opmq://QM_polaris/workorders -of -oswo
```

- The `-op` parameter defines the queue to be searched for work orders.
- The `-of` switch instructs the Commerce Suite to begin searching for work orders.
- The `-oswo` parameter defines the file extension to be searched for when searching for file-based work orders. This parameter must be included before the Commerce Suite will search for work orders.

Note: Commerce Suite always deletes work orders from either a work order directory being searched or the MQSeries queue defined as the work order queue.

If no scheme is defined within the work order path parameter, then the value is interpreted as a relative path.

Step 5 - Associating an MQSeries Queue to Trading Partners at the Relationship Level

Establishing mailbox queue associations, or relationships, is accomplished using the `addpair` command in the `p2pagent.cfg` configuration file. A *<mailbox>* parameter is used to direct inbound and outbound data to an MQSeries Queue, or mailbox. In order for the `addpair` command to execute properly, ensure that a MQSeries queue of the same name exists before starting Commerce Suite. Otherwise, a log file error message will be generated indicating that the Commerce Suite cannot connect to the queue.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
addpair <from> <to> <url> <receipt-url> <mailbox> <inbox>
<send params>
```

Example

```
addpair ibm isoft http://127.0.0.1:8080
http://127.0.0.1:8081 ibm_isoft mq://QM_polaris/misroute
-sC -e -r1

addpair isoft ibm http://127.0.0.1:4080
http://127.0.0.1:4081 isoft_ibm mq://QM_polaris/isoft_ibm
```

If no scheme is defined within the `addpair` path parameter, then the value is interpreted as a relative path.

Step 6 - Defining an MQSeries Queue as a Receipt Output Location

Defining a MQSeries queue as a receipt output location is accomplished with the `set` command using the `-rp<path>` parameter. This parameter specifies the file system directory location that should be used by Commerce Suite/MQ to store receipts that are composed for asynchronous delivery.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
set -rp<url><path>
```

Example

```
set -rpmq://QM_polaris/receipts</command>
```

If no scheme is defined within the receipt path parameter, then the value is interpreted as a relative path.

Step 7 - Defining an MQSeries Queue as an Errors Output Location

Defining a MQSeries Queue as an errors output location is accomplished with the set command using the `-ep` parameter. This parameter specifies a file-system directory location to be used to store inbound and outbound data packages that cannot be completely delivered.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
set -ep<url|path>
```

Example

```
set -epmq://QM_polaris/notices -nf
```

If no scheme is defined within the receipt path parameter, then the value is interpreted as a relative path.

Step 8 - Defining an MQSeries Queue as a Recycle Output Location

Defining an MQSeries Queue as a recycle output location is accomplished with the `set` command using the `-yp` parameter. This parameter specifies the file system directory location that should be used by Commerce Suite as a Recycle output location.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax

```
set -yp<url|path>
```

Example

```
set -ypmq://QM_polaris/recycle -yt
```

If no scheme is defined within the receipt path parameter, then the value is interpreted as a relative path.

Step 9 - Defining a MQSeries Queue For Persistent Polling

Polling a MQSeries queue for messages to send is accomplished with the `send` command using the interval (`-tC`) and expiration (`-tE`) parameters. These parameters instruct the Commerce Suite that a command must be executed iteratively until a certain time.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

To poll a queue for messages to send, the following command syntax must be used with the `send` command:

Syntax

```
send <protocol> <from> <to> [-fN<filename>|-fP<path>
-fS<spec>] [<other params>] -tC<seconds>s
-tE<yyyymmddhhmmss>
```

Example

```
send http ibm isoft -fNoutbox\datafile -sC -r1 -tC60s
-tE20030415000000
```

Outbound sends are initiated in the same way: however, MQSeries is now recognized as a supported external mailboxing system the same way as Connect:Enterprise is recognized. The following `send` command syntax will instruct the Commerce Suite to send the next logical-order datagram from the `isoft_IBM` queue:

Example

```
send http MAILBOX MAILBOX -de -dsMAILBOXID=isoft_IBM
```

If you attach interval (`-tC`) and expiration (`-tE`) parameters to the command, the command becomes persistent and the queue will be polled at regular intervals.

Example

```
send http MAILBOX MAILBOX -de -dsMAILBOXID=isoft_IBM -tC30s
-tE20030731000000
```

The `send` command example above illustrates how to establish an MQSeries queue as a live outbox to be polled. In this example, the send processor identifies the reserved keyword `MAILBOX` as the *`AS2-From`* and *`AS2-To`* names and uses the `MAILBOXID` parameter, isoft to lookup addressing information from the relationship array. Commerce Suite/MQ also interprets the `MAILBOXID` parameter as the MQSeries Queue Name from which outbound data will be sent.

Note that the `-de` parameter flags the `send` command as originating from an external data-source (the mailboxing system). If the sample `send` command above are stored as simple datagrams in the work order queue, they will be picked up and processed in the same manner as other external mailbox scenarios.

Commerce Suite/MQ Command Reference

The following Commerce Suite command parameters have been expanded to include MQSeries-specific definitions.

- `set` command
- `send` command
- `addpair` command

Note: Note that forward slash (/) is used for UNIX and Linux. Back slash (\) is for Windows operating systems.

set Command

The `set` command sets the value of a program variable. Program variables determine the behavior of many program functions, including directory locations, timeouts, and messaging levels.

Expanded Parameters

The following parameters have been expanded to include MQSeries-specific definitions.

-bh<*hostname*>
sets a mailbox servers network hostname and port. This parameter may be specified as an alternate to using the -ba and `-bp` parameters, if the mailbox server's IP address and port can be resolved using the Domain Name Service (DNS).

Example: `-bhMBXSVR08:8000`

For MQSeries Interfacing - The external mailbox hostname parameter can be edited to include an MQSeries Queue Manager hostname within the parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax: `set -bh[<scheme>://]<hostname>`

Example: `set -bhmq://QM_polaris`

-ep<*path*>
specifies a file-system directory location to be used to store inbound and outbound data packages that cannot be completely delivered.

Example: `-eperrors`

-ep-*
disables an error path.

For MQSeries Interfacing - The error-path parameter can be set to include a URL, allowing for MQSeries notice queues to be defined within the notice path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax: `set -ep<`*`url|path`*`>`

Example: `set -epmq://QM_polaris/notices -ef`

-np<*path*>

specifies the file-system location where Commerce Suite stores notice files. The `-np-` command may be used to specify the current working directory.

Example: `-np/opt/p2pagent/notices`

-np-*

disable the writing of notices to a specific file in a given directory path.

For MQSeries Interfacing - The notice-path parameter can be set to include a URL, allowing for MQSeries notice queues to be defined within the notice path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax: `set -np<`*`url|path`*`>`

Example: `set -npmq://QM_polaris/notices -nf`

The `-nf` switch enables/disables notice storage to the notice *path* for MQSeries interfacing.

-op<*path*>

specifies the file-system location where Commerce Suite searches for work orders. Work Orders may be stored in files or in the database. When they are stored as files, the Commerce Suite searches the given directory for work order files. The `-op-` command may be used to specify the current working directory.

Example: `-op/opt/p2pagent/workorders`

-op-*
disable the search for work order files.

For MQSeries Interfacing - The work order path parameter can be edited to include a URL, allowing for MQSeries work order queues to be defined within the work order path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax: `set -op<url|path>`

Example: `set -opmq://QM_polaris/workorders`

If no scheme is defined within the notice path parameter, then the value is interpreted as a relative path.

-rp<*path*>
specifies the file system directory location that should be used by Commerce Suite to store receipts that are composed for asynchronous delivery.

Example: `-rp/opt/p2pagent/receipts`

-rp-*
disable the storing of asynchronous MDN receipts to the given directory path.

For MQSeries Interfacing - The receipt path parameter can be edited to include a URL, allowing for MQSeries work order queues to be defined within the receipt path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax: `set -rp<url><path>`

Example: `set -rpmq://QM_polaris/receipts</command>`

If no scheme is defined within the notice path parameter, then the value is interpreted as a relative path.

-yp<path>

specifies the file system directory location that should be used by Commerce Suite as a Recycle output location.

Example: `-yp/opt/p2pagent/recycle`

-yf*

`-yf-*`

These two switches enable and disable the use of the recycle location to the given path.

For MQSeries Interfacing - The recycle path parameter can be edited to include a URL, allowing for MQSeries work order queues to be defined within the receipt path parameter syntax.

This parameter now supports an MQSeries scheme identifier `mq://`, that denotes that the following path identifies a Queue Manager and Queue Name into data that will be written.

Syntax: `set -yp<path>`

Example: `set -ypmq://QM_polaris/recycle</command>`

send Command

The `send` command initiates an outbound transmission of data. This command may be issued from the console or by storing a work order in the database.

Expanded Parameters

The `send` command parameters have been expanded to recognize MQSeries as a supported external mailboxing system the same way as Connect:Enterprise is recognized.

When sending from a MQSeries mailbox (or queue), no *`filename`* or *`path`* variables are defined. They are replaced by the `mailbox` keyword placeholder. These placeholders are reserved for mailbox identifiers.

The following code examples show the difference between the traditional `send` command syntax, and the syntax used to interface with a MQSeries mailbox.

Traditional Syntax

```
send <protocol> <from> <to> [<option>] [...]
```

Example

```
send http sndr rcvr -fNoutbox\edix12.txt -cE -oZ -sC
```

MQSeries Syntax

```
send <protocol> <mailbox> <mailbox> [<options>] [...]
```

Example

```
send http MAILBOX1 MAILBOX2 -de -ds MAILBOXID=isoft
```

Note that in this MQSeries example that both the sender and receiver names are set to the keyword `MAILBOX`. Also note two data parameters, `-de` and `-ds`. These indicate, respectively, that data is to be sent from an external data store and that the mailbox (queue) to be accessed is `isoft`. The batch identifiers not presently used with the Commerce Suite/MQ interface and may be set to zero.

When Commerce Suite/MQ processes a `send` command, it will resolve the mailbox name (or queue name) to the relationship established in the `addpair` command. From this command, Commerce Suite/MQ determines the destination address and default send parameters. Additional send parameters can be appended to the send command itself, enhancing or overriding the default parameters from the `addpair` command.

One-Time Sends

The `send` command supports one-time sends to the operating system file system as well as indirect sends to MQSeries queues using a mailbox identifier.

The following code provides an example of an indirect send using mailbox identifiers.

```
send http MAILBOX1 MAILBOX2 -de -ds MAILBOXID=isoft
```

Persistent Sends

The `send` command also supports persistent sends that will poll a mailbox (or queue) at regular intervals listening for messages. When messages are encountered, Commerce Suite/MQ will send the first message in the mailbox (or queue).

The following code provides an example of an indirect persistent `send` using mailbox identifiers.

```
send http MAILBOX MAILBOX -de -dsMAILBOXID=user1_ibm -tC60s
-tE20030101000000
```

In this code example, the `send` command will repeat from mailbox name `user1` every 60 seconds until January 1, 2003.

addpair Command

The `addpair` command defines a new trading partner relationship. A trading partner relationship is a set of data describing how data may be transferred from one trading partner entity to another trading partner entity. Each trading partner entity is defined by an alphanumeric sequence of characters or with a quoted identifier.

The `addpair` command always stores trading partner relationships in memory. If the `set -df` parameter has been issued, enabling the automatic write of memory updates to the database, then the `addpair` statement will have the result of inserting a record into the database.

This command now supports an MQSeries scheme identifier `mq://`, that denotes that the path identifies a Queue Manager and Queue Name into data that will be written.

Expanded Parameters

The following parameters have been expanded to include MQSeries-specific definitions.

Traditional Syntax

```
addpair <from> <to> <to-URL> <rcpt-URL> <notify-name>
<inbox> [<send-parameters>]
```

Example

```
addpair HG012 MERCFDI http://hg.com/
mailto:edi@hg.com HG012 in/hg -sC
```

MQSeries Syntax

```
addpair<scheme>//<queue-manager-name>/<queue-name>
```

Outbound Example

```
<command>addpair A B http://as2.b.com
mailto:as2@A.com A_B mq://QM_polaris/A_B
out</command>
```

Inbound Example

```
<command>addpair B A http://as2.A.com
mailto:as2@B.com B_A mq://QM_polaris/B_A
in</command>
```

The `addpair` statements illustrate how the `mq://` scheme may be applied to the `inbox` parameter to denote the queue to receive inbound data for a relationship.

Note that an optional positional parameter (`out|in`) is now supported by the `addpair` command to distinguish between inbound and outbound relationships. This parameter is optional, but should be used for implementations that apply the same notifying parameter (`A_B`, `B_A` in the above example) for both inbound and outbound relationships.

Accessing MQSeries Documentation

For further information about the MQSeries product, visit the following IBM MQSeries web site:

```
http://www-3.ibm.com/software/ts/mqseries
```

MQSeries for Windows NT and Windows 2000 is described in the following platform-specific and MQSeries family books:

Table 9-4 MQSeries for Windows NT and Windows 2000 Books

Book Number	Title
	Windows NT and Windows 2000 Specific Books
GC34-5389	*MQSeries for Windows NT and Windows 2000 Quick Beginnings*
SC34-5404	*MQSeries LotusScript Extension*
SC34-5387	*MQSeries for Windows NT Using the Component Object Model Interface*
	MQSeries Family Books
GC34-5761	*MQSeries V5.2 Release Guide*
SC33-1872	*MQSeries Intercommunication*

Book Number	Title
SC34-5349	*MQSeries Queue Manager Clusters*
GC33-1632	*MQSeries Clients*
SC33-1873	*MQSeries System Administration*
SC33-1369	*MQSeries MQSC Command Reference*
SC33-1482	*MQSeries Programmable System Management*
SC34-5390	*MQSeries Administration Interface Programming Guide and Reference*
GC33-1876	*MQSeries Messages*
SC33-0807	*MQSeries Application Programming Guide*
SC33-1673	*MQSeries Application Programming Reference*
SX33-6095	*MQSeries Programming Interfaces Reference Summary*
SC33-1877	*MQSeries Using C++*

CHAPTER

10 Server Administration

This section describes how to define and manage servers using the Commerce Suite command line interface (CLI).

Managing Commerce Suite Servers

The following topics provide instructions for managing your Commerce Suite servers using the CLI.

- Defining a New Commerce Suite Server Profile
- Inserting a Commerce Suite Server Profile Into the Database
- Displaying a List of Defined Commerce Suite Servers
- Reading Commerce Suite Server Settings From a Database
- Removing a Server Profile From a Database
- Removing a Server Profile From Memory
- Starting a Remote Commerce Suite Server on a Remote Host

Refer to Chapter 2, “Starting and Stopping P2P Agent,” for instructions on starting the Commerce Suite application and accessing the command line interface.

Defining a New Commerce Suite Server Profile

Commerce Suite server profiles are defined as server/protocol combinations defining Transport and Router Agent inbound services. Both of these services are remotely configured by an Administrative Agent and must be started remotely by an Administrative Agent

Defining a new Commerce Suite server profile is accomplished using the `addserver` command. Perform the following steps to define a new Commerce Suite server profile using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `addserver` command using the following syntax:

   ```
   addserver <name> <group> <role> <url> <control-URL>
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `addserver` command.

Inserting a Commerce Suite Server Profile Into the Database

Perform the following steps to insert a Commerce Suite server profile into the database:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `insertserver` command using the following syntax:

   ```
   insertserver <name> <group> <role> <url> <ctrlurl>
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `insertserver` command.

Displaying a List of Defined Commerce Suite Servers

Perform the following steps to display a list of defined Commerce Suite servers:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `listservers` command using the following syntax:

   ```
   listservers
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `listservers` command.

Reading Commerce Suite Server Settings From a Database

Reading Commerce Suite server settings from a database is accomplished using the `getservers` command. This command retrieves all remote service and Agent information from the database and populates the Commerce Suite memory with the material needed to remotely configure Agents and issue remote commands.

The `getservers` command is only functional if the database parameters have been defined with the `set -d?` commands and the `dbconnect` command has been issued.

Perform the following steps to display a list of defined Commerce Suite servers:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `getservers` command using the following syntax:

   ```
   getservers
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `getservers` command.

Removing a Server Profile From a Database

Perform the following steps to remove a server profile from a database:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `deleteserver` command using the following syntax:

   ```
   deleteserver
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `deleteserver` command.

Removing a Server Profile From Memory

Perform the following steps to remove a server profile from memory:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `removeserver` command using the following syntax:

   ```
   removeserver
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `removeserver` command.

Starting a Remote Commerce Suite Server on a Remote Host

Perform the following steps to start a remote Commerce Suite server on a remote host:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `remoteserver` command using the following syntax:

   ```
   remoteserver
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `remoteserver` command.

11 Trading Partner Administration

This section describes how to define and manage trading partners using the Commerce Suite command line interface (CLI).

Managing Trading Partner Relationships

The following topics provide instructions for managing your trading partner relationships using the CLI.

- Defining a New Trading Partner Pair
- Insert a Trading Partner Pair into a Database
- Display Active Trading Partner Pairs
- Read Trading Partner Pair Data From a Database
- Remove a Trading Partner Pair from a Database
- Remove a Trading Partner Pair From Memory

Refer to Chapter 2, “Starting and Stopping P2P Agent,” for instructions on starting the Commerce Suite application and accessing the command line interface.

Defining a New Trading Partner Pair

A trading partner relationship (or pair) consists of a set of data describing how data may be transferred from one defined trading partner to another defined trading partner. A trading partner may be identified and defined using an alphanumeric sequence of characters or a user-defined company or institution name.

Defining a new trading partner relationship (or pair) is accomplished by using the Commerce Suite `addpair` command. The `addpair` command defines a new trading partner relationship and stores trading partner relationship information in memory.

Perform the following steps to define a new trading partner pair from the Commerce Suite command line interface:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `addpair` command using the following syntax:

```
addpair <from> <to> <to-URL> <rcpt-URL> <notify-name> <inbox>
[<send-parameters>]
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `addpair` command.

Insert a Trading Partner Pair into a Database

You can use the Commerce Suite command-line interface to insert a trading partner pair into a database. Perform the following steps to insert a trading partner into the database:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `insertpair` command using the following syntax:

```
insertpair
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `insertpair` command.

Display Active Trading Partner Pairs

The Commerce Suite application allows you to view active and defined trading partner relationships (or pairs) using the command-line interface.

Displaying active trading partner pairs using the Commerce Suite CLI is accomplished using the `listpairs` command. Perform the following steps to display active trading partner pairs:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `listpairs` command using the following syntax:

   ```
   listpairs
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `listpairs` command.

Read Trading Partner Pair Data From a Database

You can use the Commerce Suite command-line interface to read trading partner pair data from a database. Reading trading partner pair data from a database is accomplished using the `getpairs` command. The `getpairs` command retrieves all trading partner relationship information from the database and populates the Commerce Suite memory with the configuration material needed to process message transfers.

The `getpairs` command is only functional if the database parameters have been defined with the `set -d?` commands and the `dbconnect` command has been issued.

Perform the following steps to read trading partner pair data from a database:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `listpairs` command using the following syntax:

```
getpairs
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `getpairs` command.

Remove a Trading Partner Pair from a Database

You can use the Commerce Suite command-line interface to remove a trading partner pair from a database. Removing a trading partner pair from a database is accomplished using the `deletepair` command.

Perform the following steps to remove a trading partner pair from a database:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `deletepair` command using the following syntax:

```
deletepair <from> <to> <protocol>
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `deletepair` command.

Remove a Trading Partner Pair From Memory

You can use the Commerce Suite command-line interface to remove a trading partner pair from memory. Removing a trading partner pair from memory is accomplished using the `removepair` command.

Perform the following steps to remove a trading partner pair from memory:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `removepair` command using the following syntax:

```
removepair
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `removepair` command.

CHAPTER

12 Certificate Administration

This section describes how to define and manage certificates using the Commerce Suite command line interface (CLI).

Managing Commerce Suite Certificates

The following topics provide instructions for managing your Commerce Suite certificates using the CLI.

- Creating Public-Key and Private-Key Material
- Removing a Public-Key Pair Definition From the Database
- Exporting Key-Pair Information to a File
- Reading Key-Pair Information From the Database
- Importing an X.509 Certificate and Corresponding Private-Key
- Inserting Public-Key Pair Information Into a Database
- Displaying Active Public-Key Pairs
- Replicating a Public-Key Pair to the Host
- Removing a Public-Key Pair From Memory
- Replicating a Public key-Pair to a Remote Host

Creating Public-Key and Private-Key Material

Public-key and private-key material is used for data encryption and authentication purposes and produced for a specific use by a specific trading relationship. The public-key is exportable to an X.509 digital-certificate format. The private-key is exportable to a PKS#1 RSA private-key format. Both the public and private key data may be stored in the database.

Creating public-key and private-key material is accomplished using the `addkey` command. Perform the following steps to create public and private-key material using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `addkey` command using the following syntax:

   ```
   addkey <from> <to> <usage> <key-bits> <issuer> <subject>
   ```

Refer to the *iSoft Commerce Suite Command Reference* document for additional information on using the `addkey` command.

Removing a Public-Key Pair Definition From the Database

Removing a public-key pair definition from the database is accomplished using the `deletekey` command. Perform the following steps to delete the public-key pair definition from the database using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `deletekey` command using the following syntax:

   ```
   deletekey <from> <to> <keyusage> <pending>
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `deletekey` command.

Exporting Key-Pair Information to a File

Exporting key-pair information to a file is accomplished using the `exportkey` command. Perform the following steps to export key-pair information to a file using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `exportkey` command using the following syntax:

```
exportkey <from> <to> <usage> <certificate-file>
<private-key-file>
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `exportkey` command.

Reading Key-Pair Information From the Database

Reading key-pair information from the database is accomplished using the `getkeys` command. The `getkeys` command retrieves all certificate and key material information from the database and populates the Commerce Suite memory with the security material needed to process message transfers.

Perform the following steps to read key-pair information from the database using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `getkeys` command using the following syntax:

```
getkeys
```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `getkeys` command.

Importing an X.509 Certificate and Corresponding Private-Key

Importing an X.509 certificate and corresponding private-key is accomplished using the `importkey` command. The imported key material must be associated with a defined trading partner relationship and usage code.

Perform the following steps to import an X.509 certificate and corresponding private-key using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `importkey` command using the following syntax:

   ```
   importkey <from> <to> <usage> [<option> [...] ]
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `importkey` command.

Inserting Public-Key Pair Information Into a Database

Inserting public-key pair information into a database is accomplished using the `insertkey` command. Perform the following steps to insert public-key information into a database using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `insertkey` command using the following syntax:

   ```
   insertkey <from> <to> <usage> <certfile> <keyfile> [<encrypt>
   [-p]]
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `insertkey` command.

Displaying Active Public-Key Pairs

Displaying active public-key pairs is accomplished using the `listkeys` command. Perform the following steps to display active public-key pairs using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `listkeys` command using the following syntax:

   ```
   listkeys
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `listkeys` command.

Replicating a Public-Key Pair to the Host

Replicating a public-key pair to a remote host is accomplished using the `remotekey` command. Perform the following steps to replicate a public-key pair to a remote host using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `remotekey` command using the following syntax:

   ```
   remotekey <from> <to> <usage>
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `remotekey` command.

Removing a Public-Key Pair From Memory

Removing a public-key pair from memory is accomplished using `removekey` command. Perform the following steps to remove a public-key pair from memory using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.

2. At the command prompt, enter the `removekey` command using the following syntax:

   ```
   removekey
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `removekey` command.

Replicating a Public key-Pair to a Remote Host

Replicating a public-key pair to a remote host is accomplished using `remotekey` command. Perform the following steps to replicate a public-key pair to a remote host using the Commerce Suite CLI:

1. Start the Commerce Suite application if it is not already running.
2. At the command prompt, enter the `remotekey` command using the following syntax:

   ```
   remotekey <from> <to> <usage>
   ```

Refer to *iSoft Commerce Suite Command Reference* for additional information on using the `remotekey` command.

A UNIX Configuration Information

This topic contains special topics and instructions for configuring Commerce Suite on UNIX operating systems.

Running Commerce Suite in the Background on a Linux Server

Execute the following command within a shell script to run the Commerce Suite application in the background on a Linux server.

```
nohup p2pagent -e &
```

This command completely frees the Commerce Suite application from a term session and will survive any interruption with the exception of a hardware change.

B Commerce Suite Firewall Configuration Considerations

The following configuration considerations will provide your firewall administrator the information needed to make the necessary firewall configuration changes to support communication with the Commerce Suite application.

The Commerce Suite application running in your environment requires a static IP address that is addressable from the Internet. If you are using the
Commerce Suite application behind a firewall, this address will be the address of the firewall. You must configure the firewall to support inbound and outbound connections with the Commerce Suite application.

This appendix is divided into the following two sections:

- Commerce Suite Firewall Considerations
- External Trading Partner Inbound Firewall Considerations
- External Trading Partner Outbound Firewall Considerations
- Wal-Mart Firewall Configuration

Commerce Suite Firewall Considerations

Use the following guidelines to facilitate configuration of your firewall for use with the Commerce Suite application. You can record your firewall configuration information in the spaces provided below each step.

1. Determine and record your firewall IP address.

   ____

2. Determine and record the port number that will be used for inbound AS2 messages. It is recommended that you use a port number like 4080, 5080, or 6080. This port number will be referred to as the external port number.

   ____

3. Determine and record the actual IP address of the internal machine running the Commerce Suite application.

   ____

4. Assign and record the port number that Commerce Suite, on the internal machine, will use for it’s HTTP listener. The address and port number is required during the Commerce Suite configuration process. We recommend that you use the same port number as your external port. This port number will be referred to as the internal port number.

   ____

5. Record the combination of your firewall IP address and your external port number. This address will be provided to your trading partners and used by the Commerce Suite configuration process.

   ____

6. Configure the firewall ports for TCP as the protocol.

7. If you are using Network Address Translation (NAT) to allow connections to your internal machine, you will need to create NAT rules at the firewall. Refer to the internal machine address and port information you recorded earlier in this appendix. For more information on configuring NAT rules for your firewall, consult your firewall documentation for more information on NAT.

External Trading Partner Inbound Firewall Considerations

Use the following guidelines to facilitate configuration of your external trading partner firewall for use with the Commerce Suite application.

1. You must configure a firewall outbound rule for the trading partner on the external port number that is the same as your port.
2. Identify your trading partners' sending IP address and potential port range they will use.

The following table provides the configuration information you need in order to conduct connectivity testing with iSoft.

Table B-1 Sent From iSoft Test Server Configuration Information

IP Definition	Configuration Value
IP Address	63.140.159.17
Port Range	Greater than 1023

Note: All AS2 messages sent from the iSoft Test server will originate from the IP address listed in Table C-1. In addition, the iSoft AS2 server can initiate multiple concurrent sending operations and will send from a range of ports listed in Table C-1.

3. Ensure each trading partner is configured for inbound and outbound AS2 traffic modifications to your firewall based on their trading partner specific IP address and port information.

External Trading Partner Outbound Firewall Considerations

The following configuration definitions will provide your firewall administrator the information needed to make the necessary firewall configuration changes to support outbound trading partner communications.

Your external trading partners will provide you with the external IP address and port on which they will receive the AS2 messages you send. You will use this information to configure your Commerce Suite application for the trading relationship with this partner. Additionally, you will need to configure your firewall to allow the Commerce Suite application on the secure side of your network to send messages to the trading partners AS2 server.

You must configure outbound firewall rules for each trading partner on the port number that is the same as the trading partners external port number.

Table B-2 Send To iSoft Test Server Configuration Information

IP Definition	Configuration Value
IP Address	63.140.159.17
Port	6080

Note: Each trading partner requires inbound and outbound modifications to your firewall based on trading partner specific IP address and port information.

Wal-Mart Firewall Configuration

The following Wal-Mart configuration definitions will provide your firewall administrator the information required to support communication with Wal-Mart.

Perform the following steps to configure your firewall to support communications with the Commerce Suite application:

1. Configure your firewall for Wal-Mart using the steps in the “External Trading Partner Outbound Firewall Considerations,” as a guide.
2. Wal-Mart will send data from the following four potential IP addresses:
   - 161.165.202.24
   - 161.165.202.25
   - 161.165.202.26
   - 161.165.202.27
3. Each address will send from a port range greater than 1023.
4. Configure the Network Address Translation (NAT) for the internal machine running the Commerce Suite application.
5. Configure your firewall to allow your internal machine to send AS2 messages to the Wal-Mart address of 161.165.202.30 on port 5080.

   Note: Each trading partner requires inbound and outbound modifications to your firewall based on trading partner specific IP address and port information.

C Commerce Suite for OS/400 Reference

This appendix explains how to install, configure, and use the Commerce Suite application with the OS/400 operating system.

This section contains the following topics:

- Introduction
- System Requirements
- Installing and Configuring Commerce Suite for OS/400
- Using Commerce Suite with OS/400

Introduction

The Commerce Suite application executes within the OS/400 Portable Applications Solutions Environment (PASE). The PASE is a fully integrated component of OS/400 that uses a subset of AIX functionality. It also exploits the PowerPC processor’s ability to switch between AS/400 and UNIX run-time modes.

Applications deployed using PASE run natively on the AS/400 and take full advantage of integration with its file systems, security, and DB2/400 database.

System Requirements

The PASE is an optional, nominally-priced feature of OS/400 (**Option 33**), which requires an OS/400 e-series or i-series processor-based machines or newer to run.

Perform the following steps to prepare the OS/400 operating system for Commerce Suite installation and configuration:

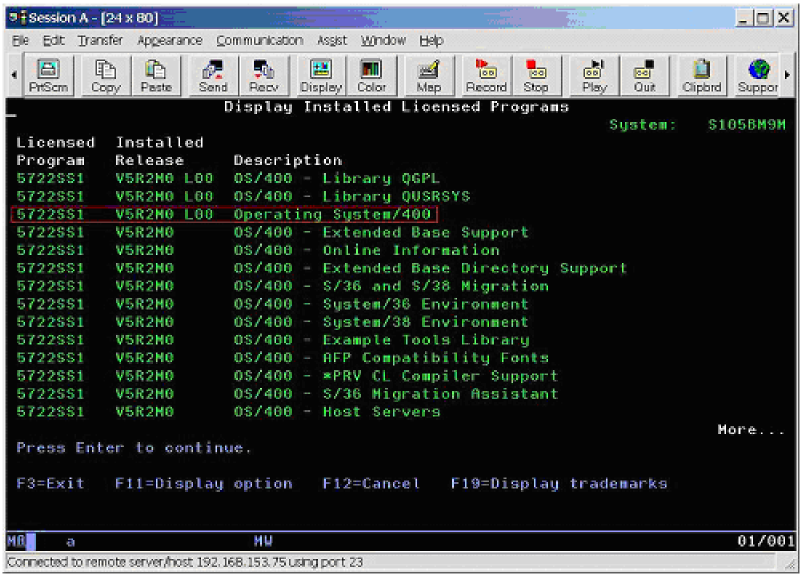
1. Verify the OS/400 operating software at version V5R2M0 or greater.
2. Verify the PASE optional feature is installed.
3. Configure and start TCP/IP for your domain.
4. Obtain the iSoft Commerce Suite for OS/400 CD-ROM containing the Commerce Suite distribution files for the OS/400 operating system.

Step 1 - Verifying the iSeries OS/400 Version

Perform the following steps to verify your OS/400 operating system is version V5R2M0 or greater:

1. From the OS/400 Main Menu, select **Option 7** (Define or change the system).
2. Select **Option 2** (Work with Licensed Programs).
3. Select **Option 10** (Display Installed Licensed Programs).
4. From the **Display Installed Licensed Programs** screen, press **F11** to switch to Display release. The release level for all installed products on your OS/400 displays as shown in the following screen shot.

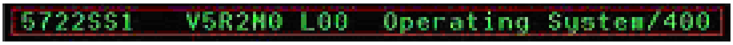
Figure C-1 Display OS/400 Release Version


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                     Display Installed Licensed Programs
                                                          System:   S105BM9M
Licensed  Installed
Program   Release     Description
5722SS1   V5R2M0 L00  OS/400 - Library QGPL
5722SS1   V5R2M0 L00  OS/400 - Library QUSRSYS
5722SS1   V5R2M0 L00  Operating System/400
5722SS1   V5R2M0      OS/400 - Extended Base Support
5722SS1   V5R2M0      OS/400 - Online Information
5722SS1   V5R2M0      OS/400 - Extended Base Directory Support
5722SS1   V5R2M0      OS/400 - S/36 and S/38 Migration
5722SS1   V5R2M0      OS/400 - System/36 Environment
5722SS1   V5R2M0      OS/400 - System/38 Environment
5722SS1   V5R2M0      OS/400 - Example Tools Library
5722SS1   V5R2M0      OS/400 - AFP Compatibility Fonts
5722SS1   V5R2M0      OS/400 - *PRV CL Compiler Support
5722SS1   V5R2M0      OS/400 - S/36 Migration Assistant
5722SS1   V5R2M0      OS/400 - Host Servers
                                                                   More...
Press Enter to continue.

F3=Exit   F11=Display option   F12=Cancel   F19=Display trademarks

MA    a             MW                                              01/001
```

Connected to remote server/host 192.168.153.75 using port 23

The required version information appears on the boxed line of the listed applications and confirms the required OS/400 version necessary to run with Commerce Suite.



```
5722SS1   V5R2M0 L00   Operating System/400
```

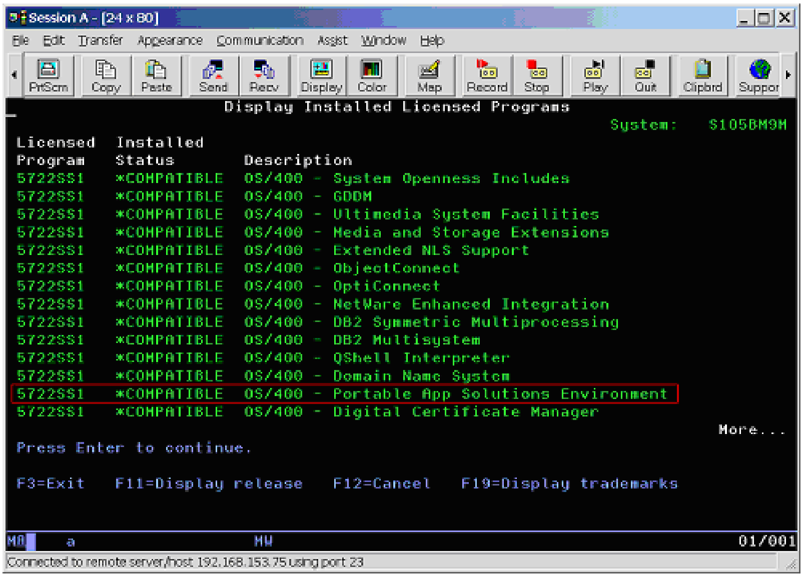
Step 2 - Verify the PASE Optional Feature is Installed

Perform the following steps to verify PASE is installed:

1. From the OS/400 Main Menu, select **Option 7** (Define or Change the System).
2. Select **Option 2** (Work with Licensed Programs).
3. Select **Option 10** (Display Installed Licensed Programs).

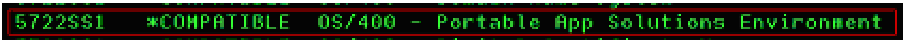
4. Scroll through the licensed programs list until the **Portable App Solutions Environment** entry is located as shown in the following screen shot.

Figure C-2 Display OS/400 Portable App Solutions Environment



```
                         Display Installed Licensed Programs
                                                              System:   S105BM9M
 Licensed   Installed
 Program    Status        Description
 5722SS1    *COMPATIBLE   OS/400 - System Openness Includes
 5722SS1    *COMPATIBLE   OS/400 - GDDM
 5722SS1    *COMPATIBLE   OS/400 - Ultimedia System Facilities
 5722SS1    *COMPATIBLE   OS/400 - Media and Storage Extensions
 5722SS1    *COMPATIBLE   OS/400 - Extended NLS Support
 5722SS1    *COMPATIBLE   OS/400 - ObjectConnect
 5722SS1    *COMPATIBLE   OS/400 - OptiConnect
 5722SS1    *COMPATIBLE   OS/400 - NetWare Enhanced Integration
 5722SS1    *COMPATIBLE   OS/400 - DB2 Symmetric Multiprocessing
 5722SS1    *COMPATIBLE   OS/400 - DB2 Multisystem
 5722SS1    *COMPATIBLE   OS/400 - QShell Interpreter
 5722SS1    *COMPATIBLE   OS/400 - Domain Name System
 5722SS1    *COMPATIBLE   OS/400 - Portable App Solutions Environment
 5722SS1    *COMPATIBLE   OS/400 - Digital Certificate Manager
                                                                       More...
 Press Enter to continue.

 F3=Exit    F11=Display release    F12=Cancel    F19=Display trademarks


MA     a                  MW                                            01/001
Connected to remote server/host 192.168.153.75 using port 23
```

The Portable App Solutions Environment entry appears in the boxed line of the Display Installed Licensed programs screen.



```
5722SS1    *COMPATIBLE   OS/400 - Portable App Solutions Environment
```

If the PASE feature is not listed as an installed licensed program, contact your IBM representative at a local branch office or contact an authorized IBM software remarketer to obtain any necessary software and license keys for the PASE product.

Step 3 - Configuring TCP/IP for Your Domain

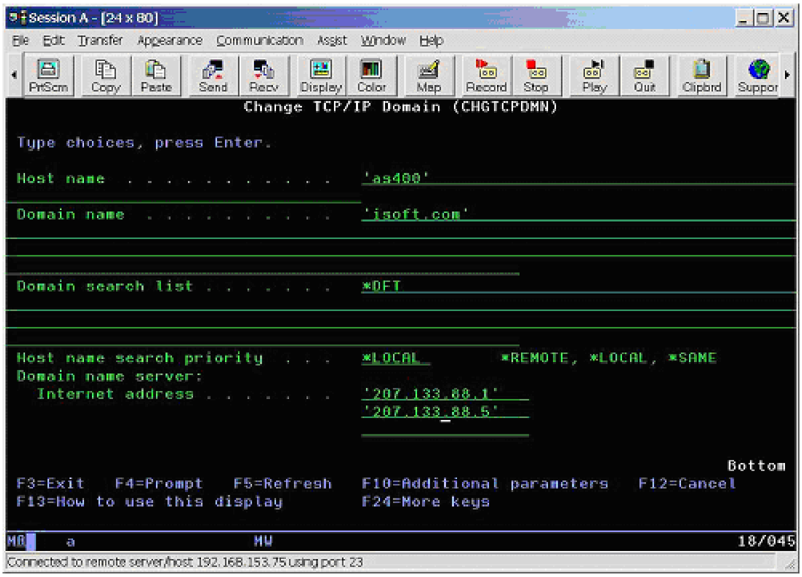
When starting the Commerce Suite application within the PASE, a reverse DNS lookup is necessary to obtain an Internet address from the hostname returned by the OS/400 system.

The host name and it's Domain name (if specified) must be either configured in the sites DNS server or in the local Host table. If no DNS server is configured here, then you must use the local Host table.

Perform the following steps to access TCP/IP domain settings:

1. From the OS/400 Main Menu, select **Option 6** (Communications).
2. Select **Option 5** (Network Management).
3. Select **Option 10** (TCP/IP Administration).
4. Select **Option 1** (Configure TCP/IP).
5. Select **Option 12** (Change TCP/IP Domain Information).

Figure C-3 Change TCP/IP Domain Settings



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                    Change TCP/IP Domain (CHGTCPDMN)

 Type choices, press Enter.

 Host name . . . . . . . . . . .   'as400'

 Domain name . . . . . . . . . .   'isoft.com'



 Domain search list . . . . . . .  *DFT



 Host name search priority . . .   *LOCAL        *REMOTE, *LOCAL, *SAME
 Domain name server:
   Internet address . . . . . . .  '207.133.88.1'
                                   '207.133.88.5'

                                                                    Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
MB     a                  MW                                         18/045
Connected to remote server/host 192.168.153.75 using port 23
```

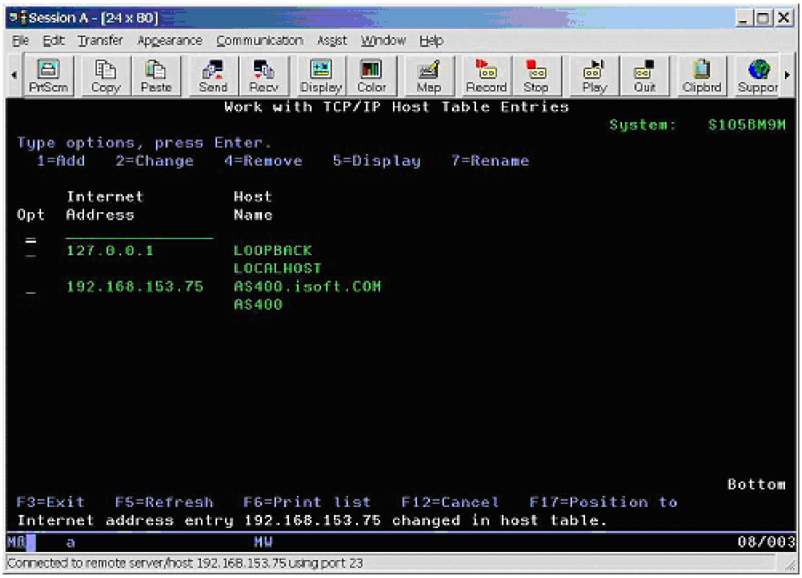
The Host name and its Domain name (if specified) must be either configured in the sites DNS server or in the local Host table.

Perform the following steps to access the TCP/IP host table:

1. From the OS/400 Main Menu, select **Option 6** (Communications).
2. Select **Option 5** (Network Management).

3. Select **Option 10** (TCP/IP Administration).
4. Select **Option 1** (Configure TCP/IP).
5. Select **Option 10** (Work with TCP/IP Host Table Entries).

Figure C-4 Work With TCP/IP Host Table Entries



```
                         Work with TCP/IP Host Table Entries
                                                          System:   S105BM9M
 Type options, press Enter.
   1=Add   2=Change   4=Remove   5=Display   7=Rename

      Internet          Host
 Opt  Address           Name

  _   127.0.0.1         LOOPBACK
                        LOCALHOST
  _   192.168.153.75    AS400.isoft.COM
                        AS400









                                                                      Bottom
 F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Position to
 Internet address entry 192.168.153.75 changed in host table.
MB     a                  MW                                         08/003
Connected to remote server/host 192.168.153.75 using port 23
```

6. Add an entry with the Internet Address of the OS/400 and the Host name with the Domain name (if specified) assigned in Figure 11-3.

Step 4 - Obtain the Commerce Suite for OS/400 Application

Contact your iSoft sales representative or authorized iSoft software remarketer to obtain a copy of the Commerce Suite software.

Installing and Configuring Commerce Suite for OS/400

Perform the following steps to install and configure Commerce Suite for OS/400:

1. Copy the product distribution file to the OS/400 Integrated File System (IFS) file system.
2. Extract the product from the `tar` file.
3. Edit the iSoft Commerce Suite `p2pstart` startup script.
4. Entering the Commerce Suite Runtime License.

All commands on the OS/400 are entered from the command line or can be accessed from the OS/400 menu system.

Step 1 - Copying the Product Distribution File to the OS/400 IFS File System

The product distribution file is a standard compressed UNIX `tar` (Tape Archiver) file. It was created on an IBM/AIX platform and is in an ASCII file format that is compatible with the OS/400 IFS running under the PASE.

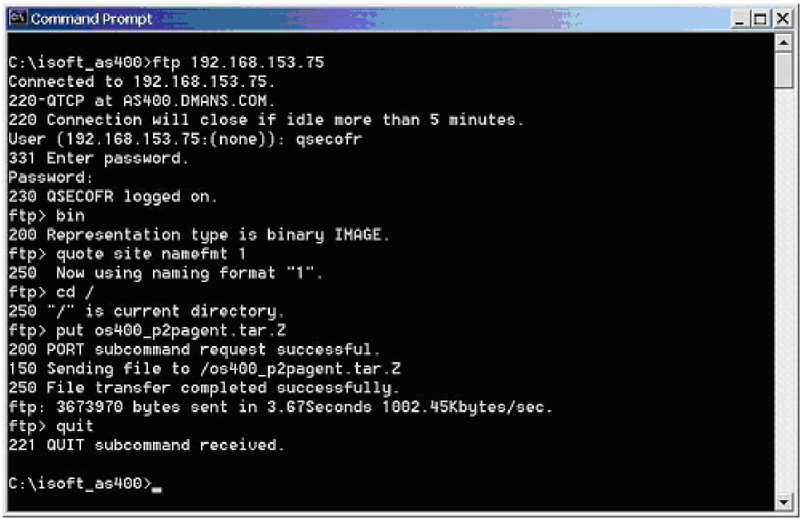
Perform the following steps to copy the distribution file to the OS/400 file system:

1. On the taskbar, click the **Start** button, then click **Programs**, then click **Accessories**, then click **Command Prompt**. The Command prompt opens.
2. Enter `ftp` and the IP address of the OS/400 system to which you are transferring the file.
3. Enter your user ID.

4. Enter your password.
5. Enter `bin` to designate the file type as binary.
6. Enter `quote site namefmt 1` to indicate that you are using the IFS file system and not the Object File System (OFS) library.
7. Enter `cd /` to change directories to the IFS root or the directory of your choice.
8. Enter `put os400_p2pagent.tar.z` to send your file.
9. Enter `quit` once your file has been transferred. The `File transfer completed successfully` message displays.

   The following screen shot provides an example of this command sequence to transfer the file using the FTP Client provided with Microsoft Windows.

Figure C-5 FTP Command Sequence



```
C:\isoft_as400>ftp 192.168.153.75
Connected to 192.168.153.75.
220-QTCP at AS400.DMANS.COM.
220 Connection will close if idle more than 5 minutes.
User (192.168.153.75:(none)): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> quote site namefmt 1
250  Now using naming format "1".
ftp> cd /
250 "/" is current directory.
ftp> put os400_p2pagent.tar.Z
200 PORT subcommand request successful.
150 Sending file to /os400_p2pagent.tar.Z
250 File transfer completed successfully.
ftp: 3673970 bytes sent in 3.67Seconds 1002.45Kbytes/sec.
ftp> quit
221 QUIT subcommand received.

C:\isoft_as400>_
```

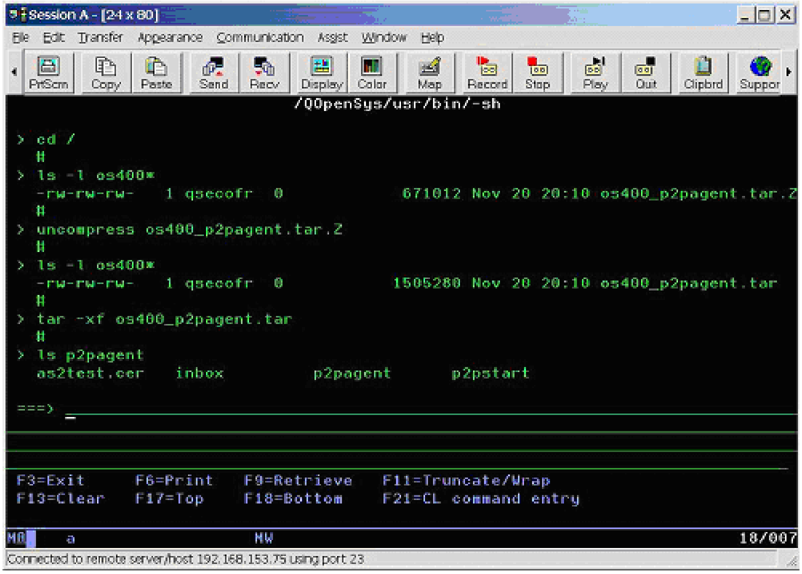
Step 2 - Extract the Product From the tar File

Once you have copied the `tar` file to the OS/400 system, you must access the PASE to extract the Commerce Suite product from the `tar` file. Extracting the `tar` file creates the `p2pagent` directory and installs all of the product files and directories.

Perform the following steps to extract the Commerce Suite product from the tar file:

1. Enter `call qp2term` on the OS/400 command line to invoke the PASE in terminal mode. This invokes a standard UNIX-like environment.
2. Enter `cd /` to change directories to the IFS root or to the directory where you placed the distribution tar file.
3. Enter `ls -1 os400*` to search the current directory for the installation `tar` file that was previous transferred. If it is not listed, then either the transfer failed or the file was stored in a directory other than the `IFS` root directory.
4. Enter `uncompress os400_p2pagent.tar.Z` to uncompresses the `tar` file so that it can be extracted. Any file with a `.Z` suffix is standard UNIX notation for a compressed file. If this command fails, it is most likely because the file was not transferred in binary mode or the OS/400 IFS file system is full.
5. Enter `ls -1 os400*` to search the current directory for the installation `tar` file. It should now be larger and not have the `.Z` suffix.
6. Enter `tar -xf os400_p2pagent.tar` to extract the installation `tar` file and all the programs, files, and subdirectories will be stored in the `p2pagent` directory.
7. Enter `ls p2pagent` to list the `p2pagent` directory and it's contents.

Figure C-6 Extracting the tar File



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                          /QOpenSys/usr/bin/-sh

 > cd /
   $
 > ls -l os400*
   -rw-rw-rw-    1 qsecofr   0           671012 Nov 20 20:10 os400_p2pagent.tar.Z
   $
 > uncompress os400_p2pagent.tar.Z
   $
 > ls -l os400*
   -rw-rw-rw-    1 qsecofr   0          1505280 Nov 20 20:10 os400_p2pagent.tar
   $
 > tar -xf os400_p2pagent.tar
   $
 > ls p2pagent
   as2test.cer    inbox          p2pagent       p2pstart

===> _

 F3=Exit      F6=Print     F9=Retrieve    F11=Truncate/Wrap
 F13=Clear    F17=Top      F18=Bottom     F21=CL command entry

MB     a                   MW                                            18/007
Connected to remote server/host 192.168.153.75 using port 23
```

The following list contains all of the files and directories contained in the installation `tar` file:

- `p2pagent/`
- `p2pagent/p2pagent`
- `p2pagent/p2pagent.cfg`
- `p2pagent/p2pstart`
- `p2pagent/inbox/`
- `p2pagent/receipt/`
- `p2pagent/log/`
- `p2pagent/as2test.cer`
- `p2pagent/as2test.prv`

Step 3 - Editing the Commerce Suite p2pstart Startup Script

If you installed the Commerce Suite in a directory other than `/p2pagent`, you must change the `p2pstart` script to reflect the directory you have chosen. This can be accomplished by either transferring the `p2pstart` script to a UNIX or Windows system with FTP Client, or editing the script directly on the OS/400 using the Edit File Utility (EDTF).

Updating the p2pstart Script on the OS/400

Perform the following steps to update the p2pstart script on the OS/400:

1. On the taskbar, click the **Start** button, then click **Programs**, then click **Accessories**, then click **Command Prompt**. The Command prompt opens.
2. Enter `EDTF /p2pagent/p2pstart` on the command line.

   Note: If entering EDTF from the command line, you must specify the fully-qualified path and file name as a parameter, or an error will be generated and returned.

   If you want to work from the OS/400 Main Menu, perform the following steps:

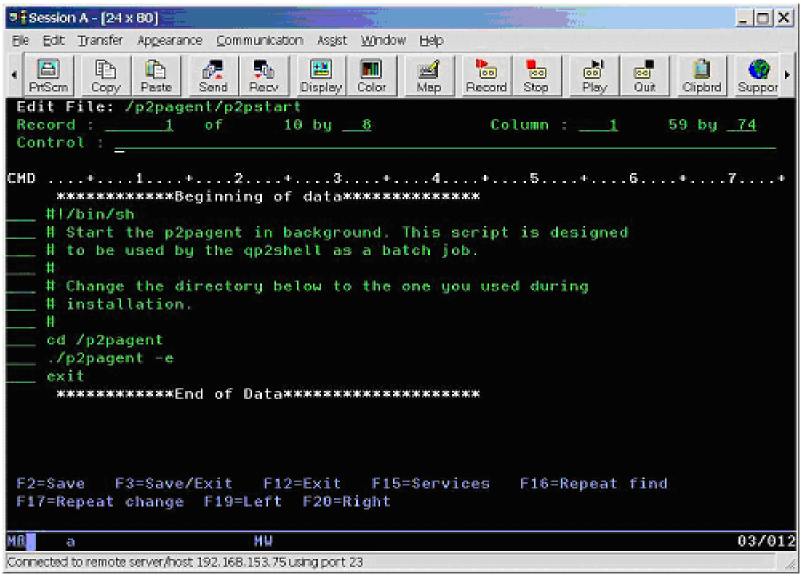
   a. Select **Option 4** (Files, Libraries, Folders)

   b. Select **Option 1** (Files)

   c. Select **Option 11** (Edit a Stream File or Database File)

   The following screen shot provides an example of the `EDTF` command with the `p2pstart` script.

Figure C-7 EDTF Command with the p2pstart Script


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
 Edit File: /p2pagent/p2pstart
 Record : _______1   of      10 by __8            Column : ___1      59 by _74
 Control : _

CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+
     ************Beginning of data**************
___ #!/bin/sh
___ # Start the p2pagent in background. This script is designed
___ # to be used by the qp2shell as a batch job.
___ #
___ # Change the directory below to the one you used during
___ # installation.
___ #
___ cd /p2pagent
___ ./p2pagent -e
___ exit
     ************End of Data********************



 F2=Save   F3=Save/Exit   F12=Exit   F15=Services   F16=Repeat find
 F17=Repeat change  F19=Left  F20=Right

MB    a                  MW                                            03/012
```

Connected to remote server/host 192.168.153.75 using port 23

Writing Your Own Script on a Platform Other Than OS/400

If you decide to write your own script on a platform other than OS/400, you must observe the following rules:

- You must enter `quote site namefmt 1` when transferring the file to/from the OS/400 to invoke the transfer to the IFS file system.
- You must transfer the file in ASCII (text) mode.

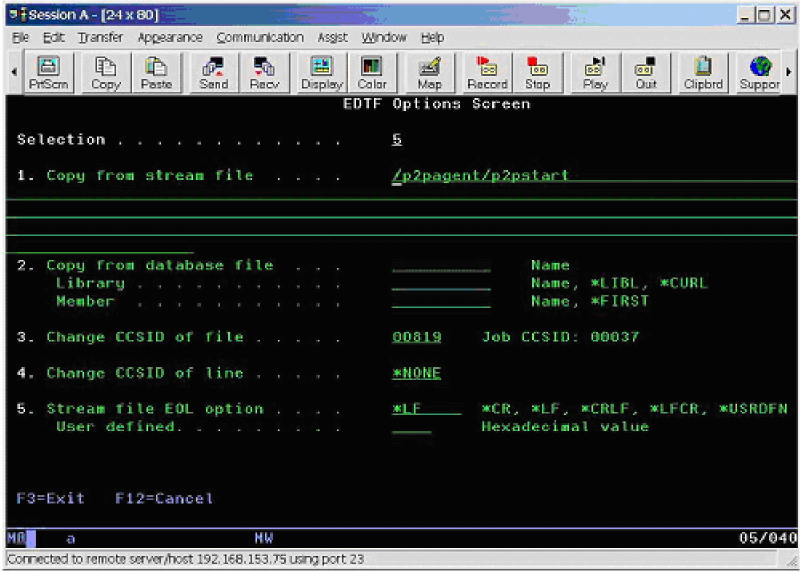
Perform the following steps on the OS/400 after the new script is transferred:

1. Once the `p2pstart` script transfer is complete, you must edit the file to change the line termination characters from OS/400 standard CRLF (Carriage Return/Line Feed) to UNIX standards LF (Line Feed) only.
2. Enter `EDTF /p2pagent/p2pstart` on the command line.
3. Once EDTF is started, press F15 to switch to the services screen.

4. Enter 5 in the **Selection** field and tab down to the **Stream file EOL** option and enter *LF for Line Feed only.

   The following screen shot provides an example of the **EDTF Options Screen**.

Figure C-8 EDTF Options Screen



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn
Copy
Paste
Send
Recv
Display
Color
Map
Record
Stop
Play
Quit
Clipbrd
Suppor
MA a MW 05/040
Connected to remote server/host 192.168.153.75 using port 23

```
                              EDTF Options Screen

 Selection . . . . . . . . . . . . .     5

 1. Copy from stream file  . . . .      /p2pagent/p2pstart

 2. Copy from database file  . . .      __________     Name
      Library . . . . . . . . . . .     __________     Name, *LIBL, *CURL
      Member  . . . . . . . . . . .     __________     Name, *FIRST

 3. Change CCSID of file . . . . .      00819     Job CCSID: 00037

 4. Change CCSID of line . . . . .      *NONE

 5. Stream file EOL option . . . .      *LF       *CR, *LF, *CRLF, *LFCR, *USRDFN
      User defined. . . . . . . . .     ____      Hexadecimal value


 F3=Exit   F12=Cancel
```

Writing Your Own Script Directly on the OS/400

If you decide to write your own script directly on the OS/400 using EDTF, the following considerations must be observed:

- After your script is entered into EDTF, you must press F15 to change the **Stream File EOF** option to *LF as shown in the previous figure.
- You must also change the CCSID (Coded Character Set Identifier) of the file to 00819 (which is the ISO8859-1 Latin-1 ASCII Character set). This is accomplished by selecting **Option 3** on the **EDTF Options** screen and tab down to **Change CCSID** of file and enter 00819.

Note: The default character set of EDTF os 00037 (which is IBM-037 Latin-1 EBDIC character set).

Step 4 - Entering the Commerce Suite Runtime License

This step configures the Commerce Suite runtime product license. The Commerce Suite product, as shipped, operates in *Demonstration* mode. When the product is purchased, you are supplied license keys to convert the product to *Authorized Installation* mode.

If you plan on running the product in Demonstration mode, you can skip this step.

Note: In Demonstration mode, Commerce Suite will not transfer payloads to a trading partner located on another host computer.

If you are configuring the product for *Authorized Installation* mode, you must have completed the following:

- TCP/IP Configuration must be complete. Refer to the *System Requirements* section of this chapter for instructions.
- You must have obtained a valid serial number for Commerce Suite from iSoft Technical Support.
- You must have obtained a valid authentication code for Commerce Suite from iSoft Technical Support.

If TCP/IP configuration is not complete or is changed after the license information is entered into the product, you must contact iSoft Technical Support to obtain new licensing information.

Part of the following license installation steps require a Windows or UNIX system.

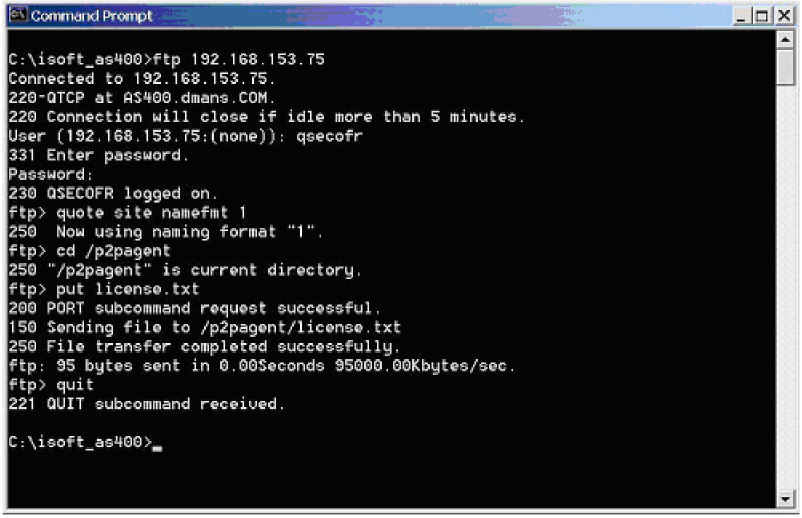
Perform the following steps to generate your Commerce Suite license key file:

1. Using either Notepad (Windows OS) or vi (UNIX), create a file named `license.txt`.
2. Enter the serial number supplied to you by iSoft Technical Support. The serial number entry should look similar to the following example:

   ```
   serial-number: 3462BFA-BF98DD3A-30AD55A4-1F66DF4B-220211C3-
   00987FCA-ED0BAB24-24F8BC14-013DC216
   ```

3. Save the `license.txt` file. Once the file is saved, you must transfer the file to the OS/400 system using the FTP Client.
4. On the taskbar, click the **Start** button, then click **Programs**, then click **Accessories**, then click **Command Prompt**. The Command prompt opens.
5. From the `c:\isoft_as400` directory, or the directory where you saved the `License.txt` file, enter `ftp` and the OS/400 TCP/UP address.
6. Enter your user ID and press **Enter**.
7. Enter your password and press **Enter**.
8. Enter `quote site namefmt 1` to invoke the transfer to the IFS file system. The file must be transferred in ASCII (Text) mode.
9. Enter `cd /` to change directories to the IFS root or the directory where the Commerce Suite was installed.
10. Enter `put license.txt` to transfer the `license.txt` file to the directory you installed Commerce Suite into, which by default is `/p2pagent`. Once the file is transferred, you must access the PASE on the OS/400.

Figure C-9 Transfer License.txt



```
C:\isoft_as400>ftp 192.168.153.75
Connected to 192.168.153.75.
220-QTCP at AS400.dmans.COM.
220 Connection will close if idle more than 5 minutes.
User (192.168.153.75:(none)): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> quote site namefmt 1
250  Now using naming format "1".
ftp> cd /p2pagent
250 "/p2pagent" is current directory.
ftp> put license.txt
200 PORT subcommand request successful.
150 Sending file to /p2pagent/license.txt
250 File transfer completed successfully.
ftp: 95 bytes sent in 0.00Seconds 95000.00Kbytes/sec.
ftp> quit
221 QUIT subcommand received.

C:\isoft_as400>_
```

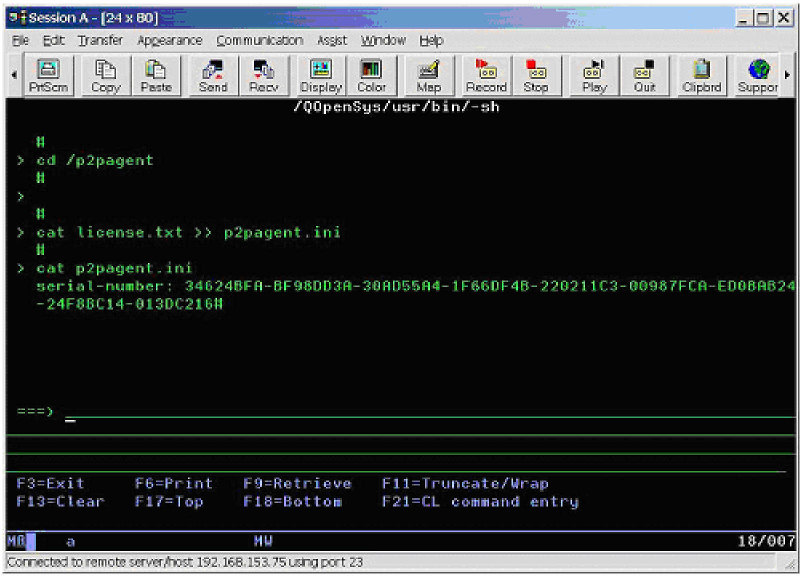
11. Enter `call qp2term` from the OS/400 command line to invoke the PASE in terminal mode.

12. Enter `cd /` to change directories to the IFS root or the directory of your choice.

13. Enter `cat license.txt >> p2pagent.ini` to append the `license.txt` file to the `p2pagent.ini` file. If the `p2pagent.ini` file does not exist, it is created with the contents of the `license.txt` file.

14. Enter `cat p2pagent.ini` to display the contents of the `p2pagent.ini` file for verification

Figure C-10 Update p2pagent.ini File with license.tct File



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                              /QOpenSys/usr/bin/-sh

   $
 > cd /p2pagent
   $
 >
   $
 > cat license.txt >> p2pagent.ini
   $
 > cat p2pagent.ini
   serial-number: 34624BFA-BF98DD3A-30AD55A4-1F66DF4B-220211C3-00987FCA-ED0BAB24
   -24F8BC14-013DC216$




 ===> _


 F3=Exit      F6=Print     F9=Retrieve    F11=Truncate/Wrap
 F13=Clear    F17=Top      F18=Bottom     F21=CL command entry
```

MB a MW 18/007
Connected to remote server/host 192.168.153.75 using port 23

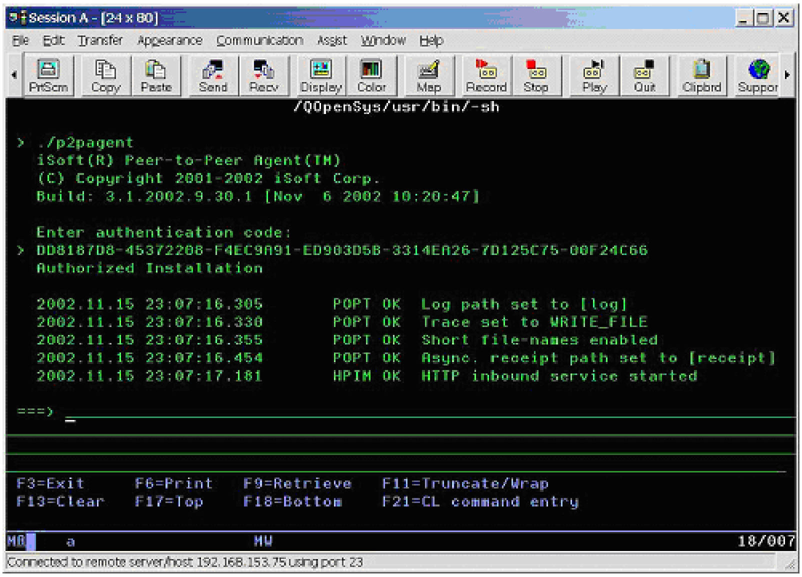
15. Enter `./p2pagent` from the `qp2term` terminal shell to start Commerce Suite.

    The `./p2pagent` command starts the Commerce Suite using the program in the current directory. When Commerce Suite is started for the first time, it will prompt you for the authentication code that was supplied to you by iSoft Technical Support. The authentication code should look similar to the following example.

    ```
    DD8187D8-45372208-F4EC9A91-ED903D5B-3314EA26-7D125C75-00F24C66
    ```

16. Enter the authentication code on the command line and press Enter. The following figure provides a screen shot of the process and the response from Commerce Suite if both the serial number and the authentication code are valid.

Figure C-11 Product Runtime License


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                            /QOpenSys/usr/bin/-sh

 > ./p2pagent
   iSoft(R) Peer-to-Peer Agent(TM)
   (C) Copyright 2001-2002 iSoft Corp.
   Build: 3.1.2002.9.30.1 [Nov  6 2002 10:20:47]

   Enter authentication code:
 > DD8187D8-45372208-F4EC9A91-ED903D5B-3314EA26-7D125C75-00F24C66
   Authorized Installation

   2002.11.15 23:07:16.305       POPT OK  Log path set to [log]
   2002.11.15 23:07:16.330       POPT OK  Trace set to WRITE_FILE
   2002.11.15 23:07:16.355       POPT OK  Short file-names enabled
   2002.11.15 23:07:16.454       POPT OK  Async. receipt path set to [receipt]
   2002.11.15 23:07:17.181       HPIM OK  HTTP inbound service started

 ===> _


 F3=Exit      F6=Print     F9=Retrieve    F11=Truncate/Wrap
 F13=Clear    F17=Top      F18=Bottom     F21=CL command entry

MB    a                    MW                                           18/007
Connected to remote server/host 192.168.153.75 using port 23
```

Using Commerce Suite with OS/400

This information contained in this section for using Commerce Suite is limited to the features that are unique to the OS/400. The following topics are discussed:

- Working with the p2pagent.cfg File
- Starting Commerce Suite as a Batch Job
- Verifying Commerce Suite is Running
- Stopping Commerce Suite as a Batch Job
- Running Commerce Suite in Interactive Mode
- Working With Commerce Suite Payload Files

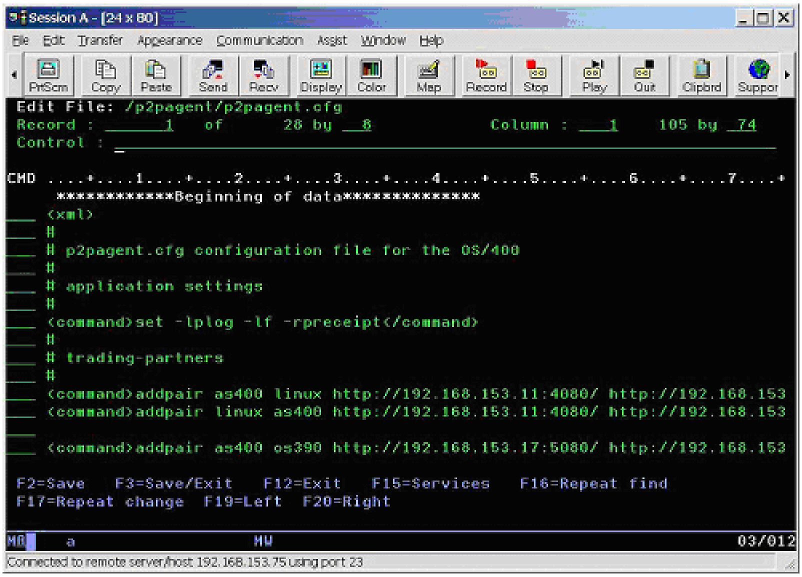
Working with the p2pagent.cfg File

The Commerce Suite configuration file (`p2pagent.cfg`) is located in the `/p2pagent` installation directory, or whatever directory you used for installation. This file contains all the default startup parameters that are used when you start the Commerce Suite program in either batch mode or interactive mode.

Note: It is recommended that either Notepad under Microsoft Windows, or vi under UNIX is used to edit the file as lines are longer then regular green screen modes and require working with left and right movement if using EDTF in a 5250 terminal session.

The following figure shows an open configuration file in the stream file editor (EDTF).

Figure C-12 Sample p2pagent.cfg in EDTF



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
 Edit File: /p2pagent/p2pagent.cfg
 Record : _______1   of       28 by __8            Column : ____1    105 by _74
 Control : _

CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+
     ************Beginning of data**************
____ <xml>
____ #
____ # p2pagent.cfg configuration file for the OS/400
____ #
____ # application settings
____ #
____ <command>set -lplog -lf -rpreceipt</command>
____ #
____ # trading-partners
____ #
____ <command>addpair as400 linux http://192.168.153.11:4080/ http://192.168.153
____ <command>addpair linux as400 http://192.168.153.11:4080/ http://192.168.153
____
____ <command>addpair as400 os390 http://192.168.153.17:5080/ http://192.168.153

 F2=Save   F3=Save/Exit   F12=Exit   F15=Services   F16=Repeat find
 F17=Repeat change  F19=Left  F20=Right

MB     a                MW                                              03/012
Connected to remote server/host 192.168.153.75 using port 23
```

The same rules for editing the `p2pagent.cfg` file apply as for the `p2pstart` script file.

Please see *Step 3 - Editing the Commerce Suite p2pstart Startup Script* for information on using the different editors available when updating the `p2pagent.cfg` file.

Starting Commerce Suite as a Batch Job

Starting Commerce Suite as a batch job is accomplished in the following two ways:

- Using the OS/400 Menu System
- Invoking PASE in Terminal Mode

Using the OS/400 Menu System

Perform the following steps to start Commerce Suite in batch mode using the OS/400 menu system:

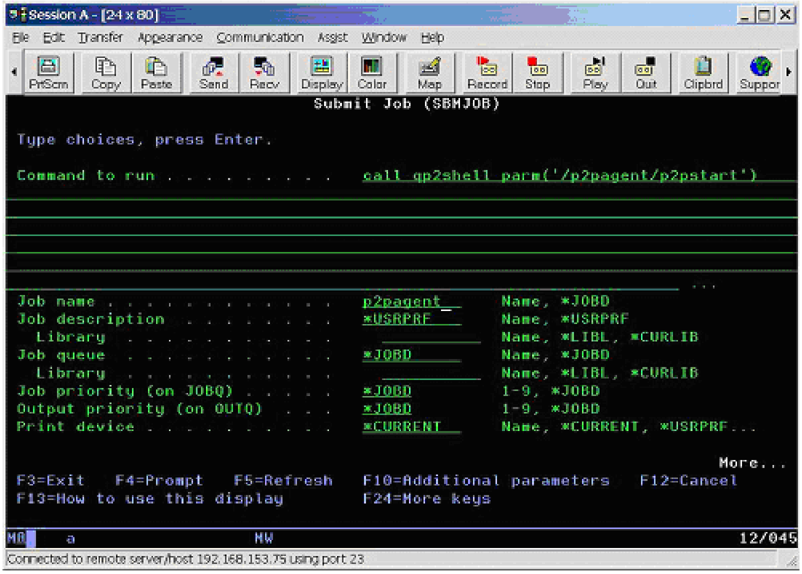
1. Enter `SBMJOB` (Submit Job) on the command line

   or

   a. Select **Option 1** (User Tasks)

   b. Select **Option 4** (Submit a Job) from the OS/400 Main Menu.

Figure C-13 Submit Job (SBMJOB) Screen


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                           Submit Job (SBMJOB)

 Type choices, press Enter.

 Command to run . . . . . . . . .   call qp2shell parm('/p2pagent/p2pstart')

                                                                         ...
 Job name . . . . . . . . . . . .   p2pagent      Name, *JOBD
 Job description  . . . . . . . .   *USRPRF       Name, *USRPRF
   Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
 Job queue  . . . . . . . . . . .   *JOBD         Name, *JOBD
   Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
 Job priority (on JOBQ) . . . . .   *JOBD         1-9, *JOBD
 Output priority (on OUTQ)  . . .   *JOBD         1-9, *JOBD
 Print device . . . . . . . . . .   *CURRENT      Name, *CURRENT, *USRPRF...

                                                                      More...
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys

MA     a                 MW                                           12/045
```

Connected to remote server/host 192.168.153.75 using port 23

2. Enter `call qp2shell parm ('/p2pagent/p2pstart')` in the **Command to run** field to specify the actual command that becomes the batch job.

Running the `qp2shell` invokes the PASE environment without a terminal session. The `parm` specifies the directory that the Commerce Suite was installed into (`/p2pagent`) and the program to execute (`p2pagent`).

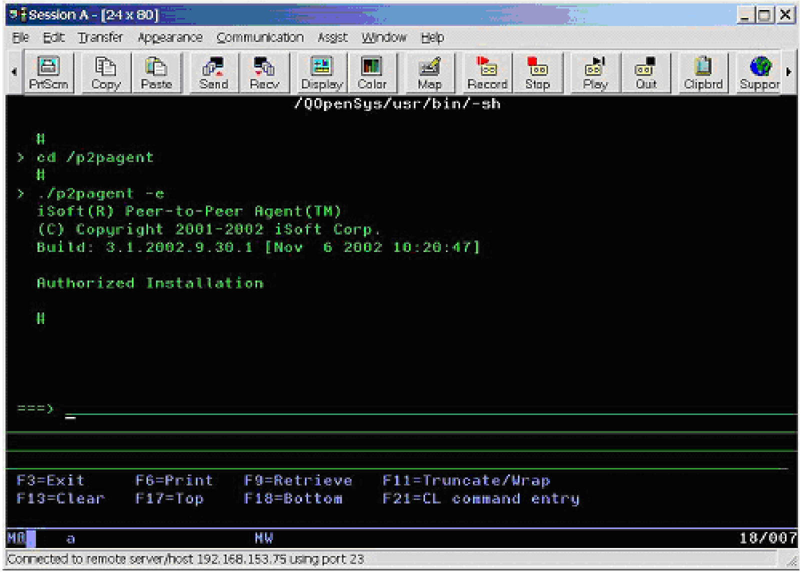
The `p2pstart` program is a shell script that invokes the Commerce Suite as a daemon (`-e` command line switch) to run in the background and sets the current directory with a UNIX `cd` (change directory) command.

Invoking PASE in Terminal Mode

Perform the following steps to start Commerce Suite as a batch job using PASE:

1. Enter `call qp2term` at the command line to start the process from PASE.

Figure C-14 Starting Commerce Suite From PASE



```
                              /QOpenSys/usr/bin/-sh

  $
> cd /p2pagent
  $
> ./p2pagent -e
  iSoft(R) Peer-to-Peer Agent(TM)
  (C) Copyright 2001-2002 iSoft Corp.
  Build: 3.1.2002.9.30.1 [Nov  6 2002 10:20:47]

  Authorized Installation

  $




===> _

F3=Exit      F6=Print     F9=Retrieve    F11=Truncate/Wrap
F13=Clear    F17=Top      F18=Bottom     F21=CL command entry

MA    a                   MW                                          18/007
Connected to remote server/host 192.168.153.75 using port 23
```

2. Enter `cd /p2pagent` to change the current directory to `/p2pagent`. If you installed the Commerce Suite in another directory, you must specify that directory.

3. Enter `./p2pagent -e` to start the Commerce Suite using the program in the current directory. The `-e` option tells the Commerce Suite to disconnect itself from the terminal session and run as a daemon (run in the background as a batch job).

Verifying Commerce Suite is Running

Verifying that Commerce Suite is running is accomplished using any of the following methods:

- View submitted jobs
- View a list of active jobs
- Invoke PASE in terminal mode

Viewing Submitted Jobs

Perform the following steps to verify Commerce Suite is running:

1. Enter `WRKSBMJOB` (Work With Submitted Jobs) on the command line.

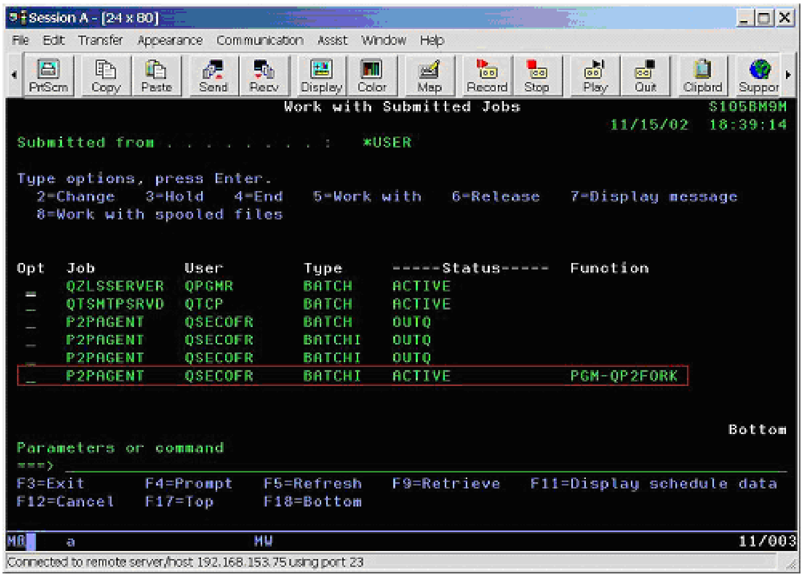
   or

   a. Select **Option 1** (User Tasks)

   b. Select **Option 6** (Work with your batch jobs) from the OS/400 Main Menu.

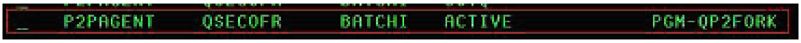
2. Scroll through the listed batch jobs and select the Commerce Suite entry. If the entry is not found, then Commerce Suite is not running.

Figure C-15 Display Batch Jobs Screen


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                        Work with Submitted Jobs                    S105BM9M
                                                          11/15/02  18:39:14
Submitted from . . . . . . . . . :   *USER

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files


Opt  Job          User         Type       -----Status-----   Function
 _   QZLSSERVER   QPGMR        BATCH      ACTIVE
 _   QTSMTPSRVD   QTCP         BATCH      ACTIVE
 _   P2PAGENT     QSECOFR      BATCH      OUTQ
 _   P2PAGENT     QSECOFR      BATCHI     OUTQ
 _   P2PAGENT     QSECOFR      BATCHI     OUTQ
 _   P2PAGENT     QSECOFR      BATCHI     ACTIVE             PGM-QP2FORK


                                                                      Bottom
Parameters or command
===>
F3=Exit      F4=Prompt    F5=Refresh   F9=Retrieve    F11=Display schedule data
F12=Cancel   F17=Top      F18=Bottom
MA   a                   MW                                             11/003
Connected to remote server/host 192.168.153.75 using port 23
```

The Commerce Suite entry (P2PAGENT) appears on the boxed line of the Work With Submitted Jobs screen.



```
 _   P2PAGENT     QSECOFR      BATCHI     ACTIVE             PGM-QP2FORK
```

Viewing a List of Active jobs

Perform the following steps to verify Commerce Suite is running:

1. Enter `WRKACTJOB` (Work With Active Jobs) on the command line.

   or

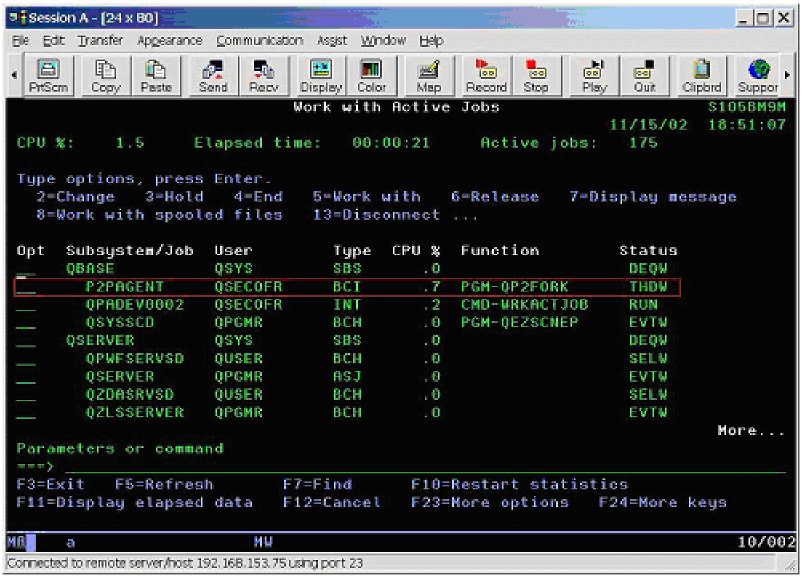
   a. Select **Option 3** (General System Tasks)

   b. Select **Option 1** (Jobs)

   c. Select **Option 2** (Work With All Active Job Statistics) from the OS/400 Main Menu.

2. Scroll through the listed active jobs and select the **Commerce Suite** entry. If the entry is not found, then the Commerce Suite is not running.

Figure C-16   Display Active Jobs Screen



```
                          Work with Active Jobs                   S105BM9M
                                                         11/15/02  18:51:07
CPU %:     1.5     Elapsed time:    00:00:21     Active jobs:   175

Type options, press Enter.
  2=Change    3=Hold    4=End    5=Work with    6=Release    7=Display message
  8=Work with spooled files     13=Disconnect ...

Opt  Subsystem/Job  User        Type   CPU %  Function          Status
___    QBASE         QSYS        SBS      .0                     DEQW
___      P2PAGENT    QSECOFR     BCI      .7  PGM-QP2FORK        THDW
___      QPADEV0002  QSECOFR     INT      .2  CMD-WRKACTJOB      RUN
___      QSYSSCD     QPGMR       BCH      .0  PGM-QEZSCNEP       EVTW
___    QSERVER       QSYS        SBS      .0                     DEQW
___      QPWFSERVSD  QUSER       BCH      .0                     SELW
___      QSERVER     QPGMR       ASJ      .0                     EVTW
___      QZDASRVSD   QUSER       BCH      .0                     SELW
___      QZLSSERVER  QPGMR       BCH      .0                     EVTW
                                                                       More...
Parameters or command
===> _________________________________________________________________________
F3=Exit    F5=Refresh        F7=Find        F10=Restart statistics
F11=Display elapsed data     F12=Cancel     F23=More options    F24=More keys

MB     a                MW                                              10/002
```

Connected to remote server/host 192.168.153.75 using port 23

The Commerce Suite (P2PAGENT) entry appears on the boxed line of the Work With Active Jobs screen.

```
___      P2PAGENT    QSECOFR     BCI      .7  PGM-QP2FORK        THDW
```

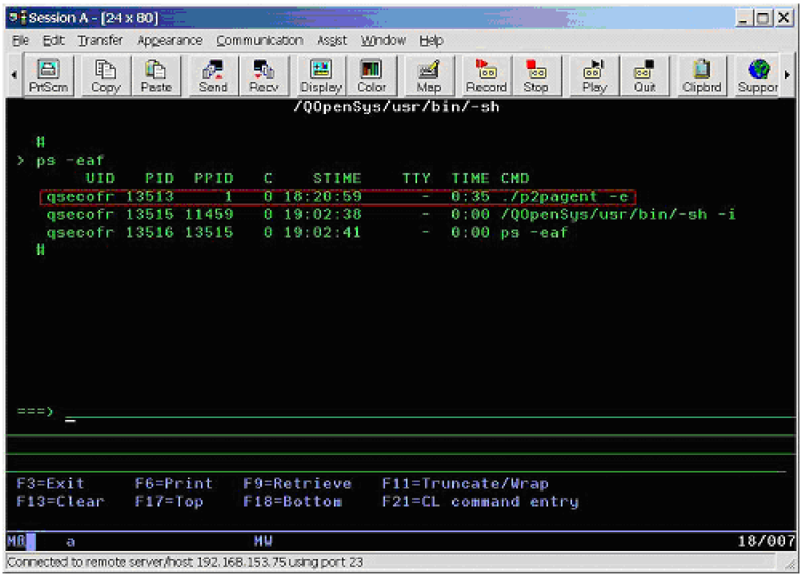
This screen also provides CPU utilization and other statistics about running the jobs.

Invoking PASE in Terminal Mode

Perform the following steps to verify Commerce Suite is running:

1. Enter `call qp2term` to invoke the PASE in terminal mode. This also invokes a standard UNIX environment.
2. Enter `ps -eaf` to display all running processes within the PASE.
3. Scroll through the listed active processes and select the **Commerce Suite** entry. If the entry is not found, then the Commerce Suite is not running.

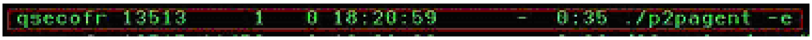
Figure C-17 Display Active Processes Within PASE


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                            /QOpenSys/usr/bin/-sh

  #
> ps -eaf
       UID   PID  PPID   C    STIME    TTY  TIME CMD
   qsecofr 13513     1   0 18:20:59      -  0:35 ./p2pagent -c
   qsecofr 13515 11459   0 19:02:38      -  0:00 /QOpenSys/usr/bin/-sh -i
   qsecofr 13516 13515   0 19:02:41      -  0:00 ps -eaf
  #

===> _

F3=Exit      F6=Print     F9=Retrieve     F11=Truncate/Wrap
F13=Clear    F17=Top      F18=Bottom      F21=CL command entry
MB    a                 MW                                        18/007
```

Connected to remote server/host 192.168.153.75 using port 23

The Commerce Suite (P2PAGENT) entry appears on the boxed line of the active screen.



```
qsecofr 13513     1   0 18:20:59      -  0:35 ./p2pagent -c
```

Stopping Commerce Suite as a Batch Job

Stopping Commerce Suite as a batch job is accomplished in the following two ways:

- Using the OS/400 Menu System
- Invoking PASE in Terminal Mode

Using the OS/400 Menu System

Perform the following steps to stop Commerce Suite in batch mode using the OS/400 menu system:

1. Enter `WRKSBMJOB` (Work With Submitted Jobs) on the command line.

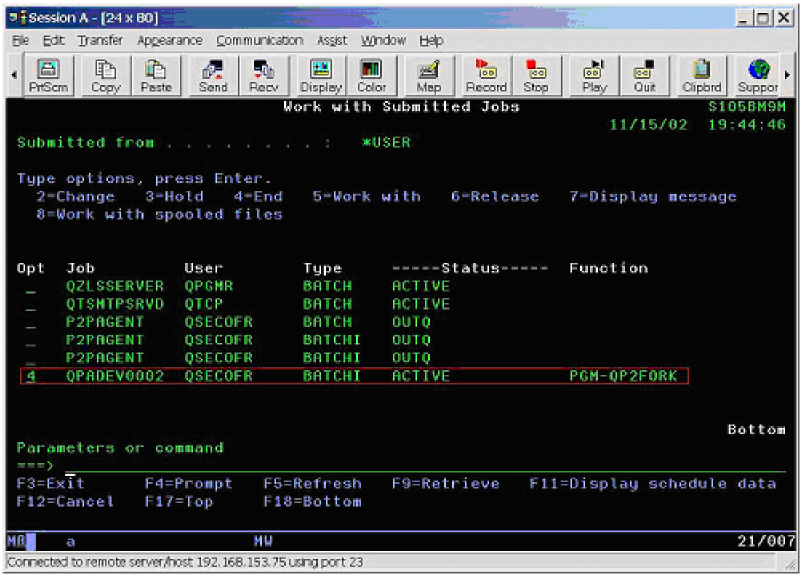
   or

   a. Select **Option 1** (User Tasks)

   b. Select **Option 6** (Work With Your Batch Jobs) from the OS/400 Main Menu.

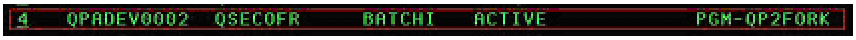
2. Scroll through the listed batch jobs and select the **P2P Agent** entry. If the entry is not found, then Commerce Suite is not running.

Figure C-18 Stopping Commerce Suite using the WRKSBMJOB Command


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                       Work with Submitted Jobs                   S105BM9M
                                                         11/15/02  19:44:46
Submitted from . . . . . . . . :    *USER

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files


Opt  Job         User        Type     -----Status-----  Function
 _   QZLSSERVER  QPGMR       BATCH    ACTIVE
 _   QTSMTPSRVD  QTCP        BATCH    ACTIVE
 _   P2PAGENT    QSECOFR     BATCH    OUTQ
 _   P2PAGENT    QSECOFR     BATCHI   OUTQ
 _   P2PAGENT    QSECOFR     BATCHI   OUTQ
 4   QPADEV0002  QSECOFR     BATCHI   ACTIVE            PGM-QP2FORK



                                                                     Bottom
Parameters or command
===>
F3=Exit        F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display schedule data
F12=Cancel     F17=Top     F18=Bottom
MB      a                  MW                                         21/007
Connected to remote server/host 192.168.153.75 using port 23
```

The submitted job entry appears on the boxed line of the Work With Submitted Jobs screen.



```
4   QPADEV0002   QSECOFR      BATCHI    ACTIVE             PGM-QP2FORK
```

3. Select **Option 4** to end the Commerce Suite application.

Note: If the system is busy, it might take a minute or so for the process to end. The process will also finish any work that is currently being performed before stopping the application.

Invoking PASE in Terminal Mode

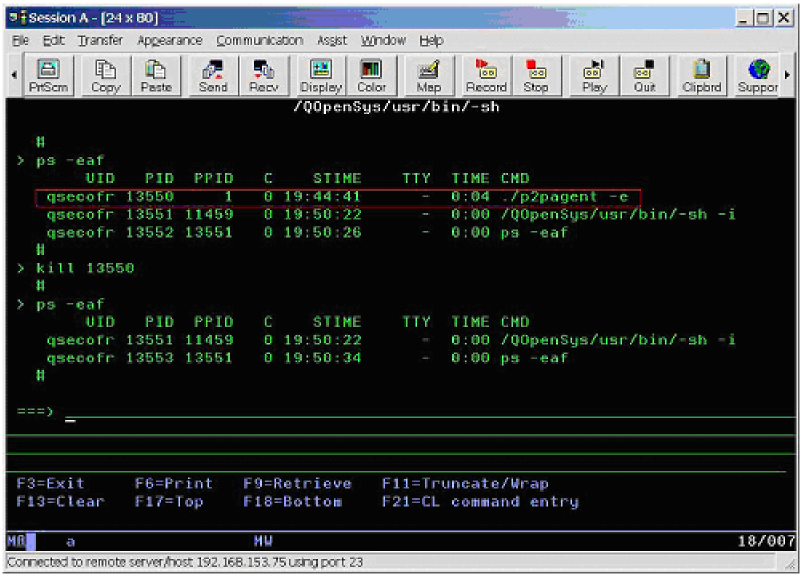
Perform the following steps to stop Commerce Suite by invoking PASE in terminal mode:

1. Enter `call qp2term` on the command line to invoke the PASE in terminal mode.

2. Enter `ps -eaf` to display all running processes within the PASE.

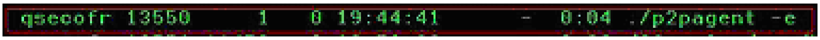
3. Scroll through the listed active processes and select the Commerce Suite entry. If the entry is not found, then the Commerce Suite is not running.

Figure C-19 Stopping Commerce Suite From PASE


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor
MB a MW 18/007
Connected to remote server/host 192.168.153.75 using port 23

```
                          /QOpenSys/usr/bin/-sh

   #
 > ps -eaf
        UID   PID  PPID   C    STIME    TTY  TIME CMD
    qsecofr 13550     1   0 19:44:41      -  0:04 ./p2pagent -e
    qsecofr 13551 11459   0 19:50:22      -  0:00 /QOpenSys/usr/bin/-sh -i
    qsecofr 13552 13551   0 19:50:26      -  0:00 ps -eaf
   #
 > kill 13550
   #
 > ps -eaf
        UID   PID  PPID   C    STIME    TTY  TIME CMD
    qsecofr 13551 11459   0 19:50:22      -  0:00 /QOpenSys/usr/bin/-sh -i
    qsecofr 13553 13551   0 19:50:34      -  0:00 ps -eaf
   #

 ===> _

 F3=Exit      F6=Print     F9=Retrieve    F11=Truncate/Wrap
 F13=Clear    F17=Top      F18=Bottom     F21=CL command entry
```

The Commerce Suite entry appears on the boxed line of the active screen.



```
  qsecofr 13550     1   0 19:44:41      -  0:04 ./p2pagent -e
```

4. Make note of the Commerce Suite process ID number (PID). It is located under the **PID** heading on the same entry line as the process name (`./p2pagent -e`)

5. Enter `kill #` where the `#` is the PID for the Commerce Suite process. In the figure above, the command would look like the following:

   ```
   kill 13550
   ```

6. Enter `ps -eaf` to ensure the process is gone.

Note: If the system is busy, it might take a minute for the process to end. The process will also finish any work that is currently being performed before stopping the application.

Running Commerce Suite in Interactive Mode

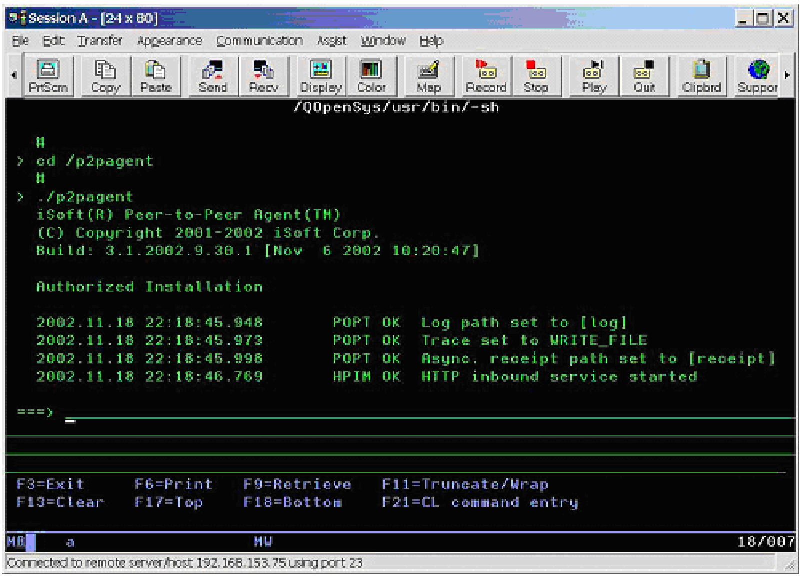
Commerce Suite can be run in either batch mode or in single user interactive mode. In order to run Commerce Suite in batch and interactive mode at the same time, Commerce Suite must be installed in separate directories as both instances would try and share the same `p2pagent.cfg` file if started from the same directory.

To run Commerce Suite in interactive mode, the PASE shell must be running in terminal mode.

Perform the following steps to run Commerce Suite in interactive mode:

1. Enter `call qp2term` from the command line to invoke the PASE in terminal mode and also invokes a standard UNIX-like environment.
2. Enter `cd /p2pagent` to change the current directory to `/p2pagent`.
3. Enter `./p2pagent` to start Commerce Suite using the application in the current directory. Without specifying any options, Commerce Suite runs in the foreground in interactive mode.

Figure C-20 Running Commerce Suite in the Foreground


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
                                  /QOpenSys/usr/bin/-sh

   #
 > cd /p2pagent
   #
 > ./p2pagent
   iSoft(R) Peer-to-Peer Agent(TM)
   (C) Copyright 2001-2002 iSoft Corp.
   Build: 3.1.2002.9.30.1 [Nov  6 2002 10:20:47]

   Authorized Installation

   2002.11.18 22:18:45.948       POPT OK  Log path set to [log]
   2002.11.18 22:18:45.973       POPT OK  Trace set to WRITE_FILE
   2002.11.18 22:18:45.998       POPT OK  Async. receipt path set to [receipt]
   2002.11.18 22:18:46.769       HPIM OK  HTTP inbound service started

 ===> _

 F3=Exit      F6=Print    F9=Retrieve    F11=Truncate/Wrap
 F13=Clear    F17=Top     F18=Bottom     F21=CL command entry

MB     a                  MW                                          18/007
```

Connected to remote server/host 192.168.153.75 using port 23

From the command line you can enter any of the transactions described in the *iSoft Commerce Suite Administration Guide*.

4. Enter `shutdown` to end the Commerce Suite process and leave you in the PASE shell. Or you can press **F3** to end the process and exit the PASE shell.

Working With Commerce Suite Payload Files

Files received and generated by Commerce Suite are placed within the IFS file system in directories specified by the `p2pagent.cfg` file or by commands issued within interactive mode.

There are a number of different directories that are used by Commerce Suite to record information generated by the process or to store files to be transmitted, or received by the process. Please refer to the *iSoft Commerce Suite Installation Guide* for a complete list of directories and their options.

The two main directories are:

- inbox

  This directory contains all the payload, messages, notices, and so forth, transmitted to the Commerce Suite by a trading partner. The directory is specified by an `addpair` statement. The directory is usually a subdirectory from the `/p2pagent` install directory.

- receipt

  This directory contains transmission receipts requested from the Commerce Suite trading partner. The directory is specified by a `set` statement `-rp` (receipt path) option. The directory is usually a subdirectory from the `/p2pagent` installation directory.

The typical format of a payload file stored in the inbox directory is:

Listing C-1 Payload File Structure

```
linux.as400.20021119230145E0D30E81file.in
  |     |     |  | | | | |   |     |   |_____________Extension
  |     |     |  | | | | |   |     |__________Inbound file name
  |     |     |  | | | | |   |___________Random sequence number
  |     |     |  | | | | |___________Second the file was received
  |     |     |  | | | |________Minute the file was received
  |     |     |  | | |______Hour the file was received
  |     |     |  | |_____Day the file was received
  |     |     |  |_____Month the file was received
  |     |     |___Year the file was received
  |     |______Our Name (To)
  |________Name of the trading partner transmitting the file (From)
```

Most of the payload file name can be customized. Files are stored in the character set in which they were transmitted, which is normally ISO8859-1 (Latin 1 ASCII Character Set). Your application can read these files directly from the IFS file system by specifying the file name in IBM OS/400 standard IFS notation.

```
/p2pagent/inbox/linux.as400.2002111923014E0D30E81file.in
```

You can translate the data (if necessary) from ASCII to EBCDIC in your program by using the ICONV library interface (LIBICONV). Please refer to the IBM publication National Language Support Guide and Reference for more information on character set translation.

You can also use the PASE utility ICONV. This is a utility that is standard on IBM operating platforms. An example of converting a file from ASCII to EBCDIC using ICONV might look similar to the following code example:

```
cat ascii_file | iconv -f ISO8859-1 -t IBM-037 > ebcdic_file
```

The above command, which is executed within the PASE environment, takes the ASCII file `ascii_file` and converts it from ASCII to EBCDIC and creates a new file `ebcdic_file`.

Copying the Payload File

Perform the following steps to copy your payload file to a OFS file system member:

1. Enter `CPYFRMSTMF` (Copy From Stream File) on the command line to copy the file to a OFS file system member.

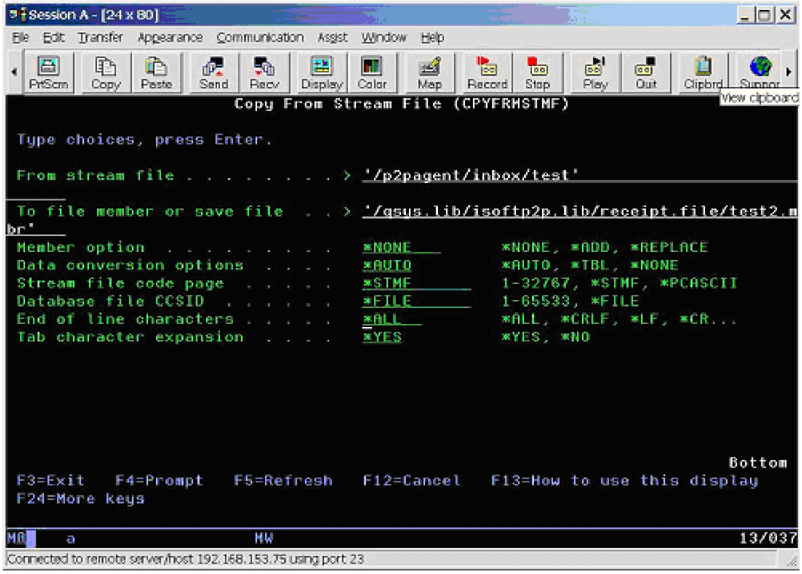
   or

   a. Select **Option 4** (Files, libraries, and folders)

   b. Select **Option 5** (Integrated File System)

   c. Select **Option 11** (Copy From Stream File)

Figure C-21 Copy From Stream File Sample


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Support
View clipboard

```
                    Copy From Stream File (CPYFRMSTMF)

 Type choices, press Enter.

 From stream file . . . . . . . . . > '/p2pagent/inbox/test'

 To file member or save file  . . . > '/qsys.lib/isoftp2p.lib/receipt.file/test2.m
br'
 Member option  . . . . . . . . . .   *NONE         *NONE, *ADD, *REPLACE
 Data conversion options  . . . . .   *AUTO         *AUTO, *TBL, *NONE
 Stream file code page  . . . . . .   *STMF         1-32767, *STMF, *PCASCII
 Database file CCSID  . . . . . . .   *FILE         1-65533, *FILE
 End of line characters . . . . . .   *ALL          *ALL, *CRLF, *LF, *CR...
 Tab character expansion  . . . . .   *YES          *YES, *NO



                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

MA     a                  MW                                             13/037
```

Connected to remote server/host 192.168.153.75 using port 23

2. In the **Stream File Code Page** field, enter ***STMF** to use the character set of the file as it was written.

3. In the **Database File CCSID** field, enter ***FILE** to use the character set the file was created with.

D Commerce Suite for OS/390 Reference

This appendix explains how to install, configure, and use the Commerce Suite application for use with the OS/390 operating system.

This section contains the following topics:

- Introduction
- System Requirements
- Installing and Configuring Commerce Suite for OS/390
- Using Commerce Suite with OS/390

Introduction

The Commerce Suite application executes under the OS/390 UNIX System Services (OS/390 UNIX). The OS/390 UNIX environment is a fully integrated component of OS/390 that provides both features and a subset of the commands found in a standard UNIX environment.

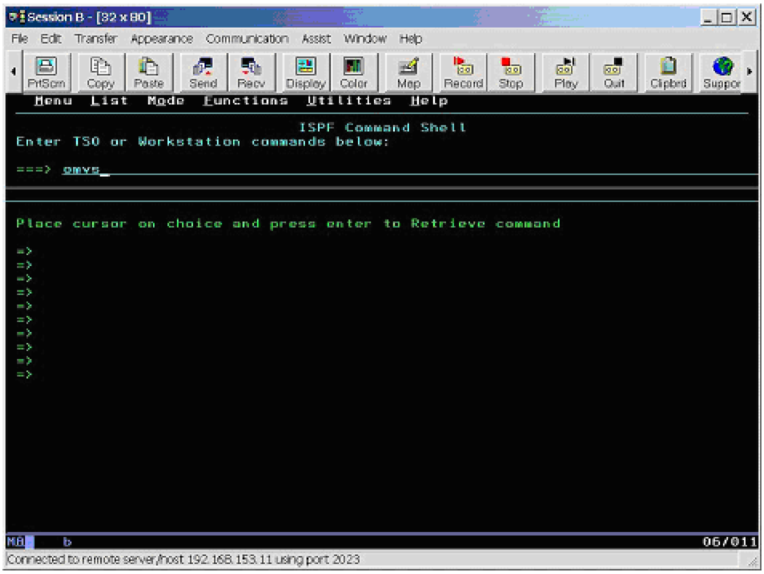
System Requirements

Perform the following steps to prepare the OS/390 operating system for Commerce Suite installation and configuration:

1. Verify the OS/390 operating software at version 02.07.00 or greater.
2. Verify the OS/390 UNIX system services is installed and active.
3. Configure and start TCP/IP for your domain.
4. Obtain the iSoft Commerce Suite for OS/390 CD-ROM containing the Commerce Suite distribution files for the OS/390 operating system.

Note: All commands used within UNIX System Services can be entered from the `OMVS` command under TSO or a telnet terminal session into the UNIX System Services region. All examples shown in this section are from the `OMVS` command under TSO.

Figure D-1 Invoking UNIX System Services from TSO


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
 Menu  List  Mode  Functions  Utilities  Help
                              ISPF Command Shell
Enter TSO or Workstation commands below:

===> omvs_

Place cursor on choice and press enter to Retrieve command

=>
=>
=>
=>
=>
=>
=>
=>
=>
=>
```

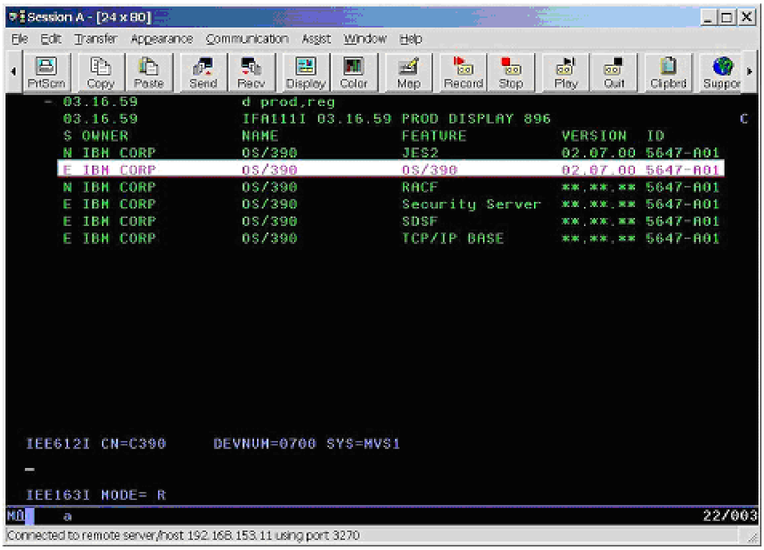
MB b 06/011
Connected to remote server/host 192.168.153.11 using port 2023

Step 1 - Verifying the OS/390 Version

Perform the following steps to verify your OS/390 operating system is version 02.07.00 or greater:

1. From an OS/390 operations console, enter `D PROD,REG`. This command displays information about registered products.

Figure D-2 Display OS/390 Release Version



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
 - 03.16.59              d prod,reg
   03.16.59              IFA111I 03.16.59 PROD DISPLAY 896                  C
   S OWNER               NAME             FEATURE           VERSION  ID
   N IBM CORP            OS/390           JES2              02.07.00 5647-A01
   E IBM CORP            OS/390           OS/390            02.07.00 5647-A01
   N IBM CORP            OS/390           RACF              **.**.** 5647-A01
   E IBM CORP            OS/390           Security Server   **.**.** 5647-A01
   E IBM CORP            OS/390           SDSF              **.**.** 5647-A01
   E IBM CORP            OS/390           TCP/IP BASE       **.**.** 5647-A01




 IEE612I CN=C390      DEVNUM=0700 SYS=MVS1

 -

 IEE163I MODE= R
MA     a                                                              22/003
```

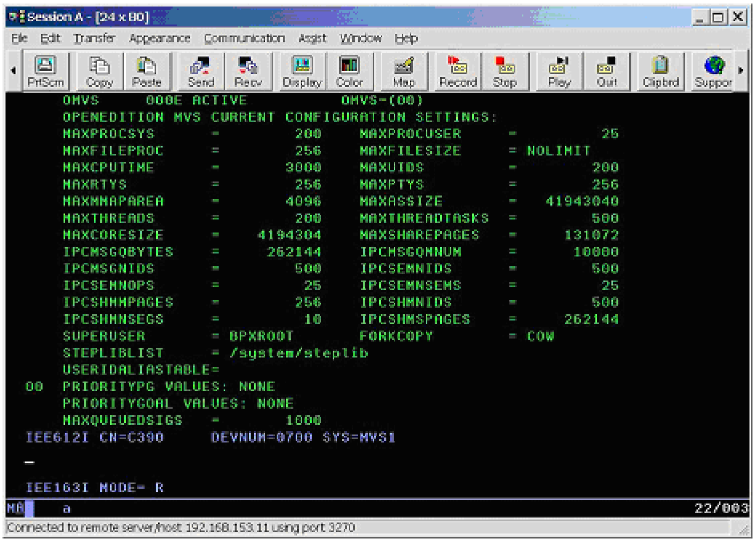
Connected to remote server/host 192.168.153.11 using port 3270

The required version information appears on the boxed line of the listed registered products and confirms the required OS/390 version necessary to run with Commerce Suite.

Step 2 - Verify UNIX System Services is Installed and Active

From an OS/390 operations console enter `D OMVS,O`. This command displays information about UNIX Systems Services and the options currently in effect.

Figure D-3 Display OS/390 UNIX System Services Environment


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
      OMVS      000E ACTIVE            OMVS=(00)
      OPENEDITION MVS CURRENT CONFIGURATION SETTINGS:
      MAXPROCSYS      =         200    MAXPROCUSER     =         25
      MAXFILEPROC     =         256    MAXFILESIZE     = NOLIMIT
      MAXCPUTIME      =        3000    MAXUIDS         =        200
      MAXRTYS         =         256    MAXPTYS         =        256
      MAXMMAPAREA     =        4096    MAXASSIZE       =   41943040
      MAXTHREADS      =         200    MAXTHREADTASKS  =        500
      MAXCORESIZE     =     4194304    MAXSHAREPAGES   =     131072
      IPCMSGQBYTES    =      262144    IPCMSGQMNUM     =      10000
      IPCMSGNIDS      =         500    IPCSEMNIDS      =        500
      IPCSEMNOPS      =          25    IPCSEMNSEMS     =         25
      IPCSHMMPAGES    =         256    IPCSHMNIDS      =        500
      IPCSHMNSEGS     =          10    IPCSHMSPAGES    =     262144
      SUPERUSER       = BPXROOT        FORKCOPY        = COW
      STEPLIBLIST     = /system/steplib
      USERIDALIASTABLE=
  00  PRIORITYPG VALUES: NONE
      PRIORITYGOAL VALUES: NONE
      MAXQUEUEDSIGS   =        1000
  IEE612I CN=C390      DEVNUM=0700 SYS=MVS1

  _

  IEE163I MODE= R
MA      a                                                               22/003
```

Connected to remote server/host 192.168.153.11 using port 3270

If the UNIX System Services environment is not active, contact your IBM support representative to obtain any necessary software, installation instructions, or support.

Step 3 - Configuring TCP/IP for Your Domain

When starting the Commerce Suite application within UNIX Systems Services, a reverse DNS lookup is necessary to obtain an Internet address from the hostname returned by the OS/390 system.

The host name and it's Domain name (if specified) must be either configured in the sites DNS server, or in the local Host table. If no DNS server is configured here, then you must use the local Host table.

Perform the following steps to access TCP/IP domain settings:

1. Enter `cd /etc` to change directories to the `etc` directory.
2. Enter `ls -l hosts` to verify that you have a local host file.
3. Enter `ls -l resolv.conf` to verify that you have a DNS resolver configuration file.

Below is a sample DNS resolver configuration file:

Listing D-1 Sample /etc/resolv.conf File

```
TCPIPJobName TCPIP
DomainOrigin isoft.com
domain isoft.com
Datasetprefix TCPIP
HostName MVS1
Messagecase mixed
NameServer 192.168.1.1
```

If DNS is not being used, you must either create an `/etc/hosts` file or append a new entry to it with the TCP/IP hostname name of your MVS system.

Add an entry with the Internet Address of the OS/390 and the Host name with and without the Domain name.

The following is an example of the `/etc/hosts` file:

Listing D-2 Sample /etc/hosts File

```
192.168.1.1  mvs1 mvs1.isoft.com
```

Step 4 - Obtain the Commerce Suite for OS/390 Application

Contact your iSoft sales representative or authorized iSoft software remarketer to obtain a copy of the Commerce Suite software.

Installing and Configuring Commerce Suite for OS/390

Perform the following steps to install and configure Commerce Suite for OS/390:

1. Copy the product distribution file to the OS/390 Hierarchical File System (HFS)
2. Extract the product from the tar file
3. Edit the p2pbatch procedure
4. Edit the p2pstart script
5. Enter the Commerce Suite Runtime License

Step 1 - Copying the Product Distribution File to the OS/390 HFS File System

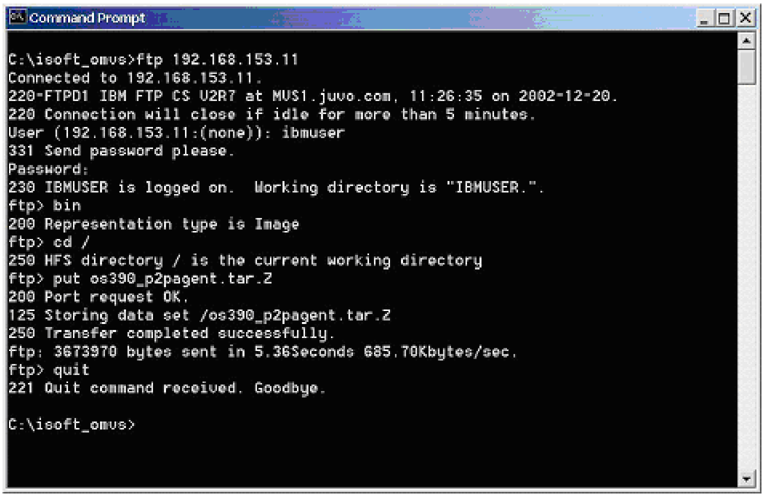
The product distribution file is a standard compressed UNIX tar (Tape Archiver) file. It was created on an OS/390 platform and is in an EBCDIC file format that is compatible with the OS/390 HFS running under UNIX System Services.

Perform the following steps to copy the distribution file to the OS/390 file system:

1. On the taskbar, click **Start**, then click **Programs**, then click **Accessories**, then click **Command Prompt**. The Command prompt opens.
2. Enter `ftp` and the IP address of the OS/390 system to which you are transferring the file.
3. Enter your user ID.
4. Enter your password.
5. Enter `bin` to designate the file type as binary.
6. Enter `cd /` to change directories to the HFS root or the directory of your choice.
7. Enter `put os390_p2pagent.tar.Z` to send your file.
8. Enter `quit` once your file has been transferred. The *File transfer completed successfully message* displays.

The following screen shot provides an example of this command sequence to transfer the file using the FTP Client provided with Microsoft Windows.

Figure D-4 FTP Command Sequence



```
C:\isoft_omvs>ftp 192.168.153.11
Connected to 192.168.153.11.
220-FTPD1 IBM FTP CS V2R7 at MVS1.juvo.com, 11:26:35 on 2002-12-20.
220 Connection will close if idle for more than 5 minutes.
User (192.168.153.11:(none)): ibmuser
331 Send password please.
Password:
230 IBMUSER is logged on.  Working directory is "IBMUSER.".
ftp> bin
200 Representation type is Image
ftp> cd /
250 HFS directory / is the current working directory
ftp> put os390_p2pagent.tar.Z
200 Port request OK.
125 Storing data set /os390_p2pagent.tar.Z
250 Transfer completed successfully.
ftp: 3673970 bytes sent in 5.36Seconds 685.70Kbytes/sec.
ftp> quit
221 Quit command received. Goodbye.

C:\isoft_omvs>
```

Step 2 - Extract the Product From the tar File

Once you have copied the tar file to the OS/390 system, you must access UNIX System Services to extract the Commerce Suite product from the tar file. Extracting the tar file creates the Commerce Suite directory and installs all of the product files and directories.

Perform the following steps to extract the Commerce Suite product from the tar file:

1. Enter `OMVS` on the TSO command line to invoke UNIX System Services in terminal mode. This invokes a standard UNIX-like environment.
2. Enter `cd /` to change directories to the HFS root or to the directory where you placed the distribution tar file.
3. Enter `ls -l os390*` to search the current directory for the installation tar file that was previous transferred. If it is not listed, then either the transfer failed or the file was stored in a directory other than the HFS root directory.

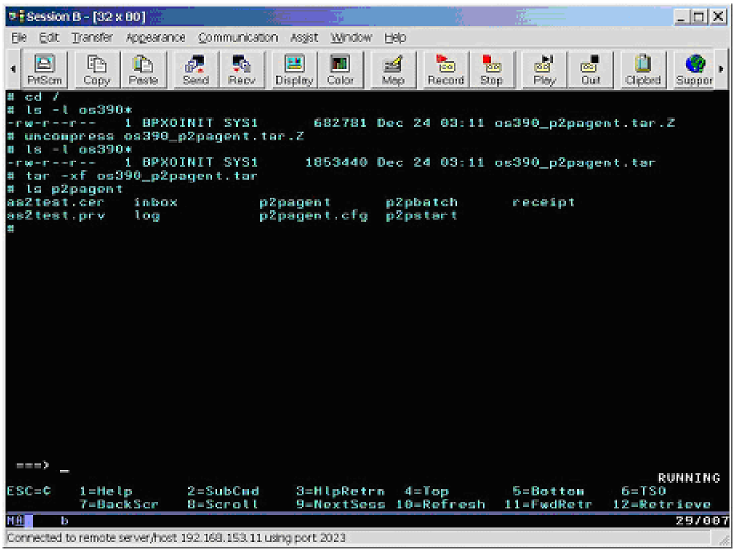
4. Enter `uncompress os390_p2pagent.tar.Z` to uncompress the tar file so that it can be extracted. Any file with a .Z suffix is standard UNIX notation for a compressed file. If this command fails, it is most likely because the file was not transferred in binary mode, you do not have permission to write to the directory where the tar file is located, or the OS/390 HFS file system is full.

5. Enter `ls -l os390*` to search the current directory for the installation tar file. It should now be larger and not have the .Z suffix.

6. Enter `tar -xf os390_p2pagent.tar` to extract the installation tar file and all the programs, files, and subdirectories will be stored in the Commerce Suite directory.

7. Enter `ls p2pagent` to list the `p2pagent` directory and it's contents.

Figure D-5 Extracting the tar File



Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
# cd /
# ls -l os390*
-rw-r--r--    1 BPXOINIT SYS1       682781 Dec 24 03:11 os390_p2pagent.tar.Z
# uncompress os390_p2pagent.tar.Z
# ls -l os390*
-rw-r--r--    1 BPXOINIT SYS1      1853440 Dec 24 03:11 os390_p2pagent.tar
# tar -xf os390_p2pagent.tar
# ls p2pagent
as2test.cer    inbox          p2pagent       p2pbatch       receipt
as2test.prv    log            p2pagent.cfg   p2pstart
#

 ===> _
                                                                    RUNNING
ESC=¢     1=Help       2=SubCmd      3=HlpRetrn   4=Top        5=Bottom     6=TSO
          7=BackScr    8=Scroll      9=NextSess  10=Refresh   11=FwdRetr   12=Retrieve
MA    b                                                                    29/007
Connected to remote server/host 192.168.153.11 using port 2023
```

The following list contains all of the files and directories contained in the installation tar file:

- `p2pagent/`
- `p2pagent/p2pagent`

- `p2pagent/p2pagent.cfg`
- `p2pagent/p2pstart`
- `p2pagent/p2pbatch`
- `p2pagent/inbox/`
- `p2pagent/receipt/`
- `p2pagent/log/`
- `p2pagent/as2test.cer`
- `p2pagent/as2test.prv`

Step 3 - Editing the Commerce Suite p2pbatch Procedure

If you installed the Commerce Suite application in a directory other than `/p2pagent`, you must change the `p2pbatch` procedure to reflect the directory you have chosen. You must also tailor the job information to meet your installations requirements.

This can be accomplished by editing the procedure using `OEDIT` from within UNIX System Services.

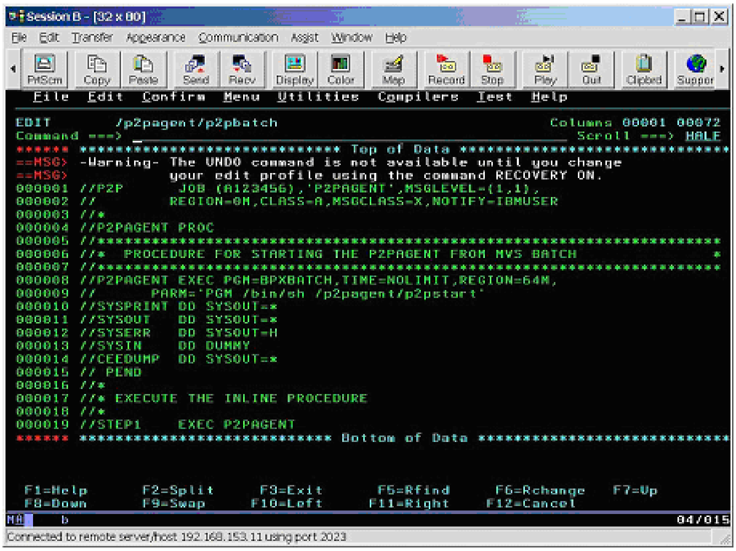
Updating the p2pstart Procedure on the OS/390

Perform the following steps to update the `p2pstart` script on the OS/390:

1. Enter `OEDIT /p2pagent/p2pbatch` from within UNIX System Services.
2. Change the directory in the `PARM= from /p2pagent` to the directory where the Commerce Suite product was installed.

The following screen shot provides an example of the `OEDIT` command with the `p2pbatch` procedure.

Figure D-6 OEDIT Command Within the p2pbatch Procedure



Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
   File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help

EDIT       /p2pagent/p2pbatch                          Columns 00001 00072
Command ===> ________________________________________________ Scroll ===> HALF
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 //P2P      JOB (A123456),'P2PAGENT',MSGLEVEL=(1,1),
000002 //        REGION=0M,CLASS=A,MSGCLASS=X,NOTIFY=IBMUSER
000003 //*
000004 //P2PAGENT PROC
000005 //*********************************************************************
000006 //*  PROCEDURE FOR STARTING THE P2PAGENT FROM MVS BATCH                *
000007 //*********************************************************************
000008 //P2PAGENT EXEC PGM=BPXBATCH,TIME=NOLIMIT,REGION=64M,
000009 //       PARM='PGM /bin/sh /p2pagent/p2pstart'
000010 //SYSPRINT DD SYSOUT=*
000011 //SYSOUT   DD SYSOUT=*
000012 //SYSERR   DD SYSOUT=H
000013 //SYSIN    DD DUMMY
000014 //CEEDUMP  DD SYSOUT=*
000015 // PEND
000016 //*
000017 //* EXECUTE THE INLINE PROCEDURE
000018 //*
000019 //STEP1    EXEC P2PAGENT
****** **************************** Bottom of Data ****************************


  F1=Help      F2=Split     F3=Exit      F5=Rfind     F6=Rchange   F7=Up
  F8=Down      F9=Swap     F10=Left     F11=Right    F12=Cancel
MA     b                                                                04/015
Connected to remote server/host 192.168.153.11 using port 2023
```

Step 4 - Editing the Commerce Suite p2pstart script

If you installed the Commerce Suite in a directory other than `/p2pagent`, you must change the `p2pbatch` procedure to reflect the directory you have chosen.

This can be accomplished editing the procedure using `OEDIT` from within UNIX System Services.

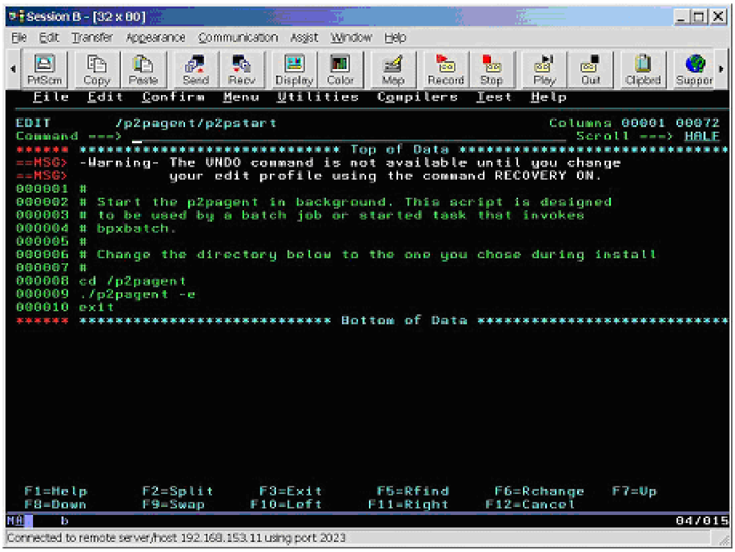
Updating the p2pstart Procedure on the OS/390

Perform the following steps to update the `p2pstart` script on the OS/390:

1. Enter `OEDIT /p2pagent/p2pstart` from within UNIX System Services.
2. Change the directory in the `cd` command from `/p2pagent` to the directory where the Commerce Suite product was installed.

The following screen shot provides an example of the `OEDIT` command with the `p2pstart` script.

Figure D-7 OEDIT Command Within the p2pstart Script


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
  File   Edit   Confirm   Menu   Utilities   Compilers   Test   Help

EDIT       /p2pagent/p2pstart                            Columns 00001 00072
Command ===> _____________________________________________  Scroll ===> HALF
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 #
000002 # Start the p2pagent in background. This script is designed
000003 # to be used by a batch job or started task that invokes
000004 # bpxbatch.
000005 #
000006 # Change the directory below to the one you chose during install
000007 #
000008 cd /p2pagent
000009 ./p2pagent -e
000010 exit
****** **************************** Bottom of Data ****************************




 F1=Help      F2=Split     F3=Exit      F5=Rfind     F6=Rchange   F7=Up
 F8=Down      F9=Swap     F10=Left     F11=Right    F12=Cancel
MA      b                                                                04/015
```

Connected to remote server/host 192.168.153.11 using port 2023

Step 4 - Entering the Commerce Suite Runtime License

This step configures the Commerce Suite runtime product license. The Commerce Suite product, as shipped, operates in Demonstration mode. When the product is purchased, you are supplied license keys to convert the product to Authorized Installation mode.

If you plan on running the product in Demonstration mode, you can skip this step.

Note: In Demonstration mode, Commerce Suite will not transfer payloads to a trading partner located on another host computer.

If you are configuring the product for Authorized Installation mode, you must have completed the following:

- TCP/IP Configuration must be complete. Refer to the *System Requirements* section of this chapter for instructions.
- You must have obtained a valid serial number for Commerce Suite from iSoft Technical Support.
- You must have obtained a valid authentication code for Commerce Suite from iSoft Technical Support.
- If TCP/IP configuration is not complete or is changed after the license information is entered into the product, you must contact iSoft Technical Support to obtain new licensing information.

Some of the following license installation steps require a Windows or UNIX system.

Perform the following steps to generate your Commerce Suite license key file:

1. Using either Notepad (Windows OS) or vi (UNIX), create a file named license.txt.
2. Enter the serial number supplied to you by iSoft Technical Support. The serial number entry should look similar to the following example:

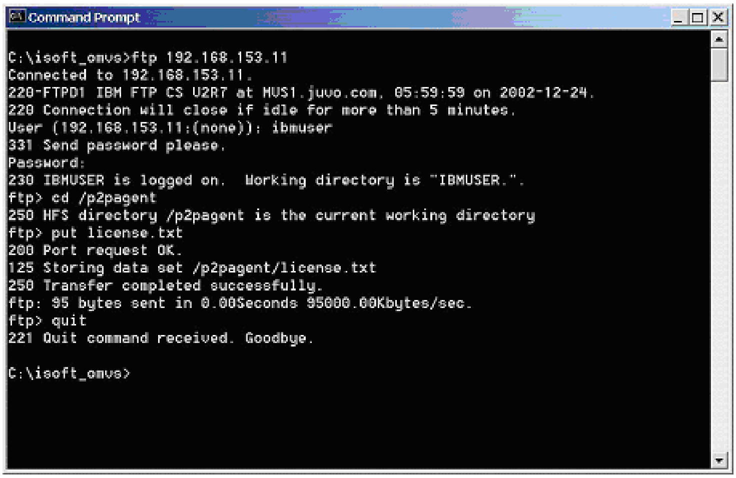
   ```
   serial-number:3462BFA-BF98DD3A-30AD55A4-1F66DF4B-220211C3-00987
   FCA-ED0BAB24-24F8BC14-013DC216
   ```

   Note: Be sure to press enter at the end of the serial-number line if you created the file with a cut and paste. This will add a carriage return/line feed to the end of the line.

3. Save the `license.txt` file. Once the file is saved, you must transfer the file to the OS/390 system using the FTP Client.
4. On the taskbar, click **Start**, then click **Programs**, then click **Accessories**, then click **Command Prompt**. The Command Prompt opens.
5. From the `c:\isoft_os390` directory, or the directory where you saved the `license.txt` file, enter `ftp` and the OS/390 TCP/IP address.

6. Enter your user ID and press Enter.
7. Enter your password and press Enter.
8. Enter `cd /p2pagent` to change directories to `/p2pagent` or specify the directory where the Commerce Suite was installed. The file must be transferred in ASCII (Text) mode.
9. Enter `put license.txt` to transfer the `license.txt` file to the directory you installed Commerce Suite into, which by default is `/p2pagent`. Once the file is transferred, you must access UNIX System Services on the OS/390.

Figure D-8 Transfer License.txt

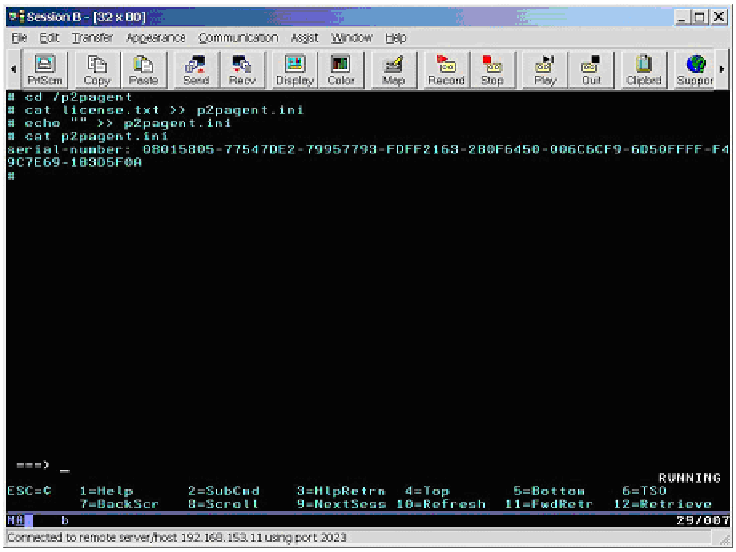


```
C:\isoft_omvs>ftp 192.168.153.11
Connected to 192.168.153.11.
220-FTPD1 IBM FTP CS V2R7 at MVS1.juvo.com, 05:59:59 on 2002-12-24.
220 Connection will close if idle for more than 5 minutes.
User (192.168.153.11:(none)): ibmuser
331 Send password please.
Password:
230 IBMUSER is logged on.  Working directory is "IBMUSER.".
ftp> cd /p2pagent
250 HFS directory /p2pagent is the current working directory
ftp> put license.txt
200 Port request OK.
125 Storing data set /p2pagent/license.txt
250 Transfer completed successfully.
ftp: 95 bytes sent in 0.00Seconds 95000.00Kbytes/sec.
ftp> quit
221 Quit command received. Goodbye.

C:\isoft_omvs>
```

10. Enter `OMVS` on the TSO command line to invoke UNIX System Services in terminal mode. This invokes a standard UNIX-like environment.
11. Enter `cd /p2pagent` to change directories to `/p2pagent` or specify the directory where the Commerce Suite was installed
12. Enter `cat license.txt >> p2pagent.ini` to append the `license.txt` file to the `p2pagent.ini` file. If the `p2pagent.ini` file does not exist, it is created with the contents of the `license.txt` file.
13. Enter `echo "" >> p2pagent.ini` to append a carriage return/line feed to the end of the serial number.

14. Enter `cat p2pagent.ini` to display the contents of the `p2pagent.ini` file for verification

Figure D-9   Update p2pagent.ini File with license.tct File


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
# cd /p2pagent
# cat license.txt >> p2pagent.ini
# echo "" >> p2pagent.ini
# cat p2pagent.ini
serial-number: 08015805-77547DE2-79957793-FDFF2163-280F6450-006C6CF9-6D50FFFF-F4
9C7E69-183D5F0A
#



 ===> _
                                                                        RUNNING
ESC=¢    1=Help       2=SubCmd     3=HlpRetrn  4=Top       5=Bottom     6=TSO
         7=BackScr    8=Scroll     9=NextSess 10=Refresh  11=FwdRetr   12=Retrieve
MA     b                                                                 29/007
```

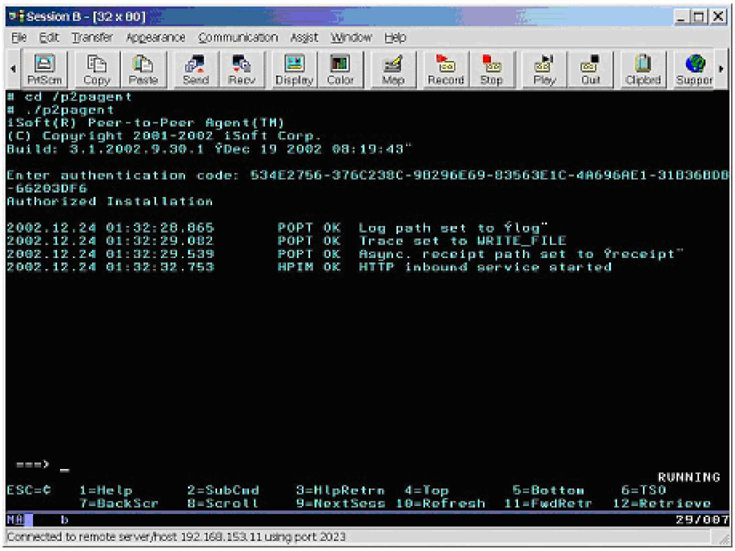
Connected to remote server/host 192.168.153.11 using port 2023

15. Enter `./p2pagent` from the UNIX System Services terminal shell to start Commerce Suite. The `./p2pagent` command starts the Commerce Suite using the program in the current directory. When Commerce Suite is started for the first time, it will prompt you for the authentication code that was supplied to you by iSoft Technical Support. The authentication code should look similar to the following example.

    ```
    DD8187D8-45372208-F4EC9A91-ED903D5B-3314EA26-7D125C75-00F24C66
    ```

16. Enter the authentication code on the command line and press Enter. The following figure provides a screen shot of the process and the response from Commerce Suite if both the serial number and the authentication code are valid.

Figure D-10 Product Runtime License


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
# cd /p2pagent
# ./p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.9.30.1 ŸDec 19 2002 08:19:43"

Enter authentication code: 534E2756-376C238C-9B296E69-83563E1C-4A696AE1-31B36BDB
-66203DF6
Authorized Installation

2002.12.24 01:32:28.865       POPT OK  Log path set to Ÿlog"
2002.12.24 01:32:29.082       POPT OK  Trace set to WRITE_FILE
2002.12.24 01:32:29.539       POPT OK  Async. receipt path set to Ÿreceipt"
2002.12.24 01:32:32.753       HPIM OK  HTTP inbound service started





 ===> _
                                                                        RUNNING
ESC=¢    1=Help       2=SubCmd      3=HlpRetrn  4=Top        5=Bottom     6=TSO
         7=BackScr    8=Scroll      9=NextSess 10=Refresh   11=FwdRetr   12=Retrieve
MA     b                                                                 29/007
```

Connected to remote server/host 192.168.153.11 using port 2023

Using Commerce Suite with OS/390

The information contained in this section is limited to the features that are unique to the OS/390. The following topics are discussed:

- Working with the `p2pagent.cfg` File
- Starting Commerce Suite as a Batch Job
- Verifying Commerce Suite is Running
- Stopping Commerce Suite as a Batch Job
- Running Commerce Suite in Interactive Mode
- Working With Commerce Suite Payload Files
- Commerce Suite Performance

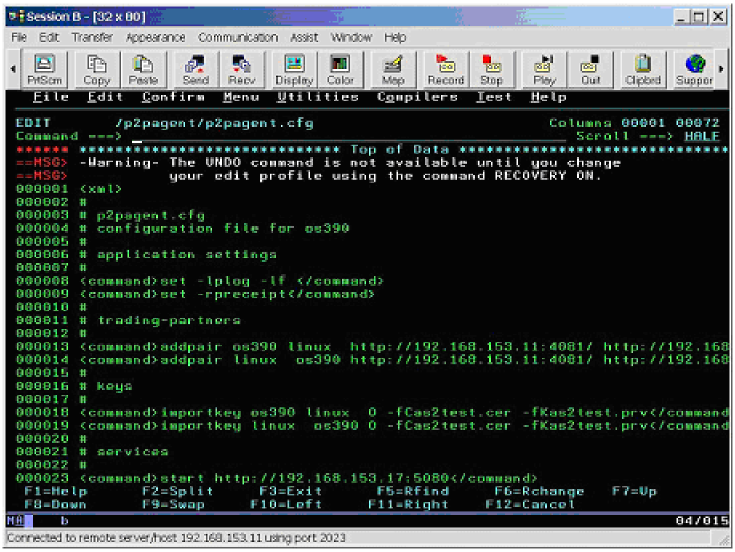
Working with the p2pagent.cfg File

The Commerce Suite configuration file (`p2pagent.cfg`) is located in the `/p2pagent` installation directory, or whatever directory you used for installation. This file contains all the default startup parameters that are used when you start the Commerce Suite program in either batch mode or interactive mode.

Note: It is recommended that either Notepad under Microsoft Windows, or vi under UNIX, is used to edit the file as lines are longer then regular green screen modes and require working with left and right movement if using `OEDIT` in a 3270 terminal session.

The following figure shows an open configuration file in the open edition editor (OEDIT).

Figure D-11 Sample p2pagent.cfg in OEDIT



Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
   File   Edit   Confirm   Menu   Utilities   Compilers   Test   Help

EDIT        /p2pagent/p2pagent.cfg                       Columns 00001 00072
Command ===>                                                Scroll ===> HALF
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 <xml>
000002 #
000003 # p2pagent.cfg
000004 # configuration file for os390
000005 #
000006 # application settings
000007 #
000008 <command>set -lplog -lf </command>
000009 <command>set -rpreceipt</command>
000010 #
000011 # trading-partners
000012 #
000013 <command>addpair os390 linux  http://192.168.153.11:4081/ http://192.168
000014 <command>addpair linux  os390 http://192.168.153.11:4081/ http://192.168
000015 #
000016 # keys
000017 #
000018 <command>importkey os390 linux  0 -fCas2test.cer -fKas2test.prv</command
000019 <command>importkey linux  os390 0 -fCas2test.cer -fKas2test.prv</command
000020 #
000021 # services
000022 #
000023 <command>start http://192.168.153.17:5080</command>
 F1=Help      F2=Split     F3=Exit      F5=Rfind     F6=Rchange   F7=Up
 F8=Down      F9=Swap     F10=Left     F11=Right    F12=Cancel
MA      b                                                              04/015
Connected to remote server/host 192.168.153.11 using port 2023
```

Starting Commerce Suite as a Batch Job

Starting Commerce Suite as a batch job is accomplished in the following two ways:

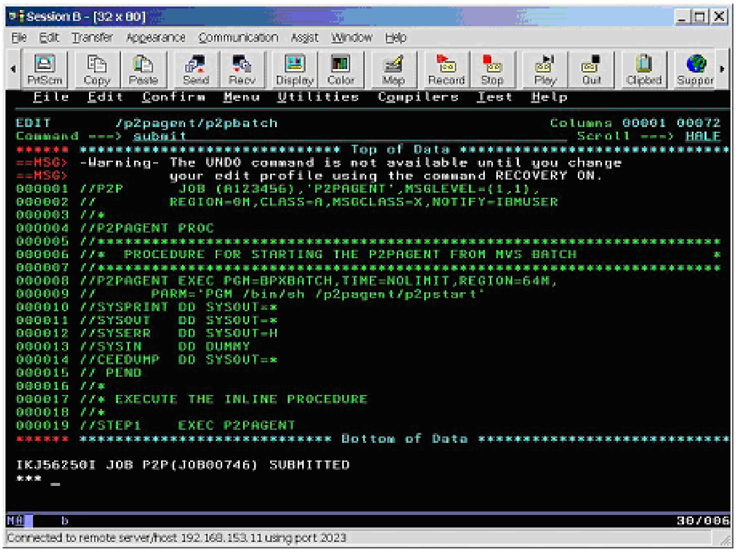
- Submitting the `p2pstart` batch job
- Invoking UNIX System Services in Terminal Mode

Submitting the p2pbatch job

Perform the following steps to submit the Commerce Suite as a batch job:

1. Enter `OEDIT /p2pagent/p2pbatch` from within UNIX System Services.
2. Enter `submit` to submit the job.

Figure D-12 Submitting the Commerce Suite as a Batch Job


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor
File Edit Confirm Menu Utilities Compilers Test Help

```
EDIT       /p2pagent/p2pbatch                               Columns 00001 00072
Command ===> submit                                            Scroll ===> HALF
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 //P2P      JOB (A123456),'P2PAGENT',MSGLEVEL=(1,1),
000002 //            REGION=0M,CLASS=A,MSGCLASS=X,NOTIFY=IBMUSER
000003 //*
000004 //P2PAGENT PROC
000005 //**********************************************************************
000006 //*  PROCEDURE FOR STARTING THE P2PAGENT FROM MVS BATCH                 *
000007 //**********************************************************************
000008 //P2PAGENT EXEC PGM=BPXBATCH,TIME=NOLIMIT,REGION=64M,
000009 //        PARM='PGM /bin/sh /p2pagent/p2pstart'
000010 //SYSPRINT DD SYSOUT=*
000011 //SYSOUT   DD SYSOUT=*
000012 //SYSERR   DD SYSOUT=H
000013 //SYSIN    DD DUMMY
000014 //CEEDUMP  DD SYSOUT=*
000015 // PEND
000016 //*
000017 //* EXECUTE THE INLINE PROCEDURE
000018 //*
000019 //STEP1    EXEC P2PAGENT
****** **************************** Bottom of Data ****************************

IKJ56250I JOB P2P(JOB00746) SUBMITTED
*** _

MA     b                                                                 30/006
```

Connected to remote server/host 192.168.153.11 using port 2023

Running `BPXBATCH` invokes the UNIX System Services environment without a terminal session. The `PARM=` statement specifies the command stream to execute. PGM specifies to execute the `/bin/sh` (The UNIX Shell) command. The other parameters are the commands and options for `/bin/sh` to execute.

These parameters are the directory that Commerce Suite was installed into (`/p2pagent`) and the program to execute (`p2pstart`). The `p2pstart` program is a shell script that invokes the Commerce Suite as a daemon (`-e` command line switch) to run in the background and sets the current directory with a UNIX `cd` (change directory) command.

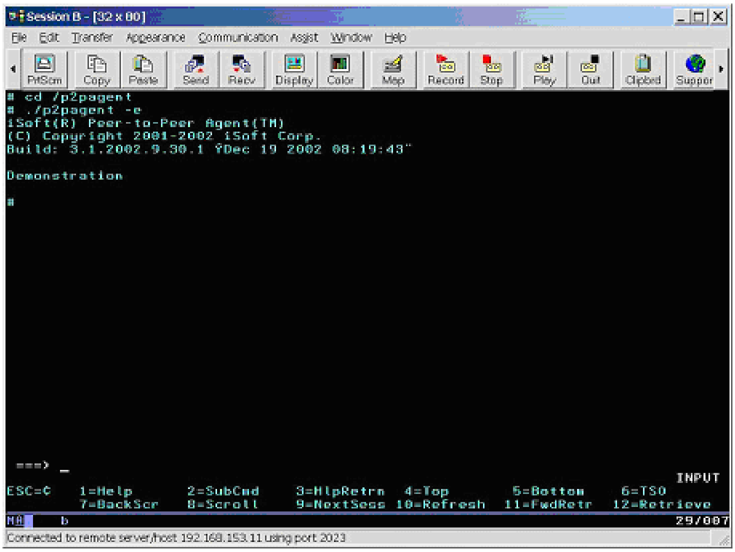
When the batch job is submitted it will end leaving the Commerce Suite process running in Background under the UNIX System Services environment as it's own batch job. You can see the new job from either a display of active jobs from the MVS operations console or from within UNIX System Services.

Invoking UNIX System Services in Terminal Mode

Perform the following steps to start Commerce Suite as a batch job from within a UNIX System Services terminal session.

1. Enter `OMVS` on the TSO command line to invoke UNIX System Services in terminal mode. This invokes a standard UNIX-like environment.

Figure D-13 Starting p2pagent From UNIX System Services


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
# cd /p2pagent
# ./p2pagent -e
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.9.30.1 ?Dec 19 2002 08:19:43"

Demonstration

#




 ===> _
                                                                     INPUT
ESC=¢     1=Help        2=SubCmd      3=HlpRetrn   4=Top        5=Bottom     6=TSO
          7=BackScr     8=Scroll      9=NextSess  10=Refresh   11=FwdRetr   12=Retrieve
MA     b                                                                  29/007
Connected to remote server/host 192.168.153.11 using port 2023
```

2. Enter `cd /p2pagent` to change the current directory to `/p2pagent`. If you installed the Commerce Suite in another directory, you must specify that directory.

3. Enter `./p2pagent -e` to start the Commerce Suite using the program in the current directory. The `-e` option tells the Commerce Suite to disconnect itself from the terminal session and run as a daemon (run in the background as a batch job).

Verifying Commerce Suite is Running

Verifying that Commerce Suite is running is accomplished using any of the following methods:

- View a list of active jobs
- View active processes within UNIX System Services
- Invoke UNIX System Services in terminal mode

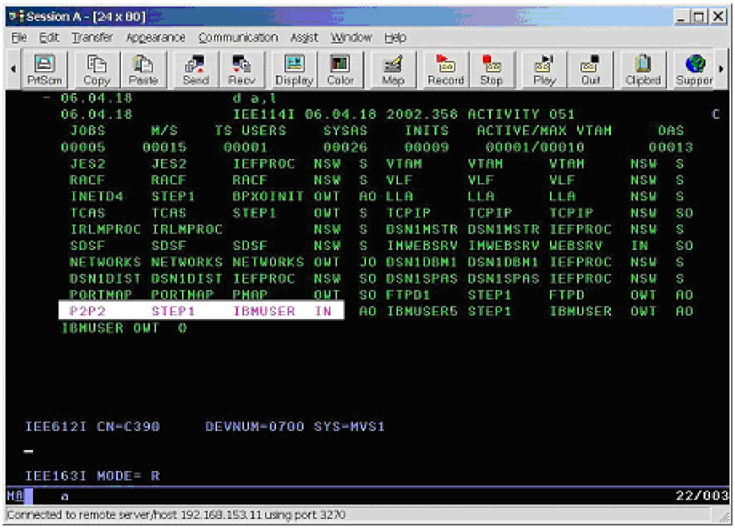
Note: The recommended method for viewing the `p2pagent` process is from within UNIX System Services in terminal mode.

Viewing a List of Active jobs

In the following example, job P2P2 is the new job that is running the Commerce Suite under UNIX System Services.

Note: This method is only effective if the original name of the submitting Batch job is known.

Figure D-14 Display Active Jobs


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
 - 06.04.18          d a,l
   06.04.18          IEE114I 06.04.18 2002.358 ACTIVITY 051                C
    JOBS     M/S     TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM    OAS
   00005    00015    00001      00026    00009    00001/00010       00013
    JES2     JES2     IEFPROC  NSW  S  VTAM     VTAM     VTAM     NSW  S
    RACF     RACF     RACF     NSW  S  VLF      VLF      VLF      NSW  S
    INETD4   STEP1    BPXOINIT OWT  AO LLA      LLA      LLA      NSW  S
    TCAS     TCAS     STEP1    OWT  S  TCPIP    TCPIP    TCPIP    NSW  SO
    IRLMPROC IRLMPROC          NSW  S  DSN1MSTR DSN1MSTR IEFPROC  NSW  S
    SDSF     SDSF     SDSF     NSW  S  IMWEBSRV IMWEBSRV WEBSRV   IN   SO
    NETWORKS NETWORKS NETWORKS OWT  JO DSN1DBM1 DSN1DBM1 IEFPROC  NSW  S
    DSN1DIST DSN1DIST IEFPROC  NSW  SO DSN1SPAS DSN1SPAS IEFPROC  NSW  S
    PORTMAP  PORTMAP  PMAP     OWT  SO FTPD1    STEP1    FTPD     OWT  AO
    P2P2     STEP1    IBMUSER  IN   AO IBMUSER5 STEP1    IBMUSER  OWT  AO
   IBMUSER OWT  0



 IEE612I CN=C390     DEVNUM=0700 SYS=MVS1

 -

 IEE163I MODE= R
MA      a                                                          22/003
```

Connected to remote server/host 192.168.153.11 using port 3270

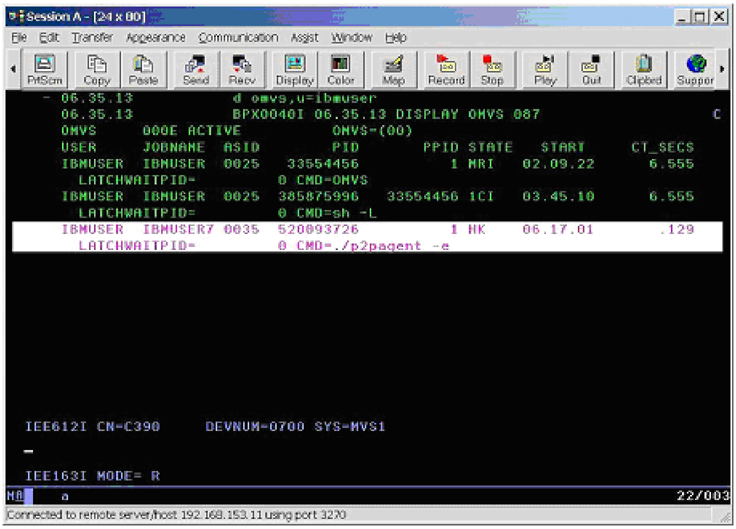
In Figure D-2, the name of the batch job being submitted was P2P. MVS will append a Unique identifier to the jobname when it starts the job to run the `p2pagent` process. In this Example a numeral "2" was added to the jobname.

Viewing Active Processes Within UNIX System Services

The `display omvs` command can be used to view active processes within UNIX System Services. Please see the IBM publication *MVS Systems Commands* for a complete list of the options available for `display omvs`.

The following example shows display `omvs` using the user ID option that displays all active processes running under the selected user ID.

Figure D-15 Display omvs Command



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
 - 06.35.13           d omvs,u=ibmuser
   06.35.13           BPXO040I 06.35.13 DISPLAY OMVS 087                    C
   OMVS      000E ACTIVE           OMVS=(00)
   USER      JOBNAME  ASID          PID       PPID STATE   START     CT_SECS
   IBMUSER   IBMUSER  0025    33554456           1 MRI    02.09.22     6.555
     LATCHWAITPID=           0 CMD=OMVS
   IBMUSER   IBMUSER  0025   385875996    33554456 1CI    03.45.10     6.555
     LATCHWAITPID=           0 CMD=sh -L
   IBMUSER   IBMUSER7 0035   520093726           1 HK     06.17.01      .129
     LATCHWAITPID=           0 CMD=./p2pagent -e

 IEE612I CN=C390      DEVNUM=0700 SYS=MVS1

 -

 IEE163I MODE= R
MA    a                                                                 22/003
```

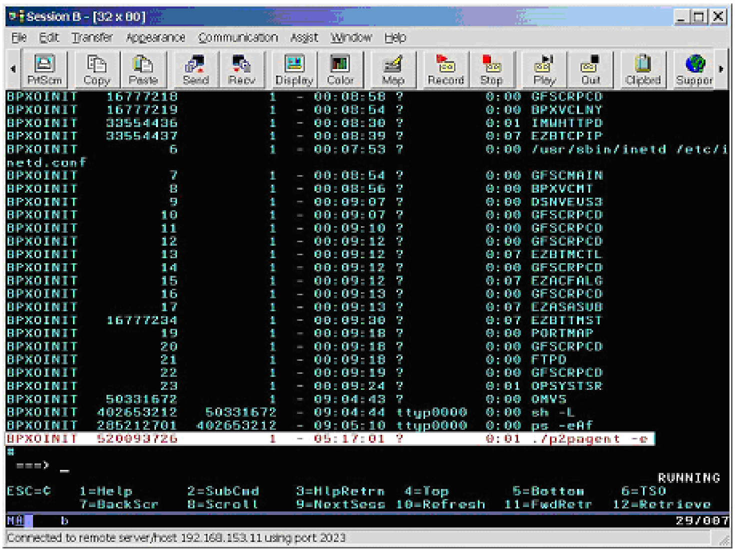
Connected to remote server/host 192.168.153.11 using port 3270

Invoking UNIX System Services in Terminal Mode

Perform the following steps to verify Commerce Suite is running:

1. Enter `OMVS` on the TSO command line to invoke UNIX System Services in terminal mode. This invokes a standard UNIX-like environment.
2. Enter `ps -eAf` to display all running processes within the PASE.
3. Scroll through the listed active processes and select the `p2pAgent` entry. If the entry is not found, then the Commerce Suite is not running.

Figure D-16 Display Active Processes Within UNIX System Services


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
BPXOINIT   16777218          1 - 00:08:58 ?         0:00 GFSCRPCD
BPXOINIT   16777219          1 - 00:08:54 ?         0:00 BPXVCLNY
BPXOINIT   33554436          1 - 00:08:30 ?         0:01 IMWHTTPD
BPXOINIT   33554437          1 - 00:08:39 ?         0:07 EZBTCPIP
BPXOINIT          6          1 - 00:07:53 ?         0:00 /usr/sbin/inetd /etc/i
netd.conf
BPXOINIT          7          1 - 00:08:54 ?         0:00 GFSCMAIN
BPXOINIT          8          1 - 00:08:56 ?         0:00 BPXVCMT
BPXOINIT          9          1 - 00:09:07 ?         0:00 DSNVEUS3
BPXOINIT         10          1 - 00:09:07 ?         0:00 GFSCRPCD
BPXOINIT         11          1 - 00:09:10 ?         0:00 GFSCRPCD
BPXOINIT         12          1 - 00:09:12 ?         0:00 GFSCRPCD
BPXOINIT         13          1 - 00:09:12 ?         0:07 EZBTMCTL
BPXOINIT         14          1 - 00:09:12 ?         0:00 GFSCRPCD
BPXOINIT         15          1 - 00:09:12 ?         0:07 EZACFALG
BPXOINIT         16          1 - 00:09:13 ?         0:00 GFSCRPCD
BPXOINIT         17          1 - 00:09:13 ?         0:07 EZASASUB
BPXOINIT   16777234          1 - 00:09:30 ?         0:07 EZBTTMST
BPXOINIT         19          1 - 00:09:18 ?         0:00 PORTMAP
BPXOINIT         20          1 - 00:09:18 ?         0:00 GFSCRPCD
BPXOINIT         21          1 - 00:09:18 ?         0:00 FTPD
BPXOINIT         22          1 - 00:09:19 ?         0:00 GFSCRPCD
BPXOINIT         23          1 - 00:09:24 ?         0:01 OPSYSTSR
BPXOINIT   50331672          1 - 09:04:43 ?         0:00 OMVS
BPXOINIT  402653212   50331672 - 09:04:44 ttyp0000  0:00 sh -L
BPXOINIT  285212701  402653212 - 09:05:10 ttyp0000  0:00 ps -eAf
BPXOINIT  520093726          1 - 05:17:01 ?         0:01 ./p2pagent -e
#
 ===> _
                                                                        RUNNING
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
MA    b                                                                   29/007
```

Connected to remote server/host 192.168.153.11 using port 2023

The p2pAgent entry appears on the boxed line of the active screen.

Stopping Commerce Suite as a Batch Job

Stopping Commerce Suite as a batch job is accomplished in the following two ways:

- From the OS/390 operations console or
- From UNIX System Services in Terminal Mode

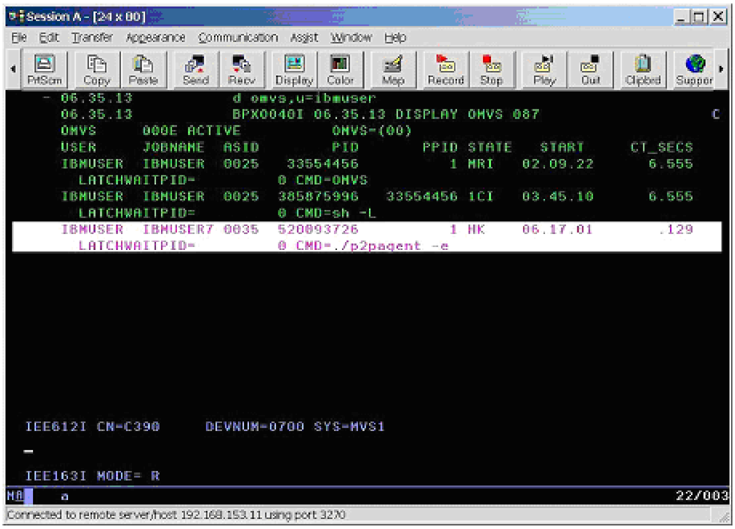
From the OS/390 Operations Console Mode

Perform the following steps to stop Commerce Suite in batch mode using the OS/390 operations console:

If The name of the batch job is known, then proceed to step 2. If not the process will have to be located. This is done with the `display omvs` command.

1. The `display omvs` command can be used to view active processes within UNIX System Services. Please see the IBM publication *MVS Systems Commands* for a complete list of the options available for `display omvs`.

Figure D-17 Display omvs Command



Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
   - 06.35.13            d omvs,u=ibmuser
     06.35.13            BPXO040I 06.35.13 DISPLAY OMVS 087                 C
     OMVS      000E ACTIVE           OMVS=(00)
     USER      JOBNAME  ASID         PID        PPID STATE   START     CT_SECS
     IBMUSER   IBMUSER  0025    33554456           1 MRI    02.09.22     6.555
       LATCHWAITPID=          0 CMD=OMVS
     IBMUSER   IBMUSER  0025   385875996    33554456 1CI    03.45.10     6.555
       LATCHWAITPID=          0 CMD=sh -L
     IBMUSER   IBMUSER7 0035   520093726           1 HK     06.17.01      .129
       LATCHWAITPID=          0 CMD=./p2pagent -e





 IEE612I CN=C390      DEVNUM=0700 SYS=MVS1

 -

 IEE163I MODE= R
MA     a                                                                  22/003
```

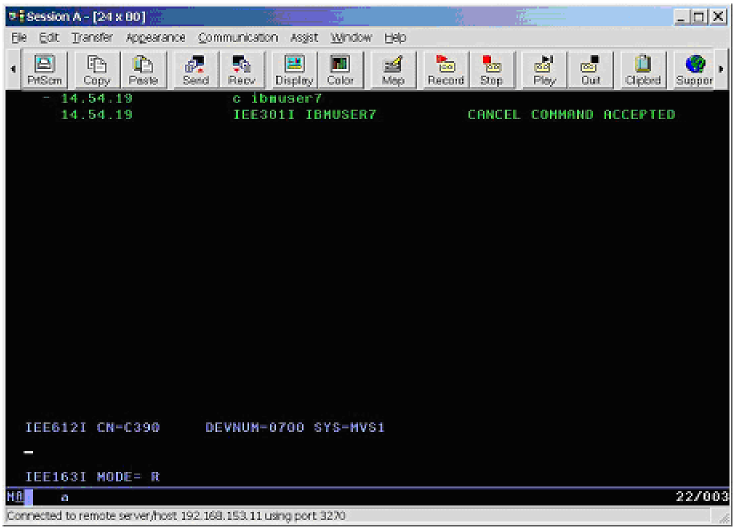
Connected to remote server/host 192.168.153.11 using port 3270

In the above example, the user ID that started the `p2pagent` process is known, so all the processes currently running that were started by the ibmuser user ID are listed.

From this list, the jobname `ibmuser7` is listed as the MVS jobname for the `p2pagent` process. This jobname can then be used in a standard MVS cancel command.

2. Issue a standard `cancel` *`jobname`* MVS console command to terminate the `p2pagent` process.

Figure D-18 Cancel jobname command


Session A - [24 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
  - 14.54.19            c ibmuser7
    14.54.19            IEE301I IBMUSER7          CANCEL COMMAND ACCEPTED


 IEE612I CN-C390      DEVNUM-0700 SYS-MVS1

 -
 IEE163I MODE= R
MA     a                                                              22/003
```

Connected to remote server/host 192.168.153.11 using port 3270

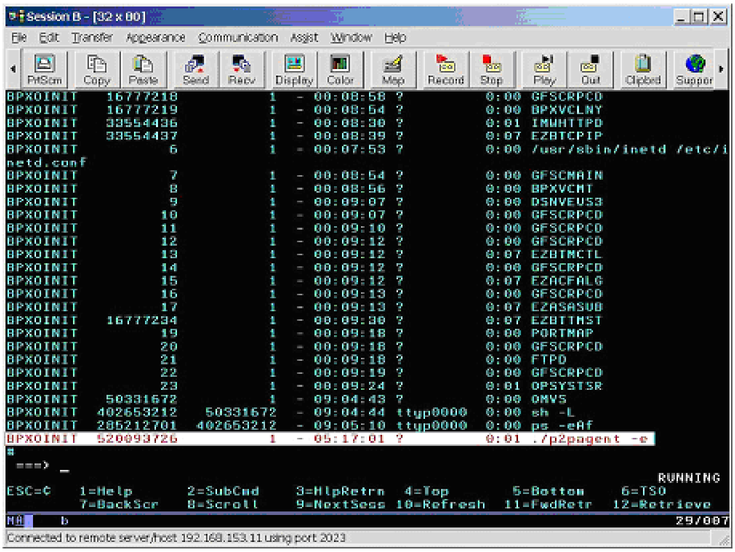
Note: If the system is busy, it might take a minute or so for the process to end.

From UNIX System Services in Terminal Mode

Perform the following steps to stop Commerce Suite by invoking PASE in terminal mode:

1. Enter `OMVS` on the TSO command line to invoke UNIX System Services in terminal mode. This invokes a standard UNIX-like environment.
2. Enter `ps -eAf` to display all running processes within the PASE.
3. Scroll through the listed active processes and select the Commerce Suite entry. If the entry is not found, then Commerce Suite is not running.

Figure D-19 Stopping p2pAgent From UNIX System Services


Session B - [32 x 80]
File Edit Transfer Appearance Communication Assist Window Help
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Clipbrd Suppor

```
BPXOINIT   16777218          1  - 00:08:58 ?         0:00 GFSCRPCD
BPXOINIT   16777219          1  - 00:08:54 ?         0:00 BPXVCLNY
BPXOINIT   33554436          1  - 00:08:30 ?         0:01 IMWHTTPD
BPXOINIT   33554437          1  - 00:08:39 ?         0:07 EZBTCPIP
BPXOINIT          6          1  - 00:07:53 ?         0:00 /usr/sbin/inetd /etc/i
netd.conf
BPXOINIT          7          1  - 00:08:54 ?         0:00 GFSCMAIN
BPXOINIT          8          1  - 00:08:56 ?         0:00 BPXVCMT
BPXOINIT          9          1  - 00:09:07 ?         0:00 DSNVEUS3
BPXOINIT         10          1  - 00:09:07 ?         0:00 GFSCRPCD
BPXOINIT         11          1  - 00:09:10 ?         0:00 GFSCRPCD
BPXOINIT         12          1  - 00:09:12 ?         0:00 GFSCRPCD
BPXOINIT         13          1  - 00:09:12 ?         0:07 EZBTMCTL
BPXOINIT         14          1  - 00:09:12 ?         0:00 GFSCRPCD
BPXOINIT         15          1  - 00:09:12 ?         0:07 EZACFALG
BPXOINIT         16          1  - 00:09:13 ?         0:00 GFSCRPCD
BPXOINIT         17          1  - 00:09:13 ?         0:07 EZASASUB
BPXOINIT   16777234          1  - 00:09:30 ?         0:07 EZBTTMST
BPXOINIT         19          1  - 00:09:18 ?         0:00 PORTMAP
BPXOINIT         20          1  - 00:09:18 ?         0:00 GFSCRPCD
BPXOINIT         21          1  - 00:09:18 ?         0:00 FTPD
BPXOINIT         22          1  - 00:09:19 ?         0:00 GFSCRPCD
BPXOINIT         23          1  - 00:09:24 ?         0:01 OPSYSTSR
BPXOINIT   50331672          1  - 09:04:43 ?         0:00 OMVS
BPXOINIT  402653212   50331672  - 09:04:44 ttyp0000  0:00 sh -L
BPXOINIT  285212701  402653212  - 09:05:10 ttyp0000  0:00 ps -eAf
BPXOINIT  520093726          1  - 05:17:01 ?         0:01 ./p2pagent -e
#
 ===> _
                                                                         RUNNING
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
MA    b                                                                   29/007
```

Connected to remote server/host 192.168.153.11 using port 2023

The `p2pAgent` entry appears on the boxed line of the active screen.

4. Make note of the `p2pAgent` process ID number (PID). It is located under the PID heading on the same entry line as the process name (`./p2pagent -e`).

5. Enter `kill #` where the `#` is the PID for the `p2pAgent` process. In the figure above, the command would look like the following:

   ```
   kill 520093726
   ```

6. Enter `ps -eAf` to ensure the process is gone.

Note: If the system is busy, it might take a minute for the process to end. The process will also finish any work that is currently being performed before stopping the application.

Running Commerce Suite in Interactive Mode

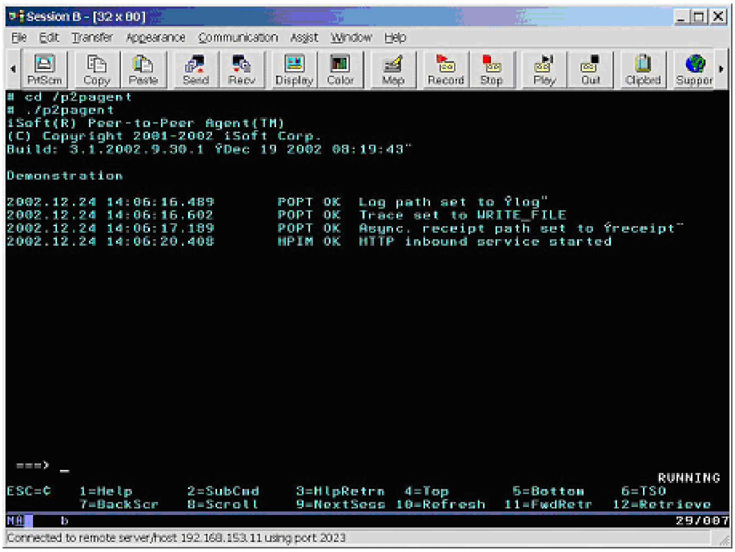
Commerce Suite can be run in either batch mode or in single user interactive mode. In order to run Commerce Suite in batch and interactive mode at the same time, Commerce Suite must be installed in separate directories as both

instances would try and share the same `p2pagent.cfg` file if started from the same directory. To run Commerce Suite in interactive mode, the UNIX System Services shell must be running in terminal mode.

Perform the following steps to run Commerce Suite in interactive mode:

1. Enter `OMVS` on the TSO command line to invoke UNIX System Services in terminal mode. This invokes a standard UNIX-like environment.
2. Enter `cd /p2pagent` to change the current directory to `/p2pagent`.
3. Enter `./p2pagent` to start Commerce Suite using the application in the current directory. Without specifying any options, Commerce Suite runs in the foreground in interactive mode.

Figure D-20 Running p2pAgent in the Foreground



```
# cd /p2pagent
# ./p2pagent
iSoft(R) Peer-to-Peer Agent(TM)
(C) Copyright 2001-2002 iSoft Corp.
Build: 3.1.2002.9.30.1 ŸDec 19 2002 08:19:43"

Demonstration

2002.12.24 14:06:16.489       POPT OK  Log path set to Ÿlog"
2002.12.24 14:06:16.602       POPT OK  Trace set to WRITE_FILE
2002.12.24 14:06:17.189       POPT OK  Async. receipt path set to Ÿreceipt"
2002.12.24 14:06:20.408       HPIM OK  HTTP inbound service started




 ===> _
                                                                  RUNNING
ESC=¢   1=Help       2=SubCmd     3=HlpRetrn  4=Top        5=Bottom     6=TSO
        7=BackScr    8=Scroll     9=NextSess 10=Refresh   11=FwdRetr   12=Retrieve
MA      b                                                                  29/007
```

Connected to remote server/host 192.168.153.11 using port 2023

4. Enter shutdown to end the Commerce Suite process.

Working With Commerce Suite Payload Files

Files received and generated by Commerce Suite are placed within the HFS file system in directories specified by the `p2pagent.cfg` file or by commands issued within interactive mode.

There are a number of different directories that are used by Commerce Suite to record information generated by the process or to store files to be transmitted, or received by the process. Please refer to the *iSoft Commerce Suite Installation Guide* for a complete list of directories and their options.

The two main directories are:

- inbox

  This directory contains all the payload, messages, notices, and so forth, transmitted to the Commerce Suite by a trading partner. The directory is specified by an `addpair` statement. The directory is usually a subdirectory from the `/p2pagent` install directory.

- receipt

  This directory contains transmission receipts requested from the Commerce Suite trading partner. The directory is specified by a `set` statement `-rp` (receipt path) option. The directory is usually a subdirectory from the `/p2pagent` installation directory.

The typical format of a payload file stored in the inbox directory is shown below.

Note: The forward slashes are not part of the structure. They are shown to help understand how the format is broken down:

Listing D-3 Payload File Structure

```
linux./as400./2002/11/19/23/01/45/E0D30E81/file/.in

  |      |      |   |  |  |  |  |     |     |     |____Extension
  |      |      |   |  |  |  |  |     |     |___Inbound file name
  |      |      |   |  |  |  |  |     |____Random sequence number
  |      |      |   |  |  |  |  |___Second the file was received
  |      |      |   |  |  |  |_____Minute the file was received
  |      |      |   |  |  |______Hour the file was received
  |      |      |   |  |_____Day the file was received
  |      |      |   |_____Month the file was received
  |      |      |___Year the file was received
  |      |______Our Name (To)
  |____Name of the trading partner transmitting the file (From)
```

Most of the payload file name can be customized. Files are stored in the character set in which they were transmitted, which is normally ISO8859-1 (Latin 1 ASCII Character Set). Your application can read these files directly from the HFS file system by specifying the file name in IBM OS/390 standard HFS notation.

```
/p2pagent/inbox/os390.as400.2002111923014E0D30E81file.in
```

You can translate the data (if necessary) from ASCII to EBCDIC in your program by using the ICONV library interface (LIBICONV). Please refer to the IBM publication *National Language Support Guide and Reference* for more information on character set translation.

You can also use the OS/390 utility ICONV. This is a utility that is standard on IBM operating platforms. An example of converting a file from ASCII to EBCDIC using ICONV might look similar to the following code example:

```
cat ascii_file | iconv -f ISO8859-1 -t IBM-037 > ebcdic_file
```

The above command, which is executed within the UNIX System Services environment, takes the ASCII file `ascii_file` and converts it from ASCII to EBCDIC and creates a new file `ebcdic_file`.

Commerce Suite Performance

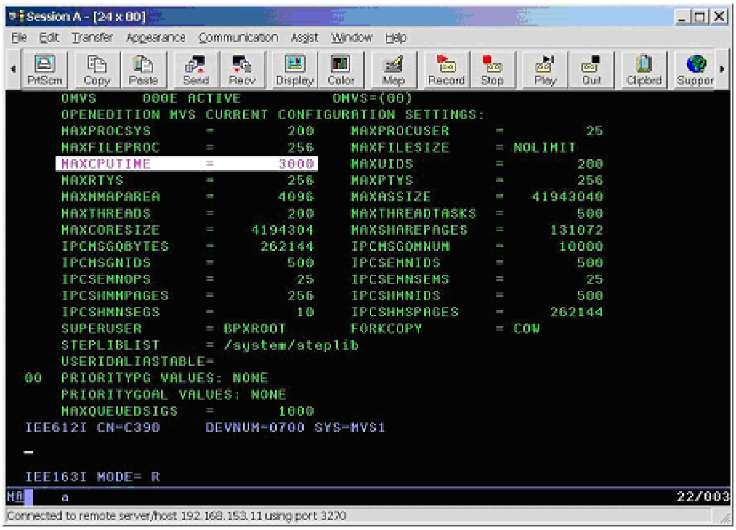
The Commerce Suite is a CPU-intensive application when processing payloads that contain signed or encrypted data. Many mathematical calculations are used to process the data.

It is recommended that Commerce Suite be submitted through batch using BPXBATCH (Refer to the *Submitting the p2pbatch job* section). It should be submitted with the user ID of the UNIX System Services root administrator. This allows the job to run with unlimited CPU time and not end when it reaches `MAXCPUTIME`.

If the Commerce Suite is not run under the user ID of the UNIX System Services root administrator, then the process or batch job will end when `MAXCPUTIME` is reached.

The following screen shot shows the global options in effect for UNIX System Services for all processes within UNIX System Services.

Figure D-21 Display omvs,options



```
      OMVS      000E ACTIVE             OMVS=(00)
      OPENEDITION MVS CURRENT CONFIGURATION SETTINGS:
      MAXPROCSYS      =        200    MAXPROCUSER      =        25
      MAXFILEPROC     =        256    MAXFILESIZE      = NOLIMIT
      MAXCPUTIME      =       3000    MAXUIDS          =       200
      MAXRTYS         =        256    MAXPTYS          =       256
      MAXMMAPAREA     =       4096    MAXASSIZE        =  41943040
      MAXTHREADS      =        200    MAXTHREADTASKS   =       500
      MAXCORESIZE     =    4194304    MAXSHAREPAGES    =    131072
      IPCMSGQBYTES    =     262144    IPCMSGQMNUM      =     10000
      IPCMSGNIDS      =        500    IPCSEMNIDS       =       500
      IPCSEMNOPS      =         25    IPCSEMNSEMS      =        25
      IPCSHMMPAGES    =        256    IPCSHMNIDS       =       500
      IPCSHMNSEGS     =         10    IPCSHMSPAGES     =    262144
      SUPERUSER       = BPXROOT       FORKCOPY         = COW
      STEPLIBLIST     = /system/steplib
      USERIDALIASTABLE=
  00  PRIORITYPG VALUES: NONE
      PRIORITYGOAL VALUES: NONE
      MAXQUEUEDSIGS   =       1000
  IEE612I CN=C390     DEVNUM=0700 SYS=MVS1

  -

  IEE163I MODE= R
MA    a                                                                   22/003
Connected to remote server/host 192.168.153.11 using port 3270
```

The highlighted area in the preceding figure shows the current value of `MAXCPUTIME`.

The option `MAXCPUTIME` can be changed either at the console or by updating the `BPXPRMxx` member of `SYS1.PARMLIB` that is in effect for your installation.

To change the `MAXCPUTIME` setting from the MVS operations console, issue the following command:

```
setomvs maxcputime=value
```

Where `value` is the maximum number of CPU seconds a process can use before it is terminated. Changing this value changes the maximum CPU time for all processes with UNIX System Services. Please see the IBM publication “MVS System Commands” for more information on the `setomvs` command.

E IBM Federated Partner Profile Support

This appendix explains how the Commerce Suite application interfaces with IBM Federated Partner profiles.

Understanding the IBM Federated Partner Profile

The IBM Federated Partner Profile resides in an XML file. This file follows IBM's unique XML format and contains the trading partner definition and certificate information. The header of the file contains Meta data that defines the action to be taken on the profile (add, edit, or delete). The Key Data section of the file lists a URL where the key certificate can be found.

Notes:

- Each XML file can contain only one partner profile definition.
- The XML file is packaged in a Commerce Suite work order file. This work order file must reside in an MQ Series queue.

Understanding the Commerce Suite Interface

The following steps describe how the Commerce Suite interfaces with IBM Federated Partner Profiles:

1. The Commerce Suite polls the MQ Series queue for information.
2. When it finds the XML file containing the partner profile definition, it reads the header and converts the header data into commands that Commerce Suite can understand.
3. The Commerce Suite then checks the key data section of the XML file for the URL where the key certificate information is located. It then issues a "get" command to get the key certification.
4. The Commerce Suite generates an `addpair` and an `importkey` command to create the trading partner relationship.
5. The database is then updated with the new relationship information.

   Note: For more information on the `addpair` and `importkey` commands, refer to *iSoft Commerce Suite Command Reference*.

F Commerce Suite Error Messages

The following table contains a description of error, informational, and warning messages that can be encountered while using the Commerce Suite software.

Table 1 Commerce Suite Error Messages

Error Code Number Decimal/Hexadecimal **Error Code**	**Error Code Description**
4096/1000 `IAPI_ERR_BADPARAM`	An invalid or missing parameter was found by the application while processing a function.
4097/1001 `IAPI_ERR_ALLOCFAIL`	The application was unable to allocate enough memory to satisfy the need of a program function.
4098/1002 `IAPI_ERR_THREADFAIL`	The application was unable to create a new process thread. A process thread is a separate processing context within the application. It is normal for the application to utilize multiple threads concurrently. However, an operating system may have limitations on the number of threads that can be created for a single process.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
4099/1003 `IAPI_ERR_LOCKFAIL`	The application was not able to grant a thread exclusive access to a resource (memory,file,database,mailbox). Some resources must be locked before use so that only one thread can update a shared resource.
4100/1004 `IAPI_ERR_EDSADD`	An error occurred attempting to add a message to an external mailbox system.
4101/1005 `IAPI_ERR_EDSEXTRACT`	An error occurred attempting to extract a message from an external mailbox system.
4352/1100 `FILE_ERR_EXISTSFAIL`	The application encountered an operating system error while attempting to determine if a file exists.
4353/1101 `FILE_ERR_RENAMEFAIL`	The application encountered an operating system error while attempting to rename a file.
4354/1102 `FILE_ERR_CREATEFAIL`	The application encountered an operating system error while attempting to create a file.
4355/1103 `FILE_ERR_TEMPFAIL`	The application encountered an operating system error while attempting to create a temporary file.
4356/1104 `FILE_ERR_DESTROYFAIL`	The application encountered an operating system error while attempting to delete a file.
4357/1105 `FILE_ERROR_OPENFAIL`	The application encountered an operating system error while attempting to open a file for read and write access.
4358/1106 `FILE_ERR_OPENAPPENDFAIL`	The application encountered an operating system error while attempting to open a file for appending data.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
4359/1107 `FILE_ERR_OPENBROWSEFAIL`	The application encountered an operating system error while attempting to open a file for browse only.
4360/1108 `FILE_ERR_CLOSEFAIL`	The application encountered an operating system error while attempting to close a file.
4361/1109 `FILE_ERR_READFAIL`	The application encountered an operating system error while attempting to read from a file.
4362/110A `FILE_ERR_WRITEFAIL`	The application encountered an operating system error while attempting to write to a file.
4363/110B `FILE_ERR_POSFAIL`	The application encountered an operating system error while attempting to obtain the current file-pointer position.
4364/110C `FILE_ERR_SEEKFAIL`	The application encountered an operating system error while attempting to move the current file-pointer position.
4365/110D `FILE_ERR_ENDFAIL`	The application encountered an operating system error while attempting to set the file-pointer to the end of a file.
4366/110E `FILE_ERR_REWINDFAIL`	The application encountered an operating system error while attempting to set the file-pointer to the beginning of a file.
4608/1200 `COMPRESS_ERR_DEFLATE`	The application was unable to compress a message.
4609/1201 `COMPRESS_ERR_INFLATE`	The application was unable to uncompress a message.
4864/1300 `SHA1_ERR_HASHFILEFAIL`	The application was unable to compute a message digest.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5120/1400 PKI_ERR_CREATEKEYFAIL	The application was unable to create an RSA public/private key-pair.
5121/1401 PKI_ERR_NOCERTSEQ	The Certificate sequence was not found in an X.509 certificate
5122/1402 PKI_ERR_NOTBSSEQ	The tbsCertificate sequence was not found in an X.509 certificate.
5123/1403 PKI_ERR_NOTBSVERSEQ	The tbsCertificate Version sequence was not found in an X.509 certificate.
5124/1404 PKI_ERR_NOTBSVERINT	The tbsCertificate Version integer was not found in an X.509 certificate.
5125/1405 PKI_ERR_BADTBSVER	The tbsCertificate Version integer is invalid or not supported.
5126/1406 PKI_ERR_NOSERNO	The serial-number part of an X.509 certificate could not be found.
5127/1407 PKI_ERR_NOSIGALGSEQ	The signatureAlgorithm sequence of an X.509 certificate could not be found.
5128/1408 PKI_ERR_NOSIGALGOID	The signatureAlgorithm Object Identifier of an X.509 certificate could not be found.
5129/1409 PKI_ERR_BADSIGALG	The signatureAlgorithm of an X.509 certificate is invalid or not supported.
5130/140A PKI_ERR_NOSIGALGRPARAM	The parameter field of a signatureAlgorithm OID of an X.509 certificate was not found.
5131/140B PKI_ERR_NOISSSEQ	The Issuer sequence of an X.509 certificate could not be found
5132/140C PKI_ERR_NOVALSEQ	The ValidityPeriod sequence of an X.509 certificate could not be found.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5133/140D `PKI_ERR_NOVALBEG`	The ValidityPeriod BeginDate of an X.509 certificate could not be found.
5134/140E `PKI_ERR_NOVALEND`	The ValidityPeriod EndDate of an X.509 certificate could not be found.
5135/140F `PKI_ERR_NOSUBSEQ`	The SubjectName of an X.509 certificate could not be found.
5136/1410 `PKI_ERR_NOKEYINFOSEQ`	The SubjectPublicKeyInfo sequence of an X.509 certificate could not be found.
5137/1411 `PKI_ERR_NOKEYALGSEQ`	The SubjectPublicKeyInfo Algorithm Sequence of an X.509 certificate could not be found.
5138/1412 `PKI_ERR_NOKEYALGOID`	The SubjectPublicKeyInfo Algorithm OID of an X.509 certificate could not be found.
5139/1413 `PKI_ERR_BADKEYALG`	The SubjectPublicKeyInfo Algorithm is invalid or not supported.
5140/1414 `PKI_ERR_NOKEYALGPARAM`	The SubjectPublicKeyInfo Algorithm Parameter field is missing.
5141/1415 `PKI_ERR_NOKEY`	The SubjectPublicKey Bit-String of an X.509 certificate could not be found.
5142/1416 `PKI_ERR_NOKEYSEQ`	The SubjectPublicKey RSAPublicKey sequence of an X.509 certificate could not be found.
5143/1417 `PKI_ERR_NOMODULUS`	The SubjectPublicKey Modulus Integer of an X.509 certificate could not be found.
5144/1418 `PKI_ERR_NOPUBEXP`	The SubjectPublicKey Public Exponent integer of an X.509 certificate could not be found.
5145/1419 `PKI_ERR_NOEXTSSEQ`	The Extensions sequence of an X.509 certificate could not be found.

Error Code Number Decimal/Hexadecimal **Error Code**	**Error Code Description**
5146/141A `PKI_ERR_NOEXTSEQ`	An Extension sequence of an X.509 certificate could not be found.
5147/141B `PKI_ERR_NOEXTOID`	An Extension OID of an X.509 certificate could not be found.
5148/141c `PKI_ERR_NOEXTOCTSTR`	An Extension Octet-String of an X.509 certificate could not be found.
5149/141D `PKI_ERR_NOUSAGEVAL`	An Extension Value of an X.509 certificate could not be found.
5150/141E `PKI_ERR_NONAMESEQ`	The Name sequence of an X.509 certificate distinguished-name could not be found.
5151/141F `PKI_ERR_NONAMESET`	The Name set of an X.509 certificate distinguished-name could not be found.
5152/1420 `PKI_ERR_NOATTRSEQ`	The AttributeTypeAndValue sequence of an X.509 certificate distinguished-name could not be found.
5153/1421 `PKI_ERR_NOATTROID`	The AttributeTypeAndValue OID of an X.509 certificate distinguished-name could not be found.
5154/1422 `PKI_ERR_NOATTRVAL`	The AttributeTypeAndValue Value of an X.509 certificate distinguished-name could not be found.
5155/1423 `PKI_ERR_NOPRVSEQ`	The PKCS1 PrivateKey sequence could not be found.
5156/1424 `PKI_ERR_NOPRVVER`	The PKCS1 PrivateKey version integer could not be found.
5157/1425 `PKI_ERR_BADPRVVER`	The PKCS1 PrivateKey version value is invalid or not supported.
5158/1426 `PKI_ERR_NOPRVMOD`	The PKCS1 PrivateKey Modulus integer could not be found.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5159/1427 PKI_ERR_BADMOD	The PKCS1 PrivateKey Modulus is invalid.
5160/1428 PKI_ERR_NOPRVPUBEXP	The PKCS1 PrivateKey Public Exponent could not be found.
5161/1429 PKI_ERR_BADPUBEXP	The PKCS1 PrivateKey Public Exponent is invalid.
5162/142A PKI_ERR_NOPRVPRVEXP	The PKCS1 PrivateKey Private Exponent is missing.
5163/142B PKI_ERR_BADKEYPAIR	The PKCS1 PrivateKey key-pair is not valid.
5164/142C PKI_ERR_NOPRVPRIME1	The PKCS1 PrivateKey First Prime (p) is missing.
5165/142D PKI_ERR_NOPRVPRIME2	The PKCS1 PrivateKey Second Prime (q) is missing.
5166/142E PKI_ERR_NOPRVEXP1	The PKCS1 PrivateKey First Exponent (dp) is missing.
5167/142F PKI_ERR_NOPRVEXP2	The PKCS1 PrivateKey Second Exponent (dq) is missing.
5168/14530 PKI_ERR_NOPRVCOEFF	The PKCS1 PrivateKey Coefficient (qinv) is missing.
5312/14C0 PKI_ERR_NOIMPORTEDREQ	The application was requested to parse a certificate request, but no request was found.
5313/14C1 PKI_ERR_NOREQSEQ	The Certificate-Request sequence of a certificate request message was not found.
5314/14C2 PKI_ERR_NOPKISEQ	The PKI sequence of a certificate-request message was not found.

Error Code Number Decimal/Hexadecimal **Error Code**	**Error Code Description**
5315/14C3 `PKI_ERR_NOOIDSEQ`	The PKI Object-Identifier of a certificate-request message was not found.
5316/14C4 `PKI_ERR_NOTRAILNULL`	The OID Parameter of a certificate-request message was not found.
5317/14C5 `PKI_ERR_BADENCBLOCK`	The decrypted message-digest of a certificate-request signature was not a valid PKCS Type-1 block
5318/14C6 `PKI_ERR_BADSIGN`	The decrypted message-digest of a certificate-request signature did not match the message-digest computed by the application.
5319/14C7 `PKI_ERR_NOATTRSET`	An Attribute set of a certificate-request message could not be found.
5376/1500 `SOCKET_ERR_STARTFAIL`	The application was unable to initialize the sockets API. This error should only occur on Microsoft Windows platforms as a result of the WSAStartup function call. This error can occur if the underlying network software could not properly initialize during system startup.
5377/1501 `SOCKET_ERR_STOPFAIL`	The application was unable to finalize its use of the sockets API on a Microsoft Windows platform.
5378/1502 `SOCKET_ERR_GETHOSTNAMEFAIL`	The application was unable to obtain the current computer's hostname from the TCP/IP networking software.
53791503 `SOCKET_ERR_GETHOSTNAMEBYFAIL`	The application was unable to obtain the current computer's IP address from the TCP/IP networking software.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5380/1504 `SOCKET_ERR_DATAGRAMFAIL`	The application was unable to create a socket of type DATAGRAM.
5381/1505 `SOCKET_ERR_STREAMFAIL`	The application was unable to create a socket of type STREAM.
5382/1506 `SOCKET_ERR_CLOSEFAIL`	The application was unable to close a TCP/IP socket
5383/1507 `SOCKET_ERR_BLOCKFAIL`	The application was unable to set a TCP/IP socket to non-blocking mode.
5384/1508 `SOCKET_FAIL_BROADCASTFAIL`	The application was unable to set a TCP/IP socket to broadcast mode.
5385/1509 `SOCKET_ERR_BINDFAIL`	The application was unable to issue a socket BIND call. The requested IP address and PORT may already be in use by another application.
5386/150A `SOCKET_ERR_GETFAIL`	The application was unable to issue a socket GET call. UDP requests may be disabled by the TCP/IP networking software.
5387/150B `SOCKET_ERR_PUTFAIL`	The application was unable to issue a socket PUT call. UDP requests may be disabled by the TCP/IP networking software.
5388/150C `SOCKET_ERR_LISTENFAIL`	The application was unable to issue a socket LISTEN call. The socket BIND may have failed.
5389/150D `SOCKET_ERR_ACCEPTFAIL`	The application was unable to issue a socket ACCEPT call. The socket BIND may have failed.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5390/150E `SOCKET_ERR_GETPEERNAMEFAIL`	The application was unable to obtain the IP address and PORT of the remotely connected host.
5391/150F `SOCKET_ERR_CONNECTFAIL`	The application was unable to connect to a remote computer. The remote computer may not be accepting connections or a fire-wall may be preventing a connection to the remote host.
5392/1510 `SOCKET_ERR_GETSOCKNAMEFAIL`	The application was unable to obtain information about the remote computer.
5393/1511 `SOCKET_ERR_READFAIL`	The application was unable to read data from a connected TCP/IP socket. A fire-wall may be preventing data traffic in an inbound direction from the remote computer.
5394/1512 `SOCKET_ERR_WRITEFAIL`	The application was unable to write data to a connected TCP/IP socket. A fire-wall may be preventing data traffic in an outbound direction to the remote computer.
5632/1600 `CMS_ERR_NOCONINFSEQ`	The ContentInfo sequence could not be found in an ASN1-encoded message.
5633/1601 `CMS_ERR_NOCONINFOID`	The ContentInfo Object Identifier (OID) could not be found in an ASN1-encoded message.
5634/1602 `CMS_ERR_BADCONINFOID`	The Object identifier found in a ContentInfo sequence of an ASN1-encoded message is invalid or is not the expected value.
5635/1603 `CMS_ERR_NOCONINFCONTENT`	The Content field of the ContentInfo sequence of an ASN1-encoded messages could not be found.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5636/1604 `CMS_ERR_NOSIGDATSEQ`	The SignedData sequence could not be found in an ASN1-encoded message that has a signedData content type.
5637/1605 `CMS_ERR_NOSIGDATVER`	The SignedData version integer could not be found in an ASN1-encoded message that has a signedData content type.
5638/1606 `CMS_ERR_NOSIGDATALGSET`	The digestAlgorithm set could not be found in an ASN1-encoded message that has a signedData content type.
5639/1607 `CMS_ERR_NOSIGDATALGSEQ`	The digestAlgorithm sequence could not be found in an ASN1-encoded message that has a signedData content type.
5640/1608 `CMS_ERR_NOSIGDATALGOID`	The digestAlgorithm Object Identifier (OID) could not be found in an ASN1-encoded message that has a signedData content type.
5641/1609 `CMS_ERR_BADSIGDATALGOID`	The digestAlgorithm Object Identifier found in an ASN1-encoded message is invalid or not supported.
5642/160A `CMS_ERR_NOENCCONINFSEQ`	The encapsulatedContentInfo Sequence could not be found in an ASN1-encoded message.
5643/160B `CMS_ERR_NOENCCONINFOID`	The encapsulatedContentInfo Object Identifier (OID) could not be found in an ASN1-encoded message.
5644/160C `CMS_ERR_BADENCCONINFOID`	The encapsulatedContentInfo OID found in an ASN1-encoded message is invalid or not supported.
5645/160D `CMS_ERR_NOSIGINFSET`	The signerInfo set could not be found in an ASN1-encoded message.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5646/160E `CMS_ERR_NOSIGINFSEQ`	The signerInfo sequence could not be found in an ASN1-encoded message.
5647/160F `CMS_ERR_NOSIGINFVER`	The singerInfo version integer could not be found in an ASN1-encoded message.
5648/1610 `CMS_ERR_NOSIGINFRID`	The IssuerNameAndSerialNbr sequence could not be found in an ASN1-encoded message.
5649/1611 `CMS_ERR_NODIGALGSEQ`	The digestAlgorithm sequence could not be found in an ASN1-encoded message.
5650/1612 `CMS_ERR_NODIGALGOID`	The digestAlgorithm Object Identifier (OID) could not be found in an ASN1-encoded message.
5651/1613 `CMS_ERR_BADAUTATTLEN`	The length of the AuthenticatedAttributes part of a signedData ASN1-encoded message is of an indefinite-length, which is not supported.
5652/1614 `CMS_ERR_NOAUTATTSEQ`	The AuthenticatedAttributes sequence could not be found in an ASN1-encoded message.
5653/1615 `CMS_ERR_NOAUTATTOID`	The AuthenticatedAttributes Object Identifier (OID) could not be found in an ASN1-encoded message.
5654/1616 `CMS_ERR_NOMSGDIGEST`	The MessageDigest set could not be found in an ASN1-encoded message.
5655/1617 `CMS_ERR_NOMSGDIGOCTSTR`	The MessageDigest octet-string could not be found in an ASN1-encoded message.
5656/1618 `CMS_ERR_NOATTSET`	The Attribute set of an ASN1-encoded message could not be found.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5657/1619 `CMS_ERR_NODIGENCALGSEQ`	The digestEncryptionAlgorithm sequence could not be found in an ASN1-encoded message.
5658/161A `CMS_ERR_NODIGENCALGOID`	The digestEncryptionAlgorithm Object Identifier (OID) could not be found in an ASN1-encoded message.
5659/161b `CMS_ERR_BADDINGENCALGOID`	The digestEncryptionAlgorithm OID in an ASN1-encoded message is invalid or not supported.
5660/161C `CMS_ERR_NOENCDIGOCTSTR`	The EncryptedDigest Octet-String in an ASN1-encoded message could not be found.
5661/161D `CMS_ERR_NOENVDATSEQ`	The EnvelopedData SEQUENCE of an ASN1-encoded message could not be found.
5662/161E `CMS_ERR_NOENVDATVER`	The EnvelopedData version INTEGER of an ASN1-encoded message could not be found.
5663/161F `CMS_ERR_BADENVDATVER`	The EnvelopedData version is invalid or not supported.
5664/1620 `CMS_ERR_BADENVDATORI`	The Envelopeddata OriginatorInfo was found but the ASN1 version is not version 2.
5665/1621 `CMS_ERR_NORCPINFSET`	The EnvelopedData RecipientInfos SET of an ASN1-encoded message was not found.
5666/1622 `CMS_ERR_NORCPINFSEQ`	The EnvelopedData RecipientInfo SEQUENCE of an ASN1-encoded message was not found.
5667/1623 `CMS_ERR_NORCPINFVER`	The EnvelopedData RecipientInfo Version INTEGER was not found.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5668/1624 `CMS_ERR_BADRCPINFVER`	The EnvelopedData RecipientInfo Version if an ASN1-encoded message is invalid.
5669/1625 `CMS_ERR_NORCPINFRID`	The EnvelopedData RecipientInfo RecipientIdentidifier of an ASN1-encoded message was not found.
5670/1626 `CMS_ERR_NOENCALGSEQ`	The EnvelopedData RecipientInfo keyEncryptionAlgorithm sequence was not found.
5671/1627 `CMS_ERR_NOENCKEYOCTSTR`	RecipientInfo.encryptedContentInfo not found.
5672/1628 `CMS_ERR_BADRCPINFSEQ`	RecipientInfo SEQUENCE is improperly formed.
5673/1629 `CMS_ERR_BADRCPINFSET`	RecipientInfo SET is improperly formed.
5674/162A `CMS_ERR_NOENCCONSEQ`	EnvelopedData.EncryptedContentInfo SEQUENCE not found.
5675/162B `CMS_ERR_NOENCCONOID`	EnvelopedData.EncryptedContentInfo OID not found.
5676/162C `CMS_ERR_BADENCCONOID`	Invalid EncryptedContentInfo OID.
5677/162D `CMS_ERR_NOCONENCALGSEQ`	EncryptedContentInfo SEQUENCE not found.
5678/162E `CMS_ERR_NOCONENCALGOID`	EncryptedContentInfo OID not found.
5679/162F `CMS_ERR_BADCONENCALGOID`	Invalid EncryptedContentInfo OID.
5680/1630 `CMS_ERR_BADCONENCALG`	Invalid EncryptedContentInfo Algorithm.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5681/1631 `CMS_ERR_NOENCALGPARAM`	Encryption algorithm parameter not found.
5682/1632 `CMS_ERR_BADENCALGPARAM`	Invalid encryption algorithm parameter.
5683/1633 `CMS_ERR_NOENCCONLEN`	No encryptedContent length.
5684/1634 `CMS_ERR_NOENCCONTENT`	No encryptedContent.
5685/1635 `CMS_ERR_NOENCCONOCTSTR`	No encryptedContent OCTETSTRING.
5686/1636 `CMS_ERR_BADENCCONTENT`	Invalid encryptedContent.
5687/1637 `CMS_ERR_BADCONENCKEY`	Invalid content-encryption key.
5688/1638 `CMS_ERR_NOCMPDATSEQ`	CompressedData SEQUENCE not found.
5689/1639 `CMS_ERR_NOCMPDATVER`	CompressedData.version INTEGER not found.
5690/163A `CMS_ERR_BADCMPDATVER`	Invalid CompressedData.version.
5691/163B `CMS_ERR_NOCMPALGSEQ`	CompressedData.compressionAlgorithm SEQUENCE not found.
5692/163C `CMS_ERR_NOCMPALGOID`	CompressedData.compressionAlgorithm OID not found.
5693/163D `CMS_ERR_BADCMPALGOID`	Invalid CompressedData.compressionAlgorithm OID value.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
5694/163E `CMS_ERR_NOCMPCONLEN`	No compressed-content length.
5695/163F `CMS_ERR_NOCMPCONOCTSTR`	No CompressedData.encapContentInfo.eContent OCTET-STRING.
5696/1640 `CMS_ERR_BADCMPCONTENT`	Invalid compressedContent.
5697/1641 `CMS_ERR_NOCMPCONTENT`	No compressedData content.
6400/1900 `IAUTH_ERR_AUTHCODEEXPIRED`	The authentication code entered by the user to license the application has expired. Authentication codes distributed with the application are valid for a period that may vary depending on a customer's license agreement.
6401/1901 `IAUTH_ERR_AUTHCODEINVALID`	The authentication code entered by the user to license the application is invalid. This may be caused by a correct code being entered incorrectly, or a code for another implementation being used with the wrong copy of the application.
6402/1902 `IAUTH_ERR_INIFILEBADLEN`	The initialization file (p2pagent.ini) has an invalid length. This can be caused if the p2pagent.ini file has been corrupted or modified such that it is too short to contain a valid serial-number.
6403/1903 `IAUTH_ERR_LICFILEBADLEN`	The license file (p2pagent.lic) has an invalid length. This can be caused if the p2pagent.lic file has been corrupted or modified such that it is not the correct length. For Commerce Suite Version 3.1, the correct length of a license file is 320 bytes.

Error Code Number Decimal/Hexadecimal Error Code	Error Code Description
8448/2100 `AS2_ERR_NOAS2FROM`	The application detected an inbound data stream that did not contain an AS2-From header within its HTTP headers.
8449/2101 `AS2_ERR_NOAS2TO`	The application detected an inbound data stream that did not contain an AS2-To header within its HTTP headers.
8450/2102 `AS2_ERR_BADFROMTO`	The application detected an inbound data stream that contained a set of AS2-From and AS2-To headers that represent a relationship of trading partners that could not be found in the transport agent's relationship array for the active protocol (HTTP or HTTPS). This error can occur if the AS2-From and AS2-To name combination is unknown or invalid or if the transport agent's relationship array has not been populated by the Admin agent or by retrieving relationship data from the database with the getpairs command.
8451/2103 `AS2_ERR_NORCPT`	The application did not receive a requested receipt (MDN) from a trading partner within the specified time-limit.
8452/2104 `AS2_ERR_MDNERR`	The application has detected that an error was reported by a trading partner in an MDN received from a trading partner.
8453/2105 `AS2_ERR_DECRYPTFAIL`	The application was unable to decrypt an encrypted message received from a trading partner. This can be caused by applying a private-key to the decryption process that does not correspond to the public-key in the certificate that was used to encrypt the data by the trading partner.

Error Code Number Decimal/Hexadecimal **Error Code**	**Error Code Description**
8454/2106 `AS2_ERR_VERIFYFAIL`	The application was unable to verify a signed message received from a trading partner. This can be caused by applying a public-key from a certificate to the verification process that does not correspond to the private-key that was used to sign the data by the trading partner.
8455/2107 `AS2_ERR_DECOMPRESSFAIL`	The application was unable to decompress a message received from a trading partner. This can be caused if the sender of the message used a different compression algorithm than the ZLIB algorithm interoperability-tested by AS2 vendors.
8456/2108 `AS2_ERR_BADURL`	The application determined that the destination Internet-Protocol (IP) address for a trading partner is invalid before attempting to connect to the trading partner. This can be caused by an invalid or incorrect To-URL value in the database. This can also be caused by a failure of the underlying network's DNS (Domain Name Service) to resolve an Internet host name to a dot-notated address.
8457/2109 `AS2_ERR_BADHEADERLEN`	The application cannot process a MIME header because it exceeds the currently supported maximum-length for a MIME header. For Commerce Suite Version 3.1 the maximum header length is 512 characters.

Glossary

A

Agent

An instance of the Peer-to-Peer Agent Version 3 (Commerce Suite) application configured to provide services to a particular role, i.e. Administrator, Transport, or Router.

Administrator Agent

An instance of the Commerce Suite application configured to provide administrative services including the remote configuration of Transport and Router Agents and access to centrally located configuration data.

Application Service

See Service.

AS1

A draft specification first published in the Internet Engineering Task Force (IETF) standard's track. AS stands for Applicability Statement and is a specification about how to transport data, not how to validate or process data. AS1 provides an Internet solution for securely exchanging EDI and XML over the Internet using SMTP.

AS2

A draft specification first published in the Internet Engineering Task Force (IETF) standard's track. AS stands for Applicability Statement and is a specification about how to transport data, not how to validate or process data. AS2 specifies the means to connect, deliver, validate, and reply to (receipt) data in a secure and reliable way. AS2 provides an Internet solution for securely exchanging EDI over the Internet using the hypertext transmission protocol (HTTP) instead of the simple mail transport protocol (SMTP) as the transport protocol.

Authentication

Ensures the accurate identification of both the sender and the receiver. Authentication is accomplished using digital signatures.

C

Cipher

A key-selected transformation between plaintext and ciphertext. An algorithm for putting a message into code by transposition and/or substitution of symbols.

Compression

The ability to represent data in forms that take less storage than the original. The limit to this is the amount of uniqueness in the data. It is not possible to compress everything down to a single byte, because a byte can only select 256 different results. Data compression is either “lossy,” in which some information is lost, or “lossless,” in which all of the original information can be completely recovered.

Configuration File

A text file containing one or more Console Command statements. A Configuration File can be processed automatically by the Commerce Suite application upon startup if it is named p2pagent.cfg and stored in the same directory location as the Commerce Suite executable program. A Configuration File can also be processed if the -f parameter is entered as a run-time program argument or as a console command.

Control Address

The IP address portion of the IP Address and Port used by the Commerce Suite Transport and Router Agents to listen for incoming control messages from a supervising Administrative Agent; configured using the -ca Set Option.

Control Port

The IP Port portion of the IP Address and Port used by the Commerce Suite Transport and Router Agents to listen for incoming control messages from a supervising Administrative Agent. Configured using the -cp Set Option.

Control Service

The set of application tasks which execute within the context of a thread of execution to process incoming commands being sent by an Administrator Agent. The Control Service is required by Commerce Suite Agents acting in the Transport or Router Role, if the Agent is being remotely configured.

Cypher Text

Data that has been transformed from a plaintext form into encrypted text (an unreadable form) using an encryption process.

D

DEFLATE

Specifies the DEFLATE compression algorithm used to reduce the file transfer overhead. The DEFLATE compression algorithm is a lossless compressed data format that compresses data using a combination of the LZ77 algorithm and Huffman coding.

Delivery Notification

A message formatted according to (AS2) that is sent to a sending host computer to indicate the disposition of a received message. The format of Delivery Notifications used by Commerce Suite is the Message Delivery Notification. or MDN, as defined in MDN.

Digital Certificate

A document that contains name, serial number, expiration dates and a copy of the owner’s public key; used to encrypt data and validate signatures.

Digital Signature

A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are a number of different encryption techniques to guarantee this level of security.

Document Digest

A unique “fingerprint” summary (128 or 160 bits long) of an input file. It is used to create a digital signature and to ensure that the file has not been altered. It is also called a hash and is produced by a checksum program that processes a file.

DSS

Specifies the Digital Signature Algorithm (DSA) for digital signature generation and verification. The DSA is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process.

E

EDI

Short for Electronic Data Interchange, the transfer of data between different companies using networks, such as the Internet. As more and more companies get connected to the Internet, EDI is becoming increasingly important as an easy mechanism for companies to buy, sell, and trade information. ANSI has approved a set of EDI standards known as the X12 standards.

EDIINT

EDI Over the Internet Working Group - a working group of the IETF that developed the AS1 and AS2 proposed standards.

Encryption

A process that uses a mathematical algorithm and a key to transform data into an unreadable format (called cyphertext). A receiver can then use a key to restore the data to its original content.

F

FIPS

Federal Information Processing Standard.

G

Graphical User Interface

A GUI (usually pronounced GOO-ee) is a graphical user interface that takes advantage of the computer's graphics capabilities to make the program easier to use. Well-designed graphical user interfaces can free the user from learning complex command languages. On the other hand, many users find that they work more effectively with a command-driven interface, especially if they already know the command language.

GZIP

Specifies a lossless compressed data format that is compatible with the widely used GZIP utility. This format includes a cyclic redundancy check value for detecting data corruption.

H

Hash

A hash value (or simply *hash*) is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact.

HTTP

See Hypertext Transfer Protocol.

Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

I

IETF

Internet Engineering Task Force - The Internet Engineering Task Force is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

In-Beacon Service

The set of application tasks that execute within the context of a single application thread to receive UDP packets sent by one or more Transport Agents. Commerce Suite Agents configured for the Router Role (Router Agents) use the In-Beacon Service to collect these UDP packets to maintain current information about active Transfer Agents on the local network segment.

Inbound Service

One or more sets of application tasks that execute within the context of one or more threads of execution to process incoming data being sent by a remote host computer. The Inbound Service consists of, at least, one inbound thread listening for incoming TCP/IP connections on a particular protocol (HTTP or HTTPS). The Inbound Service creates an Inbound Session thread for each separate incoming connection. Each discrete protocol is serviced by a separate Inbound Main thread, which is assigned a unique IP address and port on which to listen for incoming connections.

Integrity

Ensures that data is not tampered with or corrupted in transit. Integrity is accomplished using document digests and digital signatures.

K

Key Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

M

MD5

Specifies the Message Digest Algorithm used to verify a file's integrity. The MD-5 is a one-way has algorithm that takes any length of data and produces a 128-bit "fingerprint" or "message digest". This fingerprint is "non-reversible", meaning that the data cannot be determined based on its MD-5 fingerprint.

Message Disposition Notification (MDN)

A Message Disposition Notification (MDN) message is a response message defined to ensure the secure reliable delivery of messages for AS1 and AS2 protocols.

MIME

Multipurpose Internet Mail Extension - MIME is a specification for enhancing the capabilities of standard Internet electronic mail. It offers a simple standardized way to represent and encode a wide variety of media types for transmission using Internet mail.

N

NIST

National Institute of Standards and Technology. A part of the U.S. Department of Commerce, formerly called the National Bureau of Standards, that defines standards for voice, data, and video transmissions, encryption, and other kinds of technology.

Non-repudiation of Receipt

Confirms that the intended party received the data. This is accomplished using digital signatures and signed MDNs.

O

Out-Beacon Service

The set of application tasks that execute within the context of a single thread of execution to periodically transmit a small packet of data identifying the Transport Agent to one or more Router Agents. The Out-Beacon Service emits a UDP packet containing the IP Addresses and Ports on which the Agent is currently listening. Router Agents collect these packets to dynamically build a current list of Transport Agents to which inbound data can be routed for processing.

Outbound Service

The set of application tasks that execute within the context of one or more threads of execution to process requests for outgoing message delivery. The Outbound service consists of, at least, the main outbound thread that processes send transactions from the Outbound Queue. The main outbound thread creates an Outbound Session thread for each separate send request.

P

PKI Service

The set of application tasks that execute within the context of a single thread of execution to proactively search the configuration database for public-key certificates which are nearing their expiration date. The PKI Service implements the iSoft Zero-Administration PKI architecture, to facilitate the automated renewal of public-key certificates.

Plain Text

Unencrypted data.

Port

A specific communications end-point to a logical connection and the way a client program specifies a specific server program on a computer in a network.

Privacy

Ensures that only the intended receiver can view the data. This is accomplished using a combination of encryption algorithms and message packaging.

Private Key

A value known only to the owner, used to create a signature and decrypt data encrypted by its corresponding public key.

Public Key

A value, known by everyone to whom the certificate has been distributed, used to encrypt data and validate a digital signature. Although mathematically related to the private key, it is astronomically difficult to derive from the public key.

Public Key Infrastructure

Public Key Infrastructure is a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI or even a single agreed-upon standard for setting up a PKI.

R

RC2

Specifies the Rivest's Cipher encryption algorithm used to encrypt and decrypt messages. RC-2 is a conventional (secret key) block encryption algorithm and has a block size of 64-bits with a variable key size from one byte up to 128 bytes.

Role

The set of Commerce Suite Application Services operating within a single instance of the Commerce Suite application (a process) which, taken together, comprise a logical functional unit in an iSoft P2P network. The Roles supported by Commerce Suite are Administrator, Router, and Transport.

Router Agent

A instance of the Commerce Suite application configured to provide routing services including round-robin selection of Transport Agents, message-queuing and fail-over retransmission.

RSA

An internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browser from Netscape and Microsoft.

S

Serializer Service

The set of application tasks that execute within the context of a single thread of execution to serialize the access of shared application resources by other application threads. The Serializer Service is started automatically at application startup and is required by all Commerce Suite Roles. Serialized resources include shared memory areas, directories, and the database.

Service

A discrete set of Commerce Suite application tasks that provide a logical service to the Agent. The Services supported by Commerce Suite are: Serializer, Outbound, Inbound, Control, PKI, work order, User Interface, Out-Beacon, and In-Beacon. Sets of concurrently executing Services are combined to define Commerce Suite Roles.

SHA-1

Specifies the Secure Hash Algorithm used to verify a file's integrity. The SHA-1 generates a condensed representation of a message called a message digest. The SHA-1 is used by both the transmitter and intended received of a message in computing and verifying a digital signature.

S/MIME

Secure MIME - S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send a receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

SMTP

Simple Mail Transport Protocol - An Internet standard for transporting email.

SSL

Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

T

TCP/IP

Transmission Control Protocol/Internet Protocol or the suite of standard protocols that enable computers to inter-communicate on the Internet.

Thread

A logical sequence or program instructions that are executed independently.

Transport Agent

An instance of the Commerce Suite application configured to provide transport services including the compression, encryption and delivery of data, the verification of digital signatures and the construction and transmission of Delivery Notifications.

Triple Data Encryption Standard

Triple Data Encryption Standard (DES3) is a derivative of Data Encryption Standard (DES) that has served as the cornerstone of data encryption for almost 40 years. DES-3 is DES run three times with three different keys. It uses a 192-bit key and has an effective strength of 112-bits.

U

UCC

Uniform Code Council, Inc.

UDP

User Datagram Protocol. A simple, datagram-oriented, transport layer protocol, used by Commerce Suite to facilitate dynamic pools of Transport Agents marshaled by a Router Agent. The Transport Agents use UDP as the underlying protocol to transmit small informative packets of data identifying their inbound protocol ports.

User Interface Service

The set of application tasks that execute within the context of a single thread of execution to return HTML-formatted application-status information to a web-browser. The User Interface Service is not required by any Commerce Suite Role. However, any Commerce Suite Agent can enable the user interface Service so that its current status can be remotely viewed via a Web-browser.

W

work order

A set of one or more Console Commands sent to a Commerce Suite Agent to accomplish one or more specific tasks. The typical use of a work order is to initiate an outbound delivery of data (a send).

work order Service

The set of application tasks that execute within the context of a single thread of execution to query the database or a directory for Work Orders.

X

X.509V3

X.509 Public Key Certificate and CRL Profile, Version 3, defined in CERT. The version of X.509 Public Key Certificate supported by Commerce Suite.