Administrator's Guide

iPlanet™ ECXpert

Version 3.6

December 2001

Contents

List of Figures

List of Tables

List of Procedures

List of Code Examples

About This Book

This Guide explains the concepts, structure, and operation of iPlanet ECXpert, from iPlanet. It also describes iPlanet ECXpert functions and gives you guidelines for administering the system.

This chapter covers the following topics:

- Before You Begin

- The ECXpert Documentation Set

- Audience and Roles

- Organization

- Conventions

ECXpert is subject to the terms detailed in the license agreement accompanying it.

Before You Begin

This Guide is written with the assumption that you already understand the basics of EDI, relational database systems, TCP/IP communications, and the operating system on which you are running this software.

Suggested Supplementary Reading

The following documents and Web sites may be helpful supplements:

- The *iPlanet ECXpert Installation Guide*, for information about installing and configuring the ECXpert System. This and all other ECXpert documents can be downloaded from:

http://docs.iplanet.com/docs/manuals/ecxpert.html

- The iPlanet Support website at

  `http://www.iplanet.com/support/index.html`

  for ECXpert technical support.

- Your operating system manuals, particularly any pertaining to system security.

- The GE Information Services web page, *Introduction to EDI - A Primer*, at:

  `http://www.support.geis/edi/edipindx.html`

- The *Electronic Data Interchange X12 Standards*, for a technical reference on EDI implementation (document no. ASC X12S/95-533, available from the ASC X12 Secretariat, Data Interchange Standards Association, Inc., 1800 Diagonal Road, Suite 200, Alexandria, VA 22314-2852, 703.548.7005).

- *Requirements for Inter-operable Internet EDI*, by C. Shih, M. Jansson, and R. Drummond for a helpful, informational document discussing the requirements for inter-operable EDI, with sufficient background material to give an explanation of the Internet-related issues, at:

  `ftp://ftp.ietf.org/internet-drafts/draft-ietf-ediint-req-08.txt`

  If the above URL is not found, it probably means that a newer version has become available and the previous version has been retired. Try the same URL with the number before the .txt extension incremented by one.

  For example, the next URL to try would be:

  `ftp://ftp.ietf.org/internet-drafts/draft-ietf-ediint-req-09.txt`

- The Inter-operability Test Team's CommerceNet working pages for information about how leading software vendors are conducting inter-operability tests for MIME-based Secure EDI at:

  `http://www.commerce.net/`

- The Gas Industry Standards Board (GISB) site for more information on the specifications supported by ECXpert's GISB HTTP protocol at

  `http://www.NeoSoft.com/~gisb/`

- The GISB Future Technology Task Force team's web pages at:

  `http://www.gisb.org/fttf.htm`

The ECXpert Documentation Set

Refer to other ECXpert books for additional information. This section discusses each book in the ECXpert documentation set.

Release Note

IMPORTANT! After you receive the ECXpert software, download the *iPlanet ECXpert Release Note* for the current version before you do anything else:

http://docs.iplanet.com/docs/manuals/ecxpert.html

The latest Release Note contains the following:

* List of bugs fixed in the current release.

* Warnings and workarounds for known problems.

* Additional important information you should know before you install or use ECXpert.

The *iPlanet ECXpert Release Note* is platform-specific, so make sure you get the version for the platform you are using.

Installation Guide

The *iPlanet ECXpert Installation Guide* is the book you use to install the iPlanet ECXpert. It includes pre-installation tasks—including basic instructions for installing or upgrading to the required version of Oracle—as well as ECXpert installation steps and information on additional tasks you may want to perform after you install ECXpert.

The *iPlanet ECXpert Installation Guide* guide is platform-specific, so make sure you have the version for the platform you are using.

Administrator's Guide

The *iPlanet ECXpert Administrator's Guide* is written for the ECXpert administrator. This book provides an overview of the ECXpert system and how to administer it, discusses the ECXpert command line utilities, and explains how to integrate ECxpert with legacy servers such as SAP and MQSeries.

Developer's Guide

The *iPlanet ECXpert Developer's Guide* is written for C++ developers who want to customize ECXpert. Primarily, it documents the ECXpert APIs that give C++ applications full access to the database. This includes detailed documentation of each class, each method in each class, and code examples. It also documents the complete database schema.

With the release of ECXpert 3.6, a Java Native Interface is now available to build customized java-based applications that present the same information as the ECXpert C++ applications.

Operations Reference Guide

The *iPlanet ECXpert Operations Reference Guide* contains basic troubleshooting guidelines for ECXpert, for other iPlanet products, and for third-party products. It also includes a complete error message reference.

Audience and Roles

This Guide is written for the ECXpert administrator.

Organization

This Guide is structured as follows:

Table 1   Book Contents and Organization

Chapter	Description
Chapter 1, "Introducing ECXpert System"	This chapter introduces the major features and concepts of the ECXpert System.
Chapter 2, "Scenarios for Using ECXpert"	This chapter uses specific examples, or "scenarios," to illustrate the different ways in which ECXpert can be used most effectively in a wide variety of different business situations.

Table 1   Book Contents and Organization *(Continued)*

Chapter	Description
Chapter 3, "Working with the System Administration Interface"	This chapter introduces the ECXpert Product Administrative Interface and provides a "roadmap" for creating trading partnerships and all their supporting components.
Chapter 4, "Using the Product Administrative Interface"	This chapter describes the tasks involved in setting up and maintaining members in ECXpert.
Chapter 5, "Setting Up Members"	This chapter describes the tasks involved in setting up and maintaining members in ECXpert.
Chapter 6, "Setting Up Trading Partnerships"	This chapter describes the tasks involved in setting up and maintaining trading partnerships in ECXpert.
Chapter 7, "Tracking the Documents that ECXpert Processes"	This chapter describes the tasks involved in using the document tracking features of ECXpert.
Chapter 8, "Tracking the Jobs that the Scheduler Manages"	This chapter describes the tasks involved tracking the jobs that ECXpert's time-based Scheduler manages.
Chapter 9, "Working with Certificates"	This chapter describes the tasks involved in working with certificates in ECXpert.
Chapter 10, "Setting Up Services and Service Lists"	This chapter describes the tasks involved in setting up and maintaining services and service lists in ECXpert.
Chapter 11, "Command Line Utilities"	This chapter documents the command line utilities that are available for use with ECXpert.
Appendix A, "Introduction to EDI Concepts"	This appendix provides a brief introduction to basic concepts of electronic data interchange (EDI).
Appendix B, "Constructing and Referencing A Stylesheet for an XML Document"	This appendix describes the data used to reference a stylesheet for XML documents so that ECXpert can pass this information to Parse to identify the partnership and process the documents.
Appendix C, "ECXpert Initialization File (ecx.ini)"	This appendix documents the system settings that you can modify through the ECXpert System's System Administration interface.
Appendix D, "Required Mercator Settings for ANSI Functional Acknowledgment (997)"	This appendix provides detailed information on the Mercator type tree and map settings that are required to make full use of the ECXpert confirmation message capabilities.
Appendix E, "Limitations of ANSI X12 FA (997) Features"	This appendix provides information on the limitations of ANSI X12 Functional Acknowledgment (FA/997) features in ECXpert.

Table 1   Book Contents and Organization *(Continued)*

Chapter	Description
Appendix F, "AIAG Administration"	This appendix provides information on the administration and integration of the AIAG features compatible with the current E-5 2000 standard.
Appendix G, "Odette FTP (OFTP) User's Guide"	This appendix provides detailed instructions for setting up ECXpert file exchanges using OFTP, including use of a scripting a language for X.28 connections and setup of EERP (end-to-end response) reconciliation.
Appendix H, "Integrating ECXpert with Oracle Financials"	This appendix describes the steps necessary to integrate ECXpert with Oracle Financials.
Appendix I, "Integrating ECXpert with SAP"	This appendix describes the steps necessary to integrate ECXpert with SAP.
Appendix J, "Integrating ECXpert with MQ Series"	This appendix describes the steps necessary to integrate ECXpert with MQ Series.
Appendix L, "ANSI X12 Group Types and Codes"	This appendix provides a table of ANSI X12 Group Type (GS01) codes for the different ANSI values for Document Type. Use this Appendix as a reference when entering or interpreting values for **Group Type (GS01)** in the **Group Level Information (ANSI)** section of the Input EDI tab.
Appendix M, "Hexadecimal Character Codes"	This appendix provides a table of hexadecimal codes for reference when entering or interpreting values in the Delimiters and Separators section of the Output EDI tab.
Appendix N, "Mapping UI Fields to Database Columns and Import Fields"	This appendix provides a table indicating each field on the ECXpert user interface, the database column in which data for that field is stored, and the field that should be used to import data into that database column using the ECXpert *import* utility.
"Glossary"	The glossary defines the various terms and concepts of used in the documentation of the ECXpert System.

Conventions

This Guide uses typographic conventions to help you recognize special terms and instructions. Table 2 summarizes these conventions.

Table 2   Typographic Conventions

Convention	Meaning	Example
Initial capital	items on the screen that you manipulate (buttons, links, etc.)	"Click Submit to save your changes."
	names of keys	"Press Enter to clear the message."
	names of iPlanet ECXpert pages	"The main Partnerships page appears."
numbered steps	high-level descriptions of tasks you perform (detailed instructions, if needed, appear in unnumbered paragraphs immediately below the numbered paragraph)	1. Enter the group information. Type the name in the Group Name field and a short description in the Description field.
Palatino italic	key words, such as terms defined in the text	"The messages posted to a Usenet newsgroup are called *articles*."
	names of books	"For more information, refer to the *iPlanet ECXpert Installation Guide*."
Courier italic	variables in command syntax	"In the following example: `nsusrgrp [-v] insert [-l] -k` *key arguments* `-r` `act=`*relation action* substitute valid values for italicized items."
`Courier`	file names	"The associated data is stored in the `ubidubi.ini` file."
	text file content (HTML templates, config files)	*TITLE* `Password Check` */TITLE* `IMG SRC="/icons/hd_svcs.gif"`
	code samples	**Syntax** `const char* getName() const`
	URLs	"Go to the following site: `http://www.commerce.net`"
courier bold	command line input	"Type the following command: `ls *.mle`"
	what a user types in a dialog box or other space (data entry field, etc.)	**Walmart Weekly Orders**

Table 2   Typographic Conventions *(Continued)*

Convention	Meaning	Example
square brackets, [...]	In command syntax, items within square brackets are optional.	"In the following example:
vertical line (|)	In command syntax, items on either side are valid *alternatives*.	`nsusrgrp [-v] insert [-l] -k` *key arguments* `-r` `act=`*relation action* ,
		`usrid=`*ID*|`usrlogin=`*login*
		1. *-v* and *-l* are optional.
		2. You may specify either *usrid* or *usrlogin*
em dash (—)	"none" or "nothing"	Arguments: —

Introducing ECXpert System

This chapter introduces the major features and concepts of the ECXpert System. At the highest level, these topics are:

- Benefits of Using ECXpert

- Installing and Configuring ECXpert

- Overview of ECXpert Components

- Document Submission Methods

- Implementing OBI Support for BuyerXpert and SellerXpert

- Implementing HTTP SSL Support for XML

Benefits of Using ECXpert

This section gives an overview of how using iPlanet ECXpert to exchange business documents can benefit your enterprise.

ECXpert Expedites

iPlanet ECXpert lets organizations exchange commerce information quickly and easily over the Internet or over existing private networks, in support of business processes. It provides for documents and messages to be encrypted and transmitted among trading partners whose systems may be dissimilar, and it can transform information from one format to another.

By combining iPlanet ECXpert's powerful security features and data transformation capabilities with the widespread availability, high speed, and low cost of the Internet, a Global 2000 firm can expand its trade relationships among a broader array of small-to-medium-sized firms (either directly or through a service provider) -- and can at the same time lower the overall cost of the transactions that support such relationships.

Expands Trading Communities

With ECXpert, an enterprise or organization can define extranet trading communities that are based on trading and transaction workflow requirements, instead of based on what technology is available.

ECXpert lets an organization administer and manage trading communities, under appropriate controls, from anywhere on the Internet. This flexibility allows trading communities to be defined dynamically, to keep up with changing trade patterns and relationships.

Streamlines Cross-Company Communications

Transactions across trading partnerships are simpler because iPlanet ECXpert supports extensive standard communication and security protocols and a growing list of industry-specific standards. ECXpert also supports industry groups standardizing on the Internet, such as the Automotive Industry Action Group (AIAG) and the Gas Industry Standards Board (GISB).

Simplifies Information Exchange

iPlanet ECXpert's capabilities for flexible data exchange and data transformation, plus its broad back-end connectivity, make interchanges between partners faster and easier to coordinate. It supports hundreds of EDI formats and provides tools to transform almost any document from one format to another.

In addition, ECXpert provides (optional) certified interfaces with SAP R/3 and further connectivity through IBM's MQSeries middleware.

Speeds Throughput

ECXpert lets enterprises pre-define processing operations and transactions for each partner and customer so that transformations, routings, queries, and other actions are handled successfully for both EDI and non-EDI-based transactions and transactions that exchange XML data.

The processing engine automatically generates appropriate event notifications and acknowledgments for each transaction, and maintains an audit trail of activity.

Using ECXpert as the channel for all incoming and outgoing messages ensures that all transactions are handled completely and properly. It also reduces cycle time, increases productivity, and improves accuracy.

Figure 1-1   ECXpert System Interaction with Trading Partner
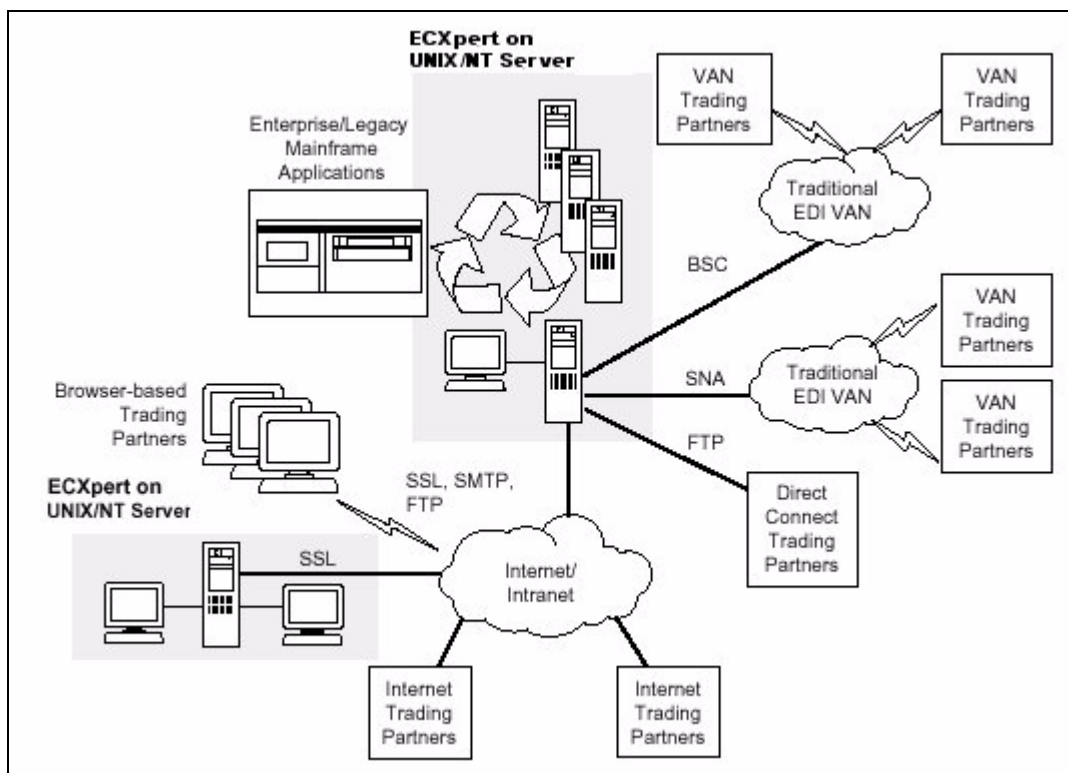
Installing and Configuring ECXpert

This Guide covers the administration and daily operation of the ECXpert System after the initial installation and configuration have been successfully completed. Refer to the manuals listed below for information not contained in this Guide:

- *iPlanet ECXpert Installation Guide*, for complete instructions on installing and configuring ECXpert. This manual covers all aspects of installation of ECXpert and the supporting Oracle database.

- *Mercator User's Guide*, for instructions on installing and using the *Mercator* map generation package.

Overview of ECXpert Components

The major components of ECXpert are diagrammed in Figure 1-2. The roles played by each of these components in ECXpert processing are described in the sections that follow.

Figure 1-2   Major components of ECXpert
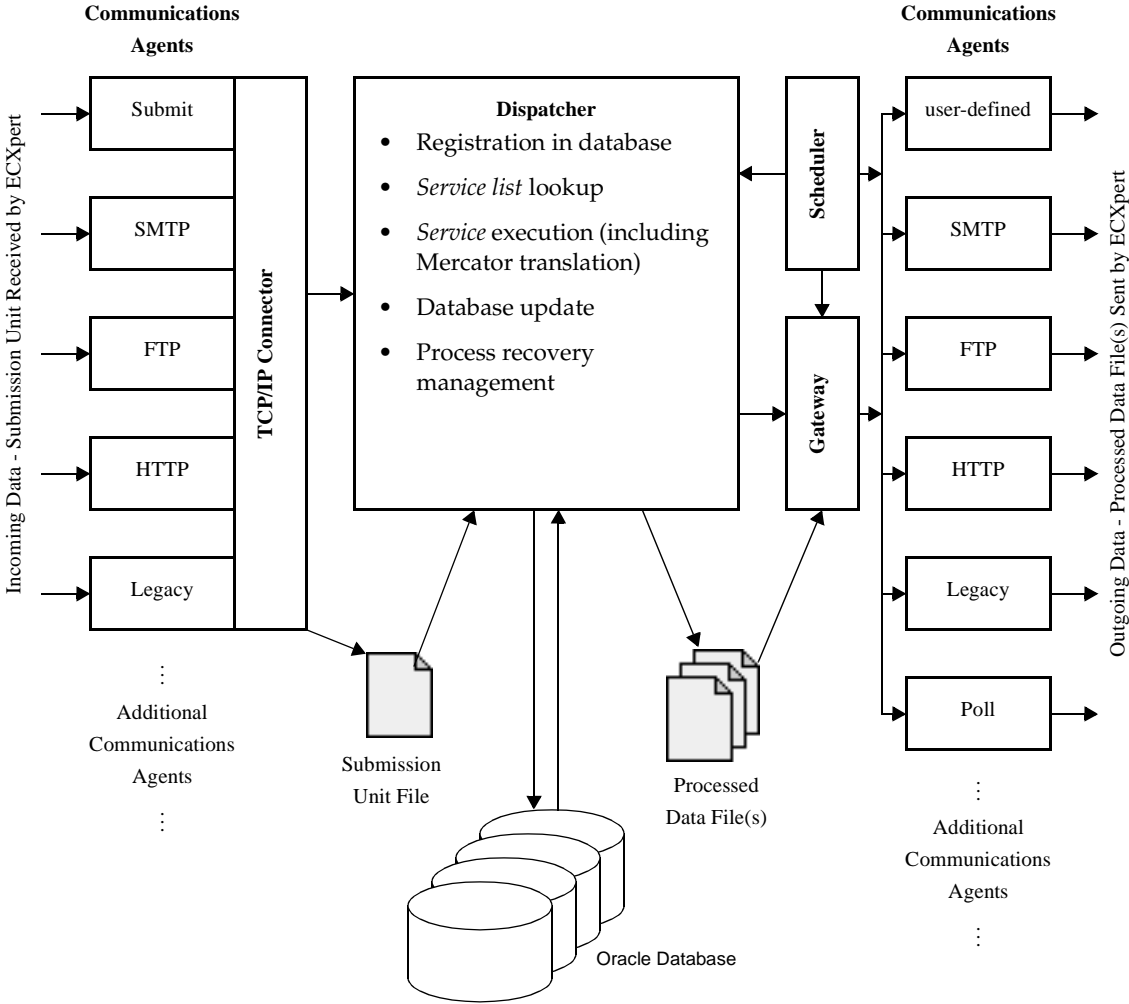
ECXpert Database

The ECXpert Database contains two kinds of information:

- **Trading partnership infrastructure**—information that sets up trading partnerships and specifies how different types of documents exchanged between trading partners are to be processed. The infrastructure for a trading partnership must be set up before ECXpert can process documents being exchanged under that partnership.

- **Data about documents being processed**—information about all the data that is being processed by ECXpert; the documents being exchanged under trading partnerships that have been set up.

Separate disk files are used to store each incoming submission unit from a trading partner that has been received and each outgoing submission unit to a trading partner that is ready to be sent.

When a file is received in inbound processing, no new files are created to store the document(s); instead a record is created in the database for each document and each component of any EDI enveloping structure.

Communications Agents

A separate Communications Agent exists for each type of communications protocol that ECXpert supports. A Communications Agent simply receives the incoming data, or sends the outgoing data, using the communications protocol for which it was designed: SMTP, FTP, HTTP, and so forth. Users may also define custom communications agents to handle additional communications protocols.

All Communications Agents pass the incoming data they receive immediately on through the TCPIP Connector to the Dispatcher, and they pass the outgoing data they receive immediately on to the communications port.

For a complete list of the Communications Agents supplied with ECXpert, see "Selecting the Right Communications Protocol" on page 222.

For other communications protocols, you can create a custom Communications Agent. Refer to the *iPlanet ECXpert Developer's Guide* chapter on "Creating a User-Defined Communications Agent" for more information.

The submit utility acts as a manual Communications Agent for submission units that, for whatever reason, do not arrive through an actual Communications Agent. Especially useful for testing, the submit utility can be run several different ways:

- **Administrative Interface**—see "Using the ECXpert Utilities" on page 181 for details.

- **Command line**—see "submit—Submitting Files to ECXpert" on page 490 for details.

- **EcxSubmit API**—see the *iPlanet ECXpert Developer's Guide* chapter on "The EcxSubmit Class" for details.

For a summary of all the methods supported for submitting incoming document files to ECXpert, see "Document Submission Methods" on page 54.

Dispatcher

Except for receipt of incoming data, most of the processing that occurs within ECXpert is done by the Dispatcher. A separate instance of the Dispatcher manages the processing of each submission unit.

The Dispatcher is a "service list processing engine" for ECXpert. When the Dispatcher receives a submission unit to be processed by ECXpert, it performs the following tasks:

1. **Registration in Database**—Dispatcher creates a record in the database for each document in the submission unit; the database record contains pointers to the source data in the submission unit file, plus fields to track the processing status of the document.

2. **Service List Lookup**—based on the Sender, Receiver, and Document Type, the Dispatcher looks up the associated service list in the database.

3. **Service Execution**—Dispatcher executes in sequence the individual services specified in the service list.

4. **Database Update**—Dispatcher updates the database record for each document in the submission unit upon completion of each service.

NOTE   The Dispatcher also recovers any processing that was aborted before successful completion. Based on the information updated in each document's database record, the Dispatcher is able to determine exactly which services were performed on which documents and resume processing with only those services that still need to be completed.

The steps to initiate processing are covered in "Reprocessing an Item that Failed" on page 373.

What is a Service?

A service is an executable script or program file used to perform a function on a submission unit or a subset of documents in a submission unit.

ECXpert provides internal (standard) services that are available as soon as the software is installed. ECXpert also supports external, user-defined custom services to perform processing that is not provided by a standard service.

Standard ECXpert Processing Services

The standard services that ship with ECXpert are available as soon as ECXpert is installed. These handle most of the common processing tasks involved in EDI processing. Table 1-1 describes the standard services provided by ECXpert.

Table 1-1   Standard ECXpert services

Service	Description
Parse	Logically breaks incoming EDI into its constituent parts.
Translate	Converts submission unit documents from one format to another.
FAGen (incoming EDI)	Creates EDI acknowledgments—only used when incoming data is EDI.
OutPrep	Used to submit a file to ECXpert to be forwarded (for example, to a VAN) without additional processing by ECXpert.
Routing	Specifies how to submit secondary output to ECXpert when there are multiple output cards from a Mercator map.
Split	Splits an incoming EDI submission unit into separate submission units for each interchange, so that the interchanges may be processed by different service lists.
Gateway	Triggers the sending of finished submission units.

Error Services

ECXpert also ships with three message notification services. These services provide feedback to users about errors that are detected following execution of a service or a service list. When any of these services are used, an exit service will also be used by default when an error is found within the selected error service's query scope.

Depending upon your site's implementation, the exit service can include in its list the generation of an email or other communication feedback to designated parties of the processing error.

An implementation example can be illustrated in this way:

Suppose the Notify Errors/Warnings service is setup after the Gateway service. A script has been written that has the ability to trigger off an email to a particular division or a set of people with the tracking id and a message.

The script is used to provide a relationship between the Notifiy Errors/Warning service and its associated exit service.

At runtime, all the services in the service list are executed, one by one. When the Notify Errors/Warnings service is encountered - a database call is made for that tracking ID to see if there were any errors with serverity >=20. If any are found, a hard fail occurs and the exit service list is triggered off.

The script associated with the exit service is now initiated and the email is sent.

Table 1-2 describes each type of message notification service provided by ECXpert.

Table 1-2   ECXpert Error Detection Services

Service	Description
Notify Error	Provides error information.
Notify Errors/Warnings	Provides both error and warning information.
Notify All	Provides data for information notifications and for errors and warnings. *Note:* This service should always be put at the end of your service list.

You can add an Error Service following a standard service such as Parse, Translate, Gateway, or Split. You can also add an Error Service at the end of the service list. When using FA Gen as one of the standard services in the service list, put the desired error service following FA Gen as opposed to after some other service in the service list.

Custom Services

Users can define custom services to handle any processing that is not accommodated by the standard services built into ECXpert. Many custom services can be created without the use of the ECXpert APIs. Any executable that performs the desired processing can be plugged in as a custom service.

For information on creating custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on "Creating a Custom Service."

Types of processing typically performed by user-defined custom services include the following:

• **Encryption and decryption**—to support a non-S/MIME standard, such as PGP, you and your trading partners agree to use specific encryption and decryption routines.

- **Compression and decompression**—to support whatever data compression algorithms you and your trading partners agree to use to make data transport more efficient.

- **Data moving and copying**—creating archival copies of data at various stages of processing for auditing, reporting, or other special purposes.

Service Lists

A user-defined *service list* that is specific to each session/user/trading partnership/document type combination tells the Dispatcher the specific services to perform and their sequence. The individual services are processes like data decompression, decryption, XML parsing, EDI parsing, and EDI translation.

Any and all processing that is to be performed on data passing through the ECXpert System must be specified ahead of time in the Service Lists component. Each individual *service* is a single processing task.

All services that must be performed on a submission unit passing (inbound or outbound) between ECXpert on your system and a trading partner's system must be specified, in sequence, in a *service list*. The ECXpert Dispatcher simply manages the service list associated with the particular document currently being processed.

Service lists are maintained through the Product Administrative Interface. See Chapter 10, "Setting Up Services and Service Lists"," for more information.

Mercator Map Authoring System

The Mercator Map Authoring System is used to create a *map file* that the Map Execution Engine can use. Maps from other sources, such as maps that have been in use by legacy systems, can also be used by ECXpert. See "Setting up Mapping and Translation" on page 69 for more information.

The Mercator Map Authoring System that is currently bundled with ECXpert is the *Mercator Authoring System*, developed by TSI International. The Mercator Map Authoring System can produce map files that translate from any supported format to any other supported format: EDI to proprietary, proprietary to EDI, XML to EDI, proprietary to XML, EDI to EDI, and proprietary to proprietary.

The *Mercator* mapping tool runs under Windows NT or Windows 95/98. The map files produced may be used on any platform supported by ECXpert. More information on Mercator can be obtained from the *Mercator User's Guide*, and from the Mercator web site at:

http://www.tsisoft.com/

Map Execution Engine

ECXpert's Map Execution Engine incorporates the Mercator map execution engine as its core.

This Map Execution Engine uses a *map file* created by the Mercator Map Authoring System to translate documents from a proprietary format to a standard EDI format, or from a standard EDI format to a proprietary format. In addition, XML data formats are supported with the current release of the Map Execution Engine. A map file details precisely how the data elements in a business document from one system must be represented in order to be processed correctly by another system.

The ECXpert Gateway Service

The ECXpert Gateway service is a service that deserves special mention because it is the most common means by which ECXpert sends out processed documents. Documents sent out via the Gateway service are sent as soon as the all the documents in the submission unit to which they belong complete processing.

The Gateway service automatically performs appropriate "bundling" or enveloping of EDI data, combining individual translated documents into larger groupings that can be transmitted as a unit. The Gateway service passes processed documents on to the appropriate Communications Agent for outgoing transmission.

The ECXpert Scheduler

The ECXpert Scheduler is used to send processed documents out on a specified time-based schedule. The Scheduler is used primarily for batch-oriented processing.

Document Submission Methods

The different methods available for submitting business documents to ECXpert for processing are summarized in Table 1-3.

Table 1-3   Available methods for submitting documents to iPlanet ECXpert.

Method	Description
submit command	The submit command is a separate program that takes a submission unit file from a specified location and submits it to ECXpert for processing.
	For information on using submit from the command line or in a script file, either locally or remotely, see "submit—Submitting Files to ECXpert" on page 490.
	For information on running submit through the ECXpert Administrative Interface, see "Using the ECXpert Utilities" on page 181.
SMTP Communications Agent	The SMTP Communications Agent automatically submits incoming submission units to ECXpert as soon as they are received.
ECXpert **FTP** Server	The ECXpert FTP Server allows you to submit files to ECXpert remotely via FTP.
	For information on using the ECXpert FTP Server, see the *iPlanet ECXpert Operations Reference Guide* topic on "Using the ECXpert FTP Server." This section also explains how to get a file from ECXpert via the FTP Server.
ECXpert **Legacy** Server	The ECXpert Legacy Server supports submission of files originating from SAP and MQSeries.
	For information on using the ECXpert Legacy Server with SAP, see Appendix I, "Integrating ECXpert with SAP." If you want to use the Legacy Server with MQSeries, see Appendix J, "Integrating ECXpert with MQ Series."
FTP via **Scheduler**	The ECXpert Scheduler submits incoming files to ECXpert via FTP on a specified time-based schedule.
	For information on using the ECXpert Scheduler, see "Scheduling ECXpert Jobs" on page 155.
HTTP Communications Agent	The HTTP Communications Agent handles standard HTTP communications.

Table 1-3   Available methods for submitting documents to iPlanet ECXpert.

Method	Description
HTTP SSL for OBI Communications Agent	Handles OBI communications over SSL.
HTTP SSL for XML Communications Agent	Handles HTTP that conforms to the XML standard over SSL.
HTTP for AIAG Communications Agent	Handles HTTP that conforms to the AIAG standard.
HTTP for GISB Communications Agent	Handles HTTP that conforms to the GISB standard.
JMS-Receive Communications Agent	Handles retrieval of Java Message Service (JMS) messages delivered to ECXpert by way of a JMS provider.
GEIS FTP Communications Agent	Handles FTP that conforms to the GEIS standard.
ECXpert SDK	The `EcxSubmit` API, included in the ECXpert SDK, is based on the NAS architecture and allows programs that incorporate it to submit document files to ECXpert directly. For more information on the `EcxSubmit` API, refer to the *iPlanet ECXpert Developer's Guide* chapter on "The EcxSubmit Class."

Implementing OBI Support for BuyerXpert and SellerXpert

Follow the steps below to set up ECXpert to use the enhanced OBI support for SellerXpert and BuyerXpert. Refer to Figure 1-3.

Figure 1-3   Connections between ECXpert systems supporting BuyerXpert and
SellerXpert
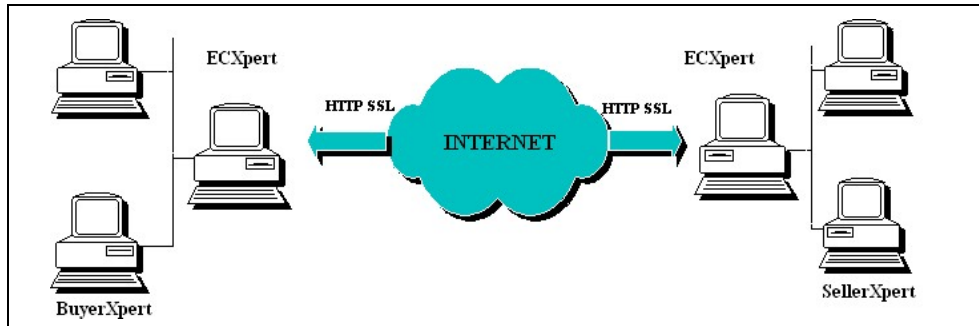
Creating and Configuring Web Servers to Support SSL

1. Obtain a server certificate for the Netscape Enterprise Server that was installed
   with each of the ECXpert systems.

   Refer to the iPlanet's Web Server Help facility for details on how to apply and
   import a server certificate.

2. On each of the ECXpert systems, create a new web server listening on a
   different port number.

   This port number is different than the one that was used for the ECXpert
   Administration Server. The new web servers are configured to support SSL
   with the following configurations:

   ❍ Encryption support should be turned on. To turn on Encryption for the
     Web server, go to the individual web server admin page and select
     "Encryption On/Off" tab.

   ❍ Configure the CGI directory for each Web server to point to the cgi-bin
     path of the ECXpert installation. To do this, click Programs in each
     individual web server admin page and enter the necessary information.

   ❍ Modify the obj.conf file of this server to add the LD_LIBRARY_PATH entry
     by copy and paste from the obj.conf file of the ECXpert admin server
     (this file is in your ECXpert installation ../ns-home/https-xxxx/config
     directory).

   ❍ Select the "Encryption preferences" tab, and click the Yes radio button for
     the Require client certificates (regardless of access control) option.

Setting Up ECXpert

1. Modify the ecx.ini files on both ECXpert systems.

   Set mmap_path and lock_path to point to a path where the SellerXpert and BuyerXpert can get to on their local network. This can be done by exporting the directory where the ECXpert systems are installed as NFS volumes.

2. Restart the ECXpert systems.

   After the modifications are made, the ECXpert systems must be restarted in order for the changes to take effect.

3. Grant read and write permissions to ECXpert.map and ECXpert.lock files to all groups.

   Go to the directory where the log files are logged and change the mode of ECXpert.map and ECXpert.lock files to have read and write permission for all users and groups. The SellerXpert and BuyerXpert need to have write access to these two files.

4. Obtain a Verisign Class 3 certificate for the member that is going to be used for trading on both machines.

   Refer to "Getting a Certificate for a CA" on page 436 for details on how to request and import the Verisign Certificate. The steps to obtain certificates from other CAs would be similar. As long as the CA is trusted by the web server, the certificate is secure for ECXpert users to use.

5. Set up trading partnerships on ECXpert with configurations as follows:

   ❍ Enter the necessary information for setting up partnerships, such as the map to be used and the version number.

   ❍ Use "HTTP SSL for OBI"as the communication protocol for the sending partnership with settings:
   - Port number = *port # of Web Server supporting SSL*
   - CGI Path = *the cgi path set up in the web server to point to ECXpert's cgi-bin directory*
   - sender certificate type = Verisign Class 3

   ❍ Create a receiving partnership on the other ECXpert system with appropriate configuration in order to process incoming OBI documents.

Implementing HTTP SSL Support for XML

Follow the steps below to set up ECXpert for use with inbound XML documents over HTTP SSL.

Creating and Configuring a Web Server to Support HTTP SSL for XML

1. Obtain a server certificate for the iPlanet Web Server that was installed with each of the ECXpert systems.

   Refer to the iPlanet's Web Server Help facility for details on how to apply and import a server certificate.

2. On each of the ECXpert systems, create a new web server listening on a different port number.

   This port number is different than the one that was used for the ECXpert Administration Server. The new web servers are configured to support SSL with the following configurations:

   ❍ Encryption support should be turned on. To turn on Encryption for the Web server, go to the individual web server admin page and select "Encryption On/Off" tab.

   ❍ Configure the CGI directory for each Web server to point to the cgi-bin path of the ECXpert installation (e.g., `$BDGHOME/ECXpert/cgi-bin`). To do this, click Programs for each individual web server admin page and enter the necessary information.

   ❍ Ensure the SSL Web Server is configured with the location of the ECXpert shared libraries. To do this, modify the obj.conf file of this server to add the `LD_LIBRARY_PATH` environment variable and have it point to `$BDGHOME/ECXpert/lib`.

   ❍ Select the "Encryption preferences" tab, and click the Yes radio button to require the client certificate presentation (regardless of access control) option.

ECXpert Settings

1. Obtain a Verisign Class 3 certificate for the member that is going to be used for trading on both machines.

    Refer to "Getting a Certificate for a CA" on page 436 for details on how to request and import the Verisign Certificate. The steps to obtain certificates from other CAs would be similar. As long as the CA is trusted by the web server, the certificate is secure for ECXpert users to use.

2. Set up trading partnerships on ECXpert with configurations as follows:

    ❍   Enter the necessary information for setting up partnerships, such as the map to be used and the version number.

    ❍   Use "HTTP SSL for XML" as the outgoing communication protocol for the sending partnership with settings:

        - Port number = *port # of Web Server supporting SSL for XML*
        - CGI Path = *the cgi path set up in the web server to point to ECXpert's cgi-bin directory*
        - sender certificate type = Verisign Class 3

    ❍   Create a receiving partnership on the other ECXpert system with appropriate configuration in order to process incoming XML documents.

Scenarios for Using ECXpert

This chapter uses specific examples, or "scenarios," to illustrate the different ways in which ECXpert can be used most effectively in a wide variety of business situations.

The following topics are covered:

- Scenarios—Different Ways of Using ECXpert
- Exchanging XML Documents
- Pass-through: Incoming CAD/CAM Files, No Processing
- Application to Application: Incoming PeopleSoft to SAP
- Using the Split Service
- Incoming EDI with Multiple Outputs Routed to Appropriate System
- Integrating ECXpert with MQSeries
- Using TradingXpert
- The ECXpert Demo Data

Scenarios—Different Ways of Using ECXpert

The ECXpert System has been designed to be extremely flexible. In the exchange of electronic business documents, ECXpert allows you to do almost anything you want, in almost any way that you or your trading partners require. This section describes a number of "scenarios," or specific ways in which ECXpert can be used.

Organizations typically use ECXpert in several different ways, so several of these scenarios might be relevant to your organization. Also, your organization might transition through different scenarios over time, as you take advantage of more and more of the functionality that ECXpert supports.

Exchanging XML Documents

XML documents can be sent and received through ECXpert. In order for you to process XML documents through ECXpert, you should understand how XML documents are processed through ECXpert, as described in "XML Document Processing Through ECXpert" on page 62. This will give you an idea of the key information that must accompany an XML document so that ECXpert can pull the key information and submit it to the XML Parser to form the partnership relationship and obtain the mapping information and communication services to be used for the outgoing, processed submission.

To access a working example of processing an XML document through ECXpert, using an XML to EDI Partnership Type, refer to "XML To EDI Processing Scenario" on page 66.

XML Document Processing Through ECXpert

ECXpert has many features that make translation to and from XML documents extremely flexible. This section provides you with information about XML structures and DTDs and how they are used to leverage these capabilities through ECXpert.

Understanding DTDs

A DTD is a Document Type Definition. It defines the rules for XML documents. DTDs are used to add structure and logic to make it easier to understand what the elements in an XML document mean. DTDs are not required for XML documents, nor are they required when using ECXpert.   For ECXpert, the DTD is important at the time you are creating the definition for the input or output XML formats.

Mercator 5.0 has features that make the mapping process for XML documents simpler than it was in previous versions. The main feature for XML is the ability to import a DTD in order to create a Type Definition. The Type Definition can then be used by a map as the source or target. This greatly reduces the time it takes to make the definition known to Mercator.

Historical Use of the Parse Service and Key Data

Parsing has many meanings in relation to ECXpert and XML data. In previous versions of ECXpert, the Parse service allowed ANSI X12, EDIFACT, and HREC/TREC wrapped data to contain the key values for sender, receiver, document type, version, and so forth. This allowed for general Sender, Receiver, Document Type to be used on the Submission of data to ECXpert. The data itself contained the key information as to which map and communication protocol to pick up.

Introducing the ECXParser

As of ECXpert 3.5, the ECXParser adds to the existing parser functionality by allowing it to recognize and parse XML documents as well. It reuses previously written code to parse the EDI and HREC data. New logic has been added to handle XML documents. The basics of understanding XML data and obtaining the relevant information are as follows:

The input file can contain multiple documents (XML or otherwise). XML documents should have the stylesheet information OR the document type (the DTD) of the XML document. Refer to the section "XML To EDI Processing Scenario" on page 66 for an example of a stylesheet and XML data.

How ECXpert Uses Stylesheets

Stylesheets are used in ECXpert to relate XML data sent to or from a Trading Partner to the key vales required by ECXpert to look up a partnership to access mapping and communication information.

XML does not have the rigid structure of the types of documents previously "Parsed" by ECXpert. However, ECXpert 3.6 gives you the same capability through use of Stylesheets and a structured Parsing routine.

Figure 2-1   XML Parsing Logic
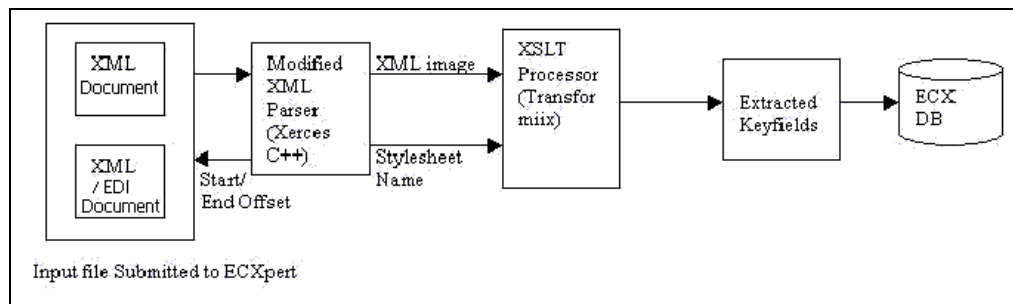
The ECX parser thus performs the following parsing logic, as shown in Figure 2-1.

Document Boundaries Determination

The parser goes through a given xml file to recognize document boundaries. For each recognized document, the appropriate parser is instantiated. The parser is then responsible for gathering information like document offsets, senderid, receiverid, doctype and other trading partnership information, and writing that information as a record, to the database.

The ECXpert parser identifies the boundaries of a XML document in a file as follows:

- it looks for the XML prolog to find the start of document, as shown in the section, "XML To EDI Processing Scenario" on page 66 under the heading Sample Data.

- the end of the document is identified by an XML parser, using the rules in the XML specification.

Once the document boundaries are obtained, an image of the document is obtained and relevant data is extracted from it.

Extraction of Key Information

Relevant data is extracted from the XML document as follows:

- each XML document must specify a corresponding stylesheet. An XML document submitted without a stylesheet specified is an erroneous submission.

- the stylesheet extracts key information from the incoming XML document; this information is represented in ECXpert format using XML. Refer to the sample output in the section "XML To EDI Processing Scenario" on page 66 under the heading Sample Output Data. This format contains information like the senderid, receiverid, doctype, and so forth.

- the converted document is then used to write information to the database. (Default values can be extracted from the stylesheet and other partnership key information is retrieved from Input XML Data)

ECXpert Parsing Look-up Logic

The iPlanet ECXpert parser uses particular look-ups to get to the information that it requires. It scans the XML document for DOCTYPE (public and system) and the stylesheet (indicated by an ecxstylesheet processing instruction). It is not required that all of the above (doctype public, doctype, system, processing instruction) be present.

The following sample code illustrates the subsequent steps.

```
if we have a stylesheet name
    get the stylesheet,
    transform the document using the stylesheet,
    parse the transformed document to get the sender, receiver,
document type.

else if we have the DOCTYPE public ID
    get the mapping to a stylesheet name from the ini file,
    if we have a mapping
        get the stylesheet,
        transform the document, using the stylesheet,
        parse the transformed document to get the sender,
receiver,
    document type.
    else
        get the list of plugins (from the ini file,
ecxstylesheets.xml),
        for each of the plugins
            load it, initialize it using the parameters from the
ini
    file.
            ask the plugin to find the stylesheet for the doctype,
            if we get the stylesheet
                transform the document using the stylesheet,
                parse the transformed document to get the sender,
     receiver, document type.
else if we have the DOCTYPE system id
    perform the same set of steps as done for the public id

else
    Fail Parse
```

Getting Stylesheet Name from External Library (PlugIn)

The list of plugins is listed in the file `$BDGHOME/config/ecxstylesheet.xml`. The plugins are libraries containing the following functions:

```
init(char **, char **, int): this function is called to initialize the
   library.
                char** : the names of the initialization parameters.
                char** : the values of the initialization parameters.
                int : the number of parameters
         getUserDefinedStyleSheet(char**, char *, int*): used to get the
   stylesheet
                char** : the stylesheet that was found.
               char* : the identifier for which the stylesheet is required.
                int* : the status of the operation

         cleanUp(): used to indicate cleanup to the library.
```

The plugins are loaded in the order listed in the `$BDGHOME/config/ecxstylesheet.xml`, initialized using the `init` function and then executed using the `getUserDefinedStyleSheet` function to get the required stylesheet. Once the stylesheet is found the search is abandoned. The `cleanUp` function is called once to complete the plugin loading operation.

XML To EDI Processing Scenario

For this processing scenario, Company "Sender1" has a Web Purchasing system and would like to send orders electronically to a supplier, "Receiver1". The Web Purchasing system of Sender1 outputs XML formatted purchase orders based on the OBI version 3.0 specification. Receiver1 processes Purchase Orders only in ANSI X12 version 3040. The two are interested in doing business so a translation between the XML Purchase Order and the X12 850 must take place.

The Web Purchasing system of Sender1 will submit the XML document to ECXpert. ECXpert will Parse the data, determine that it is Purchase Order data bound for Receiver1, call the appropriate translation map, then send the data to Receiver1.

Before any set up is done in ECXpert, the OBI XML format should be analyzed along with the ANSI X12 850 and a Mercator 5.0 map created to translate the data.

In order to understand how ECXpert should be set up, first look at the XML document that will be submitted, as shown in "Sample Data" on page 72. This document references a DTD that describes the type of data that is in the file. In this instance, the DTD reference is "OBIXMLPurchaseOrder.dtd". The sender and receiver ID Numbers are found in the body of the document. Here you can see "ABC1" as the sender and "XYZ1" as the receiver.

Since there are many flavors of XML, ECXpert has a mechanism to define where the partnership information should be pulled from the XML document. The DTD reference provided in our input data is used as a key to find the stylesheet in ECXpert so that the sender and receiver key data can be pulled from the document. (An example of this stylesheet is in the section "Stylesheet example, xmlpo.xsl" on page 79). The input data, along with the stylesheet, are passed to a routine that creates an XML key structure that in turn is used to find the partnership that indicates the map and communication protocols to be used.

Steps to complete the process in ECXpert

1. Create the map.

   a. Create the input definition. (Since Mercator 5.0 can import a DTD, the input definition can be created in a matter of minutes.)

   The OBIXMLPurchaseOrder.dtd DTD is included in the section "OBIXMLPurchaseOrder.dtd" on page 80).

   b. Create the output definition (Since this is ANSI X12 data, the definitions are pre-built. See the Mercator documentation)

   c. Drag and Drop the source data to the target in the Mercator 5.0 authoring tool.

   d. Test on the desktop.

   e. Build the map for Solaris.

   f. Place any cross reference files in the ECXpert/data/input directory (e.g. helper.txt).

   g. Place the map in the /maps directory of ECXpert.

2. Create the xmlpo.xsl stylesheet in the ECXpert/data/stylesheet directory. Refer to the section "Stylesheet example, xmlpo.xsl" on page 79.

   a. Modify the ecxstylesheets.xml document in the ECXpert/config
   directory to form a relationship between the name of the DTD and the
   name of the stylesheet. Refer to the section "Sample Data" on page 72.

NOTE	The DTD itself does not have to be available at runtime.

3. Create the Members in the ECXpert Members tab (Sender1 ZZ:ABC1 and
   Receiver1 ZZ:XYZ1)

4. Create the Partnership in the ECXpert Partnership tab of the Support User
   Interface.

Figure 2-2   Specifying the Partnership Details

   a. Specify the Partnership Details as shown in Figure 2-2.

Figure 2-3 Specifying the Input XML Parameters

b. Specify the Input XML parameters as shown in Figure 2-3.

Figure 2-4   Specifying the Output EDI Parameter

c.   Specify the EDI Envelope as shown in Figure 2-4.

Figure 2-5 Specifying the Service List
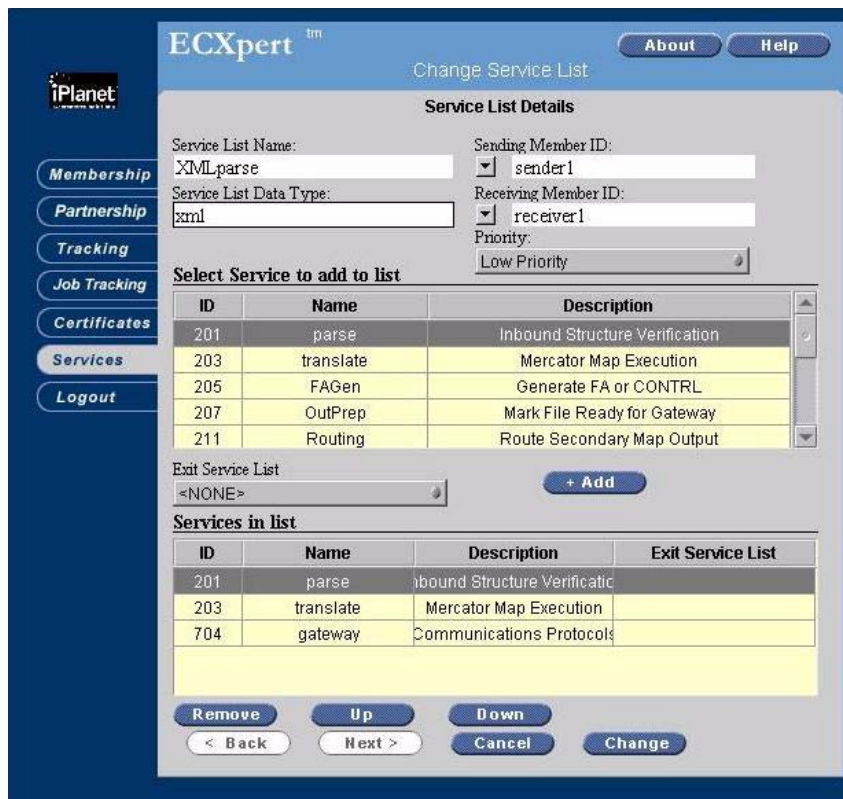
5. Create the Service List in the ECXpert Services tab. Specify Parse, Translate, and Gateway, in that order, as shown in Figure 2-5.

6. Run the sample data and view the output. Refer to the section "Sample Output Data" on page 81.

Sample Data

Code Example 2-1   Sample Data *(1 of 7)*

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE OBIPurchaseOrder SYSTEM 'OBIXMLPurchaseOrder.dtd'>

<OBIPurchaseOrder version="2.1" xml:language="1.0" revision="1">
  <Envelope>
    <Sender>
      <NamingAuthority>ZZZ</NamingAuthority>
      <PartnerName>ABC1</PartnerName>
      <Password>ZZZ</Password>
    </Sender>
    <Receiver>
      <NamingAuthority>ZZZ</NamingAuthority>
      <PartnerName>XYZ1</PartnerName>
    </Receiver>
    <TransmissionDateTime>ZZZ</TransmissionDateTime>
    <EnvelopeID>ZZZ</EnvelopeID>
  </Envelope>
    <PurchaseOrder>
      <POHeader>
  <OrderNumber> xyz0000000001abc </OrderNumber>
  <OrderDate> 10/10/2000 </OrderDate>
  <BuyingParty>
    <Organization>
      <Name> mercury.com </Name>
      <Address>
        <AddressLine1> 2000 Happy Street, Office 2000
      </AddressLine1>
        <City> Sunnyvale </City>
        <StateOrProvince> CA </StateOrProvince>
        <PostalCode> 94385 </PostalCode>
        <CountryCode> USA </CountryCode>
      </Address>
    </Organization>
    <ContactInfo>
      <Contact>
        <FirstName> Bugs Bunny1 </FirstName>
        <EMail> bugsbunny1 </EMail>
      </Contact>
    </ContactInfo>
  </BuyingParty>
  <RequisitioningParty>
    <Organization>
      <Name> mercury.com </Name>
      <Address>
        <AddressLine1> 2000 Happy Street, Office 2000
      </AddressLine1>
        <City> Sunnyvale </City>
        <StateOrProvince> CA </StateOrProvince>
        <PostalCode> 94385 </PostalCode>
```

Code Example 2-1 Sample Data *(2 of 7)*

```
      <CountryCode> USA </CountryCode>
    </Address>
  </Organization>
  <ContactInfo>
    <Contact>
      <FirstName> Bugs Bunny2 </FirstName>
      <Telephone> 1231231234 </Telephone>
    </Contact>
  </ContactInfo>
</RequisitioningParty>
<BillToParty>
  <Organization>
    <Name> mercury.com </Name>
    <Address>
      <AddressLine1>2000 Happy Street  </AddressLine1>
      <City> Sunnyvale</City>
      <StateOrProvince> CA </StateOrProvince>
      <PostalCode> 94385 </PostalCode>
      <CountryCode> USA </CountryCode>
    </Address>
  </Organization>
  <ContactInfo>
    <Contact>
      <FirstName>Jackie Li</FirstName>
      <EMail> jackie.li@sun.com </EMail>
      <Telephone> 888-8888888 </Telephone>
    </Contact>
  </ContactInfo>
</BillToParty>
<SellingParty>
  <Organization>
    <Name> staples </Name>
    <Address>
      <AddressLine1> 1000 Lucky Street </AddressLine1>
      <City> LIVONIA </City>
      <StateOrProvince> MI </StateOrProvince>
      <PostalCode> 48151 </PostalCode>
      <CountryCode> USA </CountryCode>
    </Address>
  </Organization>
  <ContactInfo>
    <Contact>
      <FirstName></FirstName>
      <EMail></EMail>
    </Contact>
  </ContactInfo>
</SellingParty>
<POType> PurchaseOrder </POType>
<MethodOfPayment>
  <VendorAccount></VendorAccount>
</MethodOfPayment>
<OrderRequestDate> 10/01/2000 </OrderRequestDate>
<RequestedDeliveryDate> 12/10/2000 </RequestedDeliveryDate>
<OrderRequestReference> xyz001acb </OrderRequestReference>
```

Code Example 2-1   Sample Data *(3 of 7)*

```
<CurrencyCode> USD </CurrencyCode>
<Shipping>
  <ShippingCarrier>Fedex</ShippingCarrier>
  <ShippingService>Over Night </ShippingService>
  <ShipToParty>
    <ShipToAddress>
      <AddressLine1> 2000 Happy Street </AddressLine1>
      <City> Sunnyvale</City>
      <StateOrProvince> CA </StateOrProvince>
      <PostalCode> 94385 </PostalCode>
      <CountryCode> USA </CountryCode>
    </ShipToAddress>
    <Organization>
      <Name></Name>
      <Address>
  <AddressLine1></AddressLine1>
  <City></City>
  <StateOrProvince></StateOrProvince>
  <PostalCode></PostalCode>
  <CountryCode></CountryCode>
      </Address>
    </Organization>
    <Contact>
      <FirstName> John Bill </FirstName>
      <Telephone> 888-8888888 </Telephone>
    </Contact>
  </ShipToParty>
</Shipping>
<ShippingRequirement>SP</ShippingRequirement>
<AllowanceOrCharge>
  <Allowance>
    <AllowanceType> DCAP </AllowanceType>
    <Amount>120.00</Amount>
  <Description></Description>
  </Allowance>
  <Charge>
    <ChargeType>Freight</ChargeType>
    <Amount> 35.00 </Amount>
  <Description></Description>
  </Charge>
</AllowanceOrCharge>
    </POHeader>
    <PODetail>
<LineItem>
  <LineItemNumber> 1 </LineItemNumber>
  <QuantityOrdered>
    <Quantity>100</Quantity>
    <UnitOfMeasure CodeValue="code">EA</UnitOfMeasure>
  </QuantityOrdered>
  <Part>
    <PartNumber>
      <SellerPartNumber>17432152</SellerPartNumber>
    </PartNumber>
    <ItemDescription>
```

Code Example 2-1   Sample Data *(4 of 7)*

```
      <Description>pencil</Description>
    <AlternateDescription>UDF</AlternateDescription>
    </ItemDescription>
    <Commodity>
      <CommodityCodeType></CommodityCodeType>
      <CommodityCode>stationary</CommodityCode>
    </Commodity>
  <URL></URL>
  </Part>
  <ShippingRequirement>SC</ShippingRequirement>
  <Cost>
    <ItemPrice>2.00</ItemPrice>
    <ExtendedPrice>200.00</ExtendedPrice>
    <ShippingCost>5.00</ShippingCost>
    <Tax>
      <TaxJurisdictionCode>All Taxes</TaxJurisdictionCode>
      <TaxAmount>20.06</TaxAmount>
    </Tax>
    <AllowanceOrCharge>
      <Allowance>
  <AllowanceType>DCAP</AllowanceType>
  <Amount>16.00</Amount>
  <Description></Description>
      </Allowance>
    </AllowanceOrCharge>
  </Cost>
</LineItem>
<LineItem>
  <LineItemNumber> 2 </LineItemNumber>
  <QuantityOrdered>
    <Quantity>100</Quantity>
    <UnitOfMeasure CodeValue="code">EA</UnitOfMeasure>
  </QuantityOrdered>
  <Part>
    <PartNumber>
      <SellerPartNumber>17432153</SellerPartNumber>
    </PartNumber>
    <ItemDescription>
      <Description>pencilbox</Description>
    <AlternateDescription>UDF</AlternateDescription>
    </ItemDescription>
    <Commodity>
      <CommodityCodeType></CommodityCodeType>
      <CommodityCode>stationary</CommodityCode>
    </Commodity>
  <URL></URL>
  </Part>
  <RequestedDeliveryDate>10/30/2000</RequestedDeliveryDate>
  <ShippingRequirement>SP</ShippingRequirement>
  <Cost>
    <ItemPrice>3.00</ItemPrice>
    <ExtendedPrice>300.00</ExtendedPrice>
    <ShippingCost>6.00</ShippingCost>
    <Tax>
```

Code Example 2-1   Sample Data *(5 of 7)*

```
      <TaxJurisdictionCode>All Taxes</TaxJurisdictionCode>
      <TaxAmount>21.06</TaxAmount>
    </Tax>
    <AllowanceOrCharge>
      <Allowance>
  <AllowanceType>DCAP</AllowanceType>
  <Amount>17.00</Amount>
  <Description></Description>
      </Allowance>
    </AllowanceOrCharge>
  </Cost>
</LineItem>
<LineItem>
  <LineItemNumber> 3 </LineItemNumber>
  <QuantityOrdered>
    <Quantity>50</Quantity>
    <UnitOfMeasure CodeValue="code">EA</UnitOfMeasure>
  </QuantityOrdered>
  <Part>
    <PartNumber>
      <SellerPartNumber>17432154</SellerPartNumber>
    </PartNumber>
    <ItemDescription>
      <Description>eraser</Description>
    <AlternateDescription>UDF</AlternateDescription>
    </ItemDescription>
    <Commodity>
      <CommodityCodeType></CommodityCodeType>
      <CommodityCode>stationary</CommodityCode>
    </Commodity>
  <URL></URL>
  </Part>
  <ShippingRequirement>SP</ShippingRequirement>
  <Cost>
    <ItemPrice>4.00</ItemPrice>
    <ExtendedPrice>200.00</ExtendedPrice>
    <ShippingCost>7.00</ShippingCost>
    <Tax>
      <TaxJurisdictionCode>All Taxes</TaxJurisdictionCode>
      <TaxAmount>22.06</TaxAmount>
    </Tax>
    <AllowanceOrCharge>
      <Allowance>
  <AllowanceType>DCAP</AllowanceType>
  <Amount>18.00</Amount>
  <Description></Description>
      </Allowance>
    </AllowanceOrCharge>
  </Cost>
  </LineItem>
<LineItem>
  <LineItemNumber> 4 </LineItemNumber>
  <QuantityOrdered>
    <Quantity>40</Quantity>
```

Code Example 2-1   Sample Data *(6 of 7)*

```
      <UnitOfMeasure CodeValue="code">EA</UnitOfMeasure>
    </QuantityOrdered>
    <Part>
      <PartNumber>
        <SellerPartNumber>17432155</SellerPartNumber>
      </PartNumber>
      <ItemDescription>
        <Description>ruler</Description>
      <AlternateDescription>UDF</AlternateDescription>
      </ItemDescription>
      <Commodity>
        <CommodityCodeType></CommodityCodeType>
        <CommodityCode>stationary</CommodityCode>
      </Commodity>
    <URL></URL>
    </Part>
    <Cost>
      <ItemPrice>5.00</ItemPrice>
      <ExtendedPrice>200.00</ExtendedPrice>
      <ShippingCost>8.00</ShippingCost>
      <Tax>
        <TaxJurisdictionCode>All Taxes</TaxJurisdictionCode>
        <TaxAmount>23.06</TaxAmount>
      </Tax>
      <AllowanceOrCharge>
        <Allowance>
    <AllowanceType>DCAP</AllowanceType>
    <Amount>19.00</Amount>
    <Description></Description>
        </Allowance>
      </AllowanceOrCharge>
    </Cost>
    </LineItem>
  <LineItem>
    <LineItemNumber> 5 </LineItemNumber>
    <QuantityOrdered>
      <Quantity>30</Quantity>
      <UnitOfMeasure CodeValue="code">EA</UnitOfMeasure>
    </QuantityOrdered>
    <Part>
      <PartNumber>
        <SellerPartNumber>17432156</SellerPartNumber>
      </PartNumber>
      <ItemDescription>
        <Description>notebook</Description>
      <AlternateDescription>UDF</AlternateDescription>
      </ItemDescription>
      <Commodity>
        <CommodityCodeType></CommodityCodeType>
        <CommodityCode>stationary</CommodityCode>
      </Commodity>
    <URL></URL>
    </Part>
    <Cost>
```

Code Example 2-1   Sample Data *(7 of 7)*

```
      <ItemPrice>6.00</ItemPrice>
      <ExtendedPrice>180.00</ExtendedPrice>
      <ShippingCost>9.00</ShippingCost>
      <Tax>
        <TaxJurisdictionCode>All Taxes</TaxJurisdictionCode>
        <TaxAmount>24.06</TaxAmount>
      </Tax>
      <AllowanceOrCharge>
        <Allowance>
    <AllowanceType>DCAP</AllowanceType>
    <Amount>20.00</Amount>
    <Description></Description>
        </Allowance>
      </AllowanceOrCharge>
    </Cost>
    </LineItem>
      </PODetail>
      <POSummary>
    <TotalTaxes>115.30</TotalTaxes>
  <TotalShipping>120.00</TotalShipping>
  <TotalMerchandise>960</TotalMerchandise>
  <TotalAllowances>120</TotalAllowances>
  <TotalLineItems>5</TotalLineItems>
  <TotalAmount>1010.30</TotalAmount>


      </POSummary>
    </PurchaseOrder>
 </OBIPurchaseOrder>
```

Stylesheet example, xmlpo.xsl

Code Example 2-2   Stylesheet example, xmlpo.xsl

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
version="1.0">

<!--############################################################ -->
<!--The actual conversion starts here -->
<!--it will help you to understand things better if you think
    of the incoming document as a tree of tags -->
<!--############################################################ -->

<!-- start looking from the root of the incoming document
     the 'match="/"' indicates it -->
<xsl:template match="/">
         <!-- start the html page here -->
  <ecx>
    <!-- recurse through the rest of the document -->
    <xsl:apply-templates/>
                <doctype>
                 xmlpo
                </doctype>
                <standard>
                 ML
                </standard>
                <senderqualifierid>
                 ZZ
                </senderqualifierid>
                <receiverqualifierid>
                 ZZ
                </receiverqualifierid>
</ecx>
</xsl:template>

<!-- these are the set of tags and the rules for converting the
     data present in those tags -->

<!-- if you find an order tag -->
<xsl:template match="Sender">
        <body>
                <senderid>
                        <xsl:value-of select="PartnerName"/>
                </senderid>
        </body>
</xsl:template>

<xsl:template match="Receiver">
        <receiverid>
                <xsl:value-of select="PartnerName"/>
        </receiverid>
</xsl:template>

</xsl:stylesheet>
```

OBIXMLPurchaseOrder.dtd

(The `OBIXMLLibrary.dtd` referenced is not included here)

Code Example 2-3   OBIXMLPurchaseOrder.dtd

```
<!-- Open Buying on the Internet (OBI) XML Document Type Definitions
Copyright Notice
OBI XML version 1.0
Copyright 2000 Open Buying on the Internet Consortium
Permission is granted to use, copy, modify and distribute the
DTD's contained subject to the terms and conditions specified at
http://www.openbuy.org/xml/version_1/copyright.html
All other rights reserved.
-->
<!-- $Id$ -->
<!-- $Header$ -->
<!ENTITY % OBIXMLLibrary SYSTEM "OBIXMLLibrary.dtd">

%OBIXMLLibrary;

<!ELEMENT OBIPurchaseOrder  (Envelope , PurchaseOrder ,
SenderDigitalSignature? )>
<!ATTLIST OBIPurchaseOrder  version      CDATA  #IMPLIED
                            xml:language CDATA  #IMPLIED
                            revision     CDATA  #IMPLIED >
<!ELEMENT PurchaseOrder (POHeader , PODetail , POSummary )>
<!ATTLIST PurchaseOrder  deploymentMode CDATA  'production' >
<!ELEMENT POHeader  (OrderNumber , OrderDate , BuyingParty , BuyerAcctInfo? ,
(RequisitioningParty | ReceivingParty )+ , BillToParty , SellingParty , POType
, ContractNumber? , POReleaseNumber? , MethodOfPayment , OrderRequestDate? ,
RequestedDeliveryDate , OrderRequestReference? , Tax? , CurrencyCode , Shipping
, ShippingRequirement? , AllowanceOrCharge? )>

<!ELEMENT PODetail  (LineItem+ )>

<!--#USAGE:BEG02 segment in PO. Set to "BK" for blanket PO, empty or "SA" for
standalone-->
<!ELEMENT POType  (#PCDATA )>

<!ELEMENT MethodOfPayment  (CreditCard | PurchasingCard | VendorAccount )>

<!ELEMENT POSummary  (%OrderSummaryRef; )>
```

Sample Output Data

The map in this case was very simple and only maps over a portion of the elements available in the XML data.

```
ISA*00*          *00*          *ZZ*ABC1          *ZZ*XYZ1
*001202*1728*U*00304*000000000*0*P*~
GS*PO*ABC1*XYZ1*001202*1728*0*X*003040
ST*850*0001
BEG*00*SA*xyz0000000001abc**001010
PO1*1*100*EA***VP*17432152
CTT*1
SE*1*0001
GE*1*0
IEA*1*000000000
```

Using the XSLT Translator

With the use of XSLT stylesheets, XML input can be transformed into any other output format. This scenario differs from the XML to EDI scenario in that instead of using a Mercator map for the translation an XSLT stylesheet is used. The process is similar to using a Mercator map:

1. Create the XSLT transformation stylesheet that maps input XML to output HTML. The stylesheet file must use the .xsl extension in order for ECXpert to recognize it, and it must be in the /maps directory.

   A sample stylesheet is shown in Code Example 2-4. (This sample file view_po.xsl can be found in the /maps directory of your EXCpert installation. For information on the XSLT standard, refer to http://www.w3.org/Style/XSL/.

Code Example 2-4   Transformation stylesheet for XML to HTML conversion

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Stylesheet PI
-->
<?ecx-stylesheet href="retrieve_keys.xsl" type="text/xml" ?>
<po>
<po_header>
  <biz_key>
    <po_number>12345</po_number>
  </biz_key>
  <po_date>03/28/2001</po_date>
  <contact_number>54321</contact_number>
```

Code Example 2-4   Transformation stylesheet for XML to HTML conversion

```
  <sender>xsltSend</sender>
  <senderqual>ZZ</senderqual>
  <receiver>xsltRecv</receiver>
  <receiverqual>ZZ</receiverqual>
  <doctype>850</doctype>
</po_header>
<shipment>
  <payment_method>Money Order</payment_method>
  <from>TXhost</from>
  <to>webuser1</to>
</shipment>
<details>
  <line_number txLoopID="1">
     <description>Sun Utra 30</description>
     <amount_each>$5000.00</amount_each>
     <qty>4</qty>
  </line_number>
  <line_number txLoopID="2">
     <description>Sun Utra 60</description>
     <amount_each>$8000.00</amount_each>
     <qty>4</qty>
  </line_number>
</details>
</po>
```

2. Create the intermediate stylesheet used to retrieve key data from the data files. An example of an intermediate stylesheet is shown in Code Example 2-5. (This example file `retrieve_keys.xsl` can be found in the `/data/stylesheet` directory of your ECXpert installation.)

Code Example 2-5   Intermediate stylesheet to retrieve key data from data file

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
version="1.0">

<xsl:template match="/">

<ecx>

   <standard>ML</standard>
   <version>NONE</version>
   <functionalid>NONE</functionalid>

   <release>0</release>

   <doctype>
      <xsl:value-of select="po/po_header/doctype"/>
   </doctype>

   <senderqualifierid>
      <xsl:value-of select="po/po_header/senderqual"/>
   </senderqualifierid>
   <senderid>
      <xsl:value-of select="po/po_header/sender"/>
   </senderid>
   <receiverqualifierid>
      <xsl:value-of select="po/po_header/receiverqual"/>
   </receiverqualifierid>
   <receiverid>
      <xsl:value-of select="po/po_header/receiver"/>
   </receiverid>

</ecx>

</xsl:template>
</xsl:stylesheet>
```

3. Create the members, using the ECXpert Members tab. You will be creating both a sending and receiving member. In this example we create only the sending member. Figure 2-6 shows the Membership Information subtab of the Members tab.

Figure 2-6   The Membership Information tab

a. Figure 2-7 shows the Contact Information subtab, in which you specify the partner's address, phone, and email information.

Figure 2-7   The Contact Information tab

  b. Figure 2-11 shows the Trading Addresses subtab, in which you specify the
          email address the partner uses for trading.

Figure 2-8   The Trading Addresses subtab

   4.   Create the partnership, using the Partnership tab illustrated in Figure 2-9

Figure 2-9   The Partnership tab

a. Figure 2-10 shows the Input XML subtab, in which you specify interchange level information.

Figure 2-10   The Input XML subtab
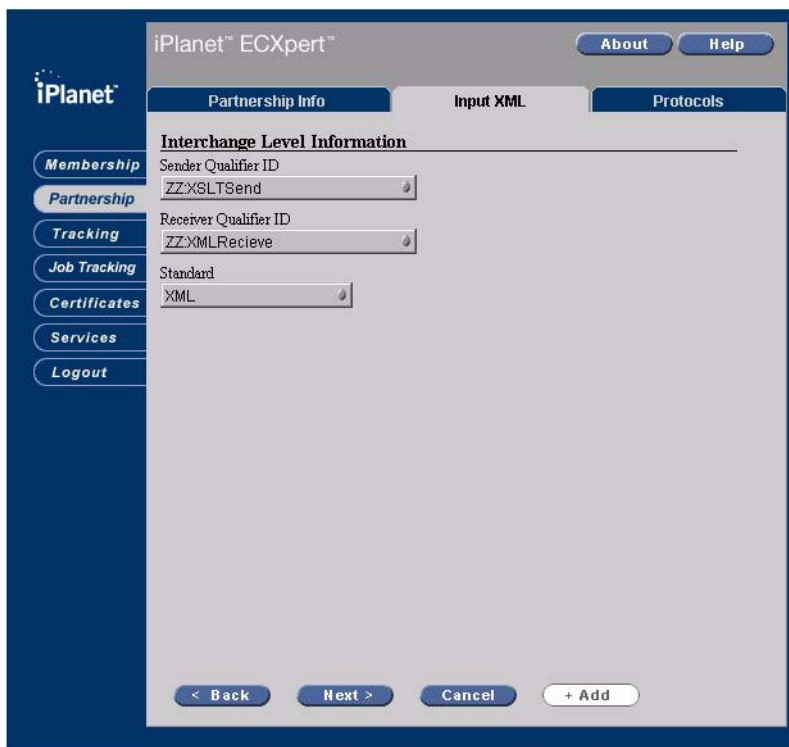
   b.   Figure 2-11 shows the Protocols subtab, in which you specify the email
         protocol and parameters for exchanging data.

Figure 2-11 The Protocols subtab
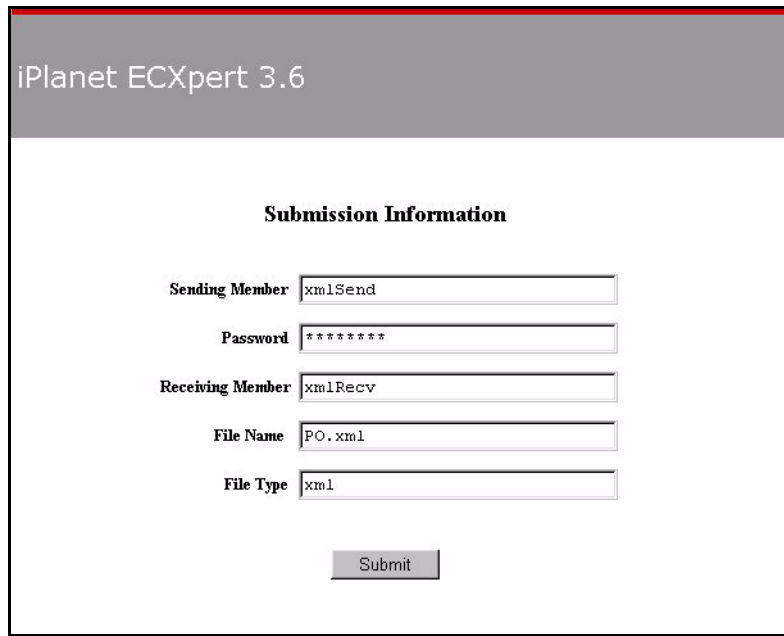
5. Create a services list using the Services tab as show in Figure 2-12, for specifying all the services that will be invoked during partnership transactions.

Figure 2-12   The Services tab
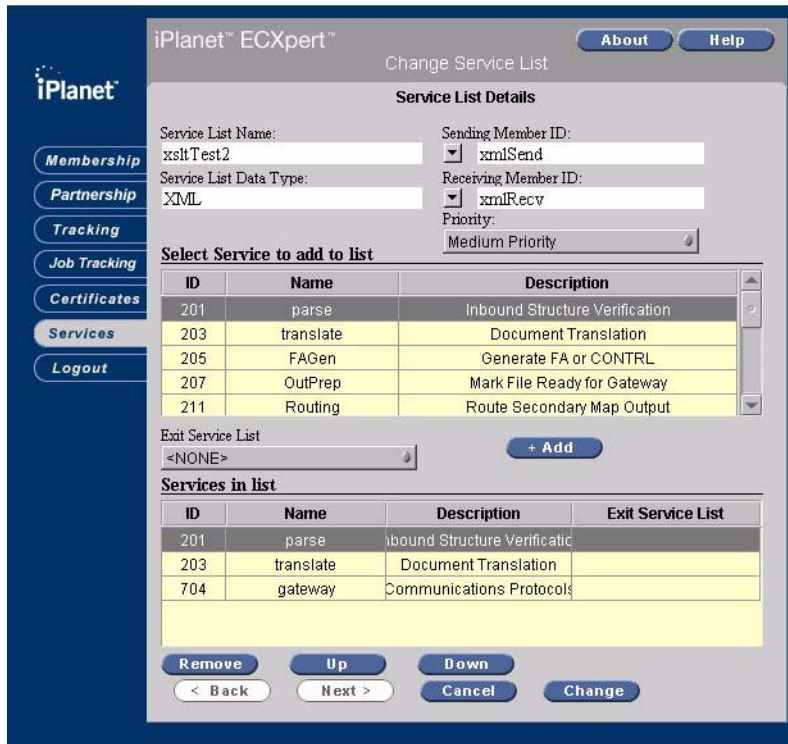
6.   Submit the document, using the Document Submission form

Figure 2-13 The Document Submission form.

Pass-through: Incoming CAD/CAM Files, No Processing

In some cases, a business might need to use ECXpert to send or receive data, without additional data processing. In this example, ECXpert receives CAD/CAM files and forwards them to a user's file system for the user to work with manually.

Service List for Incoming CAD/CAM Files

The service list for incoming CAD/CAM files must contain both the Outprep and Gateway services.

Figure 2-14   Service List for incoming CAD/CAM files, no processing
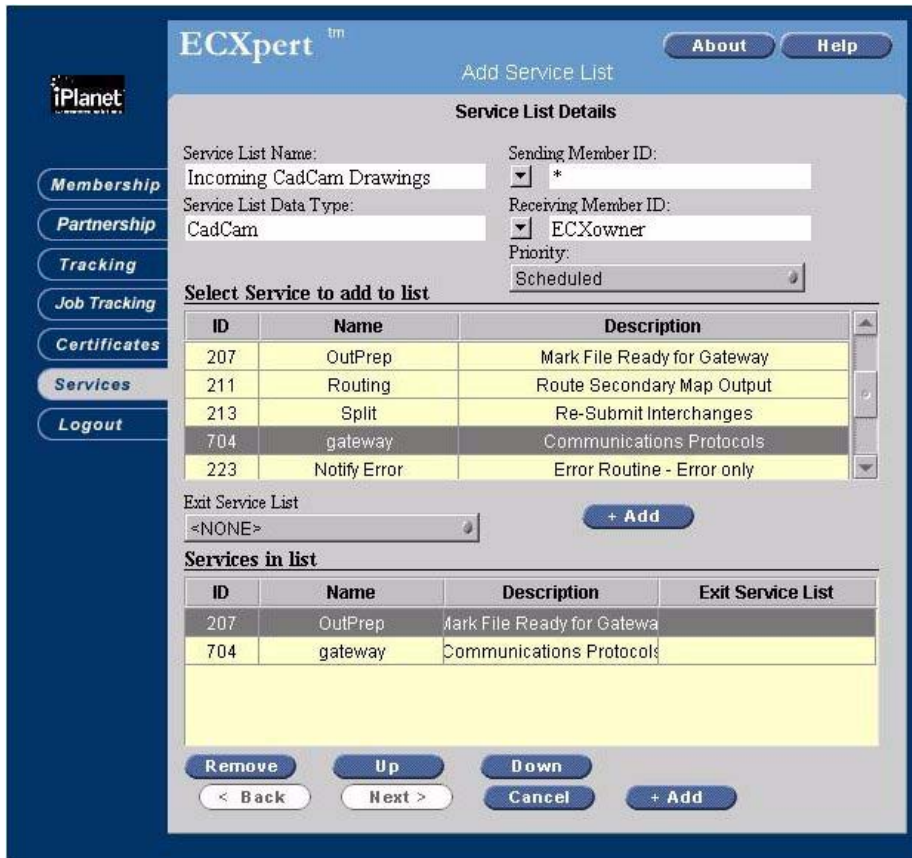
- **Outprep**—The Outprep service notifies ECXpert that the file is ready to be sent out without any processing.

- **Gateway**—The Gateway service looks up the protocol to use on the file based on the partnership. In this example, ECXpert sends the file via FTP to `/orderadmin`.

Partnership for Incoming CAD/CAM Files

In the Partnership Details for incoming CAD/CAM files, the Partnership Type has to be Application to Application and the Document Type must agree with the service list data type previously defined. Otherwise the Partnership cannot be found when the service list does not include the Parse service.

Figure 2-15   Partnership for incoming CAD/CAM files, no processing

- **Sender**: Partner7

- **Receiver:** ECXOwner

- **Document Type:** CadCam

- **Map:** none—no processing

Application to Application: Incoming PeopleSoft to SAP

If data from a PeopleSoft human resource system needs to be shared with a SAP financial system, ECXpert is able to translate defined data from one format to another. In this example, ECXpert converts PeopleSoft date into the format needed by SAP and uses the ECXpert SAP ALE interface to put the information into the SAP system.

Service List for Incoming PeopleSoft to SAP

Figure 2-16   Service List for incoming PeopleSoft to SAP
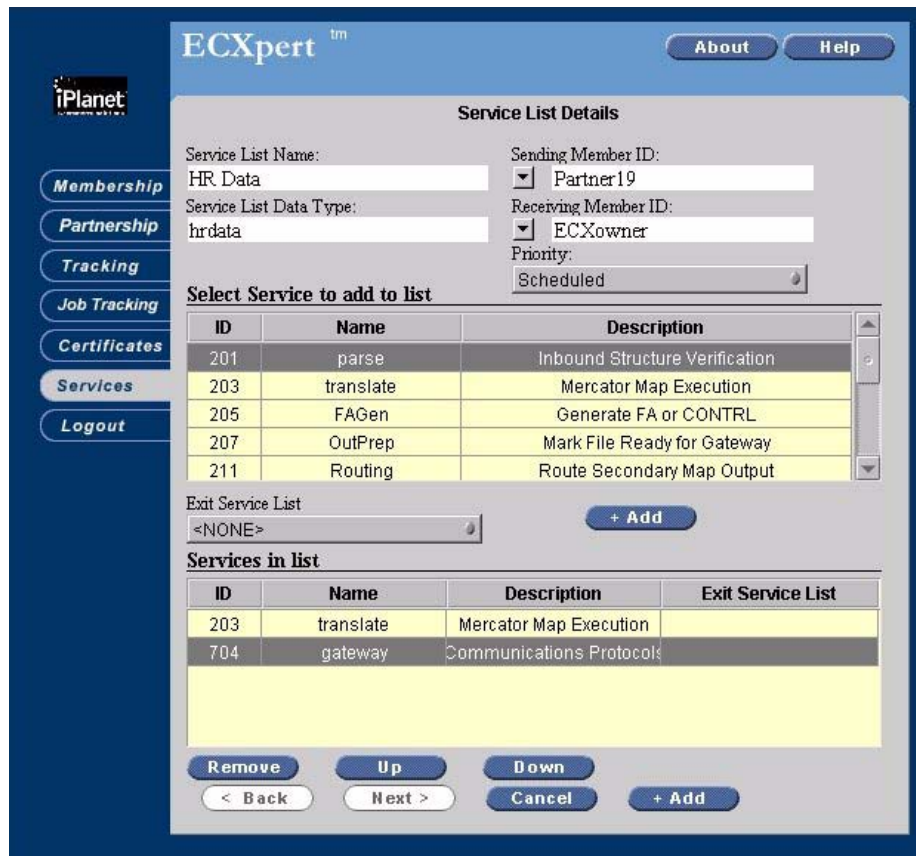
- Translate—Converts submission unit documents from one format to another.

- Gateway—Triggers the sending of finished submission units.

Partnership for Incoming PeopleSoft to SAP

Figure 2-17   Partnership for incoming PeopleSoft to SAP

- **Sender:** Partner19

- **Receiver:** ECXowner

- **Document Type:** hrdata

- **Map:** psft_sap.sun

Figure 2-18   Protocols tab for incoming PeopleSoft to SAP partnership

• **Outgoing Protocol:** Legacy Server (SAP)

Using the Split Service

ECXpert provides a service called Split, to allow individual documents within a larger file to be split into separate submission units that are processed with separate service lists. This is needed when different service lists are *required* for correct processing. For example, EDI files going to TradingXpert need only Parse and Translate in the service list. Using the pre-installed Inbound service list containing Parse, Translate, FAGen, and Gateway would cause TradingXpert files to fail.

NOTE   Split is the only ECXpert service that does not require a supporting partnership to be set up. It is executed based solely on the Sender, Receiver, and Service List Data Type in the service list that you set up matching the Sender, Receiver, and Document Type of the incoming data file.

Using the Split service involves the following tasks:

1. In the `ecx.ini` file, `[Split]` section, set parameters:

   ❍ Set **submissionDocType** to **EDI**

   ❍ Set **maxThreads** set less than or equal to the value specified for `worker_max_threads` in the `[dispatcher]` section

2. Create a service list for Split (see example in Figure 2-19):

   ❍ Set Service List Data Type to To_Be_Split; this *must not match* the value set for `submissionDocType` in the `[Split]` section of the `ecx.ini` file

   ❍ Set Sending Member ID and Receiving Member ID as necessary to cover those partnerships that need to have their submission units Split

3. Create partnership(s) to support processing of the documents after they have been Split.

   ❍ Set Sender and Receiver to the true Sender and Receiver in the file

   ❍ Set Document Type to the true Document Type in the file

NOTE   You set up these partnership(s) exactly as you would if the documents produced by Split were submitted to ECXpert directly.

---

4. Create service list(s) as necessary to support processing of the documents after they have been Split:

   ❍ Set Sender and Receiver as needed

   ❍ Set Document Type to the true Document Type in the file

NOTE	You set up these service list(s) exactly as you would if the documents produced by Split were submitted directly to ECXpert.

5. Submit to ECXpert to be processed initially by the service list for Split:

   ❍ Set Sender and Receiver as needed

   ❍ Set File Type to To_Be_Split; this *must match* the value of the special service list that contains Parse, Split

After you have submitted to ECXpert, the special service list for Split is executed. The Parse service logically splits your submission unit into separate documents (the original file is not changed or copied), and then the Split service resubmits each one to ECXpert with its own Tracking ID. ECXpert then processes each document with the appropriate service list, based on the Sender, Receiver, and Document Type that matches what you set for the submissionDocType parameter in the [Split] section of the ecx.ini file—in this example, EDI.

NOTE	The submissionDocType parameter in the ecx.ini file is a global setting. For more information on the implications of your submissionDocType setting and its interaction with Service List Data Types, see "Using the Split Service" on page 465.

Service List for Using Split

Figure 2-19   Service List for using Split

The Service List Data Type is Split, and the following services are included:

- Parse—Logically breaks incoming EDI into its constituent parts.

- Split—Splits incoming EDI submission unit into a separate submission unit for each document, so that the documents can be processed by different service lists.

Figure 2-20   Incoming EDI with Multiple Outputs Routed to Appropriate System

In this scenario, a customer who receives incoming orders using EDIINT, EDI over VANs, and proprietary files via email (SMTP) wants incoming orders to be split and sent to the appropriate systems in the proper file format. The customer also wants to receive an acknowledgement when the trading partner's system receives an order that has been sent. ECXpert handles all of the inbound protocols to meet the customer requirements. Using logic built into our translation tools, ECXpert creates multiple orders based on product numbers within an order.

The ECXpert system configuration sets up two phases of processing, based on the primary and secondary output cards of the *Mercator* mapping system. This requires two partnerships and two service lists. A third partnership is also required for sending functional acknowledgements.

In the *primary output* phase, using Mercator's primary output card, ECXpert parses an incoming EDI interchange, translates its component documents to the application formats specified in the maps used for the relevant partnerships (one partnership for each sender/receiver/document type combination), generates a functional acknowledgement, and routes the translated documents to secondary output cards—also specified in the partnerships—that determine how to further process the documents.

In the *secondary output* phase, ECXpert submits the output from *Mercator's* output card #3 to a second service list, which is then executed.

Setup for the Primary Output Phase

Creating a Membership for Each Trading Partner

For this scenario, you would first need to define a membership for each of the trading partners to be involved, using the Membership tabs on the ECXpert Product Administrative Interface. You would assign each of these members a *member ID* that is short and descriptive—in our example they are simply "TradingPartner1," who sends the orders, and "TradingPartner2," who receives them. You would also need to supply an Internet *trading address* for each member.

Details of how to do this are covered in Chapter 5, "Setting Up Members."

Creating a Service List for Incoming Orders

The next step would be to set up the list of services to be performed on the incoming orders. You must specify one of the two trading partners involved as the Sending Member, and the other as the Receiving Member.

The other important item to specify for the service list is the Service List Data Type. This, together with the two member IDs, is necessary to tie the service list to the partnership that you will define next.

Finally, you must specify in sequence the services that are to be performed when this service list is executed. In Figure 2-21, all of the services needed in this example have been selected from the list at the top and are displayed in the list at the bottom.

Details of how to set up a service list are covered in Chapter 10, "Setting Up Services and Service Lists."

Figure 2-21   Primary output: first service list

Table 2-1   Required service list details for primary output

Item	Description
Service List Details	
Service List Name	The name of the service list.
Service List Data Type	The data type being exchanged. In this example, it is EDI.
Sending Member ID	The member ID sending the service list.
Receiving Member ID	The member ID receiving the service list.
Scheduled check box	If you want to execute the service list on a time-based schedule, select this option. You must also create a scheduler job for the dispatcher via the Server Administrative interface. See "Scheduling ECXpert Jobs" on page 155 for more information.

Table 2-1   Required service list details for primary output *(Continued)*

Item	Description
Service List Details	
Services in List	
Parse	Logically breaks incoming EDI into its constituent parts.
Translate	Converts submission unit documents from one format to another. Requires you to specify a Map in the Trading Partnership Information tab.
FAGen	Creates EDI acknowledgements in the formats: 997 (ANSI), 999 (UCS), and CONTRL Messages (EDIFACT).
	This service is only used when incoming data is EDI, and when the trading partnership also specifies that FAs be generated.
Routing	Specifies how to submit secondary output when there are multiple output cards from a Mercator map. This service must be in a service list before you can fill in the Partnership Outputs tab.
Gateway	Triggers the sending of finished submission units.

Creating a Partnership that Uses the First Service List

The last major step in setting up the primary output in this scenario is to link the two trading partners in a partnership that specifies the service list to be used. Figure 2-22 shows the Partnership Info tab filled in for this partnership. The Sending Member is "TradingPartner1." The Receiving Member is "TradingPartner2," matching the Service List's Receiving Member ID. The Partnership Type is "EDI to Application," which matches the Service List Data Type for the Service List.

Details on how to create a partnership are covered in Chapter 6, "Setting Up Trading Partnerships."

Figure 2-22 Primary output: first partnership, Partnership Info tab

Table 2-2 Required partnership details for primary output

Item	Description
Partnership Details	
Sending Member	The member ID sending the document—TradingPartner1.
Receiving Member	The member ID receiving the document—TradingPartner2.
Partnership Type	EDI to Application
Map Name	two_outputs.sun
Document Type	865
[Remaining Parameters]	Modify to meet your specific needs.

Setup for the Secondary Output Phase

Setting up Secondary Outputs for the Second Application

When the Partnership Info tab specifies a map that generates multiple output types—"SamplePO.map " in our example—the Outputs tab appears on the partnership definition screen.

In order to process multiple outputs, the partnership must use a service list that includes the Routing service, which specifies how to submit secondary output. You therefore must define a Service List containing the Routing service before you can fill in the Output tab and define the trading partnership.

Details on how to fill in the Outputs tab are covered in Chapter 6, "Setting Up Trading Partnerships."

Figure 2-23   Secondary output, Outputs tab

Table 2-3   Required partnership details for secondary output

Item	Description
Specify Service List for Additional Output Cards	
[Service List Information]	Add the service list created to handle the primary output (refer to Figure 2-21). All secondary output cards used by the map for the current partnership will then appear in the bottom table. In this example, Card #5, called "Lines_Table," will be used to handle the secondary output.

Setting up the Secondary Service List

In the secondary output phase, ECXpert submits the output from *Mercator's* output card #3 to the service list labeled "Resend to 2nd Application." Figure 2-24 shows the Service List Details tab filled in for the secondary service list. All of the services needed in this example have been selected from the list at the top and are displayed in the list at the bottom.

Figure 2-24   Secondary output, Service List Details tab

Table 2-4   Required service list details for primary output

Item	Description
Service List Details	
Service List Name	The name of the service list.
Service List Data Type	The data type being exchanged. In this example, it is 2ndapp.
Sending Member ID	The member ID sending the service list.
Receiving Member ID	The member ID receiving the service list.

Table 2-4 Required service list details for primary output *(Continued)*

Item	Description
Service List Details	
Scheduled check box	If you want to execute the service list on a time-based schedule, select this option. You must also create a scheduler job for the dispatcher via the Server Administrative interface. See "Scheduling ECXpert Jobs" on page 155 for more information.
Services in List	
Outprep	The Outprep service notifies ECXpert that the file is ready to be sent out without any processing.
Gateway	Triggers the sending of finished submission units. The Gateway service looks up the protocol to use on the file based on the partnership.

Figure 2-25   Primary output, Input EDI tab

Setting up a Partnership for Secondary Output

Although TradingPartner1 is still the sender and TradingPartner2 is still the receiver, we now have non-EDI data that is being sent to a site with EDI data, so we have to set up a second partnership. Figure 2-26 shows the Partnership Info tab filled in for this partnership. Note that no Map Name is needed this time.

Figure 2-26   Secondary output, Partnership Info tab

Integrating ECXpert with MQSeries

MQSeries can be used to integrate various applications in an enterprise. For example, its Purchasing System can be one such application. ECXpert, with its MQSeries connector, can connect the enterprise (Purchasing System) with its trading partners. ECXpert acts as a document gateway to send and receive documents between these trading partners and the enterprise Purchasing System.

The company's Purchasing System does an MQSeries Put to place its purchase orders as messages in the MQSeries Purchase Order Queue, with the shopper ID stored as the Message ID. This queue was set up to allow other applications to validate and report the purchase orders.

An ECXpert Scheduler task initiates an MQSeries Get to retrieve the messages created for a partner from the Purchase Order Queue. This operation gets the messages with a specific Message ID and submits them as documents to its Partner.

The Partner receives the document and sends the acknowledgement. The Partner is then responsible for the order fulfillment. It is not necessary for the Partner to use either ECXpert or MQSeries for keeping track of the order fulfillment.

Service List for MQSeries

Figure 2-27   Service List for MQSeries

- Parse—Logically breaks incoming EDI into its constituent parts.

- Translate—Converts submission unit documents from one format to another.

- Gateway—Triggers the sending of finished submission units.

Partnership for MQSeries

Figure 2-28   Partnership for MQS, Partnership Info tab

- **Sender:** test1—Purchasing System connected to MQSeries Purchase Order Queue

- **Receiver:** test2—external trading partner

- **Document Type:** mqs

- **Map:** 850html.sun

Scheduler Task for MQSeries

Figure 2-29   Scheduler Task for MQS, basic page of input form
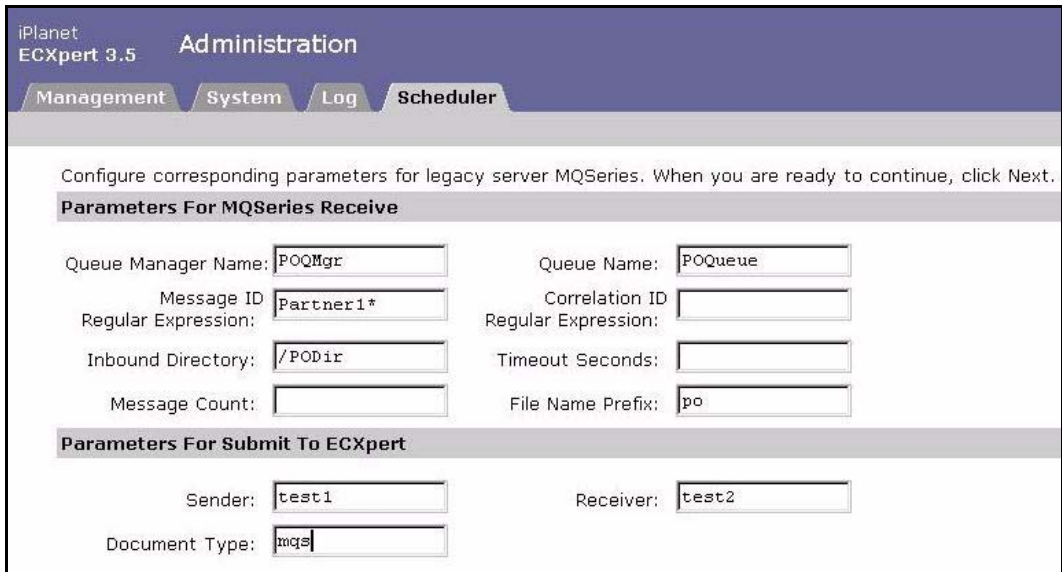
Scheduler task—First/Basic page (Figure 2-29)

- **Use:** ECX Gateway
- **Protocol:** Legacy Server for MQSeries Receive

Figure 2-30 Scheduler Task for MQS, Parameters page of input form

- Scheduler task—Parameters page (Figure 2-30)

  Parameters for MQS Receive—getting messages. from MQS Purchase Order Q

  ❍ **QMgr Name:** POQMgr

  ❍ **Queue Name:** POQueue

  ❍ **Msg ID Reg Exp:** Partner1*

  Parameters for Submit—submitting POs to partner

  ❍ **Sender:** test1—Purchasing System connected to MQSeries Purchase Order Queue

  ❍ **Receiver:** test2—external trading partner

  ❍ **Doc Type:** mqs

Using TradingXpert

Netscape TradingXpert, a component of the CommerceXpert product family, extends the functions of ECXpert to create web-based E-Commerce applications. TradingXpert allows you to extend your trading networks to reach smaller and medium sized trading partners without requiring them to invest in sophisticated and costly EDI software; web forms working with TradingXpert become another medium for communicating with business partners.

Out of the box, TradingXpert supports several business documents. Purchase orders can be sent to a web-based TradingXpert user and Purchase Order Acknowledgements and Invoices can be returned to the ECXpert owner. Customizable business logic is included to allow for automated document turnaround; that is, the solution pre-populates data into the documents to be sent back to the "hub."

On the ECXpert end, you must set up supporting partnerships for each trading partner you want to allow to view documents from (send) and/or submit documents to (receive) your ECXpert installation. For each trading partner, a separate partnership is required for each Document Type and each direction (send vs. receive).

The following example details the setup for a trading partner to view purchase orders from your ECXpert installation and submit invoices back to your ECXpert. The trading partner you want to set up with TradingXpert has a Member ID of "webuser1" and the ECXpert member set up to communicate with TradingXpert is "TXHost".

The specific tasks to perform to set up this TradingXpert scenario are:

1. Set up member TXhost with EDI trading address of 12:7771234567

2. Set up member webuser1 with EDI trading address of 12:5551112222

3. Set up a service list for sending POs to webuser1 (Figure 2-31)

4. Set up a partnership for sending POs to webuser1 (Figure 2-32, Figure 2-33)

5. Set up a service list for receiving invoices back from webuser1 (Figure 2-34)

6. Set up a partnership for receiving invoices back from webuser1 (Figure 2-35, Figure 2-36, Figure 2-37)

Setup for Partner to View Purchase Orders

The following screens and accompanying notes show how to set up ECXpert to allow "webuser1" to view purchase orders in TradingXpert.

Figure 2-31   Service List Details for using TradingXpert to view purchase orders

- **Parse**—Logically breaks incoming EDI into its constituent parts.

- **Translate**—Converts submission unit documents from one format to another.

NOTE	You must *not* include Gateway in this service list. In effect, TradingXpert replaces the Gateway function. If Gateway is in this service list, ECXpert attempts to send purchase orders directly to the trading partner.

Figure 2-32 Partnership Info for using TradingXpert to view purchase orders

- Sender: TXhost—ECXpert member set up to communicate with TradingXpert

- Receiver: webuser1—trading partner who will be viewing your purchase orders to the associated company through TradingXpert via a browser

- Document Type: 850

- **Partnership Type:** EDI to Application

- **Map Name:** 850html.sun

Figure 2-33   Input EDI for using TradingXpert to view purchase orders

- **Sender Qualifier ID:** 12:7771234567

- **Receiver Qualifier ID:** 12:5551112222

- **Standard:** ANSI

Setup for Partner to Submit Invoices

The following screens and accompanying notes show how to set up ECXpert to allow "webuser1" to submit invoices, based on purchase orders viewed, through TradingXpert.

Figure 2-34   Service List for using TradingXpert to submit invoices

- **Parse**—Logically breaks incoming EDI into its constituent parts.

- **Translate**—Converts submission unit documents from one format to another.

- Gateway—Triggers the sending of finished submission units.

Figure 2-35   Partnership Info for using TradingXpert to submit invoices

- **Sender:** TXhost—ECXpert member set up to communicate with TradingXpert

- **Receiver:** webuser1—trading partner who will be sending you invoices through TradingXpert, based on your purchase orders to the associated company viewed through TradingXpert

- **Document Type:** 810

- **Partnership Type:** Application to EDI

- **Map Name:** html810.sun

Figure 2-36   Input HREC for using TradingXpert to submit invoices

- **Sender Qualifier ID:** webuser1—trading partner who will be sending you invoices through TradingXpert, based on your purchase orders to the associated company viewed through TradingXpert

- **Receiver Qualifier ID:** TXhost—ECXpert member set up to communicate with TradingXpert

- **Standard:** ANSI

- Other fields: After selecting ANSI for Standard, you can use (or change) the default values, as appropriate for your needs.

Figure 2-37   Output EDI for using TradingXpert to submit invoices

- **EDI Envelope:** ECXpert generates (or overrides) entire envelope

- **Standard:** ANSI

- Other fields: After selecting ANSI for Standard, you can use (or change) the default values, as appropriate for your needs.

Testing your TradingXpert Setup

Follow the steps below to use the Document Submission Form to test your TradingXpert setup.

7. Enter the ECXpert URL in your browser.

Enter the following URL in your browser:

http:// *hostname*:*port* /

where *hostname* is the name of the host machine where ECXpert is installed, and *port* is the port number ECXpert is using.

The ECXpert home page (Figure 2-38) is displayed.

Figure 2-38 ECXpert home page
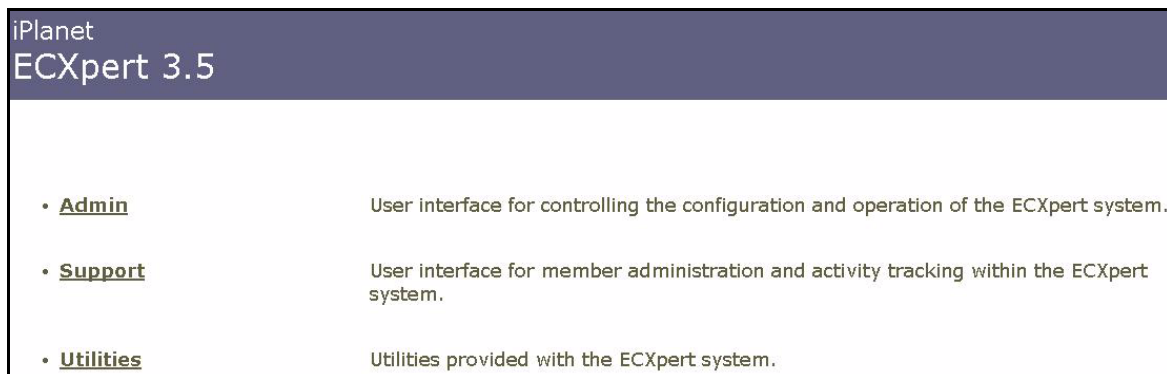
8. Click Utilities.

The ECXpert Utilities Menu (Figure 2-39) is displayed.

Figure 2-39   ECXpert Utilities Menu
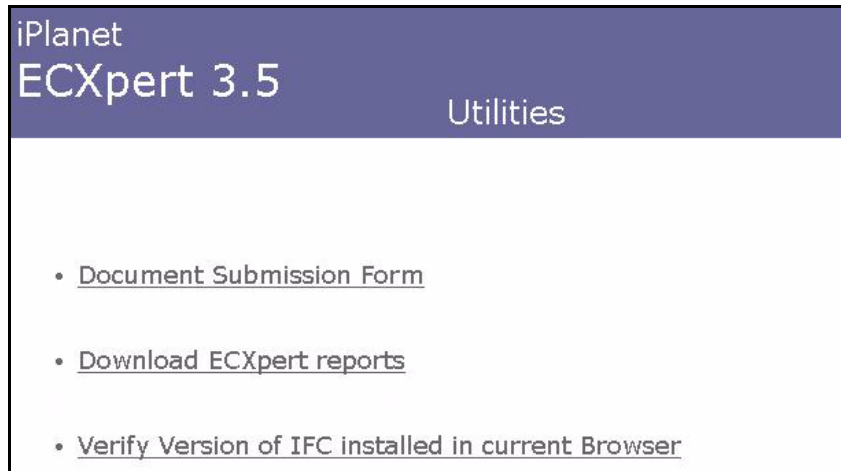
9.   Click the Document Submission Form link.

The Document Submission Form (Figure 2-40) is displayed.

Figure 2-40   Document Submission Form

10. Enter parameters for the submit command.

Refer to Table 2-5 for detailed information about the parameters.

Table 2-5   Parameters for the submit command

Parameter	Description
Sending Member	The member ID of the sending member defined in the associated partnership—TXhost.
Password	Password for the sending member—the password that you have set up for TXhost.
Receiving Member	The member ID of the receiving member defined in the associated partnership—webuser1.
File Name	The name of a file to be submitted to ECXpert (the submission unit). The file name is **input_file_850.txt**. You should also supply the full path to the location to which you have copied this file from the CD. In the picture above, the file is in the root directory.
File Type	The Document Type for the file being passed to ECXpert, as defined in the associated partnership.

11. Click Submit.

A message is displayed providing feedback on the command. If any errors are encountered they are displayed first.

12. Optionally, view the tracking information for your submission.

- ❍ Log into the ECXpert Product Administrative Interface.
- ❍ Click Tracking on the left.

  The Enter Search Constraints tab is displayed.

- ❍ Set Search Level to Document.
- ❍ Enter today's date.
- ❍ Click Search.

13. Optionally, log into TradingXpert as webuser1 to see the P.O. just sent.

The ECXpert Demo Data

ECXpert comes with inbound and outbound partnerships, input files, and maps that you can use to demonstrate how ECXpert processes 810 and 820 EDI (ANSI X12) documents. Some of these files are used in a post-installation test to be certain that ECXpert has been properly installed.

The inbound and outbound partnerships are configured by default to use the SMTP protocol. If you want to use the SMTP protocol in your own ECXpert demonstrations, you must make sure that the members have correct local e-mail addresses and remote e-mail addresses. If you want to use a protocol other than SMTP, you must change the partnership protocol information.

The maps and input files for the ECXpert demo are located in the *$NSBASE*/NS-apps/`maps` directory. The input files are:

- *$NSBASE*/NS-apps/`maps/Input_810.txt`

- *$NSBASE*/NS-apps/`maps/Input_820.txt`

NOTE	ECXpert also comes with a 997 partnership. This partnership is an example of how ECXpert can be configured to generate an EDI Functional Acknowledgement—an EDI (ANSI X12) 997 document. This partnership is provided for example purposes only, and is not set up to be part of the ECXpert Demo.

Working with the System Administration Interface

This chapter covers the ECXpert System Administration Interface. The following topics are covered:

- Overview

- Logging into the System Administration Interface

- Navigating Around and Between Tabs

- System Administration Interface Help

- Managing ECXpert Servers

- Managing ECXpert System Settings

- Viewing Log Files

- Scheduling ECXpert Jobs

- Using the ECXpert Utilities

Overview

The System Administration Interface allows you to control the operation of the ECXpert servers, configure system settings, view the system log files, and schedule time-based ECXpert processing tasks.

For information on setting up trading partnerships and the various components that support them, refer to Chapter 6, "Setting Up Trading Partnerships."

Access to the System Administration Interface is controlled separately from access to the Product Administrative Interface.

A number of functions related to the System Administration Interface are controlled outside of the interface. The *iPlanet ECXpert Operations Reference Guide* chapter on "ECXpert Operations" covers the routine functions performed outside the user interface.

Logging into the System Administration Interface

To log in to ECXpert System Administration Interface:

1. Enter the ECXpert URL in your browser.

Enter the following URL in your browser:

http://*hostname*:*port*/

where *hostname* is the name of the host machine where ECXpert is installed, and *port* is the port number ECXpert is using.

The ECXpert home page (Figure 3-1) is displayed.

Figure 3-1   ECXpert home page
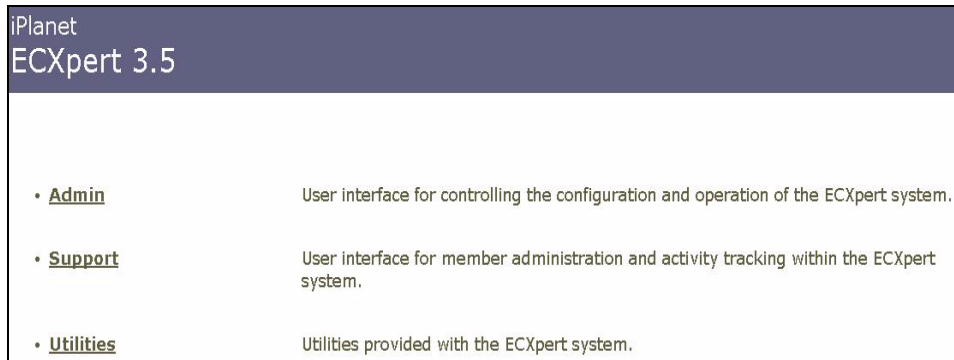
2. Click the Admin link.

The initial screen for the System Administration Interface is displayed. This initial screen looks quite different when the ECXpert Administration Server is turned off (Figure 3-2) vs. when it is turned on (Figure 3-3).

Figure 3-2 Initial System Administration Interface screen, ECXpert Administration Server turned off
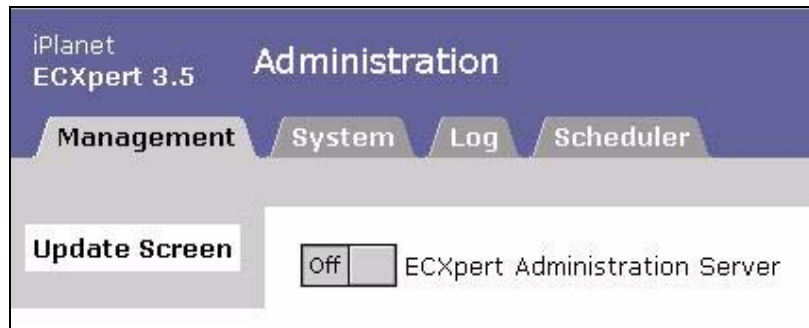
Figure 3-3 Initial System Administration Interface screen, ECXpert Administration Server turned on
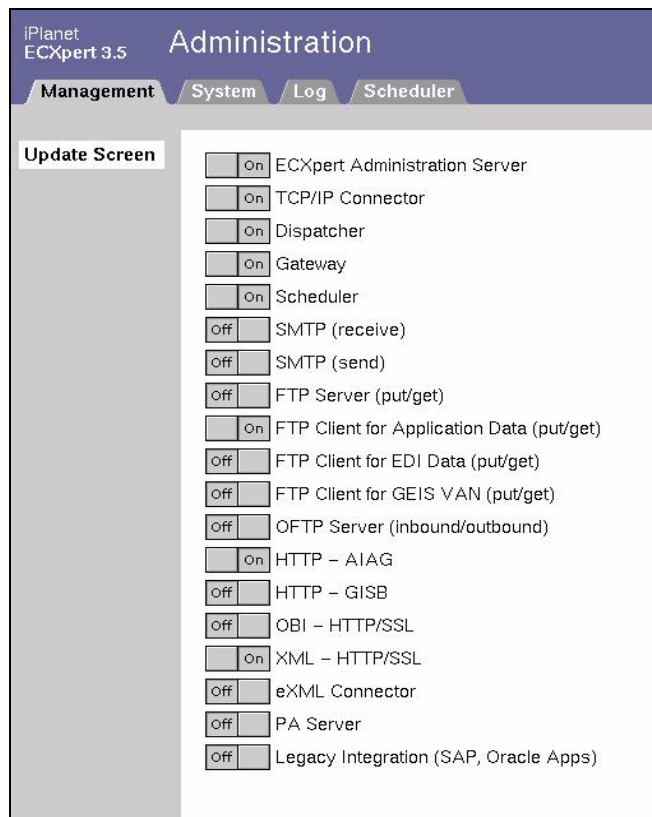
For information about turning the ECXpert Administration Server and other servers on and off, see "Managing ECXpert Servers" on page 131.

For information about the standard layout of forms in the ECXpert System Administration Interface, see "Navigating Around and Between Tabs" below.

Navigating Around and Between Tabs

All of the screens in the ECXpert System's System Administration Interface share a common general layout, as shown in Figure 3-4.

Figure 3-4   Basic layout of ECXpert System Administration Interface screens
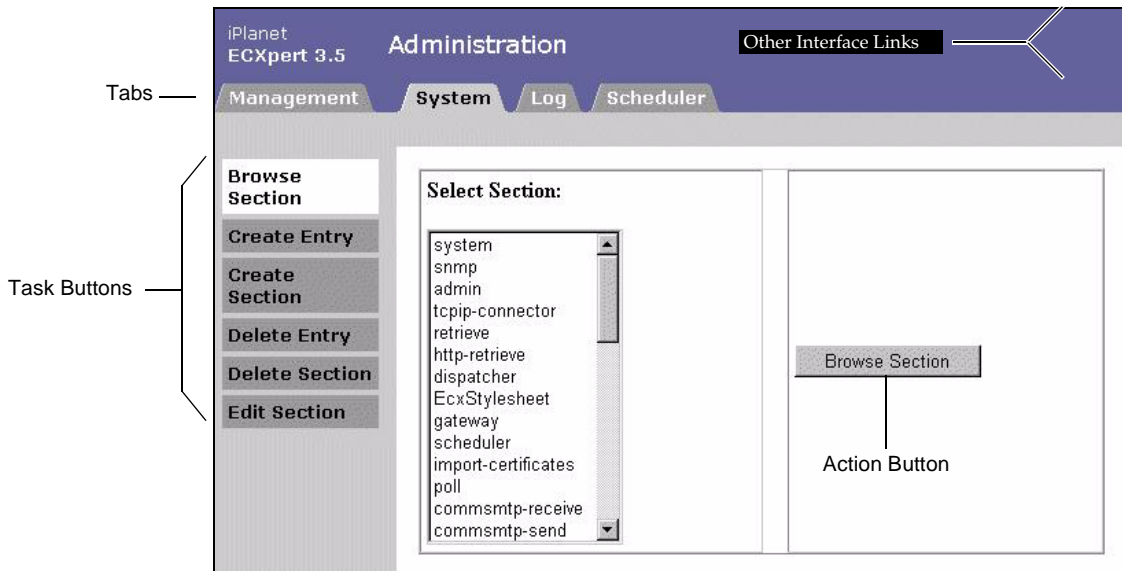
The different parts of a typical ECXpert screen are described below.

- **Tabs:** The area immediately below the header panel displays the labeled "tabs" that provide access to the different System Administration Interface functions.

This Tab...	Allows you to...
Management	Manage ECXpert servers.
System	View and change system settings in the ecx.ini file

This Tab...	Allows you to...
Log	View the system log files.
Scheduler	Set up and monitor time-based processing.

- **Tasks:** The rectangular buttons on the left side of the screen provide access to the specific tasks that can be performed on a tab.

- **Action Buttons:** Buttons found in different places on the screen perform an action that completes a task, or completes a step in a task.

- **Other Interface Links:** The labels in the upper right corner are links to other ECXpert interfaces.

System Administration Interface Help

Online help for each of the System Administration Interface tabs is available by clicking the Help link in the upper right corner. Online help is context sensitive—the help topic displayed depends on the System Administration Interface that is displayed when you click the link.

Managing ECXpert Servers

You can use the Management screen to turn on and turn off the servers that support the ECXpert System. Follow the steps below to manage ECXpert servers.

1. Log into the System Administration Interface.

2. Click the Management tab.

   The Management tab is displayed. If the ECXpert Administrative Server is *not* running, the Management tab appears as shown in Figure 3-5. If the ECXpert Administrative Server *is* running, the Management tab appears as shown in Figure 3-6.

Figure 3-5   Management tab, Administrative Server OFF
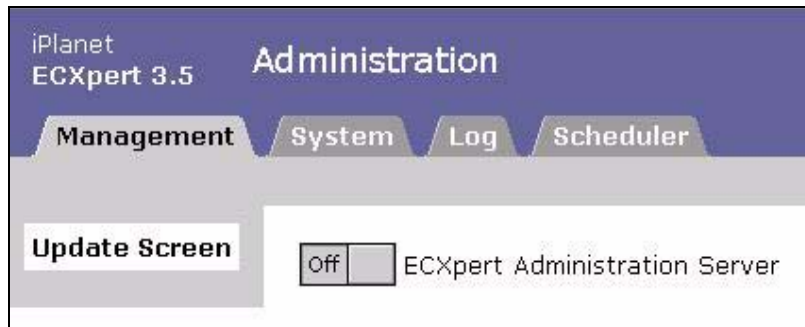
Figure 3-6   Management tab, Administrative Server ON
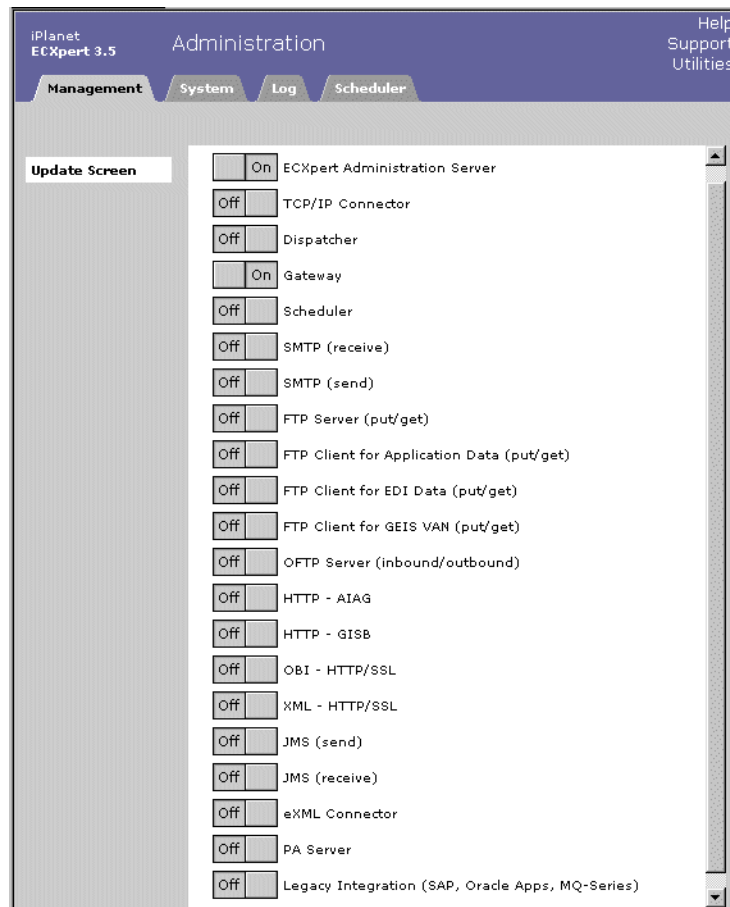
Table 3-1 describes the ECXpert 3.6 servers that always appear on the Management tab when the ECXpert Administration Server is turned on. Examples of some of the additional servers that you *might* see are shown in Table 3-2.

Table 3-1   Summary of servers that appear on the Management tab

Server	Description
ECXpert Administration Server	The server running ECXpert.
TCP/IP Connector	The ECXpert Communications Agent for sending and receiving EDI data via TCP/IP.
Dispatcher	ECXpert Dispatcher; the component that manages service list processing for each submission unit.
Gateway	ECXpert Gateway, which supports all Communications Agents, such as those for FTP and SMTP.
Scheduler	ECXpert Scheduler, which performs time-based scheduled tasks.
SMTP (receive)	ECXpert Communications Agent for receiving via SMTP.
SMTP (send)	ECXpert Communications Agent for sending via SMTP.
FTP Server (put/get)	ECXpert Communications Agent for sending and receiving via standard FTP.
FTP Client for Application Data (put/get)	ECXpert Communications Agent for sending and receiving application data via local FTP.
FTP Client for EDI Data (put/get)	ECXpert Communications Agent for sending and receiving EDI data via local FTP.
FTP Client for GEIS VAN (put/get)	ECXpert Communications Agent for sending and receiving via GEIS FTP.
OFTP Client (put/get)	ECXpert Communications Agent for sending and receiving EDI data via Odette FTP.
HTTP - AIAG	ECXpert Communications Agent for sending and receiving via HTTP for AIAG.
HTTP - GISB	ECXpert Communications Agent for sending and receiving via HTTP for GISB.
OBI - HTTP/SSL	ECXpert Communications Agent for sending and receiving via HTTP with SSL support.

Table 3-1   Summary of servers that appear on the Management tab *(Continued)*

Server	Description
XML - HTTP/SSL	ECXpert Communications Agent for sending and receiving via HTTP with SSL for XML support.
JMS (send)	ECXpert Communications Agent for sending JMS messages by way of a JMS message service.
JMS (receive)	ECXpert Communications Agent for retrieving JMS messages from a JMS message service.
eXML Connector	ECXpert XML connector.
SMG Server	ECXpert Secure Messaging Gateway server.
	Note: This server appears only in installations of ECXpert with the SMG option.
Legacy Integration (SAP, MQ-Series)	ECXpert Communications Agent communicating with supported legacy systems such as SAP and MQ Series.

To enhance ECXpert performance, you can create multiple instances of the same ECXpert server. These should have the same name as the ecx.ini section for the first instance, followed by a digit.

Two of the most likely servers to have multiple instances are Gateway and Dispatcher. The server names that would appear in the Management tab's list are shown in Table 3-2, along with a description. For more information about setting up multiple instances of an ECXpert server, see "Multiple Processes per Server" on page 556.

For more detailed information on this topic, refer to the *iPlanet ECXpert Operations Reference Guide* chapter on system monitoring and recovery procedures, under the "Using Multiple Dispatchers, Communications Agents, Other Servers" topic.

Table 3-2 Examples of servers that *might* appear on the Management tab

Server	Description
gateway2	A second ECXpert Gateway that can support all Communications Agents, such as those for FTP and SMTP.
dispatcher2	A second ECXpert Dispatcher. This is an alternate component that can manage service list processing for submission units.

NOTE	The ECXpert Administrative Server must be turned on in order for any other servers and components to appear on the Management tab. For more information on the servers listed in Table 3-1, see Appendix C, "ECXpert Initialization File (ecx.ini)."

3. Click the toggle switch for a server to turn it on or off.

The toggle switch to the left of a server name indicates its current status—On or Off. Clicking the switch flips it to the other status.

After you click a switch, a message flashes on the screen asking you to click Update Screen after ten seconds.

4. Click Update Screen after ten seconds has passed.

The screen is updated to reflect the change you just made.

After you have updated the screen, you can do any of the following:

❍ Go back to Step 3 above and turn another server on or off.

❍ Click a different tab to access a different System Administration Interface function.

Managing ECXpert System Settings

System settings stored in the `ecx.ini` file configures the behavior of most components of the ECXpert System. Editing this file directly is not recommended.

For the XML Parser, the configuration parameters are stored in the `ecxstylesheets.xml` ini file. The XML ini filename is specified in the [EcxStylesheet] section of the `ecx.ini` file as xmlinifilename entry.

Follow the steps below to view, add, change, or delete system settings through the System Administration Interface.

1. Log into the System Administration Interface.

2. Click the System tab.

The System Tab is displayed, with the Browse Section highlighted (Figure 3-7).

From this tab you can perform the following tasks:

- ❍ "Browsing a Section" on page 138
- ❍ "Creating an Entry" on page 140
- ❍ "Creating a Section" on page 144
- ❍ "Deleting an Entry" on page 146
- ❍ "Deleting a Section" on page 148
- ❍ "Editing a Section" on page 149

Figure 3-7   System Tab, with Browse Section Higlighted (the default)
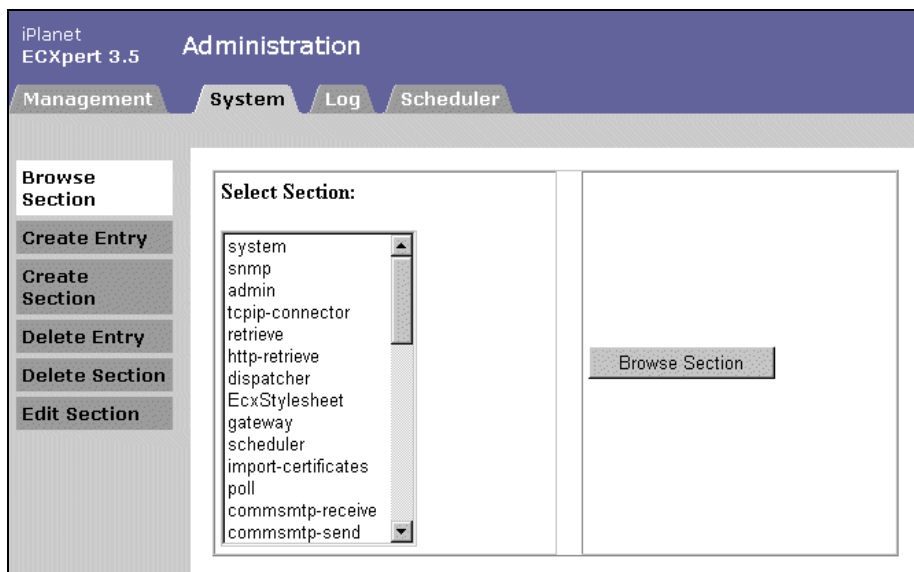
The names that appear in the Select Section list on the System tab are the section names from the ECXpert system settings file, ecx.ini. They are listed in the order in which they appear in that file.

For a more detailed description of these sections, see Appendix C, "ECXpert Initialization File (ecx.ini)." For an alphabetical list of the section names, see "Alphabetical Listing of Sections" on page 551.

Table 3-3 summarizes the functions of the tasks on the System tab.

Table 3-3   Summary of tasks on the System tab

This task...	Allows you to...
Browse Section	View system settings in the ecx.ini file. Use this command to check the current settings before you change them. See "Browsing a Section" on page 138.
Create Entry	Add a new entry to a section of the ecx.ini file. For example, you might add a section and need more parameters to define it, or you might need to modify an installation default. See "Creating an Entry" on page 140.
Create Section	Create a section to specify a Communication Agent that was not installed during the initial installation. For example, to add a new server. See "Creating a Section" on page 144.

Table 3-3   Summary of tasks on the System tab *(Continued)*

This task...	Allows you to...
Delete Entry	Delete an entry when the parameters are no longer necessary, or delete an entry from a section before you create a new entry. See "Deleting an Entry" on page 146.
Delete Section	Delete a section when it is no longer needed. See "Deleting a Section" on page 148.
Edit Section	Edit the values in the ecx.ini file. For example, to change the pathname to an executable file (such as ORACLE_HOME) if you have moved it. See "Editing a Section" on page 149.

Browsing a Section

A section is a portion of the ecx.ini file that defines configuration parameters for a particular component or process of the ECXpert System.

To browse a section:

1. Log into the System Administration Interface.

2. Click the System tab. The Browse Section is selected as the default when the screen is displayed, as shown in Figure 3-7 on page 137.

3. Select the Section that you want to view.

In the Select Section list, click the section name.

4. Click Browse Section on the right.

The settings in the selected section, [gateway], are displayed, as shown in Figure 3-8.

A second example, shown in Figure 3-9, shows what is in the [EcxStylesheet] section. When displayed, the first parameter entry, xmlinifile, is from the ecx.ini file. This parameter identifies the location of the ecxstylesheets.xml file. The rest of the entries shown are read from the ecxstylesheets.xml file, which is present in the directory $BDGHOME/config.

Figure 3-8   [gateway] settings displayed for browsing

Figure 3-9   [EcxStylesheet] settings displayed for browsing
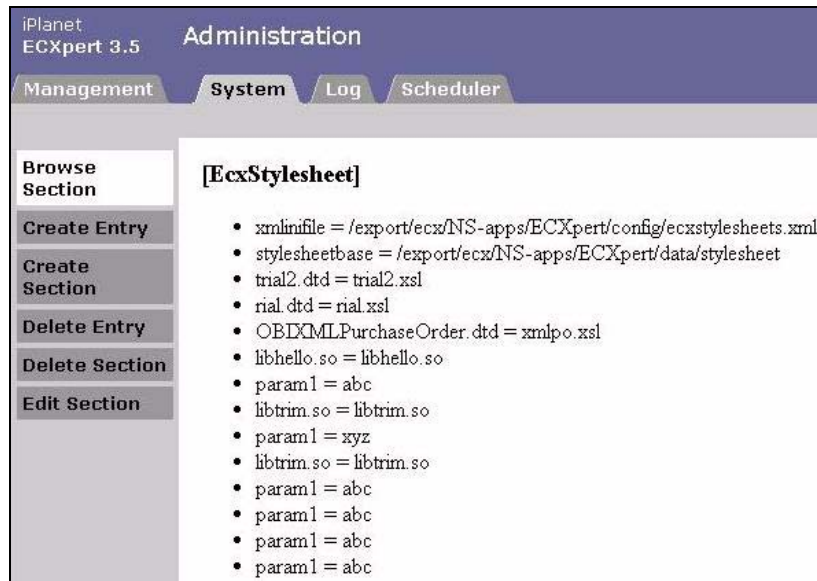
5. Browse the section.

Use the scroll bar or the browser's Find command.

When you are done browsing the section, you can do any of the following:

- ❍ Click Browse Section to browse a different section

- ❍ Click a different task to perform another task on the System tab.

- ❍ Click a different tab to access a different System Administration Interface function.

Creating an Entry

To create an entry in a section, perform the following steps.

1. Log into the System Administration Interface.

2. Click the System tab.

3. Click Create Entry on the left.

The System tab is displayed, with the Create Entry task selected (Figure 3-10).

Figure 3-10 System tab, Create Entry task selected
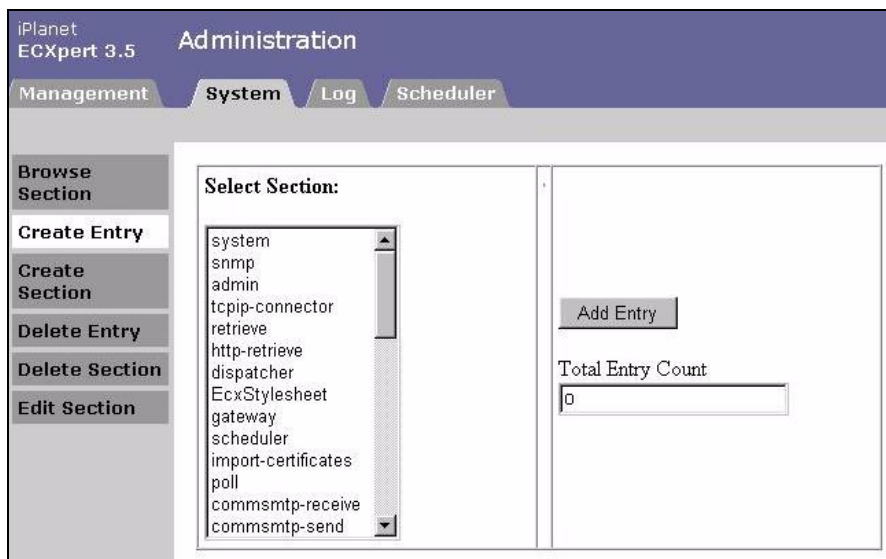
4. Select the Section in which to create the entry.

   In the Select Section list, click the section name.

5. Enter the number of entries to create in the section.

   Type the number in the Total Entry Count box.

6. Click Add Entry on the right.

   An input form is displayed, as shown in Figure 3-11. If you are creating multiple entries, the form has one row for each entry.

Figure 3-11   Input form for Create Entry task

NOTE	When creating an entry for the [EcxStylesheet] section, continue at "Creating an Entry for the [EcxStylesheet] Section" on page 143.

Table 3-4   Information on the Create_Entry input form

Item	Description
Name	The name of the entry, for example: admin_port.
Value	A value for the entry, for example: 4012
Description	A descriptive label for the entry, for example: Administration.

7. Enter the information for the entry.

    Refer to Table 3-4 for details.

8. Click Modify Entry.

    A message notifies you that the entry was added to the section.

    When you are done creating the entry, you can do any of the following:

    ❍ Click Create Entry to create another entry.

○ Click a different task to perform another task on the System tab.

○ Click a different tab to access a different System Administration Interface function.

Creating an Entry for the [EcxStylesheet] Section

You can edit the XML ini file using the following guidelines.

• The Stylesheet base is the root directory for all stylesheets. You cannot add a new Stylesheet base (there is only one place where stylesheets can be copied).

• When adding a new mapping for doctype -> stylesheet names, use the Input Entry form described in "Creating an Entry" on page 140 to enter the Name, the Value of the mapping, and provide the "map" for the Description. See Table 3-5 for more details.

• When adding new plugins, you must add a library name and a list of initialization parameters. See Table 3-5 for more details.

○ To add the library name, use the Input Entry form to specify data for the Name, Value and Description fields.

○ To add the initialization parameters, use the Input Entry form to specify the Name, Value, and Description of the new parameter. For the description, provide the library name to which the parameter will be added.

Table 3-5   Data Elements Used When Creatng An Entry To EcxStylesheet.xml

Data Element	Name	Value	Description
Mapping (dtd-->stylesheet name)	New dtd name	New stylesheet filename (full path not needed, given by `Stylesheetbase` in `ecxstylesheets.xml`)	"map" (this is the description of the new map added in the xml ini file)
Plugin - library name	Library	New library name	"library"
Plugin - parameter	New parameter name	New parameter value	Library name to add to this new parameter

Creating a Section

You create a section to specify and configure a communication agent that was not installed during initial installation (for example, to add a new server).

To create a section:

1. Log into the System Administration Interface.

2. Click the System tab.

3. Click Create Section on the left.

The System tab is displayed, with the Create Section task selected (Figure 3-12).

Figure 3-12 System tab, Create Section task selected

4. Enter the number of entries you want the new section to contain.

Type the number in the Total Entry Count box.

5. Enter a name for the new section.

Type the name in the Section Name box.

6. Click Add Section.

An input form is displayed, as shown in Figure 3-13. The form has a separate row for each entry.

Figure 3-13   Input form for Create Section task

Table 3-6   Information on the Create_Section input form

Item	Description
Name	The name of the entry, for example: admin_port.
Value	A value for the entry, for example: 4012
Description	A descriptive label for the entry, for example: Administration.

7.   Enter the information for the section.

Refer to Table 3-6 for details.

8.   Click Modify Section below the last row.

A message notifies you that the section was added to the configuration file.

When you are done creating the section, you can do any of the following:

❍   Click Create Section to create another section.

❍   Click a different task to perform another task on the System tab.

❍   Click a different tab to access a different System Administration Interface function.

Deleting an Entry

CAUTION   Make sure you do not delete an entry without verifying that it should be deleted. Deleting information that is needed by ECXpert can cause serious problems with system operation.

To delete an entry:

1. Log into the System Administration Interface.

2. Click the System tab.

3. Click Delete Entry on the left.

The System tab is displayed, with Delete Entry task selected (Figure 3-14).

Figure 3-14   System tab, Delete Entry task selected
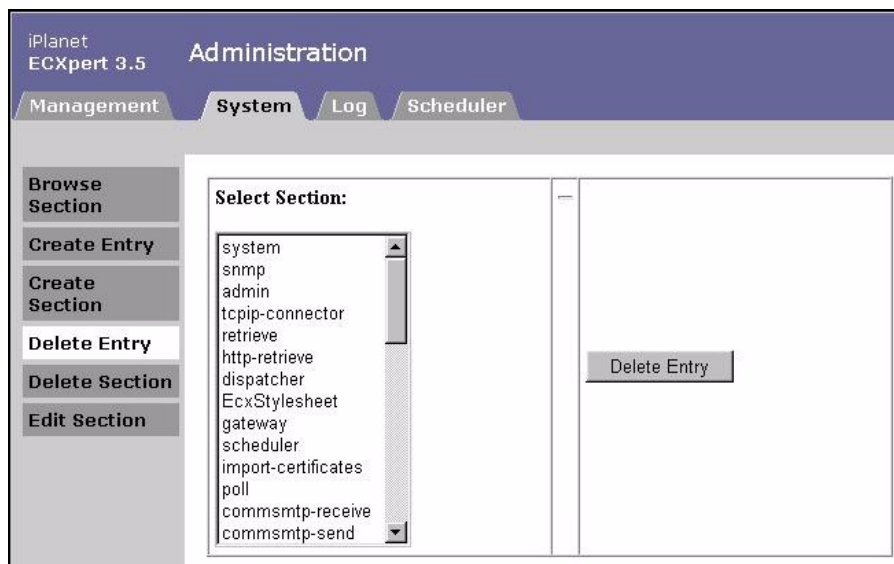
4. Select the section from which you want to delete an entry.

In the Select Section list, click the section name.

5. Click Delete Entry on the right.

A form is displayed listing all the entries in the selected section, as shown in Figure 3-15.

NOTE	When deleting an entry for the [EcxStylesheet] section, continue at "Deleting an Entry for the [EcxStylesheet] Section" on page 148.

Figure 3-15 Entry selection form for Delete Entry task

6. Select one or more entries to delete.

To the right of each entry are Yes and No radio buttons, with No selected. For each entry you want to delete, select Yes.

7. Click Delete Entries below the last row.

A message notifies you that the entry was deleted from the section.

When you are done deleting the entry, you can do any of the following:

❍ Click Delete Entry to delete an entry from another section.

❍ Click a different task to perform another task on the System tab.

❍ Click a different tab to access a different System Administration Interface function.

Deleting an Entry for the [EcxStylesheet] Section

Some elements in the XML ini file can be deleted. Use the following guidelines.

- All changes in EcxStylesheet section will be reflected in ecxstylesheets.xml and not in the ecx.ini file.

- You cannot delete the Stylesheet base (there is only one place where stylesheets should be copied).

- For all other parameters, the name of the deletable parameter will be shown.

To continue with the steps to delete an entry, go to step 6 of "Deleting an Entry" on page 146.

Deleting a Section

NOTE	Make sure you do not delete a section without verifying that it should be deleted. Deleting information that is needed by ECXpert can cause serious problems with system operation.

To delete a section:

1. Log into the System Administration Interface.

2. Click the System tab.

3. Click Delete Section on the left.

   The System tab is displayed, with the Delete Section task selected (Figure 3-16).

Figure 3-16   System tab, Delete Section task selected
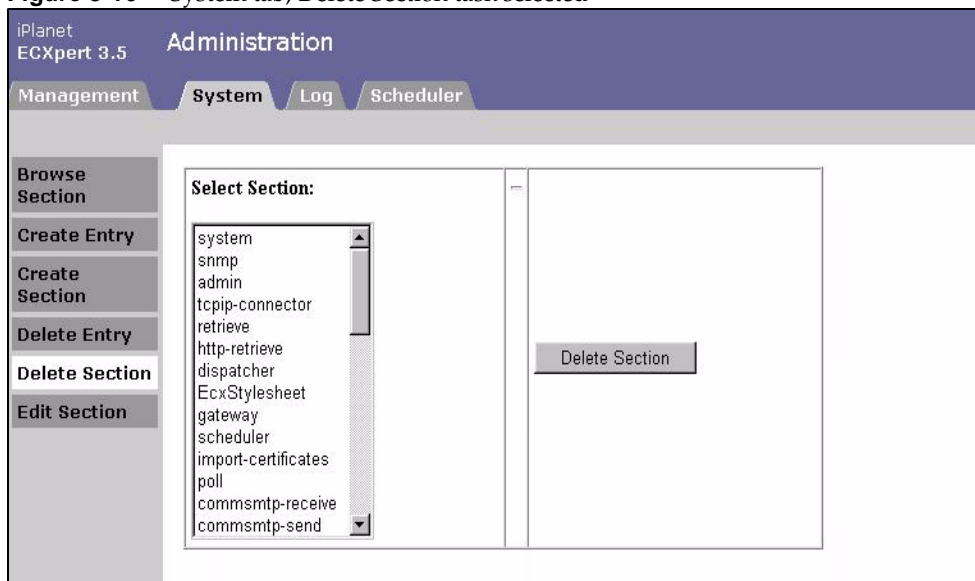
4.   Select the section you want to delete.

In the Select Section list, click the section name.

5.   Click Delete Section on the right.

A message notifies you that the section was deleted from the configuration file.

When you are done deleting the section, you can do any of the following:

❍   Click Delete Section to delete another section.

❍   Click a different task to perform another task on the System tab.

❍   Click a different tab to access a different System Administration Interface function.

Editing a Section

To edit a section:

1.   Log into the System Administration Interface.

2.   Click the System tab.

3. Click Edit Section on the left.

The System tab is displayed, with the Edit Section task selected (Figure 3-17).

Figure 3-17   System tab, Edit Section task selected
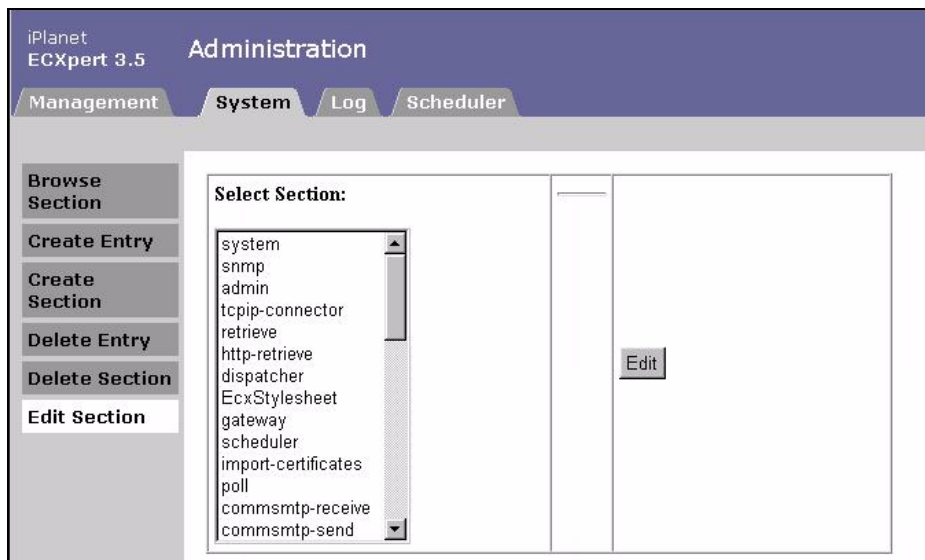
4. Select the Section that you want to edit.

In the Select Section list, click the section name.

5. Click Edit on the right.

An input form is displayed, as shown in Figure 3-18. The form has a separate row for each entry.

Figure 3-18 Input form for Edit Section task

6. Edit any information in the section.

    You can change any of the information displayed.

    Referring to Figure 3-13, the input form on which you create sections:

    o   The column on the left in Figure 3-18 is the Description column in Figure 3-13.

    o   The column on the right in Figure 3-18 is the Value column in Figure 3-13.

    o   There is no column in Figure 3-18 for the Name column in Figure 3-13—you cannot change the name of a setting.

7. Click Edit Section below the last row.

    A message notifies you that the section was updated in the configuration file.

    When you are done editing the section, you can do any of the following:

    o   Click Edit Section to edit another section.

    o   Click a different task to perform another task on the System tab.

    o   Click a different tab to access a different System Administration Interface function.

Viewing Log Files

The log screen allows you to view a log of system activity.

To view log files:

1. Log into the System Administration Interface.

2. Click the Logs tab.

   The Logs tab is displayed, with the View Log task selected (Figure 3-19).

   Figure 3-19   Logs tab, View Log task selected
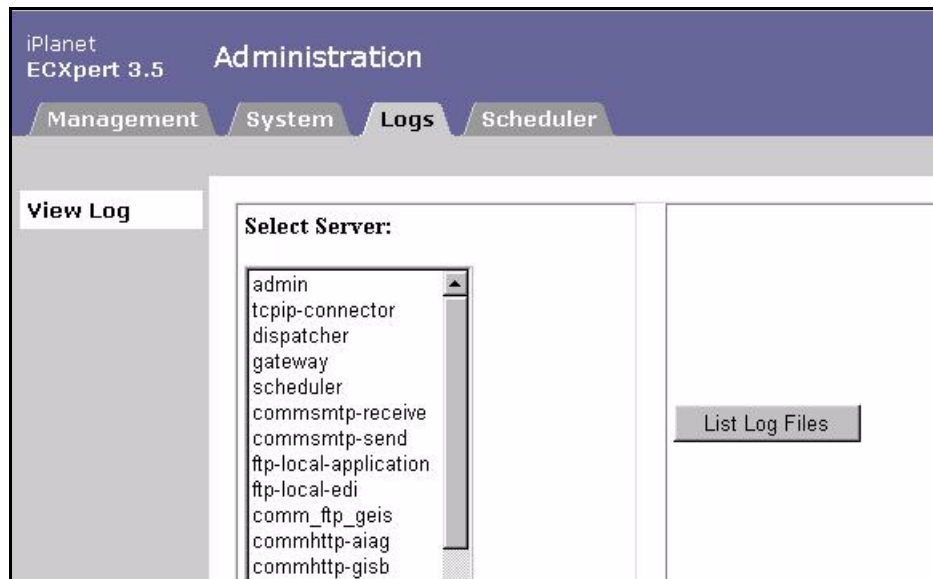
3. Select the Server for which you want to view log files.

   In the Select Server list, click the server name.

4. Click List Log Files on the right.

   A form is displayed, listing log files available for the selected server, as shown in Figure 3-20.

Figure 3-20   Log file selection for View Log task
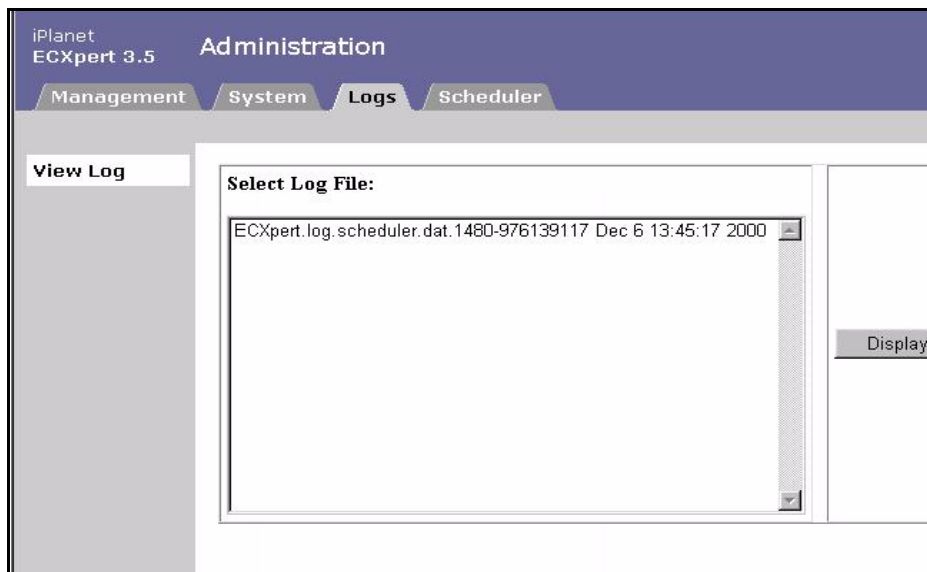
5. Select a log file to view.

    In the Select Log File list, click the file name you want to view.

6. Click Display Log File on the right.

    The selected log file is displayed, as shown in Figure 3-21.

Figure 3-21   Log file displayed for viewing

NOTE   Figure 3-21 shows the information recorded in a sample log file when the debug_timestamp parameter in the [System] section of the ecx.ini file is set to yes.

---

7. View the log file.

Use the scroll bar to move through the page displayed, or use the browser's Find command to locate specific text.

Click More at the bottom to display the next page of the log file. At the bottom of the last page, clicking More displays an "End of Log File" message.

When you are done viewing a log file, you can do any of the following:

❍ Click View Log to view another log file.

❍ Click a different tab to access a different System Administration Interface function.

Scheduling ECXpert Jobs

This section describes the use of the ECXpert Scheduler to set up and maintain time-based scheduling of ECXpert tasks, or jobs. You can use the Scheduler to create, view, change, and delete scheduled events. Processing tasks can be scheduled down to one-minute intervals.

For information on tracking the tasks that you schedule, see Chapter 8, "Tracking the Jobs that the Scheduler Manages."
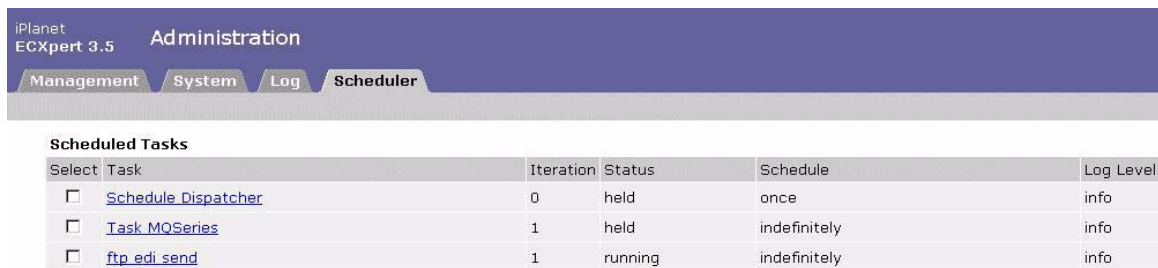
NOTE	If you use the Scheduler in the System Administration Interface, it is *not* necessary to use the Gateway service.

To display the scheduler:

1. Log into the System Administration Interface.

2. Click the Scheduler tab.

The Scheduler tab with tasks (Figure 3-22) is displayed, listing tasks that are currently scheduled.

NOTE	If you get an error message at this point, click the Management tab and make sure that the ECXpert Scheduler server is ON. See "Managing ECXpert Servers" on page 131 for details.

Figure 3-22   Scheduler tab with tasks

<table>
<tr><td colspan="6">Scheduled Tasks</td></tr>
<tr><td>Select</td><td>Task</td><td>Iteration</td><td>Status</td><td>Schedule</td><td>Log Level</td></tr>
<tr><td>☐</td><td>Schedule Dispatcher</td><td>0</td><td>held</td><td>once</td><td>info</td></tr>
<tr><td>☐</td><td>Task MQSeries</td><td>1</td><td>held</td><td>indefinitely</td><td>info</td></tr>
<tr><td>☐</td><td>ftp edi send</td><td>1</td><td>running</td><td>indefinitely</td><td>info</td></tr>
</table>

NOTE	If there are no tasks currently scheduled, the Scheduled Tasks table is empty.

From the Scheduler tab you can perform the following tasks:

Table 3-7   Information for Scheduled Tasks on the Scheduler tab

Item	Description
Select	Check this box to select the task before clicking an action button at the bottom.
Task	A descriptive label for the task.
Iteration	The number of the last iteration of the task; the number of times the task has been run.

Table 3-7   Information for Scheduled Tasks on the Scheduler tab *(Continued)*

Item	Description
Status	The current processing status of the task:
	• **done**—the task is scheduled to execute multiple times and it has executed at least once. Or, the task has finished the last iteration and is waiting for the next iteration. (Task is set to run "indefinitely" or "until xx/xx/xx".)
	• **all done**—the task is scheduled to execute once and execution is finished.
	• **held**—the task is suspended by the HOLD operation.
	• **waiting**—the task is active again after the RESUME operation. The task is waiting for the next iteration.
	• **running**—task is in the process of execution but has not yet signaled that it is done. If the task has been "running" for too long, there might be something wrong.
	• **ready**—the task is about to execute; the execution criteria (either time or event based) have been met.
	• **abort**—an error exists in the scheduled task; correct the error.
Schedule	The time-based rule determining when the task is processed.
Log Level	Logging level:
	• Info—log all messages
	• Warning—log only warning and error messages (range 11-30)
	• Error—log only error messages (range 21-30)
	• Off—disable logging
Add a New Task	See "Adding a New Task" on page 157
Modify a Task	See "Modifying a Task" on page 178
Delete a Task	See "Deleting a Task" on page 180

Adding a New Task

The process of adding a new task moves through an input form that consists of two or three pages, depending on the type of task that you specify on the first page.

First Page—Basic Task Information

Follow the steps below to start the process of adding a new task and fill in the basic task information.

1. Click Add Task.

The Add Task button is located in the lower left corner of the Scheduler tab.

Table 3-8 Information on first page of new task input form

Item	Description
Task Name	A descriptive label for the task.
Use	Select one of the radio buttons: Script, ECX Dispatcher, or ECX Gateway.
	Script—if you select this Use option:
	• Select Executable or Script from the drop-down list.
	• In the Command box, enter the name of the command to execute. **Windows NT Note:** In any pathname that you enter, you can separate directories by either a single forward slash (/) or a single backslash (\). For example, `c:/tmp/exetest.exe` OR `c:\tmp\exetest.exe`
	• In the Arguments box, enter the command arguments to pass.
	ECX Dispatcher—the ECXpert Dispatcher, with the service list that you specify.
	ECX Gateway—if you select this Use option, also select a communications agent from the drop-down list described below in this table. For a complete list of the communications agents available, see "Protocol Parameters Page—Only for ECX Gateway" on page 160.
	ECX EERP for Oftp—if you select this Use option, also specify a Sender and Receiver. EERP stands for End-to-End-Response. EERP functions as an acknowledgment in OFTP, comparable to Message Disposition Notification (MDN) in SMTP.
Command	Enter the script or executable directory path and command if its stored location is external to ECXpert.
Arguments	Enter any optional arguments to be used to run the script or executable.
Comm Agent List Box	(Gateway use only) Select the appropriate communications agent for this task.

2. Fill in the first page of the input form.

Refer to Table 3-9 for details.

3. Click Next at the bottom of the page.

Depending on the radio button you selected for Use on the first page of the input form, continue at the location indicated below:

Selection for "Use"	Continue with...
Executable	"Last Page—When to Run the Task" on page 175
ECX Dispatcher	"Service List Page—Only for ECX Dispatcher" on page 159
ECX Gateway	"Protocol Parameters Page—Only for ECX Gateway" on page 160
ECX EERP for Oftp	"Parameters Page—Only for ECX EERP for Oftp" on page 174

Service List Page—Only for ECX Dispatcher

When you select ECX Dispatcher on the first page of the input form, clicking Next on that page displays the Service List page. Here you must specify a service list for the ECXpert Dispatcher to process.

1. Specify a service list for the ECXpert Dispatcher.

If your selection for Use in Step 2 on page 159 was ECX Dispatcher, the Scheduler tab appears after you click Next, as shown in Figure 3-23.

Figure 3-23   Service list specification for ECXpert Dispatcher

> In the Service List Name box, enter the name of the service list you want the Dispatcher to execute.

2. Click Next at the bottom of the page.

> The Schedule page of the new task input form is displayed (Figure 3-32 on page 175).

> Continue instructions with "Last Page—When to Run the Task" on page 175.

Protocol Parameters Page—Only for ECX Gateway

When you select ECX Gateway on the first page of the input form, clicking Next on that page displays the Protocol Parameters page. Here you must specify all necessary communications parameters to be used by the scheduled task.

1. Fill in protocol parameters for the ECXpert Gateway.

> Based on your selection in the ECX Gateway drop-down list in Step 2 on page 159, refer to the Figure indicated in, and the table that immediately follows it, for details.

Table 3-9   Where to continue with instructions for different protocols

Protocol selected	Continue instructions using…
SMTP Send	• Figure 3-24 on page 162
	• Table 3-10 on page 163
GEIS ftp Receive	• Figure 3-25 on page 163
	• Table 3-11 on page 164
GEIS ftp Send or Both	• Figure 3-24 on page 162
	• Table 3-10 on page 163

Table 3-9   Where to continue with instructions for different protocols *(Continued)*

Protocol selected	Continue instructions using…
ftp Application Receive ftp EDI Receive	• Figure 3-26 on page 164 • Table 3-12 on page 165
ftp Application Send or Both	• Figure 3-24 on page 162
ftp EDI Send or Both	• Figure 3-24 on page 162
HTTP for AIAG Deliver	• Figure 3-24 on page 162
HTTP for AIAG Obtain	• Figure 3-27 on page 166 • Table 3-13 on page 166
HTTP for GISB	• Figure 3-24 on page 162
HTTP for SSL	• Figure 3-24 on page 162
JMS Receive	• Figure 3-28 on page 168 • Table 3-14 on page 169
JMS Send	• Figure 3-24 on page 162
Legacy Server for SAP	• Figure 3-24 on page 162
Legacy Server for Oracle Application	• Figure 3-24 on page 162
Legacy Server for MQSeries Receive	• Figure 3-29 on page 170 • Table 3-15 on page 170
Legacy Server for MQSeries Send	• Figure 3-24 on page 162
User Defined Comm Agent Receive	• Figure 3-30 on page 172 • Table 3-16 on page 172
User Defined Comm Agent Send or Both	• Figure 3-24 on page 162
Oftp Send	• Figure 3-24 on page 162
eXML Connector Send	• Figure 3-24 on page 162

Figure 3-24   Common protocol options

NOTE   The "common" protocol options shown in Figure 3-24 and described in Table 3-10 are common to the following protocols.

- SMTP Send
- GEIS ftp Send or Both
- ftp EDI Send or Both
- HTTP for AIAG Deliver
- Oftp
- HTTP for SSL

- JMS Send
- Legacy Server for SAP
- Legacy Server for MQSeries Send
- User Defined Comms Agent Send or Both
- eXML Connector

Table 3-10   Common protocol options

Item	Description
Sender	Member ID of the sending member in the supporting partnership.
Receiver	Member ID of the receiving member in the supporting partnership.
Sender Qualifier	Qualifier for the sending member.
Receiver Qualifier	Qualifier for the receiving member.
Sender Qualifier ID	Qualifier ID for the sending member.
Receiver Qualifier ID	Qualifier ID for the receiving member.
Document Type	Document Type in the supporting partnership.
Document Version	The EDI document version number.
Document Standard	The EDI document standard number.

When you have finished filling in the above options for the Protocol page, continue at "Finishing Up the New Task" on page 178.

If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

Figure 3-25   GEIS ftp Receive protocol options

Table 3-11   GEIS ftp Receive protocol options

Item	Description
Sender	Member ID of the sending member.
Receiver	Member ID of the receiving member.
Host Name	Host name or IP address.
Port	Port number to use.
User Name	User login name on specified host.
Password	User login password on specified host.

When you have finished filling in the Advanced page, continue with "Finishing Up the New Task" on page 178. If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

Figure 3-26   ftp Application Receive and ftp EDI Receive protocol options

Table 3-12 ftp Application Receive and ftp EDI Receive protocol options

Item	Description
Parameters For Receive	
Host Name	Host name or IP address.
Port	Port number to use.
User Name	User login name.
Password	User login password.
Inbound Directory	The directory to be used to store incoming files.
Receive Pattern	A wildcard pattern to be used to filter incoming files—only files matching the pattern are to be received.
Parameters For Submit To ECXpert	
Sender	Member ID of the sending member in the supporting partnership.
Receiver	Member ID of the receiving member in the supporting partnership.
File Type	Document Type in the supporting partnership.

When you have finished filling in the above options for the Protocol page, continue at "Finishing Up the New Task" on page 178.

If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

When you have finished filling in the above options for the Protocol page, continue at "Finishing Up the New Task" on page 178.

If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

Figure 3-27   HTTP for AIAG Obtain protocol options

Table 3-13   HTTP for AIAG Obtain protocol options

Item	Description
Parameters For Obtain	
API Path	URL to the AIAG API. Must be specified.
Obtain Path	URL to this AIAG service. Optional.
Acknowledge Path	URL to this AIAG service. Optional.
User Name	user name for logging into the host system.

Table 3-13   HTTP for AIAG Obtain protocol options *(Continued)*

Item	Description
Password	password for logging into the host system.
Query Parameters For Requesting a Doc (AIAG server specific)	
Transaction ID	Use for a processed document with a known transaction ID. Using this method of query obviates the need to use the remaining parameters (in this section of this table) indicated under OR.
From	Partner from which the AIAG document was obtained.
To	Partner that received the AIAG document.
Deliver Date Start	Beginning date for document delivery.
Deliver Date End	Ending date for document delivery.
Obtain Date Start	Beginning date for obtaining the document.
Obtain Date End	Ending date for obtaining the document.
Acknowledge Date Start	Beginning date for acknowledging the obtained document.
Acknowledge Date End	Ending date for acknowledging the obtained document.
Mime Type	Data type to query specific to an application for a non-EDI or EDI partnership (for example., 8-bit ASCII, html, EDI).
Sub-type Override	Data sub-type to query specific to an application for a non-EDI partnership (for example, MSword, MSexcel), or, the standard data type to query for an EDI partnership (for example, EDIFACT for EDIFACT EDI data).
Document Reference Number	Alphanumeric or numeric designation of the document.
Document Description	Keyword(s) that describe the document for which to query.
Application	Application associated with the document for this query.
Parameters For Submit To ECXpert	
Sender	Member ID of the sending member in the supporting partnership.

Table 3-13   HTTP for AIAG Obtain protocol options *(Continued)*

Item	Description
Receiver	Member ID of the receiving member in the supporting partnership.
Application Type	Application type.

When you have finished filling in the above options for the Protocol page, continue at "Finishing Up the New Task" on page 178.

If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

Figure 3-28   JMS Receive protocol options

Table 3-14   JMS Receive protocol options-Parameters for JMS Receive

Item	Description
Parameters For MQSeries Receive	
JNDI Properties FileName	Path to JNDI properties file that specifies values needed to perform JNDI lookup of JMS administered objects
Connection Factory Name	JNDI Lookup name of the QueueConnectionFactory administered object needed to establish a connection to the JMS message service
Queue Lookup Name	.JNDI Lookup name of queue administered object that represents the queue from which to retrieve JMS messages
JMS UserID	User ID needed for authentication with the JMS message service upon establishing a connection
Password	User password needed for authentication with the JMS message service upon establishing a connection (use the `bdgsetpasswd` utility to set this value)

When you have finished filling in the above options for the Protocol page, continue at "Finishing Up the New Task" on page 178.

If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

Figure 3-29 Legacy Server for MQSeries Receive protocol options

Table 3-15 Legacy Server for MQSeries Receive protocol options

Item	Description
Parameters For MQSeries Receive	
Queue Manager Name	Name of the MQSeries Queue Manager involved.
Queue Name	Name of queue from which messages are to be retrieved on the MQSeries Queue Manager.
Queue Manager Name	Name of the MQSeries Queue Manager involved. *Note:* This name is case sensitive.
Queue Name	Name of queue on the MQSeries Queue Manager. *Note:* Enter this name in upper case only.
Message ID Regular Expression	A regular expression to retrieve only those messages whose Message ID matches it. Leave blank to retrieve all messages.

Table 3-15   Legacy Server for MQSeries Receive protocol options *(Continued)*

Item	Description
Correlation ID Regular Expression	A regular expression to retrieve only those messages whose Correlation ID matches it. Leave blank to retrieve all messages.
Inbound Directory	Full path to the directory in which the retrieved messages are to be stored.
Timeout Seconds	Timeout interval, in seconds, that ECXpert MQSeries Client is to wait for the Queue to receive the messages.
Message Count	Total number of messages to be retrieved. Leave blank to retrieve all messages.
File Name Prefix	Prefix to be added to file names generated for the messages retrieved from Queue. The file name formats are as follows:
	- Header file: *prefix_time_pid*.*uniqueId*.`hdr`
	- Message file: *prefix_time_pid*.*uniqueId*.`msg`

Parameters For Submit To ECXpert
Note: Enter values for these parameters only if you want the messages that you get from MQSeries to be submitted to ECXpert for processing.

Item	Description
Sender	Member ID of the sending member in the supporting partnership.
Receiver	Member ID of the receiving member in the supporting partnership.
Document Type	Document Type in the supporting partnership.

When you have finished filling in the above options for the Protocol page, continue at "Finishing Up the New Task" on page 178.

If you want to select a different protocol, go back to "First Page—Basic Task Information" on page 158.

Figure 3-30 User Defined Comms Agent Receive protocol options

Table 3-16 User Defined Comms Agent Receive protocol options

Item	Description
Agent	Name of the user-defined communications agent as specified in its section ([. . .]) in the ecx.ini file.
Tag	Tag for first parameter to pass.
	Default value—P1
Value	Value to pass in first parameter.
Tag	Tag for second parameter to pass.
	Default value—P2
Value	Value to pass in second parameter.

Table 3-16   User Defined Comms Agent Receive protocol options

Item	Description
Tag	Tag for third parameter to pass.
	Default value—P3
Value	Value to pass in third parameter.
Tag	Tag for fourth parameter to pass.
	Default value—P4
Value	Value to pass in fourth parameter.
Tag	Tag for fifth parameter to pass.
	Default value—P5
Value	Value to pass in fifth parameter.
Tag	Tag for sixth parameter to pass.
	Default value—P6
Value	Value to pass in sixth parameter.
Tag	Tag for seventh parameter to pass.
	Default value—P7
Value	Value to pass in seventh parameter.
Tag	Tag for eighth parameter to pass.
	Default value—P8
Value	Value to pass in eighth parameter.
Tag	Tag for ninth parameter to pass.
	Default value—P9
Value	Value to pass in ninth parameter.
Tag	Tag for tenth parameter to pass.
	Default value—P10
Value	Value to pass in tenth parameter.

When you have finished filling in the above options for the Protocol page, continue at .

If you want to select a different protocol, go back to .

Parameters Page—Only for ECX EERP for Oftp

EERP functions as an acknowledgment in OFTP, comparable to Message Disposition Notification (MDN) in SMTP.

When you select ECX EERP for Oftp on the first page of the input form, clicking Next on that page displays the Parameters page for ECX EERP for Oftp. Here you must specify a sender and receiver.

1. Specify a Sender and Receiver for ECX EERP for Oftp.

   If your selection for Use in Step 2 on page 159 was ECX EERP for Oftp, the Scheduler tab appears after you click Next, as shown in Figure 3-31.

   Figure 3-31   Sender and Receiver specification for ECX EERP for Oftp

   In the Sender box, enter the Member ID of the sending member of the partnership. In the Receiver box, enter the Member ID of the receiving member of the partnership.

2. Click Next at the bottom of the page.

   The Schedule page of the new task input form is displayed (Figure 3-32 on page 175).

   Continue instructions with "Last Page—When to Run the Task" on page 175.

Last Page—When to Run the Task

Whatever options you select on the first page of the new task input form, the Schedule page, shown in Figure 3-32, appears last.

Figure 3-32   Schedule page of input form for new task

Table 3-17   Schedule page options

Item	Description
Minutes	Enter the range of minutes during an hour that task is to run.
Hours	Enter the range of hours during a day that task is to run.
Days of month	Enter numbers for days of month that task is to run. Separate numbers with commas. Selections made here add to, rather than constraining, selections made in Weekdays.
Months	Check the months in which task is to run.
Weekdays	Check days of the week that task is to run. Selections here add to, rather than constraining, selections in Days of month.

Table 3-17   Schedule page options *(Continued)*

Item	Description
Run	Defines when processing of the task is to end. Select one of the radio buttons:
	• until—task is processed until date you specify.
	• indefinitely—task is processed as scheduled until you delete it.
	• once—task is processed one time only.

1. Fill in the Schedule page.

   Refer to Figure 3-32 on page 175 and Table 3-17 above.

2. Finish up now, or enter a tcl script.

   If you do not want to use a tcl script, continue with Step 1 on page 178.

   If you do want to use a tcl script, continue with "Advanced Page—For tcl Scripts" on page 176.

Advanced Page—For tcl Scripts

By using a tcl script, you can specify additional options that are not directly supported by the ECXpert Scheduler.

1. If you want to use a tcl script, click Advanced.

   The Advanced button appears on the Schedule page. The Advanced page of the input form is displayed (Figure 3-33).

Figure 3-33 Advanced page of input form for new task

2. Fill in the Advanced page.

Enter your tcl script(s) in the Running Criterion and Blackout Criterion boxes. Click the more about tcl script link for help on writing tcl scripts. Select a Frequency of indefinitely (default) or once.

To return to the Schedule page of the New Task input form, click either Datetime or Back. Continue with instructions at .

To complete creation of the new task, continue with instructions at Step 1 below.

Finishing Up the New Task

1. Click Finish to complete the new task creation.

You might do this from either the Schedule page or the Advanced page. You are returned to the point from which you started (Figure 3-22 on page 156), and the task you added is now displayed in the list.

2. Double-check the new task.

If you need to make corrections, see "Modifying a Task" below.

When you are done creating a new task, you can do any of the following:

• Click Add Task to create another new scheduler task.

• Select tasks and use the controls at the bottom of the Scheduled Tasks list to perform another task on the Scheduler tab. See "Modifying a Task" on page 178 and "Deleting a Task" on page 180 for details.

• Click a different tab to access a different System Administration Interface function.

Modifying a Task

There are two levels at which you can modify a task:

Run parameters can be modified from the Scheduled Tasks screen, and you can modify multiple tasks in one operation. See "Modifying Run Parameters" on page 178.

You can only modify detail parameters by navigating through the same screens involved in creating a new task. Only one task at a time can be modified. See "Modifying Detail Parameters" on page 180.

Modifying Run Parameters

Follow the steps below to modify run parameters for one or more tasks:

1. Log into the System Administration Interface.

2. Click the Scheduler tab.

3. Select a task.

Check the box in the Select column on the Scheduler tab (Figure 3-22) for one or more tasks that you want to modify at the same time.

NOTE	You can use Select All at the bottom to quickly select all tasks listed. Use Unselect All to uncheck all Select boxes.

4. Make changes.

Click controls at the bottom of the list:

Click this...	To do this...
Logging drop-down list	Change Logging level:
	• Information—log all messages
	• Warning—log only warning and error messages
	• Error—log only error messages
	• None—disable logging
Hold	Change entry for Status to held
Resume	Change entry for Status to waiting

When you are done modifying run parameters for a task or group of tasks, you can do any of the following:

• Click Add Task to create a new scheduler task.

• Select tasks and use the controls at the bottom of the Scheduled Tasks list to modify run parameters for one or more tasks on the Scheduler tab. See "Modifying Run Parameters" on page 178 and "Deleting a Task" on page 180 for details.

• Select a task and modify its detailed parameters. See "Modifying Detail Parameters" on page 180.

• Click a different tab to access a different System Administration Interface function.

Modifying Detail Parameters

Follow the steps below to modify detail parameters for a single task:

1. Log into the System Administration Interface.

2. Click the Scheduler tab.

3. Click a task ID for the task (in Task column).

   The first page of the input form for adding a new task is displayed with information for the selected task filled in.

4. Move through the screens of the task input form, making changes.

   The same instructions for adding a new task apply to these screens now. See "Adding a New Task" on page 157 for details.

5. Move through the screens of the task input form, making changes.

   The same instructions for adding a new task apply to these screens now. See "Adding a New Task" on page 157 for details.

Deleting a Task

To delete a task:

1. Log into the System Administration Interface.

2. Click the Scheduler tab.

3. Select a task.

   Check the box in the Select column on the Scheduler tab (Figure 3-22) for one or more tasks that you want to delete at the same time.

4. Click Delete at the bottom of the list.

When you are done deleting a task or group of tasks, you can do any of the following:

- Click New Task to create a new scheduler task.

- Select tasks and use the controls at the bottom of the Scheduled Tasks list to perform another task on the Scheduler tab. See "Modifying a Task" on page 178 and "Deleting a Task" on page 180 for details.

- Click a different tab to access a different System Administration Interface function.

Using the ECXpert Utilities

ECXpert provides access to several utilities through the Administrative Interface. For information on all of the ECXpert utilities available from the command line, see Chapter 11, "Command Line Utilities."

Displaying the Utilities Menu

Follow the steps below to display the Utilities Menu.

1. Enter the ECXpert URL in your browser.

    Enter the following URL in your browser:

    http://*hostname*:*port*/

    where *hostname* is the name of the host machine where ECXpert is installed, and *port* is the port number ECXpert is using.

    The ECXpert home page (Figure 3-34) is displayed.

Figure 3-34   ECXpert home page
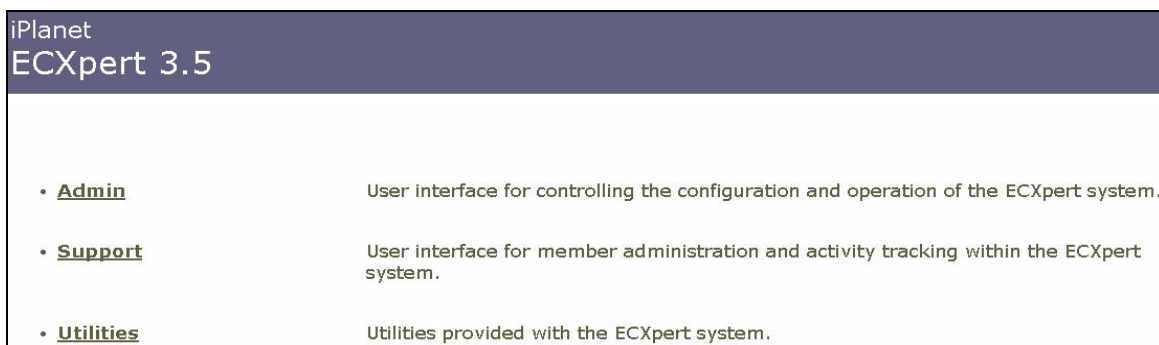
Click the Utilities link. The ECXpert Utilities Menu (Figure 3-35) is displayed.

Figure 3-35   ECXpert Utilities Menu
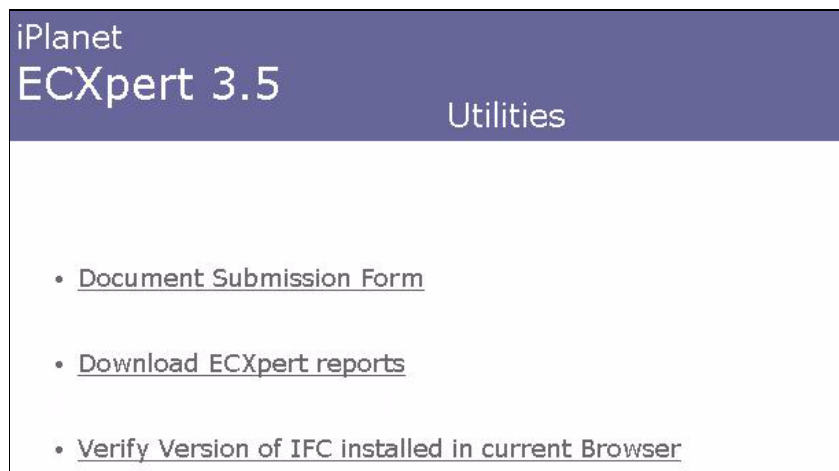
From this menu you can select any of the utilities available through the Administrative Interface.

Using the Document Submission Form

The Document Submission Form is a graphical user interface for the ECXpert `submit` command. Follow the steps below to use this interface.

1. Display the ECXpert Utilities Menu (Figure 3-35).

2. Click the Document Submission Form link.

    The Document Submission Form (Figure 3-36) is displayed.

Figure 3-36   Document Submission Form

From this form you can enter parameters for the submit command to submit documents to ECXpert.

3.   Enter parameters for the submit command.

Refer to Table 3-18 for detailed information about the parameters.

Table 3-18   Parameters for the submit command

Parameter	Description
Sending Member	The member ID of the sending member defined in the associated partnership.
Password	Password for the sending member.
Receiving Member	The member ID of the receiving member defined in the associated partnership.

Table 3-18 Parameters for the `submit` command *(Continued)*

Parameter	Description
File Name	The name of a file to be submitted to ECXpert (the submission unit). If you do not specify the path name, ECXpert looks for the file in the directory where the `tcpip-connector` server is executing.
File Type	he Document Type for the file being passed to ECXpert, as defined in the associated partnership.

4. Click Submit.

A message is displayed providing feedback on the command. If any errors are encountered they are displayed first.

Figure 3-37 Document Submission Form feedback
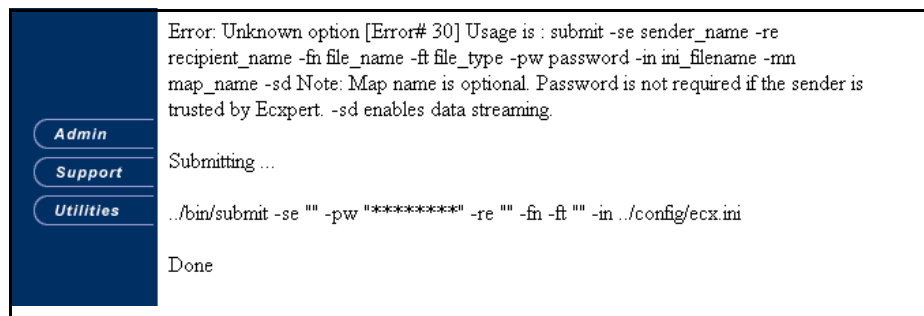
Using the Download ECXpert Reports Utility

Follow the steps below to download the compressed ECXpert reports file.

1. Display the ECXpert Utilities Menu (Figure 3-35).

2. Click the Download ECXpert Reports link.

The Unknown File Type dialog box (Figure 3-38) is displayed.

Figure 3-38   Unknown File Type dialog box
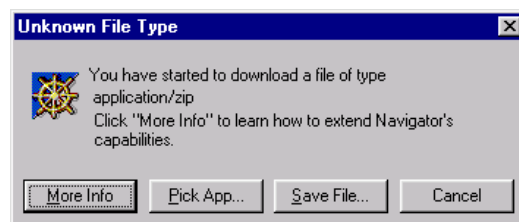
3. Save the compressed report file.

Click Save File, then specify a file name and location for the file
(`ecx_1_1_reports.zip`)

4. Decompress the reports.

Use a WinZip-compatible decompression utility.

Verifying the Version of IFC Installed in Your Browser

Follow the steps below to verify the version of IFC (Internet Foundation Class)
library installed in your browser.

1. Display the ECXpert Utilities Menu (Figure 3-35).

2. Click the Verify Version link.

The full link text is Verify Version of IFC installed in current Browser. The IFC
Install Verification page (Figure 3-39) is displayed.

If there is a problem, you are asked if you want to go to the Netscape IFC
Download page. Proceed to that page and follow the directions there to
download the proper IFC files.

Figure 3-39 IFC Install Verification page
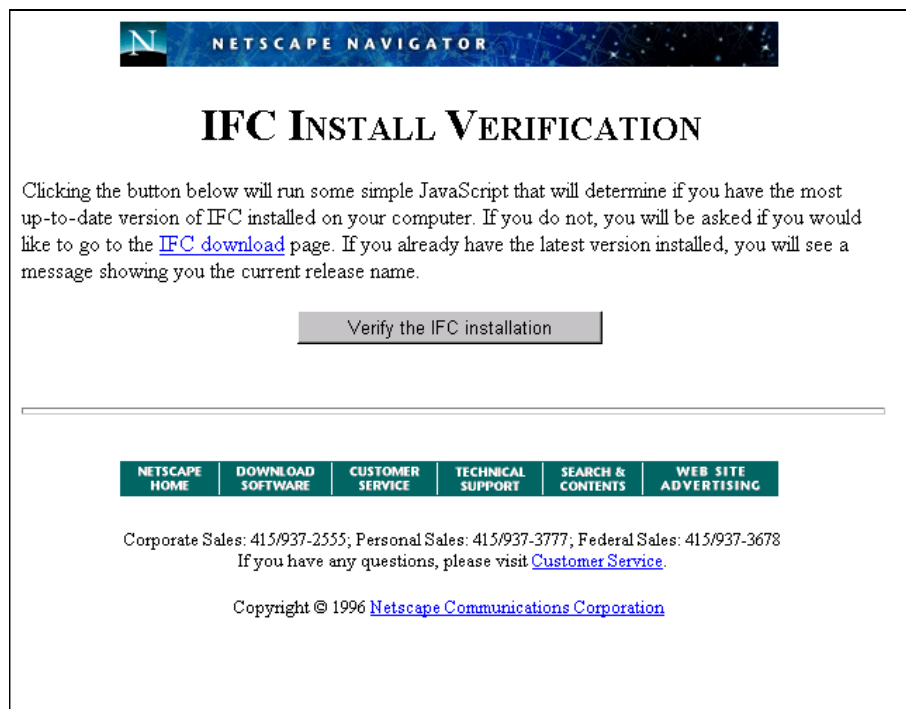
3. Click Verify.

The full button text is Verify the IFC installation. A message box appears indicating the IFC version detected and whether it is properly installed.

Using the Product Administrative Interface

This chapter introduces the ECXpert Product Administrative Interface and provides a "roadmap" for creating trading partnerships and all their supporting components. The following topics are covered:

- Overview

- Logging into the Product Administrative Interface

- Navigating Around and Between Tabs

- Online Help with Product Administrative Interface Tabs

Overview

The Product Administrative Interface allows you to view trading partnerships and all the different components that support them. This interface also allows you to track the documents processed by ECXpert. For information on controlling the operation of the ECXpert servers, configuring system settings, viewing the system log files, and scheduling time-based ECXpert processing tasks, refer to Chapter 3, "Working with the System Administration Interface."

Access to the Product Administrative Interface is controlled separately from access to the System Administration Interface.

Logging into the Product Administrative Interface

To log in to the ECXpert Product Administrative Interface:

1. Enter the ECXpert URL in your browser.

   Enter the following URL in your browser:

   http://*hostname*:*port*/

   where *hostname* is the name of the host machine where ECXpert is installed, and *port* is the port number ECXpert is using.

   The ECXpert home page (Figure 4-1) is displayed

   Figure 4-1   ECXpert home page
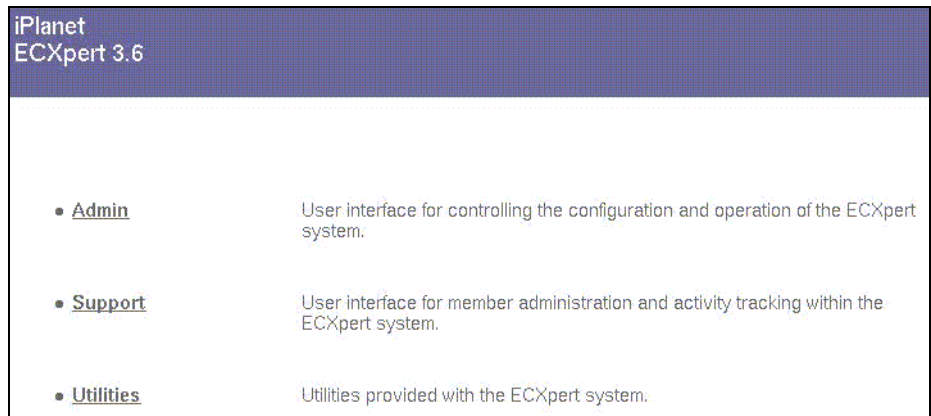
2. Click Support.

   A Login box (Figure 4-2) is displayed, with the ECXpert Product Administrative Interface in the background.

   Figure 4-2   Login box

3. Enter your ECXpert member ID and password.

Both of these entries are case sensitive.

Click in the **Name** field and type your ECXpert member ID. Then press **Tab** to move to the **Password** field and type your password.

Click **Enter**, or press the **Enter** key, to log in.

If your ECXpert ID or password is invalid, an error message is displayed. Double-check your typing and try again.

When your ECXpert ID and password are accepted, the initial screen for the Product Administrative Interface is displayed (Figure 4-3).

Figure 4-3   Initial screen for the Product Administrative Interface
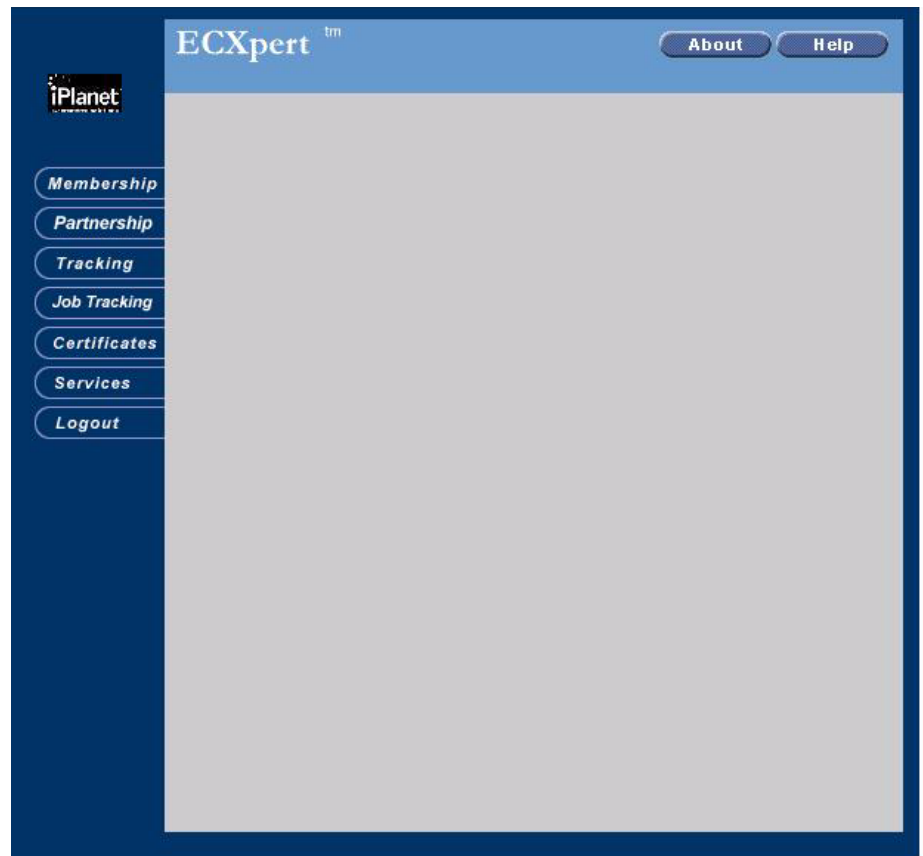
For information about the standard layout of screens in the ECXpert Product Administrative Interface, see "Navigating Around and Between Tabs."

Navigating Around and Between Tabs

All the ECXpert System Product Administrative Interface screens share a common general layout, as shown in Figure 4-4.

Figure 4-4   Basic layout of ECXpert Product Administrative Interface screens
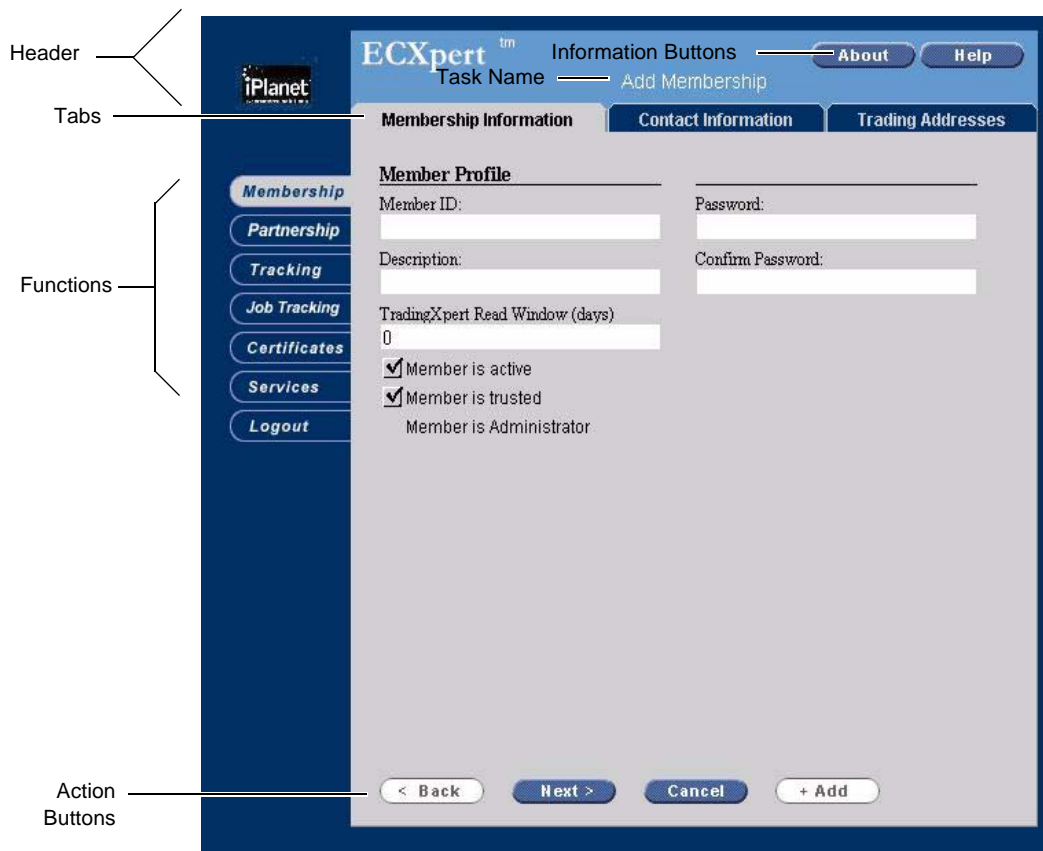
The different parts of a typical ECXpert screen are described below.

- **Header:** The area at the top of the screen displays the heading, "ECXpert," along with a description of the task you can perform in the tabs that are currently displayed, plus information buttons:

  ○ **Help** - opens a help window with information specific to the tab displayed.

  ○ **About** - displays ECXpert version information.

- **Task Name:** The name of the task that you are performing through the tabs that are currently displayed. If a task has only one tab, generally no task name is displayed.

- **Tabs:** The area immediately below the header displays the tab headers. Clicking a tab header activates that tab, putting it in front. Some tasks have only one tab, while others require two rows to display all the tab headers. After you click an administrative function, the tab that is displayed is often a "select task" tab for that function, and contains only a series of buttons, such as Add, Change, Copy, and Delete.

- **Administrative Functions:** The area on the left side of the screen contains a column of buttons that provide access to the major Product Administrative Interface functions.

This Function...	Allows you to...
Membership	View members. Covered in Chapter 5, "Setting Up Members."
Trading	View trading partnerships. Covered in Chapter 6, "Setting Up Trading Partnerships."
Tracking	Track documents processed by ECXpert. Covered in Chapter 7, "Tracking the Documents that ECXpert Processes."
Job Tracking	If you log in as an ECXpert administrator, a Job Tracking function is available. This allows you to track the jobs that are managed by the ECXpert Scheduler. This topic is covered in Chapter 3, "Working with the System Administration Interface." See "Scheduling ECXpert Jobs" on page 155.
Certificates	If you log in as an ECXpert administrator, a Certificates function is available. This allows you to manage member certificates. Covered in Chapter 9, "Working with Certificates."
Services	View services and service lists. Covered in Chapter 10, "Setting Up Services and Service Lists."
Logout	Log out of ECXpert. Click it to log out.

- **Action buttons:** At the bottom of most tabs there are buttons for the various actions you can take relative to the tab, or the series of tabs. Some common action buttons are:

    ❍ **< Back** - Move back to the previous tab in the sequence.

    ❍ **Next >** - Move forward to the next tab in the sequence. This button also causes ECXpert to validate that mandatory fields have been entered.

    ❍ **Cancel** - Abandon the task at hand, along with any information you have entered and selections you have made thus far.

    ❍ **Add**, **Change**, **Copy**, or **Delete** - Take the action the series of tabs is designed to carry out. If all the required information on the tabs has not been filled in properly, an error message is displayed.

NOTE	Copy lets you create a new item by using a copy of an existing item as a template. A Search tab allows you to retrieve the item that you want to copy.

Online Help with Product Administrative Interface Tabs

Detailed instructions on how to fill in the data on specific tabs are provided online. To display tab-level help for the Product Administrative Interface tab you are currently viewing, click Help at the top of the screen. The help text is displayed in a separate browser window, like the one shown in Figure 4-5.

Figure 4-5   Typical help window
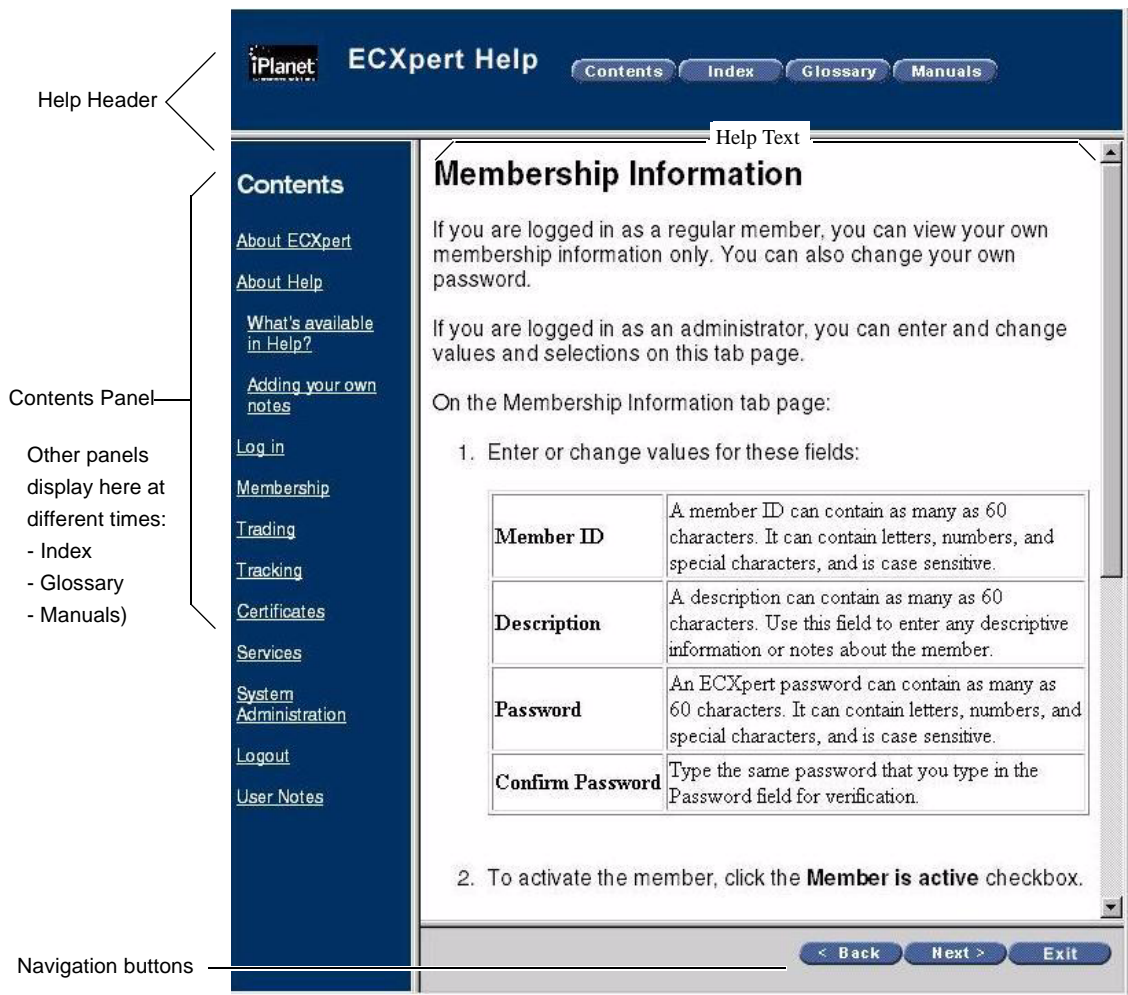
The help window is divided into a number of panels, described below:

- **Help Header:** A standard header is displayed at the top. This panel always displays the heading, "ECXpert Help," together with buttons that take you to special pages within the help topics:

  - **Contents:** Redisplays the Contents panel displayed on the left, as when the ECXpert help window first opens. Clicking a topic in this panel displays that help topic in the help text panel.

  - **Index:** Displays an Index list on the left. Clicking a term in this panel displays the indexed help topic in the help text panel.

  - **Glossary:** Displays a Glossary list on the left. Clicking a term in this panel displays the definition of the term the help text panel.

  - **Manuals:** Displays a Manuals list on the left. Clicking a manual title in this panel opens the electronic version of the manual with Adobe Acrobat.

- **Contents:** A collapsible/expandable table of contents of the entire online help for ECXpert is displayed in a tall narrow panel to the left of the screen. Clicking on any top-level heading expands the heading to display the list of topics available below that heading, and collapses any other heading that was previously expanded.

  User Notes is the last high-level heading at the bottom of the Contents panel. Clicking this link displays a list of user-defined notes that can be customized to meet the specific needs of your ECXpert installation. The second-level headings match the tab name to which the note applies. For more information, see "Adding Your Own Notes" on page 195.

- **Help Text:** The main help text is displayed in the largest panel, in the middle of the window and to the right. Summary steps, describing briefly how to complete the tab, are listed first.

  Additional information about the tab are listed after the summary steps:

  - **What's next?** A link to the next help topic in sequence to complete the task at hand.

  - **See also:** Link(s) to related topics that you might be interested in viewing, but which are not necessary to complete the task at hand.

  - **User notes:** A link that opens a window for you to add your own notes to this help topic. For more information, see "Adding Your Own Notes" on page 195.

- **Help Navigation Buttons:** Buttons that allow you to move through and print the help topics. The following buttons are available:

  ○ **Back** - Moves to the previous help topic in the sequence that you have viewed.

  ○ **Next** - Moves to the next help topic in the sequence that you have viewed. This button only becomes active after you have used Back.

  ○ **Exit** - Closes the ECXpert Help window. You can also close the help window by the standard methods provided by the operating environment in which the browser supporting ECXpert is running.

  ○ **Print** - Prints the contents of the help text panel. You can also print the help text by clicking in the panel, to be sure it is active, and then using the standard keyboard shortcut provided by the browser supporting ECXpert.

Adding Your Own Notes

ECXpert Help provides HTML pages that you can use to add your own user notes. On the HTML pages, you can add text, graphics, and links to your own information.

The HTML pages that you can edit are stored in this directory:

```
$NSBASE/NS-apps/ECXpert/UI/html/help/notes
```

The user notes pages are accessible from the ECXpert Help Contents frame and from specific areas of help. Whenever you see a User Notes link, you can click the link to find out the name of the HTML file to edit to add your own information or links.

CAUTION	Make sure that you back up the customized files in your notes directory before you install a new version of software as this directory will be overwritten by the installer. You can then copy your modified files into the new notes directory.

You can also use the User Notes pages to store reference information needed to useECXpert at your site. For example, you could store back-up contact names and information on the User Notes page for the Contact Information screen.

Setting Up Members

This chapter describes the tasks involved in setting up and maintaining members in ECXpert. The following topics are covered:

- Overview
- Controlling User Access to ECXpert
- Selecting LDAP vs. Database Storage of Member Information
- Enabling Lightweight Directory Access Protocol (LDAP) Support
- Importing Member Data from a Text File
- Displaying the Membership Administration Tab
- Displaying Information for an Existing Member
- Working with the Membership Definition Tabs
- Adding a New Member on a Blank Form
- Copying a Member—Adding a New Member Based on Another
- Changing a Member's Information
- Deleting a Member

Overview

A member is a person who is defined within ECXpert and assigned a member type that allows that person to perform specific ECXpert tasks, such as controlling ECXpert, adding new ECXpert members, and setting up trading relationships between members.

Each member is assigned a unique member ID and password. Any member can be specified as a sender or receiver in a trading relationship.

NOTE	There are several members already set up when you install the system (the password for each is the same as the Member ID):

- **GEIS**. This account is required if you will be receiving information from GE Information Service. Do not delete it or edit any of the membership information for this member.

- **ftp-local**. This account is an example of a member set up for local ftp communication that you can use to design your own.

- **ECX** and **bdgadmin**. These are sample administrator accounts that you can use to design your own.

- **PartnerA**. This is a sample user account that you can use to design your own members.

Controlling User Access to ECXpert

ECXpert ensures that only authorized users can view or change specific data. Ordinary ECXpert users are only allowed to:

- View ECXpert activity reports for trading partnerships in which they are listed as either the sending or receiving Member.

- View their own Member information and change their own password.

The ECXpert site administrator has full access to all ECXpert data and can perform all available functions.

The ECXpert member types are detailed below:

This member type:	Can perform these tasks:
Administrator	• All member administration tasks
	• All partnership administration tasks
	• All activity tracking
	• All service administration tasks
	• All certificate-related tasks
	• All system administration tasks
Standard Member	• View member administration information for own member ID only
	• View partnership administration information associated with own member ID only
	• Perform activity tracking for transactions associated with own member ID only
Trusted Member	This is a special privilege that can be granted to an administrator or standard member that allows that member to act on behalf of other members. A trusted member is either:
	• A special type of member that represents other members—usually a VAN (Value Added Network).
	• An internal application that does not require that ECXpert perform validation on a trading address that belongs to a member.

Selecting LDAP vs. Database Storage of Member Information

The following are advantages of using lightweight directory access protocol (LDAP) via a product such as Netscape's Directory Server instead of storing membership information in the database:

• **Performance**—The Netscape database is optimized for LDAP clients performing typical directory queries in which reads outnumber writes by an order of magnitude or more.

- **Richer directory search features**—Netscape Directory Server is optimized for directory lookups and consequently supports fast lookups across the full range of LDAP queries.

- **Simple but powerful data model**—Netscape Directory Server supports the flexible LDAP data model which is typically hierarchical, just like a file system. A hierarchical, attribute-value based data model allows you to easily store and retrieve information such as user/group data, preferences, configuration data, and many other data types.

- **Corruption**—At startup time, Directory Server automatically detects and recovers from data corruption that might have resulted from a power loss, hard drive failure, operating system crash, and so on. Automatic recovery from database corruption combined with a regular regimen of automated backups mean that data corruption is not a major operational problem.

If LDAP support for storing membership information was not enabled when you installed ECXpert, you can still enable it at a later time. Configuration of LDAP support is done after installation of ECXpert is completed.

By default, ECXpert uses the local database to store membership information. You must follow the steps below to enable LDAP support.

CAUTION	If you are currently using the Oracle database to store membership information, you can migrate that information over to LDAP at any time. However, once this information is stored in LDAP, it cannot be migrated back to Oracle.

Enabling Lightweight Directory Access Protocol (LDAP) Support

There are four tasks that you must perform to enable iPlanet ECXpert to use LDAP, rather than querying the iPlanet ECXpert `Members` table directly:

- Install the Netscape Directory Server version 3.11

- Configure the Netscape Directory Server

- Modify the `ecx.ini` file

- Migrate user data

Each of these tasks is described in the following sections.

Installing Netscape Directory Server

Install Netscape Directory Server version 3.11 according to the instructions in the accompanying documentation. There are no special installation requirements imposed by ECXpert. Netscape Directory Server can be installed on the same machine as ECXpert or on a different machine.

Configuring Directory Server for Use with ECXpert

Follow the steps below to configure the Netscape Directory Server for use with ECXpert.

1. Display the Netscape Server Administration page in your browser.

2. Create an Organizational Unit for use with ECXpert.

NOTE	If an organizational unit that you want to use already exists, skip this step.

   All ECXpert members will be stored under this organizational unit.

   In the General Administration panel near the top, click Users and Groups. Then click the New Organizational Unit link in the frame on the left.

   Create the organizational unit (for example, `ecx`), then click Server Administration to return to the Netscape Server Administration page.

3. Check parameters for the Netscape Directory Server.

   This should have been configured during Directory Server installation.

   From the Netscape Server Administration page, click the Netscape Directory Server 3.1 link.

   On the Netscape Directory Server page, click Server Preferences at the top, then click the View All Server Preferences link in the frame on the left.

   Under General Server Parameters, check Root DN—for example:
   `cn=Directory Manager, o=netscape.com`

   OR...

   cn=Directory Manager, o=netscape.com c=us

Under Database Parameters, set Suffix—for example:
o=netscape.com (no country code),

OR...

o=netscape.com, c=US (country code specified)

Modifying the ecx.ini File

Use the ECXpert System Administration Interface, System tab, to set the following parameters in the sections indicated.

For detailed instructions on working with the System tab, see .

Section	Parameter Setting(s)
hostname	Hostname for the LDAP server
Port	Port number for the LDAP server
membership	**accessType=ldap**
LDAP	**c=** *Directory_Server_country_code*
	If a country code is used in the Directory Server Suffix setting (e.g., **o=netscape.com, c=US**), this entry must match it exactly (e.g., **c=US**).
	If no country code is used in the Directory Server (e.g., **o=netscape.com**), this entry must be **c=** with nothing following the equal sign.
	o= *Directory_Server_suffix*
	This entry must match exactly the o= portion of the Directory Server Suffix setting (e.g., **o=netscape.com**).
	ou= *Netscape_org_unit*
	This entry must match exactly the organizational unit you set for ECXpert in the Netscape Server Administration page e.g., (**ou=ecx**).
	LDAP_USER= Directory_Server_Root_DN
	This entry must match exactly the entire Root DN entry you set for ECXpert in the Netscape Server Administration page (e.g., Directory Manager, o=netscape.com).

After the above changes have been made to the `ecx.ini` file, use the `bdgsetpasswd` utility to set a password for `LDAP_USER`:

```
# cd $NSBASE/NS-Apps/ECXpert/bin
# bdgsetpasswd -i $NSBASE/NS-apps/ECXpert/config/ecx.ini -lp
password
```

where *password* is the password you want to assign to `LDAP_USER`.

This password must be the same as your Directory manager password.

Migrating the Members Table

Follow these steps to migrate the ECXpert `Members` table to LDAP:

1. Shut down the ECXpert Administration Server.

2. Run the `bdgmbtoldap` utility to migrate the `Members` table to LDAP.

3. Restart the ECXpert Administration Server.

4. Log in to iPlanet ECXpert as Administrator ECX with password **ECX**.

CAUTION   The `bdgmbtoldap` utility resets all members' passwords to be the
same as the their login IDs when migrating the members info LDAP
server. Users must change their passwords manually after the
`Members` table has been migrated.

Importing Member Data from a Text File

You can use the ECXpert `import` utility when you want to import a batch of
records instead of entering the information for each member or partnership
through the ECXpert user interface. For details on using the ECXpert `import`
utility, see "import—Importing Records for Members, Partnerships, or Service
Lists" on page 494.

CAUTION   If you make changes to the database via the `import` utility, log out
and log in again. Changes made to the database through the `import`
utility are not displayed via the Administrative interface until the
user logs out and logs in again. This is due to caching.

Displaying the Membership Administration Tab

Follow the steps below to display the Membership tabs.

1. Log into the ECXpert Product Administrative Interface.

2. Click Membership on the left.

   The Membership Administration tab (Figure 5-1) is displayed.

Figure 5-1   Membership Administration tab
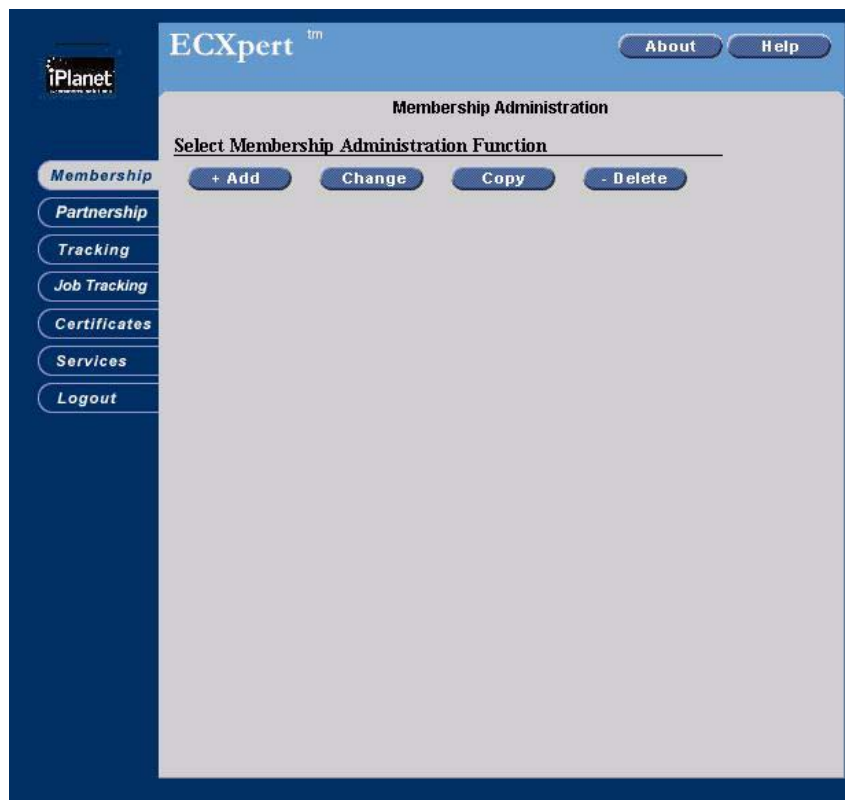
From this tab you can add, change, and delete members.

| NOTE | Except for adding a new member, for whom you enter all the information yourself, all other tasks available from this tab require you to first display the information for an existing member. See "Displaying Information for an Existing Member" below for details. |

Refer to the following sections for details on specific tasks:

❍ "Displaying Information for an Existing Member" on page 205

❍ "Working with the Membership Definition Tabs" on page 207

❍ "Adding a New Member on a Blank Form" on page 214

❍ "Copying a Member—Adding a New Member Based on Another" on page 215

❍ "Changing a Member's Information" on page 216

❍ "Deleting a Member" on page 216

Displaying Information for an Existing Member

When you add a new member, you enter all the information yourself. For all other tasks you can perform from this tab, you must first display information for an existing member. Follow the steps below to display information for an existing member.

1. Display the Membership Administration tab (Figure 5-1).

2. Click the task you want to perform.

   Click one of the following:

   ❍ **Copy**—to add a new partnership using another partnership as a template

   ❍ **Change**—to change information for an existing partnership

   ❍ **Delete**—to delete an existing partnership

   The Membership Search tab (Figure 5-2) is displayed.

Figure 5-2   Membership Search tab

3. Enter the existing member's ID into the Member ID field.

You can type the ID directly into the Member ID field.

OR...

You can select the Member ID from a list:

❍ Click the Expand ▼ button to display the drop-down List of Members.

❍ Select the ID for the sending member in the partnership that you want to change, copy, or delete.

❍ Click Expand again to roll up the list.

4. Click Retrieve.

The information for the Member ID is displayed on a series of tabs. These tabs are described below in detail in "Working with the Membership Definition Tabs."

Working with the Membership Definition Tabs

All membership administration operations require you to use the same membership definition tabs to enter or view member information. The heading above the membership definition tabs changes to reflect the task you are performing, but the details remain the same across operations.

This section describes how you fill in information on the different membership definition tabs, and how you navigate between tabs. The pictures of the membership definition tabs are specific to the Add Membership task, but the information applies equally to adding, copying, or deleting members.

If you are deleting a member, you can only view the information displayed.

Working with the Membership Information Tab

1. Display the Membership Administration tab (Figure 5-1).

2. Click the task you want to perform.

If you click Add, the Membership Information tab (Figure 5-3) is displayed immediately. For the other tasks, you must first display information for an existing member. See "Displaying Information for an Existing Member" on page 205 for details.

NOTE	The heading at the top of the membership definition tabs reflects the task you are performing.

3. Add or change information on the Membership Information tab.

Figure 5-3   Membership Information tab

Table 5-1   Information on the Membership tab

Item	Description
Member ID	A member ID can contain as many as 60 characters. It can contain letters, numbers, and special characters, and is case sensitive.
Description	A description can contain as many as 60 characters. Use this field to enter any descriptive information or notes about the member.
Password	An ECXpert password can contain as many as 60 characters. It can contain letters, numbers, and special characters, and is case sensitive.
	A password is not required if the Member is trusted box is checked.
Confirm Password	Type the same password that you type in the Password field for verification.
	You do not have to confirm a password if the Member is trusted box is checked.
TradingXpert Read Window (days)	The number of days member has to read TradingXpert documents. The number of days back that TradingXpert shows documents to this member in TradingXpert inbound and outbound document lists.
Member is active	Checked - member is active and can perform ECXpert tasks and participate in any trading partnerships.
	Unchecked - member is *not* active and *cannot* perform ECXpert tasks or participate in any trading partnerships.
Member is trusted	Checked - member is allowed to send documents on behalf of other members.
	Unchecked - member is allowed to send documents only for him/herself.
Member is Administrator	Checked - member has administrator authority.
	Unchecked - member does *not* have administrator authority.

Working with the Contact Information Tab

1. Display the Contact Information tab.

    Click Next. The Contact Information tab (Figure 5-4) is displayed.

2. Add or change information on the Contact Information tab.

Figure 5-4   Contact Information tab

Table 5-2   Information on the Contact Information tab

Item	Description
Full Name	The name of the person to contact regarding the member. A full name can be as many as 60 characters.
Company Name	The name of the company the member represents. A company name can be as many as 60 characters.
Address 1	The first line of the contact person's address (for example, 501 East Middlefield Rd., or P. O. Box 520).
Address 2	The second line of the contact person's address, if any (for example, Suite 200).
City	The name of the city for the contact person's address.
State	The name of the state for the contact person's address.
Zip	The postal code for the contact person's address.
Country	The name of the country for the contact person's address.
Phone	The area code and phone number for contact person in this format: nnn nnn-nnnn.
Fax	The area code and phone number to use to send a fax to the contact person in this format: nnn nnn-nnnn.
Email	The email address of the contact person.

Working with the Trading Addresses Tab

1. Display the Trading Addresses tab.

   Click Next. The Trading Addresses tab (Figure 5-5) is displayed.

2. Add or change information on the Trading Addresses tab.

Figure 5-5   Trading Addresses tab

Table 5-3   Information on the Trading Addresses tab

Item	Description
Address Type	Must be either EDI, Local E-Mail, or Remote E-Mail. If the SMTP protocol is used for either EDI or non-EDI communication, must be set to one of the E-Mail options.
Qualifier	• Automatically set to EL if Address Type is set to Local E-Mail. • Automatically set to ER if Address Type is set to Remote E-Mail. • If Address Type is EDI, must be an EDI qualifier.
Address	• If Address Type is one of the E-Mail options, must be a valid email address. • If Address Type is EDI, must be an EDI address.
Existing Trading Address	Lists any trading addresses that have already been added for this member.

Adding an Address

Fill in the above information for a trading address, then click Add immediately below the Qualifier field to add the address to the Existing Trading Address list.

Multiple EDI addresses are allowed. Fill in the information for each and click Add immediately below the Qualifier field.

Removing an Address

To remove an address from the Existing Trading Address list, select it and click Remove.

Changing an Address

To change an address in the Existing Trading Address list, select it and click Change.

Saving Your Work

A "completion" button always appears at the bottom of the membership definition tabs:

❍ This button has the same name as the one you clicked to begin the current task: Add, Change, Copy, or Delete.

❍ Clicking this button completes the task.

❍ This button is only active when the last tab on the series is displayed in front.

❍ For Delete, this button deletes the member's information. For the other operations, this button saves the information you have entered and/or changed for the member.

NOTE	You can click Cancel at the bottom of the membership definition tabs at any time if you decide not to complete the task.

Adding a New Member on a Blank Form

Follow the steps below to add a new member on a blank form. If you want to add a new member by editing another member's information, see "Copying a Member—Adding a New Member Based on Another" below.

1. Display the Membership Administration tab (Figure 5-1).

2. Click Add.

The membership definition tabs are displayed for the Add Membership task, with the Membership Information tab (Figure 5-3) in front.

3. Fill in the information on the membership definition tabs.

4. Save the member's information.

Click Add at the bottom of the last tab in the membership definition series of tabs.

NOTE	You can click Cancel at the bottom of any membership definition tab if you decide not to add the new member.

Copying a Member—Adding a New Member Based on Another

When the information for a new member you are adding is similar to the information for an existing member, you can save data entry time by using the existing member as a template for the new member.

Follow the steps below to do this. To enter a new member without using another member as a template, see "Working with the Membership Definition Tabs" on page 207.

1. Display the Membership Administration tab (Figure 5-1).

2. Click Copy.

   The Membership Search tab (Figure 5-2) is displayed.

3. Enter the Member ID of the member to use as a template.

   See "Displaying Information for an Existing Member" on page 205 for details.

4. Click Retrieve.

   The Membership Information tab (Figure 5-3) is displayed for the Copy Membership task.

5. Make necessary additions and changes.

   The Member ID, Password, and trading address(es) are not copied and you must add them. You can change anything else on the Membership, Contact Information, and Trading Addresses tabs.

   Refer to "Working with the Membership Definition Tabs" on page 207 for details on specific fields on the Membership, Contact Information, and Trading Addresses tabs.

6. Save the member's information.

   Click Copy at the bottom of the last tab in the series of membership definition tabs.

NOTE   You can click Cancel at the bottom of the any membership definition tab if you decide not to add the new member.

Changing a Member's Information

Follow the steps below to change information for a member.

1. Display the Membership Administration tab (Figure 5-1).

2. Click Change.

   The Membership Search tab (Figure 5-2) is displayed.

3. Enter the Member ID of the member you want to change.

   See "Displaying Information for an Existing Member" on page 205 for details.

4. Click Retrieve.

   The information for the member that you want to change is displayed in the membership definition tabs for the Change Membership task, with the Membership Information tab (Figure 5-3) in front.

5. Make necessary additions and changes.

   If you are logged in as a regular member, you can only change your own password and contact information.

   If you are logged in as an administrator, you can enter and change any information for a member. Refer to "Working with the Membership Definition Tabs" on page 207 for details on each item of information on each of the three tabs.

6. Save the member's information.

   Click Change at the bottom of the last tab in the in the series of membership definition tabs.

NOTE	You can click Cancel at the bottom of any membership definition tab if you decide not to change the member's information.

Deleting a Member

When you delete a member, the partnerships and service lists associated with that member are automatically deleted. All tracking and event log information for files you previously processed for that member, however, remain intact.

Follow the steps below to delete a member.

1. Display the Membership Administration tab (Figure 5-1).

2. Click Delete.

   The Membership Search tab (Figure 5-2)is displayed.

3. Enter the Member ID of the member you want to delete.

   See "Displaying Information for an Existing Member" on page 205 for details.

   When you click Delete on the Membership Search tab, you are prompted to view the information before deleting. Your options are:

   ○ Yes—display the member's information on the membership definition tabs before deleting.

   ○ No—delete the member immediately, without further confirmation.

   ○ Cancel—return to the Membership Administration tab without deleting the member or displaying the information.

4. Click Yes.

   The information for the member you have selected to delete is displayed in the membership definition tabs, with the Membership Information tab (Figure 5-3) in front.

5. Examine the information.

   You want to be absolutely certain that you are deleting the correct member.

6. Delete the member.

   Click Delete at the bottom of the last tab in the series of membership definition tabs.

NOTE	You can click Cancel at the bottom of any membership definition tab if you decide not to delete the member.

   After clicking Delete , you are prompted, "Are you sure?" Click Yes to confirm the deletion.

NOTE	You can still click No to cancel the deletion. This is, however, your last chance. If you click Yes, the deletion cannot be undone.

Deleting a Member

Setting Up Trading Partnerships

This chapter describes the tasks involved in setting up and maintaining trading partnerships in ECXpert. The following topics are covered:

Overview

A *trading partnership* is an agreement between two companies or internal departments to trade documents such as purchase orders, functional acknowledgments, and invoices using specific standards and communications protocols.

For example, Company A owns and operates an ECXpert system, and agrees to receive purchase orders from Company B. Company A also agrees to send Company B an acknowledgment each time it receives one or more purchase orders from Company B, and to send invoices to Company B after each purchase order is fulfilled.

Company A needs to set up a trading partnership for each type of document traded. In this example, Company A must set up a trading partnership for purchase orders and for invoices. acknowledgments can be part of the agreement for each of those document types.

To set up a trading partnership, you need to:

- Set up a member ID for the sending member

- Set up a member ID for the receiving member

- Determine the document type to be sent and received

- Determine whether acknowledgments are required

- Create a map to translate the document from the sender's format to the receiver's format

- Set up a service list (or use an existing service list) to process the document when it is sent or received

- Determine the communications protocol to use

- Determine whether the document is EDI or non-EDI

If the document type is an EDI or XML (where noted below) document, you need to:

- Select an EDI address to use for the sending member

- Select an EDI address to use for the receiving member

- Specify a beginning interchange control number for the partnership

- Specify whether the Partnership Type (document translation) is EDI/XML to Application, Application to EDI, EDI/XML to EDI, or Application to Application

- Determine the EDI standard to use and the version and release of that standard

- Specify a beginning group control number

- Determine the functional group type

- Determine whether acknowledgments are required at the functional group level or the document level

- Specify a beginning document control number

If the Partnership Type is Application to EDI, and, ECXpert is to generate or override the entire envelope, you also need to determine whether you will use standard delimiters and separators or specify which control characters will be used for:

- Segment terminator

- Sub-element delimiter

- Element delimiter

- Test or production indicator

Confirming that Sent Data is Received

ECXpert supports the confirmation messages, or data receipt notifications, that are specific to the two major EDI standards, ANSI X12 and EDIFACT. Confirmation messages can be generated only when the incoming data is EDI. Thus the information in this section only applies to partnerships where the Partnership Type is either EDI to Application or EDI to EDI.

Functional Acknowledgments report whether a file's group, transaction set (document), segment, or data elements pass a syntactical check. For example, field length, alphanumeric versus numeric-only, missing mandatory segments, and so on.

Semantic checks can also be reported back through the FA, but these are more limited. For example, correct segment count, control #s matching, lookup against an ID list, and so on. Some of the semantic checks depend on ECXpert's Parser, and others on your maps, so the FAGen service requires Translate and is always after Translate.

Instructions on setting up confirmation messages under either ANSI X12 or EDIFACT are provided in "Working with the Input EDI Tab" on page 282.

For detailed information on the *Mercator* type tree and map settings that are required to take full advantage of the confirmation message capabilities of ECXpert, see Appendix D, "Required Mercator Settings for ANSI Functional Acknowledgment (997)."

FA (997)/CONTRL Reconciliation

ECXpert 2.0 can read an ANSI X12 Functional Acknowledgment (997) or an
EDIFACT CONTRL message returned to the system and reconcile it with the
output file to which it corresponds. The reconciliation is based on matching up the
address information, functional group ID, and the control/message reference
numbers in the FA (997) or CONTRL message with the original output file.

Additionally, when you create a trading partnership, you can specify that
FA (997)/CONTRL messages are expected for each output EDI file that is created
by ECXpert and sent out of the system using one of the communications agents.

You can also specify in minutes when the FA (997)/CONTRL message should be
considered overdue.

Importing Partnership Data from a Text File

You can use the ECXpert `import` utility when you want to import a batch of
records instead of entering the information for each member or partnership
through the ECXpert user interface. For details on using the ECXpert `import`
utility, see "import—Importing Records for Members, Partnerships, or Service
Lists" on page 494.

CAUTION	If you make changes to the database via the import utility, log out and log in again. Changes made to the database through the import utility are not visible via the Product Administrative Interface until the user logs out and logs in again. This is due to caching.

Selecting the Right Communications Protocol

Some trading partners specify a particular communications protocol that you must
use to exchange electronic documents with them. In that case, set up the trading
partnership to use the protocols they specified.

If the choice is up to you, the following sections describe business requirements for
you to consider when selecting a communications protocol.

Using Poll

The default option, the ECXpert `poll` utility is not really a communications protocol at all. Select it when an external process will be pulling data from the ECXpert mailbox using the ECXpert `poll` utility. For more information on the `poll` utility, see "poll—Checking for New Documents" on page 492.

Enabling SNMP Support

You can use iPlanet ECXpert with your SNMP-compliant software to help you troubleshoot communications problems within your local network. Execute the following steps to implement SNMP support within iPlanet ECXpert:

➤ **To start SNMP before starting iPlanet ECXpert:**

1. Log in or switch (`su`) to user ID **root** on the system on which iPlanet ECXpert is installed.

NOTE	Step 2 and Step 3 below are one-time-only configuration steps.

2. Make sure the following entries are in your `/etc/services` file:

    ```
    smux 199/tcp
    snmp 161/udp
    snmp-trap 162/udp      snmptrap
    ```

3. Stop `inet.d`:

    `# kill -HUP` *pid_of_inet*

    where *pid_of_inet* is the process ID of `inet`. The reason for killing the `inet` daemon is to get it to read the setting in the `/etc/services` file the first time after that file is changed.

4. Edit the SNMP configuration file.

    Open the `$NSBASE/NS-apps$NSBASE/NS-apps/ECXpert/snmp/config/CONFIG` file using a text editor like `vi` and edit it using the example below as a guideline.

    When editing this file, be sure to observe the following four cautions:

    (1) The last line of the file must be a blank line.

(2) If you want to have more than one SNMP Management Console receive the traps, you must use a format such as the following where the "Manager" section is repeated.

(3) Use tabs, not spaces, to indent.

(4) Use capital letters for the values that have capital letters in the example; the file *is* case-sensitive.

Example SNMP configuration file:

```
MANAGER          123.123.23.45
                  SEND ALL TRAPS
MANAGER           123.123.23.56
                    SEND ALL TRAPS
COMMUNITY         public
                    ALLOW ALL
MEMBERS           123.123.23.45, 123.123.23.56
```

5. Change to the SNMP binary directory:

    # cd $NSBASE/NS-apps/ECXpert/snmp/bin

6. Start SNMP:

    # ./Program.o ../config/CONFIG *snmp_log_file* **&**

7. Modify the ECXpert ecx.ini file to set the flags to enable SNMP.

    Refer to Appendix C, "ECXpert Initialization File (ecx.ini)" for more information on the ecx.ini file. Any section with a section_type=server entry represents an ECXpert server for which you can enable SNMP.

    You must set the following parameters in the appropriate section of the iPlanet ECXpert ecx.ini file for the Administration Server ([admin] section) and for each server on which you want to enable SNMP:

```
[ section_name ]
snmp_flag = yes
snmp_trap_flag = yes
snmp_trap_level = 20 (or other desired value)
```

Do not change any other parameters in the ecx.ini file.

8. Stop and restart (or just start) ECXpert.

   When you give the command to start the ECXpert executable, you need to give as arguments:

   ❍ The location of the SNMP configuration file, which is always
      `$NSBASE/NS-apps/ECXpert/snmp/config/CONFIG`

   ❍ And the location of the SNMP log file, which is set in the `[snmp]` section of the `ecx.ini` file by the `snmp_tmp_path` parameter. The default value assigned during installation is `/tmp/SNMP_LOG`.

NOTE	If you start iPlanet ECXpert with the `ecx.ini` flags set to trap errors and messages for SNMP when there is no SNMP agent running on your subnet, ECXpert does not run, but no error messages appear.

Using SMTP—Internet Email

With the current implementation of the Internet's Simple Mail Transport Protocol (SMTP) with Secure Multipurpose Internet Mail Extensions (S/MIME), the delay between the time a message is sent and the time it is delivered is indeterminate although usually quite satisfactory.

There is always a possibility of delay, however, depending on the Internet service provider, mail gateways, and the size of the message. Very large messages (1MB or larger) might be unable to pass through some mail gateways on the open Internet, resulting in a delay.

Use SMTP if your business is involved in:

• Non-time-critical functions, where possible delays and dealing with trading partners without regard to the sequence in which orders are placed do not present a problem.

• Fairly small volume of transactions, where the submission units are not expected to exceed 1MB in size.

Avoid SMTP, unless a known Internet routing path is available, if your business is involved in:

• Just-in-time inventory management, where turn-around time is critical.

• Fulfilling orders from limited supplies, where it is critical that orders be filled in the order they were placed.

- Large volumes of transactions, where the submission units might be expected to exceed 1MB in size.

SMTP Limitation: If there are more than one SMTP partnership with the same Sender and Receiver pair for incoming encrypted messages, ECXpert might fail to find the right certificate to decrypt the message. This problem can be avoided if both partnerships have the same Receiver certificate.

SMTP to SMTP - Receive and Send

ECXpert can receive and process incoming SMTP messages from another ECXpert system or any other EDI transaction system and then turn around and send the processed document to the receiving trading member via email (SMTP).

To support this feature, ECXpert allows each trading member to have two email addresses:

- The local e-mail address (denoted in membership setup as "EL") is the local email address for your ECXpert system.

- The remote e-mail address (denoted in the membership setup as "ER") is the e-mail address of the trading partner who will receive the SMTP message.

CAUTION   When you set up SMTP to SMTP, make sure the receiving member (member B in the example below) has two unique email addresses in the version of ECXpert that is doing the receiving, processing, and sending of the final document (the ECXpert system in the middle of Figure 6-1 on page 227).

If the "EL" and "ER" e-mail addresses are the same, the document will be resubmitted and reprocessed in the same system in an infinite loop.

Figure 6-1   ECXpert SMTP to SMTP transaction flow
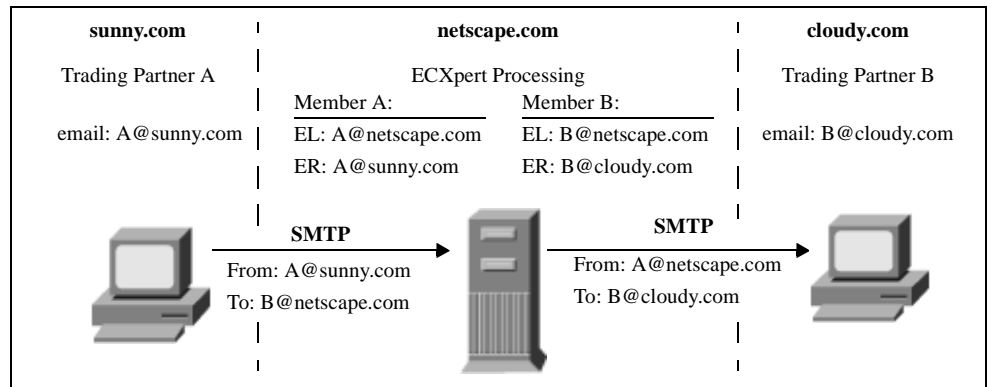
In Figure 6-1, an example, assume that there are three Internet domains representing two trading partners and ECXpert, and SMTP connecting the two trading partners.

In this example, the membership email address on system A should be set up as follows:

*   For member A, EL = A@sunny.com

*   For member B

    ❍   EL = B@netscape.com

    ❍   ER = B@cloudy.com

The partnership setup on system A should be A -> B, SMTP protocol.

The membership email address on the ECXpert system should be set up as follows:

*   For member A

    ❍   EL = A@netscape.com and

    ❍   ER = A@sunny.com

*   For member B

    ❍   EL = B@netscape.com and

    ❍   ER = B@cloudy.com

The partnership setup on ECXpert system in the middle should be A -> B, SMTP protocol.

Using this example, ECXpert would accept incoming SMTP documents, process them, and send them out via SMTP as follows:

1. After the submitted document on Trading Partner A's ECXpert System is processed, it is sent to the ECXpert system in the middle of the diagram using SMTP. If you examine the document at this point, notice that the sender email address is A@sunny.com and receiver email address is B@netscape.com.

2. The document arrives at the ECXpert system in the middle. It is retrieved by the ECXpert SMTP Receive daemon and processed.

3. After the document is processed (service list is completed), ECXpert sends the final document to member B's desktop using SMTP. The document that member B receives on his/her desktop will have sender email address A@netscape.com and receiver email address B@cloudy.com

CAUTION	When you set up SMTP-to-SMTP, make sure the receiving member (member B in our example) has two unique email addresses.
	If the EL and ER addresses are the same, the document is resubmitted and reprocessed in an infinite loop.

Configuring Microsoft Outlook Express to work with ECXpert

This section covers the workarounds to known issues you might encounter when using Microsoft Outlook Express with ECXpert's SMTP Receive agent. (This document will be updated as other possible issues are identified.)

Issue #1: Outlook's HTML Format Cannot Be Processed

By default the MS Outlook is configured to send out messages using HTML format as the mail sending format. The message sent out with this format contains nested MIME types (a MIME header embedded inside another).

The current design of the SMTP Receive Server of ECXpert is not capable of handling messages with nested MIME types. If you turn on tracing for the ECXpert SMTP Receive agent, the following error appears in the debug log file when it tries to process the incoming MS Outlook message file and fails:

```
Process rwerror.data()=File system error encountered
```

Solution

Follow the steps below to reconfigure MS Outlook to send out messages using Plain Text format:

1. From the MS Outlook menu, choose Tools > Options.

2. Select the Send tab.

3. Under Mail Sending Format, select Plain Text.

4. Click Apply, then click OK, for the changes to take effect.

Issue #2: Cannot Import Certificate from Outlook

In order to import Verisign Class 1 Certificates into ECXpert, a "Signed Only" message must be sent from the Outlook Express email client to ECXpert.

However, ECXpert is unable to process the signed message and import the certificate from Outlook Express client if certain security settings in Outlook Express are not configured correctly. If this is the case, the following error in the ECXpert's SMTP receive debug trace file appears:

```
    rwerror.data()=Incorrect or unsupported multipart/signed
    message header. check the signature protocol and MIC
 algorithm...
```

Solution

Before you begin sending Signed messages out from Outlook Express to ECXpert, you need to set the security options in Outlook Express as follows:

1. From the MS Outlook menu, choose Tools > Options.

2. Select the Security tab.

3. Click Advanced Settings to open the Advanced Security Settings dialog box.

4. Under Digitally Signed Messages, check both boxes.

5. Click Apply, then click OK, for the changes to take effect.

Issue #3: Cannot Process Signed Message

An error similar to issue #2 is displayed in the log file when processing an incoming signed message from Outlook Express, when the Verisign Class 1 certificate has already been imported.

Solution

Use the same solution for issue #2. Make sure that both boxes are checked under Digitally Signed Messages check box.

Issue #4: Cannot Parse Attached EDI File

A parsing error occurs when the service list tries to perform the Parse service on the incoming EDI file attachment. The Warning message shows up in the event log in the Tracking tabs in the Product Administrative Interface:

```
Warning - 1 unidentified envelope found in data
```

When you submit the same file sent via the Communicator Messenger mail client, the EDI is parsed without errors.

Solution

MS Outlook automatically wraps text at the column that was specified in the Send options. If an EDI file happens to have one line that has more characters than specified in this option, the is wrapped by MS Outlook before being sent to ECXpert. The insertion of non-printing characters for line wrap causes the Parse service to fail.

Follow the steps below to resolve this problem:

1. From the MS Outlook menu, choose Tools > Options.

2. Select the Send tab.

3. Under Mail Sending Format, make sure Plain Text is selected.

4. Next to the Plain Text option, click Settings to open the Settings dialog box.

5. If the Uuencode option radio button is not selected, note the option that is selected.

    You will need to restore this setting in Step 8.

6. If the Uuencode option radio button is not selected, select it now.

    When Uuencode is selected, the Automatically wrap text at... option is active.

7. Set the value for Automatically wrap text at... to 132.

8. If the Uuencode option radio button was not originally selected in Step 5, restore the option that was then selected.

Using Message Disposition Notification (MDN)

When sending any type of data via SMTP, you can request that a series of message disposition notifications (MDN) be returned to the sender of the submission unit reporting its current status as it is being received by ECXpert on the receiving end. ECXpert provides MDN to reliably track delivery of a submission unit via Internet mail.

MDN supplements the functional acknowledgment of EDI, or the CONTRL message of EDIFACT, but does not replace either. MDN is simply a transport-layer acknowledgment. It verifies only that the recipient received the message. It does not indicate whether the message was processed or passed any syntactical check.

Follow the steps below in the Product Administrative Interface to request MDN.

- In the **Trading** section, **Protocol Information** form:

  ❍ Set **Primary Protocol** to SMTP.

  ❍ Set **MDN Requested?** to Yes. If the trading partnership is exchanging signed data, you should request a signed MDN to prevent non-repudiation of receipt. In order for the sender of a submission unit to receive a signed MDN, a trading partnership must have been set up on the receiving end, and the appropriate certificate types must have been set up.

NOTE	If you are using anything other than Simple MIME, requesting a signed MDN is not recommended.

Going through a VAN

Value-added networks (VANs) provide a high level of service, but they also charge a premium price. The lower direct cost of using the Internet to bypass VANs might not be feasible or less expensive for businesses that are not equipped to perform the VAN's functions in-house.

Consider *using* VANs if your business:

- Deals with trading partners who require you to use many different protocols and you are not prepared to support the resulting complexity.

- Trades with partners who are using async dial-in, where you cannot push documents out to them over the Internet because they are not always connected.

Avoid VANs if your business:

- Deals with trading partners who allow you to use a small number of protocols that you have no trouble supporting.

- Trades with partners who are directly connected to the Internet, or who are good candidates for SMTP delivery.

Using FTP

The Internet's File Transfer Protocol (FTP) has long been used to transfer files of all types and sizes over the Internet. FTP is fast and reliable, but requires businesses receiving files via FTP to deal with the potential security risks involved in allowing a sender to transfer files onto your systems.

Consider *using* FTP if your business:

- Already operates in a technical environment where your IS personnel have experience in dealing with the security risks that FTP presents.

- Needs to move large volumes of data at high speeds.

Consider *avoiding* FTP if your business:

- Operates in a technical environment where your IS personnel are not equipped for dealing with the security risks that FTP presents.

- Deals with smaller volumes of data where transmission speed is less important.

Overall, many companies use FTP today making it a popular choice for EDI exchanges over the internet.

Using Odette FTP (OFTP)

ECXpert 3.6 supports the Odette File Transfer Protocol (OFTP) for both incoming and outgoing communications. OFTP was first specified in 1986 by the Organisation for Data Exchange by Tele Transmission in Europe (ODETTE) to address the EDI requirements of the European auto industry.

OFTP is a session level protocol that has traditionally been conducted over X.25 or X.28 dialup transport layers. A recent extension to OFTP added TCP/IP as the network layer.

OFTP was designed to provide a means of data transmission that was independent of the underlying communications medium as well as the hardware configuration and the software environment.

It has the following advantages:

- Supports systems of different ages

- Works with systems from different vendors

- Works with systems of different sizes

- Works with legacy systems, minimizing impact on IS

- Is easily scalable

- Is session-based and interactive—can reject a bad login, or a bad trading partnership in mid-session

- Supports EERPs (End-to-End-Responses), acknowledgments sent from the final recipient to the originator that are comparable to the MDNs (Message Disposition Notifications) in SMTP.

You might need to use OFTP to support existing OFTP trading partners.

NOTE If you want EERPs under OFTP, you must follow these guidelines:

- Files that are to be sent out by ECXpert using OFTP must be submitted using OFTP.

- If the file ECXpert is sending using OFTP is not being sent to its final destination, you must set up a reverse partnership to handle the EERP that is returned later. Create a separate partnership, reversing the Sender and Receiver member IDs used in the partnership sending a file using OFTP, and specifying a Document Type of EERP. No service list is required.

- Make sure that the ECXpert Date/Time Based Scheduler is running. This is necessary even for immediate EERP transmissions.

For more detailed information on setting up ECXpert's OFTP capabilities, see Appendix G, "Odette FTP (OFTP) User's Guide."

Using GEIS FTP

If you need to send and receive EDI documents with the GE Information Services EDI*EXPRESS Service, you can use the ECXpert GEIS FTP protocol.

The following requirements must be met to use GEIS FTP in the Sun Solaris environment:

- The Solaris machine must be configured to use a modem to connect to the GEIS remote access server using the PPP (Point-To-Point) communication protocol, not directly via the public Internet. This is a GEIS limitation for PPP.

- You must have a GEIS network access telephone number. Contact GEIS to obtain this.

- You must have a GEIS EDI*EXPRESS mailbox account and password. Contact GEIS to set this up.

➤ **To set up communications with GEIS FTP**

The steps below explain how to set up a Sun Solaris machine and ECXpert to communicate with GEIS FTP.

1. Set up PPP under Solaris. See "Setting Up PPP under Solaris," below for details.

2. Set up a partnership in ECXpert using the GEIS FTP as protocol to send documents.

3. Set up partnerships and service lists for the expected ultimate senders for whom GEIS is submitting documents (acting as a trusted member). For example, if the "ABC Company" is submitting documents to "Your Company" through GEIS FTP, you need:

   ❍ A partnership with sender set to "ABC Company" and receiver set to "Your Company"

   ❍ A service list with sender set to "ABC Company," receiver set to "Your Company," with appropriate services to process the documents

4. Set up a service list in ECXpert with "GEIS" as both the sender and receiver, using Parse, Translate, and Gateway services. This service list is for processing the incoming EDI documents from GEIS. When this service list is executed, it parses the incoming documents, determines the ultimate senders/receivers/document types, and executes the appropriate service list for the matching partnerships.

5. Following the administrator's documentation for GEIS' EDI*EXPRESS, set up a trading relationship on the GEIS EDI*EXPRESS Service.

6. Dial and log in to the GEIS FTP remote access server. You can do this either from the Solaris command line or using a script.

7. Submit an EDI document to ECXpert to send to the GEIS FTP server.

Setting Up PPP under Solaris

To set up a Solaris machine as a PPP client, you need to modify or create a number of configuration files and then reboot. The following procedure works for a Solaris 2.5.1 system with a US Robotics Sportster modem connected to port A.

NOTE Significant customization of these instructions might be needed, depending on hardware, software, and configuration differences on your site.

---

1. Edit the `/etc/uucp/Devices` file.

    Locate the line that begins with ACU. Comment out that line and insert the line below to replace it. This line sets up TTY A so that PPP will execute the dialer script called `lblmodem`:

    ```
    ACU cua/a - Any lblmodem
    ```

2. Edit the `/etc/uucp/Dialers` file.

    Add the following lines to the bottom of the file:

    ```
    #
    # For LBL
    #
    lblmodem =,-, "" \EAT&F1 "" \EATDT\T\r\c CONNECT
    ```

3. Edit the `/etc/uucp/Systems` file.

The only uncommented lines should be these:

```
raslbl Any ACU 38400 4864441 ""
P_ZERO "" \r\c
```

NOTE	The above assumes that you are local and can dial 486-4441. You might need to change that number.

4. Edit the /etc/asppp.cf file.

   The only uncommented lines should be these:

   ```
   ifconfig ipdptp0 plumb 1.1.1.1
   private up
   path
        inactivity_timeout 300
        interface ipdptp0
        peer_system_name Pgeis
        ipcp_async_map 0
        default_route
        negotiate_address on
        will_do_authentication chap
        chap_name    XXXXX
        chap_secret  YYYYY

   defaults
        debug_level 9
        ipcp_async_map 0
   ```

   Where *XXXXX* is your user name and *YYYYY* is your password to login to the GEIS remote access server. This is different from the user name and password used for logon to the GEIS FTP mailbox.

   Replace *ppp-geis* with actual IP address of the GEIS remote access server.

NOTE	There are TABs in front of the lines that are indented, not spaces (that might matter).

5. Edit the .cshrc file.

Insert the following commands to enable use of the startppp and stopppp commands.

```
alias startppp '/etc/init.d/asppp
stop;/usr/sbin/route -f;\
        /etc/init.d/asppp start;ping ppp-geis&'
alias stopppp '/etc/init.d/asppp stop;/usr/sbin/route -f'
```

NOTE	A user must be logged in as root (super user) to have permission to run the /etc/init.d/asppp start and /etc/init.d/asppp stop commands.

6. Test the startppp command.

   The startppp command starts the ppp service and connects to the PPP server. If you do not have any network activity, the connection will timeout after 5 minutes (300 seconds). Any connection attempt (telnet, ping, using Netscape, and so on) after that will automatically initiate a new PPP connection.

7. Test the stopppp command.

   The stopppp command disconnects you from the PPP server and prevents new PPP connections.

   After issuing the startppp command, the first thing to try is a ping. If that works, it means the connection is good.

   # ping *ip address of GEIS FTP*

8. Watch the /etc/log/asppp.log file.

   Use the following command:

   # tail -f /etc/log/asppp.log

9. See if the PPP interface comes up.

   Use the following command:

   # ifconfig -a
   lo0: flags=849 *UP,LOOPBACK,RUNNING,MULTICAST* **mtu 8232**
      inet 127.0.0.1 netmask ff000000
      ipdptp0: flags=88d1

UP,POINTOPOINT,RUNNING,NOARP,MULTICAST,
   PRIVATE **mtu 1500**
   inet 131.243.212.62 --> 131.243.212.60 netmask ff000000
   ether 0:0:0:0:0:0

10. See if a route has been added for the PPP connection.

Use the following command:

 # netstat -r

Dialing in to GEIS under Solaris—Sun Dialup Configuration Files

To dial in to GEIS using a modem under Solaris, you must set up Sun dialup configuration files.

1. First, edit the `Dialers` file.

   a. Use the *vi* editor to open the `Dialers` file:

   # vi /etc/uucp/Dialers

   b. Add the following to the bottom of the file. These lines work for a USRobotics Sportster modem and would probably work for many others.

```
#
# For LBL
#
lblmodem =,-, "" \EAT&F1 "" \EATDT\T\r\c CONNECT
```

Here is a basic line that should work with most simple 14.4 modems:

```
pract =,-, "" \dATV1M1\r\c OK\r \EATDT\T\r\c CONNECT
```

AT Commands:

   `V1` - causes modem to return words instead of numbers

   `M1` - turns modem speaker ON, which is good for testing

   `Mo` - turns modem speaker OFF

NOTE	If you have a Hayes modem, try using the default setting that are already configured in /etc/uucp/Dialers for "hayes."

---

2. Next, edit the Devices file.

    a. Use the *vi* editor to open the `Devices` file:

        `# vi /etc/uucp/Devices`

    b. There should be one line that begins with `ACU`. Comment out that line and add the line below. (This sets up TTY A so that PPP will execute the dialer script `lblmodem`.)

        `ACU cua/a - Any lblmodem`

    If you are using hayes settings in the file `/etc/uucp/Dialers` (keyword "hayes"), replace the keyword "`lblmodem`" with keyword "`hayes`" in the command above, to create this line:

        `ACU` `cua/a - Any` **`hayes`**

NOTE	The keywords "`lblmodem`" and "`hayes`" link configuration settings in the file `/etc/uucp/Devices` to configuration settings in the file `/etc/uucp/Dialers`.

3. Next, edit the `Systems` file.

    a. Use the *vi* editor to open the `Systems` file:

        `# vi /etc/uucp/Systems`

    b. There should be one line that begins with `ACU`. Comment out that line and add the line below.

        `ACU` `links /etc/uucp/Systems to /etc/uucp/Devices`

    The only uncommented line should be this:

        `pppgeis` `Any` **`ACU`** `38400 9,18002990286 * PPP ""`

    In `9,18002990286`, the `9,` is to access an outside line. Include it only if appropriate for your phone system. Also, use a local phone number instead of the toll free number shown here, if a local phone number is available.

4. Next, edit the `asppp.cf` file.

    a. Use the *vi* editor to open the `asppp.cf` file:

        `# vi /etc/asppp.cf`

    b. Make sure the following line appears in the file (add it if needed):

pppgeis links /etc/asppp.cf to /etc/uucp/Systems

The only uncommented lines should be these:

```
ifconfig ipdptp0 plumb ios-ppp ppp-geis private up
path
     inactivity_timeout 300
     interface ipdptp0
     peer_system_name pppgeis
     ipcp_async_map 0
     default_route
     negotiate_address on
     will_do_authentication chap
     chap_name   XXXXX
     chap_secret YYYYY

defaults
     debug_level 9
     ipcp_async_map 0
```

For *XXXXX* use your Userid and for *YYYYY* use your password.

5. Last, edit the `hosts` file.

   a. Use the *vi* editor to open the `hosts` file:

      # vi /etc/hosts

   b. Make sure the following lines appear in the file (add them if needed):

      10.0.0.1 **ios-ppp**
      3.19.4.66 **ppp-geis**

NOTE   The `chap_name/secret` is different from the "GEIS" network logon id, for example:

```
GEIS name: abc word: myppp
chap_name thecompany
chap_secret thepwd
```

Enter the following command sequence to test the dialup:

```
# /etc/init.d/asppp stop
# /usr/sbin/route -f
# /etc/init.d/asppp start
# ping ppp-geis
```

At this point the `ping` command should cause the modem to dial. Eventually, the `ping` command will time out.

You can create an alias to run the above commands at once:

```
# alias startppp '/etc/init.d/asppp stop;/usr/sbin/route -f;
/etc/init.d/asppp start;ping ppp-geis&'
```

To view the log file, use the following command (see example below):

```
# tail -f /var/adm/log/asppp.log
```

To see if a route has been added for the PPP connection, use the following command:

```
# netstat -nr
```

You should see a route for "`ipdptp0`" (from the `asppp.cf` file).

Use the following command to see if the PPP interface comes up:

```
# ifconfig -a
```

You should see the following:

```
lo0: flags=849 mtu 8232
      inet 127.0.0.1 netmask ff000000
ipdptp0: flags=88d1 mtu 1500
      inet 131.243.212.62 --> 131.243.212.60 netmask ff000000
      ether 0:0:0:0:0:0
```

To stop dialup, use the following commands:

```
# /etc/init.d/asppp stop
# /usr/sbin/route -f
```

You can create an alias to run the above commands at once:

```
# alias stopppp '/etc/init.d/asppp stop;/usr/sbin/route -f'
```

The following is an example of a UNIX connection log file (from `/var/adm/log`):

```
09:40:57 Link manager (20089) started 08/12/98
09:40:57 parse_config_file: Successful configuration
09:40:57 process_ipd_msg: ipdptp0 needs connection
conn(Pgeis)
Trying entry from '/etc/uucp/Systems' - device type ACU.
Device Type ACU wanted
Trying device entry 'cua/a' from '/etc/uucp/Devices'.
processdev: calling setdevcfg(ppp, ACU)
fd_mklock: ok
fixline(8, 19200)
gdial(hayes) called
Trying caller script 'hayes' from '/etc/uucp/Dialers'.
expect: ("")
got it
sendthem (DELAY
APAUSE
TE1V1X1Q0S2=255S12=255^M)
expect: (OK^M)
^M^JOK^Mgot it
sendthem (ECHO CHECK ON
A^JATTDDTT99,,118800002299990022886^M^M)
expect: (CONNECT)
^M^JCONNECTgot it
getto ret 8
expect: (*)
19200/ARQ/V34/LAPM/V42BIS^M^JBrook Park HPN W.Pad 6 port:
P13^M^J*got it
sendthem (PPP^M)
expect: ("")
got it
call cleanup(0)
09:41:39 process_ppp_msg: PPP_ERROR_IND Local Authentication
Failed
09:42:24 Link manager (20089) exited 08/12/98
```

NOTE	The message "`PPP_ERROR_IND Local Authentication Failed`" in the example above is due to use of an invalid userid/password for the PPP connection. A successful connection message looks like the following:

```
got it
call cleanup(0)
09:41::39 start_ip: IP up on interface ipdptp0, timeout
set for 600 seconds
09:42::24 Link manager (19752) exited 08/11/98
```

Using HTTP Receive

Use the HTTP Receive protocol when files should be stored without processing to be retrieved and processed.

Using HTTP SSL for OBI

Use the HTTP SSL for OBI protocol when you want HTTP with Secure Socket Layer security for OBI documents.

Using HTTP SSL for XML

Use the HTTP SSL for XML protocol when you want HTTP with Secure Socket Layer security for XML documents.

Using HTTP for AIAG

According to the following quote from their Web site (www.aiag.org), the Automotive Industry Action Groups (AIAG), a trade organization of the worldwide automotive and truck industry, has:

"...developed the concept of a TCP/IP network for all automotive trading partners, the Automotive Network eXchange (ANX).

The ANX provides automotive trading partners with a single, secure network for electronic commerce and data transfer—replacing the complex, redundant and costly multiple connections that currently exist throughout the automotive supply chain.

> "The ANX, which is being developed by the AIAG's Implementation Task Force—made up of representatives of the Big Three auto makers and several major Tier One suppliers—has the potential to offer the auto industry significant savings by organizing infrastructure requirements in support of growth in networked applications.

> "If you are a first-tier supplier and currently maintain multiple network connections to the OEMs, ANX will enable you to replace those connections with a single link, simplify your external data communications and reduce costs. If you are a second- or third-tier supplier doing business with multiple automotive trading partners through a combination of dial-up access, faxes and tapes, you will be able to use a single ANX connection (dial or dedicated) to speed up and simplify these business processes." (end of quote from http://www.aiag.org)

Netscape ECXpert supports the draft protocol specification for using HTTP to exchange EDI messages over the ANX, or any IP network. The specifications were developed by the ANX Message Routing Work Group. This work group will describe the types of software and conventions a supplier should use to communicate EDI documents over the ANX.

The protocol describes how an application emulates a client browser to initiate a file transmission or retrieval with an HTTP server.

For detailed specifications, please contact the AIAG in Southfield, Michigan, at http://www.aiag.org.

Using HTTP for GISB

The Gas Industry Standards Board (GISB) is a voluntary, independent organization comprised of, and supported by, all segments of the natural gas industry. GISB develops and maintains voluntary standards governing electronic communications for business transactions within the natural gas industry.

One of these standards is the use of HTTP protocol for sending EDI messages. Netscape ECXpert supports the data communications part of this protocol and enables users to optionally use PGP/MIME via the Exit capability in the Gateway Service.

Please refer to http://www.gisb.org/ for purchasing the GISB HTTP specification supported by ECXpert.

Using the XML Connector SDK

The ECXpert 3.6 XML SDK provides a set of C++ Class APIs for users to build applications communicating with the eXML Connector through XML-formatted messages.

The SDK library also includes APIs to allow user applications to listen to a port and/or connect to a host and port for message exchanges. There are some samples that illustrate how to build a simple 'server' and 'client' programs. There is also a utility that allows easy submission of a document to the eXML Connector.

The XML SDK is documented in the ECXpert XML SDK chapter of the *iPlanet ECXpert Developer's Guide*.

Setting up Mapping and Translation

Mapping and translation in ECXpert is supported by the *Mercator* package that is bundled with the ECXpert System. The information provided here is completely ECXpert-specific, and only supplements the basic information contained in the *Mercator User's Guide*.

Using Legacy Maps with ECXpert

If you are presently satisfied with the functions provided by an existing map, there are two ways to continue using the unaltered map file in conjunction with ECXpert processing:

- Define the legacy map as an ECXpert service.

- Execute the legacy map prior to ECXpert processing.

To use the full mapping and translating functionality available with ECXpert, you must recreate the legacy map using *Mercator*. See the *Mercator User's Guide* for details.

Defining a Legacy Map as an ECXpert Service

To have an existing map file executed as part of ECXpert processing, do the following:

1. Define the legacy map file as a service.

2. Add the service to the appropriate service list.

Executing a Legacy Map before ECXpert Processing

The details of the legacy system in use determine the steps that are necessary in order to have an existing map file execute before ECXpert processing.

It is possible that the map is already being executed as one of the last steps in processing by the legacy system. Check with the system administrator for that system to determine what preparation is still needed, if any, for processing the incoming document.

NOTE	If the map is already executed by the legacy system, select "Output data pre-enveloped" in the Partnership tabs.

Overview of *Mercator*

The *Mercator User's Guide* contains most of the information needed for using the *Mercator* map definition tool to construct a map file for use with the ECXpert System. In addition to this basic information, you must follow several guidelines to provide the tightest possible degree of integration between ECXpert and the map:

- The physical location of all files is automatically managed by ECXpert; it does not matter what the files were called or where they were located when the map was created. The ECXpert System requests the map to enumerate its cards, and changes the location and file names of all input cards before executing the map.

- Furthermore, ECXpert generates unique names for all output cards, and records these names and their location in the ECXpert's database for later disposition.

- You can use any file names in any location when testing the map, without concern as to where ECXpert will get the input or place the output. What is important in developing and testing a map that will be used with ECXpert is that the content of the input files mimics what ECXpert will present to the map.

- When you have a map that has multiple input cards, the input to the additional cards needs to be in the following directory:

      $NSBASE/NS-apps/ECXpert/data/input

  The one exception is the input to a helper card, which is obtained through the user interface in the Partnership function, Control tab.

Mapping from Application to Application Formats

ECXpert is capable of handling Any-to-Any type of mapping.

When the submission unit is of a proprietary format and needs to be translated to another proprietary format, ECXpert can accomplish this by doing file-level mapping. The entire submission unit is passed to the *Mercator* map for translation. The *Mercator* map is responsible for generating the entire output file.

Mapping from EDI to Application Formats

When the ECXpert System receives a submission unit consisting of one or more EDI interchanges, it first makes a parsing pass on that file. In the parsing pass ECXpert records the following information in the ECXpert database:

*   The location and size of every document, functional group, and interchange in the submission unit;

*   Information on interchanges and functional groups with each document; the trading partner IDs for the sender and receiver, and EDI standard document type, and optionally the sender and receiver application qualifier and code, are used to look up the map to execute for a given document.

The map is executed in a second translation pass on the submission unit file.

The ECXpert System always passes only one document's data at a time to the map execution engine. For each map execution, ECXpert provides the EDI input data to the map as card 1.

Your map must expect the EDI interchange in card 1. ECXpert pieces together the following parts:

*   the interchange header

*   the functional group header, if one is present

*   the document, including its document header and trailer

*   the group trailer, if one is present, with the transaction count set to 1

*   the interchange trailer, with the count set to 1.

ECXpert then presents this data to the map translation engine as the input stream.

NOTE	Write the map to expect normal EDI interchanges; ECXpert ensures that each interchange has only one functional group, and that each functional group presented to the map contains only one document.

The data in the original EDI submission unit file is never altered; ECXpert stores the location and size of each component in the first (parsing) pass, and assembles the pieces with adjusted trailer counts in the second (translation) pass when document data is presented to the Map Execution Engine.

Mapping from Application to EDI Formats

When an application is to provide a file of proprietary format documents to ECXpert to map into EDI documents, the application supplying the data must follow some guidelines to aid in the process flow.

Because the application data has no known structure to the ECXpert System, the application must delineate each logical record set to be provided to the map as a "document" by placing header and trailer records around each logical record set in the application file. This is how the application adds explicit structure to the application data.

ECXpert can then follow its Parse/Translate model of operations, just as in inbound EDI mapping. First, the position of each logical record set is recorded in the database during Parse. Each logical record set is then presented to the translator in one map execution, just as in the interchange/group/document model of EDI processing.

Data Structure

Application data must be packaged with the following structure:

- Header record

- Application data

- Trailer record

Terminator

The header record, the application data, and the trailer record must all be terminated by the same character, selected from the following: '0D0A' (carriage return, line feed), '0A' (line feed), or '1C'.

Header Record

The following header record must be present in the application data before each application record set:

```
HREC**, Sender Qualifier, Sender ID, Receiver Qualifier,
Receiver ID, Document ID, Document Format, Document Version,
Document Type, Other, Functional Group ID, Message Release No,
Sender App Qualifier, Sender App Code, Receiver App Qualifier,
Receiver App Code   segment terminator
```

The header record begins with 'HREC**,' and must be delimited with any of the valid ANSI X12 data element separator characters. All fields in the header record are alphanumeric.

Table 6-1 describes the maximum sizes for each field. All fields are required for both ANSI X12 and EDIFACT, unless otherwise noted.

Table 6-1   Maximum sizes for header record fields

Data Element	Description	Required?	Length
Initiator	"HREC**"	Y	6-6
Sender Qualifier	Sender ID Qualifier	Y	1-4
Sender ID	Sender ID	Y	1-35
Receiver Qualifier	Receiver Qualifier	Y	1-4
Receiver ID	Receiver ID	Y	1-35
Document ID	Document ID	Y	1-15
Document Format	Format of data: X = ANSI X12; UN = UN/EDIFACT	Y	1-5
Document Version	Version number (for ANSI X12, this is the version from the GS line of a document, *not* the version from the ISA line).	Y	1-10
Document Type	Document Type	Y	1-15

Table 6-1   Maximum sizes for header record fields *(Continued)*

Data Element	Description	Required?	Length
Other	In release 3.6, this field is not used; it remains in the HREC for backward compatibility. **Note:** You still must include a comma and a space in this location in order for the HREC to be processed correctly.	N	1-100
Functional Group ID	ANSI functional group type. For example, an 850 would have "PO" here, and an 810 would have "IN" here. Not used in EDIFACT; leave the field empty.	N	2
Message Release No	EDIFACT message release number. Not used in ANSI; leave the field empty.	N	1-3
Sender App Qualifier	Sender's application code qualifier. Not used in ANSI; leave the field empty.	N	1-4
Sender App Code	Sender's application code.	N	1-35
Receiver App Qualifier	Receiver's application code qualifier. Not used in ANSI; leave the field empty.	N	1-4
Receiver App Code	Receiver's application code.	N	1-35

These header record contents allow ECXpert to point to the correct map for the application document that follows. By having a header record in front of each application document, the application is free to mix multiple document types (multiple maps) in the same file.

ECXpert optimizes translation by keeping the map resident if the map used by the next document is the same as that used by the previous one.

Trailer Record

The following trailer record allows ECXpert to parse the application data with clarity as to where the record set terminates:

`TREC**`   *terminator*

Processing

The model of processing operation is symmetrical to inbound operation. ECXpert runs a parsing pass on the submission unit file from the application. The HREC** header (instead of the ISA, GS, ST…) is found, and the document location and size are recorded in the database.

Then, in a second translation pass, the translator is called once per document in the input file. The map translation engine is passed the header record plus all data up to the next header record. The header record does not contain all of the supporting information for the map execution; some is derived by ECXpert from the trading relationship pointed to by the header record.

ECXpert writes an extra input card containing "aids" to the mapping process derived from the trading relationship records it maintains. This extra card contains the delimiting information to assist the map translation engine in assembling the correct EDI output; that is, it contains the segment terminator, the element separator, and the sub-element separator. With the EDIFACT standard, it also contains the decimal point character, and the release character.

Note that the header record carries any extra information the user wants to convey to the map translation engine, following the DocType field. ECXpert only requires up to and including the DocType for its keying, but will store and present any other data up to the c/r to the map.

To summarize, the following information is presented to the outbound map:

- Card 1 contains one logical record set from the application data file, as bounded by the header and trailer records defined above, including these header and trailer records.

- Card 2 contains all of the possible delimiting information that the map might require in assembling EDI output, and has the following format in a comma-delimited, crlf-terminated record:

  - segment termination (min 1, max 4)

  - element separator (min 1, max 4)

  - sub-element separator (min 1, max 4)

  - decimal point character (min 1, max 4)

  - release character (min 1, max 4)

The data elements in Card 2 should be mapped to corresponding data elements in the primary output card. In the case of ANSI X12, these data elements should be mapped in the ISA segment. In the case of the EDIFACT map, these data elements should be mapped to the UNA segment. Refer to the sample maps provided in the `...../ECXpert/maps` subdirectory of your installed base directory (e.g. `$NSBASE/NS-apps`).

For both inbound and outbound processing, extra input cards are supported by ECXpert; the name of the file(s) from the map is preserved, but the location of the file is adjusted by ECXpert to its working location specified in the ECXpert configuration.

If other input cards are expected by the map, ECXpert makes sure that all input is present before permitting the map to execute. If input cards are missing, an audit message will be posted, and the map execution postponed.

The outputs from the map are placed in unique output files for each document. The names and locations of those files, along with the status of the mapping, is recorded in ECXpert's database.

The output is placed in separate files to provide the greatest possible flexibility for bundling the EDI data together at send time. This way it is permissible to have different documents use different transport methods, even between the same trading partners.

Notes on Input Cards

You should define extra input cards as input only, *not* as input/output. Extra input cards are any beyond card number 1 on inbound processing, and any beyond card number 2 on outbound processing.

The helper card must be card number 2 in the map definition. ECXpert generates the helper card automatically, to supply the delimiter characters specified in the trading relationship.

Generation of EDI Envelopes

For the outgoing EDI file, ECXpert provides the following options for generating EDI envelopes.

- **Pre-Enveloped** - The *Mercator* map has to generate the EDI envelopes and ECXpert will not touch the envelope data.

- **ECX Generates (or overrides) entire envelope**—ECXpert generates the entire EDI envelope, replacing any enveloping generated by your map.

- **Use optional elements and Ctrl/Msg Ref# from data**—The *Mercator* map generates the envelope. ECXpert preserves the optional elements and control or message reference numbers produced by the map but replaces the rest of the enveloping.

- **Use optional elements from data but ECX generates Ctrl/Msg Ref#**—The Mercator map generates the envelope. ECXpert preserves the optional elements from the data, but replaces the control or message reference numbers and the rest of the envelope.

Mapping from EDI to EDI Formats

ECXpert can also take an incoming submission unit in EDI format and translate it into another EDI format. In this mode of translation, the parsing of the incoming EDI document works the same as with EDI to Application mapping (see "Mapping from EDI to Application Formats" on page 247).

ECXpert records the interchange, functional group, document, and optionally the sender and receiver application qualifiers and codes. Based on this information, ECXpert looks up the partnership and map to execute for a given document.

After translation, ECXpert can optionally generate the EDI envelope for the outgoing file, as it does in Application to EDI mapping (see "Mapping from Application to EDI Formats" on page 248). The same generation of envelope options can be used for this type of mapping.

Mapping from XML to EDI Formats

When ECXpert receives a submission unit consisting of one or more XML documents, it first makes a parsing pass on that file. In the parsing pass it records the following information in the ECXpert Data Store:

- the location and size of each XML document

- information for each document including:

  ○ trading partner IDs for the sender and the receiver

  ○ document type

  ○ sender and receiver qualifier and code

This information is used to look up the map to execute for each document. Information such as the sender ID, sender qualifier, receiver ID, receiver qualifier, document type etc. is retrieved from the incoming data based on the XSL style sheet specified for the document.

Data Structure

Each XML document should be well-formed. Since XML documents do not have a fixed structure as compared to EDI documents, an XSL stylesheet needs to be specified to ECXpert to extract the required key data from the input document. The sender ID, receiver ID and document type are mandatory. The stylesheet must be specified using one of the following methods:

1. Specify the name of the stylesheet in a processing instruction:

   <? ecx-stylesheet href="<name_of_style_sheet>" type="text/xml" ?>

2. Specify the name of a known Data Type Definition (DTD) file for the XML document in a DOCTYPE declaration The stylesheet can be obtained by mapping the DTD name to a stylesheet name.

3. Invoke a user-defined function that returns the stylesheet data.

For more information on how to construct the stylesheet and reference the stylesheet to ECXpert, refer to Appendix B, "Constructing and Referencing A Stylesheet for an XML Document."

Processing

In the first processing pass of the XML document, the document is parsed to retrieve key information. In this parse phase, the XML parser identifies and records information about the document to get the stylsheet information. The XML document is then processed with the stylesheet using an XSLT processor to extract the required key information, such as the sender ID, receiver ID, document type, and so forth. This data is then stored in the ECXpert Data store.

The map is executed in a second translation pass on the submission unit file. ECXpert always passes only one document's data at a time to the map execution engine.

The data in the original XML submission unit file is never altered; ECXpert stores the location and size of each component in the first(parsing) pass, and assembles the pieces in the second (translation) pass when document data is presented to the Map Execution Engine.

Generation of EDI envelopes

For the outgoing EDI file, ECXpert provides the same options to generate EDI envelopes as that described in the topic "Generation of EDI Envelopes" on page 252 of the section "Mapping from Application to EDI Formats" on page 248.

Mapping from XML to Application/XML

ECXpert is capable of mapping from one XML standard to any other XML standard or to a proprietary standard, provided a Mercator map exists to do the required translation. The submission unit can contain many XML documents, as the ECXpert parser is capable of detecting an XML document in a file containing multiple documents and storing information, including key fields for processing, for each document to the ECX data store. The Mercator map is responsible for generation of the entire output file.

Avoiding Potential Problems with *Mercator* Maps

There are several potential problems with use of *Mercator* maps that can easily be avoided. One involves use of the comma as the decimal character in EDIFACT maps. Most are related to data validation.

These potential problems are listed below:

- Using comma for decimal character (EDIFACT only)

- Reporting missing mandatory segments

- Validating the document segment count

- Not using "Reject" cards when *Mercator* "Restart" feature is turned off

- Unable to port map from NT to UNIX.

The following sections tell how to avoid these potential problems. The examples given are ANSI X12, but the same process works with EDIFACT.

Using Comma for Decimal Character (EDIFACT Only)

If you are using *Mercator* 1.3e to create EDIFACT maps, the period decimal character is accepted but the comma decimal character is not.

The problem is fixed in the version of *Mercator* Execution Engine included in ECXpert Version 1.1.

Reporting Missing Mandatory Segments

If an entire mandatory segment is missing from an EDI document, the error is not surfaced from *Mercator* to ECXpert unless you have turned off "Restart" in your type tree for the components in question.

Follow the steps below to turn off "Restart" in *Mercator*:

4. Launch the *Mercator* Type Editor.

5. Open your type tree.

6. Expand your type tree.

In this example, the ANSI X12 version 003020 type tree with an 810 document looks like this:

```
EDI
|--Interchange
   |--Inbound
      |--X12
         |--Partner
```

7. Double-click a component.

In this example, you would double-click the "Partner" component. With "Restart" on, the Component window shows a small box with the letter "R" to the left of the Component name.

8. Turn off "Restart."

Click [R] on the menu bar, or choose Component > Restart from the menus.

The small box with the letter "R" to the left of the Component name is removed, indicating that "Restart" is turned off.

9. Repeat these steps for the rest of the tree.

Repeat the steps above for each component in the tree that is involved.

NOTE	Be sure to choose Type > Save from the menu bar to save each type tree.

10. Without closing the *Mercator* Type Editor, launch the *Mercator* Map Editor.

11. Open your map.

NOTE	You must select Card	Edit Input and specifically select the same type tree again to force it to re-read the modified file.

12. Build and run your map on "good" sample data.

Use a sample input data file that does not have any required segments missing.

13. If necessary, port the map again to Sun Solaris.

Copy the map, or FTP the map in binary mode, to your ECXpert directory, *$NSBASE*/NS-apps/`ECXpert/maps`.

14. Test the new map on "bad" sample data.

Submit a document that is missing a mandatory segment. Your Activity Tracking Event Log should show errors.

The following error sample is produced by sample data for an 810 that is missing the BIG segment:

```
Error 8 performing mapping
PM_INPUTINVALID: A validation error occurred on an input file
```

Validating the Document Segment Count

Both ANSI X12 and EDIFACT provide for a segment count in the document that can be used as a cross-check to ensure that all segments sent are present. In ANSI X12, this segment count occurs as the first offset field in the SE segment.

To make sure that the segment count matches the number of segments in a Transaction Set, you must modify the standard component rule in the tree.

In ANSI X12, in each transaction set group, the unmodified component rule for the SE Segment would read something like the following:

```
TSCtrl# Element:$ = TSCtrl# Element:ST Segment
```

This rule checks to make sure the control number in the ST matches the control number in the SE.

For each transaction set where you want to add the check for the number of segments, this rule to the following:

```
InclSegments Element:$ = Count(Segment IN COMPONENT)
   & TSCtrl# Element:$ = TSCtrl# Element:ST Segment
```

No "Reject" Cards when *Mercator* "Restart" Feature is Turned Off

Note that *Mercator*'s mapping features "`Restart`" and "`Reject`" work in tandem. If you turn off "`Restart`" in order to get proper data validation, or for some other reason, you must design your map so that it does not use any "`Reject`" cards.

Getting the Tracking ID into Your Map

ECXpert can provide the Tracking ID of a submission to one of the map input cards. This is passed in memory for any process that needs to access it. It is then up to the user to do what they want with this.

Having the tracking ID allows the map to access the relevant entries in the tracking tables in the Oracle Database.

The input card must have the special reserved name, PARAMS_FROM_ECX. Whenever Translate sees this it passes the Tracking ID. If this input card is not defined in your map, the Tracking ID is not passed.

In the Authoring Tool

Define an Input Card named PARAMS_FROM_ECX. Its Type Tree should point to a single item whose item format must be "character" that can be interpreted as either "text" or "number".

The actual file that you create for testing should contain just a number, with no carriage return or line feed.

On Your Operational Platform

There is no need to port this Tracking ID file to your operational platform. ECXpert will generate it internally.

Displaying the Partnership Administration Tab

Follow the steps below to display the Partnership Administration tab.

1. Log into the ECXpert Product Administrative Interface.

2. Click the Partnership function on the left.

The Partnership Administration tab (Figure 6-2) is displayed.

Figure 6-2   Partnership Administration tab

From this tab you can add, change, and delete trading partnerships.

NOTE	Except for adding a new trading partnership on a blank form, all other partnership administration tasks require you to first display information for an existing partnership. See "Displaying Information for an Existing Partnership," for details.

Refer to the following sections for details on specific tasks:

❍   "Displaying Information for an Existing Partnership" on page 260

❍   "Working with the Partnership Definition Tabs" on page 266

Displaying Information for an Existing Partnership

Except for adding a new trading partnership, for which you enter all the information yourself, all other tasks that you can perform from this tab require you to first display information for an existing partnership. Follow the steps below to display information for an existing partnership.

1. Display the Partnership Administration tab (Figure 6-2).

2. Click the task you want to perform.

Click one of the following:

❍ **Copy**—to add a new member using another member as a template

❍ **Change**—to change information for an existing member

❍ **Delete**—to delete an existing member

The Partnership Search tab (Figure 6-3) is displayed.

NOTE	Figure 6-3 shows the Partnership Search tab in the Copy Partnership operation. If you click Change or Delete, then "Change" or "Delete" appears in place of "Copy."

Figure 6-3 Partnership Search tab
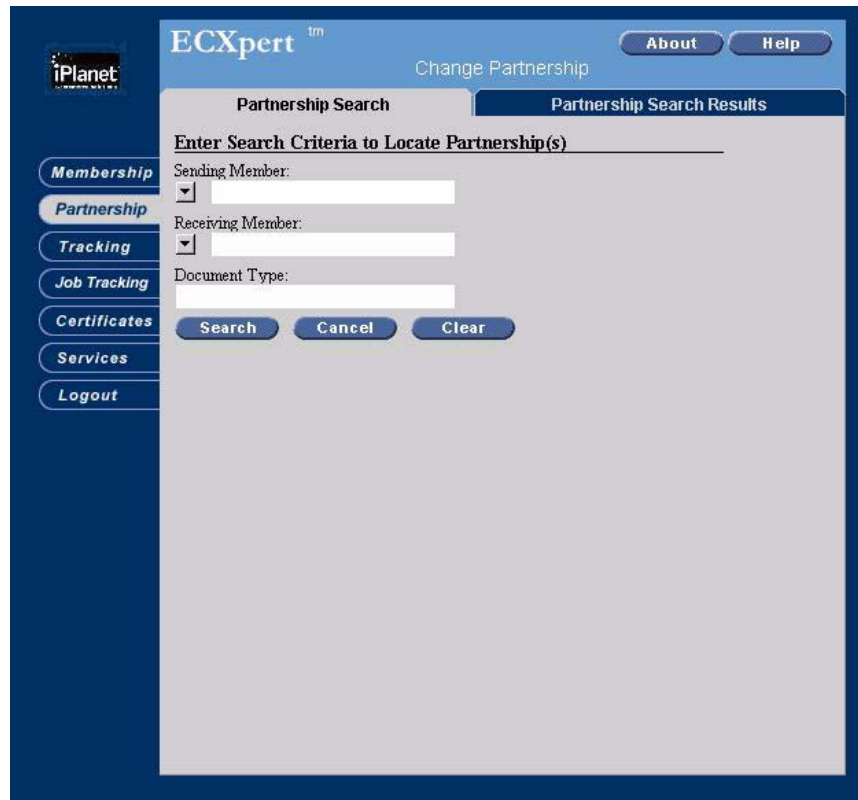
Table 6-2 Information on the Partnership Search tab

Item	Description
Sending Member	The member ID of the member who sends a document in the partnership that you want to find.
Receiving Member	The member ID of the member who receives a document in the partnership that you want to find.
Document Type	The type of document sent or received in the partnership that you want to find (for example, 850, or Invoice).

NOTE	Only the information that you enter is matched. If you enter only the sending member's ID, all partnerships in which that member ID is the sending member are returned on the Partnership Search Results tab (Figure 6-4). If you leave all three fields blank, all partnerships are returned on the Partnership Search Results tab.

3. Enter the sending member's ID.

The sending member is the one who sends documents in the trading partnership. You must supply the member ID for this member in the Sending Member field.

You can type the ID directly into the Sending Member field.

OR...

You can select the sending member's ID from a list:

❍ Click the Expand button ▼ to drop down the List of Members.

❍ Select the ID for the sending member in the partnership that you want to change, copy, or delete.

❍ Click Expand again to close the list.

4. Enter the receiving member's ID.

The receiving member is the one who receives the documents in the trading partnership. You must supply the member ID for this member in the Receiving Member field.

You can type the ID directly into the Receiving Member field.

OR...

You can select the receiving member's ID from a list:

❍ Click the Expand ▼ button to drop down the List of Members.

❍ Select the ID for the receiving member in the partnership that you want to change, copy, or delete.

❍ Click Expand again to close the list.

5. Optionally, enter the document type.

The document type identifies the type of document that is sent from the receiving member to the receiving member in the partnership that you want to change, copy, or delete.

Type the document type in the Document Type field.

NOTE	If you do not enter a document type, the search results will include all the partnerships for the sending and receiving member IDs that you supplied. If more than one partnership is listed, you can select the one for the document type of interest from that list.

6. Click Search.

One or more partnerships matching the information that you just entered are displayed on the Partnership Search Results tab (Figure 6-4).

NOTE	If you see an error message, it means that the information you provided does not match any existing partnerships. Try the search again, specifying only one of the trading partners (sending member or receiving member only) and no document type.

Figure 6-4   Partnership Search Results tab
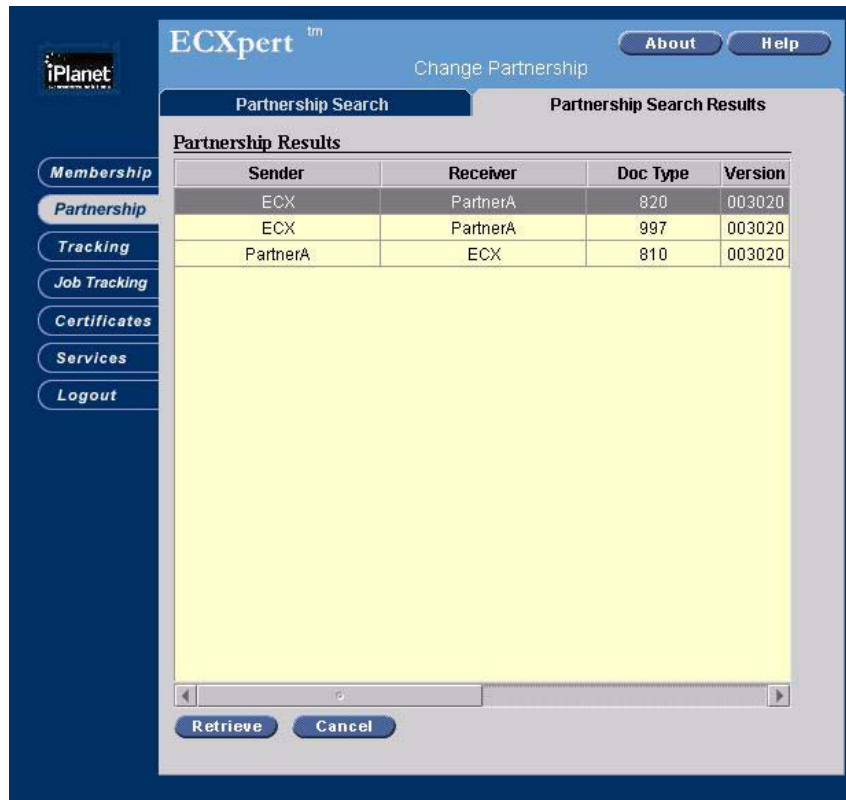
Table 6-3   Information on the Partnership Search Results tab

Item	Description
Sender	The entry in the **Sending Member** field on the Partnership Info tab for the partnership.
Receiver	The entry in the **Receiving Member** field on the Partnership Info tab for the partnership.
Doc Type	The entry in the **Document Type** field on the Partnership Info tab for the partnership.
Version	The EDI (ANSI or EDIFACT) from either the Input EDI or Output EDI tab for the partnership.
Interchange Sender Qual ID	The Interchange Sender QualID for ISA Sender for ANSI Doc Types.

Table 6-3   Information on the Partnership Search Results tab *(Continued)*

Item	Description
Interchange Receiver Qual ID	Interchange Receiver QualID for ISA Receiver for ANSI Doc Types.
Group Sender App Code	Group Sender App Code" for GS02 Sender for ANSI Doc Types
Group Sender Qualifier	The Group Sender Qualifier" for EDIFACT Doc Types.
Group Receiver App Code	The Group Receiver App Code for GS03 Receiver for ANSI Doc Types.
Group Receiver Qualifier	The Group Receiver Qualifier for EDIFACT Doc Types.

7. Display a partnership's information.

Select a partnership, then click Retrieve — Delete if you are deleting the partnership.

NOTE	Note on Deleting:
	If you are deleting the partnership, you are prompted to view information before deleting. Your options are:
	• Yes—display the partnership's information on the partnership definition tabs before deleting.
	• No—delete the partnership immediately, without further confirmation.
	• Cancel—return to the Partnership Administration tab without deleting the partnership or displaying its information.
	If you are changing or copying the partnership, or viewing the partnership information before deleting, the information for the partnership is now displayed in the partnership definition tabs.
	These tabs are described in detail in "Working with the Partnership Definition Tabs" below.

Working with the Partnership Definition Tabs

You can delete a partnership without first viewing its information on the partnership definition tabs. All other partnership administration tasks require you to use the same partnership definition tabs to enter or view partnership information.

The heading on the partnership definition tabs changes to reflect the task you are performing, but the details remain the same across tasks. The partnership definition tabs can include as many as five different tabs, depending on the selections you make.

This section describes how you fill in information on the different partnership definition tabs, and how you navigate between tabs.

The pictures of the tabs are specific to the Change Partnership task, but the information applies equally to adding, changing, or copying partnerships. If you are deleting a partnership, you can only view the information displayed.

Working with the Partnership Info Tab

1. Display the Partnership Administration tab (Figure 6-2) on page 259.

2. Click the task you want to perform.

   If you click Add, the Partnership Info tab (Figure 6-5) is displayed immediately. For the other buttons (such as Change or Copy), you must first display information for an existing partnership and then call up the Partnership you want to change or copy information from for a new partnership.

   See "Displaying Information for an Existing Partnership" on page 260 for details. The heading at the top of the partnership definition tabs reflects the task you are performing.

3. Fill in the information on the Partnership Info tab.

Figure 6-5   Partnership Info tab

Table 6-4   Information on the Partnership Info tab

Item	Description
Partnership Details	
Sending Member	The member ID of the member who sends a document in this partnership. This field is required.
Receiving Member	The member ID of the member who receives a document in this partnership. This field is required.

Table 6-4 Information on the Partnership Info tab *(Continued)*

Item	Description
Partnership Type	From the drop-down menu, select one of the following: • Application to Application—an application data format is being translated from one application data format to another application data format • Application to EDI—an application data format is being translated to an EDI data format • EDI to Application—an EDI data format is being translated to an application data format • EDI to EDI—an EDI data format is being translated to another EDI data format • XML to EDI—XML data format is being translated to an EDI data format • XML to Application/XML—an XML data format is being translated another proprietary application or XML data format.
Document Type	The type of document sent or received in this partnership (for example, 850 or INVOIC). This Document Type is used to specify how to translate incoming data by linking it to a Service List. This field is required. For EDI data, this must correspond to an EDI standard document type; for non-EDI data, this can be any mutually agreed upon document type. For non-EDI data, you must match this field exactly when setting up a Service List. For XML data, the document type is not limited to xml. **Note:** If you are using SMTP protocol, this must be the MIME subtype agreed upon by the partners. You can set the MIME type and subtype in your email system. (For example, with Netscape Messenger, this is set in the Edit | Preferences dialog, Navigator, Applications section.)
Billing Code	Use this field to enter the billing code if your site uses billing codes to track the number of sender, receiver, and document type transactions that occur in a specified time period for billing purposes. **Note**: This feature is used in conjunction with the billing data capture utility described in the *iPlanet ECXpert Developer's Guide*.

Table 6-4   Information on the Partnership Info tab *(Continued)*

Item	Description
Partnership Description	Use this field to enter any descriptive information or notes about the partnership. A description can contain as many as 60 characters. This field is optional.
Do not purge for (days)	The number of days to retain a document in the ECXpert data store. The default is 5 days. The maximum number of days you can specify is 999. Documents that are older than their retention period are selected by the Purge utility for either purging or archiving.
Processing Options	
Enable Trading vs. **Disable Trading**	**Enable Trading** activates the trading partnership. This is the default. **Disable Trading** deactivates the trading partnership.
Map Name	The name of the map file to use to translate the document sent or received in this partnership, if incoming information needs to be translated. If the map is located in the *$NSBASE*/NS-apps/*ECXpert/maps* directory, you do not need to specify the full path to the map file. If the map you select generates multiple output cards, specify how they should be processed on the Outputs tab (Figure 6-8 on page 280).
Incoming SMTP	
Sender Certificate Type and **Receiver Certificate Type**	For each, select one of the following: • None—(default) if no certificate is used • Self-Signed Certificate—if a self-signed certificate is used • New VeriSign Class 3—if a new VeriSign class 3 certificate is used • VeriSign Class 1—if a VeriSign class 1 certificate is used • VeriSign Class 2—if a VeriSign class 2 certificate is used

Table 6-4   Information on the Partnership Info tab *(Continued)*

Item	Description
Encryption and Authentication	Select one of the following for incoming SMTP data:
	• **Not Signed or Encrypted (plain)**—Arrives in plain text (MIME), and provides no security or authentication.
	• **Encrypted Only**—Arrives encrypted, but provides no authentication.
	• **Signed Only**—Arrives signed, authenticating the sender of a document, but provides no security.
	• **Signed and Encrypted**—Arrives signed, authenticating the sender, and encrypted. Use for confidental data when authentication is also required.

4. Continue with the next tab.

Click Next. Based the tab that appears next, continue with these instructions at the location listed below:

Tab	Continue with...
Input EDI	"Working with the Input EDI Tab" on page 282
Input XML	"Working with the Input XML Tab" on page 271
Input HREC	"Working with the Input HREC Tab" on page 291
Output EDI	"Working with the Output EDI Tab" on page 296
Outputs	"Working with the Input XML Tab" on page 271
Protocols	"Working with the Protocols Tab" on page 314

Working with the Input XML Tab

When you set the Partnership Type to either XML to EDI, or XML to Application/XML, the Input XML tab is displayed on the Partnership Administration screen.

For the XML to EDI Partnership Type, the Output EDI tab is also displayed. The Output EDI tab is described in the section "Working with the Output EDI Tab" on page 296.

How ECXpert's Parse Service Keys XML Input Data to Determine a Partnership

When using Parse in your service list, there are two things that need to match up to successfully find a Partnership after Parsing an input transaction in ECXpert:

- The key values that the Parse service determines from the input data (e.g., sender ID, receiver ID, doctype), and

- The database fields written at the time that the Partnership was established.

Table 6-5   StyleSheet Tags (Lookup Keys) Used By Parse to Determine A Partnership

StyleSheetTag[1]	XML to EDI & Standard -XML	XML to EDI & Standard -ANSI[2]	XML to EDI & Standard - EDIFACT[2]
Sender Qualifier	Input XML - Sender Qualifer ID (text string before colon character)	Input XML - Sender Qualifer ID (text string before colon character)	Input XML - Sender Qualifer ID (text string before colon character)
Sender ID	Input XML - Sender Qualifer ID (text string after colon character)	Input XML - Sender Qualifer ID (text string after colon character)	Input XML - Sender Qualifer ID (text string after colon character)
Receiver Qualifier	Input XML - Receiver Qualifer ID (text string before colon character)	Input XML - Receiver Qualifer ID (text string before colon character)	Input XML - Receiver Qualifer ID (text string before colon character)
Receiver ID	Input XML - Receiver Qualifier ID(text string after colon character)	Input XML - Receiver Qualifier ID(text string after colon character)	Input XML - Receiver Qualifier ID(text string after colon character)
Doc Type	Partnership Info - Document Type	Partnership Info - Document Type	Partnership Info - Document Type

Table 6-5   StyleSheet Tags (Lookup Keys) Used By Parse to Determine A Partnership *(Continued)*

Doc ID	Input XML - Not visible Default: NONE	This should match what you enter for the Functional ID (GS01). If you do not enter any value here, and you have a standard doctype of, say, 850, this value defaults to PO (in the Input XML tab). The docid in the stylesheet should correspond to this value.	For EDIFACT, by default the value is set to be the same as the doctype on the the Partnership Info tab. So the docid value from the stylesheet MUST be the same as the doctype.
Standard	Input XML - XML - Uses value "ML"	Input XML - ANSI - Uses value "X"	Input XML - EDIFACT - Uses value "UN"
Version	Not visible Default : 0	Input XML - Group Version (GS08) - Example 003040	Message Version (UNG...)
Release	Not visible Default : 0	Not visible Default : 0	Message Release (UNG...)

For XML input data, Table 6-5 indicates the complete list of look-up keys in the Stylyesheet Tags data column. These values were established by applying a stylesheet to the input data, thus producing another XML document.

When XML to EDI partnerships are being established, certain fields are written to the database. Since the choice of available fields changes based on whether you select XML, ANSI, or EDIFACT, the relationship between the data you see on the ECXpert admin screens and the data stored in the database changes. For example, if you choose XML as the input type, the version number is not shown on the admin UI, so a default of 0 is written to the database.

The stylesheet used to create the partnership lookup XML structure must match the partnership in the database, so be sure the stylesheet puts 0 in the version element or, do not use the version element reference at all in the stylesheet.

NOTE	If you are adding a new partnership, the Standard field is set to ANSI by default (Figure 6-9). You can change this to EDIFACT or XML as needed. If you are displaying an existing partnership, Standard can be set to either ANSI, **EDIFACT**, or XML. Using XML as the standard has no field entry requirements.

1. Specify Interchange Level Information on the Input XML tab, as shown in Figure 6-6 and described by the fields in Table 6-6. This information applies to both ANSI and EDIFACT standards.

Figure 6-6   Input XML tab, ANSI Standard selected

Table 6-6   Input XML tab, ANSI or EDIFACT standard-Interchange Level
Information

Item	Description
Interchange Level Information	
Sender Qualifier ID	The Sender Qualifier ID. The options available in the drop-down list are the trading address(es) on file for the member specified as the Sending Member in the Partnership Information tab (see "Working with the Partnership Info Tab" on page 266).
	Caution: If the only option listed is *NONE* , the member has no trading address on file. Proceed directly to the Membership tabs (see "Displaying Information for an Existing Member" on page 205) and enter a trading address for this member. You cannot save the partnership data without specifying a trading address for each member.
Receiver Qualifier ID	The Receiver Qualifier ID. The options available in the drop-down list are the trading address(es) on file for the member specified as the Receiving Member in the Partnership Information tab (see "Working with the Partnership Info Tab" on page 266).
	Caution: If the only option listed is *NONE* , the member has no trading address on file. Proceed directly to the Membership tabs (see "Displaying Information for an Existing Member" on page 205) and enter a trading address for this member. You cannot save the partnership data without specifying a trading address for each member.
Standard	Selecting ANSI (default) makes the rest of the tab below look this way. **ANSI** provides the ISA-IEA envelope structure and syntax and ANSI X12 997 Functional acknowledgments apply. Selecting EDIFACT changes the Group Level Information to that shown in
Group Level Information	

For information on items in these sections, if Standard is set to ANSI refer to Table 6-7
on page 275; if Standard is set to EDIFACT, refer to Table 6-8 on page 277.

2. Continue with the Input XML standard (for ANSI or for EDIFACT)-Group Level Information section that applies to your selection:

Standard selected	Continue with...
ANSI	"Specifying Input XML, ANSI Standard-Group Level Information" on page 275
EDIFACT	"Specifying Input XML, EDIFACT Standard-Group Level Information" on page 276

NOTE	If your standard is set to XML, there are no field entry requirements. The next step in this case is to go to the Output EDI tab, if using the XML to EDI Partnership Type (described in "Working with the Output EDI Tab" on page 296), or, the Protocols Tab, if using the XML to Application/XML Partnership Type (described in "Working with the Protocols Tab" on page 314).

Specifying Input XML, ANSI Standard-Group Level Information

1. If ANSI is specified as the standard, fill in the Group Level Information section of the Input XML tab.

Refer to Figure 6-6 and Table 6-7 for details. For information on the Interchange Level Information section, refer to Table 6-6 on page 274.

Table 6-7   Input XML tab, ANSI standard-dependent sections

Item	Description
Group Level Information (ANSI)	
Application Sender (GS02)	Application sender's identification.
Application Receiver (GS03)	Application recipient's identification.
Functional ID Code (GS01)	Functional group type. Use the **Document Type** to look up the corresponding **Group Type** in Appendix L, "ANSI X12 Group Types and Codes" and enter that **Group Type** value here. For example, an **850** would have **PO** here, and an **810** would have **IN** here.

Table 6-7 Input XML tab, ANSI standard-dependent sections *(Continued)*

Item	Description
Group Version (GS08)	The version of the ANSI standard you and your trading partner have agreed to use (for example, 003060).

2. Continue by clicking the Next button.

   Click Next. The Output EDI tab will be next if your Partnership Type is set to XML to EDI. The Protocols tab will be next if your Partnership Type is set to XML to Application/XML.

   Based on the tab that appears next, continue with these instructions at the location listed below:

Tab	Continue with...
Output EDI	"Working with the Output EDI Tab" on page 296
Protocols	"Working with the Protocols Tab" on page 314

Specifying Input XML, EDIFACT Standard-Group Level Information

1. If EDIFACT is specified as the standard, fill in the Group Level Information section of the Input XML tab.

   Refer to Figure 6-7 and Table 6-8 on page 277 for details. For information on the Interchange Level Information section, refer to Table 6-6 on page 274.

Figure 6-7   Input XML tab, EDIFACT Standard selected

Table 6-8   Input XML tab, EDIFACT standard-dependent sections

Item	Description
Group Level Information (EDIFACT)	
App Sender ID (UNG-S006-0040)	Application sender's identification code.
Message Version (UNG-S008-0052)	The EDIFACT message version number.
App Sender ID Qual (UNG-S006-0007)	Application sender's identification code qualifier.

Table 6-8   Input XML tab, EDIFACT standard-dependent sections *(Continued)*

Item	Description
Message Release (UNG-S008-0054)	The EDIFACT message release number. UNG-S008-0054, or, if no UNG segment is used, these are UNH-S009-0052 and UNH-S009-0054.
App Receiver ID (UNG-S007-0044)	Application receiver's identification code.
App Receiver ID Qual (UNG-S007-0007)	Application receiver's identification code qualifier.

2. Continue by clicking the Next button.

Click Next. The Output EDI tab will be next if your Partnership Type is set to XML to EDI. The Protocols tab will be next if your Partnership Type is set to XML to Application/XML.

Based on the tab that appears next, continue with these instructions at the location listed below:

Tab	Continue with...
Output EDI	"Working with the Output EDI Tab" on page 296
Protocols	"Working with the Protocols Tab" on page 314

Working with the Outputs Tab

If your map generates multiple output cards, the Partnership window will display the Outputs tab.

The Outputs tab (Figure 6-8) only appears if the map name you specify on the Partnership Info tab (Figure 6-5) generates multiple output cards. The information on this tab specifies the service list to use for additional output cards.

When you are adding a new partnership, the only way to display the Outputs tab for the first time is to click Next from the Partnership Info tab.

At other times, whenever you can see an Outputs tab at the top of the partnership definition tabs, you can click the Outputs tab to bring it forward (Figure 6-8).

NOTE	You must have the Routing service in the service list to process multiple outputs.
	When a map generates multiple output types, Routing specifies how to submit secondary output. You must define a Service List containing the Routing service before you can fill in the Output tab and define the trading partnership.
	See "Adding a New Service List on a Blank Form" on page 484, and "Copying a Service List—Adding a New Service List Based on Another" on page 484, for instructions.

3. Add or change information on the Outputs tab. Refer to Table 6-9 for field descriptions.

NOTE	The exact combination of tabs displayed when you first click Next from the Partnership Info tab depends on the Partnership Type you have selected.
	Figure 6-8 shows the Outputs tab with the other tabs that are present when Partnership Type is set to EDI to Application and the map specified on the Partnership Info tab requires multiple outputs.

Figure 6-8 Outputs tab

Table 6-9 Information on the Outputs tab

Item	Description
Specify Service List for Additional Output Cards	
ID	The Service List ID.
Sender	The sender in the sender/receiver/document type combination for which the Service List is defined.
Receiver column	The Receiver in the Sender/receiver/document Type combination for which the Service List is defined. If "*" is displayed here, you can use the Receiver drop-down list to select a specific receiver.
Doc Type	The Document Type in the Sender/receiver/document Type combination for which the Service List is defined.

Table 6-9   Information on the Outputs tab *(Continued)*

Item	Description
Receiver drop-down list	A list from which you can select a specific receiver for a selected Service List for which Receiver is listed as "*" in the table above.
Add	Adds the selected Service List data from the table above to the selected card in the table below.
Remove	Removes Service List data from the card selected in the table below.
(Output Card table)	
Card #	Output card number.
Card Name	Output card name.
Sender	Sender in the Service List for the output card.
Receiver	Receiver in the Service List for the output card.
Doc Type	Document type in the Service List for the output card.

4. Select an output card.

    If there are multiple cards listed in the table at the bottom, select the card to process with the service list. If there is only one card, it is automatically selected.

NOTE	Only the secondary cards appear in this list. You must know the naming and order of the output cards to match them to the appropriate service lists.

5. Select a service list.

    If there are multiple service lists in the table at the top, select the service list to use with the selected card. If there is only one service list, it is automatically selected.

6. Add the service list to the output card.

Click Add. The Sender, Receiver, and Type information from the selected service list are entered into the selected output card Sender, Receiver, and Doc Type columns.

NOTE	You can click Remove to clear the selected card's Sender, Receiver, and Doc Type information.
	This is only necessary if you want to clear these fields. If you made a mistake, just go back to Step 4 and make different selections.

7. Repeat as necessary for additional output cards.

   Repeat these steps until you have specified the correct service lists to use for all the secondary output cards listed.

Working with the Input EDI Tab

8. If Partnership Type is EDI to Application, or EDI to EDI, the Input EDI tab is displayed on the Partnership Administration screen.

NOTE	The Input EDI tab appears only when the Partnership Info tab has Partnership **Type** set to EDI to Application or EDI to EDI.
	To display the Input EDI tab, click Next on the previous tab. The Input EDI tab is displayed. If you are adding a new partnership, Standard is set to ANSI by default (Figure 6-9). You can change this to EDIFACT as needed. If you are displaying an existing partnership, Standard can be set to either ANSI or **EDIFACT**.

9. Specify Interchange Level Information on the Input EDI tab.

NOTE	The exact combination of tabs displayed with the Input EDI tab depends on the Partnership Type you have selected on the Partnership Info tab. Figure 6-9 shows the Input EDI tab with the other tabs that are present when Partnership Type is set to EDI to Application.

Figure 6-9 Input EDI tab, ANSI Standard selected

Table 6-10   Input EDI tab, ANSI or EDIFACT standard-Interchange Level
Information

Item	Description
Interchange Level Information	
Sender Qualifier ID	The Sender Qualifier ID. The options available in the drop-down list are the trading address(es) on file for the member specified as the Sending Member in the Partnership Information tab (see "Working with the Partnership Info Tab" on page 266).
	Caution: If the only option listed is *NONE* , the member has no trading address on file. Proceed directly to the Membership tabs (see "Displaying Information for an Existing Member" on page 205) and enter a trading address for this member. You cannot save the partnership data without specifying a trading address for each member.
Receiver Qualifier ID	The Receiver Qualifier ID. The options available in the drop-down list are the trading address(es) on file for the member specified as the Receiving Member in the Partnership Information tab (see "Working with the Partnership Info Tab" on page 266). *Caution:* If the only option listed is *NONE* , the member has no trading address on file. Proceed directly to the Membership tabs (see "Displaying Information for an Existing Member" on page 205) and enter a trading address for this member. You cannot save the partnership data without specifying a trading address for each member.
Standard	Selecting ANSI (default) makes the rest of the tab below look this way. **ANSI** provides the ISA-IEA envelope structure and syntax and ANSI X12 997 Functional acknowledgments apply.
Group Level Information and Functional Acknowledgment	

For information on items in these sections, if Standard is set to ANSI refer to
Table 6-11 on page 285; if Standard is set to EDIFACT, refer to Table 6-12 on page 289.

10. Continue with the Input EDI standard (for ANSI or for EDIFACT)-Group Level Information section that applies to your selection:

Standard	Continue with...
ANSI	"Specifying Input EDI, ANSI Standard-dependent Information" on page 285
EDIFACT	"Specifying Input EDI, EDIFACT Standard-dependent Information" on page 288

Specifying Input EDI, ANSI Standard-dependent Information

1. Fill in the Group Level Information (ANSI) and Functional Acknowledgment (997) sections.

Refer to Figure 6-9 and Table 6-11 for details. For information on the Interchange Level Information section, refer to Table 6-10 on page 284.

Table 6-11   Input EDI tab, ANSI standard-dependent sections

Item	Description
Group Level Information (ANSI)	
Functional ID Code (GS01)	Functional group type. Use the **Document Type** to look up the corresponding **Group Type** in Appendix L, "ANSI X12 Group Types and Codes" and enter that **Group Type** value here. For example, an **850** would have **PO** here, and an **810** would have **IN** here.
Group Version (GS08)	The version of the ANSI standard you and your trading partner have agreed to use (for example, 003060).
Use App Codes (GS01/GS03) to locate partnerships	Check this box if you want ECXpert to locate partnerships based on the GS02 and GS03 values you enter below.
App Sender (GS02)	Application sender's identification.
App Receiver (GS03)	Application recipient's identification.

Table 6-11   Input EDI tab, ANSI standard-dependent sections *(Continued)*

Item	Description
Functional Acknowledgment (997)	
Generate FA	First choose when you want functional acknowledgments (FA) to be generated:
	• Never—Never generate FAs.
	• Always—For FA in all cases (acknowledgment codes "A", "E", or "R").
	• On Errors Only—For FA only when errors occur; when a transmission is rejected (acknowledgment code "R"), or accepted with errors (acknowledgment code "E").
	Warning: If you select **Always** or **On Errors Only**, ECXpert automatically creates a reverse partnership to support the FA, but you must edit that partnership so that the FA can be received successfully. See "Reverse Partnerships for ANSI Functional Acknowledgments (FAs/997s)" on page 352 for instructions.
FA Level	Second, choose the level at which you want FA generated (you can expand this level for errors by setting **Error Reporting Level** to a lower level):
	• Functional Groups—For functional acknowledgment at functional group level only (AK1 and AK9, before expansion by **Error Reporting Level** setting)
	• Transaction Set—For transaction set-level functional acknowledgment (AK1, AK2, AK5, and AK9, before expansion by **Error Reporting Level** setting)
	Note: This setting is ignored if **Generate FA** is **Never**.
Error Reporting Level	Last, choose the level to which you want FA to expand any errors reported:
	• Transaction Set—If there is an error, expand reporting to AK5 level
	• Segment—If there is an error, expand reporting to AK3 level
	• Element—If there is an error, expand reporting to AK4 level if possible (error is in data element)
	Note: This setting is ignored if **Generate FA** is **Never**.

Table 6-11   Input EDI tab, ANSI standard-dependent sections *(Continued)*

Item	Description
Comment Type	If you set **Error Reporting Level** to either **Segment** or **Element**, this field must contain the segment ID used as "comment" type in the *Mercator* map. The default, NTE, is used for the comment type in many Mercator type trees.

Examples of Functional Acknowledgment (997) Settings

Example 1: If you chose the following configuration when setting up your partnership:

- ❍ **Generate FA** set to **Always**

- ❍ **FA Level** set to **Functional Groups**

- ❍ **Error Reporting Level** set to **Transaction Set**

You would get a 997 which contains: AK1 and AK9 only for transaction sets in which there are no errors (acknowledgment code "A"); AK1, AK2, AK5, and AK9 for transaction sets with errors (acknowledgment code "E" or "R").

Example 2: If you chose the following configuration when setting up your Partnership:

- ❍ **Generate FA** set to **On Errors Only**

- ❍ **FA Level** set to **Functional Groups**

- ❍ **Error Reporting Level** set to **Element**

You would no 997 at all on an error-free file (acknowledgment code "A"), but if there is an error (acknowledgment code "E" or "R"), you would see AK1, AK2, AK3, AK4 (if the error was in a data element), AK5, and AK9.

Mercator Map Considerations: For important information on Mercator map settings, see Appendix D, "Required Mercator Settings for ANSI Functional Acknowledgment (997)."

2. Continue with the next tab.

Click Next. Based on the tab that appears next, continue with these instructions at the location listed below:

Tab	Continue with...
Output EDI	"Working with the Output EDI Tab" on page 296
Protocols	"Working with the Protocols Tab" on page 314

Specifying Input EDI, EDIFACT Standard-dependent Information

1. Fill in the Group Level Information (EDIFACT) section.

   Refer to Figure 6-10 below and Table 6-12 on page 289 for details. For information on the Interchange Level Information section, refer to Table 6-10 on page 284.

Figure 6-10   Input EDI tab, EDIFACT Standard selected

Table 6-12   Input EDI tab, EDIFACT standard-dependent sections

Item	Description
Group Level Information (EDIFACT)	
Message Version Number (UNG-S008-0054)	The EDIFACT message version number.
Message Release Number (GS08)	The EDIFACT message release number. UNG-S008-0052, or, if no UNG segment is used, these are UNH-S009-0052 and UNH-S009-0054.
Use UNG to locate partnerships	Check this box if you want ECXpert to locate partnerships based on the UNG values you enter below.

Table 6-12   Input EDI tab, EDIFACT standard-dependent sections *(Continued)*

Item	Description
App Sender Code (UNG-S006-0040)	Application sender's identification code.
App Receiver Code (UNG-S007-0044)	Application receiver's identification code.
App Sender Code Qual (UNG-S006-0007)	Application sender's identification code qualifier.
App Receiver Code Qual (UNG-S007-0007)	Application receiver's identification code qualifier.
CONTRL Information	
Generate CONTRL	Choose when you want CONTRL messages to be generated:
	• Never—Never generate CONTRL messages.
	• Always—For CONTRL messages in all cases.
	• On Errors Only—For CONTRL messages only when errors occur.
	Warning: If you select **Always** or **On Errors Only**, ECXpert automatically creates a reverse partnership to support the CONTRL message, but you must edit that partnership so that CONTRL message can be received successfully. See "Reverse Partnerships for EDIFACT CONTRL Messages" on page 353 for instructions.
Response Level	**Message**—For message/package response CONTRL messages.

2. Continue with the next tab.

Click Next. Based on the tab that appears next, continue with these instructions at the location listed below:

Tab	Continue with...
Output EDI	"Working with the Output EDI Tab" on page 296
Protocols	"Working with the Protocols Tab" on page 314

Working with the Input HREC Tab

1. Display the Input HREC tab.

NOTE	The Input HREC tab appears only when Partnership Type on the Partnership Info tab is Application to EDI.
	To display the Input HREC tab, click Next from the previous tab. The Input HREC tab (Figure 6-11) is displayed.

Figure 6-11 shows the Input HREC tab as it looks when you are adding a new partnership. If you are changing or copying a partnership, the Standard field might already be set to EDIFACT and the Group Level Information section appears as shown in Figure 6-12 on page 295.

Figure 6-11   Input HREC tab

2.   Specify the Interchange Level Information on the Input HREC tab.

Make selections for the Interchange Level Information items. These are described in Table 6-13 on page 293.

Table 6-13 Interchange Level Information on the Input HREC tab

Item	Description
Sender Qualifier ID	The Sender Qualifier ID. The options available in the drop-down list are the trading address(es) on file for the member specified as the Sending Member in the Partnership Information tab (see "Working with the Partnership Info Tab" on page 266). *Caution:* If the only option listed is *NONE* , the member has no trading address on file. Proceed directly to the Membership tabs (see "Displaying Information for an Existing Member" on page 205) and enter a trading address for this member. You cannot save the partnership data without specifying a trading address for each member.
Receiver Qualifier ID	The Receiver Qualifier ID. The options available in the drop-down list are the trading address(es) on file for the member specified as the Sending Member in the Partnership Information tab (see "Working with the Partnership Info Tab" on page 266). *Caution:* If the only option listed is *NONE* , the member has no trading address on file. Proceed directly to the Membership tabs (see "Displaying Information for an Existing Member" on page 205) and enter a trading address for this member. You cannot save the partnership data without specifying a trading address for each member.
Standard	Select one of the following: • ANSI—The ANSI (American National Standards Institute) ASC (Accredited Standards Committee) X12 standard for EDI, widely used in North America. • EDIFACT—Electronic Data Interchange For Administration, Commerce, and Transportation, widely used internationally. ISO 9735 defines the syntax rules.

3. Continue with EDI standard-dependent information.

Your selection for Standard determines what information is displayed on the rest of the tab. Based on your selection, continue with these instructions at the location listed below:

Standard	Continue with...
ANSI	"Specifying ANSI Standard-dependent Settings" on page 294
EDIFACT	"Specifying EDIFACT Standard-dependent Settings" on page 295

Specifying ANSI Standard-dependent Settings

1. Display the Group Level Information settings for ANSI.

Set **Standard** to **ANSI** (default). The Input HREC tab looks like Figure 6-11.

2. Specify Group Level Information settings.

Refer to Table 6-14 for details.

Table 6-14   Information under Group Level Information (ANSI)

Item	Description
Application Sender (GS02)	Application sender's identification.
Application Receiver (GS03)	Application recipient's identification.
Functional ID Code (GS01)	Functional group type. For example, an 850 would have "PO" here, and an 810 would have "IN" here.
Group Version (GS08)	The message version number.

3. Display the next tab.

After specifying all the settings for the Input HREC tab, click Next. Continue with "Working with the Output EDI Tab" on page 296.

Specifying EDIFACT Standard-dependent Settings

1. Display the Group Level Information settings for EDIFACT.

Set **Standard** to **EDIFACT**. The Input HREC tab looks like Figure 6-12.

Figure 6-12   Input HREC tab, EDIFACT selected

2. Specify Group Level Information settings.

Refer to Table 6-15 for details.

Table 6-15   Information under Group Level Information (EDIFACT)

Item	Description
App Sender ID (UNG-S006-0040)	Application sender's identification code.
Message Version **(UNG-S008-0052)**	The EDIFACT message version number.
Appl Sender ID Qualifier (UNG-S006-0007)	Application sender's identification code qualifier.
Message Release (UNG-S006-0054)	The EDIFACT message release number.
App Receiver ID (UNG-S007-0040)	Application receiver's identification code.
App Receiver ID Qual (UNG-S007-0007)	Application receiver's identification code qualifier.

3. Display the next tab.

After specifying all the settings for the Input HREC tab, click Next. Continue with "Working with the Output EDI Tab" below.

Working with the Output EDI Tab

1. Display the Output EDI tab.

NOTE	The Output EDI tab appears only when Partnership Type on the Partnership Info tab is Application to EDI or EDI to EDI.
	To display the Output EDI tab, click Next from the previous tab. The Output EDI tab is displayed.
	If you are creating a new partnership, the Output EDI tab looks like Figure 6-13. If you are working with an existing partnership, the tab might look different.

Figure 6-13 Output EDI tab
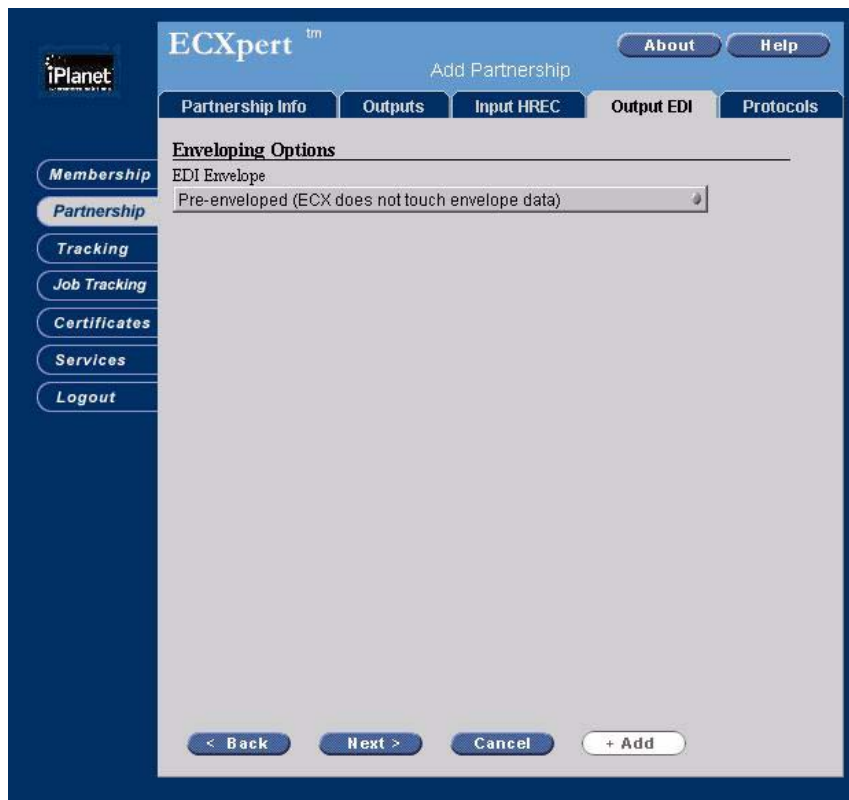
2. Specify the Envelope option on the Output EDI tab.

The fields that appear below the selected envelope option will vary depending upon the option selected. The list of available EDI envelope options, along with the two key field settings are described in Table 6-16.

Table 6-16   Key field settings and field descriptions on the Output EDI tab

Item	Description
Enveloping Options	
EDI Envelope	This option lets you specify which portions of the EDI enveloping produced by your map should be replaced by ECXpert and which portions should be left as is. Your options are:
	• **Pre-Enveloped (ECX does not touch envelope data)**—if you want ECXpert to leave all existing enveloping as is; no other fields are displayed (this is the default)
	The next three options also call up the Standard field, described below.
	• ECX Generates (or overrides) entire envelope—if you want ECXpert to override all existing enveloping
	• Use optional elements and Ctrl/Msg Ref# from data—if you want ECXpert to preserve the optional elements and control or message reference numbers produced by your map, but replace the rest of the enveloping
	• Use optional elements from data but ECX generates Ctrl/Msg Ref#—if you want ECXpert to preserve the optional elements from the data, but replace the control or message reference numbers and the rest of the envelope
Standard (does not appear when EDI Envelope is set to Pre-enveloped)	Select one of the following: • ANSI—The ANSI (American National Standards Institute) ASC (Accredited Standards Committee) X12 standard for EDI, widely used in North America. • EDIFACT—Electronic Data Interchange For Administration, Commerce, and Transportation, widely used internationally. ISO 9735 defines the syntax rules.

Select an EDI Envelope option from the drop-down list.

If Standard is displayed, select either ANSI or EDIFACT.

NOTE	If you select any option for EDI Envelope other than Pre-Enveloped... (the default), the additional fields displayed on the Output EDI tab shown in Figure 6-13 vary. For all EDI Envelope options except Pre-Enveloped..., your selection for the Standard also determines what appears on the rest of the tab.

Based on your selections for EDI Envelope and Standard, continue with these instructions at the location listed below:

EDI Envelope	Standard	Continue with...
Pre-Enveloped (ECX does not touch envelope data)	N/A	"Saving Your Work" on page 351—there are no additional selections to make on the Output EDI tab when the EDI Envelope selection is Pre-Enveloped...
ECX Generates (or overrides) entire envelope	ANSI	"Specifying Settings for ECX Generating Entire Envelope (ANSI)" on page 300
ECX Generates (or overrides) entire envelope	EDIFACT	"Specifying Settings for ECX Generating Entire Envelope (EDIFACT)" on page 302
Use optional elements and Ctrl/Msg Ref# from data	ANSI	"Specifying Settings for Using Optional Elements from Data (ANSI)" on page 305
Use optional elements and Ctrl/Msg Ref# from data	EDIFACT	"Specifying Settings for Using Optional Elements from Data (EDIFACT)" on page 308
Use optional elements from data but ECX generates Ctrl/Msg Ref#	ANSI	"Specifying Settings for ECX Generating Control Numbers (ANSI)" on page 309

EDI Envelope	Standard	Continue with...
Use optional elements from data but ECX generates Ctrl/Msg Ref#	EDIFACT	"Specifying Settings for ECX Generating Control Numbers (EDIFACT)" on page 311

Specifying Settings for ECX Generating Entire Envelope (ANSI)

If you set the **EDI Envelope** option to **ECX Generates (or overrides) entire envelope** and Standard is set to ANSI (default), the Output EDI tab looks like Figure 6-14.

Figure 6-14 Output EDI tab, ECX Generates entire envelope/ANSI selected

Table 6-17 Output EDI tab, ECX Generates entire envelope/ANSI selected

Item	Description
Enveloping Options	
EDI Envelope and **Standard**	Setting **EDI Envelope** to ECX Generates Envelopes and Standard to ANSI makes the rest of the tab look this way.
Version Information	
Interchange Version (ISA 12)	The interchange version number. This field is optional.
Generate Control Numbers Starting With	
Interchange	Starting number to use for generating interchange control numbers. *Default:* the interchange control number last used by this partnership, incremented by 1
Group	Starting number to use for generating group control numbers. *Default:* the group control number last used by this partnership, incremented by 1
Document	Starting number to use for generating document control numbers. *Default:* the document control number last used by this partnership, incremented by 1
FA Information	
FA (997) Expected	Check if functional acknowledgment (997) is expected.
FA overdue in (minutes)	Number of minutes after which the functional acknowledgment should be flagged as overdue.
Delimiters and Separators	
Segment Terminator (hex value)	Enter the segment terminator character value in hexadecimal notation. *Default:* 0D0A
Test or Production	Select one: • PRODUCTION—if this is production data • TEST—if this is test data

Table 6-17   Output EDI tab, ECX Generates entire envelope/ANSI selected

Item	Description
Sub-Element Delimiter (hex value)	Enter the sub-element delimiter character value in hexadecimal notation.
	Default: 3E
Element Delimiter (hex value)	Enter the element delimiter character value in hexadecimal notation.
	Default: 2A

Specify the rest of the settings for Output EDI tab for Standard set to ANSI, then continue with "Working with the Protocols Tab" on page 314.

Specifying Settings for ECX Generating Entire Envelope (EDIFACT)

If you set the **EDI Envelope** option to **ECX Generates (or overrides) entire envelope** and then set Standard to EDIFACT, the Output EDI tab looks like Figure 6-15.

Figure 6-15   Output EDI tab, ECX Generates entire envelope/EDIFACT selected

Table 6-18   Output EDI tab, ECX Generates Envelopes/EDIFACT selected

Item	Description
Enveloping Options	
EDI Envelope and **Standard**	Setting **EDI Envelope** to ECX Generates Envelopes and Standard to EDIFACT makes the rest of the tab look this way.
Version Information	
Version Number (UNH-S009-0052)	The EDIFACT version number.
Release Number (UNH-S009-0054)	The EDIFACT release number.
Generate Message Reference Numbers Starting With	

Table 6-18 Output EDI tab, ECX Generates Envelopes/EDIFACT selected *(Continued)*

Item	Description
Interchange	Starting number to use for generating interchange reference numbers. *Default:* the interchange message reference number last used by this partnership, incremented by 1
Group	Starting number to use for generating group reference numbers. *Default:* the group message reference number last used by this partnership, incremented by 1
Document	Starting number to use for generating document reference numbers. *Default:* the document message reference number last used by this partnership, incremented by 1
CONTRL Information	
CONTRL Message Expected	Check if a CONTRL message is expected.
CONTRL overdue in (minutes)	Number of minutes after which the CONTRL message should be flagged as overdue.
Delimiters and Separators	
Segment Terminator (hex value)	Enter the segment terminator character value in hexadecimal notation. *Default:* 27
Decimal Notation (hex value)	Enter the release character value in hexadecimal notation. *Default:* 3F
Release Character (hex value)	Enter the decimal character value in hexadecimal notation. *Default:* 2E
Element Delimiter (hex value)	Enter the element delimiter character value in hexadecimal notation. *Default:* 2B
Sub-Element Delimiter (hex value)	Enter the sub-element delimiter character value in hexadecimal notation. *Default:* 3A
Test or Production	Select one: • PRODUCTION—if this is production data • TEST—if this is test data

Table 6-18   Output EDI tab, ECX Generates Envelopes/EDIFACT selected *(Continued)*

Item	Description
Generate UNA	Check if you want to generate the optional UNA segment from the information supplied above.
	Default: 3F

Specify the rest of the settings for Output EDI tab for Standard set to EDIFACT, then continue with .

Specifying Settings for Using Optional Elements from Data (ANSI)

If you set the **EDI Envelope** option to **Use optional elements and Ctrl/Msg Ref# from data** and Standard is set to ANSI (default), the Output EDI tab looks like .

Figure 6-16   Output EDI tab, Use optional elements from data/ANSI selected

Table 6-19 Output EDI tab, Preserve Control Numbers/ANSI selected

Item	Description
Enveloping Options	
EDI Envelope and **Standard**	Setting **EDI Envelope** to ECX Generates Envelopes and Standard to ANSI makes the rest of the tab look this way.
Enveloping Options	
Interchange Version (ISA 12)	Interchange version. This field is optional.
Version Information	
Segment Terminator (hex value)	Enter the segment terminator character value in hexadecimal notation. *Default:* `0D0A`
Test or Production	Select one: • PRODUCTION—if this is production data • TEST—if this is test data
Sub-Element Delimiter (hex value)	Enter the sub-element delimiter character value in hexadecimal notation. *Default:* `3E`
Element Delimiter (hex value)	Enter the element delimiter character value in hexadecimal notation. *Default:* `2A`

Specify the rest of the settings for Output EDI tab for Standard set to ANSI, then continue with .

Specifying Settings for Using Optional Elements from Data (EDIFACT)

If you set the **EDI Envelope** option to **Use optional elements and Ctrl/Msg Ref# from data** and then set Standard to EDIFACT, the Output EDI tab looks like Figure 6-17.

Figure 6-17 Output EDI tab, Use optional elements from data/EDIFACT selected

Table 6-20   Output EDI tab, Preserve Control Numbers/EDIFACT selected

Item	Description
Enveloping Options	
EDI Envelope and **Standard**	Setting **EDI Envelope** to ECX Generates Envelopes and Standard to EDIFACT makes the rest of the tab look this way.
Version Information	
Version Number (UNH-S009-0052)	The EDIFACT version number.
Release Number (UNH-S009-0054)	The EDIFACT release number.
Delimiters and Separators	
Segment Terminator (hex value)	Enter the segment terminator character value in hexadecimal notation. *Default:* 27
Decimal Notation (hex value)	Enter the decimal character value in hexadecimal notation. *Default:* 2E
Release Character (hex value)	Enter the release character value in hexadecimal notation. *Default:* 3F
Element Delimiter (hex value)	Enter the element delimiter character value in hexadecimal notation. *Default:* 2B
Sub-Element Delimiter (hex value)	Enter the sub-element delimiter character value in hexadecimal notation. *Default:* 3A

Specify the rest of the settings for Output EDI tab for Standard set to EDIFACT, then continue with "Working with the Protocols Tab" on page 314.

Specifying Settings for ECX Generating Control Numbers (ANSI)

If you set the **EDI Envelope** option to **Use optional elements from data but ECX generates Ctrl/Msg Ref#** and Standard to ANSI, the Output EDI tab looks like Figure 6-18.

Figure 6-18   Output EDI tab, ...ECX generates Ctrl/Msg Ref#/ANSI selected

Table 6-21   Output EDI tab, ECX Generates Control Numbers/ANSI selected

Item	Description
Enveloping Options	
EDI Envelope and **Standard**	Setting **EDI Envelope** to Use optional elements from data but ECX Generates Ctrl/Msg Ref#, and Standard to ANSI, makes the rest of the tab look this way.
Generate Control Numbers Starting With	
Interchange	Starting number to use to generate interchange control numbers. *Default:* the interchange control number last used by this partnership, incremented by 1

Table 6-21   Output EDI tab, ECX Generates Control Numbers/ANSI selected

Item	Description
Group	Starting number to use to generate group control numbers. *Default:* the group control number last used by this partnership, incremented by 1
Document	Starting number to use to generate document control numbers. *Default:* the document control number last used by this partnership, incremented by 1
FA Information	
FA (997) Expected	Check if functional acknowledgment (997) is expected.
FA overdue in (minutes)	Number of minutes after which the functional acknowledgment should be flagged as overdue.
Delimiters and Separators	
Segment Terminator (hex value)	Enter the segment terminator character value in hexadecimal notation. *Default:* 0D0A
Test or Production	Select one: • PRODUCTION—if this is production data • TEST—if this is test data
Sub-Element Delimiter (hex value)	Enter the sub-element delimiter character value in hexadecimal notation. *Default:* 3E
Element Delimiter (hex value)	Enter the element delimiter character value in hexadecimal notation. *Default:* 2A

Specify the rest of the settings for Output EDI tab for Standard set to ANSI, then continue with

Specifying Settings for ECX Generating Control Numbers (EDIFACT)

If you set the **EDI Envelope** option to **Use optional elements from data but ECX generates Ctrl/Msg Ref#** and then set Standard to EDIFACT, the Output EDI tab looks like Figure 6-19.

Figure 6-19   Output EDI tab, ...ECX generates Ctrl/Msg Ref#/EDIFACT selected

Table 6-22   Output EDI tab, ECX Generates Control Numbers/EDIFACT selected

Item	Description
Enveloping Options	
EDI Envelope and **Standard**	Setting **EDI Envelope** to Use optional elements from data but ECX Generates Ctrl/Msg Ref#, and Standard to EDIFACT, makes the rest of the tab look this way.
Generate Message Reference Numbers Starting With	
Interchange	Starting number to use for generating interchange reference numbers. *Default:* the interchange message reference number last used by this partnership, incremented by 1

Table 6-22   Output EDI tab, ECX Generates Control Numbers/EDIFACT selected

Item	Description
Group	Starting number to use for generating group reference numbers. *Default:* the group message reference number last used by this partnership, incremented by 1
Document	Starting number to use for generating document reference numbers. *Default:* the document message reference number last used by this partnership, incremented by 1
Generate UNG	Check if you want to generate UNG. Check if you want to generate the optional UNG segment from the information supplied above.
CONTRL Information	
CONTRL Message Expected	Check if CONTRL message is expected.
CONTRL overdue in (minutes)	Number of minutes after which the CONTRL message should be flagged as overdue.
Delimiters and Separators	
Segment Terminator (hex value)	Enter the segment terminator character value in hexadecimal notation. *Default:* 27
Decimal Notation (hex value)	Enter the decimal character value in hexadecimal notation. *Default:* 2E
Release Character (hex value)	Enter the release character value in hexadecimal notation. *Default:* 3F
Element Delimiter (hex value)	Enter the element delimiter character value in hexadecimal notation. *Default:* 2B
Sub-Element Delimiter (hex value)	Enter the sub-element delimiter character value in hexadecimal notation. *Default:* 3A

Specify the rest of the settings for Output EDI tab for Standard set to EDIFACT, then continue with

Working with the Protocols Tab

1. Display the Protocols tab.

   Click Next from the previous tab. The Protocols tab is displayed. If you are creating a new partnership, the Protocols tab looks like Figure 6-20. If you are working with an existing partnership, the tab might look different.

2. Select an outgoing protocol.

   Select an **Outgoing Protocol** from the drop-down list. Refer to Figure 6-20 on page 314 and Table 6-23 on page 315 for details.

Figure 6-20　Protocols tab, POLL selected
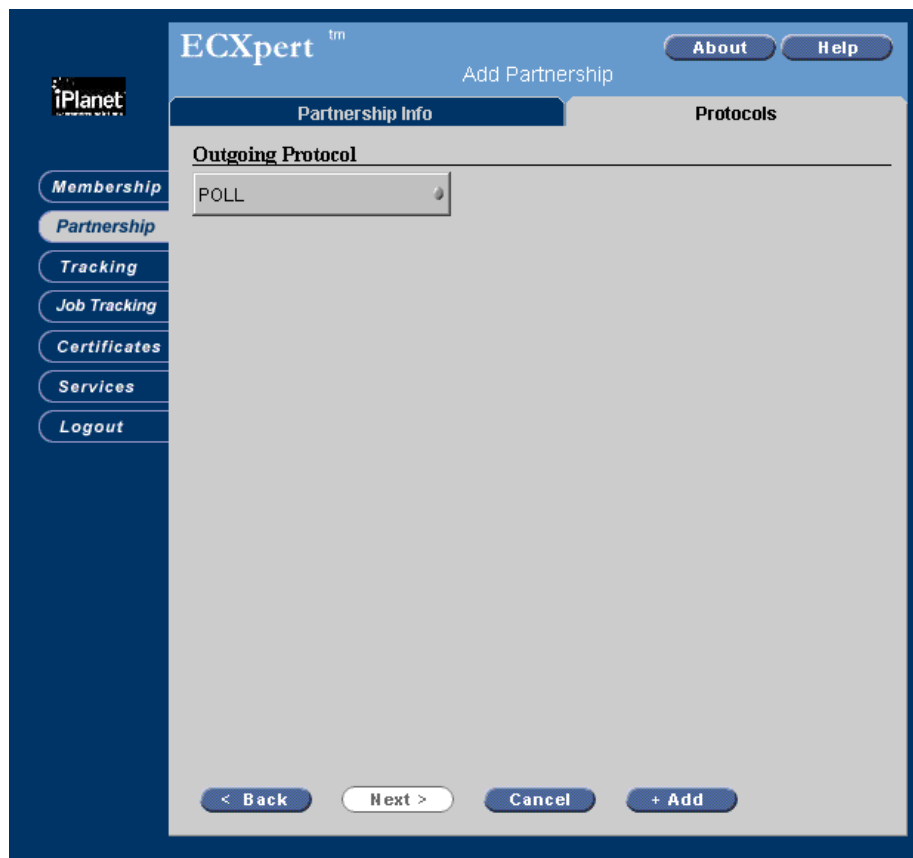
Table 6-23 Protocols tab. Outgoing Protocol Options

Outgoing Protocol	Description	After selecting, continue with instructions at...
POLL	No active protocol (default). Used when an external process will be pulling data from the ECXpert mailbox using the ECXpert poll utility. For more information on the poll utility, see Chapter 11, "Command Line Utilities."	"Saving Your Work" on page 351—there are no additional selections to make on the Protocols tab when the Outgoing Protocol is POLL
HTTP Receive	Files should be stored without processing to be picked up and processed.	"Specifying Settings for HTTP Receive" on page 316
JMS Send	To send JMS messages to a partner by way of a JMS message service.	"Specifying Settings for JMS Send" on page 343
Legacy Server (SAP)	To exchange documents between ECXpert and SAP.	"Specifying Settings for Legacy Server (SAP)" on page 345
Legacy Server (MQ Series)	To exchange documents between ECXpert and MQSeries.	"Specifying Settings for Legacy Server (MQ Series)" on page 347
SMTP	Simple Mail Transfer Protocol using MIME or S/MIME.	"Specifying Settings for SMTP" on page 320
FTP	File Transfer Protocol.	"Specifying Settings for FTP" on page 323
GEIS FTP	GE Information Services' EDI*EXPRESS Service FTP access.	"Specifying Settings for GEIS FTP" on page 325
Odette FTP (OFTP)	FTP developed by the Organisation for Data Exchange by Tele Transmission (Odette) for the European auto industry.	"Specifying Settings for Odette FTP (OFTP)" on page 328
HTTP for AIAG	HTTP using the automotive industry standard.	"Specifying Settings for HTTP for AIAG" on page 336
HTTP for GISB	HTTP using the North American natural gas industry standard. *Note:* This protocol is for sending only, not for receiving.	"Specifying Settings for HTTP for GISB" on page 340
HTTP SSL for OBI	HTTP with Secure Sockets Layer security for OBI documents.	"Specifying Settings for HTTP SSL for OBI" on page 332
HTTP SSL for XML	HTTP with Secure Sockets Layer security for XML documents.	"Specifying Settings for HTTP SSL for XML" on page 334
eXML Connector	To use the ECXpert XML connector. See the *iPlanet ECXpert Developer's Guide* for setup details.	"Specifying Settings for eXML Connector" on page 318

Table 6-23   Protocols tab. Outgoing Protocol Options *(Continued)*

Outgoing Protocol	Description	After selecting, continue with instructions at...
User Defined	To use other protocols defined for your site by your site administrator.	"Specifying Settings for User Defined" on page 349

3. Specify the rest of the protocol options.

   If you select any option other than POLL (the default), the details on the Protocols tab change. Based on your selection, continue with these instructions at the location listed in Table 6-23 on page 315.

Specifying Settings for HTTP Receive

If you select **HTTP Receive** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-21.

Figure 6-21   Protocols tab, HTTP Receive selected
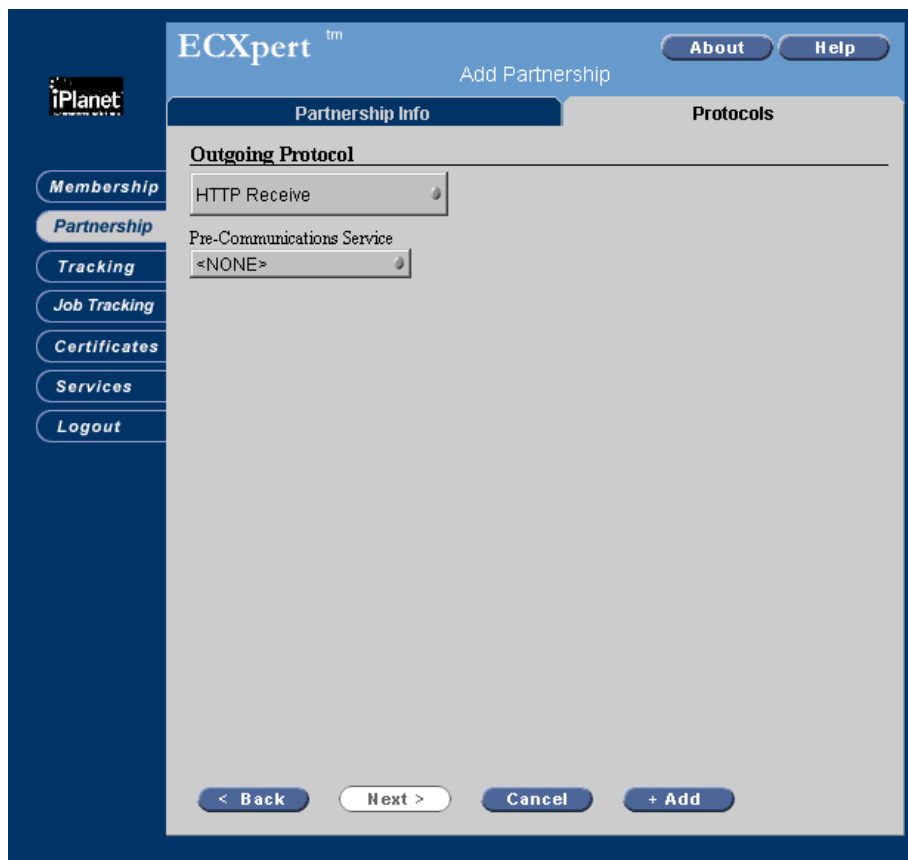
Table 6-24   Protocols tab, HTTP Receive selected
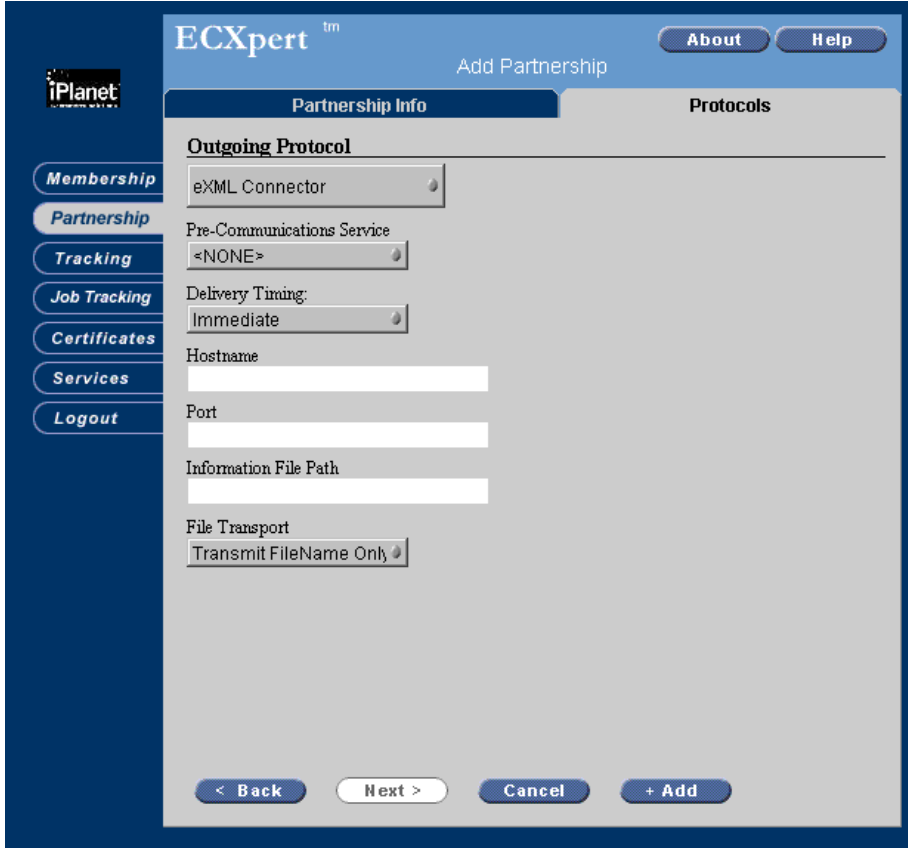
Item	Description
Outgoing Protocol	Selecting **HTTP Receive** caused the tab to look like that in Figure 6-21.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.

Select a Pre-Communications Service for HTTP Receive, or *NONE* , then continue with "Saving Your Work" on page 351.

Specifying Settings for eXML Connector

If you select **eXML Connector** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-22.

Figure 6-22   Protocols tab, eXML Connector selected

Table 6-25   Protocols tab, eXML Connector selected

Item	Description
Outgoing Protocol	Selecting **eXML Connector** caused the tab to look like that in Figure 6-22.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Hostname	The destination IP address.
Port	The destination port number.
Information File Path	The full path to the eXML Connector information file.
File Transport	Select: • **Transmit File Name Only**—to transmit only the file name. • **Transmit Entire File**—to transmit the file contents along with the file name

Fill in the rest of the options for eXML Connector, then continue with "Saving Your Work" on page 351.

Specifying Settings for SMTP

If you select **SMTP** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-23.

Figure 6-23   Protocols tab, SMTP selected

Table 6-26   Information on the Protocols tab, SMTP selected

Item	Description
Outgoing Protocol	Selecting **SMTP** caused the tab to look like that in Figure 6-23.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Parameters	
Delivery Timing	Select:
	• **Immediate**—to send all messages as soon as they are ready to be sent.
	• **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
MDN Requested	Select one of the following for Message Disposition Notification (MDN):
	• **No MDN** - no MDN requested
	• **Plain MDN** - unsigned MDN requested (default)
	• **Signed MDN** - signed MDN requested
	MDN is a newer Internet standard for signed receipt notice and non-repudiation of receipt functions.
MIME Sub-Type Override (optional)	Enter the MIME type to use. This field is only available if you selected non-EDI on the Partnership Information Tab. If you select EDI, the Internet EDI Work Group Standard default values are used. The default values are:
	• **EDI-X12** for ANSI EDI data
	• **EDIFACT** for EDIFACT EDI data
	• **application** for non-EDI data. You can change this to the specific application data type. For example, `msexcel` to identify Microsoft Excel format data.

Table 6-26 Information on the Protocols tab, SMTP selected *(Continued)*

Item	Description
Process Method	One of these methods of sending data: • **Not Signed or Encrypted**—Sends data in plain text (MIME), and provides no security or authentication. • **Encrypted Only**—Encrypts data, but provides no authentication. • **Signed Only**—Authenticates the sender of a document, but provides no security. • **Signed and Encrypted**—Authenticates the sender of a document and encrypts the data. Use for confidental data when authentication is also required.

Specify the rest of the protocol information for SMTP, then continue with
"Saving Your Work" on page 351.

Specifying Settings for FTP

If you select **FTP** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-24.

Figure 6-24   Protocols tab, FTP selected

Table 6-27 Information on the Protocols tab, FTP selected

Item	Description
Outgoing Protocol	Selecting **FTP** caused the tab to look like that in Figure 6-24.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select:
	• **Immediate**—to send all messages as soon as they are ready to be sent.
	• **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Host Name	The host name of the FTP server.
Port	The IR port number for the FTP server.
User Name	The FTP user ID for the member.
Account	The FTP account ID, if one is required in addition to the **User Name**.
Password	The FTP password for the member's User Name.
Confirm Password	Enter the password again to confirm.
Outbound Transfer Mode	Select BINARY or ASCII. In general, you should use BINARY mode. Use ASCII mode if you want to send text information to an MVS system and have it converted to *EBCDIC* format.
Outbound Dir	A fully qualified pathname for the directory where ECXpert is to place outbound documents (ftp put). The User Name specified above must have write permission for this directory.
Outbound Pattern	A pattern (any set of characters) that ECXpert is to add to the filename when placing it in the Outbound directory.
Inbound Dir	A fully qualified pathname for the directory from which ECXpert will retrieve inbound documents. (ftp get)

Table 6-27   Information on the Protocols tab, FTP selected *(Continued)*

Item	Description
Inbound Pattern	A pattern (any set of characters) to search for in the Inbound Dir. Files matching the pattern are retrieved into ECX; other files are left in the directory. If you leave the field blank, no files are retrieved. You can use any wildcard supported by FTP (like *, for example PO.*) to pick up multiple files.
Inbound File Type	The file type of inbound files. This must match the data type (document type) specified in the Service List.

NT Users: In the NT version of ECXpert, file names used in FTP operations are case sensitive.

Specify the rest of the protocol information for FTP, then continue with "Saving Your Work" on page 351.

Specifying Settings for GEIS FTP

If you select **GEIS FTP** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-25.

Figure 6-25   Protocols tab, GEIS FTP selected

Table 6-28   Information on the Protocols tab, GEIS FTP selected

Item	Description
Outgoing Protocol	Selecting **GEIS FTP** caused the tab to look like that in Figure 6-25.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.

Table 6-28   Information on the Protocols tab, GEIS FTP selected *(Continued)*

Item	Description
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Operation	Select one of the following: • **Send and Receive**—To allow both sending and receiving (default). • **Send Only**—To allow sending only. • **Receive Only**—To allow receiving only.
Host Name	The host name of the GEIS FTP server.
Port	The IR port number for the GEIS FTP server.
User Name	The GEIS EDI*EXPRESS Service User Number or account ID for the member.
Password	The GEIS EDI*EXPRESS Service password for the member's user number.
Confirm Password	Enter the password again to confirm.

NOTE	You must set up GEIS as a *trusted member* before members can use GEIS FTP. For more information, see "Working with the Membership Definition Tabs" on page 207 and "Controlling User Access to ECXpert" on page 198.

NT Users: In the NT version of ECXpert, file names used in FTP operations are case sensitive.

Specify the rest of the protocol information for GEIS FTP, then continue with "Saving Your Work" on page 351.

Specifying Settings for Odette FTP (OFTP)

If you select **Odette FTP (OFTP)** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-26.

Figure 6-26 Protocols tab, Odette FTP (FTP) selected

Table 6-29 Information on the Protocols tab, Odette FTP (OFTP) selected

Item	Description
Outgoing Protocol	Selecting **Odette FTP (OFTP)** caused the tab to look like that in Figure 6-26.

Table 6-29 Information on the Protocols tab, Odette FTP (OFTP) selected *(Continued)*

Item	Description
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Username	The OFTP server user ID for the member.
Password	The OFTP server password for the member's Username.
Confirm Password	Enter the password again to confirm.
Transport Method	Select: • **X.25**—to use X.25 transport • **X.28**—to use X.28 transport • **TCP/IP**—to use TCP/IP transport

Specify the above protocol information for Odette FTP (OFTP). The information required to complete the tab depends on the **Transport Method** that you select:

Transport Method	After selecting, continue with instructions at...
X.25	Table 6-30 on page 330
X.28	Table 6-31 on page 331
TCP/IP	Table 6-32 on page 331

Table 6-30 OFTP Information for X.25 Transport Method

Item	Description
Destination X.121 Address	The X.121 standard specification of the X.25 address of the destination OFTP node. Typically a string of up to 16 digits. If left blank, defaults to local X.121 address.
Facility Information	Information on X.25 node facilities, specified using hex codes, allowing connecting X.25 client to enable the facilities.
Logical Channel Number	If the receiving OFTP node is configured with a pre-assigned port (logical channel) number, also referred to as a permanent virtual circuit configuration (PVC), then you must specify the port (logical channel) number here in addition to the **Destination X.121 Address**. If the receiving OFTP node is configured to dynamically assign a port (logical channel) number, also referred to as a switched virtual circuit configuration (SVC), then you can leave this blank.
Routing Entry	Routing table entry for X.25 implementations that route incoming connection attempts based on a routing table. Not used under Solaris, NT, or HPUX.
Call User Data	If X.25 application is set up to listen for connections that have specified call user data, enter the hex code here.

When you have completed filling in the specific information for the **Transport Method** you selected, continue with .

Table 6-31   OFTP Information for X.28 Transport Method

Item	Description
Telephone Number	Telephone number for X.28 dial-up connection.
PAD Password	Password (case-sensitive) for PAD program receiving X.28 dial-up connection.
Connection Script	Full path name of connection script to use. Required.
Confirm PAD Password	Re-enter **PAD Password** to confirm. The two password entries must match exactly.
PAD Username	Username for PAD program receiving X.28 dial-up connection.
Destination X.121 Address	Network user address of the destination.

When you have completed filling in the specific information for the **Transport Method** you selected, continue with .

Table 6-32   OFTP Information for TCP/IP Transport Method

Item	Description
Destination Address	The TCP/IP host address of the remote OFTP receiver node. Can be either the IP address or the hostname. If left blank, defaults to local IP address.
Destination Port	The TCP/IP port number that the receiver OFTP process is listening on. Can be either the port number or the port name. If left blank, defaults to OFTP standard port 3305.

When you have completed filling in the specific information for the **Transport Method** you selected, continue with .

Specifying Settings for HTTP SSL for OBI

If you select **HTTP SSL for OBI** as the **Outgoing Protocol**, the Protocols tab appears as shown in Figure 6-27.

Figure 6-27   Protocols tab, HTTP SSL for OBI selected

Specify the rest of the protocol information for HTTP SSL for OBI, then continue with "Saving Your Work" on page 351.

Table 6-33   Information on the Protocols tab, HTTP SSL for OBI selected

Item	Description
Outgoing Protocol	Selecting **HTTP SSL for OBI** causes the tab to look like that in Figure 6-27.

Table 6-33   Information on the Protocols tab, HTTP SSL for OBI selected *(Continued)*

Item	Description
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Host Name	The host name of the HTTP SSL for OBI server.
Port	The IR port number for the HTTP SSLfor OBI server.
CGI Path	The CGI path used by the HTTP SSL for OBI server.
Sender	The HTTP SSL for OBI server user ID for the sending member.
File Type	The Document Type being exchanged.
Sender Certificate Type	Select one of the following: • None—(default) if no certificate is used • Self-Signed Certificate—if a self-signed certificate is used • New VeriSign Class 3—if a new VeriSign class 3 certificate is used • VeriSign Class 1—if a VeriSign class 1 certificate is used • VeriSign Class 2—if a VeriSign class 2 certificate is used

Specifying Settings for HTTP SSL for XML

If you select **HTTP SSL for XML** as the **Outgoing Protocol**, the Protocols tab appears as shown in Figure 6-28.

Figure 6-28   Protocols tab, HTTP SSL for XML selected

Specify the rest of the protocol information for HTTP SSL for XML, then continue with "Saving Your Work" on page 351.

Table 6-34   Information on the Protocols tab, HTTP SSL for XML selected

Item	Description
Outgoing Protocol	Selecting **HTTP SSL for XML** caused the tab to look like that in Figure 6-28. XML documents can be sent and received through ECXpert using this protocol provided any incoming XML document includes information about which XSL stylesheet to use, to allow Parse to receive the necessary document information to proceed with submitting the docs.
	The stylesheet name can be found in the following sequence.
	1. provide stylesheet name as ecx-stylesheet processing instruction in xml data file.
	2. provide DTD name in xml data file, so that `ecxstylesheets.xml ini` file can find mapping between the DTD name & stylesheet name.
	3. provide stylesheet name using external shared library(plugin).
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select:
	• **Immediate**—to send all messages as soon as they are ready to be sent.
	• **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Host Name	The host name of the HTTP SSL for XML server.
Port	The IR port number for the HTTP SSL for XML server.
CGI Path	The CGI path used by the HTTP SSL for XML server.
Sender	The HTTP SSL for XML server user ID for the sending member.

Table 6-34   Information on the Protocols tab, HTTP SSL for XML selected *(Continued)*

Item	Description
Receiver	The HTTP SSL for XML server user ID for the receiving member. (Optional)
File Type	The Document Type being exchanged.
Content Type	The Document content format being exchanged (noted in Figure 6-28).
Sender Certificate Type	Select one of the following: • None—(default) if no certificate is used • Self-Signed Certificate—if a self-signed certificate is used • New VeriSign Class 3—if a new VeriSign class 3 certificate is used • VeriSign Class 1—if a VeriSign class 1 certificate is used • VeriSign Class 2—if a VeriSign class 2 certificate is used

Specifying Settings for HTTP for AIAG

If you select **HTTP for AIAG** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-29.

CAUTION   Currently, sending binary files in excess of 1 megabyte to ECXpert are not recommended and can cause the system to fail (without an error message conveyed to the user) due to an inherent binary file size limitation in the iPlanet Web Server. ASCII files can be sized to 5 megabytes processed through ECXpert without any problems.

Figure 6-29   Protocols tab, HTTP for AIAG selected

Table 6-35   Information on the Protocols tab, HTTP for AIAG selected

Item	Description
Outgoing Protocol	Selecting **HTTP for AIAG** caused the tab to look like this.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Parameters	

Table 6-35 Information on the Protocols tab, HTTP for AIAG selected *(Continued)*

Item	Description
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
User Name	The user name to use to log in to the HTTP AIAG server. This user must be set up on both sides of the trading partnership with **Member is Trusted** selected in ECXpert on the Membership Information tab. (See "Working with the Membership Definition Tabs" on page 207.)
Sender	The member ID of the sending member in the partnership. This must be set up on the local machine and on the remote HTTP server.
User Parameter	Optional field used to further identify the user to the AIAG server according to site implementation criteria.
Password	The password for User Name to use to log in to the HTTP server.
Receiver	The member ID of the receiving member in the partnership. This must be set up on the local machine and on the remote HTTP server.
Reference Number	An agreed-upon number embedded into documents to verify their authenticity.
Confirm Password	Enter the password again to confirm it.
Application	The type of document to by transferred via this protocol. For example, EDI. *Note:* There must be a trading partnership on both the remote and local machines set up with the same **Sender**, **Receiver**, and **Document Type** (Application).
URIs	Uniform Resource Identifers
API Definition URI	The full path identifier to the
Login URI (including filename)	The full path identifier to the login page for the AIAG Server. *Example:* `http://trading_partnerA.com/login.html`

Table 6-35 Information on the Protocols tab, HTTP for AIAG selected *(Continued)*

Item	Description
Deliver URI (including filename)	The full path identifier to the deliver page for the AIAG Server.
	Example: `http://trading_partnerA.com/deliver.html`
Obtain URI (including filename)	The full path identifier to the obtain page for the AIAG Server.
	Example: `http://trading_partnerA.com/obtain.html`
Acknowledge URI (including filename)	The full path identifier to the acknowledge page for the AIAG Server.
	Example: `http://trading_partnerA.com/acknowledge.html`
Loopback Test URI	The full path identifier

Specify the rest of the protocol information for HTTP for AIAG, then continue with "Saving Your Work" on page 351.

Specifying Settings for HTTP for GISB

If you select **HTTP for GISB** as the **Outgoing Protocol**, the Protocols tab, changes to look like Figure 6-30.

Figure 6-30   Protocols tab, HTTP for GISB selected

Table 6-36   Information on the Protocols tab, HTTP for GISB selected

Item	Description
Outgoing Protocol	Selecting **HTTP for GISB** caused the tab to look like that in Figure 6-30.

Table 6-36   Information on the Protocols tab, HTTP for GISB selected *(Continued)*

Item	Description
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Parameters	
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Password	The password to use to log in to the HTTP server.
Host Name	The name of the HTTP server to connect to.
Confirm Password	Enter the password again to confirm it.
Port	The IP port number of the remote HTTP server. (This field is optional.)
From	The sending member of the trading partnership. This must be set up on the local machine and on the remote HTTP server.
Operation	Select the operation to perform: • **DELIVER** to transfer documents to the HTTP server. • OBTAIN to transfer document from the HTTP server.
To	The receiver member of the trading partnership. This must be set up on the local machine and on the remote HTTP server.
User Name	The user name to use to log in to the HTTP server. This user must be set up on both sides of the trading partnership with **Member is Trusted** selected in ECXpert on the Membership Information tab. (See "Working with the Membership Definition Tabs" on page 207.)

Table 6-36 Information on the Protocols tab, HTTP for GISB selected *(Continued)*

Item	Description
Input Format	The type of document to by transferred via this protocol. For example, **EDI**. *Note:* There must be a trading partnership on both the remote and local machines set up with the same **Sender (From)**, **Receiver (To)**, and **Document Type (Input Format)**.
Deliver CGI Pathname (including filename)	The full path to the deliver CGI. *Default:* `/bin/gisb-deliver`

Specify the rest of the protocol information for HTTP for GISB, then continue with "Saving Your Work" on page 351.

Specifying Settings for JMS Send

If you select JMS Send as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-32.

Figure 6-31   Protocols tab, JMS Send selected

Table 6-37   Information on the Protocols tab, JMS Send selected

Item	Description
JNDI Properties Filename	Path to JNDI properties file that specifies values needed to perform JNDI lookup of JMS administered objects
Conn Factory	JNDI Lookup name of the QueueConnectionFactory administered object needed to establish a connection to the JMS message service
Queue	JNDI Lookup name for the queue to which messages are being sent
JMS User ID	User ID needed for authentication with the JMS message service upon establishing a connection
Password	User password needed for authentication with the JMS message service upon establishing a connection
Expiration	Specifies value (in seconds) to set for the JMSExpiration message header field. A value of zero means message lives forever
Priority	Specifies value (1 -10) to set for the JMSPriority message header field. A value of 10 is the highest priority.
Delivery Mode	Specifies value (persistent or non-persistent) to set for the JMSDeliveryMode message header field

Specify the rest of the protocol information for Legacy Server (SAP), then continue with "Saving Your Work" on page 351.

Specifying Settings for Legacy Server (SAP)

If you select Legacy Server (SAP) as the **Outgoing Protocol**, the Protocols tab
changes to look like Figure 6-32.

Figure 6-32   Protocols tab, Legacy Server (SAP) selected

Table 6-38   Information on the Protocols tab, Legacy Server (SAP) selected

Item	Description
Outgoing Protocol	Selecting **Legacy Server (SAP)** caused the tab to look like this.

Table 6-38   Information on the Protocols tab, Legacy Server (SAP) selected *(Continued)*

Item	Description
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Client Number	The client number required by the SAP system.
User ID	The user ID for logging into the SAP system.
Password	The password for User ID for logging into the SAP system.
Confirm Password	Re-enter the password here to confirm it.
RFC Section Key	The section name in the `saprfc.ini` file.

Specify the rest of the protocol information for Legacy Server (SAP), then continue with "Saving Your Work" on page 351.

Specifying Settings for Legacy Server (MQ Series)

If you select Legacy Server (MQ Series) as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-33.

Figure 6-33   Protocols tab, Legacy Server (MQ Series) selected

Table 6-39 Information on the Protocols tab, Legacy Server (MQ Series) selected

Item	Description
Outgoing Protocol	Selecting **Legacy Server (MQ Series)** caused the tab to look like this.
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
Queue Name	The name of the MQSeries queue to which you want to connect.
Queue Manager	The name of the MQSeries queue manager in charge of the queue to which you want to connect.
Message Header File	The name of the message header file to use.

Specify the rest of the protocol information for Legacy Server (MQ Series), then continue with "Saving Your Work" on page 351.

Specifying Settings for User Defined

If you select **User Defined** as the **Outgoing Protocol**, the Protocols tab changes to look like Figure 6-34.

Figure 6-34   Protocols tab, User Defined selected

Table 6-40   Information on the Protocols tab, User Defined selected

Item	Description
Outgoing Protocol	Selecting **User Defined** caused the tab to look like this.

Table 6-40 Information on the Protocols tab, User Defined selected *(Continued)*

Item	Description
Pre-Communications Service	If you want a custom, pre-communications service to be used before using this protocol, select it here. A pre-communications service can be used to perform custom encryption or compression on your data. For more information on custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.
Delivery Timing	Select: • **Immediate**—to send all messages as soon as they are ready to be sent. • **Scheduled**—to send messages at regularly specified times using the ECXpert Scheduler. For instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155.
First Parameter	First parameter to pass to the user-defined protocol. Details are specific to the user-defined protocol's design.
Second Parameter	Second parameter to pass. Details are specific to the user-defined protocol's design.
Third Parameter	Third parameter to pass to the user-defined protocol. Details are specific to the user-defined protocol's design.
Fourth Parameter	Fourth parameter to pass to the user-defined protocol. Details are specific to the user-defined protocol's design.
Fifth Parameter	Fifth parameter to pass to the user-defined protocol. Details are specific to the user-defined protocol's design.
Sixth Parameter	Sixth parameter to pass. Details are specific to the user-defined protocol's design.
Seventh Parameter	Seventh parameter to pass to the user-defined protocol. Details are specific to the user-defined protocol's design.
Eighth Parameter	Eighth parameter to pass to the user-defined protocol. Details are specific to the user-defined protocol's design.

Specify the rest of the protocol information for TradingXpert, then continue with "Saving Your Work" on page 351.

Saving Your Work

A "completion" button always appears at the bottom of the partnership definition tabs. Keep these points in mind:

- This button has the same name as the one you clicked to begin the current task: Add, Change, Copy, or Delete.

- Clicking this button completes the task.

- For Delete, this button deletes the partnership's information. For the other operations, this button saves the information you have entered and/or changed for the partnership.

- This button is only active when the Protocols tab, on the last tab in the partnership definition series, is displayed in front.

NOTE	You can click Cancel at the bottom of any tab in the partnership definition series at any time if you decide not to complete the task.

Important Note on Functional Acknowledgments and CONTRL Messages

If the partnership that you just created or changed does not specify Functional Acknowledgments (ANSI X12) or CONTRL Messages (EDIFACT), you are finished—this section does not apply to what you are doing.

When you need to edit a reverse partnership: If you have just added a new partnership, and you have requested Functional Acknowledgments (ANSI X12) or CONTRL Messages (EDIFACT), then you *might* need to edit the "reverse partnership" that ECXpert creates automatically to handle these document exchanges.

If you have changed an existing partnership so that it specifies Functional Acknowledgments (ANSI X12) or CONTRL Messages (EDIFACT), then you might also need to edit the "reverse partnership" that ECXpert creates.

Or, you might not need to edit the reverse partnership: Multiple partnerships with the same Sender and Receiver, but with different Document Types, all share the same reverse partnership; you only need to edit the reverse partnership once.

If you need to edit the reverse partnership, continue with instructions according to the EDI standard you are using:

- **ANSI**—"Reverse Partnerships for ANSI Functional Acknowledgments (FAs/997s)" on page 352

- **EDIFACT**—"Reverse Partnerships for EDIFACT CONTRL Messages" on page 353

Reverse Partnerships for ANSI Functional Acknowledgments (FAs/997s)

Main Partnership: The following steps are necessary to request FAs—if you just saved your work on a new partnership or a change to an existing partnership, **you have completed these steps already** and this is just a summary:

In the **Partnership** function, do the following on the **Partnership Info** tab (see "Working with the Partnership Info Tab" on page 266):

1. Set **Partnership Type** to EDI to Application or EDI to EDI. This causes the **Input EDI** tab to appear.

2. In the **Partnership** function, **Input EDI** tab (see "Working with the Input EDI Tab" on page 282):

3. Set **EDI Standard** to ANSI.

4. Set **Generate FA** to Always or On Errors Only.

5. Set **FA Level** and **Error Reporting Level** as desired.

ANSI reverse partnership: A *reverse partnership* is one that reverses the Sender and Receiver roles, is required to process the 997 that is returned when you request functional acknowledgments in a partnership. ECXpert automatically creates this for you, but before the reverse partnership can be used, you should edit it as described below.

Multiple partnerships with the same Sender and Receiver, but with different Document Types, all share the same reverse partnership; you only need to edit the reverse partnership once.

Unless a reverse partnership with the same Sender and Receiver but different Document Type already exists for main partnership that you just created or changed, **you must complete these steps now**:

1. Display the reverse partnership—see "Changing a Partnership's Information" on page 356. Remember to reverse the Sender and Receiver roles from the original partnership when displaying the reverse partnership.

2. In the **Partnership** function, on the **Partnership Info** tab (see "Working with the Partnership Info Tab" on page 266), the following values must *not* be changed:

   a. Leave Partnership Type set to Application to EDI

   b. Leave Document Type set to 997

CAUTION	Do *not* check FA (997) Expected? on this tab.

3. In the **Partnership** function, do the following on the **Protocols** tab (see "Working with the Protocols Tab" on page 314):

   a. Set **Outgoing Protocol** to the protocol you want to use for the FA.

   b. Fill in the options for that protocol.

Reverse Partnerships for EDIFACT CONTRL Messages

Main Partnership: The following steps are necessary to request CONTRL messages (if you just saved your work on a new partnership or a change to an existing partnership, **you have completed these steps already** and this is just a summary):

1. In the **Partnership** function, do the following on the **Partnership Info** tab (see "Working with the Partnership Info Tab" on page 266):

   o Set **Partnership Type** to EDI to Application or EDI to EDI. This causes the **Input EDI** tab to appear.

2. In the **Partnership** function, do the following on the **Input EDI** tab (see "Working with the Input EDI Tab" on page 282):

   o Set **EDI Standard** to EDIFACT.

   o Set **Generate CONTRL** to Always or **On Error Only**.

EDIFACT reverse partnership: A *reverse partnership*, one that reverses the Sender and Receiver roles, is required to process the CONTRL message that is returned when you request CONTRL messages in a partnership. ECXpert automatically creates this for you, but before the reverse partnership can be used, you must edit it as described below.

Multiple partnerships with the same Sender and Receiver, but with different Document Types, all share the same reverse partnership; you only need to edit the reverse partnership once.

Unless a reverse partnership with the same Sender and Receiver but different Document Type already exists for main partnership that you just created or changed, **you must complete these steps now**:

1. Display the reverse partnership—see "Changing a Partnership's Information" on page 356. Remember to reverse the Sender and Receiver roles from the original partnership when displaying the reverse partnership.

CAUTION	Do *not* check CONTRL Expected? on this tab.

2. In the **Partnership** function, do the following on the **Protocols** tab (see "Working with the Protocols Tab" on page 314):

a. Set **Outgoing Protocol** to the protocol to use for the CONTRL message

b. Fill in the options for that protocol

Adding a New Partnership on a Blank Form

Follow the steps below to add a new partnership on a blank form.

If you want to add a new partnership by editing another partnership's information, see "Copying a Partnership—Adding a New Partnership Based on Another" below.

1. Display the Partnership Administration tab (Figure 6-2) on page 259.

2. Click Add.

The Partnership Info tab (Figure 6-5) on page 267 is displayed.

3. Fill in the information on the different partnership definition tabs.

See "Working with the Partnership Definition Tabs" on page 266 for details.

4. Save the partnership's information.

Click Add at the bottom of the Protocols tab, on the last partnership definition tab.

NOTE	You can click Cancel at the bottom of any partnership definition tab if you decide not to add the new partnership.

Copying a Partnership—Adding a New Partnership Based on Another

When the information for a new partnership that you are adding is similar to the information for an existing partnership, you can save data entry time by using that existing partnership as a template for the new partnership. Follow the steps below to do this. To enter a new partnership without using another partnership as a template, see "Adding a New Partnership on a Blank Form" on page 354.

1. Display the Partnership Administration tab (Figure 6-2) on page 259.

2. Click Copy.

   The Partnership Search tab (Figure 6-3) on page 261 is displayed.

3. Find the partnership you want to use as a template.

   See "Displaying Information for an Existing Partnership" on page 260 for details.

4. Click Retrieve.

   The Partnership Info tab (Figure 6-5) on page 267 is displayed, but with "Copy Partnership" at the top.

NOTE	The specific settings of the partnership you have chosen to copy can also make the details on your screen look different from Figure 6-5.

5. Make necessary additions and changes.

All information is copied from the existing partnership. Partnerships are identified by a *unique combination* of the following fields:

• Sender Qualifier	• Doc Type	• Group Sender Qualifier
• Sender Qualifier ID	• EDI Standard	• Group Sender Qualifier ID
• Receiver Qualifier	• Version of the Standard	• Group Receiver Qualifier
• Receiver Qualifier ID	• Release of the Standard	• Group Receiver Qualifier ID

NOTE	You *must* change at least one of these items in order to create a unique new partnership, and the changes you make must not cause the above combination of fields to match any other existing partnership.
	You can change anything else on the partnership definition tabs as necessary to define the new partnership. Refer to "Working with the Partnership Definition Tabs" on page 266 for details on specific fields on the different tabs.

6. Save the partnership's information.

   Click Copy at the bottom of the Protocols tab, on the last partnership definition tab.

NOTE	You can click Cancel at the bottom of any partnership definition if you decide not to save the changes to the partnership.

Changing a Partnership's Information

Follow the steps below to change information for a partnership. Refer to "Working with the Partnership Definition Tabs" on page 266 for details on each item of information on each of the three tabs.

1. Display the Partnership Administration tab (Figure 6-2) on page 259.

2. Click Change.

   The Partnership Search tab (Figure 6-3) on page 261 is displayed.

3. Enter the Member IDs and Document Type for the partnership you want to change.

   See "Displaying Information for an Existing Partnership" on page 260 for details.

4. Click Retrieve.

   The information for the partnership that you want to change is displayed with the Partnership Information tab in front, as in Figure 6-5 on page 267.

5. Make necessary additions and changes.

6. Save the partnership's information.

   Click Change at the bottom of the Protocols tab, on the last partnership definition tab.

NOTE   You can click Cancel at the bottom of any partnership definition tab if you decide not to save the changes to the partnership.

Deleting a Partnership

NOTE   When you delete a *member*, the partnerships and service lists associated with that member are *also* automatically deleted.

   All tracking and event log information for files you previously processed for that member, however, remain intact.

Follow the steps below to delete a partnership.

1. Display the Partnership Administration tab (Figure 6-2) on page 259.

2. Click Delete.

   The Partnership Search tab (Figure 6-3) on page 261 is displayed.

3. Display the partnership that you want to delete.

See "Displaying Information for an Existing Partnership" on page 260 for details.

4. Click Delete.

   You are prompted to view the information before deleting:

   ❍ If you click Yes, the information is displayed.

   ❍ If you click No, the partnership is deleted without displaying the information.

   ❍ If you click Cancel, the deletion is canceled.

5. Click Yes.

   The information for the partnership you have selected to delete is displayed. The Partnership Info tab is in front, as in Figure 6-5 on page 267, but with "Copy Partnership" at the top.

NOTE	The specific settings of the partnership you have chosen to delete can also make the details on your screen look different from Figure 6-5.

6. Examine the information.

   You want to be absolutely certain that you are deleting the correct partnership.

7. Delete the partnership.

   Click Delete at the bottom of the Protocols tab, on the last partnership definition tab.

NOTE	You can click Cancel at the bottom of any partnership definition tab if you decide not to delete the partnership.

   After clicking Delete, you are prompted, "Are you sure?" Click Yes to confirm the deletion.

NOTE	You can still click No to cancel the deletion, but this is your last chance.

Tracking the Documents that ECXpert Processes

This chapter describes the tasks involved in using the document tracking features of ECXpert. The following topics are covered:

Overview

ECXpert provides a query facility through the Product Administrative Interface that allows you to locate information on specific documents and document groups being processed by ECXpert.

Information about this query facility begins with and continues through the end of this chapter.

Setting Up and Tracking Scheduled Jobs

Documents whose processing is started by a time-based ECXpert Scheduler job do not show up in the Tracking tabs until processing has been started. To set up and track scheduled jobs, log into the Product Administrative Interface as an administrator.

For more information, refer to the following sections of this Guide:

- For information about setting up scheduled jobs, refer to "Scheduling ECXpert Jobs" on page 155.

- For information about checking on the status of these scheduled jobs, refer to Chapter 8, "Tracking the Jobs that the Scheduler Manages."

Reprocessing Failed Submissions

Occasionally a submission fails to complete processing at some point in the service list. When this happens, the first thing to do is determine why it failed and fix the problem. See the *iPlanet ECXpert Operations Reference Guide*, "Manual Reprocessing of Submitted Files" topic, for tips on tracking down and fixing problems with failed submissions.

Once you have fixed the problem that caused the submission to fail, you do not have to resubmit the submission unit. Instead, you can reprocess the unfinished portion of the submission through the Product Administrative Interface. See "Reprocessing an Item that Failed" on page 373 for details.

Reprocessing Interrupted Submissions

If the ECXpert system is unexpectedly interrupted while a submission is being processed, for example by a power outage, it needs to be shut down and restarted. Once ECXpert is restarted, processing of submitted jobs resumes from the point at which the processing was interrupted, if the dispatcher `recovery` parameter is set to `yes`.

See the *iPlanet ECXpert Operations Reference Guide*, "Manual Recovery Reprocessing of Interrupted Jobs" topic, for more information about recovering interrupted jobs.

Displaying the Tracking Tabs

Follow the steps below to display the Tracking tabs.

1. Log into the ECXpert Product Administrative Interface.

2. Click Tracking.

   The Enter Search Constraints tab (Figure 7-1) is displayed.

   From these tabs you can get information on the business documents currently being processed by ECXpert.

   Most of your tracking tasks will probably begin from the Enter Search Constraints tab, but you can start from any tab if you know the tracking ID of the file involved.

   For more information on using each of the tracking tabs, see the following:

   ○ "Working with the Enter Search Constraints Tab" on page 361

   ○ "Working with the File Level Results Tab" on page 367

   ○ "Working with the Interchange Level Results Tab" on page 376

   ○ "Working with the Group Level Results Tab" on page 386

   ○ "Working with the Document Level Results Tab" on page 395

   ○ "Working with the Event Log Tab" on page 404

Working with the Enter Search Constraints Tab

When you click Tracking, the Enter Search Constraints tab appears. On the Enter Search Constraints tab, enter search criteria to display information about specific ECXpert activities.

For EDI documents, you can view information at the file, interchange, group, or document level. For both EDI and non-EDI documents, you can also view the event log which provides more detailed information about processing.

Follow the steps below to work with the Enter Search Constraints tab.

1. Log into the ECXpert Product Administrative Interface.

2. Click Tracking on the left.

   The Enter Search Constraints tab (Figure 7-1) is displayed.

Figure 7-1   Enter Search Constraints tab

Table 7-1   Information on the Enter Search Constraints tab

Item	Description
Sender/Receiver	
Note: This section does not appear when Search Level is set to System.	
Sending Member ID	The ECXpert member ID of the member who sent the file or document for which you want to view information.
	You can type the ID directly into the Sending Member ID field.
	OR...
	You can select the Sending Member ID from a list:
	• Click Expand ▼ to display a drop-down List of Members.
	• Select the ID for the sending member in the partnership that you want to change, copy, or delete.
	• Click Expand again to roll up the list.
Receiving Member ID	The ECXpert member ID of the member who received the file or document for which you want to view information.
	You can type the ID directly into the Receiving Member ID field.
	OR...
	You can select the Receiving Member ID from a list:
	• Click Expand ▼ to drop down the List of Members.
	• Select the ID for the sending member in the partnership that you want to change, copy, or delete.
	• Click Expand again to roll up the list.
Date/Time	
From Date	The beginning date to use to search for files or documents processed within a particular date and time range. Click ▣ to enter today's date.
From Date	The beginning time on the beginning date to use to search for files or documents processed within a particular date and time range. Click ⏱ to enter the current time.

Table 7-1   Information on the Enter Search Constraints tab *(Continued)*

Item	Description
To Date	The ending date to use to search for files or documents processed within a particular date and time range. Click to enter today's date.
To Time	The ending time on the ending date to use to search for files or documents processed within a particular date and time range. Click to enter the current time.
Processing State	
Completed	Check this box to see files or documents that are completed.
In Progress	Check this box to see files or documents that are in progress.
Warning	Check this box to see files or documents that are have generated warnings during processing.
Failed	Check this box to see files or documents that have failed to process.
MDN/EDI Acknowledgment State	
Note: The heading on this section depends on the selection made for Search Level. • MDN Acknowledgment State—when Search Level is set to File (the default). • EDI Acknowledgment State—when Search Level is set to Interchange, Group, or Document. • No acknowledgment section appears when Search Level is set to System.	
Accepted	Check this box to see files or documents with an acknowledgment status of "accepted."
Accepted/Errors	Check this box to see files or documents with an acknowledgment status of "accepted with errors."
Rejected	Check this box to see files or documents with an acknowledgment status of "rejected."
Waiting	Check this box to see files or documents with an acknowledgment status of "waiting."
Overdue	Check this box to see files or documents with an acknowledgment status of "overdue."
Not Expected	Check this box to see files or documents with an acknowledgment status of "not expected."
Search Level	

Table 7-1   Information on the Enter Search Constraints tab *(Continued)*

Item	Description
File	Select this option to search at the file level.
Interchange	Select this option to search at the EDI interchange level. Not applicable for non-EDI data.
Group	Select this option to search at the EDI functional group level. Not applicable for non-EDI data.
Document	Select this option to search at the document level.
System	Select this option to search at the system level.

File/Interchange/Group/Document/System Level Constraints

Note: The heading on this section depends on the selection made for Search Level.

- File Level Constraints—when Search Level is set to File (the default).

- Interchange Level Constraints—when Search Level is set to Interchange.

- Group Level Constraints—when Search Level is set to Group.

- Document Level Constraints—when Search Level is set to Document.

- No Constraints section appears when Search Level is set to System.

External Reference #	The reference or tracking number assigned to a file by the application from which it originated. (Appears only when Search Level is set to File.)
External File	The full path name of the original file. (Appears only when Search Level is set to File.)
Data Type	The data type, such as EDI or a non-EDI type, of the original file. (Appears only when Search Level is set to File.)
Interchange Control #	The Interchange Control number for the interchange, functional group, or document. (Appears when Search Level is set to Interchange, Group, or Document.)
Functional Group Control #	The functional group control number for the functional group or document. (Appears when Search Level is set to Group or Document.)
Document Control #	The document control number for the document. (Appears only when Search Level is set to Document.)
Document Type	The document type of the original file. (Appears only when Search Level is set to Document.)

3. Select the Search Level.

   Set **Search Level** based on the level at which you want to obtain tracking information. The selection you make here determines what other sections are displayed, the heading labels used, and the options available.

4. Enter your search criteria.

   Fill in the rest of the Enter Search Criteria tab. Refer to Table 7-1 on page 363 for information on specific items.

5. Click Search.

NOTE	If you do not fill in any values on the Enter Search Constraints tab other than for the Search Level, a message box appears asking whether you are sure you want to display the entire activity tracking database:
	• Click Yes to continue below.
	• Click No to cancel the search and continue with Step 4 above.

The search is performed and the results are displayed on the tab that corresponds to the Search Level you have selected:

For this Search Level...	Continue with...
File	"Working with the File Level Results Tab" on page 367
Interchange	"Working with the Interchange Level Results Tab" on page 376
Group	"Working with the Group Level Results Tab" on page 386
Document	"Working with the Document Level Results Tab" on page 395
System	"Working with the Event Log Tab" on page 404

Working with the File Level Results Tab

The files displayed on the File Level Results tab depend on the method you use to display the tab:

- From the Enter Search Constraints tab, set Search Level to File and click Search. The File Level Results tab displays all the files that match the search constraints.

- From a lower level results tab, select an interchange, group, or document and click Back until you reach the File Level Results tab. This tab displays the file containing the selected document, group, or interchange.

- From any other Tracking tab, click the File Level Results tab header directly. The File Level Results tab displays whatever content it had when last viewed.

Figure 7-2   File Level Results tab
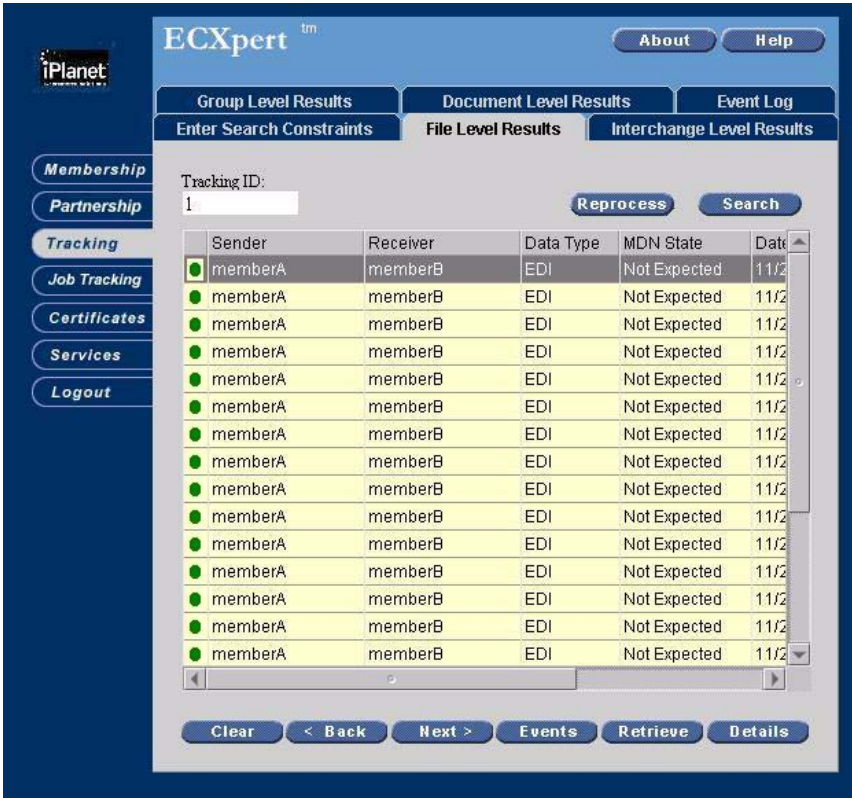
Table 7-2   Information on the File Level Results tab

Item	Description
Tracking ID	The tracking ID assigned to the selected file.
Status icon	A graphic icon shows the status:
	- red exclamation point indicates an error.
	- yellow triangle indicates a warning.
	- yellow oval indicates that it is still processing.
	- green oval indicates that it processed correctly.
	- blue question mark indicates that ECXpert cannot identify the item. You should not encounter this icon.
Sender	The member ID of the trading partner who sent the file.
Receiver	The member ID of the trading partner who is to receive the file.
Data Type	The type of data contained in the file that was sent, for example EDI.
MDN State	The Message Disposition Notification (MDN) status of the file. This state is applicable to SMTP exchanges, but the column appears even if there are no SMTP exchanges.
Date/Time	The date and time the file was sent.

What You Can Do on the File Level Results Tab

For more information on what you can do on the File Level Results tab, see the following:

- "Viewing More Detailed Information for a File" on page 369

- "Displaying the Next Lower Level of Information for a File" on page 370

- "Viewing the EDI Data for a File" on page 371

- "Viewing Event Log Entries for a File" on page 372

- "Reprocessing an Item that Failed" on page 373

- "Locating the File for a Specific Tracking ID" on page 374

- "Clearing the Search Fields on the File Level Results Tab" on page 376

Viewing More Detailed Information for a File

Follow the steps below to view more detailed information for a file that is displayed on the File Level Results tab.

1. Select a file.

2. Click Details.

Detailed information about the selected file is displayed in a separate window, as shown in Figure 7-3.

Figure 7-3   Detailed information for a selected file
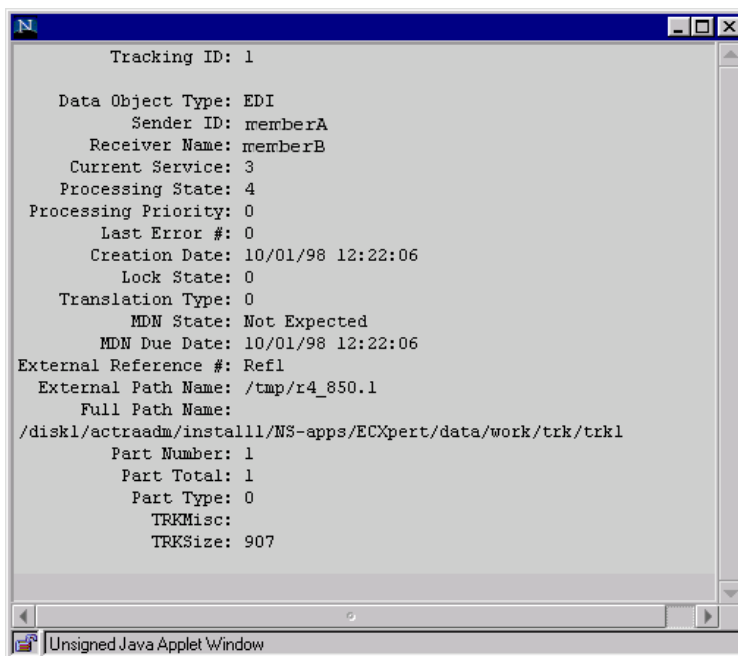
3. Close the details window.

When you are finished viewing the detailed information for the file, use the window controls to close the window.

For more information about other tasks you can perform in the File Level Results tab, see "What You Can Do on the File Level Results Tab" on page 368.

Displaying the Next Lower Level of Information for a File

When you are viewing information for a file, you might want to "drill down" and display the information for the next lower level in that file.

For EDI data, this would be the interchange level. For non-EDI data with HREC/TREC structure, this would be the document level. For non-EDI data there is only the file level.

Follow the steps below to view the next lower level of information for a file that is displayed on the File Level Results tab.

1. Select the file.

2. Click Next.

   The appropriate results tab is displayed, with information filled in for the selected file. For EDI data, the Interchange Level Results tab is displayed. For non-EDI data, the Document Level Results tab is displayed.

NOTE	Do not simply click another tab, such as the Interchange Level Results tab for EDI data.
	If you click another results tab directly, the information for the file you selected on the File Level Results tab is not automatically displayed.

   For more information about what you can do on the tab that is displayed, refer to the sections below.

For this tab...	See this heading...
Interchange	"Working with the Interchange Level Results Tab" on page 376
Group	"Working with the Group Level Results Tab" on page 386
Document	"Working with the Document Level Results Tab" on page 395

Viewing the EDI Data for a File

Follow the steps below to view the EDI data for a file that is displayed on the
File Level Results tab.

1. Select a file.

2. Click Retrieve.

EDI data for the selected file is displayed in a separate window, as shown in
Figure 7-4.

Figure 7-4　　EDI data for a selected file

3. Close the EDI window.

When you are finished viewing the EDI data, use the window controls to close the window.

For more information about other tasks you can perform in the File Level Results tab, see "What You Can Do on the File Level Results Tab" on page 368.

Viewing Event Log Entries for a File

Follow the steps below to view the log entries for a file that is displayed on the File Level Results tab.

1. Select a file.

2. Click Events.

    The Event Log tab is displayed, showing Event Log entries for the selected file as shown in Figure 7-5.

Figure 7-5   Event Log tab, showing entries for a selected file

For more information about what you can do on the Event Log tab, see
"Working with the Event Log Tab" on page 404.

Reprocessing an Item that Failed

Reprocessing a failed item applies even at the document level. For example, if an
interchange is received with 100 documents and the 99th document fails, you can
re-start processing from the 99th document.

Follow the steps below to reprocess an item that failed.

1. Enter a Tracking ID.

Clicking on a row for a file appearing in the list automatically enters the file's
tracking ID in the **Tracking ID** field.

2. Click Reprocess.

Processing of the failed item is resumed at the first document that has not successfully completed processing. A message is displayed indicating that the item was submitted for reprocessing.

For more information on what you can do next, see "What You Can Do on the File Level Results Tab" on page 368.

Locating the File for a Specific Tracking ID

Follow the steps below to locate the file for a specific tracking ID on the File Level Results tab.

1. Enter a tracking ID in the **Tracking ID** field.

2. Click Search.

Information for the file with the tracking ID you entered is displayed in the File Level Results tab, as shown in Figure 7-6.

Figure 7-6   File Level Results tab, showing information for a specific tracking ID
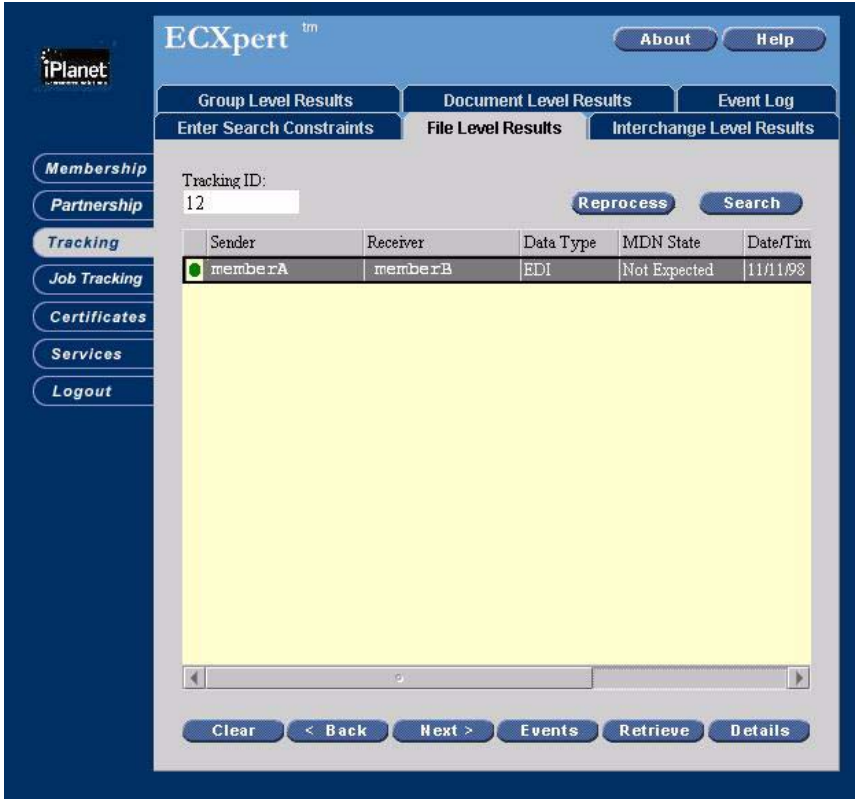
For more information on what you can do next, see "What You Can Do on the File Level Results Tab" on page 368.

Clearing the Search Fields on the File Level Results Tab

When you want to perform a new search on the File Level Results tab, you can clear the search fields with a single click before entering your new search criteria. This saves you the trouble of manually deleting the contents of each field that you do not want to use.

Follow the steps below to clear the search fields on the File Level Results tab.

1. Click Clear.

When you click Clear, the search fields for Tracking ID, Interchange ID, Group ID, and Document ID are cleared.

2. Enter new search criteria.

Continue with .

Working with the Interchange Level Results Tab

The interchanges displayed on the Interchange Level Results tab depend on the method you use to display the tab:

• From the Enter Search Constraints tab, set Search Level to Interchange and click Search. The Interchange Level Results tab displays all the interchanges in all the files that match the search constraints.

• From the File Level Results tab, select a file and click Next. The Interchange Level Results tab displays the interchanges in the selected file.

• From the Document Level Results tab, click Back. The Interchange Level Results tab displays the interchange for the selected document.

• From any other Tracking tab, click the Interchange Level Results tab header directly. The Interchange Level Results tab displays whatever content it had when last viewed.

Figure 7-7   Interchange Level Results tab

Table 7-3   Information on the Interchange Level Results tab

Item	Description
Tracking ID	The tracking ID assigned to the file that contains the interchange you select.
Interchange ID	The tracking ID assigned to the interchange you select.

Table 7-3   Information on the Interchange Level Results tab *(Continued)*

Item	Description
Status icon	A graphic icon shows the status: 🔴 - red exclamation point indicates an error. 🔻 - yellow triangle indicates a warning. 🟡 - yellow oval indicates that it is still processing. 🟢 - green oval indicates that it processed correctly. ❓ - blue question mark indicates that ECXpert cannot identify the item. You should not encounter this icon.
Sender Qual:ID	The trading address of the trading partner who sent the interchange.
Receiver Qual:ID	The trading address of the trading partner who is to receive the interchange.
Control #	The interchange control number assigned to the interchange.
Ack State	The acknowledgment state. For a detailed breakdown of Ack State values and their meaning, see "Detailed Description of Ack State Values" on page 408.
Standard	The EDI standard, such as ANSI, UCS, or EDIFACT, that the sending and receiving trading partners have agreed to use.
Ver-Rel	The version and release number of the EDI standard that the sending and receiving trading partners have agreed to use.
Date/Time	The date and time that the interchange was sent.

To view all the fields for each interchange, drag the scroll bar or click the arrow buttons below the entries for the interchanges.

What You Can Do on the Interchange Level Results Tab

For more information on what you can do on the Interchange Level Results tab, see the following:

Viewing More Detailed Information for an Interchange

Follow the steps below to view more detailed information for an interchange on the Interchange Level Results tab.

1. Select an interchange.

2. Click Details.

   Detailed information about the selected interchange is displayed in a separate window, as shown in Figure 7-8.

Figure 7-8   Detailed information for a selected interchange

```
N                                                              _ □ ×
              Tracking ID: 129                                      ▲
   Interchange Tracking ID: 1

           Current Service: 5
          Processing State: 1
              Last Error #: 0
             Parse Error #: 0
       Processing Priority: 50
         Sender EDI Qual ID: ZZ
              Sender EDI ID: memberA
       Receiver EDI Qual ID: ZZ
            Receiver EDI ID: memberB
                  Standard: ANSI
                   Version: 003020
                   Release: 0
     Acknowledgment State: Not Expected
  Test or Production Flag: 1
     Interchange Control #: 000005641
                 File Name:
/disk1/actraadm/install1/NS-apps/ECXpert/data/work/trk/trk129
             Creation Time: 10/06/98 19:22:47
          Interchange Size: 911
     Header Starting Offset: 0
  Interchange Header Size: 106
   Trailer Starting Offset: 895                                     ▼
◀                             ○                               ▶
🖻 Unsigned Java Applet Window
```

3. Close the details window.

When you are finished viewing the detailed information for the interchange, use the window controls to close the window.

For more information about other tasks you can perform in the Interchange Level Results tab, see "What You Can Do on the Interchange Level Results Tab" on page 379.

Displaying Next Lower or Higher Level of Information for an Interchange

NOTE	This section is applicable only to EDI data. Non-EDI data does not have interchanges and groups.

When you are viewing information for an interchange, you can "drill down" and display the information for the next lower level in that interchange, or you can "drill up" and display the information for the next higher level.

Only EDI data has interchanges in its structure. For such data, the next lower level would be the group, and the next higher level would be the file.

Follow the steps below to display the next lower or next higher level of information for an interchange displayed on the Interchange Level Results tab.

1. Select the interchange.

2. Click Next to "drill down," click Back to "drill up."

Clicking Next displays the Group Level Results tab, showing the groups in the selected interchange. For more information about what you can do on the Group Level Results tab, see "Working with the Group Level Results Tab" on page 386.

Clicking Back displays the File Level Results tab, showing the file containing the selected interchange. For more information about what you can do on the File Level Results tab, see "Working with the File Level Results Tab" on page 367.

NOTE	Do not simply click another tab, such as the Group Level Results tab when you want to "drill down" or "drill up" from the selected interchange. If you click another results tab directly, the information for the interchange you selected on the Interchange Level Results tab is not automatically displayed.

Viewing the EDI Data for an Interchange

Follow the steps below to view the EDI information for an interchange displayed on the Interchange Level Results tab.

1. Select an interchange.

2. Click Retrieve.

EDI data for the selected interchange is displayed in a separate window, as shown in Figure 7-9.

Figure 7-9   EDI data for a selected interchange
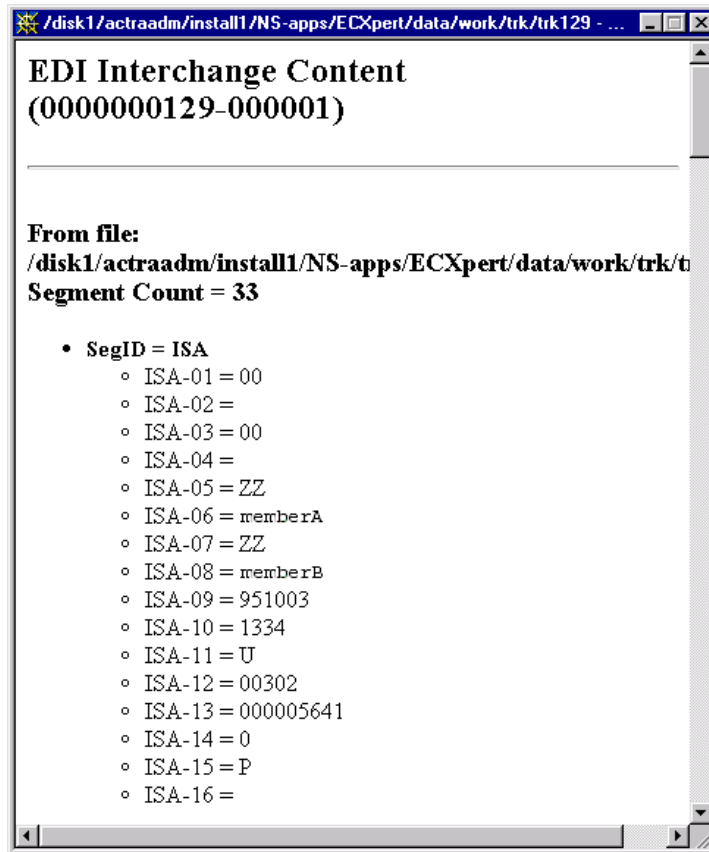
3. Close the EDI window.

   When you are finished viewing the EDI data, use the window controls to close the window.

   For more information about other tasks you can perform in the Interchange Level Results tab, see "What You Can Do on the Interchange Level Results Tab" on page 379.

Viewing Event Log Entries for an Interchange

Follow the steps below to view the Event Log entries for an interchange displayed on the Interchange Level Results tab.

1. Select an interchange.

2. Click Events.

   The Event Log tab is displayed, showing Event Log entries for the selected interchange as shown in Figure 7-10.

Figure 7-10   Event Log tab, showing entries for a selected interchange

For more information about what you can do on the Event Log tab, see

Locating the Interchange(s) for a Specific Tracking ID

Follow the steps below to locate the interchange(s) for a specific tracking ID on the
Interchange Level Results tab.

1. Enter a tracking ID in the **Tracking ID** field.

2. Optionally, enter an interchange ID in the **Interchange ID** field.

If you leave the Interchange ID field blank, your search displays all the
interchanges for the file with the tracking ID you enter.

3. Click Search.

   Information for the file with the tracking ID you entered is displayed in the Interchange Level Results tab, as shown in Figure 7-11.

   Figure 7-11   Interchange Level Results tab, showing information for a specific tracking ID

For more information on what you can do next, see "What You Can Do on the Interchange Level Results Tab" on page 379.

Clearing the Search Fields on the Interchange Level Results Tab

When you want to perform a new search on the Interchange Level Results tab, you can clear the search fields with a single click before entering your new search criteria. This saves you the trouble of manually deleting the contents of each field that you do not want to use.

Follow the steps below to clear the search fields on the Interchange Level Results tab.

1. Click Clear.

The search fields for Tracking ID and Interchange ID are cleared.

2. Enter new search criteria.

Continue with "Locating the Interchange(s) for a Specific Tracking ID" on page 384.

Working with the Group Level Results Tab

The groups displayed on the Group Level Results tab depend on the method you use to display the tab:

- From the Enter Search Constraints tab, set Search Level to Group and click Search. The Group Level Results tab displays all the groups in all the files that match the search constraints.

- From a higher level results tab (File Level Results or Interchange Level Results), select an item and click Next until the Group Level Results tab appears. The Group Level Results tab displays the groups in the selected file or interchange.

- From the Document Level Results tab, click Back. The Group Level Results tab displays the group for the selected document.

- From any other Tracking tab, click the Group Level Results tab header directly. The Group Level Results tab displays whatever content it had when last viewed.

Figure 7-12 Group Level Results tab
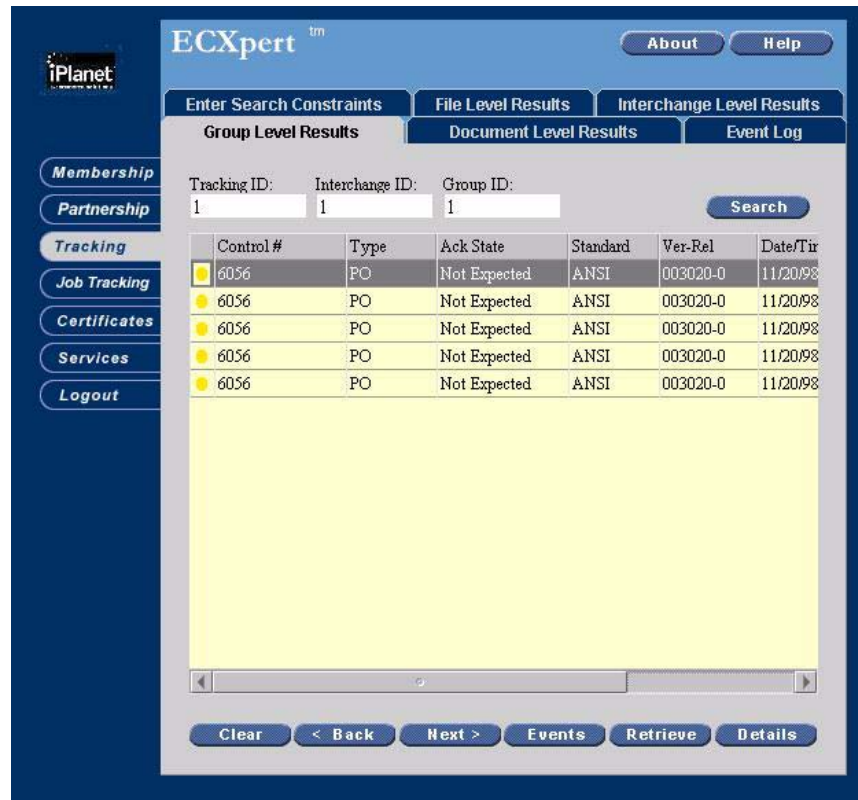
Table 7-4 Information on the Group Level Results tab

Item	Description
Tracking ID	The tracking ID assigned to the file that contains the group you select.
Interchange ID	The tracking ID assigned to the interchange that contains the group you select.
Group ID	The tracking ID assigned to the group you select.

Table 7-4 Information on the Group Level Results tab *(Continued)*

Item	Description
Status icon	A graphic icon shows the status:
	🛑 - red exclamation point indicates an error.
	🔻 - yellow triangle indicates a warning.
	🟡 - yellow oval indicates that it is still processing.
	🟢 - green oval indicates that it processed correctly.
	❓ - blue question mark indicates that ECXpert cannot identify the item. You should not encounter this icon.
Control #	The group control number assigned to the group.
Type	The functional group type for the group.
Ack State	The acknowledgment state. For a detailed breakdown of Ack State values and their meaning, see "Detailed Description of Ack State Values" on page 408.
Standard	The EDI standard, such as ANSI, UCS, or EDIFACT, that the sending and receiving trading partners have agreed to use.
Ver-Rel	The version number and release of the EDI standard that the sending and receiving trading partners have agreed to use.
Date/Time	The date and time that the group was sent.

To view all the fields for each group, drag the scroll bar or click the arrow buttons below the entries for the groups at the bottom of the display box.

What You Can Do on the Group Level Results Tab

For more information on what you can do on the Group Level Results tab, see the following:

Viewing More Detailed Information for a Group

Follow the steps below to view the more detailed information for a group displayed on the Group Level Results tab.

1. Select a group.

2. Click Details.

Detailed information about the selected group is displayed in a separate window, as shown in Figure 7-13.

Figure 7-13   Detailed information for a selected group
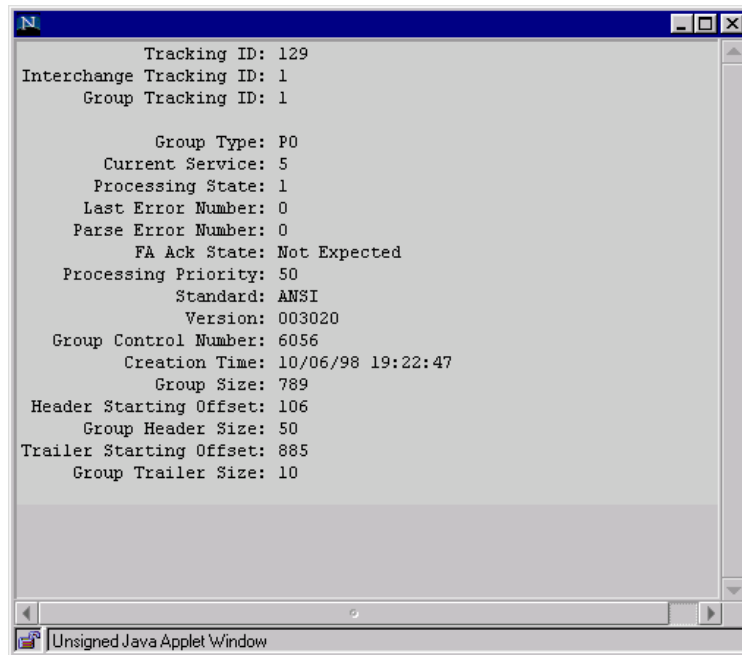

```
                Tracking ID: 129
   Interchange Tracking ID: 1
          Group Tracking ID: 1

                 Group Type: PO
            Current Service: 5
           Processing State: 1
           Last Error Number: 0
           Parse Error Number: 0
               FA Ack State: Not Expected
        Processing Priority: 50
                   Standard: ANSI
                    Version: 003020
       Group Control Number: 6056
              Creation Time: 10/06/98 19:22:47
                 Group Size: 789
      Header Starting Offset: 106
          Group Header Size: 50
     Trailer Starting Offset: 885
         Group Trailer Size: 10
```

Unsigned Java Applet Window

3. Close the details window.

When you are finished viewing the detailed information for the group, use the window controls to close the window.

For more information about other tasks you can perform in the Group Level Results tab, see "What You Can Do on the Group Level Results Tab" on page 388.

Displaying Next Lower or Higher Level of Information for a Group

When you are viewing information for a group, you can "drill down" and display the information for the next lower level in that group, or you can "drill up" and display the information for the next higher level.

Only EDI data has groups in its structure. For such data, the next lower level would be the document, and the next higher level would be the interchange.

Follow the steps below to view the next lower or next lower level of information for a group displayed on the Group Level Results tab.

1. Select the group.

2. Click Next to "drill down," click Back to "drill up."

Clicking Next displays the Document Level Results tab, showing the documents in the selected group. For more information about what you can do on the Document Level Results tab, see "Working with the Document Level Results Tab" on page 395.

Clicking Back displays the Interchange Level Results tab, showing the interchange containing the selected group. For more information about what you can do on the Interchange Level Results tab, see "Working with the Interchange Level Results Tab" on page 376.

NOTE	Do not simply click another tab, such as the Document Level Results tab when you want to "drill down" or "drill up" from the selected group. If you click another results tab directly, the information for the group you selected on the Group Level Results tab is not automatically displayed.

Viewing the EDI Data for a Group

Follow the steps below to view the EDI data for a group displayed on the Group Level Results tab.

1. Select a group.

2. Click Retrieve.

EDI data for the selected group is displayed in a separate window, as shown in Figure 7-14.

Figure 7-14 EDI data for a selected group
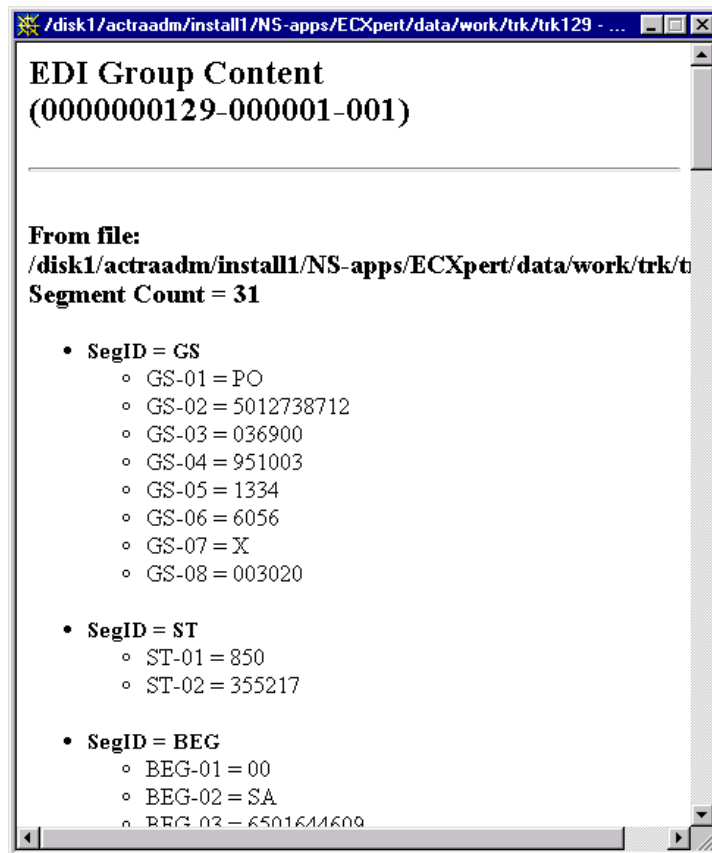
3. Close the EDI window.

   When you are finished viewing the EDI data, use the window controls to close the window.

   For more information about other tasks you can perform in the Group Level Results tab, see "What You Can Do on the Group Level Results Tab" on page 388.

Viewing Event Log Entries for a Group

Follow the steps below to view the Event Log entries for a group displayed on the Group Level Results tab.

1. Select a group.

2. Click Events.

   The Event Log tab is displayed, showing Event Log entries for the selected group as shown in Figure 7-15.

Figure 7-15 Event Log tab, showing entries for a selected group

For more information about what you can do on the Event Log tab, see "Working with the Event Log Tab" on page 404.

Locating the Group(s) for a Specific Tracking ID

Follow the steps below to locate the group(s) for a specific tracking ID on the Group Level Results tab.

1. Enter a tracking ID in the **Tracking ID** field.

2. Optionally, enter an interchange ID in the I**nterchange ID** field.

   If you leave the **Interchange ID** field blank, your search displays *all* the interchanges for the file with the tracking ID you enter.

3. Optionally, enter a group ID in the **Group ID** field.

If you leave the **Group ID** field blank, your search displays *all* the groups for the file with the tracking ID you enter.

4. Click Search.

Information for the file with the tracking ID you entered is displayed in the Group Level Results tab, as shown in Figure 7-6.

Figure 7-16   Group Level Results tab, showing information for a specific tracking ID

For more information on what you can do next, see "What You Can Do on the Group Level Results Tab" on page 388.

Clearing the Search Fields on the Group Level Results Tab

When you want to perform a new search on the Group Level Results tab, you can clear the search fields with a single click before entering your new search criteria. This saves you the trouble of manually deleting the contents of each field that you do not want to use.

Follow the steps below to clear the search fields on the Group Level Results tab.

1. Click Clear.

    The search fields for Tracking ID, Interchange ID, and Group ID are cleared.

2. Enter new search criteria.

    Continue with .

Working with the Document Level Results Tab

The documents displayed on the Document Level Results tab depend on the method you use to display the tab:

*   From the Enter Search Constraints tab, set the Search Level to Document and click Search. The Document Level Results tab displays all the documents in all the files that match the search constraints.

*   From a higher level results tab (File Level Results, Interchange Level Results, or Group Level Results), select an item and click Next until the Document Level Results tab appears. The Document Level Results tab displays the documents in the selected file, interchange, or group.

*   From any other Tracking tab, you click the Document Level Results tab header directly. The Document Level Results tab displays whatever content it had when last viewed.

Figure 7-17   Document Level Results tab
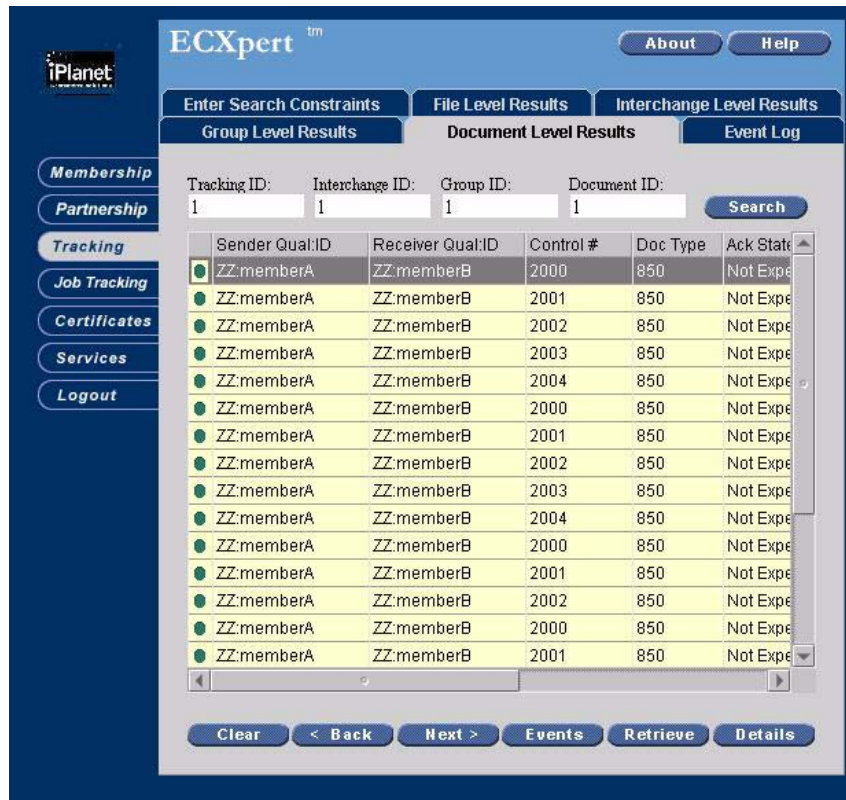
Table 7-5   Information on the Document Level Results tab

Item	Description
Tracking ID	The tracking ID assigned to the file that contains the group you select.
Interchange ID	The tracking ID assigned to the interchange that contains the group you select.
Group ID	The tracking ID assigned to the group you select.

Table 7-5 Information on the Document Level Results tab *(Continued)*

Item	Description
Status icon	A graphic icon shows the status:
	![red] - red exclamation point indicates an error.
	![triangle] - yellow triangle indicates a warning.
	![oval] - yellow oval indicates that it is still processing.
	![green] - green oval indicates that it processed correctly.
	![blue] - blue question mark indicates that ECXpert cannot identify the item. You should not encounter this icon.
Control #	The group control number assigned to the group.
Type	The functional group type for the group.
Ack State	The acknowledgment state. For a detailed breakdown of Ack State values and their meaning, see "Detailed Description of Ack State Values" on page 408.
Standard	The EDI standard, such as ANSI, UCS, or EDIFACT, that the sending and receiving trading partners have agreed to use.
Ver-Rel	The version number and release of the EDI standard that the sending and receiving trading partners have agreed to use.
Date/Time	The date and time that the group was sent.

What You Can Do on the Document Level Results Tab

For more information on what you can do on the Document Level Results tab, see the following:

Viewing More Detailed Information for a Document

Follow the steps below to view more detailed information for a document displayed on the Document Level Results tab.

1. Select a document.

2. Click Details.

    Detailed information about the selected document is displayed in a separate window, as shown in Figure 7-18.

Figure 7-18   Detailed information for a selected document


```
              Tracking ID: 151
  Interchange Tracking ID: 1
        Group Tracking ID: 1
     Document Tracking ID: 1

        Processing  State: 2
      Processing Priority: 50
          Current Service: 4
        Last Error Number: 0
       Parse Error Number: 0
        Translation State: 3
 Translation Error Number: 0
   Translation Start Time: 10/07/98 14:13:37
     Translation End Time: 10/07/98 14:13:37
                Lock Flag: 0
  Test or Production Flag: 1
     Sender EDI Qualifier: ZZ
           Sender EDI ID: memberA
   Receiver EDI Qualifier: ZZ
          Receiver EDI ID: memberB
                 Map Name: Invoices.map
                 Standard: ANSI
                  Version: 003020
                  Release: 0
         Translation Type: 1
```

Unsigned Java Applet Window

3. Close the details window.

    When you are finished viewing the detailed information for the document, use the window controls to close the window.

For more information about other tasks you can perform in the Document Level Results tab, see "What You Can Do on the Group Level Results Tab" on page 388.

Displaying the Next Higher Level of Information for a Document

When you are viewing information for a document, you can "drill up" and display the information for the next higher level. For EDI data, the next higher level would be the group.

Follow the steps below to view next higher level of information for a document displayed on the Document Level Results tab.

NOTE	For EDI data, the next higher level of information is the group. For non-EDI data with HREC/TREC structure, the next higher level of information is the file. For other non-EDI data, there is only the file level and this section is not applicable.

1. Select the document.

2. Click Back to "drill up."

   Clicking Back displays the Group Level Results tab, showing the interchange containing the selected document. For more information about what you can do on the Group Level Results tab, see "Working with the Group Level Results Tab" on page 386.

NOTE	Do not simply click another tab, such as the Group Level Results tab when you want to "drill down" or "drill up" from the selected document. If you click another results tab directly, the information for the document you selected on the Document Level Results tab is not automatically displayed.

Viewing the EDI Data for a Document

Follow the steps below to view the EDI data for a document displayed on the Document Level Results tab.

1. Select a document.

2. Click Retrieve.

   EDI data for the selected document is displayed in a separate window, as shown in Figure 7-19.

   Figure 7-19 EDI data for a selected document
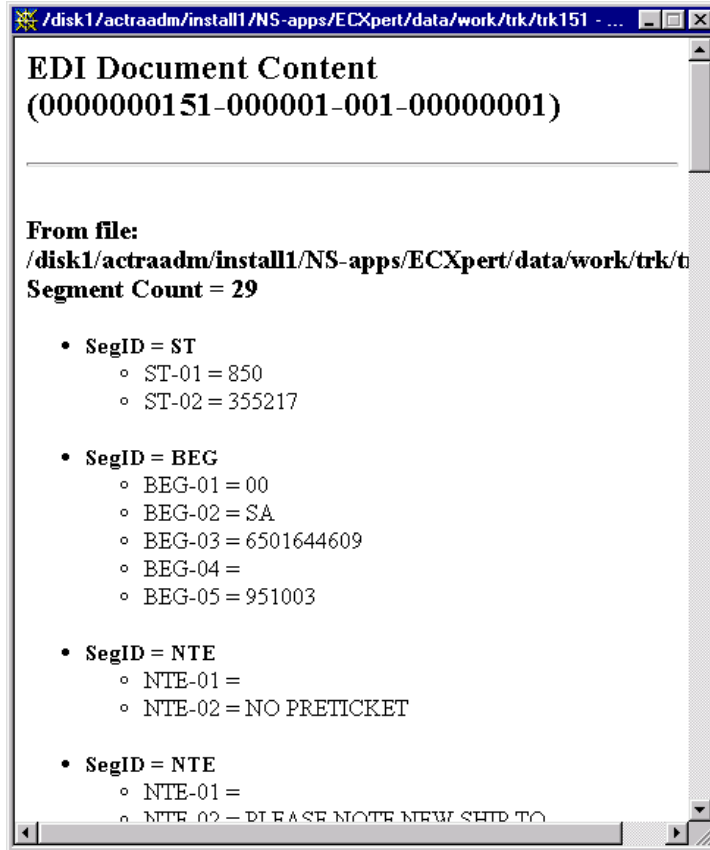
3. Close the EDI window.

   When you are finished viewing the EDI data, use the window controls to close the window.

   For more information about other tasks you can perform in the Document Level Results tab, see "What You Can Do on the Document Level Results Tab" on page 397.

Viewing Event Log Entries for a Document

Follow the steps below to view the Event Log entries for a document displayed on the Document Level Results tab.

1. Select a document.

2. Click Events.

   The Event Log tab is displayed, showing Event Log entries for the selected document as shown in Figure 7-5.

Figure 7-20 Event Log tab, showing entries for a selected document
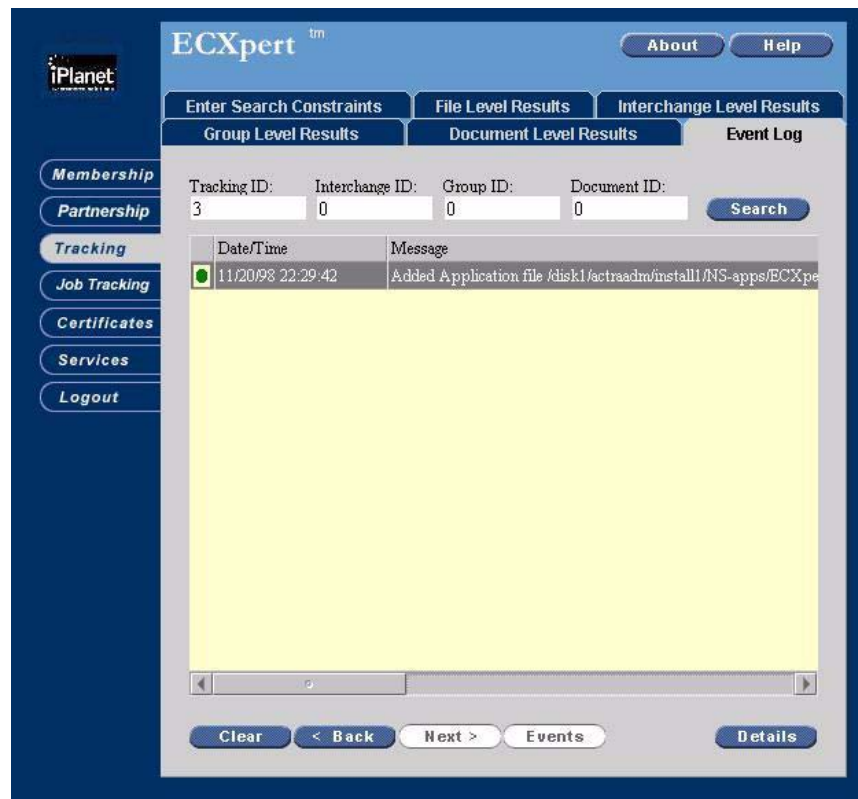
For more information about what you can do on the Event Log tab, see "Working with the Event Log Tab" on page 404.

Locating the Document(s) for a Specific Tracking ID

Follow the steps below to locate the document(s) for a specific tracking ID on the Document Level Results tab.

1. Enter a tracking ID in the **Tracking ID** field.

2. Optionally, enter an interchange ID in the **Interchange ID** field.

   If you leave the **Interchange ID** field blank, your search displays all the interchanges for the file with the tracking ID you enter.

3. Click Search.

   Information for the file with the tracking ID you entered is displayed in the Document Level Results tab, as shown in Figure 7-6.

Figure 7-21   Document Level Results tab, showing information for a specific tracking ID

For more information on what you can do next, see "What You Can Do on the Interchange Level Results Tab" on page 379.

Clearing the Search Fields on the Document Level Results Tab

When you want to perform a new search on the Document Level Results tab, you can clear the search fields with a single click before entering your new search criteria. This saves you the trouble of manually deleting the contents of each field that you do not want to use.

Follow the steps below to clear the search fields on the Document Level Results tab.

1. Click Clear.

   The search fields for Tracking ID, Interchange ID, and Group ID are cleared.

2. Enter new search criteria.

   Continue with

Working with the Event Log Tab

You can get to the Event Log tab several different ways. The content displayed on the Event Log tab depends on the method you used to get to the tab:

- For events "above" the file level, such as messages from servers, invalid SMTP sender/receiver messages, and "nothing to reprocess" messages, use Enter Search Constraints.

- For events for the file selected on File Level Results, use **File Level Results.**

- For events for the interchange selected on Interchange Level Results, use **Interchange Level Results.**

- For events for the group selected on Group Level Results, use **Group Level Results.**

- For events for the document selected on Document Level Results, use **Document Level Results.**

- For whatever events were displayed the last time the tab was active, click directly on the Event Log tab.

Figure 7-22   Event Log tab
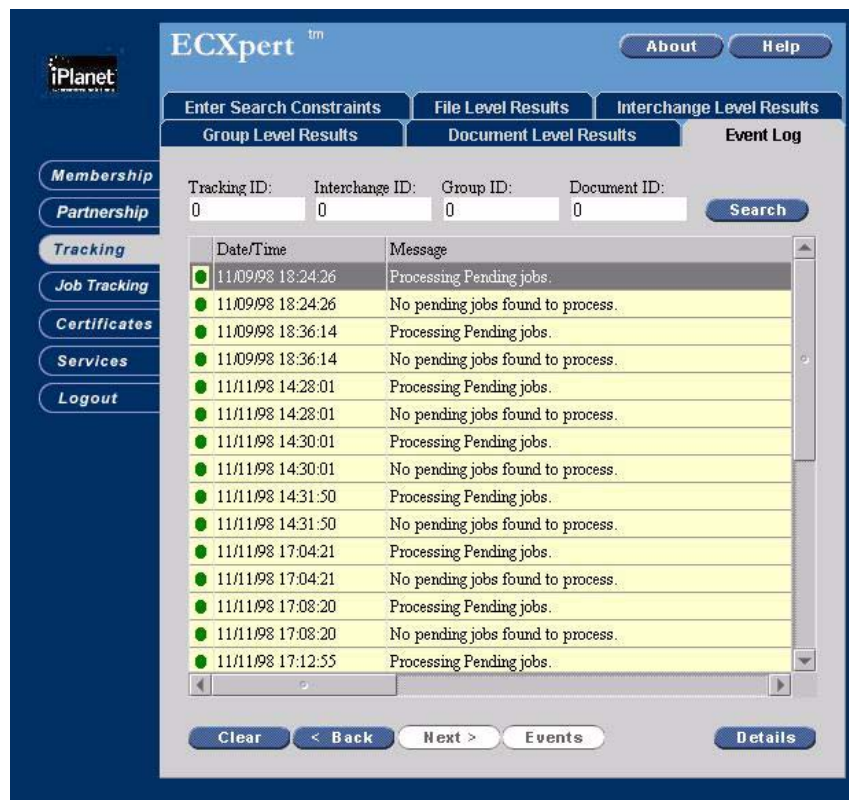
Table 7-6   Information on the Event Log tab

Item	Description
Tracking ID	The tracking ID assigned to the original file that was either sent or received.
Interchange ID	The tracking ID assigned to the interchange.
Group ID	The tracking ID assigned to the group.
Document ID	The tracking ID assigned to the document.

Table 7-6   Information on the Event Log tab *(Continued)*

Item	Description
Status icon	A graphic icon shows the status: ![red exclamation] - red exclamation point indicates an error. ![yellow triangle] - yellow triangle indicates a warning. ![yellow oval] - yellow oval indicates that it is still processing. ![green oval] - green oval indicates that it processed correctly. ![blue question mark] - blue question mark indicates that ECXpert cannot identify the item. You should not encounter this icon.
Date/Time	The date and time the item was sent.
Message	Describes the detailed processing steps performed on the file as it is parsed through the Service List indicated at the top of the log. Messages are recorded at the beginning, during, and at the end of each individual service in the list. A green circle indicates that the event was successful; a red exclamation point indicates an error condition. A yellow circle indicates that the event is still processing. A blue "?" indicates that ECXpert cannot identify the item. You should not encounter this icon.

What You Can Do on the Event Log Tab

For more information on what you can do on the Event Log tab, see the following:

- ❍ "Searching for Entries" on page 406
- ❍ "Viewing More Details on an Entry" on page 407
- ❍ "Viewing Information for Document(s) for an Entry" on page 408
- ❍ "Clearing the Search Fields on the Event Log Tab" on page 408

Searching for Entries

Follow the steps below to search for entries on the Event Log tab.

1. Enter information to match.

Enter values for that you want to match in **Tracking ID**, **Interchange ID**, **Group ID**, and **Document ID** fields at the top of the tab.

2. Click Search.

    Event Log entries matching the information you entered are displayed.

Viewing More Details on an Entry

Follow the steps below to view more details on an entry displayed on the Event Log tab.

1. Select an entry.

2. Click Details.

    Detailed information about the selected entry is displayed in a separate window, as shown in Figure 7-23.

Figure 7-23   Detailed information for a selected Event Log entry
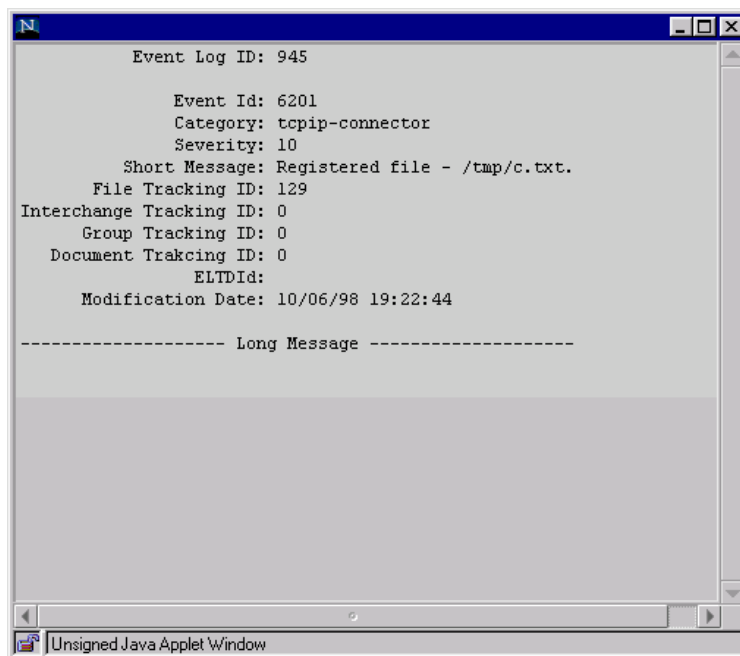
Viewing Information for Document(s) for an Entry

Follow the steps below to view information for document(s) for an entry displayed on the Event Log tab.

1. Select an entry.

2. Click Back.

The Document Level Results tab is displayed, listing the document(s) related to the selected Event Log tab entry.

Clearing the Search Fields on the Event Log Tab

When you want to perform a new search on the Event Log tab, you can clear the search fields with a single click before entering your new search criteria. This saves you the trouble of manually deleting the contents of each field that you do not want to use. Follow the steps below to clear the search fields on the Event Log tab.

1. Click Clear.

The search fields for Tracking ID, Interchange ID, Group ID, and Document ID are cleared.

2. Enter new search criteria.

Continue with

Detailed Description of Ack State Values

Ack State column is displayed on all the search results tabs below the File Level Results. This section presents a detailed breakdown of the values that you can see in this column.

The `AckState` column stores the acknowledgment status when Functional Acknowledgments (FAs/997s) or CONTRL messages are requested. The column appears in the `TrkIntchg` (`TIAckState`), `TrkGroup` (`TGAckState`), and `TrkDoc` (`TDAckState`) tables.

The actual value of `AckState` is computed by adding together the applicable combination of the following values:

Defined State	Value
ASunknown	0
ASwaiting	1
ASok	2
ASerror	4
ASreject	6
ASpreject	16
ASsent	32
ASsendFailed	64
ASreconciled	128

To understand the usage of these values, we can break the above definitions into three categories:

- basic state (Asunknown, ASwaiting)

- acknowledgment status (ASok, ASerror, ASreject, ASpreject)

- acknowledgment flavor (ASsent, ASsendFailed, ASreconciled)

The acknowledgment status can be added to the acknowledgment flavor to get a complete picture of a document record's corresponding acknowledgment state.

Let's consider some scenarios and see how this would work.

Outbound EDI

In the case of outbound EDI, the map direction is Application to EDI or EDI to EDI. After successful translation, Translate assigns ASwaiting to the document record.

When the 997 or CONTRL is returned in response to this document, this is parsed and the AckState of the gets a flavour of ASreconciled added to the state extracted from the acknowledgment.

Thus, if the trading partner rejects this document for whatever reason, the AckState for this document would be ASreconciled added to ASreject.

Inbound EDI

In this case, the map direction is EDI to application. FAgen generates the acknowledgment and assigns an initial status to the document (ASok, ASreject, etc.). When Gateway sends the acknowledgment out, the AckState of the original document is updated with the ASsent or ASsendFailed flavor.

Thus, if we reject an inbound EDI document and Gateway succeeds in sending this out, the AckState of this document would be ASsent added to ASreject.

Messages Displayed

Table 7-7 lists the messages displayed in the Tracking tabs for various values of AckState.

Table 7-7   Tracking tab messages for various AckState values.

If AckState has...	And...	Message Displayed is...
ASwaiting only added (AckState = ASwaiting)	acknowledgment Overdue Date > current date	Waiting
	acknowledgment Overdue Date <= current date	Overdue
ASreconciled added	ASok has been added to AckState	Reconciled (OK)
	ASerror has been added to AckState	Reconciled (Error)
	ASreject has been added to AckState	Reconciled (Reject)
	ASpreject has been added to AckState	Reconciled (Partial) Reject
	otherwise	Reconciled

Table 7-7   Tracking tab messages for various `AckState` values. *(Continued)*

If AckState has...	And...	Message Displayed is...
ASsendFailed added	ASok has been added to AckState	Sent (OK)
	ASerror has been added to AckState	Sent (Error)
	ASreject has been added to AckState	Sent (Reject)
	ASpreject has been added to AckState	Sent (Partial) Reject
	otherwise	Sent
ASsent added	ASok has been added to AckState	Send Failed (OK)
	ASerror has been added to AckState	Send Failed (Error)
	ASreject has been added to AckState	Send Failed (Reject)
	ASpreject has been added to AckState	Send Failed (Partial) Reject
	otherwise	Send Failed
otherwise, if acknowledgment Overdue Date > current date	ASok has been added to AckState	Generated (OK)
	ASerror has been added to AckState	Generated (Error)
	ASreject has been added to AckState	Generated (Reject)
	ASpreject has been added to AckState	Generated (Partial) Reject
otherwise, if acknowledgment Overdue Date <= current date	ASok has been added to AckState	Send-Overdue (OK)
	ASerror has been added to AckState	Send-Overdue (Error)
	ASreject has been added to AckState	Send-Overdue (Reject)
	ASpreject has been added to AckState	Send-Overdue (Partial) Reject

Detailed Description of Ack State Values

Tracking the Jobs that the Scheduler Manages

This chapter describes the tasks involved tracking the jobs that ECXpert's time-based Scheduler manages. The following topics are covered:

- Overview

- Enabling the Job Tracking Tabs

- Displaying the Job Tracking Tabs

- Working with the Scheduled Jobs Tab

- Working with the Job Instances Tab

- Working with the Job Instance Log Tab

Overview

Processing jobs set up on a time-based schedule through the ECXpert Scheduler can be tracked through the Job Tracking tabs. Information available here supplements the information available through the Tracking tabs.

If a job has not yet begun processing, or was prevented from starting processing by an error condition, the Job Tracking tabs might contain the only information available on these documents.

Enabling the Job Tracking Tabs

The functions of the Job Tracking tabs in the Product Administrative Interface require the ECXpert Date/Time Based Scheduler server to be turned on. See "Managing ECXpert System Settings" on page 136 for information on turning on ECXpert servers.

Displaying the Job Tracking Tabs

Follow the steps below to display the Job Tracking tabs.

1. Log into the ECXpert Product Administrative Interface.

2. Click Job Tracking.

   The Job Tracking tabs are displayed, with the Scheduled Jobs tab in front.

   Figure 8-1 shows this tab as it looks after clicking Search to display current jobs being managed by the ECXpert Scheduler. When you first display this tab in an ECXpert session, no scheduled jobs are displayed.

   From these tabs you can get information on the jobs that have been scheduled through the ECXpert Scheduler for time-based processing by ECXpert.

Working with the Scheduled Jobs Tab

The Scheduled Jobs tab allows you to list the jobs that the ECXpert Scheduler is managing, and then get more information on one that you select. Follow the steps below to work with the Scheduled Jobs tab.

1. Log into the ECXpert Product Administrative Interface.

2. Click Job Tracking on the left.

   The Scheduled Jobs tab (Figure 8-1) is displayed.

3. Click Search.

   The Scheduled Jobs tab now displays any jobs that the ECXpert Scheduler is currently managing, as shown in Figure 8-1.

NOTE	If there are no scheduled jobs, the informational message, "No matching data found," is displayed.

Figure 8-1   Scheduled Jobs tab, data displayed

Table 8-1   Information on the Scheduled Jobs tab

Item	Description
Name	The Name given the job in the ECXpert Scheduler.
State	The Status of the job in the ECXpert Scheduler.
Type	The type of job:
	• If Executable is Dispatcher or Gateway, this field is set to daemon.
	• If Executable is executable, this field is set to exec.
	• If Executable is script, this field is set to exec.

Table 8-1 Information on the Scheduled Jobs tab *(Continued)*

Item	Description
Executable	The Use selection for the job from the first Scheduler page when the job is defined: • script • executable • dispatcher • gateway
Iterations	The number of times the job has been executed since the current schedule was set up in the ECXpert Scheduler.
Last Run	The date and time that the job was last run.

4. Locate the job you are interested in.

Refer to Table 8-1 for a description of the information that is displayed.

5. Select the job for which you want to see more information.

Click on the row for the job to select it.

6. Click Next.

Figure 8-2 displays more detailed information for the job you selected on the Scheduled Jobs tab.

Working with the Job Instances Tab

The Job Instances tab displays summary information for specific instances of the job you selected on the Scheduled Jobs tab. All specific instances of the job that have been run are listed.

Records of jobs that have run are not automatically aged out of the database, but are retained until purged by the ECXpert site administrator.

For information of using the ECXpert purge utilities, see "bdggenManifest and bdgrealpurge—Purging Aged Data" on page 528.

1. Display the ScheduledJobs tab (Figure 8-1).

2. Click Search to display Scheduler jobs.

3. Select the job you are interested in.

4. Click Next.

   Figure 8-2 shows information on each instance of the job you selected on the Scheduled Jobs tab.

Figure 8-2   Job Instances tab
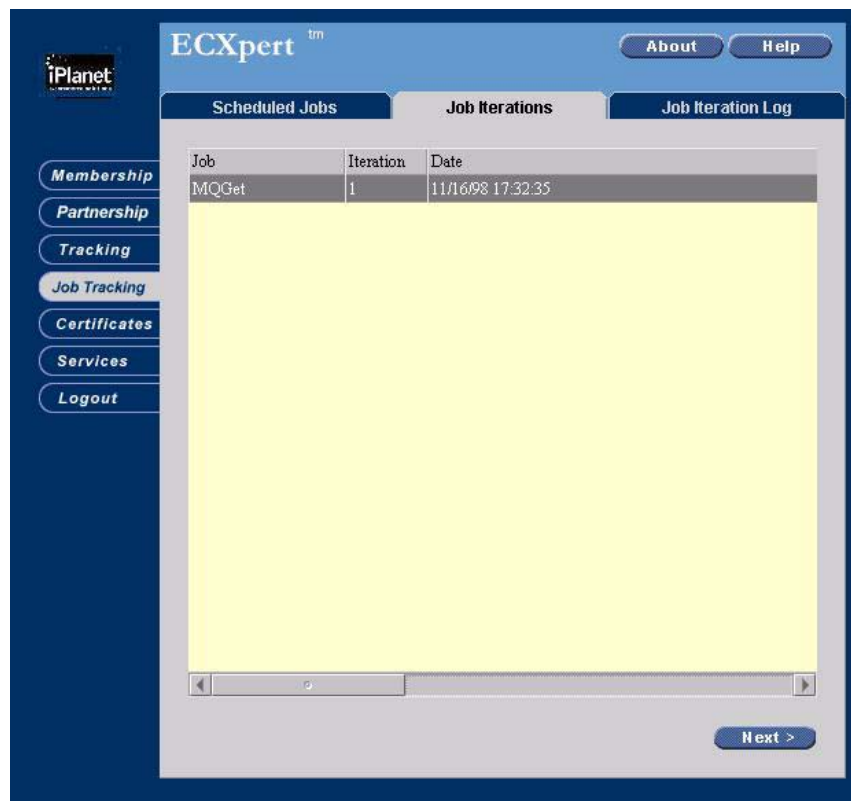
Table 8-2   Information on the Job Instances tab

Item	Description
Job	The job Name on the Scheduler screens.
Iteration	The number of the job iteration listed.
Date	The date and time that this iteration was run.

5. Locate the job instance you are interested in.

   Refer to Table 8-2 for a description of the information that is displayed. If a job instance has encountered an error, "Aborted" appears in the Message column.

6. Select the job instance for which you want to see more information.

   Click on the row for the job instance to select it.

7. Click Next.

   Figure 8-2 displays more detailed information for the job you selected on the Scheduled Jobs tab.

Working with the Job Instance Log Tab

The Job Instance Log tab displays detailed information for the specific instance of the job you selected on the Job Instances tab. Follow the steps below to work with the Job Instance Log tab.

1. Select a job instance on the Job Instances tab.

   Select a job instance for which you want to see more detailed information.

2. Click Next.

   The Job Instance Log tab is displayed (Figure 8-3) with more detailed information for the selected job instance.

Figure 8-3   Job Instance Log tab
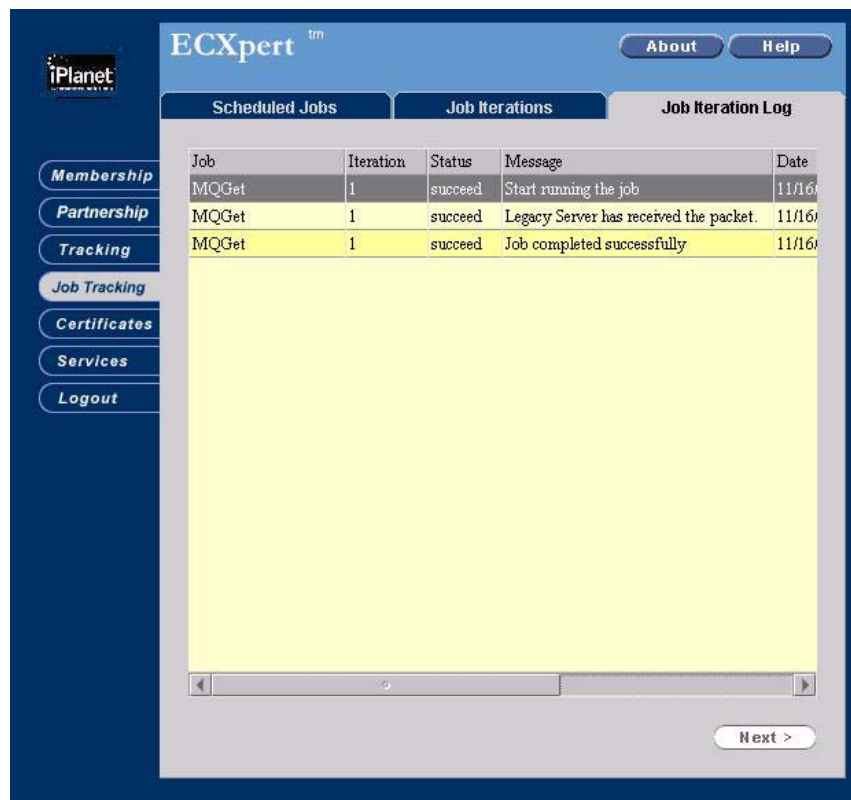
Table 8-3   Information on the Job Instance Log tab

Item	Description
Job	The Task on the main Scheduler tab.
Iteration	The number of the job iteration listed.
Status	The completion status of this iteration of the job. **Note:** This status refers only to the Scheduler's execution of the task; for status of processing of submitted documents, you would have to note the Tracking ID given in the Message column and search on it in the Tracking tabs.
Message	An abbreviated event log. Usually an error or routine completion message. The Tracking ID for data files submitted to ECXpert also appears here.

Table 8-3   Information on the Job Instance Log tab *(Continued)*

Item	Description
Date	The date and time that this iteration was run.

3. Examine the information displayed in the log.

   Refer to Table 8-3 for a description of the information that is displayed.

   If a job instance has encountered an error, a complete description appears in the Message column.

   Additional information about the Job Instance Log entries:

   ❍ If the job does not submit a data file to ECXpert, two entries appear for it in the log; a start entry and a stop entry.

   ❍ If a job submits a data file, a third line appears between the start and stop entries; this line shows the Tracking ID created in the Message column.

NOTE	**Note on Error rc-256:** If you see an error, "Job encountered error (rc-256)", it means that the executable for the job cannot be found.

4. Navigate to information on other jobs.

   From the Job Instances Log tab, you can go on to view detailed information on other instances of the same job, or summary information on other jobs.

To see information on…	Click this tab…	Continue with instructions at…
A different iteration of the same job	Job Instances	"Working with the Job Instances Tab" on page 416
A different job	Scheduled Jobs	"Working with the Scheduled Jobs Tab" on page 414

Working with Certificates

Whether you are using email or accessing web servers, ECXpert gives you the means to carry on secure communications. By using certificates, obtained either from ECXpert or certification authorities like the iPlanet Certificate Management System, ECXpert partners can use a number of messaging protocols and message formats to communicate over the internet in a secure manner. This chapter describes the tasks involved in working with certificates in ECXpert and covers the following topics:

- Principles of Security

- ECXpert security support

- Generating member certificates

- Exchanging certificates

- Managing certificates

If you are not familiar with the basic concepts of security, you should start by reading the first section, "Principles of Security." Otherwise, you should start with the section "ECXpert Security Support" on page 432.

Principles of Security

If the internet consisted of two networked computers, with data flowing directly between them, there would be no need for security schemes. In reality, however, the internet consists of a vast array of computers that are linked together. A message that is sent from one computer to another is routed through any number of intermediate links and each one of those links represents a security risk: a third party might read a private message, might change a message, or might misrepresent itself as a trusted partner.

Security techniques are used to avoid these problems in the following ways:

- By scrambling or *encrypting* a message, it is rendered unintelligible to a third party. The receiving party can unscramble or *decrypt* the message and read it.

- By sending a special message profile called a *message digest*, a sender can make sure that the receiver has a way of checking that the message has not been changed in transit.

- By having the sender sign a message using a *digital signature*, a receiver can obtain proof that the sender actually sent the message.

- By using *certificates* to authenticate the sender of a message, the receiver can be confident that a message originated where it claims to have originated.

This section examines each of these techniques in turn and then describes how libraries that implement security protocols use these techniques to support secure communications.

Encryption and Decryption

To encrypt data is to transform it in such a way that it is meaningless to anyone who does not know how it was transformed and therefore, cannot restore it to its original form. The means used to transform a message is called a *key*. There are two kinds of keys: symmetric and asymmetric. The following subsections explain how these keys work and the advantages of each scheme. Most security systems use both kinds of keys in their encryption schemes.

Symmetric Key Encryption

Keys used in symmetric key encryption are either identical or one key may be calculated from the other. Figure 9-1 on page 423 shows how symmetric key encryption works. The data sent is encrypted using the sender's key and decrypted using the receiver's key. While it is in transit, the data is scrambled and therefore inaccessible to any third party.

Symmetric keys are highly efficient: users may not experience any noticeable time delay as a result of the encryption and decryption process. However, the problem with symmetric keys lies in transmitting the key securely to the parties involved. It is certainly not secure to send a symmetric key over the network unless the key itself is encrypted, which raises the very problem the key is supposed to solve. What is the solution to this impasse?

There are a number of possibilities. For example, a courier could be charged to carry the key to the principals. But this would not be a practical solution for a high-volume of messages or for routine use. Another possibility is to use asymmetric key encryption to transmit the symmetric key over the wire, and then to use the symmetric keys for encrypting and decrypting the data itself. Asymmetric key encryption is described in the next section.

Figure 9-1   Symmetric Key Encryption
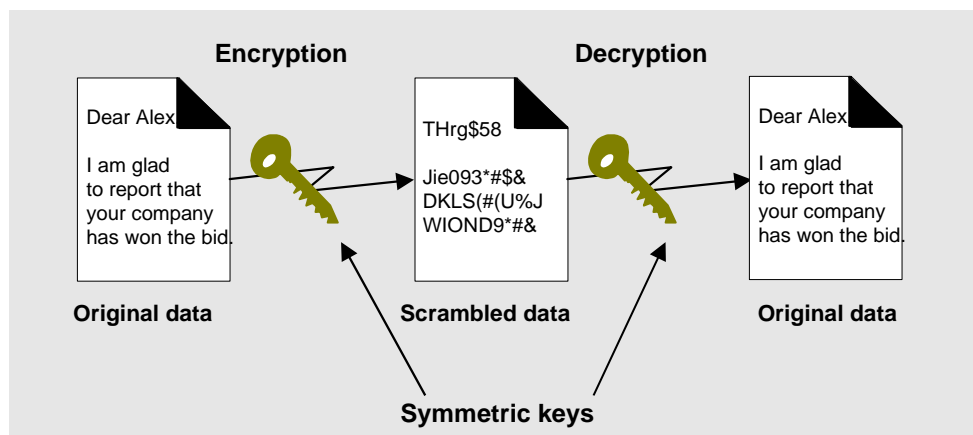
Asymmetric Key Encryption

Asymmetric key encryption, as its name suggests, depends upon the use of two keys, a public key and a private key, that are related in the following ways:

* one key can be used to decrypt a message that has been encrypted with the other key

* one key cannot be derived from the other; this is what makes them *asymmetric*

Before any data is transmitted, you send the public key over the wire to the party who wants to send the encrypted message. Because having access to one key does not give you the ability to determine the other key, sending the key over the wire does not compromise the security of future communication. Once the public key is received, the receiver can use it to encrypt data that he wants to send securely. When you receive the encrypted data, you use your private key to decrypt it. Figure 9-2 on page 424 shows how public and private keys are used to encrypt and decrypt data.

Figure 9-2   Asymmetric Key Encryption
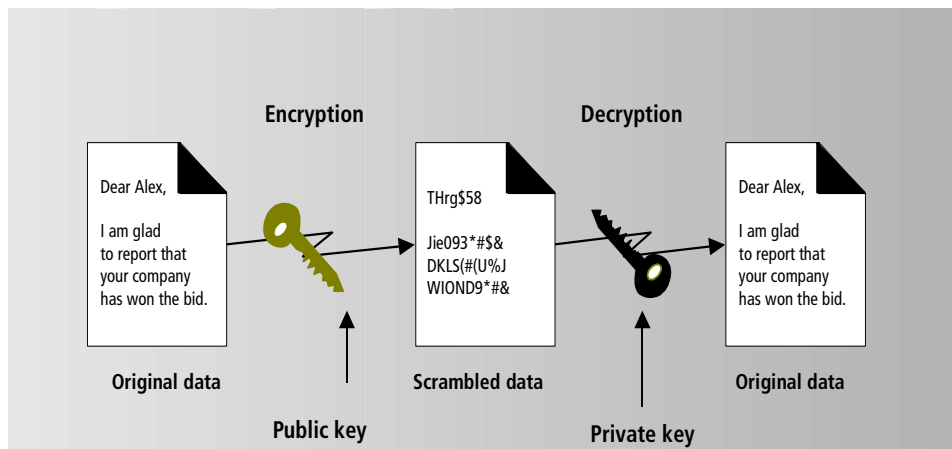
Of course, communication (secure or otherwise) is usually bidirectional. What this means is that the principals involved in a secure communication must both exchange public keys before they can transmit data securely:

• Principal A sends his public key to Principal B. B can now send secure messages to A. A uses his private key to decrypt them.

• Principal B sends his public key to Principal A. A can now send secure messages to B. B uses his private key to decrypt them.

The exchange of public keys is usually done through the exchange of certificates. For more information, see "Exchanging Certificates" on page 445.

Asymmetric Keys and Performance

One disadvantage in using asymmetric keys to secure communication is that asymmetric-key encryption is much more time consuming than symmetric key encryption. Thus it is best not to use this type of encryption for the main body of the message. However, public-key encryption can be used to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol.

Using Private Keys for Encryption

The scheme shown in Figure 9-2 can be reversed. That is, you can use your private key to encrypt data; the data can then be decrypted by someone who holds the corresponding public key. This is not ideal for secure data transmission because anyone holding the public key can decrypt your messages; however, you can use your private key to generate a digital signature. Client software, like

Communicator, can then use the public key to confirm that a message was signed with your private key. Because only one principal has a private key, Communicator can use this means to authenticate the originator of the message. The next section provides more information about digital signatures.

Message Digests and Digital Signatures

Message digests and digital signatures are two techniques that are implemented by security protocols to make sure that the data you receive has not been tampered with in transit and to confirm the identity of the signer.

When you send data using a secure protocol, the data is sent along with a message digest. To create the message digest, a hashing algorithm is applied to the data. The resulting digest is much smaller than the original document. The digest is then encrypted with the sender's private key; the encrypted digest constitutes a *digital signature.* (The digital signature also includes the hashing algorithm.) Figure 9-3 shows how this works.

Figure 9-3   Digital Signatures and Integrity
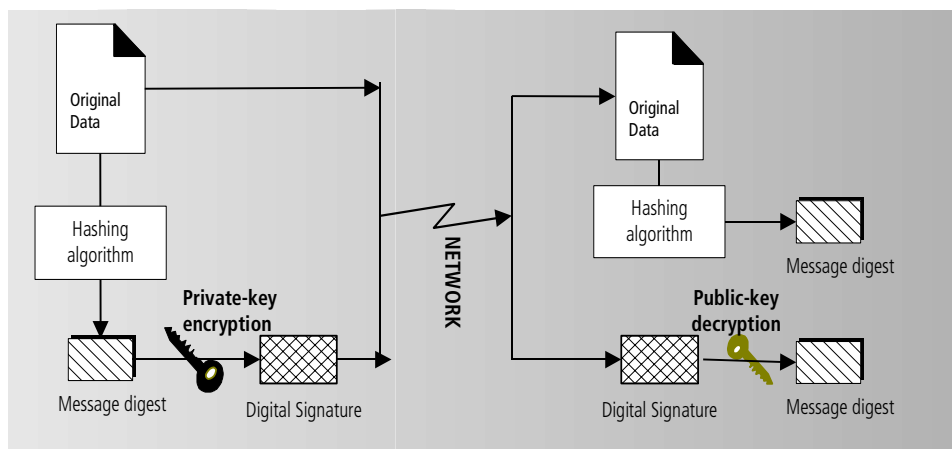
After the digital signature is created, the data and the digital signature are sent across the wire. In delivering the message, SSL does the following:

- It uses the signer's public key to decrypt the digital signature. This restores the message digest.

- It obtains the hashing algorithm from the digital signature and it applies this algorithm to the data it has received to create another message digest.

- It compares the two message digests. If they are the same, this means that the data has not been tampered with during transmission.

The use of digital signatures affects the legal standing of an electronic document as well as the security of data transmission. A digital signature carries legal guarantees that are comparable to those of a normal signature: it associates the signer with the signed document; it underlines the seriousness of the signer's intention; it is evidence of the signer's approval or authorization of the data; and it imparts finality to the transaction. In short, a digital signature gives the recipient legal proof of the sender's authenticity and the seriousness of her intent.

Certificates

The use of encryption, digital signatures, and message digests protects sensitive data from being read or tampered with by a third party, but it does not solve the problem of impersonation. For example, if you access a server over the internet to make a purchase, the server may send you a public key that you can use to secure a transaction, but how do you know that the server is who it represents itself to be? To solve this kind of problem, a certification authority (CA) issues a certificate that binds a distinguished name with a public key, guaranteeing that the principal issuing a public key is indeed who it is claiming to be. (A *distinguished name* is a standard way to identify a network entity.) Typically, when two principals want to have a secure communication over the net, the first step is to exchange certificates.

A certificate is the digital equivalent of a driver's license. Just as you know that a driver's license belongs to a person by looking at their picture, a server knows a public key belongs to a principal because a certificate says that it does. A *certificate* confirms the identity of the principal to whom it has been issued; it supports the principal's claim to ownership of a public key. That principal might be a client, a server, or any entity that can be found on a network.

Certificates are typically issued by a *certification authority*. A certificate

- identifies the principal to whom it has been issued

- provides the recipient with the public key of the principal to whom it is issued

- carries the digital signature of the certification authority that has issued it

Every certificate includes the information described in Table 9-1:

Table 9-1   Certificate Information

Field	Description
Version	Version number of the x.509 standard supported by the certificate
Serial number	The certificate's serial number. Every certificate issued by a certification authority has a unique serial number.
Public key information	A representation of the key and the algorithm used.
CA distinguished name	The distinguished name of the CA that issued the certificate.
Validity	The period during which the certificate is valid
The distinguished name of the certificate subject.	For example, in a client SSL certificate, this would be the user's distinguished name.
Extension	Additional information; for example, the type of the certificate: client, server, email, etc.
Signature information	The cryptographic algorithm used by the CA to create its own digital signature.
CA's digital signature	The signature obtained by hashing all the data in the certificate and encrypting with the CA's private key.

Certificates are either issued by an external certification authority or they are *self-signed*. Self-signed certificates are issued by ECXpert. Certificates bestow the same level of security against snooping whether they are issued by an external certification authority or not. However, certification authorities may offer, for an additional charge, additional guarantees as to the certificate owner's credit worthiness or other claims that interest you.

Certification Authorities

A *certification authority* (CA) is a trusted entity that issues and manages certificates. There are three ways that an organization can use certificate authorities when implementing a secure network:

• Use a public certification authority to issue each certificate.

   This is easy but expensive for a large network. Moreover, in a secure intranet you may not want to allow everyone that owns a certificate issued by a public certification authority to have access to your network.

- Allow a public certification authority to manage certificate issuance.

  This is a way of outsourcing certificate management. The CA will create special certificates and implement the security policies required by your organization. This approach is more cost effective.

- Use certificate-generating software to be your own certification authority.

  You can use ECXpert to generate your own certificates. If your partners trust this solution, it can be the simplest and cheapest method for implementing secure communications.

  For large networks or networks with specialized security requirements, it may be necessary to implement security systems using certificate servers, such as iPlanet Certificate Management System 4.1. This solution also requires establishing security policies and training personnel to implement these policies.

Getting and Validating Certificates

Any client (browser) or server that supports certificates maintains a collection of trusted CA certificates.These CA certificates determine which other certificates the client or server can trust. This means that security software can validate only the certificates that were issued by a CA whose certificate is known to the software.

A user can get certificates in any number of ways:

- The user can visit a CA web site and use that site to generate keys and obtain a certificate.

- The user can receive an email message that contains a certificate. (In Netscape Navigator you can check the People Certificates panel to view the certificates that were sent in email messages.)

- The user can also transparently collect a certificate when she connects to a web site offering an encrypted web page. (In Netscape Navigator, check the Web Sites panel to view all the site certificates you have collected.)

When the software attempt to use a certificate, it first checks to see that it has a valid certificate for the CA that issued the certificate.

Certificate Types

Certificates are issued in different formats, which are often referred to as *certificate types*. Since all certificates are a means of supporting Public Key Cryptography Standards (PKCS), their format is identified by a number appended to the PKCS acronym. For example, a request for a certificate uses the PKCS10 format.

ECXpert can handle the following two certificate types:

- Certificates in PKCS7 format. These certificates are exchanged by principals needing to use secure email. They can be generated by ECXpert (self-signed) or can be issued by the iPlanet Certificate Management System. In either case, they are stored in the Oracle database that is set up when you install ECXpert.

- Certificate requests in PKCS10 format. You can use ECXpert to generate certificate requests, which you then use to obtain certificates from certification authorities. For more information, see "Getting a Certificate from a CA" on page 438.

Certification Authority Hierarchies and Certificate Chains

A certification authority hierarchy is a means of delegating responsibility for issuing certificates to several related certificate authorities. For example, a large company may want to organize this hierarchy based on the kinds of certificates that are issued, on the regions where those certificates will be used, or on administrative policies used to manage certificates. Figure 9-4 shows a sample CA hierarchy.

Figure 9-4 Sample CA Hierarchy
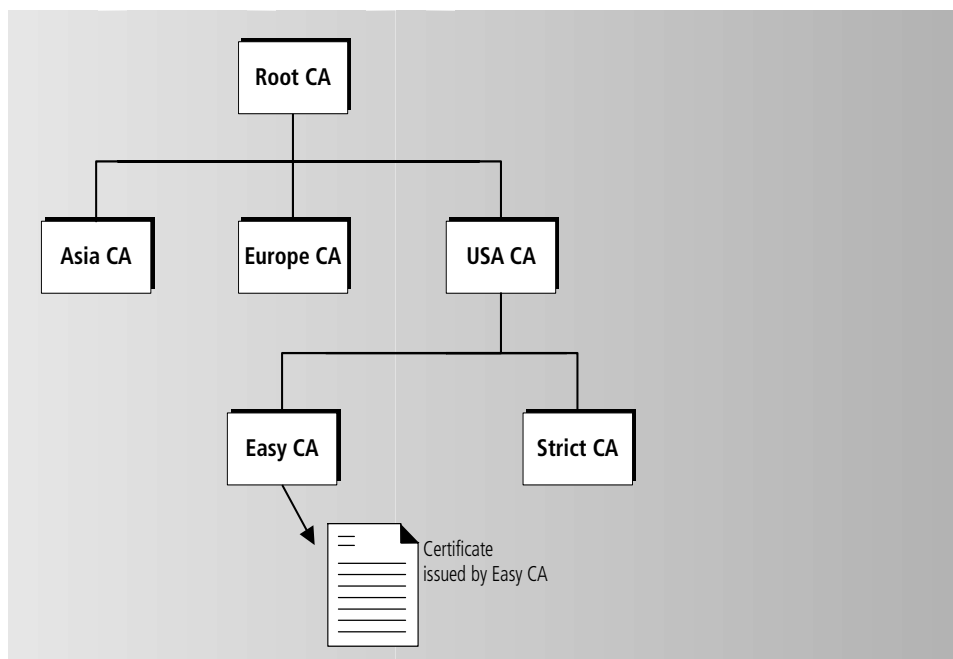
In this figure, certification authorities are organized first by location and then by the level of authentication (easy or strict). The top of the hierarchy is known as the root. The root's CA is a self-signed certificate. That is, the certificate is digitally signed by the root CA which the certificate also identifies. The CAs that are directly subordinate to the root have CA certificates signed by the root CA. The CAs that are subordinate to them have their certificates signed by the higher-level subordinate. For example, the certificates of Easy CA and Strict CA are signed by USA CA.

The hierarchy of the certification authorities are reflected in a parallel certificate chain, as shown in Figure 9-5.

Figure 9-5   Certificate Chains
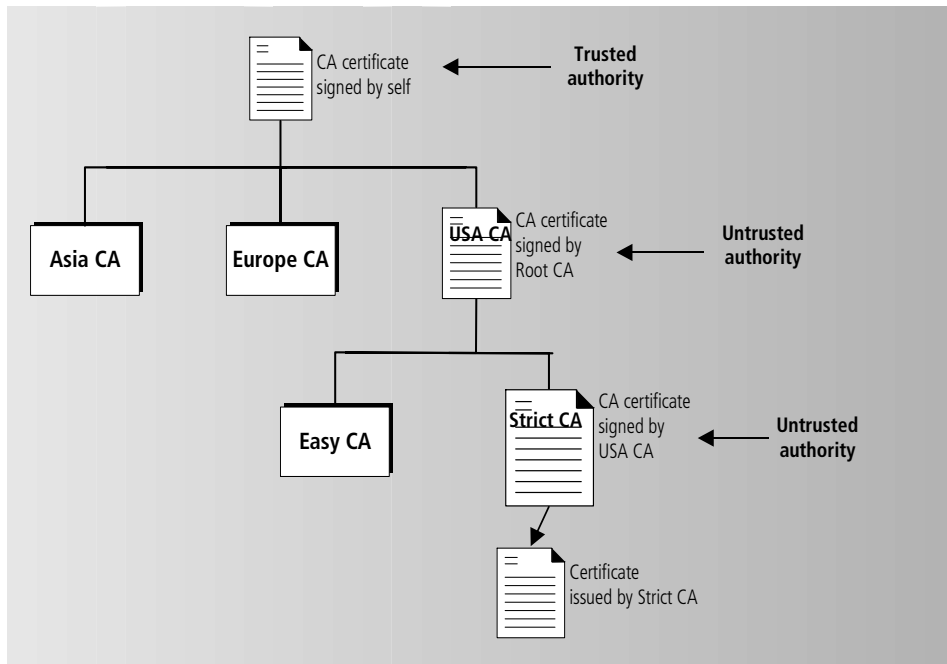
A *certificate chain* is a series of certificates issued by successive CAs. The chain traces a path from a branch in the hierarchy to the root. In a certificate chain, the following is true:

- each certificate is subordinate to the certificate of its issuer

- each certificate contains the distinguished name of its issuer which is the same as the subject name of the higher certificate in the chain. For example, in Figure 9-5 the certificate for Strict CA contains the distinguished name of the USA CA. The certificate for USA CA, in turn, contains the distinguished name of the root CA.

- each certificate is signed with the private key of the CA that issued it. The signature can be verified with the public key in the issuer's certificate, which is the next highest certificate in the chain. For example, in Figure 9-5 the public key in the USA CA certificate can be used to verify the USA CA's digital signature on the certificate for Strict CA.

If a network entity uses a certificate that is part of a certificate chain, the process of *certificate chain verification* is used to find whether that certificate is trustworthy. For example, Netscape software does the following when a certificate (in a chain) is presented for authentication:

1. The certificate validity period is checked

2. The issuer's certificate is located. The source might be in the verifier's local certificate database or in the certificate chain provided by the subject.

3. The certificate signature is verified using the public key in the issuer's certificate.

4. If the issuer's certificate is trusted by the verifier's certificate database, verification stops here. Otherwise, the issuer's certificate is checked to make sure it contains the appropriate reference to the subordinate certificate, and chain verification returns to step 1, but with the next higher certificate.

   For example, with respect to Figure 9-5, each certificate in the chain is processed as described above until the root certificate is reached which checks out as a trusted authority. If any certificate in the chain has expired, has an invalid signature, or is missing a certificate for the issuing CA, the authentication process fails.

ECXpert Security Support

ECXpert partners can use a number of messaging protocols and message formats to communicate over the internet in a secure manner. This section describes these services briefly; they include

- S/MIME over SMTP

    ECXpert can use email (SMTP protocol) to send messages to and receive messages from another SMTP host. Messages are in S/MIME format. See "Using Secure Email" on page 432 for more information.

- SSL

    A web server can communicate securely with ECXpert using the SSL protocol. See "Communicating Securely with a Web Server" on page 433 for more information.

- Secure FTP

    This service allows you to transfer files securely between ECXpert partners.

Using Secure Email

ECXpert can send a message in S/MIME format to an SMTP host. S/MIME is a standard for secure email based on asymmetric key cryptography.

When an email program that implements the S/MIME format sends a signed message (email), it adds an attachment consisting of a signature in PKCS7 format, a hash of the message, and a signed certificate. As explained in "Principles of Security" on page 421, these elements ensure that the communication is private, that it has not been tampered with, and that it cannot be repudiated.

Figure 9-6 shows how one client sends encrypted email to another using an SMTP host.

Figure 9-6   S/MIME over SMTP
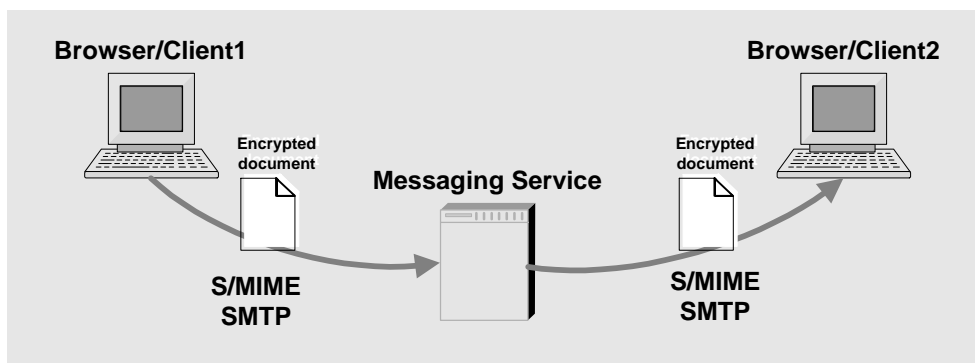
In Figure 9-6 either Client1 or Client2 could be ECXpert.

In order to use secure email, the administrator must make sure of the following:

*   The principals must obtain or generate certificates. See "Generating Member Certificates" on page 438 for more information.

*   The principals must exchange certificates. See "Exchanging Certificates" on page 445 for more information.

*   The principals must specify that they want to use public key encryption. See "Specifying Encryption" on page 452 for more information.

Communicating Securely with a Web Server

In the case where an ECXpert member wants to gain access to a secure web site, security is handled dynamically (transparently to the user and the administrator) by the SSL protocol.

The only requirement is that the web client have the certificate root for the web server being accessed. For information about getting a root certificate, see "Getting a Certificate for a CA" on page 436.

Figure 9-7 SSL Communication
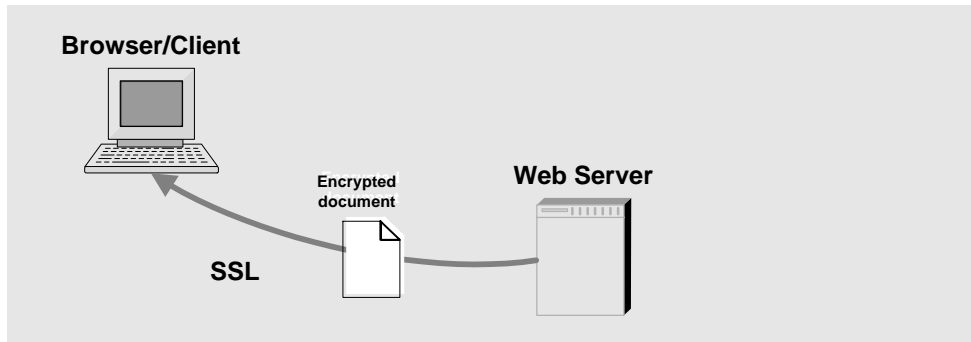
The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP. It uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client, it (optionally) allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

Working with the Certificate Administration Tab

The certificate administration tab is your interface to ECXpert's certificate administration options. It allows you to

- Generate self-signed certificates or certificate requests

- Import and export certificates

- List existing certificates

- Delete certificates

This section introduces the Certificate Administration graphical interface. The sections that follow explain how you use this interface to obtain, exchange, and manage certificates.

➤ **To display the Certificate Administration tab.**

1. Log into the ECXpert Product Administrative Interface.

2. Click Certificates on the left.

   The Certificate Administration tab is displayed as shown in Figure 9-8.

Figure 9-8 Certificate Administration tab

You can work with certificates by clicking on one of the buttons on the tab. The action of each button is described in Table 9-2.

Table 9-2 Certificate Administration tab buttons

Item	Description
Generate	Generate a self-signed certificate for a member or generate a certificate request.
List	List all root and member certificates in ECXpert.
Import	Import a certificate in text-file format for the member.

Table 9-2   Certificate Administration tab buttons *(Continued)*

Item	Description
Export	Export a certificate for a member to a file. This step is done after you generate a certificate. You can send this file as an email attachment. For more information, see "Exporting the Local Member's Certificate to the Remote Member" on page 446.
Delete	Delete a certificate for a member.

Getting a Certificate for a CA

There are two situations in which you need a certificate from a certification authority or root certificate:

- If a certificate you are importing is issued by a certification authority, you must also obtain and import a certificate for that authority. For example, if Principal R (a remote partner) sends a certificate to Principal L (a local partner), she must also send the root certificate for the certification authority that issued the certificate.

- If you are accessing a secure web site, you must have the root certificate for the web server you are accessing.

Currently, for members that are local to ECXpert, the only external certification authority that issues useful certificates is the iPlanet Certificate Management System (CMS). Remote members can also get certificates from Verisign and then send the local member such certificates, which are then imported into ECXpert. The Verisign root certificate is bundled with ECXpert. (The problem with local members obtaining certificates from Verisign is that ECXpert cannot process the PKCS12 format used to package the certificates. It can handle the certificates themselves, as for example, when importing a Verisign certificate obtained from a remote member.)

➤ **To get the root certificate and certificate chain for the CMS certification authority**

1. Navigate to the main screen of the iPlanet Certificate Management System.

2. Select the **Retrieval** tab.

3. Select **Import CA Certificate Chain**

4. Under **Administration**, click the radio button with the text

   ```
   Display the CA certificate chain in PKCS#7 for importing into a
   server.
   ```

5. Click the **Submit** button.

   This displays the encrypted text that is bracketed by the words

   ```
   ---Begin certificate---
   ```

   and

   ```
   ---End certificate----
   ```

6. Copy the encrypted text that is bracketed by these phrases and paste into an empty text file, for example `MyRootCA`.

   By default, ECXpert expects to find this file in the directory

   ```
   /.../ECXpert/certificates/import
   ```

   You can save yourself some typing by putting it there.

After obtaining the CA root and saving it in a file, you must import it into ECXpert as described next.

➤ **To import a CA certificate.**

1. Navigate to the **Certificates > Import** form.

2. For **Certificate Root Type**, select **New Root Certificate**.

3. Ignore the **Member Qualifier** field.

4. In the **Member ID** field, enter the name you want to assign to the root certificate.

5. In the **Certificate File Name** field, enter the name of the file into which you have pasted the certificate. If you have saved the file in a directory other than `/.../ECXpert/certificates/import`, you must specify the full path name. Otherwise, the leaf name is sufficient.

   Note: On Solaris, file names are case sensitive.

6. In the **Base 64 Encoded** field, select **Yes** or **No**.

   Examine the contents of the file in which you saved the certificate. If the certificate is encoded in ASCII, then select **YES**. If it's encoded in binary, select **No.**

7. Verify that the certificate was imported by clicking List in the Certificates tab. The certificate you imported should be shown in the list.

You are now ready to import any certificates that have been issued by the iPlanet Certification Management server. For instructions on how to get the NCM server to issue a member certificate, see "Getting a Certificate from a CA" on page 438.

Generating Member Certificates

You can generate certificates in one of two ways:

- Use ECXpert to create a certificate signing request (CSR) and send the CSR to a certification authority, who will issue a certificate in PKCS7 format.

- Have ECXpert generate its own certificate. This kind of certificate is called a self-signed certificate.

The following sections describe each of these options.

Getting a Certificate from a CA

In order to get a certificate from a CA, you must do the following:

1. Generate a certificate signing request (CSR).

2. Submit the request

3. Import the resulting certificate into ECXpert

This section describes these steps in detail.

➤ **To generate a certificate signing request**

   1. Display the Certificate Administration tab.

   2. Click **Certificates**.

      The Certificate Information tab is displayed.

   3. Click the **Generate** button.

Figure 9-9   Generate Certificate tab

4.   Fill out the fields as shown in Table 9-3.

Table 9-3   Information on the Certificate Information tab

Item	Description
Member ID	The member ID of the member to whom the certificate is assigned. Note that this member must already have a local (EL) email address.
Modulus Bit	Select the public/private key length for the S/MIME encryption algorithm. The options are: 512, 678, or 1024 (default is 1024).
Certificate type	Select **Certificate Signing Request**.

Table 9-3   Information on the Certificate Information tab *(Continued)*

Item	Description
Base File Name	The name of the file in which to store the certificate request. ECXpert adds the extension `.PKCS10` to the file name you enter.
	If you do not enter the full path here, this file is placed in the directory *$NSBASE*/NS-apps/ECXpert/certificates/export/
Member Qualifier	Specify **EL**: the trading address for the Member ID is a local email address.
	(You can only generate a CSR for a local member; the private key is generated when you create the CSR.)
Country Code	The two-character code for the country in which the member resides. This is based on the ISO 3166:1988 standard. See Internet Roadmap Codes from ISO 3166 for these codes.
State or Province	The state or province in which the member resides.
City	The city in which the member resides.
Company	The name of the company that employs the member.
Department	The department in which the member works.

5. Click **Generate** to create the CSR in the base file you specified above.

You are prompted, "Are you sure?," to confirm the certificate generation.

6. Confirm the certificate generation.

Click **Yes** to confirm the certificate generation and return to the Certificate Administration tab.

Click **No** to return to the Certificate Information tab. There you can make changes in the certificate information and resume at Step 2 above, or you can click Cancel to cancel the certificate generation entirely.

7. Open the file in which you have generated the CSR and copy its contents.

8. Navigate to the main screen of Netscape's Certificate Management System:

9. Select the **Enrollment** tab.

10. Select **Object Signing (PKCS10)**

    This displays a form on the right side of the window that you can use to enter information about the certificate you want.

11. In the **PKCS #10 Request** field, paste the contents of the file into which you generated the certificate request. Be sure that you do NOT include the `--Begin--` and `--End--` statements.

12. In the **Select Signing Type** field, enter

    `Netscape Object-Signing`

13. In the **Contact Information** field, enter your contact information.

14. Click **Submit** to submit your request.

The request is reviewed by a CMS agent. After the agent approves the request, you will receive information about the certificate via email. Specifically, the email contains the number of your certificate.

➤ **To import the certificate into ECXpert**

1. Navigate to the main screen of Netscape's Certificate Management System:

2. Select the **Retrieval** tab.

3. Select either **List Certificates** or **Search Certificates**.

4. Look for or search for the number of the certificate. This is the number specified in the certificate you received from Netscape in response to your certificate signing request.

5. Once you find the certificate, click on the **Details** button.

   A lengthy window is displayed showing you a lot of information about your certificate. At the bottom of the window, there will be two versions of your certificate: with and without the root CA chained to it. If you have already imported the root CA (), you will need the simpler version.

6. Copy the simpler version, selecting just the text bracketed by the BEGIN CERTIFICATE/END CERTIFICATE statements. Do not include the BEGIN CERTIFICATE/END CERTIFICATE statements.

7. Paste the text into an otherwise empty file.

8. Place the file into the `/.../ECXpert/certificates/import` directory.

9. Go to **Certificates > Import** to import the member's certificate.

10. In the **Certificate Root Type** field, select the name of the issuing CA.

11. In the **Certificate File Name**, specify the name of the file into which you pasted the certificate.

12. Click the **Import** button to import the certificate.

Next, to carry on secure communication, you must send the certificate to your trading partner by email or physical transfer (like a courier). It is not sent automatically by ECXpert. See "Exchanging Certificates" on page 445 for additional information.

Generating a Self-Signed Certificate

When ECXpert generates its own certificate, the certificate and private key are stored in the Oracle database. The certificate and the public key is also stored in the export directory so that we can send it to trading partners who need to send us encrypted data.

When ECXpert generates certificates, it creates two files, one with a .CERT extension and another with a .PKCS7 extension. CERT files contain self-signed certificates; the PKCS7 files contain certificate chains, that is, the member certificate plus any certificates needed to validate that certificate.

➤ **To generate a self-signed certificate**

1. Select the **Certificates** function.

   The Generate Certificate tab is displayed as shown in Figure 9-10 on page 443.

Figure 9-10   Certificate Information tab

Use the information listed in Table 9-4 to fill out the tab's fields.

Table 9-4   Certificate Information tab fields

Item	Description
Member ID	The member ID of the member to whom the certificate is assigned.
Modulus Bit	Select the public/private key length for the S/MIME encryption algorithm. The options are: 512, 678, or 1024 (default is 1024).
Certificate type	Select **Self-Issued Certificate** to issue an X.509-compliant certificate.
	Self-generated files by default use a .CERT filename. This format is also used when you export a certificate.
Base File Name	The name of the file in which to store the certificate or certificate request, as applicable. ECXpert adds the extension .PKCS7 to the file name you enter.
	If you do not enter the full path here, this file is placed in: *$NSBASE*/NS-apps/ECXpert/certificates/export/
Member Qualifier	Select **EL**: you can only generate a self-signed certificate for a local member.
Country Code	The two-character code for the country in which the member resides. This is based on the ISO 3166:1988 standard. See Internet Roadmap Codes from ISO 3166 for these codes.
State or Province	The state or province in which the member resides.
City	The city in which the member resides.
Company	The name of the company that employs the member.
Department	The department in which the member works.

2. Click Generate.

You are prompted, "Are you sure?," to confirm the certificate generation.

3. Confirm the certificate generation.

Click Yes to confirm the certificate generation and return to the Certificate Administration tab.

Click No to return to the Certificate Information tab. There you can make changes in the certificate information and resume at Step 2 above, or you can click Cancel to cancel the certificate generation entirely.

After generating the certificate, you must send it to your trading partner by email or physical transfer (like a courier). It is not sent automatically by ECXpert. See "Exchanging Certificates" on page 445 for additional information.

Exchanging Certificates

There are two ways for members to exchange certificates prior to using secure email:

- The two members can attach the certificates to email they send each other.

- The two members can send signed emails to each other.

  Each member receives a signed email: A signed email has the signing certificate containing the sender's public key, embedded in the signed email. ECXpert will automatically recognize and import the certificate (assuming it can chain the certificate to a root certificate if it is not self-signed) and associate it with the member that has the email sender's address.

This section describes each method in detail. Before proceeding however, please take a look at Figure 9-11. Note that all ECXpert members have both a local and remote address. Under this arrangement, ECXpert can generate a self-signed certificate (in PKCS7 format) for the EL addresses and import a iPlanet certificate or other CA-generated certificate for the ER address.

Figure 9-11   Local and Remote Email Addresses
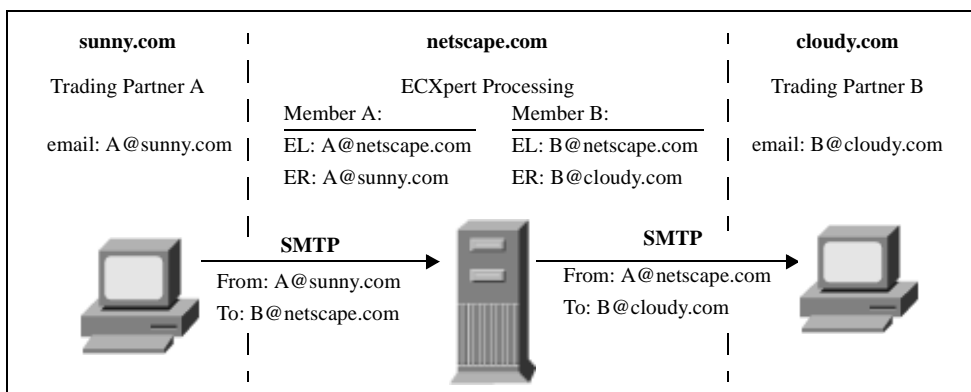
Attaching Certificates to Email

To exchange certificates using this method, you must complete the following steps. Note that *local member* refers to a member with a local (EL) address and r*emote member* refers to a member with a remote (ER) address.

- The local member exports his certificate to a file, attaches the file to an email, and sends the email to the remote member. For details, see "Exporting the Local Member's Certificate to the Remote Member" on page 446.

- The local member may need to import a certificate root from the certificate authority (CA) that generated the certificate it is importing. For more information, see "Getting a Certificate from a CA" on page 438.

- The remote mailbox attaches the remote certificate to an email and sends the email to the local member. The local member imports the certificate into ECXpert. For details, see "Importing the Remote Member's Certificate for the Local Member" on page 448.

NOTE	If you are trying to send an encrypted message to Communicator, you should use a key length of 40, 64, or 128 only.

Exporting the Local Member's Certificate to the Remote Member

Follow the steps below to send a local member's certificate to a remote member.

➤ **Export the local member's certificate.**

You can skip this procedure if you have just created a certificate for the local member and you know the Base File Name that you used.

1. In the Product Administrative Interface, use the Certificates function and click Export to display the List Certificates tab.

2. From the Existing Certificates list, select the certificate to export.

3. Click **Export** to display the certificate in the Certificate Information tab.

Figure 9-12   Exporting a Certificate

4. Fill in the information in the Export Information section at the bottom of the tab:

    Make sure you write down the value you use in the **Filename (no paths allowed)** field. ECXpert adds the extension .PKCS7 to the name you enter and stores the file in the directory:

    $NSBASE/NS-apps/ECXpert/certificates/export/

5. Make sure that the Base 64 Encoded check box is checked. Base 64 encoding is required if you are sending certificate data through SMTP Email to your trading partner.

6. Click Export to submit the information.

This exports the certificate to a file that can then be sent to a trading partner. You specified the name of the file in Step 4. The exported certificate is saved in two files (the raw encoding of the certificate with a .CERT extension, and the whole chain of the certificate to the root with the .PKCS7 extension) in the directory

> *$NSBASE*/NS-apps/ECXpert/certificates/export/

➤ **Send the certificate to the remote member.**

1. Using your email program, compose a message to the remote member's contact email address. Be sure to use the contact email address, not the trading address.

2. Attach the certificate file to the email.

3. Send the email.

NOTE	As an alternative, use any other means that is convenient and trustworthy to transport the certificate file, such as secure FTP or a diskette carried by hand.

Importing the Remote Member's Certificate for the Local Member

Follow the steps below to receive an remote member's certificate for a local member.

➤ **Receive the remote member's certificate via email.**

1. In your email program, open the email message that has the certificate file attached.

2. Save the attached file to disk.

If you save it in the *$NSBASE*/NS-apps/ECXpert/certificates/import/ directory at this point, you do not need to specify a directory in Step ‰.

3. Make sure the certificate file contains only the encoded certificate.

In a text editor, do the following:

❍ Open the certificate file that you just saved to disk.

❍ Look for unencoded header or trailer lines and, if you find them, delete them and save the file.

You are now ready to import the certificate into ECXpert.

➤ **To import the remote member's certificate into ECXpert.**

  1. In the Product Administrative Interface, use the Certificates function and click **Import** to display the Import Certificates tab (Figure 9-13):

  Figure 9-13 Import Certificates tab

  2. Select the desired Certificate Type as Member Certificate from the drop-down list.

  3. Select the Certificate Root Type for the certificate. This would be the name of the CA that issued the certificate or Self-Signed Certificate.

  4. For the **Member Qualifier** field, choose ER.

  5. For the **Member ID** field, you can use the drop-down list or type the member ID directly into the field.

6. Enter a value in the **Certificate File Name field**. If you already saved it in the *$NSBASE*/NS-apps/ECXpert/certificates/import/ directory, you do not need to specify a directory now.

   Nothing is appended to the file name. Be sure to enter the full file name, including the extension.

7. If the certificate root you are importing has been base 64 encoded, set Base 64 Encoded? to Yes. Otherwise, set it to No.

   If the certificate file was sent through email, the file is base 64 encoded. You can verify this by making sure that it contains only alphabetic and numeric characters.

8. Click **Import** to submit the information.

9. To verify that the import function was successful, you can list all of the certificates that are known to ECXpert.

Using the importCertificate Utility

As an alternative to using the Product Administrative Interface, ECXpert provides a command line utility for importing certificates. The importCertificate utility allows you to import a certificate from a file for an ECXpert member, or to import a new root certificate.

For more information on this utility, see .

Exchanging Signed Emails

The following sample procedure illustrates how you can exchange certificates by exchanging signed emails. It assumes the following:

• MemberR is an ECXpert member whose remote email address is MemberR@somewhere.com.

• MemberL is an ECXpert member whose local (ECXpert) email address is MemberL@ecxpert.com.

The next step is to obtain and exchange certificates.

➤ **The local member sends her certificate to the remote member**

1. Generate a self-signed certificate for MemberL.

1. Set up a partnership in ECXpert with MemberL as the sender, MemberR as the receiver, and the communications protocol as SMTP.

2. Configure the SMTP options to be "Signed Only," with both certification types as "Self-signed Certificate."

3. Set up a Service List containing only Outprep/Gateway.

4. Submit a file containing any text. ECXpert will generate the email; the email should be from `MemberL@ecxpert.com` to `MemberR@somewhere.com`.

   When the remote email client receives the email, it will automatically import the sender's (MemberL's) certificate.

➤ **The remote member sends his certificate to the local member.**

1. MemberR obtains a certificate from the iPlanet Certificate Server and imports it.

   See "Generating Member Certificates" on page 438 for details on this procedure.

2. Set up a partnership in ECXpert with MemberR as the sender and MemberL as the receiver.

3. Configure the Partnership Information screen by specifying Incoming SMTP options as "Signed Only." Specify both certificate types as "Self-Signed Certificate."

4. Have MemberR send an email addressed to `MemberL@ecxpert.com` (from `MemberR@somewhere.com`).

   When ECXpert receives the email, it will automatically import the certificate for MemberR.

Before these two members can exchange emails securely, they must specify that future emails be encrypted. See the next section for information on how this is done.

Specifying Encryption

You only need to specify that an outgoing message be encrypted if you are using one of the S/MIME protocols.

Once your trading partner has obtained your certificate, he can receive and decrypt the messages you send.

➤ **To specify that a message you send should be encrypted**

1. In the Product Administrative Interface, click the Partnership tab.

2. In the Partnership form, click the **Add** or **Change** button, depending whether you are newly defining or redefining a membership.

3. Choose the **Protocols** tab.

4. In the **Protocols** form, choose **SMTP** from the **Outgoing Protocol** drop-down list.

5. Set **Encryption and Authentication** to one of the following values:

   ❍ Encrypted Only—encryption without authentication

   ❍ Signed and Encrypted—both authentication and encryption

Managing Certificates

Managing certificates involves

- Listing existing certificates

- Determining the validity of certificates

- Deleting certificates that are no longer needed or are invalid

The following sections describe each of these tasks.

Listing Certificates

You need to list certificates to verify that import operations were successful, to check whether certificates have expired, or to determine what certificates are assigned to different members.

NOTE	If you are logged in as a regular member, you can see only your own certificates.

➤ **To list certificates**

1. In the Product Administrative Interface, choose the **Certificates** function.

2. Click the **List** button.

   The List Certificates tab is displayed, as shown in Figure 9-14.

   Figure 9-14   List Certificates tab
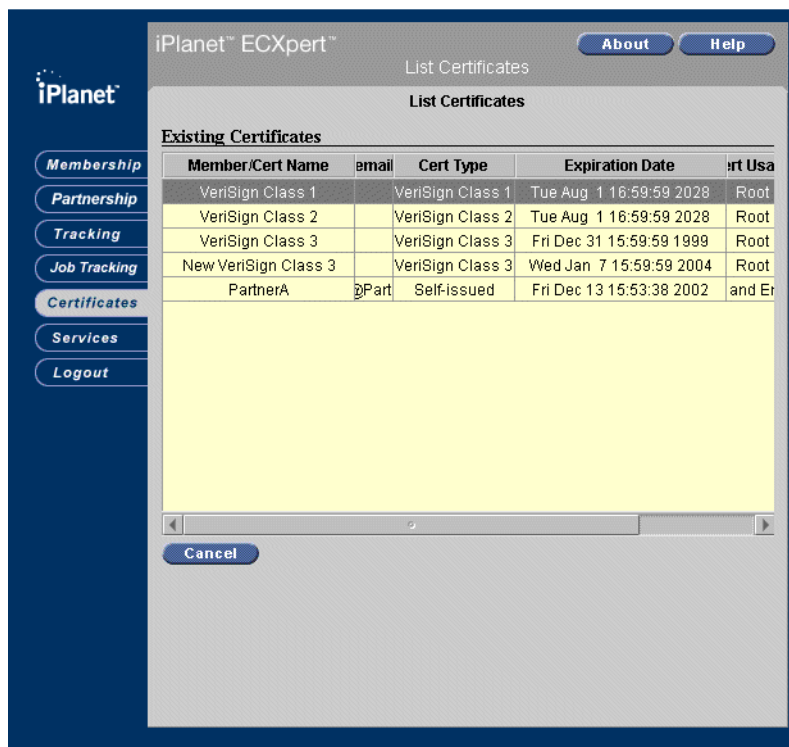
Table 9-5 describes the contents of each column in the certificates display.

Table 9-5   Information on the List Certificates tab

Item	Description
Member/Cert Name	The member ID of the member owning the certificate, or the name of the certificate if it is a root certificate.
email	The email address of the member owning the certificate (This entry is blank if the entry in Member/Cert column is a certificate name).
Cert Type	The certificate type: • self signed certificates • Other root certificates that are used to validate certificate issued by this root
Expiration Date	Expiration date and time for the certificate. When a certificate has expired, ECXpert automatically removes it from the certificate list and from its database.
Cert Usage	Possible uses for the certificate: • Root—to validate and chain certificates signed by this root. • Sign and Encrypt—for both signing and encryption. • Sign—for signing only. • Encrypt—for encryption only.

Determining the Validity of Certificates

Once a certificate has exceeded its period of validity, ECXpert automatically deletes that certificate from its database and from the list of certificates it displays. The administrator is responsible for making sure that certificates that have been revoked are also deleted.

A *certificate revocation list* (CRL) is list of certificates that have been revoked by the certificate authority (CA) that issued them and should no longer be accepted. CRLs are often sent out by Certificate Authorities, usually in a .PKCS7 file.

You can import a `.PKCS7` file containing a CRL just as you would import a certificate from that CA: simply use any member who has a certificate issued by that CA and select the certificate type corresponding to that CA to perform the import task.

ECXpert stores the embedded CRL in the database; all certificates from that CA are checked against that CRL before being accepted. ECXpert rejects any certificate that appears on a CRL that you have imported. ECXpert also checks whether any of the certificates issued by that CA has been revoked. If a certificate has been revoked, ECXpert deletes it from its database and from the list it displays.

Deleting Certificates

Follow the steps below to delete a certificate when it is no longer needed.

1. Display the Certificate Administration tab.

2. Click the **Delete** button.

   The List Certificates tab is displayed for the Delete Certificates task.

3. Select a certificate on the List Certificates tab.

4. Click **Delete**.

   A delete verification message is displayed.

5. Confirm the deletion.

   Click **Yes** to confirm the deletion. Click **No** to cancel the deletion.

Setting Up Services and Service Lists

This chapter describes the tasks involved in setting up and maintaining services and service lists in ECXpert. The following topics are covered:

- Overview

- Special Options with Service Lists

- Displaying the Service Administration Tab

- Displaying Information for an Existing Service

- Working with the Service Details Tab

- Adding a New Service on a Blank Form

- Copying a Service—Adding a Service Based on Another

- Changing the Information for a Service

- Deleting a Service

- Displaying Information for an Existing Service List

- Working with the Service List Details Tab

- Adding a New Service List on a Blank Form

- Copying a Service List—Adding a New Service List Based on Another

- Changing the Information for a Service List

- Deleting a Service List

Overview

What is a Service?

A *service* is an executable program file or script file used to perform a function on a submission unit or a subset of documents in a submission unit.

ECXpert provides standard services that are available as soon as the software is installed. ECXpert also supports custom, user-defined services to perform processing that is not provided by a standard service.

For information on creating custom services, refer to the *iPlanet ECXpert Developer's Guide* chapter on creating a custom service.

Table 10-1 describes the standard services provided by ECXpert.

Table 10-1   Standard ECXpert services

Service	Description
Parse	• Records information about a submission unit's incoming data for processing.
	• Verifies a received envelope's structure, along with its documents, and records the correctness of envelopes.
	• Notes the validity of all interchange, group and document envelopes, for incoming EDI; notes the starting position and size of every bounded (HREC through TREC) application record for incoming non-EDI.
	• Records the offset and sizes of all interchanges, groups and documents (or private application record sets) in the database Reconciles all incoming FAs (997), ARAs (999), and CONTRL messages with the previously sent documents.
	• Sets the correct state for each document so that translation will pick up only documents that are ready.

Table 10-1   Standard ECXpert services *(Continued)*

Service	Description
Translate	• Converts submission unit documents from one format to another.
	• Certifies the correctness of the document body.
	• Manages the execution of appropriate Mercator map program translation for both EDI and non-EDI data to translate data in one format to data in another format. To use the Translate service, you must select a Map in the Trading Partnership Information tab. (See "Working with the Partnership Info Tab" on page 266.) If you want to use FAgen, you must also use Translate.
	Note: If you are using a Mercator map, you must use the Translate service.
FAGen (incoming EDI)	Creates EDI acknowledgments in the formats: 997 (ANSI), 999 (UCS), and CONTRL Messages (EDIFACT). This service is only used when incoming data is EDI.
	These messages inform a user whether or not the document was received with any syntax compliance errors. If used, this service must follow Translate. This service can be in a Service List even if FAs are not requested. When this option is in a service list, a functional acknowledgment will be generated if specified by the trading partnership. If this option is not in the service list, a functional acknowledgment will not be generated even if specified in the trading partnership agreement. If the EDIFACT standard is used, a received interchange can include a request to generate a functional acknowledgment, which will be generated if FAgen is included in the service list, even if the trading partnership does not require functional acknowledgments.
OutPrep	Used when you want to submit a file to ECXpert to be forwarded (for example, to a VAN) without additional processing by ECXpert. This service marks the files as ready for the Gateway service. It is normally used either when using an external EDI translator so that the file is already ready to transmit and you plan to submit the transmission file to ECXpert with a service list including OutPrep and Gateway service, or when you are transferring proprietary data files to a trading partner and no translation is required. Do not use OutPrep with the Translate service.

Table 10-1 Standard ECXpert services *(Continued)*

Service	Description
Routing	Handles data when there are multiple output cards from a Mercator map. The Routing service specifies how to submit secondary output. It joins the secondary output transmission to a transport type and generates a new tracking ID. If your map produces multiple outputs, the Routing service must be used to submit the additional outputs. This service must be in a service list before you can fill in the Partnership Outputs tab. (See "Working with the Input XML Tab" on page 271.)
Split	Splits incoming submission unit into separate interchanges for subsequent processing by different service lists.
Gateway	• Manages any communications protocol supported by ECXpert for outbound communication • Triggers the sending of finished submission units to a trading partner • Triggers the sending of finished submission units to an internal application on a different computer or in a different directory If you use the Scheduler in the System Administration Interface, it is not necessary to use the Gateway service.

What is a Service List?

A *service list* is a collection of services to be performed on a submission unit.

All services are executed as part of a pre-defined service list. Service lists can be based on the data type being presented to ECXpert, or based on the sending and/or receiving member ID.

You can use an asterisk (*) as a wildcard for the Sender, Receiver, or Data Type for a service list. The list will then be used for all files that do not match one of the specific lists.

ECXpert controls executing each entry in the service list. If there is no service list defined that matches the file, the file is registered in the database, but no transactions are executed on the file and it is not processed through ECXpert.

NOTE   If a service list is to be used in conjunction with data files that represent information to be routed to more than one output (for example, sales data to the sales department, accounting data to accounting, items ordered data to manufacturing, and so on), each of the data parts must have its own service list controlled by the Routing Service and the Outputs tab.

Make sure that the Gateway service appears only once in all of the service lists for all of the related data parts.

If you use the Scheduler in the System Administration Interface, it is not necessary to use the Gateway service.

Some examples of possible service lists are:

*   **EDI to Application translation** (Default Inbound * * EDI list shipped with ECXpert) This is an example of a service list used to convert inbound EDI data to application data. The service list contains the following services:

    ❍   Parse

    ❍   Translate

    ❍   FAGen

    ❍   Gateway

    NOTE   This list should never contain OutPrep.

- **Application to EDI translation** (Default Outbound * * EDI list shipped with ECXpert) This is an example of a service list used to convert application data to outbound EDI data. The service list contains the following services.

  ❍ Parse (not necessary if you send delimited application data)

  ❍ Translate

  ❍ Gateway

NOTE	This list should never contain OutPrep.

- **Application to Application translation. This service list contains the following services:**

  ❍ Translate

  ❍ Gateway

- **Application data with no translation. This service list contains the following services:**

  ❍ OutPrep

  ❍ Gateway

Importing Service Data from a Text File

You can use the ECXpert `import` utility when you want to import a batch of records instead of entering the information for each service through the ECXpert user interface.

For details on using the ECXpert `import` utility, see "import—Importing Records for Members, Partnerships, or Service Lists" on page 494.

NOTE	This list should never contain OutPrep.

Changes made to the database through the import utility are not visible to a user of the Product Administrative Interface until the user logs out and logs in again.

Guidelines for Combining Services

Many standard ECXpert services can only be used in certain situations, or have dependencies on other services, which requires upfront planning on your part. The following is a summary of guidelines to observe when combining standard services into a service list:

- Never repeat any standard Service in a Service List.

- Parse must be followed immediately by Translate or Split.

- Gateway cannot be used alone; as a minimum it must be preceded by OutPrep.

- When you use Routing for secondary outputs, you might *not* need Gateway in the same Service List with Routing -- Gateway would appear in the Service Lists for each of the secondary outputs.

  If Gateway is to send the first output of the map, Gateway would appear in the same Service List with Routing.

- Routing must always be before FAGen, never after.

- Use Split when you want to split the documents within a submission unit into separate submission units, each of which is then processed by a Service List determined by document-level data.

- Split should only be used after Parse. A Service List containing Split would have only Parse, then Split as the Services.

- Use Parse to prepare for document-level translation of EDI and HREC files. Parse reads the submitted file and records in the database the offsets of each interchange, group, document (or in the case of an incoming HREC file, each application set). Translate can then use this information to do document-level translation, rather than file-level translation of the submitted file.

For additional information on using different combinations of services to achieve the results you want in different situations, see the following topics:

- All of Chapter 2, "Scenarios for Using ECXpert"

- *iPlanet ECXpert Operations Reference Guide*, "ECXpert Operations" chapter, "Understanding Document Workflow" heading.

Special Options with Service Lists

Fine-tuning Parse and Trouble-shooting Your Map

Parse uses a text file called *$NSBASE*/NS-apps/`ECXpert/maps/parser.res` plus additional restrictions written into the code itself to validate the contents of a file. Parse has trace file called `/tmp/parser.trace`.

For more detailed information on using the `parser.res` and `parser.trace` files, see the *iPlanet ECXpert Operations Reference Guide*.

Two special parameters in the `ecx.ini` file allow you to optimize Parse performance:

- In the `[parse]` section, the **dbUpdaterArraySize** parameter controls the behavior of Parse. Increasing the value for **dbUpdaterArraySize** tends to speed up Parse. Always set it to a value less than or equal to the value for the `[DB_SECTION]` parameter **DB_ARRAY_SIZE**.

- In the `[DB_SECTION]` section, the **DB_ARRAY_SIZE** parameter controls the database API behavior (event log, bdgdocument, bdginterchange, etc.). Increasing the value for **DB_ARRAY_SIZE** tends to speed up Parse.

Processing Secondary Outputs

If your map generates more than one output card, you must specify the service lists to use on each of the additional outputs. This provides flexibility in processing different parts of the same input document in different ways.

To set up secondary output processing first create a map that generates more than one output card. Then specify this map on the Partnership Info tab (Figure 6-5 on page 267), causing the Outputs tab (Figure 6-8 on page 280) to be displayed. On the Outputs tab specify the service lists to use to process the additional outputs.

See "Working with the Input XML Tab" on page 271 for more information.

Using the Split Service

In previous versions of ECXpert, all documents within a single incoming file were processed by a single service list. The Split service allows ECXpert to process different documents from a single incoming file with different service lists, with each document having its own Tracking ID.

The Split service requires the Parse service to first parse an incoming file to determine the document boundaries. Split then creates a separate submission unit for each document, resubmitting each to ECXpert with its own Tracking ID. ECXpert then processes these documents with the appropriate service list, based on each document's Sender, Receiver, and Document Type.

NOTE	Split is the only ECXpert service that does not require a supporting partnership to be set up. It is executed based solely on the Sender, Receiver, and Service List Data Type in the service list that you set up matching the Sender, Receiver, and Document Type of the incoming data file.

Task List for Using Split

Using the Split service involves the following tasks:

1. In the ecx.ini file, [Split] section, set the following parameters:

    ❍ Set **submissionDocType** to the Document Type that the Split service is to assign to the individual documents that it Splits out of the original file.

    This setting, together with the individual document's Sender and Receiver, determines the service list that is used to process a document after it has been Split out of the original file.

NOTE	**submissionDocType** is a *global* setting that applies to *all* ECXpert processing.
	Using **EDI** here allows the post-split documents to be processed by the */*/EDI service list, which allows the individual documents to have different specific EDI document types, such as 850.
	Using a more specific Document Type here would greatly restrict the types of documents that could be Split and processed.

❍ Set **maxThreads** less than or equal to the value specified for **worker_max_threads** in the [dispatcher] section.

If this is absent or set to 1, the Split service submits the files in the input file serially. If this is greater than 1, Split spawns a maximum of maxThreads threads, with each thread used for re-submitting one document. A semaphore is used to control the number of threads.

If the maximum number of threads is reached and there are re-submissions pending, these are placed in the queue waiting for available threads.

❍ Optionally, set **workdir** to a particular directory where work files are to be generated and deleted (for example, */tmp*). The installation sets this to:

$NSBASE/NS-apps/ECXpert/data/work

2. Create a service list for Split:

❍ Set **Service List Data Type** to a unique name, such as **To_Be_Split**

CAUTION	The name for the Service List Data Type *must not match* the value set for **submissionDocType** in the [Split] section of the ecx.ini file.
	If the two names are the same, ECXpert processing goes into an endless loop, with the separate documents produced by the Split service list being re-submitted to the Split service list over and over again.

❍ **Set Sending Member ID** and **Receiving Member ID** as necessary to cover those partnerships that need to have their submission units Split

3. Create partnership(s) to support processing of the documents after they have been Split.

❍ Set **Sender** and **Receiver** to the true Sender and Receiver in the file

❍ Set **Document Type** to the true Document Type in the file

NOTE	You set up these partnership(s) exactly as you would if the documents produced by Split were submitted directly to ECXpert.

4. Create service list(s) as necessary to support processing of the documents after they have been Split:

   ❍ Set **Sender** and **Receiver** as needed

   ❍ Set **Service List Data Type** to the true Document Type in the file

NOTE	Set up these service list(s) exactly as you would if the documents produced by Split were submitted directly to ECXpert.

5. Submit to ECXpert to be processed initially by the service list for Split:

   ❍ Set **Sender** and **Receiver** as needed

   ❍ Set **File Type** to the same value you specified for **Service List Data Type** in Step 2 (**To_Be_Split**, in our example). This *must match* the value of the special service list that contains Parse, Split.

After you have submitted to ECXpert, the special service list for Split is executed. The Parse service logically splits your submission unit into separate documents (the original file is not changed or copied), and then Split resubmits each one to ECXpert with its own Tracking ID.

ECXpert then processes each document with the appropriate service list, based on the Sender, Receiver, and Document Type that match what you set for the **submissionDocType** parameter in the [Split] section of the ecx.ini file.

Prioritizing Service Lists for Execution

A service list can be executed by priority or it can be scheduled by the ECXpert Scheduler. From the Priority list box on the Service List Detail tab of the Product Administration Interface (Figure 10-5 on page 481), you can prioritize or schedule the processing of a service list by selecting:

- high priority, medium priority, low priority, or

- scheduled

Scheduled jobs can also be administered from the Scheduler tab of the Server Administration interface. Refer to "Adding a New Task" on page 157 for more information.

How Files in Service Lists are Processed by Priority

When prioritizing service lists for execution, the *fifo_interval* parameter in the "[tcpip-connector] Section" on page 573 of the ecx.ini file controls how many files are processed in priority order before one file is processed in first in, first out (FIFO) order (irrespective of priority). The following example describes how priority processing can be applied in a business document processing environment for three jobs.

The fifo_interval is set to 500

Job 1 contains 2500 files and is set to priority low

Job 2 contains 3000 files and is set to priority medium

Job 3 contains 5000 files and is set to priority high

The jobs enter the processing queue in numeric order.

Priority Processing occurs as follows:

When the tcpip-connector passes job 2 to the dispatcher, job 2 takes priority over job 1 until the 500th file is processed. Then, one file is processed from job 1 and processing continues with job 2.

When the tcpip-connector passes job 3 to the dispatcher, job 3 takes priority over jobs 1 and 2. When the 500th job 3 file is processed, one file from job 1 is processed next and then priority reverts to job 3 again until its next 500 files are processed. Job 2 files remain on hold in the queue until job 3's files complete processing.

Note that in this simple example we used a large amount of files for Job 1. If job 1 had less than 10 files, processing of job 1 would complete before job 3, thereby moving job 2 into the 'one file processed for every 500 job 3 files processed' category.

Creating User-defined Custom Services

To supplement the standard services that are included with ECXpert, you can create user-defined services to perform processing such as custom encryption or compression.

For information on creating user-defined services, refer to the *iPlanet ECXpert Developer's Guide* chapter on defining custom services.

Using Exit Service Lists

For any service list, you can specify an *exit service list* to be used only if the first service list fails to complete. The exit service list is set up in the same way as a "normal" service list, but you design it specifically to perform processing when a particular service list fails.

Error services are added to the ECXpert 3.5 release. When an error service is used, an exit service list is called upon the discovery of a processing error within the scope of the error service's error severity setting. These services are described further in the section "Error Services" on page 50.

Specify the exit service list on the Service List Details tab (Figure 10-5 on page 481). See "Working with the Service List Details Tab" on page 481 for more information.

In general, an exit service list includes one or more custom user-defined services that perform some special processing or send an e-mail message notifying someone about the error condition.

For more information on user-defined services, refer to the *iPlanet ECXpert Developer's Guide* chapter on defining custom services.

Using Parameters for Services within Service Lists

When you create a custom service, you are able to pass parameters between the custom service and the services immediately preceding and following it. This allows your custom service to integrate very closely with the service list processing flow.

For more information, refer to the *iPlanet ECXpert Developer's Guide* chapter on defining custom services.

Using Pre-communications Services

A pre-communications service is a custom service that is executed immediately before a submission unit that has completed processing is sent to the receiving member by an ECXpert communications agent. A pre-communications service typically performs functions like data compression or encryption.

Specify a pre-communications service on the Protocols tab; see "Working with the Protocols Tab" on page 314 for details.

For more information on creating a custom service, refer to the *iPlanet ECXpert Developer's Guide* chapter on defining custom services.

Displaying the Service Administration Tab

Follow the steps below to display the Service Administration tab.

1. Log into the ECXpert Product Administrative Interface.

2. Click Services.

    The Service Administration tab (Figure 10-1) is displayed.

    From this tab you add, change, and delete services and service lists.

Figure 10-1   Service Administration tab
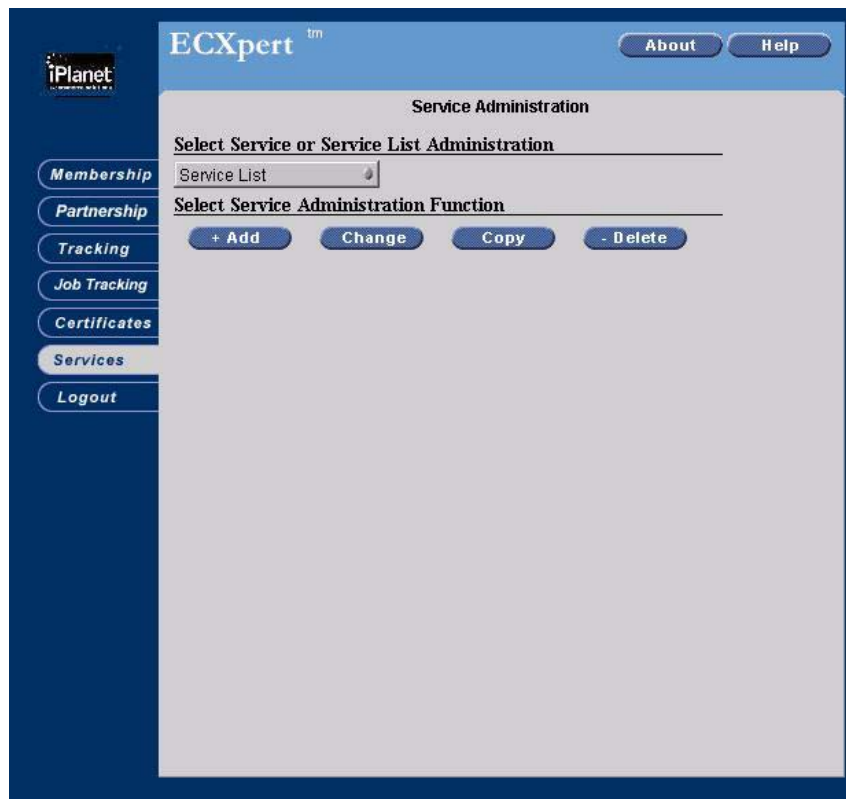
Table 10-2   Information on the Service Administration tab

Item	Description
Select Service or Service List Administration	Your selection from the drop-down list determines whether the operations below involve a service or service list.
Add	Add a new service or service on a blank form.
Change	Change an existing service or service list
Copy	Add a new service or service using an existing service or service list as a template.
Delete	Delete an existing service or service list

3. Select Service or Service List Administration.

From the Select Service or Service List Administration list, select either Service or Service List.

4. Select the task you want to perform.

Click Add, Change, Copy, or Delete. Continue as indicated in the following table:

Function	For more information, see...
Service (Service selected in drop-down list)	
Add	"Adding a New Service on a Blank Form" on page 476
Change	"Changing the Information for a Service" on page 477
Copy	"Copying a Service—Adding a Service Based on Another" on page 476
Delete	"Deleting a Service" on page 478
Service List (Service List selected in drop-down list)	
Add	"Adding a New Service List on a Blank Form" on page 484
Change	"Changing the Information for a Service List" on page 485

Function	For more information, see...
Copy	"Copying a Service List—Adding a New Service List Based on Another" on page 484
Delete	"Deleting a Service List" on page 486

NOTE	When you add a new service or service list on a blank form, you enter all the information yourself. For all other tasks you can perform from this tab, you must first display the information for an existing service or service list.
	If you are working with services, see "Displaying Information for an Existing Service," below for details.
	If you are working with service lists, see "Displaying Information for an Existing Service List" on page 479.

Displaying Information for an Existing Service

When you add a new service on a blank form, you enter all the information yourself. For all other tasks available from this tab, you must first display the information for an existing service.

Follow the steps below to display information for an existing service.

1. Display the Service Administration tab (Figure 10-1).

2. Specify Service Administration.

From the Select Service or Service List Administration list, select Service.

3. Click the task you want to perform.

Click one of the following:

❍ **Copy**—to add a new service using another service as a template

❍ **Change**—to change information for an existing service

❍ **Delete**—to delete an existing service

The Select Service tab (Figure 10-2) is displayed.

Figure 10-2 Select Service tab
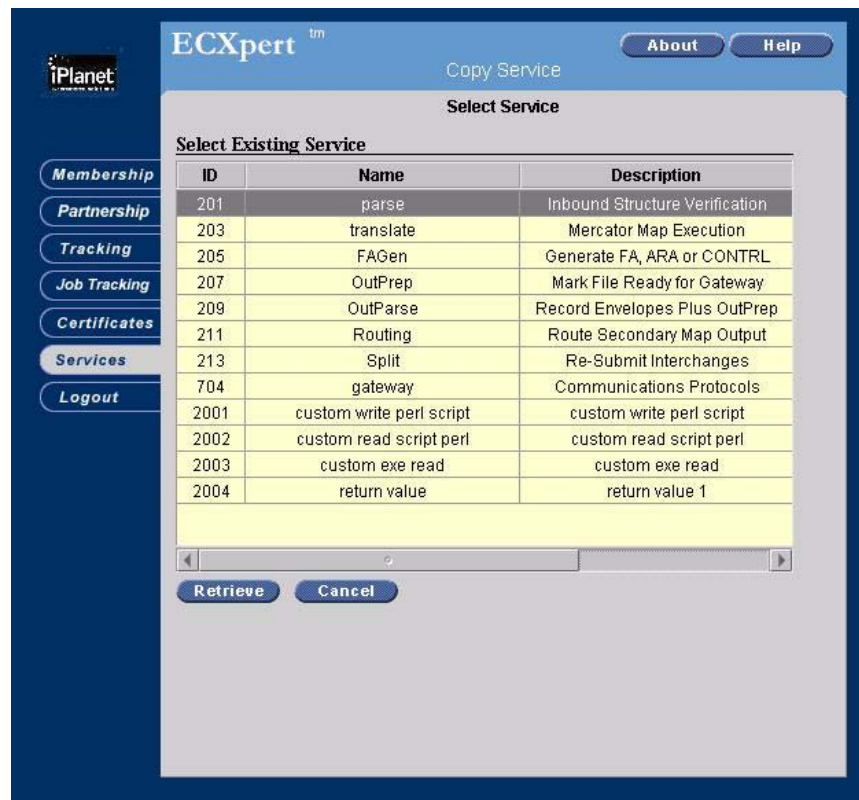
Table 10-3 Information on the Select Service tab

Item	Description
ID	Service identifier.
Name	Name of the service.
Description	Description of what the service is used for.

4. Select a service.

Click in the row for the service you want to select.

5. Click Retrieve.

The information for the selected service is displayed on the Service Details tab (Figure 10-3).

Working with the Service Details Tab

The operations to add, copy, and delete service lists all use the same Service Details tab. The Service Details tab appears in the different forms for each of these operations.

Follow the steps below to work with this tab.

1. Fill in or change information on the tab.

Refer to Table 10-4 for details on the specific fields.

Figure 10-3 Service Details tab

Table 10-4   Service Details tab

Item	Description
Service Name	A service name can contain as many as 60 characters. It can contain letters, numbers, and special characters, and is case-sensitive.
Service Type	Select Executable or Script.
Path Name	The full path to the service executable or script. (See note following this table.)
Additional Parameters	Parameters required for the executable.
Maximum Threads (1-99)	The maximum number of threads allowed for the service.
Service Description	A text description of the service.

NOTE	Enter your path carefully. The system does not check for accuracy of the path until the Dispatcher attempts to run the executable or script defined for this custom service.

2. Save your work.

A "completion" button always appears at the bottom of the Service Details tab.

This button has the same name as the one you clicked to begin the current task: Add, Change, Copy, or Delete. The task is not completed until you click this button.

For Delete, this button deletes the service. For the other operations, this button saves the information for the service.

NOTE	You can click Cancel at the bottom of the Service Details tab at any time if you decide not to complete the task.

Adding a New Service on a Blank Form

Follow the steps below to add a new service on a blank form.

If you want to add a new service by editing the information for an existing service, see "Copying a Service—Adding a Service Based on Another."

1. Display the Service Administration tab (Figure 10-1).

2. Click Add.

   The Service Details tab (Figure 10-3) is displayed.

3. Fill in the information on the Service Details tab.

4. Save the information for the service.

   Click Add at the bottom of the Service Details tab.

NOTE	Click Cancel at the bottom of the Service Details tab if you decide not to add the new service.

Copying a Service—Adding a Service Based on Another

When the information for a new service that you are adding is similar to the information for an existing service, you can save data entry time by using that existing service as a template for the new service. Follow the steps below to do this.

To create a new service without using another service as a template, see "Adding a New Service on a Blank Form" on page 476.

1. Display the Service Administration tab (Figure 10-1).

2. Click Copy.

   The Select Service tab (Figure 10-2) is displayed.

3. Select the service to use as a template.

   See "Displaying Information for an Existing Service" on page 472 for details.

4. Click Retrieve.

   The Service Details tab (Figure 10-3) is displayed.

5.   Make necessary additions and changes.

Refer to "Working with the Service Details Tab" on page 474 for details on specific fields on the Service Details tab.

6.   Save the information for the service.

Click Copy at the bottom of the last tab in the Service Details tab.

NOTE	You can click Cancel at the bottom of the Service Details tab if you decide not to add the new service list.

Changing the Information for a Service

Follow the steps below to change information for a service.

1.   Display the Service Administration tab (Figure 10-1).

2.   Click Change.

The Select Service tab (Figure 10-2) is displayed.

3.   Select the service to change.

See "Displaying Information for an Existing Service" on page 472 for details.

4.   Click Retrieve.

The information for the selected service is displayed in the Service Details tab (Figure 10-3)

5.   Make necessary additions and changes.

Refer to "Working with the Service Details Tab" on page 474 for details on each item of information on each of the three tabs.

6.   Save the information for the service.

Click Change at the bottom of the Service Details tab.

NOTE	You can click Cancel at the bottom of the Service Details tab if you decide not to change the information for the service.

Deleting a Service

Follow the steps below to delete a service.

1. Display the Service Administration tab (Figure 10-1).

2. Click Delete.

The Select Service tab (Figure 10-2) is displayed.

3. Select the service to delete.

When you click Delete on the Select Service tab, you are prompted to view the information before deleting. Your options are as follows:

  ❍ Yes—display the information for the service on the Service Details tab before deleting.

  ❍ No—delete the service immediately, without further confirmation.

  ❍ Cancel—return to the Service Administration tab without deleting the service or displaying the information.

4. Click Yes.

The information for the service you have selected to delete is displayed in the Service Details tab (Figure 10-3).

5. Examine the information.

Be absolutely certain that you are deleting the correct service.

6. Delete the service.

Click Delete at the bottom of the Service Details tab.

NOTE	You can click Cancel at the bottom of the Service Details tab if you decide not to delete the service.

After clicking Delete, you are prompted, "Are you sure?" Click Yes to confirm the deletion.

NOTE	You can still click No to cancel the deletion at this point, but this is your last chance.

Displaying Information for an Existing Service List

When you add a new service list on a blank form, you enter all the information yourself. For all other tasks available from this tab, you must first display the information for an existing service list.

Follow the steps below to display information for an existing service list.

1. Display the Service Administration tab (Figure 10-1).

2. Specify Service List Administration.

From the Select Service or Service List Administration list, select Service List.

3. Click the task you want to perform.

Click one of the following:

❍ **Copy**—to add a new service list using another service list as a template

❍ **Change**—to change information for an existing service list

❍ **Delete**—to delete an existing service list

The Select Service List tab (Figure 10-4) is displayed.

Figure 10-4 Select Service List tab
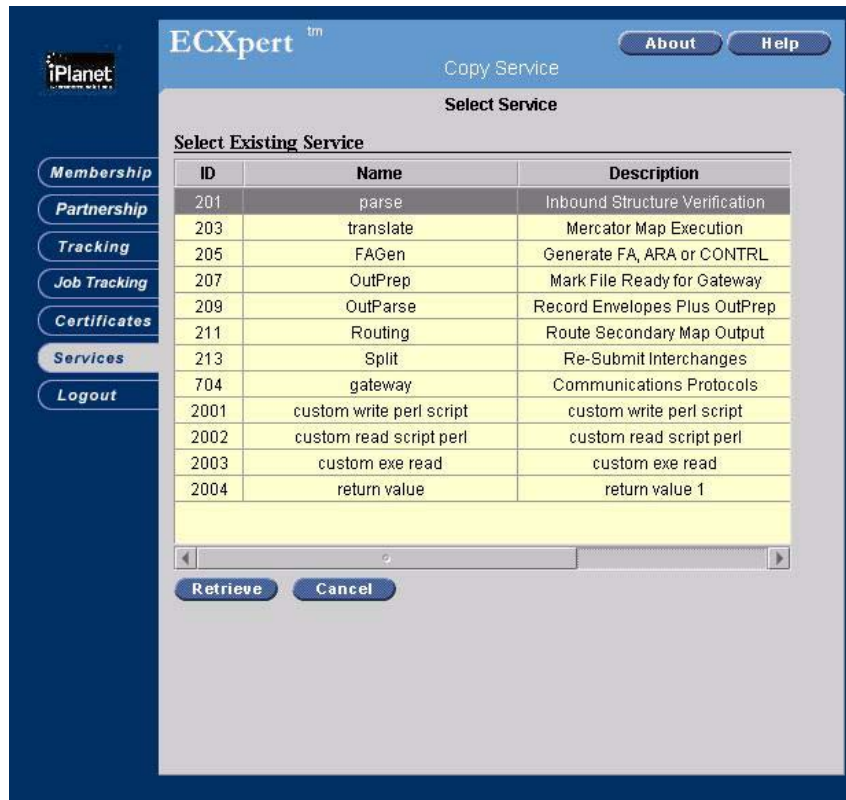
4. Select a service list.

   Click in the row for the service list you want to select.

5. Click Retrieve.

   The information for the selected service list is displayed on the
   Service List Details tab (Figure 10-5).

Working with the Service List Details Tab

The operations to add, copy, and delete service lists all use the same
Service List Details tab. The Service List Details tab appears in the different forms
for each of these operations.

Follow the steps below to work with this tab.

1. Fill in or change information for the first four items.

   Refer to Table 10-4 for details on the specific fields.

Figure 10-5   Service List Details tab

Table 10-5   Service List Details tab

Item	Description
Service List Name	A service list name can contain as many as 60 characters. It can contain letters, numbers, and special characters, and is case-sensitive.
Service List Data Type	Select the data type being exchanged. For example, XML or EDI. For partnerships trading non-EDI data, this must match the Document Type entered on the Partnership Information tab. (For EDI, it is not necessary to match the Document Type.) To use the list for multiple Data Types, use the * wildcard in place of a specific name.
Sending Member ID	The member ID sending the service list. Service lists can be used by two members or by multiple members. To be used by all users, use the * wildcard in place of a specific name.
Receiving Member ID	The member ID receiving the service list. Service lists can be used by two members or by multiple members. To be used by all users, use the * wildcard in place of a specific name.
Priority	A pulldown list of available priority levels (high, medium, low) for processing, or scheduled processing, of document files.
Select Service to add to list	The scrollable list of services that are available for use in service lists.
Exit Service List	A drop-down list of exit services that are available. An exit service is executed only if execution of the service list

NOTE	If a service list is to be used in conjunction with data to be separated and exchanged with multiple parties, each of the data parts to be separated has to have its own service list. Make sure that the Gateway service appears only *once* in all of the service lists for all of the related data parts.

2.   Add services to the list.

To add a service to the service list, select a service in the Select Service to add to list section, and then click Add. The service then appears in the Services in list section.

NOTES	When FA Gen is added to the service list and you want to use an error service, place the desired error service after FA Gen. Otherwise, place the error service after a standard service or at the end of the service list.
	If you are adding an Exit Service to a service list, be sure to click **Add**, and then click **Change** after you have selected the Exit Service from the **Exit Service List** drop-down.
	If you only click Change, it does not save your Exit Service List selection.

3. Rearrange services in the list.

   To rearrange the list, select a service in the Services in list section, then click Up or Down to move the service in that direction.

4. Delete services from the list.

   To delete a service from the list, select a service in the Services in list section, then click Remove to remove the service.

5. Save your work.

   A "completion" button always appears at the bottom of the Service List Detail tab.

   This button has the same name as the one you clicked to begin the current task: Add, Change, Copy, or Delete. The task is not complete until you click this button.

   For Delete, this button deletes the service list. For other operations, this button saves the information for the service list.

NOTE	Click Cancel at the bottom of the Service List Detail tab at any time if you decide not to complete the task.

Adding a New Service List on a Blank Form

Follow the steps below to add a new service list on a blank form.

If you want to add a new service list by editing the information for an existing service list, see "Copying a Service List—Adding a New Service List Based on Another."

1. Display the Service Administration tab (Figure 10-1).

2. Specify Service List Administration.

   From the Select Service or Service List Administration list, select Service List.

3. Click Add.

   The Service List Details tab (Figure 10-5) is displayed.

4. Fill in the information on the Service List Details tab.

   Refer to Table 10-5 on page 482 for information on specific fields.

5. Save the information for the service list.

   Click Add at the bottom of the Service List Details tab.

NOTE	Click Cancel at the bottom of the Service List Details tab if you decide not to add the new service list.

Copying a Service List—Adding a New Service List Based on Another

When the information for a new service list that you are adding is similar to the information for an existing service list, you can save time by using the existing service list as a template for the new service list. Follow the steps below to do this.

To create a new service list without using another service list as a template, see "Adding a New Service List on a Blank Form" on page 484.

1. Display the Service Administration tab (Figure 10-1).

2. Specify Service List Administration.

   From the Select Service or Service List Administration list, select Service List.

3. Click Copy.

The Select Service List tab (Figure 10-4) is displayed.

4. Select the service list to use as a template.

See "Displaying Information for an Existing Service" on page 472 for details.

5. Click Retrieve.

The Service List Details tab (Figure 10-5) is displayed.

6. Make necessary additions and changes.

Refer to "Working with the Service List Details Tab" on page 481 for details on specific fields on the Service List Details tab.

7. Save the information for the service list.

Click Copy at the bottom of the last tab in the Service List Details tab.

NOTE	Click Cancel at the bottom of the Service List Details tab if you decide not to add the new service.

Changing the Information for a Service List

Follow the steps below to change information for a service list.

1. Display the Service Administration tab (Figure 10-1).

2. Specify Service List Administration.

From the Select Service or Service List Administration list, select Service List.

3. Click Change.

The Select Service List tab (Figure 10-4) is displayed.

4. Select the service list you want to change.

See "Displaying Information for an Existing Service List" on page 479 for details.

5. Click Retrieve.

The information for the selected service list is displayed in the Service List Details tab (Figure 10-5)

6. Make necessary additions and changes.

   Refer to "Working with the Service Details Tab" on page 474 for details on each item of information on each of the three tabs.

7. Save the information for the service list.

   Click Change at the bottom of the Service List Details tab.

NOTE	Click Cancel at the bottom of the Service List Details tab if you decide not to change the information for the service list.

Deleting a Service List

NOTE	When you delete a *member*, the partnerships and service lists associated with that member are *also* deleted automatically.
	All tracking and event log information for files you previously processed for that member, however, remain intact.

Follow the steps below to delete a service list.

1. Display the Service Administration tab (Figure 10-1).

2. Click Delete.

   The Select Service List tab (Figure 10-4) is displayed.

3. Select the service list you want to delete.

   When you click Delete on the Select Service List tab, you are prompted to view the information before deleting. Your options are as follows:

   ❍ Yes—displays the information for the service list on the Service List Details tab before deleting.

   ❍ No—deletes the service list immediately, without further confirmation.

   ❍ Cancel—returns to the Service List Administration tab without deleting the service or displaying the information.

4. Click Yes.

The information for the service list you have selected to delete is displayed in the Service List Details tab (Figure 10-5).

5. Examine the information.

Be absolutely certain that you are deleting the correct service list.

6. Delete the service list.

Click Delete at the bottom of the Service List Details tab.

NOTE	Click Cancel at the bottom of the Service List Details tab if you decide not to delete the service list.

After clicking Delete, you are asked, "Are you sure?" Click Yes to confirm the deletion.

NOTE	You can still click No to cancel the deletion at this point, but this is your last chance.

Deleting a Service List

Command Line Utilities

This chapter documents the command line utilities that are available for use with ECXpert. The following topics are covered:

bdgsetpasswd—Changing Passwords

The `bdgsetpasswd` command lets you change the following passwords:

- An ECXpert member's password, kept in the ECXpert database or directory:

    ```
    ./bdgsetpasswd -m MBName  -p  MBPassword
    ```

- The ECXpert Oracle DB user's password, kept in the `ecx.ini` file:

    ```
    ./bdgsetpasswd -i ecx.ini -p  DB_PASSWORD
    ```

- The ECXpert POP3 user's password, kept in the `ecx.ini` file:

    ```
    ./bdgsetpasswd -i ecx.ini -pp POP3_pwd
    ```

- The ECXpert LDAP user's password, kept in the `ecx.ini` file:

    ```
    ./bdgsetpasswd -i ecx.ini -lp LDAP_PASSWORD
    ```

    This password must be the same as your Directory manager password.

submit—Submitting Files to ECXpert

The `submit` command allows you to submit files to ECXpert from the command line. It is intended to be included in a script to automate the submission process.

The `submit` command requires the following environment variables to be properly set:

- `BDG_HOME`, set to *NSBASE*/NS-apps/`ECXpert`

- `LD_LIBRARY_PATH`, set to *NSBASE*/NS-apps/`ECXpert/lib`

Syntax

The syntax of the `submit` command is as follows:

`submit` *parameter_list*

Table 11-1   Parameters for the `submit` command

Parameter	Usage
`-se`	Sender, the member ID of the member who is submitting the request to the Dispatcher.
`-re`	Recipient, the member ID of the member to whom the interchange(s) should be sent.
`-fn`	File name, the name of a file to be submitted to ECXpert (the submission unit). If you do not specify the path name, ECXpert looks for the file in the directory where the `tcpip-connector` server is executing.
`-ft`	File type, the type of the file being passed to ECXpert.
`-in`	Full path to the configuration file.
`-pw`	Password for the sending member. (Not needed if sending member is *trusted*.)
`-mn`	Map file name.
`-sd`	Causes the file to be sent to the tcpip-connector via a socket connection. Use this mode only if the tcpip-connector is running on a different machine and cannot be accessed directly.

NOTE	The combination of values for -se, -re, and -ft must match the corresponding values for a Service List in order for the submission to be processed.

You can also use an HTML form to submit files to ECX. To display the Submission Information form, enter the following URL in your browser:

```
http://ECXhome/BDGsubmit.html
```

where `ECXhome` is the fully qualified DNS servername and port of the ECXpert http server.

ECXpert also provides functions that allow you to implement a file submission capability within application programs. For API documentation, refer to the *iPlanet ECXpert Developer's Guide* chapter on "The EcxSubmit Class."

Example

The following example shows how to submit a file (the command should be all on one line):

```
submit -se kmem1 -pw kmem1 -re ux_ecx7 -fn /tmp/850.edi -ft EDI
-in $NSBASE/NS-apps/ECXpert/config/ecx.ini
```

Running submit from a Remote Machine

To use the `submit` command from a system other than the one on which ECXpert is installed (a "remote" system), you must do the following:

1. Install the ECXpert libraries on the remote system.

   To install the ECXpert libraries on the remote system, do the following:

   a. Perform a full installation of ECXpert on the system.

   b. Manually remove everything except the `submit` command, the `ecx.ini` file, and the contents of the `lib` directory.

2. Modify the following portions of the `[tcpip-connector]` section in the `ecx.ini` file on the local machine:

`port_location` = **static**

`admin_port_type` = **manual**

`admin_port` = **6001**

`listener_port_type` = **manual**

`listener_port` = **6002**

3. Copy the same `ecx.ini` file from the local machine to the remote machine.

4. Ensure that the `ECXpert.map` file is available to the remote system.

If TCP/IP is involved, either set up the TCP/IP connector to have static ports, or cross-mount the file system of the ECXpert host on the client system and make sure that the paths within the `ecx.ini` file are valid on the remote system.

When submitting a file from the remote machine to another ECXpert system, use the data streaming option (`-sd`).

poll—Checking for New Documents

The `poll` command allows you to check for availability of new documents and retrieve them from ECXpert.

Typically, use the `poll` command from a script to handle situations where you want to control when data is delivered to your application, rather than allowing ECXpert to push the documents to you asynchronously.

For example, you can use the `poll` command in the following situations:

- you want to implement a "mailbox" interface to ECXpert in which documents are retrieved at the user's request

- you want to retrieve documents periodically, as part of a scheduled job

Syntax

The syntax of the poll command is as follows:

poll *inifile section_name parameter_list*

Where

- *inifile* is the full path to the ECXpert configuration file (ecx.ini)

- *section_name* must be poll

- *parameter_list* consists of options selected from Table 11-2

Table 11-2   Parameters for the poll command

Parameter	Usage
-se	Sender, the member ID of the sender. Optional.
-re	Recipient, the member ID of the recipient. Optional.
-dm	Delivery mode. You must specify the following mode: retrieve, copy files from ECXpert.
-op	Operation. You must specify the following flag: recv, receive from ECXpert.
-fn	You must specify the full path of the file into which ECXpert output is copied.

Example

If you have installed ECXpert in the *$NSBASE*/NS-apps/ECXpert directory, and if your sender and receiver are MemberA and MemberB, respectively, you would use the poll command as follows:

```
# $NSBASE/NS-apps/ECXpert/bin/poll
      $NSBASE/NS-apps/ECXpert/config/ecx.ini poll
      -se MemberA -re MemberB -dm retrieve -op recv
      -fn /tmp/myoutputfile.txt
```

Note that the command must be typed on a single line with spaces separating each of the parts; the lines shown above must be a single line when entered as a command.

ecx.ini Settings

The following settings in the [retrieve] section of the ecx.ini file are required for the poll command to execute properly:

```
[retrieve]
...
pre_enveloped_edi = True
data_type = both
bundle_all = yes
```

The bundle_all setting is recommended, but not required.

If necessary, modify your ecx.ini file to reflect these settings before using the poll command.

import—Importing Records for Members, Partnerships, or Service Lists

The import command allows you to import member-, partnership-, service-, or service list-related records from a text file. You can use the import command when you want to import a batch of records instead of entering the information for each member or partner through the ECXpert user interface.

NOTE	You cannot import a record for a membership, partnership, service, or service list when a record for it already exists in the database.

Syntax

The syntax for the import command is as follows:

import *user password data_file [log_file [discard_file]]*

Table 11-3   Arguments for the import command

Argument	Description
user	User login name of an administrator.

Table 11-3　Arguments for the `import` command *(Continued)*

Argument	Description
password	Administrator's password.
data_file	Full path name of the file containing the records to import.
log_file	Full path name of the log file created by the `import` utility.
	Default: - if *log_file* is omitted entirely—base name of *data_file*, with `.log` extension, created in same directory as *data_file* - if *log_file* extension omitted, *log_file* plus `.log` extension, created in directory specified
	Option: `-A` immediately after *log_file* causes data to be appended to the file if it already exists, instead of overwriting it.
discard_file	Full path name of the file created by the `import` utility to hold rejected records.
	Default: - if *discard_file* is omitted entirely—base name of *data_file*, with `.dsc` extension, created in same directory as *data_file* - if *discard_file* extension is omitted, *discard_file* plus `.dsc` extension, created in directory specified
	Option: `-A` immediately after *discard_file* causes data to be appended to the file if it already exists, instead of overwriting it.

Running the `import` command creates the specified log file. The log file reports the number of input records, the number of records that were accepted, the number of records that were rejected, and error messages for rejected records.

During processing, rejected input records are placed in the discard file; processing does not stop when an error occurs. Rejected records are copied without change from the data file to the discard file. You can modify records in the discard file and then use that file as the data file in a subsequent `import` command.

CAUTION　The contents of the log file and discard file are overwritten each time you run the `import` command unless you include the `-A` option immediately after the names you specify for log file and discard file.

Examples

Create a `foo.log` and a `foo.dsc` in the same directory as `foo.imp`:

`# ./import ECX ECX foo.imp`

Append to the log file, but overwrite the discard file:

`# ./import ECX ECX foo.imp foo.log-A foo.dsc`

Data File Control Structure

The data file contains a control structure that specifies the format of the data, which is followed immediately by the data in the specified format. The data file can contain multiple sets of control structures and data.

NOTE	Typically, an import file is used to insert first the Members, then the MBAddresses information, then the Partnership(s), then the Service List(s) information—each with its own set of control structures and data.
	If you use the import file to delete Members, however, you do not need to also delete the Partnerships and Service Lists — they are deleted automatically when you delete the Member names.

Syntax

The syntax for the control structure is as follows:

```
[# comment ]
[ object = record_type; operation = action; field_delim = delimeter;
fields = { name [ :value val | :position pos ]}, ... ]
```

Table 11-4 Parameters for the control structure

Parameter	Description
#	Comment.
object	The kind of record you want to create in the database. Valid values for *record_type* are member, mbaddress, partnership, service, or servicelist.
operation	The kind of action you want to perform. Valid values for *operation* are insert, delete, or update.
	Note: When you delete a Member using this utility, all member trading address, partnership, and service list data for that Member is also automatically deleted.
field_delim	The character that delimits fields within the data.
fields	The fields you want to insert or update, or the key field for the record you want to delete. See Table 11-5.
:value	(Optional) A constant value you want to specify for the field in each record.
:position	(Optional) The number of a column that contains the value for the field.

- The square brackets at the beginning and end of the control structure, shown above, are required.

- You can place comments, which start with a pound-sign character (#) and continue for the entire line, anywhere in the data file.

- Each parameter and associated value or values is set off by a semicolon (;).

You can add as many field names as you desire. Each field name entry is set off with a comma (,). Use the information in Table 11-5 to determine which fields parameters to pass for the associated database schema columns.

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(1 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
member Table (object=member)				
MBName	Name	Y	varchar2(60)	Member name.
MBType	Type		integer	Member type. LDAP name: BusinessCategory Valid values: 0 = MBTunknown 1 = MBTsysAdmin 2 = MBTmembershipAdmin (not used in release 3.6) 3 = MBTgroupAdmin (not used in release 3.6) 4 = MBTinternalMember (not used in release 3.6) 5 = MBTtradingPartner (external member)
MBIsGroup	IsGroup		integer	Is member a group? Valid values: 1 = yes 0 = no
MBActive	Active		integer	Is member active? LDAP name: EmployeeType, bit 0x01 Valid values: 1 = yes 0 = no
MBPassword	Password		varchar2(255)	Member password (encrypted)

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(2 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
MBTrusted	Trusted		integer	Is member trusted
				LDAP name: EmployeeType, bit 0x02
				Valid values:
				1 = yes
				0 = no
MBContactName	ContactName		varchar2(60)	Member contact's name. LDAP name: FullName
MBContactAddress1	ContactAddress1		varchar2(60)	Contact's address line 1. LDAP name: Address, bytes 0-59
MBContactAddress2	ContractAddress2		varchar2(60)	Contact's address line 2. LDAP name: Address, bytes 60-119
MBContactCity	ContactCity		varchar2(60)	Contact's city. LDAP name: Locality
MBContactState	ContactState		varchar2(60)	Contact's state or province. LDAP name: State
MBContactZip	ContactZip		varchar2(60)	Contact's zip or postal code. LDAP name: PostalCode
MBContactCountry	ContactCountry		varchar2(60)	Contact's country. LDAP name: Address, bytes 120-179
MBContactPhone	ContactPhone		varchar2(60)	Contact's phone number. LDAP name: PhoneNo
MBContactFax	ContactFax		varchar2(60)	Contact's fax number. LDAP name: Fax
MBContactDesc	Description		varchar2(255)	Contact's company name. LDAP name: Description
MBContactEmailId	ContactEmailId		varchar2(255)	Contact's email. LDAP name: Email
MBObjPerm	ObjPerm		integer	Object permission (not used in 3.0)
mbaddress Table (object=mbaddress)				

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(3 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
MBAName	`Member`	Y	varchar2(60)	Member name
MBAQual	`Qual`	Y	varchar2(60)	Qualifier for trading address. Valid values:
				YourEDIQualifier=`EDI` (any value other than "EL" or "ER")
				EL=Local E-mail
				ER=Remote E-mail
MBAQualId	`QualId`	Y	varchar2(60)	Main trading address
partnership Tables (object=partnership)				
PNId	`PartnerId`	Y	integer	Partnership ID
PSId	`StandardId`	Y	integer	Standards ID
PDDDocType	`DocumentType`	Y	varchar2(60)	Document type
PNSndrMBName	`SenderName`		varchar2(60)	Sending member name
PNSndrQual	`SenderQual`	Y	varchar2(60)	Qualifier for sending member's trading address
PNSndrQualId	`SenderQualId`	Y	varchar2(60)	Sending member's main trading address
PNSndrCertType	`SenderCertificate Type`		integer	Certificate type. Valid values: 0 = CTUnknown 1 = CTSelf 2 = CTVerisignC3 3 = CTVerisignC2 4 = CTVerisignC1 5+ Other CA root(s) user imports
PNRcvrMBName	`ReceiverName`		varchar2(60)	Receiving member name
PNRcvrQual	`ReceiverQual`	Y	varchar2(60)	Qualifier for receiving member's trading address
PNRcvrQualId	`ReceiverQualId`	Y	varchar2(60)	Receiving member's main trading address

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(4 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PNRcvrCertType	`ReceiverCertifica teType`		integer	Certificate type. Valid values: 0 = CTUnknown 1 = CTSelf 2 = CTVerisignC3 3 = CTVerisignC2 4 = CTVerisignC1 5+ Other CA root(s) user imports
PNActive	`Active`		integer	Is partnership active? Valid values: 1=yes 0=no
PNSecurity	`Security`		integer	SMTP security. Valid values: 0 = Plain MIME (send as base64 encoding only) 1 = Encrypted (encrypted with receiver's public key) 2 = Signed (signed with sender's private key) 3 = SignedAndEncrypted (signed first, then encrypted)
PNDesc	`Description`		varchar2(255)	Partnership description
PSStandard	`StandardName`	Y	varchar2(60)	EDI standard
PSVersion	`StandardVersion`	Y	varchar2(60)	EDI standard version number
PSRelease	`StandardRelease`	Y	varchar2(60)	EDI standard release number
PSLastIntgCtrlNum	`IntchngLastContro lNumber`		varchar2(60)	Last interchange control number generated
PSLockIntg	`IntchngLock`		integer	(internal use)
PSTestProdFlag	`TestProductionFla g`		integer	Test vs. production data flag. Valid values: 0 = TPFunknown 1 = TPFproduction (production data) 2 = TPFtest (test data)
PSSegTerm	`SegmentTerminator`		varchar2(6)	Segment terminator character

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(5 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PSElmtSep	ElementSeparator		varchar2(6)	Data element separator character
PSSubElmtSep	SubElementSeparator		varchar2(6)	Data sub-element separator character
PSDecPtChar	DecimalPointCharacter		varchar2(6)	Decimal point character
PSOutStandard	OutStandard		varchar2(60)	Interchange standard user wants to appear in bundled EDI documents
PSOutVersion	OutVersion		varchar2(60)	Interchange version user wants to appear in bundled EDI documents
PSOutRelease	OutRelease		varchar2(60)	Interchange release user wants to appear in bundled EDI documents
PGGroupType	GroupType	Y	varchar2(60)	Partnership group
PGSndrQual	SndrAppQual	Y	varchar2(60)	Qualifier for the application sender code. Used only in EDIFACT.
PGSndrAppCode	SndrAppCode	Y	varchar2(60)	Application sender code.
PGRcvrQual	RcvrAppQual	Y	varchar2(60)	Qualifier for the application receiver code.
PGRcvrAppCode	RcvrAppCode	Y	varchar2(60)	Application receiver code.
PGLastGroupCtrlNum	GroupLastControlNumber		varchar2(60)	Last group control number generated
PGLockGroup	GroupLock		integer	(internal use)
PGGenDocAck	GroupGenerateDocAck		integer	Generate document acknowledgments flags (internal use)
PDDocType	DocType	Y	varchar2(60)	Document type

Table 11-5   Schema column names and associated `fields` parameters for the `import` utility *(6 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PDPriority	`DocPriority`		integer	Processing priority. Valid values: 0 = PDunknown 1 = PDhigh 2 = PDmedium 3 = PDlow
PDMapName	`MapName` Note: The `import` utility does not verify if the specified map exists in the `maps` directory. If the map does not exist, documents sent using the partnership will not be translated.		varchar2(60)	Map file name
PDMapDirection	`MapDirection` (or `XlatType`, old name for backward compatibility)		integer	Translation type. Valid values: 0 = XLTunknown 1= XLTinbound (EDI-to-Application) 2 = XLToutbound (Application-to-EDI) 3 = XLTedi2edi (EDI-to-EDI) 4 = XLTapp2app (Application-to-Application) 5 = XLTnoxlat (None; pass-through mode)
PDAckExpected	`AckExpected`		integer	Is functional acknowledgment expected? Valid values: 1=yes 0=no
PDLastCtrlNum	`DocLastControlNumber`		varchar2(60)	Last control number generated

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(7 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PDLock	DocLock		integer	(internal use)
PD1stXportType	PrimaryXportType See Table 11-6 for a list of values for this field, as well as the required parameters for each transport type.		varchar2(60)	Primary transport protocol. Requires a delimiter of (|) or (;). Valid values include: "comm_ftp_geis" for GEIS FTP "commhttp-aiag" for HTTP AIAG "commhttp-gisb" for HTTP GISB "commsmtp-send" for SMTP "ecxoftp-server" for Odette FTP (OFTP) "eXML-connector" for eXML Connector "ftp-local-application" for local FTP (application) "ftp-local-edi" for FTP (EDI) "http-retrieve" for HTTP Receive "legacy-mq-series" for Legacy Server (MQ Series) "legacy-oracle-apps" for Legacy Server (Oracle) "legacy-sap" for Legacy Server (SAP) "retrieve" for POLL See Table 11-6 on page 510 for the required parameters for each protocol.

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(8 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PD1stXportParam	`PrimaryXportParam` (requires a delimiter of | or `;`) See Table 11-6 for the required parameters for each transport type (PrimaryXportType).		varchar2(255)	Primary transport protocol parameter See Table 11-6 on page 510 for the required parameters for each transport protocol.

Table 11-5   Schema column names and associated `fields` parameters for the `import` utility *(9 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PD2ndXportType	SecondaryXportType See Table 11-6 for a list of values for this field, as well as the required parameters for each transport type.		varchar2(60)	Alternate transport protocol. Requires a delimiter of (|) or (;). Valid values include: "comm_ftp_geis" for GEIS FTP "commhttp-aiag" for HTTP AIAG "commhttp-gisb" for HTTP GISB "commsmtp-send" for SMTP "ecxoftp-server" for Odette FTP (OFTP) "eXML-connector" for eXML Connector "ftp-local-application" for local FTP (application) "ftp-local-edi" for FTP (EDI) "http-retrieve" for HTTP Receive "legacy-mq-series" for Legacy Server (MQ Series) "legacy-oracle-apps" for Legacy Server (Oracle) "legacy-sap" for Legacy Server (SAP) "retrieve" for POLL See Table 11-6 on page 510 for the required parameters for each protocol.

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(10 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
PD2ndXportParam	SecondaryXportParam See Table 11-6 for the required parameters for each transport type (SecondaryXportType).		varchar2(255)	Alternate transport protocol parameter See Table 11-6 on page 510 for the required parameters for each transport protocol.
PDSendType	SendType		integer	Immediate or scheduled. Valid values: 1=immediate 2=scheduled
PDDeleteWait	DeleteWaitPeriod		integer	Retention period (days) before delete
PDArchiveWait	ArchiveWaitPeriod		integer	Retention period (days) before archiving (not used in release 3.6)
PDPreEnveloped	PreEnveloped		integer	Is data pre-enveloped? Valid values: 0 = PEunknown 1 = PEenveloped (bundle preserves all envelopes) 2 = PEnonenveloped (bundle generates and/or replaces all envelopes) 3 = PEpreenvelopedEDI(not used in 3.0) 4 = PEGetCtrlNo (Bundle only supplies the control number and preserves everything else in envelope) 5 = PEPreserveCtrlNo (Bundle only preserves the envelope control number)
DTServices Table (object=servicelist)				
DTSServiceListName	ServiceListName	Y	varchar2(60)	Service list name
DTSSeqNum	SeqNum	Y	integer	Order of the service in service list

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(11 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
DTSSndrMBName	SndrMBName	Y	varchar2(60)	Sending member name
DTSRcvrMBName	RcvrMBName	Y	varchar2(60)	Receiving member name
DTSTypeName	TypeName	Y	varchar2(60)	Service file type name OR service data object type name
DTSSVRId	SVRId		integer	Service ID
DTSSVRName	SVRName		varchar2(60)	Service name
DTSServiceParams	ServiceParams		varchar2(255)	Service parameters
DTSErrorHandler	ErrorHandler		varchar2(60)	Name of user-specified service for error handler
DTSDesc	Desc		varchar2(255)	Service description
DTSObjPerm	ObjPerm		integer	Object permission (not used in 3.0)
Services Table (object=service)				
SVRId	Id	Y	integer	Service ID. Valid values: 201 =parse 203 =translate 205 = FAGen 207 = OutPrep 209 = OutParse 211 = Routing 213 = Split 704 = Gateway 2001 and above = custom services
SVRName	Name		varchar2(60)	Service name (e.g., parse)

Table 11-5 Schema column names and associated `fields` parameters for the `import` utility *(12 of 12)*

Database Schema Column to Import Into	Import `fields` Parameter to Pass	Req	Database Data Type (Length)	Description
SVRType	Type		integer	Service type. Valid values: 0 = STunknown 1 = STinternal (ECXpert internal service, e.g. parse, xlat) 2 = STscript (ECXpert external script file) 3 = STexe (ECXpert external executable file) 4 = STdll (function in a shared library, e.g. DLL)
SVRPathName	PathName		varchar2(255)	Path name to service code file
SVREntryName	EntryName		varchar2(60)	Entry name
SVRMaxThread	MaxThread		integer	Maximum number of threads
SVRParam	Param		varchar2(255)	Service description
SVRObjPerm	ObjPerm		integer	Object permission (not used in 3.0)

Partnership Transport Protocol Parameters

Table 11-6 indicates the required parameters for each transport protocol type in imported data files; each `PrimaryXportParam` and `SecondaryXportParam` value must include the indicated `PrimaryXportType` and `SecondaryXportType` fields.

The table also includes an example of how the data should be structured in imported partnership data files.

NOTE	These transport types and corresponding parameters are associated with the following columns in the PNDocs table of the database: the `PD1stXportType` and `PD2ndXportType` columns, and the corresponding `PD1stXportParam` and `PD2ndXportParam` columns.
	The entire string for each `PD1stXportType` and `PD2ndXportType` column is encrypted when it is entered in the column, whether the data is added from an import file or from the user interface.

NOTE	Each parameter listed for a protocol must be included in the control structure for an import file, even if it is optional.
	Optional parameters can be left blank by not including a value. For example, `TH|;` indicates no value for the `TH` parameter.

Table 11-6 Partnership transport protocol parameters *(1 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	**Delimiter: (;)**	

`comm_ftp_geis`	TP|*transport protocol*; (*comm_ftp_geis*)
	
	OO|*operation*; (*send*, *recv*)
	
	HN|*hostname*; (name or IP address)
	
	PT|*portnumber*; (Optional)
	
	UN|*username*;
	
	PW|*userPassword*
		`comm_ftp_geis,`
		`  TP|comm_ftp_geis;OO|send;`
		`  HN|hostname;PT|999;`
		`  UN|username;`
		`  PW|userpassword,`

Table 11-6 Partnership transport protocol parameters *(2 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	**Delimiter: (;)**	
`commhttp-aiag`	HN|*hostname*; (name or IP address)	`commhttp-aiag,`
	PT|*portnumber*; (Optional)	`  HN|hillary.mcom.com;PT|20`
	UN|*username*;	`00;`
	OO|*operation*;	`  UN|actraadm;OO|DELIVER;`
	(*DELIVER, OBTAIN*)	`  PW|actraadm;SS|user1;`
	PW|*password*;	`  RR|user2;RN|1;AN|EDI;`
	SS|*sender*;	`  UP|actraadm;`
	RR|*receiver*;	`  PL|/bin/aiag-logon;`
	RN|*reference number*; (Optional)	`  PD|/bin/aiag-deliver;PO|,`
	AN|*application type*;	
	(e.g., *EDI, application*, etc.)	
	UP|*user parameter*; (Optional)	
	PL|*login cgi-pathname*;	
	PD|*deliver cgi-pathname*	
	(if *OO=DELIVER*)	
	PO|*obtain cgi-pathname*	
	(if *OO=OBTAIN*)	
`commhttp-gisb`	HN|*hostname*; (name or IP address)	`commhttp-gisb,`
	PT|*portnumber*; (Optional)	`  HN|hillary.mcom.com;PT|20`
	UN|*username*;	`00;`
	OO|*operation*; (*DELIVER*)	`  UN|actraadm;OO|DELIVER;`
	PW|*password*;	`  PW|actraadm;SS|user1;`
	SS|*sender*;	`  RR|user2;IF|EDI;`
	RR|*receiver*;	`  PD|/bin/gisb-deliver,`
	IF|*input format*;	
	(e.g., *EDI, application,* etc.)	
	PD|*deliver cgi-pathname*	

Table 11-6 Partnership transport protocol parameters *(3 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	**Delimiter: (;)**	
`commsmtp-send`	Note: Only MT is string; all other parameters are numbers.	`commsmtp-send,PR|0;MA|28;MR` `|1;` `MT|application;KL|128;` `CS|;CR|,`
	PR	*ProcessMethod*; (0=SimpleMime, 1=EncryptedOnly, 2=SignedOnly, 3=Signed&Encrypted)	
	MA	*MIC_Algorithm*; (If PR=1, 2, or 3) (28=SHA_1, 5=MD5)	
	MR	*MDN_Requested*; (0=No MDN, 1=Plain MDN, 2=Signed MDN)	
	MT	*Mime_subtype*; (Optional)	
	KL	*Key_length*; (If PR=1, 2, or 3) (56, 64, 75, 128, 255, 512, 1024)	
	CS	*senderCertType*; (0=CTUnknown, 1=CTSelf, 2=CTVerisignC3, 3=CTVerisignC2, 4=CTVerisignC1, 5=Other CA root(s) user imports)	
	CR	*receiverCertType* (see values for CS)	

Table 11-6 Partnership transport protocol parameters *(4 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	Delimiter: (;)	
| ecxoftp-server | OU\|*username;* | ```
TCP/IP:
ecxoftp-server,OU|actraadm;
  OL|actraadm;OX|TCP/IP;
  XN|;XL|;XC|;XF|;XR|;XT|;X
S|;
  XU|;XY|;XZ|;TX|9999;
  TH|destination.mcom.com,
X.25:
ecxoftp-server,OU|actraadm;
  OL|actraadm;OX|X.25;
  XN|123456789;XL|;XC|1234;
  XF|;XR|;XT|;XS|;XU|;XY|;X
Z|;
  TX|;TH|,
X.28:
ecxoftp-server,OU|actraadm;
  OL|actraadm;OX|X.28;XN|;
  XL|;XC|;XF|;XR|;XT|;
  XS|/tmp/conn_script;XU|;
  XY|;XZ|;TX|;TH|,
``` |
	OL|*userPassword;*	
	OX|*transportMethod;* (X.25, X.28, or TCP/IP)	
	XN|*destination_X.121Address;* (Optional; if OX=X.25, defaults to local network user address)	
	XL|*LogicalChannelNumber;* (Optional; numeric)	
	XC| *CallUserData* (Optional; numeric {typically hex})	
	XF|*X.25 FacilityInformation;* (Optional; numeric {typically hex})	
	XR|*RoutingEntry;* (Optional)	
	XT|*X.28 Tel number;* (Optional)	
	XS|*X.28 Connection script pathname;*	
	XU|*X.28 PAD user name;* (Optional)	
	XY|*X.28 PAD user password;* (Optional)	
	XZ|*X.28 destination NUA;* (Optional; numeric network user address)	
	TX|*TCP/IP destination port;* (Optional for OX=TCP/IP; defaults to 3305)	
	TH|*TCP/IP destination host;* (Optional for OX=TCP/IP; name or IPaddress; defaults to local host name)	

Table 11-6 Partnership transport protocol parameters *(5 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	**Delimiter: (;)**	
eXML-connector	HN|*hostname*; (name or IP address)	eXML-connector,
	PT|*portnumber*; (Optional)	HN|hillary.mcom.com;PN|55 5;
	AI|*informationFilePath;* (file path and file name)	AI|/tmp/infofile.dat;
	XT|*fileTransport;* (file—to transmit filename only, stream—to transmit entire file)	XT|file,
ftp-local-applicati on	TP|*ftp-local-application;*	ftp-local-application,
	HN|*hostname*; (name or IP address)	TP|ftp-local-application; HN|hostname;PT|;
	PT|*portnumber*; (Optional)	UN|username;PW|userpasswo rd;
	UN|*username;*	SS|test1;RS|;OD|/tmp;
	PW|*userPassword;*	ID|;IT|;MD|I,
	SS|*SendPattern;*	
	RS|*ReceivePattern;*	
	OD|*outboundDirectory;*	
	ID|*InboundDirectory;*	
	IT|*InboundFileType;*	
	MD|*transfer mode* ("A" for ASCII, "I" for Binary)	

Table 11-6 Partnership transport protocol parameters *(6 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	Delimiter: (;)	

`ftp-local-edi`	TP|*ftp-local-application*;
	 HN|*hostname*; (name or IP address)
	 PT|*portnumber*; (Optional)
	 UN|*username*;
	 PW|*userPassword*;
	 SS|*SendPattern*;
	 RS|*ReceivePattern*;
	 OD|*outboundDirectory*;
	 ID|*InboundDirectory*;
	 IT|*InboundFileType*;
	 MD|*transfer mode* ("A" for ASCII, "I" for Binary)
		```ftp-local-edi,```
		 ``` TP|ftp-local-application;```
		 ```HN|hostname;PT|;```
		 ``` UN|username;PW|userpasswo```
		 ```rd;```
		 ``` SS|test1;RS|;OD|/tmp;```
		 ``` ID|;IT|;MD|I,```

`commhttp-ssl`	HN|*hostname*; (name or IP address)
	 PT|*portnumber*; (Optional)
	 PN|*cgi pathname*;
	 SE|*sender*;
	 PW|*password*;
	 RE|*receiver*;
	 FT|*file type*;
	 CY|*certificate type*
		```commhttp-ssl,HN|hostname;```
		 ``` PT|999;PN|cgiPathname;```
		 ``` SE|sender;PW|userpassword```
		 ```;```
		 ``` RE|receiver;FT|filetype;```
		 ``` CY|certificateType,```

`http-retrieve`	—	```http-retrieve,,```

`legacy-mq-series`	QN|*QUEUENAME*; (uppercase)
	 QM|*queue manager*;
	 MH|*message header file*
		```legacy-mq-series,```
		 ``` QN|TESTQ;QM|testqmgr;```
		 ``` MH|/tmp/msgheadr.txt,```

Table 11-6 Partnership transport protocol parameters *(7 of 7)*

PD1stXportType or PD2ndXportType Value	Corresponding PD1stXportParam and PD2ndXportParam Values	Example of Control Structure Syntax for Imported Partnership Object
Delimiters: (|) or (;)	Delimiter: (;)	

legacy-oracle-apps	MN|*map name*;
	
	DB|*database name*;
	
	UN|*username*;
	
	PW|*password*
		legacy-oracle-apps,
		  MN|xobi850.sun;DB|orafind b;
		  UN|apps;PW|apps,

legacy-sap	CN|*client number*; UI|*user id*; PW|*password*	legacy-sap,CN|800;UI|scott; PW|scott,
retrieve	—	retrieve,,

Control Structure Example for Importing Partnerships

The member, mbaddress, and partnership objects allow you to populate the database with new member and partnership data.

In the command below, insert.imp is specified as the data file:

import *user password* insert.imp *log_file discard_file*

The contents of the insert.imp file are listed below. It contains a set of control structures and data for first the member object, then the mbaddress object, and finally the partnership object.

```
#
# Setting up a Partnership
#
# add a partnership; specify all fields
#
# 1) add 2 new members
# 2) add mbaddresses for the members
# 3) add a partnership for the member pair


# insert a couple of member records

[object = member; field_delim = "|"; operation = insert;
```

```
 fields = Name, Type, IsGroup, Active, Password, Trusted,
ContactName,
  ContactAddress1, ContactAddress2, ContactCity, ContactState,
ContactZip, ContactCountry,
  ContactPhone, ContactFax, ContactCompany, ContactEmailId,
ObjPerm ]

test1 | 0 | 0 | 1 | test1 | 0 | Test User 1 \
| 610 Caribbean Drive | Apt. 1 | Sunnyvale | California |
94089-1108 | USA \
| 650 234-3429 | 650 829-2422 | Actra Business System |
mbtest@actracorp.com | 175
kmem2 | 0 | 0 | 1 | kmem2 | 0 | Test User 2 \
| 610 Caribbean Drive | Apt. 1 | Sunnyvale | California |
94089-1108 | USA \
| 650 234-3429 | 650 829-2422 | Actra Business System |
mbtest@actracorp.com | 175


# insert member address records for the members

[object = mbaddress; field_delim = "|"; operation = insert;
 fields = Member, Qual, Qualid ]

test1 | 12 | 9161111111
kmem2 | 12 | 4152222222
kmem2 | EM | kmem2@actracorp.com


# insert a partnership for the member pair

[object = partnership; field_delim = ","; operation = insert;
 fields = SenderName, SenderQual, SenderQualId,
SenderCertificateType,
   ReceiverName, ReceiverQual, ReceiverQualId,
ReceiverCertificateType,
   Active, Security, Description,
   StandardName, StandardVersion, StandardRelease,
   IntchngLastControlNumber, IntchngLock, IntchngGenerateAck,
IntchngAckWaitPeriod,   TestProductionFlag, SegmentTerminator,
ElementSeparator, SubElementSeparator,   DecimalPointCharacter,
OutStandard, OutVersion, OutRelease, GenOptEnv,
   GroupType, GroupLastControlNumber, GroupLock,
GroupGenerateDocAck,
   SndrAppQual, SndrAppCode, RcvrAppQual, RcvrAppCode,
   DocType, DocPriority, MapName,
   MapDirection, AckExpected,
   DocLastControlNumber, DocLock,
   PrimaryXportType, PrimaryXportParam,
   SecondaryXportType, SecondaryXportParam,
   SendType, DeleteWaitPeriod, ArchiveWaitPeriod, PreEnveloped
]
```

```
test1, 12, 9161111111, 0,\
kmem2, 12, 4152222222, 0,\
1, 0, 850,\
X, 003020, 0,\
1, 0, 0, 5259600,\
1, 0D0A, 2A, 3E,
,, ,, 0,\
PO, 1, 0, 0,\
NONE, NONE, NONE, NONE,\
850, 0, SamplePO.sun,\
1, 0,\
1, 0,\
ftp-local-application,TP|ftp-local-application;HN|hostname;PT|;U
N|username;\
    PW|userpassword;SS|test1;RS|;OD|tmp;ID|;IT|;MD|I,\
,,\
1,5,0,2
```

Table 11-7 describes the fields included in the `insert.imp` example, as well as the specific values for the first record for each object.

Table 11-7 Fields in the sample imported partnerships

Field Name	Description	Value in the Example File
Member Data Fields		
Name	Member name	test1
Type	Member type	0 = MBTunknow
IsGroup	Is member a group?	0
Active	Is member active?	1
Password	Member password	test1
Trusted	Is member trusted?	0
ContactName	Member contact's name	Test User 1
ContactAddress1	Contact's address line 1	610 Caribbean Drive
ContactAddress2	Contact's address line 2	Apt. 1
ContactCity	Contact's city	Sunnyvale
ContactState	Contact's state or province	California
ContactZip	Contact's zip or postal code	94089-1108
ContactCountry	Contact's country	USA

Table 11-7   Fields in the sample imported partnerships *(Continued)*

Field Name	Description	Value in the Example File
ContactPhone	Contact's phone number	650 234-3429
ContactFax	Contact's fax number	650 829-2422, 650 829-2422
ContactCompany	Contact's description	Actra Business System
ContactEmailId	Contact's email	mbtest@actracorp.com
ObjPerm	Object permission	175
Membership Address Data Fields		
Member	Member name	test1
Qual	Qualifier for trading address	12
Qualid	Main trading address	9161111111
Partnership Address Data Fields		
SenderName	Sending member name	test1
SenderQual	Qualifier for sending member's trading address	12
SenderQualId	Sending member's main trading address	9161111111
SenderCertificate Type	Sending member's certificate type.	0 = CTUnknown
ReceiverName	Receiving member name	kmem2
ReceiverQual	Qualifier for receiving member's trading address	12
ReceiverQualId	Receiving member's main trading address	4152222222
ReceiverCertificat eType	Receiving member's certificate type	0 = CTUnknown
Active	Is partnership active?	1
Security	SMTP security	0 = Plain MIME (send as base64 encoding only)
Description	Partnership description	850
StandardName	EDI standard	X
StandardVersion	EDI standard version number	003020
StandardRelease	EDI standard release number	0
IntchngLastContr olNumber	Last interchange control number generated	1

Table 11-7 Fields in the sample imported partnerships *(Continued)*

Field Name	Description	Value in the Example File
IntchngLock	(internal use)	0
IntchngGenerate Ack	Generate interchange acknowledgments flags (internal use)Enveloping Options	0
IntchngAckWaitP eriod	The number of minutes to wait before the acknowledgment becomes overdue. Default: 525600.	5259600
TestProductionFl ag	Test vs. production data flag.	1 = TPFproduction (production data)
SegmentTerminat or	Segment terminator character	0D0A
ElementSeparator	Data element separator character	2A
SubElementSepar ator	Data sub-element separator character	3E
DecimalPointCha racter	Decimal point character	—
OutStandard	Interchange standard user wishes to appear in bundled EDI documents	—
OutVersion	Interchange version user wishes to appear in bundled EDI documents	—
OutRelease	Interchange release user wishes to appear in bundled EDI documents	—
GenOptEnv	Enveloping Options	0 = No UNA, No UNG
GroupType	Partnership group	PO
GroupLastContro lNumber	Last group control number generated	1
GroupLock	(internal use)	0
GroupGenerateD ocAck	Generate document acknowledgments flags (internal use)	0
SndrAppQual	Qualifier for the application sender code. Used only in EDIFACT.	NONE
SndrAppCode	Application sender code.	NONE
RcvrAppQual	Qualifier for the application receiver code.	NONE
RcvrAppCode	Application receiver code.	NONE

Table 11-7 Fields in the sample imported partnerships *(Continued)*

Field Name	Description	Value in the Example File
DocType	Document type	850
DocPriority	Processing priority.	0 = PDunknown
MapName	Map file name	SamplePO.sun
	Note: The Import utility does not verify if the specified map exists in the maps directory. If it does not exist, documents sent using the partnership will not be translated.	
MapDirection	Translation type.	1= XLTinbound (EDI-to-Application)
AckExpected	Is functional acknowledgment expected?	0
DocLastControlNumber	Last control number generated	1
DocLock	(internal use)	0
PrimaryXportType	Primary transport protocol. Requires a delimiter of (|) or (;).	ftp-local-application
PrimaryXportParam	Primary transport protocol parameter	TP|ftp-local-application;HN|hostname;PT|;UN|username;PW|userpassword;SS|test1;RS|;OD|tmp;ID|;IT|;MD|I,
SecondaryXportType	Alternate transport protocol.	—
SecondaryXportParam	Alternate transport protocol parameter	—
SendType	Immediate or scheduled	1
DeleteWaitPeriod	Retention period (days) before delete	5
ArchiveWaitPeriod	Retention period (days) before archiving (not used in release 3.6)	0
PreEnveloped	Is data pre-enveloped?	2 = PEnonenveloped (bundle generates and/or replaces all envelopes)

Control Structure Example for Deleting Partnerships

You can use the import utility not only to populate the database with new member and partnership data, but also to delete existing data.

To delete partnership data, use the "delete" operation instead of the "insert" operation, and use *only* the following fields in your data file control structure: SenderName, ReceiverName, DocType, StandardVersion, StandardRelease.

CAUTION	If you use the same import data file that you used to insert a partnership, but change only the operation from "insert" to "delete," you will not be able to delete the Partnership.

In the command below, delete.imp is specified as the data file:

import *user password* delete.imp *log_file discard_file*

The contents of the delete.imp file are listed below. It contains a set of control structures and data for the member object.

```
#
# Deleting a Partnership
#
[object = partnership; field_delim = ","; operation = delete;
fields = SenderName, ReceiverName, DocType, StandardVersion,
StandardRelease]

test1, kmem2, 850, 003020, 0
```

Table 11-8 describes the fields included in the delete.imp example, as well as their specific values in the imported data.

Table 11-8 Fields in the sample imported custom service

Field Name	Description	Value in the Example File
Partnership Address Data Fields		
SenderName	Sending member name	test1
ReceiverName	Receiving member name	kmem2
DocType	Document type	850
StandardVersion	EDI standard version number	003020
StandardRelease	EDI standard release number	0

Control Structure Example for Importing Services

The `service` object allows you to populate the database with new custom services. The user can then define a service list using this custom service.

In the command below, `insert.imp` is specified as the data file:

import *user password* insert.imp *log_file discard_file*

The contents of the `insert.imp` file are listed below.

```
#
# insert.imp
#
# used to insert new service
#

[object = service; field_delim = "|"; operation = insert; fields
= Name, Type, PathName, EntryName, MaxThread, Param, ObjPerm ]


test1 | 2 | /disk1/actraadm/service/CustomSvr.pl | none | 1 |
Test Service 1 | 755
```

Table 11-9 describes the fields included in `insert.imp` as well as their specific values in the imported data.

Table 11-9   Fields in the sample imported service list

Field Name	Description	Value in the Example File
Name	Service Name	test1
Type	Service Type	2= STscript (ECXpert external script)
PathName	Path name to the service script or executable	`/disk1/actraadm/service/CustomS vr.pl`
EntryName	Entry name	none
MaxThread	Maximum number of threads	1
Param	Service description	Test Service 1
ObjPerm	Object permission	755

Control Structure Example for Importing Service Lists

The following example illustrates the use of the `import` utility to import service list data from a text file. In the command below, `insert.imp` is specified as the data file:

`import` *user password* `insert.imp` *log_file discard_file*

The contents of the `insert.imp` file are listed below. It contains two service lists:

• The first, `smtp-snd-test`, has two services in it, Outprep and Gateway.

- The second service list, `ftp-rec-test`, has three services, Parse, Translate and Gateway:

```
#
# insert.imp
#
# used to insert new service list
#

[object = servicelist; field_delim = "|"; operation = insert;
 fields = ServiceListName, SeqNum, SndrMBName, RcvrMBName,
TypeName,
      SVRId, SVRName, ServiceParams, ErrorHandler, Desc,
      ObjPerm ]

#
smtp-snd-test | 1 | SenderName | RcvrName | app |\
207 | Outprep | | | Sending SMTP  | 644

smtp-snd-test | 2 | SenderName | RcvrName | app |\
704 | gateway | | | Sending SMTP | 644

#
ftp-test-rec | 1 | Sender | Receiver | EDI |\
201 | parse | | | recv from GEIS | 644

ftp-test-rec | 2 | Sender | Receiver | EDI |\
203 | translate | | | recv from GEIS | 644

ftp-test-rec | 3 | Sender | Receiver | EDI |\
704 | gateway | | | recv from GEIS | 644
```

Table 11-10 describes the fields included in the insert.imp example file as well as their specific values for the first service list.

Table 11-10 Parameters for the `importCertificate` command

Field Name	Description	Value in the Example File
ServiceListName	Service List Name	smtp-snd-test
SeqNum	Order of the service in service list	1, 2

Table 11-10 Parameters for the `importCertificate` command *(Continued)*

Field Name	Description	Value in the Example File
SndrMBName	Sender Name	SenderName
RcvrMBName	Receiver Name	RcvrNam
TypeName	Document Type	app
SVRId	Service ID	207=OutPrep, 704=Gateway
SVRName	Service Name	Outprep, gateway
ServiceParams	Service Parameters	—
ErrorHandler	Exit Service List	—
Desc	Service Description	Sending SMTP
ObjPerm	Object permission	644

importCertificate—Importing Certificates

The `importCertificate` command allows you to import a certificate from a file for an ECXpert member, or to import an new root certificate.

Syntax

The syntax of the `importCertificate` command is as follows:

`importCertificate -f` *certFileName* **`[-r|nr] [-b|nb] -ct`** *certType*
`-m memberName -el|-er`

Parameter	Usage
-f *certFileName*	File name, where *certFileName* is the full path to the certificate file being imported.
-b|-nb	Is the certificate base64 encoded (-b) or not (-nb)? Optional—the default is -b if -nb is not specified.
-r|-nr	Is the certificate a root (-r) or not (-nr)? Optional—the default is -nr if -r is not specified.

Parameter	Usage
-ct *certType*	The certificate type, where *certType* is the type of certificate being imported. - if a root already exists for this type of certificate, pass the name of the root as *certType* (this name is case sensitive—if you are not sure of the exact name, look it up in the Product Administrative Interface, Certificates tabs; refer to Chapter 9, "Working with Certificates"," for detailed instructions) - if this is a new root, pass 0 as *certType* and pass the new root name as *memberName*.
-m *memberName*	Member name, where *memberName* is the member ID of the ECXpert member for whom the certificate is being imported. If the certificate is a new root, then *memberName* is the new root name.
-el|-er	The local (-el) or remote (-er) email address member qualifier associated with the certificate. Omit if certificate being imported is a new root.

Example

If you have a new root certificate in a file named newroot.cert in the directory *$NSBASE*/NS-apps/ECXpert/certificates/import/, and you want to use the root name "special2" with the certificate, you would use the importCertificate command as follows:

importCertificate -f
***$NSBASE*/NS-apps/ECXpert/certificates/import/newroot.cert -r ct 0 -m**
special2

If you have a certificate for in a file named `stormy.cert` in the directory *$NSBASE*/NS-apps/`ECXpert/certificates/import/`, and you want to import the certificate for member ID "stormy" for use with that user's local email address, you would use the `importCertificate` command as follows:

```
importCertificate -f
$NSBASE/NS-apps/ECXpert/certificates/import/stormy.cert -nr -ct
special2 -m stormy
```

NOTE	In each example, the command must be typed on a single line with spaces separating each of the parts—in other words, the multiple lines shown in the examples above must be typed on a single line when entered as a command.

bdggenManifest and bdgrealpurge—Purging Aged Data

ECXpert provides a purge service for removing old, obsolete database tracking and event log rows and all the associated obsolete files that have passed the retention period.

This purge service is a two-step process implemented by two executables (both located in *$NSBASE*/NS-apps/`ECXpert/data`):

- `bdggenManifest` marks the documents and generate a manifest file (*$NSBASE*/NS-apps/`ECXpert/data/purge.manifest`) that lists all the associated file names.

- `bdgrealpurge` performs the actual purge.

NOTE	Running `bdggenManifest` first to generate a manifest *is not required* in order to run `bdgrealpurge` and actually purge the aged data. Generating the manifest first simply gives you an opportunity to examine it and verify that no data that you still need is at risk.
	If you choose to run `bdgrealpurge` without running `bdggenManifest` first, a manifest listing will still be generated in the location specified by the `manifest_filename` parameter in the `[purge]` section of the `ecx.ini` file.
	Optionally, you can use the generated manifest of files to archive certain files or change the retention period before running `bdgrealpurge`. ECXpert does not provide the archiving utility; you must supply one.

ECXpert Configuration File *[purge]* Parameters

Parameters in the `[purge]` section of the ECXpert configuration file (`ecx.ini`) control the way the ECXpert purge programs operate.

Be sure to set the following two parameters in the `[purge]` section of the ECXpert configuration file (`ecx.ini`) before you run the `bdgrealpurge` utility.

Entry	Description
`manifest_filename`	The full path to the manifest file that will contain the listing of all documents to be purged. Default value is `$NSBASE/NS-apps/ECXpert/data/purge.manifest`, where `$NSBASE` is the directory under which you installed ECXpert.
`default_retention_p eriod`	The default number of days to retain files before purging. This value will be used if no retention period is defined in the related partnership. Default value is 5.

Affected Database Tables and Directories

The following database tables that are affected by the `bdgrealpurge` command:

- `Tracking`

- `TrkIntchg`

- `TrkGroup`

- `Trkdoc`

- `TrkDocDetails`

- `EventLog`

- `UniqueKey`

See the *iPlanet ECXpert Developer's Guide*, "ECXpert Database Schema" appendix, for documentation of these tables.

Following are the directories where obsolete files are deleted:

- *$NSBASE*/NS-apps/`ECXpert/smtp/log`

- *$NSBASE*/NS-apps/`ECXpert/smtp/inbound`

- *$NSBASE*/NS-apps/`ECXpert/smtp/inmsg`

- *$NSBASE*/NS-apps/`ECXpert/smtp/outbound`

- *$NSBASE*/NS-apps/`ECXpert/smtp/outmsg`

- *$NSBASE*/NS-apps/`ECXpert/smtp/archive/sent`

- *$NSBASE*/NS-apps/`ECXpert/smtp/archive/unsent`

- *$NSBASE*/NS-apps/`ECXpert/data/bundle`

- *$NSBASE*/NS-apps/`ECXpert/data/work/trk`

- *$NSBASE*/NS-apps/`ECXpert/data/output`

Using *bdggenManifest* and *bdgrealpurge* on Solaris

To successfully run the `bdggenManifest` or `bdgrealpurge` command, you must set your `$PATH` to include `$NSBASE/NS-apps/ECXpert/bin` and set your `$LD_LIBRARY_PATH` to include `$NSBASE/NS-apps/ECXpert/lib`.

You must also do one or the other of the two actions listed here:

- change to the `$NSBASE/NS-apps/ECXpert/bin` directory before you run the command

-OR-

- when you run the command, enter the absolute path to the `bdggenManifest` or `bdgrealpurge` executable:

  ❍ `$NSBASE/NS-apps/ECXpert/bin/bdggenManifest`

  ❍ `$NSBASE/NS-apps/ECXpert/bin/bdgrealpurge`

Using bdggenManifest

The following command will create a manifest file that contains the manifest listing of all database tracking and event log rows and all the associated files that have passed the retention period specified in the `ecx.ini` file.

bdggenmanifest -in *$NSBASE*/NS-apps/ECXpert/config/ecx.ini

where *$NSBASE* is the directory under which you installed ECXpert.

The manifest file is created in the location specified in the `ecx.ini` file.

Using bdgrealpurge

You can use the `bdgrealpurge` command in any of the following three ways:

The following command will purge all ECXpert database tracking and event log rows and all associated files that have passed the retention period specified in the `ecx.ini` file:

bdgrealpurge -in $NSBASE/NS-apps/ECXpert/config/ecx.ini

where *$NSBASE* is the directory under which you installed ECXpert.

The following command will purge all ECXpert database tracking and event log rows and all associated files, regardless of whether they have passed the retention period specified in the ecx.ini file, and will reset the `UniqueKeys` table back to zero for tracking related items.

bdgrealpurge -in $NSBASE/NS-apps/ecxpert/config/ecx.ini -all -reset

The following command will purge all ECXpert database tracking and event log rows and all associated files, regardless of whether they have passed the retention period specified in the `ecx.ini` file, but will *not* reset the `UniqueKeys` table back to zero for tracking related items.

**bdgrealpurge -in $NSBASE/NS-apps/ECXpert/config/ecx.ini -all
-noreset**

where *$NSBASE* is the directory under which you installed ECXpert.

NOTE   **Important:** The `-reset` option should *only* be used with the `-all` option.

Using *bdggenManifest* and *bdgrealpurge* on Windows NT

To successfully run the `bdggenManifest` or `bdgrealpurge` command on Windows NT, you must enter the absolute path to the `bdggenManifest` or `bdgrealpurge` executable when you run the command:

```
C:\$NSBASE\NS-apps\ECXpert\bin\bdggenManifest
```

```
C:\$NSBASE\NS-apps\ECXpert\bin\bdgrealpurge
```

Using bdggenManifest

The following command will create a manifest file that contains the manifest listing of all database tracking and event log rows and all the associated files that have passed the retention period specified in the ecx.ini file.

From the Windows NT Desktop, choose **Start** > **Run**.

In the **Run** dialog box that appears, type the following command:

```
C:\$NSBASE\NS-apps\ECXpert\bin\bdggenManifest
```

where C:\ is the drive on which you have installed ECXpert and *$NSBASE* is the directory under which you have installed ECXpert.

The manifest file is created in the location specified in the ecx.ini file.

Using bdgrealpurge

You can use the bdgrealpurge command in any of the following three ways:

- To purge all ECXpert database tracking and event log rows and all associated files that have passed the retention period specified in the ecx.ini file:

  ```
  C:\$NSBASE\NS-apps\ECXpert\bin\bdgrealpurge -in
  C:\$NSBASE\NS-apps\ECXpert\config\ecx.ini
  ```

  where C:\ is the drive on which you have installed ECXpert and *$NSBASE* is the directory under which you installed ECXpert.

- To purge all ECXpert database tracking and event log rows and all associated files, regardless of whether they have passed the retention period specified in the ecx.ini file, and will reset the UniqueKeys table back to zero for tracking related items.

  ```
  C:\$NSBASE\NS-apps\ECXpert\bin\bdgrealpurge -in
  C:\$NSBASE\NS-apps\ECXpert\config\ecx.ini -all
  ```

- To purge all ECXpert database tracking and event log rows and all associated files, regardless of whether they have passed the retention period specified in the ecx.ini file, but will *not* reset the UniqueKeys table back to zero for tracking related items.

  ```
  C:\$NSBASE\NS-apps\ECXpert\bin\bdgrealpurge -in
  C:\$NSBASE\NS-apps\ECXpert\config\ecx.ini -all -noreset
  ```

  where *$NSBASE* is the directory under which you installed ECXpert.

NOTE   **Important:** The -noreset option can only be used in conjunction with the -all option.

---

bdggenManifest and bdgrealpurge—Purging Aged Data

Introduction to EDI Concepts

This appendix provides a brief introduction to basic concepts of electronic data interchange (EDI). The following topics are presented:

- History of EDI
- EDI Concepts

History of EDI

Automated Data Processing within a Business

In the 1950s, large business enterprises began automating their routine paperwork. By the late 1960s, core business functions like purchasing, billing, and accounting were taken over by large business data processing systems in most larger organizations.

In general, these systems were implementations of entirely independent, proprietary solutions restricted in scope to a single organization. For example, the system at Company A would generate a purchase order that had to be mailed to Company B, and data entry workers at Company B had to re-key the data from the paper form to get the data into their system.

The process of mailing and re-keying paper documents was expensive and error-prone. Connecting the systems at Company A and Company B through a telecommunications connection was the obvious next step. Each company's systems had been developed independently, however, using incompatible proprietary data formats. This made it impossible for the two systems to "talk to" each other even when a physical connection was established.

It would have taken considerable time to write programs that could translate Company A's invoices into the precise form that Company B's system required, and the cost of doing this for hundreds of different "Company B's" was prohibitive. Clearly there had to be a better solution.

The Electronic Data Interchange (EDI) Bridge

Electronic Data Interchange (EDI) was developed to allow data processing systems to "talk to" each other even though the two systems use different proprietary data formats. The concept behind EDI was to define an *EDI standard format* for each different type of business document.

Programmers at Company A could then write code to translate their system's proprietary invoice format into an EDI standard invoice format. Company A could then send electronic invoices to any other company that supported EDI.

Likewise, programmers at Company B could write code to translate the EDI standard format into their system's proprietary invoice format. Company B could then receive electronic invoices from any other company that supported EDI.

Any two companies that want to exchange business documents electronically can now set up a *trading partner agreement* (also called a *trading partnership*), specifying which EDI standard formats will be used between them and how the documents will be transmitted. This agreement also specifies all legal and business requirements that are to be met when exchanging EDI transmissions.

Value Added Networks (VANs)

As companies adopted EDI, value added networks (VANs) began offering the telecommunications links between those companies' systems. Some VANs also supported certain proprietary formats.

The value that these VANs added was:

- Communications protocol conversion
- Storage for retrieval
- Audit trails
- Consulting
- Trading partner implementation programs

Business Moves to the Internet

The Internet was originally established to allow university researchers, defense contractors, and military planners to exchange email and data files between many different types of computers scattered all over the world. In the mid-1990's business suddenly "discovered" that the Internet was often the best, cheapest, easiest-to-implement way to connect their computers as well.

The Internet provides businesses with an environment that is more open, faster, lower in cost, and more widely deployed than any proprietary alternative.

EDI Concepts

The following sections explain these basic EDI concepts:

- Electronic data interchange

- EDI translation and mapping

- A document, message, or transaction set

- EDI standard formats for document types

- The electronic envelope

- Enveloping and parsing

- Trading partners and trading partner agreements

- The Functional Acknowledgment (FA) and the CONTRL message

Electronic Data Interchange

Electronic data interchange (EDI) is a set of standardized formats for different types of business documents that allow otherwise incompatible business data processing systems to exchange documents without manual intervention.

Its standardized formats permit a company's programmers to write code to convert the proprietary formats of a company's legacy systems to and from EDI standards. The company is then able to exchange business documents electronically with any other company that supports EDI.

Worldwide, two different EDI standards have become the most commonly used. One, the ANSI X12 standard, is maintained by the American National Standards Institute's X12 Committee and is used widely in North America. ANSI X12 document types have numeric identifiers.

The other standard, EDIFACT (Electronic Data Interchange For Administration, Commerce, and Transportation), is an international implementation of EDI sponsored by the United Nations and the European Union. EDIFACT is widely used for messages exchanged internationally and for messages exchanged within a country that has adopted EDIFACT as its national EDI standard. EDIFACT document types have alphanumeric identifiers.

EDI Translation and Mapping

EDI translation is the process of converting data in application-specific, or proprietary, formats to and from EDI standard formats.

Originally this required programmers to write application code. Currently, third party translation software is widely available to expedite this process. In general, this software helps a user to create a "map" file that specifies in detail how a particular type of business document in a proprietary format is to be represented in a standard EDI format, or vice-versa. This process is called *mapping*.

The Map Definition Tool bundled with ECXpert is *Mercator*, developed by TSI International. ITo perform EDI translation, a Map Execution Engine built into ECXpert reads the map file produced by *Mercator*.

Document, Message, or Transaction Set

In EDIFACT terminology, the business document that EDI revolves around is called a message, or a transaction set. In ANSI X12 terms, it is commonly referred to as a document.

To minimize possible confusion, this Guide uses the term "document" or "business document" (instead of "message" or "transaction set").

EDI Standard Formats for Document Types

Each of the EDI standard formats describes a particular type of business document. These are commonly referred to as document types.

Each document type definition specifies the syntax, or rules governing the allowable structure of the documents transmitted under *EDI*, including the following:

• Valid data types and relationships within a segment

• Valid order, position, and frequency of repetition of segments in a document

• Organization of documents composing functional groups and interchanges

The EDI structural elements below the document level are described below. Structural elements above the document level are described in "Electronic Envelope" on page 539.

Data Element

A data element is the fundamental unit of information within an EDI document. It contains the primary data that remains intact when the document is translated between EDI and proprietary formats. A data element is comparable to a *field* in a database.

Data elements sometimes are divided into sub-elements. The most common example of this is the use of the first few characters of a data element as a qualifier that specifies how the data in the remainder of the field is to be interpreted. The trading partner ID qualifier is the one you encounter most frequently.

Data Segment

A data segment is a structured sequence of data elements, separated by data element separators (special characters that cannot be used in the data), and ended by a segment terminator (another special character). Some number of data segments make up an EDI document.

A data segment is comparable to a *record* in a database. A data segment might also be comparable to a line item on a printed form, when similar data segments repeat within a document.

Electronic Envelope

Even if only one document at a time is sent, there is still a need for the type of information that might be included on a paper envelope for a printed document, such as the identify of the sender and recipient.

In the electronic environment of EDI, multiple documents can be combined in the same package, requiring additional levels of information for the "electronic envelope."

Document Envelope

The EDI document envelope includes the address of the intended recipient and the return address of the sender. For the recipient to properly interpret the document, the exact EDI document type (and version number) must also be specified.

Functional Group Envelope

A *functional group* is a collection, or batch, of one or more documents that is being sent to the same trading partner and that share a logical correlation.

In ANSI X12, functional groups are required and each functional group must consist of documents of the same document type and of the same group type as defined by the standard (for example, PO, IN).

In EDIFACT, functional groups are optional and, if present, must consist of documents of the same document type.

Interchange Envelope

An interchange is the highest level of enveloping in EDI.

In an ANSI X12 interchange, the interchange is made up of one or more functional groups. In an EDIFACT interchange, functional groups are optional.

Transport via SMTP requires one interchange per message file.

Enveloping and Parsing

The process of combining multiple documents for transmission as a unit in EDI is called *enveloping*. This is also referred to as bundling.

Parsing reverses this process, extracting all the data components of each separate document so that the data can be processed.

Trading Partners & Trading Partner Agreements

A *trading partner* in EDI is an external business party to whom you send, or from whom you receive, business documents.

A *trading partner agreement* is a contractual agreement between two business parties that specifies all legal and business requirements that are to be met when exchanging EDI documents as trading partners.

Functional Acknowledgment (FA), and CONTRL Message

In the ANSI X12 standard (document type 997), a *functional acknowledgment* is a message sent to the sender acknowledging that a particular functional group has been received and compliance checked.

A functional acknowledgment indicates the syntactical correctness of the business documents that have been received, informing the sender of any problems encountered, but does *not* deal with application-specific data content.

ECXpert supports functional acknowledgment at both the functional group and document levels.

In the EDIFACT standard, a *CONTRL message* is a message sent to the sender acknowledging that a particular interchange has been received and compliance checked. Like a functional acknowledgment, a CONTRL message indicates the syntactical correctness of the business documents that have been received, informing the sender of any problems encountered, but does *not* deal with application-specific data content.

ECXpert supports CONTRL messages at the interchange, functional group, and document levels.

EDI Concepts

Constructing and Referencing A Stylesheet for an XML Document

This appendix describes the construction guidelines for a stylesheet and the referencing of the stylesheet in the ecxstylesheets.xml initialization file. The following topics are presented:

- Overview
- Stylesheet Construction Guidelines
- Structure of the ecxstylesheets.xml Configuration File

Overview

The ECXpert XML parser reads configuration information from the `ecxstylesheets.xml` configuration file. This file is in the `$BDGHOME/config` directory.

The ECXpert XML parser refers to this file for information such as the base directory for the stylesheet, mappings from a DTD name to a XSL stylesheet name, and a listing(s) of the external library to be loaded in case a stylesheet cannot be obtained from data in the incoming document.

The path to this file is specified in EcxStylesheet section of the the ecx.ini file. The contents of this file can be modified through the Admin UI. Refer to "Creating an Entry for the [EcxStylesheet] Section" on page 143.

Stylesheet Construction Guidelines

The stylesheet that relates to the xml document should provide the following output HTML / XML structure:

The senderid, receiverid and doctype tags are mandatory. In the absence of any of the other tags, a default value of NONE is assigned to the corresponding parameters in the partnership user interface, input XML tab.

The data that is listed below is what the intermediate output should look like after the incoming XML Document is processed with the stylesheet. In short, the stylesheet should present the listed data.

```
<ecx>
        <senderid>
                value
        </senderid>
        <receiverid>
                value
        </receiverid>
<senderqualifierid>
                value
        </senderqualifierid>
        <receiverqualifierid>
                value
        </receiverqualifierid>
        <doctype>
                value
        </doctype>
        <docid>
                value
        </docid>
        <standard>
                value
        </standard>
<version>
                value
        </version>
        <release>
                value
        </release>
</ecx>
```

Structure of the ecxstylesheets.xml Configuration File

The ecxstylesheets file has the following structure:

```
<ecxstylesheets>
        <stylesheetbase>
                < !-- This is where you specify the base directory
 for the
    stylesheet -->
        </stylesheetbase>
        <mappings>
          <!-- This section specifies the mapping from a DTD name
to a stylesheet
  name -->
            <map>
                 <name>
                          <!-- DTD Name -->
                </name>
                <value>
                        <!-- Stylesheet Name -->
                </value>
            </map>
                .
                .
            <map>
                  .
                  .
            </map>
        </mappings>
        <plugins>
          <!-- This section specifies the list of libraries,
 their
            corresponding parameters are specifies as name value
pairs -->
            <library name= "{name of the library eg. libxyz.so} ">
            <param name = "{param. name eg. initData}">
                <!-- Value of the parameter  {eg. 0 i.e initData =
0} -->
            </param>
        </library>
                    .
                    .
        <library name="...">
          <param name = "..."> ... </param>
        </library>
     </plugins>
</ecxstylesheets>
```

Refer to Table B-1 for details on each section in the above file.

Table B-1   Detailed Explanation of Each Section in ecxstylesheets.xml

Section	Description	Comments
Root Element : `<ecxstylesheets>`	`<ecxstylesheets>` is the tag for the root of the xml document.	

Specifying the Stylesheet Path: `<stylesheetbase>`	The path to the stylesheet directory where all the stylesheets are stored is indicated using the `<stylesheetbase>` tag. An example would be:
	
	 ```<stylesheetbase>```
	 ```/export/local/newECX35/NS-apps/ECXpert/data/stylesheet/```
	 ``` </stylesheetbase>```	

Mapping from a DTD to a stylesheet	The mappings element contains the element map which has name and value tags to map from a specific DTD name to a stylesheet. For example, to map from `PO.dtd` to `PO.xsl` the mappings section on the `ecxstylesheets.xml` file should be as follows:
	
	 ```<mappings>```
	 ``` <map>```
	 ``` <name>PO.dtd</name>```
	 ``` <value>PO.xsl</value>```
	 ``` </map>```
	 ```</mappings>```
		Multiple map elements can exist within a parent mappings element.

Loading a userdefined plugin	The plugins element contains a library element having an attribute name that specifies the name of the library and contains a param element, the value of which is the value of the paramater. The param element has an attribute name which specifies the name of the parameter. (continued next page)	The plugins section can have more than one library element.

Table B-1   Detailed Explanation of Each Section in ecxstylesheets.xml

A library can have multiple param elements. These name-value pairs specified by the parameter are passed to the initialization function of the plugin. For example, if you have a library named `myLib.so` and you need to pass to the initialization routine a paramater "base" which has value "`/export/stylesheet`", the plugins element will be as follows:

```
<plugins>
  <library name= "myLib.so">
     <param name = "base">
        "/export/stylesheet"
     </param>
  </library>
                  .
                  .
  <library name="...">
     <param name = "..."> ... </param>
  </library>

</plugins>
```

Overview

ECXpert Initialization File (ecx.ini)

This appendix documents the system settings, stored in the `ecx.ini` file, that you can modify through ECXpert's System Administration Interface. The following topics are documented:

- Overview
- Alphabetical Listing of Sections
- Scaling the ECXpert Engine Threads
- System Settings by Section

Overview

The ECXpert system settings are stored in the `ecx.ini` file, located in the *$NSBASE*/NS-apps/`ECXpert`/`config`/ directory. You should avoid editing this file directly, making changes only through the System Administration Interface.

See "Managing ECXpert System Settings" on page 136 for more about changing the `ecx.ini` file.

NOTE   Always back up the `ecx.ini` file before making any changes to it, even through the System Administration Interface.

Unique Port Numbers

If you change the port type to static (`admin_port_type=static`, or `listener_port_type=static`), all port numbers assigned to ECXpert servers (`section_type=server`) must be unique.

The default setting for all port types is dynamic. With this default setting, the assigned port number is ignored. If you assign the same port number to multiple servers with static port type set to static, only the first server started on that port will come up.

Year 2000 Compliance

ECXpert is enabled for year 2000 compliance, but you must set certain parameters correctly. Each Communications Agent (is_comm_agent = yes) has a use4digit_year parameter that must be set to yes to turn on year 2000 compliance for that Communications Agent.

NOTE	This is only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072, version 4010, and later versions).

Creating an EDI Envelope With an Eight-Digit GSO4 Date

To enable ECXpert to create an EDI envelope that uses an eight-digit date in the GS04 field, you must add the following keyword-value pair to the applicable comm agent section in the ECXpert configuration file (ecx.ini) :

```
use4digit_year = yes
```

For example, if you are using use an Application-to-EDI Partnership, and the outgoing protocol is FTP, you must add the above keyword-value pair to the appropriate ftp section of the configuration file, as shown below:

```
[ftp-local-edi]
...
use4digit_year = yes
```

The use4digit_year parameter tells ECXpert to use "1999" instead of "99," or "2000" instead of "00" in the GS04—but only for versions of the X12 standard which support an eight-digit GS04 value.

The versions of the X12 standard that support this are 3072 and 4010. However, for ECXpert - Solaris, this is only supported for version 4010 (and later versions).

For ECXpert - Solaris, the following four conditions must be in place for ECXpert to properly format the eight-digit date:

5. You must be using the X12 standard version 4010, or a later version, in your trading agreement with your trading partner.

6. You must add the `use4digit_year` parameter to the `ecx.ini` file in the appropriate `comm agent` section.

7. The `use4digit_year` parameter must be set to `yes`.

8. This only applies to Partnerships where the Output EDI enveloping option has been set to "ECX generates (or overrides) the entire envelope."

When all of these conditions are met, you will get a date formatted like this:

`19990121`

instead of a date formatted like this:

`990121`

in the GS04 field of the envelope ECXpert generates for the bundled file.

Alphabetical Listing of Sections

The configuration file sections in this appendix are shown here in the order in which they appear in the `ecx.ini` file. This order is based on related functions.

If you know the name of a particular section, you can use the alphabetical listing, below, to locate the section quickly.

Table C-1   Alphabetical listing of configuration file sections

`ecx.ini` File Section	What the Section Settings Control/Configure
"[admin] Section" on page 561	Administrative Server
"[attributes] Section" on page 711	lists descriptions for parameters in all sections
"[comm_ftp_geis] Section" on page 621	Communications Agent for GEIS FTP protocol
"[commhttp-aiag] Section" on page 647	Communications Agent for AIAG HTTP protocol (automotive industry)
"[commhttp-gisb] Section" on page 653	Communications Agent for the GISB HTTP protocol (natural gas industry)
"[commhttp-ssl] Section" on page 627	Communications Agent for SSL over OBI
"[commhttp-ssl-XML] Section" on page 633	Communications Agent for SSL over XML

Table C-1   Alphabetical listing of configuration file sections *(Continued)*

`ecx.ini` File Section	What the Section Settings Control/Configure
"[commsmtp-receive] Section" on page 594	Communications Agent for receiving using SMTP
"[commsmtp-send] Section" on page 588	Communications Agent for sending using SMTP
"[comm_ftp_geis] Section" on page 621	Communications Agent for sending and receiving using GEIS FTP
"[DB_SECTION] Section" on page 697	Controls aspects of database interface that are vendor-independent
"[dispatcher] Section" on page 581	Dispatcher
"[ecxftp-client] Section" on page 663	ECXpert FTP client
"[ecxftp-server] Section" on page 658	ECXpert FTP server
"[ecxoftp-server] Section" on page 615	ECXpert OFTP server
"[ecxpa-server] Section" on page 664	ECXpert Partner Agent for ECXpert Server server
"[EcxStylesheet] Section" on page 586	ECXpert Stylesheet path for xml.
"[eXML-connector] Section" on page 676	ECXpert XML connector
"[FAGen] Section" on page 695	Functional acknowledgment generation
"[ftp-local-application] Section" on page 602	Communications Agent for sending and receiving application data using local FTP
"[ftp-local-edi] Section" on page 608	Communications Agent for sending and receiving EDI data using local FTP
"[gateway] Section" on page 569	Communications servers, such as those for FTP and SMTP
"[http-retrieve] Section" on page 580	HTTP server's data retrieval
"[import-certificates] Section" on page 586	Defaults used in the process of importing certificates
"[LDAP] Section" on page 684	LDAP support
"[legacy-mq-series] Section" on page 708	Legacy Server for MQSeries
"[legacy-oracle-apps] Section" on page 699	Legacy Server for Oracle Applications
"[legacy-sap] Section" on page 705	Legacy Server for SAP
"[membership] Section" on page 683	Sets membership to use either ECXpert database or LDAP

Table C-1   Alphabetical listing of configuration file sections *(Continued)*

`ecx.ini` **File Section**	**What the Section Settings Control/Configure**
"[migrate] Section" on page 682	Migration of ECXpert database schema
"[ORACLE_ENV] Section" on page 696	Vendor-specific aspects of Oracle database interface
"[parse] Section" on page 688	Parsing data in outbound submission units
"[poll] Section" on page 587	Polling for presence of new submission units
"[purge] Section" on page 601	Operation of ECXpert purge utilities (`bdggenManifest` and `bdgrealpurge`)
"[retrieve] Section" on page 578	Manual receipt of data (using `poll` command)
"[scheduler] Section" on page 671	Scheduler
"[snmp] Section" on page 560	SNMP support
"[Split] Section" on page 690	Split service
"[submit] Section" on page 600	Submission Agent (`submit` command)
"[system] Section" on page 559	Global ECXpert system settings
"[tcpip-connector] Section" on page 573	Communications Agent for sending and receiving EDI data using TCP/IP
"[TradingXpert] Section" on page 669	Interface with TradingXpert
"[translate] Section" on page 691	Translation of data formats
"[ui_section] Section" on page 695	User interface operation
"[user-defined-#] Sections" on page 685	Operation of specific user-defined communications processes

Scaling the ECXpert Engine Threads

In multiple sections of the ecx.ini file, the same parameters (shown in Table C-2) appear and are used in the same way to control ECXpert's use of threads for the process controlled in the section.

By tuning these parameters, you can manage the number of file handles and the number of server processes that run at any one time, to optimize ECXpert performance on your hardware.

Table C-2   Thread control parameters in the configuration file

Entry	Description
max_listeners	Maximum number of listener threads allowed.
listener_level	Listener level. Number of listener threads to launch on startup. *Default*: 1; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
master_max_threads	Maximum number of master threads to run in parallel.
master_max_threads_queued	Maximum number of master threads to queue.
master_max_threads_queued_flag	Whether master thread are to queue (yes/no).
worker_max_threads	Number of worker threads to run in parallel.
server_type	Type of server.
admin_time_out	Admin server time out period, in seconds.

The following sections provide more information about setting the parameters shown in Table C-2.

Process Threading

Figure C-1 presents the ECXpert threading model in graphical form, related specifically to the ECXpert Dispatcher. Refer to this diagram as you follow the accompanying text.

Figure C-1 ECXpert threading model

In Figure C-1, when a request is received by the Dispatcher from the TCP/IP Connector, it is received by the ECXpert Listener thread. The Listener thread then spawns a Master Thread for the Dispatcher, and then it spawns one or more Worker Threads to actually perform the task. In the case of the Dispatcher, the Worker Thread is in charge of the service list for the incoming file.

The `master_max_thread_stacked` parameter is used to control the number of requests that can be sitting in the TCP/IP system queue. Because it takes time for the Listener to spawn Master Threads to handle the request, and the number of Master Threads that can be spawned at any one time is also limited, requests will be queuing at the Listener level. The number of requests that can be queued up at the Listener is controlled by the parameter `master_max_thread_stacked`.

Each process can also have more than one Listener running. By default, the number of Listeners is one and is controlled by the `listener_level` parameter. Currently, this must not be changed; ECXpert automatically increases the number of Listeners as processing proceeds, up to the maximum number allowed. The number of Listeners running cannot exceed the value set in the `max_listeners` parameter.

When a Listener spawns a new Master Thread for a request, it can be in either one of two possible states, namely running or blocked. The maximum number of Master Threads running at once is controlled by the parameter `master_max_threads`. If that number is reached, any new Master Thread spawned by the Listener is blocked on a semaphore.

Each Master Thread requires opening a new socket. To control the number of sockets being opened, ECXpert also limits the number of Master Threads that can be in a blocked state. That number is governed by the parameter `master_max_threads_queued`.

So at any one time, the total number of Master Threads that can be spawned by the Listener is `master_max_threads` + `master_max_threads_queued`. This includes both those that are running and those that are blocked. Note that `master_max_threads_queued_flag` must be set to `yes`; if it is not, all connections will result in a Master Thread being spawned.

The Master Thread spawns Worker Threads to perform the actual operation on the incoming file. The Master Thread can spawn as many Worker Threads as needed to process the file, but the number of running Worker Threads is controlled by the parameter `worker_max_threads`. All the non-running Worker Threads are blocked until a running Worker Thread has finished its work.

Multiple Processes per Server

ECXpert Version 1.0.2.1 and higher also uses a multiple process model for each server. On Solaris, the recommended maximum number of file descriptors is 1024. Thus if the system is overloaded with a large number of requests, a single process risks running out of file descriptors.

By allowing multiple processes of the same service running at the same time, more file descriptors are available for use. The load is also distributed across multiple processors for processing.

The ecx.ini file now allows the following syntax, illustrating setting up two instances of the Dispatcher:

```
[dispatcher]
section_type = server
server_type = 3
snmp_trap_flag = no
snmp_trap_level = 0
port_location = mmap
...
stderr_path =
$NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.dispatcher.dat
stdout_path =
$NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.dispatcher.dat
...

[dispatcher02]
section_type = server
server_type = 3
snmp_trap_flag = no
snmp_trap_level = 0
port_location = mmap
...
stderr_path =
$NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.dispatcher02.dat
stdout_path =
$NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.dispatcher02.dat
...
```

The matching `server_type` value (3 in the above example) identifies these two servers as being separate instances of the same process. When the Dispatcher is started up, in this case it will start two processes for the Dispatcher service.

NOTE	If you manually edit the `ecx.ini` file to create additional sections for a particular server, as in the above example for Dispatcher, make sure that you *do not change the name of the original section*. In the Dispatcher example, the first Dispatcher section must *always* be named `[dispatcher]`.
	Make sure that you **do** *change the name of the log files* for additional instances of the same server, as was done in the example above for Dispatcher. If multiple processes are writing to the same log file, there is no way to determine which process was the source of a particular message.

The diagram in Figure C-2 demonstrates this configuration.

Figure C-2   ECXpert process model

When an NSClient object (piece of code ECXpert uses to manage multi-tasking and multi-threading) searches for a Dispatcher listener, it consults the MMAP file to see which process has a lower number of Master Threads. It then submits the request to the process with the lower number of Master Threads.

The processes periodically update the MMAP file on the number of Master Threads they currently have. The update interval is controlled by the parameter `admin_time_out` (in seconds). Typically, this should be set to less than five seconds.

System Settings by Section

The remainder of this appendix documents the specific system settings, grouped by the functional sections into which they are organized.

[system] Section

Settings in the `[system]` section apply globally to the ECXpert. Only those that are configurable are listed below. Do not change any others.

Table C-3   Configurable settings in the `[system]` section

Entry	Description
Configurable options	
range_min_port	Low bound dynamic port. The lowest port number ECXpert should use.
	Restrictions: Ports used by ECXpert must not be used by other applications.
range_max_port	High bound dynamic port The highest port number ECXpert should use.
	Restrictions: Ports used by ECXpert must not be used by other applications.
mmap_path	Full path to the ECXpert memory map.
	Restrictions: Must be valid path on your system.
	Default: $NSBASE/NS-apps/`ECXpert/data/log/` `ECXpert.map`
file_no	Number of file descriptors allowed per process.
	Recommended maximum: 1024
debug_timestamp	Debug timestamp.
	Restrictions—valid values: `yes`, `no`
	Default: `no`

[snmp] Section

Settings in the [snmp] section configure ECXpert's SNMP support.

Table C-4   Settings in the [snmp] section

Entry	Description
Parameters that should not be changed	
snmp_version	SNMP version number.
	Restrictions: Must be 1.0; do not change.
snmp_server_type	SNMP server type.
	Restrictions: Must be ECXpert; do not change.
snmp_methods	Supported SNMP methods.
	Restrictions: Must be get, put and trap—do not change.
snmp_exec_path	Not currently used.
snmp_config_path	Not currently used.
snmp_object_id	SNMP object identifier.
	Default: 2b060104018b2a04
Machine dependent information	
snmp_host_name	Name of SNMP host machine.
	Default: set during installation
Configurable options	
snmp_time_out	SNMP refresh interval (seconds).
	Default: 10
snmp_description	Description for the SNMP service.
	Default: set during installation
snmp_protocol	Protocol supported for SNMP.
	Default: http
snmp_organization	SNMP contact organization.
	Default: set during installation
snmp_location	SNMP contact location/address.
	Default: set during installation

Table C-4   Settings in the [snmp] section *(Continued)*

Entry	Description
snmp_contact	SNMP primary contact name. *Default:* set during installation
snmp_name	SNMP secondary contact name. *Default:* set during installation
snmp_tmp_path	Full path to SNMP log file. *Default:* $NSBASE/NS-apps/data/log/SNMP_LOG

[admin] Section

Settings in the [admin] section configure the Administrative Server.

Table C-5   Settings in the [admin] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section. *Restrictions:* Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same *server_type* value are treated as multiple instances of same server. *Default:* 0; do not change.
port_location	Location to pick up the port. *Default:* mmap
listener_level	Listener level. Number of listener threads to launch on startup. *Default:* 1; do not change.
listener_type	Listener type. *Restrictions*—valid values: – thread = runs as a thread – process = runs as a process *Default:* thread

Table C-5   Settings in the `[admin]` section *(Continued)*

Entry	Description
`max_listeners`	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 1
`thread_mode`	Thread operational mode.
	Restrictions—valid values: – `threaded` = run threaded – `serialized` = run serialized
	Default: `serialized` (only the Admin. server should be serialized)
`runnable_flag`	Can executable be run?
	Restrictions—valid values: – `yes` = executable will be run as needed – `no` = executable will not be run (e.g., test situation)
	Default: `yes`
`listener_time_out`	Listener timeout, in seconds.
	Default: 10
`admin_time_out`	Admin server time out period, in seconds.
	Default: 10
`start_mode`	Server start mode.
	Restrictions—valid values: `commandline`, `background`
	Default: `background`
Machine dependent information	
`host_name`	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	

Table C-5 Settings in the [admin] section *(Continued)*

Entry	Description
lock_path	Location of the ECXpert lock file.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.lock
exec_path	Executable path. Full path to the executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/ bdgadm-m-server
start_page	Startup Page for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-st art-template.html
stop_page	Shutdown Page for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-st op-template.html
header_template	Header template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-he ader-template.html
footer_template	Footer template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-fo oter-template.html
editlist_template	Edit List template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ed itlist-template.html
editsection_template	Edit Section template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ed itsection-template.html
editsection_template1	Edit Section template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ed itsection-template1.html

Table C-5 Settings in the `[admin]` section *(Continued)*

Entry	Description
autoheader_template	Auto-header template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-au toheader-template.html
editcfg_template	Edit Configuration template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ed itcfg-template.html
startlist_template	Start List template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-st artlist-template.html
deletesection_template	Delete Section template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-de letesection-template.html
deleteentry_template	Delete Entry template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-de leteentry-template.html
deleteentry_template1	Delete Entry template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-de leteentry-template1.html
addentry_template	Add Entry template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ad dentry-template.html
addentry_template1	Add Entry template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ad dentry-template1.html
addsection_template	Add Section template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-ad dsection-template.html

Table C-5   Settings in the [admin] section *(Continued)*

Entry	Description
addsection_template1	Add Section template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-addsection-template1.html
start_template	Start template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-start-template.html
browse_template	Browse template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-browse-template.html
procstat_template	Process Status template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-procstatus-template.html
thrdstat_template	Thread Status template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-thrdstatus-template.html
manage_fs	Manage Section template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-mgmt-top.html
pending_status_template	Pending Status template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-pending-template.html
log_plist_template	Log PList template for the Administration server.
	Default: *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-logplist-template.html

Table C-5   Settings in the [admin] section *(Continued)*

Entry	Description
log_flist_template	Log FList template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-lo gflist-template.html
log_header_template	Log Header template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-lo gheader-template.html
log_footer_template	Log Footer template for the Administration server. *Default:* *$NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-lo gfooter-template.html
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system? *Restrictions*—valid values: yes, no *Default:* yes; do not change.
worker_max_threads	Number of worker threads to run in parallel. *Default:* 4; do not change.
master_max_threads	Number of master threads to run in parallel. *Default:* 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads? *Restrictions*—valid values: yes, no *Default:* yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue. *Default:* 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack. *Default:* 500; do not change.
Port information	
admin_port	Administrative port number. *Restrictions:* Ports used by ECXpert must not be used by other applications.
admin_port_type	Administrative port type. *Restrictions*—valid values: – dynamic = Administrative Server assigns – manual = always use value in admin_port *Default:* dynamic

Table C-5 Settings in the [admin] section *(Continued)*

Entry	Description
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: – dynamic = Administrative Server assigns – manual = always use value in admin_port
	Default: dynamic
Configurable options	
snmp_flag	Enable SNMP?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: – 0 = all messages – 10 = information, warning, and error mesages – 20 = warning and error messages – 30 = error messages only
	Default: 0
autostart_flag	Start admin servers automatically when ECXpert is started?
	Restrictions—valid values: yes, no
	Default: no

Table C-5   Settings in the [admin] section *(Continued)*

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values: – yes = automatically restart when ECXpert is restarted (you are confident manual intervention is not required) – no = do not restart when ECXpert is restarted (you expect that manual intervention might be required)
	Default: no
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.admin.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.admin.dat
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.admin.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

[gateway] Section

Settings in the [gateway] section configure the communications servers, such as those for FTP and SMTP.

Table C-6   Settings in the [gateway] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 1; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: – 0 = all messages – 10 = information, warning, and error messages – 20 = warning and error messages – 30 = error messages only
	Default: 0
protocol_id	Protocol identifier.
	Default: 775; do not change.
port_location	Location to pick up the port.
	Default: mmap; do not change.
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
listener_type	Listener type. *Restrictions*—valid values: – thread = runs as a thread – process = runs as a process *Default:* thread

Table C-6   Settings in the [gateway] section *(Continued)*

Entry	Description
max_listeners	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel. *Restrictions:* Total number of threads you specify must be supported by your hardware. *Default:* 4
runnable_flag	Can executable be run? *Restrictions*—valid values: – yes = executable will be run as needed – no = executable will not be run (e.g., test situation) *Default:* yes
thread_mode	Thread operational mode. *Restrictions*—valid values: – threaded = run threaded – serialized = run serialized *Default:* threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
listener_time_out	Listener timeout, in seconds. *Default:* 10
admin_time_out	Admin server time out period, in seconds. *Default:* 10
start_mode	Server start mode. *Restrictions*—valid values: commandline, background *Default:* background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run. *Restrictions*: Must be a valid IP address in your domain. *Default:* set during installation
File and directory information	
exec_path	Executable path. Full path to the Gateway executable. *Default: $NSBASE*/NS-apps/ECXpert/bin/bdggwd

Table C-6   Settings in the [gateway] section *(Continued)*

Entry	Description
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
admin_port_type	Administrative port type.
	Restrictions—valid values: – dynamic = Administrative Server assigns – manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation

Table C-6 Settings in the [gateway] section *(Continued)*

Entry	Description
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: – dynamic = Administrative Server assigns – manual = always use value in admin_port
	Default: dynamic
Configurable options	
autostart_flag	Start communications servers automatically when ECXpert is started?
	Restrictions—valid values: yes, no
	Default: yes
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	 – yes = automatically restart when ECXpert is restarted
	   (you are confident manual intervention is not required)
	 – no = do not restart when ECXpert is restarted
	   (you expect that manual intervention might be required)

	Default: no
repository	Full path to repository location.
	Default: set in installation
remove_precomm_service_files	Remove precommunications service files.
	Restrictions—valid values: yes, no
	Default: yes
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/data/log/ ECXpert.log.gateway.dat

Table C-6   Settings in the [gateway] section *(Continued)*

Entry	Description
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/data/log/ ECXpert.log.gateway.dat
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no *Default:* yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.gateway.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

[tcpip-connector] Section

Settings in the [tcpip-connector] section control the way the tcpip-connector process operates. The tcpip-connector process is the ECXpert Communications Agent for sending and receiving EDI data using TCP/IP.

Table C-7   Settings in the [tcpip-connector] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 2; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no

Table C-7   Settings in the [`tcpip-connector`] section *(Continued)*

Entry	Description
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)

Table C-7   Settings in the [tcpip-connector] section *(Continued)*

Entry	Description
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation)
	Default: yes
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of machine where instances of tcpip-connector are run.
	Restrictions: Must be a valid host name in your domain.
File and directory information	
exec_path	Full path to the ftp-local-edi executable.
	Default: *$NSBASE*/NS-apps/ECXpert/bin/tcpconnmain
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.*Default:* 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.

Table C-7   Settings in the `[tcpip-connector]` section *(Continued)*

Entry	Description
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
Configurable options	
`restart_flag`	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- `yes` = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- `no` = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: `no`

Table C-7   Settings in the [tcpip-connector] section *(Continued)*

Entry	Description
repository	Full path to repository location.
	Default: set at installation
remote_dir	Remote directory path.
	Restrictions: must be *$NSBASE*/NS-apps/ECXpert/ data/work/remote/ (the default), do not change
retry	Number of times to retry tcpip-connector process.
	Default: 10
retry_after	Number of minutes to wait before retrying.
	Default: 2
process_pending	Determines whether or not the TCP/IP connector should process pending jobs in the database upon its startup.
	Default: Yes
max_request_queued	Protects the TCP/IP connector from saturation when the dispatcher stops responding. Default indicates no limit.
	Default: 0
fifo_interval	One earliest-submitted file will be processed when the number of the files processed in priority order (highest to lowest) meets this number. This parameter is to prevent the low priority jobs from starving.
	Default: 10
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: yes, no
	Default: yes
Debug output configuration	
debug_flag	Turn on low level tracing information? *Restrictions*—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.tcpip-connector.dat

Table C-7   Settings in the [`tcpip-connector`] section *(Continued)*

Entry	Description
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.tcpip-connector.dat
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.tcpip-connector.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for
   max_listeners and max_threads, according to the following formula:
   Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

[retrieve] Section

Settings in the [`retrieve`] section specify the way in which data is to be manually retrieved in ECXpert. The `poll` command uses these settings.

Table C-8   Settings in the [`retrieve`] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes

Table C-8   Settings in the [`retrieve`] section *(Continued)*

Entry	Description
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both)
type	Only set when adding your own network_id.
	Restrictions: Must be none; do not change
Configurable options	
internal_name	The name used internally within ECXpert. Must be POLL1. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: POLL
operation	Type of communications operation involved.
	Restrictions: must be send, do not change
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, in a test situation)
	Default: yes
thread_mode	Thread operational mode.
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year-2000 compliant - no = use only last two digits, not year-2000 compliant
	Default: no
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).

Table C-8   Settings in the [retrieve] section *(Continued)*

Entry	Description
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no

[http-retrieve] Section

Settings in the [http-retrieve] section specify the way in which data is to be retrieved using HTTP in ECXpert. The HTTP server uses these settings.

Table C-9   Settings in the [http-retrieve] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section. *Restrictions:* Must be configuration; do not change.
is_comm_agent	Is this a Communications Agent?
	Restrictions: Must be yes; do not change.
operation	Type of communications operation involved.
	Restrictions: must be send; do not change.
data_type	Type of data involved.
	Restrictions: Must be both; do not change.
type	Only set when adding your own network_id.
	Restrictions: Must be none; do not change
internal_name	The name used internally within ECXpert. Must be HTTP RETRIEVE1. Do not change.
Configurable options	
visible_name	The name displayed externally by ECXpert.
	Default: HTTP Receive

Table C-9   Settings in the [http-retrieve] section *(Continued)*

Entry	Description
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: no
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).

[dispatcher] Section

Settings in the [dispatcher] section control the way the ECXpert Dispatcher operates.

NOTE	If you are running multiple instances of the Dispatcher, the name of the section for the primary instance in the ecx.ini file *must* be [dispatcher].
	You can name sections for additional instances—for example, dispatcher2], [dispatcher3], or whatever name you like.

Table C-10   Settings in the [dispatcher] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 3; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no

Table C-10 Settings in the `[dispatcher]` section *(Continued)*

Entry	Description
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap; do not change
listener_level	Listener level. Number of listener threads to launch on startup.
	. *Default:* 1; do not change.
listener_type	Listener type. *Restrictions*—valid values: - thread = runs as a thread - process = runs as a process *Default:* thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel. *Restrictions:* Total number of threads you specify must be supported by your hardware. *Default:* 4
runnable_flag	Can executable be run? *Restrictions*—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, a test situation)
	Default: yes
thread_mode	Thread operational mode *Restrictions*—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)

Table C-10 Settings in the `[dispatcher]` section *(Continued)*

Entry	Description
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the Dispatcher executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/ bdgdispatchmain
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.

Table C-10   Settings in the `[dispatcher]` section *(Continued)*

Entry	Description
`master_max_threads_queued`	Maximum number of master threads to queue. Lowered from ECX 3.0 default value of 500 to reduce the number of waiting master threads.
	Default: `1`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack. Lowered from the ECX 3.0 default value of 500 to reduce the number of waiting requests in the system socket queue.
	Default: `1`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port_type`	Listener port type.
	Restrictions: must be `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Configurable options	
`restart_flag`	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- `yes` = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- `no` = do not restart when ECXpert is restarted
	  (you expect manual intervention might be required)

	Default: `no`

Table C-10 Settings in the `[dispatcher]` section *(Continued)*

Entry	Description
`autostart_flag`	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
`recovery`	On startup, automatically process partially completed jobs (those that Dispatcher started processing but somehow never completed)?
	Restrictions—valid values: - `yes` = recover interrupted jobs automatically - `no` = interrupted jobs processing must be manually started
	Default: `no` (if you change `recovery` to `yes`, it is recommended that you make sure `restart_flag` is set to `no` to ensure that Dispatcher does not attempt to start processing before servers it depends on, such as Gateway, are started)
`process_pending`	Should pending jobs automatically be found and processed when ECXpert starts up?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
	Note: A job is "pending" when `Tracking.TrkState=3` and `Tracking.TrkCurServiceIdx=1`
Debug output configuration	
`debug_flag`	Turn on low level tracing information?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
`stderr_path`	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/`ECXpert/data/log/` `ECXpert.log.dispatcher.dat`
`stdout_path`	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/`ECXpert/data/log/` `ECXpert.log.dispatcher.dat`

Table C-10 Settings in the `[dispatcher]` section *(Continued)*

Entry	Description
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
log_prefix	File prefix used for name generation.
	Default: `ECXpert.log.dispatcher.dat`
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/data/log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for
  `max_listeners` and `max_threads`, according to the following formula:
  Oracle maximum connections = (total (`max_listeners`) + total (`max_threads`)) x 2

[EcxStylesheet] Section

The New XML Parser will completely depend on this file and EcxStylesheet section
in the ecx.ini file. Note that there is no name-value relation between the parameters
in ecxstylesheets.xml ini file.

Table C-11 Settings in the [EcxStylesheet] section

Entry	Description
Configurable options	
xmlinifile	Fully qualified path for xml filename.
	Default: `no`

[import-certificates] Section

Settings in the `[import-certificates]` section affect the defaults used in the
process of importing certificates.

Table C-12 Settings in the `[import-certificates]` section

Entry	Description
Parameters that should not be changed	
section_type	Must be `configuration`. Do not change.

Table C-12   Settings in the [import-certificates] section *(Continued)*

Entry	Description
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.import-certificates.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.import-certificates.dat

[poll] Section

Settings in the [poll] section configure the poll command.

Note that the [retrieve] section also affects the poll command.

Table C-13   Settings in the [poll] section

Entry	Description
Parameters that should not be changed	
section_type	Must be configuration. Do not change.
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.poll.dat

Table C-13 Settings in the [poll] section *(Continued)*

Entry	Description
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default:$NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.poll.dat

[commsmtp-send] Section

Settings in the [commsmtp-send] section control the way the commsmtp-send process operates. The commsmtp-send process is the ECXpert Communications Agent for sending using SMTP.

Table C-14 Settings in the [commsmtp-send] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 4; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
protocol_id	Protocol identifier.
	Default: 2

Table C-14   Settings in the `[commsmtp-send]` section *(Continued)*

Entry	Description
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 1
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, in a test situation)
	Default: yes
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
type	Type of executable.
	Restrictions: must be daemon, do not change.
operation	Type of communications operation.
	Restrictions: must be send, do not change

Table C-14 Settings in the `[commsmtp-send]` section *(Continued)*

Entry	Description
multi_part	Enable sending of multiple body parts (attachments) using MIME?
	Note: This can only be done using ECXpert's Submit API. Refer to the *iPlanet ECXpert Developer's Guide* chapter on the Submit Class.
	Restrictions—valid values: - t *or* y *or* 1 = yes (true, yes, 1) - f or n or 0 = no (false, no, 0)
	Default: t
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both) (internally coded[2] in ECXpert)
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	

Table C-14 Settings in the `[commsmtp-send]` section *(Continued)*

Entry	Description
`exec_path`	Executable path. Full path to the Dispatcher executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/SMTPSend
`smtp_home`	SMTP home directory.
	Default: $NSBASE/NS-apps/ECXpert/smtp/
Multi-threading parameters—do not change	
`max_thread_flag`	Limit the number of threads running in system?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
`worker_max_threads`	Number of worker threads to run in parallel.
	Default: `4`; do not change.
`master_max_threads`	Number of master threads to run in parallel.
	Default: `4`; do not change.
`master_max_threads_queued_flag`	Queue master threads above `master_max_threads`?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`

Table C-14 Settings in the [commsmtp-send] section *(Continued)*

Entry	Description
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Configurable options	
mail_host	Name of mail host through which email is sent and received.
	Restrictions: Must be a valid host name in your domain.
	Default: set during installation
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: no
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes? *Restrictions*—valid values: - true = yes, pre-enveloped - false = no, not pre-enveloped *Default:* true
mdn_wait_time	Number of minutes to wait for message disposition notification (MDN), if it is requested. *Default:* 60

Table C-14 Settings in the `[commsmtp-send]` section *(Continued)*

Entry	Description
bundle_all	Package all data together as one file (one body part)? *Note:* Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data if `bundle_all` is set to `true`. *Restrictions*—valid values: - yes - no *Default:* no
use4digit_year	Use all four digits for year, for year 2000 compliance? *Restrictions*—valid values: - `yes` = use all four digits, year 2000 compliant - `no` = use only last two digits, not year 2000 compliant *Default:* no *Note:* Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started? *Restrictions*—valid values: yes, no *Default:* yes
internal_name	The name used internally within ECXpert. Must be SMTP1. Do not change.
visible_name	The name displayed externally by ECXpert. *Default:* SMTP
Debug output configuration	
debug_flag	Turn on low level tracing information? *Restrictions*—valid values: yes, no *Default:* no
stderr_path	Fully specified path for log file to receive standard output from low level trace. *Default:* *$NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.commsmtp-send.dat

Table C-14 Settings in the `[commsmtp-send]` section *(Continued)*

Entry	Description
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ `ECXpert.log.commsmtp-send.dat`
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
log_prefix	File prefix used for name generation.
	Default: `ECXpert.log.commsmtp-send.dat`
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/data/log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for `max_listeners` and `max_threads`, according to the following formula:
Oracle maximum connections = (total (`max_listeners`) + total (`max_threads`)) x 2

2 "Internally coded in ECXpert" means that the entry does not appear in the System Settings screens in the System Administration Interface after installation and that you only need to add it if you want to override the default value listed.

[commsmtp-receive] Section

Settings in the `[commsmtp-receive]` section control the way the `commsmtp-receive` process operates. The `commsmtp-receive` process is the ECXpert Communications Agent for receiving using SMTP.

Table C-15 Settings in the `[commsmtp-receive]` section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be `server`; do not change.
server_type	Type of server. All servers (`section_type = server`) sharing same `server_type` value are treated as multiple instances of same server.
	Default: 5; do not change.

Table C-15 Settings in the `[commsmtp-receive]` section *(Continued)*

Entry	Description
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - `0` = all messages - `10` = information, warning, and error messages - `20` = warning and error messages - `30` = error messages only
	Default: `0`
protocol_id	Protocol identifier.
	Default: `3`
port_location	Location to pick up the port.
	Default: `mmap`
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: `1`
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: `0`; do not change.
listener_type	Listener type.
	Restrictions—valid values: - `thread` = runs as a thread - `process` = runs as a process
	Default: `thread`
runnable_flag	Can executable be run?
	Restrictions—valid values: - `yes` = executable will be run as needed - `no` = executable will not be run (for example, in a test situation)
	Default: `yes`

Table C-15   Settings in the [commsmtp-receive] section *(Continued)*

Entry	Description
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: no
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 2
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/SMTPReceive
smtp_home	Full path to the SMTP home directory.
	Default: $NSBASE/NS-apps/ECXpert/smtp/
Multi-threading parameters—do not change	

Table C-15 Settings in the `[commsmtp-receive]` section *(Continued)*

Entry	Description
`max_thread_flag`	Limit the number of threads running in system?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
`worker_max_threads`	Number of worker threads to run in parallel.
	Default: `4`; do not change.
`master_max_threads`	Number of master threads to run in parallel.
	Default: `4`; do not change.
`master_max_threads_queued_flag`	Queue master threads above `master_max_threads`?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`

Table C-15   Settings in the `[commsmtp-receive]` section *(Continued)*

Entry	Description
listener_port_type	Listener port type. Only set when adding your own network_id. *Restrictions*—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port *Default:* dynamic
Configurable options	
is_sendmail	Should Sendmail be used instead of POP3? *Restrictions*—valid values: yes, no *Default:* set during installation; depends on mail server being used
mail_file	Full path to the commsmtp-recv mail file. *Default:* (only if is_sendmail is set to yes) *$NSBASE*/NS-apps/ECXpert/mail
mail_host	Name of mail host that commsmtp-recv is to use. *Restrictions*: Must be a valid host name in your domain. *Default:* set during installation
max_mail_process_number	Maximum number of incoming messages that commsmtp-receive will process before releasing the messages to the dispatcher. *Default:* 5
POP3_user	POP3 user name to use with commsmtp-receive. *Default:* Set during installation.
POP3_pwd	POP3 user password to use with commsmtp-receive. *Default:* Set during installation; change it using bdgsetpasswd in the $NSBASE/NS-apps/bin directory.

restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)
	Default: no

max_send_times	Maximum number of times to send, if message disposition notification (MDN) time expires. *Default:* 1 (cannot override in release 3.6)

Table C-15 Settings in the `[commsmtp-receive]` section *(Continued)*

Entry	Description
mdn_wait_time	Number of minutes to wait for message disposition notification (MDN), if it is requested. *Default:* 60
internal_name	The name used internally within ECXpert. Must be SMTP1. Do not change.
visible_name	The name displayed externally by ECXpert. *Default:* SMTP
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started? *Restrictions*—valid values: yes, no *Default*: yes
poll_wait_time	Wait time (seconds) between mail polling processes. *Default:* 300
Debug output configuration	
debug_flag	Turn on low level tracing information? *Restrictions*—valid values: yes, no *Default:* no
stderr_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.commsmtp-receive.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.commsmtp-receive.dat
log_flag	Should entry appear in the logging API? *Restrictions*—valid values: yes, no *Default:* yes
log_prefix	File prefix used for name generation. *Default:* ECXpert.log.commsmtp-receive.dat
log_dir	Full path to directory for log files. *Default: $NSBASE*/NS-apps/data/log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for
   max_listeners and max_threads, according to the following formula:
   Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

[submit] Section

Settings in the [submit] section control the operation of the Submission Agent.

Table C-16   Settings in the [submit] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section. *Restrictions:* Must be configuration; do not change.
retry	Number of times to retry. the submit process. *Default:* 10
retry_after	Number of minutes to wait before retrying. Default: 2
Debug output configuration	
debug_flag	Turn on low level tracing information? *Restrictions*—valid values: yes, no *Default:* no
stderr_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.submit.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.submit.dat

[purge] Section

Settings in the `[purge]` section control the way the purge programs provided with ECXpert (`bdggenManifest` and `bdgrealpurge`) operate.

Table C-17 Settings in the `[purge]` section

Entry	Description
Parameters that should not be changed	
`section_type`	Type of section.
	Restrictions: Must be `configuration`; do not change.
File and directory information	
`manifest_filename`	The full path to the file that is to receive the manifest listing of documents that is output by `bdggenManifest`.
	Default: *$NSBASE*/NS-apps/ECXpert/data/`purge.manifest`
Configurable options	
`default_retention_period`	Default number of days to retain files before purging. User can override when running `bdggenManifest`.
	Default: 5
Debug output configuration	
`debug_flag`	Turn on low level tracing information?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
`stderr_path`	Fully specified path for log file to receive standard output from low level trace.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log/`purge.dat.out`
`stdout_path`	Fully specified path for log file to receive standard output from low level trace.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log/`purge.dat.err`

[ftp-local-application] Section

Settings in the [ftp-local-application] section control the way the
ftp-local-application process operates. The ftp-local-application process
is the ECXpert Communications Agent for sending and receiving application data
using local FTP.

NOTE	The FTP command sequence is as follows:
	• send=cdo | put
	• recv=cdi | mkdir | ls | get | rename | rmdir
	• sendrecv=cdo | put | cdi | mkdir | ls | get | rename | rmdir

Table C-18   Settings in the [ftp-local-application] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 7; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap

Table C-18 Settings in the `[ftp-local-application]` section *(Continued)*

Entry	Description
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
type	Type of executable.
	Restrictions—valid values: none, daemon, process
	Default: daemon
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: a (application) (internally coded[2] in ECXpert)

Table C-18   Settings in the `[ftp-local-application]` section *(Continued)*

Entry	Description
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - `yes` = display in protocol selection lists - `no` = do not display in protocol selection lists
	Default: `yes`
listener_time_out	Listener timeout, in seconds.
	Default: `10`
admin_time_out	Admin server time out period, in seconds.
	Default: `10`
start_mode	Server start mode.
	Restrictions—valid values: `commandline`, `background`
	Default: `background`
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Full path to the `ftp-local-application` executable.
	Default: *$NSBASE*/NS-apps/`ECXpert`/bin/`bdgftpd`
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: `4`; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: `4`; do not change.

Table C-18 Settings in the `[ftp-local-application]` section *(Continued)*

Entry	Description
`master_max_threads_queued_flag`	Queue master threads above `master_max_threads`?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`; do not change.
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Configurable options	

Table C-18 Settings in the `[ftp-local-application]` section *(Continued)*

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- `yes` = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- `no` = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: `no`
runnable_flag	Can executable be run?
	Restrictions—valid values: - `yes` = executable will be run as needed - `no` = executable will not be run (e.g., test situation)
	Default: `yes`
operation	Type of communications operation involved.
	Restrictions—valid values: - `send` = send only - `recv` = receive only - `sendrecv` = send and then receive
	Default: `send`
internal_name	The name used internally within ECXpert. Must be `FTP1`. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: `FTP (APPLICATION)`
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes, no`
	Default: `yes`
receive_params	Parameters used in Scheduler Admin for Receive Operation.
	Default: `Host Name|HN;Port|PT;Username|UN;Password|PW;Inbound Pattern|RS;Inbound Directory|ID;Inbound File Type|IT`

Table C-18 Settings in the `[ftp-local-application]` section *(Continued)*

Entry	Description
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with `bundle_all` set to `true`.
	Restrictions—valid values: - yes - no
	Default: `no`
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: `no` *Note:* Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/`ECXpert`/data/log/ `ECXpert.log.ftp-local-application.dat`
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/`ECXpert`/data/log/ `ECXpert.log.ftp-local-application.dat`
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
log_prefix	File prefix used for name generation.
	Default: `ECXpert.log.ftp-local-application.dat`

Table C-18 Settings in the `[ftp-local-application]` section *(Continued)*

Entry	Description
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log
FTP command sequence	
send	Send command sequence
	Default: cdo
recv	Receive command sequence
	Default: cdi | mkdir | ls | get | rename | rmdir
sendrecv	Send and receive command sequence
	Default: cdo | put | cdi | mkdir | ls | get | rename | rmdir

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for
   `max_listeners` and `max_threads`, according to the following formula:
   Oracle maximum connections = (total (`max_listeners`) + total (`max_threads`)) x 2

2 "Internally coded in ECXpert" means that the entry does not appear in the System Settings screens in the System Administration
   Interface after installation and that you only need to add it if you want to override the default value listed.

[ftp-local-edi] Section

Settings in the `[ftp-local-edi]` section control the way the *ftp-local-edi* process operates. The `ftp-local-edi` process is the ECXpert Communications Agent for sending and receiving EDI data using local FTP.

NOTE	The FTP command sequence is as follows:
	• send=cdo | put
	• recv=cdi | mkdir | ls | get | rename | rmdir
	• sendrecv=cdo | put | cdi | mkdir | ls | get | rename | rmdir

Table C-19 Settings in the `[ftp-local-edi]` section

Entry	Description
Parameters that should not be changed	

Table C-19 Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 8; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4

Table C-19 Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
`thread_mode`	Thread operational mode
	Restrictions—valid values: - `threaded` = run threaded - `serialized` = run serialized
	Default: `threaded` (only the Admin. server should be `serialized`; in all other sections where `section_type= server`, it is strongly recommended that you leave this setting as `threaded`)
`type`	Type of executable.
	Restrictions—valid values: `none, daemon, process`
	Default: `daemon`
`data_type`	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: `e (edi)` (internally coded[2] in ECXpert)
`is_comm_agent`	Is this a Communications Agent?
	Restrictions—valid values: - `yes` = display in protocol selection lists - `no` = do not display in protocol selection lists
	Default: `yes`
`listener_time_out`	Listener timeout, in seconds.
	Default: `10`
`admin_time_out`	Admin server time out period, in seconds.
	Default: `10`
`start_mode`	Server start mode.
	Restrictions—valid values: `commandline, background`
	Default: `background`
Machine dependent information	

Table C-19 Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Full path to the `ftp-local-edi` executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/bdgftpd
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: `4`; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: `4`; do not change.
master_max_threads_queued_flag	Queue master threads above `master_max_threads`?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: `500`; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.

Table C-19 Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Configurable options	

`restart_flag`	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values:
	- `yes` = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- `no` = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)
	Default: `no`

`runnable_flag`	Can executable be run? *Restrictions*—valid values: - `yes` = executable will be run as needed - `no` = executable will not be run (e.g., test situation)
	Default: `yes`
`operation`	Type of communications operation involved. *Restrictions*—valid values: - `send` = send only - `recv` = receive only - `sendrecv` = send and then receive *Default:* `sendrecv`

Table C-19 Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes? *Restrictions*—valid values: - `true` = yes, pre-enveloped - `false` = no, not pre-enveloped *Default:* `true`
internal_name	The name used internally within ECXpert. Must be `FTP1`. Do not change.
visible_name	The name displayed externally by ECXpert. *Default:* `FTP (EDI)`
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started? *Restrictions*—valid values: `yes`, `no` *Default*: `no`
output_fname_unique	Set output filename to be the same as the output pattern string?. *Restrictions*—valid values: - `yes` - `no` *Default:* `no`
receive_params	Parameters used in Scheduler Admin for Receive Operation. *Default:* `Host Name|HN;Port|PT;Username|UN;Password|PW;Inbound Pattern|RS; Inbound Directory|ID;Inbound File Type|IT`
bundle_all	Package all data together as one file (one body part)? *Note:* Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data if `bundle_all` is set to `true`. *Restrictions*—valid values: - `yes` - `no` *Default:* `no`

Table C-19   Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: yes
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.ftp-local-edi.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.ftp-local-edi.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.ftp-local-edi.dat
FTP command sequence	
send	Send command sequence *Default:* cdo
recv	Receive command sequence *Default:* cdi | mkdir | ls | get | rename | rmdir

Table C-19 Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
sendrecv	Send and receive command sequence
	Default: cdo | put | cdi | mkdir | ls | get | rename | rmdir

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for max_listeners and max_threads, according to the following formula:
  Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

2 "Internally coded in ECXpert" means that the entry does not appear in the System Settings screens in the System Administration Interface after installation and that you only need to add it if you want to override the default value listed.

[ecxoftp-server] Section

Settings in the `[ftp-local-edi]` section control the way the `ecxoftp-server` process operates. The `ecxoftp-server` process is the ECXpert Communications Agent for sending and receiving data using Odette FTP (OFTP).

The ECXpert OFTP server also has its own separate initialization file, for low-level communications parameters, such as modem settings and structure of the connection script. For information on this separate initialization file, see "Sample OFTP Server Initialization File (ecxoftp-server.ini)" on page 777.

Table C-20 Settings in the `[ftp-local-edi]` section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 14; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: yes

Table C-20   Settings in the [ftp-local-edi] section *(Continued)*

Entry	Description
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 10
protocol_id	Protocol identifier.
	Default: 775
port_location	Location to pick up the port.
	Default: mmap
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation)
	Default: yes

Table C-20   Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
thread_mode	Thread operational mode
	Restrictions—valid values: - `threaded` = run threaded - `serialized` = run serialized
	Default: `threaded` (only the Admin. server should be serialized; in all other sections where `section_type= server`, it is strongly recommended that you leave this setting as `threaded`)
listener_time_out	Listener timeout, in seconds.
	Default: `10`
admin_time_out	Admin server time out period, in seconds.
	Default: `10`
start_mode	Server start mode.
	Restrictions—valid values: `commandline`, `background`
	Default: `commandline`
type	Type of executable.
	Restrictions—valid values: `none`, `daemon`, `process`
	Default: `daemon`
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with `bundle_all` set to `true`.
	Restrictions—valid values: - `yes` - `no`
	Default: `no`
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - `yes` = display in protocol selection lists - `no` = do not display in protocol selection lists
	Default: `yes`
internal_name	The name used internally within ECXpert. Must be `OFTP1`. Do not change.

Table C-20   Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
visible_name	The name displayed externally by ECXpert.
	Default: `Odette FTP (OFTP)`
operation	Type of communications operation involved.
	Restrictions—valid values: - `send` = send only - `recv` = receive only - `sendrecv` = send and then receive
	Default: `send`
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - `e` = "edi," EDI format - `a` = "application," proprietary application format - `b` = "both," both EDI and proprietary formats
	Default: `b (both)`
Machine dependent information	
host_name	IP address of host machine where instances of executable are run. *Restrictions*: Must be a valid IP address in your domain. *Default:* set during installation
File and directory information	
exec_path	Full path to the `ecxoftp-m-server` executable. *Default:* *$NSBASE*/NS-apps/ECXpert/bin/ecxoftp-m-server
oftp_server_ini	Full path to the OFTP initialization file. *Default:* *$NSBASE*/NS-apps/ECXpert/config/ecxoftp-server.i ni
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system? *Restrictions*—valid values: `yes`, `no` *Default:* `yes`; do not change.
worker_max_threads	Number of worker threads to run in parallel. *Default:* 4; do not change.
master_max_threads	Number of master threads to run in parallel. *Default:* 4; do not change.

Table C-20   Settings in the `[ftp-local-edi]` section *(Continued)*

Entry	Description
`master_max_threads_queued_flag`	Queue master threads above `master_max_threads`? *Restrictions*—valid values: `yes`, `no` *Default:* `yes`; do not change.
`master_max_threads_queued`	Maximum number of master threads to queue. *Default:* `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack. *Default:* `500`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Configurable options	

Table C-20   Settings in the [ftp-local-edi] section *(Continued)*

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: no
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: yes, no
	Default: no
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log/ecxoftp-server.log
stdout_path	Fully specified path for log file to receive standard output from low level trace. *Default:* *$NSBASE*/NS-apps/ECXpert/data/log/ecxoftp-server.log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for
   max_listeners and max_threads, according to the following formula:
   Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

[comm_ftp_geis] Section

Settings in the [comm_ftp_geis] section control the way the comm_ftp_geis process operates. The comm_ftp_geis process is the ECXpert Communications Agent for sending and receiving using GEIS FTP.

Table C-21 Settings in the [comm_ftp_geis] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 6; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
listener_type	Listener type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in listener_port
	Default: thread

Table C-21   Settings in the [comm_ftp_geis] section *(Continued)*

Entry	Description
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation)
	Default: yes
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
data_type	Must be GEIS; do not change.
type	Type of executable.
	Restrictions—valid values: none, daemon, process
	Default: daemon
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes
internal_name	The name used internally within ECXpert. Must be GEIS FTP1. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: GEIS FTP

Table C-21 Settings in the `[comm_ftp_geis]` section *(Continued)*

Entry	Description
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the comm_ftp_geis executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/bdgftpd
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.

Table C-21   Settings in the [comm_ftp_geis] section *(Continued)*

Entry	Description
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
admin_port_type	Administrative port type.
	Restrictions—valid values:
	- dynamic = Administrative Server assigns
	- manual = always use value in admin_port
	Default: dynamic
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values:
	- dynamic = Administrative Server assigns
	- manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Configurable options	
restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted (you expect that manual intervention might be required)
	Default: no
operation	Type of communications operation involved.
	Restrictions—valid values:
	- send = send only
	- recv = receive only
	- sendrecv = send and then receive
	Default: send

Table C-21 Settings in the `[comm_ftp_geis]` section *(Continued)*

Entry	Description
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with `bundle_all` set to `true`.
	Restrictions—valid values: - yes - no
	Default: no
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: no
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - true = yes, pre-enveloped - false = no, not pre-enveloped
	Default: true
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: yes, no
	Default: no
output_fname_unique	Set output filename to be the same as the output pattern string?.
	Restrictions—valid values: - yes - no
	Default: no
Debug output configuration	

Table C-21   Settings in the [comm_ftp_geis] section *(Continued)*

Entry	Description
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.comm_ftp_geis.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.comm_ftp_geis.dat
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.comm_ftp_geis.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log
receive_params	Parameters used in Scheduler Admin for Receive Operation.
	Default: Host Name|HN;Port Number|PT;Username|UN;Password|PW
FTP command sequence	
send	Send command sequence
	Default: cdo /send | site parm=MC=A | ls BYPARM | put | ls
recv	Receive command sequence
	Default: cdi /receive | ls | site parm=ow=s | ls BYPARM | get BYPARM | ls
sendrecv	Send and receive command sequence
	Default: cdo /send | site parm=MC=A | ls BYPARM | put | ls | cdi /receive | ls | site parm=ow=s | ls BYPARM | get BYPARM | ls

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for max_listeners and max_threads, according to the following formula:
Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

[commhttp-ssl] Section

Settings in the [commhttp-ssl] section apply to the communications agent for the SSL HTTP for OBI protocol.

Table C-22   Settings in the [commhttp-ssl] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 13; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread

Table C-22   Settings in the `[commhttp-ssl]` section *(Continued)*

Entry	Description
max_listeners	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel. *Restrictions:* Total number of threads you specify must be supported by your hardware. *Default:* 4
listener_level	Listener level. Number of listener threads to launch on startup. *Default:* 1; do not change.
runnable_flag	Can executable be run? *Restrictions*—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation) *Default:* yes
thread_mode	Thread operational mode. *Restrictions*—valid values: - threaded = run threaded - serialized = run serialized *Default:* threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
type	Type of executable. *Restrictions*—valid values: none, daemon, process *Default:* daemon
data_type	Object type(s) to bundle for send. *Restrictions*—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats *Default:* b (both) (internally coded in ECXpert)
is_comm_agent	Is this a Communications Agent? *Restrictions*—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists *Default:* yes

Table C-22 Settings in the `[commhttp-ssl]` section *(Continued)*

Entry	Description
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
operation	Type of communications operation involved.
	Restrictions—valid values: - send = send only - recv = receive only - sendrecv = send and then receive
	Default: send
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable file.
	Default: $NSBASE/NS-apps/ECXpert/bin/ bdghttpssl-server
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.

Table C-22   Settings in the `[commhttp-ssl]` section *(Continued)*

Entry	Description
`master_max_threads_queued_flag`	Queue master threads above `master_max_threads`?
	Restrictions—valid values: `yes, no`
	Default: `yes`; do not change.
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
Configurable options	
`autostart_flag`	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes, no`
	Default: `no`

Table C-22 Settings in the `[commhttp-ssl]` section *(Continued)*

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values: - yes = automatically restart when ECXpert is restarted (you are confident manual intervention is not required) - no = do not restart when ECXpert is restarted (you expect that manual intervention might be required)
	Default: no
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - true = yes, pre-enveloped - false = no, not pre-enveloped
	Default: true
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to true with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with bundle_all set to true.
	Restrictions—valid values: - yes - no
	Default: no
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: no
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
internal_name	The name used internally within ECXpert. Must be HTTP SSL. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: HTTP SSL for OBI
obi_tag	OBI file type

Table C-22   Settings in the `[commhttp-ssl]` section *(Continued)*

Entry	Description
obi_filetype	OBI file type
	Default: OBI
obi_decodesize	OBI decode size
	Default: 2048
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: yes
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.commhttp-ssl.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.commhttp-ssl.dat
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.ssl.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

[commhttp-ssl-XML] Section

Settings in the [commhttp-ssl-XML] section apply to the communications agent for the SSL HTTP for XML protocol.

Table C-23 Settings in the [commhttp-ssl-XML] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 13; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread

Table C-23   Settings in the `[commhttp-ssl-XML]` section *(Continued)*

Entry	Description
max_listeners	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
runnable_flag	Can executable be run?
	Restrictions—valid values: - `yes` = executable will be run as needed - `no` = executable will not be run (e.g., test situation)
	Default: `yes`
thread_mode	Thread operational mode.
	Restrictions—valid values: - `threaded` = run threaded - `serialized` = run serialized
	Default: `threaded` (only the Admin. server should be serialized; in all other sections where `section_type= server`, it is strongly recommended that you leave this setting as `threaded`)
type	Type of executable.
	Restrictions—valid values: `none, daemon, process`
	Default: `daemon`
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: `b (both)` (internally coded in ECXpert)
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - `yes` = display in protocol selection lists - `no` = do not display in protocol selection lists
	Default: `yes`

Table C-23 Settings in the [commhttp-ssl-XML] section *(Continued)*

Entry	Description
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
operation	Type of communications operation involved.
	Restrictions—valid values: - send = send only - recv = receive only - sendrecv = send and then receive
	Default: send
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
	Note: When selecting commandline for start_mode and setting the autostart_flag to *yes*, it is known that running ecxstart from the command line does not start the ftp server. The workaround for this is to use the System Administration User Interface>Management tab (as described in *"Managing ECXpert Servers" on page 131* to click the ftp server button to the On position to start it.
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable file.
	Default: $NSBASE/NS-apps/ECXpert/bin/ecxhttps-server
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.

Table C-23   Settings in the `[commhttp-ssl-XML]` section *(Continued)*

Entry	Description
`worker_max_threads`	Number of worker threads to run in parallel.
	Default: `4`; do not change.
`master_max_threads`	Number of master threads to run in parallel.
	Default: `4`; do not change.
`master_max_threads_queued_flag`	Queue master threads above `master_max_threads`?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`; do not change.
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`

Table C-23 Settings in the `[commhttp-ssl-XML]` section *(Continued)*

Entry	Description
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values: - `yes` = automatically restart when ECXpert is restarted (you are confident manual intervention is not required) - `no` = do not restart when ECXpert is restarted (you expect that manual intervention might be required)
	Default: `no`
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - `true` = yes, pre-enveloped - `false` = no, not pre-enveloped
	Default: `true`
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with `bundle_all` set to `true`.
	Restrictions—valid values: - `yes` - `no`
	Default: `no`
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - `yes` = use all four digits, year 2000 compliant - `no` = use only last two digits, not year 2000 compliant
	Default: `no`
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).

Table C-23   Settings in the `[commhttp-ssl-XML]` section *(Continued)*

Entry	Description
internal_name	The name used internally within ECXpert. Must be `HTTP SSL NONOBI`. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: `HTTP SSL for XML`
session_timeout	Idle time (seconds) to elapse before logout.
	Default: `300`
xml_tag	XML file type
xml_filetype	XML file type
	Default: `XML`
xml_decodesize	XML decode size
	Default: `2048`
xml_encodesize	XML encode size
	Default: `2048`
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: `yes, no`
	Default: `yes`
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ `ECXpert.log.commhttp-xmlssl.dat`
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ `ECXpert.log.commhttp-xmlssl.dat`
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: `yes, no`
	Default: `yes`
log_prefix	File prefix used for name generation.
	Default: `ECXpert.log.xmlssl.dat`

Table C-23   Settings in the `[commhttp-ssl-XML]` section *(Continued)*

Entry	Description
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

[commjms-send] Section

Settings in the `[commjms-send]` section apply to the JMS-Send communications agent.

Table C-24   Settings in the `[commjms-send]` section

Entry	Description
Parameters that should not be changed	
server_type	Type of server
	Default: 23
section_type	Defines section
	Default: server
snmp_trap_flag	Server snmp trap flag
	Default: no
snmp_trap_level	Server snmp trap level
	Default: 0
port_location	Location to pick up the port
	Default: mmap
listener_type	Listener Type
	Default: thread
max_listeners	Maximum Number of Listeners
	Default: 4
listener_level	Listener Level
	Default: 1
runnable_flag	Runnable Flag
	Default: yes

Table C-24   Settings in the `[commjms-send]` section *(Continued)*

Entry	Description
thread_mode	Thread Operational Mode
	Default: threaded
type	Type
	Default: daemon
data_type	EDI, Application, or GEIS Ftp data, to be processed by connector
	Default: Both
is_comm_agent	Identifies a communications agent
	Default: yes
listener_time_out	Listener time out
	Default: 10
admin_time_out	Admin server time out period
	Default: 10
operation	Send and/or Receive communications
	Default: send
start_mode	Server start mode
	Default: commandline
host_name	Host Name
	Default: 192.18.112.190
exec_path	Location of the Server Executable
	Default: /ECXpert/bin/JMSSend
Multithreading Parameters	
max_thread_flag	Limit the number of threads running in system
	Default: yes
worker_max_threads	Number of worker threads to run in parallel
	Default: 4
master_max_threads	Number of master threads to run in parallel
	Default: 4

Table C-24 Settings in the `[commjms-send]` section *(Continued)*

Entry	Description
`master_max_threads_queued_flag`	Whether to quese master threads
	Default: yes
`master_max_threads_queued`	Maximum number of master threads to queue
	Default: 500
`master_max_threads_stacked`	Maximum number of master threads to place on stack
	Default: 500
Port Information	
`admin_port_type`	Admin Port Allocation
	Default: dynamic
`listener_port`	Listener Port
	Default: 4010
`admin_port`	Administration Port
	Default: 4011
`listener_port_type`	Listener Port Allocation
	Default: dynamic
Configurable Options	
`autostart_flag`	Automatic Startup of Servers
	Default: no
`restart_flag`	Automatic Restart Required
	Default: no
`pre_enveloped_edi`	Retrieve EDI documents with existing envelopes
	Default: True
`bundle_all`	Connector is to handle all files/interchanges at once
	Default: no
`use4digit_year`	Specify to generate a 4-digit year to get an 8-digit GS04 value for Y2K-compliance
	Default: no
`internal_name`	Internal name for a protocol
	Default: JMS Send

Table C-24 Settings in the `[commjms-send]` section *(Continued)*

Entry	Description
visible_name	Visible name (appears on Protocol tab) for protocol
	Default: JMS Send
classpath	Class Path
	Default: /ECXpert/bin/jms/jms.jar:/opt/SUNWjmq/lib/jmq.jar
jmsvendor_classpath	Variable for the JVM that specifies the provider-specific JMS-implementation libraries (`jms.jar`)
	Default: `/ECXpert/bin/jms/jms.jar`
libpath	LD_LIBRARY PATH
	Default: /ECXpert/lib
debug_flag	Optional switch for turning low level tracing information
	Default: yes
stderr_path	File location for stderr output from debugging
	Default: /ECXpert/data/log/ECXpert.log.commjms-send.dat
stdout_path	File location for stdout output from debugging
	Default: /ECXpert/data/log/ECXpert.log.commjms-send.dat
log_flag	This specifies that the entry should appear in the Admin logging UI
	Default: yes
log_prefix	File prefix used for name generation
	Default: ECXpert.log.commjms-send.dat
log_dir	Root directory for log files
	Default: /ECXpert/data/log
JMS_LogDir	JMS (Send) Log file
	Default: /ECXpert/data/log/javaJMSSend.log
scheduledjms_logDir	Log file for JMS Receiver when using the Scheduler
	Default: /ECXpert/data/log/schedulJMS.log

Table C-24   Settings in the `[commjms-send]` section *(Continued)*

Entry	Description
workdir	Fully qualified pathname for temporary work files
	Default: /tmp
timeout	Time out period for the JMS Listener when scheduled
	Default: 11

[commjms-receive] Section

Settings in the `[commjms-send]` section apply to the JMS-Send communications agent.

Table C-25   Settings in the `[commjms-receive]` section

Entry	Description
Parameters that should not be changed	
server_type	Type of server
	Default: 21
section_type	Defines section
	Default: server
protocol_id	Protocol Identifier
	Default: 3
port_location	Location to pick up the port
	Default: mmap
max_listeners	Maximum Number of Listeners
	Default: 1
listener_level	Listener Level
	Default: 0
listener_type	Listener Type
	Default: thread
runnable_flag	Runnable Flag
	Default: yes

Table C-25 Settings in the [commjms-receive] section *(Continued)*

Entry	Description
thread_mode	Thread Operational Mode
	Default: threaded
is_comm_agent	Identifies a communications agent
	Default: no
listener_time_out	Listener time out
	Default: 10
admin_time_out	Admin server time out period
	Default: 10
start_mode	Server start mode
	Default: background
host_name	Host Name
	Default: 192.18.112.190
exec_path	Location of the Server Executable
	Default: /ECXpert/bin/JMSReceive
Multithreading Parameters	
max_thread_flag	Limit the number of threads running in system
	Default: yes
worker_max_threads	Number of worker threads to run in parallel
	Default: 4
master_max_threads	Number of master threads to run in parallel
	Default: 4
master_max_threads_queued_flag	Whether to quese master threads
	Default: yes
master_max_threads_queued	Maximum number of master threads to queue
	Default: 500
master_max_threads_stacked	Maximum number of master threads to place on stack
	Default: 500

Table C-25   Settings in the `[commjms-receive]` section *(Continued)*

Entry	Description
jvmThreads	Number of threads created in the thread pool for the jms listenter. change only if needed.
	Default: 15
Port Information	
listener_port	Listener Port
	Default: 4008
admin_port	Administration Port
	Default: 4009
admin_port_type	Admin Port Allocation
	Default: dynamic
listener_port_type	Listener Port Allocation
	Default: dynamic
Configurable Options	
restart_flag	Automatic Restart Required
	Default: no
qcfName	Connection Factory Lookup Name
	Default:
nqueues	Number of Queues
	Default:
q1	Queue Number #1
	Default:
javaLog	JMS (Receive) Log file
	Default: /ECXpert/data/log/javaJMSReceive.log
workdir	Fully qualified pathname for temporary work files
	Default: /tmp
ID	ID
	Default: 1
jndiPropFile	Filename containing JNDI provider information
	Default:

Table C-25 Settings in the `[commjms-receive]` section *(Continued)*

Entry	Description
`classpath`	Class Path
	Default: `/ECXpert/config/jndi.properties`
`jmsvendor_classpath`	Variable for the JVM that specifies the provider-specific JMS-implementation libraries (`jms.jar`)
	Default: `/ECXpert/bin/jms/jms.jar`
`libpath`	LD_LIBRARY PATH
	Default: `/ECXpert/lib`
`jmsuser`	JMS User ID to connect to message serve
	Default:
`jmspasswd`	Password for JMS User ID to connect to message server
	Default:
`internal_name`	Internal name for a protocol
	Default: JMS1
`visible_name`	Visible name (appears on Protocol tab) for protocol
	Default: JMS Receive
`autostart_flag`	Automatic Startup of Servers
	Default: no
`debug_flag`	Optional switch for turning low level tracing information
	Default: yes
`stderr_path`	File location for stderr output from debugging *Default:* /ECXpert/data/log/ECXpert.log.commjms-receive.dat
`stdout_path`	File location for stdout output from debugging *Default:* ECXpert/data/log/ECXpert.log.commjms-receive.dat
`log_flag`	This specifies that the entry should appear in the Admin logging UI
	Default: yes
`log_prefix`	File prefix used for name generation
	Default: ECXpert.log.commjms-receive.dat
`log_dir`	Root directory for log files
	Default: ECXpert/data/log

[commhttp-aiag] Section

Settings in the [commhttp-aiag] section apply to the communications agent for the AIAG HTTP protocol (automotive industry).

Table C-26 Settings in the [commhttp-aiag] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 9; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread

Table C-26 Settings in the `[commhttp-aiag]` section *(Continued)*

Entry	Description
`max_listeners`	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel. *Restrictions:* Total number of threads you specify must be supported by your hardware. *Default:* 4
`listener_level`	Listener level. Number of listener threads to launch on startup. *Default:* 1; do not change.
`thread_mode`	Thread operational mode. *Restrictions*—valid values: - `threaded` = run threaded - `serialized` = run serialized *Default:* `threaded` (only the Admin. server should be `serialized`; in all other sections where `section_type= server`, it is strongly recommended that you leave this setting as `threaded`)
`type`	Type of executable. *Restrictions*—valid values: `none`, `daemon`, `process` *Default:* `daemon`
`data_type`	Object type(s) to bundle for send. *Restrictions*—valid values: - `e` = "edi," EDI format - `a` = "application," proprietary application format - `b` = "both," both EDI and proprietary formats *Default:* `e` (edi) (internally coded in ECXpert)
`is_comm_agent`	Is this a Communications Agent? *Restrictions*—valid values: - `yes` = display in protocol selection lists - `no` = do not display in protocol selection lists *Default:* `yes`
`listener_time_out`	Listener timeout, in seconds. *Default:* 10

Table C-26   Settings in the `[commhttp-aiag]` section *(Continued)*

Entry	Description
admin_time_out	Admin server time out period, in seconds.
	Default: 10
operation	Type of communications operation involved.
	Restrictions—valid values: - send = send only - recv = receive only - sendrecv = send and then receive
	Default: send
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, test situation)
	Default: yes
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable.
	Default: *$NSBASE*/NS-apps/ECXpert/bin/agentaiag
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.

Table C-26 Settings in the [commhttp-aiag] section *(Continued)*

Entry	Description
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation

Table C-26 Settings in the `[commhttp-aiag]` section *(Continued)*

Entry	Description
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values: - `yes` = automatically restart when ECXpert is restarted (you are confident manual intervention is not required) - `no` = do not restart when ECXpert is restarted (you expect that manual intervention might be required)
	Default: `no`
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - `true` = yes, pre-enveloped - `false` = no, not pre-enveloped
	Default: `true`
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with `bundle_all` set to `true`.
	Restrictions—valid values: - `yes` - `no`
	Default: `no`
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - `yes` = use all four digits, year 2000 compliant - `no` = use only last two digits, not year 2000 compliant
	Default: `no`
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).

Table C-26 Settings in the `[commhttp-aiag]` section *(Continued)*

Entry	Description
internal_name	The name used internally within ECXpert. Must be HTTP AIAG. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: HTTP for AIAG
session_timeout	Idle time (seconds) to elapse before logout.
	Default: 300
receive_params	Parameters used in Scheduler Admin for Receive Operation.
	Default: Host Name|HN;Port|PT;Username|UN;Password|PW;Sender| SS;Receiver|RR;File Type|AN;Operation|OO;File Name|FN;Reference Number|RN;User Parameter|UP
dtdpath	Fully qualified path to the directory where the dtd's are stored.
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: /tmp/ECXpert.log.commhttp-aiag.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: /tmp/ECXpert.log.commhttp-aiag.dat
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.commhttp-aiag.dat
log_dir	Full path to directory for log files.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log

[commhttp-gisb] Section

Settings in the [commhttp-gisb] section apply to the communications agent for the GISB HTTP protocol (natural gas industry).

Table C-27 Settings in the [commhttp-gisb] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 10; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.

Table C-27   Settings in the [commhttp-gisb] section *(Continued)*

Entry	Description
max_listeners	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation)
	Default: yes
thread_mode	Thread operational mode.
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
type	Type of executable.
	Restrictions—valid values: none, daemon, process
	Default: daemon
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both) (internally coded in ECXpert)
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes

Table C-27 Settings in the [commhttp-gisb] section *(Continued)*

Entry	Description
operation	Type of communications operation involved.
	Restrictions—valid values: - send = send only - recv = receive only - sendrecv = send and then receive
	Default: send
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/agentgisb
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.

Table C-27 Settings in the [commhttp-gisb] section *(Continued)*

Entry	Description
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: yes, no
	Default: no

Table C-27 Settings in the [commhttp-gisb] section *(Continued)*

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: no
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - true = yes, pre-enveloped - false = no, not pre-enveloped
	Default: true
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: no
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
internal_name	The name used internally within ECXpert. Must be HTTP GISB. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: HTTP for GISB
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.commhttp-gisb.dat

Table C-27   Settings in the [commhttp-gisb] section *(Continued)*

Entry	Description
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.commhttp-gisb.dat
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to true with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with bundle_all set to true.
	Restrictions—valid values: - yes - no
	Default: no
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.commhttp-gisb.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

[ecxftp-server] Section

Settings in the [ecxftp-server] section apply to the ECXpert FTP Server.

Table C-28   Settings in the [ecxftp-server] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.

Table C-28 Settings in the [ecxftp-server] section *(Continued)*

Entry	Description
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 15; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: yes
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 10
protocol_id	Protocol identifier.
	Default: 775
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
max_listeners	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4

Table C-28 Settings in the [`ecxftp-server`] section *(Continued)*

Entry	Description
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation)
	Default: yes
thread_mode	Thread operational mode.
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/ ecxftp-m-server
ftp_server_ini	Full path to the FTP Server's initialization file.
	Default: $NSBASE/NS-apps/ECXpert/config/ ecxftp-server.ini

Table C-28   Settings in the [ecxftp-server] section *(Continued)*

Entry	Description
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation

Table C-28   Settings in the [ecxftp-server] section *(Continued)*

Entry	Description
listener_port_type	Listener port type. Only set when adding your own network_id. *Restrictions*—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port *Default:* dynamic
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started? *Restrictions*—valid values: yes, no *Default*: no

restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	
	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)
	
	Default: no

Debug output configuration	
debug_flag	Turn on low level tracing information? *Restrictions*—valid values: yes, no *Default:* no
stderr_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.ecxftp-server.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace. *Default: $NSBASE*/NS-apps/ECXpert/data/log/ ECXpert.log.ecxftp-server.dat

[ecxftp-client] Section

Settings in the [ecxftp-client] section apply to the ECXpert FTP client.

Table C-29 Settings in the [ecxftp-client] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
File and directory information	
ftp_client_ini	Full path to the FTP client's initialization file.
	Default: $NSBASE/NS-apps/ECXpert/config/ecxftp-client.ini
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.ecxftp-client.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ECXpert.log.ecxftp-client.dat

[ecxpa-server] Section

Settings in the [ecxpa-server] section apply to the Partner Agent for ECXpert Server.

NOTE	This section appears only for installations of ECXpert that include the optional Partner Agent for ECXpert Server; it is added as part of the Partner Agent for ECXpert Server installation process

Table C-30   Settings in the [ecxpa-server] section

Entry	Description
Parameters that should not be changed	
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 19; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: yes
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 10
section_type	Type of section.
	Default: server; do not change.
protocol_id	Protocol identifier.
	Default: 775
port_location	Location to pick up the port.
	Default: mmap
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.

Table C-30   Settings in the [ecxpa-server] section *(Continued)*

Entry	Description
listener_type	Listener type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in listener_port
	Default: thread
max_listeners[1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, a test situation)
	Default: yes
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
start_mode	Server start mode.
	Restrictions—valid values: commandline , background
	Default: background

Table C-30   Settings in the [ecxpa-server] section *(Continued)*

Entry	Description
type	Type of executable.
	Restrictions—valid values: none, daemon, process
	Default: daemon
Machine independent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/ pa-m-server
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	

Table C-30 Settings in the [ecxpa-server] section *(Continued)*

Entry	Description
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
Start and stop scripts	
pa_server_start_admin	Program that starts the PA Server HTTPS admin server, which provides a browser-based user interface to configure the PA Server installation, from the command line. Spawned when the PA Server server is started.
	Default: $NSBASE/NS-apps/paserver/bin/start_admin
pa_server_start_agentd	Program that starts the PA Server agent server, which runs the ActiveAgent programs that perform the back-end ECXpert interactions, from the command line. Spawned when the PA Server server is started.
	Default: $NSBASE/NS-apps/paserver/bin/start_agentd
pa_server_start_httpd	Program that starts the PA Server HTTP server from the command line. Spawned when the PA Server server is started.
	Default: $NSBASE/NS-apps/paserver/bin/start_httpd

Table C-30   Settings in the [ecxpa-server] section *(Continued)*

Entry	Description
pa_server_start_ftpd	Program that starts the PA Server ftp server from the command line. Spawned when the PA Server server is started.
	Default: $NSBASE/NS-apps/paserver/bin/start_ftpd
pa_server_stop_admin	Program that stops the PA Server HTTPS admin server, which provides a browser-based user interface to configure the PA Server installation, from the command line. Spawned when the PA Server server is shut down.
	Default: $NSBASE/NS-apps/paserver/bin/stop_admin
pa_server_stop_agentd	Program that stops the PA Server agent server, which runs the ActiveAgent programs that perform the back-end ECXpert interactions, from the command line. Spawned when the PA Server server is shut down.
	Default: $NSBASE/NS-apps/paserver/bin/stop_agentd
pa_server_stop_httpd	Program that stops the PA Server HTTP server from the command line. Spawned when the PA Server server is shut down.
	Default: $NSBASE/NS-apps/paserver/bin/stop_httpd
pa_server_stop_ftpd	Program that stops the PA Server ftp server from the command line. Spawned when the PA Server server is shut down.
	Default: $NSBASE/NS-apps/paserver/bin/stop_ftpd
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: yes, no
	Default: no
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: no
Debug output configuration	

Table C-30   Settings in the [ecxpa-server] section *(Continued)*

Entry	Description
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.ecxpa-server.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.log.ecxpa-server.dat

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for max_listeners and max_threads, according to the following formula:
Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

[TradingXpert] Section

Settings in the [TradingXpert] section apply to the ECXpert interface with the TradingXpert System.

This product was originally called "FormsXpert" in early development, and "DeveloperXpert" for most of ECXpert version 1.1x life cycle. You might encounter these terms for TradingXpert in earlier ECXpert documentation.

Table C-31   Settings in the [TradingXpert] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes

Table C-31 Settings in the [TradingXpert] section *(Continued)*

Entry	Description
Configurable options	
use4digit_year	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - yes = use all four digits, year 2000 compliant - no = use only last two digits, not year 2000 compliant
	Default: no
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
internal_name	The name used internally within ECXpert. Must be FX1. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: TradingXpert
receive_params	Parameters used in Scheduler Admin for Receive Operation.
	Default: Template Filename|TF
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.DevXpert.dat
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.DevXpert.dat

[scheduler] Section

Settings in the [scheduler] section control the way the ECXpert Scheduler operates. The Scheduler is the ECXpert component that manages scheduling of time-based processing.

Table C-32 Settings in the [scheduler] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 11; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
protocol_id	Protocol identifier.
	Default: 69
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.

Table C-32 Settings in the [scheduler] section *(Continued)*

Entry	Description
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners [1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 1
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, a test situation)
	Default: yes
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
time_out	Scheduler's wake-up interval (seconds).
	Default: 600
time_out_callback	Must be 1000. Do not change.
listener_time_out	Listener timeout, in seconds.
	Default: 60
admin_time_out	Admin server time out period, in seconds.
	Default: 10

Table C-32 Settings in the [scheduler] section *(Continued)*

Entry	Description
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the Scheduler executable.
	Default: $*NSBASE*/NS-apps/ECXpert/bin/ ecxsched-server
header_template	Full path to template file for Scheduler screen header.
	Default: $*NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-he ader-template.html
footer_template	Full path to template file for Scheduler screen footer.
	Default: $*NSBASE*/NS-apps/ECXpert/UI/html/admin/bdgadm-fo oter-template.html
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.

Table C-32   Settings in the [scheduler] section *(Continued)*

Entry	Description
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500; do not change.
Port information	
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
Configurable options	
restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- yes = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- no = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: no

Table C-32 Settings in the `[scheduler]` section *(Continued)*

Entry	Description
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
queue_scan_interval	The interval (in seconds) at which Scheduler is to scan the job queue for jobs that should be run.
	Restrictions: range of *min* to *max*
	Default: `60`
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
debug_sleep	Internal use for debugging.
trace_level	Job processing trace level.
	Restrictions—valid values: - `0` = show all messages - `1` = show only error messages
	Default: `0`
stderr_path	Fully specified path for log file to receive standard output from low level trace.
	Default: `/tmp/ECXpert.log.scheduler.dat`
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: `/tmp/ECXpert.log.scheduler.dat`
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
log_prefix	File prefix used for name generation.
	Default: `ECXpert.log.scheduler.dat`
log_dir	Full path to directory for log files.
	Default: *$NSBASE*/NS-apps/`ECXpert`/data/log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for max_listeners and max_threads, according to the following formula:
Oracle maximum connections = (total (max_listeners) + total (max_threads)) x 2

[eXML-connector] Section

Settings in the [eXML-connector] section configure the ECXpert extension that supports XML.

Table C-33   Settings in the [eXML-connector] section

Entry	Description
Parameters that should not be changed	
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 18; do not change.
section_type	Type of section.
	Restrictions: Must be server; do not change.
snmp_trap_flag	Trap information for SNMP service?
	Restrictions—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error mesages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread

Table C-33 Settings in the [eXML-connector] section *(Continued)*

Entry	Description
max_listeners	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: set during installation
listener_level	Listener level. Number of listener threads to launch on startup.
	.Default: 1; do not change.
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (e.g., test situation)
	Default: yes
thread_mode	Thread operational mode.
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
type	Type of executable.
	Restrictions—valid values: none, daemon, process
	Default: daemon
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application,"proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both) (internally coded in ECXpert)
listener_time_out	Listener timeout, in seconds.
	Default: 10

Table C-33 Settings in the [eXML-connector] section *(Continued)*

Entry	Description
admin_time_out	Admin server time out period, in seconds.
	Default: 10
operation	Type of communications operation involved.
	Restrictions—valid values: - send = send only - recv = receive only - sendrecv = send and then receive
	Default: send
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Full path to the executable.
	Default: $*NSBASE*/NS-apps/ECXpert/bin/xmlconnectord
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes

Table C-33   Settings in the [eXML-connector] section *(Continued)*

Entry	Description
master_max_threads_queued	Maximum number of master threads to queue.
	Default: 500; do not change.
master_max_threads_stacked	Maximum number of master threads to place on stack.
	Default: 500
Port information	
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
admin_port	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
listener_port	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
listener_port_type	Listener port type. Only set when adding your own network_id.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
Configurable options	
autostart_flag	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: yes, no
	Default: no

Table C-33   Settings in the [`eXML-connector`] section *(Continued)*

Entry	Description
Restart_flag	Restart this executable automatically if it experiences an abnormal exit?

	Restrictions—valid values:
	- `yes` = automatically restart when ECXpert is restarted
	  (you are confident manual intervention is not required)
	- `no` = do not restart when ECXpert is restarted
	  (you expect that manual intervention might be required)

	Default: `no`
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - `true` = yes, pre-enveloped - `false` = no, not pre-enveloped
	Default: `true`
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - `yes` = display in protocol selection lists - `no` = do not display in protocol selection lists
	Default: `yes`
internal_name	The name used internally within ECXpert.
	Default: `XML1`
visible_name	The name displayed externally by ECXpert.
	Default: `eXML Connector`
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
stderr_path	Fully specified path for log file to receive error output from low level trace.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log/ `ECXpert.log.xmlconnector.dat`

Table C-33   Settings in the [eXML-connector] section *(Continued)*

Entry	Description
stdout_path	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.xmlconnector.dat
bundle_all	Package all data together as one file (one body part)?
	Note: Do not set this parameter to true with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with bundle_all set to true.
	Restrictions—valid values: - yes - no
	Default: no
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.xmlconnector.dat
log_dir	Full path to directory for log files.
	Default: $NSBASE/NS-apps/data/log
CX server required parameters that should not be changed	
cxlistener_port_type	eXML listener port allocation.
	Default: static; do not change
cxadmin_port_type	eXML admin port allocation.
	Default: static; do not change
cxlistener_thread_no	eXML listener thread number.
	Default: 1; do not change
cxadmin_thread_no	eXML admin thread number.
	Default: 1; do not change
cxmulti_thread	eXML multi-thread.
	Default: yes; do not change
Configurable options	

Table C-33 Settings in the [`eXML-connector`] section *(Continued)*

Entry	Description
cxlistener_port	eXML listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
cxadmin_port	eXML admin port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
cxthread_poll_interval	eXML thread polling interval in seconds.
	Default: 1
cxthread_poll_skipping	eXML thread polling interval in number of connections.
	Default: 10
cxmax_threads_stacked	Maximum number of threads to place on stack.
	Default: 500
cxremote_dir	Directory to use when XML is streaming data.
	Default: *$NSBASE*/NS-apps/ECXpert/data/work/remote

[migrate] Section

Settings in the [`migrate`] section apply to migration of the ECXpert database schema from version 1.0 to version 1.1.x.

Table C-34 Settings in the [`migrate`] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section. *Restrictions:* Must be configuration; do not change.
Debug output configuration	
debug_flag	Turn on low level tracing information? *Restrictions*—valid values: yes, no *Default:* no

Table C-34 Settings in the [migrate] section *(Continued)*

Entry	Description
log_flag	Should entry appear in the logging API?
	Restrictions—valid values: yes, no
	Default: yes
log_prefix	File prefix used for name generation.
	Default: ECXpert.log.migrate.dat
log_dir	Full path to directory for log files.
	Default: *$NSBASE*/NS-apps/ECXpert/data/log

[membership] Section

Settings in the [membership] section configure ECXpert membership to use either the ECXpert database or LDAP.

Table C-35 Settings in the [membership] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
Configurable options	
accessType	Membership access type.
	Restrictions—valid values: - db = using database - ldap = using LDAP
	Default: db
	Note: Any entry other than ldap is treated as db.

[LDAP] Section

Settings in the [LDAP] section apply to the ECXpert LDAP support.

Table C-36   Settings in the [LDAP] section

Entry	Description
Parameters that should not be changed	
section_type	configuration
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
Configurable options	
port	Port number to use for LDAP.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
c	Country ID, from LDAP server.
	If a country code is used in the Directory Server Suffix setting (for example, **o=netscape.com, c=US**), this entry must match it exactly (for example, **c=US**).
	If no country code is used in the Directory Server (for example, **o=netscape.com**), this entry must be **c=** with nothing following the equal sign.
o	Organization, from LDAP server.
ou	Organization unit, from LDAP server.
cn	Common name (authenticated as directory manager), from LDAP server.
LDAP_USER	The user who has authority to perform inserts, deletes and updates to the directory tree. An example is what the Directory Server uses as the default manager, Directory Manager. This entry must match exactly the entire Root DN entry you set for ECXpert in the Netscape Server Administration page (for example, **Directory Manager, o=netscape.com**).

Table C-36 Settings in the `[LDAP]` section *(Continued)*

Entry	Description
LDAP_PASSWORD	Password for LDAP user. Set using `bdgsetpasswd` in the *$NSBASE*/NS-apps/bin directory.
LDAP_MAX_CONNECTIONS	The maximum number of connections allowed to the Directory Server at one time.
	Default: 100
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: `yes`, `no`
	Default: `no`
	Note: When set to `yes`, debug statements are automatically written to the file, *$NSBASE*/NS-apps/ECXpert/data/log/ECXpert.cgi.log file.

[user-defined-#] Sections

Settings in a user-defined communication section control the way a specific user-defined communications process operates.

You must create one of these sections, each with a unique name, for each user-defined communications process you want to implement. Each section should be named sequentially—`[user-defined-1]`, `[user-defined-2]`, `[user-defined-2]`, and so on.

NOTE	When deleting the original user-defined-1 comm agent, the second comm agent created must be moved to the user-defined-1 comm agent section in order to maintain the ability to select this comm agent from the Partnership UI protocol tab. Any additional comm agents should be fine in their ordered position (i.e., user-defined-3, use-defined-4, and so forth).

Table C-37 Settings in the `[user-defined]` section

Entry	Description
Parameters that should not be changed	

Table C-37 Settings in the `[user-defined]` section *(Continued)*

Entry	Description
section_type	Type of section.
	Restrictions: Must be `network`; do not change.
type	Type of executable (`process` or `thread`).
	Restrictions: must be `process`
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both)
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes
Configurable options	
cmd_and_args	Full path to the executable for the user-defined communications process, plus arguments. Enter this exactly as you would from the operating system command line.
append_data_file	Append the data file to the end of the `cmd_and_args` and the trading partnership parameters?
	Restrictions—valid values: - 0 = no, do not append data file - 1 = yes, append data file
	Default: 1
prefix_data_file	Prefixed data file name to pass to user-defined communications process.
	Restrictions: - must begin with "-f filename=" - rest is full path to data file (with no space after "-f filename=")
cmd_type	Type of command (`script` or `executable`).
	Restrictions—valid values: `script`, `executable`
	Default: `script`

Table C-37   Settings in the [user-defined] section *(Continued)*

Entry	Description
operation	Type of communications operation involved.
	Restrictions—valid values: - send = send only - recv = receive only - sendrecv = send and then receive
	Default: sendrecv
internal_name	The name used internally within ECXpert. Must be USER DEFINED #, where # is an integer between 1 and 8. Must be unique for each user-defined communications protocol.
visible_name	The name displayed externally by ECXpert. Must be unique for each user-defined communications protocol.
	Default: USER DEFINED #
parameter_name_1	First parameter for user-defined Communications Agent.
parameter_name_2	Second parameter for user-defined Communications Agent.
parameter_name_3	Third parameter for user-defined Communications Agent.
parameter_name_4	Fourth parameter for user-defined Communications Agent.
parameter_name_5	Fifth parameter for user-defined Communications Agent.
parameter_name_6	Sixth parameter for user-defined Communications Agent.
parameter_name_7	Seventh parameter for user-defined Communications Agent.
parameter_name_8	Eighth parameter for user-defined Communications Agent.
receive_params	Parameters used in Scheduler Admin for Receive Operation.
	Default: First Parameter|P1;Second Parameter|P2;Third Parameter|P3;Fourth Parameter|P4;Fifth Parameter|P5;Sixth Parameter|P6;Seventh Parameter|P7;Eighth Parameter|P8

[parse] Section

Settings in the [parse] section control the way the parse process operates. The parse process "parses" the data in a submission unit, identifying each item and creating database records with pointers that ECXpert uses to access the data during processing.

Table C-38   Settings in the [parse] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
Configurable options	
restrictionsFile	Name of file containing EDI envelope restrictions.
	Default: $NSBASE/NS-apps/ECXpert/maps/parser.res
	Restrictions: Do not modify this file unless told so by Netscape tech support.
validateElements	Should all elements in envelopes be validated?
	Default: yes
traceFile	Full path to trace file for debugging. Turns parse tracing on if set.
	Default: NONE (parse tracing off)
	Example: /tmp/parser.trace
traceLevel	Level of parse tracing to record.
	Restrictions—valid values: –0 = no tracing -1 = minimal tracing (basically outputs start and end times) -2 = more tracing (outputs validation results) -3 = maximum tracing (outputs validation results and reader)
	Default: 0 (none)

Table C-38 Settings in the [parse] section *(Continued)*

Entry	Description
readerMMapSize	Size (KB) of the memory map used for the input file.
	Restrictions: Should be a multiple of the system memory page size. Should be left blank unless the input file is exceptionally large.
	Default: NONE - entire input file is memory mapped.
	Example: 4096
envDumpFnm	Name of file where dump of parsed envelopes in memory is placed. Used for debugging only.
	Default: NONE - parsed envelope data no written to file.
	Example: /tmp/env.dmp
resDumpFnm	Name of file where dump of restrictions structures in memory is placed after loading the file identified in restrictionsFile. Used for debugging only.
	Default: NONE - restrictions structures in memory not written to file.
	Example: /tmp/res.dmp
useTrackingDate	Should the original date in TRACKING be used when adding EDI envelopes to database?
	Restrictions—valid values: yes, no
	Default: no
detailedReporting	Should reporting of EDI envelopes to the EVENTLOG table be detailed?
	Restrictions—valid values: yes, no
	Default: no
dateResolutionYear	The base year used to resolve the century when interpreting two-digit year data.
	Two-digit years less than the last two digits of this date are interpreted as being in the *next* century, while two-digit years equal to or greater than this date are interpreted as being in the *same* century.
	For example, if set to 1923, 00 is interpreted as 2000, 22 is interpreted as 2022 and 23 is interpreted as 1923. *Default:* 1950

Table C-38   Settings in the [parse] section *(Continued)*

Entry	Description
dbUpdaterArraySize	Controls the behavior of Parse only.
	Restrictions: must always be set less than or equal to value for [DB_SECTION] parameter DB_ARRAY_SIZE.
	Default: 1

[Split] Section

Settings in the [Split] section control the way the Split service operates. The Split service "splits" the data in a submission unit into a separate submission unit for each document, so that different documents can be processed by different service lists.

Table C-39   Settings in the [Split] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
Configurable options	
workdir	Full path to the working directory for the Split service.
	Restrictions: Must be a valid path on your system
	Default: $NSBASE/NS-apps/ECXpert/data/work
maxThreads	Maximum number of threads to run in parallel.
	Default: 1
fileBufSize	The size of the memory buffer used when copying from the input file to the temporary file before re-submission.
	Default: 8192
submissionDocType	Document Type that each interchange submission unit is to be set to after being split off from the original submission unit. (Used, with Sender and Receiver, to look up the service list.)
	Restrictions: Must match the Document Type specified for the associated partnership (Sender/Receiver).
	Default: AFTER_SPLIT

Table C-39   Settings in the [Split] section *(Continued)*

Entry	Description
submissionDelay	The number of seconds to wait before re-submission.
	Default: 1

[translate] Section

Settings in the [translate] section control the way the translate process operates. The translate process uses the map associated with EDI data to perform the specified data translations.

NOTE	This entire section is internally coded in ECXpert. It does not appear in the System Administration interface until you add it. You only need to add this section when you want to change any of the default values for any of the entries listed.

Table C-40   Settings in the [translate] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
vldIgnoreAll	Should Parse maps ignore all validations?
	Restrictions—valid values:
	– yes, ignore all validations
	– no, ignore no validations
	Default: no (internally coded[1] in ECXpert)
vldIgnorePresentation	Should Parse maps ignore presentation validations?
	Restrictions—valid values:
	– yes, ignore presentation validations
	– no, never ignore presentation validations
	Default: no (internally coded* in ECXpert)

Table C-40 Settings in the [`translate`] section *(Continued)*

Entry	Description
vldIgnoreRestrictions	Should Parse maps ignore restrictions validations?
	Restrictions—valid values: – `yes` ignore restrictions validations – `no`, never ignore restrictions validations
	Default: `no` (internally coded* in ECXpert)
vldIgnoreSize	Should Parse maps ignore size validations?
	Restrictions—valid values: – `yes`, ignore size validations – `no`, never ignore size validations
	Default: `no` (internally coded* in ECXpert)
inOrderReceived	Translate documents in order received (vs. in order by document type)?
	Restrictions—valid values: – `yes`, sort by order received – `no`, sort by document type
	Default: `yes` (internally coded* in ECXpert)
File and directory information	
workDir	Full path to working files directory.
	Default: *$NSBASE*/NS-apps/data/`work` (internally coded* in ECXpert)
auditDir	Path, relative to *$NSBASE*/NS-apps/`ECXpert`, to directory for audit file generated by Mercator map.
	Default: *$NSBASE*/NS-apps/*data*/`work`
	Warning: This option is *not* multi-thread-safe. Use only when debugging a map.
inputDir	Location of non-primary input files for the mapper. For example, if the map requires supportive cross-reference tables or other input files aside from the primary data file, this is where they are located.
	Default: *$NSBASE*/NS-apps/data/`input` (internally coded* in ECXpert)
outputDir	Location for output files for the mapper.
	Default: *$NSBASE*/NS-apps/data/`output` (internally coded* in ECXpert)

Table C-40 Settings in the [translate] section *(Continued)*

Entry	Description
mapsDir	Location for map files for the mapper.
	Default: $NSBASE/NS-apps/data/maps (internally coded* in ECXpert)
traceDir	Full path name to a parse trace file. Presence of an entry turns on map tracing (for Parser and Audit maps), using the specified file for map trace output.
	Default: $NSBASE/NS-apps/data/work
	Warning: This option is *not* multi-thread-safe. Use only when debugging a map.
Configurable options	
keepFiles	Should temporary files used in parsing be kept after successful completion of Parse? Files involved are the audit file (output from the Parser map) and the normalized offset file (output from the Audit map).
	Note: These temporary files have unique names and do not overwrite earlier files; keep_files should only be turned on for a limited time for testing purposes.
	Restrictions—valid values: – yes, always retain temp files – no, retain temp files only on error
	Default: no (internally coded* in ECXpert)
useMemory	Should Mercator platform API do all work in memory?
	Restrictions—valid values: - yes, do all work in memory - no, do no work in memory
	Default: no (internally coded* in ECXpert)
	Recommendation: Set to yes to reduce the amount of disk I/O.
pageCount	Page count for TSI mapper to control its paging and memory use. Adjust this to tune performance.
	Default: 8 (internally coded* in ECXpert)
pageSize	Page size for TSI mapper to control its paging and memory use. Adjust this to tune performance.
	Default: 64 (internally coded* in ECXpert)

Table C-40   Settings in the [translate] section *(Continued)*

Entry	Description
additionalRunMapSwitches	Any additional switches that need to be passed to the Mercator engine during translation.
	Restrictions: all switches must be lowercase and preceded by a dash
	Default: none
dateResolutionYear	The base year used to resolve the century when interpreting two-digit year data.
	Two-digit years less than the last two digits of this date are interpreted as being in the *next* century, while two-digit years equal to or greater than this date are interpreted as being in the *same* century.
	For example, if set to 1923, 00 is interpreted as 2000, 22 is interpreted as 2022 and 23 is interpreted as 1923.
	Default: 1950
auditDumpFilename	Internal debugging use only.
auditSwitch	Reads the Mercator map and overrides or allows what is indicated in the map with respect to the audit function.
	Restrictions—valid values – yes: executes audit logging function if enabled in the map, does not execute audit logging function if disabled in the map. – no: overrides audit logging function if enabled in the map.
	Default: yes
traceSwitch	Reads the Mercator map and overrides or allows what is indicated in the map with respect to the trace function.
	Restrictions—valid values – yes: executes trace function if enabled in the map, does not execute trace function if disabled in the map. – no: overrides trace function if enabled in the map.
	Default: no

1 "Internally coded in ECXpert" means that the entry does not appear in the System Settings screens in the System Administration Interface after installation and that you only need to add it if you want to override the default value listed.

[FAGen] Section

Settings in the [FAGen] section control the way the FAGen service operates. The FAGen service generates functional acknowledgments.

NOTE	This entire section is internally coded in ECXpert. It does not appear in the System Administration interface until you add it. You only need to add this section when you want to change any of the default values for any of the entries listed.

Table C-41 Settings in the [FAGen] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change. (internally coded[1] in ECXpert)
Configurable options	
output_dir	Full path to directory for output files for FAGen.
	Default: $NSBASE/NS-apps/ECXpert/data/output/ (internally coded* in ECXpert)

1 "Internally coded in ECXpert" means that the entry does not appear in the System Settings screens in the System Administration Interface after installation and that you only need to add it if you want to override the default value listed.

[ui_section] Section

Settings in the [ui_section] section control the way the user interface (UI) and CGIs operate.

Table C-42 Settings in the [ui_section] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
	Restrictions: Must be configuration; do not change.

Table C-42   Settings in the [ui_section] section *(Continued)*

Entry	Description
stdfile_flag	Standard file flag.
	Restrictions—valid values: - static = unique logfile per cgi
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no
stderr_path	Fully specified path for log file to receive error output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ ECXpert.log.cgi.dat

[ORACLE_ENV] Section

Settings in the [ORACLE_ENV] section control the vendor-specific aspects of the interface to the Oracle database that is used with ECXpert.

Table C-43   Settings in the [ORACLE_ENV] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
Configurable options	
ORACLE_HOME	Home directory where Oracle is installed.
	Default: set during installation
NLS_LANG	Character set support for database.
	Restrictions—must be a standard character set identifier—most commonly used: - AMERICAN_AMERICA.US7ASCII = standard US ASCII - AMERICAN_AMERICA.WE8ISO8859P1 = western European 8-bit
	Default: AMERICAN_AMERICA.US7ASCII

Table C-43 Settings in the [ORACLE_ENV] section *(Continued)*

Entry	Description
ORA_NLS	Location of Oracle NLS files.
	Default: $ORACLE_HOME/ocommon/nls/admin/data
ORA_NLS33	Location of Oracle NLS33 files.
	Default: $ORACLE_HOME/ocommon/nls/admin/data
ORA_NLS32	Location of Oracle NLS32 files.
	Default: $ORACLE_HOME/ocommon/nls/admin/data/Oracle7nlb

[DB_SECTION] Section

Settings in the [DB_SECTION] section control the aspects of the interface to the database which are independent of the vendor-specific database software used with ECXpert.

Table C-44 Settings in the [DB_SECTION] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be configuration; do not change.
DB_VENDOR	Database vendor.
	Restrictions: Must be ORACLE; do not change.
DB_TYPE	With Oracle, the name of the database access library.
	Restrictions: Must be libora4d.so for release version and libora7d.so for debug version; do not change.
DB_ENV_SECTION	The section to use for database parameters.
	Restrictions: Must be ORACLE_ENV for release 3.6
Configurable options	
DB_SERVER	Oracle's tns name for the remote/local database server.
	Default: set during installation

Table C-44   Settings in the [DB_SECTION] section *(Continued)*

Entry	Description
DB_DATABASE	With Oracle, the database name within Oracle (usually null; this feature of Oracle not generally used).
	Default: set during installation
DB_DEFAULT_CONNECTIONS	Number of connections in pool.
	Default: 25
DB_TRIGGER_PROCEDURE	Use database triggers for faster access
	Restrictions—valid values: - 0 = off - 1 = on
	Default: 1
DB_USER	Master database user's ID.
	Default: set during installation
DB_PASSWORD	Master database user's password.
	Restrictions: must be encrypted using bdgsetpasswd
	Default: set during installation
DB_ARRAY_SIZE	Controls the database API behavior (event log, bdgdocument, bdginterchange, etc.)
	Default: 100
Debug output configuration	
DB_TRACE	Database trace level.
	Restrictions—valid values: - 0 = none - 1 = low - 3 = high
	Default: 0
debug_flag	Turn on low level tracing information? (Used by database API applications that do not have a section in ecx.ini.)
	Restrictions—valid values: yes, no
	Default: no

[legacy-oracle-apps] Section

Settings in the [legacy-oracle-apps] section control the way the Legacy Server for Oracle Financials operates.

NOTE	Settings in the [legacy-oracle-apps] section provide a "foundation" for the [legacy-sap] (see "[legacy-sap] Section" on page 705) and [legacy-mq-series] (see "[legacy-mq-series] Section" on page 708) sections.
	All settings for parameters in the [legacy-oracle-apps] section automatically apply to the other sections. When the other sections explicitly contain the same parameter with a different setting, that setting overrides the setting in the [legacy-oracle-apps] section.

Table C-45   Settings in the [legacy-oracle-apps] section

Entry	Description
Parameters that should not be changed	
section_type	Type of section.
	Restrictions: Must be server; do not change.
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 12; do not change.
snmp_trap_flag	Trap information for SNMP service? *Restrictions*—valid values: yes, no
	Default: no
snmp_trap_level	SNMP event level to trap.
	Restrictions—valid values: - 0 = all messages - 10 = information, warning, and error messages - 20 = warning and error messages - 30 = error messages only
	Default: 0
port_location	Location to pick up the port.
	Default: mmap

Table C-45   Settings in the [`legacy-oracle-apps`] section *(Continued)*

Entry	Description
listener_type	Listener type.
	Restrictions—valid values: - thread = runs as a thread - process = runs as a process
	Default: thread
max_listeners[1]	Maximum number of listener threads that are allowed. Base on concurrent processing needs, if multiple submission units are to be processed in parallel.
	Restrictions: Total number of threads you specify must be supported by your hardware.
	Default: 4
listener_level	Listener level. Number of listener threads to launch on startup.
	Default: 1; do not change.
runnable_flag	Can executable be run?
	Restrictions—valid values: - yes = executable will be run as needed - no = executable will not be run (for example, a test situation)
	Default: yes
thread_mode	Thread operational mode
	Restrictions—valid values: - threaded = run threaded - serialized = run serialized
	Default: threaded (only the Admin. server should be serialized; in all other sections where section_type= server, it is strongly recommended that you leave this setting as threaded)
type	Type of executable.
	Restrictions: must be daemon, do not change.
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both)

Table C-45 Settings in the [legacy-oracle-apps] section *(Continued)*

Entry	Description
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
operation	Type of communications operation.
	Restrictions: must be send, do not change
start_mode	Server start mode.
	Restrictions—valid values: commandline, background
	Default: background
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
File and directory information	
exec_path	Executable path. Full path to the executable.
	Default: $NSBASE/NS-apps/ECXpert/bin/legacyroled
Multi-threading parameters—do not change	
max_thread_flag	Limit the number of threads running in system?
	Restrictions—valid values: yes, no
	Default: yes; do not change.
worker_max_threads	Number of worker threads to run in parallel.
	Default: 4; do not change.
master_max_threads	Number of master threads to run in parallel.
	Default: 4; do not change.
master_max_threads_queued_flag	Queue master threads above master_max_threads?
	Restrictions—valid values: yes, no
	Default: yes; do not change.

Table C-45 Settings in the [`legacy-oracle-apps`] section *(Continued)*

Entry	Description
`master_max_threads_queued`	Maximum number of master threads to queue.
	Default: `500`; do not change.
`master_max_threads_stacked`	Maximum number of master threads to place on stack.
	Default: `500`; do not change.
Port information	
`admin_port`	Administrative port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`admin_port_type`	Administrative port type.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
`listener_port`	Listener port number.
	Restrictions: Ports used by ECXpert must not be used by other applications.
	Default: set during installation
`listener_port_type`	Listener port type. Only set when adding your own `network_id`.
	Restrictions—valid values: - `dynamic` = Administrative Server assigns - `manual` = always use value in `admin_port`
	Default: `dynamic`
Configurable options	
`autostart_flag`	Start this process automatically when the ECXpert Administrative Server is started?
	Restrictions—valid values: `yes, no`
	Default: `no`

Table C-45   Settings in the [legacy-oracle-apps] section *(Continued)*

Entry	Description
restart_flag	Restart this executable automatically if it experiences an abnormal exit?
	Restrictions—valid values: - yes = automatically restart when ECXpert is restarted (you are confident manual intervention is not required) - no = do not restart when ECXpert is restarted (you expect that manual intervention might be required)
	Default: no
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - true = yes, pre-enveloped - false = no, not pre-enveloped
	Default: true
MERCATORMAP_DEBUG_FLAGS	Flags to pass to Mercator for map debugging.
	Restrictions—valid values: - -TIO = trace on input/output - -AD = trace on database transactions
	Notes: You can pass either or both parameters; a leading dash (-) is part of each parameter.
	Default: NONE - no flags passed
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists
	- no = do not display in protocol selection lists *Default:* yes
internal_name	The name used internally within ECXpert. Must be LOA. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: Legacy Server (Oracle)
Debug output configuration	
debug_flag	Turn on low level tracing information?
	Restrictions—valid values: yes, no
	Default: no

Table C-45 Settings in the [`legacy-oracle-apps`] section *(Continued)*

Entry	Description
`stderr_path`	Fully specified path for log file to receive error output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ `ECXpert.log.legacyserver.dat`
`stdout_path`	Fully specified path for log file to receive standard output from low level trace.
	Default: $NSBASE/NS-apps/ECXpert/data/log/ `ECXpert.log.legacyserver.dat`
`bundle_all`	Package all data together as one file (one body part)?
	Note: Do not set this parameter to `true` with EDI data. Sending multiple interchanges in one email violates EDI standards, so ECXpert will not send EDI data with `bundle_all` set to `true`.
	Restrictions—valid values: - `yes` - `no`
	Default: `no`
`use4digit_year`	Use all four digits for year, for year 2000 compliance?
	Restrictions—valid values: - `yes` = use all four digits, year 2000 compliant - `no` = use only last two digits, not year 2000 compliant
	Default: `no`
	Note: Only applicable in versions of X12 standard that support an 8-digit GS04 value (specifically, version 3072 and version 4010 and later versions).
`log_flag`	Should entry appear in the logging API?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
`log_prefix`	File prefix used for name generation.
	Default: `ECXpert.log.legacyserver.dat`
`log_dir`	Full path to directory for log files.
	Default: $NSBASE/NS-apps/ECXpert/data/log

1 The Oracle database parameter for maximum number of connections should be set to accommodate all your settings for
`max_listeners` and `max_threads`, according to the following formula:
Oracle maximum connections = (total (`max_listeners`) + total (`max_threads`)) x 2

[legacy-sap] Section

Settings in the [legacy-sap] section control the way the Legacy Server for SAP operates.

NOTE	Settings in the [legacy-sap] section build upon the settings in the [legacy-oracle-apps] section (see "[legacy-oracle-apps] Section" on page 699).
	All settings for parameters in the [legacy-oracle-apps] section automatically apply to the [legacy-sap] section. When this section explicitly contains the same parameter with a different setting, that setting overrides the setting in the [legacy-oracle-apps] section.

Table C-46   Settings in the [legacy-sap] section

Entry	Description
Parameters that should not be changed	
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 12; do not change.
port_location	Location to pick up the port.
	Default: mmap
type	Type of executable.
	Restrictions: must be daemon, do not change.
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both)
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10

Table C-46   Settings in the `[legacy-sap]` section *(Continued)*

Entry	Description
operation	Type of communications operation.
	Restrictions: must be send, do not change
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes
internal_name	The name used internally within ECXpert. Must be LSAP. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: Legacy Server (SAP)
Machine dependent information	
host_name	IP address of host machine where instances of executable are run.
	Restrictions: Must be a valid IP address in your domain.
	Default: set during installation
Port information	
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
Configurable options	
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values: - true = yes, pre-enveloped - false = no, not pre-enveloped
	Default: true

Table C-46   Settings in the [legacy-sap] section *(Continued)*

Entry	Description
ale_server_auto_start	Automatically attempt to connect to SAP, using rfc_server_section, when the [legacy-oracle-apps] server is started?
	Restrictions—valid values: yes, no
	Default: no
	Note: You can leave this set to no if you only want to send documents from ECXpert to SAP. It *must* be set to yes for bi-directional exchanges.
rfc_server_section	The RFC server section name in the saprfc.ini file, located in *$NSBASE*/NS-apps/ECXpert/cgi-bin.
	Default: [YOUR SECTION]
	Note: You *must* replace this default with a valid name.
outbound_idoc_workingdir	SAP outbound directory.
	Default: [working dir] (for example, /tmp/TIDDIR)
	Note: You *must* replace this default with a valid path.
outbound_idoc_dir	Idoc outbound directory.
	Default: [final dir e.g. /tmp/outboundidocs]
	Note: You *must* replace this default with a valid path.
ale_idoc_submit_mode	Idoc submission mode.
	Restrictions—valid values: - ecx = file is submitted to ECXpert, using the combination of values specified for idoc_sender, idoc_receiver, and idoc_doctype to determine the service list. - directory = file is left in directory
	Default: directory
idoc_sender	The sending Member ID specified in the supporting partnership.
	Default: [*]
	Note: You *must* replace this default with the sending Member ID from the supporting partnership if ale_idoc_submit_mode is set to ecxpert.

Table C-46   Settings in the [legacy-sap] section *(Continued)*

Entry	Description
idoc_receiver	The receiving Member ID specified in the supporting partnership.
	Default: [*]
	Note: You *must* replace this default with the receiving Member ID from the supporting partnership if ale_idoc_submit_mode is set to ecxpert.
idoc_doctype	Document Type specified in the supporting partnership.
	Default: [idocs]
	Note: You *must* replace this default with the Document Type from the supporting partnership if ale_idoc_submit_mode is set to ecxpert.

[legacy-mq-series] Section

Settings in the [legacy-mq-series] section control the way the Legacy Server for MQSeries operates.

Table C-47   Settings in the [legacy-mq-series] section

Entry	Description
Parameters that should not be changed	
server_type	Type of server. All servers (section_type = server) sharing same server_type value are treated as multiple instances of same server.
	Default: 12; do not change.
port_location	Location to pick up the port.
	Default: mmap
type	Type of executable.
	Restrictions: must be daemon, do not change.

Table C-47 Settings in the [legacy-mq-series] section *(Continued)*

Entry	Description
data_type	Object type(s) to bundle for send.
	Restrictions—valid values: - e = "edi," EDI format - a = "application," proprietary application format - b = "both," both EDI and proprietary formats
	Default: b (both)
listener_time_out	Listener timeout, in seconds.
	Default: 10
admin_time_out	Admin server time out period, in seconds.
	Default: 10
operation	Type of communications operation.
	Restrictions: must be send, do not change
is_comm_agent	Is this a Communications Agent?
	Restrictions—valid values: - yes = display in protocol selection lists - no = do not display in protocol selection lists
	Default: yes
internal_name	The name used internally within ECXpert. Must be LMQ. Do not change.
visible_name	The name displayed externally by ECXpert.
	Default: Legacy Server (MQ Series)
Port information	
admin_port_type	Administrative port type.
	Restrictions—valid values: - dynamic = Administrative Server assigns - manual = always use value in admin_port
	Default: dynamic
Configurable options	
header_separator	The text string to use for the header separator.
	Default: ECX_MQSERIES_HEADER_SEPARATOR

Table C-47 Settings in the `[legacy-mq-series]` section *(Continued)*

Entry	Description
MQSERVER	Your MQServer definition.
	Restrictions: channel/`TCP`/*ip_address* where *channel* is any channel name and *ip_address* is the IP address of the machine where the MQServer is installed
	Default: [`YOUR MQSERVER Definition. e.g.` `CHAN1/TCP/111.22.33.444`]
	Note: You *must* replace this default with a valid MQServer definition.
	Caution: If you plan to exchange messages 4MB or larger in size, do not set this parameter. Instead set MQCHLLIB and MQCHLTAB.
MQCHLLIB	The path to the directory containing the client channel definition table file.
	Default: [`The directory that contains...`]
	Note: If you use this parameter, you *must* replace this default with a valid path to the directory containing the client channel definition table file, and delete the "#" in front of the line.
	Caution: Do not set MQSERVER if you set this parameter; a non-null setting for MQSERVER causes this parameter to be ignored. If you do not plan to exchange messages 4MB or larger in size, you only need to set MQSERVER.
MQCHLTAB	The client channel definition table file name.
	Default: `AMQCLCHL.TAB`
	Note: If you use this parameter, you *must* replace this default with a valid name of the client channel definition table file.
	Caution: Do not set MQSERVER if you set this parameter; a non-null setting for MQSERVER causes this parameter to be ignored. If you do not plan to exchange messages 4MB or larger in size, you only need to set MQSERVER.
dead_letter_q_flag	If `MQ put` fails, write to dead letter queue?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`
header_in_separate_file	Put MQS message header in separate file?
	Restrictions—valid values: `yes`, `no`
	Default: `yes`

Table C-47 Settings in the `[legacy-mq-series]` section *(Continued)*

Entry	Description
pre_enveloped_edi	Allow retrieval of EDI documents with existing envelopes?
	Restrictions—valid values:
	- `true` = yes, pre-enveloped
	- `false` = no, not pre-enveloped
	Default: `true`

[attributes] Section

Settings in the `[attributes]` section are not really settings at all. The "value" listed for an entry in this section is simply a description for the entry. The entry itself appears in one or more other sections.

Required *Mercator* Settings for ANSI Functional Acknowledgment (997)

This appendix provides detailed information on the Mercator type tree and map settings that are required to make full use of the ECXpert confirmation message capabilities. The following topics are presented:

- Mercator ANSI X12 Type Trees
- Audit Settings Needed by Mercator Maps

Mercator ANSI X12 Type Trees

To use the segment and element acknowledgment levels in ECXpert, Mercator type trees must have certain attributes and Mercator maps must be built with additional audit settings.

The following discussion assumes a standard ANSI X12 type tree supplied by Mercator. If you have a custom ANSI X12 type tree supplied by another source, the segment and element acknowledgment levels might not work properly. Please contact iPlanet for more details.

1. Ensure that the first component of the `Partner X12 Inbound Transmission EDI group` has the `Restart` attribute set.

2. In the `Partner X12 Inbound Interchange EDI` group, ensure that the first component has the `Identifier` attribute set, and the fifth component has the `Restart` attribute set.

Partner X12 Inbound Interchange EDI	
Component	**Rule**
[I] Partner Inbound ISA Segment Control ANSI	
ISB Segment Control ANSI (0:1)	
ISE Segment Control ANSI (0:1)	
TAI Segment Control ANSI [s]	
[R] Inbound Partner Funct'lGroup ANSI (0:99999)	
ICA Segment Control ANSI	Intercha

3. In the `ANYTS ANYFG Inbound Partner Funct'lGroup ANSI EDI` group, where `ANYTS` refers to the specific Transaction Set you are using as input, such as `#850`, and `ANYFG` refers to the X12 standard you are using, such as `F4010`, ensure that the first component has the `Identifier` attribute set and the second component has the `Restart` attribute set.

#850 F4010 Inbound Partner Funct'lGroup ANSI EDI	
Component	**Rule**
[I] GS Segment V4010	Funct
[R] Transaction #850 Inbound Partner Set V4010 [s]	
GE Segment V4010	Group

4. In the `Transaction ANYTS Inbound Partner Set ANYFG ANSI EDI`, where `ANYTS` refers to the specific Transaction Set you are using as input, such as `#850`, and `ANYFG` refers to the X12 standard you are using, such as `F4010`, ensure that the first component has the `Identifier` attribute set.

Transaction #850 Inbound Partner Set V4010 ANSI EDI	
Component	**Rule**
[I] ST Segment	TSIDC
DCG Segment	
CUR Segment [0:1]	
REF Segment (s)	
PER Segment (0:3)	
TAX Segment [s]	

5. It is possible to use the `Restart` attribute for components within the Transaction Set. This is to allow Mercator to "Restart" whenever input data fails validation. Mercator will only map valid records.

It is strongly recommended that you use this `Restart` attribute within a Transaction Set judiciously: assign the `Restart` attribute only to components that have large repetitions.

For example, if you typically receive a purchase order with thousands of line items, you would assign the Restart attribute to the LoopPO1 component. This would ensure that the map does not fail and any valid records would be output, given an erroneous line item.

Transaction #850 Inbound Partner Set V401D ANSI EDI
Component
PKG Segment (0:200)
TD1 Segment (0:2)
TD5 Segment (0:12)
TD3 Segment (0:12)
TD4 Segment (0:5)
MAN Segment [0:10]
PCT Segment (s)
CTB Segment (0:5)
TXI Segment (s)
LoopAMT_1 (s)
LoopN9_1 (0:1000)
LoopN1_1 (0:200)
LoopLM_1 (s)
LoopSPI (s)
LoopADV (s)
[R] LoopPO1 (1:100000)
LoopCTT (0:1)
SE Segment

Audit Settings Needed by Mercator Maps

The following screen capture shows the input card for the 850 Transaction Set of the 004010 version of ANSI X12.

The following table shows the items that have to be audited and the type of audit for each item.

Table D-1   Audit Settings for *Mercator* maps

Audit Item	Track	Detail	Item Data
Transaction ANY Inbound Partner Set ANY:ANY<>Inbound Partner Funct'lGroup ANSI:Partner X12 Inbound Interchange:input	Occurrence	None	None
ANY Segment IN Transaction ANY Inbound Partner Set ANY:ANY<>Inbound Partner Funct'lGroup ANSI:Partner X12 Inbound Interchange:input	Occurrence	None	None
Segment IN Transaction ANY Inbound Partner Set ANY:ANY<>Inbound Partner Funct'lGroup ANSI:Partner X12 Inbound Interchange:input	Error	None	None
ANY Segment IN Transaction ANY Inbound Partner Set ANY:ANY<>Inbound Partner Funct'lGroup ANSI:Partner X12 Inbound Interchange:input	Error	Occurrence	Occurrence

Note that the specific Transaction Set numbers and specific ANSI X12 version numbers have been replaced by the keyword ANY. This facilitates copying of these audit settings from one map to another. iPlanet will also provide a sample map with these audit settings already defined.

Limitations of ANSI X12 FA (997) Features

This appendix provides information on the limitations of ANSI X12 Functional Acknowledgment (FA/997) features in ECXpert. The following topic is presented:

- Limitations of ANSI X12 FA (997) Features

Limitations of ANSI X12 FA (997) Features

ECXpert derives information on translation problems from the *Mercator* map's audit log file. The audit log file does not, however, provide all the information that is necessary to generate some FA error codes.

This appendix shows how the AK1, AK2, AK3, AK4, AK5 and AK9 segments are used in acknowledging an inbound EDI functional group in ECXpert 3.6, and how the missing information in *Mercator* audit log files limits what ECXpert can report in FAs.

Two tables appear for every segment used in the ANSI X12 functional acknowledgment document (transaction set 997):

- The first table is simply a copy of the standard and lists the data elements contained in the segment, along with some basic attributes.

- The second table shows which data elements are used by ECXpert and how this element is used.

Further explanation and limitations appear in the Notes for each segment.

AK1 — Functional Group Response Header

Functional Group Response Header (as of Version 004010).

Table E-1   Standard segment data elements

REF	ELE ID	NAME	Attributes		
01	479	Functional Identifier Code	M/Z	ID	2/2
02	28	Group Control Number	M/Z	N0	1/9

Table E-2   Data elements used by iPlanet ECXpert

EL	USED	EXPLANATION
AK101	Y	Reflects GS01 element from inbound functional group, for example, PO.
AK102	Y	Reflects control number (GS06) from inbound functional group.

Transaction Set Response Header

Transaction set response header (as of Version 004010).

Table E-3   Standard data elements

REF	ELE ID	NAME	Attributes		
01	143	Transaction Set Identifier Code	M/Z	ID	3/3
02	329	Transaction Set Control Number	M/Z	AN	4/9

Table E-4   Data elements used by iPlanet ECXpert

EL	USED	EXPLANATION
AK201	Y	Reflects ST01 element from inbound transaction set. For example,, 850.
AK202	Y	Reflects control number (ST02) from inbound transaction set.

AK3—Data Segment Note

Data segment note (as of Version 004010).

Table E-5 Standard data elements

REF	ELE ID	NAME	Attributes		
01	721	Segment ID Code	M	ID	2/3
02	719	Segment Position in Transaction Set	M	N0	1/6
03	447	Loop Identifier Code	O	AN	1/6
04	720	Segment Syntax Error Code	O	ID	1/3

Table E-6 Data elements used by iPlanet ECXpert

EL	USED	EXPLANATION
AK301	Y	The segment ID of the data segment in error. For example,, PO1.
AK302	Y	The position within the transaction set of the segment in error, with the ST segment being at position 1.
AK303	N	See Note 1 below.
AK304	Y	See Note 2 below.

NOTE	1. The Mercator Audit Log does not supply the Loop Identifier Code.
	2. Only the subset from the allowed error codes in data element 720, shown in the following table, are used.

:

Table E-7   Subset from allowed error codes in data element 720

Code	Definition	Explanation
2	Unexpected segment	This code is applied whenever the Mercator parser encounters an unexpected segment in the input file. This code would apply to: • Invalid or undefined segments • Segments out of place or out of sequence • The first segment of a loop that exceeds its maximum use • Segments that exceed their maximum use
3	Mandatory segment missing	This code is applied whenever a mandatory segment is missing from the input file.
8	Segment has data elements in errors	This code is applied whenever a segment has data elements in error. This only appears for ANSI X12 versions above 003040.

AK4—Data Element Note

Data element note (as of Version 004010).

Table E-8   Standard data elements

REF	ELE ID	NAME	Attributes		
01	C030	Position in Segment	M		
02	725	Data Element Reference Number	O	N0	1/4
03	723	Data Element Syntax Error Code	M	ID	1/3
04	724	Copy of Bad Data Element	O/Z	AN	1/99

Table E-9   Data elements used by iPlanet ECXpert

EL	USED	EXPLANATION
AK401	Y	The position in the segment of the data element in error, with the segment ID being at position 1. See Note 1 below.
AK402	N	See Note 2 below.
AK403	Y	See Note 3 below.
AK404	Y	Copy of the data element in error.

NOTE	1. In ANSI X12 Version 004010, this element is actually a composite element, with the first component indicating the position in the segment of the composite data element in error, and the second component indicating the component data element position in the composite element.
	2. In other words, if the element in error is a composite element, the first component of AK401 reflects the position in the segment of the composite element, and the second component of AK402 reflects the component in error of this composite element.
	3. ECXpert does not build composite elements. Thus, if a composite element is in error, only the position of the composite element in the segment is reported.
	4. The Mercator Audit Log does not supply the Data Element Reference Number.
	5. Only the subset from the allowed error codes in data element 720, shown in the following table, are used.

Table E-10 Subset from the allowed error codes in data element 720

Code	Definition	Explanation
1	Mandatory data element missing	This code is applied whenever a mandatory data element is missing.
4	Data element too short	This code is applied whenever the Mercator Audit Log reports that an element failed size restriction. Since Mercator does not report how the element failed size restriction, this code is applied for data elements that are too short or too long.
6	Invalid character in data element	This code is applied whenever the Mercator Audit Log reports that an element failed presentation.
7	Invalid code value	This code is applied whenever the Mercator Audit Log reports that an element failed restriction.

Table E-10 Subset from the allowed error codes in data element 720 *(Continued)*

Code	Definition	Explanation
8	Invalid date	This code is applied whenever the Mercator Audit Log reports that an element failed presentation **and** the element's name in the type tree definition contains the literal Date. It is important to note that even if the data element in error was a date but its type tree definition did not contain the literal Date, code 6 will be used instead. This is because the Mercator Audit Log does not report anything beyond "failed presentation".
9	Invalid time	This code is applied whenever the Mercator Audit Log reports that an element failed presentation **and** the element's name in the type tree definition contains the literal Time. It is important to note that even if the data element in error was a time but its type tree definition did not contain the literal Time, code 6 will be used instead. This is because the Mercator Audit Log does not report anything beyond "failed presentation".
10	Exclusion condition violated	This code is applied whenever the Mercator Audit Log reports that an element failed a component rule. Code 10 has very little to do with its real meaning in the standard.

AK5—Transaction Set Response Trailer

AK5 Transaction set response trailer (as of Version 004010).

Table E-11   Standard data elements

REF	ELE ID	NAME	Attributes		
01	717	Transaction Set Acknowledgment Code	M	ID	1/1
02	718	Transaction Set Syntax Error Code	O	ID	1/3
03	718	Transaction Set Syntax Error Code	O	ID	1/3
04	718	Transaction Set Syntax Error Code	O	ID	1/3
05	718	Transaction Set Syntax Error Code	O	ID	1/3
06	718	Transaction Set Syntax Error Code	O	ID	1/3

Table E-12   Data elements used by iPlanet ECXpert

EL	USED	EXPLANATION
AK501	Y	A code indicating whether the inbound transaction set was accepted or rejected. See Note 1 below.
AK502	Y	For AK5 segments with a AK501 value of 'E' (transaction set in error) or with a AK501 value of 'R' (transaction set rejected), this data element supplies an error code. See Note 2 below.
AK503	N	See Note 3 below.
AK504	N	See Note 3 below.
AK505	N	See Note 3 below.
AK506	N	See Note 3 below.

| NOTE | 1. The following list shows how the 'A' (accepted), 'E' (errors noted) and 'R' (rejected) codes are used: |

- A transaction set is accepted (code 'A') if Mercator completes successfully **and** the first output card (file) has length greater than 0.

- A transaction set is in error (code 'E') if Mercator completes successfully but reports input errors **and** the first output card (file) has length greater than 0.

- A transaction set is rejected (code 'R') if it fails parse **or** Mercator fails to complete successfully **or** Mercator completes successfully **and** the first output card(file) has length 0.

2. Only the subset from the allowed error codes in data element 718, shown in the following table, are used.

3. Only one instance of data element 718 is used.

Table E-13 Subset from allowed error codes in data element 718

Code	Definition	Explanation
2	Transaction set trailer missing	Self-explanatory.
3	Transaction Set control number in header and trailer do not match	Self-explanatory.
4	Number of included segments does not match actual count	Self-explanatory.
5	One or more segments in error	This code is applied for all other cases when AK501 has an 'E' or an 'R'.

AK9—Functional Group Response Trailer

AK9 Functional group response trailer (as of Version 004010).

Table E-14   Standard data elements

REF	ELE ID	NAME	Attributes		
01	715	Functional Group Acknowledgment Code	M	ID	1/1
02	97	Number of Transaction Sets Included	M	N0	1/6
03	123	Number of Received Transaction Sets	M	N0	1/6
04	2	Number of Accepted Transaction Sets	M	N0	1/6
05	716	Functional Group Syntax Error Code	O	ID	1/3
06	716	Functional Group Syntax Error Code	O	ID	1/3
07	716	Functional Group Syntax Error Code	O	ID	1/3
08	716	Functional Group Syntax Error Code	O	ID	1/3
09	716	Functional Group Syntax Error Code	O	ID	1/3

Table E-15   Data elements used by iPlanet ECXpert

EL	USED	EXPLANATION
AK901	Y	A code indicating whether the inbound functional group was accepted or rejected. See Note 1 below.
AK902	Y	Reflects the included transaction sets element (GE01) from the original functional group.
AK903	Y	Reflects the number of transaction sets received and processed.
AK904	Y	Reflects the number of transaction sets processed successfully and accepted.
AK905	Y	For AK9 segments with a AK901 value of 'E' (some transaction sets in error) or with a AK901 value of 'P' (some transaction sets rejected) or with a AK901 value of 'R' (functional group rejected), this data element supplies an error code. See Note 2 below.
AK906	N	See Note 2 below.
AK907	N	See Note 2 below.
AK908	N	See Note 2 below.

Table E-15   Data elements used by iPlanet ECXpert *(Continued)*

EL	USED	EXPLANATION
AK909	N	See Note 2 below.

NOTE	
	1. The following list shows how the 'A' (accepted), 'E' (errors noted in some transaction sets), 'P' (some transaction sets rejected) and 'R' (rejected) codes are used:
	• A functional group is accepted (code 'A') if **all** included transaction sets are accepted.
	• A functional group is in error (code 'E') if one or more included transaction sets is in error **and** no included transaction sets are rejected.
	• A functional group has a code 'P' (some transaction sets rejected) if one or more included transaction sets are rejected.
	• A functional group is rejected (code 'R') if it fails parse **or all** included transaction sets are rejected.
	2. Only the subset from the allowed error codes in data element 716, shown in the following table, are used
	3. Only one instance of data element 716 is used.

Table E-16   Subset from allowed error codes in data element 716

Code	Definition	Explanation
3	Functional group trailer missing	Self-explanatory.
4	Group control number in header and trailer do not match	Self-explanatory.
5	Number of included transaction sets does not match actual count	Self-explanatory.

AIAG Administration

This appendix discusses the AIAG E-5 2000 guideline as implemented in ECXpert version 3.5 . It is assumed that the reader is familiar with the AIAG E-5 2000 specifications before reading this document.

The following topics are covered:

- Overview

- AIAG Server

    - Configuring the Servlets

    - Configuring the aiag.ini File

    - Configuring the RMI Server

    - AIAG Server Changes in ecx.ini File

- AIAG Server Handling of E-5 2000 Functions

    - API Definition

    - Deliver

    - Obtain

    - Acknowledge

    - Loop Back Test

- AIAG comm agent (client)

- The Manual API

- AIAG Transaction Table

- Error Numbers and Messages

Overview

AIAG E-5 2000 is a B2B document exchange protocol which defines the meta-data (XML) and transport (HTTP) mechanism that are used to exchange documents between trading partners. The ECXpert implementation of the v2000 guidelines consists of two components- the server and the client. The server component is implemented as a set of servlets and a seperately initialized RMI server. The client is implemented as a comm-agent for ECXpert which can be started using the admin UI.

Before attempting to run any of the AIAG features, the database setup script AIAG_setup.sh must be run. This script enables support for AIAG. For details on running the script, see the section on post-installation tasks in the *iPlanet ECXpert Installation Guide*.

AIAG Server

The AIAG Server implementation in ECXpert 3.5 consists of a set of servlets and a standalone RMI server. To configure the server, the following steps must be performed after the AIAG_setup.sh script has been run. For details on running the script, see the section on post-installation tasks in the *iPlanet ECXpert Installation Guide*.

1. Configure the servlets - see the section "Configuring the Servlets" below

2. Configure the aiag.ini file - see the section "Configuring the aiag.ini File" on page 734

3. Configure the RMI Server - see the section "Configuring the RMI Server" on page 738

4. Configure the ecx.ini file - see the section "AIAG Server Changes in ecx.ini File" on page 738

Configuring the Servlets

The servlets can be found in the directory $BDGHOME/servlet directory. To enable them to serve the clients, some web server configuration is required. Perform the following steps to set up the servlets.

1. Verify that the following line appears in the `obj.conf` file:

   ```
   NameTrans fn="pfx2dir" from="/servlet" dir={$BDGHOME}/servlet
   ```

NOTE	It is assumed that you have run the AIAG_setup.sh script to enable support for AIAG E-5 2000 communications in ECXpert in accordance with the instructions provided in the post-installation tasks section of the *iPlanet ECXpert Installation Guide*.

2. If there is any other line starting with `NameTrans fn="pfx2dir" from="/servlet"`, remove it.

Configuring the aiag.ini File

This file contains many parameters to specify the behavior of the AIAG Server as well as information related to the E-5 services and default messages that the server sends out with every reply. Table F-1 describes the sections in the aiag.ini file. Following the table is the representation of the file itself, which exists in the `$NSBASE/NS-apps/ECXpert/config` directory.

Table F-1   Description of aiag.ini File Sections and Parameters

Section	Parameter	Description
serverinfo	services	The various services offered by the server, each of which is separated by a semi-colon.
		Example: `deliver;obtain;APIAccess`
	messages	The default messages to be sent along with the server responses. Each message is separated by a semi-colon:
		Example: `message1;MessageA`
	defcontactURI	The default URI to contact the server admin/mgr. It is expressed as a http URL with default parameters, if any.
	lastAccess	DateTime that specifies when the server was last accessed.
		"last Access" is the DateTime when the APIs were last UPDATED and not accessed. This DateTime should be changed appropriately whenever the API configuration is changed.
		Also, it should conform to the ISO 8601 standard.
		Example: `YYYY-MM-DDTHH:MM:SS.mmmZ.`
Service		For every service specified in the services option of the serverinfo section, there exists a section with the following information.
	submitDTDURI	A http URL specifying the path of the DTD for the Submit XML.
		Example: `http://server.com/E5_V20_Deliver_Submit.dtd`
		(as an exception it doesn't exist for the API Access service)
	resultDTDURI	A http URL specifying the path of the DTD for the Result XML.
		Example.
		`http://server.com/E5_V20_Deliver_Result.dtd`

Table F-1 Description of aiag.ini File Sections and Parameters *(Continued)*

Section	Parameter	Description
	submit	Type of the Http Post request supported.
		Example. `FormEncodedPostWithFile,FormEncodedPost`
	result	Type of the Http Response expected
		Example. `Single, Multiple`
	httpURI	The URI where this service can be accessed
Message		For every message specified in the messages option of the serverinfo section, there exists a section with the following information.
	codetype	Type of the message
		Example. `Informational Serious, Warning`
	codenumb	The message code number.
		Example. `310`
	datetime	DateTime when the message was posted.
		Example. `2000-12-10T18:23:59.742Z`
	description	Description of the message.
		Example. `The system will be unavailable.`
	explanation	Explanation of the description.
		Example. `Due to hardware problems, the system will not be available.........`
	contactURI	The URI to contact for further information
		Example. `http://server.com/contact.html?Code=900`
	params	List of parameters (if any) with respect to the message.
		Example. `fromtime, totime`
	param	The parameter and its value
		Example. `fromtime = 2001-12-10T18:23:59.742Z`

Code Example F-1   `aiag.ini` File Representation

```
##############################################
#                                            #
#                 AIAG Server                #
#                                            #
##############################################
    [serverinfo]
    #
    # These parameters should not be changed
    #
    lastAccess = 2000-09-10T18:23:59.742Z
    services = deliver;obtain;acknowledge;APIsAccess;deliverTest
    messages = message1;message2
    defcontactURI = http://server.com/contact.html?Code=310

    [deliver]
    #
    # deliver service details
    #
    submitDTDURI = http://server.com/E5_V20_Deliver_Submit.dtd
    resultDTDURI = http://server.com/E5_V20_Deliver_Result.dtd
    submit = FormEncodedPostWithFile
    result = Single
    httpURI = http://kriti:15010/servlet/aiag.AIAGDeliverServlet

    [obtain]
    #
    # obtain service details
    #
    #
    submitDTDURI = http://server.com/E5_V20_Obtain_Submit.dtd
    resultDTDURI = http://server.com/E5_V20_Obtain_Result.dtd
    submit = FormEncodedPost
    result = Multiple
    httpURI = http://kriti:15010/servlet/aiag.AIAGObtainServlet

    [acknowledge]
    #
    # acknowledge service details
    #
    submitDTDURI = http://server.com/E5_V20_Acknowledge_Submit.dtd
    resultDTDURI = http://server.com/E5_V20_Acknowledge_Result.dtd
    submit = FormEncodedPost
    result = Single
    httpURI = http://kriti:15010/servlet/aiag.AIAGAcknowledgeServlet

    [APIsAccess]
    #
    # APIsAccess service details
    #
    resultDTDURI = http://server.com/E5_V20_APIsAccess_Result.dtd
    submit = FormEncodedPost
    result = Single
```

Code Example F-1   `aiag.ini` File Representation *(Continued)*

```
    httpURI = http://kriti:15010/servlet/aiag.AIAGAPIDefinitionServlet

    [deliverTest]
    #
    # deliverTest service details
    #
    submitDTDURI = http://server.com/E5_V20_Deliver_Submit.dtd
    resultDTDURI = http://server.com/E5_V20_Obtain_Result.dtd
    submit = FormEncodedPostWithFile
    result = Single
    httpURI = http://kriti:15010/servlet/aiag.AIAGDeliverTestServlet

    [message1]
    *
    * message details
    *
    codetype = Informational
    codenumb = 310
    description = Default description of the sample message
    explanation = Default explanation of the sample message1 not be available
...
    contactURI = htjjtp://server.com/contact.html?Code=310
    params = msg1par1;msg1par2
    msg1par1 = msg1val1;
    msg1par2 = msg1val2;

    [message2]
    *
    * message details
    *
    codetype = Informational
    codenumb = 310
    datetime = 2000-09-10T18:23:59.742Z
    description = The system will be unavailable
    explanation = Due to hardware problems the system will not be available ...
    contactURI = http://server.com/contact.html?Code=310
    params = msg2par1;msg2par2
    msg2par1 = msg2val1;
    msg2par2 = msg2val2;
```

Configuring the RMI Server

The AIAG RMI server works in conjunction with the servlets to serve AIAG E-5 requests. The server can be started and stopped using the shell script `aiagserver` available in `$BDGHOME/bin` directory. Run the command using the following syntax:

```
aiagserver -[start|stop]
```

CAUTION	The server will not work properly if `ecx.ini` and `aiag.ini` files are not configured properly.

NOTE	If ECX admin server is shutdown for some reason and then restarted then the RMI server also needs to be restarted (stopped and started) to work properly.

AIAG Server Changes in ecx.ini File

The ecx.ini file contains a section for the comm-httpaiag, as shown on . This section is used to specify the parameters for the comm-agent. One new addition to this section is the addition of `dtdpath` variable at the end. This specifies the full path name for the directory where dtd's are stored. The other variables are not relevant to the server but are related to the comm-agent.

AIAG Server Handling of E-5 2000 Functions

This section describes how the AIAG server handles the different services. All the messages specified in the mesages section are added to all the output XML.

API Definition

The API Definition results are generated using the information specified in `aiag.ini` file, described and displayed in

CAUTION	If the `aiag.ini` file is not configured properly, the generated XML might be wrong. Make sure you configure all the required parameters.

Deliver

The Deliver function basically submits the incoming file to ECXpert using the `from`, `to`, and `application` fields as the `ECXpert sender`, `receiver` and `FileType`. All the other parameters are stored in the AIAGTransaction table.

Obtain

The following assumptions would be made for the incoming Obtain request.

1. If present, the `transasactionId` should be in an 'equals' tag with no other parameter present. ECXpert will return all the information associated with the document whose `transactionId` is specified. It also returns the document if `returnDocument` is true.

2. If present, the `to` parameter must be in an 'equals' tag and MUST be equal to the login member (the member specified in HTTP basic authentication) unless the member is trusted in which case it should be *. A blank tag is unacceptable since it is supposed to match null fields; an error will be returned. It will be matched with the receiver name.

3. If present the following parameters must be in an 'equals' tag.

    ❍ `from`

    ❍ `application`

    ❍ `documentDescription`

    ❍ `mimeType`

    ❍ `subSubType`

    ❍ `documentReferenceNumber`

4. The `deliverDateTime`, `obtainDateTime`,`acknowledgeDateTime` parameters should be contained in a 'between' tag; if these parameters are contained in an 'equals' tag, the values for each should either be blank or indicated as *.

5. If `transactionId` is specified, the server will just return the pre-bundled file associated with the incoming obtain request. It will only return information known to it (i.e. `from= sender, to= receiver` , `mimeType`,`subSubType` -derived from EDI doctype, otherwise blank ,`application=doctype`, `availableNow, deliverDateTime = creation datetime` of original tracking).

6. If any of the search parameters is specified, the server will poll for the documents and then return the documents and the associated parameters in XML.

7. Documents which are to be obtained should have the outgoing comm-agent specified as `HTTP-Receive` in the partnership.

Acknowledge

The Acknowledge function when called accepts acknowledgement for an Obtained document and updates the database accordingly.

Loop Back Test

The Loop Back Test function will accept a Deliver submit XML and return an Obtain results stream with no documents to test the functionality.

AIAG comm agent (client)

The AIAG client is implemented as an ECXpert comm-agent. The functions associated with the client include:

• Specifying the AIAG comm-agent as outgoing comm-agent in the Partnership Administration Protocol page - described in "Specifying Settings for HTTP for AIAG" on page 336.

• Scheduling an AIAG Obtain request - described in Table 3-13 on page 166.

• Scheduling a Deliver request - described in Table 3-13 on page 166.

The Manual API

The Manual API allows a user to Obtain or manually deliver a document to ECXpert. The manual API is the only way to access the LoopBackTest service.

The manual API simply consists of a set of HTML pages that can be found in the directory `$BDGHOME/UI/html/aiag`

These pages can be accessed by adding the default suffix, `/aiag,` to the ECXpert admin URL. For example, if you access the ECXpert Admin UI at:

`'http://server.com:8080/'`

the manual API can be accessed at: `http://server.com:8080/aiag`

You can customize these pages to add more HTML as long as the form fields are preserved.

AIAG Transaction Table

To support AIAG E-5 2000, another table has been added to the ECXpert database schema. The AIAG Transaction Table, shown in Table F-3, describes the data fields.

Table F-2   AIAG Transaction Table

Field	Null?	Type	Description
TransactionID	Not Null	varchar2(38)	TransactionId of the document.For a document delivered to ECXpert, it is the same as the tracking id of the submission unit. For a document obtained from ECXpert, the `transactionid` is generated. The remote AIAG client uses it to acknowledge receipt of the document.
AvailableStatus	Not Null	integer	Indicates the availability status of the document.
AIAGFrom		varchar2(60)	Identifies sending member.
AIAGTo		varchar2(60)	Identifies receiving member.
DocumentDescription		varchar2(256)	The description of the document as sent in the Submit XML of the Deliver.
MimeType		varchar2(256)	Mime Type of the document as specified in the Submit XML of the Deliver. For example, `application/EDI-X12', 'text/html'`

Table F-2   AIAG Transaction Table *(Continued)*

Field	Null?	Type	Description
SubSubType		varchar2(256)	SubSubType as provided in the Deliver Submit XML. Usually the EDI document identifier. For example: `820,997`
Application		varchar2(256)	Maps of the FileType of ECXpert used to identify the service list.
Docrefnum		varchar2(256)	A number by which the AIAG client identifies the document.
DeliverDateTime		date	Date and time when the document was delivered.
ObtainDateTime		date	Date and time when the document was last obtained.
AcknowledgeDateTime		date	Date and time when the document was last acknowledged.
AvailableDateTime		date	Not currently used.
BundleState		integer	Internal use only.

Error Numbers and Messages

Table F-3 lists the AIAG error numbers and messages that can occur to convey information or a problem with communications or processing.

Table F-3   AIAG Error Numbers and Messages List

Error No	Description
`12151`	Incorrect HTTP Path
`12152`	HTTP Content Type Not Found
12153	Corrupt HTTP Body
12154	Missing MIME boundary
12155	Corrupt Mime Component
12156	Error Parsing Mime Message
12157	Corrupt MIME boundary
12158	Unexpected Content Type
12159	Internal XML parser error
12160	Serious AIAG Message Received

Table F-3   AIAG Error Numbers and Messages List *(Continued)*

Error No	Description
12161	Deliver URL Unavailable
12162	Serious error in received XML
12163	Obtain URL Unavailable
12164	Empty MIME content
12165	Acknowledge URL Unavailable
12166	Loop back test failed
12167	Warning aiag msg received
12168	Informational aiag msg received
12169	Http connection timeout
12170	Aiag obtain transaction id

Error Numbers and Messages

Odette FTP (OFTP) User's Guide

This appendix provides detailed instructions for setting up ECXpert file exchanges using OFTP, including use of a scripting a language for X.28 connections and setup of EERP (end-to-end response) reconciliation. The following topics are covered:

- Overview
- The Odette File Transfer Protocol
- The ECXpert OFTP Server
- Setting Up OFTP Partnerships
- End-to-end Response (EERP) Support
- ECXpert OFTP Clients
- Running Two or More ECXpert OFTP Servers
- Sample OFTP Server Initialization File (ecxoftp-server.ini)
- Configuration for Two ECXpert OFTP Servers

Overview

Beginning with release 3.0, ECXpert has supported the Odette File Transfer Protocol (OFTP) both for incoming and outgoing communications. This document begins by supplying a background to OFTP.

ECXpert ships with the following suite of programs. Taken together, they implement OFTP server and client functionality over TCP/IP, X.25, and X.28 transport layers:

- ecxoftp-m-server

- ecxoftp-tcp-file-submit

- ecxoftp-tcp-eerp-submit

- ecxoftp-x25-file-submit

- ecxoftp-x25-eerp-submit

- ecxoftp-x28-file-submit

- ecxoftp-x28-eerp-submit

- ecxoftp-x28-scr-ck

Each of these programs is discussed in detail.

A 3rd party API was provided by *Techland Systems International*. Techland also provide a scripting language for X.28 connections. For testing purposes, a testing tool, *goftp*, is supplied by Techland. It can act both in client capacity and in a simplistic server capacity, handling only one connection at a time.

Related Documentation

Refer to the following sources for more details on these features of the ECXpert OFTP Server:

- The OFTP Server section in the ECXpert initialization file—"[ecxoftp-server] Section" on page 615

- The Oftp table in the ECXpert database schema—"Oftp" in the *iPlanet ECXpert Operations Reference Guide*.

- The Techland Systems International goftp scripting language—locate the following documents in the *$NSBASE*/NS-apps/ECXpert/Documentation/OFTP directory:

The Odette File Transfer Protocol

OFTP was first specified in 1986 by the Organisation for Data Exchange by Tele Transmission in Europe (ODETTE) to address the EDI requirements of the European car industry. OFTP is a session level protocol that has traditionally been conducted over X.25 or X.28 dialup transport layers. A recent extension to OFTP added TCP/IP as the network layer. OFTP was designed to provide data transmission independent of the underlying communications medium as well as the hardware configuration and software environment.

OFTP was required to support the following:

- systems of different ages

- interoperation with systems from different manufacturers

- interoperation with systems of different sizes

- interoperation with existing systems - minimizing impact

- easy scalability ("future-proof"_

OFTP is modeled on the OSI reference model. It uses a transport layer (level 3) such as X.25, X.28 dial up, or TCP/IP. It provides a file level service (layers 4-7).

An OFTP session can be divided into the following operating phases:

-

-

-

-

-

Start Session

The client makes a physical connection to the OFTP server. The server then initiates the OFTP session by replying to the physical connection with a protocol level Start Session Ready Message (SSRM). The client and server then exchange Start Session ID (SSID) messages. These include user name and password information to authenticate the session. Some parameters are also set and negotiated to determine the nature of the session. The following features are negotiable.

- **Compression** capability of the OFTP node.

- **Restart capability**—the OFTP node can handle the restart of a partially transmitted file. The OFTP specifies that restarts occur at the last kilobyte boundary that was transmitted.

- **Send and receive** capability of the OFTP node.

- **Special logic** capability.

- **Credit**. The number of consecutive data blocks sent by the sender during the transfer phase before it must wait for the receiver to allow it to continue by sending a CDT command.

Start File

The client sends in a Start File ID (SFID) message that the server can accept or reject by replying with either a SFPA or a SFNA message. The roles can be reversed by the initiating client sending a Change Direction command (CD), as described in "End Session" on page 749. The Start File command specifies a destination address that can be an explicitly defined location or a group address. The group address supports broadcasting to multiple addresses.

The End to End Response (EERP) command notifies the original sender of a file that it has been successfully delivered to its final destination. This allows the sender to perform housekeeping and audit trail tasks. The EERP can be sent in the same session or in a subsequent session.

Data can be sent using an intermediate location (the clearing center/VAN scenario). When an intermediate location forwards a file it must receive a corresponding EERP notification from all the destinations it sent the file to, before constructing its own EERP and dispatching it to the original sender. This ensures the EERP received by the original sender accounts for all the ultimate destinations. Hence an intermediate location must maintain tracking information for all the files it processes over time.

Data Transfer

The Credit (CDT) command provides a protocol level flow control mechanism. An initial credit limit is negotiated in the start session phase. This is the number of data blocks the client is allowed to send before it is forced to wait for a CDT command. The credit limit can be changed in subsequent CDTs. It is important to send a CDT as soon as possible, as the client blocks till it receives one.

End File

The client notifies the server it is done transferring data by sending an End File (EFID) message. The server can accept or reject the data transfer with an End File Positive Acknowledgment (EFPA) or an End File Negative Acknowledgment (EFNA) respectively. It can also take control of the session by requesting a Change Direction (CD). It can then dispatch EERP messages or initiate a data transfer.

End Session

Whoever has control of the session breaks off by sending the End Session (ESID) command.

OFTP Extensions Support

A standard extension to the OFTP protocol is supported. The OFTP Start Session ID (SSID) message contains a user-definable field. It is commonly used as a means to request a change for the user's password. The old password is placed in the user defined field (which gets validated by the authenticating authority) and the new password is placed in the SSID password field. ECXpert uses this mechanism to both receive and send password change requests.

The ECXpert OFTP Server

The ECXpert OFTP server (ecxoftp-m-server) is analogous to other servers within ECXpert. It typically gets started at ECXpert system start-up time and terminates when the ECXpert system is brought down. It has a section in the `ecx.ini` file. You can configure the server to start and stop the server on the command-line, using the ecxstart and ecxstop utilities.

You manage the OFTP server from the administration screens in the same way as other servers. You can start and stop the server, configure the ecx.ini parameters, and view the log files. You can track submissions and service list executions from the tracking screens in the Support User Interface in standard ECXpert fashion.

You can bring the server up in one of two modes by configuring it to accept either TCP/IP or X.25 incoming connections. This is done in the ECXpert OFTP server's initialization file. The name of this file is specified in the `ecx.ini` file.

X.28 is a term for a dialup connection over a modem to a X.25 network. This is analogous to a PPP connection to the Internet using a service provider. Typically, an X.28 connection is made to a PAD, which then makes an X.25 call to the receiving application (for example, the ECXpert OFTP server) on behalf of the initiator. Hence, the ECXpert OFTP server interprets incoming X.28 calls as incoming X.25 calls.

Regardless of which transport method the ECXpert server is configured to use for incoming connections, it can make outbound connections using any of the three supported transport methods (X.25, X.28, TCP/IP). It dynamically determines the transport method according to the partnership criteria.

Settings in the ECXpert Initialization File (ecx.ini)

Refer to "[ecxoftp-server] Section" on page 615 for details on the ECXpert OFTP Server parameters in the ecx.ini file.

The ECXpert OFTP Server Initialization File

Refer to "Configuration for Two ECXpert OFTP Servers" on page 772 for a sample of this file. Explanations for parameters are given here. The parameters within this file can be modified, but with care. The first section below details the parameters that are independent of the underlying communications method. Subsequent sections describe the communications-specific parameters.

Parameters Independent of Communications Method

- consumer_count refers to the number of concurrent OFTP sessions the ECXpert OFTP server can handle simultaneously. If this limit is exceeded incoming OFTP session attempts will be rejected.

- trace_mode can assume values of 0, 1, or 2. For trace files to be produced the BDGHOME environment variable should be set. This is typically set to *$NSBASE*/NS-apps/ECXpert. The trace file(s) will be deposited in *$NSBASE*/NS-apps/ECXpert/data/log.

Table G-1 trace_mode values

Value	Description
0	No tracing is enabled.
1	OFTP-level tracing is enabled, which is useful for diagnosing protocol related problems.
	A file with a name of the format oftp.trc.<pid> is created in the appropriate location. The process ID contained in the trace file name is the process ID of the ECXpert OFTP server logging to the file. The file contains a trace of the OFTP-level commands transmitted or received over the communications link. Each line of data is preceded by either XMT (for transmitted) or RCV (for received). This is followed by the name of the OFTP command and the data contained within that command block. The actual customer data sent across the link is not recorded here.

Table G-1   trace_mode values

Value	Description
2	Low-level tracing is enabled, which is useful for diagnosing communications related issues.
	A file with a name of the format comms.trc.\<pid\> is created in the appropriate location. It contains a trace of every byte transmitted or received over the communications link. The format of this file resembles the output of the UNIX utility od. The hexadecimal representation of the bytes is given as well as the human readable form. Each line of data is preceded by either TX (for transmitted) or RX (for received).

- `oftp_node_id` Required. This value indicates how to identify this OFTP node. It is inserted in the SSIDCODE field of the SSID command in an OFTP session. It has a maximum length of 25 characters. The remote OFTP node must verify that this SSIDCODE is valid for their system.

- `oftp_node_password` Required. This value refers to the password for this OFTP node. This value is inserted in to the SSIDPSWD field of the SSID command in an OFTP session. It has a maximum length of 8 characters. This node id and node password is only used for incoming sessions to the ECXpert OFTP server, not from outgoing sessions. For outgoing sessions the username and password are taken from the partnership screen. The remote OFTP node must verify that this SSIDPSWD is valid for their system.

- `oftp_node_userdata` Optional. This value refers to any user-specified data for this OFTP node. This value is inserted in to the SSIDUSER field of the SSID command in an OFTP session. It has a maximum length of 8 characters. The remote node can use this data by mutual agreement.

The above three values are passed back to OFTP initiators attempting to connect to the ECXpert OFTP server. The remote node should validate their values. When the ECXpert OFTP server makes an outbound connection to another OFTP node, the SSID values are taken from the partnership protocols tab. The SSID values of the remote OFTP node are authenticated against the ECXpert database. Be sure to set the remote OFTP SSIDCODE and SSIDPSWD as a valid ECXpert member.

- `oftp_outbound_dir_capability` can assume values of 'b' or 's'. This is case-insensitive.

Table G-2   oftp_outbound_dir_capability values

Value	Description
b	Denotes an outbound direction capability of both. This means outbound OFTP sessions from the ECXpert OFTP server can both transmit and receive files and/or EERPs.
s	Denotes an outbound direction capability of send only. This means outbound OFTP sessions from the ECXpert OFTP server can only transmit files and/or EERPs. It cannot receive files. It can receive EERPs.

The inbound direction capability of the ECXpert OFTP server is hardwired to receive only. Files cannot be transmitted from the ECXpert OFTP server to an initiating OFTP node. However, a file transmitted from an initiating OFTP node can be acknowledged immediately within the same session (that is, an EERP can be returned immediately if appropriate).

- `oftp_restarts_supported`. For this release of the ECXpert OFTP server, restarts are not supported. Legitimate values for this parameter are 'y' or 'n'. This is case-insensitive. If a value of 'y' is given it is silently deprecated to 'n'.

- `oftp_special_logic_supported`. Legitimate values for this parameter are 'y', 'n' or 'm'. This is case-insensitive.

Table G-3   oftp_special_logic_supported values

Value	Description
n	Denotes that this ECXpert OFTP server does not support special logic.
y	Denotes that this ECXpert OFTP server would prefer to support special logic.
m	Denotes that this ECXpert OFTP server must have special logic.

Special logic means that extra integrity information is added to each packet transmitted across the communications link to ensure that the received data is the same as the transmitted data, and that packet order can be determined correctly. Both X.25 and TCP/IP guarantee that packets arrive at their destination in the order sent. Both transport methods also guarantee the integrity of the packet contents. For these transport methods, set oftp_special_logic_supported to 'y' or 'n'.

X.28 is unreliable, and asynchronous, so oftp_special_logic_supported should be set to 'm'.

- `oftp_compression_supported`. Legitimate values for this parameter are 'y' or 'n'. This is case-insensitive.

- `oftp_timeout`. Required. An integer (minutes) that specifies the maximum amount of session level inactivity that should occur before aborting the session.

- `inbound_transport_method`. Legitimate values for this parameter are the strings 'tcp/ip', or 'x.25'. This is case-insensitive. This is how the ECXpert OFTP server determines whether to accept incoming OFTP sessions using TCP/IP or X.25.

- `external_API`. For this release the only legitimate value for this parameter is the string 'techland'. It is case-insensitive. For future releases, alternative libraries might be used, and this parameter provides a simple selection mechanism.

Parameters for Incoming TCP/IP Sessions

- `tcp_listen_port`. Optional. If the ECXpert OFTP server is configured to accept incoming TCP/IP connections, the value of this parameter specifies the well known port it is listening on. The format can be either the service name or the port number. The value is taken as is. If no value is supplied, the port defaults to 3305, the standard reserved ODETTE port. The host name defaults to the local host name.

Parameters for Incoming X.25 Sessions

- `x25_device_driver`. Required. The value of this parameter specifies the hardware device for accessing X.25 services. For Solaris, an example would be '/dev/x25:3'. For NT, an example would be 'COM1'. This value also indicates the device from which this ECXpert OFTP server makes outbound X.25 connections.

- `x25_listen_nua`. Optional. The X.121 (network user address) address of the local X.25 port (optional). If a value is not supplied, the local X.121 address is automatically determined. This value also specifies the address from which this ECXpert OFTP server makes outbound X.25 connections.

- `x25_lcn_for_pvc`. Optional. X.25 handles incoming connections in two ways. Connections are assigned to logical channels. A logical channel can either be pre-assigned (Permanent Virtual Circuit - PVC -), or assigned dynamically (Switched Virtual Circuit - SVC -) when the connection comes in. If no value is supplied for this parameter then SVC's are assumed and the next available logical channel is assigned when an incoming connection is received. To force this behavior, supply a value of '-1' (default behavior if left blank). If PVC's are being used (a dedicated channel to a particular trading partner that is kept permanently up), provide the integer value.

- `x25_facility_info`. Optional. This represents the X.25 facilities that should be present when answering a call. Typically, this is a string of hexadecimal digits that represents the binary facility codes requested for the particular network in use.

- `x25_call_user_data`. Optional. This represents X.25 call user data that should be present when answering a call. Typically, this is a string of hexadecimal digits. An example of it's use would be to differentiate between separate X.25 listener applications. A listener application would advertise a particular call user data value, and clients would need to include that call user data when making a connection in order for the connection to succeed.

- `x25_route_name`. Optional. Some X.25 system implementations (for example, AIX) include a screening feature. A routing entry specifies the screening criteria that must be met before incoming connection attempts are presented to the listening application. The routing entry is the value supplied here. (Neither Solaris nor NT currently implements this feature.)

The remaining parameters in the ECXpert OFTP server's initialization file are concerned with X.28 outbound connectivity and are discussed in "Configuring X.28 OFTP Sessions through the Initialization File" on page 757.

Setting Up OFTP Partnerships

This section discusses the steps necessary to exchange documents with trading partners using OFTP using the ECXpert OFTP server, and details some of the peculiarities of OFTP.

➤ **To set up OFTP partnerships**

1. Create ECXpert members.

   OFTP restricts the length of Member ID's to 25 characters.

2. Set up a service list.

   The Service List Data Type should match the Document Type in the Partnership screen. The ECXpert OFTP server uses the User Data field (SFIDUSER) in the OFTP SFID (Start File) command to hold this information. This field is restricted to a maximum length of 8 characters. Partner ECXpert OFTP servers will interpret the contents of this field as the Document Type. Non-ECXpert OFTP servers could interpret this field differently.

3. To configure an outgoing OFTP transmission, select Odette FTP (OFTP) as the Outgoing Protocol in the Protocols tab of the Partnership screen.

   ECXpert returns an EERP to the originator if the Outgoing Protocol for the partnership has been set to anything other than OFTP. This allows the recipient to retrieve their data using any method they choose.

   a. Select the appropriate Delivery Timing value: Immediate or Scheduled.

   b. Enter a username and password in the appropriate fields.

      These correspond to the SSIDCODE and SSIDPSWD in the SSID (Start Session) OFTP command to be transmitted at the beginning of the OFTP session. The remote OFTP node will authenticate these values against its database.

Below these fields in the Protocols tab are Transport Method-specific parameters.

For more details on completing the Partnerships Protocol tab, refer to .

Outgoing TCP/IP OFTP Sessions

To configure an outgoing TCP/IP OFTP session you select TCP/IP from the Transport Method drop-down menu.

Destination Address is the IP address or name of the machine hosting the remote OFTP server node.

Destination Port is the port number or service name of the port on which the remote OFTP server is accepting OFTP connections.

Taken together the two values uniquely identify the address of the remote OFTP node.

For more details on completing the OFTP TCP/IP settings, refer to Table 6-32 on page 331.

Outgoing X.25 OFTP Sessions

To configure an outgoing X.25 OFTP session you select X.25 from the Transport Method drop-down menu. All X.25 fields refer to the properties of the remote OFTP node.

Destination X.121 Address refers to the X.25 Network User Address of the machine hosting the remote OFTP server node. A value must be specified for this field.

Facility Information is optional.

Logical Channel Number is optional. SVC is the default.

Routing Entry is optional.

Call User Data is optional.

Taken together these values uniquely identify the address of the remote OFTP node.

For more details on completing the OFTP TCP/IP settings, refer to Table 6-30 on page 330.

Outgoing X.28 OFTP Sessions

The ECXpert OFTP server can make dialup connections by modem to an X.25 PAD. A scripting interface exists to accomplish this. A simple scripting language provided by Techland (*goftp*) manages the modem configuration and the dialing.

Different PAD's have different login procedures. Techland's procedural scripting language provides a flexible way to automate this process, similar to the Unix utiliy expect. It lets the user specify certain strings to wait for, such as password prompts, and to send strings, such as the password, to the PAD at the appropriate time. Outgoing X.28 OFTP sessions from the ECXpert OFTP server are conducted by

calling the specified connection script. The ECXpert OFTP server has an built-in engine that loads, parses and executes the script. After a connection is made, the OFTP session is conducted as normal. When the OFTP session has completed, the termination section of the script is executed to disconnect and hang up the modem.

There are two places where you can configure outbound X.28 OFTP sessions for the ECXpert OFTP server: in the initialization file, and in the Protocols tab of the Partnership screen. These options are discussed below.

Configuring X.28 OFTP Sessions through the Initialization File

In general, the parameters in the initialization file are concerned with lower level configuration than in the Partnership screen. These parameters relate to modem settings, and the structure of the connection script.

- x28_configured. Legitimate values for this parameter are 'y' or 'n'. This is case-insensitive. It is simply a flag indicating whether to parse and validate the subsequent x28_* parameters. If this flag is not set to 'y', then no outbound X.28 OFTP sessions should be attempted.

All of the following parameters are optional. If they are specified, their values are passed through to the connection script. Their values are referenced in the connection script using the same variable name. It is left to the user's discretion how to write the scripts. It is possible to simply hard-code all the parameter values directly in the script itself. Maximum flexibility is provided by allowing the user to determine how best to make use of this feature.

- x28_device_driver. The value of this parameter is the hardware device being used to access the modem. For Solaris, an example would be '/dev/cua/b'. For NT, an example would be 'COM1'.

- x28_modem_parity. Legitimate values for this parameter are as follows. This is case-insensitive.

Table G-4   modem_parity values

Value	Description
n	Specifies that the modem has been configured with no parity.
o	Specifies that the modem has been configured with odd parity.
p	Specifies that the modem has been configured with even parity.

- `x28_modem_physical_word_len`. This modem configuration parameter specifies the physical size of the data words exchanged between the port and the modem. Legitimate values for this parameter are '5', '6', '7', or '8'.

- `x28_modem_stop_bits`. This modem configuration parameter specifies the number of stop bits to terminate each byte of data transferred between the port and the modem. Legitimate values for this parameter are '1', or '2'.

- `x28_modem_baud_rate`. This modem configuration parameter specifies the speed, in bits per second, at which data is exchanged between the port and the modem.

- `x28_modem_init_string`. This modem configuration parameter is the modem initialization string to be sent to the modem when opening the port. It is a standard Hayes compatible command string. Do not include the leading 'AT' string.

- `x28_modem_connect_timeout`. This modem configuration parameter specifies the number of seconds time-critical operations, such as connecting and reading, will wait before timing out.

The remaining parameters are required and are concerned with the script structure. For the ECXpert OFTP server to correctly execute the script, the script must provide implementations for 3 procedures. The names of these 3 procedures are specified in the initialization file.

- `x28_label_start`. The name of the start procedure in the connection script. This procedure typically contains port opening, configuration, and dialling operations.

- `x28_label_online`. The name of the online procedure in the connection script. This procedure typically contains the login operations, such as sending a username, and password to the PAD.

- `x28_label_hangup`. The name of the hang-up procedure in the connection. This procedure typically contains disconnection and hang-up operations.

For a complete description of the parameters in the ECXpert OFTP Server initialization file, refer to "The ECXpert OFTP Server Initialization File" on page 750.

Configuring X.28 OFTP Sessions through the Partnership/Protocols Tab

To configure an outgoing X.28 OFTP session you select X.28 from the Transport Method drop-down menu. The parameter values specified in the Protocols tab of the Partnership screen can be passed through to the connection script in the same way as the parameter values in the initialization file. The variable names used are detailed below.

- **Connection Script**. Required. The full pathname of the connection script used to connect to this trading partner.

All the remaining parameters are optional. If they are specified, their values are passed through to the connection script. For maximum flexibility, is left to the user's discretion how to write the scripts, and to determine what information is required to connect to a specific PAD. It is possible to simply hard-code all the parameter values directly in the script itself.

- **Telephone Number**. The telephone number for the modem to dial. The variable x28_partner_telno can be used in the script to access it's value.

- **PAD Username**. The user ID with which to log in to the PAD. The variable x28_partner_paduser can be used in the script to access it's value.

- **PAD Password**. The password with which to log in to the PAD. The variable x28_partner_passwd can be used in the script to access it's value.

- **Destination NUA**. The X.121 address (Network User Address) for the PAD to call to access the remote OFTP node. The variable x28_partner_nua can be used in the script to access it's value.

In order to debug and test connection scripts independently of the ECXpert OFTP server, the scripting language has been extended to include a print function, `ECHO()`. Literal strings can be passed as parameters to this function by enclosing them in double quotes. The values of variables of numeric type can be printed out by preceding the variable name with a '$'. Values of variables of string type can be printed by simply passing the variable name. Two command-line utilities can be used to drive a connection script independently of the ECXpert OFTP server. A command-line utility (ecxoftp-x28-scr-ck) is provided to syntax-check a connection script.

However, it is of limited use, as most of the parsing and syntax-checking is done at execution time. Once the connection script has been tested and verified independently of the ECXpert OFTP server, it can be 'plugged in' to the ECXpert OFTP server by establishing a trading partnership that includes the connection script name.

NOTE	Remember to remove the debug ECHO() statements from the connection script as they are no longer required. The script will fail if they are included and the ECXpert OFTP server is driving the script.

For more details on completing the OFTP TCP/IP settings on the Partnership Protocols tab, refer to Table 6-31 on page 331.

End-to-end Response (EERP) Support

End-to-end Responses (EERPs) are a concept central to OFTP. An EERP notifies the original sender of a file that it has been successfully delivered to its final destination, no matter how many intermediate hops it made, or how it might have been split into multiple files or combined with other files. An EERP is an acknowledgment from the ultimate recipient that the data has been received.

The ECXpert OFTP server keeps track of how many EERPs are expected for a particular file. When a file is submitted to the ECXpert OFTP server it creates an entry in the database. If the trading partnership has not been configured with an 'Outgoing Protocol' of 'OFTP' then an EERP is generated and returned immediately. The ECXpert OFTP server assumes the file has reached its ultimate destination. If the partnership has been configured to conduct an outgoing OFTP session, then the number of files that are formed from the original submission (as a result of executing the Service List) is recorded in the database. This is the number of EERPs that must be received for this item of data before a corresponding EERP can be generated and dispatched to the original sender.

In order to keep track of files (units of data that require acknowledgment - the OFTP RFC calls this a 'virtual file'), the OFTP tags files with unique identifying information. This tag is sent along with the file. It is forbidden for intermediate OFTP nodes to alter this tag in any way. This tag is composed of the tuple:

- **Virtual File Date Stamp**. Read-only. This is the SFIDDATE field in the SFID Start File OFTP command. It is exactly 6 characters long, and has the format YYMMDD.

- **Virtual File Time Stamp**. Read-only. This is the SFIDTIME field in the SFID Start File OFTP command. It is exactly 6 characters long, and has the format HHMMSS.

- **Virtual File Dataset Name**. Read-only. This is the SFIDSN field in the SFID Start File OFTP command. It has a maximum length of 26 characters.

Files destined to be transmitted from ECXpert over OFTP should be submitted using OFTP. This is important because the above tracking information is stored when the file is submitted to ECXpert and used when the file is sent from ECXpert over OFTP. Errors will result on the outbound transmission if this information is not available. This precludes using other means of getting data into the system than OFTP, if OFTP is to be used as the outbound protocol.

EERPs can be returned in the same session as the file transmission or at a later time.

In general a separate relationship should be established for EERP transmission. If A sends a file to B, the EERP should flow in the reverse direction, from B to A. Hence, a partnership should be established with a sender of B, and a receiver of A. The Document Type must have the value EERP. It is not necessary to configure a Service List with this data type.

The ECXpert OFTP server will return an EERP in the same session as the file transmission being acknowledged if the file has reached its ultimate destination (that is, the outgoing protocol is non-OFTP). In this case the server knows which trading partner should be sent the EERP. A separate EERP relationship is not required.

A pre-requisite for EERP support is to ensure the ECXpert Date/Time Based Scheduler is running. This is necessary even for Immediate EERP transmissions.

EERP transmissions can be immediate, or scheduled. The following sections describe each scenario in turn.

Immediate EERP Transmissions

If all the expected EERPs for a particular virtual file have been received, the ECXpert OFTP server generates an EERP for dispatch to the originator.

For immediate transmission, the Delivery Timing parameter in the Partnership screen corresponding to the appropriate EERP document type should be set to Immediate. Exactly one EERP is sent to the address specified in the Protocols tab of this EERP Partnership screen.

Scheduled EERP Transmissions

EERP transmissions can be scheduled. This allows EERPs to be batched, and for the entire batch to be dispatched at one time. Refer to "Scheduling ECXpert Jobs" on page 155, and especially to "Adding a New Task" on page 157 and "Parameters Page—Only for ECX EERP for Oftp" on page 174.

For scheduled transmissions, the Delivery Timing parameter in the Partnership screen corresponding to the appropriate EERP document type should be set to Scheduled. When all the expected EERPs for a particular virtual file have been received, the ECXpert OFTP server marks the corresponding scheduled EERP entry in the database as ready for transmission. At the scheduled time the ECXpert Date/Time Based Scheduler connects to the ECXpert OFTP server with the configured sender and partner information. The ECXpert OFTP server extracts from the database all the EERPs that have been marked as ready for transmission for the specified sender-receiver combination. It sends the EERPs to the address specified in the Protocols tab of the corresponding EERP Partnership screen.

A schedule is required. For details, refer to "Adding a New Task" on page 157. In the Administration/Scheduler/New Task screen, choose ECX EERP for Oftp as the type application to execute the scheduled task.

The second screen, "Parameters Page—Only for ECX EERP for Oftp" on page 174, lets you select the sender and receiver of the EERP transaction.

The third screen, "Last Page—When to Run the Task" on page 175, specifies the timing of the schedule. The example screen shot establishes a schedule of immediate transmission.

ECXpert OFTP Clients

A suite of command-line driven client programs is supplied with the ECXpert OFTP server so that files for an EERP can be sent to any OFTP node, not just an ECXpert OFTP server, over the chosen communications medium. They also allow the user to change their password on that OFTP node. This feature relies on the target OFTP node having implemented this common extension to the OFTP. The ECXpert OFTP server implements the extension.

The client programs are divided according to transport method (TCP/IP, X.25, or X.28), and function (File or EERP transmission). The structure of this section reflects these divisions. There is much commonality between the programs, as discussed in the first section below.

Common Parameters

This subsection discusses the options common to all the client programs. Explanations are provided for each of the options. Table G-5 lists the parameters common to all the OFTP clients.

Table G-5   Common parameters for ECXpert OFTP clients

Parameter	Description
-u	`<Local User ID>` mandatory. The OFTP user ID used to log in to the remote OFTP node. Max length of 25 chars.
-l	`<User Login Password>` mandatory. The OFTP user's password used to log in to the remote OFTP node.
-f	`<Name of File>` mandatory. The OFTP user's password used to log in to the remote OFTP node. Max length of 26 chars. This is one of three option values that uniquely identify the file. If the file does not originate here, these values should be taken from the originating information. Do not alter the original values as they are used to maintain tracking information.
-T	`<Timestamp of file - HHMMSS>` mandatory. Must be in the proscribed format. This is one of three option values that uniquely identify the file. If the file does not originate here, these values should be taken from the originating information. Do not alter the original values as they are used to maintain tracking information.
-D	`<Datestamp of file - YYMMDD>` mandatory. Must be in the proscribed format. This is one of three option values that uniquely identify the file. If the file does not originate here, these values should be taken from the originating information. Do not alter the original values as they are used to maintain tracking information.
-U	`<User data field - doc type>` mandatory. If the submission is to the ECXpert OFTP server, this field represents the 'Service List Data Type'/'Document Type'. The OFTP leaves the interpretation of this field to the OFTP implementation. Maximum length of 8 chars.
-R	`<Receiver ID>` mandatory. The OFTP user ID of the receiver of the file/EERP transmission. Maximum length of 25 chars.

Table G-5   Common parameters for ECXpert OFTP clients *(Continued)*

Parameter	Description
-O	`<Originator's ID> mandatory.` The OFTP user ID of the sender of the file/EERP transmission. Maximum length of 25 chars. This might differ from the <Local User ID> given. ECXpert allows submissions to be made on behalf of other users if the member has been so configured. This is implementation dependent for other OFTP nodes.
-d	`<New Password if change required> optional.` The ECXpert OFTP server supports this common OFTP extension. A member's password can be changed at the beginning of an OFTP session. It is not possible for a user to simply logon to an OFTP node and change their password without submitting anything. This is a protocol violation. The ECXpert OFTP code has implemented this feature as follows. The current password is placed in the SSIDUSER field in the OFTP SSID command. The new password is placed in the SSIDPSWD field in the OFTP SSID command.
-t	`<Timeout (min)> defaults to 1 min.` Length of time of session inactivity before the session is aborted.
-v	`<Verbosity flag> defaults to OFF.` Typical exception behavior on running one of these client programs is to report errors to standard error, and exit on failure. On successful termination, the file identifying information (filename, datestamp, timestamp) is printed to standard output. Whether the file was acknowledged immediately is also reported. If this flag is specified the progress of the session is also reported to standard output. A debug log file is also created in the default ECXpert logfile directory, $NSBASE/NS-apps/ECXpert/data/log.
-Z	`<Trace flag> defaults to OFF.` Specifying this flag creates an OFTP-level trace file in the default ECXpert logfile directory, $NSBASE/NS-apps/ECXpert/data/log. A file with a name of the format oftp.trc.<pid> is created in the appropriate location. The process ID contained in the trace file name is the process ID of the client program logging to the file. The file contains a trace of the OFTP-level commands transmitted or received over the communications link. Each line of data is preceded either by XMT (for transmitted) or RCV (for received). This is followed by the name of the OFTP command, followed by the data contained within that command block. The actual customer data sent across the link is not recorded here. This level of tracing is useful for diagnosing protocol related problems.

TCP/IP File Submission Parameters—Using ecxoftp-tcp-file-submit

Table G-6 lists the parameters for the `ecxoftp-tcp-file-submit` client.

Table G-6   TCP/IP file submission parameters

Parameter	Description
-P	`<Destination port/service name> defaults to ODETTE OFTP port.` The default ODETTE-specified port is 3305.
-A	`<Destination address/hostname> mandatory` The IP address or hostname of the machine hosting the remote OFTP server node.
-Y	`<File size> mandatory`

-S	`<File record structure - 'F', 'V', 'T', 'U'>`
	`defaults to 'U'.`
	A file can be composed of records that have any one of four structures: 'F' (fixed), 'V' (variable), 'T' (text) and 'U' (unstructured). These four file types match the four types defined in the OFTP documentation and are implemented as such. Unix files are not stored in record format.

-x	`<Max file record size> optional.` The maximum record size parameter serves as an upper limit on the record before it is transmitted.

TCP/IP EERP Submission Parameters—Using ecxoftp-tcp-eerp-submit

Table G-7 lists the parameters for the `ecxoftp-tcp-eerp-submit` client.

Table G-7   TCP/IP EERP submission parameters

Parameter	Description
-P	`<Destination port/service name> defaults to ODETTE OFTP port.` The default ODETTE-specified port is 3305.
-A	`<Destination address/hostname> mandatory` The IP address or hostname of the machine hosting the remote OFTP server node.

X.25 File Submission—Using ecxoftp-x25-file-submit

Table G-8 lists the parameters for the `ecxoftp-x25-file-submit` client.

Table G-8   X.25 file submission parameters

Parameter	Description
`-Y`	`<File size> mandatory`

`-S`	`<File record structure - 'F', 'V', 'T', 'U'>`
	`defaults to 'U'.`
	A file can be composed of records that have any one of four structures: 'F' (fixed), 'V' (variable), 'T' (text) and 'U' (unstructured). These four file types match the four types defined in the OFTP documentation and are implemented as such. Unix files are not stored in record format.

`-x`	`<Max file record size> optional.` The maximum record size parameter serves as an upper limit on the record before it is transmitted.
`-n`	`-n <Local X.25 NUA> optional` The X.121 (network user address) of the local X.25 port. If a value is not supplied, the local X.121 address is automatically determined. This value also specifies the address from which this ECXpert OFTP server makes outbound X.25 connections.
`-p`	`-p <Local X.25 device driver name> mandatory` The hardware device being used to access X.25 services. This value also specifies the device from which this ECXpert OFTP server makes outbound X.25 connections.
`-N`	`-N <Remote X.25 NUA to connect to> mandatory` The X.25 network user address of the machine hosting the remote OFTP server node.
`-L`	`-L <Logical Channel Number for PVC to connect to>` `defaults to -1 (SVC assumed)`
`-F`	`-F <Facility Info> defaults to NULL`
`-C`	`-C <Call User Data> defaults to NULL`

X.25 EERP Submission—Using ecxoftp-x25-eerp-submit

Table G-9 lists the parameters for the `ecxoftp-x25-eerp-submit` client.

Table G-9   X.25 EERP submission parameters

Parameter	Description
-n	`-n <Local X.25 NUA> optional` The X.121 (network user address) of the local X.25 port. If a value is not supplied, the local X.121 address is automatically determined. This value also specifies the address from which this ECXpert OFTP server makes outbound X.25 connections.
-p	`-p <Local X.25 device driver name> mandatory` The hardware device being used to access X.25 services. This value also specifies the device from which this ECXpert OFTP server makes outbound X.25 connections.
-N	`-N <Remote X.25 NUA to connect to> mandatory` The X.25 network user address of the machine hosting the remote OFTP server node.
-L	`-L <Logical Channel Number for PVC to connect to>` `defaults to -1 (SVC assumed)`
-F	`-F <Facility Info> defaults to NULL`
-C	`-C <Call User Data> defaults to NULL`

X.28 File Submission—Using ecxoftp-x28-eerp-submit

Table G-10 lists the parameters for the `ecxoftp-x28-eerp-submit` client.

Table G-10   X.28 file submission parameters

Parameter	Description

-P	`<Destination port/service name> defaults to ODETTE`
	`OFTP port.`
	The default ODETTE-specified port is 3305.

-A	`<Destination address/hostname> mandatory` The IP address or hostname of the machine hosting the remote OFTP server node.
-Y	`<File size> mandatory`

Table G-10 X.28 file submission parameters *(Continued)*

Parameter	Description
-S	`<File record structure - 'F', 'V', 'T', 'U'>` `defaults to 'U'.` A file can be composed of records that have any one of four structures: 'F' (fixed), 'V' (variable), 'T' (text) and 'U' (unstructured). These four file types match the four types defined in the OFTP documentation and are implemented as such. Unix files are not stored in record format.
-x	`<Max file record size> optional.` The maximum record size parameter serves as an upper limit on the record before it is transmitted.
-n	`-n <Local X.25 NUA> optional` The X.121 (network user address) of the local X.25 port. If a value is not supplied, the local X.121 address is automatically determined. This value also specifies the address from which this ECXpert OFTP server makes outbound X.25 connections.
-p	`-p <Local X.25 device driver name> mandatory` The hardware device being used to access X.25 services. This value also specifies the device from which this ECXpert OFTP server makes outbound X.25 connections.
-N	`-N <Remote X.25 NUA to connect to> mandatory` The X.25 network user address of the machine hosting the remote OFTP server node.
-L	`-L <Logical Channel Number for PVC to connect to>` `defaults to -1 (SVC assumed)`
-F	`-F <Facility Info> defaults to NULL`
-C	`-C <Call User Data> defaults to NULL`
-X	`<X.28 PAD login user ID> optional` The user ID for logging in to the PAD. The variable X28_partner_paduser can be used in the script to access its value.
-c	`<X.28 Connection script connect section name>` `mandatory` The full pathname of the connection script used to connect to this trading partner.
-o	`<X.28 Connection script online section name>` `mandatory` The name of the online procedure in the connection script.
-h	`<X.28 Connection script hangup section name>` `mandatory` The name of the hangup procedure in the connection script.

Table G-10 X.28 file submission parameters *(Continued)*

Parameter	Description
-W	`<Modem physical Word Length ('5', '6', '7', '8' bits)>` `optional` The physical size of the data words exchanged between the port and modem.
-s	`<Modem stop bits ('1', '2' bits)>` `optional` The number of stop bits to use to terminate each byte of data transferred between the port and modem.
-B	`<Modem baud rate>` `optional` The speed, in bits per second, at which data is exchanged between the port and modem.
-I	`<Modem initialization string if any>` `optional` The modem initialization string to be sent to the modem when opening the port. It is a standard Hayes compatible command string. Do not include the leading 'AT' string.
-i	`<Special logic integrity>` `OFF if not specified` Set this value to guarantee delivery of packets in the correct order and packet integrity.

X.28 EERP Submission—Using ecxoftp-x28-eerp-submit

Table G-11 lists the parameters for the `ecxoftp-x28-eerp-submit` client.

Table G-11 X.28 EERP submission parameters

Parameter	Description
-P	`<Destination port/service name>` `defaults to ODETTE` `OFTP port.` The default ODETTE-specified port is 3305.
-A	`<Destination address/hostname>` `mandatory` The IP address or hostname of the machine hosting the remote OFTP server node.
-Y	`<File size>` `mandatory`
-S	`<File record structure - 'F', 'V', 'T', 'U'>` `defaults to 'U'.` A file can be composed of records that have any one of four structures: 'F' (fixed), 'V' (variable), 'T' (text) and 'U' (unstructured). These four file types match the four types defined in the OFTP documentation and are implemented as such. Unix files are not stored in record format.

Table G-11 X.28 EERP submission parameters *(Continued)*

Parameter	Description
-x	`<Max file record size> optional.` The maximum record size parameter serves as an upper limit on the record before it is transmitted.
-n	`-n <Local X.25 NUA> optional` The X.121 (network user address) of the local X.25 port. If a value is not supplied, the local X.121 address is automatically determined. This value also specifies the address from which this ECXpert OFTP server makes outbound X.25 connections.
-p	`-p <Local X.25 device driver name> mandatory` The hardware device being used to access X.25 services. This value also specifies the device from which this ECXpert OFTP server makes outbound X.25 connections.
-N	`-N <Remote X.25 NUA to connect to> mandatory` The X.25 network user address of the machine hosting the remote OFTP server node.
-L	`-L <Logical Channel Number for PVC to connect to> defaults to -1 (SVC assumed)`
-F	`-F <Facility Info> defaults to NULL`
-C	`-C <Call User Data> defaults to NULL`
-X	`<X.28 PAD login user ID> optional` The user ID for logging into the PAD. The variable X28_partner_paduser can be used in the script to access its value.
-c	`<X.28 Connection script connect section name> mandatory` The full pathname of the connection script used to connect to this trading partner.
-o	`<X.28 Connection script online section name> mandatory` The name of the online procedure in the connection script.
-h	`<X.28 Connection script hangup section name> mandatory` The name of the hangup procedure in the connection script.
-W	`<Modem physical Word Length ('5', '6', '7', '8' bits)> optional` The physical size of the data words exchanged between the port and modem.

Table G-11 X.28 EERP submission parameters *(Continued)*

Parameter	Description
-s	`<Modem stop bits ('1', '2' bits)> optional` The number of stop bits to use to terminate each byte of data transferred between the port and modem.
-B	`<Modem baud rate> optional` Specifies the speed, in bits per second, at which data is exchanged between the port and the modem.
-I	`<Modem initialization string if any> optional` The modem initialization string to be sent to the modem when opening the port. It is a standard Hayes compatible command string. Do not include the leading 'AT' string.
-i	`<Special logic integrity> OFF if not specified` Set this in order to guarantee delivery of packets in the correct order and packet integrity.

Running Two or More ECXpert OFTP Servers

One reason for running more than one ECXpert OFTP server might be, to be able to accept OFTP sessions over both X.25 and TCP. Other reasons could include distributing heavy incoming OFTP traffic across several listening servers.

In order to achieve this, the ecx.ini file should be amended to include a new section for each additional ECXpert OFTP server. Appendix G shows an example ecx.ini file that has been amended to include one additional section. This ECXpert has been configured to have one ECXpert OFTP server accepting incoming OFTP sessions over TCP/IP, and one ECXpert OFTP server accepting OFTP sessions over X.25. Note the following:

- An additional section to [ecxoftp-server] should be added. Do not change the section name [ecxoftp-server]. Regardless of how many servers are configured, or what transport methods they are listening on, outbound OFTP sessions will always be executed by the server corresponding to the [ecxoftp-server] section.

- Each additional section should have a unique server_type value.

- It is important to ensure the oftp_server_ini values are different per ECXpert OFTP server section.

- If debug_flag = yes you should also set stderr_path and stderr_path values to be different per ECXpert OFTP server section.

- *ecxoftp-server.ini* corresponds to the TCP/IP listener. It also handles all outbound OFTP sessions. It must contain valid values for the x25_ * parameters in order for outbound X.25 OFTP sessions to succeed.

- *ecxoftp-server-x25.ini* corresponds to the X.25 listener. It will not receive any requests for outbound OFTP sessions.

For a future ECXpert release the requirement for separate oftp_server_ini files might be removed. Instead, a mechanism will be implemented to have separate sections (representing different listening servers) in the one oftp_server_ini file.

Configuration for Two ECXpert OFTP Servers

This section presents sample ECXpert and ECXpert OFTP Server initialization files with settings configured to support two ECXpert OFTP Servers.

Code Example G-1   ECXpert Initialization File (ecx.ini)

```
...
[ecxoftp-server]
#
# These parameters should not be changed.
#
server_type = 14
snmp_trap_flag = yes
snmp_trap_level = 10
section_type = server
protocol_id = 775
port_location = mmap
listener_level = 1
listener_type   = thread
max_listeners = 4
runnable_flag = yes
thread_mode = threaded
listener_time_out = 10
admin_time_out = 10
start_mode = background
type = daemon
bundle_all = yes

is_comm_agent = yes
internal_name = OFTP1
visible_name = Odette FTP (OFTP)
operation = send
data_type = both

#
# Machine dependent information.
#
```

Code Example G-1   ECXpert Initialization File (ecx.ini) *(Continued)*

```
host_name = 206.222.246.67
#
# File and directory information
#
exec_path = /export/disk1/actraadm/NS-apps/ECXpert/bin/ecxoftp-m-server
oftp_server_ini =
/export/disk1/actraadm/NS-apps/ECXpert/config/ecxoftp-server.ini
#
# Multi-Threading parameters.  Do not change.
#
max_thread_flag = yes
worker_max_threads = 4
master_max_threads = 4
master_max_threads_queued_flag = yes
master_max_threads_queued = 500
master_max_threads_stacked = 500
#
# Port information.
#
listener_port = 4200
admin_port_type = dynamic
listener_port_type = dynamic
admin_port = 4201
#
# Configurable option.
#
autostart_flag = no
restart_flag = no
#
# Debug output configuration.
#
stderr_path =
/export/disk1/actraadm/NS-apps/ECXpert/data/log/ecxoftp-server.log
stdout_path =
/export/disk1/actraadm/NS-apps/ECXpert/data/log/ecxoftp-server.log
debug_flag  = yes
...
[ecxoftp-server-x25]
#
# These parameters should not be changed.
#
server_type = 19
snmp_trap_flag = yes
snmp_trap_level = 10
section_type = server
protocol_id = 775
port_location = mmap
listener_level = 1
listener_type   = thread
max_listeners = 4
runnable_flag = yes
thread_mode = threaded
listener_time_out = 10
```

Code Example G-1   ECXpert Initialization File (ecx.ini) *(Continued)*

```
admin_time_out = 10
start_mode = background
type = daemon
bundle_all = yes

is_comm_agent = yes
internal_name = OFTP1
visible_name = Odette FTP (OFTP)
operation = send
data_type = both

#
# Machine dependent information.
#
host_name = 206.222.246.67
#
# File and directory information
#
exec_path = /export/disk1/actraadm/NS-apps/ECXpert/bin/ecxoftp-m-server
oftp_server_ini =
/export/disk1/actraadm/NS-apps/ECXpert/config/ecxoftp-server-x25.ini
#
# Multi-Threading parameters.  Do not change.
#
max_thread_flag = yes
worker_max_threads = 4
master_max_threads = 4
master_max_threads_queued_flag = yes
master_max_threads_queued = 500
master_max_threads_stacked = 500
#
# Port information.
#
listener_port = 4200
admin_port_type = dynamic
listener_port_type = dynamic
admin_port = 4201

#
# Configurable option.
#
autostart_flag = no
restart_flag = no
#
# Debug output configuration.
#
stderr_path =
/export/disk1/actraadm/NS-apps/ECXpert/data/log/ecxoftp-server-x25.log
stdout_path =
/export/disk1/actraadm/NS-apps/ECXpert/data/log/ecxoftp-server-x25.log
debug_flag  = yes
...
```

Code Example G-2   First ECXpert OFTP Server Initialization File (*ecxoftp-server-x.ini*)

```
[server]
consumer_count  = 10

# (0 - none, 1 - low. 2 - high)
trace_mode      = 0

oftp_node_id =
oftp_node_password =
oftp_node_userdata =

# ('B' - Both, 'S' - Send)
oftp_outbound_dir_capability = B

oftp_restarts_supported = N
oftp_special_logic_supported = Y
oftp_compression_supported = N

# Specified in minutes
oftp_timeout = 1

# 'TCP/IP' or 'X.25'
inbound_transport_method = TCP/IP

external_API = techland

tcp_listen_port = moose1

x25_device_driver = /dev/x25:3
x25_listen_nua =
x25_lcn_for_pvc =
x25_facility_info =
x25_call_user_data =
x25_route_name =


x28_configured = N

x28_device_driver =
x28_modem_parity =
x28_modem_physical_word_len =
x28_modem_stop_bits =
x28_modem_baud_rate =
x28_modem_init_string =
x28_modem_connect_timeout =

# These are all mandatory if x28_configured = Y
x28_label_start =
x28_label_online =
x28_label_hangup =
```

Code Example G-3   Second ECXpert OFTP Server Initialization File (*ecxoftp-server-x25.ini*)

```
[server]
consumer_count  = 10

# (0 - none, 1 - low. 2 - high)
trace_mode      = 0

oftp_node_id =
oftp_node_password =
oftp_node_userdata =

# ('B' - Both, 'S' - Send)
oftp_outbound_dir_capability = B

oftp_restarts_supported = N
oftp_special_logic_supported = Y
oftp_compression_supported = N

# Specified in minutes
oftp_timeout = 1

# 'TCP/IP' or 'X.25'
inbound_transport_method = X.25

external_API = techland

tcp_listen_port =

x25_device_driver = /dev/x25:3
x25_listen_nua =
x25_lcn_for_pvc =
x25_facility_info =
x25_call_user_data =
x25_route_name =


x28_configured = N

x28_device_driver =
x28_modem_parity =
x28_modem_physical_word_len =
x28_modem_stop_bits =
x28_modem_baud_rate =
x28_modem_init_string =
x28_modem_connect_timeout =

# These are all mandatory if x28_configured = Y
x28_label_start =
x28_label_online =
x28_label_hangup =
```

Sample OFTP Server Initialization File (ecxoftp-server.ini)

Below is a sample OFTP Server initialization file for reference in the above discussion of parameters.

- **File Location**—*$NSBASE*/NS-apps/*ECXpert/config/ecxoftp-server.ini* is the default location after ECXpert installation.

- *ecx.ini* **File Parameter**—[ecxoftp-server] section, oftp_server_ini parameter controls the name and location of this file.

Code Example G-4   Sample OFTP Server Initialization File

```
################################################################
######
# File: ecxoftp-server.ini
# Description: ECXpert OFTP server configuration file.
#
# Notes:
#    This file can be modified, but with utmost care.
#    Erroneous configuration might cause ECXpert OFTP server to
perform
#    and behave unexpectedly.
#
################################################################
######

[server]
consumer_count  = 10
trace_mode      = 0

oftp_node_id            = moose
oftp_node_password      = moose
oftp_node_userdata      = moose
oftp_outbound_dir_capability = b
oftp_restarts_supported = n
oftp_special_logic_supported = y
oftp_compression_supported = n

oftp_timeout = 1

inbound_transport_method = X.25
external_API = techland

tcp_listen_port =

x25_device_driver = /dev/x25:3
x25_listen_nua =
x25_lcn_for_pvc =
x25_facility_info =
```

Code Example G-4   Sample OFTP Server Initialization File

```
x25_call_user_data =
x25_route_name =

x28_configured = y

x28_device_driver =
x28_modem_parity =
x28_modem_physical_word_len =
x28_modem_logical_word_len =
x28_modem_stop_bits =
x28_modem_monitor_DCD =
x28_modem_baud_rate =
x28_modem_init_string =
x28_modem_connect_timeout =

x28_label_start = Start
x28_label_online = Online
x28_label_hangup = Hangup x
```

The OFTP Table

Refer to the *iPlanet ECXpert Developer's Guide* appendix on the "ECXpert Database Schema."

Integrating ECXpert with Oracle Financials

This appendix describes the steps necessary to integrate ECXpert with Oracle Financials. The following topics are presented:

- Overview
- Starting the ECXpert Legacy Integration Server
- Setting Up Oracle Financials
- Setting Up ECXpert
- Customizing the Integration Maps

Overview

ECXpert integration with Oracle Financials has been tested using Oracle Financials Release 10.7. It is assumed that an operational Oracle Financials system is in place for you to connect to.

No instructions for Oracle Financials are provided in this Guide.

The following connections between ECXpert and Oracle Financials are currently supported by the ECXpert Legacy Server and map templates that you can customize for your specific needs:

- **Purchase Order into Purchasing**—An EDI purchase order from a procurement system can be mapped into Oracle Purchasing.

- **Purchase Order into Order Entry**—An EDI purchase order from a customer can be mapped in the supplier's Oracle Order Entry System.

- **Invoice into Payables**—An EDI invoice from a supplier can be mapped to a customer's Oracle Payables system.

Most other connections between ECXpert and Oracle Financials that you might want to implement can be handled by the ECXpert Legacy Server if you can create your own map. Additional map templates to facilitate the most commonly requested connections are planned for inclusion in future releases of ECXpert.

Figure H-1 shows the typical process flow between an Oracle Financials module and ECXpert when these two systems are integrated. Dashed lines indicate *optional* functions.

Figure H-1   Typical process flow between Oracle Applications and ECXpert

Starting the ECXpert Legacy Integration Server

The ECXpert Legacy Integration server is one of the server processes managed by the ECXpert Administrative Server. During installation this server is provided with a "switch" on the Administrative Server's Management tab. Follow the steps below to enable the Legacy Integration server by turning its switch to the "on" position.

1. Display the ECXpert Main Menu page in your browser.

   Enter the URL http://*hostname:portnum*
   where *hostname* is the name of the ECXpert host machine and *portnum* is the port number that ECXpert uses.

   The ECXpert Main Menu page (Figure H-2) is displayed.

   Figure H-2   ECXpert Main Menu page

   iPlanet
   ECXpert 3.5

   • **Admin**   User interface for controlling the configuration and operation of the ECXpert system.

   • **Support**   User interface for member administration and activity tracking within the ECXpert system.

   • **Utilities**   Utilities provided with the ECXpert system.

2. Display the ECXpert Administration Interface.

   Click Admin on the ECXpert Main Menu page. The ECXpert Administrative Interface, Server Management tab (Figure H-3) is displayed.

Figure H-3   ECXpert Administrative Interface, Server Management tab

If the Server Management tab shows only the ECXpert Administration server, and its switch is in the OFF position, click it to turn it to the ON position and start up the Administration server. This also causes the switches for additional servers to be displayed, as shown in Figure H-3.

The installation default for this switch is OFF. You can change the default by editing the ECXpert system settings file (ecx.ini) and setting the autostart_flag in the [legacy-oracle-apps] section to yes. Refer to Appendix C, "ECXpert Initialization File (ecx.ini)"," for more details.

3. Start up the Legacy Integration server.

Scroll down in the Server Administration tab to locate the switch for the Legacy Integration server.

If this switch is in the OFF position, click it to switch it to the ON position and start up the Legacy Integration Server.

4. Return to the ECXpert Main Menu page.

Use your browser's Back button or Go menu.

Setting Up Oracle Financials

On the Oracle Financials end, you need to perform different tasks listed below, depending on which connection(s) between ECXpert and Oracle Financials you want to implement.

This outline is intended only to serve as an aid in locating the functions in the Oracle Financials software.

For full details on all the steps involved, please refer to your Oracle Financials documentation or online help.

Oracle Purchasing

For details on these tasks, see "Running Scripts in Oracle (Oracle Purchasing Only)" on page 784.

1. Create new `PO_LOG_CAI` table.

2. Run `grant/synonym` script.

Oracle Order Entry

Define a Netscape ECXpert OrderImport source:

1. Navigate to the OrderImport Source window.

2. Enter the OrderImport source: **ECXpert**

3. Enter Description: **Orders Imported from Netscape ECXpert**

4. Check Enabled to activate the OrderImport source.

5. Save your work.

Oracle Accounts Payable

To create a Quickcode whose type is `SOURCE`, used to submit Payables Invoice Import, define a Netscape ECXpert Quickcode.

1. Navigate to the Quickcode window.

2. Enter the type: **Source**

3. Enter the name: **Create invoices from ECXpert**

4. Check Enable to activate the Quickcode.

5. Save your work.

Running Scripts in Oracle (Oracle Purchasing Only)

In order to integrate ECXpert with Oracle Applications you must run several SQL scripts. These scripts create `po_log_cai` table in the PO Module, create a synonym, create a procedure, and install the trigger.

Follow the steps below to run the SQL scripts in Oracle.

1. Open a command prompt window.

2. Change directories to the location of the `install_cai_integration.sh` script.

   Enter the following command:

   >cd $ECX_HOME/dbadmin/oracle/legacy/oracleapps

3. Run the `install_cai_integrtaion.sh` script.

   Enter the following command:

   ./install_cai_integrtaion.sh

   The following text is displayed:

   ```
   ================================================================
   This (cshell)script creates a table specific to this integration
   module, initiates the purchasing module, and creates a
   corresponding synonym in the applications. In order to do
   this, you need user/passwords for both, make sure you have
   them with you.
   =============Creating the log
   table=============================
   ```

   Then you are prompted for Oracle Purchasing Module logon information.

4. Answer prompts to log into the Oracle Purchasing Module database.

```
Enter the Oracle Purchasing Module database name:
    your purchasing module database name
Enter the Oracle Purchasing Module user name:
    your user name
Enter the Oracle Purchasing Module password name:
    your password
```

After entering your password, the login text for the Oracle Purchasing Module database is displayed:

```
DB Name = your purchasing module database name
User name = your user name
Password = your password
$ORACLE_HOME/bin/sqlplus
your user name/your password@your purchasing module database name
```

5. Answer prompts for synonym installation.

```
Enter the Oracle Applications database name:
    Application database names
Enter the Oracle Applications user name:
    your user name
Enter the Oracle Applications password name:
    password
DB Name = Application database names
User name = your user name
Password = password
```

After entering your password, the login text for the Oracle Applications database is displayed:

```
$ORACLE_HOME/bin/sqlplus
your user name/password@Application database names @iposyn.sql
```

The scripts you have run created the `po_log_cai` table in the Oracle Applications database. Table H-1 shows the structure of the `po_log_cai` table.

Table H-1   The `po_log_cai` table

Name	Req	Type (Len)	Description
ECX_PO_NUMBER	Y	varchar2(40)	ECXpert PO number.
APPS_PO_NUMBER		varchar2(40)	Application PO number.
STATUS	Y	varchar2(15)	PO status. Possible values: - STAGED = passed to Oracle Applications by ECXpert - IMPORTED = picked up by Oracle Applications - ACKNOWLEDGED = acknowledgment sent from ECXpert to BuyerXpert
CREATE_DATE		date	Date PO number was created.
LAST_UPDATE_DATE		date	Date PO number was last updated.

Generating Reports

For guidance in generating POs from a requisition import, refer to your Oracle Applications documentation.

Setting Up ECXpert

In order to integrate ECXpert with Oracle Applications, you must perform the following tasks in ECXpert:

- Plan for integration with Oracle Financials.
- Set up a supporting trading partnership in ECXpert.
- Set up a scheduled task in ECXpert.
- Run SQL scripts in Oracle.
- Generate reports in Oracle Applications.

Each of these tasks is detailed in the following sections.

When all of these tasks have been performed, remember that the ECXpert Legacy Integration Server must be started in order for the integration to operate. See "Starting the ECXpert Legacy Integration Server" on page 781 for details.

Planning for Integration with Oracle Financials

The integration between Oracle Applications and ECXpert requires an understanding of both EDI and Oracle Application semantics.

Also, make sure that you are familiar with Oracle's *SQL*Plus* and TSISoft's *Mercator Authoring System* and *DBEditor*, as well as the VISION demo database provided by Oracle Applications. Your specific EDI implementation might vary from our example implementation.

Further, you might prefer to populate different fields in the Oracle Interface tables. We suggest that you perform the following tasks:

- Examine the example EDI Documents in the *$NSBASE*/NS-apps/ECXpert/maps/legacy/OracleApps/R107 directory.

  The files are prefixed with either 810 or 850. Notice the use of the mutually defined identifier code, "zz." In many cases, an Oracle Application ID is the actual identifier that has been mutually defined.

- Compare your EDI implementation with our examples. Note the differences you find.

- Examine the tables described in the mapping section, "Customizing the Integration Maps" on page 791.

  When using *Oracle Financials* and *Oracle Government Financials, Release 10.7 Open Interfaces Modules*, consider whether you need to populate different fields.

- Determine how to mediate the differences between your EDI implementation and Oracle's Interface Table. Consider the following changes:

  ○ Add entries to or modify existing entries in orainxref.txt ("Example Lookup File (orainxref.txt) to Support Maps" on page 798), which is the lookup file used as an input to the Mercator maps. You must modify orainxref.txt so that the IDs correspond with the IDs in your application.

  ○ Use Mercator's DBLookup function to query the Oracle Applications Database to access required information.

  ○ Change your EDI Implementation.

- Using the Map found in `OracleApps/R107/`*Oracle_Module_specific_directory*, make the necessary changes and run the map.

  Check that the rows have been inserted into the correct interface tables. In some cases, a trigger exists on the interface table to automatically clean up the table. You can disable the trigger.

- From the Oracle Applications Concurrent request screen submit the Import request.

Setting Up the Supporting Trading Partnership in ECXpert

Integration of ECXpert with your legacy Oracle Applications requires setup of a dummy trading partnership in ECXpert. Such a trading partnership is necessary to allow ECXpert to exchange documents with any external system. Follow the steps below to set up this partnership.

1. Display the ECXpert Product Interface.

From the ECXpert Main Menu page (Figure H-2), click Support.

2. Create the members.

Click Membership in the ECXpert side panel to display the membership forms. Create two members. Each member must have a unique name.

3. Enter the basic trading partnership information.

Click Trading in the ECXpert side panel to display the partnership forms. Figure H-4 shows the Partnership Info form filled in with sample data.

Figure H-4   Partnership Info tab with sample data filled in

Enter the basic partnership information:

❍   Sending Member and Receiving Member must be the two members you just created; it does not matter which is sender and which is receiver.

❍   Partnership Type must be EDI to Application.

❍   Document Type must be 850.

❍   Map Name must be left blank here. Enter the map name on the Protocols tab (Figure H-5) instead.

NOTE	The above parameters are standard settings. You can use other values that better fit your specific needs.
	Refer to the online help for the various forms, for more details on coordinating these entries.

4. Enter the trading partnership protocol information.

Click the Protocols tab to display the protocols information form. Figure H-5 shows the Protocols tab with sample data filled in.

Figure H-5 Protocols tab with sample data filled in

Enter the protocol information:

○ Outgoing Protocol must be Legacy Server (Oracle).

○ Map Name must be the full path to the map file you are using. The sample maps supplied with ECXpert are:

```
$NSBASE/NS-apps/ECXpert/maps/legacy/OracleApps/R107/obi850.sun
$NSBASE/NS-apps/ECXpert/maps/legacy/OracleApps/R107/x850E.sun
$NSBASE/NS-apps/ECXpert/maps/legacy/OracleApps/R107/x810AP.sun
```

You can modify this default map or replace it with your own.

NOTE   For use in customization, map source and type trees are provided under the following:

```
$NSBASE/NS-apps/ECXpert/maps/legacy/OracleApps/inv2o-ap
```

```
$NSBASE/NS-apps/ECXpert/maps/legacy/OracleApps/ord2o-oe
```

```
$NSBASE/NS-apps/ECXpert/maps/legacy/OracleApps/ord2o-po
```

CAUTION   Make sure that you have not entered a map name on the Partnership Info tab (Figure H-4).

---

5. Save the trading partnership.

Click Save at the bottom of the form.

Setting Up a Scheduled Task in ECXpert

See "Scheduling ECXpert Jobs" on page 155 for instructions on setting up a scheduled task.

On the first page of the task definition form, select ECX_Gateway, with Legacy Server (Oracle).

On the Protocols page (Figure 3-24 on page 162), there are no special requirements to support Oracle Financials integration.

Customizing the Integration Maps

The current framework for Oracle Applications integration works with the VISION demo database provided by Oracle Applications.

Most Oracle Applications installations are customized to some extent. If you have customized your Oracle Applications installation, you need to make corresponding changes to the maps provided.

The source files for these maps is provided with ECXpert. This file is documented in Use the Mercator Authoring Tool to view the map source and determine which elements need to be modified to match your Oracle Applications installation.

NOTE	Names and locations of sample map files are given at the end of the topic that begins with "Setting Up the Supporting Trading Partnership in ECXpert" on page 788.

Table H-2   Summary of ECXpert/Oracle Financials connections

Connection	Source Table Name	Destination Table Name	Comments
Purchase Order into Purchasing	N/A	`PO_REQUISITIONS_INTERFACE_ALL`	Outbound 850 from a procurement system is mapped into interface table.
Purchase Order into Order Entry	N/A	`SO_HEADERS_INTERFACE_ALL,` `SO_LINES_INTERFACE_ALL`	EDI 850 is posted into Order Entry as a Sales Order using the interface tables.
Invoice into Payables	N/A	`AP_EXPENSE_REPORT_HEADERS_ALL,` `AP_EXPENSE_REPORT_LINES_ALL`	EDI 810 is mapped into these interface tables.

Table H-3 provides an example of how one of the *Mercator* source files provided with ECXpert is organized. Table H-4 through Table H-7 provide examples of the data translations that these sample maps can perform when you customize them to meet your specific needs.

Table H-3   Organization of source file (obi850)

	Item	Description
Executable map: XOBI850		
	Purpose	Transform X12 850 transmission into rows in 2 Oracle tables.
Input	Card1	X12 850 version 003040 transmission
	Card2	Lookup file with external values
Output	Card1	Work card with a variety of values used in subsequent steps. Delete at map conclusion
	Card2	PO Requisition table
	Card3	PO Log table
Calls	EachPODetail	
	EachPOLog	
Functional map: EachPODetail		
	Purpose	Create a row in the PO Requisition table for each PO line item transmitted. Data created will come from a combination of EDI data and values determined from the external lookup file.
Input	Card1	PO1 loop from 850 transaction
	Card2	850 transaction associated with the PO1 loop
	Card3	Lookup file with external values
Output	Card1	Row in PO Requisition table
Calls	None	

Table H-3   Organization of source file (obi850) *(Continued)*

	Item	Description
Functional map: EachPOLog		
	Purpose	Create a row in the PO Log table for each PO transmitted.
Input	Card1	850 transaction associated with the PO1 loop
	Card2	Lookup file with external values
	Card3	Work file that contains current date in CCYYMMDD format
Output	Card1	Row in PO Log table containing PO number, staged status and created/last update date
Calls	MakeOracleDate	
Functional map: MakeOracleDate		
	Purpose	Format Date/Time field for Oracle table
Input	Card1	Date in CCYYMMDD format
Output	Card1	Date/Time in format CCYY-MM-DD HH:MM:SS
Calls	MakeOracleDateCC	
Functional map: MakeOracleDateCC		
	Purpose	Format Date/Time field for Oracle table
Input	Card1	Date in CCYYMMDD format
Output	Card1	Date/Time in format CCYY-MM-DD HH:MM:SS
Calls	None	

The following tables provide an overview of how EDI Document data can be mapped into Oracle Financials. These are just sample implementations. You must customize the map templates provided to fit your particular business needs.

Accounts Payable

Table H-4 and Table H-5 provide examples of the data translations that the Accounts Payable sample maps can perform when you customize them to meet your specific needs.

Table H-4   Accounts Payable sample map (`x810AP.sun`) - header translation example

EDI 810	AP_EXPENSE_REPORT_HEADERS_ALL
Key file	`REPORT_HEADER_ID`
InvDate Element:BIG Segment or CURRENTDATE	`WEEK_END_DATE`
CURRENTDATE	`CREATION_DATE`
Lookup File	`CREATED_BY`
CURRENTDATE	`LAST_UPDATE_DATE`
0	`VOUCHNO`
TotalInvAmt Element:TDS Segment	`TOTAL`
Lookup File	`VENDOR_ID`
Lookup File	`VENDOR_SITE_ID`
Inv# Element:BIG Segment	`INVOICE_NUM`
Lookup File	`ACCTS_PAY_CODE_COMBINATION`
Lookup File	`SET_OF_BOOKS_ID`
"ECXpert"	`SOURCE`
"Y"	`PURGEABLE_FLAG`
CURRENTDATE	`ACCOUNTING_DATE`
Desc'n Element:REF Segment	`DESCRIPTION`
CurrencyCd Element:CUR Segment or "USD"	`DEFAULT_CURRENCY_CODE`
Key file	`VOUCHER_NUM`
Lookup File	`ORG_ID`

Table H-5   Accounts Payable sample map (`x810AP.sun`) - line item translation example

EDI 810	AP_EXPENSE_REPORT_LINES_ALL
Key file	`REPORT_HEADER_ID`
CURRENTDATE	`LAST_UPDATE_DATE`
Lookup File	`CODE_COMBINATION_ID`
Desc'n Element:PID Segment (Free Form)	`ITEM_DESCRIPTION`
Lookup File	`SET_OF_BOOKS_ID`
QtyInvoiced Element:IT1 Segment * UnitPrice Element:IT1 Segment	`AMOUNT`
CurrencyCd Element:CUR Segment or "USD"	`CURRENCY_CODE`
"ITEM"	`LINE_TYPE_LOOKUP_CODE`
Lookup File	`ORG_ID`

Order Entry

Table H-4 and Table H-5 provide examples of the data translations that the Accounts Payable sample maps can perform when you customize them to meet your specific needs.

Table H-6   Order Entry sample map (x850OE.sun) - translation example 1

EDI 850	SO_HEADERS_INTERFACE_ALL
CURRENTDATE	CREATION_DATE
CURRENTDATE	LAST_UPDATE_DATE
PONumber Element:BEG Segment	ORIGINAL_SYSTEM_REFERENCE
Name Element:N1 Segment (Buyer)	CUSTOMER_NAME
IDCd Element:N1 Segment (Buyer's D-U-N-S Number)	CUSTOMER_NUMBER
Lookup File	ORDER_TYPE
Lookup File	ORDER_SOURCE_ID
"R"	ORDER_CATEGORY
CURRENTDATE	DATE_ORDERED
CurrencyCd Element or "USD"	CURRENCY_CODE
Lookup File	SALESREP_ID
Name Element:N1 Segment (Buyer)	INVOICE_CUSTOMER
IDCd Element:N1 Segment (Ship To)	INVOICE_ADDRESS_ID
IDCd Element:N1 Segment (Ship To)	SHIP_ADDRESS_ID
Lookup File	PRICE_LIST_ID
Lookup File	TERMS_ID
"Entered"	ENTERED_STATE_NAME
PONumber Element:BEG Segment	PURCHASE_ORDER_NUM
"INSERT"	OPERATION_CODE
Lookup File	ORG_ID

Table H-7   Order Entry sample map (x850OE.sun) - translation example 2

EDI 850	SO_HEADERS_INTERFACE_ALL
CURRENTDATE	CREATION_DATE
CURRENTDATE	LAST_UPDATE_DATE
PONumber Element:BEG Segment	ORIGINAL_SYSTEM_REFERENCE
Index generated from map	ORIGINAL_SYSTEM_LINE_REFERENCE
Index generated from map	LINE_NUMBER
"REGULAR"	LINE_TYPE
Lookup File	UNIT_CODE
QtyOrdered Element: PO1 Segment	ORDER_QUANTITY
UnitPrice Element:PO1 Segment	LIST_PRICE
UnitPrice Element:PO1 Segment	SELLING_PRICE
ProdServiceID Element:PO1 Segment (Vendor's Part Number)	INVENTORY_ITEM_SEGMENT1
ProdServiceID Element:PO1 Segment (Vendor's Part Number)	INVENTORY_ITEM_ID
ORDER_SOURCE_ID	ORDER_SOURCE_ID
Lookup File	ORG_ID

Example Lookup File (orainxref.txt) to Support Maps

The lookup file template shown below is self-explanatory.

For example, the line

```
UOM/\LINE/\*/\Each/\Ea
```

is constructed based on the syntax specified in the first line of the file. The following bullet points explain each part of the line shown above:

- UOM (TYPE) is the, or key, into this lookup table, through which this particular record can be selected.

- LEVEL indicates whether it is at the header or line item (LINE) level.

- ORACLEAPPSHORTNAME is optional. An asterisk (*) indicates it is not required.

- **SOURCEVALUE** specifies the symbol (Each) that needs to translated.

- **DESTINATION** specifies the target symbol (Ea).

Use this template as a guideline for constructing your own lookup files whenever creating lookup files becomes necessary to support a map.

```
TYPE/\LEVEL/\ORACLEAPPSHORTNAME/\SOURCEVALUE/\DESTINATIONVALUE
--------/\------------------------/\--------------------------
-----/\------------------------/\-------------
ORG_ID/\HEADER/\*/\*/\{INSERT ID HERE}
CREATED_BY/\HEADER/\*/\*/\{INSERT ID HERE}
ORDER_TYPE/\HEADER/\OE/\SA/\Standard
UOM/\LINE/\*/\Each/\Ea
DESTINATION_TYPE_CODE/\HEADER/\PO/\*/\EXPENSE
INTERFACE_SOURCE_CODE/\HEADER/\PO/\*/\ECXPERT
DESTINATION_ORGANIZATION_CODE/\HEADER/\PO/\*/\{INSERT ID HERE}
CHARGE_ACCOUNT_ID/\HEADER/\PO/\*/\{INSERT ID HERE}
CATEGORY_ID/\LINE/\PO/\*/\{INSERT ID HERE}
VENDOR_ID/\HEADER/\AP/\*/\{INSERT ID HERE}
VENDOR_SITE_ID/\HEADER/\AP/\*/\{INSERT ID HERE}
ACCTS_PAY_CODE_COMBINATION_ID/\HEADER/\AP/\*/\{INSERT ID HERE}
SET_OF_BOOKS_ID/\HEADER/\AP/\*/\{INSERT ID HERE}
CODE_COMBINATION_ID/\LINE/\AP/\*/\{INSERT ID HERE}
ORDER_SOURCE_ID/\HEADER/\OE/\*/\{INSERT ID HERE}
SALESREP_ID/\HEADER/\OE/\*/\{INSERT ID HERE}
PRICE_LIST_ID/\HEADER/\OE/\*/\{INSERT ID HERE}
TERMS_ID/\HEADER/\OE/\*/\{INSERT ID HERE}
```

Integrating ECXpert with SAP

This appendix describes the steps necessary to integrate ECXpert with SAP. The following topics are presented:

- Overview

- Setting Up SAP

- Setting Up ECXpert

- Customizing the Integration Maps

Overview

ECXpert integration with SAP has been certified using interface software for the SAP R/3 3.1H System (*SAP report 525 from 8/21/1998*, tested on SUN Ultra 1 with Solaris 2.6). These instructions assume that you can connect to an operational SAP system. This guides does not provide instructions for installing SAP.

Before you can use the ECXpert SAP connectivity, you must set up the infrastructure on both the ECXpert and SAP ends:

- In SAP, you must set up any logical systems and logical message types that are needed, if they do not already exist. Then you must add the logical message types to be exchanged to the SAP logical systems involved.

- On the ECXpert end, you must set up any members that are needed, if they do not already exist. Then you must set up the usual partnership(s) and service list(s), and create or modify any maps that are necessary to perform the required data translations. Finally, you must configure system settings in the `[legacy-sap]` section of the `ecx.ini` file.

When the ECXpert Legacy Server starts up, based on `ecx.ini` settings, it connects to SAP and keeps that connection "hot" for the entire duration of its execution. Whenever an IDOC from SAP is available, ECXpert picks it up and handles it as an incoming document. Outgoing documents are not handled differently from standard ECXpert documents.

NOTE	For properly configured SAP connectivity to function, the ECXpert Legacy Integration Server must be started. See "Starting the ECXpert Legacy Integration Server" on page 781 for more details.

Setting Up SAP

For the SAP end, you need to perform the tasks listed below. This outline is intended only to serve as an aid in locating the functions in the SAP software. For full details on all the steps involved, refer to your SAP documentation or online help.

1. Define a logical system to represent ECXpert.

   ❍ Transaction code **SALE** - to go directly to **Distribution (ALE)**

   ❍ **Basic Configuration** > **Set up logical system** > **Maintain local systems**

2. Add all the ECXpert logical message types to the ECXpert logical system and to *each* SAP logical system involved.

NOTE	You do not need to do this for SAP logical systems for which a given message type is already added.

   ❍ Transaction code **SALE** - to go directly to **Distribution (ALE)**

   ❍ **Distribution customer model** > **Maintain customer distribution model directly**

3. (Optional) If you plan to have ECXpert automatically submit IDocs from SAP to ECXpert trading partners as soon as they are received, set the SAP output mode to collect IDocs.

   For more predictable performance, set up SAP to collect IDocs for manual submission to the ECXpert Legacy Server:

   ❍ Transaction code **SALE** - to go directly to **Distribution (ALE)**

- ❍ **Communication → Manual Maintenance of partner profiles → Maintain partner profiles**

- ❍ Fill in the **Logical System** and click the **Change** icon.

- ❍ Go to **outbound parameters** and double-click on the message type.

- ❍ Change the **packet size** to something between 30 and 50.

- ❍ Change the **output mode** to **Collect IDocs**.

Now, IDocs sent from BALE will have a status of 30 (IDoc ready for dispatch by ALE Service) and will be ready to be sent to the ECXpert Legacy Server.

Sending Collected IDocs to the Legacy Server

Each time you want to send collected IDocs to the ECXpert Legacy Server, perform these steps:

1. Go to **BALE** > **Period Work** > **ALE outbound IDocs**.

2. Click on the radio button for **Dispatch and Execute**.

3. Click **Execute** again to send the IDocs to ECXpert.

NOTE	If you do not perform Step 3, SAP will automatically add IDocs that are ready to the tRFC queue, to be sent to the ECXpert Legacy Server.
	However, IDocs in the tRFC queue are submitted to the Legacy Server only about once every 15 minutes, and the documents appear on the server at the rate of about three or four per second. After the Legacy Server receives the documents, it submits them to the appropriate trading partners; initial calls to submitDoc take longer than subsequent ones.
	Therefore, the delay between the time SAP originally dispatches the IDocs and the time ECXpert sends them to trading partners might not be constant.
	If this is not a concern for your installation, you do not need to perform Step 3.

SAP System Settings

CAUTION	These changes should only be made by the SAP System Administrator, or by someone authorized by that system administrator.

Add the following lines to `/etc/services`:

```
sapdp00    3200/tcp      sap #sap dialog process(cots)
sapgw00    3300/tcp      sap #sap(cots)
sapgw01    3301/tcp      sap #sap gateway(cots)
```

Setting Up ECXpert

On the ECXpert end, there are two tasks to perform to enable integration with SAP:

- **System settings** must be modified once in several system files.

- **A trading partnership** must be set up for each sender/receiver/document type combination involved.

ECXpert System Settings

Follow the steps below to modify ECXpert system settings for integration with SAP.

1. In *ecx.ini*, set the following in the `[legacy-sap]` section:

   `rfc_server_section=`*DEST value in the saprfc.ini file*
   `outbound_idoc_workingdir=`*full path to work directory*
   `outbound_idoc_dir=`*full path to outbound idoc directory*
   `ale_server_auto_start=yes`

```
ale_idoc_submit_mode=directory|ecx
```
idoc_sender=*member id of Sender in ECXpert partnership*
idoc_receiver=*member id of Receiver in ECXpert partnership*
idoc_doctype=*Document Type in ECXpert partnership*

NOTE   When `ale_idoc_submit_mode=ecx`—such that the ECXpert
legacy server automatically submits IDocs from SAP to ECXpert
as they are received—set the SAP output mode to collect IDocs
(see Step 3 on page 802).

See "[legacy-sap] Section" on page 705 for more details on these parameters.

2. Edit `$NSBASE/NS-apps/ECXpert/cgi-bin/saprfc.ini` to point to a
`program ID` of the logical system setup in SAP that will be used for ECXpert.

The section will look something like the following:

```
DEST=SDR
TYPE=R
PROGID=qa-ale
GWHOST= sap.mcom.com
GWSERV=sapgw00
RFC_TRACE=1
```

NOTE   When testing your SAP connectivity with ECXpert, be sure to
make use of the SAPRFC trace file, `dev_rfc`, located in the
$NSBASE/NS-apps/`ECXpert/cgi-bin/` directory.

Trading Partnership(s)

You must set up a separate partnership for each sender/receiver/document type
combination involved. Follow the steps below to set up each partnership.

1. Set up members for SAP.

Set up a member for each SAP logical system to which ECXpert will send
documents. No specific SAP partnership is needed for SAP to send documents
to ECXpert.

2. Set up any additional ECXpert members needed.

3. Set up service lists.

   Set up a service list for each ECXpert member/SAP logical system/SAP logical message type combination.

4. Set up partnerships.

   Set up a partnership for each ECXpert member/SAP logical system/SAP logical message type combination.

5. Set up a scheduled task for any sending to SAP that is to be time-based.

Customizing the Integration Maps

As part of this integration solution, example TSI Mercator maps that translate IDOCS to EDI formats, and EDI messages to IDOCS, are located in the *$NSBASE*/NS-apps/`ECXpert/maps/legacy/SAP/R31H` directory. Each of the four subdirectories (`idoc2inv`, `idoc2ord`, `inv2idoc`, and `ord2idoc`) contains the source files to build a map.

Since every SAP installation is customized to some extent, the source files include type trees and maps. To use these maps, you must make whatever customizations are required by your specific SAP environment.

Integrating ECXpert with MQ Series

This appendix describes the steps necessary to integrate ECXpert with MQ Series. The following topics are presented:

- Overview
- Setting Up a Queue Manager on the MQSeries Server
- Setting Up the MQSeries Client
- Setting Up ECXpert

Overview

ECXpert integration with MQSeries has been tested using MQSeries version 5.0. These instructions assume that you can connect to an operational MQSeries Server with Queue Manager (local or remote).

No instructions for installing MQSeries Server are provided in this Guide.

Before you can use the ECXpert MQSeries connectivity, you must first set up an MQSeries client, local to the same system on which ECXpert is installed. The MQSeries client communicates with the Queue Manager using an MQI channel, as shown in Figure J-1.

For an overview of what is involved on the ECXpert end in setting up integration with MQSeries, see "Integrating ECXpert with MQSeries" on page 110.

NOTE   For properly configured MQSeries connectivity to function, the ECXpert Legacy Integration Server must be started.

See "Starting the ECXpert Legacy Integration Server" on page 781 for more details.

Figure J-1   MQSeries client communication with Queue Manager using an MQI channel

In the above diagram, when ECXpert sends a message to the MQSeries queue manager, the operation is called a put in MQSeries terminology; ECXpert "puts" a message into an MQSeries queue.

Communication in the opposite direction is called a get; ECXpert "gets" a message out of an MQSeries queue.

Setting Up a Queue Manager on the MQSeries Server

Follow the steps below to set up MQSeries Server for integration with ECXpert.

1. Install MQSeries 5.0 server for NT or SUN Solaris.

    Follow the instructions supplied with the product.

2. Create a default queue manager and start the queue manager:

    Enter these commands:

    ```
    crtmqm -q venus.queue.manager
    strmqm venus.queue.manager
    ```

3. Invoke MQSC.

Enter the command:

runmqsc

4. Define a local queue.

   For example, if your local queue is called "orange.queue":

   define qlocal (orange.queue)

NOTE	Whether your queue name is in upper case, lower case, or a combination of the two, MQSeries converts it to upper case when it stores it.

5. Define a channel.

   Enter the command:

   define channel *ChannelName* chltype *ChannelType* trptype *TransportType*

   where

   ❍ *ChannelName* is the channel name you want to use

   ❍ *ChannelType* is the channel type to use

   ❍ *TransportType* is the transport type to use

   For example:

   ```
   define channel (CHAN1) chltype (SVRCONN) trptype (TCP)
   ```

Setting Up the MQSeries Client

Complete the tasks outlined in this section to set up an MQSeries Client for integration with ECXpert. It is highly recommended that you read the MQSeries installation guidelines, available on the IBM web site at:

http://www.software.ibm.com/ts/mqseries/library/manuals/amqdac/AMQD AC01.HTM

NOTE	The MQSeries Client must be installed on the same system on which ECXpert is installed.

Configuring the Kernel

MIBM documentation suggests that you use the set of kernel parameters described below for running MQSERVER. Make sure your system matches these kernel parameters. For additional details on IBM recommended kernel configuration, see:

```
http://www.software.ibm.com/ts/mqseries/library/manuals/amqdac/AMQD
AC15.HTM
```

IBM recommended kernel parameters for MQSeries:

```
    set shmsys:shminfo_shmmax = 4194304
    set shmsys:shminfo_shmseg = 1024
    set shmsys:shminfo_shmmni = 1024
    set shmsys:shminfo_shmem  = 1
    set semsys:seminfo_sema   = 1
    set semsys:seminfo_semaem = 16384
    set semsys:seminfo_semvmx = 32767
    set semsys:seminfo_semmni = 1024 (semmni < semmns)
    set semsys:seminfo_semmap = 1026 (semmni +2)
    set semsys:seminfo_semmns = 16384
    set semsys:seminfo_semmsl = 100
    set semsys:seminfo_semopm = 100
    set semsys:seminfo_semmnu = 2048
    set semsys:seminfo_semume = 256
    set msgsys:msginfo_msgmni = 50
    set msgsys:msginfo_msgmap = 1026
    set msgsys:msginfo_msgmax = 4096
    set msgsys:msginfo_msgmnb = 4096
    set msgsys:msginfo_msgssz = 8
    set msgsys:msginfo_msgtql = 40
    set msgsys:msginfo_msgseg = 1024
    set maxusers = 32
```

To change the values, add a set *parameter* = *value* line to the /etc/system file.

For further details on setting up the system, refer to the *Sun Solaris Version 2.5 System Administration Guide*.

After installation, review the machine's configuration by entering the following command:

sysdef -i

Establishing Communication between the Client and Server

1. Set up the MQSERVER environment variable on the client.

Enter the command:

setenv *ChannelName* / *TransportType* / *MQSHost*

where

○ *ChannelName* is the channel name you want to use

○ *TransportType* is the channel type to use

○ *MQSHost* is the IP address or host name of the MQSeries host

For example:

```
MQSERVER CHAN1/TCP/111.22.33.44
```

2. Put a message in the queue.

For example, if your local queue is called "`orange.queue`," you could use the sample with the following syntax:

```
/opt/mqm/samp/bin/amqsputc ORANGE.QUEUE
```

NOTE	MQSeries converts the queue name you created to upper case. You must enter queue names in upper case only.

3. Get the message on the server.

Use the sample with the following syntax:

```
/opt/mqm/samp/bin/amqsgetc ORANGE.QUEUE
```

NOTE	Remember to enter queue names in upper case only.

4. Check available disk space.

Before installing MQSeries client, you must make sure you have enough space in `/var` and `/opt`. The MQSeries documentation recommends having at least 4MB free in both directories.

If you have less space free, rearrange files to make the space available before proceeding.

5. Install the MQSeries Client 5.0 for Sun Solaris.

   pkgadd -d /cdrom/mq_solaris/mqs500.img

   Reply **all** to the package when prompted.

   At some point you will see a list of 40+ packages to install. Choose the MQSeries client for Solaris.

Setting Up ECXpert

On the ECXpert end, you must perform the following tasks to enable integration with MQSeries.

- For **both Put** *and* **Get**:
  - ❍ **System settings** must be modified once in the ecx.ini file. See "System Settings (ecx.ini File)" on page 812 for details.

- For **Put**:
  - ❍ **Message Header File** for MQSeries must be created.
  - ❍ **Memberships** for the Sender (MQSeries) and the Receiver (ECXpert) must be created.
  - ❍ **Trading Partnerships** must be set up for each MQSeries Queue and document type to be exchanged.

- For **Get**:
  - ❍ **Scheduler task** must be created.

System Settings (ecx.ini File)

Entries for MQServer need to be specified in the [legacy_mq_series] section of the ecx.ini file.

For details on the MQSeries parameters in this file, see "[legacy-mq-series] Section" on page 708.

Parameters Needed to Connect to the Queue

The following parameters are needed to connect to the queue.

MQSERVER

If you do not need to send messages larger than 4MB, you can set the MQSERVER parameter to be able to connect to the MQSeries queue manager.

Set the MQSERVER parameter as follows:

MQSERVER=*channel*/TCP/*MQSHost*

where:

channel is any name, and

MQSHost is the IP address of the machine on which the MQSeries server is installed.

MQCHLLIB and MQCHLTAB

To send messages of more than 4MB, set MQCHLLIB and MQCHLTAB and do *not* set MQSERVER.

Client and server connection of the channel needs to be defined in MQSC as specified below:

1. Invoke MQSC.

Enter the command:

runmqsc

2. Create Channel CHAN2 Server Connection.

For example:

DEFINE CHANNEL(CHAN2) CHLTYPE(SVRCONN) TRPTYPE(TCP)

3. Create Channel CHAN2 Client Connection.

   For example, where the IP Address is 111.22.33.144 and the queue name is TEST.QMGR:

   ```
   DEFINE CHANNEL(CHAN2) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
   CONNAME(IP NAME) QMNAME(Queue Manager Name)
   ```

NOTE	The Queue Manager name is case-sensitive, so enclose the queue manager name in single quotes if it is lower case, for example, 'lowercase.qmname'.
	TCP should always be in upper case.

   The channel definition described above is kept in the client channel definition table associated with the queue manager running on the server. This table is called AMQCLCHL.TAB, and it is a binary file that cannot be edited directly.

   AMQCLCHL.TAB is created in the directory:

   ```
   /var/mqm/qmgrs/QUEUEMANAGERNAME/@ipcc
   ```

   For more details on creating channel definitions on the server, see the IBM Documentation at:

   ```
   http://www.software.ibm.com/ts/mqseries/library/manuals/csqzaf/C
   SQZAF25.HTM
   ```

4. Alter the sizes for messages larger than 4MB.

   If you expect to exchange messages larger than 4MB in size, use the alter command to change the sizes of Queue Manager, queue, and channel. For more details on the alter command, refer to the IBM documentation.

5. Set MQCHLLIB to the path to the directory containing the client channel definition table in ecx.ini

   ```
   MQCHLLIB = MQCHLLIB_path
   ```

6. Set MQCHLTAB to the file name of the client channel definition table.

   ```
   MQCHLTAB = MQCHLTAB_filename
   ```

7. Comment out the MQSERVER parameter in ecx.ini.

   Otherwise MQSERVER will be used.

   ```
   # MQSERVER =
   ```

Dead Letter Queue Status

On an error in `Put`, ECXpert will try to put the message in the dead letter queue, if the dead letter flag is set to `yes`:

```
dead_letter_q_flag = yes
```

Header Separator for Get Operation

If the `header_in_separate_file` parameter is set to `yes`, after a message is retrieved from the queue, the message body and the header are placed in separate files.

If the flag is set to `no`, the `header_separator` value is used to separate header and body.

```
header_separator = ECX_MQSERIES_LEGACY_SERVER_HEADER_SEPARATOR
```

Message Header File

You must create a message header file to pass information to MQSeries about the message you are sending.

The rules governing the MQSeries message header file are as follows:

- A line beginning with a "#" indicates a comment.

- The file need not contain all the fields in the header. If a field name is absent in the file, the Legacy Server assigns it a default value.

- If a file name appears in the file without a value (for example, `Format=` or `Format`), the Legacy Server ignores it.

- Field names must appear *exactly* as described in the following sample file; if a field name does not appear as described, the field is ignored. For example, if `MsgId` appears as `msgId` or `MSGID` in the file, it is ignored.

- Names and values are separated by an equals sign ("=").

- Fields are ignored if white spaces are included before a field name or before an equals sign ("=").

  For example, the Legacy Server ignores the following two lines

  ```
  MsgId =100
   MsgId=100
  ```

  because the first has a space before the equals sign and the second has a space before the field name `MsgId`.

- Each line must contain only one *name=value* pair.

- Any characters after the "=" until the end of line are considered to be specifying a value.

- MQSeries uses certain fields, such as `StrucId` and `Version`, so the Legacy Server assigns default values recognized by MQSeries to these fields. It is advisable *not* to assign values to these fields unless necessary. For example, if `Version` has a value other than `1`, the `PUT` operation will fail.

- Fields such as `PutApplName`, `PutTime`, `PutDate` are assigned values by MQSeries. MQSeries overwrites any values you assign to these fields.

Below is a sample MQSeries header file:

```
MsgID=100
CorrelId=12
GroupId=3
MsgSeqNumber=6
```

Below is a complete listing of all valid fields and their data types:

```
MQCHAR4   StrucId;          /* Structure identifier */
MQLONG    Version;          /* Structure version number */
MQLONG    Report;           /* Report options */
MQLONG    MsgType;          /* Message type */
MQLONG    Expiry;           /* Expiry time */
MQLONG    Feedback;         /* Feedback or reason code */
MQLONG    Encoding;         /* Data encoding */
MQLONG    CodedCharSetId;   /* Coded character set identifier */
MQCHAR8   Format;           /* Format name */
MQLONG    Priority;         /* Message priority */
MQLONG    Persistence;      /* Message persistence */
MQBYTE24  MsgId;            /* Message identifier */
MQBYTE24  CorrelId;         /* Correlation identifier */
MQLONG    BackoutCount;     /* Backout counter */
MQCHAR48  ReplyToQ;         /* Name of reply-to queue */
MQCHAR48  ReplyToQMgr;      /* Name of reply queue manager */
MQCHAR12  UserIdentifier;   /* User identifier */
MQBYTE32  AccountingToken;  /* Accounting token */
MQCHAR32  ApplIdentityData; /* Application data relating to identity */
MQLONG    PutApplType;      /* Type of application that put the message*/
MQCHAR28  PutApplName;      /* Name of application that put the message */
MQCHAR8   PutDate;          /* Date when message was put */
MQCHAR8   PutTime;          /* Time when message was put */
MQCHAR4   ApplOriginData;   /* Application data relating to origin */
MQBYTE24  GroupId;          /* Group identifier */
MQLONG    MsgSeqNumber;     /* Sequence number of logical msg w/in group */
MQLONG    Offset;            /* Offset of data in physical msg from start
                              of logical msg */
MQLONG    MsgFlags;         /* Message flags */
MQLONG    OriginalLength;   /* Length of original message */
```

Following are the actual data types:

```
typedef unsigned char MQBYTE;
typedef char MQCHAR;
typedef long MQLONG;
//array data types
typedef MQCHAR MQCHAR48[48];
```

Following are the default values that MQSeries supplies if they are not explicitly set in your message header file:

```
StrucId=MD
Version=1
Report=0
MsgType=8
Expiry=-1
Feedback=0
Encoding=273
CodedCharSetId=819
Format=MQSTR
Priority=0
Persistence=0
MsgId=AMQ Test.Default6K6
CorrelId=
BackoutCount=0
ReplyToQ=
ReplyToQMgr=Test.Default.Queue.Manager
UserIdentifier= user_name
AccountingToken=11054
ApplIdentityData=
PutApplType=6
PutApplName=main
PutDate=19981007
PutTime=04251360
ApplOriginData=
GroupId=
ApplIdentityData=
MsgSeqNumber=1
Offset=0
MsgFlags=0
OriginalLength=-1
```

Memberships

Set up memberships for both the Sender (MQSeries) and the Receiver (ECXpert).

1. Set up a member for MQSeries.

An existing member can be used.

2. Set up a member for ECXpert.

Use the membership definition tabs—there are no MQSeries-specific settings.

Trading Partnership(s)

For MQSeries Put only, you must set up a separate partnership for each MQSeries Queue and document type to be sent. Follow the steps below to set up each partnership.

1. Set up a partnership.

    In the partnership definition tabs, set the following (only MQSeries-specific settings are shown):

Item	Setting
Protocols tab	
Outgoing Protocol	Legacy Server (MQS)
Queue Name	Must be all upper case
Queue Manager	Case sensitive.
Message Header	Path and file name to the message header file.

2. If you are sending to MQSeries, submit a test document.

    ○   **Using Command Line:** Use the following syntax to run the submit command to put a message to the queue from the command line.

    ```
    $NSBASE/NS-apps/ECXpert/bin/submit -se Sending_Member_ID
    -re Receiving_Member_ID -fn File_Name -ft Document_Type
    -in $NSBASE/NS-apps/ECXpert/config/ecx.ini
    ```

    ○   **Using Administrative Interface:** Use the Submit interface from the Utilities menu to enter the above parameters through a graphical interface. See "Using the ECXpert Utilities" on page 181 for more details.

    ○   **Using a Scheduled Task:** If you want your messages to be exchanged with MQSeries on a time-based schedule, set up a scheduled task. See "Scheduling MQSeries Exchanges" on page 820 for more details.

Scheduling MQSeries Exchanges

For time-based, batch-type scheduling of your MQSeries exchanges, follow the steps below to set up a scheduled task through the ECXpert Scheduler.

1. Display the ECXpert Scheduler.

For detailed instructions on using the ECXpert Scheduler, refer to "Scheduling ECXpert Jobs" on page 155. The instructions provided here are only a summary.

2. Create a new task.

Click Add Task.

3. Fill in the first page of the new task input form.

For Task Name, enter a unique task name.

For Use, select ECX Gateway. Then, from the drop-down list to the right, select the following:

❍ For Get, select Legacy for MQSeries Receive

❍ For Put, select Legacy for MQSeries Send

Click Next to display the Parameters page. Based on your selection from the ECX Gateway drop-down list, continue with instructions at the location indicated below.

ECX Gateway Selection	Continue with instructions at...
Legacy for MQSeries Receive (Get)	Step 4 on page 820
Legacy for MQSeries Send (Put)	Step 6 on page 821

4. Specify parameters for MQSeries `Get`.

Fill in the screen from the information in Table J-1.

Table J-1   Parameters for MQSeries `Get`

Item	Description
Parameters For MQSeries Receive	
Queue Manager Name	The name of the MQSeries Queue Manager involved. *Note:* This name is case sensitive.

Table J-1 Parameters for MQSeries `Get`

Item	Description
Queue Name	The name of queue on the MQSeries Queue Manager. *Note:* Enter this name in upper case only.
Message ID Regular Expression	A regular expression to retrieve only those messages whose Message ID matches it. Leave blank to retrieve all messages.
Correlation ID Regular Expression	A regular expression to retrieve only those messages whose Correlation ID matches it. Leave blank to retrieve all messages.
Inbound Directory	The full path to the directory in which the retrieved messages are to be stored.
Timeout Seconds	The timeout interval, in seconds, that ECXpert MQSeries Client is to wait for the Queue to receive the messages.
Message Count	The total number of messages to be retrieved. Leave blank to retrieve all messages.
File Name Prefix	The prefix to be added to file names generated for the messages retrieved from Queue. The file name formats are as follows: - Header file: `prefix _ time _ pid . uniqueId .hdr` - Message file: `prefix _ time _ pid . uniqueId .msg`

Parameters For Submit To ECXpert
Note: Enter values for these parameters only if you want the messages that you get from MQSeries to be submitted to ECXpert for processing.

Item	Description
Sender	Member ID of the sending member in the supporting partnership.
Receiver	Member ID of the receiving member in the supporting partnership.
Document Type	Document Type in the supporting partnership.

5. Continue at .

After you have finished specifying parameters for MQSeries Get, skip to . Do NOT go on to the next step below.

6. Specify parameters for MQSeries Put.

Fill in the screen from the information in Table J-2.

Table J-2   Parameters for MQSeries `Put`

Item	Description
Sender	Member ID of the sending member in the supporting partnership.
Receiver	Member ID of the receiving member in the supporting partnership.
Document Type	Document Type in the supporting partnership.
Document Version	The EDI document version number.
Document Standard	The EDI document standard number.

7. Specify a schedule.

   Click Next on the Parameters page to display the schedule page. Specify the scheduling parameters that you want.

   See "Last Page—When to Run the Task" on page 175 for more details on scheduling options.

8. Save your work.

   Click Finish.

Integrating ECXpert with JMS

ECXpert supports JMS messaging: it lets ECXpert receive or send data using messages that conform to the Java Message Service (JMS) specification. This support is provided through two communications agents—JMS-Receive (`commjms-receive`) and JMS-Send (`commjms-send`). The JMS-Receive communication agent retrieves JMS messages from preconfigured queue destinations on a JMS message service. Similarly, the JMS-Send communication agent sends JMS messages to specified queue destinations on a JMS message service.

This appendix provides information you need to integrate ECXpert with a JMS provider.

- Architectural Overview

- Setting up JMS Support

- Receiving JMS Messages

- Sending JMS Messages

The appendix assumes familiarity with concepts and terminology explained in the JMS 1.0.2 Specification.

Note the following limitations in ECXpert's JMS support:

- It is restricted to retrieval and sending of text messages only.

- It cannot send messages to or retrieve messages from topic destinations.

Architectural Overview

Two ECXpert communications agents—JMS-Receive (`commjms-receive`) and JMS-Send (`commjms-send`)— support the receiving and sending of text by way of JMS messages. These communications agents employ JMS client applications to receive JMS messages from and send JMS messages to a JMS provider.

The architectures employed by these two communications agents are described in the following sections.

JMS-Receive

The architecture for receiving JMS messages by ECXpert is shown in Figure K-1. At startup, the JMS-Receive communications agent spawns a (Java) JMSReceive client application that retrieves and consumes messages from a number of specified queue destinations on a JMS message service. The JMSReceive client runs continuously (so long as the JMS-Receive communications agent process is running), listening for messages that have been placed in the specified queues by any number of ECXpert sending members.

Figure K-1   Architecture for JMS-Receive

The JMSReceive client retrieves messages that have been placed in the specified queues and consumes them (passes them to ECXpert). They are processed by ECXpert based on information found in JMS message property fields within the message, namely: the sending member ID, the receiving member ID, and an ECXpert doctype (see Table K-1 on page 829).

In order to consume JMS messages, the JMSReceive client needs to be able to access the appropriate JMS queue destinations on the appropriate JMS message service. It does this by performing a JNDI lookup of JMS administered objects (QueueConnectionFactory and queue destinations) that reside in a JNDI object store. In order to perform the lookup, JMSReceive needs to know the lookup names of the administered objects as well as JNDI object store properties. This information is provided when you configure the JMS-Receive communications agent (see "Receiving JMS Messages" on page 829).

The JMSReceive client also needs to be authenticated by the JMS message service. A valid user name and password must be provided when you configure the JMS-Receive communications agent.

JMS-Send

The architecture for sending JMS messages from ECXpert is shown in Figure K-2.

Figure K-2   Architecture for JMS-Send

As each JMS message is ready to be sent, the JMS-Send communications agent spawns a (Java) JMSSend client application that sends (produces) the message to a specified queue destination on a JMS message service. Once the message is sent, the JMSSend client shuts down to conserve system resources. However, the JMS-Send communications agent can spawn any number of concurrent JMSSend client applications.

The JMSSend client application produces a message that is destined for a particular receiving member. The member might receive the message directly from a JMS message service or by way of an ECXpert installation. To accommodate the latter, the JMSSend client places information in the message's properties fields that can be used by a remote ECXpert installation to process the message, namely: the sending member ID, the receiving member ID, and an ECXpert doctype (see Table K-1 on page 829).

In order to produce a JMS message, the JMSSend client needs to be able to access the appropriate JMS queue destination on the appropriate JMS message service. It does this by performing a JNDI lookup of JMS administered objects (QueueConnectionFactory and queue destination) that reside in a JNDI object store. In order to perform the lookup, JMSSend needs to know the lookup names of the administered objects as well as JNDI object store properties. This information is provided when you configure the protocol settings for the corresponding ECXpert partnership (see "Sending JMS Messages" on page 834).

The JMSSend client also needs to be authenticated by the JMS message service. A valid user name and password must be provided when you configure the protocol settings for the corresponding ECXpert partnership.

Setting Up JMS Support

ECXpert's JMS support requires coordination among individuals playing the following roles:

- JMS message service administrator
- ECXpert administrator
- developers of JMS client applications (if any)

The tasks each of these individuals must perform are outlined in the following sections.

JMS Message Service Administrator Tasks

The JMS message service administrator sets up and manages the message service supplied by a JMS provider. A JMS administrator must perform the following tasks to support JMS messaging for ECXpert:

1. Configure and start up a message service.

2. If needed, create user name/password repository for authenticating users of the message service (or configure the message service to use an existing user repository).

3. Create a QueueConnectionFactory administered object used to make a connection to the message service and store it in a JNDI object store, typically an LDAP server.

4. Create queue destinations on the message service to be used by ECXpert members to send and/or receive JMS messages processed by ECXpert.

5. Create the corresponding queue destination administered objects and store them in the same JNDI object store as in Step 3.

6. Provide the following information to the ECXpert Administrator:

   ○ valid user names and passwords for accessing the message service.

   ○ JNDI lookup names for the QueueConnectionFactory and queue destination administered objects.

   ○ object store properties (initial context factory, provider URL, and access property values) needed to look up QueueConnectionFactory and queue destination administered objects (see "An Example JNDI Properties File" on page 836).

For information on performing these tasks, consult the documentation supplied by your JMS provider.

ECXpert Administrator Tasks

As an ECXpert administrator there are a number of tasks you must perform to support JMS messaging. These include the following:

1. Configure ECXpert to use your provider-specific JMS implementation.

   You must tell JMS communications agents where the provider-specific JMS jar files reside. See the `jmsvendor_classpath` property of both the JMS-Receive (Table K-2 on page 830) and JMS-Send (Table K-3 on page 833) communications agents. The provider-specific values must be added to the default value.

   iMQ Example:
   ```
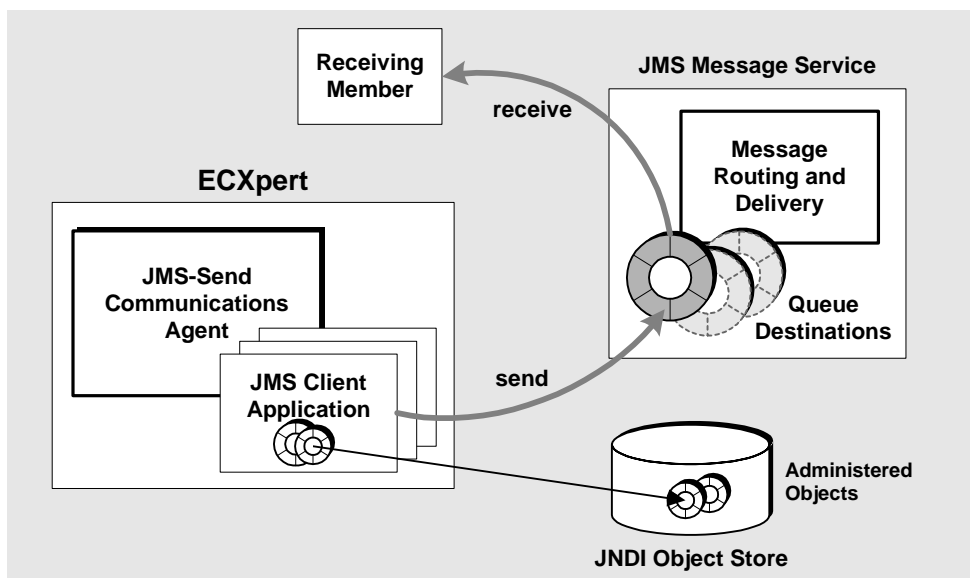   jmsvendor_classpath=
   $NSBASE/NS-apps/ECXpert/bin/jms/jms.jar:/opt/SUNWjmq/lib/jmq.jar
   ```

   (assuming iMQ is installed in `/opt`)

   MQSeries Example:
   ```
   jmsvendor_classpath=
   $NSBASE/NS-apps/ECXpert/bin/jms/jms.jar:/opt/mqm/java/lib/com.
   ibm.mqjms.jar:/opt/mqm/java/lib/com.ibm.mq.jar
   ```

   (assuming MQSeries is installed in `/opt`)

2. Create a JNDI properties file that contains values needed to access the desired JNDI object store.

   See "An Example JNDI Properties File" on page 836.

3. Configure ECXpert for retrieval of JMS messages.

   For real time retrieval of JMS messages, see "Configuring Real Time Retrieval" on page 830. For scheduled retrieval of JMS messages, see "Configuring Scheduled Retrieval" on page 832.

4. Start up the JMS-Receive communications agent (if the Scheduler is not being used to retrieve JMS messages).

   See "Managing ECXpert Servers" on page 131.

5. Start up the JMS-Send communications agent.

   See "Managing ECXpert Servers" on page 131

6. Configure ECXpert for sending JMS messages.

   You must configure the protocol parameters for all partnerships in which the receiving member will be sent data using JMS messaging. See "Sending JMS Messages" on page 834.

JMS Client Application Developer Tasks

A JMS client application developer writes applications that access a JMS message service. Such applications are used by ECXpert members that receive messages directly from a JMS message service or send messages directly to a JMS message service.

There is nothing particularly unique about writing JMS client applications involved in ECXpert partnerships, except for those that produce messages for ECXpert. In this case, the messages produced by the JMS client application must meet two requirements:

*   the message body must be text

*   the message must contain three special message property fields and their corresponding values. These properties, shown in Table K-1, are used by ECXpert to determine the service list for processing the message.

Table K-1   JMS Message Properties Needed by ECXpert

Property Name	Description
MSGSender	Sending member ID
MSGReceiver	Receiving member ID
MSGType	ECXpert doctype

JMS client applications that consume ECXpert messages can also make use of these message properties, since ECXpert includes them in any JMS messages it produces.

Receiving JMS Messages

There are two general approaches to retrieving JMS messages: real time retrieval and scheduled retrieval.

Real time retrieval   In this approach, you configure the JMS-Receive communications agent (see "Configuring Real Time Retrieval" on page 830) and then start it up. the JMS-Receive communications agent spawns a JMSReceive client application which listens for newly arrived messages at all specified queue destinations. These messages are retrieved and consumed by the JMSReceive client and passed to ECXpert for processing. You stop the retrieval of JMS messages at any time by simply shutting down the JMS-Receive communications agent.

Scheduled retrieval   In this approach you do *not* configure the JMS-Receive communications agent because you do not start it up. Instead you set up the ECXpert scheduler, providing it with protocol configuration information that it uses in starting up the JMS-Receive communications agent on a scheduled basis. The agent spawns a JMSReceive client application which retrieves and consumes all messages waiting in a specified queue. When no messages are retrieved for a configurable period of time (see the `timeout` setting of Table K-3 on page 833), the JMS-Receive communications agent is shut down, until the next scheduled retrieval of JMS messages.

Unless there is some specific reason for scheduling message retrieval, you would normally use the real time approach for retrieving messages. The configuration information needed for real time and scheduled retrieval is provided in the following sections.

Configuring Real Time Retrieval

The configuration settings for the JMS-Receive communications agent are specified in the JMS-Receive section of the `exc.ini` file. This section can either be edited by hand or by using the System tab of the ECXpert System Administration Interface. The configuration settings specific to this agent are described in Table K-2.

Table K-2   System Settings for the JMS-Receive Communications Agent

Setting (internal name)	Description	Default Value
jndiPropFile	Path to JNDI properties file that specifies values needed to perform JNDI lookup of JMS administered objects	$NSBASE[1]/NS-apps/ ECXpert/config/ jndi.properties
qcfName	JNDI Lookup name of the QueueConnectionFactory administered object needed to establish a connection to the JMS message service	none
nqueues	Number of queue destinations from which messages will be retrieved	0
q1	JNDI Lookup name of administered object for queue #1	none
q2	JNDI Lookup name of administered object for queue #2	none

Table K-2   System Settings for the JMS-Receive Communications Agent

Setting (internal name)	Description	Default Value
qn	JNDI Lookup name of administered object for queue #n, where n is the value of nqueues	none
jmsuser	User ID needed for authentication with the JMS message service upon establishing a connection	none
jmspasswd	User password needed for authentication with the JMS message service upon establishing a connection (use the bdgsetpasswd utility to set this value)	none
ID	An initial number that is incremented to provide a unique name to each message consumed	1
classpath	CLASSPATH variable for the JVM that includes the ecxsdkjni.jar and ecxjms.jar	$NSBASE/NS-apps/ ECXpert/...
jmsvendor_classpath	Variable for the JVM that specifies the provider-specific JMS-implementation libraries (jms.jar)	$NSBASE/NS-apps/ ECXpert/bin/jms/ jms.jar
libpath	LD_LIBRARY_PATH for the JVM (should not be changed)	$NSBASE/NS-apps/ ECXpert/lib/
javaLog	Path to log file that will be created to monitor message retrieval by the JMSReceive client application	$NSBASE/NS-apps/ ECXpert/data/log/ javaJMSReceive.log
workdir	Path to directory where temporary files are stored	/tmp

1. $NSBASE is the value of an environment variable that sets the ECXpert installation path

Configuring Scheduled Retrieval

The settings for scheduled retrieval are configured using the Scheduler tab of the ECXpert System Administration Interface (see "Scheduling ECXpert Jobs" on page 155). Unlike real time retrieval, a scheduled retrieval task can only check a single queue. To check more queues you have to schedule additional retrieval tasks.

The JMS settings you have to specify for each scheduled JMS retrieval task are similar to settings of the JMS-Receive communications agent (Table K-2 on page 830) as shown in Figure K-3.

Figure K-3   Settings for Scheduled Retrieval of JMS Messages

Scheduled retrieval depends upon internal ECXpert mechanisms governed by the JMS-Send (*not* the JMS-Receive) communications agent. Hence, to use scheduled retrieval, you have to configure the JMS-Send communications agent using settings in the JMS-Send section of the ecx.ini file (and you have to start up the JMS-Send communications agent).

This section can either be edited by hand or by using the System tab of the ECXpert System Administration Interface. The configuration settings specific to this agent are described in Table K-3. In particular, the timeout setting is required to tell the system when to no longer listen for new messages.

Table K-3   System Settings for the JMS-Send Communications Agent

Setting (internal name)	Description	Default Value
timeout	The timeout period in seconds of the JMS message listener—the length of time the system will wait for the next message before shutting down JMS scheduled message retrieval (minimum value is 11)	11
classpath	CLASSPATH variable for the JVM that includes the ecxsdkjni.jar and ecxjms.jar	$NSBASE[1]/NS-apps/ ECXpert/...
jmsvendor_classpath	Variable for the JVM that specifies the provider-specific JMS-implementation libraries (jms.jar)	$NSBASE/NS-apps/ ECXpert/bin/jms/ jms.jar
libpath	LD_LIBRARY_PATH for the JVM (should not be changed)	$NSBASE/NS-apps/ ECXpert/lib/
JMS_LogDir	Path to log file that will be created to monitor message production by the JMSSend application	$NSBASE/NS-apps/ ECXpert/data/log/ javaJMSSend.log
scheduledjms_logDir	Path to log file that will be created to monitor scheduled JMS tasks	$NSBASE/NS-apps/ ECXpert/data/log/ scheduledJMS.log
workdir	Path to directory where temporary files are stored	/tmp

1. $NSBASE is the value of an environment variable that sets the ECXpert installation path

Sending JMS Messages

Sending JMS messages is relatively straight forward. You can use a real time send operation or schedule your JMS sends.

Before you can send JMS messages, you need to configure the JMS-Send communications agent. The settings are shown in Table K-3.

Each JMS message must be sent to a specific JMS message service and a specific queue destination, depending on the receiving ECXpert member in a partnership. Hence, the send operation (whether real time or scheduled) is configured on a partnership by partnership basis, and is performed when creating ECXpert partnerships (see Chapter 6, "Setting Up Trading Partnerships").

The partnership protocol settings used in configuring a JMS send operation are shown in Figure K-4 and specified in Table K-4 on page 835.

Figure K-4   Partnership Protocols Tab for JMS Send

Note in Figure K-4 that you can set Delivery Timing to `immediate` or `scheduled`. If you choose to schedule JMS send operations for a partnership, you have to also create a scheduled task for that partnership (see "Scheduling ECXpert Jobs" on page 155).

Table K-4 Partnership Protocol Settings for JMS Send Operation

Field Name	Description	Default Value
JNDI Properties Filename	Path to JNDI properties file that specifies values needed to perform JNDI lookup of JMS administered objects	$NSBASE[1]/NS-apps/ ECXpert/config/ jndi.properties
Conn Factory	JNDI Lookup name of the QueueConnectionFactory administered object needed to establish a connection to the JMS message service	none
Queue	JNDI Lookup name for the queue to which messages are being sent	none
JMS User ID	User ID needed for authentication with the JMS message service upon establishing a connection	none
Password	User password needed for authentication with the JMS message service upon establishing a connection	none
Expiration	Specifies value (in seconds) to set for the JMSExpiration message header field. A value of zero means message lives forever	0
Priority	Specifies value (1 -10) to set for the JMSPriority message header field. A value of 10 is the highest priority.	4
Delivery Mode	Specifies value (persistent or non-persistent) to set for the JMSDeliveryMode message header field	Persistent

1. $NSBASE is the value of an environment variable that sets the ECXpert installation path

An Example JNDI Properties File

The following example illustrates a JNDI properties file that specifies JNDI object store properties (initial context factory, provider URL, and access property values) needed to look up JMS administered objects.

```
java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory

java.naming.provider.url=ldap://philly.green.iplanet.com:269/
ou=IMQOU,o=iplanet.com

java.naming.security.authentication=simple

java.naming.security.principal=cn=Directory Manager

java.naming.security.credentials=netscape
```

ANSI X12 Group Types and Codes

ANSI X12 Group Types(GS01)

This topic provides a table of ANSI X12 Group Type (GS01) codes for the different ANSI values for Document Type. Use this Appendix as a reference when entering or interpreting values for **Group Type (GS01)** in the **Group Level Information (ANSI)** section of the Input EDI tab. The following topic is presented:

- ANSI X12 Group Type (GS01) for a Given Document Type

ANSI X12 Group Type (GS01) for a Given Document Type

Use the following table to look up the **Group Type (GS01)** in the **Group Level Information (ANSI)** section of the Input EDI tab. This table supplements the instructions given in "Working with the Input EDI Tab" on page 282.

To look up the appropriate Group Type:

- Note the **Document Type** for the partnership that is entered on the Partnership Info tab.

- Look up that Document Type in the **Document Type** column of Table L-1.

- The entry in the column to the right (**Group Type (GS01) Entry**) is the corresponding Group Type to enter in the **Group Type (GS01)** in the **Group Level Information (ANSI)** section of the Input EDI tab.

Table L-1   Group type (GS01) entry for ANSI document type *(1 of 9)*

Document Type	Group Type (GS01) Entry
104	SA
110	IA
120	VC
121	VS
124	VD
125	MR
126	VA
127	VB
128	DI
129	VH
130	ED
131	AK
135	SL
139	SL
140	WA
141	WA
142	WA
143	WA
144	LT
146	RY
147	RZ

Table L-1   Group type (GS01) entry for ANSI document type *(2 of 9)*

Document Type	Group Type (GS01) Entry
148	IJ
149	NT
150	TN
151	TA
152	GR
154	UC
159	MP
161	TR
163	AS
170	ER
175	FC
176	TC
180	AN
185	RD
186	UW
188	EC
189	AF
190	SV
191	SD
194	GT
195	LA
196	PK
197	TO
199	TO
200	MB
201	ML
203	MH
204	SM
206	MG

Table L-1   Group type (GS01) entry for ANSI document type *(3 of 9)*

Document Type	Group Type (GS01) Entry
210	IM
213	MI
214	QM
217	FG
218	FH
242	DS
250	PV
251	CP
255	UI
256	PE
260	MG
261	ME
262	ME
263	PZ
264	MG
265	TO
266	MG
270	HS
271	HB
272	LN
273	ID
275	PI
276	HR
277	HN
278	HI
288	WI
290	CO
300	RO
301	RO

Table L-1   Group type (GS01) entry for ANSI document type *(4 of 9)*

Document Type	Group Type (GS01) Entry
303	RO
304	SO
309	SO
310	IO
311	SO
312	IO
313	QO
315	QO
317	SO
319	SO
322	SO
323	SO
324	SO
325	SO
326	SO
350	SO
352	SO
353	SO
354	SO
355	SO
356	SO
357	SO
358	SO
361	SO
362	OC
404	SR
410	IR
414	CR
417	WB

Table L-1   Group type (GS01) entry for ANSI document type *(5 of 9)*

Document Type	Group Type (GS01) Entry
418	IC
419	SR
420	CH
421	IS
422	DM
423	RL
425	WT
426	SR
429	RU
431	RM
432	RX
433	RG
435	SF
436	LI
440	WR
451	EV
452	PL
453	ST
455	PB
456	EI
466	TP
468	TP
475	RF
485	TP
490	TP
492	TP
494	TP
501	WG
503	PH

Table L-1   Group type (GS01) entry for ANSI document type *(6 of 9)*

Document Type	Group Type (GS01) Entry
504	CC
511	RN
517	MV
527	MD
536	LR
561	D4
567	D3
568	D5
601	SE
602	TS
715	GL
805	CP
806	PJ
810	IN
811	CI
812	CD
813	TF
815	CS
816	OR
818	RP
819	IN
820	RA
821	FR
822	AA
823	LB
824	AG
826	TI
827	FR
828	DA

Table L-1 Group type (GS01) entry for ANSI document type *(7 of 9)*

Document Type	Group Type (GS01) Entry
829	PY
830	PS
831	CT
832	SC
833	ML
834	BE
835	HP
836	RQ
837	HC
838	TD
839	PK
840	RQ
841	SP
842	NC
843	RR
844	CF
845	PA
846	IB
847	MX
848	MS
849	CF
850	PO
851	LS
852	PD
853	RI
854	DD
855	PR
856	SH
857	BS

Table L-1   Group type (GS01) entry for ANSI document type *(8 of 9)*

Document Type	Group Type (GS01) Entry
858	SI
859	FB
860	PC
861	RC
862	SS
863	RT
864	TX
865	CA
866	SQ
867	PT
868	MT
869	RS
870	RS
871	CM
872	PM
875	OG
876	OG
877	CJ
878	QG
879	QG
880	GP
881	CN
882	IG
883	DF
884	MF
885	UA
886	UB
887	CN
888	QG

Table L-1 Group type (GS01) entry for ANSI document type *(9 of 9)*

Document Type	Group Type (GS01) Entry
889	QG
891	UD
893	QG
894	DX
895	DX
896	QG
920	GC
924	GC
925	GC
926	GC
928	AI
940	OW
943	AR
944	RE
945	SW
947	AW
980	(two spaces)
990	GF
996	FT
997	FA
998	AL

Hexadecimal Character Codes

This appendix provides a table of hexadecimal codes for reference when entering or interpreting values in the Delimiters and Separators section of the Output EDI tab. The following topic is presented:

- Hexadecimal Values for Delimiters and Separators

Hexadecimal Values for Delimiters and Separators

Whenever you are working with EDI standard document types in ECXpert, you must specify special characters to delimit various pieces of data. Table M-1 lists the ASCII character codes that you must use to specify these characters.

NOTE	Consult the X12, EDIFACT, or UCS standards documentation to find out what character set is supported by the standard you want to use.
	When entering the Hex value into the ECXpert Partnership Control page, you must omit the "0x" prefix. For example, to specify the greater-than sign, "0x3E", enter only "3E" for the value.

Table M-1   Table of ASCII character codes

		Numeric Code	
Character	**Description**	**Decimal**	**Hexidecimal**
^@	Null (NUL)	0	0x00

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
^A	Start of heading (SOH)	1	0x01
^B	Start of text (STX)	2	0x02
^C	End of text (ETX)	3	0x03
^D	End of tansmission (EOT)	4	0x04
^E	Enquiry (ENQ)	5	0x05
^F	Acknowledge (ACK)	6	0x06
^G	Bell (BEL)	7	0x07
^H	Backspace (BS)	8	0x08
^I	Character (horizontal) tab (HT)	9	0x09
^J	Linefeed (LF)	10	0x0A
^K	Line (vertical) tab (VT)	11	0x0B
^L	Formfeed (FF)	12	0x0C
^M	Carriage Return (CR)	13	0x0D
^N	Shift out (SO)	14	0x0E
^O	Shif in (SI)	15	0x0F
^P	Datalink escape (DLE)	16	0x10
^Q	Device control one (DC1)	17	0x11
^R	Device control two (DC2)	18	0x12
^S	Device control three (DC3)	19	0x13
^T	Device control four (DC4)	20	0x14
^U	Negative acknowledge (NAK)	21	0x15
^V	Synchronous idle (SYN)	22	0x16
^W	End of transmission block (ETB)	23	0x17
^X	Cancel (CAN)	24	0x18
^Y	End of medium (EM)	25	0x19
^Z	Substitute (SUB)	26	0x1A
^[	Escape (ESC)	27	0x1B
^\	File separator (FS, IS4)	28	0x1C

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
^]	Group separator (GS, IS3)	29	0x1D
^^	Record separator (RS, IS2)	30	0x1E
^_	Unit separator (US, IS1)	31	0x1F
	Space	32	0x20
!	Exclamation point	33	0x21
"	Double quote	34	0x22
#	Number sign	35	0x23
$	Dollar sign	36	0x24
%	Percent sign	37	0x25
&	Ampersand	38	0x26
'	Single quote	39	0x27
(	Open parenthesis	40	0x28
)	Close parenthesis	41	0x29
*	Asterisk	42	0x2A
+	Plus sign	43	0x2B
,	Comma	44	0x2C
-	Hyphen, dash, minus sign	45	0x2D
.	Period	46	0x2E
/	Forward slash (solidus)	47	0x2F
0		48	0x30
1		49	0x31
2		50	0x32
3		51	0x33
4		52	0x34
5		53	0x35
6		54	0x36
7		55	0x37
8		56	0x38

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	**Hexidecimal**
9		57	0x39
:	Colon	58	0x3A
;	Semicolon	59	0x3B
<	Less-than	60	0x3C
=	Equal sign	61	0x3D
>	Greater than	62	0x3E
?	Question mark	63	0x3F
@	At sign	64	0x40
A		65	0x41
B		66	0x42
C		67	0x43
D		68	0x44
E		69	0x45
F		70	0x46
G		71	0x47
H		72	0x48
I		73	0x49
J		74	0x4A
K		75	0x4B
L		76	0x4C
M		77	0x4D
N		78	0x4E
O		79	0x4F
P		80	0x50
Q		81	0x51
R		82	0x52
S		83	0x53
T		84	0x54

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
U		85	0x55
V		86	0x56
W		87	0x57
X		88	0x58
Y		89	0x59
Z		90	0x5A
[	Open square bracket	91	0x5B
\	Backslash (reverse solidus)	92	0x5C
]	Close square bracket	93	0x5D
^	Caret, grave accent	94	0x5E
_	Underscore	95	0x5F
'	Apostrophe	96	0x60
a		97	0x61
b		98	0x62
c		99	0x63
d		100	0x64
e		101	0x65
f		102	0x66
g		103	0x67
h		104	0x68
i		105	0x69
j		106	0x6A
k		107	0x6B
l		108	0x6C
m		109	0x6D
n		110	0x6E
o		111	0x6F
p		112	0x70

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
q		113	0x71
r		114	0x72
s		115	0x73
t		116	0x74
u		117	0x75
v		118	0x76
w		119	0x77
x		120	0x78
y		121	0x79
z		122	0x7A
{	Open curly bracket	123	0x7B
|	Piping symbol, vertical line	124	0x7C
}	Close curly bracket	125	0x7D
~	Tilde	126	0x7E
^?	Delete (DEL)	127	0x7F
M-^@		128	0x80
M-^A		129	0x81
M-^B		130	0x82
M-^C		131	0x83
M-^D		132	0x84
M-^E		133	0x85
M-^F		134	0x86
M-^G		135	0x87
M-^H		136	0x88
M-^I		137	0x89
M-^J		138	0x8A
M-^K		139	0x8B
M-^L		140	0x8C

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
M-^M		141	0x8D
M-^N		142	0x8E
M-^O		143	0x8F
M-^P		144	0x90
M-^Q		145	0x91
M-^R		146	0x92
M-^S		147	0x93
M-^T		148	0x94
M-^U		149	0x95
M-^V		150	0x96
M-^W		151	0x97
M-^X		152	0x98
M-^Y		153	0x99
M-^Z		154	0x9A
M-^[		155	0x9B
M-^\		156	0x9C
M-^]		157	0x9D
M-^^		158	0x9E
M-^_		159	0x9F
		160	0xA0
¡		161	0xA1
¢		162	0xA2
£		163	0xA3
¤		164	0xA4
¥		165	0xA5
			166	0xA6
§		167	0xA7
¨		168	0xA8

Table M-1 Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	**Hexidecimal**
©		169	0xA9
ª		170	0xAA
«		171	0xAB
¬		172	0xAC
		173	0xAD
®		174	0xAE
¯		175	0xAF
°		176	0xB0
		177	0xB1
		178	0xB2
		179	0xB3
´		180	0xB4
		181	0xB5
¶		182	0xB6
·		183	0xB7
¸		184	0xB8
		185	0xB9
		186	0xBA
»		187	0xBB
		188	0xBC
		189	0xBD
		190	0xBE
¿		191	0xBF
À		192	0xC0
Á		193	0xC1
Â		194	0xC2
Ã		195	0xC3
Ä		196	0xC4

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
Å		197	0xC5
Æ		198	0xC6
Ç		199	0xC7
È		200	0xC8
É		201	0xC9
Ê		202	0xCA
Ë		203	0xCB
Ì		204	0xCC
Í		205	0xCD
Î		206	0xCE
Ï		207	0xCF
		208	0xD0
Ñ		209	0xD1
ò		210	0xD2
ó		211	0xD3
ô		212	0xD4
õ		213	0xD5
ö		214	0xD6
x		215	0xD7
Ø		216	0xD8
Ù		217	0xD9
Ú		218	0xDA
Û		219	0xDB
Ü		220	0xDC
		221	0xDD
		222	0xDE
ß		223	0xDF
à		224	0xE0

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	Hexidecimal
á		225	0xE1
â		226	0xE2
ã		227	0xE3
ä		228	0xE4
å		229	0xE5
æ		230	0xE6
ç		231	0xE7
è		232	0xE8
é		233	0xE9
ê		234	0xEA
ë		235	0xEB
ì		236	0xEC
í		237	0xED
î		238	0xEE
ï		239	0xEF
		240	0xF0
ñ		241	0xF1
ò		242	0xF2
ó		243	0xF3
ô		244	0xF4
õ		245	0xF5
ö		246	0xF6
		247	0xF7
ø		248	0xF8
ù		249	0xF9
ú		250	0xFA
û		251	0xFB
ü		252	0xFC

Table M-1   Table of ASCII character codes

Character	Description	Numeric Code	
		Decimal	**Hexidecimal**
		253	0xFD
		254	0xFE
ÿ		255	0xFF

Hexadecimal Values for Delimiters and Separators

Mapping UI Fields to Database Columns and Import Fields

This appendix indicates each field on the ECXpert user interface as well as the database column in which data for that field is stored. It also indicates the field that should be used to import data into that database column using the ECXpert `import` utility.

For more details about the member, partnership, service, and service list tabs on the ECXpert user interface, see "Working with the Membership Definition Tabs" on page 207, "Working with the Partnership Definition Tabs" on page 266, and "Working with the Service Details Tab" on page 474.

For more details about the ECXpert database schema, see the *iPlanet ECXpert Developer's Guide*, Appendix A, "ECXpert Database Schema."

For more details about the ECXpert `import` utility, see "import—Importing Records for Members, Partnerships, or Service Lists" on page 494.

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(1 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Membership Information Tab				
Member ID		Members.MBName		Object=member
				Field=Name
Password		Members.MBPassword (encrypted)		Object=member
				Field=Password
Description		Members.MBInfoSource		Object=member
				Field=Description
Confirm Password		N/A		N/A
TradingXpert Read Window (days)		MBReadSpan		N/A
Member is active	Checked=yes	Members.MBActive	1=yes	Object=member
	Not checked=no		0=no	Field=Active
Member is trusted	Checked=yes	Members.MBtrusted	1=yes	Object=member
	Not checked=no		0=no	Field=Trusted
Member is Administrator	Checked=yes	Members.MBType	0=MBTunknown 1=MBTsysAdmin	Object=member
	Not checked=no			Field=Type
Membership Contact Information Tab				
Full Name		Members.MBContactName		Object=member
				Field=ContactName
Company Name		Members.MBContactDesc		Object=member
				Field=ContactCompany

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(2 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Address 1		Members.MBContactAddress1		Object=member Field=ContactAddress1
Address 2		Members.MBContactAddress2		Object=member Field=ContractAddress2
City		Members.MBContactCity		Object=member Field=ContactCity
State		Members.MBContactState		Object=member Field=ContactState
Zip		Members.MBContactZip		Object=member Field=ContactZip
Country		Members.MBContactCountry		Object=member Field=ContactCountry
Phone		Members.MBContactPhone		Object=member Field=ContactPhone
Fax		Members.MBContactFax		Object=member Field=ContactFax
Email		Members.MBContactEmailId		Object=member Field=ContactEmailId

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns
and to import fields *(3 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Membership Trading Addresses Tab				
Address Type	EDI	MBAddresses. MBName	Field=Qual:	Object=mbaddress
	Local E-mail		*YourEDIQualifier*=EDI (any value other than "EL" or "ER")	Field=Member
	Remote E-maill	*and*		*and*
Qualifier	According to Address Type selected:	MBAddresses. MBAQual	EL=Local E-mail	Object=mbaddress
			ER=Remote E-mail	Field=Qual
	EDI=*YourEDIQualifier*			
	EL=Local E-mail			
	ER=Remote E-mail			
Address		MBAddresses. MBAQualId		Object=mbaddress
				Field=QualId
Partnership Info Tab				
Sending Member		Partnerships.PNSndrMBName		Object=partnership
				Field=SenderName
Receiving Member		Partnerships.PNRcvrMBName		Object=partnership
				Field=ReceiverName

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Partnership Type	Application to Application Application to EDI EDI to Application EDI to EDI	PNDocs.PDMapDirection	0=XLTunknown 1= XLTinbound (EDI-to-Application) 2=XLToutbound (Application-to-EDI) 3=XLTedi2edi (EDI-to-EDI) 4=XLTapp2app (Application-to-Application) 5=XLTnoxlat (None; pass-throughmode)	Object=partnership Field=MapDirection
Document Type		PNDocs.PDDocType		Object=partnership Field=DocType
Partnership Description		Partnerships.PNDesc		Object=partnership Field=Description
Do not purge for (days)		PNDocs.PDDeleteWait		Object=partnership Field=DeleteWaitPeriod
Enable Trading vs. Disable Trading	Selected=yes Not selected=no	Partnerships.PNActive	1=yes (enable) 0=no (disable)	Object=partnership Field=Active

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns
and to import fields *(5 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Map Name		PNDocs.PDMapName		Object=partnership Field=MapName Note: The Import utility does not verify if the specified map exists in the maps directory. If it does not exist, documents sent using the partnership will not be translated.
Sender Certificate Type	None Self-Signed Certificate VeriSign Class 2 VeriSign Class 3 Verisign Class 1	Partnerships.PNSndrCertType	0=CTUnknown 1=CTSelf 2=CTVerisignC3 3=CTVerisignC2 4=CTVerisignC1 5=Other CA root(s) user imports	Object=partnership Field=SenderCertificateType
Receiver Certificate Type		Partnerships.PNRcvrCertType	0=CTUnknown 1=CTSelf 2=CTVerisignC3 3=CTVerisignC2 4=CTVerisignC1 5=Other CA root(s) user imports	Object=partnership Field=ReceiverCertificateType
Encryption and Authentication	Not Signed or Encrytped (Plain) Encrypted Only Signed Only Signed and Encrypted	Partnerships.PNSecurity	0=Plain MIME (send as base64 encoding only) 1=Encrypted 2=Signed 3=SignedAndEncrypted (signed, then encrypted)	Object=partnership Field=Security

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(6 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Partnership Outputs Tab				
ID		PNCard.PDDPGId		N/A
Sender		PNCard.PDDSdrMBName		N/A
Receiver		PNCard.PDDRcvrMBName		N/A
Doc Type		PNCard.PDDDocType		N/A
Partnership Input EDI Tab				
Sender Qualifier ID		Partnerships.PNSndrQualId		Object=partnership Field=SenderQualId
Receiver Qualifier ID		Partnerships.PNRcvrQualId		Object=partnership Field=ReceiverQualId
Standard	ANSI EDIFACT	PNStd.PSStandard	X=ANSI UN=EDIFACT	Object=partnership Field=StandardName
Functional ID Code (GS01)-ANSI only		PNGroup.PGGroupType		Object=partnership Field=GroupType
Group Version (GS08)-ANSI only		PNStd.PSVersion		Object=partnership Field=StandardVersion
Use App Codes to locate parnerships-ANSI only	Checked=yes Not checked=no	N/A	N/A	N/A
App Sender (GS02)-ANSI only		PNGroup.PGSndrAppCode		Object=partnership Field=SndrAppCode

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(7 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
App Receiver (GS03)-ANSI only		PNGroup.PGRcvrAppCode		Object=partnership Field=RcvrAppCode
Generate FA-ANSI only	Never Always On Errors Only	PNGroup.PGGenDocAck	0=Never 248=Always,Transaction Set, Element	Object=partnership Field=GroupGenerateDocAck
FA Level-ANSI only	Functional Groups Transaction Set		120=Always, Transaction Set, Segment 56=Always, Transaction Set, Transaction Set	
Error Reporting Level-ANSI only	Transaction Set Segment Element		232=Always, Functional Groups, Element 104=Always, Functional Groups, Segment 40=Always, Functional Groups, Transaction Set 250=On Errors, Transaction Set, Element 122=On Errors, Transaction Set, Segment 58=On Errors, Transaction Set, Transaction Set 234=On Errors, Functional Groups, Element 106=On Errors, Functional Groups, Segment 42=On Errors, Functional Groups, Transaction Set	
Comment Type-ANSI only		PNDocs.PDMapComment-SegId		N/A

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(8 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Message Version Number (UNG-S008-0054)-EDIFACT only		PNStd.PSVersion		Object=partnership Field=StandardVersion
Message Release Number (GS08)-EDIFACT only		PNStd.PSRelease		Object=partnership Field=StandardRelease
Use UNG to locate partnerships-EDIFACT only	Checked=yes Not checked=no	N/A	N/A	N/A
App Sender Code (UNG-S006-0040)-EDIFACT only		PNGroup.PGSndrAppCode		Object=partnership Field=SndrAppCode
App Receiver Code (UNG-S007-0044)-EDIFACT only		PNGroup.PGRcvrAppCode		Object=partnership Field=RcvrAppCode
App Sender Code Qual (UNG-S006-0007)-EDIFACT only		PNGroup.PGSndrQual		Object=partnership Field=SndrAppQual
App Receiver Code Qual (UNG-S007-0007)-EDIFACT only		PNGroup.PGRcvrQual		Object=partnership Field=RcvrAppQual

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Generate CONTRL-EDIFACT only	Never Always On Errors Only	PNStd.PSGenIntgAckFlags	Field=IntchgGenerateAck: 0=Never 16=Always	Object=partnership Field=IntchgGenerateAck *and*
Response Level-EDIFACT only	Message		22=On Errors Only *and* Field=GroupGenDocAck: 0=Never 0=Always 0=On Errors Only	Object=partnership Field=GroupGenDocAck
Partnership Input HREC Tab				
Sender Qualifier ID		Partnerships.PNSndrQualId		Object=partnership Field=SenderQualId
Receiver Qualifier ID		Partnerships.PNRcvrQualId		Object=partnership Field=ReceiverQualId
Standard	ANSI EDIFACT	PNStd.PSStandard	X=ANSI UN-EDIFACT	Object=partnership Field=StandardName
App Sender (GS02)-ANSI only		PNGroup.PGSndrAppCode		Object=partnership Field=SndrAppCode
App Receiver (GS03)-ANSI only		PNGroup.PGRcvrAppCode		Object=partnership Field=RcvrAppCode
Functional ID Code (GS01)-ANSI only		PNGroup.PGGroupType		Object=partnership Field=GroupType

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(10 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Group Version (GS08)-ANSI only		PNStd.PSVersion		Object=partnership Field=StandardVersion
App Sender ID (UNG-S006-0040)-EDIFACT only		PNGroup.PGSndrAppCode		Object=partnership Field=SndrAppCode
App Receiver ID (UNG-S007-0044)-EDIFACT only		PNGroup.PGRcvrAppCode		Object=partnership Field=RcvrAppCode
App Sender ID Qual (UNG-S006-0007)-EDIFACT only		PNGroup.PGSndrQual		Object=partnership Field=SndrAppQual
App Receiver ID Qual (UNG-S007-0007)-EDIFACT only		PNGroup.PGRcvrQual		Object=partnership Field=RcvrAppQual
Message Version (UNG-S008-0054)-EDIFACT only		PNStd.PSVersion		Object=partnership Field=StandardVersion
Message Release (GS08)-EDIFACT only		PNStd.PSRelease		Object=partnership Field=StandardRelease
Partnership Output EDI Tab				

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(11 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
EDI Envelope	Pre-Enveloped (ECX does not touch envelope data)	PNDocs.PDPreEnveloped	0=PEunknown	Object=partnership
			1=PEenveloped (bundle preserves all envelopes)	Field=PreEnveloped
	ECX Generates (or overrides) entire envelope		2=PEnonenveloped (bundle generates and/or replaces all envelopes)	
	Use optional elements and Ctrl/Msg Ref# from data		3=PEpreenvelopedEDI (not used)	
			4=PEGetCtrlNo (Bundle only supplies the control number and preserves everything else in envelope)	
	Use optional elements from data but ECX generates Ctrl/Msg Ref#		5=PEPreserveCtrlNo (Bundle only preserves the envelope control number)	

Partnership Output EDI Tab—ECX generates (or overrides) entire envelope

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Standard	ANSI	PNStd.PSOutStandard	X=ANSI	Object=partnership
	EDIFACT		UN=EDIFACT	Field=OutStandard
Interchange Version (ISA 12)-ANSI only		PNStd.PSOutVersion		Object=partnership
				Field=OutVersion
Version Number (UNH-S009-0052)-EDIFACT only		PNStd.PSOutVersion		Object=partnership
				Field=OutVersion
Release Number (UNH-S009-0054)-EDIFACT only		PNStd.PSOutRelease		Object=partnership
				Field=OutRelease
Interchange		PNStd.PSLastIntgCtrlNum		Object=partnership
				Field=IntchngLastControlNumber

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns
and to import fields *(12 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Group		PNGroup.PGLastGroupCtrlNum		Object=partnership
				Field=GroupLastControlNumber
Document		PNDocs.PDLastCtrlNum		Object=partnership
				Field=DocLastControlNumber
Generate UNA-EDIFACT only	Checked=yes	Partnerships.PNGenOptEnv	0=No UNA, No UNG	Object=partnership
	Not checked=no		1=UNA only	Field=GenOptEnv
			2=UNG only	
			3=UNA and UNG	
FA (997) Expected?-ANSI only		PNDocs.PDAckExpected	1=yes	Object=partnership
			0=no	Field=AckExpected
FA overdue in (minutes)-ANSI only		PNDocs.PDAckWait		N/A
CONTRL Message Expected?-EDIFACT only		PNDocs.PDAckExpected	1=yes	Object=partnership
			0=no	Field=AckExpected
CONTRL overdue in (minutes)-ANSI only-EDIFACT only		PNDocs.PDAckWait		N/A
Segment Terminator (hex value)		PNStd.PSSegTerm		Object=partnership
				Field=SegmentTerminator
Release Character (hex value)-EDIFACT only		PNStd.PSRelChar		Object=partnership
				Field=ReleaseCharacter
Sub-Element Delimiter (hex value)		PNStd.PSSubElmtSep		Object=partnership
				Field=SubElementSeparator

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns
and to import fields *(13 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Decimal Notation (hex value)-EDIF ACT only		PNStd.PSDecPt Char		Object=partnership Field=DecimalPoint Character
Element Delimiter (hex value)		PNStd.PSElmtS ep		Object=partnership Field=ElementSepa rator
Test or Production	Production Test	PNStd.PSTestPr odFlag	0=TPFunknown 1=TPFproduction 2=TPFtest	Object=partnership Field=TestProducti onFlag
Generate UNG	Checked=yes Not checked=no	Partnerships.P NGenOptEnv	0=No UNA, No UNG 1=UNA only 2=UNG only 3=UNA and UNG	Object=partnership Field=GenOptEnv
Partnership Output EDI Tab—Use optional elements and Ctrl/Msg Ref# from data				
Standard	ANSI EDIFACT	PNStd.PSStand ard	X=ANSI UN=EDIFACT	Object=partnership Field=OutStandard
Interchange Version (ISA 12)-ANSI only		PNStd.PSOutSt andard		Object=partnership Field=OutVersion
Version Number (UNH-S009-0052)- EDIFACT only		PNStd.PSOutV ersion		Object=partnership Field=OutVersion
Release Number (UNH-S009-0054)- EDIFACT only		PNStd.PSOutR elease		Object=partnership Field=OutRelease
Segment Terminator (hex value)		PNStd.PSSegTe rm		Object=partnership Field=SegmentTer minator

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(14 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Release Character (hex value)-EDIF ACT only		PNStd.PSRelChar		Object=partnership Field=ReleaseCharacter
Sub-Element Delimiter (hex value)		PNStd.PSSubElmtSep		Object=partnership Field=SubElementSeparator
Decimal Notation (hex value)-EDIF ACT only		PNStd.PSDecPtChar		Object=partnership Field=DecimalPointCharacter
Element Delimiter (hex value)		PNStd.PSElmtSep		Object=partnership Field=ElementSeparator
Test or Production-ANSI only	Production Test	PNStd.PSTestProdFlag	0=TPFunknown 1=TPFproduction 2=TPFtest	Object=partnership Field=TestProductionFlag
Partnership Output EDI Tab—Use optional elements from data but ECX generates Ctrl/Msg Ref#				
Standard	ANSI EDIFACT	PNStd.PSOutStandard	X=ANSI UN=EDIFACT	Object=partnership Field=OutStandard
Interchange		PNStd.PSLastIntgCtrlNum		Object=partnership Field=IntchngLastControlNumber
Group		PNGroup.PGLastGroupCtrlNum		Object=partnership Field=GroupLastControlNumber
Document		PNDocs.PDLastCtrlNum		Object=partnership Field=DocLastControlNumber

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(15 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Generate UNA-EDIFACT only	Checked=yes Not checked=no	Partnerships.PNGenOptEnv	0=No UNA, No UNG 1=UNA only 2=UNG only 3=UNA and UNG	Object=partnership Field=GenOptEnv
FA (997) Expected?-ANSI only		PNDocs.PDAckExpected		Object=partnership Field=AckExpected
FA overdue in (minutes)-ANSI only		PNDocs.PDAckWait		N/A
CONTRL Message Expected?-EDIFACT only		PNDocs.PDAckExpected		Object=partnership Field=AckExpected
CONTRL overdue in (minutes)-ANSI only-EDIFACT only		PNDocs.PDAckWait		N/A
Segment Terminator (hex value)		PNStd.PSSegTerm		Object=partnership Field=SegmentTerminator
Release Character (hex value)-EDIFACT only		PNStd.PSRelChar		Object=partnership Field=ReleaseCharacter
Sub-Element Delimiter (hex value)		PNStd.PSSubElmtSep		Object=partnership Field=SubElementSeparator
Decimal Notation (hex value)-EDIFACT only		PNStd.PSDecPtChar		Object=partnership Field=DecimalPointCharacter
Element Delimiter (hex value)		PNStd.PSElmtSep		Object=partnership Field=ElementSeparator

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(16 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Test or Production-ANSI only	Production Test	PNStd.PSTestProdFlag	0=TPFunknown 1=TPFproduction 2=TPFtest	Object=partnership Field=TestProductionFlag
Partnership Protocols Tab				
Outgoing Protocol	POLL HTTP Receive SMTP FTP GEIS FTP Odette FTP (OFTP) HTTP for AIAG HTTP for GISB HTTP SSL eXML Connector Legacy Server (Oracle) Legacy Server (SAP) Legacy Server (MQ Series)	PNDocs.PD1stXportType	retrieve= POLL http-retrieve= HTTP Receive commsmtp-send= SMTP ftp-local-application=local FTP (application) ftp-local-edi= FTP (EDI) comm_ftp_geis= GEIS FTP commhttp-aiag= HTTP AIAG commhttp-gisb= HTTP GISB ecxoftp-server= Odette FTP (OFTP) eXML-connector= eXML Connector legacy-oracle-apps=Legacy Server (Oracle) legacy-sap= Legacy Server (SAP) legacy-mq-series=Legacy Server (MQ Series) Note: The following subsections list parameters for each value.	Object=partnership Field=PrimaryXportType

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns
and to import fields *(17 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Partnership Protocols Tab—POLL (PNDocs.PD1stXportType=retrieve)				
N/A	N/A	N/A	N/A	N/A
Partnership Protocols Tab—HTTP Receive (PNDocs.PD1stXportType=http-retrieve)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A
Partnership Protocols Tab—SMTP (PNDocs.PD1stXportType=commsmtp-send)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
MDN Requested	No MDN	[encrypted]	MR|*MDN_Requested*;	N/A
	Plain MDN (default)		0=No MDN	
			1=Plain MDN,	
	Signed MDN		2=Signed MDN	
MIME Sub-Type Override (optional)	EDI-X12	[encrypted]	MT|*Mime_subtype*;	N/A
	EDIFACT			
	application			

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Process Method	Not Signed or Encrypted Encrypted Only Signed Only Signed and Encrypted	Partnerships.PNSecurity	PR	*ProcessMethod*; 0=SimpleMime 1=Encrypted Only 2=Signed Only 3=Signed and Encrypted If PR	1, 2, or 3, also use these parameters: CS	*senderCertType*; 0=CTUnknown 1=CTSelf 2=CTVerisignC3 3=CTVerisignC2 4=CTVerisignC1 5=Other CA root(s) user imports CR	*receiverCertType;* (same values as for CS | *senderCertType;*) KL	*Key_length*; 56, 64, 75, 128, 255 MA	*MIC_Algorithm*; 28=SHA_1 5=MD5	N/A
Partnership Protocols Tab—FTP **(PNDocs.PD1stXportType=ftp-local-application or =ftp-local-edi)**				
Pre-Commuications Service		PNDocs.PDPreCommSVRId		N/A

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(19 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Host Name		[encrypted]	HN | *hostname*; (name or IP address)	N/A
Port		[encrypted]	PT | *portnumber*; (Optional)	N/A
User Name		[encrypted]	UN | *username*;	N/A
Account		[encrypted]	AC | *account number* (Required if host requires it)	N/A
Password		[encrypted]	PW | *userPassword*;	N/A
Confirm Password		N/A	N/A	N/A
Outbound Transfer Mode	Binary	[encrypted]	MD | *transfer mode*	N/A
	ASCII		A=ASCII	
			I=Binary	
Outbound Dir		[encrypted]	OD | *outboundDirectory*;	N/A
Outbound Pattern		[encrypted]	SS | *SendPattern*;	N/A
Inbound Dir		[encrypted]	ID | *InboundDirectory*;	N/A
Inbound Pattern		[encrypted]	RS | *ReceivePattern*;	N/A
Inbound File Type		[encrypted]	IT | *InboundFileType*;	N/A
Partnership Protocols Tab—GEIS FTP (PNDocs.PD1stXportType=comm_ftp_geis)				
Pre-Commuications Service		PNDocs.PDPreCommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(20 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Operation	Send and Receive	[encrypted]	OO | *operation*;	N/A
	Send Only		sendrecv=send and receive	
	Receive Only		send=send	
			recv=receive	
Host Name		[encrypted]	HN | *hostname*; (name or IP address)	N/A
Port		[encrypted]	PT | *portnumber*; (Optional)	N/A
User Name		[encrypted]	UN | *username*;	N/A
Password		[encrypted]	PW | *userPassword*;	N/A
Confirm Password		N/A	N/A	N/A
Partnership Protocols Tab—Odette FTP (OFTP) (PNDocs.PD1stXportType=ecxoftp-server)				
Pre-Commuications Service		PNDocs.PDPreCommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
User Name		[encrypted]	OU | *username*;	N/A
Password		[encrypted]	OL | *userPassword;*	N/A
Confirm Password		N/A	N/A	N/A
Transport Method	X.25	[encrypted]	OX | *transportMethod*;	N/A
	X.28		X.25	
	TCP/IP		X.28	
			TCP/IP	
Destination X.121 Address-X.25 only		[encrypted]	XN | *destination_X.121Address*; (Optional)	N/A
			Defaults to local network user address	

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(21 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Facility Information-X.25 only		[encrypted]	XF | *X.25 FacilityInformation*; (Optional)	N/A
Logical Channel Number -X.25 only		[encrypted]	XL | *LogicalChannelNumber*; Optional)	N/A
Routing Entry-X.25 only		[encrypted]	XR | *RoutingEntry*; (Optional)	N/A
Call User Data-X.25 only		[encrypted]	XC | *CallUserData* (Optional)	N/A
Telephone Number-X.28 only		[encrypted]	XT | *X.28 Tel number*; (Optional)	N/A
PAD Password-X.28 only		[encrypted]	XY | *X.28 PAD user password*; (Optional)	N/A
Connection Script-X.28 only		[encrypted]	XS | *X.28 Connection script pathname*;	N/A
Confirm PAD Password-X.28 only		N/A	N/A	N/A
PAD Username-X.28 only		[encrypted]	XU | *X.28 PAD user name*; (Optional)	N/A
Destination X.121 Address-X.28 only		[encrypted]	XZ | *X.28 destination NUA*; (Optional; numeric network user address)	N/A
Destination Address-TCP/IP only		[encrypted]	TH | *TCP/IP destination host* (Optional; name or IPaddress) Defaults to local hostname	N/A
Destination Port-TCP/IP only		[encrypted]	TX | *TCP/IP destination port*; (Optional) Defaults to 3305	N/A

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(22 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Partnership Protocols Tab—HTTP for AIAG (PNDocs.PD1stXportType=commhttp-aiag)				
Pre-Commuications Service		PNDocs.PDPreCommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Sender		[encrypted]	SS|*sender*;	N/A
Host Name		[encrypted]	HN|*hostname*; (name or IP address)	N/A
Receiver		[encrypted]	RR|*receiver*;	N/A
Port		[encrypted]	PT|*portnumber*; (Optional)	N/A
Application		[encrypted]	AN|*application type*; (e.g., EDI, application, etc.)	N/A
User Name		[encrypted]	UN|*username*;	N/A
User Parameter		[encrypted]	UP|*user parameter*; (Optional)	N/A
Password		[encrypted]	PW|*password*;	N/A
Login CGI Pathname (including filename)		[encrypted]	PL|*login cgi-pathname*;	N/A
Confirm Password		N/A	N/A	N/A
Deliver CGI Pathname (including filename)		[encrypted]	OO|DELIVER;PD|*deliver cgi-pathname;*	N/A
Reference Number		[encrypted]	RN|*reference number*; (Optional)	N/A

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns
and to import fields *(23 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Obtain CGI Pathname (including filename)		[encrypted]	OO	OBTAIN; PO	*obtain cgi-pathname*;	N/A
Note: Must be set up in UI using the scheduler				
Partnership Protocols Tab—HTTP GISB (PNDocs.PD1stXportType=commhttp-gisb)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSen dType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Password		[encrypted]	PW	*password*;	N/A
Host Name		[encrypted]	HN	*hostname*; (name or IP address)	N/A
Confirm Password		N/A	N/A	N/A
Port		[encrypted]	PT	*portnumber*; (Optional)	N/A
From		[encrypted]	SS	*sender*;	N/A
Operation		[encrypted]	OO	*operation*; (DELIVER)	N/A
To		[encrypted]	RR	*receiver*;	N/A
User Name		[encrypted]	UN	*username*;	N/A
Input Format		[encrypted]	I F	*input format*; (e.g., EDI, application, etc.)	N/A
Deliver CGI Pathname (including filename)		[encrypted]	PD	*deliver cgi-pathname*;	N/A
Partnership Protocols Tab—HTTP SSL (PNDocs.PD1stXportType=commhttp-ssl)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(24 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Host Name		[encrypted]	HN|*hostname*; (name or IP address)	N/A
Port		[encrypted]	PT|*portnumber*; (Optional)	N/A
CGI Path		[encrypted]	PN|*cgi pathname*;	N/A
Sender		[encrypted]	SE|*sender*;	N/A
Password		[encrypted]	PW|*password*;	N/A
Confirm Password	N/A	N/A	N/A	N/A
Receiver		[encrypted]	RE|*receiver*;	N/A
File Type		[encrypted]	FT|*file type*;	N/A
Sender Certificate Type		[encrypted]	CY|*certificate type*	N/A
Partnership Protocols Tab—eXML Connector (PNDocs.PD1stXportType=eXML-connector)				
Pre-Commuications Service		PNDocs.PDPreCommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Hostname		[encrypted]	HN|*hostname*; (name or IP address)	N/A
Port		[encrypted]	PT|*portnumber*; (Optional)	N/A
Information File Path		[encrypted]	AI|*informationFilePath*; (path and filename)	N/A
File Transport		[encrypted]	XT|*fileTransport*;	N/A
			file=transmit filename only	
			stream=transmit entire file	

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(25 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Partnership Protocols Tab—Legacy Server (Oracle) (PNDocs.PD1stXportType=legacy-oracle-apps)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSen dType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Map Name		[encrypted]	MN|*map name;*	N/A
Database Name		[encrypted]	DB|*database name;*	N/A
User Name		[encrypted]	UN|*username;*	N/A
Password		[encrypted]	PW|*password;*	N/A
Confirm Password	N/A	N/A	N/A	N/A
Partnership Protocols Tab—Legacy Server (SAP) (PNDocs.PD1stXportType=legacy-sap)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A
Delivery Timing	Immediate	PNDocs.PDSen dType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Client Number		[encrypted]	CN|*client number;*	N/A
User ID		[encrypted]	UI|*user id;*	N/A
Password		[encrypted]	PW|*password;*	N/A
Confirm Password	N/A	N/A	N/A	N/A
RFC Section Key		[encrypted]	RK|*SD1;*	N/A
			Note: This value comes from the saprfc.ini file in /cgi-bin/.	
Partnership Protocols Tab—Legacy Server (MQ Series) (PNDocs.PD1stXportType=legacy-mq-series)				
Pre-Commuications Service		PNDocs.PDPre CommSVRId		N/A

Table N-1   Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(26 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Delivery Timing	Immediate	PNDocs.PDSendType	1=immediate	Object=partnership
	Scheduled		2=scheduled	Field=SendType
Queue Name		[encrypted]	QN|*QUEUENAME*; (uppercase)	N/A
Queue Manager		[encrypted]	QM|*queue manager*;	N/A
Message Header File		[encrypted]	MH|*message header file*;	N/A
Service Details Tab				
Service Name		Services.SVRName		Object=service
				Field=Name
Service Type	Executable	Services.SVRType	0=STunknown	Object=service
	Script		1=STinternal (ECXpert internal service, e.g. parse, xlat)	Field=Type
			2=STscript (ECXpert external script file)	
			3=STexe (ECXpert external executable file)	
			4=STdll (function in a shared library, e.g. DLL)	
Path Name		Services.SVRPathName		Object=service
				Field=PathName
Additional Parameters		Services.SVREntryName		Object=service
				Field=EntryName
Maximum Threads (1-99)		Services.SVRMaxThread		Object=service
				Field=MaxThread
Service Description		Services.SVRParam		Object=service
				Field=Param

Table N-1 Map of iPlanet ECXpert user interface fields to database table columns and to import fields *(27 of 27)*

UI Field	Value	Associated Database Table.Column	Values	Associated Import Object and Data Field
Service List Details Tab				
Service List Name		DTServices.DTSServiceListName		Object=servicelist
				Field=ServiceListName
Service List Data Type		DTServices.DTSTypeName		Object=servicelist
				Field=TypeName
Sending Member ID		DTServices.DTSSndrMBName		Object=servicelist
				Field=SndrMBName
Receiving Member ID		DTServices.DTSRcvrMBName		Object=servicelist
				Field=RcvrMBName
Exit Service List		DTServices.DTSErrorHandler		Object=servicelist
				Field=ErrorHandler

Glossary

997   A *confirmation message* in the *ANSI X12* standard. Comparable to the *CONTRL message* in the *EDIFACT* standard.

Administrative Interface   The component of *ECXpert* that provides access to ECXpert's administrative functions. The Administrative Interface consists of forms where users enter data to update the ECXpert *Data Store*. In ECXpert Version 3.6, the Administrative Interface is divided into two separate interfaces, the *Product Administrative Interface* and the *System Administration Interface*.

AIAG HTTP   Automotive Industry Action Group's (AIAG) industry-specific implementation of *HTTP*.

ANSI X12   The ANSI (American National Standards Institute) ASC (Accredited Standards Committee) standard for *EDI*. X12 is used widely in North America. The *EDIFACT* EDI standard is used more widely internationally.

application format   An application-specific data format for *documents*. Also referred to as a *proprietary format*.

archive   To remove *ECXpert* data from the production *Data Store* and store it in another location. Such archived data can be restored to the ECXpert Data Store if necessary.

authentication   A process in which the recipient of an electronic transmission can verify that the sender's identity is as it is represented and the data received is as it was sent.

batch processing   Business data processing in which transaction data is accumulated until some time interval has passed or some trigger volume is exceeded. The accumulated transactions are then processed in a batch. The opposite end of the processing spectrum from *real-time transaction processing*.

bundling   Combining multiple documents for transmission as a unit. Generally synonymous with *enveloping*. Functionally the reverse of *parsing*.

CA   See *certificate authority (CA)*.

card   A logical unit in the *Map Definition Tool* software that specifies the details of the *EDI translation* between a *data element* in an input format (EDI or non-EDI) and the corresponding data element in an output format (EDI or non-EDI), or vice versa.

certificate   A digital document that supports a *trading partner's* claim to ownership of a *public key*. A certificate validates a trading partner's claim that a given public key belongs to that trading partner, thus making it more difficult for a fraudulent third party to impersonate a trading partner.

certificate authority (CA)   An agency that issues certificates.

certificate revocation list (CRL)   A list of *certificate*s that have been revoked by the *certificate authority (CA)* (CA) that issued them and should no longer be accepted. If you receive a certificate revocation list (CRL), you can import it into ECXpert just as you would import a certificate from that CA. ECXpert stores it in the database and then rejects any certificate from that CA that appear on the CRL.

Communications   The component of *ECXpert* that handles all incoming and outgoing communications sessions for your ECXpert installation. In *inbound processing*, when the *submission unit* originates outside of the domain of your ECXpert installation, the Communications component receives the submission unit and writes it to a disk file. In *outbound processing*, when the submission unit originates within the domain of your ECXpert, the Transport component sends the submission unit.

Communications Agent   A subcomponent of the *Communications* component. A separate Communications Agent exists for each *communications protocol* that *ECXpert* supports. A Communications Agent simply receives data and materializes a file on the ECXpert system.

communications protocol   A standard set of rules that the systems on both the sending and receiving end follow in a communications session.

compliance   Conforming to the rules of a standard, as in *year 2000 compliance*. In *EDI*, being in agreement with the syntax rules of an EDI standard.

compliance check   Examining a *submission unit* to ensure that it is in agreement with requirements of the standard used to create it.

compression   The process of compacting data so that it is represented by fewer bytes, thereby reducing the size of the file that has to be stored on disk or transmitted over communications lines. The reverse of *decompression* or expansion.

confirmation message   A message returned to the Sender, confirming that the Receiver has received the document(s) that were sent. In the *ANSI X12* standard, this is a *997* document. In the *EDIFACT* standard, this is a *CONTRL message*.

CONTRL message   In the *EDIFACT* standard, a message sent to the sender of an EDIFACT message, acknowledging that a particular *interchange* has been received and *compliance checked*. A CONTRL message indicates the syntactical correctness of the business *documents* that have been received, informing the sender of any problems encountered. A CONTRL message does not deal with data content, which is application-specific. ECXpert supports CONTRL message at the *interchange*, *functional group*, and document levels. In *ANSI X12*, the document type that is comparable to an EDIFACT CONTRL message is called a *functional acknowledgment*.

CRL   See *certificate revocation list (CRL)*.

data delimiters   Special characters in *EDI* that mark the boundary between data elements or sub-elements. In the *ANSI X12* standard, delimiters cannot appear anywhere in the data within an interchange. In the *EDIFACT* standard, delimiters appearing in the data must be preceded by a *release character*.

data element   The basic unit of *EDI* data, roughly corresponding to a field in a database setting. Typical examples of data elements are unit price, quantity, and product code.

data element separator   See *data delimiters*.

data segment   In *EDI*, a structured sequence of *data elements*, separated by *data element separators*. A data segment is comparable to a record in a database. A data segment might also be comparable to a line item on a printed form, when similar data segments repeat within a *document*.

Data Store   The database containing all the data being processed by *ECXpert*. Separate disk files are used to store each incoming *submission unit* from a *trading partner* that has been received and each outgoing submission unit to a trading partner that is ready to be sent. Audit information is also stored separately. All other data in the ECXpert is maintained in the Data Store. All access to the Data Store is handled through application calls to the *ECXpert Data Store API*. The Data Store is similar in concept to what is commonly called a "mailbox."

decompression   The process of restoring compacted data to its original format so that it can be read and processed. The reverse of *compression*.

decryption   The process of decoding data that has been encrypted, or encoded, in such a way that it is only readable by someone who possesses a decoding key. The reverse, encoding process is called *encryption*. See also *public key encryption*.

digital certificate   See *certificate*.

Dispatcher   The component of the *ECXpert* that acts as the "traffic cop". Except for receipt of incoming data by the *Communications* component, most of the processing that occurs within ECXpert is initiated by the Dispatcher. A separate instance of the Dispatcher manages the processing of each *submission unit*. The total number of Dispatchers that are permitted to be active at one time can be set by the ECXpert site administrator.

document   A business document, such as a purchase order or an invoice. In *EDI*, a document is more narrowly defined as a collection of *data segments* with a defined structure that carries all the information necessary to complete a specified part of a business transaction. A document can also be referred to as a *message*, or a *transaction set*.

document type   A specific *EDI standard document* definition. Each EDI document type has a document type number (*ANSI X12*) or name (*EDIFACT*). Many document type numbers also have version numbers.

document tracking   Determining the current status of *documents* being processed by *ECXpert*. This is done through the Tracking tabs of the *Product Administrative Interface*.

dual certificates   In *public key encryption*, use of one *certificate* for *encryption* and another for *signing*, instead of using the same certificate for both.

ECXpert   Short name for the *iPlanet ECXpert*.

ECXpert Data Store API   The API that moves data back and forth between the ECXpert *Data Store* and the forms of the *Administrative Interface*.

EDI   Electronic data interchange. A set of standardized formats for different types of business *document* that allow otherwise incompatible business data processing systems to exchange documents without manual intervention.

EDI translation   The conversion of data in *application formats* to and from *standard EDI format*.

EDI Translator/Mapper   The component of the *ECXpert* that handles the translation of business *document* between different *application formats* and *standard EDI formats*.

EDIFACT   Electronic Data Interchange For Administration, Commerce, and Transportation. An international implementation of *EDI* sponsored by the United Nations and the European Union. The syntax rules are identified as ISO 9735. EDIFACT is widely used internationally, while *ANSI X12* is more widely used in North America.

EERP   See *end-to-end response (EERP)*.

encryption   Encoding data in such a way that it is only readable by someone who possesses a key for decoding the data. The reverse, decoding process is called *decryption*. See also *public key encryption*.

end-to-end response (EERP)   In *OFTP* transport, an end-to-end response, or EERP, notifies the original sender of a file that it has been successfully delivered to its final destination, no matter how many intermediate hops it made, or how it might have been split into multiple files or combined with other files. An EERP is an acknowledgment from the ultimate recipient that the data has been received. An EERP is comparable to *message disposition notification (MDN)* in *SMTP* transport.

envelope   In *EDI* communications, the structural and communications data added onto the basic *document*(s) that are sent as a unit. Information about the *envelope* is added at the *interchange*, *functional group* (optional in *EDIFACT*), and *document* levels.

enveloping   The *EDI* process of adding the *envelope* data, including *delimiter characters*, to basic *documents* that are sent as a unit. Usually used synonymously with *bundling*. Functionally the reverse of *parsing*.

ERP systems   Enterprise Resource Planning systems. Major data processing applications that support resource management in an enterprise. Examples include Oracle Financials and SAP.

eXML Connector   The ECXpert extension that supports *XML*.

expansion   See *decompression*.

external member   An ECXpert *member* that operates outside your ECXpert data processing domain. External members are usually other independent business entities outside of your organization. External members are often customers of or vendors to your organization.

format, proprietary   See *proprietary format*.

format, standard EDI   See *standard EDI format*.

FTP   File transfer protocol. A data communications *protocol* for transferring files directly between servers and clients over the Internet, without use of electronic mail. See also *TCP/IP*.

functional acknowledgment   In the *ANSI X12* standard (*document type 997*), a message sent to the sender of submission unit acknowledging that a particular *functional group* has been received and compliance checked. A functional acknowledgment indicates the syntactical correctness of the business *documents* that have been received, informing the sender of any problems encountered. A functional acknowledgment does not deal with data content, which is application-specific. ECXpert supports functional acknowledgment at both the functional group and *document* levels. In *EDIFACT*, the document type that is comparable to an ANSI X12 functional acknowledgement is called a *CONTRL message*.

functional group   In *EDI*, a collection of one or more *documents* that is being sent to the same *trading partner* that share a logical correlation. One or more functional groups compose an *interchange*. In *ANSI X12*, functional groups are required and each functional group must consist of documents of the same *document type* and of the same *group type* as defined by the standard (e.g., PO, IN). In *EDIFACT*, functional groups are optional and, if present, must consist of documents of the same document type.

Communications Controller   A subcomponent of the *Communications* component. The Communications Controller is a multi-threaded server, started at ECXpert startup, that is responsible for all communications between ECXpert and other systems.

GEIS FTP   A *protocol* for accessing the General Electric Information Systems (GEIS) EDI*EXPRESS service using *FTP*.

GISB HTTP   Gas Industry Standards Board (GISB) industry-specific implementation of *HTTP*.

group type   In the *ANSI X12* standard, a family of related *document types*. Most group types contain only one document type, but a few contain as many as ten or twenty.

HTTP   Hypertext transfer protocol. A set of rules for exchanging web pages on the World Wide Web. A web page can be composed of multiple files, containing both text and graphics. See also *TCP/IP*.

IFC   Internet Foundation Class. A set of libraries that must be available to your browser in order to support the Java-based *Product Administrative Interface*.

inbound processing   The flow of processing that occurs when ECXpert is receiving a *submission unit*. The reverse of *outbound processing*.

interchange   In *EDI*, the highest level of *enveloping*. An *ANSI X12* interchange is composed of one or more *functional groups*. In an *EDIFACT* interchange, functional groups are optional. A ECXpert *submission unit* can contain multiple interchanges. Transport using *SMTP* requires one interchange per message file. ANSI X12 specifies that a new interchange be created whenever any of the following changes:

- either sender ID (From) or recipient ID (To)

- *standard EDI format*

- test/production flag

- delimiter or terminator

EDIFACT specifies that a new interchange be created, in addition to the above situations, whenever the detailed routing information changes within the same recipient.

internal member   An ECXpert *member* that operates within your ECXpert data processing domain. Internal members are usually departments or other administrative units within your organization.

ISO 9735   See *EDIFACT*.

job tracking   Determining the current status of jobs managed by the *Scheduler*. This is done through the Job Tracking tabs in the *Product Administrative Interface*.

LDAP   Lightweight Directory Access Protocol. An internet standard protocol for interfacing with directories.

legacy system   A business data processing system that existed before your ECXpert was implemented and which might require data translation by ECXpert. In ECXpert 3.6, the legacy systems that you can integrate with ECXpert are Oracle Financials, SAP, and MQSeries.

manifest   The list of documents contained in a *submission unit*.

map   A specification of the way in which *data* in one format, such as an *standard EDI format*, must be transformed into another format, such as an *application format*.

map, ECXpert-cooperative   In *outbound processing*, a *map* that allows the outbound submission unit to be constructed *document* by document in separate files. The documents can then be bundled by recipient and transmitted directly to their respective recipients. This feature requires the application producing the outbound submission unit to place a header and trailer around each logical document.

Map Definition Tool   The ECXpert program used to create a *map file* that the *Map Execution Engine* can use. *Maps* from other sources, such as maps that have been in use by *legacy systems*, have to be reconstructed through the *Map Definition Tool* in order to be used by ECXpert.

Map Execution Engine   The ECXpert program that uses a map file created by the *Map Definition Tool* to translate documents from an *application format* to a *standard EDI format*, or from a standard EDI format to an application format.

map file   A file supplied by the user that contains *map* information.

mapping   The process of specifying the way in which *data* in one format, such as an *standard EDI format*, must be transformed into another format, such as an *application format*.

MD5   Message digest (MD) hashing algorithm. Hashing algorithms are a key component of *public key encryption*. MD5 is a revision earlier of versions that improves the level of security. The MD5 algorithm is slightly faster than *SHA-1*, but it is less secure.

MDN   See *message disposition notification (MDN)*.

member   A participant in your ECXpert system that is fully defined using the *Administrative Interface*. A member is a data processing system and/or an individual that sends or receives business documents through your ECXpert. *Internal member* operate within your ECXpert data processing domain. *External members* operate outside your ECXpert data processing domain. *Trusted members* act as agents for others and handle data validation for those they represent. Specific *trading address* are assigned to individual members, and can only be assigned to a single member.

Mercator   The *Map Definition Tool* that is bundled with ECXpert, developed by TSI International. It can produce *map files* that translate from any supported format to any other supported format: EDI to application, application to EDI, EDI to EDI, and application to application.

message   See *document*.

message disposition notification (MDN)   In *SMTP* transport, a process that provides a series of notifications to the sender of a *submission unit* about its current status as it is being received by the Communications Controller. The *Communications* component provides MDN to reliably track delivery of a *submission unit* using Internet mail. MDN supplements the *functional acknowledgment* of *ANSI X12*, or the *CONTRL message* of *EDIFACT*, but does not replace either.

MIME   Multi-purpose internet mail extensions. The standard Internet protocol that lets users exchange application-specific file formats using Internet email. Web servers and clients use the data type specified in the MIME header that is inserted at the beginning of any Web transmission with an appropriate receiver application. The MIME specification is an amendment to the original SMTP mail protocol. The *S/MIME* specification adds security functions to MIME.

multiple body parts   The ECXpert feature that allows structured business documents to be accompanied by attached application-specific data files of any defined format. For example, an EDI request for quote might be accompanied by a CAD file containing related engineering drawings and a spreadsheet file that can be used as a worksheet in generating the quote. ECXpert treats each "body part" as

a separate *submission unit* with its own *tracking ID* and *service list*. ECXpert cross-references all related body parts and none are sent until all have completed processing. Currently *SMTP* is the only protocol that can support this feature. The `multi_part` parameter in the `commsmtp-send` section of the system settings must be set to true to enable ECXpert to send multiple body parts. No special settings are required for ECXpert to be able to receive them.

OBI   Open Buying on the Internet. An Internet standard providing for support of purchase transactions over the Internet. OBI is based on current standards, including *SSL* for secure Internet communications, HTML for content display, SET for credit card transactions, and X.509 for *certificates*.

Odette FTP (OFTP)   Organisation for Data Exchange by Tele Transmission in Europe ("Odette") file transfer protocol, originally developed for the European auto industry. OFTP is not a variation of *FTP*, but a completely separate protocol.

OFTP   See *Odette FTP (OFTP)*.

outbound processing   The flow of processing that occurs when ECXpert is sending a *submission unit*. The reverse of *inbound processing*.

parsing   The process of breaking out all the data components of a *submission unit*. Functionally the reverse of *bundling* or *enveloping*.

partnership   See *trading partnership*.

partnership, reverse   See *reverse partnership*.

pass-through   Use of ECXpert as a simple gateway through which documents are passed without *parsing* or translation.

poll command   The ECXpert utility that polls a specified port or file location for the presence of data. When found, it initiates ECXpert processing of a *submission unit* by ECXpert.

primary service   A *service* that is internal to the ECXpert, available as soon as the software is installed. Primary services process all *documents* within a *submission unit* the same way. Examples of primary ECXpert services are *parsing*, translation, and *functional acknowledgment* generation. You can create *user-defined services* to supplement ECXpert's primary services.

private key   The key belonging to an intended message recipient that is never published. The message sender uses the intended recipient's *public key* to encrypt the message. A message encrypted using the intended recipient's public key can only be decrypted using the intended recipient's private key.

Product Administrative Interface   In *ECXpert* Version 3.6, the portion of the *Administrative Interface* that handles normal system functions involving maintenance of the information infrastructure that supports the automated processing of business *document*s in ECXpert. Setting up users, trading partnerships, and EDI parameters are typical routine administrative functions. System administration functions in Version 3.6 are handled by the *System Administration Interface* portion of the *Administrative Interface*.

proprietary format   An application-specific data format for *documents*. Also called an *application format*.

protocol   A special pre-defined set of communication rules that both the sender and receiver in a telecommunication connection agree to use in a communication. The Internet is supported by the *TCP/IP* family of protocols.

public key   The published key belonging to an intended message recipient. The message sender uses the intended recipient's public key to encrypt the message. A message encrypted using the intended recipient's public key can only be decrypted using the intended recipient's *private key*.

public key encryption   An *encryption* method in which sender and receiver each have two keys, one public and one private. The *public key* is published as widely as necessary so that anyone can determine with certainty the correct public key for a given trading partner. The relationship between a trading partner's public and private keys is such that a message encrypted by the public key can only be correctly decrypted using the *private key*.

qualifier   In *EDI*, a code at the beginning of a *data element* that specifies how the data in the remainder of the field is to be interpreted. The *trading address qualifier* is the one you encounter most frequently in the ECXpert *Administrative Interface*.

real-time transaction processing   Business data processing in which data for a transaction is processed as soon as it is received. The opposite end of the processing spectrum from batch processing.

release character   In the *EDIFACT* standard, a character that is used to restore a character to its original meaning when it has been specified as a *data delimiters*. A release character allows a data delimiter to appear within the data.

reverse partnership   A *trading partnership* automatically created by ECXpert when the original partnership is set up to have ECXpert generate a *confirmation message*; either a *functional acknowledgment* (*ANSI X12* document type *997*) or a *CONTRL message* (*EDIFACT*). The reverse partnership is required to support the exchange of the these messages. ECXpert automatically creates the reverse partnership for you when you request a confirmation message for a partnership. In order for the confirmation messages to be processed correctly, you must edit the reverse partnership and specify appropriate *envelope* and *protocol* information. Also the service list for the original partnership must contain FAGen.

A reverse partnership reverses the Sender and Receiver information from the original partnership, using the same EDI standard and version. The Partnership Type is Application to EDI. The Document Type is *997* for ANSI X12 or CONTRL for EDIFACT. Multiple partnerships with the same Sender and Receiver, but with different Document Types, all share the same reverse partnership.

A reverse partnership is also required to support end-to-end response (EERP) under Odette FTP, but ECXpert does not create it for you automatically.

scheduled service list   A *service list* for which processing is time-based, triggered by the *Scheduler*.

Scheduler   The component of *ECXpert* that manages scheduling of time-based processing.

scenario   A specific example that illustrates a way in which *ECXpert* can be used.

segment   See *data segment*.

segment terminator   In *EDI*, A special character that is used to mark the end of a *data segment*.

System Administration Interface   In *ECXpert* Version 3.6, the portion of the *Administrative Interface* that handles system administration functions, such as configuring the system, starting and stopping ECXpert servers, and setting up time-based processing jobs. Maintenance of the information infrastructure that supports the automated processing of business *document*s in ECXpert is handled through the *Product Administrative Interface* portion of the *Administrative Interface*.

service   A specific action that can be performed on a *submission unit*, or a subset of *documents* in the *submission unit*, which changes, moves, or copies the data. A service is an external executable file. *ECXpert* provides internal, or *primary services*, and supports external, or *user-defined services*.

service list   A list of *services* that are to be performed in sequence on a *submission unit*. Service list processing is managed by the *Dispatcher*.

service list, scheduled   See *scheduled service list*.

service, primary   See *primary service*.

service, user-defined   See *user-defined service*.

session   The entire sequence of *ECXpert* processing of a *submission unit*, including the communications session in which it is received or sent.

SHA-1   Secure hashing algorithm (SHA). Hashing algorithms are a key component of *public key encryption*. SHA-1 is a revision of SHA that corrects a flaw in the original algorithm. The SHA-1 algorithm is slightly slower than *MD5*, but it is more secure.

signing   Use of a certificate for *authentication* of the sender of an electronic transmission.

site administrator   The person with primary responsibility for ongoing operation of your *ECXpert* installation. This person might also be referred to as the system administrator.

S/MIME   Secure multi-purpose internet mail extensions. An extension to the *MIME* protocol that adds encryption, decryption, and authentication to prevent unauthorized recipients from being able to make use of the information.

SMTP   Simple mail transport protocol. The standard Internet protocol under which electronic mail is transmitted.

SNMP   Simple network management protocol. A set of rules governing the management of networks and the monitoring of network devices and functions. SNMP is used in conjunction with *TCP/IP*, although it has evolved independently.

SSL   Secure sockets layer. Netscape Communications Corporation's public key encryption and authentication software that can be used with *HTTP*.

standard EDI format   A specific standard format for *documents* defined under *EDI*.

Submission Agent   The *Communications Controller* calls a Submission Agent and passes it the output of the *Communications Agent*. The Submission Agent writes the file to a disk, and submits the file to the ECXpert *Dispatcher* for processing.

submission unit   A collection of one or more business *documents* that is processed as a unit by the *ECXpert*. In *inbound processing* a submission unit is received from an *external member* and passed on to an *internal member*. In *outbound processing* a submission unit from an internal member is sent to an external member. ECXpert allows a submission unit to be composed of whatever combination of data is required by the internal and external members that are involved. With *SMTP* transport, the *EDI* component of a submission unit must be composed of a single *interchange* sent to a single *trading partner*.

submit command   An ECXpert command line utility that can be used to present a *submission unit* to the ECXpert for processing.

syntax (EDI)   The rules governing structure of *documents* transmitted under *EDI*, including the following:
- valid data types and relationships within a *data segment*
- valid order, position, and frequency of repetition of data segments in a document
- organization of documents composing *functional groups* and *interchanges*

TCP/IP   Transmission Control Protocol/Internet Protocol. The primary Internet *protocols* which govern the exchange of messages between Internet points at the information packet level and the Internet address level.

tracking ID   The unique identifier that ECXpert generates and assigns to all *documents* in a *submission unit* so that all pieces of the submission unit can be tracked to completion of processing.

trading address   A unique identifier for a *trading partner*. A trading address *data element* consists of a *trading address qualifier* and the actual ID.

trading address qualifier   The first characters of a trading address *data element*, the value of which specifies how the remainder of the trading address is to be interpreted. For example, in *ANSI X12* '12' indicates a phone number, while '01' indicates a Duns number, and 'ZZ' indicates a unique, mutually agreed upon ID established in a *trading partner agreement*.

trading partner   Either one of the two *members* involved in a *trading partnership*.

trading partner agreement   A contractual agreement between two business parties that specifies all legal and business requirements that are to be met when exchanging *EDI* transmissions.

trading partnership   The set of data defining a relationship between an external trading partner and an internal trading partner on your ECXpert.

transaction set   See *document*.

trusted member   A *member*, such as a *VAN*, who acts as an agent for other *trading partners*, sending *documents* on their behalf. A trusted member assumes the responsibility for validation of *trading addresses* referenced in documents sent on behalf of others.

user-defined service   A *service* that a ECXpert user defines to perform processing that is not provided by a *primary service*. User-defined services are defined by creating an executable program that uses the *ECXpert Data Store API* to access the *Data Store*. Examples of user-defined services are encryption/decryption, compression/decompression, and data moving/copying.

VAN   Value-added network. A third-party communications service that handles large volumes of *EDI* transmissions for its clients.

X12   See *ANSI X12*.

XML   eXtensible Markup Language. A web standard defining an extensible markup language that can be used to encode complex document data. See also *eXML Connector*.

year 2000 compliance   Being able to correctly process dates in different centuries. Much of the early software developed in the 1950's and '60's processed dates using only the last two digits of the year, which would not allow correct computation of the elapsed time between years beginning with 19 and years beginning with 20. Software such as *ECXpert* that is "year 2000 compliant" processes dates using all four digits of the year.

Index

O

P

R

T

Section **Y**